أكاديمية التعلم
Academy Of Learning

مراجعة للاختبار الشامل

دبلوم الأمن السيبراني

الفهرس

ما هو الاختبار الشامل؟

هو اختبار تعقده المؤسسة العامة للتدريب التقني والمهني للمتدربين للذين أنهوا متطلبات البرنامج التدريبي أو الدبلوم بنجاح لكافة منشآت التدريب الأهلية المرخص لها بمزاولة النشاط التدريبي في مجال البرامج التدريبية والدبلوم.

تعليمات الاختبار الشامل

كما هو موضح في موقع المؤسسة العامة للتدريب التقني والمهني

1. يشترط لدخول المتدرب الاختبار الشامل إنهاء متطلبات الخطة التدريبية واجتياز جميع اختبارات الفترات التدريبية وحصوله على معدل تراكمي لا يقل عن 2 من 5.
2. يتم تسجيل المتدربين الذين يحق لهم دخول الاختبار الشامل على موقع الإدارة العامة للتدريب الأهلي على الانترنت من قبل المنشأة التدريبية بعد أخذ موافقتهم الخطية لدخول الاختبار ورفع سجلاتهم التدريبية وفق المواعيد والطريقة التي تحددها المؤسسة.
3. يشترط لاجتياز الاختبار الشامل حصول المتدرب على 60% من درجة الاختبار.
4. تتكون نتيجة الاختبار الشامل من جزأين: 70% من درجة الاختبار و30% من درجة المعدل التراكمي.
5. ترصد نتيجة الاختبار الشامل في شهادة المتدرب ويتم تحديد التقدير بناءً على هذه النتيجة.
6. بعد اجتياز المتدرب الاختبار الشامل الذي تعقده المؤسسة تصدر المنشأة التدريبية للمتدرب شهادة اجتياز البرنامج التدريبي أو الدبلوم والسجل التدريبي وتصدق من المؤسسة.
7. كل متدرب يغش أو يحاول الغش أو يخالف تعليمات وقواعد الاختبار يعتبر راسباً في الاختبار الشامل.
8. يحق للمتدرب في حال رسوبه أو غيابه عن الاختبار الشامل أو في حال رغبته تحسين تقديره (للحاصلين على تقدير مقبول فقط) طلب إعادة الاختبار الشامل حسب المواعيد المحددة للاختبار الشامل بعد سداد أجر قدره 100 ريال.

للتنويه تم إعداد هذه المراجعة لتلخيص بعض المواد التي تم دراسته في **دبلوم الأمن السيبراني**، وذلك حرصاً من معهد أكاديمية التعلم على منح طالبات المعهد وسيلة تمكنهم من استرجاع معلوماتهم خلال فتره دراستهم بالمعهد، ولضمان النجاح في اجتياز الاختبار الشامل يجب الرجوع للمنهج العلمي الخاص بكل مادة والتي سبق ودرستها الطالبة.

ملخص لمقرر أساسيات التشفير

الفصل الأول
مقدمة في التشفير

- **مصطلحات مهمة في التشفير:**

- التشفير (Encryption): هو عملية تحويل البيانات من شكلها الطبيعي المقروء إلى شكل غير مفهوم وغير واضح.
- فك التشفير(Decryption) : عكس عملية التشفير وهو تحويل البيانات من شكلها غير المفهوم والغير واضح الى شكلها الطبيعي المقروء.
- النص الواضح(Plain text) : هي المعلومات السرية التي نريد حمايتها (تعميتها) (النص الأصلي).
- النص المشفر(Cipher text) : رسالة غير واضحة وغير مفهومة النص الذي تم تشفيره
- مفتاح التشفير(Encryption Key) : يقوم مفتاح التشفير بقفل وإلغاء قفل الخوارزمية مما يسمح بتشغيل عملية التشفير أو فك التشفير.
- مدخلات عملية التشفير: النص الواضح(Plain text) + المفتاح (Key) والناتج النص المشفر (Ciphertext).
- مدخلات عملية فك التشفير: النص الغير واضح المشفر(Ciphertext) +المفتاح (Key) والناتج النص الواضح (Plain text).

- مميزات التشفير

- السرية: وهي لا يمكن الوصول للمعلومات إلا من قبل الشخص المقصود بها ولا يمكن لأحد غيره
- المصادقة: يتم التأكد من هوية المرسل والمستقبل وكذلك مصدر المعلومات .
- ا لنزاهة: لا يمكن تعديل المعلومات في التخزين أو الانتقال بين المرسل والمستقبل .
- تم استخدام التشفير بكثرة من العرب في وقت الحروب .

- أنواع التشفير:

ينقسم التشفير الى نوعين أساسية وهي التشفير المتماثل أو (المتناظر) وغير المتماثل أو (غير المتناظر).

- التشفير المتماثل او المتناظر (Symmetric Encryption): هو أسلوب من أساليب التشفير يستخدم فيه نفس المفتاح لتشفير الرسائل وفك تشفيرها. (عدد المفاتيح: واحد فقط)

- التشفير غير المتماثل او غير المتناظر (Asymmetric Encryption): هو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر، ولهذا السبب سمي

بالتشفير غير المتناظر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير، وبالتالي فإنه يسمح بتوزيع صلاحيات التشفير وفك التشفير على الجهات المختلفة بأن يعطي لبعضهم مفاتيح التشفير فقط ويعطي للآخرين مفاتيح فك التشفير.(عدد المفاتيح: اثنان فقط)

- المفتاح العام Public key:

المفتاح العام الذي يستخدم لتشفير الرسالة، ويتم أرساله لمن تريد (شخص، مجموعه)

- المفتاح الخاص Private key :

المفتاح الخاص الذي يستخدم لفك التشفير تحتفظ به في جهازك الخاص، ولا يمكن فك الشفرة عن الرسالة الا عن طريق المفتاح الخاص فقط، فإذا ضاع المفتاح الخاص فلا يمكنك فك التشفير عن الرسالة

- تنقسم المعلومات السرية الى نوعين:
- سرية فردية تشمل الفرد نفسه فقط مثل: كلمة السر – المذكرات الشخصية – رقم الحساب البنكي .
- سرية جماعية تشمل شخصين فأكثر مثل: المراسلات الدبلوماسية – الخطط العسكرية .

- للحفاظ على أمن التشفير نزيد من طول حجم المفتاح السري مثال: المفتاح 1234 أقل أمان من المفتاح 12734761684634794778923478923478923478954789345789
- لتحقيق امن المعلومات يتم استخدام تقنيات مثل التعمية Cryptography والتوريةSteganography

- من الوسائط التي تستخدم في التورية لإخفاء المعلومات: الملفات الصوتية، الملفات النصية، الصور، الفيديو
- في دراسات علم التشفير دائما ما نستخدم بعض الأسماء للدلالة على:
  - اسم المرسل Alice, A >
  - اسم المستقبل Bob ,B>
  - اسم العدو Eve>

الفصل الثاني
التشفير المتماثل وسرية الرسائل

- في التشفير المتماثل يتم اتباع طريقتين لتحقيق التشفير وهي الاستبدال او المناقلة:
- مثال على التشفير المتناظر خوارزمية DES
- التشفير بالاستبدال:

يهدف هذا الأسلوب من التشفير إلى استبدال رمز بآخر :

- إذا كانت الرموز عبارة عن خانات الأحرف يمكن استبدال Z بالحرف D ،T بالحرف A.
- إذا كانت الرموز عبارة عن خانات عددية (0-9) فيمكن استبدال 3بـ 7, و2بـ 6 وهكذا

- تنقسم طرق الاستبدال الى وحيدة الحروف ومتعددة الحروف
- وحيدة الحرف (كل حرف يقابله حرف واحد مثلا A>T وعلاقتها تكون One-to-One)
- متعددة الحروف (الحرف الواحد يقابله عدة أحرف مثلا A>VGHFU وعلاقتها تكون One-to-Many)

- التشفير بالمناقلة: يتم تدوير حروف النص غير المشفر ضمن جدول بحيث تملئ خانات الجدول سطرًا فسطر ويجري ارساله(تشفيره) عمودًا فعمود.

- مثال: يمكن للطرفين أن يتفقا حول عدد الأعمدة ضمن الجدول الذي يجري ملئه قبل ارسال الرسالة. ثم يجري نقل الرسالة عمود فعمود.
- أما الطرف المستقبل للرسالة فإنه يتبع الخطوات المعاكسة لعملية الإرسال لفك تشفير الرسالة، حيث يقوم بكتابتها ضمن الجدول عمود فعمود، ثم يقرأها سطرًا فسطر.

m	E	e	T
m	E	a	T
t	H	e	P
a	R	k	

- تمت الكتابة (تعبئة الجدول بطريقة سطر سطر او بشكل أفقي)

- تم التشفير (بأخذ الاحرف بطريقة عمود عمود أو بشكل عمودي)
- لنحصل على الرسالة المشفرة MMTAEEHREAEKTTP

- خوارزمية DES

تعرف خوارزمية DES(Data Encryption standard) بأنها خوارزمية تشفير متناظر المفتاح.

- بنية الخوارزمية: تجري عملية التشفير بواسطة صندوقي تدويرP-Boxes و 16 جولة تشفير تستخدم كل جولة مفتاحًا مختلفًا بطول 48 خانة(بت).
- طريقة عمل الخوارزمية تتلخص في 4 خطوات:

يتجزأ النص الواضح (Plain text) الى كتل (Blocks) من طول 64 خانة(بت)

- ال 64 بت كتلة (block) تدخل في التدوير الأولي (initial permutation) (IP) باستعمال جدول التدوير الاولي
- بعد ذلك ال 64 بت كتلة (block) ينقسم الى جزأين مكون من 32 بت Right (R) ,left (L) القيم الابتدائية لهما هي L0 ,R0
- توجد هناك 16 جولة (round) من العمليات .
- فك التشفير في خوارزمية DES :

عند التشفير يوجد مفتاح لكل جولة (الجولة الأولى لديها مفتاح تشفير رقم 1) وعند فك التشفير نقوم بعكس ارقام المفاتيح مع الجولات بحيث تكون الجولة الأولى من فك التشفير لديها مفتاح فك تشفير رقم 16 والجولة الثانية من فك التشفير لديها مفتاح فك تشفير رقم 15 وهكذا.

- خوارزمية AES

تعرف خوارزمية AES (Advanced Encryption Standard) بالقدرة على التعامل مع كتل بحجم 128بت ويقوم باستخدام 10 أو 12 أو 14 جولة وذلك تبعًا لطول المفتاح المستخدم والذي يمكن أن يكون 128 أو 192 أو 256بت على التوالي

- تستخدم خوارزمية AES أربعه أنواع من التحويلات للتشفير وهي :

1. الاستبدال (SubBytes)

Nr	Key size
10	128
12	192
14	256

2. التدوير (ShiftRows)
3. الخلط (MixCoulmns)

4. إضافة مفتاح (AddRoundKey)

- عند فك التشفير، يجري التعامل مع تحويلات معاكسة للتحويلات السابقة، وهي:

1. InvShiftRows
2. InvSubByte
3. InvMixColumns
4. AddRoundKey

- نلاحظ انها مثل التحويلات في التشفير، ولكن معاكسة وذلك لان عملية التشفير وفك التشفير عمليتان عكسيتان.

الفصل الثالث والرابع
التشفير غير المتماثل والتشفير بالمفاتيح العامة وتوثيق الرسائل

- تكامل الرسائل: يمكن الحفاظ على تكامل المعطيات من خلال البصمة المرتبطة بها للحفاظ على محتوياتها بواسطة توابع تهشير Hash Functions
- حل بعض المشاكل الامنية باستعمال تكامل الرسائل:

- تساعد تقنية تكامل الرسائل على حل المشاكل التالية:
- تعديل المحتوى:

  عند تعديل محتوى رسالة سيؤدي ذلك إلى تعديل المحتوى توليد بصمة الكترونية مختلفة عن بصمتها السابقة وبالتالي سيتم اكتشاف عملية التعديل بسهولة.
- تحديد الهوية:

  لا يمكن لطرف ثالث أن يرسل رسالة مزورة لأنه لا يمكن له توليدها وفقًا لبصمة الرسالة الأصلية.
- تعديل الوقت:

  يمكن للمرسل أن يضيف إلى رسالته ختم زمني بحيث لا يمكن لأي طرف ثالث تعديل الرسالة وتوليد بصمة الكترونية لها مماثلة للرسالة الأصلية.
- من استعمالات توثيق الرسائل حماية المعلومات.
- مصطلح الطرف الثالث بناء على نوع المفاتيح المستعملة في التشفير المفاتيح غير المتماثلة او غير المتناظرة

  Center Certificate Authority (CCA) سلطة التراخيص
- مصطلح الطرف الثالث بناء على نوع المفاتيح المستعملة في التشفير المفاتيح المتماثلة او المتناظرة

  Key Distribution Center (KDC) مركز توزيع المفاتيح

- لتوثيق الرسائل يتم التعامل مع الاكواد التالية:

- كود التقاط التعديل MDC يعمل على تحديد فيما إذا عدلت الرسالة أم لا.
- كود هوية المرسل MAC يعمل على تحديد هوية المرسل .

- التوقيع الرقمي كالتوقيع المكتوب يستخدم للمصادقة على صحة مضمون الملف الموقع عليه والذي يسمى عادة الرسالة. يمكن أن تكون هذه الرسالة على شكل بريد إلكتروني أو عقد معين أو حتى رسالة معقدة مرسلة ببروتوكول معين.

- خطوات الية عمل التوقيع الرقمي :

1. ادخال الملف في دالة التهشير (Hash function) بعد ذلك نأخذ ناتج التهشير .
2. ادخال ناتج التهشير في عملية التشفير باستخدام المفتاح الخاص للمرسل .
3. يتم دمج ناتج عملية التشفير وهو التوقيع الرقمي مع الملف المراد ارساله.

الأسئلة

1. في خوارزمية ال DES يتجزأ النص الواضح (Plain text) الى كتل (Blocks) من طول:			
60 بت	61 بت	64 بت	70 بت
2. في خوارزمية ال DES ال 64 بت كتلة (block) ينقسم الى جزأين مكون من:			
65 بت	32 بت	70 بت	40 بت
3. خوارزمية ال DES تمر بـ 16 جولة في كل جولة تستخدم مفتاح بطول .... خانة.			
16	1	5	48
4. في التوقيع الرقمي يتم تشفير مخرج تابع التهشير (Hash function)باستعمال(جهة المرسل)			
المفتاح العلني	المفتاح العام	الخاص	المفتاح المتماثل
5. تشفير كلمة WELCOME CYBER باستعمال تشفير المناقلة بدون مفتاح حيث عدد الأعمدة 3وتمت الكتابة سطر سطر هو:			
WCEBEOCELMYR	XCEBEOCELMYR	A. WCDBEMNELMYR	CEBEOCELMYR
6. يستخدم للمصادقة على صحة مضمون الملف الموقع عليه			
كود الاتصال	التوقيع الرقمي	كود التقاط التعديل	كود الرسالة
7. في توثيق الرسائل الكود الذي يعمل على تحديد فيما إذا عدلت الرسالة أم لا:			
MDCكود التقاط التعديل	MACكود هوية المرسل	MVCكود الشبكة	MWEكود التحرير
8. مصطلح الطرف الثالث بناء على نوع المفاتيح المستعملة في التشفير المفاتيح غير المتناظرة:			
lDigital Signature لتوقيع الرقمي	Key Distribution Center (KDC)مركز ت المفاتيح	Center Certificate Authority (CCA)سلطة التراخيص	التحويل التلقائي
9. المشفرات متعددة الحروف علاقتها تكون :			
One-to-Many واحد لأكثر	One-to-Oneو احد لواحد	Many-to-Many كثير لكثير	Two-to-twoاثنين لاثنين
10. استبدال رمز باخر في التشفير يعرف ب :			
التشفير بالاستبدال	التشفير بالمناقلة	التشفير المتعدد	التشفير الثنائي
11. تمر خوارزمية ال DES بصفة عامة تجري عدد معين من الجولات وهو			
14جولة	12جولة	16جولة	18جولة
12. عكس عملية التشفير تعرف ب:			
فك التشفير	فك التحويل	فك الخوارزميات	فك المفاتيح
13. عملية تحويل البيانات من شكلها الطبيعي إلى شكل غير مفهوم تعرف ب:			

التشفير	الخوارزميات	النص الواضح	التحويل
14. تسمى المعلومات السرية التي نريد حمايتها (تعميتها):			
النص الواضح	النص المشفر	التشفير	فك التشفير
15. لفك تشفير خوارزمية ال AES يتم استخدام التحويلات المعاكسة ومنها :			
Mix Column	ShiftRows	InvSubByte	SubByte
16. في خوارزمية ال AES في حالة كان حجم المفتاح 128 بت تصبح عدد الجولات :			
14جولة	10جولات	16جولة	20جولة
17. كلما كان طول مفتاح التشفير أطول :			
تزيد قوة امان التشفير	تنقص قوة امان التشفير	لا تتأثر قوة امان التشفير	تنقص قوة امان التشفير بنسبة بسيطة
18. استخدم العرب التشفير بكثرة حينها في:			
في الحروب وذلك خوفاً من وقوع الرسائل في يدي العدو	في القصائد الشعرية	في السفر	في الحياة اليومية
19. لا يمكن الوصول للمعلومات إلا من قبل الشخص المقصود بها ولا يمكن لأحد غيره يعرف هذا ب			
السرية	النزاهة	المصادقة	عدم التنصل
20. في دراسات علم التعمية دائما نستخدم اسم Eve للدلالة على:			
اسم العدو	اسم المرسل	اسم المستقبل	اسم الشبكة
21. يتم التأكد من هوية المرسل والمستقبل وكذلك مصدر المعلومات:			
السرية	النزاهة	المصادقة	عدم التنصل
22. مدخلات (عملية التشفير) (Encryption function):			
النص المشفر، المفتاح.	النص الواضح، المفتاح	النص الواضح، النص المشفر.	المفتاح العلني، المفتاح العام
23. (عملية فك التشفير) (Decryption function)مدخلات:			
النص المشفر، المفتاح.	النص الواضح، المفتاح.	النص الواضح، النص المشفر.	المفتاح الخاص
24. المشفرات وحيدة الحرف علاقتها تكون :			
One-to-Many	One-to-One	Many-to-Many	Two-to-twoاثنين لاثنين
25. تساعد تقنية تكامل الرسائل على حل بعض من المشاكل منها :			
عدم تحديد الهوية	تعديل المحتوى	التقاط كود هوية الرسالة	التقاط كود الشبكة

.26 في دراسات علم التعمية دائما نستخدم اسم Alice للدلالة على :			
اسم العدو	اسم المرسل	اسم المستقبل	اسم الشبكة
.27 في دراسات علم التعمية دائما نستخدم اسم Bob للدلالة على :			
اسم العدو	اسم المرسل	اسم المستقبل	اسم الشبكة
.28 لا يمكن تعديل المعلومات في التخزين أو الانتقال بين المرسل والمستقبل يعرف ب:			
السرية	النزاهة	المصادقة	عدم التنصل
.29 من استعمالات توثيق الرسائل:			
حماية المعلومات الحساسة	حماية اسم المرسل	حماية الشبكة	حماية الانترنت
.30 في التشفير غير المتماثل يتم استخدام عدد معين من المفاتيح للتشفير وفك التشفير وهو :			
4مفاتيح	مفتاحين	مفتاح واحد	7مفاتيح
.31 تضمن البصمة الالكترونية تكامل الرسالة وعدم تعديلها			
صح	خطأ		
.32 الكود المستعمل في التحقق من هوية المرسل هو MAC			
صح	خطأ		
.33 المفتاح العام : هو الذي يستخدم لتشفير الرسالة، ويتم أرساله لمن تريد (شخص , مجموعه)			
صح	خطأ		
.34 مثال على التشفير المتناظر خوارزمية RSA			
صح	خطأ		
.35 تعتمد أساليب التشفير بمفتاح متناظر على وجود 5 مفاتيح			
صح	خطأ		
.36 لتحقيق امن المعلومات يتم استخدام تقنيات مثل التعمية Cryptography والتورية Steganography			
صح	خطأ		
.37 النص المشفر" Ciphertext" هو رسالة واضحة يمكن لأي شخص قراءتها			
صح	خطأ		
.38 من الوسائط التي تستخدم في التورية لإخفاء المعلومات: الملفات الصوتية			
صح	خطأ		
.39 المعلومات السرية الجماعية هي المعلومات السرّية المتعلّقة بأكثر من طرف واحد			
صح	خطأ		
.40 يقوم مفتاح التشفير : بقفل وإلغاء قفل الخوارزمية مما يسمح بتشغيل عملية التشفير أو فك التشفير.			
صح	خطأ		

ملخص لمقرر نظم التشغيل (1)

الفصل الأول
نظام تشغيل الشبكات

- يوجد إصدارين من أنظمة الشبكات، وهي:

Standard: متاح لك بشكل قانوني أن تُنشئ جهازين وهميين، أي أن عدد الـ VM (virtual Machin) التي تسمح بها مايكروسوفت لهذا الإصدار 2 فقط.

Datacenter: مُتاح لك إنشاء عدد لا محدود من الأجهزة الوهمية.

- تصحيحات وأدوات الإدارة المتاحة في نظام windows:

Active Directory best practice analyzer: تقوم هذه الأداة بتحليل اعدادات الدليل النشط وبقية الإعدادات الأخرى لفحص فيما إذا كانت تلك الإعدادات تطابق أفضل مقاييس الممارسات التي توصي بها مايكروسوفت.

Active Directory Explorer: برنامج مشاهدة وتحرير للدليل النشط، يسمح بمشاهدة قاعدة بيانات الدليل النشط الخاص بالويندوز سيرفر.

Viewfinity local admin discovery: تسمح بعمل مسح شامل لكل مستخدمي الشبكة لمعرفة أي منهم يمتلك صلاحيات المدير، لإلغاء أي صلاحيات او امتيازات يتمتع بها أي مستخدم لا يستحقها تجنبًا لحصول اختراقات أمنية.

Remote Desktop Manager: تسمح بجمع الكثير من أنواع الاتصال عن بُعد بشكل مركزي مع كلمات المرور الخاصة بها وصلاحيات المعدات المختلفة.

- بيئة تنفيذ الأوامر PowerShell:

- عبارة عن بيئة مُحدثة لتوجيه الأوامر. تدعم تنفيذ أكواد برمجية جاهزة "Scripts" تم كتابتها بأكثر من لغة برمجية. تتفوق بيئة الأوامر PowerShell على بيئة الأوامر cmd عند مقارنتها بها.
- مُعظم أوامر PowerShell تأتي بصيغة التالية: (verb-noun). حيث يكون الجزء الأول من الأمر على شكل فعل باللغة الإنجليزية مثل "get" أو "stop". والجزء الثاني عبارة عن اسم مفعول به مثل "command" أو "service" ويفصل بينهما علامة (–)

على سبيل المثال: get-command

الفصل الثاني
خدمات المجال للدليل النشط AD DS

- الدليل النشط Active Directory:

عبارة عن قاعدة بيانات مشتركة. الغرض الرئيسي من الدليل النشط هو توفير خدمات مركزية لتحديد الهوية، والتوثيق لشبكة من الحواسب التي تستخدم نظام تشغيل ويندوز، والسماح لمسؤولي الشبكات بتوزيع البرمجيات وتثبيت التحديثات.

الدليل النشط يُعد مصدر للمعلومات، إذ يحوي معلومات حول الكائنات الهامة كالخوادم والمستخدمين والملفات.

- المتحكم بالمجال Domain Controller:
- أحد الخدمات التي أنشأتها مايكروسوفت. وهي عبارة عن مجموعة من الخوادم "Servers" ومحطات العمل التي تتفق فيما بينها على حفظ وإدارة أسماء وكلمات مرور حسابات المستخدمين والأجهزة في قاعدة بيانات مشتركة يُطلق عليها الدليل النشط.
- مكونات المتحكم بالمجال:

1. كائن Object: أي مُدخل موجود داخل الدليل النشط، له خصائص معينة مثل حسابات المستخدمين، الأجهزة، الطابعات... إلخ.

يتم تصنيف الكائن إلى 3 مجموعات وهي: الموارد، الخدمات، المستخدمين.

ما المقصود بالموارد؟

المعلومات المخزنة بالنظام، وحدة المعالجة المركزية CPU ، القرص الصلب... إلخ.

2. النطاق Domain: عبارة عن مجموعة من أجهزة ومستخدمين مرتبطة فيما بينها، تتشارك في بعض الخصائص المشتركة ولها قاعدة بيانات واحدة.

يحتوي الدليل النشط على نطاق واحد أو أكثر.

3. الشجرة Tree: مجموعة من النطاقات المرتبطة فيما بينها والتي تتكون من نطاق الأب ونطاق الطفل، أي يُمكن تمثيلها بعلاقة (الأب والأبناء).

4. الغابة Forest: تُعد أكبر محتوى من محتويات الدليل النشط، وتُمثل مجموعة الأشجار والنطاقات التي تتشارك في المميزات والخصائص. وتربطها علاقة ثقة ثنائية الاتجاه.
5. الوحدات التنظيمية Organizational units: مجموعة كائنات تعمل على تنظيمها داخل النطاق. تسمح ببناء هرمي للنطاق.

الفصل الثالث
إدارة خدمات المجال للدليل النشط AD DS

- إدارة حسابات المستخدمين:
- لا يُمكن لأي شخص الدخول للأجهزة الموجودة في الشبكة دون أن يكون له حساب مستخدم تم إنشاؤه من قِبل مدير الشبكة على الدليل النشط.
- إنشاء حساب مستخدم جديد:

عند إنشاء حساب مستخدم جديد بعد كتابة بياناته واختيار كلمة المرور، تظهر لنا عدة خيارات ومنها:

User must change password at next login:

ويعني أن المستخدم لن يستطيع الدخول لأجهزة الشبكة دون تغيير كلمة المرور.

وهذه خاصية تتيح للمستخدم تغيير كلمة المرور بحيث لا يستطيع حتى مدير الشبكة معرفة كلمة المرور.

User cannot change password:

وتعني أن المستخدم لا يستطيع تغيير كلمة المرور. وهذا الخيار يحدد حسب طبيعة عمل المؤسسة والسياسات التي تفرضها.

- خصائص حساب المستخدم:

Profile: تعرض ملخص عن بيانات صاحب الحساب، مثل البريد الإلكتروني وغيرها.

Account: تعرض معلومات الحساب، مثل مدة صلاحيته، الساعات المسموح بها لاستخدام الحساب.

Member of: تعرض المجموعات التي ينتمي إليها الحساب.

- إدارة المجموعات: المجموعات هي أحد خدمات المجال للدليل النشط. وهي عبارة عن وعاء يحتوي على مجموعة من حسابات المستخدمين، والأجهزة المتصلة بالشبكة، أو حتى مجموعات أخرى. تكوين المجموعات يُفيد في: إعطاء الصلاحيات لمجموعة من المستخدمين دفعةً واحدة.
- أنواع المجموعات:

Security: يُستخدم هذا النوع لإعطاء الصلاحيات لمجموعة من المستخدمين.

Distribution: يُستخدم لإرسال البريد الإلكتروني فقط.

الفصل الرابع
كيفية جعل خدمات المجال للدليل النشط AD DS تعمل بشكل آلي

- استخدام PowerShell:

يتم استخدام PowerShell لإدارة خدمات المجال للدليل النشط. هناك 3 عمليات يتم إجراؤها في بيئة الدليل النشط "Active Directory" باستخدام بيئة الأوامر PowerShell وهي: إنشاء، تعديل، حذف.

الفصل الخامس
بروتوكولات الشبكة والعنونة وتقسيم الشبكة

- البروتوكولات: عبارة عن مجموعة من القوانين والإجراءات التي تُستخدم للاتصال.
- الخطوة الأولى التي تنفذها البروتوكولات في الجهاز المرسل: عبارة عن (تقسيم البيانات إلى حزم).
- يُطلق على حركة البيانات من الشبكة المصدر source إلى الشبكة الوجهة Destination، عبر عدة مسارات اسم: التوجيه Routing
- تُقسم البروتوكولات إلى قسمين:

Connection-Oriented Network Protocol بروتوكول مُحدد الوجهة: هذا النوع من البروتوكولات يُوفر اتصال مباشر مع الكمبيوتر المستقبل. ويُحقق موثوقية عالية لتسليم البيانات، ولكنه قد يؤدي إلى بطئ في أداء الشبكة.

من أمثلته: **TCP** "Transmission Control Protocol"

Connectionless Network Protocol بروتوكول عديم الاتصال: هذا النوع لا يُوفر اتصال مباشر مع الكمبيوتر المستقبل قبل إرسال البيانات، مما يعني أن البيانات تنتقل بسرعة أكبر مما يُحسن أداء الشبكة. ولكن هذه الطريقة ليست تامة الموثوقية لأنه لا سبيل لمعرفة إن حدث خطأ أثناء الإرسال أم لا. من أمثلته: بروتوكول **IP** "Internet Protocol".

- أنواع البروتوكولات:

بروتوكول التحكم بنقل البيانات TCP: "Transmission Control Protocol" أحد البروتوكولات الموجهة، مُصمم لإرسال حزم البيانات عبر الإنترنت وضمان تسليمها بشكل ناجح من طرف إلى آخر. يُوفر اتصال مباشر وموثوقية عالية في تسليم البيانات.

بروتوكول نقل البريد البسيط SMTP: "Simple Mail Transfer Protocol" البروتوكول القياسي الأكثر استخدامًا في خدمات البريد الإلكتروني المتوافرة عبر شبكة الإنترنت العالمية. يُوفر القدرة على إرسال واستقبال رسائل البريد الإلكتروني من طرف إلى طرف بناءً على عنوان البريد الإلكتروني الخاص بكلٍ منهُما.

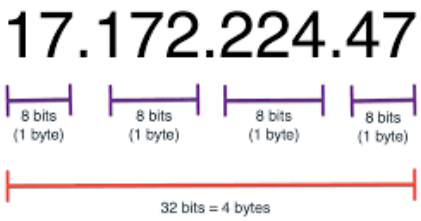
بروتوكول نقل النص التشعبي HTTP: "Hypertext Transfer Protocol" البروتوكول الأساسي الذي يُستخدم عبر شبكة الويب العالمية. أما الاصدار الآمن من بروتوكول نقل النص التشعبي يُشار إليه بـ HTTPS وهو قادر على تأمين الاتصال الذي يتم بين المُستخدم والموقع الإلكتروني بشكل مُشفر.

بروتوكول نقل الملفات FTP: "File Transfer Protocol" البروتوكول المُستخدم لنقل وتبادل الملفات بين جاهزي كمبيوتر متصلين بشبكة واحدة.

- نظام العنونة:

IP Address: مُعرف رقمي يتم تعيينه لكل جهاز على الشبكة بحيث يُصبح له عنوانً يسمح بالاتصال بغيره من الأجهزة. (فريد لا يتكرر)

- في نظام العنونة إصدار IPv4: يتكون عنوان الـ IP من 4 بايت يفصل بينهم بـنقطة، كل بايت عبارة عن 8 بت من قيم الـ 0 و 1، لذلك سيكون مجموع البت (Bit) الكُلي للعنوان = 32 بت، يُكتب بالنظام العشري.



- يتكون عنوان الـ IP من قسمين وهما: الأول (مُعرف الشبكة)، الثاني (مُعرف المُضيف).
- ينقسم عنوان الـ IP إلى فئات (Class): بناءً على قيمة البايت الأول من العنوان، نُحدد تحت أي فئة يندرج هذا العنوان.

IP Address	First Octet
Class A	1 - 126
Class B	128 - 191
Class C	192 - 223

- مثال: 143.20.10.2: ينتمي هذا العنوان إلى الفئة B
- عنوان الـ IP (127): لا يُمكن استخدامه، لأنه محجوز للفحص الذاتي لكرت الشبكة.
- عنوان الشبكة: يُستخدم لإرسال بيانات إلى شبكة محددة عن بُعد، ونحصل عليه بتبديل جميع معرفات المضيف بالأصفار: مثال: 10.0.0.0 ، يُمثل عنوان الشبكة للفئة A
- قناع الشبكة: نحصل عليه باستبدال جميع معرفات الشبكة بـ 255، مثال: 255.0.0.0 يُمثل قناع الشبكة للفئة A.

الفصل السادس
بروتوكولات التكوين الديناميكي للمضيف DHCP

- بروتوكول التكوين الديناميكي للمضيف DHCP: هو بروتوكول شبكة يخصص معلومات IP والتكوين للأجهزة مثل الخوادم وأنظمة سطح المكتب والهواتف المحمولة.

الفصل السابع
نظام أسماء النطاقات DNS

- خادم اسم النطاق DNS: "Domain Name System" يقوم بربط العديد من المعلومات بأسماء النطاقات، وعلى وجه الخصوص يُخزن عنوان الـ IP.

الفصل الثامن
نظام العنونة IPv6

- نظام العنونة إصدار IPv6: يتكون عنوان الـ IP من **128 بت** (bit)، ويكون مقسم إلى 8 أقسام، كل قسم عبارة عن byte. يُكتب بالنظام السادس عشري.
- الهدف الرئيسي من نظام العنونة IPv6: لتوفير عدد لا حصر له من العناوين.

الفصل التاسع
تكنولوجيا التخزين المحلي

- أنواع الأقراص: Logical Partition وPrimary Partition

Primary Partition: نوع من أنواع الأقراص الصلبة، يُمكن أن يتم تنزيل نظام التشغيل عليه ويمكن أن يحمل ملفات الـ Boot الخاصة بالنظام منه، إذا كان في وضع Active Partition

الفصل العاشر
خدمات الطباعة وتأمين الملفات

- أنظمة الحماية: تقوم بـ حماية موارد الكمبيوتر من الوصول غير المُصرح به والتغييرات الضارة والتناقض.
- من أنواع الملفات التي تحتاج إلى تشفير:

أولًا: الملفات التي تحتوي على كلمة سر، لمنع أي شخص من تغيير كلمة السر.

ثانيًا: الملفات التي لها حقوق تأليف لمنع أي شخص من تغيير الحقوق.

ثالثًا: أي أكواد أو سكربتات يملكها شخص ولا يُريد أي أحد أن يطلع على محتواها.

- يمُكن التحكم في الملفات بعدة أنواع مختلفة من العمليات:

Read: القراءة من ملف

Write: كتابة الملف أو إعادة كتابته.

Execute: تحميل الملف وبعد التحميل تبدأ عملية التنفيذ

Delete: حذف الملف الذي لا فائدة منه واستخدام مساحته لبيانات أخرى.

List: سرد اسم الملف وسماته.

- صلاحيات الوصول للمجلدات:

Full control: يمتلك كامل الصلاحيات الخاصة بالمجلد والملفات التي يحتويها.

Change: يُمكن للمستخدم إنشاء المجلدات وحذفها، إنشاء الملفات وتغيير محتواها.

Read: يُمكن للمستخدم مشاهدة المجلدات والملفات.

- صلاحيات الطباعة:

Print: السماح للمستخدمين بالطباعة فقط.

Manage this printer: إعطاء صلاحيات للمستخدم لتعديل الإعدادات الخاصة بالطابعة.

الفصل الحادي عشر
نهج المجموعة

- **نهج المجموعة Group Policy:** أن تكون نقطة التحكم مركزية بحيث يتم تحديد الصلاحيات والقوانين دفعةً واحدة.

الفصل الثاني عشر
تأمين نظام تشغيل الشبكات

- **تكوينات اعدادات الأمان:**

أداة تقييم الأمان من Microsoft: أداة مجانية تساعد في تحديد وتقييم التهديدات الأمنية.

محلل أساس أمان Microsoft: أحد تكوينات الأمان، يساعد في فحص الأنظمة المحلية والبعيدة بثمان فئات من الفاعلية، حيث يبحث في توصيات النظام ويُرجع الأخطاء عند عدم التطابق، أو التحذيرات عند تطابق الشروط بنسبة 50–80%

الفصل الثالث عشر
الأنظمة الوهمية و Hyper-

- تطبيق Hyper-V: هو أحد الأدوات المُستخدمة لتثبيت أنظمة التشغيل الافتراضية، وهو عبارة عن قواعد "Roles"، يتم تثبيتها في Windows Server 2012
- أنواع الـ Network Adapter: هناك 3 أنواع ولكل نوع خصائص مختلفة وهي كالتالي:

Private	Internal	External
يمكن من خلال هذا الخيار عمل إتصال مابين الأنظمة الإفتراضية فقط.	يمكن من خلال هذا الخيار عمل إتصال ما بين الجهاز الحقيقي والأنظمة إفتراضية.	يسمح هذا الخيار بالإتصال بالشبكات الخارجية"Internet".

الأسئلة

1. إصدار نظام تشغيل الشبكة من نوع (Standard) يسمح بإنشاء جهازان وهميان			
صح	خطأ		
2. إصدار أنظمة تشغيل الشبكة من نوع (DataCenter)، يسمح بإنشاء.....من الأجهزة الوهمية.			
	4	8	عدد لا محدود
3. أحد تصحيحات وأدوات نظام Windows server وهي أداة تسمح بجمع الكثير من أنواع الاتصال عن بُعد			
Active Directory Explorer	viewfinity local admin discovery	Remote Destop manager	Active Directory Best Practice Analyzer
4. بيئة الأوامر Powershell تتفوق على بيئة الأوامر Cmd			
صح	خطأ		
5. يتم كتابة الأوامر في بيئة (موجه الأوامر المُحدث Powershell) بالصيغة التالية			
(verb - noun) , Get - command	(verb " noun") , Get "command"	(verb + noun) , Get + command	(verb / noun) , Get / command
6. توفير خدمات مركزية لتحديد الهوية والتوثيق لشبكة من الحواسب التي تستخدم نظام تشغيل ويندوز، والس لمسؤولي الشبكات بتوزيع البرمجيات وتثبيت التحديثات، ما سبق يُعتبر الغرض الرئيسي من:			
الكائن Object	الشجرة Tree	الدليل النشط Active Directory	الوحدات التنظيمية Organizational units
7. الدليل النشط Active Directory، يُعد مصدر للمعلومات، إذ يحوي معلومات حول الكائنات الهامة كالخوادم والمستخدمين والملفات			
صح	خطأ		
8. أحد مكونات المتكم بالمجال: تتمثل في مجموعة النطاقات المرتبة فيما بينها والتي يُمكن تمثيلها بعلاقة (الأب والأبناء)، هي:			
الكائن Object	النطاق Domain	الشجرة Tree	الغابة Forest
9. المعلومات المخزنة بالنظام، وحدة المعالجة المركزية CPU، القرص الصلب)، جميع ما سبق من أمثلة.....التي ت تحت الكائنات في الدليل النشط			
الموارد	الخدمات	المستخدمين	الوحدات التنظيمية

10. تُعد أكبر محتوى من محتويات الدليل النشط، وتُمثل مجموعة الأشجار والنطاقات التي تتشارك في المميزات والخصائص

الكائن Object	النطاق Domain	الشجرة Tree	الغابة Forest

11 . أحد الخيارات التي تظهر عند إنشاء حساب مستخدم جديد واختيار كلمة المرور، وتعني أن المستخدم لن يستطيع الدخول دون تغيير كلمة المرور

user cannot change password	user must change password at next login	Password never expires	Account is disabels

12. إحدى خصائص حساب المُستخدم ويتم من خلالها عرض ملخص عن بيانات صاحب الحساب، مثل عنوان البريد الإلكتروني

user	Member of	Profile	Account

13. خاصية من خصائص حساب المستخدم وتحتوي على المجموعات التي ينتمي إليها الحساب

user	Member of	Profile	Account

14. المجموعة من نوع Security تُستخدم لإعطاء الصلاحيات لمجموعة من المستخدمين

صح	خطأ		

15. هي أحد خدمات المجال للدليل النشط AD DS، عبارة عن وعاء يحتوي على مجموعة من حسابات المستخدمين والأجهزة المتصلة بالشبكة

حسابات المستخدمين	المجموعات	حسابات الحواسيب	كلمات المرور

16. تكوين المجموعات يُفيد في إعطاء الصلاحيات لمجموعة من المستخدمين، دفعةً واحدة

صح	خطأ		

17. أنواع العمليات التي يتم إجراؤها في بيئة Ative Directory باستخدام بيئة الأوامر PowerShell، تتمثل في:

إنشاء وتعديل	تعديل وحذف	إنشاء وحذف	إنشاء وحذف وتعديل

18. عبارة عن مجموعة من القوانين والإجراءات التي تُستخدم للاتصال

الكائن	الملفات	البروتوكولات	العنونة

19. أي من الخيارات التالية يتم تنفذها من قبل البروتوكولات في جهاز المرسل أولا.

تقسيم البيانات إلى حزم	إضافة معلومات العنونة الحزم	تحضير البيانات للإرسال	تمرير البيانات إلى البرنامج في صورة مفهومة

20. البروتوكولات التي تُوفر اتصال مباشر تُسمى Connectionless Network

صح	خطأ		
21. يُطلق على حركة البيانات من الشبكة المصدر إلى الشبكة الوجهة، عبر عدة مسارات اسم:			
التوجيه Routing	القابلة للتوجيه Routable protocol	الطبقات Layering	المكدس Stack
22. البروتوكول المستخدم في خدمات البريد الإلكتروني البسيط هو:			
HTTPS	UDP	SMTP	TCP
23. البروتوكول المُستخدم لنقل وتبادل الملفات بين جاهزي كمبيوتر متصلين بشبكة واحدة			
POP	FTP	SMTP	SNMP
24. أحد البروتوكولات الموجهة والتي توفر اتصال مباشر وتحقق موثوقية عالية لتسليم البيانات:			
IP	UDP	SNMP	TCP
25. TCP من البروتوكولات التي لا تقوم بإعداد اتصال مباشر			
صح	خطأ		
26. بروتوكول نقل النص التشعبي الآمن الذي يُستخدم عبر شبكة الويب العالمية يُطلق عليه:			
TCP	HTTP	HTTPS	UDP
27. HTTP هو الإصدار الآمن من بروتوكول نقل النص التشعبي			
صح	خطأ		
28. IPv4 هو أحد إصدارات بروتوكولات الإنترنت IP، ويتكون من .....بت؟			
8	32	64	128
29. IPv6 هو أحد إصدارات بروتوكولات الإنترنت IP، ويتكون من .....بت؟			
8	32	64	128
30. يتم كتابة عناوين الـ IP بالإصدار IPv4 بالنظام .....، أما إصدار IPv6 فيُكتب بالنظام.....			
العشري – السادس عشري	العشري – الثنائي	العشري – الثماني	الثماني – السادس عشري
31. يتكون عنوان الـ IP من قسمين وهما: الأول.....والثاني.....			
معرف المضيف، معرف الشبكة	عنوان النشر، معرف الشبكة	عنوان النشر، معرف المضيف	معرف الشبكة، معرف المضيف
32. ينتمي عنوان الـ IP التالي : 172.20.10.11 إلى الفئة:			
Class A	Class B	Class C	Class D
33. عنوان الـ IP: (192.168.16.1)، يندرج تحت الفئة؟			

Class A	Class B	Class C	Class D
34. قومي بذكر نوع الفئة التي ينتمي إليها عنوان الـ IP التالي: (40.50.3.4)			
Class A	Class B	Class C	Class D
35. عنوان الشبكة الذي لا يُمكن استخدامه لأنه محجوز من أجل الفحص الذاتي لكرت الشبكة، هو			
126	127	128	129
36. قناع الشبكة 255.0.0.0 ينتمي للفئة (Class)؟			
Class A	Class B	Class C	Class D
37. قناع الشبكة 255.255.0.0 يحتوي على .....بت مملوءة			
8	16	24	32
38. يُستخدم لإرسال البيانات إلى شبكة محددة عن بُعد، ونحصل عليه بتبديل جميع معرفات المضيف بأصفار			
عنوان النشر Broadcast address	عنوان الشبكة Network Address	معرف الشبكة ID Network	معرف المضيف ID Host
39. برتوكول يعمل على تخصيص معلومات الـ IP للأجهزة:			
FTP	HTTPS	DHCP	POP
40. خادم اسم النطاق (DNS) يقوم بربط العديد من المعلومات بأسماء النطاقات، وعلى وجه الخصوص يُخزن عنوان الـ IP المرتبط بذلك النطاق			
صح	خطأ		
41. الهدف الرئيسي من الإصدار السادس IPv6 من نظم عنونة الـ IP، هو:			
لتوفير عدد لا حصر له من عناوين الـIP، لتلبية الطلب المتزايد	مجرد طريقة تمثيل أخرى للعناوين	لكتابة عناوين IP أقصر من التي تُكتب بإصدار IPv4	لكتابة عناوين IP بالنظام الثنائي
42. نوع من أنواع الأقراص الصلبة، يُمكن أن يتم تنزيل نظام التشغيل عليه ويمكن أن يحمل ملفات الـ Boot الخاصة بالنظام منه، إذا كان في وضع Active Partition			
الديناميكي Dynamic Drive(Volumes)	الرئيسي Primary Partition	المنطقي Logical Partition	البسيط simple
43. أنظمة الحماية هي: حماية موارد الكمبيوتر من الوصول غير المُصرح به والتغييرات الضارة والتناقض			
صح	خطأ		
44. أحد الحالات التي نحتاج إلى تشفير الملفات فيها:			

الملفات التي تحتوي على كلمة سر	الملفات الفارغة	الملفات التي ليس بها حقوق	الملفات التالفة
45. يُمكن التحكم في عدة أنواع مختلفة من العمليات على الملفات، منها حذف الملف الذي لا فائدة منه عن طريق العملية			
Read	Write	Delete	List
46. أحد عمليات التحكم في الملفات، عبارة عن سرد (اسم الملف، وسماته)، هذه العملية تُسمى:			
Read	Write	Delete	List
47. من صلاحيات الوصول للمجلدات المشارك بها، حيث يمتلك كامل الصلاحيات الخاصة بالمجلد والملفات التي يحتويها، ويستطيع تغيير الصلاحيات أيضًا:			
Change	Full Control	Read	Delete
48. اختاري الصلاحية التي يجب أن يُعطيها مدير الشبكة للمستخدمين لاستخدام الطابعة، حيث تسمح لهم بالطباعة فقط:			
Print	Manage this printer	Manage document	server print
49. الفائدة من تطبيق نهج المجموعة Group Policy هي : أن تكون نقطة التحكم المركزية بحيث يتم تحديد الصلاحيات والقوانين دفعةً واحدة			
صح	خطأ		
50. أحد تكوينات الأمان، يساعد في فحص الأنظمة المحلية والبعيدة بثمان فئات من الفاعلية، حيث يبحث في توصيات النظام ويُرجع الأخطاء عند عدم التطابق، أو التحذيرات عند تطابق الشروط بنسبة 80–50%			
مدير التوافق الأمني لـ Microsoft	إدارة حقوق Active Directory	محلل أساس أمان Microsoft	أداة تقييم الأمان من Microsoft
51. تطبيق Hyper-V هو أحد الأدوات المُستخدمة لتثبيت أنظمة التشغيل الافتراضية، وهو عبارة عن قواعد "Roles"، يتم تثبيتها في Windows Server 2012			
صح	خطأ		
52. الخاصية التي يمتلكها الـ Network Adapter أو ما يعرف بـ (Virtual switches)، وتسمح بالاتصال بالشبكات الخارجية "Internet"، هي:			
Private	Internal	External	Public/Private

ملخص لمقرر نظم التشغيل (2)

الفصل الأول والثاني
مقدمة في اللينكس

تطور اللينكس وأنظمة التشغيل المشهورة :

اللينكس هو نظام تشغيل حر ومفتوح المصدر وهو نظام تشغيل كامل مكون من النواة والحزم والمكتبات المصاحبة له .

يتمتع لينكس بدرجة عالية من الحرية في التعديل والتشغيل والتوزيع والتطوير ويصنف نظام لينكس من ضمن عائلة نظام تشغيل يونكس .

سبب الحرية التي يتمتع بها نظام لينكس كونه خاضعا لرخصة (جنو العمومية GPL)

دور الأنظمة مفتوحة المصدر :

نظام التشغيل مفتوحة المصدر هو نظام تشغيل يمكنك من عرض وتعديل واستخدام ومشاركة الكود الخاص بالنظام .

توزيعات نظام لينكس :

تستعمل النواة الخاصة بلينكس كجزء من مجموعة شاملة من النظام وتطبيقاته وتسمى باسم (توزيعة – distro) ، وكل توزيعة يتم بنائها وترجمتها برمجيا وتجميعها من قبل افراد او شركات .

يتم انشاء التوزيعات بأهداف مختلفة .

يوجد العديد من التوزيعات المختلفة في لينكس حول العالم ويتم تطوريها بشكل مستمر ، ومن اشهرها :

- Debian
- RedHat
- Gentoo
- Ubuntu-Linux
- Manjaro

التوزيعة النموذجية تتضمن دوما النواة وبعض المكتبات الحرة والأدوات الضرورية للحوسبة

احتياجات العتاد لتثبيت نظام لينكس :

- ذاكرة الوصول العشوائي RAM بحد ادنى 1 جيجا بايت
- القرص الصلب بحد ادنى 4 الى 5 جيجا بايت

معايير اختيار نظام التشغيل :

نظام تشغيل Microsoft windows :

- هو نظام تشغيل من انتاج شركة مايكروسوفت ويمكن لاي احد استخدامه وتثبيته وتنزيله على أي جهاز حاسب تريد ن والأنظمة الجديدة منه تحتاج الى عتاد قوي يتحمل احتياجات النظام .
- يتميز ويندوز بانه اكثر منصة مدعومة من جميع الشركات البرمجية وفرق التطوير
- يتميز بانه الأنسب والأفضل للمستخدم ومناسب للمصممين والمحررين ولما يقدمه من مجموعة من البرامج الكبيرة والمتطورة في هذا المجال
- مناسب لصانعي الألعاب والأفلام المتحركة .
- من العيوب الموجودة في هذا النظام هي الحماية الأمنية لأنك ستحتاج الى برنامج حماية قوي للحماية من الملفات الضارة و الخبيثة مثل Malwares , Viruses .

نظام تشغيل Mac OS :

- هو من انتج شركة apple ويعمل فقط على الأجهزة الخاصة بالشركة، وهذا النظام يعمل على أجهزة ذات عتاد قوي من حيث معالجة البيانات والرسومات .
- المستخدمين المهتمين بالبرمجة بشكل عام وتصميم المواقع بجانب بعض برامج تحرير الصور والفيديوهات بجودة عالية .

نظام تشغيل ليكنس :

- هو نظام مفتوح المصدر وطور وبرمج من قبل مؤسسة البرمجيات الحرة (Free software foundation)
- من اهم مميزات هذا النظام كونه مجاني ويدعم الحواسب ذات العتاد المتوسط والضعيف
- لن يحتاج النظام الى برامج حماية لان النظام لا يدعم الكثير من الفيروسات ومحكوم ومؤمن اكثر من نظام ويندوز .
- يحتوي على مجموعة كبيرة من المكتبات للأشخاص المهتمين بالبرمجة والعاملين في مجال الحماية الأمنية الالكترونية وأيضا المخترقين .
- من عيوبه ان هذا النظام لا زال غير داعم بشكل قوي من قبل الشركات البرمجية وشركات صانعي الألعاب

تطبيقات أجهزة سطح المكتب :

يمكن للبرامج مفتوحة المصدر التي يراد مشاركتها وتعديلها بحرية من قبل الاخرين ان تستخدم العلامة التجارية مفتوحة المصدر ، من الأمثلة على هذه البرامج :

- Linux
- Oracle
- Open Office
- Mozilla Firefox

أولاً :برامج مكافحة الفيروسات :

العرض منها حماية الكمبيوتر من التهديدات القادمة من الويب والبريد الالكتروني والشبكات ، ومنها :

1. برنامج Kaspersky free
2. برنامج Avira Free

برامج مكافحة البرامج الضارة :

العرض منها تنظيف جهاز الكمبيوتر من البيانات المهملة والفيروسات .

المتصفحات المجانية مثل :

1. Google chrome
2. Mozilla Firefox

مفهوم البرامج مفتوحة المصدر ورخص الاستخدام :

البرمجيات الحرة والمفتوحة المصدر هي البرامج التي يمكن تصنيفها على حد سواء ، أي ان أي شخص مرخص له بحرية استخدام البرنامج ونسخه ودراسته وتعديله باي شكل من الاشكال .

تحتفظ البرمجيات الحرة والمفتوحة المصدر بحقوق الحرية المدنية لمستخدم البرنامج وهي :

- حرية تشغيل البرنامج كما يحلو لك ولاي غرض
- حرية توزيع نسخ من اصداراتك المعدلة للأخرين من خلال القيام بذلك

من مميزات استخدامها أيضا هي انخفاض تكاليف البرامج وزيادة الأمان والاستقرار وحماية الخصوصية .

نماذج تجارية لأنظمة مفتوحة المصدر :

- Square online
- Wix
- WooCommerce

الفصل الثالث والرابع

سطر الأوامر CLI

هي واجهة بين الانسان والالة وأين ايتم الاتصال بين المستخدم والحاسوب بأخذ صيغ نصية منه .

ويمكن استخدامها في البدء في تنفيذ مختلف البرمجيات ولإجراء الحوارات مع المستخدم هذه البرامج .

- **مميزات استخدام واجهة سطر الأوامر :**
- سهولة الاستخدام .
- تتطلب مساحة تخزين قليلة
- تعزز الإنتاجية
- الأكثر كفاءة في الذاكرة

المحاكاة الافتراضية والحوسبة السحابية :

تمثل المحاكاة الافتراضية انشاء نسخة غير فعلية لشيء ما ، مثل نظام التشغيل او الخادم او جهاز تخزين وتعرف أيضا بانها وسيلة فصل تطبيق ما والموارد اللازمة لتشغيله (المعالج والذاكرة ونظام التشغيل والخ) من مضيف الأجهزة الأساسي .

- أولا : المحاكاة الافتراضية للأجهزة : يسمح لك لخادم واحد بتشغيل أنظمة تشغيل متعددة في نفس الوقت ، مما يقلل من عدد الخوادم .
- ثانياً : المحاكاة الافتراضية للتخزين : هي دمج البيانات في موقع مركزي ، حيث يمكن لعدة مستخدمين الوصول اليها ويسمح بتقليل البيانات المكررة وتقليل عدد الخوادم .

الفرق بين المحاكاة الافتراضية والحوسبة السحابية :

- ان المحاكاة الافتراضية هي جزء من بنية تحتية مادية بينما الحوسبة السحابية هي خدمة مقدمة الى المستخدم ،
- تكاليف استخدام الحوسبة السحابية منخفضة مقارنة بالمحاكاة الافتراضية .

استخدام نظام لينكس لعمل :

لاستخدام نظام لينكس نحتاج الى تثبيت برنامج المحاكاة الافتراضية Virtual box وتستخدم هذا البرنامج في تجربة نظام جديد او تجربة برامج قبل استخدامها على الحاسوب الشخصي او عمل شروحات عليه .

كيف يحافظ نظام لينكس على جهاز الكمبيوتر الام :

تقييد الوصول :

توجد حقوق وصول الى ملفات الجذر وهي ملفات خاصة بمسؤول النظام فقط ولن يتم منح أي مستخدم عادي حق الوصول لها وبالتالي عند اختراق نظام لينكس لن تتمكن الفيروسات او البرامج الضارة من الوصول الى الجذر او اتلاف النظام على نطاق واسع .

ويؤدي هذا الى اقل تأثير للفيروس في الأنظمة التي تعمل بنظام لينكس لان مستخدمي لينكس ليس لديهم الحق في الوصول الى الجذر .

نظام الملفات الافتراضي :

في ليكنس كل شي عبارة علن ملف ويتم التعامل مع هذه الملفات عبر نظام يعرف باسم Virtual file system والذي يتضمن (الدليل وملف عادي وجهاز شخصي ولوحة مفاتح و محرك أقراص صلبة والخ ...) ونظرا لان كل شي يعتبر ملفا فيمكن تقييد الوصول اليه مما يجعل هذا النظام امنا ومحميا .

المصدر المفتوح :

نواة لينكس Linux kernel هو برنامج مفتوح المصدر وهذا يعني ان الكود قد تم تطويره وصيانته من قبل مجموعة من الأشخاص يطلق عليهم اسم المجتمع .

إدارة الذاكرة :

في نظام لينكس يتم فصل مساحة المستخدم ومساحة النواة بشكل جيد ولن يتم عرض العنوان الفعلي المخصص لاي عملية للمستخدمين وبهذه الطريقة في إدارة الذاكرة تجعل من نظام لينكس اكثر امانا .

واجهة سطر الأوامر :

قبل ظهور الواجهات الرسومية في أنظمة التشغيل كان يوجد طرفيات وهي الوسيلة التي نصل فيها الى سطر الأوامر ، وسطر الأوامر هي طريقة مختلفة لتشغيل البرامج كما هي في الواجهات الرسومية في أنظمة ماك او ويندوز ولينكس .

الوصول الى واجهة سطر الأوامر :

أولا : الموجه

يمكن الوصول له عن طريق الطرفية والتي يمكن تشغيلها في اغلب توزيعات لينكس التي توفر واجهة رسومية عبر تطبيق اسمه (Terminal) .

ثانياً : الشل :

هي النسخة المحسنة والمطورة و المجانية من قبل Gnu ، ويوفر برنامج الشل الوصول الى مكونات نظام التشغيل و يمنح المستخدمين طريقة الدخول لداخل النظام أيضا

ويستخدم حاصة عند الحاجة الى البحث عن اعداد كبيرة من الملفات او كميات كبيرة من البيانات او فرزها او معالجتها باي طريقة .

الشكل العام للأوامر :

```
sammy@webapp:~$
```

Sammy هو اسم المستخدم الحالي

Webapp هو اسم المضيف الحالي hostname

الامر ls :

هو امر يستخدم لعرض كل الملفات و المجلدات في المسار الحالي

الامر CD :

امر يستخدم للانتقال من المسار الحالي الى مسار اخر ، مثل :

```
cd /usr/bin
```

الامر ls – l :

يستخدم لطباعة أي تفاصيل إضافية في المسار مثل اذونات الملفات و الملكية و الحجم والتوقيت .

الامر ls – a :

يستخدم لعرض جميع محتويات المسار المعين بما في ذلك الملفات المخفية .

متغيرات البيئة :

هي عبارة عن قيم تقوم بتغيير طريقة تنفيذ الأوامر والعمليات عند تسجيل الدخول لأول مرة الى الخوادم

امر عرض جميع متغيرات البيئة ENV :

يستخدم لعرض جميع متغيرات البيئة التي تم ضبطها لجلسة طرفية معينة .

متغير البيئة path :

عبارة عن قائمة مفصول عناصرها ب(:) وتتكون من قائمة المسارات التي سيقوم الشل بالبحث عن البرامج عند تنفيذ امر معين .

عرض قيمة متغير :

يمكن جلب قيمة متغير بيئة عن طريق وضع علامة $ قبل اسم المتغير

```
echo $PATH
```

الامر man :

يستخدم لعرض دليل المستخدم لاي امر يمكن تشغيله عليه .

- `man [command/tool name]`

```
man ls
```

الامر info :

يقرأ هذا الامر الوثائق بتنسيق المعلومات ويعطي معلومات مفصلة عن الامر عند مقارنته بصفحة الدليل .

```
info [OPTION]... [MENU-ITEM...]
```

مصادر اضافية للمساعدة :

هي سلسلة من الأدوات التي يمكن ان تساعد أي شخص في اتقان سطر الأوامر او انجاز مهمة مطلوبة بسرعة وكفاءة اكبر .

الامر help : يقدم المساعدة في البرامج المضمنة فقط .

الامر whereis : يستخدم للعثور على امر ووثائقه .

الفصل السادس والسابع

مفهوم الملفات والأدلة :

في نظام لينكس كل شي عبارة عن ملف وحتى الدليل عبارة عن ملف والأجهزة أيضا مثل الفارة ولوحة التحكم هي ملفات في النظام .

أنواع الملفات في نظام لينكس :

الملفات العامة :

قد تكون صورة او فيديو او برنامج او ملفات نصية بسيطة

ملفات الدليل :

تعد هذه الملفات مستودعا لملفات من أنواع أخرى

ملفات الجهاز :

يتم تمثيل الأجهزة مثل القرص المضغوط ومحركات الأقراص الثابتة على شكل ملفات

يقوم نظام لينكس بتخزين البيانات والبرامج في ملفات ويتم تنظيم كل هذا في الدلائل .

الدليل الرئيسي هو جزء من القرص الصلب ويتم فيه حفظ جميع البيانات التي تريدها في ملفات وادلة في الدليل الرئيسي ، للوصول الى الدليل الرئيسي نستخدم الامر :

```
echo $HOME
```

الامر cat :

يستخدم هذا الامر لكتابة جميع محتويات الملف على الشاشة .

```
cat file-name
```

الامر cp :

يستخدم لنسخ الملف او مجموعة من الملفات او الدليل ويقوم بأنشاء صورة دقيقة للملف على القرص باسم مختلف .

انظر المثال التالي :

Example1:

```
$ ls
a.txt

$ cp a.txt b.txt

$ ls
a.txt  b.txt
```

الامر mv :

يستخدم هذا الامر لنقل ملف او مجلد واحد او اكثر من مكان لأخر ، وهذا الامر له وظيفتان :

يعيد تسمية ملف او مجلد

ينقل مجموعة من الملفات الى دليل مختلف

مثال :

```
$ ls
b.txt  c.txt  d.txt  test.txt

$ cat test.txt
India

$ cat b.txt
tessst

$ mv test.txt b.txt

$ ls
b.txt  c.txt  d.txt

$ cat b.txt
India
```

انشاء الملفات الجديدة :

الامر cat يستخدم لأنشاء ملف جديد والكتابة فيه أيضا .

ملاحظة :بعد كتابة النص في الملف نضغط على ctrl + D للحفظ والخروج من وضع الكتابة .

مثال :

```
File  Edit  View  Search  Terminal  Help
[root@localhost Public]# cat > file1
Hi
Bye
[root@localhost Public]# ls
file1
```

الامر Touch :

يستخدم لأنشاء ملف او عدة ملفات فارغة , و الهدف الأساسي منه هو تغيير الطابع الزمني للملف او تحديثه

مثال :

انشأ ملف ثم باستخدام الامر cat لعرض البيانات :

```
File  Edit  View  Search  Terminal  Help
[root@localhost Public]# touch filea
[root@localhost Public]# cat filea
[root@localhost Public]#
```

التعامل مع الأدلة :

امر mkdir لأنشاء دليل جديد :

يستخدم هذا الامر لأنشاء دليل واحد او عدة ادلة في وقت واحد (تسمى مجلدات ايضا) .

Syntax:

```
mkdir [options...] [directories ...]
```

امر rmdir لحذف الدليل :

يستخدم هذا الامر لإزالة الدلائل الفراغة من نظام الملفات في لينكس ، ويزيل هذا الامر كل دليل محدد في سطر الأوامر فقط اذا كانت هذه الدلائل فارغة ، اما اذا كانت تحتوي على بيانات فلا يمكن ازالتها باستخدام هذا الامر .

ضغط الملفات :

هو استعمال عدة خوارزميات مختلفة لتقليل وتصغير حجم الملفات بغرض توفير مساحة تخزينية إضافية .

صيغ ضغط الملفات :

Gzip :

تتميز هذه الصيغة بسرعتها وشهرتها وكثرة استعمالها وتكتب بالأمر التالي :

```
tar -cvzf archive.tar.gz file-or-folder-to-compress
```

ولفك الضغط نستخدم الامر :

```
tar -xvzf archive.tar.gz
```

Bzip2 :

تتميز هذه الصيغة بفعاليتها في ضغط الملفات ولكنها قليلة الاستعمال لبطيء هذه الصيغة وتكتب بالأمر التالي :

```
tar -cvjf archive.tar.bz2 file-or-folder-to-compress
```

ولفك الضغط نستخدم الامر :

```
tar -xvjf archive.tar.bz2
```

Xz :

تتميز هذه الصيغة بفعاليتها الكبيرة اكثر من النوعين السابقين وقلة استعماله بسبب بطئه الشديد ، وتكتب بالأمر التالي :

```
tar -cvJf archive.tar.xz file-or-folder-to-compress
```

ولفك الضغط نستخدم الامر :

```
tar -xvJf archive.tar.xz
```

ارشفة الملفات :

هي تجميع العديد من الملفات في ملف واحد بغرض عمل نسخة من هذه الملفات وتخزينها احتياطيا

صيغة الارشفة Tar :

هي المسؤولة عن ارشفة الملفات ويتمثل عملها في تجميع جميع الملفات المراد ارشفتها في ملف واحد .

نكتب الامر التالي لأرشفة مجلد معين :

```
tar -cvf archive.tar folder/
```

ولأرشفة ملف او عدة ملفات معا نستخدم الامر :

```
tar -cvf archive.tar file1 file2 file3
```

ملفات ZIP :

هي عبارة عن أرشيف عالمي شائع الاستخدام على أنظمة الويندوز و ماك وحتى لينكس، ويمكن انشاء أرشيف مضغوط او فك ضغط الملفات من احدهما باستخدام بعض أوامر لينكس الشائعة

الفصل الثامن والتاسع

البحث عن الملفات باستخدام الامر find :

يستخدم هذا الامر للبحث عن ملفات في الدليل والأدلة الفرعية أيضا ويمكن البحث عن الملفات حسب اسم الملف او نوع الملف او المستخدم .

عرض الملفات باستخدام الامر less :

يعتبر الامر less هو الطريقة الرئيسية التي نقوم من خلالها بعرض الملفات وندعوه باسم pager لأنه يسمح لنا بالتنقل عبر صفحات ملف معين .

الامر head and tail :

مهمة هذين الامرين هي ان الامر الأول head يقوم بإخراج الجزء الأول من الملف بينما الامر tail يقوم بإخراج الجزء الأخير من الملف

Syntax:

```
tail [OPTIONS] FILES
```

Syntax :

```
head [OPTIONS] FILES
```

برنامج الشل النصي :

هو عبارة عن سلسلة من الأوامر المخزنة في ملف نصي عادي ، وتعد نصوص الشل البرمجية جزء أساسي من برمجة اللينكس .

يتكون كل برنامج نصي من :

- كلمات رئيسية
- أوامر الشل مثل pwd , test , echo الخ
- أوامر لينكس الثنائية مثل w , who
- أدوات معالجة النصوص
- الوظائف
- تحكم في بيانات التدفق مثل if , else او حلقات لأداء إجراءات متكررة .

التعديل على البرامج :

يمكن استخدام محررات نصوص لينكس لتحرير الملفات النصية وكتابة الرموز وتحديث ملفات تعليمات المستخدم والمزيد .

محرر vi/vim editor :

- يعد هذا المحرر احد اكثر المحررات القائمة على سطر الأوامر استخداما وقوة في نظام لينكس
- وهو محرر سهل الاستخدام ويوفر نفس البيئة لجميع توزيعات لينكس .

لاستدعاء المحرر ، قم بكتابة الامر التالي :

```
vi <file name>
```

المحرر Nano editor :

- نانو محرر مباشر ، حيث تم تصميمه لكل ممن المستخدمين المبتدئين والمتقدمين ولديه العديد من ميزات التخصيص ومنها :
- يدعم بناء تسليط الضوء على بناء الجملة
- توجد خيارات التراجع والإعادة
- يوفر عرض خط كامل على الإخراج القياسي

ولفتح ملف باستخدام محرر nano نكتب الامر التالي :

```
nano <file name>
```

اساسيات البرمجة :

المتغيرات :

يمكن استخدام المتغيرات لتخزين البيانات وخيارات التكوين ، ويوجد نوعين من المتغيرات هم :

متغيرات النظام :

يتم أنشاءه وصيانته بواسطة Linux bash shell ، لمشاهدة جميع متغيرات النظام اكتب الامر التالي في سطر الاوامر :

```
set
```

OR

```
env
```

OR

```
printenv
```

متغيرات شل شائعة الاستخدام :

متغير النظام	المعنى	لعرض نوع قيمة المتغير
BASH_VERSION	يحمل نسخة هذا المثيل من bash.	echo $ BASH_VERSION
HOSTNAME	اسم جهاز الكمبيوتر الخاص بك.	echo $ HOSTNAME
CDPATH	مسار البحث عن الأمر cd.	echo $ CDPATH
HISTFILE	اسم الملف الذي يتم حفظ محفوظات الأوامر فيه.	echo $ HISTFILE
HISTFILESIZE	أقصى عدد من الأسطر الموجودة في ملف المحفوظات.	echo $ HISTFILESIZE
HISTSIZE	عدد الأوامر التي يجب تذكرها في محفوظات الأوامر. القيمة الافتراضية هي 500.	echo $ HISTSIZE
HOME	الدليل الرئيسي للمستخدم الحالي.	echo $ HOME
IFS	فاصل المجال الداخلي الذي يُستخدم لتقسيم الكلمات بعد التوسيع ولتقسيم الأسطر إلى كلمات باستخدام الأمر read المدمج. القيمة الافتراضية هي <space><tab><newline>.	echo $ IFS
LANG	يستخدم لتحديد فئة الموقع لأي فئة لم يتم تحديدها بشكل خاص بمتغير يبدأ بـ LC	echo $ LANG
PATH	وهي قائمة من الدلائل مفصولة بنقطتين حيث يبحث الغلاف. مسار البحث عن الأوامر عن الأوامر.	echo $ PATH
PS1	الإعدادات السريعة الخاصة بك.	echo $ PS1
TMOUT	المهلة الافتراضية لأمر read builtin. أيضًا في الصدفة التفاعلية ، يتم تفسير القيمة على أنها عدد الثواني لانتظار الإدخال بعد إصدار الأمر. إذا لم يتم إدخال إدخال سيتم تسجيل خروج المستخدم.	echo $ TMOUT
TERM	نوع محطة تسجيل الدخول الخاصة بك.	echo $ TERM export TERM = vt100
SHELL	تعيين المسار إلى قذيفة تسجيل الدخول.	echo $SHELL

المتغيرات المعرفة من قبل المستخدم :

تم انشاءها وصيانتها من قبل المستخدم وقد يستخدم هذا النوع من المتغيرات المعرفة اي اسم متغير صالح .

ادوات الشرط :

يمكن استخدام عبارة if لاختبار الشرط ، الصيغة العامة لها هي :

```
if condition
then
     command1
     command2
     ...
     commandN
fi
```

الحلقات التكرارية Loops :

- يمكن bash shell ان يقوم بتكرار تعليمات معينة لمرات عديدة وحتى يتم تلبية حالة معينة .
- ويدعم باش الحلقة for و while .

يجب على كل حلقة ان :

- يجب تهيئة المتغير في حالة الحلقة ثم يبدأ تنفيذ الحلقة .
- يتم اجراء اختبار في بداية كل تكرار
- ينتهي جسم الحلقة ببيان يعدل قيمة متغير الاختبار
- تكرار تنفيذ مجموعة من العبارات .

الصيغة العامة for loop

```
for var in item1 item2 ... itemN
        do
                command1
                command2
                ....
                ...
                commandN
        done
```

الفصل العاشر والحادي عشر

الحاسوب هو الة إلكترونية تستقبل البيانات وتعالجها الى معلومات ذات قيمة ، كما يخزنها في وسائط تخزين مختلفة

تشتغل الحواسيب ببرمجيات خاصة تسمى انظمة التشغيل وتبين انظمة التشغيل للحاسوب كيفية تنفيذ المهام .

تنقسم مكونات الحاسوب الى قسمين رئيسيين هم :

- عتاد الحاسوب
- البرمجيات

المعالجات :

هو الجزء المسؤول عن تفسير وتنفيذ معظم الاوامر التي تصدرها البرامج والاجهزة المتصلة بجهاز الحاسوب ويتكون المعالج من :

- وحدة التحكم
- وحدة الحساب والمنطق

اللوحة والنواقل :

اللوحة الام هي لوحة تحتوي على دوائر كهربائية تمكن جميع مكونات الحاسب الالي من التواصل مع بعضها

ذاكرة الوصول العشوائي RAM :

هي وحدة التخزين المؤقتة في جهاز الحاسوب ، حيث تفقد المعلومات المخزنة فيها بمجرد اغلاق الجهاز وتثبت هذه الذاكرة على اللوحة الام .

الاجهزة الطرفية :

تنقسم الى ثلاثة اقسام هي :

- اجهزة الادخال
- اجهزة الاخراج
- اجهزة التخزين

الاقراص :

هي وحدات يخزن عليها كافة البيانات من صور وملفات و مقاطع فيديو والخ

يوجد نوعين من وحدات التخزين في الحاسوب :

- القرص الصلب المتحرك HDD
- قرص الصلب الثابت SSD

ادارة الاجهزة :

لوحة التحكم في انظمة التشغيل تسمح بعرض و التحكم بالعتاد الصلب المتصل بالحاسب .

عندما لا يعمل احدى مكونات الحاسب الصلبة يتم ابرازها ضمن مدير الاجهزة لتمكين المستخدم من التعامل معها .

مزود الطاقة :

يسمى ايضا باسم وحدة امداد الطاقة PSU وله وظائف منها :

- يوفر الطاقة لجهاز الحاسب
- يسحب الكمية المناسبة من التيار الكهربائي
- يحول التيار المتردد الى تيار مستمر
- ينظم الجهد الكهربي للقضاء على الطفرات الناتجة من الانظمة الكهربائية

ادارة الحزم في نظام لينكس

ادارة الحزمة Debian package management :

- يرجع سبب قوة توزيعة دبيان في الغالب الى نظام ادارة الحزم فيها ، فكل شي في النظام مبني في صورة حزمة برمجية ، من التطبيقات والبرامج الى المكونات .
- ادارة الحزم المتطورة في دبيان APT هي مجموعة من الادوات لتحميل الحزم وتثبيتها وترقيتها واداراتها ، ومن ثم كل البرمجيات المثبتة على نظام دبيان .
- يستخدم مدير الحزم في ادارة الحزم المثبتة Package Management tools قائمة مدراء الحزم والادوات المرتبطة بها

نواة اللينكس :

تشير النواة الى برامج النظام الذي يوفر وظائف اساسية مثل طبقة تجريد الاجهزة والتحكم في القرص ونظام الملفات و المهام لمتعددة ، وهي الطبقة السفلية لنظام التشغيل كله

وظائف نواه ليكنس :

- ادارة العمليات
- نظام الملفات
- برنامج تشغيل الاجهزة
- ادارة الذاكرة

- وظيفة الامان
- النظام الفرعي للشبكة

ادارة العمليات :

متى تكون العملية ؟

يتم وضع البرامج في وسائط تخزين مثل الاقراص الصلبة والاقراص المدمجة وما الى ذلك ، وتوجد كنوع من انواع الملفات الفعلية

العملية : بعد بدء تشغيل البرنامج يتم تحميل اذونات وسمات المنفذ ورمز البرنامج والبيانات المطلوبة للبرنامج في الذاكرة ويمنح نظام التشغيل الوحدة في هذه الذاكرة رمز التعريف والعملية هي برنامج قيد التشغيل .

الفصل الثاني عشر والثالث عشر

- **مصطلحات الشبكة الرئيسية :**

الشبكة المحلية LAN

هي شبكة بنطاق جغرافي صغير وتنتشر في المنازل ومكاتب العمل .

الشبكة الواسعة WAN

هي مجموعة من الشبكات الضخمة الممتدة على مساحات واسعة ومن امثلتها شبكة مزود الخدمة الخاص بك

IP Address

يستخدم للتعبير عن العنوان الخاص بجهازك على الشبكة ، وكل جهاز على الشبكة يمتلك عنوان IP خاص به ويسهل علمية تواصل الاجهزة المختلفة مع بعضها البعض من خلال هذا العنوان

DHCP

هو عملية طلب العنوان Ip من قبل جهاز الحاسوب بمجرد الاتصال بالشبكة والاعدادات الاخرى الخاص بالشبكة وذلك من خلال الراوتر .

DNS

هو النظام الذي يقوم بتحويل domain name الى عنوان IP

Wi-Fi

هي شبكة لاسلكية ومن مميزاتها سهولة الاستخدام وقدرتها ايضا على اختراق الجدران نظرا لتغطيتها لمساحة جيدة وسرعتها التي تصل الى 54 ميجا بات في الثانية .

Host name

لكل جهاز اسم معروف على الشبكة ومن خلال هذا الاسم يمكن للأجهزة الاخرى المتصلة على الشبكة الاتصال بجهازك من خلال توجيهها الى عنوان Ip الخاص بك .

Domain name :

يشكل نوع اخر من انواع Host name والخاص بالمواقع المنتشرة على الانترنت .

Ethernet :

تمثل نوع من انواع الشبكات السلكية الواسعة الانتشار ويكون الاتصال بها عن طريق كابل من خلال المدخل الخاص ب Ethernet على جهازك .

MAC address

يطلق عليه اسم العنوان الفيزيائي يضاف هذا العنوان الى كل الاجهزة التي من الممكن ان تتصل بالشبكة ويتم استخدامه كنظام حماية لشبكة الوايفاي وذلك من خلال استخدام MAC filter

من الممكن استخدامه في المطارات ايضا حيث تسمح انظمتها باستخدام الانترنت لمدة نصف ساعة مجانا .

- **مصطلحات خصائص الشبكة :**

برتوكول المستخدم بواسطة لينكس TCP/IP

هذا البرتوكول هو عائلة من البرتوكولات الشبكة التي تقدم خدمات متنوعة

برتوكول TCP

هو بروتوكول التحكم في الارسال وهو برتوكول امن مهيأ للاتصال ويتم ارسال البيانات المراد نقلها اولا بواسطة التطبيق كتدفق بيانات .

يحدد هذا البرتوكول ما اذا كانت اي من البيانات قد فقدت اثناء الارسال او انه لا يوجد اي خلط فيها .

برتوكول UDP

بروتوكول مخطط بيانات المستخدم وهو برتوكول غير متصل وغير امن ويتم ارسال البيانات المراد ارسالها على شكل حزم تم انشاؤها بالفعل بواسطة التطبيق

وهذا البرتوكول غير مضمون ويحتمل فقدان البيانات وهو مناسب للتطبيقات الموجهة للتسجيل

برتوكول ICMP

هو برتوكول تحكم خاص يصدر تقارير الاخطاء ويمكنه التحكم في سلوك الاجهزة المشاركة في نقل بيانات TCP/IP .

- **ادوات الشبكة :**

امر ifconfig :

يتم استخدام هذا الامر لتهيئة الواجهة وتعيين عنوان IP للواجهة وتمكين الواجهة او تعطيلها عند الطلب .

باستخدام هذا الامر يمكنك عرض عنوان IP وعنوان الجهاز MAC المخصص للواجهة وكذلك حجم MTU

امر ping :

هو افضل طريقة لاختبار الاتصال بين عقدتين سواء كانت الشبكة محلية او شبكة واسعة

ويستخدم ping ICMP للاتصال بالأجهزة الاخرى .

الامر ssh :

يوفر هذا الامر اتصال مشفر امن بين المضيفين عبر الشبكة الغير امنه ويمكن ايضا استخدام هذا الاتصال لوصول الى المحطة الطرفية ونقل الملفات ولإنشاء نفق للتطبيقات الاخرى .

حسابات المستخدم :

نظام لينكس هو نظام تشغيل متعدد المستخدمين و متعدد المهام ومشاركة الوقت، ويجب على اي مستخدم يريد استخدام الموارد في النظام ان يتقدم بطلب لحصول على حساب مع مسؤول النظام .

مهام حسابات المستخدمين :

- مساعدة مسؤولي النظام على تتبع المستخدمين الذين يستخدمون النظام والتحكم في وصولهم الى موارد النظام
- يمكنهم مساعدة المستخدمين على تنظيم الملفات وتزويد المستخدمين بحماية امنية
- يمكنهم ادخال النظام والدليل الرئيسي لتحقيق ادارة حسابات المستخدمين

ملف passwd :

- يخزن في هذا الدليل معلومات المستخدم نظام التشغيل ويكون الملف مرئي لجميع المستخدمين
- ويخزن في هذا الملف معلومات المستخدم

استعراض معلومات حساب المستخدم :

الامر id :

هو اداة مساعدة بسيطة لسطر الاوامر لعرض معرفات مجموعة و مستخدمين حقيقين وفعالين .

```
$ id tecmint

uid=1000(tecmint) gid=1000(tecmint)
groups=1000(tecmint),4(adm),24(cdrom),27(sudo),30(dip),46(pl
ugdev),113(lpadmin),130(sambashare)
```

الامر finger

يستخدم الامر للبحث عن معلومات حول المستخدم على نظام لينكس ، ويظهر الاسم الحقيقي للمستخدم والدليل الرئيسي والشل و تسجيل الدخول والاسم و الوقت

```
$ finger tecmint

Login: tecmint                          Name: TecMint
Directory: /home/tecmint                      Shell: /bin/bash
On since Fri Sep 22 10:39 (IST) on tty8 from :0
   2 hours 1 minute idle
No mail.
No Plan.
```

حسابات المجموعات :

الملف group : يخزن معلومات حول مجموعات المستخدمين المحليين مثل اسم المجموعة وكلمة المرور و رقم تعريف المجموعة وقائمة المستخدمين في المجموعة .

يتم استخدام الامر group لإظهار جميع المجموعات التي ينتمي اليها المستخدم، انظر الصورة التالية :

```
$ groups tecmint

tecmint : tecmint adm cdrom sudo dip plugdev lpadmin
sambashare
```

استخدام الامر su :

هذا الامر هو اختصار الى super user وهذا الامر يسمح بالتغيير من الحساب الحالي الى حساب اخر يسمى الحساب المستهدف وتشمل الحسابات المستهدفة حساب المستخدم الجدر (المسؤول) .

```
su [username]
```

حيث يُستبدل [username] باسم حساب المستخدم المراد التبديل إليه والوصول إلى صلاحياته.

استخدام الامر sudo :

هذا الامر هو اختصار الى super user do ويقوم هذا الامر بترقية صلاحيات المستخدم الحالي الى صلاحيات الجذر المعطاة له بصفة مؤقتة دون الحاجة لتسجيل الدخول الى حساب الجذر .

```
sudo [command]
```

استخدام الامر who :

يستخدم لعرض المستخدمين الذين قاموا بتسجيل الدخول الى النظام بما في ذلك الأجهزة الطرفية التي يتصلون من خلالها .

استخدام الامر w :

يظهر الامر w جميع المستخدمين الذين قاموا بتسجيل الدخول الى النظام وماذا يفعلون .

إدارة المجموعات :

طريقة انشاء مجموعة باستخدام الامر groupadd :

Syntax:

```
groupadd [option] group_name
```

Example:

```
sudo groupadd developers
```

تعديل المجموعة باستخدام الامر groupmod :

لتغيير اسم المجموعة من test_gr إلى test_group ، يمكننا استخدام الأمر التالي:

```
bob@ubuntu:~$ sudo groupmod -n test_group test_gr
```

استخدام الامر delgroup لحذف المجموعة :

في هذا الامر لا يمكن حذف المجموعة الأساسية للمستخدم الحالي بل يجب حذف المستخدم أولا او تغيير مجموعته الأساسية .

```
bob@ubuntu:~$ sudo delgroup test_group
Removing group `test_group' ...
Done.
bob@ubuntu:~$
```

ملكية الملفات :

يحتوي كل ملف في لينكس على ملكيتين احدهما ملكية المستخدم والأخر ملكية مجموعة المستخدم .

الامر group :

يقوم هذا الامر بسرد جميع المجموعات التي يكون المستخدم عضوا فيها وهو امر يطبق بدون وسائط.

الامر chgrp :

يقوم هذا الامر بتغيير ملكية مجموعة المستخدم لملف ، ولكن لابد من الحصول أولا على اذن المسؤول لإضافة المجموعات او حذفها ويمكن تسجيل الدخول كجذر لهذا الغرض .

الامر chown :

يستخدم هذا الامر لتغيير مالك الملف او المجموعة .

Example: To change owner of the file:

```
chown owner_name file_name
```

التصاريح :

Read يسمح للمستخدم بقراءة الملفات والأدلة ولن يسمح له بقراءة الدلائل والأدلة الفرعية المخزنة فيه .

Write يسمح للمستخدم بتعديل وحذف الملف كما يسمح للمستخدم بتعديل محتوياته.

Execute يسمح هذا التصريح بالأذن للملف بالتنفيذ (أي تشغيله)

User يؤثر هذا النوع من اذونات الملف على مالك الملف

Group : يؤثر هذا النوع من اذونات الملف على المجموعة التي تمتلك الملف .

الروابط الثابتة والروابط الرقمية :

- الرابط الثابت في لينكس عبارة عن ادخال دليل مكرر ، كلا ادخالات الدليل تشير الى نفس الملف .
- الارتباط الرقمي في لينكس هو نوع خاص من الملفات تشير الى ملفات أخرى بدلا من الإشارة الى البيانات الموجودة على القرص الصلب على عكس الروابط الثابتة .

الأسئلة

1. نظام تشغيل لينكس مغلق المصدر			
صح	خطأ		
2. سرعة تطور نظام لينكس يرجع الى كونه نظام حر			
صح	خطأ		
3. من امثلة التوزيعات المتواجدة في لينكس هيDebian			
صح	خطأ		
4. الحد الأدنى للذاكرة Ram في لينكس هي			
3 GB	1 GB	5 GB	4 GB
5. مستخدمي نظام تشغيل windows يحتاجون الى برامج حماية قوية للنظام			
صح	خطا		
6. يستخدم الامر env لاستعراض كل المتغيرات التي ينشأها المستخدم			
صح	خطأ		
7. هو مفسر سطر أوامر مطور ضمن مشروع GNU			
CLI	linux	terminal	shell
8. يقوم الامر ..... يعرض المزيد من المعلومات عن أي امر نريد في لينكس			
man	info	whereis	env
9. تتميز صيغة الضغط .....بسرعتها وشهرتها وكثرة استعمالها			
GZIP	XZ	TAR	ZIP
10. ما هو الامر الصحيح لاستدعاء محرر النصوصnano			
Nano file1	Nano -file1	Nano =file1	Nano file1/
11. ينظم الجهد الكهربي في الجهاز :			
مروحة التبريد	المعالج	الطاقة مزود	الام اللوحة
12. تتميز شبكة .....بقدرتها على الامتداد لمساحة جغرافية ضيقة			
WAN	MAN	LAN	INTERNET
13. شبكة wifi تمتلك القدرة على اختراق الجدران نظرا للتغطية الجيدة الخاصة بها			
صح	خطأ		
14. نظام لينكس امن جدا لأنه يمكن تقييد الوصول لكل الملفات في النظام			
صح	خطا		
15. لا يظهر الامر finger الاسم الحقيقي للمستخدم			
صح	خطا		
16. يمكن لحسابات المستخدمين في لينكس مساعدة مسؤولي النظام			
صح	خطا		
17. برنامج kwrite هو مثال على محرر نصوص في سطر الأوامر			
صح	خطا		
18. الرقم الفريد الذي يحدد نقطة الوصول إلى واجهة الشبكة الخاصة بك			

network mask	ip address	WAN	LAN
19. يحدد برتوكول ..... اذا ما كانت أي بيانات قد فقدت اثناء الارسال			
FTB	IP	UDP	TCP
20. يخزن ملف ..... معلومات مستخدم نظام التشغيل ويكون الملف مرئي للجميع			
passwd	groups	finger	pass words
21. أمر يُحدد المسار الذي يجب الانتقال إليه :			
cp	cd	rm	mv
22. يعرض محتويات المسار الحالي من ملف ومجلدات :			
ls	cd	rm	mv
23. من أنواع أدوات المساعدة Info command			
صح	خطأ		
24. من الصعب الحاق الضرر بنظام لينكس لان مستخدمي لينكس لديهم حق الوصول الى الجذر			
صح	خطأ		
25. الشبكة المحلية هي مجموعة الشبكات الضخمة الممتدة على مساحات واسعة			
صح	خطأ		
26. الحوسبة السحابية هي جزء من بنية تحتية مادية			
صح	خطأ		
27. تجميع العديد من الملفات في ملف واحد بغرض عمل نسخة من هذه الملفات وتخزينها احتياطا			
ضغط الملفات	أرشفة الملفات	الحافظة	البرنامج
28. الملفات الأكثر استخداما في نظام لينكس			
ملفات الدليل	ملفات العامة	ملفات الجهاز	المحمية ملفات
29. نظام مناسب للأشخاص المهتمون بالحماية الأمنية الإلكترونية والمُخترقين			
ابل	اندرويد	لينكس	ويندوز
30. من مميزات استخدام البرمجيات الحرة والمفتوحة المصدر			
انخفاض تكاليف البرامج	سهولة الاستخدام	سرعة الوصول للبرامج	وضوح النظام
31. نظام لينكس يعمل على أجهزة ذات عتاد قوي من حيث معالجة البيانات والرسوميات			
صح	خطأ		
32. المحاكاة الافتراضية هي وسيلة فصل تطبيق ما والموارد اللازمة لتشغيله من مضيف الاجهزة الأساسي			
صح	خطأ		
33. يقوم بسرد جميع محتويات المسار الحالي بما في ذلك الملفات المخفية ls-a			
صح	خطأ		
34. لطباعة قيمة المتغيّر PATH يكتب الأمر echo $PATH			
صح	خطأ		
35. هو دمج البيانات في موقع مركزي ، حيث يمكن لعدة مستخدمين الوصول اليها:			

المحاكاة الافتراضية للأجهزة	المحاكاة الافتراضية لسطح المكتب	المحـــاكـــاة الافتراضـــيـــة للبرامج	المحـــاكـــاة الافتراضـــيـــة للتخزين
36. ملفات الدخول هي أداة قيمة لاكتشاف الأخطاء واصلاحها عندما تواجه مشكلة في النظام			
صح	خطا		
37. الامر .... يطبع عدد من الرسائل على الشاشة التي تعرض معلومات حول الأجهزة التي يكتشفها النواة اثناء عملية التمهيد			
dmesg	mkdr	rmdir	ZIP

ملخص لمقرر أساسيات الأمن السيبراني

الفصل الأوّل
مقدمة في الأمن السيبراني

- **مفهوم الأمن السيبراني والهدف منه**

عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية. تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية. يمثل تنفيذ تدابير الأمن السيبراني تحديًا كبيرًا اليوم نظرًا لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكارًا.

- **أهداف الأمن السيبراني**
- يشمل كافة الأمور المرتبطة بحماية البيانات من المهاجمين المُختصين في سرقة المعلومات والتسبب بالضرر، إذ يمكن أن تكون هذه البيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية، أو بيانات تعريف شخصية، أو حقوق ملكية فكرية.
- يُشكّل وجود برامج الأمن السيبراني وآليات الدفاع الإلكترونية وسيلة متطورة ذات أهمية كبيرة في حماية البيانات وخدمة مصلحة الجميع، إذ يعتمد جميع أفراد المجتمع على البُنية التحتية الحيوية كالمستشفيات، ومؤسسات الرعاية الصحية، وبرامج الخدمات المالية التي يجب المحافظة عليها.
- تقليل مخاطر الهجمات الإلكترونية على الصعيد الفردي، إذ يمكن أن تتسبب هذه الهجمات إلى تعرض الأفراد لسرقة هوياتهم وابتزازهم، وبالتالي إحداث أضرار وخيمة في حياة الأفراد.
- **متطلبات وركائز الأمن السيبراني**

الأشخاص:

يمثّل هذا العنصر الأشخاص المعنيين بإدارة شبكة الأمن السيبراني، بحيث يجب أن يتوفر لديهم القدرة على التحقق من التهديدات الإلكترونية والدخول غير المصرّح به للأنظمة ومعالجتها، وتأمين الرد السريع للحوادث والهجمات.

السُلطة:

يجب تعيين شخص مسؤول عن تنفيذ عملية الأمن السيبراني، حيث يجب منحه النفوذ اللازم والصلاحيات للقيام بالتغيرات التنظيمية المطلوبة، وتطبيق برنامج الأمن السيبراني بسهولة.

الدعم من الإدارة العليا:

يجب الحصول على الدعم والتأييد من مجلس الإدارة، وفريق القيادة، وما يليه في التسلسل الإداري في الشركات، إذ يجب أن يتمتع برنامج الأمن السيبراني بالدعم التام لضمان نجاح تطبيقه.

العملية الفعّالة:

يجب أن يشتمل برنامج الأمن السيبراني على نهج فعّال يضمن إدارة عملية الأمن ومواجهة المخاطر الإلكترونية، بحيث يجب أن تحدد عملية الاستجابة للحوادث الإلكترونية الفعّالة كيفية استخدام الأشخاص للأدوات والتقنيات، وكيفية التصدي للهجمات الإلكترونية المُكتشفة.

التقنيات المناسبة:

يجب أن تكون التقنيات المُستخدمة في برنامج الأمن السيبراني قادرة على مواجهة 75٪ من التهديدات المُكتشفة، والتحقيق فيما نسبته 25٪ من التهديدات المحتملة، والتي تشكّل خطورة، وبالتالي يجب التحقق من صحتها من قِبل الأشخاص ذوي الخبرة.

التواصل في الوقت المناسب:

تضمن عملية التواصل الداخلية في برنامج الأمن السيبراني والتي تحدث في الوقت المناسب نجاح برنامج الأمن، إذ يجب التنسيق بين فريق الأمن السيبراني وبين الجهات التي تتطلب الحماية من خلال مسؤولي الشبكات، ومهندسي الأنظمة، ومكتب المساعدة، والإدارة، وغيرهم.

الميزانية:

يتطلب نجاح برنامج الأمن السيبراني على المدى الطويل تخصيص ميزانية مناسبة له، والذي يعد أحد أهم عناصر الأمن السيبراني.

- خطوات تحقيق الأمن السيبراني في المنظمات

هناك عشر توصيات لتحقيق الامن السيبراني داخل المنظمات:

- تزويد جميع المستخدمين بمستويات تناسب أدوارهم والتحكم في منح امتيازات النظام وإدارتها.
- وضع استراتيجية لإزالة أو تعطيل الوظائف غير الضرورية لتجنب التضارب بين الأنظمة والمعلومات.
- التأكد من وجود نظام لإدارة المخاطر
- تأمين الشبكة للحد من فرص تعرض الأنظمة للتهديد السيبراني.
- وضع سياسات وعمليات فاعلة لإدارة الحوادث الأمنية
- رفع وعي وثقافة المستخدم عن كيفية حماية البيانات
- التصدي للبرامج الضارة لتقليل المخاطرة عبر تطوير وتنفيذ سياسات مكافحة البرامج الضارة

- إنشاء سياسات تدعم العمل المتنقل أو الوصول عن بعد إلى الأنظمة
- الالتزام بضوابط الوسائل المتعددة القابلة للإزالة
- المراقبة ومتابعة الأنظمة والكشف عن الهجمات الفعلية على الأنظمة والخدمات الإلكترونية.

إدارة المخاطر

أن الخطوة الأولى تتمثل في نظام إدارة المخاطر لتقييم المخاطر التي تتعرض لها معلومات وأنظمة المنظمة بتحديد نظام ملائم لإدارة المخاطر والتأكد من أن جميع منسوبي المنظمة على علم تام بهذا النظام.

التنظيم الآمن للمنظمة

فيما تتركز الخطوة الثانية في التنظيم الآمن للمنظمة ويتم بها وضع استراتيجية لإزالة أو تعطيل الوظائف غير الضرورية لتجنب التضارب بين الأنظمة والمعلومات.

تأمين الشبكات

تعتبر تأمين الشبكة هي الخطوة الثالثة لتحقيق الأمن السيبراني للحد من فرص تعرض الأنظمة للتهديد السيبراني، وبما أن الشبكات تغطي العديد من المواقع وتستخدم الاتصالات المتنقلة والخدمات السحابية، لذا يتطلب من المنظمات إنشاء وتنفيذ السياسات والاستجابات الهندسية والتقنية المناسبة التي تحمي شبكات المنظمة

إدارة صلاحيات المستخدم

تتمثل الخطوة الرابعة في إدارة صلاحيات المستخدم، فإذا تم تزويد المستخدمين بامتيازات نظام غير ضرورية أو حقوق وصول إلى البيانات، فإن ذلك يؤدي لزيادة خطر إساءة الاستخدام

التثقيف الإلكتروني

الخطوة الخامسة تتلخص في وضع سياسات وعمليات فاعلة لإدارة الحوادث الأمنية،

رفع وعي وثقافة المستخدم

فيما تأتي الخطوة السادسة في رفع وعي وثقافة المستخدم عن كيفية حماية البيانات، إذ إن المستخدم يعتبر عاملا أساسيا في رفع مستوى الأمن المعلوماتي.

التصدي للمحتوى الضار

أن التصدي للبرامج الضارة هي الخطوة السابعة والمحققة للأمن السيبراني، وتتمثل في التصدي لأي كود أو محتوى له تأثير ضار وغير مرغوب فيه على الأنظمة، وأن أي تبادل

للمعلومات يحمل في طياته درجة من المخاطرة وقد تؤثر على أنظمة المنظمة،

المراقبة ومتابعة الأنظمة

كما أن المراقبة ومتابعة الأنظمة والكشف عن الهجمات الفعلية على الأنظمة والخدمات الإلكترونية والتي تعتبر الخطوة الثامنة، أمر ضروري من أجل الاستجابة بفعالية للهجمات إضافة لإتاحتها لضمان استخدام الأنظمة بشكل مناسب وفقا للسياسات التنظيمية.

دعم العمل المتنقل

الخطوة التاسعة والعاشرة تتمثل في أهمية الالتزام بضوابط الوسائل المتعددة القابلة للإزالة، وسياسات ومراقبة العمل عن بعد، وذلك يعني إعداد سياسة للتحكم في الوصول إلى الوسائط القابلة للإزالة وهي وسائط التخزين الحاسوبية التي بالإمكان تنصيبها وإزالتها من الحاسوب والتي من المهم فحصها بحثا عن البرامج الضارة قبل استخدامها

- أمن المعلومات والأمن السيبراني

مفهوم أمن المعلومات

نشأ مفهوم أمن المعلومات في بدايته عن طريق وكالة الاستخبارات المركزية الأمريكية ((CIA، بهدف حماية المعلومات من التهديدات والمخاطر التي من الممكن التعرض لها، كما يمكننا تعريفه على أنه العلم المختص بحماية وتأمين المعلومات الالكترونية عن طريق عدة أدوات واستراتيجيات تتبعها الدولة لضمان أمن وسلامة وسرية المعلومات الخاصة بها.

امن المعلومات: حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، او العبث المعلومات اثناء التخزين او المعالجة او النقل. والحفاظ على المعلومات وسريتها وتشفيرها بجميع اشكالها.

الامن السيبراني: فالأمن السيبراني يعتني بأمن كل ما يوجد ف الفضاء المعلوماتي ومن ضمنه" أمن المعلومات الرقمية".

- الفرق بين الأمن السيبراني وأمن المعلومات

من السيبراني	ن المعلومات
عى إلى حماية البيانات، ومصادر التخزين، أجهزة من مخاطر الهجمات الإلكترونية ي الفضاء السيبراني.	عى إلى حماية البيانات من أي نوع من اع التهديدات سواء كانت رقمية أم ظرية أو قياسية
عامل مع الجرائم الإلكترونية، والاحتيال كتروني، وتنفيذ القانون.	عامل مع عملية الوصول غير المصرّح به، كشف عن أي تعديل أو خلل.
تمد تطبيق الأمن السيبراني على وجود خاص محترفين ومدربيّن على التعامل ع التهديدات وبالأخص تهديدات (APT) تقدمة.	فّر أمن المعلومات قاعدة أساس ن البيانات، ويتم من خلاله تدريب شخاص ى تحديد أولويات الموارد قبل مواجهة هديدات أو الهجمات.

- تهديدات أمن المعلومات

الفيروسات

تعتبر من أهم تهديدات أمن المعلومات فهي عبارة عن برامج مكتوبة بإحدى لغات البرمجة، الهدف منها هو إلحاق الضرر بالمعلومات الموجودة في الحاسوب، ولها 3 خواص وهي التخفي والتضاعف وإلحاق الأذى، حيث أنه لابد أن يكون مختفى داخل الجهاز وبمجرد إضافة الملف يتضاعف حجمه، كما انه يلحق الاذى بهذه الملفات أو بجهاز الحاسوب ككل.

اختراق المعلومات المرسلة

تحدث عن طريق اختراق شبكة معلوماتية معينة ومراقبة ما يحدث عليها او عن طريق اختراق حساب شخصي ومتابعة الرسائل التي تنتقل منه أو إليه مما يهدد أمن هذه المعلومات المرسلة وسهولة التجسس على الهيئات والمؤسسات وليس الأشخاص فحسب.

تهديد التجسس

يعتبر واحد من أهم تهديدات أمن المعلومات حيث إنه لا يصيب الضرر بالجهاز، فمن الممكن ألا يتم التعرف عليه أو اكتشافه لأنه يقتصر على مراقبة الجهاز ومتابعة معلوماته دون إلحاق ضرر به، وهو من أخطر التهديدات لأمن وسرية المعلومات السياسية أو الشخصية وغيرها.

السيطرة الكاملة

يحدث هذا التهديد عن طريق إرسال ملف صغير من قبل المخترق إلى جهاز الضحية عبر أحد الرسائل مثلًا أو يقوم بإرسال رابط يحتوي على فيروس يمكنه من مراقبة جهاز المستخدم ومتابعة تفاصيلها، وبإمكانه من خلال هذا التهديد أيضًا تعطيل أحد الخدمات على جهاز المستهدف مما يعيق تعامله بحرية على جهازه.

هجوم التضليل

يحدث هذا الهجوم أو التهديد عن طريق انتحال موقع موثوق أو شخصية ما موثوقة، حتى يتمكن المخترق من خلالها من الحصول على معلومات الحسابات الشخصية أو غيرها من المعلومات السرية والحساسة.

- **أنماط التهديدات الأمنية وأبعاد أمن المعلومات**

تتراوح التهديدات الأمنية الشائعة من التهديدات الداخلية إلى التهديدات المستمرة المتقدمة، ويمكنها أن تسبب الخسائر ما لم يكن فريق الأمن الداخلي على علم بها ومستعد للرد. حيث أن التهديد الأمني هو عمل خبيث يهدف إلى إفساد أو سرقة البيانات أو تعطيل أنظمة المؤسسة أو المنظمة بأكملها. والحدث الذي ينتج عنه خرق للبيانات أو الشبكة يسمى الحادث الأمني، أهم 10 أنواع من تهديدات أمن المعلومات:

1. **التهديدات الداخلية:**

يحدث التهديد من الداخل عندما يسيء الأفراد المقربون من مؤسسة ما الذين أذن بالوصول إلى شبكتها عن قصد أو عن غير قصد استخدام هذا الوصول للتأثير سلبًا على البيانات أو الأنظمة المهمة للمؤسسة. الموظفون المهملون الذين لا يمتثلون لقواعد وسياسات عمل مؤسساتهم يتسببون في تهديدات داخلية. على سبيل المثال، قد يرسلون بيانات العملاء عبر البريد الإلكتروني عن غير قصد إلى أطراف خارجية، أو ينقرون على روابط التصيد الاحتيالي في رسائل البريد الإلكتروني أو يشاركون معلومات تسجيل الدخول الخاصة بهم مع الآخرين.

2. **الفيروسات والديدان:**

الفيروسات والديدان هي برامج ضارة تهدف إلى تدمير أنظمة وبيانات وشبكات المؤسسة. حيث أن فيروس الكمبيوتر هو رمز ضار يتكرر عن طريق نسخ نفسه إلى برنامج أو نظام أو ملف مضيف آخر. ويظل كامنًا حتى يقوم شخص ما بتنشيطه عن قصد أو عن غير قصد، وينشر العدوى دون علم أو إذن من المستخدم أو إدارة النظام. بينما دودة الكمبيوتر هي برنامج يتكاثر ذاتيًا ولا يحتاج إلى نسخ نفسه إلى برنامج مضيف أو يتطلب تفاعلًا بشريًا للانتشار. وتتمثل مهمتها الرئيسية في إصابة أجهزة الكمبيوتر الأخرى مع استمرار نشاطها على النظام المصاب. وغالبًا ما تنتشر الديدان باستخدام أجزاء من نظام التشغيل تكون تلقائية وغير مرئية للمستخدم. وبمجرد دخول الدودة إلى النظام، فإنها تبدأ

على الفور في تكرار نفسها، ممّا يؤدي إلى إصابة أجهزة الكمبيوتر والشبكات غير المحمية بشكل كافٍ.

3. **بوت نت:**

وتسمى الروبوتات وهي عبارة عن مجموعة من الأجهزة المتصلة بالإنترنت، بما في ذلك أجهزة الكمبيوتر والأجهزة المحمولة والخوادم وأجهزة تقنيات عمليات التي تقوم إصابة وعن بعد التي تسيطر عليها نوع شائع من البرامج الضارة. وعادةً ما تبحث برامج الروبوتات الضارة عن الأجهزة المعرضة للخطر عبر الإنترنت. الهدف من إنشاء عامل التهديد الذي ينشئ شبكة الروبوتات هو إصابة أكبر عدد ممكن من الأجهزة المتصلة، باستخدام قوة الحوسبة وموارد تلك الأجهزة للمهام الآلية التي تظل مخفية عمومًا لمستخدمي الأجهزة.

4. **هجمات التنزيل:**

في هجوم التنزيل من محرك الأقراص، يتم تنزيل التعليمات البرمجية الضارة من موقع ويب عبر متصفح أو تطبيق أو نظام تشغيل متكامل دون إذن المستخدم أو علمه. ولا يتعين على المستخدم النقر فوق أي شيء لتنشيط التنزيل. مجرد الوصول إلى موقع الويب أو تصفحه يمكن أن يبدأ التنزيل. ويمكن لمجرمي الإنترنت استخدام التنزيلات من خلال محرك الأقراص لضخ أحصنة طروادة المصرفية وسرقة المعلومات الشخصية وجمعها بالإضافة إلى تقديم مجموعات استغلال أو برامج ضارة أخرى إلى نقاط النهاية.

5. **.هجمات التصيد:**

تعد هجمات التصيد الاحتيالي نوعًا من تهديد أمن المعلومات الذي يستخدم الهندسة الاجتماعية لخداع المستخدمين لكسر ممارسات الأمان العادية والتخلي عن المعلومات السرية، بما في ذلك الأسماء والعناوين وبيانات اعتماد تسجيل الدخول وأرقام الضمان الاجتماعي ومعلومات بطاقة الائتمان والمعلومات المالية الأخرى. وفي معظم الحالات، يرسل المتسللون رسائل بريد إلكتروني مزيفة تبدو وكأنها قادمة من مصادر مشروعة، مثل المؤسسات المالية و eBay (و PayPalوحتى الأصدقاء والزملاء.

6. **.هجمات حجب الخدمة الموزعة :**

في هجوم رفض الخدمة الموزع (DDoS)، تهاجم العديد من الأجهزة المخترقة هدفًا، مثل خادم أو موقع ويب أو مصدر شبكة آخر، ممّا يجعل الهدف غير قابل للتشغيل تمامًا. وقد يجبر تدفق طلبات الاتصال أو الرسائل الواردة أو الحزم المشوهة النظام المستهدف على الإبطاء أو التعطل والإغلاق، ممّا يحرم المستخدمين أو الأنظمة الشرعية من الخدمة.

7. **برامج الفدية:**

في هجوم برامج الفدية، يتم قفل كمبيوتر الضحية، عادةً عن طريق التشفير، ممّا يمنع الضحية من استخدام الجهاز أو البيانات المخزنة عليه. ولاستعادة الوصول إلى الجهاز أو البيانات، يتعين على الضحية دفع فدية للمتسلل، عادةً بعملة افتراضية مثل .(Bitcoin) يمكن أن تنتشر برامج الفدية عبر مرفقات البريد الإلكتروني الضارة وتطبيقات البرامج المصابة وأجهزة التخزين الخارجية المصابة ومواقع الويب المخترقة.

8. **مجموعات استغلال:**

هي أداة برمجة تسمح للشخص من دون أي خبرة كتابة التعليمات البرمجية البرمجيات لإنشاء وتخصيص وتوزيع البرامج الضارة. ومن المعروف أن مجموعات استغلال من جانب مجموعة متنوعة من الأسماء، بما في ذلك عدة العدوى، مجموعة برمجيات الجريمة وأدوات البرمجيات الخبيثة. ويستخدم مجرمو الإنترنت مجموعات الأدوات هذه لمهاجمة نقاط الضعف في النظام لتوزيع البرامج الضارة أو الانخراط في أنشطة ضارة أخرى، مثل سرقة بيانات الشركة أو شن هجمات رفض الخدمة أو بناء شبكات الروبوت.

9. **هجمات التهديد المستمر المتقدمة:**

التهديد المستمر المتقدم (APT) هو هجوم إلكتروني مستهدف يخترق فيه متطفل غير مصرح به شبكة ويظل غير مكتشفة لفترة طويلة من الزمن. بدلاً من التسبب في تلف نظام أو شبكة، فإن الهدف من هجوم (APT) هو مراقبة نشاط الشبكة وسرقة المعلومات الوصول، بما في ذلك مجموعات الاستغلال والبرامج الضارة. وعادةً ما يستخدم مجرمو الإنترنت هجمات (APT) لاستهداف أهداف عالية القيمة، مثل الشركات الكبيرة والدول القومية، لسرقة البيانات على مدى فترة طويلة.

10. **هجوم: (Malvertising)**

وهي تقنية يستخدمها مجرمو الإنترنت لإدخال تعليمات برمجية ضارة في شبكات الإعلانات وأيضاً في صفحات الويب المشروعة عبر الإنترنت.

- **مفهوم الفضاء السيبراني**

يُعرّف الفضاء السيبرانيCyperspace :بأنه عالم الحاسوب الافتراضي، أو الوسيلة الإلكترونية المُستخدمة لتسهيل التواصل عبر شبكة الإنترنت، ويشمل الفضاء السيبراني شبكة حاسوب كبيرة مكونة من عدّة شبكات حاسوب فرعية منتشرة في جميع أنحاء العالم يعتمد الفضاء السيبراني على بروتوكولTCP /IP ؛ لتسهيل تبادل البيانات والملفات، والتواصل بفاعلية بين مجموعة كبيرة من المستخدمين، وتتيح لهم تبادل المعلومات والأفكار؛ والمشاركة في مُختلف المناقشات؛ أو المنتديات الاجتماعية؛ وممارسة الألعاب؛ من خلال وسائط سهلة الاستخدام، وغيرها الكثير من الخدمات.

- **الفرق بين الفضاء السيبراني والإنترنت**

الإنترنت إحدى الشبكات العالمية التي تنشأ من خلال ربط شبكات أصغر من الحواسيب والخوادم، بينما الفضاء السيبراني حيّز رمزي أو افتراضي

يوجد ضمن نطاق الإنترنت. الفضاء السيبراني داخل نطاق شبكة الإنترنت، وإنجاز جميع العمليات داخل حيّزه عن طريق شبكة الإنترنت، مثل: إرسال البريد الإلكتروني، أو فتح مواقع الويب.

- **الحروب السيبرانية**

ما هي الحرب السيبرانية؟ وما مدى خطورتها؟

مفهوم الحرب السيبرانية بانه عبارة عن هجمات الكترونية بقيادة عسكرية تقوم باختراق الأنظمة الالكترونية العالمية وكل ما يعتمد على التكنولوجيا، لتضر بالحواسيب والأجهزة التي تستخدم شبكة الانترنت العالمية والتي قد تفضي لنتائج كارثية، مثل سرقة بيانات خاصة، وغيرها من الكوارث التي قد تكون عالمية مثل الحروب النووية وغيرها.

- **المراحل الأساسية للأمن السيبراني**

أنواع ومراحل الأمن السيبراني يُصنف الأمن السيبراني إلى عدة أنواع، وفيما يأتي أشهرها:

أمن الشبكة:

يُعنى أمن الشبكة بتوفير الحماية لشبكة الكمبيوتر من تهديدات المتطفلين، وتكون هذه التهديدات إما من المهاجمين المُستهدفين أو من البرامج الانتهازية الضارّة.

أمن التطبيقات:

يهتم أمن التطبيقات بإبقاء البرمجيات، والأجهزة دون أي تهديدات، إذ يمكن أن يسهّل التطبيق المُخترق إمكانية الوصول إلى البيانات التي صُممّت لتأمين الحماية، وبالتالي فإنَّ برنامج الأمن الناجح يبدأ في مرحلة التصميم الأوليّة، أي قبل نشر البرامج أو الأجهزة. أمن المعلومات يركّز أمن المعلومات على تأمين الحماية لسلامة البيانات وخصوصيتها، وذلك أثناء عملية تخزينها، أو أثناء عملية تناقلها.

الأمن التشغيلي:

يندرج تحت مظلة الأمن التشغيلي العمليات والقرارات المرتبطة بمعالجة أصول البيانات وحمايتها، بالإضافة إلى الأذونات التي يحتاج لها المستخدمين للوصول إلى الشبكة، والإجراءات الخاصة بكيفية ومكان تخزين البيانات أو مشاركتها.

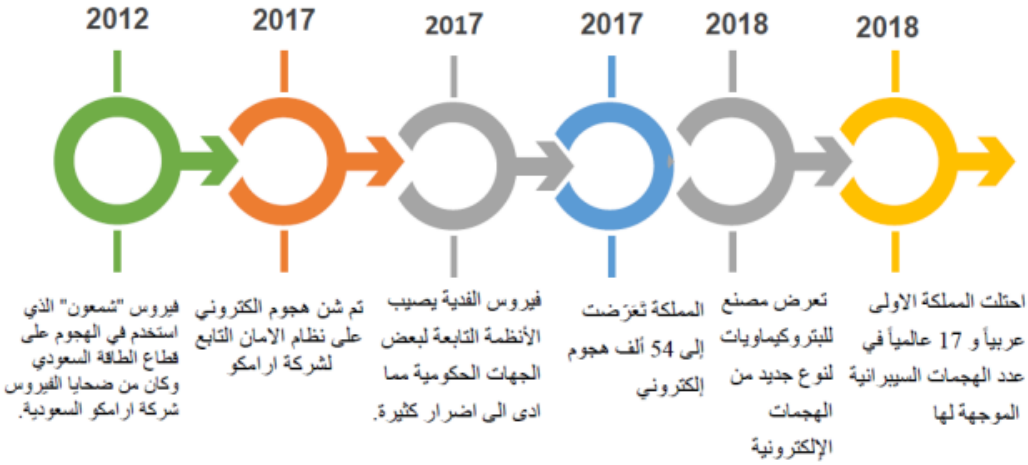
الاسترداد بعد الكوارث واستمرارية الأعمال:

يهتم هذا النوع من الأمن بتحديد الكيفية المتبّعة في استجابة المنظّمة لحادث أمن سيبراني أو أي حدث آخر يؤدي إلى فقدان العمليات أو البيانات، إذ تضع سياسات التعافي من الكوارث طرق استرداد المؤسسة لعملياتها ومعلوماتها بهدف استمرارية العمل.

تعليم أو تثقيف المستخدم الجديد :

يجب الأخذ بعين الاعتبار تعليم الأشخاص، إذ يمكن أن يتسبّب أي شخص دون قصد بإدخال أحد الفيروسات إلى نظام الأمن نتيجة عدم اتبّاع ممارسات الأمن الصحيحة، بحيث تعد عملية تعليم المستخدمين لآلية حذف مرفقات رسائل البريد الإلكتروني المشبوهة، وعدم توصيل محركات الأقراص مجهولة المصدرUSB وغيرها من أهم الأمور الواجب تعلّمها

- جهود المملكة العربية السعودية في الأمن السيبراني



الفصل الثاني
حماية الأنظمة واستراتيجيات الأمن السيبراني

- **مفهوم حماية الأنظمة**

نحن اليوم بحاجة إلى الحماية أكثر من أي وقت مضى، خاصة عند الحديث عن العالم الالكتروني والشبكة العنكبوتية التي يؤثر اختراقها على كل نواحي الحياة بالنسبة لنا. والتي من الممكن ان يتضرر الجانب النفسي والمادي والعملي لدينا في حال تم تسريب أي من محتوانا الخاص او بياناتنا الشخصية المرفقة والمحفوظة على منصاتنا الشخصية على الانترنت.

مفهوم حماية الأنظمة بأنه علم مختص ب تأمين المعلومات الم تداوله عبر شبكة الانترنت من المخاطر التي تهددها. أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

- **أنظمة المعلومات ومكوناتها**

1- المكونات المادية:

يساهم وجود الأجهزة في تحقيق السرعة لنظم المعلومات، والدقة والسعة التي تحتاجها، لوجود كميّات هائلة من البيانات، وتضمّ المكونات المادية أجهزة الملحقات الطرفية كأجهزة الإدخال والاخراج، وأجهزة التخزين الثانوية، والمعالجات والذاكرة الرئيسية،

2- المكونات البرمجية:

تشمل المكونات البرمجية (software Computer) ما يأتي: برنامج النظام: وهي أنظمة التشغيل، مهمتها تقديم الدعم والتحكّم في عمليات نظام الكمبيوتر.

برامج التطبيقات: تهدف هذه البرامج لتوجيه أجهزة معينة للعمل بها من المستخدم النهائيّ، مثل: برنامج تحليل المبيعات، وبرنامج الرواتب.

الإجراءات: هي التعليمات الخاصة، حيث يعمل عليها ممّن يستخدمون نظام المعلومات فإما أن تكون هذه الإجراءات على شكل نموذج ورقيّ أو برنامج حاسوبيّ.

3- البيانات:

قواعد البيانات ومستودعات البيانات قواعد للبيانات (Databases) هي مستودع المادة الأساسية التي تعمل بها المكونات الأخرى، وتعدّ مجمع البيانات التي تسترجع من خلال الاستعلام عنها حسب ضوابط محددة، في حين أنّ مستودع البيانات warehouses data تشمل

جميع البيانات بأي شكل تحتاجه المؤسسة وقد برزت أهميتها في أنظمة المعلومات مع وجود البيانات الضخمة، حيث توجد بيانات هائلة من الممكن جمعها وتحليلها.

4- افراد والاجراءات:

الموارد البشرية والإجراءات يلعب قسم الموارد البشرية (Human resources and procedures) دوراً مهماً، ويرجع السبب في ذلك إلى أنّ جميع مكوّنات نظم المعلومات لا يمكن تشغيلها ووضع الإجراءات اللازمة لإدخالها، تخزينها وتحليلها دون وجود العنصر البشريّ الذي يحوّل هذه المعرفة لقواعد بيانات.

5- الشبكات:

الاتصال عن بعد ترتبط الأجهزة في نظم المعلومات ببعضها من خلال اتصال سلكي، مثل كابلات الإيثرنت (Ethernet) والألياف البصرية، أو لاسلكية، مثل شبكة الواي فاي(Fi-Wi) ، إذ يمكن إنشاء شبكة تربط ما بين أجهزة الكمبيوتر كالتي توجد بالجامعات، مثل الشبكات (local area network)المحلية

- عناصر أمن المعلومات وتهديدات الأنظمة المعلوماتية

1- عناصر امن المعلومات

تسع ى كافة وسائل أمن المعلومات لتحقيق الغاية الرئيسية المتمثلة في ضمان حماية المعلومات والمحافظة عليها. ان هدف الابحاث والاستراتيجيات ووسائل أمن المعلومات يتمثل في ضمان توفر ثلاثة عناصر رئيسية لأية معلومات، وهي :

(1) سرية المعلومات confidentiality

تشمل كافة التدابير اللازمة لمنع اطلاع الجهات غير المصرح لها على المعلومات الحساسة او السرية.

(2) تكامل وسلامة المعلومات Integrity

تشمل كافة التدابير اللازمة لحماية المعلومات من التغيير.

(3) توفر المعلومات Availability

تشمل كافة التدابير اللازمة لضمان التأكد من استمرار القدرة على تقديم الخدمات والتفاعل مع المعلومات والوصول إليها

(4) عدم انكار التصرف المرتبط بالمعلومات ممن قام به Non – Reputation ضمان عدم انكار الشخص انه قام بتصرف ما متصل بالمعلومات .

2- تهديدات أمن المعلومات

تتزايد التهديدات التي تتعرض لها المنظمات نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بالمنظمة بشكل غير مصرح به بهدف تعديلها او سرقتها او حتى تدميرها. يمكن تصنيف أساليب الاحتيال الالكتروني بهدف الحصول على المعلومات بأسلوب غير

مصرح به الي ثلاث أساليب وهي:

(1) اختراق الشبكات :(Hacking)

ويقصد به الوصول غير المصرح به للشبكة او نظام المعلومات المحاسبي بهدف تعديل البيانات، او المعلومات، او سرقتها او تدميرها.

ويحتوي هذا الأسلوب على عدة تقنيات منها كمثال لتقنيات شائعة في هذا المجال:

أ- سرقة كلمة السر: (Cracking Password)

اختراق الشبكة والاطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة.

ب- هجمات حقن قواعد البيانات: (Attack Injection Language Query structured)

مثلا من خلال إدخال برمجية ضارة مكان كلمة السر او اسم المستخدم إذ تمكن المحتال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها.

ج- التعرض للاختراق أثناء محاولة معالجة اختراق سابق. (attack-day-Zero)

(2) الهندسة الاجتماعية:

ويقصد بها تحفيز المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة شبهة.

ويحتوي هذا الأسلوب على عدة تقنيات منها:

أ- التوأمة الشريرة: (Twin Evil)

اي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به.

ب- سرقة الهوية: (Theft Identity)

اي ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر.

ج- التصيد: (phishing)

ويقصد منها وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات او التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

(3) البرمجيات الضارة :(Malware)

وهي عبارة عن برامج متخصصة لتسهيل التسلل الي النظام او الشبكة بهدف تدميرها، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جدا إزالتها.

ويحتوي هذا الاسلوب على عدة تقنيات منها كمثال على تقنيات شائعة في هذا المجال:

أ– حصان طروادة: (Horse Trojan)

وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال.

ب – الفيروسات: (Viruses)

وهي برامج تدخل إلى الحاسوب ويتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات.

ج – برامج التجسس: (Spyware)

وهي البرمجيات التي تؤدى إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت.

- **العلاقة بين مستويات أمان المعلومات**

المستوى الفردي: إن التركيز على الفرد كمستوى رئيسي في التحليل الأمني جاء من المخاوف المثار حول علاقة الفرد بالحكومة، حيث إن أمن الفرد لابد أن يكون في المقدمة دائما، كما يركز على 3 نقاط:

1. الدولة لا تقدم الأمن لكافة سكانها، بل على استعداد أن تتخلى على أمن أفرادها في سبيل كيانها.
2. هناك دول تفشل في توفير الاحتياجات الضرورية لسكانها كالصومال، وأخرى تنتهك حقوق أفرادها.
3. الدول التي تدعي أنها دولاً حارسة، فإنها قد تقوم بذلك بهدف الوصول إلى أمنها كدولة، ولا يتم التركيز على أمن الأفراد بشكل خاص، ويركز "بريان" جوب على أن أمن الأفراد والفئات الاجتماعية في دول العالم الثالث، حيث يرى أن الأمن لهؤلاء لم يتحسن بعد انتهاء الحرب الباردة إلى حد الان، يعيشون في اضطهاد وعليه فإن الأمن الفرد هو وصول الإنسان إلى حالة من الطمأنينة،

وقدرته على ممارسة الخيارات المختلفة من خلال توفير سبل الحياة الاقتصادية الهانئة من خلال عمل ثابت ودخل ملائم.

• المستوى الوطني: يركز على مجمل الأخطار الداخلية والخارجية التي تمس كيان الدولة ويرى البعض أن أمن الدولة يشمل عنصرين:

1. . حماية كيان الدولة ضد أعمال العدوان وسياسات التوسع، يستلزم قيام قوة عسكرية تمكنه من أداء هذه الوظيفة.
2. حماية النسيج الداخلي للدولة وعدم تعرضها لحرب دعائية أو ضغوط اقتصادية أو عمليات إرهابية.

ويعرف الأمن الوطني على أنه: التعبير السياسي والاجتماعي عن الحالة الحقيقية التي يعيشها المجتمع وهو مفهوم ديناميكي يتفاعل ضمن دوائر ثلاث محلية، إقليمية، دولية. ويتضمن أمن المواطن ومستهلكاته وتاريخيه وتراثه ومعتقداته وحرياته الأساسية وسيادة الدولة.

• المستوى الإقليمي: يرتبط بالنظام الإقليمي في منطقة معينة ويشترط فيه:

- يشمل ثلاث دول على الأقل
- أن يتعلق بمنطقة جغرافية معينة
- أن تكون ذات صفات ومميزات مشتركة تدفعها نحو التفاعل فيما بينها.

المستوى الدولي: المقصود بالنظام الدولي هي مجموعة من الأحداث السياسية المستقلة التي تتفاعل فيما بينها بانتظام. أو هي مجموعة من التحولات والتغيرات التي يشهدها العالم والتي مازالت في طور التكوين الكوني ولم تتبلور بعد في شكل كامل. ويمكن اعتباره على أنه مجموعة من الوحدات السياسية المتدرجة لجهة القوة والمتفاعلة في علاقاته على نحو يهيئ لاتزان قواها ولانتظام علاقاتها بعيدا عن الفوضى. أعطت الأمم المتحدة تصوراً للأمن الدولي يشمل عدة آليات:

- يتعين على الدول الالتزام بمجموعة من المبادئ والوقائع منها عدم التدخل في الشؤون الداخلية للدول الأعضاء، عدم اللجوء لاستخدام القوة والتهديد، وتسوية النزاعات بالطرق الدبلوماسية.
- وجود هيئة مسؤولة عن مراقبة سلوك الدول والحفاظ على السلم والأمن الدوليين.
- وجود مجموعة من الأجهزة والآليات المساعدة التي تهدف إلى التعاون الدولي.

- **الأمان وعلاقته بالتكلفة أو بالزمن**

من الضروري اختيار الحلول الأمنية التي تناسب احتياجاتك. وإلا ، فقد تدفع الكثير مقابل شيء لا تحتاجه، أو أسوأ من ذلك ، قد تدفع القليل جدًا لحماية شبكتك بشكل صحيح.

ومن الأهمية بمكان لاي حكومة او شركة او منظمة معرفة حجم ما هو ضروري للاستثمار في الأمن السيبراني والى أي مدى هو كاف من خلال تحليل استراتيجيات الأمن السيبراني على المستوى الوطني NCSS (national cyber security strategies)، وذلك للعمل على تقييم العناصر الاقتصادية الأساسية لصياغة واعتماد نموذج من استراتيجيات الأمن السيبراني على المستوى الاقليمي، ومعالجة ذلك من منظور صنع السياسات العامة للدولة، ومحاولة قياس تكلفة انعدام الأمن السيبراني، وتقييم الكفاءة والحوافز الاقتصادية لجميع أصحاب المصلحة المعنيين .وبذلك فقد عدت قضية الامن السيبراني وعلاقته بالاقتصاد من ضمن الأهداف بالغة الاهمية لكافة اصحاب المصلحة، وذلك من اجل تحقيق الرخاء الاقتصادي للمجتمعات البشرية.

مؤشرات الأداء الرئيسية المستندة إلى الوقت إلى تحويل تركيز استراتيجية المدافع من رد الفعل إلى الاستباقي.

MTTD (متوسط الوقت اللازم للكشف) هو مقدار الوقت الذي تستغرقه الشركة لتحديد حادثة أمنية محتملة.

MTTF (متوسط الوقت حتى الفشل) هو المدة التي يمكن أن يعمل بها النظام المعيب حتى يتم إيقاف تشغيله.

MTTR (متوسط وقت الاستجابة) هو الوقت الذي يستغرقه الفريق للسيطرة على التهديد أو علاجه أو القضاء عليه بعد تحديده.

MTBF (متوسط الوقت بين الإخفاقات) يعكس موثوقية وتوافر النظام. يتم استخدامه لتقييم أداء النظام في ظل ظروف محددة مسبقًا لفترة زمنية محددة.

- التخطيط الاستراتيجي للأمن السيبراني

على الرغم من أن الخطة الإستراتيجية لأمن المعلومات لا تدعو على وجه التحديد إلى مزيد من الإنفاق لجعل الأمن "أكبر" ، إلا أنها تحدد الخطوات التي يجب اتخاذها لجعل الأمن "أفضل". تعطي هذه الخطة الأولوية لمبادرات إدارة ومراقبة وحماية أصول معلومات الدولة. ويحدد 18 استراتيجية رئيسية تأمل MNIT (Services IT Minnesota) في تحقيقها على مدى السنوات الخمس المقبلة، إذا سمحت الموارد بذلك. كما تسلط الخطة الضوء على معالم محددة للسنة التالية، وهي الأشياء التي تتوقع MNIT تحقيقها بالموارد الموجودة.

- **تنظم الخطة الاستراتيجيات والمعالم في أربعة محاور:**

1- إدارة استباقية للمخاطر:

تعمل بعض أهم استراتيجيات الأمان على منع حدوث أحداث أمنية معاكسة. مع التهديدات الأكثر تقدمًا واستمرارًا، عادةً ما تقوم المؤسسات الكبيرة بتشغيل أدوات متطورة للمساعدة في إدارة المخاطر الإلكترونية في الوقت الفعلي. ومن الأمثلة على إحدى هذه الأدوات برنامج إدارة الثغرات الأمنية، والذي يساعد المتخصصين في مجال الأمن في العثور على الثغرات الأمنية وإصلاحها قبل أن يستغلها المتسللون.

2- تحسين الوعي بالظروف:

الوعي بالظروف هو مفتاح برنامج أمان فعال. يسمح الوعي بالتهديدات، سواء الكوارث الطبيعية أو ذات الدوافع البشرية، بالتخصيص الفعال للموارد والتنفيذ الفعال للضوابط. يساعد الوعي بنقاط الضعف في تحديد أولويات جهود الإصلاح، والوعي بالأحداث الأمنية يؤدي إلى اتخاذ إجراءات استجابة مناسبة وفي الوقت المناسب.

3- الأزمة القوية والاستجابة للحوادث

ليس من الممكن منع كل حادث أمني يمكن تصوره يمكن أن يؤثر على أنظمة معلومات الدولة. يتضمن برنامج أمن المعلومات المتوازن القدرة على تحليل الظروف المحيطة بالحادث واستعادة وظائف النظام العادية في الوقت المناسب.

4- شريك للنجاح

مع ظهور الأنظمة المترابطة والإنترنت، تعمل حكومة الولاية في عالم معادي للغاية. تأتي هجمات القراصنة ضد حكومة الولاية من كل دولة، ولا تتوقف أبدًا. في كل يوم، يحاول الأفراد عديمو الضمير اختراق أنظمة الدولة لسرقة البيانات وإغلاق الخدمات الحيوية واستخدام البنية التحتية للتكنولوجيا لدينا لشن هجمات مجهولة ضد الآخرين .

- التصديق الرقمي

شهادة التصديق الرقمي: هو وثيقة إلكترونية يصدرها مقدم خدمات تصديق، تستخدم لتأكيد هوية الشخص الحائز على منظومة التوقيع الإلكتروني وتحتوي على بيانات التحقق من

توقيعه. ويصاحب كل شهادة رقمية مصدّرة عادة مفتاح عام ومفتاح خاص يستخدم أحدهما للتشفير أو التوقيع الإلكتروني والآخر لفك التشفير أو التحقق من التوقيع الإلكتروني.

- **أنظمة كشف التطفل IDS**

نظام كشف التسلل (IDS) هو برنامج مصمم خصيصاً لمراقبة حركة مرور الشبكة واكتشاف المخالفات، حيث تشير تغييرات الشبكة غير المبررة أو غير المبررة إلى نشاط ضار في أي مرحلة، سواء كان ذلك بداية هجوم أو اختراق كامل، هناك نوعان رئيسيان من أنظمة كشف التسلل (IDS)هما، نظام كشف التسلل عبر الشبكة (NIDS) ونظام كشف التسلل المعتمد على المضيف.(HIDS)

"Intrusion detection system"."لـ اختصار هي"IDS "

"Host-based intrusion detection system"."لـ اختصار هي"HIDS"

الفصل الثالث
سياسات الأمن السيبراني ومعاييره

- **مفهوم السياسة الأمنية**

تعريف السياسة الأمنية: يمكن تعريف الأمن السياسي بأنه التحرر من الخوف والحاجة، وضمان تأمين الحماية من تهديد القمع السياسي، والحماية من التعرض للصراعات والحروب والهجرة لجميع المواطنين في الوقت ذاته دون استثناء أو تمييز على اعتبارها حقاً من الحقوق المكتسبة للإنسان، مما يقود إلى الاستقرار التنظيمي للدول، ونظم الحكومات والأيديولوجيات التي تستمد منها شرعيتها.

- **أهمية السياسة الأمنية:**

فالأمن السياسي يقود إلى حرية الأفراد في تقديم الأفكار والمساعدات المختلفة لتطوير مجتمعهم وتقدّمه بين مجتمعات العالم. زيادة الدخل الاقتصاديّ للدولة من خلال المشاريع التي يتم إنشاؤها، فالمستثمرون من جميع أنحاء العالم يبحثون عن المكان المستقر ليستطيعوا بناء مشاريعهم وتحقيق الأرباح منها، لذلك عندما يكون المجتمع آمناً سياسياً

- **أنواع السياسات الأمنية**

الأمن القومي: يشير الأمن القومي إلى أمن الدولة بما في ذلك شعبها واقتصادها ومؤسساتها. من الناحية العملية، تعتمد حكومات الولايات على مجموعةٍ واسعةٍ من الوسائل بما في ذلك الدبلوماسية والقوة الاقتصادية والقدرات العسكرية.

1. **البعد العسكري** :يركز على ضرورة حماية استقلال الدولة وسلامة أراضيها ضد أي اعتداء قد يقع عليها من خلال امتلاكها للأسلحة الحديثة أو اهتمامها بخطط الدفاع سواء في أوقات النزاع أو السلم واعداد الخطط الدفاعية والدراسات اللازمة لهذا يكون مرادف لمعنى السياسة الدفاعية والهجومية .
2. **البعد السياسي** :يعتبر العنصر الأساسي الذي يحدد كيفية تنظيم وإدارة قوى الدولة ومواردها داخليا وخارجياً. ومن متطلبات تحقيقه داخلياً هو تحقيق الاستقرار السياسي مع الأخذ بالاعتبار الاتجاهات والقيم والأفكار التي تسيطر على الحياة السياسية، أما خارجياً قدرة الجهاز الدبلوماسي وكفاءته في تحقيق أهداف السياسة الخارجية للدولة والقدرة على التأثير على الدول والجماعات الخارجية.

3. **البعد الاقتصادي**: يعنى بتطوير اقتصاد الدولة في شتى القطاعات حتى لا تكون تابعة لدولة أخرى تهيمن عليها وهو يعني التنمية والازدهار، واستقرار الاقتصاد، والاكتفاء الذاتي والرفاهية
4. **البعد الاجتماعي**: يعرف في بعده هذا هو الحالة التي يكون فيها الانسان محميا – ضد أو بعيد عن – خطر يتهدده ويتمثل في حالة الهدوء والاستقرار والوئام والاتفاق والانسجام داخل المجتمع الانساني وفي العلاقة بين شرائحه وأفراده وقواه المتعددة والمختلفة ويهدف هذا البعد إلى إيجاد حالة استقرار للمجتمع وإلى تماسك نسيجه مع توازن العوامل السكانية والاجتماعية المختلفة.
5. **البعد الثقافي**: تكتسب دور كبير في تحليل الظواهر السياسية والمقصود بالأمن في البعد الثقافي هو قدرة الدولة على توفير الحماية المطلوبة للثقافة بهدف تحقيق حرية الإبداع من جهة والحفاظ على مكتسبات الشعوب الثقافية والفنية والدينية من جهة أخرى.
6. **البعد البيئي**: هو تحقيق أقصى حماية للبيئة بكافة جوانبها في البر والبحر والجو ومنع أي تعد عليها قبل حدوثه منعا لحدوث الضرر من هذا التعدي الذي قد لا يمكن تداركه من خلال اتخاذ الاجراءات الوقائية اللازمة سواء كانت من خلال سن القوانين واللوائح التي تمنع التعريفات التي تؤدي لهذا الضرر أو باستخدام وسائل الملاحظة والمتابعة والقياس أو وسائل الضبط في حال ارتكاب جرائم فيها تعدي على البيئة

- مفهوم المعايير القياسية وتصنيفها واستخدامها

قامت الهيئة الوطنية للأمن السيبراني في المملكة بتطوير المعايير الأساسية للأمن السيبراني التي تهدف إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات الداخلية والخارجية. مقسمة على خمس مكونات رئيسية، هي:

- حوكمة الأمن السيبراني
- تعزيز الأمن السيبراني
- صمود الأمن السيبراني
- الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية
- الأمن السيبراني لأنظمة التحكم الصناعي

1. حوكمة الأمن السيبراني

تعريف حوكمة الأمن السيبراني تُعرّف حوكمة الأمن السيبراني) بالإنجليزية : (Cybersecurity Governanceبأنّها النظام المكون من العمليات والإجراءات التي تُساعد المؤسسات على اكتشاف الهجمات السيبرانية، وتحديد كيفية الاستجابة لها، ومنع حدوثها.

2. تعزيز الأمن السيبراني

إدارة الأصول: للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العالقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية، والتقنية للجهة، ودقتها، وتوافره.

إدارة هويات الدخول والصلاحيات: ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access)إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.

حماية الأنظمة وأجهزة معالجة المعلومات: ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.

حماية البريد الإلكتروني: ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.

إدارة أمن الشبكات: يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة

أمن الأجهزة المحمولة: ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة.

حماية البيانات والمعلومات:

– ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة

– ملكية المعلومات والبيانات

– تصنيف البيانات والمعلومات وآلية ترميزها

– خصوصية البيانات والمعلومات

التشفير cryptography: ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية

إدارة النسخ الاحتياطية: ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية

إدارة الثغرات: ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية الهدف استغال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة

اختبار الاختراق: تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة.

وذلك وفقاً للمتطلبات التشريعية والتنظيمية

- **اللوائح والقوانين المتعلقة بالأمن السيبراني**

اهمية القوانين السيبرانية في إنها :

• اولاً: تفرض إجراءات للاستخدام وتقيس ردود الفعل العام في الفضاء السيبراني.

• ثانياً: ترتفع نسبة الأمان والحماية للمعاملات التي تجرى عبر الإنترنت.

• ثالثاً: تخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي القانون السيبراني.

• رابعاً: توفير الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة.

• خامساً: يساعد في الحد من الأنشطة السيبرانية غير القانونية من خلال بذل الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة.

• سادساً: ردود الفعل التي يتم قياسها على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها، سواء كان يتعلق بالتجارة أو بالخدمات او الامن

• سابعاً: وجود قوانين سيبرانية يعني وجود اتفاقيات دولية في هذا المجال مما يتيح تتبع جميع السجلات الإلكترونية من خلال تحقيق التعاون الدولي لتتبع الجرائم المنظمة.

• ثامناً: يساعد على إنشاء الحوكمة الإلكترونية والتي بدورها ترفع جودة حياة المستفيدين من خدمات الحكومة الالكترونية .

تعريف اللوائح: هي لوائح تشتمل على توجيهات متخصصة لحماية تقنية المعلومات وأنظمة الحاسب بغرض إجبار الشركات والمؤسسات على حماية أنظمتها

ومعلوماتها من الهجمات الإلكترونية مثل الفيروسات والديدان وأحصنة طروادة والتصيد وهجمات رفض الخدمة (DOS) والوصول غير المصرح به

- **الأطراف المعنية بتنفيذ القواعد التي يجب الالتزام بها**

نظام مكافحة الجرائم المعلوماتية:

يهدف نظام مكافحة الجرائم المعلوماتية للحد من الجرائم المعلوماتية بهدف تحديد الجرائم والعقوبات المترتبة عليها، وذلك للمساعدة في تحقيق أمن المعلومات، وحماية المصلحة العامة والأخلاق، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية الاقتصاد الوطني.

- **المعايير العالمية للأمن السيبراني**

مما لا شك فيه أن أمن المعلومات تلعب دوراً مهما في حماية أصول الشركة أو المؤسسة. وكثيراً ما نسمع في الاخبار عن الحوادث الأمنية لأمن المعلومات، مثل تشويه المواقع ، وقرصنة الخادم ، وتسرب البيانات. ولذلك المنظمات بحاجة ماسة إلى أن تدرك الحاجة إلى تكريس المزيد من الموارد لحماية أصول المعلومات. وأمن المعلومات يجب أن يصبح مصدر قلق كبير في كل من الحكومة وقطاع الأعمال. وبما أنه لا يمكن أن نضمن حماية للمؤسسة أو الشركة بنسبة 100 %. لذلك نحن بحاجة لوضع مجموعة من المقاييس أو المعايير التي يمكن من خلالها تحقيق مستوى ملائم من الأمن .ومن خلال هذه المقدمة فإننا سنذكر أهم المعايير العالمية التي تساعد على تحقيق الحد الأدنى لأمن المعلومات مثل :

الآيزو ISO والكوبيت COBIT و ITIL وكذلك بعض القوانين المرتبطة بأمن المعلومات مثل:

HIPAA, COSO, SOX FISMA

- **اللوائح والقوانين المتعلقة بأمن المعلومات:**

بما أن هناك بعض المعايير العالمية والمبادئ التوجيهية، وضرورة الالتزام بالمبادئ والمعايير التي حددتها تلك المؤسسات أو الهيئات، فإننا سنذكر بعض القوانين واللوائح للولايات المتحدة الأمريكية ومنها. HIPAA COSO, SOX FISMA

- **تصنيف المعلومات ومستوياتها**

كلمة المعلومات اصطلاحا، فهي تعني البيانات التي تمت معالجتها حتى تصبح لها معنى وأيضا مغزى معين للاستعمالات المحددة، وذلك بهدف اتخاذ القرار، وبتلك الطريقة من الممكن تداولها وأيضا تسجيلها ونشرها وتوزيعها، ويكون ذلك في إطار رسمي او حتى غير رسمي، وذلك لأنها تكون حقيقية يستند اليها الكثير من البحوث العلمية وذلك بعد عدد كبير من المراحل للتنقيب وأيضا للاستقصاء والاستقراء والتجارب والتي تم بنائها على المناهج العلمية.

- اشكال وأنواع المعلومات

1. **المعلومات التطويرية أو الإنمائية**: هي تلك المعلومات التي تعمل على تحسين المستوى العلمي وأيضا الثقافي للشخص، كما انها تعمل على توسيع مداركه بشكل كبير، مثل القراءة للكتب.

2. **المعلومات الانجازية**: هي المعلومات الخاصة التي تعمل على افادة الانسان في اعماله وأيضا في مشاريعه، او اتخاذ أي قرارات خاصة بها.

3. **المعلومات التعليمية**: وهي تلك المعلومات التي يتلقاها الطلبة في كل مراحلهم التعليمية الاكاديمية.

4. **المعلومات الفكرية**: في تلك الأفكار وأيضا النظريات الفرضية والتي يتم وضعها الانسان حول كل العلاقات التي من الممكن ان تتواجد بين عناصر المشكلة المختلفة.

5. **المعلومات البحثية**: هي تلك المعلومات التي يتم الحصول عليها من بعض التجارب الشخصية او حتى تجارب الاخرين، وسواء كانت تلك التجارب هي تجارب معملية او حتى تجارب شخصية، او حتى حصيلة تجارب الاخرين من تجارب معملية او أبحاث أدبية . كما تشمل أيضاً التجارب النفسية وعملية اجراءها وأيضا نتيجة المطلوبة منها.

6. **المعلومات الأسلوبية النظامية**: هي المعلومات التي تعمل على مساعدة الباحث على انجاز بحثه بطريقة دقيقة للغاية، كما انه يشمل الوسائل التي تستعمل للحصول على المعلومات وأيضا البيانات الصحيحة.

7. **المعلومات السياسية**: وهي تلك المواضيع التي تخص كل المواضيع السياسية وأيضا عمليات اتخاذ القرار.

8. **المعلومات التوجيهية**: هي المعلومات التي يحصل عليها الشخص من خلال توجيه الاخرين له.

- التدريب والتوعية بالأمن السيبراني

أمن المعلومات مسؤولية جماعية يعد الخطأ البشري في انتهاكات الأمن السيبراني مشكلة قديمة العهد، لذلك يجب على جميع المنظمات أن تظل يقظة وأن تثقف موظفيها للتخفيف من هذه

الأخطاء. من السهل أن نتخيل أن خروقات/انتهاكات الشبكة هي من عمل مجموعات الهاكرز المتطورة. في الواقع، يتم بدء نسبة كبيرة من الانتهاكات باستخدام استراتيجيات هجوم منخفضة التقنية مثل التصيد الاحتيالي والهندسة الاجتماعية. من خلال مطالبة المستخدم النهائي بكشف بيانات اعتماد تسجيل الدخول الخاصة به أو فتح مرفق ضار، يمكن للمهاجمين اختراق الشبكات التي يصعب اختراقها.

الفصل الرابع
أمن الحاسوب والبرمجيات

- **أمن الحاسوب**

الهدف: حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، بينما يسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها المستهدفين.

مصطلح أمن نظام الحاسوب، تعني العمليات والآليات الجماعية التي من خلالها تُحمى المعلومات والخدمات الحساسة والقيمة من النشر، والعبث بها أو الانهيار الذي تسببه الأنشطة غير المأذون بها أو الأفراد غير الجديرين بالثقة، والأحداث غير المخطط لها على التوالي.

- **أمن الملفات**

الملف هو عبارة عن كائن موجود على جهاز الكمبيوتر، يقوم بتخزين البيانات، أو المعلومات، أو الإعدادات، أو الأوامر المستخدمة في برنامج الكمبيوتر، وفي واجهة المستخدم الرسومية مثل مايكروسوفت ويندوز يتم عرض الملفات على هيئة رموز تتعلق بالبرنامج الذي يفتح

❖ على الرغم من أن طريقة تعامل البرامج مع الملفات تختلف تبعاً لنظام التشغيل ونظام الملفات المستخدم، إلا أن العمليات التالية على الملفات شائعة:

- إنشاء ملف جديد باسم معين
- تغيير خصائص الملف التي تتحكم في العمليات التي تجرى عليه
- فتح ملف واستخدام محتوياته
- قراءة أو تغيير محتويات الملف
- حفظ التعديلات المجراة على الملف
- إغلاق الملف، وبالتالي عدم القدرة على استخدامه إلا بعد فتحه مجدداً

كيفية حماية الملفات: إذا كانت لديك ملفات تفضل ألا يتمكن الآخرون من الوصول إليها، فقد يكون حماية الملفات بكلمة مرور هو أبسط طريقة للحصول على حماية معلوماتك.

- **أمن أنظمة التشغيل**

المقصود بأنظمة حماية نظم التشغيل

❖ مزايا أمان عديدة منها لحماية سرية البيانات أثناء التخزين والنقل والمعالجة
❖ لضمان أمانتها أي عدم إجراء تعديل غير مرغوب به عليها أثناء تخزينها ونقلها ومعالجتها

- لضمان توافرها وعدم خسارتها بفعل خبيث أو بشكل غير مقصود.
- إمكانية إدارة التحكم بالوصول إلى الموارد

تستهدف أغلب التطبيقات الخبيثة نظام التشغيل نفسه، إذ أن ذلك يخولها اخفاء تواجدها عن المستخدم وبقية التطبيقات مثل Antimalware كلما كان نظام التشغيل أكثر شيوعا كلما كان أكثر عرضة للاستهداف من قبل المخترقين وبالتالي أكثر عرضة لاكتشاف واستغلال ثغرات أمنية فيه، وبالتالي يحمل استخدامه بشكل عام خطورة أعلى من استخدام نظام تشغيل أقل انتشارا أو نظام تشغيل مبهم.

اختراق أنظمة التشغيل – مزايا الأمان في أنظمة التشغيل

إدارة حسابات المستخدمين

وتعني أن نظام التشغيل يتيح إمكانية إنشاء عدد من حسابات المستخدمين على الحاسب، وأن نظام التشغيل يتيح التحكم بالوصول .

تحديثات الأمان Updates Security

تقوم الشركات التي تصدر نسخ أنظمة التشغيل بإصدار تحديثات الأمان بشكل دوري أو طارئ، لسد الثغرات الأمنية ولتحسين أداء واستقرار نظام التشغيل.

حالة الدعم التقني

تقوم الجهة المصدرة لنظام التشغيل بتقديم الدعم التقني لنظام التشغيل الذي يتضمن إصدار التحديثات، لسد الثغرات الأمنية بعد اكتشافها.

سلة المهملات

وهي مجلد يحتفظ بالملفات التي يقوم المستخدمون بحذفها إلى حين افراغها. إذا هي ميزة تتيح للمستخدم استعادة ملف تم حذفه سابقا طالما كان الملف موجودا في سلة المهملات. وهذا يعني أن احتمال فقدان ملف بسبب حذفه بالخطأ يصبح صغيرا.

النسخ الاحتياطي

يعتبر إجراء النسخ الاحتياطية Backups للبيانات من أفضل الطرق لضمان عدم ضياع البيانات. توفر أنظمة التشغيل عادة ميزة إجراء النسخ الاحتياطي للبيانات على الجهاز أو لجزء منها كما تقدم إمكانية اجراء نسخة احتياطية لحالة نظام التشغيل بما في ذلك التطبيقات المنصبة على نظام التشغيل والتخصيصات التي قام المستخدم بتحديدها.

مضاد الفيروساتAntivirus

قد تتضمن نسخة نظام التشغيل برنامج مضاد للفيروسات Antivirus تنتجه وتدعمه الشركة التي تصدر نظام التشغيل وتبقي قاعدة بياناته محدثة بشكل مستمر.

جدار النارFirewall

ويقصد هنا جدار الحماية Firewall التي تعد جزءا من نظام التشغيل. يقوم جدار النار بحماية الجهاز المتصل بشبكة حواسيب من الاختراق أو التخريب أو تعطيل الخدمة عبر شبكة الحواسيب.

تشفير قرص نظام التشغيل يعد تشفير القرص الصلب الطريقة الأفضل للإبقاء على البيانات الموجودة على القرص الصلب سرية في حال ضياع الحاسب أو تعرضه للسرقة. فلو كان القرص الصلب غير مشفرا، يمكن للسارق معاينة محتويات القرص بدون الحاجة لكلمة سرّ نظام التشغيل على الجهاز وذلك عبر ربط القرص الصلب (فيزيائيا) بحاسب آخر يملكه السارق.

الخصوصيةPrivacy

تختلف أنظمة التشغيل فيما بينها بمستوى الخصوصية التي تؤمنه للمستخدم. فالكثير من أنظمة التشغيل تقوم مثلا بشكل دوري بإرسال سجلات الاستخدام إلى الجهة المصنعة لنظام التشغيل بهدف توفير معلومات تساعد على تحسين الخدمة.

سجلات نظام التشغيلLogs System

تقوم أنظمة التشغيل عادة بالاحتفاظ بسجل أو أكثر يقوم نظام التشغيل بتدوين بيانات تتعلق بحالة وعمل نظام التشغيل مثل تسجيل الدخول وتسجيل الخروج، الأخطاء التي تطرأ خلال تشغيل البرامج، حالة الاتصال بالشبكة، وغيرها من المعلومات.

- **المخاطر الأمنية لنظم قواعد البيانات**

يتعلق أمن قاعدة البيانات باستخدام مجموعة واسعة من ضوابط أمن المعلومات لحماية قواعد البيانات (من المحتمل أن تشمل البيانات، وتطبيقات قواعد البيانات أو الوظائف المخزنة، وأنظمة قواعد البيانات، وخوادم قواعد البيانات، وروابط الشبكة المرتبطة) ضد التنازلات عن سريتها وسلامتها والتوفر. وهي تتضمن أنواعًا أو فئات مختلفة من الضوابط،

تشمل مخاطر الأمان على أنظمة قواعد البيانات، على سبيل المثال:

• الإصابات بالبرامج الضارة التي تسبب حوادث مثل الوصول غير المصرح به، أو تسرب أو الكشف عن البيانات الشخصية، أو الخاصة ، أو حذف البيانات ،أو البرامج أو إتلافها ، أو انقطاع أو رفض الوصول المصرح به إلى قاعدة البيانات ، والهجمات على الأنظمة الأخرى ، والفشل غير المتوقع لخدمات قاعدة البيانات ؛

• الأحمال الزائدة وقيود الأداء وقضايا السعة التي تؤدي إلى عدم قدرة المستخدمين المصرح لهم على استخدام قواعد البيانات على النحو المنشود؛

• الأضرار المادية لخوادم قاعدة البيانات الناتجة عن حرائق غرفة الكمبيوتر أو الفيضانات، والسخونة الزائدة، والبرق، وانسكاب السوائل العرضي ، والتفريغ الساكن ، والأعطال الإلكترونية / أعطال المعدات وتقادمها ؛

• عيوب التصميم وأخطاء البرمجة في قواعد البيانات والبرامج والأنظمة المرتبطة بها، مما يؤدي إلى ظهور العديد من نقاط الضعف الأمنية (مثل تصعيد الامتيازات غير المصرح به) وفقدان / تلف البيانات وتدهور الأداء وما إلى ذلك؛

• تلف و / أو فقدان البيانات الناتج عن إدخال بيانات أو أوامر غير صالحة، وأخطاء في قاعدة البيانات أو عمليات إدارة النظام، والتخريب / الضرر الجنائي وما إلى ذلك.

- **جدران الحماية وأنواعها**

جدران الحماية خط الدفاع الأول في الأمان الشبكي، فهي تنشئ حاجزًا "جهاز أو برنامج "بين الشبكات الداخلية الآمنة والمسيطر عليها وبين الشبكات الخارجية غير الموثوق بها، مثل الإنترنت، فيرفض أو يسمح بمرور بيانات او برنامج وفقاً لقواعد معينة، فمن دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة، ومن ثم بعدها بدأت الاجيال والتعديلات لهذه التقنية.

أنواع جدران الحماية

هنالك العديد من فئات الجدران النارية بناءً على مكان عمل الاتصال ومكان تشفير الاتصال والحالة التي يتم تتبعها.

الحزم ومفلترات الشبكة طبقات

يعمل على أنظمةIP\TCPمنخفضة المستوى، ولا يسمح للحزم بالمرور عبر الجدار الناري دون أن تطابق مجموعة القوانين المحددة، المحددة من المسؤول عن الجدار النار.

·طبقات التطبيقات

يمكن أن يعترض جميع الحزم المنتقلة من وإلى التطبيق فيمكنه ان يحجب الحزم الأخرى دون إعلام المرسل عادة، يمكن للجدار الناري أن يمنع الديدان(worms) والأحصنة الطروادة(horses Trojan)من الانتشار عبر الشبكة،

·خادم الوكيل

يجعل العبث بالأنظمة الداخلية من شبكة خارجية أصعب ويجعل إساءة استخدام الشبكة الداخلية لا يعني بالضرورة اختراق أمني متاح من خارج الجدار الناري طالما بقي تطبيق الخادم سليماً ومعداً بشكل ملائم

·ترجمة عنوان الشبكة

- التهديدات الالكترونية الشائعة

استخراج البيانات

يعتبر استخراج البيانات نسخ أو نقل غير مُصرَّح به للبيانات خارج نطاقك. قد يتم إجراء هذا النقل يدويًا بواسطة شخص يمكنه الوصول لموارد داخل مؤسستك، أو قد يكون النقل تلقائيًا تنفذه برامج ضارة في شبكتك. على سبيل المثال، يمكن سرقة البيانات عن طريق خرق حساب يمتلك إمكانية الوصول إلى البيانات، أو من خلال تثبيت تطبيق طرف ثالث يُرسل البيانات خارج نطاقك.

تسرُّب البيانات

تسرُّب البيانات هو عملية نقل غير مصرّح بها لبيانات حساسة خارج نطاقك. يمكن حدوث تسرُّب البيانات عن طريق البريد الإلكتروني أو Meet Google أو Drive Google أو المجموعات أو أجهزة الجوَّال. قد تحدث التسريبات بسبب سلوك ضار أو غير ضار، مثلاً بسبب تفعيل الوصول للجميع إلى المجموعات أو من إعدادات المشاركة السهلة لخدمة Google Drive أو من أجهزة الجوَّال المُخترَقة أو من مرفقات البريد الإلكتروني الصادر.

حذف البيانات

حذف البيانات هو الحذف الضار للبيانات والذي ينتج عنه صعوبة استرداد البيانات أو استحالة استردادها. على سبيل المثال، قد ينفّذ مهاجم برنامج فدية يُشفّر بياناتك، ثم يطلب دفعة نقدية لمفتاح التشفير الذي يفك تشفير البيانات.

مستخدم داخلي ضار

المستخدم الداخلي الضار هو مستخدم موافق عليه أو مشرف في مؤسستك يُسرب معلومات حساسة بشكل خبيث خارج نطاقك. المستخدم الداخلي الضار قد يكون موظفًا، أو موظفًا سابقًا، أو مقاولاً أو شريكًا. قد يُسرب المستخدم الداخلي الضار البيانات عبر أجهزة جوال مُخترَقة أو عن طريق إرسال المحتوى خارج نطاقك عبر البريد الإلكتروني.

خرق الحساب

خرق الحساب هو وصول غير مُصرَّح به لحساب مستخدم أو مشرف داخل نطاقك. يحدث خرق الحساب بسبب سرقة مستخدم غير مفوَّض لبيانات اعتماد تسجيل الدخول. وبحسب هذا التصور، يتم اختراق الحساب في نطاقك بطريقة يُمكن أن يستخدمها مهاجم للتفاعل مع الموارد. إحدى الطرق الشائعة في سرقة بيانات الاعتماد هي التصيد الاحتيالي المُوجَّه عندما يُرسل المخترقون رسالة إلكترونية احتيالية تَبدو وكأنها واردة من فرد أو منشأة تجارية تعرفها وتثق بها.

تعلية الامتيازات

يشير تعلية الامتيازات إلى مهاجم تَمكَّن من اختراق حساب أو أكثر في نطاقك، ويعمل على الاستفادة من تلك الامتيازات المحدودة للحصول على إمكانية الدخول إلى حسابات ذات امتيازات أكبر. عادةً ما يحاول هذا النوع من المخترقين الوصول إلى امتيازات المشرف العام للحصول على تحكُّم أكبر في موارد نطاقك.

اختراق كلمة المرور

اختراق كلمة المرور هي عملية استرداد كلمات المرور باستخدام برنامج متخصص وحوسبة ذات سعة عالية. يمكن للمهاجمين تجربة عدة مجموعات مختلفة لكلمة المرور خلال مدة زمنية قصيرة. من إحدى استراتيجيات منع خرق كلمة المرور، هي فرض التحقُّق بخطوتين

التصيُّد الاحتيالي/التصيُّد الاحتيالي للبيانات المهمة

التصيُّد الاحتيالي/التصيُّد الاحتيالي للبيانات المهمة هو ممارسة احتيالية تتم بإرسال رسائل إلكترونية تبدو أنها واردة من شركات معروفة لخداع الأفراد من أجل كشف معلومات شخصية، مثل كلمات المرور وأرقام الحسابات، أو للحصول على التحكُّم في حساب مستخدم في نطاقك.

الانتحال

الانتحال هو تزييف رأس الرسالة الإلكترونية بواسطة مهاجم لكي تبدو الرسالة صادرة من شخص آخر غير المصدر الحقيقي. عندما يرى أحد المستخدمين مُرسِل الرسالة، قد يبدو له شخصًا يعرفه أو أنها صادرة من نطاق يثق به.

البرامج الضارة

البرامج الضارة هي برامج تم تصميمها لغرض ضار، مثل فيروسات الكمبيوتر وفيروسات حصان طروادة وبرامج التجسس والبرامج الضارة الأخرى.

الفصل الخامس
أمن الشبكات

- ## مفهوم أمن الشبكات

هندسة امن الشبكات والمعلومات هي عملية اتخاذ تدابير وقائية مادية وبرمجية لحماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به أو سوء الاستخدام، أو الأعطال أو التعديل أو التدمير أو الكشف غير المناسب، وبالتالي إنشاء نظام أساسي آمن لأجهزة الكمبيوتر والمستخدمين والبرامج لأداء المسموح لهم من وظائف حاسمة في بيئة آمنة.

- ## يتكون أمن الشبكة من:

• الحماية من مهددات امن المعلومات والشبكات: يجب عليك تكوين أنظم تك وشبكاتك بشكل صحيح قدر الإمكان

• الكشف: يجب أن تكون قادرًا على تحديد متى تغير التكوين أو عندما تشير بعض حركة مرور الشبكة إلى وجود مشكلة

• رد الفعل: بعد تحديد المشكلات بسرعة، يجب أن تستجيب لها وتعود إلى الحالة الآمنة بأسرع ما يمكن

- ## أهداف الحماية الأمنية للشبكات

سرية المعلومات

Data Confidentiality وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد.

تكامل المعلومات

Data Integrity في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير

والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من 100 إلى 1000000 وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال

توافرية الشبكة

Availability وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

- مفهوم الثغرات في أمن الشبكات

الثغرات الأمنية

هي نقطة ضعف أو عيب أو خطأ يتم العثور عليه داخل النظام والذي يُمكن أن يتم الاستفادة منه من قبل المخترقين لاختراق شبكة آمنة.

يتم إنشاء الثغرات الأمنية

الثغرات الأمنية هي عيب في ك تابة أكواد البرنامج أو خطأ في تكوين النظام والسبب البسيط هو أن الثغرات الأمنية هي خاصية ناشئة للبرامج وهناك ثلاثة أسباب رئيسية: جودة الكود ، والتعقيد ، ومدخلات البيانات الموثوقة.

يتم استغلال الثغرات الأمنية

الاستغلال هو الخطوة التالية في دليل المخترق بعد اكتشاف الثغرة الأمنية وهو جزء من برنامج أو نص برمجي يمكن أن يسمح للقراصنة بالسيطرة على النظام واستغلال نقاط الضعف فيه ويستخدم المخترقون عادةً أدوات فحص الثغرات الأمنية مثل Nessus وNexpose و OpenVAS وغيرها للعثور على هذه الثغرات الأمنية.

يمكن الكشف عن الثغرات الأمنية

عن طريق فحص الأمان لتطبيق باستخدام أدوات الطرف الثالث ومراقبة الثغرات الأمنية بانتظام في التطبيقات أو البيئات ذات الصلة واختبارات الاختراق

اختبار الاختراق:

هو محاكاة هجوم إلكتروني ضد نظام الكمبيوتر لديك للتحقق من نقاط الضعف القابلة للاستغلال.

- التهديدات الرقمية لشبكات الحاسب

الاختراق

الاختراق الأمني هو أي حادث ينتج عنه وصول غير مصرح به إلى بيانات الكمبيوتر أو التطبيقات أو الشبكات أو الأجهزة. كما ينتج عنه الوصول إلى المعلومات دون إذن. ويحدث عادةً عندما يتمكن المتسلل من تجاوز آليات الأمان.

يوجد فرق بين الاختراق الأمني واختراق البيانات. يُعد الاختراق الأمني بمثابة اختراق فعال، في حين يتم تعريف اختراق البيانات على خروج المجرم الإلكتروني بالمعلومات.

ومن المهم أيضًا التمييز بين تعريف الاختراق الأمني وتعريف الحادث الأمني. فقد يتضمن الحادث إصابة بالبرامج الضارة أو هجوم DDOS أو ترك أحد الموظفين لكمبيوتر محمول في سيارة أجرة، ولكن إذا لم ينتج عنه وصول إلى الشبكة أو فقدان البيانات، فلن يتم اعتباره اختراقًا أمنيًا.

أنواع الاختراقات الأمنية

توجد عدة أنواع للاختراقات الأمنية مُقسَّمةً حسب كيفية الوصول إلى النظام:

• هجمات استغلال الثغرات تستهدف الثغرات الموجودة في النظام، مثل أنظمة التشغيل غير المُحدَّثة. الأنظمة القديمة التي لم يتم تحديثها، على سبيل المثال، في الشركات التي يتم فيها استخدام إصدارات قديمة من نظام Microsoft Windows والتي لم تعد مدعومة، تكون عرضة بشكل خاص لهجمات استغلال الثغرات.

• يمكن اختراق كلمات المرور الضعيفة أو تخمينها. حتى الآن، لا يزال بعض الأشخاص يستخدمون كلمة المرور"password "، كما لا تُعد "word$$pa "أكثر أمانًا.

• يمكن استخدام هجمات البرامج الضارة، مثل رسائل التصيّد الاحتيالي عبر البريد الإلكتروني لإيجاد ثغرة للدخول. حيث لا يتطلب الأمر سوى نقر موظف واحد على رابط في رسالة تصيّد احتيالي عبر البريد الإلكتروني، للسماح للبرامج الضارة بالبدء في الانتشار عبر الشبكة.

• تستخدم التنزيلات العرضية الفيروسات أو البرامج الضارة التي تصل من خلال موقع ويب مخترق أو مخادع.

• كما يمكن أيضًا استخدام الهندسة الاجتماعية لاكتساب صلاحية الوصول. كأن يقوم أحد المتسللين مثلًا بالاتصال بموظف ويدعي أنه من مكتب المساعدة في قسم تكنولوجيا المعلومات بالشركة ويطلب كلمة المرور من أجل "إصلاح" الكمبيوتر.

المهاجمين

عبارات بسيطة الهجمات الالكترونية عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الاجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات . يمكن تقسيم الهجمات الالكترونية (الهجمات السيبرانية) الى نوعين رئيسيين على النحو التالي:

– هجمات يكمن الهدف من ورائها الى تعطيل جهاز الكمبيوتر المستهدف

– هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه.

- **أنواع الهجمات التي تتعرض لها الشبكة**

هناك سبعة انواع من الهجمات الالكترونية (الهجمات السيبرانية):

- البرامج الضارة(Malware)
- التصيد(Phishing)
- حجب الخدمات (Denial Of Service)
- الرجل في المنتصف (Man in the middle)
- التعدين الخبيث (Cryptojacking)
- حقن هجومSQL
- هجمات دون انتظار(Zero- Day)

البرامج الضارة Malware

هي اختصار لكلمة برنامج ضار ويمكن ان يشير البرنامج الضار الى اي نوع من البرامج ،بصرف النظر عن طريقة تكوينه او تشغيله، وهو "مصمم لإلحاق الضرر بجهاز الكمبيوتر او السيرفر او شبكة جهاز الكمبيوتر مثلما تعرفه : Microsoft إن الفيروسات المتنقلة والفيروسات وحصان طروادة تندرج كلها تحت البرامج الضارة، ولا يميزها عن بعضها البعض سوى الوسائل التي يتم استخدامها لإنشائها ونشرها.

التصيد(Phishing)

التصيد تقنية يستخدمها مجرمو الفضاء الإلكتروني في إرسال رسائل بريد إلكتروني لخداع المستهدف من أجل القيام ببعض الأعمال الضارة. ربما يتم خداع المستلم في تنزيل برنامج ضار متخفي في صيغة مستند هام، على سبيل المثال ، او مطالبته بالنقر فوق احد الروابط التي تقوم بتوجيهه الى موقع ويب زائف حيث يتم سؤاله عن معلومات حساسة مثل اسماء المستخدمين وكلمات المرور الخاصة بالبنك. لكثير من رسائل البريد الإلكتروني المتصيدة تكون بدائية الى حد ما ويتم إرسالها الى الالاف من الضحايا المحتملين

حجب الخدمات (Denial Of Service)

هجوم حجب الخدمات هو اسلوب استخدام القوة الغاشمة لمحاولة إيقاف تشغيل بعض الخدمات عبر الإنترنت . على سبيل المثال، قد يقوم المهاجمون بإرسال الكثير من البيانات الى احد مواقع الويب او الكثير من الطلبات الى احدى قواعد البيانات والتي تتسبب في ملئ تلك الأنظمة وتعطيلها عن العمل ، وهو ما قد يجعلها غير متاحة لأي شخص.

الرجل في المنتصف (Man in the middle)

هجوم الرجل في المنتصف (MITM) (طريقة ينجح بها المهاجمون في إقحام أنفسهم سرا بين المستخدم وخدمة الويب التي يحاولون الوصول اليها. على سبيل المثال ربما يقوم المهاجم بإعداد شبكة Fi-Wi مزودة بشاشة تسجيل مصممة بشكل يحاكي احدى شبكات الفنادق ؛وبعد ان يقوم المستخدم بتسجيل الدخول ، يمكن ان يجمع المهاجم اي معلومات يرسلها المستخدم ، ويشمل ذلك كلمات المرور الخاصة بالبنك الذي يتعامل معه.

التعدين الخبيث (Cryptojacking)

التعدين الخبيث عبارة عن هجوم مخصص وفيه يتم اختراق احد اجهزة الكمبيوتر الخاصة بأحد الاشخاص واستخدامها لتعدين العملات الرقمية المشفرة (إجراء يطلق عليه التعدين في قاموس مصطلحات عملات التشفير).سيحاول المهاجمون إما تثبيت احد البرامج الضارة على جهاز الكمبيوتر الخاص بالضحية لتنفيذ العمليات الحسابية المطلوبة او احيانا تشغيل التعليمة البرمجية في JavaScript والتي يتم تنفيذها في المستعرض الخاص بالضحية.

حقن SQL

حقن SQL عبارة عن وسيلة تُمكن المهاجم من استغلال الثغرات في السيطرة على قاعدة بيانات الضحية. توجد العديد من قواعد البيانات المُصممة لتنفيذ أي أوامر مكتوبة في لغة الاستعلامات المركبة(SQL) ، وتقوم العديد من مواقع الويب التي تجمع المعلومات من المستخدمين،بإرسال هذه البيانات إلى قواعد بيانات

هجمات دون انتظار(Zero- Day)

الهجمات دون انتظار هي عبارة عن ثغرات في البرامج لم يتم حلها الى الان وسميت كذلك لأنه بمجرد إصدار حزمة ، يتناقص كل يوم عدد الأجهزة المفتوحة المعرضة للهجوم اثناء تسجيل المستخدم تحديثات الأمان . كثيرا ما يتم شراء وبيع تقنيات استغلال الثغرات هذه على الانترنت المظلم (Web Dark) واحيانا يتم اكتشافها من خلال الوكالات الحكومية التي قد تستخدمها لأغراض الاختراق بدلا من إصدار معلومات عامة لأجل المنفعة المشتركة.

- أمن الشبكات اللاسلكية

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجلات ضمن وخارج حقل تقنية المعلومات. قد نتكلم مثلً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

- أمن وسائل نقل المعلومات

في التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الاتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم (أمن أنظمة المعلومات Information Systems Security – INFOSEC) يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب وهي كالتالي:

- السرية.
- التحقق من الهوية.
- الكمال.
- التوفر.

أمن المعلومات في الشبكات اللاسلكية

تعرّف توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي: "حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات."

الخصائص الأمنية الخمس في الشبكات اللاسلكية

- **السرية**
- **التحقق من الهوية**
- **الكمال**
- **التوفر**
- **مكافحة الانكار – المسؤولية**
- الشبكات المحلية الافتراضية وأمنها

الشبكة المحلية الافتراضية، هي أي نطاق بث مجزأ ومعزول داخل شبكة الحاسوب ضمن طبقة ربط البيانات. حتى نستطيع تقسيم الشبكة إلى شبكات محلية وهمية، يحتاج الشخص إلى فهم الشبكة وطريقة ربط معداتها. هنالك معدات بسيطة يمكن استخدامها للتجزئة من خلال المنافذ الموجودة على الجهاز نفسه (إذا وجدت), وفي هذه الحالة كل شبكة محلية وهمية يتم شبكها بكيبل مخصص لها.

- الاتصال الآمن بالإنترنت

أمان الإنترنت هو مصطلح يصف أمن الأنشطة والمعاملات التي تتم عبر الإنترنت. إنه مكون خاص من الأفكار الأكبر للأمن الإلكتروني وأمن الكمبيوتر، بما في ذلك موضوعات تشمل أمان المتصفح والسلوك عبر الإنترنت وأمن الشبكة. إننا نقضي جزءًا كبيرًا من حياتنا على الإنترنت

أكثر تهديدات أمن الإنترنت شيوعًا

التصيُّد الاحتيالي

التصيُّد الاحتيالي هو هجوم إلكتروني يمارس عبر رسائل بريد إلكتروني متنكرة. يحاول المتسللون خداع مستلمي البريد الإلكتروني للاعتقاد بأن الرسالة حقيقية وأن شأنها يعنيهم – كأن تتنكر في صيغة طلب من مصرفهم أو ملاحظة من زميل في العمل مثلاً – بحيث ينقرون على رابط أو يفتحون مرفقًا. والهدف من ذلك هو خداع الأشخاص ليقوموا بالكشف عن معلوماتهم الشخصية أو تنزيل برامج ضارة.

التسلل والوصول عن بُعد

يسعى المتسللون دائمًا إلى استغلال نقاط ضعف الشبكة أو النظام الخاصة حتى يتمكنوا من سرقة المعلومات والبيانات السرية. وتمنحهم تقنية الوصول عن بُعد هدفًا آخر يمكنهم استغلاله. إذ يسمح برنامج الوصول عن بُعد للمستخدمين بالوصول إلى جهاز الكمبيوتر والتحكم فيه عن بُعد. ومنذ انتشار الجائحة، ومع زيادة عدد الأشخاص الذين يعملون عن بُعد يسمى البروتوكول الذي يسمح للمستخدمين بالتحكم في جهاز كمبيوتر متصل بالإنترنت عن بُعد بروتوكول سطح المكتب البعيد أو, .(RDP)

البرمجيات الضارة والإعلانات الضارة

يمكن وصف أي برنامج يهدف إلى إتلاف جهاز كمبيوتر أو خادم أو شبكة على أنه برنامج ضار. "الإعلانات الضارة" عبارة عن مصطلح مفرداته "الإعلان" و"الضرر". وهو يشير إلى الإعلان عبر الإنترنت الذي يوزع البرامج الضارة. يُعد الإعلان عبر الإنترنت نظامًا معقدًا يتضمن مواقع

الناشرين وتبادل الإعلانات وخوادمها وشبكات إعادة الاستهداف وشبكات توصيل المحتوى. يستغل المخترقون عبر الإعلانات هذا التعقيد لوضع تعليمات برمجية ضارة في أماكن لا يكتشفها الناشرون

وشبكات الإعلانات دائمًا. ويمكن لمستخدمي الإنترنت الذين يتفاعلون مع إعلان ضار تنزيل برامج ضارة على أجهزتهم أو أن تتم إعادة توجيههم إلى مواقع ويب

ضارة.

برامج طلب الفدية

برنامج طلب الفدية هو نوع من البرامج الضارة التي تمنعك من استخدام جهاز الكمبيوتر الخاص بك أو الوصول إلى ملفات معينة عليه ما لم تدفع فدية. غالبًا ما يتم توزيع هذه البرامج كأحصنة طروادة، أي برامج ضارة متخفية كبرنامج مشروع أو أصيل. لكن بمجرد التثبيت يقفل البرنامج شاشة نظام التشغيل أو ملفات معينة إلى أن تدفع.

شبكات بوت نت

مصطلح بوت نت هو اختصار "الشبكة الروبوتية". الشبكة الروبوتية عبارة عن شبكة من أجهزة الكمبيوتر التي تم إصابتها عن قصد ببرامج ضارة حتى تتمكن من تنفيذ المهام الآلية على الإنترنت دون إذن أو معرفة مالكي أجهزة الكمبيوتر.

وبمجرد أن يتحكم مالك الروبوتات في جهاز الكمبيوتر الخاص بك، يمكنه استخدامه لتنفيذ أنشطة ضارة. ومن بينها:

- توليد حركة مرور وهمية على الإنترنت على مواقع الطرف الثالث لتحقيق مكاسب مالية.
- استخدام قوة جهازك للمساعدة في هجمات رفض الخدمة الموزعة (DDoS) لإغلاق مواقع الويب.
- إرسال بريد إلكتروني عشوائي إلى ملايين مستخدمي الإنترنت.
- الاحتيال وسرقة الهوية.
- مهاجمة أجهزة الكمبيوتر والخوادم.

تهديدات شبكةFi-Wi ، في الأماكن العامة وفي المنزل

تنطوي شبكات Fi-Wi العامة على مخاطر لأن الأمن على هذه الشبكات – في المقاهي ومراكز التسوق والمطارات والفنادق والمطاعم وما إلى ذلك – غالبًا ما يكون ضعيفًا أو حتى غير موجود بالمرة. ويعني الافتقار إلى الأمان أن المجرمين الإلكترونيين ولصوص الهوية يمكنهم مراقبة ما تفعله عبر الإنترنت وسرقة كلمات المرور والمعلومات الشخصية الخاصة بك. تشمل مخاطر Fi-Wi العامة الأخرى:

- اكتشاف الحزم – يقوم المهاجمون بمراقبة البيانات غير المشفرة واعتراضها أثناء انتقالها عبر شبكة غير محمية.

• هجمات الوسطاء – يقوم المهاجمون باختراق نقطة اتصال شبكة Fi-Wi لإقحام أنفسهم في الاتصالات بين الضحية المستهدفة ونقطة الاتصال لاعتراض البيانات أثناء النقل وتعديلها.

• شبكات Fi-Wi المخادعة – يقوم المهاجمون بإعداد نقطة جذب على شكل شبكة Fi-Wiمجانية لجمع البيانات القيمة. تصبح نقطة اتصال المهاجم هي قناة الممر لجميع البيانات التي يتم تبادلها عبر الشبكة.

- التدابير الأمنية العامة لأمن شبكات الحاسب

إذا كنت تتساءل عن كيفية ضمان الحماية بشكل عام على الإنترنت ولا سيَّما حماية بياناتك، فستجد فيما يلي بعضًا من نصائح أمان الإنترنت المعقولة التي يمكنك اتباعها:

بتمكين المصادقة متعددة العناصر

المصادقة متعددة العناصر (MFA) هي طريقة للمصادقة تطلب من المستخدمين توفير طريقتين أو أكثر من طرق التحقق للوصول إلى حساب عبر الإنترنت. على سبيل المثال، بدلاً من مجرد طلب اسم مستخدم أو كلمة مرور، تذهب المصادقة متعددة العناصر إلى أبعد من ذلك من خلال طلب معلومات إضافية، مثل:

• كلمة مرور إضافية تُستخدم مرة واحدة، ترسلها خوادم مصادقة موقع الويب إلى هاتف المستخدم أو عنوان بريده الإلكتروني.

• إجابات عن أسئلة الأمان الشخصية.

• بصمة الإصبع أو غيرها من المعلومات الحيوية، مثل الصوت أو التعرف على الوجه.

استخدام جدار حماية

يعمل جدار الحماية كحاجز بين جهاز الكمبيوتر الخاص بك وشبكة أخرى، مثل الإنترنت. تحجب جدران الحماية حركة المرور غير المرغوب فيها ويمكن أن تساعد أيضًا في منع البرمجيات الضارة من إصابة جهاز الكمبيوتر. غالبًا ما يكون نظام التشغيل ونظام الأمان لديك مزودًا بجدار حماية مثبت مسبقًا.

الحذر عند اختيار المستعرض

المستعرضات هي بواباتنا الأساسية إلى الويب، وبالتالي تلعب دورًا رئيسيًا في الأمن على الإنترنت. يجب أن يكون مستعرض الويب الجيد آمنًا ويساعد على حمايتك من انتهاكات البيانات. قامت مؤسسة Freedom of the Press بتجميع دليل مفصل هنا، يشرح إيجابيات الأمان مستعرضات الويب الرائدة في السوق وسلبياتها.

إنشاء كلمات مرور قوية واستخدام مدير كلمات مرور آمن

ستساعدك كلمة المرور القوية في الحفاظ على أمنك على الإنترنت. تتصف كلمة المرور الجيدة بما يلي:

• طويلة – تتكون من 12 حرفًا على الأقل، وُفضل أطول من ذلك.

• مزيج من الأحرف – أي تشمل أحرفًا كبيرة وصغيرة بالإضافة إلى الرموز والأرقام.

• تتجنب الاحتمالات الواضحة – مثل استخدام الأرقام المتسلسلة ("1234") أو المعلومات الشخصية التي قد يخمنها شخص يعرفك، مثل تاريخ ميلادك أو اسم حيوانك الأليف .

• تتجنب تراتيب أزرار لوحة المفاتيح السهل تذكرها.

احتفظ ببرنامج أمان محدث مثبتًا على أجهزتك

يعد برنامج مكافحة فيروسات لحفظ أمنك على الإنترنت أداة بالغة الأهمية لضمان الخصوصية والأمان. سيحميك أفضل برنامج لأمن الإنترنت من أنواع مختلفة من هجماته ويحمي بياناتك عبر الاتصال به. ومن المهم لأن تحرص على تحديث برامج مكافحة الفيروسات باستمرار، كما تقوم معظم البرامج الحديثة بتحديث نفسها تلقائيًا للبقاء على اطلاع بأحدث تهديدات الأمن على الإنترنت.

الفصل السادس
الهندسة الاجتماعية

- ## مفهوم الهندسة الاجتماعية وأهدافها

الهكر وفن اختراق العقل البشري، ويعرفها على أنها مجموعة من الأنماط والسلوكيات البشرية التي نمارسها بقصد أو دون قصد، والتي يستخدمها المختصون عامة في التسويق لإقناع الجمهور بمنتج بعينه والترويج

لمؤسسات

كيف تعمل الهندسة الاجتماعية؟

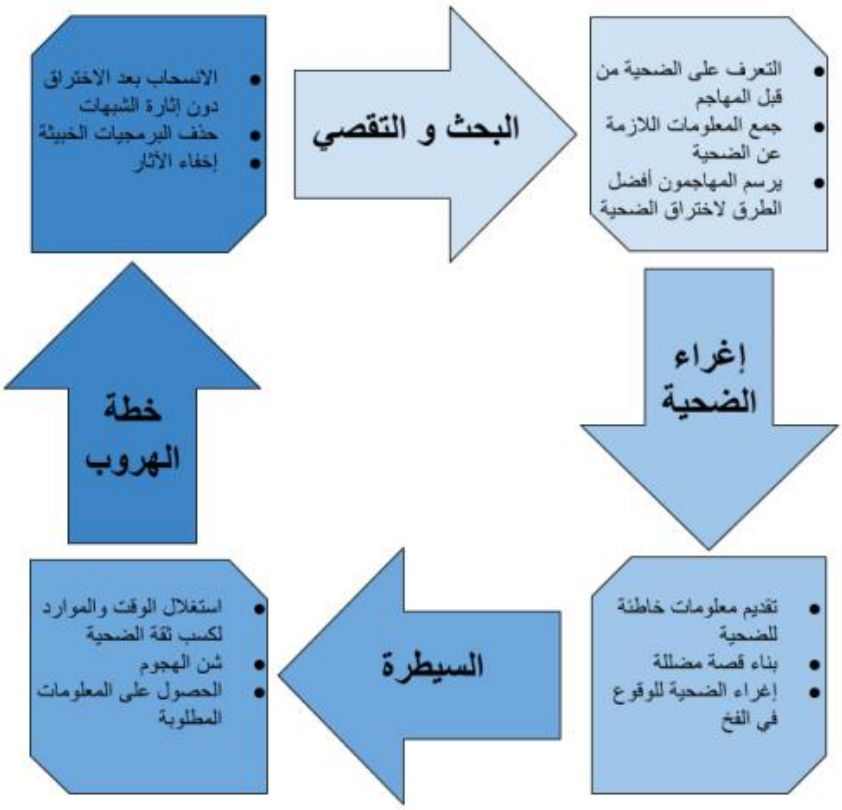
تعتمد معظم هجمات الهندسة الاجتماعية على التواصل الفعلي بين المهاجمين والضحايا. حيث يميل المهاجم لخداع المستخدم من خلال تحفيزه لأداء مهمة معينة تعرضه من خلالها للاختراق، بدلاً من استخدام الأساليب الواضحة لاختراق بياناتك من خلال استغلال نقاط

الضعف في البرامج وانظمة التشغيل.

عادة ما تكون خطوات دورة هجوم الهندسة الاجتماعية كما يلي:

- جمع معلومات أساسية عنك أو عن مجموعة أكبر أنت جزء منها.
- تسلل من خلال تواصل يبدأ ببناء الثقة.
- استغلال الضحية بمجرد أن تنشأ الثقة لتعزيز الهجوم.
- قطع العلاقة بالضحية بمجرد أن يتخذ الضحية الإجراء المطلوب.

يمكن أن تتم هذه العملية في رسالة بريد إلكتروني واحدة أو على مدار أشهر في سلسلة من محادثات عبر الوسائل الاجتماعية. كما يمكن أن يكون تفاعلًا وجهاً لوجه. ينتهي في النهاية بالحصول على بيانات حساسة او اجراء معين ينفذه الضحية، مثل مشاركة معلومات مهمة أو تنزيل برامج ضارة. لا يدرك العديد من الموظفين والمستهلكين أن مجرد معلومات بسيطة يمكن أن تمنح المتسللين إمكانية الوصول إلى شبكات وحسابات متعددة.



- **أنواع الهندسة الاجتماعية**

بالتأكيد يوجد أنواع للهندسة الاجتماعية والتي يستخدمها المقرصنون من أجل اختراق العقول والحصول على المعلومات الكافية للإيقاع بالضحية وسرقة بياناته وفي أحيان كثير أمواله، وهنا سنوضح أشهر أنواع الهندسة الاجتماعية.

اصطياد الضحية

يستغل المقرصن في هذه الحالة فضول الضحية، فيقدم له أحد الوعود الكاذبة من أجل الإيقاع بالضحية في المصيدة وسرقة بياناته الشخصية أو التلاعب بالنظام الأمني من خلال إرسال رابط يحمل فيروس إلكتروني ليبدأ في سحب البيانات من الجهاز الإلكتروني.

سكير ويرScarware

نوع أخر من أشكال البرمجيات الخبيثة، والتي غالبًا ما تتضمن إنذار كاذب بوجود فيروس اختراقي لجهازك، أو تهديد بأن جهازك مراقب، والتي توجه المستخدمين لتحميل برنامج لحماية جهازك، والذي يكون هذا البرنامج هو التهديد بحد ذاته.

الهجوم الإلكتروني Pretexting

نوع آخر يستخدمه المقرصنون من أجل الحصول على البيانات الشخصية للطرف الآخر سواء إلكترونيًا أو باستخدام أي وسيلة للتواصل مع الضحية مثل هاتفيًا، بإرسال رسالة نصية ينتحل فيه المقرصن شخصية أخرى، ويسعى لاستخراج البيانات من الضحية.

- **جوانب الهجمات بأسلوب الهندسة الاجتماعية**

تتمحور هجمات الهندسة الاجتماعية حول استخدام المهاجم للإقناع والثقة. عندما تتعرض لهذه التكتيكات، فمن المرجح أن تتخذ إجراءات دون إدراكك أو التفكير في مدى خطورتها.

في معظم هجمات الهندسة الاجتماعية، يقوم المهاجم بالتلاعب بالضحية واقناعه من خلال:

التلاعب بالمشاعر:

يمنح التلاعب العاطفي للمهاجمين اليد العليا في أي تفاعل. أنت أكثر عرضة لاتخاذ – إجراءات غير عقلانية أو محفوفة بالمخاطر عندما تكون في حالة عاطفية محسّنة. يتم استخدام جميع المشاعر التالية (الخوف – الاثارة – حب الاستطلاع – الغضب – الذنب – حزن) بشكل متوازي لإقناعك.

الاستعجال:

الفرص أو الطلبات الحساسة للوقت هي أساليب أخرى يستخدمها المهاجم في هجمات الهندسة الاجتماعية. قد يقوم المخترق بأقناعك بوجود مشكلة خطيرة تحتاج إلى اهتمام فوري واتخاذ اجراء سريع فهنا لا يكون عناك وقت للتفكير حيث يستخدم هذا التكتيك في الهندسة الاجتماعية لتشتيت تفكيرك وتحفيزك لتنفيذ شيء معين.

الثقة:

المصداقية لا تقدر بثمن وضرورية لهجوم الهندسة الاجتماعية. نظرًا لأن المهاجم يكذب عليك في النهاية، فإن الثقة تلعب دورًا مهمًا هنا. حيث يقوم المهاجم بإجراء أبحاثًا كافية عنك لصياغة قصة يسهل عليك تصديقها ومن غير المرجح أن تثير الشكوك.

- **أساليب الهجوم باستخدام الهندسة الاجتماعية**

جمع المعلومات

باختلاف نوايا المهندس الاجتماعي وأغراضه، فإن ما يبحث عنه هو المعلومات، فمهما كانت تلك المعلومات بسيطة، فهو يدرك أهمية حفظها، فربما قد يحتاجها مستقبلًا.

تقديم حقائق واستنتاجات

تتبع تلك السياسة أغلب أجهزة الاستخبارات العالمية وذلك من أجل كسب ثقة الطرف الأخر وإرضاء غروره، ومن ثم يبدأ في الحديث عن الكثير من المعلومات المهمة سواء عن حياته أو عن الأشخاص الذين يعرفهم.

انتحال الهوية

من أكثر السبل انتشارًا في الفضاء الإلكتروني، كما أنها أخطرها، حيث ينتحل هذا المهندس أو المقرصن شخصية أخرى من أجل استخلاص المعلومات من الطرف الأخر، وذلك بالطبع بعد أن يجمع المهندس كافة المعلومات اللازمة عن تلك الشخصية حتى يتمكن من الرد بعفوية وسريعًا على أي سؤال أو استفسار، وحتى يقنع الضحية بخدعته حتى يحصل على ما يريد.

- **الأثار المترتبة على الهندسة الاجتماعية**

تُعتبر الهندسة الاجتماعية الطريقة الأسرع والأقوى لكسب معلومات ذات قيمة كبيرة عن الأشخاص بشكل عام، حيث يقوم المُهاجم باستخدام المعلومات القليلة التي يملكها ليكسب ثقة ضحيته، وبواسطة هذه الثقة ينتهي الأمر بالضحية أن يقدم للمُهاجم معلومات حساسة يستطيع من خلالها اكتشاف خصائص النظام. وهناك أساليب يمكن أن يتم إيقاع الضحايا بها، مثل الهاتف. حيث أكثر الهجمات الهندسة الاجتماعية تقع عن طريق الهاتف، وحتى يتمكن الفرد من حماية نفسه من الاختراق عليه ألا يُشارك جُزافاً في أية معلومات، وأن يعرف الأشخاص الذين يتعامل معهم رقميا

كيف ننجو من الهجمات ونحمي أنفسنا من مخاطر الهندسة الاجتماعية؟

– التثقيف في مجال الأمن الرقمي وأساليب الاختراق المتجددة.

– تجنب إعطاء أي معلومات سرية أو بيانات شخصية إلا بعد التأكد من هوية الشخص المتحدث، وأن الاتصال تمّ من جهة رسمية أو معروفة.

– تجنب الحديث في الأسرار الشخصية مع الأصدقاء المجهولين عبر وسائل التواصل الاجتماعي.

– عدم فتح ملفات أو مرفقات البريد الإلكتروني المُرسَل من أشخاص غير معروفين. والتأكد من الروابط المرسلة بأنّها ليست روابط خبيثة من خلال فتحها عبر استخدام موقع فيروس توتال.

– العمل على تأمين هواتفنا أو حواسيبنا واستخدام برامج لمكافحة الفيروسات.

- **إجراءات الحد من مخاطر الهندسة الاجتماعية**

• الاتصال الآمن وإدارة الحساب

الاتصال عبر الإنترنت هو المكان الذي تكون فيه عرضة للخطر بشكل خاص حيث تعد وسائل التواصل الاجتماعي والبريد الإلكتروني والرسائل النصية أهدافًا شائعة ودائمة.

• استخدام شبكة امنة للاتصال بالأنترنت

يمكن أن تكون شبكات الإنترنت المُخترقة نقطة ضعف أخرى يتم استغلالها لاعتراض اتصالك والحصول على بيانات وصول لحساباتك. لتجنب ذلك، اتخذ إجراءات وقائية لأي شبكة تتصل بها.

• الحفظ على أمن جهازك

إن الحفاظ على أجهزتك نفسها لا يقل أهمية عن جميع سلوكياتك الرقمية الأخرى. احمي هاتفك المحمول وجهازك اللوحي وأجهزة الكمبيوتر من خلال: استخدم برامج الأمان ففي حالة نجاح هجوم الهندسة الاجتماعية في اقناعك بتحميل برنامج ضار. ولمكافحتها والحماية منها عليك استخدام برامج مكافحة الفيروسات والبرامج الضارة للقضاء على كل مصادر الخطر.

- **طرق رئيسية لحماية الأجهزة والمعلومات من الاختراق**

نظرًا لما تحمله تلك الهجمات من خطورة بالغة سواء على مستوى الأفراد أو المؤسسات، وجب التحصين ضد هجمات الهندسة الاجتماعية، ومحاولة استخدام أي أدوات من أجل حفظ بياناتك أنت وأسرتك أو حتى شركتك من تلك القرصنة الخبيثة.

• عدم مشاركة بياناتك الشخصية مع أي شخص حتى وإن كان محل ثقة، وخاصة بياناتك البنكية.

• لا تضغط على أي روابط تصلك من أي شخص، حتى وإن كان صديقك المقرب –قد يكون حسابه اخترق بالفعل، وأنت الضحية القادمة.

• لا تضغط على أي ملفات تصلك عبر البريد الإلكتروني، فهي أشهر السبل المستخدمة عالميًا لنشر البرامج الخبيثة.

• استخدم تقنيات حديثة لترشيح رسائل البريد التي تصل إليك، حيث تؤدي تلك التقنيات وظيفة حارسك الشخصي، لترسل أي رسالة مرسلة من جهة مجهولة الهوية إلى ملف الرسائل المزعجة في البريد الإلكتروني.

• احرص على تثبيت برامج حماية من الفيروسات فعالة وذات سمعة طيبة، أو استعن بأحد الشركات المتخصصة في الأمن السيبراني لتساعدك على تلك المهمة.

الفصل السابع
الاصطياد والهجوم الالكتروني

- ## نظام البريد الالكتروني

مكونات نظام البريد الالكتروني

ما هو عنوان البريد الإلكتروني؟

من الأمور التي تُمكّنك من الدخول إلى التطبيقات والمواقع المتاحة على الإنترنت هو البريد الإلكتروني، إذ عليك أن تنشئ حسابًا مخصصًا لك لتتمكن من الدخول والاستفادة من هذه التطبيقات، ويُعرف عنوان البريد الإلكتروني؛ على أنه مُعرّف فريد لحسابات البريد الإلكتروني، والتي تُستخدم لإرسال واستقبال رسائل البريد الإلكتروني عبر الإنترنت، وكما هو الحال في البريد الفعلي، تتطلب رسالة البريد الإلكتروني عنوانًا لكل من المرسل والمستقبل لتتمكن من إرسالها بنجاح.

- ## أجزاء عنوان البريد الإلكتروني

ويتكون عنوان البريد الإلكتروني

النموذجي من ثلاثة مكونات، لكل منها دور وأهمية في عملية تبادل الرسائل، فإذا كان أحد هذه المكونات خاطئًا أو مفقودًا ستصلك رسالة خطأ أو سترسل رسالة البريد الإلكتروني إلى الجهة غير المقصودة بدلًا من ذلك، وفيما يلي سنوضح لك المكونات الثلاثة الأساسية لعنوان البريد الإلكتروني:

• اسم المستخدم:" Username "

يعد اسم المستخدم الجزء الأول من عنوان البريد الإلكتروني، وهو الاسم الفريد الذي تحدده أنت أو موفر خدمة الإنترنت، ويمكنك اختيار اسمك الحقيقي أو لقبك كاسم مستخدم لعنوان بريدك الإلكتروني، ومن الضروري أن يكون اسم المستخدم فريدًا بمعنى أنه يجب ألا يكون لشخصين أو مؤسستين نفس اسم المستخدم مع نفس الموفر.

• رمز "@":

يُعد الرمز "at "أو "@" الجزء الثاني من عنوان البريد الإلكتروني، والذي يقع بين اسم المستخدم ومجال عنوان بريدك الإلكتروني، وعندما تدخل الرمز، يتعرف برنامج البريد الإلكتروني الخاص بك على الحرف ويرسل البريد الإلكتروني إلى اسم المجال الذي يليه .

• اسم النطاق أو المجال:

وهو الجزء الأخير من عنوان البريد الإلكتروني، والذي يمكن تقسيمه إلى جزأين هما؛ خادم البريد ونطاق المستوى الأعلى، ويُعرف خادم البريد بأنه المسؤول عن استضافة حساب البريد الإلكتروني، فعلى سبيل المثال تستخدم حسابات البريد الإلكتروني في شركة ياهو الاسم "Yahoo "كاسم الخادم، بينما يستخدم حساب الجيميل الاسم "Gmail "كاسم الخادم، بينما يُعرف نطاق المستوى الأعلى بالامتداد مثل؛ (com.) أو (net.) أو (info.)، وغالبًا ما تحتوي رسائل البريد الإلكتروني الواردة من المؤسسات التعليمية على الامتداد (Edu.) ، بينما يستخدم موظفو الهيئات الحكومية الامتداد (gov.).

الرسائل البريد الالكترونية غير المرغوبة

العديد من رسائل البريد الإلكتروني غير المرغوب فيها ذات طابع تجاري ولكن قد تحتوي أيضا على روابط مقنعة تبدو أنها لمواقع ويب مألوفة ولكنها تؤدي في الواقع إلى مواقع ويب أو مواقع ويب تستضيف برامج ضارة. وقد تتضمن رسائل البريد الإلكتروني غير المرغوب فيها أيضا برامج ضارة مثل النصوص البرمجية أو مرفقات الملفات القابلة للتنفيذ الأخرى (أحصنة طروادة).

يجمع مرسلو الرسائل غير المرغوب فيها عناوين البريد الإلكتروني من غرف الدردشة والمواقع الإلكترونية وقوائم العملاء ومجموعات الأخبار والفيروسات التي تحصد كتابة عناوين المستخدمين. كما يتم أحيانا بيع عناوين البريد الإلكتروني التي يتم جمعها إلى مرسلي الرسائل غير المرغوب فيها الآخرين.

- **الاصطياد الالكتروني**

الاصطياد الإلكتروني " "phishingهو نوع من هجمات الهندسة الاجتماعية للحصول على معلومات خاصة بمستخدمي الانترنت سواء كانت معلومات شخصية أو مالية عن طريق الرسائل الالكترونية أو مواقع الانترنت المزيفة.

وتتم هذه العملية عن طريق إرسال رسائل إلكترونية زائفة من قبل أشخاص يطلق عليهم المتصيدون phishers تطلب من الهدف أو الضحية بالنقر على رابط ضار، مما قد يؤدي إلى تثبيت برامج ضارة أو تجميد النظام كجزء من هجوم برامج الفدية أو الكشف عن معلومات حساسة. وقد يكون هذا الرابط هو عنوان لموقع انترنت مزيف صمم من قبل المتصيدون ويكون دائما شبيهاً بالموقع الأصلي، أما فيما يخص روابط الصفحات المزورة فهي تكون غالبا مكشوفة لأنه غير مطابق لرابط الموقع الأصلي و لهذا يلجأ بعض المتصيدون إلى قنص ضحايا عن طريق وضع روابط تشبه بشكل كبير الروابط الأصلية بحيث يكون الاختلاف بسيط جدا و يصعب على مبتدأ أو حتى شخص يعي هذه الأمور الانتباه إلى أن هذا الرابط هو لصفحة مزورة. نأخذ موقع الفيس بوك كمثال فالكل يعلم أن رابط الموقع هو

com.facebook.www يقوم المتصيد بإنشاء رابط يكون الاختلاف فيه بسيط جدا بحيث يكون رابط الصفحة المزورة مثلا com.facabook.www هنا قام المتصيد بتغيير حرف واحد فقط وهو حرف e ليصبح a.

الاصطياد الإلكتروني

لا يعتمد فقط على رسائل البريد الإلكتروني فقط فقد تطورت هذه العملية لتشمل تقنيات جديدة للوصول إلى الضحايا ومن أهم هذه التقنيات هي:

Redirection and Other Malicious Code-Based Schemes

وتعتمد هذه الطريقة على أن يقوم المستخدم عن غير معرفة بتحميل برامج خبيثة على حاسوبه حيث وظيفة هذه البرامج هي إعادة توجيه المستخدم من دون علمه إلى موقع شبيه تماما بالموقع الذي يريد الدخول إليه ويقوم المتصيد بجمع المعلومات الخاصة التي يدخلها المستخدم وتسمى هذه العملية Redirection إعادة التوجيه.

phishing voice or Vishing ويقصد بها التصيد الصوتي:

وتتم هذه العملية عن طريق إرسال رسالة إلى الضحية تحتوي على رقم هاتف مزيف لخدمة العملاء وعندما يقوم الضحية بالاتصال به يتم سؤاله عن معلومات الشخصية والمالية، أو أن يقوم المتصيد بالاتصال مباشرة بالضحية ويوهمه على أنه أحد موظفي خدمة العملاء، ومع استخدام تقنية الصوت عبر الإنترنت وبعض البرامج التي توحي للمستخدم بأن الرقم الذي اتصل به هو رقم مركز خدمة عملاء فعلى وبهذا يصعب على الضحية معرفة أنه واقع في مصيدة .

- تصنيفات الاصطياد الالكتروني ودوافعه

1. **هجمات التصيد الاحتيالي (PHISHING ATTACKS)**

التصيد الاحتيالي هو نوع من هجمات الهندسة الاجتماعية يُستخدم غالباً لسرقة بيانات المستخدم، بما في ذلك بيانات اعتماد تسجيل الدخول وأرقام بطاقات الائتمان.

يبدأ هذا الهجوم عندما يتمكن المجرم الإلكتروني من خداع ضحية ما بعد تنكره على شكل كيان موثوق به، حيث يصل للضحية بريد إلكتروني أو رسالة نصية تحفزه على النقر فوق ارتباط ضار، وحالما يستجيب المستلم وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج الفدية أو الكشف عن معلومات حساسة

خاصة بالمستلم.

2. **هجمات التصيد الاحتيالي بالرمح (SPEAR PHISHING)**

التصيد بالرمح هو عملية احتيال تتم أيضاً عبر البريد الإلكتروني أو الاتصالات الإلكترونية، وتستهدف فرداً أو منظمة أو شركة معينة. على الرغم من أن مجرمي الإنترنت يسعون غالباً إلى سرقة البيانات لأغراض ضارة، إلا أنهم قد يعلمون أيضاً تثبيت برامج ضارة على جهاز كمبيوتر الضحية.

تصل رسالة بريد إلكتروني للضحية وتبدو بأنها من مصدر موثوق، ولكنها بدلاً من ذلك تقود المستلم إلى موقع ويب مزيف مليء بالبرامج الضارة، وغالباً ما تستخدم رسائل البريد الإلكتروني هذه تكتيكات ذكية لجذب انتباه الضحايا.

على سبيل المثال، حذر مكتب التحقيقات الفيدرالي (FBI) من عمليات التصيد بالرمح حيث كان يصل للضحايا رسائل بريد إلكتروني تبدو بأنها واردة من المركز الوطني للأطفال المفقودين والمستغلين لتبدو أنها كيان موثوق، وقد كانت تلك الرسائل مزيفة وتهدف لاختراق أجهزة مستلميها.

3. **هجمات تصيد الحيتان (WHALE PHISHING)**

تصيد الحيتان هو مصطلح يستخدم لوصف هجوم التصيد الذي يستهدف بشكل خاص الوصول إلى معلومات حساسة وسرية لشخصيات قوية من الأفراد الأثرياء أو الأقوياء أو البارزين (على سبيل المثال، الرئيس التنفيذي لأي شركة). إذا أصبح فرد ما ضحية لهجوم تصيد احتيالي من هذا النوع، فيمكن اعتباره" تصيداً كبيراً "أو ما يسمى، "حوت."

4. **هجمات DRIVE- BY**

يشير هجوم by-Drive إلى هجوم إلكتروني يتسبب فيه برنامج نصي ضار في قيام برنامج ما بتنزيل وتثبيت نفسه على جهاز الضحية، دون إذن صريح منه. يمكن أن يحدث هذا النوع من الهجمات السيبرانية على أي جهاز مستخدم يعمل بأي نظام تشغيل، وغالباً ما تحدث هذه الهجمات عندما ينتقل المستخدم إلى صفحة ويب تم اختراقها ويتصفحها .

5. **برامج الفدية (RANSOMWARE)**

تعتبر برامج الفدية أحد أكثر الهجمات السيبرانية خطورة في هذا العصر، والذي تمكن من جعل المعلومات الحساسة للأفراد والمنظمات على المحك.

في هذا النوع من الهجمات، يضطر الضحية إلى حذف جميع المعلومات الضرورية من نظامه إذا فشل في دفع فدية ضمن الجدول الزمني الذي قدمه مجرمو الإنترنت، حيث إنهم غالباً يبتزون المستخدم بنشر ملفاته الهامة بحال لم يتم دفع الفدية.

6. **الهجوم بكلمة المرور**

في هذا النوع من الهجمات السيبرانية، يحاول المهاجمون اختراق حسابات مختلفة للضحايا من خلال اختراق ملفاتهم الشخصية وكلمات المرور الخاصة بهم مما يمنحهم وصولاً غير قانوني إلى جميع معلومات الضحية ليتم استخدامها من المهاجمين لتحقيق أهدافهم من سرقة البيانات أو التصيد الاحتيالي أو إدخال البرامج الضارة على الشبكات.

7. **هجمات التنصتEAVESDROPPING**

هجوم التنصت، المعروف أيضاً باسم هجوم sniffing أو التطفل snooping، هو سرقة المعلومات حيث يتم نقلها عبر شبكة عن طريق جهاز كمبيوتر أو هاتف ذكي أو جهاز آخر متصل. يستفيد هذا النوع من الهجمات السيبرانية من اتصالات الشبكة غير الآمنة للوصول إلى البيانات أثناء إرسالها أو استلامها من قبل مستخدمها عبر الشبكة لسرقتها.

8. **هجمات البرامج الضارة (MALWARE ATTACKS)**

هجمات البرامج الضارة هي أي نوع من البرامج الضارة المصممة لإحداث ضرر أو تلف لجهاز كمبيوتر أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي.

9. **حصان طروادة(TROJAN HORSES)**

وهو نوع من البرامج الضارة يتم إخفاؤه عادةً كمرفق في رسالة بريد إلكتروني أو ملف مجاني للتنزيل ، ثم ينتقل إلى جهاز المستخدم. بمجرد التنزيل، سينفذ الكود الضار المهمة التي صممها المهاجم من أجلها، مثل الوصول إلى الباب الخلفي لأنظمة الشركة، أو التجسس على نشاط المستخدمين عبر الإنترنت، أو سرقة البيانات الحساسة.

10. **هجمات الرجل في الوسط**

هجوم middle-the-in-man هو نوع من هجمات التنصت، حيث يقاطع المهاجمون محادثة موجودة أو نقل بيانات سرية بين طرفين.

11. **هجمات رفض الخدمة (DOS: SERVICE-OF-DENIAL وهجمات رفض الخدمة (DDOS: DISTRIBUTED DENIAL-OF-SERVICE)الموزعة**

يؤدي هجوم رفض الخدمة (DoS) إلى إغراق الخادم بحركة المرور، مما يجعل موقع الويب أو المورد غير متاح. أما هجوم رفض الخدمة الموزع (DDoS) هو هجوم DoS يستخدم أجهزة كمبيوتر أو أجهزة متعددة لإغراق مورد مستهدف.

12. التلاعب بـ URL (URL Manipulation).

لا تعد عناوين URL مجرد عناوين للمتصفحات والخوادم لاستخدامها أثناء انتقال المستخدمين من صفحة إلى أخرى باستخدام الروابط، فهي عبارة عن طلبات من المتصفح إلى الخادم والتي تعمل كشكل من أشكال البرمجة منخفضة المستوى .عندما يطلب المتصفح X من الخادم، يستجيب الخادم بـ Y.

13. DNS TUNNELING

هو هجوم يصعب اكتشافه يقوم بتوجيه طلبات DNS إلى خادم المهاجم، مما يوفر للمهاجمين قناة قيادة وتحكم سرية ومسار لتصفية البيانات.

14. اختطاف الجلسة SESSION HIJACKING

يعمل هجوم Session Hijacking على استغلال آلية التحكم في جلسة الويب، والتي تتم إدارتها عادةً لرمز مميز للجلسة. يتّبع هذا النوع من الهجمات السيبرانية طريقة للاستيلاء على جلسة مستخدم الويب عن طريق الحصول خلسة على معرف الجلسة والتنكر في صورة المستخدم المصرح له.

بمجرد الوصول إلى معرف جلسة المستخدم، يمكن للمهاجم أن يتنكر مثل هذا المستخدم ويفعل أي شيء مخول للمستخدم القيام به على الشبكة.

15. القوة الغاشمة(BRUTE FORCE)

يعل المهاجمون في هذا النوع من الهجمات السيبرانية على تجربة مجموعات مختلفة من أسماء المستخدمين وكلمات المرور حتى يعثروا على واحدة تعمل، وقد يعمل المهاجم على تخمين المفتاح الذي يتم إنشاؤه عادةً من كلمة المرور باستخدام وظيفة اشتقاق المفتاح (function derivation key) ويُعرف هذا بالبحث الشامل عن مفتاح .

16. هجمات البرمجة النصية عبر المواقع (CROSS- SITE SCRIPTING)

هجمات البرمجة النصية عبر المواقع (XSS) هي نوع من الحقن، حيث يتم حقن البرامج النصية الخبيثة في مواقع الويب الحميدة والموثوقة.

تحدث هجمات XSS عندما يستخدم المهاجم تطبيق ويب لإرسال تعليمات برمجية ضارة، بشكل عام في شكل نص برمجي من جانب المستعرض، إلى مستخدم نهائي مختلف. لا بد من العمل بشكل دائم على اكتشاف العيوب التي قد تسمح لهذه الهجمات بالنجاح.

17. حقن SQL (SQL INJECTION)

يتكون هجوم حقن SQL من إدخال أو "حقن" استعلام SQL عبر حقول الإدخال من العميل إلى التطبيق من أجل التأثير على تنفيذ أوامر SQL المحددة مسبقاً. يمكن للمهاجم الذي يستخدم هذه الطريقة بحال نجاحها قراءة البيانات الحساسة من قاعدة البيانات، وتعديل بيانات قاعدة البيانات من (إدراج / تحديث / حذف)، وتنفيذ عمليات الإدارة على قاعدة البيانات (مثل إيقاف تشغيل DBMS)، واستعادة محتوى ملف معين موجود في DBMS وفي بعض الحالات إصدار أوامر لنظام التشغيل.

18. التهديدات من الداخل

تحدث العديد من أنواع الهجمات السيبرانية يومياً، والحقيقة الأكثر إثارة للصدمة هي أنه في معظم الأحيان، يكون هناك شخص من الداخل يشارك في العملية لمساعدة مجرمي الإنترنت في الحصول على معلومات حول منظمتهم، ويتم ذلك من خلال تزويد أولئك المجرمين بكل المعلومات الضرورية للولوج، مما يؤدي إلى عواقب كارثية على المنظمة. تعتبر التهديدات من الداخل أحد التهديدات الشائعة للهجمات السيبرانية على البنوك والمؤسسات المالية.

19. هجمات الذكاء الاصطناعي

يركز التعلم الآلي على تعليم الكمبيوتر لأداء عدة مهام بمفرده بدلاً من الاعتماد على البشر في إجرائها يدوياً. يستخدم الذكاء الاصطناعي، في بعض الأحيان، لاختراق الأنظمة الرقمية للحصول على معلومات غير مصرح بها، كما يمكن استخدامه أيضاً لسرقة البيانات المالية السرية.

20. هجمات عيد الميلاد(ATTACKS BIRTHDAY)

هجمات عيد الميلاد هي من أنواع القوة الغاشمة من الهجمات السيبرانية التي تهدف إلى تشويه الاتصال بين العملاء ومختلف الأفراد في الشركة بدءاً من المدير التنفيذي وانتهاءً بموظفيها. هجوم عيد الميلاد هو نوع هجوم التشفير الذي يكسر خوارزميات الرياضيات من خلال إيجاد التطابقات في دالة التجزئة.

- التجسس الالكتروني

التجسس الإلكتروني هو عبارة عن عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على معلومات غير معلنة على العلن.

أكثر الاسلاك التي تعاني من التجسس الالكتروني هي الأسلاك الأمنية وكل ما يتعلق بها، خاصة وان العالم يعيش في حالة تنافسية لا تنتهي بين الدول العظمى وبين دول الصراع في الشرق الأوسط. ويقوم بهذا النوع من الاختراقات المحوسبة مجموعات من المبرمجين الذين يكون هدفهم الأساسي هو الحصول على المعلومات اما عن طريق جهة رسمية او عن طريق اشخاص عابثين لا يملكون هدفا واضحا من التجسس بقدر ما يمارسون التجسس لتنمية مهاراتهم التجسسية عبر

المنصات الالكترونية ومواقع التواصل الاجتماعي. يتم التجسس عن طريق الوصول الى الملفات الرئيسية في الحواسيب والأجهزة الذكية وزرع برامج تجسس وتسجيل بيانات ثم رفعها الى أجهزة الشخص القائم بأعمال الابتزاز وحفظها في ملفات خاصة ليتم استخدامها في الوقت المناسب.

- **أهداف التجسس الإلكتروني**

للتجسس الالكتروني عدة مهام وهي:

• تجسس الهجوم: ينفذ من أجل التجسس على العدو من خلال اختراق منظومة حواسيبه ومواقعه الإلكترونية ومهاجمة شبكات العدو بالفيروسات والتخريب وتدمير منظوماته الإلكترونية وهذه من اكثر طرق التجسس اتباعا بين الأطراف التي ينشب بينها صراع سياسي .

• تجسس الرقابة: هذا الأسلوب تقوم به الدول في غالب الأحيان من خلال مراقبة وسائل التواصل الاجتماعي ومراقبة حركة الأموال ومراقبة إيميلات وحواسيب المشتبه بهم وحتى مراقبة حركة عجلات الشرطة والجيش ضمن منظومة gps.

• تجسس الوقاية: لصد تجسس العدو وتحصين شبكة حواسيب الدولة والأجهزة الأمنية لحماية الشبكات من الفيروسات وأي محاولات تخريبية ويتمثل ذلك بالتحول الرقمي وهذا النوع بالذات يأتي ردا على النوع الأول أي نوع التجسس الهجومي.

- **أشهر أساليب وطرق التجسس الإلكتروني**

يمكن للتجسس ان يحدث بأكثر من طريقة وأسلوب، ولكن ما هي اكثر الطرق تطورا في المجال على ارض الواقع وكيف تعمل:

• ساعة حائط: من أشهر أساليب التجسس هي ساعة الحائط حيث تحتوي على كاميرا مخفية وتعمل بتقنية G3، مزودة ببطارية ذات عمر طويل. يمكن الاتصال بها عبر شريحة مزودة بها والاستماع إلى التسجيلات، كما يمكن أن تستقبل رسائل نصية لتفعيل عملها وبدء التسجيل أو الإيقاف، وبها إمكانية التسجيل بشكل مباشر إلى ذاكرة تخزين SD ويمكن وضع ذاكرة بحجم 32 جيجا بايت. إضافة الى انه من الممكن بث تسجيل مباشر واستقباله بواسطة هاتف

androidومتابعة ما يجري. هناك الكثير من هذه الأجهزة مثل أجهزة على شكل قلم أو ساعة يد أو ميدالية مفتاح سيارة شبيهة بجهاز الريموت للسيارات وغيرها وهي الأجهزة المتعارف عليها في الجاسوسية التقليدية، ولكنها تطورت فيما بعد لتصبح احد اقوى أدوات التجسس الالكترونية.

• أقمار التجسس التي تحتل السماء: تعتبر الأقمار الصناعية من اهم أساليب التجسس الالكتروني حيث انها تتطور كل عام مع تطور التكنولوجيا في العالم، يوجد 5000 قمر صناعي في سماء العالم وظيفتها مراقبة الدولة لسكانها ومراقبة الدول الأخرى التي من شأنها ان تحدث صراعات بينهما،

غالبية الدول تصرح بأن اقمارها الصناعية هي أقمار مدنية وليست جاسوسية، ولكن التنافس على شراء هذه الأقمار والفائدة التي تعود اليهم منها تثبت عكس كلامهم المحكي.

• تطبيقات الجاسوسية الالكترونية: يستخدم هذا الأسلوب بالاعتماد على التنقل الجغرافي للشخص مع الربط على مواقع التواصل الاجتماعي ومتابعة المنشورات التي يقوم الشخص بنشرها والتفاعل معها، استخدمت هذه التطبيقات والبرامج مع الإرهابيين في دول العالم، الذين كانوا ينتمون الى جهات مشكوك بأمرها، يقوم البرنامج بمراقبة نشاط الفرد على المنصات الالكترونية وتتبع انتقاله وتسجيل الجهات التي يلتقي معها على ارض الواقع مع تسجيل صوتي للحديث الذي يدور بين هؤلاء الأطراف.

• نظارات التجسس الاستخباراتية: تعتبر هذه النظارات أداة تجسس حكومي اذ يشتهر بها رجال الشرطة في الموانئ والمطارات، وهي عبارة عن نظارة شمسية تعطي الملف الجنائي الكامل لأي احد يقع نظر الشرطي عليه، هذه النظارات وظيفتها الإمساك بالمجرم والتعرف عليه، حتى لو كان بين عشرات الالاف من الناس.

• الحشرات التجسسية: اليعسوف والصرصار والذبابة هم 3 أنواع حشرات تم تطوير أجهزة تجسس تشبههم تماما ولكل واحد منهم تقنيات ومميزات تختلف عن الاخر، تم تطوير هذه الأجهزة في سنوات مختلفة ولكل منهم لوظيفة، اهم ووظيفة وأكثرها حساسية هي التي تملكها ذبابة التجسس وهي ان تحط على جسد الشخص المطلوب بمساعدة أجهزة الاستشعار والكاميرات الدقيقة وبعد ان تحط على جسده تقوم بسحب عينة حمض نووي من الشخص وحملها الى المركز المختص دون ان يشعر الشخص.

- **مفهوم الهجوم الالكتروني**

يطلق على الهجوم الإلكتروني اسم الهجوم السيبراني، ويُعرّف بأنهُ محاولة من قبل فرد أو مجموعة لتهديد نظام كمبيوتر أو شبكة أو جهاز، بقصد التسبب في ضرر معين، ومن الممكن أن تكون هذه الهجمات ضد الحكومات أو الشركات أو الأفراد وليست بالضرورة واسعة النطاق، وتشير بعض الدراسات أنّه يمكن للهجوم الإلكتروني أن يشل نظام الكمبيوتر بالكامل، مما يعني أن الشركة تخسر المال لأن موقعها على الويب لا يمكن الوصول إليه، أو يمكن أن تمنع هيئة حكومية من تقديم خدمة أساسية، وقد يؤدي إلى سرقة كميات كبيرة من البيانات الحساسة، والتي يمكن أن تؤثر بعد ذلك على الأفراد على المستوى الشخصي أو المالي

- **أنواع الهجوم الالكتروني**

وأبرز أنواع الهجمات الإلكتروني ما يأتي:

هجوم تعطيل الخدمة

يعمل هجوم رفض الخدمة على إغراق الأنظمة أو الخوادم أو الشبكات بسيل من حركة مرور البيانات لاستنفاد الموارد والنطاق الترددي. ونتيجة لذلك، يتعذر على النظام تنفيذ الطلبات المشروعة. كما يمكن للمهاجمين استخدام العديد من الأجهزة المخترقة لشن هذا الهجوم. ويُعرف هذا بهجوم رفض الخدمة الموزّع DDoS

هجوم اختطاف البروتوكول

هو هجوم يتم فيه الاستيلاء على جلسة المستخدم من قبل المهاجم. ومن المتعارف ان الجلسة تبدأ عند قيامك بتسجيل الدخول إلى إحدى المواقع او الخدمات، على سبيل المثال المواقع المصرفية او المتاجر، وتنتهي الجلسة عند تسجيل الخروج. وبالتالي يتم الاستلاء على هذه الجلسة والتصرف بها كأنه مالك الجلسة الفعلي.

الفصل الثامن
أمن التعاملات الالكترونية

- ## مفهوم التصفح الأمن ومميزاته

يُعرف التصفح الآمن بأنّه أحد الخدمات التي أطلَقها فريق الأمان الخاص بِشركة جوجل العالمية، وذلك بهدف تحديد مواقع الويب غير الآمنة عند تصفح الإنترنت وتنبيه المستخدمين وأصحاب تلك المواقع بالمخاطر المُتوقعة، ويَسمح التصفح الآمن باستعمال بنية تحتية خاصة تُتيح للمستخدم تَصفح المواقع الإلكترونية بِشكل محمي من أنواع مختلفة من الهجمات الإلكترونية كالبرامج الخبيثّة والضارة ومحاولات الاحتيال، وهُناك العديد من مُتصفحات الإنترنت التي تُستخدم لاستِعراض المواقع المختلفة، لِذا يجب اختيار متصفح الإنترنت الذي يتيح التصفح الآمن.

- ## مميزات التصفح الآمن لشبكة الإنترنت

هُناك العديد من قواعد الاستخدام الآمن للإنترنت التي يجب الالتزام بها، إذ يُتيح التصفح الآمن عددًا من المزايا للمستخدمين، وفيما يأتي توضيح أبرز مميزات التصفح الآمن:

• التحقق من مواقع الويب ومُقارنتها مع قوائم التصفح الآمن للمواقع الضارة بِناءً على الاستراتيجية المُطبقة في موقع جوجل وأنواع التهديدات المُحتملة.

• تَنبيه المُستخدم قبل النقر على الروابط المَوجودة في أي موقع ويب والتي قد تَنقلُه إلى صفحات مليئة بالفيروسات.

• مَنع المُستخدم من نَشر أي روابط لِصفحات مَعروفة بأنّها خطيرة على أي موقع ويب.

• حِماية جميع مُستخدمي الويب من التصيد والبرامج الضارة والخبيثة من خِلال إشعارهم بِمحاولة زِيارة موقع خطير.

• إتاحة مِيزة التصفح الآمن مجانًا من قبل شركة جوجل للشركات الأخرى لاستخدامِها في مُتصفحاتِهم وعَدم اقتِصاره على مُستخدمي كروم فقط لِجعل الإنترنت أكثر أمانًا.

• حَظر المواقع غير المُلائمة للأطفال، إذ يساعد التصفح الآمن لشبكة الإنترنت على حماية الأطفال من مخاطر الإنترنت.

- ## المخاطر التي تهدد المستخدم أثناء تصفح الإنترنت

التطبيقات الخبيثة

برنامج يحمل حمولة مدمرة، ويتكرر وينتشر بسرعة لإصابة الأنظمة الأخرى. حيث إنه إلى حد بعيد، لا تزال الفيروسات / البرامج الضارة هي التهديد الأكثر انتشارًا للحوسبة.

رسائل البريد المجهولة

التحميل من مواقع غير موثوقة

يُنفّذ هذا الخطر من خلال استهداف مواقع الويب الضعيفة، وتحميل عدد من الرموز الخطيرة عليها، وفي حال دخول أحد المستخدمين لهذه المواقع سرعان ما يتعرّض النظام الخاص به للسرقة، أو التسبب بتعطل الخدمات الرئيسية فيه. يُمكن الوقاية من خطر الهجوم من خلال تطبيق أمر إيقاف تشغيل البرامج النصية للصفحات، أو تثبيت الوظائف الخاصة بحظر البرامج النصية على المتصفح

- **خطوات التصفح الأمن من خلال الإنترنت**

يُمكن تفعيل تصفح جوجل الآمن لِمتصفحات كروم في أجهزة الحاسوب باتِباع الخُطوات الآتية أدناه:

• فتح متصفح كروم على جهاز الحاسوب.

• الانتقال إلى أعلى يمين الشّاشة والضغط على الثلاث نقاط الرأسية، ثم اختيار الإعدادات. (Settings)

• الانتقال إلى جزء الخصوصيّة والأمان (Privacy and security)، والضغط على الأمان

•. (Security) تحديد مستوى التصفح الآمن الذي يَرغب به المستخدم، إذ تَظهر عدة خيارات وهي؛ الحماية العادية، أو الحماية المحسنة، أو بلا حماية.

- **أمن الصحة الالكترونية**

تعرّف منظمة الصحة العالمية الصحة الإلكترونية بأنها الاستخدام الفعّال من حيث التكلفة والآمن لتكنولوجيات المعلومات والاتصالات في دعم المجالات المتصلة بالصحة، بما في ذلك خدمات الرعاية الصحية، والمراقبة الصحية، والمؤلفات الصحية، والتعليم الصحي، والمعرفة والبحوث الصحية.

- **الأمان في مواقع التواصل الاجتماعي**

التواصل مع أشخاص جدد هو شيء جيد ويمكن لمواقع التواصل الاجتماعية مثل فيسبوك وإنستغرام أن تساعدك على الشعور بالتواصل أكثر مع بلدك ان كنت مغتربا أو مع عائلتك. لكن مواقع التواصل الاجتماعية ممكن أن تكون خطرة. من المهم أن تفهم المخاطر حتى تتمكن من حماية نفسك.

- **طرق حماية نفسك في وسائل التواصل الاجتماعي:**

تسمى معلوماتك الشخصية أحياناً بالبيانات. لا تحتاج أبداً إلى إعطاء بيانات شخصية مهمة، مثل أرقام الهوية، أو أرقام البنوك، أو كلمات المرور ،أو عنوانك على مواقع التواصل الاجتماعي. للحفاظ على أمان مستخدميها، تحتوي الشبكات الاجتماعية على إعدادات خصوصية يمكنك استخدامه لجعل معلوماتك (البيانات) آمنة.

– حافظ على بياناتك آمنة على فيسبوك

عند وضع بياناتك على فيسبوك، وعند تسجيل الدخول إلى التطبيقات والمواقع، فإنك تتيح الوصول إلى بياناتك. قد تستخدم هذه التطبيقات والمواقع البيانات بطرق لا تريدها. في الغالب يستخدموها للسماح للمعلنين ببيع المنتجات لك. يمكنك إيقاف التطبيقات المواقع من استخدام بياناتك. في فيسبوك، انتقل إلى إعداداتك. للعثور على الإعدادات، انقر فوق "v "(الرمز السفلي) في الزاوية اليمنى العليا من الشاشة وحدد "settings."ثم انقر على " Websites and Apps "في القائمة على اليسار. ثم سترى التطبيقات التي لديها حق الوصول إلى البيانات الخاصة بك. يمكنك النقر على كل تطبيق لـ تعديل ما يمكنهم الوصول إليه. للبقاء آمناً على وسائل التواصل الاجتماعي، يمكنك أيضاً حذف التطبيقات تماماً.

– استخدام كلمات مرور قوية

ينصحنا خبراء أمن الإنترنت دائماً بأن يكون لدينا كلمات مرور قوية ومختلفة لجميع حساباتنا. كما ينصحوننا باستخدام المصادقة الثنائية (خطوات إضافية لتسجيل الدخول) أو أدارة كلمات المرور.

– الحفاظ على الخصوصية على مواقع التواصل الاجتماعي

لا تشارك التفاصيل الشخصية أو الصور عبر الإنترنت التي تمانع في رؤيتها من أي شخص، مثل رئيسك في العمل. قد تعتقد أنك تشاركها فقط مع أصدقائك المقربين وعائلتك، ولكن بمجرد أن يكون هناك شيء عبر الإنترنت، يمكن مشاركته على نطاق أوسع. أيضاً،بمجرد أن يكون على الانترنت، لا يمكنك التخلص منه لأن الآخرين لديهم نسخ منه. تم طرد العديد من الأشخاص أو رفضوا للحصول على وظيفة بسبب ملفاتهم الشخصية على الإنترنت.

– لا تصدق كل شيء ولا تصدق الجميع

الكثير من المعلومات على وسائل التواصل الاجتماعي كاذبة. في بعض الأحيان ، الناس على وسائل التواصل الاجتماعي ليسوا حتى أشخاصاً حقيقيين ، وفي كثير من الأحيان لا تكون الأمور حقائق على الإطلاق. قد يكون هؤلاء الأشخاص مع أسماء كاذبة أو bot (a fake robot) قد تكون تقارير إخبارية مزيفة أو رسائل رسمية تتظاهر بأنها من مسؤول حكومي أو مسؤول تجاري .

لا تصـدق كل ما تقرأه على وسـائل التواصـل الاجتماعي]. إذا كنت تقرأ شـيئاً ما، فتحقق من مصادر أخرى، مثل الموقع الإلكتروني لصحيفة وطنية.

– البقاء آمناً دون اتصال، أيضاً

فكر في أمانك في العالم الحقيقي عند نشـر معلومات حول أنشـطتك. لا تحتاج إلى نشـر عنوانك عبر الإنترنت ثم نشـر صـور العطلة لإعلام الجميع بأنك بعيد. إذا كنت تنشـر على الفيسبوك قضاء العطلة خارجاً مع عائلتك، سيعرف الناس أن منزلك فارغ .

– كن حذر جداً إذا كنت تلتقي بشخصٍ ما

تسـهل وسـائل التواصـل الاجتماعي على الناس تعويض الهويات. على الانترنت، يمكنهم التظاهر بأنهم شـخص آخر. إذا كنت تتصـل مع شـخص ما عبر الإنترنت ، لا ترتب أبداً لمقابلة هـذا الشـخص بمفرده أو الـذهـاب إلى منزلـه أو دعوتـه إلى منزلـك إلا إذا كنـت تعرف بـأنهم من يدعون فعلاً. أجتمع بالغرباء دائماً في مكان عام وعندما يكون هناك أشخاص آخرين حولكم .

– عدم إرسال الأموال أو كلمات المرور

لا ترسـل الأموال إلى أي شـخص عندما لا تكون متأكداً 100٪ منهم. المكاتب الحكومية، مثل IRS ، والشـركات الحقيقية، مثل مايكروسـوفت، لا تطلب منك إرسـال الأموال مباشـرة إلى حسـابات مصـرفية غريبة. كما أنهم لا يطلبون كلمة المرور الخاصـة بك إلى أي شـيء. لا ترسـل كلمة المرور الخاصة بك إلى أي شخص تلتقي به من مواقع التواصل الاجتماعية أو أماكن أخرى على الإنترنت.

– حماية نفسك من الأشخاص العدائيون أو غير اللطفاء

يسـتهدف الناس المعادون أو غير اللطفاء اللاجئين والمهاجرين. لا تقبل طلبات الصـداقة من أشـخاص لا تعرفهم. قم على الفور بحظر أي شـخص ينشـر شيء مهدد على أي من حسـاباتك. لا ترد. لا تكتب أشـياء فظة أو عدائية قد تجعلك أكثر من هدف. قم بالإبلاغ عن التهديدات الشخصية للشرطة وموقع التواصل الاجتماعي الذي تم نشره عليه.

– حماية نفسك من الحيل والمخترقون

لا تنقر على الروابط فقط لأنها ترسـل إليك، حتى لو كانت تأتي من صـديق (قد لا يعرفون أن الرابط خطير ، أو ربما تم اختراقه). فقط قم بحذفها. لن يتم إرسـال أي شـيء مهم لك بهذه الطريقة. من المرجح أن تحتوي الروابط التي لم تطلبها على فيروسـات من شـأنها أن تضـر جهازك أو تسـمح للأشـخاص بالدخول إلى جهازك لسـرقة معلوماتك وأموالك وهويتك.

– حافظ على سلامة أطفالك

حتى إذا كنت لا تسـتخدم وسـائل التواصـل الاجتماعية أو تفهمها، فسـتحتاج إلى معرفة ما يكفي حول هـذا الموضـوع للحفاظ على أطفالك في مأمن من مخاطر مواقع التواصـل الاجتماعي.

إذا كنت تستخدم وسائل التواصل الاجتماعية بنفسك، أحمي أطفالك بعدم وضع معلومات عنهم عبر الإنترنت. إذا كنت لا تستخدم وسائل التواصل الاجتماعية، اسأل أطفالك عن الشبكات الاجتماعية التي يستخدموها. يمكن أن يتعرضوا للتنمر، وللمفترسين الجنسيين، وللمحتوى السيئ ،والإعلان.

- **حماية البيانات الشخصية في التجارة الالكترونية**

التجارة الالكترونية تعني ممارسة الاعمال التجارية على شبكة الانترنت وتشمل عمليات بيع وشراء السلع او الخدمات عبر الانترنت. في الوقت الحاضر العديد من الشركات ذات السمعة الطيبة مقبلة على هذا النمط من ممارسة الاعمال التجارية لتغطية سوق اوسع. ويغطي الامن الالكتروني او امن الانترنت مجموعة واسعة من الانشطة للحفاظ على المعلومات الالكترونية الامنة.

البيانات الشخصية

البيانات الشخصية هي البيانات الهامة لكل شخص والتي يتم تداولها عادة عند اجراء عمليات متعلقة بالتجارة الالكترونية ومنها ما يلي:

- الاسم والعنوان
- ارقام الهاتف
- البريد الالكتروني
- كلمة السر للحسابات
- البيانات المالية
- البيانات الاجتماعية

المقصود بحماية البيانات الشخصية

حماية البيانات الشخصية تعني حماية المعلومات المتعلقة بشخص الفرد وحياته الخاصة من التعرض للاعتداء وخاصة في ظل التحديات الرقمية.

اجراءات الامان عند التعاملات الالكترونية

توجد عدد من الاجراءات التي يمكن اتباعها لتحقيق الامان عند التعاملات الالكترونية ومنها ما يلي:

- استخدام بروتوكولات الامان العالمية المتعددة
- استخدام وسائل الدفع الامنة
- عدم مشاركة البيانات الشخصية
- اختيار كلمة مرور قوية
- عدم التصريح لاي شخص بكلمة السر

- الحفاظ على المعلومات البنكية
- التأكد من المواقع التي يتم التعامل من خلالها

- **التحقق الرقمي من الهوية**

الهوية الرقمية هي وسيلة إلكترونية لتعريف الشخص. وتتكون من شهادة تحتوي على مفتاح عام يمكن مشاهدته ومفتاح خاص يظل سرًا . يتيح لك المفتاح الخاص التوقيع على مستند إلكتروني بتوقيع يمكن للآخرين التحقق منه باستخدام المفتاح العام الخاص بك فقط. وبالمثل، يمكن للمفتاح الخاص إلغاء تشفير المستندات التي قام آخرون بتشفيرها باستخدام المفتاح العام الخاص بك.

التحقق من الهوية الرقمية

في الماضي كان ذلك سهلاً من خلال تواجدك في الفرع وإتمامك جميع الإجراءات بشكل شخصي، حيث يستطيع موظف البنك التحقق من هويتك بكل سهولة. لذا، في هذا العالم الرقمي، كيف يمكنك إنشاء إجراءات صارمة للتحقق من الهوية والتي تكون أيضًا سهلة من وجهة نظر العميل؟؟؟ قبل الانتقال للإجابة على هذا التساؤل، يجب توضيح الآتي، الهوية الرقمية المقصودة في حوارنا هذا هي المعرِّفات التي تحتاجها الجهة للتأكد من أن مستخدم النظام هو الشخص المعني بذلك وليس شخص آخر، وهذا المفهوم يختلف اختلافا كليا عن النسخة الرقمية من الهوية الشخصية التي باتت تستخدم بكثرة في كافة الدول المتقدمة، مثل الهوية الرقمية المرتبطة بتطبيق أبشر في المملكة العربية السعودية، فهذه الهوية هي نسخة إلكترونية

الفصل التاسع
وسائل الأمن المادي وأساليب أمن التقنيات المختلفة

- ## مفهوم الأمن المادي وخصائصه

يصف الأمن المادي Physical security التدابير الأمنية security التي تم تصميمها لمنعة الوصول غير المصرح به إلى المرافق والمعدات والموارد، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس Espionage أو السرقة Theft، أو الهجمات الإرهابية .(Terrorist ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة CCTV، وحراس الأمن Security guards، حواجز واقية Protective barriers، والأقفال locks، وبروتوكولات التحكم في الوصول control Access ، والعديد من التقنيات الأخرى.

- ## أهمية الأمن المادي

تهدف أنظمة الأمن المادي للمرافق المحمية عموما إلى:

• ردع المتسللين المحتملين (مثل علامات التحذير وعلامات الحدود الخارجية).

• تمييز الأشخاص المأذون لهم من غير المصرح لهم (مثل استخدام بطاقات المفاتيح / شارات الوصول).

• تأخير إحباط، ومنع محاولات التسلل (مثل الجدران قوية، وأقفال الأبواب وخزائن).

• كشف الاختراقات ورصد / تسجيل الدخلاء (مثل أجهزة الإنذار عن الدخلاء وأنظمة الدوائر التلفزيونية المغلقة)

• إطلاق ردود الفعل المناسبة (على سبيل المثال من قبل حراس الأمن والشرطة)

- ## أنظمة الأمن المادي

طرق الردع

هدف الردع هي إقناع المهاجمين المحتملين بأن الهجوم الناجح غير مرجح بسبب الدفاعات القوية. طبقة الأمان الأولية للحرم الجامعي، أو المبنى، أو المكتب، أو استخدامات المساحة المادية الأخرى منع الجريمة من خلال التصميم البيئي لردع التهديدات. بعض الأمثلة الأكثر شيوعًا هي أيضًا الأكثر أساسية: علامات التحذير أو ملصقات النوافذ، الأسوار ، حواجز المركبات ، قيود ارتفاع السيارة ، نقاط الوصول المقيدة ، الإضاءة الأمنية والخنادق.

حواجز طبيعية

تعمل الحواجز المادية مثل الأسوار والجدران وحواجز المركبات كطبقة خارجية من الأمان. إنها تعمل على منع ، أو على الأقل تأخير ، الهجمات ، وتعمل أيضًا كرادع نفسي من خلال تحديد محيط المنشأة وجعل عمليات الاقتحام تبدو أكثر صعوبة. غالبًا ما يتم وضع سياج طويل يعلوه أسلاك شائكة أو أسلاك شائكة أو مسامير معدنية على محيط العقار ، مع نوع من اللافتات التي تحذر الأشخاص من محاولة الدخول.

حواجز الجمع

تم تصميم الحواجز عادة لهزيمة التهديدات المحددة. هذا جزء من ارقام المباني وكذلك رموز الحريق. بصرف النظر عن التهديدات الخارجية ، هناك تهديدات داخلية نار وهجرة الدخان وكذلك التخريب.

فيجب هزيمة التهديدات المتعددة في وقت واحد ، والتي يجب أخذها في الاعتبار في التصميم.

المراقبة الطبيعية

شكل رئيسي آخر من أشكال الردع التي يمكن دمجها في تصميم المرافق هو المراقبة الطبيعية، حيث يسعى المهندسون المعماريون إلى بناء مساحات أكثر انفتاحًا ومرئية لموظفي الأمن والمستخدمين المصرح لهم ، بحيث لا يتمكن المتسللون / المهاجمون من أداء نشاط غير مصرح به دون رؤيتهم. مثال على ذلك هو تقليل كمية النباتات الطويلة الكثيفة في المناظر الطبيعية حتى لا يتمكن المهاجمون من إخفاء أنفسهم بداخله

الإضاءة الأمنية

يقل احتمال دخول المتسللين إلى مناطق جيدة الإضاءة خوفًا من رؤيتهم. يجب أن تكون الأبواب والبوابات والمداخل الأخرى ، على وجه الخصوص ، مضاءة جيدًا للسماح بالمراقبة الدقيقة للأشخاص الذين يدخلون ويخرجون. تكون الإضاءة المنخفضة الكثافة الموزعة على نطاق واسع أفضل بشكل عام من البقع الصغيرة للإضاءة عالية الكثافة ، لأن الأخيرة قد تميل إلى إنشاء نقاط عمياء لأفراد الأمن وكاميرات الدوائر التلفزيونية المغلقة.

أنظمة الإنذار وأجهزة الاستشعار

تعمل أنظمة الإنذار جنبًا إلى جنب مع الحواجز المادية والأنظمة الميكانيكية وحراس الأمن، مما يؤدي إلى إطلاق استجابة عندما يتم اختراق هذه الأشكال الأخرى من الأمان. وهي تتكون من أجهزة استشعار بما في ذلك مجسات المحيط، مجسات الحركة ومستشعرات الاتصال و كاشفات كسر الزجاج.

المراقبة بالفيديو

كاميرات الدوائر التلفزيونية المغلقة، كاميرات المراقبة يمكن أن يكون رادعا عند وضعها في مواقع مرئية للغاية وتكون مفيدة

لتقييم الحوادث والتحليل التاريخي. على سبيل المثال، إذا تم إنشاء إنذارات وكانت هناك كاميرا في مكانها، يقوم أفراد الأمن بتقييم الموقف عبر موجز الكاميرا. في الحالات التي حدث فيها هجوم بالفعل وكانت الكاميرا في مكانها عند نقطة الهجوم، يمكن مراجعة الفيديو المسجل.

صلاحية التحكم صلاحية الدخول

صلاحية التحكم صلاحية الدخول يتم استخدام الطرق لمراقبة حركة المرور والتحكم فيها من خلال نقاط وصول ومناطق محددة في المنشأة الآمنة. يتم ذلك باستخدام مجموعة متنوعة من الأنظمة بما في ذلك CCTV مراقبة، بطاقات هوية، حراس الأمن، القراء البيومترية وأنظمة التحكم الإلكترونية / الميكانيكية مثل الأقفال والأبواب الدوارة.

أنظمة التحكم في الوصول الميكانيكية

الباب الدوار البصري ذو الذراع المسقطة نظام إلكتروني للتحكم في الدخول ، يتحكم في الدخول من خلال باب.

أنظمة التحكم في الوصول الميكانيكية تشمل الأبواب الدوارة، والبوابات، والأبواب، والأقفال. مفتاح التحكم من الأقفال مشكلة مع عدد كبير من المستخدمين وأي معدل دوران للمستخدمين. مفاتيح سرعان ما يصبح غير قابل للإدارة، مما يؤدي في كثير من الأحيان إلى اعتماد التحكم الإلكتروني في الوصول.

أنظمة التحكم في الدخول الإلكترونية

التحكم الإلكتروني في الوصول يدير عددًا كبيرًا من المستخدمين، ويتحكم في أوقات دورات حياة المستخدم والتواريخ ونقاط الوصول الفردية. على سبيل المثال، يمكن أن تسمح حقوق الوصول للمستخدم بالوصول من الساعة 0700 إلى الساعة 1900 من الاثنين إلى الجمعة وتنتهي الصلاحية في غضون 90 يومًا. [بحاجة لمصدر] غالبًا ما يتم ربط أنظمة التحكم في الوصول هذه بأبواب دوارة للتحكم في الدخول في المباني لمنع الوصول غير المصرح به. يقلل استخدام البوابات الدوارة أيضًا من الحاجة إلى أفراد أمن إضافيين لمراقبة كل فرد يدخل المبنى مما يسمح بإنتاجية أسرع.

نظم تحديد الهوية وسياسات الوصول

شكل آخر من أشكال التحكم في الوصول (إجرائية) يشمل استخدام السياسات والعمليات والإجراءات لإدارة الدخول إلى المنطقة المحظورة. مثال على ذلك هو نشر أفراد الأمن الذين يقومون بفحص الدخول المصرح به في نقاط الدخول المحددة مسبقًا.

أفراد الأمن

أفراد الأمن تلعب دورًا مركزيًا في جميع مستويات الأمان. جميع الأنظمة التكنولوجية المستخدمة لتعزيز الأمن المادي غير مجدية بدون قوة أمنية مدربة على استخدامها وصيانتها، يقوم أفراد الأمن بالعديد من الوظائف: تسهيلات الدوريات، وإدارة التحكم في الوصول الإلكتروني، والرد على الإنذارات، ومراقبة وتحليل لقطات الفيديو

- **الحماية المادية لمركز البيانات**

مركز البيانات، في أبسط صوره، عبارة عن مرفق مادي تستخدمه المؤسسات لإيواء تطبيقاتها وبياناتها المهمة. يستند تصميم مركز البيانات إلى شبكة من موارد الحوسبة والتخزين التي تمكّن تسليم بيانات وتطبيقات البرامج التي تمت مشاركتها. تشمل المكونات الرئيسية لتصميم مركز البيانات أجهزة التوجيه، والمبدلات، وجدران الحماية، وأنظمة التخزين والخوادم ووحدات التحكم في تسليم التطبيقات. ليس من المفيد الحصول على جميع المعدات وأحدث أنظمة تكنولوجيا المعلومات في مركز البيانات التي ليس لديها رقابة صارمة على أنظمة الدخول والخروج.

- **أمن البيانات الضخمة**

هنالك حلول عدة لأمن البيانات الضخمة، من أهمها :

قابلية التوسع يجب أن تكون الحلول الأمنية قادرة على التوسع لتشمل أي زيادة في الحجم من دون التأثير في الأداء.

استمرارية الأداء

على أنظمة تحليل البيانات أن تكون ذكية ودقيقة بالقدر الكافي دون الحاجة لتدخل أي عنصر بشري. لذا، من المهم تأمين البيانات الضخمة مزايا الذكاء الاصطناعي دون انقطاع.

الإتاحة والتكيف

تحتاج هذه الحلول لأن تكون قادرة على الوصول الكامل للبيانات أياً كان مكانها في المؤسسة أو الجهة المعنية.

المرونة

تستخدم بعض المؤسسات أطر عمل مفتوحة المصدر للبيانات الضخمة مثلSpark، لكن هذه البيئات تعمل على أنظمة قديمة، لذلك من المهم أن تتمتع حلول تأمين البيانات الضخمة بالمرونة الكافية flexiblity لمواكبة التحديثات المتتابعة في مجال البيانات.

تغطية جميع البيئات

معظم التطبيقات المستخدمة أصبحت مُستضافة في السحابة based-cloud، كما أصبحت مصدرا مهما لتخزين البيانات، لذا يجب أن تكون حلول تأمين البيانات قادرة على تأمين الأنظمة الرقمية والبيانات بمختلف أنواعها: المستضافة سحابياً، والمستضافة في بيئة داخل المؤسسات الحكومية، وكذلك الهجين.

الترميز

وهو يعني عملية الاستعاضة عن عناصر حساسة في البيانات بعناصر أخرى tokenization ، وهي خاصية مهمة ستساعد – إن توفرت – على تأمين بيانات المؤسسة لسنوات طويلة مقبلة، واستبعاد المخاوف المتعلقة بالخصوصية.

- أمن الهواتف النقالة

الهواتف الذكية تحتوي على كمية كبيرة من المعلومات الحساسة التي يجب الحفاظ عليها وحمايتها. كما يجب معرفة أن جميع الهواتف الذكية، وأجهزة الحاسوب هي الأهداف المفضلة للهجمات. وهذه الهجمات غالباً ما تستغل نقاط الضعف المتعلقة بالهواتف الذكية التي يمكن أن تأتي من وسائل الاتصال مثل خدمة الرسائل القصيرة SMS، وخدمة الرسائل متعددة الوسائط MMS، وجي اس ام GSM وشبكات الواي فاي Fi-Wi

- المواطنة الرقمية

المواطنة الرقمية باختصار هي توجيه وحماية، توجيه نحو منافع التقنيات الحديثة، وحماية من أخطارها. أو باختصار أكبر هي التعامل الذكي مع التكنولوجيا. الأمن الرقمي
يمكن تعريف المواطنة الرقمية كذلك بأنها قواعد السلوك المعتمدة في استخدامات التكنولوجيا المتعددة، مثل استخدامها من أجل التبادل الإلكتروني للمعلومات، والمشاركة الإلكترونية الكاملة في المجتمع، وشراء وبيع البضائع عن طريق الإنترنت، وغير ذلك. وتعرف أيضا بأنها القدرة على المشاركة في المجتمع عبر شبكة الإنترنت، كما أن المواطن الرقمي هو المواطن الذي يستخدم الإنترنت بشكل منتظم وفعال.

- الأمن الرقمي

الطرق المختلفة والمتعددة التي تكون غايتها هي حماية حسابات الإنترنت المتعلقة في الحاسب الآلي وحماية الملفات من التسلل أو التدخل والتطفل من قبل مستخدمين خارجيين (غير مصرحين) تأتي أهميّة الامن الرقمي في حماية هذه البيانات المعرّضة للخطر:

• بيانات التعريف الشخصيّة: وهي تتضمّن الاسم والبريد الإلكتروني والعنوان، ورقم الضمان الاجتماعي الذي يعدّ الأكثر خطرًا. حيث يمكن استخدام رقم الضمان الاجتماعي من قبل المُخترق، لفتح حساب بطاقة ائتمان باسم الشخص.

• بيانات الدفع الشخصيّة: وهي تشمل أرقام بطاقات الائتمان، وأرقام الخدمات المصرفيّة، وأكواد PIN. والتي يمكن لمجرمي الانترنت استخدامها، لتحويل الأموال من حسابك المصرفي، أو لإجراء عمليات شراء.

• بيانات الصحة الشخصيّة: ويقصد بها المعلومات الصحيّة، والأدوية الموصوفة للشخص، والتأمين الصحي، والزيارات إلى الأطباء أو المشافي. وهي معلومات هامة جدًا، لمجرمي الانترنت الذين يستغلّون هذه المعلومات الصحيّة للمطالبة بالتأمين الصحي، أو طلب أدوية وإعادة بيعها.

- **ما الفرق بين الامن الرقمي والأمن السيبراني**

بشكلٍ عام، تخلق الحاجة إلى الامن الرقمي والأمن السيبراني عند حدوث الجرائم الالكترونية، كانتهاك بيانات شخص ما. مع ذلك هناك فرق بين الأمن القومي والأمن السيبراني. فالأمن القومي يضمن حماية تواجد الأشخاص على الانترنت، من خلال حماية بياناتهم وهويتهم وأصولهم، في حين يحمي الأمن السيبراني جميع الشبكات، وأنظمة كمبيوتر، والمعلومات من الاختراق. وبذلك يمكن اعتبار الأمن الرقمي جزءًا من الأمن السيبراني.

- **الاتصالات الرقمية**

هي الاتصالات التي تتعامل بمبدأ النظام الثنائي. يتصف هذا النوع من الاتصالات بقوتها وجودتها العالية مقارنة بالاتصالات التناظرية؛ من أمثلة الأجهزة التي تعتمد الاتصالات الرقمية: التلفاز الرقمي، اتصالات السوائل، والحواسيب.

مزايا الاتصالات الرقمية

- القدرة على استخدام «المعيدات التي تعيد توليد الإشارة» مما يجعل الإشارات الرقمية تعطي نتائج فائقة الجودة والدقة.
- سهولة تطبيق أنظمة الترميز للتحكم في الخطأ من خلال ومقارنة النتائج المتحصل عليها بالنتائج المستقبلة للتحقق من عدم وجود خطأ، وتستطيع هذه النظم أن تصحح الخطأ في ظروف معينة

- إمكانية تطبيق أنظمة التشفير، والتي لا يمكن
- فهم معناها إلا بإجراء العمليات الحسابية العكسية. ولا يتاح ذلك إلا لمن يمتلك المفتاح الشفري.
- إمكانية الضغط والتخزين حيث يمكن تخزين هذه الإشارات في صورة مدلولات رقمية في ذاكرة مثل ذاكرة الحاسوب، أو ضغطها لتشغل مكانًا أقل في الذاكرة، أو لتستغرق وقتًا أقل عند الإرسال.

الأسئلة

1. خادم الوكيل (Servers Proxy) هو الجيل الرابع من جدران الحماية			
صح	خطأ		
2. التشفير (cryptography) يعد من معايير تعزيز الأمن السيبراني			
صح	خطأ		
3. من أنواع الهجمات التي تتعرض لها الشبكة التصيد (Phishing) وهي عبارة عن ثغرات في البرامج لم يتم حلها الى الان.			
صح	خطأ		
4. تعرّف منظمة الصحة العالمية الصحة الإلكترونية بأنها الاستخدام الفعّال من حيث التكلفة والآمن لتكنولوجيات المعلومات والاتصالات في دعم المجالات المتصلة بالصحة.			
صح	خطأ		
5. تكامل البيانات : (Integrity) تشمل كافة التدابير اللازمة لمنع اطلاع الجهات غير المصرح لها على المعلومات الحساسة او السرية			
صح	خطأ		
6. يعتمد الفضاء السيبراني على بروتوكول TCP /IP			
صح	خطأ		
7. سكير وير: (Scarware) إنذار كاذب بوجود فيروس اختراقي لجهازك، أو تهديد بأن جهازك مراقب، والتي توجه المستخدمين لتحميل برنامج لحماية جهازك، والذي يكون هذا البرنامج هو التهديد بحد ذاته.			
صح	خطأ		
8. هي عملية اتخاذ تدابير وقائية مادية وبرمجية لحماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به أو سوء الاستخدام، أو الأعطال أو التعديل أو التدمير أو الكشف غير المناسب			
هندسة أمن الشبكات والمعلومات	أمن الملفات	أمن المجلدات	أمن المعلومات
9. من اهمية السرعة في الامن السيبراني استبعاد مؤشرات الاداء الرئيسية لـ DevOps I مثل ..... وهو المدة التي يمكن أن يعمل بها النظام المعيب حتى يتم إيقاف تشغيله			
MTTF (متوسط الوقت حتى الفشل	TF (متوسط الفشل	MTTR (متوسط وقت الاستجابة	MTTD (متوسط الوقت اللازم للكشف
10. هي وثيقة إلكترونية يصدرها مقدم خدمات تصديق، تستخدم لتأكيد هوية الشخص الحائز على منظومة التوقيع الإلكتروني			
شهادة التصديق الرقمي	الفضاء السيبراني	التهديدات	التوقيع الرقمي
11. هي مجموع القواعد والضوابط والمعايير والأعراف والأفكار والمبادئ المتبعة في الاستخدام الأمثل والقويم للتكنولوجيا التي يحتاجها المواطنون			
المواطنة الرقمية	الفضاء الإلكتروني	أمن المعلومات	الخوارزميات
12. اكثر الاسلاك التي تعاني من التجسس الالكتروني هي			
الأسلاك الأمنية	الأسلاك التعليمية	الأسلاك التجارية	الأسلاك الطبية
13. تعمل على منع حدوث أحداث أمنية معاكسة وتقوم المؤسسات الكبيرة بتشغيل أدوات متطورة للمساعدة في إدارة المخاطر الإلكترونية في الوقت الفعلي			
إدارة الاستباقية	المخاطر	بوت نت	التحليلات الإحصائية

للمخاطر			
14. محاكاة هجوم إلكتروني ضد نظام الكمبيوتر لديك للتحقق من نقاط الضعف القابلة للاستغلال			
الفايروسات	اختبار الاختراق	إدارة الاستباقية للمخاطر	الديدان
15. تستهدف الثغرات الموجودة في النظام، مثل أنظمة التشغيل غير المُحدثَّة والأنظمة القديمة التي لم يتم تحديثها			
هجمات استغلال الثغرات	اتخاذ القرارات	اختراق كلمات المرور	التحقق من الهوية
16. من أنواع الهجمات التي تتعرض لها الشبكة : عبارة عن ثغرات في البرامج لم يتم حلها الى الان			
(CryptoJacking) التعدين الخبيث	(Denial Of Service) حجب الخدمات	(Zero-Day) هجمات دون انتظار	(SQL) حقن
17. ترجمة عنوان الشبكة (Network Address Translation) من أنواع			
جدران الحماية	التوقيع الرقمي	شهادة التصديق الرقمي	الثغرات
18. حيّز رمزي أو افتراضي يوجد ضمن نطاق الإنترنت			
الفضاء السيبراني	الأنترنت	المهاجمين	الشبكة العنكبوتية
19. تركز الحوكمة على			
التخطيط الإستراتيجي	الإشراف على تنفيذ أعمال الأمن السيبراني	الهندسة الاجتماعية	أمن المعلومات
20. تشمل كافة التدابير اللازمة لضمان التأكد من استمرار القدرة على تقديم الخدمات والتفاعل مع المعلومات والوصول إليها			
سرية المعلومات – confidentiality	تكامل وسلامة المعلومات – Integrity	توفر المعلومات Availability –	الأمن – security
21. العديد من الجامعات السعودية تضمن مجالي الذكاء الاصطناعي والأمن السيبراني في خططها			
صح	خطأ		
22. 2023تعرضت شركة ارامكو السعودية على هجوم الكتروني في عام			
صح	خطأ		
23. من أنظمة كشف التسلل(IDS) نظام كشف التسلل عبر الشبكة (NIDS) ونظام كشف التسلل المعتمد على المضيف(HIDS)			
صح	خطأ		
24. المستوى الوطني لأمن المعلومات يركز على مجمل الأخطار الداخلية والخارجية التي تمس كيان الدولة			
صح	خطأ		
25. من أنواع الشهادة الرقمية الشهادة المخصصة بغرض الاختراق			
صح	خطأ		
26. الفرق بين الحوكمة والإدارة: أن الإدارة تركز على التخطيط الاستراتيجي			
صح	خطأ		
27. من البرامج والمبادرات الوطنية في سبيل الامن المعلوماتي : الأكاديمية الوطنية للأمن السيبراني			
صح	خطأ		
28. من أنواع الاختراقات الأمنية اختراق كلمات المرور الضعيفة أو تخمينها			

صح	خطأ		
29. الاتصال عن بعد ترتبط الأجهزة في نظم المعلومات ببعضها من خلال اتصال سلكي، مثل ، Wi-Fi والألياف البصرية			
التطبيقات	الشبكات	الأجهزة	المستخدمين
30. يقصد منها وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات او التحقق منها ، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة			
التوأمة الشريرة	حقن قواعد البيانات sql	حجب الخدمات	التصيد
31. تعني ممارسة الاعمال التجارية على شبكة الانترنت وتشمل عمليات بيع وشراء السلع او الخدمات عبر الانترنت			
التجارة الإلكترونية	الفضاء السيبراني	أمن المعلومات	أمن الشبكات
32. من مراحل اختطاف الجلسة			
مراقبة الشبكة	اتخاذ القرارات	الاصطياد	الهجوم
33. تضم المكونات المادية			
الأجهزة الطرفية	تحليل المواقع والبيانات	الأنظمة	البرمجيات
34. سرقة كلمة السر وهجمات حقن قواعد البيانات والتعرض للاختراق أثناء محاولة معالجة اختراق سابق يعتبر من تهديدات امن المعلومات لـ			
اختراق الشبكات	الهندسة الاجتماعية	البرمجيات الضارة	حصان طروادة
35. برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال			
التوأمة الشريرة (Evil Twin)	سرقة الهوية (Identity Theft)	حصان طروادة (Trojan Horse)	حقن Sql ( )
36. من أنماط التهديدات الأمنية وأبعاد أمن المعلومات			
الفيروسات والديدان	سرية المعلومات	التصفح المستمر	البريد الإلكتروني
37. كشف التسلل والمراقبة الإلكترونية يتم من خلال			
المراقبة بالفيديو	الحواجز الطبيعية	بناء الهمجمة	المهاجمين
38. تعتبر من أهم تهديدات أمن المعلومات فهي عبارة عن برامج مكتوبة بإحدى لغات البرمجة، الهدف منها هو إلحاق الضرر بالمعلومات الموجودة في الحاسوب			
الفيروسات	التجسس	هجوم التظليل	السيطرة الكاملة
39. الجيل الثالث من أجيال جدران الحماية			
مرشحات (Packet Filters) الحزم	فلتر محدد الحالة (Stateful Filters)	طبقة التطبيقات (Application Layer Firewall)	الحزم (Packet)
40. هي البيانات التي تتضمّن الاسم والبريد الإلكتروني والعنوان، ورقم الضمان الاجتماعي			
بيانات التعريف الشخصية	بيانات الدفع الشخصية	بيانات الصحة الشخصية	بيانات الرخصة الدولية

ملخص لمقرر الإنترنت وشبكات الحاسب

الفصل الأول
مقدمة الى عالم الشبكات

- ## مفهوم الإنترنت

هي شبكة كأي شبكة من شبكات الحاسوب، ولكنه شبكة كبيرة بعض الشيء يتصل بها أكثر من 21 مليار جهاز حول العالم وفقًا لإحصائية عام 2020

- ## أنظمة نقل البيانات في الشبكات

- نموذج الشبكة الطبقي OSI Model
- نموذج بروتوكولTCP/IP Model

- ## بروتوكولات الشبكات

- **IP**– هو من أهمّ البروتوكولات الأساسية لعمل الإنترنت، وهو عنوان منطقي فريد تُعنون به جميع الشبكات والأجهزة المتصلة بها
- **ICMP** – يستخدم هذا البروتوكول لإرسال رسائل بين الأجهزة للتأكد من توافرها على الشبكة أو عدم اتصالها
- **TCP** – يُحدد في طبقة النقل ضمن نموذج بروتوكول IP/TCP ويستطيع تأمين اتصالات موثوقة كما يعمل على تغليف البيانات ضمن رزم ونقلها عبر الطبقات الأدنى، ثمَّ التأكد من أنَّ البيانات قد استُلِمت دون أخطاء عبر انتظار تقريرٍ من المستلم
- **UDP** – يُحدَّد ضمن طبقة النقل ضمن نموذج بروتوكول IP/TCP و يؤمِّن اتصالات غير موثوقة فلا يعمل على التأكد من تسليم البيانات دون أخطاء إلى وجهتها لذا يتميز هذا البروتوكول بسرعة نقل كبيرة .
- **HTTP** – يعمل في طبقة التطبيقات وهو الأساس في عملية التواصل على الويب إذ يعمل على نقل وتبادل النصوص
- **FTP** – يُحدَّد ضمن طبقة النقل، ويعمل على نقل الملفات من مضيف إلى آخر عبر الشبكة، هذا البروتوكول غير آمن لذا يستخدم في عملية تنزيل الملفات العامة فقط.
- **DNS** – يُستخدم في طبقة التطبيقات ويعمل على تحويل أسماء المضيفين إلى عناوينIP فإذا أردت الاتصال بأحد المواقع فليس عليك تذكر عنوان IP له بل كتابة عنوان URL في متصفحك
- **SSH** – يُستخدم في طبقة التطبيقات، وهو بروتوكول مشفَّر وآمن يستطيع الاتصال بالخادم البعيد والتحكم به.

- **تعريف شبكات الحاسب**

شبكة الحاسب هي مجموعة من أجهزة الحاسب وأجهزة ملحقة (Peripherals) التي تتصل ببعضها والتي تسمح لمستخدميها أن يشتركوا في استخدام موارد الشبكة (Resources) والأجهزة المتصلة بالشبكة مثل الطابعة printer والمودم Modem ومحرك الأقراص المدمج CD-ROM Drive وغيرها.

- **مكونات شبكة الحاسب**

تتكون شبكة الحاسب من مكونات مادية (Hardware) وبرمجية.(Software)

- **خصائص الشبكات ونوع الاتصال**

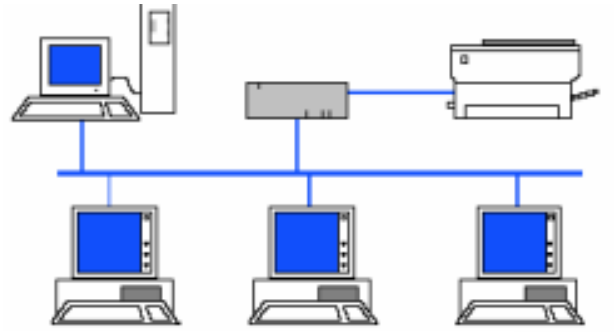
- إمكانية التخلص من شكل أسلاك الإنترنت غير المناسب.
- مشاركة الطابعة وأجهزة ملحقة أخرى بالحاسوب، حيث يتم توفير شبكة السلكية واحدة في البيت.
- ممارسة ألعاب الحاسوب فتمتاز الألعاب في أنها تمكنك من اللعب بها بواسطة شبكة الإنترنت، حيث يتنافس اللاعبون بالرغم من تواجدهم في مواقع مختلفة
- تمتاز بالمرونة والسهولة حيث تتوافر خدمات الشبكة، فيمكنك الاتصال بها عن طريق الحواسيب والأجهزة المتنقلة على شبكة الإنترنت من خلال أي موقع في المنزل دون الحاجة للبقاء متصلاً بالأسلاك.

- **طبوغرافيا الشبكات**

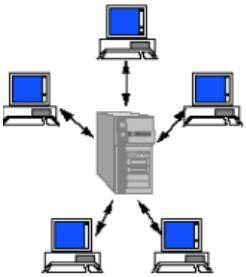
هي الطريقة المستخدمة لتوصيل كابلات الشبكة وربط الكمبيوتر بالكابلات، تحدد بحسب بروتوكول طبقة البيانات ونوع الكابل

شبكات النطاق المحلي قائمة على ثلاث تصاميم أساسية هي:

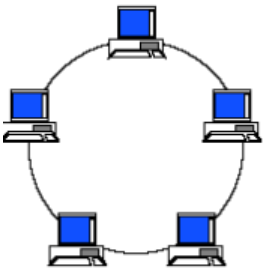
أولا: البنية الخطية يقوم تصميمها بتوصيل الأجهزة في صف على طول سلك واحد تمتاز ببساطة وسهولة توسعتها وقلة تكلفتها.



ثانيا: البنية النجمية تتميز بوجود جهاز مركزي يسمى hub توصل اليه جميع الأجهزة بواسطة كيابل خاصة.



ثالثا: البنية الحلقية يتم ربط الأجهزة في الشبكة بحلقة دائرة من السلك بدون نهايات.



- أنواع الشبكات حسب الدخول للموارد
- شبكة الند للند Peer -to- Peer
- شبكة عميل–خادم Client/Server
- أنواع الشبكات حسب التوزيع الجغرافي
- الشبكات المحلية Lan
- الشبكات الواسعة Wan
- الشبكات الإقليمية Man
-
- أنظمة تشغيل الشبكات وعملائها

نظام تشغيل الشبكة هو نظام تشغيل مصمم لغرض وحيد هو دعم محطات العمل ومشاركة قاعدة البيانات ومشاركة التطبيقات ومشاركة الملفات والطابعات بين أجهزة كمبيوتر متعددة في شبكة بعض أنظمة التشغيل المستقلة.

الفصل الثاني
الأجهزة المستخدمة في الشبكات

- **بطاقة الشبكة**
- تعتبر بطاقة الشبكة هي الواجهة التي تصل بين الحاسب وكبل الشبكة، وتسمى محول الشبكة Network Interface Card NIC.
- **وظائف بطاقة الشبكة**

تعتبر المسئولة عن القيام بمعظم بروتوكولات طبقة ربط البيانات والطبقة الفيزيائية، **ويتلخص دورها فيما يلي:**

١ – تغليف البيانات .

٢ – تحويل الإشارات والبتات .

٣– إرسال واستقبال البيانات.

٤ – التخزين المؤقت.

5– التحويل التوازي / التوالي.

٦ – التحكم بالوصول إلى الوسيط.

- **أنواع الكابلات ومواصفاتها**

- **الكيبل المحوري (Coaxial Cable)** – هو أحد أقدم أنواع كابلات الشبكة ومن أكثر استخداماتها الحديثة هي وصلات الإيثرنت Ethernet والتي تصل سرعة اتصالها لـ 10 ميغابايت.
- **الألياف الضوئية (Optical Fibers)** – هناك نوعان من الألياف الضوئية وهما:

1. الألياف الضوئية أحادية النمط (Single-Mode Fibers) تُستخدَم في الشبكات التي تغطي مناطق واسعة.
2. الألياف الضوئية متعددة النمط (Multimode Fibers) تُعد جيّدة في توفير النطاق الترددي (Bandwidth)للشبكات المحلية.

- **الزوج المجدول (Twisted Pair)** – استخدمت لأول مرة لنقل البيانات بمعدل 10 ميغابايت وتطورت لتتمكن من نقل البيانات بسرعة 100 ميغابايت في الثانية ويوجد نوعان المحمي (STP) والغير محمي(UTP)
- **الناقل التسلسلي العالمي (USB)** – يتم استخدامها في الغالب لربط الأجهزة الملحقة مثل الطابعة والفأرة ولوحة المفاتيح وكاميرا الويب بوحدة المعالجة المركزية

- **كابلات العبور (Crossover Cables)** – تستخدم بشكل أساسي لربط أجهزة الشبكة من نفس النوع.

الأجهزة المستخدمة في الشبكات وطريقة عملها

- **Repeater**– جهاز يستخدم لتقوية الإشارة لغرض زيادة عدد الأجهزة التي يمكن وصلها ببعض في الشبكة الواحدة.
- **Hub** - جهاز يستخدم لربط الأجهزة ببعضها يتم وصل كل جهاز كمبيوتر بأحد المنافذ (Port) في الـ Hub يتلقى هذا الجهاز الإشارة من أحد المنافذ وينقلها إلى جميع المنافذ الأخرى.
- **Bridge** - جهاز يعمل على ربط شبكتي LAN ببعضهما بحيث يعملان كشبكة واحدة ينشئ ايضا جدول توجيه يتضمن العناوين الفعلية للأجهزة يحدد هذا الجدول الوجهة الصحيحة للرسالة المارة فيها ويعمل على الحد من تدفق البيانات عبر الشبكة وازدحامها بالرسائل
- **switch** - جهاز يعمل على ربط أجهزة الشبكة بعضها ببعض وفكرة عمله مشابهة للـ bridge الاثنين يقعوا في نفس المستوى Datalink في الـ OSI Model يتميز هذا الجهاز بسرعة أدائه وأنه أكثر كفاءة من أجهزة الـ Hub.
- **Router** - يعتبر من أهم الأجهزة المستخدمة في ربط الشبكات يعمل هذا الجهاز في مستوى ال Network في OSI Model.
- **Access Point** - جهاز يعمل مثل الـ hub لتوصيل الأجهزة الاختلاف ال hub توصل الأجهزة فيه عن طريق سلك ولكن AP تعتمد في نقل البيانات على موجات الراديو RF أو الإشارات غير المرئية IR.
- **Gateway** - يعتبر هذا الجهاز من أذكى أجهزة ربط الشبكات ويعمل في كل مستويات OSI Model وهو يربط بين شبكتين مختلفتين كلياً حيث يعمل كمترجم أو وسيط بين الشبكتين.
- **modem** - هو كارت يستخدم في عملية modulator-demodulator وهي عملية تحويل البيانات من Analog to Digial أو العكس.

طرق توصيل الكابلات – يوجد نوعان من التوصيل وهما:

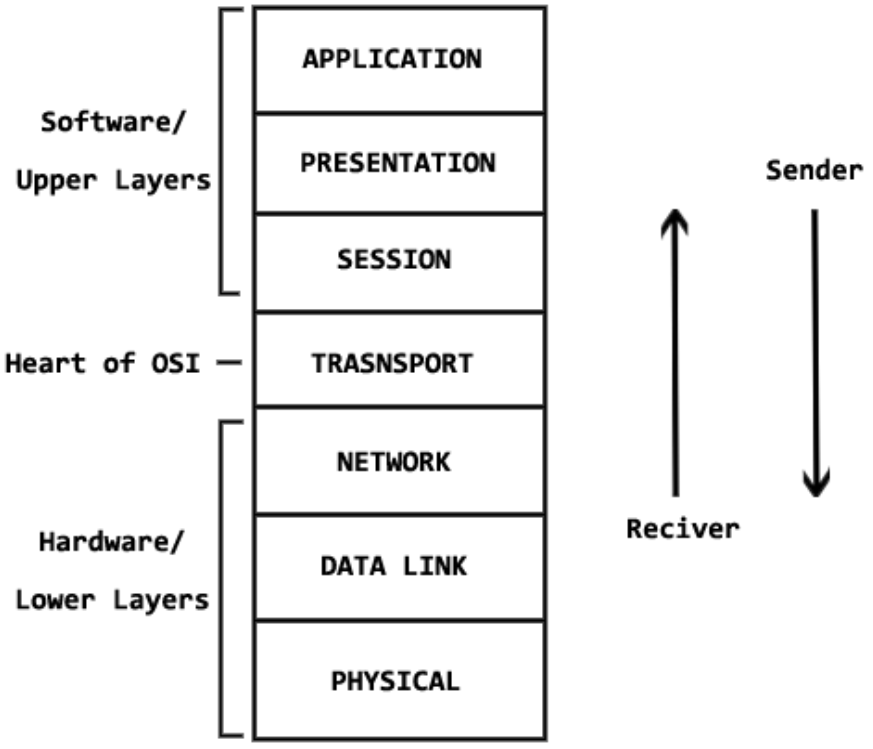
- **Straight** – لتوصيل جهازين مختلفين مثلاً(Pc + Switch)
- **Cross** – لتوصيل جهازين متشابهين ببعض مثل (Router + Router)

الفصل الثالث

نماذج البنية المعمارية للشبكات

- ### معمارية OSI او معمارية الطبقات السبع

ليس بروتوكول، ولكنه يعتبر نموذج مرجعي ويستخدم لتصميم وفهم بنية النظام .يتكون من سبع طبقات .ليس ملموس .يتبع نهج من الاسفل الى الاعلى.



- ### معمارية الإنترنت TCP/IP

بروتوكول قياسي حيث يتم استخدامه لكل شبكة بما في ذلك شبكه الإنترنت – يتكون من أربع طبقات – ملموس – يتبع نهج من الأعلى الى الأسفل.

طبقات OSI

الطبقة	وظائفها		
١) الطبقة الفيزيائية physical	الطبقه الفزيائيه هي المسؤلة عن نقل البيانات بصيغة بتات تحدد هذه الطبقة المواصفات الميكانيكية والكهربائية الخاصة بالكابل وكرت الشبكة، كما تحدد كيفيه الاتصال بين الكابل وكرت الشبكة		
٢) طبقة ربط البيانات data link	تحديد التكنولوجيا المستخدمة في الشبكة .	بروتوكولات طبقة ربط البيانات	وظائف البروتوكول
		Ethernet	إنشاء إطارات خاصة بالتكنولوجيا المستخدمة
		Token Ring	
		PPP	
٣) طبقة الشبكة network	١- مسئولة عن الاتصال بين الأجهزة الطرفية (الاتصال والتوجيه) . ٢- مسئولة عن عنونة الرسائل وترجمة العناوين المنطقية والأسماء إلى عناوين مادية تفهمها الشبكة .	بروتوكول الانترنت IP	العنونة وإرسال البيانات
		IPX	تبادل الرزم على الشبكات الجامعة
		ARP	حل العناوين
٤) طبقة النقل transport	تعتبر متممة لخدمات طبقة الشبكة وتعمل على التأكد من أن المعلومات قد وصلت خالية من الأخطاء وبالترتيب الصحيح	TCP	يوفر خدمات تعتمد على الاتصال بين الأجهزة وخدمات إضافية لا يوفرها UDP
		UDP	أداء نفس مهام TCP لكن بأكثر بساطة مما يؤدي إلى تبادل بيانات أسرع
٥) طبقة الجلسة sesion	هي المسئولة عن تنظيم الحوار وهو تبادل المعلومات بين نظامين على الشبكة باختيار الأسلوب الذي يستخدمه النظامان لتبادل الرسائل كأسلوب التناوب ثنائي الاتجاه وأسلوب التزامن ثنائي الاتجاه		
٦) طبقة التقديم presentation	هذه الطبقة تعمل على ضغط وفك وتشفير البيانات		
٧) طبقة التطبيق application	تتحكم بالاتصال بين تطبيقات الحاسب	بروتوكولات طبق التطبيق	وظائف البروتوكول
		بروتوكول نقل الملفات FTP	التحكم في نقل الملفات
		بروتوكول نقل البريد البسيط SMTP	التحكم في تبادل الرسائل بين الملقمات عبر الشبكة

طبقات TCP/IP

الطبقة	وظائفها	بروتوكولات الطبقة	وظيفة البروتوكول
١) طبقة الوصول إلى الشبكة	استخدام البروتوكولات اللازمة لإنشاء إطارات خاصة بالتكنولوجيا المستخدمة. تحويل البتات إلى إشارات لغرض نقلها على الوسيط المعني بالأمر. وتكافئ طبقة ربط البيانات والفيزيائية في OSI	Ethernet	إنشاء إطارات خاصة بالتكنولوجيا المستخدمة
		Token Ring	
٢) طبقة الاتصال بالانترنت	• مسئولة عن إمكانية الاتصال بين الأجهزة محلية كانت أو جامعة . • العنونة والتوجيه . • توفير المعلومات لطبقة الوصول للشبكة . • توجيه البيانات على الشبكة الجامعة . • تتيح للأجهزة إمكانية تبادل معلومات حول مشاكل وأعطال الشبكة . • التبليغ المتعدد بإرسال معلومات معينة إلى عدد من الأجهزة في نفس الوقت .	بروتوكول الانترنتIP	العنونة وإرسال البيانات
		بروتوكول حل العناوين ARP	تحويل عنوان IP إلى عنوانه العتادي الثابت
		RARP	تحويل أي عنوان عتادي إلى عنوان IP
		RIP	توجيه البيانات على الشبكة الجامعة .
		بروتوكول التحكم في رسائل الانترنت ICMP	يتيح تبادل معلومات حول مشاكل وأعطال الشبكة .
		بروتوكول ادارة المجموعات IGMP	التبليغ المتعدد بإرسال معلومات معينة إلى عدد من الأجهزة في نفس الوقت .
٣) طبقة النقل	تقديم الخدمات اللازمة لتوفير اتصال موثوق بين الأجهزة ، وتكافئ طبقتي النقل والجلسة في OSI	بروتوكول التحكم في النقل TCP	١ـ تجزئة وتجميع البيانات. ٢ـ الإشعار بالإستلام . ٣ـ تحديد المنافذ . ٤ـ الكشف عن الأخطاء . ٥ـ التحكم في الجريان . ٦ـ ترقيم زرم البيانات .
		بروتوكول المخطط البياني للمستخدم UDP وهو عديم الاتصال	أداء نفس مهام TCP لكن بأكثر بساطة مما يؤدي إلى تبادل بيانات أسرع لخلوه من وظائف الإشعار بالإستلام والتحكم بالجريان وكشف الأخطاء.
٤) طبقة التطبيقات والخدمات	تقديم خدمات تستخدمها البرامج للوصول إلى الشبكة .	بروتوكول نقل الملفات FTP	التحكم في نقل الملفات بين أنظمة TCP/IP
		بروتوكول نقل النصوص الفائقة HTTP	تبادل الملفات بين ملقمات وعملاء الويب .
		ملقم نظام أسماء النطاقات DNS	تحويل أسماء الأجهزة التي تستضيف مواقع على الانترنت إلى عناوين منطقية
		بروتوكول نقل البريد البسيط SMTP	إرسال الرسائل بين ملقمات البريد الإلكتروني .
		بروتوكول مكتب البريد POP3	يتيح للعميل الحصول على الرسائل من ملقم البريد .
		بروتوكول التكوين الديناميكي للمضيف DHCP	إعطاء عناوين IP للمضيفات بصفة ديناميكية أو متغيرة .
		بروتوكول الإدارة البسيطة للشبكات SNMP	جمع معلومات حول مختلف مكونات الشبكة .

الفصل الرابع

عنونة الشبكات

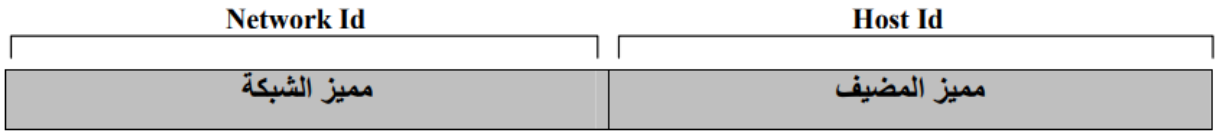
- ## تعريف عنوان IPv4

هو عنوان بطول ٣٢ بت يعطى لكمبيوترات TCP/IP والتجهيزات الأخرى على الشبكة حيث يميز تلك الأجهزة بشكل فريد. ينقسم عنوان IP إلى أربعة أجزاء بواسطة نقاط يحتوي كل جزء على ٨ بت، ويطلق على كل جزء اسم Octet

ويتم كتابته بأحد الأساليب التالية:

1. باستخدام النظام العشري ويكون كل قسم مفصول عن الأخر بنقطة مثل: 172.19.37.12
2. باستخدام النظام الثنائي مثل 00010000.00011110.00111000. 10101101

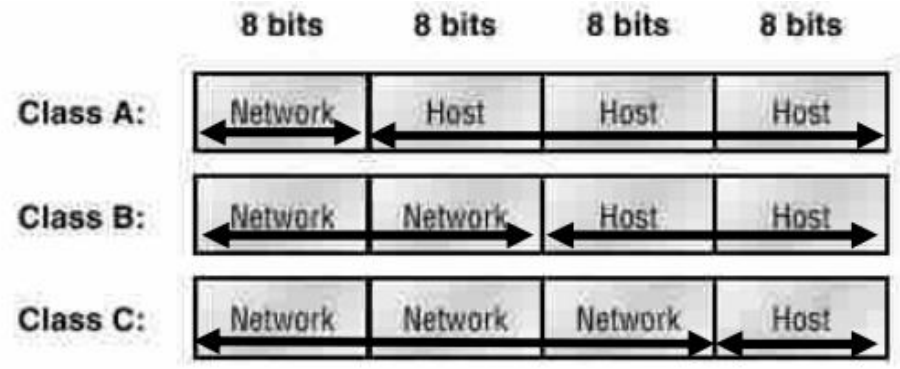
ويتألف أي عنوان IP من جزأين وهما مميز الشبكة Network Id ومميز المضيف Host Id



- ## فئات عناوين IP

قرر مصممو شبكة الإنترنت إنشاء عدة أنواع من الشبكات وفقاً لحجم الشبكة، حيث يوجد خمس فئات وهي: A,B,C,D,E الفئات الأساسية المستخدمة هي A,B,C أما الفئات D,E هي مخصصة للبلاغات المتعددة وأغراض تجريبية، ونفرق بين الفئات في قيمة الثمانية بتات الأولى.

نلاحظ في الصورة التالية كيفية تقسيم العناوين في كل من الأنواع السابقة:



يوضح الجدول التالي فئات العناوين وعدد الأجهزة في كل فئة:

فئات	أول بايت	مجموع عدد الشبكات	عدد الأجهزة في كل شبكة
A	من ١ إلى ١٢٦	١٢٦	١٦٧٧٧٢١٤
B	من ١٢٨ إلى ١٩١	١٦٣٨٢	٦٥٥٣٤
C	من ١٩٢ إلى ٢٢٣	٢٠٩٧١٥٠	٢٥٤

- ## أقنعة الشبكة الفرعية Subnetting

تعريف قناع الشبكة Subnetmask: هو بارامتر لتكوين TCP/IP يحدد أي البنات في العنوان IP يميز المضيف وأيها يميز الشبكة.

فيما يلي جدول بأقنعة الشبكة لكل فئة:

الفئة	عدد بتات الشبكة	عدد بتات الأجهزة	قناع الشبكة
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

- ## تقسيم الشبكات Subnetting

نظراً لظهور بعض العيوب في الشبكات الكبيرة التي تحوي عدد كبير من المضيفات، وتتمثل في صعوبة إدارة وصيانة الشبكة وبطء عملية الاتصال بين الأجهزة أصبح من الضروري إجراء عملية تفريع للشبكة لأنها تؤدي إلى تحسين أداء الشبكة والمتمثلة في ارتفاع سرعة إرسال واستقبال البيانات.

كيف يتم تفريع الشبكة؟ يتم ذلك من خلال التغيير أو التلاعب في قناع الشبكة ويعني ذلك استخدام قناع تفرع غير افتراضي، ولكن من غير المساس في الأجزاء من القناع التي تحمل القيمة 255، بل يتم التقسيم بتغيير الأجزاء التي تحمل القيمة صفر من القناع، وذلك بأخذ بعض البنات من جزء عنوان المضيف.

مثال: لو قمنا باستخدام 3 بت من بتات المضيف في شبكة من نوع CLASS C فسوف تكون قيمة قناع التفرع كما يلي:

11111111.	11111111.	11111111.	11100000
255.	255.	255.	224

والذي يمكن أن يعطينا ست شبكات فرعية تحتوي كل واحدة منها على 30 جهاز(مضيف).

- **الفرق بين IPv4 وIPv6**

- **بروتوكول الإنترنت الإصدار 4** (IPv4) هو الإصدار الحالي من بروتوكول الإنترنت، وهو نظام التعريف الذي يستخدمه الإنترنت لتبادل المعلومات بين الأجهزة.
- **بروتوكول الإنترنت الإصدار 6** (IPv6) هو الإصدار الجديد من بروتوكول الإنترنت. وهو يحتوي على مساحة عنوان بسعة 128 بت؛ أي أكبر بأربعة أضعاف من مساحة عنوان بروتوكول الإنترنت IPv4 بسعة 32 بت.

الفصل الخامس والسادس
الشبكات المحلية والواسعة

- **الشبكة المحلية – LAN – Local Area Network**

- هي اتصال مجموعة من الحاسبات بحاسوب رئيسي في أماكن متقاربة جغرافيا قد تكون غرفة او مبنى واحد او عدة مباني متقاربة، حيث يتم هذا الاتصال عن طريق وصالت سلكية مباشرة او ال سلكية.
- تستخدم هذه الشبكات في الشركات الصغيرة، المدارس، المنازل وغيرها.

- **مميزات الشبكة المحلية:**

- محدودة المكان فهي مخصصة لغرض محدد مثل معمل المدرسة أو الجامعة أو شركة .
- سرعة الإرسال لقصر المسافة بين الأجهزة .
- يستخدمها عدد محدد من المستخدمين .
- تدار هذه الشبكة في المدارس والجامعات أو الشركات والمؤسسات الخاصة.

- **الشبكة الواسعة – WAN – Wide Area Network**

- هي اتصال مجموعة متباعدة من الحاسبات او مجموعة من الشبكات المحلية بحاسوب رئيسي، قد تكون في نفس البلد او في بلد آخر او قارة اخرى، وعادة ما يكون الحاسوب الرئيسي من النوع الكبير Mainframeاو المتوسط .Minicomputer
- تستخدم هذه الشبكات في الجهات الحكومية والمؤسسات والشركات الكبيرة التي لديها فروع متباعدة.

- **مميزات الشبكة الواسعة:**

- تمتد بين المدن .
- محدودة سرعة الإرسال لطول المسافات بين الوحدات المختلفة .
- يستخدمها عدد كبير من المستخدمين
- تدار هذه الشبكة من هيئة عامة أو جهة حكومية.

الفصل السابع
التبديل والتوجيه

▪ المبدلات Switches

المبدل هو جهاز يربط الأجهزة مع بعضها في بنية نجمية، ويجمع بين المجمع والجسر حيث يشبه المجمع في الشكل وعدد المنافذ ويشبه الجسر في الوظيفة، فهو عبارة عن جسر متعدد المنافذ، ويعمل على طبقة ربط البيانات.

عيوب المبدلات: أنها تنقل كل رسائل التبليغ إلى كل الأجهزة على الشبكة.

الفرق بين المجمع (HUP) والمبدل Switch

الجهاز	التصادم والإزدحام	توجيه الرزم	عرض النطاق
المبدل (Switch)	تكون الشبكة فيه خالية من التصادم والازدحام	يوجه الرزم فقط إلى المنفذ الموصل بجهاز الوجهة	يخصص كامل النطاق الترددي لكل زوج من الأجهزة المتصلة مع بعضها
المجمع (HUP)	ينشئ نطاق تصادم تتشارك فيه كل الأجهزة على الشبكة	يوجه كل الرزم الواردة إلى كل المنافذ	يخصص لكل جهاز جزء من سرعة بطاقة الشبكة مما يقلل السرعة والكفاءة

▪ الموجهات Routers

الموجهة هو جهاز يستخدم لربط شبكتين محليتين مختلفتين أو في الشبكات الكبيرة لربط ٢٠ شبكة أو أكثر، ويعمل على طبقة الشبكة.

طريقة عمل الموجهات:

يستقبل الموجه البيانات عبر أحد بطاقاته حتى تصل إلى طبقة الشبكة، ويتم إزالة إطار طبقة ربط البيانات، وبعدها يمررها الموجه للأسفل عبر بطاقة شبكة ثانية حيث تقوم بتعليقها بإطار جديد ثم إرسالها على الشبكة المحلية.

- **مزايا الموجهات** أنها تعزل نطاق التصادم والبث بحيث لا توجه رسائل التبليغ من قبل جهاز ما إلى شبكة أخرى إنما تتركها على نفس الشبكة الموجود بها الجهاز المولد للبلاغ

الفصل الثامن

بناء شبكة صغيرة

تحديد احتياجات الشبكة

1. احسب عدد أجهزة الكمبيوتر التي ترغب بتوصيلها (ستحتاج إلى جهاز راوتر فقط إن كنت ستوصل أربعة أجهزة الكمبيوتر أو أقل وستحتاج على الأرجح إلى محول شبكة لزيادة عدد المنافذ المتاحة إن كنت ستوصل أكثر من أربعة أجهزة).
2. حدد ما إن كنت ترغب بإنشاء شبكة لاسلكية ستحتاج إلى جهاز راوتر لاسلكي (في الاتصال لاسلكياً لا يمكن استخدام محولات الشبكة لتوصيل الأجهزة اللاسلكية ويقتصر استخدامها على توسيع عدد المنافذ المتاحة في جهاز الراوتر في حالة الشبكات السلكية).
3. حدد ما إن كنت ترغب بامتلاك أجهزة الشبكة للوصول إلى الإنترنت إن كنت ترغب بوصول كل أجهزة الشبكة المتصلة إلى الإنترنت. ستحتاج إلى جهاز راوتر قادر على التعامل مع الاتصالات، بينما لن تحتاج إلا لمحول شبكة فقط إن لم تكن بحاجة لوصول الأجهزة إلى الإنترنت.
4. قس المسافة بين كل أجهزة الشبكة المتصلة (فكر في احتياجاتك المستقبلية إن كنت قد استهلكت كل المنافذ في عتادك، فكر في تجهيز منافذ أخرى للسماح لمزيد الأجهزة بالاتصال مستقبلاً).

اعداد شبكة محلية بسيطة

1. اجمع عتاد الشبكة ستحتاج إلى جهاز راوتر أو محول شبكة لإنشاء الشبكة المحلية.
2. يقوم جهاز الراوتر بالتعامل مع تعيين عناوين IP لكل جهاز من أجهزة الشبكة واستخدامه ضروري إن كنت تنوي مشاركة اتصال الإنترنت بين الأجهزة المتصلة.
3. محول الشبكة عبارة عن نسخة مبسطة من جهاز الراوتر حيث يسمح محول الشبكة للأجهزة بالتواصل مع بعضها، ولكنه لا يعين عناوين IP فريدة ولا يسمح بمشاركة اتصال الإنترنت، هدفها (توسيع عدد المنافذ المتاحة على شبكتك).
4. اضبط جهاز الراوتر لن تحتاج إلى فعل الكثير حتى تضبط جهاز الراوتر لإنشاء شبكة محلية بسيطة فكل ما عليك فعله هو توصيل جهاز الراوتر في مصدر طاقة، ويفضل أن يكون قريباً من جهاز المودم إن كنت تخطط لمشاركة اتصال الإنترنت من خلال.
5. وصل المودم بجهاز الراوتر.

6. إن كنت تستخدم محول شبكة لتوسيع عدد المنافذ المتاحة في جهاز الراوتر وصل كابل الشبكة بجهاز الراوتر ووصل الطرف الآخر في أي منفذ بمحول الشبكة
7. وصل أجهزة الكمبيوتر في منافذ شبكة متاحة استخدم كابلات شبكة لتوصيل كل جهاز كمبيوتر بمنفذ شبكة مفتوح في جهاز الراوتر أو محول الشبكة، ولا يهم ترتيب توصيل المنافذ.
8. لا يمكن الاعتماد على كابلات الشبكة لنقل البيانات لمسافة أكثر من ١٠٠ متر.

- **اوامر مهمه لفحص الشبكة**
- **امر tracert**

وظيفته الرئيسية في تتبع المسارات يعمل لاستكشاف المسار من عنوان المصدر إلى عنوان الوجهة

- **امرping**

يعمل على فحص إمكانية الوصول إلى عنوان IP، مضيف أو خادم. ويكثُر استخدام الأمر للتدقيق في أخطاء الشبكة وتحديد مشاكلها

الأسئلة

1. من عناصر الشبكة وهو جهاز الحاسب الذي يزود المصادر المشتركة Resources إلى مستخدمي الشبكة ويتميز بخصائص السرعة الفائقة والسعة التخزينية العالية جدا.			
الخادم – Server	العميل – Client	الوسط – Medium	البيانات المتقاسمة – data Shared
2. من فوائد الشبكات نقل البيانات والمعلومات والبريد الالكتروني من مقدمي الخدمات وتوزيعها على المستفيدين في أماكن مختلفة وبعيدة.			
صح	خطا		
3. من عيوب الشبكة .....أن أي خطأ في التوصيل أو الانهاء أو حصول انقطاع في الكبل سيؤثر على عمل كامل الشبكة، الاشارات التي لا تستطيع تجاوز نقطة معينة تفشل في الوصول إلى كافة الاجهزة التي تلي تلك النقطة.			
الشبكة النجمية	الشبكة الخطية	الشبكة الحلقية	شبكة الند للند
4. شبكة تحتاج لجهاز إضافي وهو المجمع المركزي (Hub)أو (Switch) فإذا حصل وفشل هذا المجمع المركزي ستنهار كامل الشبكة، ولو أن حدوث ذلك نادرًا نسبيًا.			
الشبكة النجمية	الشبكة الخطية	الشبكة الحلقية	شبكة الند للند
5. المقصود بـ طبوغرافية الشبكة الطريقة المستخدمة لتوصيل كابلات الشبكة وربط الكمبيوتر بالكابلات، تحدد بحسب بروتوكول طبقة البيانات ونوع الكابل.			
صح	خطا		
6. بروتوكول..... يُستخدم في برامج فحص وتشخيص الشبكة مثل الامر" ping" والامر." traceroute"			
ICMP	HTTP	TCP	UDP
7. وهو أحد أقدم أنواع كابلات الشبكة التي استُخدِمت لربط جهاز التلفاز بالهوائي، من أكثر استخداماتها الحديثة هي وصلات الايثرنت Ethernet			
الكبل المحوري Cable Coaxial	الالياف الضوئية Fibers Optical	الزوج المجدول Pair Twisted	كابالت العبور (Cables Crossover)
8. هناك نوعان من الالياف الضوئية وهما أحادية النمط (Fibers Mode-Single) ومتعددة النمط (Fibers Multimode) تُستخدَم الالياف متعددة النمط في الشبكات التي تغطي مناطق واسعة.			
صح	خطا		
9. أعلى طبقات نموذج IP/TCP ،تحتوي على تطبيقات الشبكة التي تسمح بالاتصال بواسطة الطبقات السفلى، تتواصل برامج هذه الطبقة عن طريق برتوكولات طبقة النقل TCP وUDP			
طبقة التطبيقات	طبقة النقل	طبقة الشبكة	طبقة الوصول لشبكة

10. في هيكل النموذج المرجعي OSI ماهي الطبقة المسئولة عن تشكيل البيانات بالهيئة المناسبة للطبقة المجاورة العليا أو السفلى حسب الحالة ، كما أنها مسئولة عن الترجمة بين البروتوكولات المختلفة

Presentation Layer	Session Layer	Application Layer	Transport layer

11. تقوم هذه الطبقة بأخذ عينة من آخر جزء من البيانات تم إرساله عند توقف الشبكة عن العمل وذلك لكي يتم إرسال البيانات عندما تعود الشبكة الى العمل من النقطة التي توقف عندها الارسال

Presentation Layer	Session Layer	Application Layer	Transport layer

12. هيكل النموذج المرجعي OSI هي الطريقة التي بها تستطيع ان تفهم كيفية نقل البيانات عبر الشبكات

صح	خطا		

13. بروتوكول IP / TCP هو نموذج يتكون من سبع طبقات ،اماOSI فهو يحتوي على اربع طبقات.

صح	خطا		

14. هي الطبقة التي تفصل بين الطبقات الموجهة للمستخدم Oriented-User والطبقات الموجهة للشبكة Network-Oriented

Presentation Layer	Session Layer	Application Layer	Transport layer

15. بروتوكول .....هو بروتوكول قياسي حيث يتم استخدامه لكل شبكة بما في ذلك شبكه الانترنت.

TCP/IP	IOS	TCP/UDP	OSI

16. العنوان 155.34.54.66 يعتبر عنوان من الفئة أو الصف.....

A	B	C	E

17. هو بروتوكول قياسي حيث يتم استخدامه لكل شبكة بما في ذلك شبكه الانترنت

IP / TCP	IOS	TCP/UDP	OSI

18. حددي الـ Host ID من ال IPالتالي 192.168.10.34

192	168	10	34

19. هي مجموعه من اجهزة الكمبيوتر والاجهزة التي ترتبط في منطقة محدودة مثل المدارس والمعامل والمنازل

LAN	MAN	WAN	SAN

20. إذا قام جهاز المستخدم بإرسال بيانات للسويتش في نفس الوقت الذي يقوم فيها السويتش بإرسال البيانات للجهاز تقع في مجال تصادم

Broadcast Domain واحد	Broadcast Domain منفصل	Collision Domain واحد	Collision Domain منفصل

21. تشير إلى مجموعة الشبكات الضخمة الممتدة على مساحات واسعة.....

LAN	MAN	WAN	SAN

22. ما هو تعريف تبديل الشبكة (LAN Switching) وما الدور الرئيسي الذي يقوم به في الشبكات المحلية؟

تبديل الشبكة هو عملية توجيه حزم البيانات في الشبكة المحلية باستخدام البروتوكولات	تبديل الشبكة هو عملية نقل الحزم بين مختلف الشبكات	تبديل الشبكة هو عملية نقل البيانات داخل الشبكة المحلية بين الأجهزة باستخدام تبديل	تبديل الشبكة هو عملية توجيه حزم البيانات بين الشبكات الواسعة

23. ما هو دور الموجّه (Router) في شبكة الإنترنت؟

تخزين البيانات على الخوادم	تحقيق الاتصالات اللاسلكية	توجيه حركة البيانات بين الأجهزة والشبكات	إجراء عمليات تشفير للبيانات

24. هو عبارة عن بروتوكول أو طبقة تشفير آمنة يتم استخدامها لجعل البيانات آمنة عند نقلها عبر الإنترنت ويستخدم بشكل خاص على مواقع التسوق للحفاظ على أمان البيانات المالية

SSL	SMTP	HTTP	Hyperlink

25. هي شبكة اتصال لاسلكي تستخدم لإرسال واستقبال البيانات لا سلكيا بين الأجهزة المحمولة

شبكات محلية	شبكات الأجهزة الخلوية	شبكات واسعة او عالمية	شبكات المناطق الشخصية

26. يبلغ حجم عناوين شبكةIPv6

32	64	128	24

27. هو عباره عن خادم شبكة يوفر ويعين تلقائياً عنوانIP

DHCP	SMTP	FTP	Hub

28. هي الطبقة المواجهة لوسط الإرسال والمسؤولة عن إرسال البيانات التي تم تجهيزها من قبل الطبقات العليا عبر وسط الإرسال

طبقة الشبكة	طبقة النقل	الطبقة المادية	طبقة التطبيقات

29. ما هي الطبقة المسؤولة عن تحويل الـ Logical Names أي أسماء الأجهزة مثلا إلى Physical Addresses؟			
طبقة الشبكة (Network Layer)	طبقة العرض (Presentation Layer)	طبقة التطبيقات (Application Layer)	طبقة النقل (Transport Layer)
30. طرق توصيل الكابلات وهو لتوصيل جهازين متشابهين ببعض مثل (Router + Router) او غيرها وكذلك للدخول Consoleعلى اي Devices			
Cross	Twisted	Straight	Ethernet
31. ما هو الامر المستخدم لتكوين كلمة مرور مشفرة			
enable password	enable secret	pasword secret	secret password
32. ماهي وظيفة الامر التالي: copy running-config startup-config			
لحفظ اعدادات الموجه او المبدل	السماح بالتنقل بين اوضاع الموجه او المبدل	لنقل اعدادات الموجه الى المبدل	نسخ الاوامر على الموجه او المبدل
33. ماهي وظيفة بطاقة الشبكة			
مشاركة الطابعة وأجهزة ملحقه أخرى من الحاسوب	ارسال البيانات على الشبكة	تقوية الجهاز	بناء تطبيقات جديدة
34. المنافذ والكابلات مهمه وقد تسبب اخطاء في الشبكة لاختبار المنافذ والكابلات نستخدم			
VRF	Ping	ipconfig	show
35. ما هو العنصر الأساسي الذي يحتاج إلى اهتمام خاص عند بناء شبكة محلية صغيرة؟			
حجم التخزين الخارجي	سرعة الاتصال بالإنترنت	أمان الشبكة	عدد الكابلات

ملخص لمقرر مقدمة في أمن الشبكات

- **تعريف امن الشبكات :**

هو منظومة متكاملة تتضمن كل من البروتوكولات والتقنيات والأجهزة والأدوات والتكتيكات لحماية البيانات وتقليل الخطر.

- **مصطلحات امن الشبكات :**

1) نقاط الضعف (VULNERABILITY) : تعرف بانها ضعف او خلل فالشبكة ويقوم المهاجم باستغلال هذا الضعف ويشمل: نقاط الضعف على بروتوكولات الشبكة الضعيفة والغير امنة وأخطاء في التكوين والسياسات الأمنية ضعيفة.

2) التهديدات (THREAT): هو احتمال تحول نقاط الضعف الى هجوم على الشبكة

3) الخطر (RISK): هو احتمال وجود تهديد لاستغال نقاط الضعف في الأصول ويتم قياس الخطر باستخدام احتمال وقوع الحدث والأثار المترتبة عليه.

4) نواقل هجمات الشبكات: هي الطريق للدخول الى السيرفر او جهاز او الشبكة، ويمكن تصنيف النواقل إلى نوعين :تهديدات خارج الشبكة مثل : الانترنت وتهديدات داخل الشبكة مثل :

سرقة ونسخ البيانات السرية الى الوسائط القابلة للنقل او البريد.

التحايل على الخوادم الداخلية او أجهزة البنية التحتية.

التسبب في انقطاع الشبكة .

توصيل الوسائط القابلة للنقل الى أجهزة الشركة.

- تعتبر التهديدات الداخلية أخطر وتسبب ضرر أكبر من الخارجية

5) فقدان البيانات(DATA LOSS): هو عندما تفقد الشركة البيانات بقصد او دون قصد بهدف سرقتها او تسريبها.

6) فقدان البيانات(DATA LOSS):هو أي عملية أو حدث ينتج عنه تلف البيانات، أو حذفها، أو تسريبها، أو جعلها غير قابلة للقراءة من قبل مستخدم أو برنامج.

- **أسباب فقدان البيانات:**

1. أجهزة غير مشفرة: إذا لم يتم تخزين البيانات باستخدام خوارزمية تشفير، فيمكن للص استخراج البيانات السرية.
2. أجهزة التخزين السحابية : حفظ البيانات على السحابة لديه العديد من الفوائد المحتملة ومع ذلك، يمكن أن تضيع البيانات الحساسة إذا تم التحايل في الوصول إلى السحابة بسبب إعدادات الأمان الضعيفة.

3. البريد الإلكتروني /الشبكات الاجتماعية : أشهر وسائل فقد البيانات هي برامج المراسلة الفورية ومواقع وسائل التواصل الاجتماعي، على سبيل المثال: يمكن اعتراض البريد الإلكتروني أو رسائل المحادثات مما يمكن من الاستيلاء عليها وكشف معلومات سرية.
4. التحكم في الوصول الخاطئ: كلمات السر هي خط الدفاع الأول، كلمات السر المسروقة أو كلمات السر الضعيفة التي تعرضت لما يثير الشبهة يمكن أن توفر للمهاجم سهولة الوصول إلى بيانات الشركات
5. النسخ الورقية: يجب التخلص من بيانات الشركة الورقية اذا لم تعد لها حاجه لأنه يمكن للسارق استرداد تقارير مهملة والاستيلاء على معلومات ثمينة
6. الوسائط القابلة للنقل: خطر واحد هو أن الموظف يمكنه أن يؤدي إلى نقل غير مصرح به للبيانات إلى محرك أقراص USB وهناك خطر آخر هو أن محرك USB قد يحتوي على بيانات قيمة للشركة تكون معرضة للضياع.

أنواع الشبكات:

1. شبكة المكاتب الصغيرة (SOHO)SMALL OFFICE HOME OFFICE): هذا النوع من الشبكات يواجه خطر المهاجمين بهدف استخدام الاتصال بالإنترنت أو رؤية المعاملات البنكية، اما تكون متصلة عن طريق الموجهات اللاسلكية وتوفر هذه الموجهات ميزات الأمان الأساسية.
2. الشبكة الواسعة (WAN)WIDE AREA NETWORK): تغطي مساحة جغرافية واسعة وغالبا يكون الاتصال عن طريق الإنترنت
3. شبكة مراكز البيانات: شبكة مراكز البيانات قد تكون خارج الموقع وتستخدم لتخزين البيانات الحساسة والمملوكة ويتم توصيلها عبر VPNويتم ربطة بالمحولات switches

- تقوم مراكز البيانات بتخزين بيانات حساسة ولذلك فان الأمان امر بالغ الأهمية، ولذلك يتم حمايتها

4. الشبكة السحابية والافتراضية : الحوسبة السحابية والافتراضية تستخدم في نفس المجال علما بانها مختلفة عن بعض ،فالحوسبة الافتراضية اوجدت الحوسبة السحابية الافتراضية فالحوسبة الافتراضية هي من سمحت \ سهلت للحوسبة السحابية هذا الانتشار الكبير الحوسبة السحابية تفصل التطبيقات عن الأجهزة ،المحاكاة الافتراضية تفصل نظام التشغيل عن الأجهزة.

- طرق حمايه وتامين الشبكة

1. VPN: جهاز ISP Cisco ISPيقوم بحماية البيانات من داخل الحرم الجامعي الى العالم الخارجي عن طريق انشاء شبكات خاصة افتراضية ،ويضمن سالمة وسرية البيانات.

2. ASA Firewall: الجدار الناري او جدار الحماية من نوع filtering packet Stateful ويقوم تصفية حزم البيانات العائدة من الخارج الى داخل الحرم.
3. IPS: جهاز Cisco ذو نظام منع الاختراق ويقوم برصد حركة المرور الواردة والصادرة من اجل الكشف عن أي نشاط ضار ويحاول منعة والابلاغ عنه
4. ESA/WSA: الأداة الأمنية للبريد الإلكتروني والأداة الأمنية للويب توفر حماية من التهديدات وتطبيق الرؤية والتحكم وانشاء التقارير والحماية المتنقلة.

- **تهديدات الشبكة :**

1. الهاكر THE HACKER: هو مصطلح عام يستخدم لوصف مهاجم الشبكة ينقسم الهاكر الى ثلاث اقسام :

a. White Hat Hacker القبعة البيضاء: هؤلاء قراصنة أخلاقيون يستخدمون مهاراتهم في البرمجة لأغراض طيبة وأخلاقية وقانونية، يقومون بإجراء اختبارات ومحاولة اختراق الشبكات وأنظمتها باستخدام معرفتهم في أنظمة أمن الحاسوب لاكتشاف نقاط ضعف الشبكة والثغرات الأمنية
b. GREY HAT HACKER القبعة الرمادية: الافراد الذين يرتكبون جرائم ويفعلون أشياء غير أخلاقية ولكن ليس لتحقيق مكاسب شخصية ولا من أجل إلحاق الضرر
c. BLACK HAT HACKER القبعة السوداء: هؤلاء المجرمون الغير أخلاقيون الذين ينتهكون أمن أجهزة وشبكات الحاسب لتحقيق مكاسب شخصية، أو لأسباب خبيثة مثل مهاجمة الشبكات، الهاكر ذوي القبعات السوداء يستغلون نقاط الضعف في اختراق أنظمة الحاسب والشبكات.

2. البرامج الضارة :.

a. الفايروس : هو كود خبيث يهاجم لينفذ ملف غالبا يكون لبرنامج نظامي، اغلب الفيروسات تكون في حالة سبات حتى يقوم المستخدم بتشغيلها/ تنفيذها او يكون مدمج بها وقت عملها.

- اغلب الفيروسات أصبحت تنتشر عن طريق USB و CDومشاركة الشبكة والبريد الإلكتروني، فيروسات البريد الإلكتروني هي الأكثر رواج في هذا العصر

b. حصان طروادةTROJANHORSES : هو برمجيات خبيثة تحمل بداخل ملف تشغيل اخر يظهر بشكل الوظيفة المطلوبة مفهوم حصان طروادة مرن، من الممكن ان يسبب اضرار فورية، يعطي تحكم عن بعد للنظام، او الدخول من خلال الباب الخلفي وبإمكانه أيضا ان يرصد الحركات كالأوامر مثال «قم بإرسال كلمات المرور مره في الأسبوع

3. الهجوم على الشبكات: يتم تصنيف الهجوم على الشبكات الى ثلاث وهم:

a. هجوم الاستطلاع: هو محاولة معرفة المزيد عن النظام المستهدف كـ معلومات النظام، الخدمات أو الثغرات.
b. هجوم الوصول: هو السعي لكشف اسم المستخدم وكلمة المرور للوصول لموارد الكمبيوتر او الشبكة.
c. هجوم حجب الخدمة: هو نوع من الهجوم تنشأ عنه كمية كبيرة من الطلبات بشكل غير عادي الى خوادم الشبكة، مثل البريد الإلكتروني أو خادم الويب، يكمن الهدف من الهجوم خفض سرعة التطبيقات والعمليات أو تعطيلها على جهاز الشبكة .

الفصل الرابع
تطبيق تقنيات جدار الحماية

- قوائم التحكم بالوصول ACL: هي تقنية تقوم بالتحكم في عملية الاتصال بين الشبكات وتقوم بتحديد الأجهزة أو الشبكات المصرح لها بالدخول والشبكات الغير مصرح لها بالدخول وذلك يتم من خلال تسجيل عناوين الأجهزة في قائمة المنع أو قائمة الوصول.
- أنواع قوائم التحكم بالوصول:

1. قوائم التحكم في الوصول القياسيةSTANDARD : يتم استخدامه في حالة الرغبة بمنع الشبكة كلها من الوصول إلى شبكة أخرى منعا كاملا دون تحديد يعتمد هذا النوع في عملية السماح والمنع على عنوان المرسل المصدر (IP ADDRESSS)

   مثل منع وصول أجهزة الشبكة إلى الشبكة نفسها ومنع خروج الحزم من الراوتر إلى الشبكة.

2. قوائم التحكم في الوصول الموسعةEXTENDED : هذا النوع يتم استخدامه في حال الرغبة بمنع الوصول لخدمة معينة مثل الـ WEB SERVER أو ما شابه، في هذا النوع يتم منع البروتوكول المستخدم ورقم المنفذ التي تعمل عليها الخدمة مثل بروتوكول HTTP أو بروتوكولTELNET

- يتم تحديد القائمة برقم:
- 1-99: قوائم التحكم في الوصول القياسيةSTANDARD
- 100-199: قوائم التحكم في الوصول الموسعةEXTENDED
- امر السماح (PERMIT) أو منع(DENY) الوصول لعنوان محدد.
- منافذ بروتوكولTCPوUDP:
- المنافذ: عبارة عن ممرات تسمح بتبادل المعلومات والبيانات بين شبكة الأنترنت وجهاز الكمبيوتر حيث ان الشخص الذي يريد ان يتصل بخدمة شبكة الأنترنت لابد وان يستخدم ممر او منفذ للعبور الى هذا العالم الواسع حتى يتم الاتصال والتواصل، ويبلغ عدد المنافذ في الجهاز 65535منفذ، وكل من هذه المنافذ له وظيفة او خدمة محددة وتستخدم برامج محددة منافذ محددة وعلى سبيل المثال من المعروف ان المنفذ 80غالبًا ما يكون مخصصا لتصفح الإنترنت.
-
  - بروتكول TCP,UDP

المهام	TCP	UDP
موثوقية البيانات	موثوق	غير موثوق
العبء على الشبكة	يشكل عبء على الشبكة	أقل عبء بكثير مقارنة مع بروتوكول TCP
الخطأ في نقل البيانات	لا تقبل اي نسبة خطأ خلال نقل البيانات	تقبل نسبة معينة من الأخطاء
البيانات المفقودة	يقوم بإعادة ارسال البيانات المفقودة	لا يقوم بإعادة ارسال البيانات المفقودة
سرعة نقل المعلومات	أقل سرعة في التوصيل	سرعة عالية في التوصيل
جودة البيانات	جودة عالية في نقل البيانات	أقل جودة في نقل البيانات

- **منافذ بروتوكول TCP وUDP:**

اسم الخدمة	البروتوكول	المنفذ
FTP	TCP	20, 21
SSH	TCP	22
Telnet	TCP	23
SMTB	TCP	25
DNS	TCP, UDP	53
DHCP	UDP	67
HTTP	TCP	80
HTTPS	TCP	443

- جدار الحماية Firewall: هو جهاز أو برنامج يقوم بمراقبة حركة مرور الشبكة الواردة والصادرة ويقرر ما إذا كان سيتم المساح بحركة مرور معينة أو حضرها.
- يكون هذا برنامًجا أو مزيًجا من النظام والعتاد (جهاز)، ويعمل عن طريق الحظر الانتقائي لحزم البيانات أو السماح بها.
- الهدف الأساسي منه في معظم الحالات هو المساعدة في منع النشاط الضار ومنع أي شخص داخل شبكة خاصة أو خارجها من المشاركة في أنشطة غير مصرح بها على الإنترنت
- **أنواع جدار الحماية:**

1. جدار تصفية الحزم PACKET FILTERING FIREWALL: من أقدم أنواع جدران الحماية، ومن أفضل الأنواع التي يمكن أن تعتمد عليها لسرعتها وجودتها في فحص الاتصالات.

2. جدار النار المعتمد على الحالة STATEFUL FIREWALL: يعرف باسم جدار الحماية التفتيشي، وهو نوع من أنواع جدار الحماية التقليدي أيضا حيث يقوم بمراقبة حركة المرور الصادرة والواردة ويقوم بتصفيتها بشكل تلقائي بناءً على القواعد الأمنية المُعدة بشكل مسبق من المستخدم ولكن يتميز بمراقبة الاتصال من اللحظة الأولى من الاتصال حتى إغلاق الموقع بالكامل.
3. جدار بوابة التطبيقات PROXY FIREWALL: يعرف باسم جدار الحماية الوسيط، فهو وسيطبين الشبكات الداخلية والخارجية والإنترنت.

الفصل الخامس
تنفيذ أنظمة منع الاختراق

- IDS:جهاز يوضع في الشبكة ويقوم بمراقبة حركة مرور الشبكة وينسخ حركة المرور ويقوم بتحليل النسخة، يقوم بمقارنة النسخ مع توقيع البرمجيات الضارة المعروفة.
- حركة البيانات لا تمر من خلال IDS مالم يتم نسخها.
- يراقب IDSحركة المرور ويولد تنبيه (سجل) عندما يكتشف حركة مرور ضارة.
- الفرق بين IDS وIPS : IPS:يستجيب فورا ولا يسمح بمرور البرمجيات الضارة في حين ان IDS:يسمح بمرور البرمجيات الضارة
- IPS: يعمل في وضع الاتصال، ما يعني انه جميع حركة المرور الداخلة والخارجة يجب ان تمر من خلاله للمعالجة و لا يسمح بمرور الحزم الى الشبكة الخاصة/ الموثوق بها قبل ان يقوم بتحليله ، يمكنه التحقق وعنونة المشكلة فورا.
- أنواع IPS:

1. المعتمد على التوقيع Signature-based-IPS : هذه الطريقة تطابق النشاط مع تواقيع التهديدات المعروفة، أحد عيوب هذه الطريقة هو أنها تستطيع فقط إيقاف الهجمات المحددة مسبقا ولن تكون قادرة على التعرف على الهجمات الجديدة.
2. المعتمد على حركات المرور الشاذة Anomaly-Based-IPS: تراقب هذه الطريقة السلوك غير الطبيعي من خلال مقارنة عينات عشوائية من نشاط الشبكة بمعيار أساسي ،إنها أكثر قوة من المراقبة القائمة على التوقيع، لكنها قد تؤدي أحياناً إلى نتائج إيجابية خاطئة، تستخدم بعض انظمة منع التطفل الأحدث والأكثر تقدماً الذكاء الاصطناعي وتكنولوجيا التعلم الآلي لدعم المراقبة القائمة على الشذوذ
3. المعتمدة على السياسات Policy-based-IPS: يستخدم سياسات الأمان التي تحددها المؤسسة ويحظر النشاط الذي ينتهك تلك السياسات، يتطلب هذا من المسؤول إعداد وتكوين سياسات الأمان

الفصل السادس
تأمين الشبكة المحلية

- أمان الشبكة NETWORK SECURITY: هو أي نشاط مصمم لحماية إمكانية استخدام الشبكة والبيانات لديك وتكاملاها وتتضمن التقنيات كلا من الأجهزة والبرامج وتستهدف مجموعة متنوعة من التهديدات كما تمنعها من الدخول إلى الشبكة أو الانتشار بها.
- طرق تامين الأجهزة :

1. جدران الحماية
2. أمان البريد الإلكتروني والويب
3. برامج مكافحة الفيروسات والبرامج الضارة
4. تجزئة الشبكة: إنشاء شبكات فرعية داخل شبكة شركة أو مؤسسة، تسمح تجزئه الشبكة باحتواء البرامج الضارة والتهديدات الأخرى، تضع التجزئة المحددة بالبرامج حركه مرور الشبكة في تصنيفات مختلفة وتجعل فرض سياسات الأمان أسهل
5. التحكم في الوصول: لا يجب أن تتوفر لدى كل مستخدم إمكانية الوصول إلى شبكتك، لإبعاد المهاجمين المحتملين، تحتاج إلى التعرف على كل مستخدم وكل جهاز ،وحينها يمكنك فرض سياسات الأمان لديك، يمكنك حظر الأجهزة الطرفية غير المتوافقة أو منحها إمكانية وصول محدودة فقط
6. أمان التطبيق: يجب حماية أي برامج تستخدمها لإدارة أعمالك سواء تم إنشاؤه بواسطة موظفي تكنولوجيا المعلومات أو قمت بشرائها
7. منع فقدان البيانات: يجب على المؤسسات التأكد أن موظفيها ال يرسلون معلومات حساسة خارج الشبكة
8. أنظمة كشف التطفل
9. شبكةVPN
10. الأمان اللاسلكي: الشبكات اللاسلكية ليست آمنة بقدر الشبكات السلكية

- تامين الطبقة الثانية DATA LINK : قد تكون التهديدات الكهربائية أكثر شيوعا وهي تتراوح بين ارتفاع مفاجئ في الجهد إلى التيار الكهربائي غير المستقر أو إلى فقدان تام للطاقة الكهربائية يمكن تجنب هذه المخاطر باستخدام وحدات عدم انقطاع التيار.

1. ضبط كلمة مرور للمبدل:
2. ضبط لافتة تسجيل الدخول: ستساعدك لافتات تسجيل الدخول على إيصال رسالة معينه إلى المستخدمين الذين تم الاشتياق من دخولهم إلى المبدل يمكن للافتات خدمة إظهار معلومات، وعرض السياسات للمستخدمين

- يمكنك ضبط اللافتة بواسط الامر .BANNER

3. الوصول عبرSSH &Telnet

Telnet : أشهر الخيارات للوصل بين موجهين ن لأغراض الإدارة، وكذلك للاتصال إلى المبدلات لكنه غير آمن لأنه لا يوفر تشفير للاتصال SHH؛سيشفر عملية نقل البيانات .

4. ضبط حماية المنافذ:
5. تأمين المنافذ غير المستخدمة: أفضل الممارسات العملية هي تأمين المنافذ غير المستخدمة .

الاسئلة

1. تعرف بانها ضعف او خلل فالشبكة، ويقوم المهاجم من خلالها باستغلال هذا الضعف			
التهديد (Threat)	(نقاط الضعف) Vulnerability	خطر (Risk)	التخفيف (mitigation)
2. هو احتمال وجود تهديد لاستغلال نقاط الضعف في الاصول ويتم قياسه باستخدام احتمال وقوع الحدث والأثار المترتبة عليه.			
التهديد (Threat)	نقاط الضعف Vulnerability	خطر (Risk)	التخفيف (mitigation)
3. هي الطريق للدخول الى السيرفر او جهاز او الشبكة			
حجب الخدمة.	الاستطلاع	نواقل هجمات الشبكة	التهديد
4. من الأمثلة على نواقل الهجمات من خارج الشبكة			
سرقة ونسخ البيانات السرية	الانترنت	التحايل على الخوادم الداخلية	التسبب في انقطاع الشبكة.
5. هي التي تغطي مساحة جغرافية واسعة وغالبًا يكون الاتصال عن طريق الانترنت			
شبكات المكاتب الصغيرة	الشبكات الواسعة (WAN)	شبكة مراكز البيانات	الشبكة السحابية الافتراضية
6. من الأمثلة على أمن المحيط الداخلي			
رجال أمن المنشآت	اجهزة استشعار الدخول والخروج	الاسوار	أنظمة المراقبة
7. جهاز Cisco ISP يقوم بحماية البيانات من داخل الحرم الجامعي الى العالم الخارجي عن طريق انشاء شبكات خاصة افتراضية، ويضمن سلامة وسرية البيانات			
ASA Firewall	VPN	IPS	ESA/WSA
8. هي الأداة الأمنية للبريد الإلكتروني توفر حماية من التهديدات وتطبيق الرؤية والتحكم وأنشاء التقارير والحماية المتنقلة.			
WSA	ESA	VPN	IPS
9. هؤلاء الافراد الذين يرتكبون جرائم ويفعلون أشياء غير أخلاقية، ولكن ليس لتحقيق مكاسب شخصية ولا من أجل إلحاق الضرر			
White Hat Hacker	Grey Hat Hacker	Black Hat Hacker	red Hat Hacker
10. النقاط او الأجهزة النهائية التي يتم تأمينها عن طريق مكافح الفايروسات او مكافح البرمجيات الخبيثة			
Host	AAA Server	Wireless Host	Branch Site
11. هؤلاء قراصنة أخلاقيون يستخدمون مهاراتهم في البرمجة لأغراض طيبة، وأخلاقية، وقانونية			
White Hat Hacker	Grey Hat Hacker	Black Hat Hacker	red Hat Hacker
12. هؤلاء المجرمون الغير أخلاقيين الذين ينتهكون أمن أجهزة وشبكات الحاسب لتحقيق مكاسب شخصية			
White Hat Hacker	Grey Hat Hacker	Black Hat Hacker	red Hat Hacker

13. هو الذي يقوم بتثبيت نفسه في اول سطر في الكود او في ملف التنفيذ وفي حالة التشغيل يقوم بنقل العدوى للأقراص

الفيروسات	حصان طروادة	المتسلل	الهاكر

14. هو السعي لكشف اسم المستخدم وكلمة المرور للوصول لموارد الكمبيوتر او الشبكة

هجوم الوصول	هجوم الاستطلاع	هجوم حجب الخدمة	هجوم الفيضان

15. هو نوع من الهجوم تنشأ عنه كمية كبيرة من الطلبات بشكل غير عادي إلى خوادم الشبكة

هجوم الوصول	هجوم الاستطلاع	هجوم حجب الخدمة	الهندسة الاجتماعية

16. يكمن الهدف من هجوم حجب الخدمة زيادة سرعه التطبيقات والعمليات

صح	خطا		

17. يُنفذ المهاجم هجوم.....من خلال اعتراض الاتصالات بين أجهزة الكمبيوتر لسرقة المعلومات المنتقلة عبر الشبكة

الهندسة الاجتماعية	كسر كلمة المرور	رجل في المنتصف	القوة العمياء

18. يترك المهاجم جهازاً مصاباً بالبرامج الضارة، مثل محرك أقراص USB في مكان عام ويعثر الضحية على الجهاز ثم يحمله على الجهاز الخاص به ليثبت البرنامج الضار دون قصد

التمثيل	التصيد الاحتيالي	البريد غير المرغوب	الاصطياد بالطُعم

19. فيها يحاول المهاجم تركيب معلومات يعرفها عن الضحية كرقم هاتفه او تاريخ ميلاده

القوه العمياء	التخمين	القاموس	حجب الخدمة

20. هو لائحة بالكلمات التي يعتقد ان تستخدم لصياغة كلمات السر

القوه العمياء	التخمين	القاموس	حجب الخدمة

21. هو نظام منع التسلل يوفر تحقق في نفس الوقت بالإضافة الى المنع

IDS	IPS	Firewall	IP

22. هو الذي يقوم بمنع حركة المرور الغير مرغوبة، ويكون اما برمجيات في الراوتر او جهاز مستقل

IDS	IPS	Firewall	IP

23. نهج الامان هو مجموعة من الاهداف الامنية التي تضمن الامان للشبكة والبيانات وأنظمة الكمبيوتر

صح	خطأ		

24. هو الذي يضمن توافق كلمات المرور مع الحد الادنى للمتطلبات وتغييرها يدويا

نهج التعريف والتصديق	نهج كلمة المرور	نهج الوصول عن بعد	نهج هجوم الوصول

25. يوفر هذا النوع من الموجهات جدار حماية يعمل كنقطة تفتيش افتراضيه

نهج جهاز التوجيه الفردي	نهج الدفاع في العمق	DMZ roach	نهج الوصول عن بعد

26. يمتلك هذا النوع من الموجهات منطقة أمنية منزوعة السلاح تستخدم غالبًا لوضع أجهزة السيرفر

نهج جهاز التوجيه الفردي	نهج الدفاع في العمق	DMZ roach	نهج الوصول عن بعد

27. من الأمثلة على الأمان المادي للراوتر

ضبط الرطوبة	زيادة حجم الذاكرة	النسخ الاحتياطي	تامين التحكم الإداري

28. من الأمثلة على تقوية وتأمين الموجه بتقليل نقاط الضعف

ضبط الرطوبة	زيادة حجم الذاكرة	ضبط درجة الحرارة	تامين التحكم الإداري

29. هو البروتكول الذي يتم من خلاله ارسال البيانات بين المستخدم والاجهزة البعيدة بصورة غير مشفره

SSH	https	Telnet	tcp

30. عند تفعيل ssh فإن الراوتر يعمل كخادم او عميل.

صح	خطأ		

31. هي التي يتم فيها تخزين الرسائل في ذاكرة الموجه، ويتم مسحها عند إعادة تشغيل جهاز التوجيه

Console	Logging buffer	Terminal Lines	Syslog server

32. من المزايا الأمنية التي تقيد المالك الى تصرفات محدودة

Message integrity and authentication	Encryption	Access control	Access

33. هو البروتكول المستخدم في اكتشاف طبقة الوصول

CDP	LLDP	TCP	UDP

34. هي اثبات هوية المستخدم الذي يريد الوصول الى الشبكة

المصادقة	التفويض	التدقيق	التصحيح

35. هي التي تحدد الموارد التي يستطيع المستخدم الوصول لها وماهي العمليات المسموحة له

المصادقة	التفويض	التدقيق	التصحيح

ملخص لمقرر الجريمة الالكترونية ومخاطرها

الفصل الأول
الجرائم الإلكترونية وتطورها

- **مفهوم الجريمة الإلكترونية Cybercrime والتطور التاريخي لها**

مرت الجرائم الإلكترونية بتطور تاريخي تبعا لتطور التقنية واستخداماتها وقد مرت بثالث مراحل هي:

المرحلة الأولى

تتمثل في انتشار استخدام الحواسيب في **الستينيات والسبعينيات**

ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الحاسب وعالجت عددا من قضايا الجرائم الفعلية وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

أبرز جريمة هي جريمة سرقة بنك مينيسوتا الأمريكي عام 1966 م والتي اعتبرت أول سرقة إلكترونية تقع على بنك وبعد ذلك توالت بعض المقالات الصحفية في الظهور متناولة بعض الحالات التي أطلق عليها في هذا الوقت **جرائم الحاسوب Computer Crime** رغم استمرار تطور ظاهرة الجريمة الإلكترونية خلال السبعينيات إلى أن الحالات التي سجلت في تلك الفترة الزمنية كانت قليلة.

وقد تعود أسباب تلك القلة إلى كون مكمن الخطر كان داخليا ويكاد أن يكون خطرا ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطيعون الوصول إلى تلك الأنظمة بصورة مباشرة

ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي كما أن سبب قلتها أيضا يعود إلى عدم الإبلاغ عن الكثير من تلك الجرائم

لكون الشركات والوكالات كانت تحرص على عدم اهتزاز الثقة بها وبأنظمتها الحديثة وأعقبت تلك الحقبة الزمنية إجراء دراسات ومقالات صحفية بشأن الجريمة الإلكترونية من قبل الباحثين الصحفيين.

وفي السبعينيات أيضا شهد العالم بداية لظهور بعض التشريعات والقوانين التي تجرم بعض الممارسات

ذات الصلة بإساءة استخدام الحاسوب وقررت لها عقوبات محددة كما حدث في السويد والتي **اعتبرت بذلك أول دولة يصدر فيها قانون يجرم بعض الأفعال والممارسات المرتبطة بالحواسيب.**

المرحلة الثانية

في الثمانينيات طفا على السطح مفهوم جديد للجرائم الإلكترونية ارتبط بعمليات اقتحام نظام الحاسب عن بعد وأنشطة نشر وزراعة الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو

البرامج وانتشر مصطلح **المخترق Hacker** المعبر عن مُقتحمي النُظم كما ظهر ما يُعرف باسم **"المجرم المعلوماتي أو الإلكتروني"**

فقد حدث تغيرا" ملحوظا في التعامل مع ظاهرة الجريمة الإلكترونية وذلك من جانب الباحثين والعامة على السواء **بسبب ارتفاع مؤشر عدد القضايا ذات الصلة بإساءة استخدام الحاسوب ولاسيما بعد اهتمام الصحافة وإبرازها لتلك القضايا حيث أصبح بعضها يؤرق المجتمع الدولي كقضايا الاختراق و قرصنة البرمجيات والتلاعب في أنظمة النقد الإلكتروني و انتشار العديد من الفيروسات** كما شهد ذلك العهد الانطلاقة الأولى للقوانين والتشريعات الخاصة بحماية البرامج الحاسوبية **والتي أطلق عليها قوانين حماية الملكية الفكرية واعتبرت من القوانين الأكثر وضوحا و نضجا"**

وكذلك في تلك الفترة الزمنية ظهر الاهتمام العربي بظاهرة الجريمة الإلكترونية وتمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة الإلكترونية و عقد الندوات المختلفة ذات الصلة بذلك حيث عقدت في 1986م

ندوة أمن المعلومات في الحاسبات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية.

المرحلة الثالثة

تتمثل في فترة التسعينيات حيث شهدت تزايد هائل في مجال الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات.

شهدت التسعينيات والسنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الإلكترونية حيث ارتبط بتحول شبكة الإنترنت في ذلك الوقت من شبكة أكاديمية إلى شبكة تعني بخدمة المجالات التجارية والفردية حيث بلغ مستخدميها في عام 1996 م ما يقارب من 40 مليون مستخدم الأمر الذي أدي إلى نشأة عبء كبير على المختصين بمكافحة الجريمة الإلكترونية ولذلك وُجد مفهوم جديد عرفها **" بالجرائم العابرة حيث يستطيع المجرمون تنفيذ مخططاتهم الإجرامية في دول أخرى .**

- **أشهر الجرائم الإلكترونية في التاريخ**

منذ انتشار الحواسيب وشبكة الأنترنت، حدثت العديد من الهجمات الإلكترونية ضد الأفراد والشركات والحكومات، ابرز واشهر تلك الهجمات

1- **هجمة فايروس ميليسا**

يعتبر فايروس ميليسا أحد أكبر وأقدم التهديدات الإلكترونية، ففي عام 1999 م، قام ديفيد لي سميث باختراع فايروس ميليسا وهو فايروس بسيط يصيب مستندات مايكروسوفت ورد، وينشر نفسه تلقائيًا كمرفق عبر البريد الإلكتروني، تسبب هذا الفيروس في دمار شديد في أنظمة شركة مايكروسفت والعديد من الشركات الأخرى، وقدر أن إصلاح هذا الأنظمة المتدمرة كلف ما يقارب 80 مليون دولار.

2- الهجوم الإلكتروني على ناسا

في عام 1999 م قام جيمس جوناثان وهو شاب يبلغ من العمر 15 عامًا فقط، باختراق أجهزة الحاسب التابعة لوكالة ناسا، وتسبب هذا الاختراق بإغلاق أجهزة حاسب ناسا لمدة 21 يومًا، مما كلف الوكالة حوالي 41000 دولار في الإصلاحات.

3- الهجوم الإلكتروني على إستونيا

في أبريل من عام 2007 م، شهدت دولة إستونيا أول هجوم إلكتروني على البلد بأكمله، بحيث سبب هذا الهجوم توقف حوالي 58 موقعًا إستونيًا عن الاتصال بالإنترنت، بما في ذلك مواقع الحكومات والبنوك ووسائل الإعلام.

4- الهجوم الإلكتروني على شركة PlayStation سوني

في أبريل من عام 2011 م، أدى هجوم إلكتروني على شبكة Network PlayStation التابعة لشركة Sony، إلى المطالبة بالمعلومات الشخصية لحوالي 77 مليون مستخدم.

5- الهجوم الإلكتروني على موقع Yahoo

في عام 2014 م، شهد موقع Yahoo هجومًا إلكترونيًا كبيرًا تمثل في سرقة المعلومات الأساسية وكلمات المرور لحوالي 500 مليون حساب مستخدم على الموقع.

6- الهجوم الإلكتروني على شبكة كهرباء أوكرانيا

في عام 2015 م، تم القيام بهجوم إلكتروني على شبكة الكهرباء في أوكرانيا بحيث أدى هذا الهجوم إلى انقطاع التيار الكهربائي عن نصف المنازل في منطقة إيفانو فرانكيفسك.

7- الهجوم على خط أنابيب توزيع الوقود الخاص بشركة كولونيال بايبالين

في عام 2021 م، أجبر هجوم إلكتروني شركة كولونيال بايبالين، وهي شركة طاقة أمريكية على إغلاق خط أنابيب توزيع الوقود للساحل الشرقي للواليات المتحدة، ودفعت شركة كولونيال بايبالين ما يقرب من5 ملايين دولار للقراصنة من أوروبا الشرقية للمساعدة في استعادة أكبر خط أنابيب للوقود في البالد.

- **تعريف الجرائم الإلكترونية**

الجرائم الإلكترونية أو ما يسمى أيضا الهجمات الإلكترونية

هو استخدام الكمبيوتر كأداة لتحقيق غايات غير قانونية، مثل ارتكاب الاحتيال أو سرقة الملكيات الفكرية أو سرقة الهويات أو اختراق الخصوصيات، وتعتبر الجرائم الإلكترونية امتداداً للسلوك الإجرامي العادي إلى أن الجرائم الإلكترونية تمتاز بأنها نمط جرائم مستحدث غير تقليدي ويمكن تعريف الجرائم الإلكترونية أيضا بأنه عبارة عن هجوم على المعلومات المتعلقة بالأفراد أو الشركات أو الحكومات، **وتتميز الجرائم الإلكترونية بإمكانية حدوثها في منطقة بعيدة جدا عن منطقة المهاجم ومثال على ذلك يستطيع شخص القيام بمهاجمة دولة تقع في قارة أخرى بعيدة عنه، كمهاجمة شخص في كندا لشخص في أستراليا إلكترونيا .**

- **مفاهيم الجرائم الإلكترونية**
- هي كل نشاط إجرامي يتم ضد أو باستخدام الحواسيب الآلية والبرامج والتطبيقات المختلفة وشبكات المعلومات، خاصتا شبكة الإنترنت.
- هي كل نشاط إجرامي تُستخدم فيه التقنية الإلكترونية الرقمية) الحاسب الآلي وشبكة الإنترنت(بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي ال ُمستهدف"
- هي فعل أو نشاط إجرامي يرتكب متضمنا استخدام الحاسب الآلي، أو شبكة المعلومات العالمية أو أي وسيلة من وسائل الاتصالات وتقنية المعلومات الأخرى كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود بطريقة مباشرة أو غير مباشرة.
- هي كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنويه
- هي نشاط إجرامي يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهازا متصلا بالشبكة وتحاول استخدامهم.

- **الجريمة التقليدية والجريمة الإلكترونية**

تتشابه أطراف الجريمة الإلكترونية والجريمة التقليدية من حيث وجود مجرم له دافع ارتكاب الجريمة سواء كان شخصا" طبيعيا أو اعتباريا" ولكن الاختلاف في الأداة المستخدمة في ارتكاب الجريمة والمتمثلة في شبكة الإنترنت وهي أداة عالية التقنية كما ال يتطلب مكان الجريمة انتقال ماديا" للجاني، فقد انتشرت الجرائم الإلكترونية على شبكة الإنترنت وتعددت صورها وأشكالها.

- **تطور الجريمة من الشكل التقليدي إلى الشكل الإلكتروني**

الجريمة التقليدية	الجريمة الإلكترونية
الإحتيال	الاحتيال على الشبكة – المزاد الإلكتروني
السطو	القرصنة – الحرمان من الخدمة – نشر الفيروسات
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية – سرقة الملكية

- **أوجه التطابق بين الجريمة الإلكترونية والتقليدية**
- الركن الأول:

أن يكون هناك نص يحظر الجريمة ويعاقب عليها وهو ما يسمى في الاصطلاح القانوني بالركن الشرعي للجريمة

- الركن الثاني:

إتيان العمل المكون للجريمة سواء كان فعال أو امتناعا وهو ما يسمى في القانون بالركن المادي للجريمة

- الركن الثالث:

أن يكون الجاني مكلفا أي مسؤول عن الجريمة وهو ما يسمى في الاصطلاح القانوني بالركن الأدبي

- وهذه الأركان جميعها متوافرة في الجريمة التقليدية والجريمة المعلوماتية على حد سواء
- **تشتمل طرق الجريمة الإلكترونية**
- سرقة وتخريب وتزوير المعلومات وإساءة استخدامها.
- اختراق الخصوصية من خلال سرقة حسابات الأفراد ونشر معلومات سرية عنهم بهدف إفشاء أسرارهم.
- التصنت وتشمل الدخول لقواعد المعلومات تسجيل المحادثات عبر الهاتف.
- التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
- التشهير ويشمل المعلومات الخاصة أو ذات الصلة بالانحراف ونشرها بشكل القصد منه الإساءة إلى شخصية الأفراد.
- السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
- سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
- قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

- قرصنة البيانات والمعلومات ويشمل اعتراض البيانات والاستيلاء عليها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
- ارسال الفيروسات على شكل رسائل الكترونية بهدف تدمير البيانات
- الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق او المالية او الهاتفية.
- سرقة الأرقام والمتاجرة بها وخاصة ارقام الهواتف السرية واستخدامها في الاتصالات الدولية او ارقام بطاقات الائتمان
- المطاردة والملاحقة من خلال استخدام البريد الإلكتروني أو إرسال الرسائل.
- **الجريمة المعلوماتية**
- هو سلوك غير قانوني يحدث عند اختراق الأجهزة الإلكترونية والذكية والحواسيب، التي تعتمد على الإنترنت في عملها

الجرائم الإلكترونية جرائم ترتكب ضد أفراد أو جماعات أو مؤسسات كاملة؛باستخدام وسائل الاتصال الحديثة واستخدام الحاسوب، والهدف الأساسي منها يكون ابتزاز الشخص أو تشويه سمعته، وإلحاق الضرر به؛ للحصول على مقابل مادي مثل النقود أو لتحقيق أهداف سياسية، أو إفشاء أسرار أمنية تكون خاصة بالمؤسسة.

الجريمة المعلوماتية أي فعل يُرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لنظام مكافحة الجرائم المعلوماتية.

الجريمة الالكترونية هي فعل غير مشروع يعتمد على الدراية والمعرفة الفنية بتقنية المعلومات ويتم بأي أداة من أدوات الاتصال الذكي والبرمجي ويكون فيه الفضاء الإلكتروني هو مكانها.

شرح التعريف:

1- فعل غير مشروع:

يشمل كل فعل أو امتناع تجرمها الشريعة الإسلامية أو نصوص القانون وتقرر له عقوبة تُطال مرتكب ذلك الفعل.

2- يعتمد الدراية والمعرفة الفنية بتقنية المعلومات:

هو جوهر الجريمة الإلكترونية حيث يستحيل على الذي يجهل بشؤون هذه التقنية ارتكاب هذا النوع من الجرائم فالبد من دراية ومعرفة ولو يسيرة لإتمام هذه الجريمة وهذا الفعل الغير مشروع قد يقوم به شخص أو مجموعة أشخاص ويمكن أن تقوم بها دولة أو عدة دول.

3- أدوات الاتصال الذكي والبرمجي:

لم يعد يقتصر في هذا النوع من الجرائم استخدام الحاسبات الآلية التقليدية لإتمام هذا النوع من الجرائم حيث أصبح هنالك البطائق الممغنطة والأجهزة الرقمية الحديثة كالتليفونات والشرائح الإلكترونية القارئة والناسخة للمعلومات والبرامج والمخترقة للثغرات الأمنية والتجسسية والفيروسية والتي لولاها لما وجدت جرائم إلكترونية من الأساس.

4- يكون فيه الفضاء الإلكتروني محال ومسرحا لها:

نقلت هذه الجرائم مسرح الجريمة من أبعادها المحدودة إلى بعد جديد غير مقيد بزمان أو مكان يكون فيها الجاني بعيد عن الضحية بحيث تذوب فيه الحدود الجغرافية وقد تستمر محاولات ارتكاب هذا النوع من الجرائم لأسابيع وشهور بخالف الجرائم التقليدية.

- **المجرم في الجريمة الإلكترونية والضحية في الجريمة الإلكترونية**

المجرم في الجريمة الإلكترونية	الضحية في الجريمة الإلكترونية
ه شخص طبيعي يعمل لحسابه ويهدف إلى تحقيق مصلحة صة به من وراء الجريمة التي يرتكبها. حيث م تصنيف معظم من يرتكب جرائم الحاسب الآلي إلى جيل الحديث من الشباب وهم قد يكونوا محترفين أو عاملين جال الحاسب الآلي أو قد يكونون هواة. إلى جانب الشخص طبيعي قد يوجد مشتركون يمدونه بما يحتاجه من أدوات امج ومعدات أو على الأقل يبيعون له تلك المنتجات والبرامج ي بدونها لن يكون هناك جريمة من الأساس . **حما من الممكن أن يكون المجرم مجموعة من الأشخاص أو مؤسسات**	د يكون شخص طبيعي، أو مجموعة أشخاص، أو خاص معنوية أو أنظمة ودول. عظم الجرائم الإلكترونية تستهدف المؤسسات الية والتجارية والصناعية للمجتمع كما أنها أيضا تهدف الأنظمة السياسية والمصالح الخدمية دنية والعسكرية والأمنية وذلك عن طريق تدمير أو ف ثرواتهم المعلوماتية الخاصة بها.

- تنقسم الجريمة الإلكترونية الى نوعان

الأول	الثاني

خرائم الموجهة ضد الحاسب الآلي أو أنظمة تقنية علومات والاتصالات الأخر ى بقصد إتلافها أو تدميرها طيلها	خرائم التي يكون فيها الحاسب الآلي وسيلة للارتكاب ائم الاحتيال وسرقة الهويات وبطاقات الائتمان و صدة المالية والتزوير والاختلاس وسرقة حقوق الملكية كرية و غيرها.

- **أركان الجريمة الإلكتروني**

الركن المادي للجريمة الإلكترونية

أ –السلوك الإجرامي وهو السلوك المادي الصادر عن إرادة الفرد الذي يتعارض مع القانون

ب– النتيجة الإجرامية يراد بها التغير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي

جـ– الرابطة السببية هي العلاقة التي تربط بين السلوك الإجرامي والنتيجة الإجرامية وبانتفاء أو انقطاع هذه الرابطة بين السلوك الإجرامي والنتيجة فإن الركن المادي للجريمة ال يتحقق وبالتالي لا يعود ممكنا إسناد هذه النتيجة إلى مرتكب الفعل.

الركن المعنوي

يعرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها بالتالي يتكون هذا الركن من عنصرين هما العلم والإرادة.

–فالعلم: هو إدراك الأمور على نحو مطابق للواقع، يسبق الارادة.

–أما الإرادة: فهي اتجاه لتحقيق السلوك الإجرامي.

الركن القانوني

هو الذي يضع النص لتجريم هذا الفعل.

أنواع الجرائم الإلكترونية

يمكن تقسيم أنواع الجريمة الإلكترونية إلى أربع مجموعات:

– المجموعة الأولى:

تشمل الجرائم التي تتمثل في استغلال البيانات المخزنة على الحاسب بشكل غير قانوني.

– المجموعة الثانية:

تشمل الجرائم التي يتم من خلالها اختراق الحاسب لتدمير البرامج والبيانات الموجودة في الملفات المخزنة عليه وتدخل ضمن الفيروسات الإلكترونية.

– المجموعة الثالثة:

تشمل الجرائم التي يتم فيها استخدام الحاسب بشكل غير قانوني من قبل الأفراد المرخص لهم باستعماله أي الموظفين المستغلين لمنصبهم.

– المجموعة الرابعة:

تشمل الجرائم التي يتم فيها استخدام الحاسب بشكل غير قانوني من قبل الأفراد غير المرخص لهم باستعماله أي غير مسموح لهم.

- **أدوات الجرائم الإلكترونية:**

برامج نسخ المعلومات المخزنة في أجهزة الحاسب الالي.

1. الإنترنت كوسيط لتنفيذ الجريمة.
2. خطوط الاتصال الهاتفي التي تستخدم لربط الكاميرات ووسائل التجسس.
3. أدوات مسح الترميز الرقمي(الباركود)
4. الطابعات.
5. أجهزة الهاتف النقال والهواتف الرقمية الثابتة.
6. الهندسة الاجتماعية
7. برامج مدمرة مثل:

– برنامج حصان طروادة horse trojan: بحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وأمن ويؤدي تشغيله إلى تعطيل الحاسب المصاب.

– برنامج الدودة: الذي يشبه الفيروس، ولكنه يصيب اجهزة الحاسب دون الحاجة إلى أي فعل وغالبًا يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.

– القنبلة الإلكترونية يوجد نوعين:

–القنبلة المنطقية: عبارة عن برنامج صغير يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو فترة زمنية منظمة بحيث تعمل على مبدأ التوقيت فتحدث تدميرًا في المعلومات والبرامج عند إنجاز أمر معين في الحاسب أو برنامج معين.

–القنبلة الزمنية: سميت كذلك لقيامها بالعمل التخريبي في وقت يحدد سلفًا.

8. الباركود وهو عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز.

- **خصائص الجرائم الإلكترونية**

تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجريمة التقليدية فلها طبيعة خاصة لا وجود لها في عالم الجرائم التقليدية، ساعد ذلك في انتشار تقنية المعلومات والتطور التكنولوجي ما أضفى عليها مجموعة من الخصائص من أهمها:

1 –الجريمة الإلكترونية جريمة عابرة للحدود:

أي أن الجرائم الإلكترونية تتسم بأنها ذات طابع دولي ولذلك تعتبر من الجرائم الدولية، التي اتفق المجتمع الدولي بمُقتضى عهد دولي على أنها تُشكل عدوانًا في كل دولة.

2 –صعوبة إثبات الجريمة الإلكترونية:

لا تحتاج الجرائم الإلكترونية إلى أي عنف أو اقتحام لسرقة الأموال وإنما هي أرقام وبيانات تتغير أو تُمحى من السجلات المخزنة في الحاسبات الآلية ولأن هذه الجرائم لا تترك أي أثر خارجي مرئي لها وتكون في الخفاء فيصعب إثباتها وكذلك نتيجة إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبًا للإساءة إلى السمعة وهز الثقة في المنظمات والمؤسسات.

3–الجريمة الإلكترونية جريمة مُستحدثة

تُعد الجرائم الإلكترونية من أنواع الجرائم الجديدة التي يُمكن أن تُشكل أخطارًا جسيمة في ظل العولمة حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته وإمكانياته أجهزة الدولة الرقابية أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.

4 –من حيث موضوع الجريمة:

يختلف موضوع الجريمة الإلكترونية وفقا لحالتين:

الحالة الأولى

يجتمع فيها الجرائم التقليدية وجرائم المعلوماتية بمعناها الفني وحيث يكون موضوع الجريمة هو النظام المعلوماتي أي أن أحد المكونات المادية للنظام المعلوماتي كالأجهزة والمعدات والكابلات وإذا لم يكن ثمة أهمية للتقنية في ارتكاب الجريمة فتكون جريمة تقليدية كما هو الحال في سرقة أو إتلاف الحاسب أو شاشته إما إذا كان موضوع الجريمة هو أحد المكونات غير المادية للنظام المعلوماتي كالبيانات والبرامج فتكون جريمة معلوماتية.

الحالة الثانية

يكون النظام المعلوماتي والحاسب هو وسيلة تنفيذ الجريمة وأدائها.

5 –عدم وجود مفهوم مشترك للجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بعدم وجود مفهوم مشترك لماهية الجريمة الإلكترونية و كذلك عدم وجود تعريف قانوني موحد لها بسبب عدم وجود تنسيق دولي في مجال الجريمة الإلكترونية و يرجع ذلك إلى عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة الإلكترونية أو لاختلاف مفهوم الجريمة تبعًا لاختلاف النظم القانونية و هذا يتطلب إيجاد الوسائل المناسبة لتشجيع المجتمع الدولي لمواجهة الجرائم الإلكترونية و العمل على سن التشريعات الخاصة التي تواجه هذا

النوع من الجرائم و إبرام المعاهدات التي تحث على تبادل المعلومات و الخبرات و تسليم و تبادل المجرمين.

6 –قلة الإبلاغ عن الجريمة الإلكترونية:

- في الغالب لا يتم الإبلاغ عن جرائم الإنترنت
- إما لعدم اكتشاف الضحية لها
- وإما الخوف من التشهير،
- معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

7 –جرائم متجددة دائمة التطور:

الجرائم الإلكترونية تدور في فلك تقنية المعلومات والتكنولوجيا الحديثة ووجودها وتطورها مرتبط بوجود وتطور تكنولوجيا المعلومات ويترافق مع التطور الدائم والمتجدد لتقنية المعلومات والتكنولوجيا الرقمية تطور أساليب وطرق ارتكاب الجرائم الإلكترونية حيث يستغل المجرمون شبكة الإنترنت لتبادل المعلومات والأفكار والخبرات الإجرامية.

8 –جرائم غير عنيفة الأداء:

فهي محصورة فقط في استهداف المعلومات والبيانات التي يتم بواسطتها الوصول للأموال والأشخاص فهي ليست ذات طبيعة مادية ملموسة.

- **خصوصية المجرم الإلكتروني:**

هي جرائم فنية تقنية ومن يرتكبها يكون ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه أدنى حد من المعرفة والقدرة على استخدام جهاز الحاسب والتعامل مع شبكة الإنترنت.

- **خصائص المجرم الإلكترونية**

1 –الذكاء والمعرفة التقنية

2 –الاحتراف

3 –الخبرة والمهارة

4 –غير عنيف: فهو ينتمي إلى إجرام الحيلة.

5 –لديه نزعة إجرامية: هذه النزعة الإجرامية تتكون نتيجة لتأثره بعوامل نفسية صاحبت نشأته وتظل طاقة كامنة إلى أن تظهر في شكل عمل إجرامي

6 –لديه الدافع: وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الدافع الأول وراء ارتكاب الجريمة المعلوماتية أو الانتقام من صاحب العمل.

7 –يمتلك حب المخاطرة.

8 –يمتلك خيال نشط وحب انتحال الشخصيات.

9 –يمتلك الوسيلة: يراد بها الإمكانيات التي يحتاجها المجرم المعلوماتي لإتمام جريمته

10 –يمتلك المجرم المعلوماتي السلطة: يقصد بالسلطة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في اختراق المعلومات.

- **أنماط المجرم الإلكتروني**

- المخترقون (Hackers): هم الأشخاص الذين يستخدمون مهارات الحاسب المتقدمة للهجوم على أجهزة حاسب أخرى، ولكن ليس لديهم أي نوايا خبيثة وإنما لكشف العيوب وتحسين الأمن المعلوماتي.
- (القراصنة)Crackers : هم الأشخاص الذين يخترقون أمن النظام ولديهم نوايا خبيثة، كذلك لديهم مهارة متقدمة بأجهزة الحاسب والشبكات والمهارات اللازمة لتدمير البيانات، وحرمان المستخدمين الشرعيين من الخدمة أو التسبب بمشاكل خطيرة على الأجهزة.
- الأطفال أو المراهقون المستهترون : (Kiddies Script): هم أشخاص غير مهرة ويقومون باختراق أجهزة الحاسب باستخدام برامج اختراق يحملونها من الإنترنت ويعتبرون من أخطر أنماط المجرمين لعدم درايته بما يفعل فهو لا يملك الإلمام الكافي بالتقنية.
- المتجسسون :(Spies): هم أشخاص يستهدفون أجهزة معينة ليس بشكل عشوائي ولذلك لسرقة معلومات معينة أو تدمير أجهزة معينة وغالبًا ما تكون أهدافهم ألسباب مالية.
- الموظفون : (Employees): من أكبر المهددين للأمنية التي تهدد الشركات، فهم يقتحمون أجهزة شركاتهم لعدة أسباب: إما عرض الضعف الموجود في نظام الشركة أو لأهداف مادية أو لسخطهم من الشركة وتهديدهم عندما ينوي العودة للعمل في شركتهم.
- الإرهابيون :(Cyber terrorists): هم أشخاص متخصصون ولديهم مهارات عالية غالبا ما يهددون البنية التحتية لأجهزة الكمبيوتر والشبكات ليسببوا الذعر والمهاجمة من أجل نشر أفكارهم ومبادئهم، وقد يقوموا بنشر معلومات خاطئة وإشاعات كاذبة عن جهات معادية لهم، ويعتبر الإنترنت بحد ذاته من أهم أهدافهم.

- **أهداف الجرائم الإلكترونية**

– التمكن من الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو حذفها والاطلاع عليها.

– التمكن من الوصول بواسطة الشبكة العنكبوتية إلى أجهزة الخوادم الموفرة للمعلومات وتعطيلها أو التلاعب ببياناتها.

– الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم إما لتحقيق هدف مادي أو سياسي

– الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية.

- **دوافع الجرائم الإلكترونية**

1 –دوافع مادية ويتمثل في: تحقيق الكسب المادي تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت

2 –دوافع شخصية وتتمثل في : الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقتهم في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.

3 –دوافع ذهنية أو نمطية : غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في إثبات الذات وتحقيق الانتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا تخريبية.

4 –دوافع إنتقامية: تعد من أخطر الدوافع التي يمكن أن تُفيد شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.

5 –دافع التسلية: هي جريمة ترتكب من أجل التسلية لا يقصد من ورائها إحداث جرائم.

6 –دافع سياسي: يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الأخبار والمعلومات، تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العال.

الفصل الثاني
جرائم الإنترنت

- **مفهوم جرائم الإنترنت**

هيً أفعال تتم باستخدام او عبر شبكة الأنترنت، مخالفة للقانون والتنظيمات المعمول بها وتلحق أضرار بنظام المعلومات، أو بالأموال، أو الأشخاص، أو النظام العام.

كما استعمل مصطلح جرائم الأنترنت – Internet crimes - في مؤتمر جرائم الأنترنت المنعقد في استراليا 1998

- **خصائص جرائم الإنترنت**

تعتبر الجرائم التي ترتكب من خلال شبكة الإنترنت، جرائم ذات خصائص منفردة، لا تتوافر في الجرائم التقليدية، سواء من حيث أسلوب وطرق ارتكابها أو الشخص مرتكبها، وتعددت هذه الخصائص والمميزات، فيرى الدكتور مراد عبد الفتاح، انها جرائم تتسم بكونها:

أولاً: عالمية ال تعترف بالحدود الجغرافية كونها تقع عبر حدود دولية كثيرة.

ثانيا: صعبة المتابعة والاكتشاف ألنها ال تترك أثر كونها مجرد ارقام كما تفوق معلومات المحقق التقليدية.

ويرى الأستاذان منير محمد الجلبيهي وممدوح محمد الجلبيهي إن لجرائم الإنترنت أربع خصائص:

اولا: الحاسب الآلي هو أداة ارتكابها، فال يمكن ارتكاب أي جريمة على شبكة الإنترنت الا وكان جهاز الحاسب وسيلة ارتكابها، وهذا ما يميزها عن باقي الجرائم.

ثانيا: ترتكب عبر شبكة الإنترنت، فتعتبر شبكة الإنترنت أنها حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك، الشركات وغيرها.

ثالثا: مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الحاسب الآلي، فحتى تقع جريمة الإنترنت يجب ان يكون الفاعل متمكن من التقنية ومتمتع بالدراية العالية الاستخدام الحاسب الآلي، فالكثير من الجرائم، اكتشف ان فاعليها من خبراء الحاسب الآلي.

رابعا: هي جريمة ال حدود جغرافية لها، تقع جرائم الإنترنت متخطية حدود الدولة التي ارتكبت فيها ويمكن ان ترتب أثارها عبر كافة دول العالم.

- **بروتوكولات الإنترنت**

1. بروتوكول التحكم في الإرسال (TCP)

TCP (Protocol Control Transmission) أو بروتوكول التحكم في الإرسال هو بروتوكول اتصال شائع يستخدم للتواصل عبر الشبكة، كما يقسّم أي رسالة إلى سلسلة من ا لحزم التي يتم إرسالها من المصدر إلى الوجهة وهناك يتم إعادة تجميعها في الوجهة موصُوف بالوثيقة، أي يُؤمن نقالً موثوقًا خاليًا من الأخطاء لدفق من البايتات بين مُضيفين يتصلان مع بعضهما البعض عبر شبكة تدعم بروتوكول الإنترنت.

2. بروتوكول الإنترنت (IP)

بروتوكول الإنترنت هو بروتوكول الاتصال الأساسي في حزمة بروتوكولات الإنترنت ويُشكّل الأساس الذي تعتمد عليه عمليّة توجيه الرزم ضمن الشبكة، ويسمح ذلك بالاتصال بين الشبكات المُختلفة، وهذا هو جوهر شبكة الإنترنت. تم تصميم بروتوكول الإنترنت IP (Protocol Internet) بشكل صريح كبروتوكول عنونة، كما أنه يتم استخدامه في الغالب مع بروتوكول TCP تساعد عناوين IP في الحزم على توجيهها عبر عقد Nodes مختلفة في الشبكة حتى تصل إلى النظام الوجهة IP / TCP هو البروتوكول الأكثر شيوعًا الذي يربط بين الشبكات.

3. بروتوكول مخطط بيانات المستخدم (UDP)

UDP (Protocol Datagram User) هو بروتوكول اتصال بديل لبروتوكول التحكم في الإرسال، كما يتم تنفيذه بشكل أساسي لإنشاء ارتباط يتسامح مع زمن الانتقال المنخفض بين التطبيقات المختلفة. تناقل البيانات باستعمال UDP أسرع ألنه ال يتحقق من صحة المعلومة ألنه إذا أراد التحقق من صحة المعلومة يحتاج إلى إرسال المزيد من المعلومات للتحقق من صحة النقل وهذا يزيد من حجم البيانات المرسلة ويؤدي إلى زيادة الوقت المستغرق في التراسل ولهذا جعلت مسؤولية التحقق من الإرسال من مسؤولية البرنامج نفسه.

4. بروتوكول مكتب البريد (POP)

تم تصميم بروتوكول POP (Protocol office Post) لتلقي رسائل البريد الإلكتروني الواردة.

5. بروتوكول نقل البريد البسيط (SMTP)

تم تصميم بروتوكول SMTP (Protocol transport mail Simple) لإرسال البريد الإلكتروني الصادر وتوزيعه.

6. بروتوكول نقل الملفات (FTP)

يتيح FTP (Protocol Transfer File) للمستخدمين نقل الملفات من جهاز إلى آخر، كما قد تتضمن أنواع الملفات ملفات البرامج وملفات الوسائط المتعددة والملفات النصية والمستندات وما إلى ذلك.

7. بروتوكول نقل النص التشعبي (HTTP)

تم تصميم بروتوكول نقل النص التشعبي HTTP (Protocol Transfer Text Hyper) لنقل نص تشعبي بين نظامين أو أكثر، تستخدم عالمات HTML لإنشاء الروابط، قد تكون هذه الروابط بأي شكل مثل النص أو الصور، تم تصميم HTTP وفقًا لمبادئ خادم العميل والتي تسمح لنظام العميل بإنشاء اتصال بجهاز الخادم لتقديم طلب يقر الخادم بالطلب الذي بدأه العميل ويستجيب وفقًا لذلك.

8. بروتوكول نقل النص التشعبي الآمن (HTTPS)

بروتوكول HTTPS (Secure Protocol Transfer Text Hyper هو بروتوكول قياسي لتأمين الاتصال بين جهازي حاسوب، أحدهما يستخدم المتصفح والآخر لجلب البيانات من خادم الويب، يتم استخدام HTTP لنقل البيانات بين متصفح الويب لدى العميل (الطلب) وخادم الويب (الاستجابة) بتنسيق النص التشعبي، كما هو الحال في حالة HTTPS فيما عدا أن نقل البيانات يتم بتنسيق مشفر، لذلك يمكن القول أن https تمنع المتسللين من مشاهدة أو تعديل البيانات طوال عملية نقل الحزم.

9. بروتوكول Telnet

بروتوكول Telnet عبارة عن مجموعة من القواعد المصممة لربط نظام بآخر، عملية الاتصال هنا تسمى تسجيل الدخول عن بعد، النظام الذي يطلب الاتصال هو الحاسوب المحلي، والنظام الذي يقبل الاتصال هو الحاسوب البعيد.

10. بروتوكول غوفر Gopher

هو عبارة عن مجموعة من القواعد المطبقة للبحث والاسترجاع، وكذلك عرض المستندات من المواقع المعزولة كما يعمل Gopher ايضًا على مبدأ العميل / الخادم.

- **أولاً: مسميات الجرائم الإلكترونية وتصنيفها**

ونظرًا لتعدد وتنوع أنماط وصور الجرائم الإلكترونية فقد أسهم ذلك في ظهور مسميات لها تتناسب مع طبيعتها وشكلها والأدوات المستخدمة فيها مثل:

1. الجرائم الحاسوبية.
2. جرائم الإنترنت.
3. جرائم الاتصالات.
4. الجرائم الإلكترونية.
5. الجرائم المعلوماتية.
6. جرائم التقنية العالية.
7. الجريمة السيبرانية.
8. جرائم أصحاب الياقات البيضاء.

- **الجرائم ذات الصلة بالحاسوب:**

الجرائم المتعلقة بالتزوير والجرائم المتعلقة بالغش.

الجرائم المتعلقة بالمواد الإباحية عن الأطفال.

الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة.

ثانيا: تصنيف الجرائم الإلكترونية

قسم الفقهاء ودارسو الجرائم الإلكترونية إلى فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه تقسيم المعنى.

أولا: تصنيف الجرائم الإلكترونية حسب نوع المعلومات ومحل الجريمة وهي تنقسم إلى:

1- الجرائم الماسة بقيمة معلومات الحاسب وتنقسم إلى فئتين:

الفئة الأولى: الجرائم الواقعة على ذات المعلومات كإتلاف البيانات والمعلومات وإتلاف برامج الحاسب ذاتها بما في ذلك استخدام الفيروسات.

الفئة الثانية: الجرائم الواقعة على ما تمثله هذه المعلومات جرائم واقعة على الأموال والأصول كجرائم غش الحاسب التي تستهدف الحصول على المال أو جرائم الإتجار بالمعلومات وجرائم التلاعب بالمعلومات المخزنة داخل الحاسب واستخدامها دون وجه حق كتزوير المعالجة الآلية واستخدامها.

2- الجرائم الماسة بالمعلومات الشخصية والبيانات المتصلة بالحياة الخاصة

تشمل هذه الفئة الهجوم على المعلومات والبيانات المتعلقة بالحياة الخاصة وتُعد هذه الجرائم من أخطر الصور ألنها تحتوي على استغلال المعلومات المخزنة في الحاسب في أمور غير مشروعة، وقد تأخذ هذه الجرائم صورة أو تسجل المحادثات الخاصة في وسائط الاتصال وتتنصت عليها واستغلالها في التشهير ألن معظم الأفراد تكون بياناتهم مُخزنة في المؤسسات وسرقتها تُعد من الجرائم التي تمس الحياة الخاصة ولا يشترط القانون في بعض الدول أن تكون هذه البيانات حقيقية.

3- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسب ونظمه

تشمل نسخ وتقليد البرامج وإعادة إنتاجها دون ترخيص وتتميز عن باقي الفئات بأنها محلها هو البرامج فقط والاستخدام غير المشروع لها.

ثانيا: تصنيف الجرائم الإلكترونية حسب دور الحاسب الآلي في الجريمة

وتنقسم إلى:

1- جرائم التخزين: يقصد بها تخزين المواد المستخدمة في ارتكاب الجريمة

2- جرائم المحتوى: حيث أصبح المحتوى غير القانوني يرمز إلى جرائم متعلقة بأفعال غير أخلاقية.

ثالثا: تصنيف الجرائم الإلكترونية حسب مساسها بالأفراد والأموال وتنقسم إلى:

1– جرائم تستهدف الأفراد مثل الملاحقة عبر الوسائل الإلكترونية، نشر المعلومات المزيفة / التسبب بالوفاة وأنشطة البريد الإلكتروني غير المرغوب فيه.

2– جرائم تستهدف الأموال أي الاقتحام أو الدخول غير المصرح به خلال شبكة المعلومات.

3– جرائم الاحتيال والسرقة مثل استخدام البطاقات الائتمانية بعد سرقة أرقامها.

4– جرائم التزوير مثل تزوير البريد الإلكتروني الخاص بالفرد أو مؤسسة معينة أو تزوير للوثائق والسجلات وتزوير الهوية.

رابعا: التصنيف حسب التنفيذ

- فردي– جماعي

يكون المجرم فردًا وبدوافعه الشخصية ايضًا يقوم بمهاجمة أو التعرض لمجموعة أفراد في نفس الوقت كأن يهاجم منظمة أو مؤسسة أو شركة وذلك بهدف الانتقام أو التشهير أو ألي سبب كان.

- جماعي – فردي

يكون المهاجمون جماعة تتكون من أكثر من فرد يقومون بأعمال تخريبية أو تجسسية أو أي نوع من أنواع الجرائم المعلوماتية ويكون الهدف بالنسبة لها فردًا واحدًا كأن يقوموا جميعًا بإرسال رسائل متكررة إلى بريد شخص بذاته أو التآمر للدخول على موقعه في نفس الوقت مما يسبب له الدمار والخراب.

- جماعي – جماعي

يقوم عدة أشخاص بمهاجمة موقع جهات ذات شخصيات اعتبارية كالمنظمات والهيئات والشركات وغيرهم بهدف القيام بأي عمل تخريبي أو التجسس على معلومات تلك المنظمات والهيئات.

خامسا: التصنيف حسب النوع

- التسلل والتجسس

يوجد فئة من الأفراد يحبون التجسس على الآخرين بطرق مختلفة من استرقاق السمع إلى تركيب أجهزة التصنت صوتية ومرئية إلى ابتكار طرق بأساليب حديثة للدخول بها إلى أجهزة الحاسب الآلي الخاصة

بالشخص المستهدف للحصول على أكبر معلومات ممكنة.

- الاتلاف والتدمير

استطاعة شخص ما الدخول إلى جهاز شخص أخر وإتلاف محتوياته وتدميرها وحذفها أو نقلها إلى مكان أخر داخل هذا الجهاز أو خارجه، حسب نوع تلك الوثائق وأهميتها التي ممكن أن يحصل عليها فهو يسعى

إلى معلومات مالية أو أسرار حربية للاستفادة منها أو تخريبها.

- التغيير والتزوير

يقوم بها شخص له أهداف مريبة، أتاحت له الفرصة لتغيير الحقائق والوثائق وتواريخ المستندات الموجودة على ذلك الجهاز وتغيير البيانات والصور والأشخاص الموجودين في هذه الصور لاستخدامها ألهداف

التشهير وتشويه السمعة وبالمثل ملفات الفيديو.

- الخداع والتغرير

بسبب تطور التقنية والبرامج الحاسوبية التي أسيء استخدامها من قبل ضعاف النفوس حيث إنه باستخدام البرامج الاحترافية يستطيع الشخص الحصول على صور محسنة غير الصور الحقيقية وإخفاء العيوب منها ومن مظاهر الخداع هو تقمص شخصية غير الشخصية الأساسية وخاصةً بعض البرامج تغير الصوت.

- **مزايا الإنترنت وعلاقتها بالجرائم الإلكترونية**

لقد وفرت السهولة النسبية الاستخدام التقنية الجديدة و الحصول على الإنترنت على نحو متزايد أكثر عن طريق الاشتراك بأسعار معقولة و الحصول على أجهزة الحاسب مع أجهزة المودم فائقة السرعة كل ذلك يمكن الأفراد من التواصل و تكوين الصداقات الجديدة و التجارة و الترفيه و التعليم و القيام بأعمال تجارية و دفع الفواتير عبر الإنترنت و كونت شبكة ويب عالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني و الذي يعرف بأنه ً مكان لأجل غير مسمى حيث يتفاعل الأفراد و المجتمعات مما أتاح الكثير من الأفراد الانتقال من العالم الواقعي إلى العالم الافتراضي مما أدى إلى ظهور الجريمة فهي ظاهرة اجتماعية يحاول المجرمون اليوم الاستفادة من تكنولوجيا المعلومات و الاتصالات في ارتكاب الجريمة و لهذا ظهرت أنماط جديدة من الجرائم لم تكن موجودة من قبل تتسم بصعوبة اكتشافها و ملاحقتها ،حيث أنه رغم الفوائد المتعددة للحكومة و الإدارة الإلكترونية إلا انه في نفس الوقت تزايدت أساليب إساءة الاستخدام لمكوناتها و أصبح الحاسب الآلي بشكل عام و شبكة الإنترنت بشكل خاص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث و مكنت مجرمي الفضاء الإلكتروني تصفح الإنترنت و ارتكاب جرائم القرصنة و الاحتيال و التخريب و غسيل الأموال و ما هو يتسبب في مشاكل قانونية و اجتماعية و اقتصادية و أمنيهما يستدعى بالضرورة إصدار قوانين خاصة بالجريمة

الإلكترونية و يتوافق مع خصوصياتها و تضمن أمن المعلومات الإلكترونية داخل المنظمات و خارجها و للأفراد و حماية خصوصيتهم

- دور الحاسب في الجرائم الإلكترونية

- يؤدي الحاسب والتقنية المعلوماتية دورًا مهما في الجريمة الإلكترونية فقد يكون هدف إجرامي يستهدف البيانات المعالجة أو المخزنة أو المتبادلة بواسطة الأجهزة التقنية والشبكات وقد يكون الحاسب وغيره من التقنيات الإلكترونية وسيلة ارتكاب جريمة أخرى أي هو بيئة للجريمة.

- يكون الحاسب الآلي هو الوسيلة للتسهيل للنتيجة الإجرامية باستخدام النظام المعلوماتي ويكون الهدف من ورائها القيام بطريق غير مشروع بالاستيلاء على الأموال واختراق خصوصية الأفراد وأمن الدولة.

تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظم المعلوماتية والمعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

1–الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد به الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله والقيام بسرقة هذه المعدات أو عن طريق الاتلاف المتعمد لها.

2 –الجرائم الواقعة على برمجيات النظام المعلوماتي:

يقوم بها مجرم محترف البرمجة وتقع هذه الجرائم على البرامج التطبيقية ونظم التشغيل. المعلومات المعالجة هي أساس عمل أي نظام معلوماتي لأنها ذات قيمة معرفية واقتصادية لذلك تُعد هدفًا للجرائم الإلكترونية من خلال تعديلها أو سرقتها أو إتلافها.

الفصل الثالث
مخاطر الجرائم الإلكترونية

- أسباب الجرائم الإلكترونية

1 –الحصول على الشهرة.

2–تضييع أوقات الفراغ وحب الاستطلاع من الشباب الهواة.

3 –استغلال الأشخاص لمصالح شخصية نابعة عن سلوك عدواني من داخل المجرم نتيجة مؤثرات خارجية قد تكون من الماضي او بسبب سوء التربية منذ الصغر.

4–سهولة ارتكاب الجرائم المعلوماتية مما يؤدي الى زيادة نسبة ارتكابها في المجتمع

- العوامل التي ساعدت على انتشار الجرائم الإلكترونية

المجرم الإلكتروني هو شخص يختلف عن المجرم العادي فهو مُلم للتقنيات الحديثة الإلكترونية وساعد على انتشار الجرائم ما يلي :

- انفتاح شبكة المعلوماتية فهي فضاء مفتوح على مصراعيه ال يخضع للرقابة والملكية الأمر الذي سهل عمليات التسلل إليه واختراقه.
- انعدام الحواجز الجغرافية.
- صعوبة الكشف عن هوية المستخدم إذ يمكن ألي شخص انتحال شخصية أو التخفي وراء إنسان وهمي.
- سهولة التعامل مع الوسائل التكنولوجية وزهد أثمانها.
- صعوبة التحقق وإثبات الجرائم.
- الثغرات القانونية بين مختلف الدول فما هو صارم في نظام ما مخفف في نظام أخر مما يتيح الفرصة للمجرمين سرعة التكيف وانتقال من نقطة جغرافية لأخرى أكثر أمانًا
- إشكالية الاختصاص القضائي والقوانين الواجب تطبيقها.
- مرتكبو الجرائم الإلكترونية

- القراصنة الهواة: يقصد بهم الأشخاص الذي يستهدفون المعلومات والحسابات الآلية ويكونون من فئة الشباب البالغين ومعظمهم يكون من الطلبة. وبالتالي يقومون هؤلاء الأشخاص بالدخول إلى أنظمة الحاسب الآلي بطرق غير مصرّح لهم الدخول إليها، فَهُم بذلك يكسرون الحواجز الأمنية لأغراض عدّة منها الخبرة أو حتى الفضول.
- القراصنة المحترفين: يقصد بهم الأشخاص التي تكون أعمارهم محصورة ما بين 45–25 سنة بحيث يحتلّون مكانة في المجتمع الجرائمي بالإضافة إلى اختصاصهم في مجال التقنية الإلكترونية؛بحيث يتسمون بالخطورة وتكرارهم للجرائم مرة أخرى.
- طائفة الحاقدين: يقصد بهم الأشخاص المنتقمون فمعظمهم يكونون ضد أصحاب العمل والمنشآت التي عملوا بها فهم يسعون إلى الانتقام من المدراء في العمل، بالإضافة إلى أنَّ هذه الطائفة تكون أقل خطورة مقارنة بغيرها من الطوائف. يكمن الهدف وراء هذه الطائفة هو التعمد في إخفاء وإنكار الأفعال والأنشطة، التي يقومون بها مستخدمين تقنيات متخصصة في زراعة

الفيروسات والبرامج المضرّة؛ بهدف تخريب الأنظمة المعلوماتية، حيث إنَّ هذه الطائفة ال تهدف إلى إثبات قدراتهم ومهاراتهم الفنية وال ايضًا يهدفون إلى تحقيق مكاسب مادية، أو حتى سياسية.

- طائفة الفكريين: فهم عبارة عن أشخاص يستعملون شبكة الإنترنت في نشر، بث، استقبال، إنشاء المواقع التي من شأنها تسهّل عملية الانتقال والترويج لكافة المواد الفكرية التي تساهم في تغذية الطرف الفكري. وقد يقوم المفكرين باستعمال الشبكات العالمية الإخبارية وكافة المواقع الإلكترونية بهدف تحقيق أغراض دعائية تحقق مصالحهم.
- طائفة المتجسسين : يقصد بهم الأشخاص الذي يسعون إلى التخريب أو إ تالف المحتويات الشبكية، التي تشكّل خطرًا كبيرًا، مثل إرسال أسرار العمل في إحدى الشركات عبر الإنترنت ومواقع التواصل الاجتماعي إلى الشركات المنافسة، فهي تهدف في المقام الأول على الحصول على قاعدة بيانات معلوماتية عن الاعداء والاصدقاء.
- طائفة مخترقي الأنظمة: هؤلاء الأشخاص يقومون بتبادل المعلومات فيما بينهم؛ بهدف معرفة نقاط الضعف في الأنظمة المعلوماتية مستعملين بذلك النشرات الإعلامية الإلكترونية؛ من مثل مجموعات الأخبار وبالتالي يقومون هؤلاء الأشخاص بعقد وتولي المؤتمرات لجميع مخترقي الأنظمة المعلوماتية، مع أهمية وجود خبراء وذلك بهدف المشاركة والتشاور حول وسائل الاختراق وآلياتها.
- **أشكال الجرائم الإلكترونية ومخاطرها**

أبرز أشكال الجرائم الإلكترونية التي مخاطرها تتسبب في ضرر تلحقه على المجتمعات والأفراد والأنظمة المالية والمصرفية والعسكرية هي:

1 –الجرائم الإلكترونية التي تستهدف الأموال:

منها أو المؤسسات التجارية و الصناعية ظهرت جرائم تستهدف هذه المراكز الدخول التكنولوجيا الرقمية و التقنية و المعلوماتية عالم المال و الأعمال من المعاملات البنكية ،الشخصية لمالية لتحقيق مكاسب مادية و الاستيلاء على الأموال بشقيها المادي النقدي أو المعلوماتي و ذلك بتزوير بطاقات الائتمان و الشيكات الإلكترونية أو عن طريق قرصنة الحوالات المالية و سرقة صرفات السحب الآلي التابعة للمؤسسات المالية و المصرفية أو عن طريق مهاجمة البيانات المعلوماتية للبنوك و الأنظمة المصرفية بقصد سرقة الأموال و الاستيلاء عليها أو عن طريق النصب و الاختلاس و الاحتيال الإلكتروني

2 –الجرائم الإلكترونية التي تستهدف المجتمعات:

تطورت الجرائم الإلكترونية لتشمل قطاعات واسعة حيث إن الفضاء الإلكتروني والشبكة العالمية أصبحت في متناول الجميع ولم تعد محصورة على مجتمع دون أخر وبالتالي انتشرت الجرائم الإلكترونية التي استهدفت إفساد المجتمعات في أخلاقياتها ودينها وسلوكياتها وعاداتها

وتقاليدها وترتب عليها آثار اجتماعية سيئة مثل تضليل الرأي العام وبث سموم الكراهية في المجتمعات كازدراء العقائد، والأديان، والتفرقة، والعنصرية.

3–الجرائم الإلكترونية التي تستهدف الأفراد:

تعاني المجتمعات الإلكترونية في الفترة الأخيرة من اختراق الخصوصية الإلكترونية وذلك في ظل انتشار الجريمة الإلكترونية الأمر الذي دفع الدول إلى العمل للحد من هذه الجرائم التي تلحق الضرر بالأفراد مثل جرائم السب والتحقير التي تُصل الأشخاص عبر شبكة الإنترنت واختراق البيانات الشخصية للأفراد والابتزاز وانتحال الشخصيات في مواقع التواصل الاجتماعي، والمواقع الإلكترونية، والتشهير، والتهديد.

4–الجرائم الإلكترونية التي تستهدف الملكية الفكرية:

تُشير الملكية الفكرية بمفهومها الشامل على أنها إبداعات العقل من اختراعات و مصنفات أدبية و فنية و تصاميم و شعارات و أسماء و صور مستخدمة في التجارة و الملكية الفكرية محمية قانونًا مثل البراءات و حق المؤلف و العلامات التجارية التي تمكن الأشخاص من كسب الاعتراف أو فائدة مالية من ابتكارهم أو اختراعاتهم و بالتالي فإن الملكية الفكرية تم استهدافها من قبل الجرائم الإلكترونية و يتم ذلك بقيام الجاني بالاستحواذ على تلك الملكية و الاستيلاء عليها و الاستفادة منها و التصرف فيها و حرمان المالك من الفائدة المالية و المنفعة التي تأتي من وراء تلك الملكية .

5–الجرائم الإلكترونية التي تستهدف الأمن القومي للدول:

التطور التكنولوجي فقد ارتبطت مصالح الدول الحيوية بتقنية المعلومات و أصبح الفضاء الإلكتروني الشريان النابض لإدارة شؤون الدول في شتى المجالات سواء في النظام الصحي أو العلمي أو الاقتصادي أو العسكري أو الخدمي ظهر نوع جديد من الجرائم الإلكترونية على هيئة هجوم رقمي إلكتروني أصبح يهدد أمن و استقرار الدول من خلال استهداف النظام المعلوماتي و مهاجمة المصالح الحيوية للدول مثل اختراق الأنظمة العسكرية و التجسس الإلكتروني عليها وتخريبها بنشر الفيروسات و تشويه الصورة الذهنية للمواطنين يشير إلى أنها أي نزاع يحدث في الفضاء الإلكتروني عبر تقنية المعلومات و يكون له طابع دولي وبالتالي فإن الشبكة المعلوماتية العالمية ساحات تُشن فيها الحروب و تتصارع الدول فيما بينها أو مع منظمات إرهابية على قدر عالي من التدريب و التأهيل أو حتى مع مجموعة صغيرة محترفة أو شخص من المخترقين.

- **جرائم الهواتف الذكية**

فالهواتف الذكية تمثل المفهوم الحقيقي للتطور الحادث في ثورة الاتصالات والمعلومات، فتزايد استخدامها ينبأ عن تفضيلها عن باقي أجهزة التقنية الأخرى كالحاسبات الآلية والكاميرا الرقمية والراديو وإلى غير ذلك من أجهزة تقنية أخرى، ومع ذلك رافق ازدياد الإقبال على هذه الأجهزة، ازدياد

مطرد في سوء استخدامها، حيث استغل البعض ما لدى الهاتف المحمول من قدرات وإمكانيات يمكن تطويعها في خدمة الجريمة، كالكاميرا الرقمية المدمجة وتقنية البلوتوث وخدمة الرسائل النصية والمصورة، هذا فضلاً عن إمكانية ارتباطها بشبكة الإنترنت التي أعطت فعالية أكبر الارتكاب الجريمة عبر هذه الهواتف الذكية وما تتضمنه من تقنيات عالية تتيح التصوير والتسجيل والبث والنشر والتواصل وغيرها، إلى أداة جريمة يمثل بعد ثبوتها الأفراد أمام القانون ليواجهوا عقوبات رادعة، نتيجة الاستخدام السيئ غير المسؤول أو المقبول اجتماعيًا ودينيًا، فالتقنيات سهلة الاستخدام الموجودة في الهواتف الذكية، سهلت عملية اختراق الخصوصية ، حيث إنه خلال ثوانٍ معدودة تتم عملية التصوير والبث والنشر دون علم الشخص أو بعلمه، كما أدى الأمر نفسه إلى اندفاع الأفراد نحو تصوير الوقائع والأحداث والتسابق في نشرها دون شعور بالمسؤولية أو إدراك بمدى تأثير ذلك الفعل في المجتمع، ليجد الشخص نفسه أحيانًا وقد اخترق خصوصية الآخرين، ويواجه العقوبات المترتبة على ذلك الجرم الذي سنت له الدولة قوانين صارمة ورادعة، تتمثل في القانون الخاص بالجرائم الإلكترونية الذي يتضمن عقوبات مغلظة وذلك للحد من استخدام الهواتف الذكية بشكل يسيء للأخرين و للمجتمع ، وايضًا للحفاظ على خصوصيات الآخرين.

- **الفضاء الإلكتروني**

هو ما يوصف بتدفق البيانات الرقمية من خلال شبكة من أجهزة الحاسب المتصلة لان الفرد لا يمكنه تحديد موقعه مكانيًا ككائن ملموس ولا تظهر آثاره بشكل واضح مثلما تظهر في العالم الحقيقي ويمكن اعتبار الفضاء الإلكتروني واجهة جديدة للمجتمعات نظرًا لاحتوائه على خلفيات جديدة تعمل على إعادة تشكيل المجتمع و الثقافة من خلال الهويات الخفية لمستخدميه، أي يمكن وصفه بأنه عالم افتراضي يتشابك مع العالم المادي يتأثر به ويؤثر فيه بشكل مُعقد حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف .

- **جرائم الفضاء الإلكترونية**

جرائم الفضاء الإلكتروني التي يتعرض لها الفرد

سرقة الهوية الشخصية.

• سرقة بطاقة الائتمان الخاصة به.

• الابتزاز والتهديد.

- عمليات الاحتيال.
- تحويل أو نقل حسابه المصرفي.
- نقل ملكية الأسهم.
- زيادة الفواتير بتحويل فواتير المجرم للضحية.

- **الجرائم الإلكترونية التي تتعرض لها البنوك**

- السطو الإلكتروني.
- تعطيل النظام.
- التلاعب بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها.
- نقل ملكية الأسهم.
- اختراق الموقع الخاص بالبنك.

- **جرائم الفضاء الإلكتروني التي قد تتعرض لها المنظمات والمؤسسات**

- الاطلاع على معلومات سرية والاستفادة منها.
- التلاعب بمخازن المعلومات الخاصة بالمنظمة، أو المؤسسة بحذفها، أو تعديلها، أو تعطيل الوصول إليها.
- الابتزاز والتهديد.
- اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة.

- **جرائم الفضاء الإلكتروني التي قد تتعرض لها الجهات والأجهزة الحكومية**

- الوصول إلى المعلومات سرية والاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.
- دعم الإرهاب والأفكار المتطرفة ونشر الشائعات.
- تعطيل الإنترنت بالكامل.
- تعطيل وتخريب الخوادم الموفرة للمعلومات.

- **الجريمة الفضائية الاقتصادية**

قد نتج عن الثورة التكنولوجية ظهور نوع جديد من المعاملات الإلكترونية يسمى المعاملات الإلكترونية هذه المعاملات فقد سمحت المعلوماتية والأنترنت في تداول الأنشطة التجارية عبر الشبكة مما أتاح للأنشطة الإجرامية تحقيق عوائد مالية عن طريق وسائل غير مشروعة ناتجة عن عمليات التزوير والاحتيال. تتم عملية التحويل الإلكتروني للأموال بشكل غير مشروع من خلال التحايل

و ذلك بالحصول على رقم كلمة السر من جهاز حاسب محتال عليه أو عن طريق انتحال شخصية وهمية و إيهام المحتال عليه بوجود مشروع مربح و بالتالي يتم تحويل الإلكتروني للأموال لصالح المحتال كما يمكن أن يتم الاحتيال باستعمال بطاقات الائتمان و هي بطاقة بنكية للدفع أو السحب الإلكتروني تصدرها هيئات عالمية تسمح هذه البطاقات بعمليات البيع و الشراء عبر الإنترنت تحمل أرقامًا خاصة بكل عميل و تطور البرمجيات أصبح بالإمكان الاستيلاء على هذه الأرقام و الحصول على الأموال منها.

- **الوقاية من الجريمة الإلكترونية يتطلب الآتي:**

– استخدام كلمات مرور ال يمكن الوصول إليها.
– استخدام مضادات للفيروسات.
– التحديث المستمر لبرامج مكافحة التجسس.
– ضبط التعامل مع وسائل التواصل الاجتماعي.
– تحديث منظم التشغيل للحاسوب بصورة خاصة منعًا للاختراق أو التجسس.
– إيجاد أقصى درجات الحماية للبيانات.
– تأمين الشبكة اللاسلكية Fi-Wi وتحديث الإعدادات الخاصة بها مع تجنب إجراء المعاملات المالية عليها.
– حماية البيانات المتعلقة بالبريد الإلكتروني في مجالات استخدام المعاملات المالية وغيرها.
– تجنب الأخطاء الناتجة عن عدم معرفة التعامل مع الحاسوب.
– الاتصال بالجهات الرسمية عند وقوع المستخدم ضحية لتجسس أو اختراق.

الفصل الرابع
أبعاد وأثار الجرائم الإلكترونية

- **أبعاد وأثار الجرائم الإلكترونية عربيًا وعالميًا**

أولاً: الأبعاد الاقتصادية للجريمة الإلكترونية وأثارها

- إن التحول الاقتصادي العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي وتحول التعاملات التجارية والمالية إلى الشكل الإلكتروني زاد من خطورة الجريمة الإلكترونية والتي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة القادمة نتيجة تزايد عدد الشركات التي تعتمد على الإنترنت في ممارسة نشاطها.

- وبحسب تقدير Thornton Grant يعتبر القطاع المالي الأكثر عرضة للهجمات بنسبة 46 يليه قطاع الرعاية الصحية بنسبة 24 ثم قطاع الطاقة بنسبة 23.

- وتُعد منطقة الشرق الأوسط من بين الأكثر تضررا في العالم من الهجمات الإلكترونية بحسب تقرير أصدرته PWC وأظهر أن 56 من شركات المنطقة تعرضت لهجوم إلكتروني خسرت 500 ألف دولار.

- مع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد، بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلبي على الاقتصاد.

- **الخسائر المالية للجريمة الإلكترونية**

وبحسب تقرير أعدته شركة مكافئ المتخصصة في حماية أمن المعلومات فإن الجريمة الإلكترونية تجارة مربحة منخفضة التكلفة قليلة المخاطر تدر أرباحًا طائلة تزيد على إجمالي الدخل القومي للكثير من الدول ولا تقتصر خسائر الجريمة الإلكترونية فقط على الخسائر المباشرة و إنما تشمل ايضًا الخسائر غير المباشرة مثل حقوق الملكية الفكرية و سرقة الأصول المالية و المعلومات التجارية المهمة و تكلفة استعادة البيانات و تكلفة الفرص البديلة و لا يمكن تجاهل تأثير الجريمة الإلكترونية على الاقتصاد الوطني و على أداء الشركات و على حركة التجارة العالمية و على القدرة التنافسية و الابتكار.

ثانيا: الأبعاد الاجتماعية للجريمة الإلكترونية وأثارها

- وأهم التأثيرات السلبية للجرائم الإلكترونية تدمير الحاسب الخاص بالضحية ثم إلحاق آثار نفسية وعقلية بالضحية يليها إلحاق خسائر مادية له.

- وأشكال جرائم وسائل التواصل الاجتماعي تتمثل في التنمر والمطاردة وسرقة الهوية ونشر مقاطع الفيديو، والحيل، والسرقات، والاحتيال.

- **ثالثا: الأبعاد المادية للجريمة الإلكترونية وأثارها**

- خسائر مالية:

- الهجوم الإلكتروني له تأثيرات، ولكن بعيدة المدي ومنها سرقة الملكية الفكرية والخسائر المالية، وفقدان ثقة المستخدم وعند تحديد الأثر المادي الإجمالي للجريمة الإلكترونية على الحكومة والمجتمع يقدر بعدة مليارات الدولارات كل سنة وبعض المجرمون يستفيدوا من التكنولوجيا بطرق عديدة ومختلفة وخصوصًا الإنترنت، لأنها وسيلة يستخدمها المحتالين لكي يمارسوا التجارة الخاصة بهم عندما يقوموا بالتخفي وراء درع الخفاء الهوية الرقمية لهم.

عندما يقع شخص ضحية الجريمة الإلكترونية يكون لها آثار على مدى طويل على الحياة والتصيد الاحتيالي من الأساليب المنتشر استخدامها من قبل المحتالون، ومنها إرسال رسالة مزيفة عبر البريد الإلكتروني على أنها واردة من مؤسسة مالية أو بنك تريد منه معلومات شخصية. وعندما يقوم الشخص بإرسال تلك المعلومات يقوم المجرم بالوصول لحسابات الائتمانية والمصرفية، وتقوم بتدمير التصنيف الائتماني وفتح حسابات جديدة.

- تكاليف الأمن:

مجرمون الإنترنت يقوموا بالتركيز في هجماتهم على كال من الشركات الصغيرة والكبيرة فيقومون بالاستيلاء على الخوادم لهذه الشركات والقيام بسرقة المعلومات الخاصة بها أو يقومون باستخدام أجهزة لتساعدهم في أغراضهم الخاصة. ولهذا تقوم بعض الشركات تعيين موظفين واستخدام تحديث للبرامج التي تقوم بحمايتهم من الاختراقات تم إيجاد دراسة استقصائية للشركات الكبيرة توضح متوسط الإنفاق على الأمن السيبراني وهو حوالي 9.8 مليون دولار سنويا.

متطلبات الأمن السيبراني ودوافع اهتمام الدول به:

1. متطلبات الأمن السيبراني:

- تعريف الإطار القانوني المناسب لتعزيز الصمود السيبراني ومرونته ضد الهجمات وتطوير آليات فعالة للتشفير، ورفع مستوى وعي المجتمع العالمي بالأمن السيبراني وتعزيز التواصل معه.
- تعزيز الثقافة الأمنية الوطنية واعتبار أمن الخدمات جزء لا يتجزأ من الخدمات التي تقدمها الدولة للمواطن.
- الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف على هوية مُرتكبي الجريمة والاستدلال عليه بأقل وقت ممكن.
- رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت ويستلزم التدخل الحكومي والدولي نظرا للخطورة الجسيمة للأمر.
- توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.
- مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

2. دوافع اهتمام الدول بالأمن السيبراني:

حماية العالم السيبراني هي حماية للعالم الفعلي، فليس العالم السيبراني سوى وسيلة من وسائل العالم الفعلي غايتها جعله أكثر فاعلية في أداء الأعمال والنشاطات المختلفة، سواء ما يرتبط منها بشؤون الخدمات الحكومية، أو الأعمال المهنية، أو النشاطات الاجتماعية، وليس ذلك في إطار محدود الأبعاد، بل على مستوى العالم بأسره، وعلى هذا الأساس، فإن أمن العالم السيبراني جزء مهم لا يتجزأ عن أمن العالم الفعلي، وهو بذلك يرتبط بأربع دوائر رئيسة، هي:

1. الدائرة الشخصية أي دائرة الفرد وسلوكه والتزاماته.
2. دائرة المؤسسات وسعيها إلى حماية ذاتها وتعاملاتها مع الآخرين،
3. دائرة الدولة المهتمة بخدمة الأمة وحمايتها.
4. دائرة العالم بأسره المعنية بالتعاون الدولي والعمل المشترك لحماية العالم بأسره

الإنسان هو العنصر الحي في جميع هذه الدوائر، وهو المحرك لها، تبعا لموقعه فيها وليست هذه الدوائر منفصلة عن بعضها بعضًا، بل هي متداخلة، وأي خلل أو مشكلات أمنية تقع في إطار أي منها، أثرها واقعًا بدرجات مختلفة على الجميع، وعلى ذلك، فإن حماية الأمن السيبراني مسؤولية تقع على عاتق الجميع .

جهود الدول في مجال الأمن السيبراني وطرق مكافحة الجرائم الإلكترونية :

أثبت الواقع العملي أن كل دولة لا تستطيع بجهودها المنفردة القضاء على الجرائم الإلكترونية مع هذا التطور الملموس في كافة المجالات الذي أدى إلى الانتشار الواسع والمتزايد لها و نظرًا لخطورتها و زيادة انتشارها على الصعيد الدولي ووجود قصور في التشريعات الوطنية في مكافحتها الأمر الذي تطلب جهود موحدة لمكافحتها و لذلك أصبحت هناك احتياج لوجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله الأجهزة المختلفة في الدول خاصةً فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة و المجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الهاربين من وجه العدالة و لتخطي الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين و تعقب مصادر التهديد سواء كانت مساعدة متبادلة قانونيًا أو قضائية أو شرطية و سواء اقتصرت على دولتين فقط أو امتدت إقليميًا أو عالميًا .

جهود الدول في مجال الأمن السيبراني وطرق مكافحة الجرائم الإلكترونية :

في إطار الجهود المبذولة قام المجلس الأوربي بالشراكة مع الولايات المتحدة واليابان، وغيرهم من الدول بالتصديق على اتفاقية مكافحة الجرائم السيبرانية عام 2004 ،والتي لا تزال التشريع الدولي الوحيد الملزم الذي يتناول مسألة الجرائم السيبرانية.

وترجع أصول هذه الاتفاقية إلى نوفمبر 1996، عندما أوصت اللجنة الأوربية المعنية بمشكلات الجرائم، بأن يشكل المجلس الأوربي لجنة من المختصين بالجرائم السيبرانية، ومنذ البداية، أقرت اللجنة الأوربية المعنية بمشكلات الجرائم بطبيعة جرائم الفضاء السيبراني، في أنها حينما ترتكب خلال الإنترنت الاختصاص الإقليمي للسلطات الوطنية لإنفاذ القانون، ومن ثم كان هناك جهد دولي منسق للتعامل مع مثل هذه الجرائم، ولا يمكن ذلك إلا من خلال أداة دولية ملزمة تضمن الفعالية اللازمة لمكافحة هذه الظواهر الجديدة. وتُعرف اتفاقية المجلس الأوربي الخاصة بمكافحة الجرائم السيبرانية **باسم اتفاقية بودابست**

وتتناول تلك الاتفاقية **تحديد مفهوم الجرائم السيبرانية، بالإضافة إلى المخالفات التي ترتكب ضد الأنظمة الحاسوبية، وعن طريقها ، وقد تم إنشاء تلك الاتفاقية ردًا على التهديد العالمي للجرائم السيبرانية، فهي تعتبر الأداة الدولية القانونية الوحيدة الملزمة للتعامل مع الجرائم السيبرانية،**

تحتوي اتفاقية بودابست على أربعة فصول:

الفصل الأول: يشتمل على استخدام المصطلحات.

الفصل الثاني: على الإجراءات التي يتم اتخاذها على المستوى الدولي.

الفصل الثالث: على التعاون الدولي.

الفصل الرابع: فيشمل الأحكام النهائية للاتفاقية

- **وفيما يتعلق بالقوانين الموضوعية قسمت الاتفاقية الجرائم السيبرانية إلى أربع أنواع:**

1. الجرائم ضد السرية ونزاهة وتوافر البيانات والأنظمة الحاسوبية، مثل الدخول غير القانوني إلى نظام حاسوبي واعتراض نقل البيانات غير العمومية إلى نظام حاسوبي أو منه أو داخله، وعرقلة البيانات أو الأنظمة الحاسوبية مثل تخريب الحاسوب أو إساءة استخدام الأجهزة المرتبطة به(مثل أدوات القرصنة).

2. الجرائم المتعلقة بالحاسوب، والتي تشمل الجرائم التقليدية المتمثلة في الاحتيال والتزوير، عند تنفيذها من خلال نظام الحاسوب.

3. الجرائم ذات الصلة بالمحتوى.

4. الجرائم المتعلقة بانتهاك حقوق التأليف والنشر وحقوق.

- **وإدراكًا للتحديات العالمية للجريمة السيبرانية، وخاصة إمكانية تأثيرها على العالم النامي، يعتمد مكتب الأمم المتحدة المعني بالجريمة منهجا قائم على ما يلي:**

1. زيادة التشريعات ووضع برامج تدريبية لموظفي إنفاذ القانون، ووكلاء النيابة، والسلطات القضائية بشأن تقنيات مكافحة الجرائم السيبرانية، ونهج العدالة الجنائية.

2. الأنشطة الوقائية ورفع الوعي، بما في ذلك التعاون المشترك بين مؤسسات إنفاذ القانون، والقطاع الخاص، من خلال زيادة الوعي العام بالجريمة السيبرانية.

3. زيادة التعاون الإقليمي والدولي من خلال زيادة التواصل والتنسيق خارج الحدود الوطنية.

4. جمع البيانات والبحث والتحليل بشأن الروابط بين الجريمة المنظمة والجريمة السيبرانية

جهود المملكة العربية السعودية في مجال الأمن السيبراني وطرق مكافحتها

1. خدمة ترشيح محتوى الإنترنت

بهدف حماية المجتمع السعودي من أخطار الإنترنت الضارة وضمان تقديم المحتوى الجيد تقوم هيئة الاتصالات وتقنية المعلومات بتقديم خدمة ترشيح محتوى الإنترنت في المملكة وذلك من خلال وضع الضوابط والمتطلبات الخاصة بترشيح خدمات الإنترنت بالتنسيق مع اللجنة الأمنية الدائمة للإنترنت كما توفر قوائم خاصة بالمواقع المحجوبة يوميًا لمزودي خدمة المعطيات ويتم حجب المواقع والمواد التي تتنافي مع الدين الحنيف والأنظمة الوطنية.

2. سياسة الخصوصية وسرية المعلومات للتعاملات البنكية الإلكترونية

يقوم كل قطاع بنكي بنشر سياسات الخصوصية والسرية على الموقع الرسمي للبنك ويقر البنك بحقوق العميل المتعلقة بسرية البيانات الشخصية التي يقدمها للبنك خلال أدائه المعاملات

المصرفية عبر الإنترنت والبنك ملتزم بتوفير مستوى عالي من الأمن والسرية ألي معلومات تتعلق بخدماته البنكية التي يقدمها للأفراد عبر الإنترنت ويضمن معالجة أي عملية مصرفية تتم عبر الإنترنت وأي معلومات شخصية أو مالية يتم تبادلها بمثل هذه الوسائل بطريقة مأمونة ومشفرة تلتزم بالمعايير الأمنية الخاصة بالصناعة.

3. جهود هيئة الاتصال السعودية

تولي هيئة الاتصالات وتقنية المعلومات اهتمامًا بالتثقيف بسالمة أمن المعلومات ونشر الوعي في المجتمع السعودي وخدمتهم في تقديم أحدث المستجدات في مجال تأمين المعلومات بجانب توفير معلومات شاملة وموسعة عن كل ما من له صلة بأمن المعلومات والتقنيات المرتبطة فيها وأسست الهيئة مركزًا وطنيًا يكون مقصدًا لكل من يحتاج إلى إرشادات أو معلومات أمنية عن أي نوع من التقنيات ذات الصلة بمهام هيئة الاتصالات وتقنية المعلومات وأطلق عليه المركز الوطني الإرشادي ألمن المعلومات.

هذا المركز الوطني هو مركز غير ربحي يهدف إلى رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات ويعمل بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية.

الأسئلة

1. بروتوكول من بروتوكولات الأنترنت يتصف بالموثوقية لأنه يوفر نقل آمن للرسائل:

pop	UDP	SMTP	TTR

2. مجموعة من القواعد المصممة لربط نظام بأخر:

Telnet	Gopher	Https	CSS

3. بروتوكول يقوم بنقل البيانات بين متصفح الويب(العميل) والخادم بشكل مشفر:

Https	Gopher	DDI	CSS

4. تعد جريمة اتلاف المعلومات وبرامج الحاسب ذاتها مثل استخدام الفيروسات من :

الجرائم الواقعة على ذات المعلومات	الجرائم الواقعة على ما تمثله هذه المعلومات	الجرائم الواقعة على برمجيات النظام	الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

5. تصنف الملاحقة عبر الرسائل الالكترونية ونشر المعلومات المزيفة من الجرائم الالكترونية التي تستهدف.....

الأفراد	الاموال	المنظمات	البنوك

6. يقصد بالجريمة التي يقوم بها مجرم محترف بالبرمجة وتقع هذه الجريمة على البرامج التطبيقية ونظم التشغيل بـ:

الجرائم الواقعة على المكونات المادية للنظام المعلوماتي	الجرائم الواقعة على برمجيات النظام المعلوماتي	الجرائم الواقعة على ذات المعلومات	الجرائم الواقعة على ما تمثله هذه المعلومات

7. / تصنف الجرائم التي يقوم بها شخص بالدخول الى جهاز شخص اخر واتلاف محتوياته وتدميرها من جرائم:

التسلل والتجسس	الاتلاف والتدمير	الخداع والتغرير	التغير والتزوير

8. من الجرائم الالكترونية التي تستهدف الأمن القومي للدول تشويه الصورة الذهنية للمواطنين تجاه بلدهم ليصل الى نشوب حرب الكترونية

صح	خطأ	-	-

9. مرتكبو الجرائم الالكترونية الذين يقومون بالدخول الى أنظمة الحاسب الالي بطرق غير مصرح لهم الدخول اليها هم:

القراصنة الهواة	طائفة الفكرين .	القراصنة المحترفين	طائفة الحاقدين .

10. الأشخاص الذين يسعون الى التخريب او اتلاف المحتويات الشبكية يقصد بهم:

طائفة الحاقدين	طائفة المتجسسين	طائفة الفكرين	القراصنة الهواة
11. من أمثلة الجرائم الالكترونية التي تستهدف..... قرصنة الحوالات المالية:			
الاموال	المجتمعات	الافراد	الملكية الفكرية
12. جرائم الكترونية تقوم ببث سموم الكراهية في المجتمعات مثل ازدراء العقائد والأديان والتفرقة العنصرية فتصنف من الجرائم الالكترونية التي تستهدف:			
المجتمعات	الافراد	الاموال	المنظمات
13. تعد جريمة الاطلاع على المعلومات السرية والاستفادة منها من جرائم:			
الفضاء الالكتروني التي تتعرض لها المنظمات والمؤسسات	لانعد جريمة ابدا	خسائر الاموال في سوق العقارات	خسائر الاموال في سوق الاسهم
14. للوقاية من الجريمة الالكترونية يتطلب:			
استخدام مضادات للفيروسات	تعطيل النظام	انتحال الشخصيات في مواقع التواصل الاجتماعي	عدم استخدام الأنظمة الرقمية
15. ارسال رسالة مزيفة عبر البريد الالكتروني على انها واردة من مؤسسة مالية او بنك تريد منه معلومات شخصية تعد هذه من الابعاد المادية التي تسبب			
خسارة الموارد	هجمات سبرانية	تكاليف الأمن	خسائر مالية
16. من متطلبات الأمن السيبراني			
توعية الأفراد ونصحهم لماهية الجرائم الالكترونية وكل ما يترتب عليها من مخاطر	حماية الأطفال	التشهير في مواقع التواصل الاجتماعي	التحديث
17. مركز غير ربحي يهدف الى رفع الوعي والمعرفة بأخطار أمن المعلومات			
مركز قياس	المركز الوطني الارشادي لأمن المعلومات	الهيئة السعودية للبيانات والذكاء الاصطناعي	المركز الوطني للتعليم الالكتروني
18. من جهود المركز الوطني الارشادي التركيز على القضايا الطويلة والمتوسطة مثل الثغرات المكشوفة حديثا تعود هذه النقطة لعنصر			
الإعلانات	الاحتفالات	تقديم المشورة	الدراسات المكثفة
19. مجموعة من برامج وأدوات معدة لمعالجة البيانات وادارتها وتشغيل الحاسبات الألية يقصد بهذا المصطلح			
النظام المعلوماتي	الشبكة المعلوماتية	برامج الحاسب الالي	الموقع الإلكتروني

20. مكان اتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد يقصد به			
الموقع الالكتروني	SoundCloud	النظام الجغرافي	القرص الصلب
21. عقوبة شخص ما قام بالاختلاس من الشركة التي يعمل بها بغرض الاستيلاء على هذه الأموال لنفسه تكون			
سجن لا يزيد عن 3 سنوات وغرامة لا تزيد عن 2 مليون	سجن لا يزيد عن 8 سنوات	غرامة لا تزيد عن 2 مليون	غرامة لا تزيد عن 12 مليون
22. تكون عقوبة انشاء مواقع على الشبكة العنكبوتية بغرض الاتجار بالجنس البشري			
سجن لا يزيد عن 18 سنه وغرامة لا تزيد عن 4 مليون	سجن لا يزيد عن 5 سنوات وغرامة لا تزيد عن 3 مليون	سجن لا يزيد عن 6 سنوات	غرامة لا تزيد عن 9 مليون
23. عقوبة انشاء مواقع لمنظمات إرهابية على الشبكة العنكبوتية			
سجن لا يزيد عن7 اشهروغرامة لا تزيد عن 100 الف	سجن لا يزيد عن 10 سنوات وغرامة لا تزيد عن 5 مليون	سجن لا يزيد عن 9 سنوات وغرامة لا تزيد عن 31 مليون	غرامة لا تزيد عن 8 مليون
24. هي كل نشاط إجرامي يتم ضد أو باستخدام الحواسيب الآلية والبرامج والتطبيقات المختلفة وشبكات المعلومات، خاصة شبكة الإنترنت			
الجرائم باستخدام السلاح الأبيض	الجرائم التقليدية	الجرائم الالكترونية	الجرائم المعلوماتية
25. تعتبر الجرائم الالكترونية التي تضر بذات المستخدم وشخصه مثل السب والقذف والتشهير من			
الجرائم التي تضر المستخدم بصورة مباشرة	الجرائم التي تضر المجرم بصورة غير مباشرة	الجرائم التي تضر المستخدم بصورة غير مباشرة	الجرائم التي تضر جهاز الحاسب
26. الركن الأول للجريمة الالكترونية هو			
الركن المادي	الركن القانوني	الركن غير المادي	الركن غير القانوني
27. هي العلاقة التي تربط بين السلوك الإجرامي والنتيجة الإجرامية وبانقطاع هذه الرابطة بين السلوك الإجرامي والنتيجة فإن الركن المادي للجريمة لا يتحقق			
السلوك الإجرامي	النتيجة الإجرامية	الرابطة السببية	السلوك المعنوي
28. يتكون الركن المعنوي من عنصرين هما:			
العلم والإرادة	الإرادة وسلاح الجريمة	العلم والركن المادي	الجريمة والإرادة

29. جميع النقاط التالية من خصائص الجرائم الإلكترونية ماعدا:			
جرائم عنيفة الأداء	جرائم متجددة دائمة التطور	جرائم صعبة الاثبات	جرائم مستحدثة
30. هم الأشخاص الذين يستخدمون مهارات الحاسب المتقدمة للهجوم على أجهزة حاسب أخرى، ولكن ليس لديهم أي نوايا خبيثة وإنما لكشف العيوب وتحسين الأمن المعلومات:			
المخترقون	القراصنة	المتجسسون	الارهابيون
31. هم أشخاص متخصصون ولديهم مهارات عالية غالبا ما يهددون البنية التحتية لأجهزة الحاسوب والشبكات ليسببوا الذعر والمهاجمة من أجل نشر أفكارهم ومبادئهم:			
المخترقون	القراصنة	المتجسسون	الارهابيون
32. يقتحمون أجهزة شركاتهم لعدة أسباب: إما عرض الضعف الموجود في نظام الشركة أو لأهداف مادية أو لسخطهم من الشركة وتهديدهم:			
الموظفين	القراصنة	المتجسسون	الأطفال او المراهقون المستهترون
33. جميع النقاط التالية من خصائص المجرم الإلكترونية ماعدا:			
لا يحب المخاطرة أبدًا	الذكاء والمعرفة التقنية	لديه نزعة اجرامية	الاحتراف
34. أصبحت الجرائم الإلكترونية تمثل خطراً كبيراً على			
الأفراد والمؤسسات وبياناتهم	الألعاب الافتراضية	العلوم الفيزيائية	علوم الطاقة
35. تسمى الجرائم الإلكترونية أيضا:			
الهجمات الالكترونية	غسيل الأموال	نزعات الكترونية	نظم رقمية
36. تعد الجريمة الالكترونية تجارة مربحة تدر ارباحا طائلة تزيد على اجمالي الدخل القومي للكثير من الدول			
منخفضة التكلفة قليلة المخاطر	مرتفعة التكلفة كثيرة المخاطر	منخفضة التكلفة كثيرة المخاطر	مرتفعة التكلفة قليلة المخاطر

ملخص لمقرر أمن شبكات الحاسب المتقدم

- **التشفير**

هو عملية أساسية في مجال أمان الشبكات، حيث يقوم بتحويل البيانات والمعلومات إلى صيغة مشفرة غير قابلة للقراءة، مما يضمن سرية هذه المعلومات ويمنع الوصول إليها من قبل الأشخاص ص غير المصرح لهم . يتم تنفيذ التشفير لتحقيق أمان عمليات التخزين والنقل للبيانات سواًء كانت داخل ملفات أو عبر الشبكات .

- **أهمية التشفير**

1 . حماية البيانات الحساسة: يمنع التشفير البيانات الحساسة من التعرض للتنصت أثناء النقل عبر الشبكات. على سبيل المثال، المعلومات الطبية للمرضى التي تنتقل بين المستشفيات وشركات التأمين تحتاج إلى تأمين قوي لمنع الوصول غير المصرح .

2 . منع التلاعب والتغيير : يقلل التشفير من احتمالية تغيير البيانات أثناء النقل. هذا يضمن سالمة البيانات ويمنع تلاع ب أطراف غير مصرح به ا

3 . الالتزام بالمتطلبات القانونية: في العديد من القطاعات مثل الصحة والمالية، يجب تحقيق معايير أمان صارمة للبيا نات. التشفير يساعد على الامتثال لهذه المتطلبات وتجنب العقوبات ت

4 . الحفاظ على السمعة: عندما يكون لدى المؤسسات معاملا ت تحتاج للحماية من التنصت، يسهم التشفير في الحفاظ على سمعتها وبناء الثقة بين العملاء ء والشركاء .

5 . الاحتفاظ بالخصوصية : التشفير يسهم في الحفاظ على خصوصية البيانات الشخصية والمعلومات الحساسة، مما يحمي الأفراد والمنظمات من الاختراقات والتسريبات.

- **الأجزاء الأساسية للتشفير :**

1 . الخوارزمية : تُعد الخوارزمية هي الاساسية في عملية التشفير، حيث تحدد كيفية تحويل البيانات إلى شكل مشفر وكيفية استعادتها بشكل صحيح .

2 . المفتاح: المفتاح السري يمثل عنصرًا أساسيًا، حيث يستخدم مع الخوارزمية لتشفير وفك تشفير البيانات . يجب حماية المفتاح بشكل جيد لمنع وصول الأفراد غير المصرح لهم .

استخدام الخوارزميات المعقدة: الخوارزميات المعقدة تعزز م ن أمان عمليا ت التشفير، حيث يصبح من الصعب للمهاجمين اختراقها بسهولة .

المفاتيح القوية: المفاتيح القوية المكونة من سلاسل بتات عشوائية تعزز من أمان العمليات التشفيرية وتحميه ا من الهجمات .

- **التشفير والبرمجيات والأجهزة :**

البرمجيات: تسمح البرمجيات بتنفيذ عمليات التشفير باستخدام واجهات سهلة للمستخدم. لكن يجب متابعة تحديثها لمنع الاختراقات.

الأجهزة : تستخدم الأجهزة المتخصصة لتحقيق التشفير بأمان أكبر وأداء أفضل، حيث تستفيد من الدوائر المتكاملة المخصصة .

- **خدمات التشفير وأبعادها:**

السرية : Confidentiality تعني أن الأطراف غير المصرح لها ا لا يمكنها الوصول إلى المعلومات. يتم تحقيق هذه السرية من خلال تشفير البيانات بحيث يكون الوصول إليها مقتصرًا على أولئك الذين يمتلكون المفتاح السري المناسب .

الأصالة : Authentication تُستخدم للتحقق من مصدر الرسالة للتأكد من أن المرسل هو من يدعي أنه، وتأكيد صحة هويته. هذا يمنع استقبال البيانات من مصادر غير معتمدة .

النزاهة : Integrity تضمن عدم تعديل البيانات أثناء عملية الإرسال، سواء بالخطأ أو بشكل متعمد، وبذلك تحافظ على سالمة البيانات ومصداقيتها .

عدم التنصل :Nonrepudiation تمنع المستلم من إنكار استلامه ا. تقدم الأدلة التي تمنع رفض المرسل إرساله للبيانات في وقت الحق، وكذلك ي تثبت إرسال واستلا م البيانات، بما في ذلك الهوية ووقت الإرسال .

- **أنواع التشفير:**

◦ هناك نوعان من خوارزميات التشفير :

1 . التشفير المتماثل : من حيث التكلفة يستخدم نفس المفتاح لتشفير وفك ◦ يتطلب تأمين تشفير البيانات، مما يجعله فعال تخ زين المفتاح .

2 . التشفير غير المتماثل : يستخدم مفتاحين مختلفين؛ مفتاحا عاما وآخر خاصًا. يستخدم المفتاح العام للتشفير والمفتاح الخاص لفك التشفير. أكثر فعالية ، ولكن أكثر تكلفة، يوفر أمانًا أكبر .

- **الشبكة الافتراضية الخاصة (VPN):**

هي نوع من الشبكات يتم إنشاؤها داخل الشبكة العامة مثل الإنترنت، تمكن الأجهزة من الاتصال بشبكات خاصة بشكل آمن من أماكن بعيدة

نوع الشبكة	الوصف
VPN Access	تتيح إمكانية الوصول عن بُعد للعاملين المتنقلين، ولمكاتب صغيرة أو منازل، إلى شبكة الإنترنت التابعة للمقر الرئيسي عبر بنية تحتية مشتركة. تستخدم شبكات VPN وسائل اتصال متنوعة وتقنيات الكابلات لتوصيل المستخدمين عن بُعد والمكاتب الفرعية بأمان.
Intranet VPNs	تربط المكاتب الإقليمية والبعيدة بشبكة العمل الداخلية للمقر الرئيسي عبر بنية تحتية مشتركة باستخدام اتصالات مخصصة. تمتاز شبكات VPN على الإنترانت بأنها تُمكّن الوصول فقط لموظفي المؤسسة.
Extranet VPNs	تربط شركاء الأعمال بشبكة المقر الرئيسي عبر بنية تحتية مخصصة. تختلف شبكات VPN للإكسترانت عن الإنترانت بأنها تُمكّن الوصول للمستخدمين خارج المؤسسة.

- **مميزات شبكات VPN**

1 . الخصوصية والأمان: توفير تشفير قوي للبيانات المرسلة عبر الشبكة العامة، مما يحميها من الاختراق والتجسس.

2 . الوصول البعيد : إمكانية للموظفين والمستخدمين بعد الوصول إلى موارد الشبكة الداخلية بأمان من أي مكان في العالم .

3 . توفير التكاليف: استغناء عن استخدام شبكات خاصة مكلفة، حيث يمكن استخدام الإنترنت العامة بدالً من ذلك.

4 . التوفير في الوقت والجهد: توفير اتصال سهل وسريع بموارد الشبكة دون الحاجة الاستخدام بنية تحتية خاصة .

5 . إمكانية التوسع : القدرة على ربط مكاتب فروع الشركة والموظفين عن بعد بسهولة دون الحاجة لتوفير بنية تحتية معقدة.

6 . إدارة مركزية : القدرة على إدارة حقوق الوصول وسياسات الأمان بشكل مركزي من المقر الرئيسي.

7 . التنقل والمرونة : إمكانية استخدام شبكات ال VPN على مجموعة متنوعة من الأجهزة والمنصات.

ما هي فوائد اتصال VPN ؟

1 . التشفير الآمن :

تحتاج إل ى مفتاح تشفي ر لقراءة البيانات. وبدون امتلاك مفتاح، سيستغرق الكمبيوتر ملايين السنين لفك الشفرة.

2 . إخفاء أماكن تواجدك:

وهذا يعني أن أي سجل محتمل لسلوكك كمستخدم يظل مخفيًا بشكل دائم .

3 . الوصول إلى المحتوى المحلي:

لا يكون من الممكن دائمًا الوصول إلى محتوى الويب المحلي من كل مكان، حيث تحتوي الخدمات والمواقع في كثيرٍ من الأحيان على محتوى لا يمكن الوصول إليه إلا من أجزاء معينة من العالم. وهنا تستخدم الاتصالات القياسية الخوادم المحلية في البلد لتحديد موقعك، وهذا يعني أنه لا يمكنك الوصول إلى المحتوى في بلدك أثناء السفر، ولا يمكنك الوصول إلى المحتوى الدولي من بلدك. هنا تتدخل خدمة تغيير الموقع عبر VPN لتسمح لك بتبديل الخادم إلى بلدان أخرى و"تغيير" موقعك بشكل فعّال.

4 . النقل الآمن للبيانات :

إذا كنت تعمل عن بُعد، فقد تحتاج إلى الوصول إلى الملفات المهمة على شبكة شركتك. ولأسباب أمنية، يتطلب هذا النوع من المعلومات اتصالًا آمنًا. غالبًا ما يلزم وجود اتصال VPN للوصول إلى الشبكة، حيث تتصل خدمات VPN بالخوادم الخاصة وتستخدم أساليب التشفير للحد من خطر تسرب البيانات .

IPsec هو اختصار لبروتوكول أمان الإنترنت . Security Protocol Internet . إنه مجموعة من المعايير والبروتوكولات التي تم تصميمها لحماية حركة المرور عبر الشبكة. يهدف IPsec إلى توفير الخصوصية والأما ن والتكامل والمصداقية للبيانات التي تنتقل عبر الشبكة.

- **وظيفة ال IPSec**

1 . يراقب تدفق حركة المرور

2 . تحديد حركة المرور الضارة

3 . اتخاذ الإجراءات التصحيحية لحماية الشبكة

"جدار الحماية " تشير عادةً إلى الأنظمة أو الأجهزة الموضوعة بين شبكة موثوقة وأخرى غير موثوقة .

التهديدات التي يتم استخدام IPS لمنع التهديدات التالية:

1 . هجوم رفض الخدمة DoS

2 . هجوم حجب الخدمة الموزعة DDoS

3 . الفيروسات

4 . الديدان

- **أنواع جدران الحماية :**

A. Packet Filtering Firewalls .

إنه يعتبر واحدًا من أقدم وأفضل أنواع جدران الحماية ويمكن الاعتماد عليه بسبب سرعته وفعاليته في فحص حركة الاتصالات. يقوم هذا الجدار بمراقبة جميع البيانات التي تأتي من الخوادم الخارجية إلى شبكتك، وذلك من خلال جمع معلومات مثل عنوان IP ، ونوع الاتصال، ورقم البوابة المستخدمة،

B. Proxy Firewalls .

هي أحد أنواع الجدران التي تستخدم لحماية الشبكات. يُعرف أيضًا باسم "جدار الحماية الوسيط" لأنه يعمل كوسيط بين الشبكات الداخلية والشبكة الخارجية، مثل الإنترنت .

C. Next-generation Firewalls .

تُستخدم هذه الجدران بشكل شائع في الشركات الكبرى والمؤسسات لتعزيز أمان الشبكة .

D. Circuit-Level Gateway .

يُستخدم هذا النوع لفحص حركة المرور على مستوى الاتصال بين جهاز العميل والخادم. بدلاً من فحص محتوى الحزم أو البيانات في الحزم، يقوم جدار الحماية بهذا النوع بمراقبة الاتصال نفسه.

E. Stateful Inspection Firewalls .

هو نوع متقدم من جدران الحماية يراقب حركة المرور عبر الشبكة بشكل ذكي ويحلل الاتصالات منذ بدايتها وحتى نهايتها. يستخدم لفحص رؤوس الحزم والبيانات المرافقة لها لضمان مطابقتها لقواعد الأمان المعينة.

- جهاز Cisco ASA (Adaptive Security Appliance) :

هو جهاز متعدد الوظائف يدمج عدة وسائل أمان مثل جدار الحماية ونظام الوقاية من التسلل IPS (وتقنيات الشبكة الخاصة الافتراضية) VPN (في جهاز واحد. هذا الجهاز يوفر حلاً شاملاً لأمان الشبكة، حيث يمكنه حماية الشبكة من التهديدات دون الحاجة إلى تركيب معدات إضافية أ وإجراء تعديلات معقدة على الشبكة .

شاشات ASA

الشاشة	الوظيفة
شاشة التكوين	تُستخدم لإعداد أو تعديل تكوين الجهاز ASA Cisco.
شاشة المراقبة	تُعرض إحصائيات ومعلومات حية حول حالة الجهاز وميزاته.

أمان الشبكة:

هو مجموعة من التقنيات والتدابير المستخدمة لحماية الشبكات والبيانات من التهديدات والهجمات الرقمية، بما في ذلك التحكم في الوصول، واستخدام التشفير، ورصد الاختراق، والاستجابة للتهديدات.

يهدف إلى حماية البيانات والحفاظ على سلامة الشبكات،

ويعتبر أساسيًا في العصر الرقمي للمحافظة على السرية، والسلامة، وسمعة المؤسسات ،والأفراد .

اختبار الشبكة والتحليل الأمن ي هما عمليتان أساسيتان في مجال الأمان السيبراني. يتضمن اختبار الشبكة محاكاة هجمات إلكترونية حقيقية على بنية تكنولوجيا المعلومات لتحديد الثغرات والضعف فيها قبل أن يتم استغلالها من قبل مهاجمين حقيقيين. يتم توجيه الاختبارات من وجهة نظر المخترقين لتقييم مدى تأمين النظام .

يهدف الهدف الرئيسي اختبار الشبكة والتحليل الأمني إلى تحديد وإصلاح الثغرات المكتشفة وتعزيز أمان الشبكة وأنظمة تكنولوجيا المعلومات. يمكن أن يتضمن ذلك تحسين سياسات الأمان وإجراءات التحكم في الوصول وتنفيذ تحديثات أمنية .

تطوير سياسة الأمن الشامل يتضمن العديد من الأهداف والمرافقات،بما في ذلك :

1 . حماية الموظفين والمعلومات.

2 . تحديد السلوك المتوقع من المستخدمين والمديرين وأعضاء الإدارة وموظفي الأمن .

3 . تفويض مهام موظفي الأمن للرصد والمراقبة والتحقيق .

4 . تحديد عواقب الانتهاكات وتفويض اتخاذ الإجراءات الضرورية .

إستراتيجية الأمن السيبراني:

هي نهج محدد لحماية البيانات والشبكات والأنظمة التكنولوجية والمستخدمين في الفضاء السيبراني. تشمل هذه الإستراتيجية معالجة جميع نقاط الهجوم المحتملة التي يمكن استهدافها من قبل أطراف مهاجمة. الأمن السيبراني يشغل مكانة مهمة في معظم الإستراتيجيات الإلكترونية بسبب تزايد تقدم وخطورة التهديدات السيبرانية نتيجة تطور أدوات وتقنيات الاستغلال .

نعمل على تحسين أمن البنية التحتية في بضع خطوات:

الأسئلة

1. عملية تحويل البيانات والمعلومات أو خلطها إلى إصدار غير قابل للقراءة لا يمكن قراءته إلا من خلال الوصول المصرح به			
التشفير	البيانات الحساسة	السرية	الخوارزمية
2. هي مجموعة القواعد الرياضية، توضح كيف يتم التشفير وكيفية فك التشفير			
الشفرة	المفاتيح العامة	الدوال	الخوارزمية
3. من خدمات السلامة والموثوقية .....وتعني أن الأطراف غير المصرح لها لا يمكنها الوصول إلى المعلومات			
السرية	الأصالة	النزاهة	عدم التنصل
4. من خدمات السلامة والموثوقية .....وتعني التحقق من مصدر الرسالة للتأكد من تحديد المرسل بشكل صحيح؛ وهذا هو أن جهاز النظير الذي تتواصل معه شرعي وليس جزءاً من جلسة تم الاستيلاء عليها .			
السرية	الأصالة	النزاهة	عدم التنصل
5. من خدمات السلامة والموثوقية .....وتعني ضمان عدم تعديل الرسالة أثناء الإرسال، بطريق الخطأ أو عمدا			
السرية	الأصالة	النزاهة	عدم التنصل
6. نوع من انواع التشفير يستخدم مفتاح واحد للتشفير وفك التشفير			
التشفير المتماثل	التشفير الغير المتماثل	التشفير المميز	التشفير البسيط
7. نوع من انواع التشفير يستخدم مفتاحين مختلفين واحد للتشفير والاخر لفك التشفير			
التشفير المتماثل	التشفير الغير المتماثل	التشفير المميز	التشفير البسيط
8. مصطلح يصف المعلومات الفعلية الموجودة في حزمة البيانات			
العنوان	الحمولة	المعلومات	بيانات
9. نوع من انواع جدار الحماية يتم الاعتماد عليها لسرعتها وجودتها في فحص الاتصالات			
packet filtering firewalls	proxy firewalls	next-generation firewalls	simple firewalls
10. نوع من انواع جدار الحماية ويستخدم ليكون وسيط بين الشبكات الداخلية والخارجية			
packet filtering firewalls	proxy firewalls	next-generation firewalls	simple firewalls

11. مصطلح يعني بإثبات هوية المستخدم الذي يريد الوصول الى الشبكة ، من الممكن أن تكون اسم المستخدم وكلمة المرور،			
المصادقة Authentication	التفويض	التدقيق	النزاهة
12. جهاز حماية يتميز بكامل ميزاته للشركات الصغيرة والمكاتب الفرعية والبيئات الخاصة بالشركات العاملة عن بعد			
جهاز Cisco ASA	الراوتر	السويتش	الكمبيوتر
13. هو بروتوكول ينشئ اتصالاً آمنًا بين جهازين على الإنترنت،			
تغليف حمولة الأمان (ESP)	تبادل مفتاح الإنترنت (IKE)	عنوان المصادقة (AH)	تغليف العنوان (MAC)
14. يتضمن بيانات مصادقة المرسل ويحمي محتويات الحزمة من التعديل من قِبل أطراف غير مصرَّح لها			
تغليف حمولة الأمان (ESP)	عنوان المصادقة (AH)	تبادل مفتاح الإنترنت(IKE)	تغليف العنوان (MAC)
15. التشفير غير المتماثل أكثر فعالية، ولكنه أيضًا أكثر تكلفة.			
صح	خطأ	-	-
16. يوفر التشفير العديد من الخدمات، أربعة منها السرية والأصالة والنزاهة وعدم التنصل			
صح	خطأ	-	-
17. بعد تحويل الرسالة إلى نص مشفر، ينبغي أن يكون الإنسان والآلة قادرين على معالجته بشكل صحيح قبل أن يتم فك تشفيره			
صح	خطأ	-	-
18. هو تحويل البيانات إلى رمز مشفر يتم فك تشفيره وإرساله عبر شبكة خاصة أو عامة.			
Cryptography	Ciphers	Cipher text	Asymmetric encryption
19. هي خوارزميات تستخدم لتشفير أو فك تشفير البيانات			
Cryptography	Ciphers	Cipher text	Asymmetric encryption
20. رسالة مشفرة غير قابلة للقراءة تسمى:			
Cryptography	Ciphers	Cipher text	Asymmetric encryption
21. توفر إمكانية الوصول عن بُعد لعامل متنقل ومكتب صغير أو منزل			
VPN Access	Intranet VPNs	Extranet VPNs	Simple VPNs
22. ربط المكاتب الإقليمية والنائية بشبكة العمل الداخلية للمقر الرئيسي عبر بنية تحتية مشتركة باستخدام اتصالات مخصصة هي:			
VPN Access	Intranet VPNs	Extranet VPNs	Simple VPNs

23. تدمج أجهزة الامان ASA التكيفية لشركة ..... جدار الحماية و IPS و إمكانيات VPN ، فهي توفر حلولًا متعددة الامكانات لشبكتك

DELL	WINDOWS	APPLE	Cisco

24. يمكن للمخترقين الإجراميين اختراق المؤسسات من خلال ثغرات معينة في الشبكات، أو أنظمة تكنولوجيا المعلومات والتطبيقات والهواتف المحمولة

صح	خطأ	-	-

25. الاختبار الفعال للاختراق والتحليل الأمني لتكنولوجيا المعلومات قد يزيد الثغرات المحتملة التي قد يستغلها المخترقون

صح	خطأ	-	-

26. نهج موثق تجاه مختلف جوانب الفضاء السيبراني cyberspace يتم تطويرها في الغالب لتلبية احتياجات الأمن السيبراني

إستراتيجية الأمن السيبراني	هيكلة الامن السيبراني	سياسة الامن السيبراني	الامن السيبراني

27. مصطلح يعني أن المرسل لا يمكنه رفض إرسال الرسالة في وقت لاحق، ولا يمكن للمتلقي إنكار استلامه، مع عدم الإنكار

عدم التنصل	النزاهة	السرية	التفويض

28. يوفر التشفير العديد من الخدمات، أربعة منها ....

السرية والأصالة و النزاهة وعدم التنصل.	السرية والأصالة والنزاهة وعدم التحديث.	المصادقة والأصالة والنزاهة وعدم التنصل.	السرية والتشفير والنزاهة وعدم التنصل.

29. يدعم IPSec انواع مختلفة من التشفير

صح	خطأ	-	-

30. يضيف تغليف حمولة الأمان عنوانًا ومعلومات ملحقة لحزمة البيانات عند التشفير

صح	خطأ	-	-

31. يوفر Cisco ASA نوعين من واجهات المستخدم وهي:

واجهة سطر الأوامر وواجهة مستخدم رسومية	واجهة سطر الاوامر وواجهة برمجية	واجهة التكوين وواجهة المراقبة	واجهة المراقبة وواجهة التنفيذ

32. ربط شركاء الاعمال بشبكة المقر الرئيسي، حيث إنها تسمح بالوصول إلى المستخدمين خارج المؤسسة.

VPN Access	Intranet VPNs	Extranet VPNs	Simple VPNs
33. تعرض شاشة .....إحصائيات حول ميزات الأجهزة والبرامج الخاصة بجهاز الأمن، يوفر رسومًا بيانية في الوقت الفعلي لمراقبة صحة الجهاز وحالته			
المراقبة	التكوين	الرسومية	البرمجية
34. يمكن تحسين أمن البنية التحتية في بضع خطوات اول خطوه هي تجميع المعلومات وتتكون من			
جمع المعلومات المرتبطة بالهجمات	تحديد الثغرات	توثيق التقارير	استغلال الثغرات
35. هو إطار من المعايير المفتوحة لضمان الخصوصية الآمنة الاتصالات عبر شبكات IP بناءً على المعايير التي طورها فريق هندسة الإنترنت			
Internet Protocol Security (Ipsec)	Internet Protocol safty	VPN	Extranet Protocol EX

ملخص لمقرر أمن الحكومة الالكترونية

الفصل الأول
الحكومة الإلكترونية

مفاهيم وتعريفات الحكومة الإلكترونية

- **الحكومة الإلكترونية:**

قدرة الجهاز الحكومي على استخدام التكنولوجيا المتطورة وخاصة الحاسبات والشبكات التي توفر المواقع الإلكترونية المختلفة، لدعم وتعزيز الحصول على المعلومات والخدمات الإلكترونية وتوصيلها للمواطنين ومؤسسات الأعمال في المجتمع بشفافية وكفاءة وعدالة عالية.

- **مفهوم الدولة:**

هي جماعة دائمة ومستقلة من الأفراد يملكون إقليماً معيّنا وتربطهم رابطة سياسية مصدرها الاشتراك في الخضوع لسلطة مركزية تكفل لكل فرد منهم التمتع بحريته ومباشرة حقوقه.

ووفقًا لهذا المفهوم، فإن الدولة تتكون من الأركان التالية:

–السكان: جماعة من السكان يكون بينهم قدر من الترابط.

–الإقليم: موقع من الأرض محدد ويتواجد به السكان الدائمون ويتحكمون في إدارته.

–الحكومة: الجهاز السياسي والإداري الذي يمارس مهامه من خلال الوظائف العامة للدولة السياسة، القضاء، الإدارة، الاقتصاد، التشريع.

–السيادة: هي استقلال الدولة عن أي سلطة خارجية وعدم التبعية، وتعني هذه السلطة بإصدار الأوامر والتعليمات للسكان القاطنين في إقليمها.

- **مفهوم الحكومة:**

الحكومة هي الجهاز الذي من خلاله تقوم الدولة بوظائفها العامة، أو هي ما يعبر عنه بالكيان التنظيمي للسلطة التنفيذية وبالتالي فالحكومة وأجهزتها التنظيمية تأخذ صلاحياتها من سلطات الدولة وهي تعتبر مفوضة من الدولة التي تمثل الكيان الأساسي لها في ممارسة سلطاتها، فأجهزة الدولة المختلفة تقوم بكافة الأعمال التنفيذية، وهو ما يعرف بإدارة الدولة أو الإدارة العامة، وقد عرفها لينور دوايت بأنها "تتكون من جميع العمليات التي تستهدف تنفيذ السياسة العامة للدولة.

- **مشروع التعاملات الإلكترونية الحكومية:**

عبارة عن سلسلة متتابعة من التجارب والمشروعات السابقة لكثير من الدول العربية والأجنبية وبنسب متفاوتة.

- **نشأة وتاريخ الحكومة الإلكترونية:**

كانت بدايات فكرة الحكومة الإلكترونية في الواليات المتحدة الأمريكية بصدور قانون الضمان الاجتماعي 1935م، وتطبيق إصدار أرقام الضمان الاجتماعي لعدد 26 مليون عامل أمريكي عام 1937م واستخدمت وزارة العمل الأمريكية الحاسب في تجميع ملفات الضمان الاجتماعي لخدمة أغراضها، ثم تسلمت في عام 1955م جهاز حاسب مبرمج للقيام بخدمات منها استلام الاشتراكات وحفظ السجلات.

بدأت تطبيقات التعاملات الإلكترونية الحكومية، وانحصر استخدامها في بعض برامج الحاسب في أغراض مختلفة مثل الإحصاء السكاني، وعرض وتوزيع موازنة الدولة، وعرض التقارير الحكومية، وحفظ بيانات وملفات الموظفين في قواعد بيانات، واستخدام الجداول الحسابية في حساب الرواتب.

- **مفهوم الحكومة الإلكترونية:- E-Government :**

هي قدرة الأجهزة والهيئات الحكومية على إتاحة المعلومات وتقديم الخدمات الحكومية فيما بينها وبين المواطنين ومنظمات الأعمال والجهات الأخرى التي تتعامل معها بأسلوب سهل ويسير وسريع وأكثر مرونة وفي أي وقت 24 ساعة يوميًا طوال الأسبوع وتوفير الخدمات الحكومية التقليدية للمواطنين وإنجاز المعاملات عبر شبكة الإنترنت بسرعة ودقة متناهيتين وبتكاليف ومجهود أقل ومن خلال موقع واحد على الشبكة".

- **أهمية الحكومة الإلكترونية:**

قدرتها على موا كبة التطور النوعي والكمي الهائل في مجال تطبيق تقنيات ونظم المعلمات وما يرافقها من ثورة المعلوماتية المستمرة أو ثورة تكنولوجيا المعلومات والاتصالات الدائمة.

- **أهداف الحكومة الإلكترونية**

• تقديم مكان واحد للمعلومات الحكومية.

• نقل التدابير الحكومية على الخط.

• تطبيق النماذج الرقمية وإتاحة تعبئتها على الخط.

• تقديم الخدمة الحكومية على الخط.

• تسهيل نظام الدفع الإلكتروني.

• تحقيق فعالية الأداء الحكومي.

- **مميزات الحكومة الإلكترونية أهمها**

• توفير مناخ جيد ومشجع للمستثمرين.

- تسهيل السياحة الداخلية والخارجية.
- القضاء على الفساد الإداري والتأخر الوظيفي.
- تهيئة الجهاز الحكومي للاندماج في النظام العالمي.
- توفر معلومات حديثة ودقيقة لمتخذ وصانعي القرار.
- رفع كفاءة أعمال الجهاز الحكومي وضغط الإنفاق الحكومي.
- القضاء على البيروقراطية والروتين العقيم في الجهاز الإداري.
- القضاء على التميز الطبقي في المجتمع ونشر العدالة الاجتماعية.

- **الآثار السلبية للحكومة الإلكترونية**

-1 مشكلة البطالة:

أداء الخدمات الإلكترونية يؤدي إلى تقليل عدد الموظفين الذين كانوا يعملوا في الحكومة التقليدية وبمختلف المستويات، إذ يؤدي استخدام التعاملات الإلكترونية إلى تخفيض حجم العمالة مع التغيير الكبير في هيكلية العمالة من حيث الكم والنوع مما يؤدي إلى زيادة البطالة.

-2 فقدان الخصوصية:

يقصد بالخصوصية حماية المعلومات الشخصية التي تجمعها الحكومة حول الأفراد والمؤسسات فمن الآثار السلبية للحكومة الإلكترونية فقدان الأفراد للخصوصية، وحقهم في الحفاظ على سرية البيانات المتعلقة بهم، فقواعد المعلومات المرتبطة بعضها بالبعض الأخر والتي تحتوي على أسماء الأفراد

-3 فقدان الأمان:

يؤدي التعامل الإلكتروني إلى فقدان الأمان تماً ما في كثير من التعاملات والتي من أهمها التحويلات الإلكترونية والتعاملات المالية عن طريق بطاقات الائتمان. مما يجعلها عرضها للاختراق، كالسطو على المعلومات الشخصية والخاصة بطالب الخدمة مثل إمكانية الاستيلاء على أمواله عن طريق بطاقات الائتمان الخاصة به وغيرها.

- **مبادئ الحكومة الإلكترونية**
- القدرة على تأمين كافة الاحتياجات الاستعلامية والخدمية للمواطن.
- تقليل الاعتماد على العمل الورقي في المعاملات الحكومية.
- المرونة في التعامل مع المواطنين.
- كسر الحواجز الجغرافية بين المواطن والحكومة.
- **مبادئ تطبيق الحكومة الإلكترونية**

المبدأ الأول تقني :Technological

التخزين :Storage

حفظ المعلومات الهائلة في أحجام صغيرة كتحويل الملفات الورقية إلى ملفات إلكترونية صغيرة الحجم تستوعب الكم الهائل من المعلومات.

– النقل :Transportation

انتقال المعلومات المخزنة إلكتروني رونية إلى مواقع جغرافية أخرى، سواء كانت في إطار المنظمة ذاتها أو الإطار الجغرافي المحلي أو الإطار العالمي الخارجي.

– المعالجة :Transaction

إجراء مختلف العمليات المطلوبة للبيانات والمعلومات المخزنة إلكترونياً بواسطة أجهزة الحاسب الآلي التي تعمل وفقاً لبرامج متنوعة تلبي احتياجات المستفيدين المتنوعة.

المبدأ الثاني إجرائي :Procedural

يتضمن طلب وتنفيذ المعاملات والخدمات عن بعد عبر شبكة الإنترنت مع ضمان صحتها ومصداقيتها دون الحاجة إلى المتابعة والمراقبة أو استخدام النماذج والوثائق الورقية.

- **نظريات الحكومة الإلكترونية**

يوجد أربع نظريات مهمة تدور جميعها حول تطبيق الحكومة الإلكترونية والنتائج التي قد تترتب على تزايد تطبيق أنظمتها إلا أنها تتنافس فيما بينها في مدى مساعدتها الحكومات على القيام بالمهام المطلوبة منها بصورة أفضل قياسا" على معايير المصالح الرئيسية التي تشكل عمليات صنع القرار، كما تتنافس في قدرتها على تقديم المساندة الكافية لإنجاز العمل بسرعة، وكل واحدة من هذه النظريات يمكن النظر إليها كأحد السيناريوهات المستقبلية المتاحة لفهم التأثيرات المتوقعة للحكومة الإلكترونية وهذه النظريات هي:

1- العقلانية:

بعض الاتجاهات ترى أن استخدام التقنيات يمثل تحسنا" كبيرا" دائما" في مقدرات الحكومة الإلكترونية ذلك على أقل تقدير في الاستناد إلى العقلانية عند اتخاذ القرارات، والتكلفة الوحيدة المتكبدة هي تكلفة شراء هذه التقنيات وتشغيلها ووفقا" لهذا الرأي فإن هذه الأنظمة سوف تقلل بصورة مطردة من تكاليف الحصول على المعلومات وترتيبها وترميزها وتنظيمها وإدارتها واستخدامها وتبعا لذلك فإن هذه الأنظمة سوف تحقق عائدا" يفوق تكاليف إنشائها خلال فترة حياتها الافتراضية وهذا التفاؤل مبني على نظرية قديمة، تقول إن المعلومات تقلل من احتمالية صحة القرار المتخذ.

2- الثمن:

مجموعة أخرى من النظريات تقبل إمكانية زيادة قدرات التحكم وانعكاس ذلك على نوعية عمليات اتخاذ القرار وعقلا نيتها ، لكنها في الوقت نفسه ترى أن ذلك ال يأتي بدون ثمن ، و هذه النظريات تؤمن بضرورة عمل ترتيبات الحماية و الوقاية و إلا سوف يكون الثمن غاليا" فيما يتعلق بالحرية والخصوصية الشخصية للمواطنين و الحفاظ على سرية المعلومات.

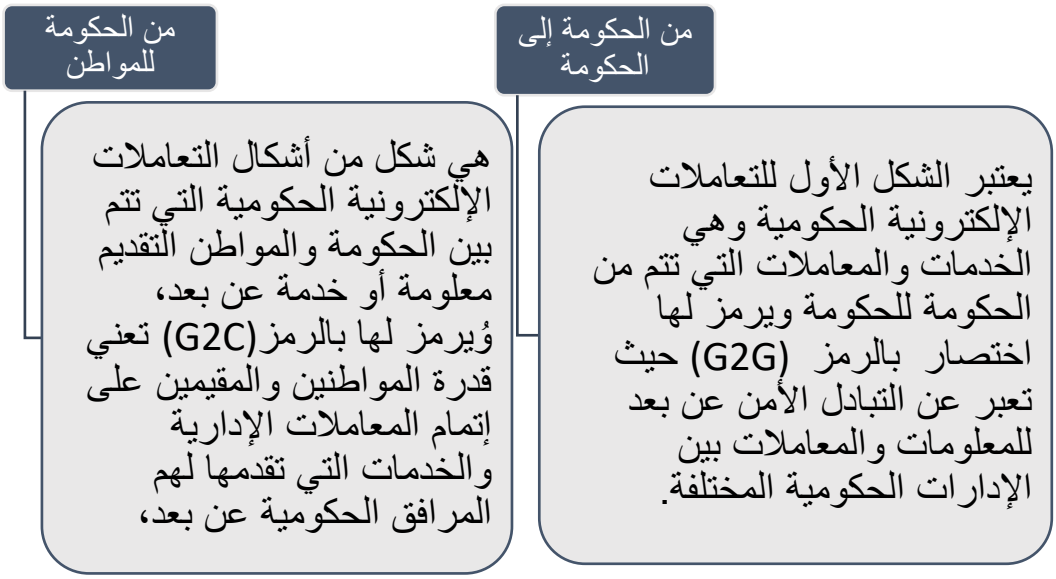
3- ضوضاء المعقولية وتأكلها:

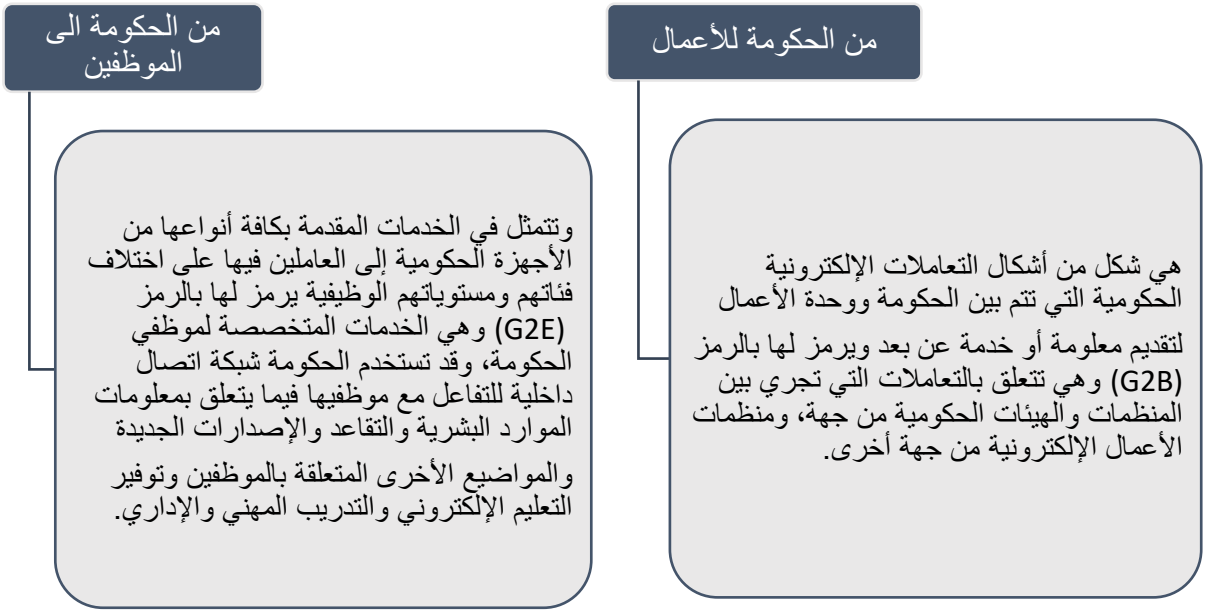
النظرية الثالثة هي الأكثر تشاؤما" إذ أنها تقوم على الادعاء القائل بأن الحكومة الإلكترونية سوف تقضي على العقلانية بصورة عامة وعلى الزعم السائد بضعف قدرة القطاع العام على إدارة المعلومات بصورة جيدة بالمقارنة مع مؤسسات القطاع الخاص وعلى الهواجس الأخرى للسيطرة التي تقوم بصرف انتباه صانعي القرارات بعيدا" عن العوامل الضمنية النوعية لكي يركزوا انتباههم على العوامل الواضحة وربما يكون الأكثر أهمية. هذه النظرية تتخوف من عدة أشياء مثل التفسير المبسط بأكثر مما ينبغي للبيانات والنمذجة المبسطة والتبسيط الشديد بدءا من عمليات التحليل حتى صياغة التوصيات وهذه النظرة ترفض مطلقا"بصورة مطلقة الاعتقاد السائد بأن المعلومات هي التحكم والرقابة وتفضل أن تعتبر المعلومات مجازاً كالضوضاء.

4- التقنية:

هي أداة مهمة في ظروف الصراع الاجتماعي القائمة، والنظريات التي وردت في المجموعة الرابعة والمجموعة الأخيرة ركزت على أنه لن يكون للتقنية نفسها تأثير جوهري.

- **أنواع الحكومات الإلكترونية ودعائمها**





- **مرادفات الحكومة الإلكترونية**

مصطلح التعاملات الإلكترونية الحكومية بصورة مترادفة مع مصطلح الحكومة الإلكترونية إلى غير ذلك من المفاهيم والمصطلحات التي تربط ما بين الأنشطة والاتصالات في العالم الرقمي وعادة ما تسبقها البادئة E "كإشارة لتعامل الإلكتروني الرقمي.

تسمى أيضا" الحكومة الرقمية أو الخدمات الحكومية على الإنترنت

- **إستراتيجيات الحكومة الإلكترونية**

هي استراتيجيات تضمن انسجام وتناسق البرامج والمشاريع التي سيتم إطلاقها وتساهم جميعها في تحقيق رؤية موحدة

تتمثل هذه الاستراتيجيات في التالي:

1. سد الفجوة بين المهارات المطلوبة والمتاحة
2. سد الفجوة الشاسعة بين التوقعات وإدراك المواطنين
3. الوصول للمواطنين
4. التحول في الخدمات
5. التحول للديناميكية والتفاعل في الأداء
6. إتاحة الخدمات من خلال بوابات مكرسة
7. وضع خريطة واضح

الفصل الثاني
التغيير الذي أحدثته الإدارة الإلكترونية في الحكومة الإلكترونية

- **مفهوم الإدارة الإلكترونية**

هي منظومة إلكترونية متكاملة تهدف إلى تحويل العمل الإداري العادي من إدارة يدوية إلى إدارة باستخدام الحاسب وذلك بالاعتماد على نظم معلوماتية قوية تســـــاعد في اتخاذ القرار الإداري بأسرع وقت وبأقل التكاليف ويمكن أن تشمل كال من الاتصالات الداخلية والخارجية ألي منظمة. أي تحويل كافة العمليات الإدارية ذات الطبيعة الورقية إلى عمليات ذات طبيعة إلكترونية باستخدام مختلف التقنيات الإلكترونية وهذا يعني تحويل الدورة المستندية الورقية في المنظمة إلى دورة إلكترونية، وهذا ما يطلق علىه العمل الإلكتروني أو الإدارة بلا ورقManagement Paperless وهي مصطلحات مترادفة من حيث المعنى المدلول.

- **الترابط بين الحكومة الإلكترونية والإدارة العامة**

الترابط ينتج من الصلة الوثيقة للإدارة العامة بأجهزة الدولة وحكومتها فالإدارة العامة هي تلك النشاطات التي تمارسها حكومة ما سعياً لتنفيذ وتحقيق السياسة العامة للدولة، ويعتبر علماً شاملا أكثر من الإدارة، وتركز على ضرورة الكفاءة والفعالية العاليتين في تحقيق الأهداف المنشودة، ويمكن تطبيقها في العلوم النظرية والتطبيقية، وترتبط ارتباطا وثيقاً بسياسة الدولة العامة. وهي تعتبر من الإدارات الشاملة لكافة الهيئات العامة والمنظمات المركزية أو المحلية، وتعرف بأنها بمثابة جهة توكل إليها مهمة تلبية الاحتياجات العامة وتنفيذها حتى في حال اختلاف صورها، ويكون ذلك بتزويدها بجميع الوسائل اللازمة والمواد الضرورية لذلك و الحكومة الإلكترونية هي إدارة الشؤون العامة بواسطة وسائل إلكترونية لتحقيق أهداف اجتماعية واقتصادية وسياسية والتخلص من الأعمال الروتينية والمركزية وإنجاز الأعمال والخدمات الحكومية بين الجهات المختلفة مثل العالقة بين الحكومة والحكومة ، العالقة بين الحكومة والأفراد ، والعالقة بين الحكومة والشركات ، والعالقة بين الحكومة والموظف.

- **متطلبات الإدارة الإلكترونية**

1- البنية التحتّية:

إن الإدارة الإلكترونية تتطلب وجود مستوى مناسب وعالي تتضمن شبكة حديثة للاتصالات والبيانات وبنية تحتية متطورة للاتصالات السلكية واللاسلكية تكون قادرة على تأمين التواصل ونقل المعلومات بين المؤسسات الإدارية نفسها من جهة وبين المؤسسات والمواطن من جهة أخرى.

2- توفر الوسائل الإلكترونية اللازمة للاستفادة من الخدمات:

الوسائل التي يستطيع الأفراد بواسطتها التواصل معها ومنها أجهزة الشخصية والمحمولة والهاتف الشبكي وغيرها من الأجهزة التي تمكنهم من الاتصال بالشبكة العالمية أو الداخلية في البلد و بأسعار معقولة تتيح لمعظم الأفراد الحصول عليها.

3- وافر عدد ال بأس به من مزودي الخدمة بالإنترنت:

تكون الأسعار معقولة قدر الإمكان من أجل فتح المجال لأكبر عدد ممكن من المواطنين للتفاعل مع الإدارة الإلكترونية في أقل جهد وأقصر وقت وأقل كلفة ممكنة

4- التدريب وبناء القدرات:

هو يشمل تدريب كافة الموظفين على طرق استعمال أجهزة الكمبيوتر وإدارة الشبكات وقواعد المعلومات والبيانات وكافة المعلومات اللازمة للعمل على إدارة وتوجيه "الإدارة الإلكترونية" بشكل سليم ويفضل أن يتم ذلك بواسطة معاهد أو مراكز تدريب متخصصة وتابعة للحكومة، ويجب نشر ثقافة استخدام "الإدارة الإلكترونية" وطرق ووسائل استخدامها للمواطنين.

5- توافر مستوى مناسب من التمويل:

بحيث يمكّن التمويل الحكومي من إجراء صيانة دورية وتدريب للكوادر والموظفين والحفاظ على مستوى عالي من تقديم الخدمات وموا كبة أي تطور يحصل في إطار التكنولوجيا و "الإدارة الإلكترونية" على مستوى العالم.

6- توفر الإرادة السياسية:

بحيث يكون هناك مسؤول أو لجنة محددة تتولى تطبيق هذا المشروع وتعمل على تهيئة البيئة اللازمة والمناسبة للعمل وتتولى الإشراف على التطبيق وتقييم المستويات التي وصلت إليها في التنفيذ.

7- وجود التشريعات والنصوص القانونية:

التي تسهل عمل الإدارة الإلكترونية وتضفي عليها المشروعية والمصداقية وكافة النتائج القانونية المترتبة عليها.

8- توفير الأمن الإلكتروني والسرية الإلكترونية:

على مستوى عالي لحماية المعلومات الوطنية والشخصية ولحفظ الأرشيف الإلكتروني من أي اختراق والتركيز على هذه النقطة لما لها من أهمية وخطورة على الأمن القومي والشخصي للدولة أو الأفراد.

9- خطة تسويقية دعائية شاملة للترويج الاستخدام الإدارة إلكترونية:

وإبراز محاسنها وضرورة مشاركة جميع المواطنين فيها والتفاعل معها ويشارك في هذه الحملة جميع وسائل الأعلام الوطنية من إذاعة وتلفزيون وصحف والحرص على الجانب الدعائي وإقامة

النـدوات والمؤتمـرات واستضافة المسؤولين والـوزراء والموظفين في حلقات نقاش حول الموضوع لتهيئة مناخ شعبي قادر على التعامل مع مفهوم الإدارة الالكترونية.

- **وظائف الإدارة الإلكترونية**

يتطلب التحول من العمل وفقاً للأسلوب التقليدي إلى العمل وفقاً لأسلوب الإدارة الإلكترونية إعادة هندسة كل نظم العمل المعمول به في المؤسسات التقليدية، وينتج ذلك عن تغير في الوظائف التقليدية

للتسيير، حيث تتحول إلى وظائف إلكترونية الثورة الرقمية أدت إلى تغييرات عميقة وواسعة في بيئة الأعمال وأساليبها وطريقة تنظيمها ومصادر ميزتها التنافسية وغير ذلك الكثير

- **التخطيط الإلكتروني**

يعتمد التخطيط الإلكتروني على تبسيط نظم وإجراءات العمل التي تتسم في ظل الإدارة التقليدية بالتعقيد الشديد، حيث يتم استبدالها بنظم وإجراءات سريعة وحاسمة، تعتمد بالدرجة الأولي على استخدام شبكات الإدارة الإلكترونية التي تجعل أداء الأعمال يتم لحظيا ونظم الادارة الإلكترونية كنظم دعم القرار، النظم الخبيرة، ونظم الشبكات العصبية الاصطناعية التي تؤدى إلى توظيف أساليب تخطيط عديدة ومبتكرة، وعمليات التوقع، وترفع من كفاءة التخطيط، وتزيد من فعالية صنع واتخاذ القرارات.

- **التنظيم الإلكتروني**

يعرف التنظيم بأنه ترتيب الأنشطة بطريقة تساهم في تحقيق أهداف المنظمة وإن هذا التنظيم هو الذي يعطي للمنظمة شخصيتها وميزتها وهذا ما يظهر من خلال المكونات الأساسية للتنظيم والتي يمكن تحديدها فيما يلي:

- **القيادة الإلكترونية**

واجهت القيادة في السابق تحديين أساسيين تمثلا في المهام والعاملين، ومع تطور الفكر الإداري تحولا إلى مدخلين في القيادة، وهما: المدخل المرتكز على المهام والمدخل المرتكز على العاملين. حيث يمثل الأول المدخل الصلب للقيادة القائمة على قوة التنظيم المتمثل في قوة المركز الإداري وقوة العاملين، أما الثاني فهو المدخل الناعم القائم على القوة الشخصية وقوة العالقة بين القائد والمرؤوسين.

وتعرف القيادة الإلكترونية على أنها القدرة على التأثير في الآخرين وتوجيههم نحو تحقيق الأهداف وهي التي تجمع المجموعات البشرية وتحفزها على العمل. وأدي التغير في بيئة الأعمال الإلكترونية، والتحول في المفاهيم الإدارية إلى إحداث نقلة نوعية كان من نتائجها الانتقال إلى نمط القيادة الإلكترونية، والتي **تنقسم للأنواع الثالثة التالية:**

- **لقيادة التقنية الصلبة:**

تعتمد هذه القيادة على الاستخدام المكثف لتكنولوجيا الإنترنت في إدارة أعمالها وعلاقاتها المختلفة، كما تقوم على اكتساب ميزة من هذا الاستخدام، كزيادة المعلومات وسرعة الحصول عليها وتحسين جودتها من أجل اتخاذ قرارات أشمل وأسرع وأفضل، وهذه ميزة شبكات الأعمال التي تجعل المدير في كل مكان يمتلك نفس القدر من المعلومات، ويتعامل مع نفس الحاسوب المحمول، ويتصل بكل العاملين عبر شبكة الأعمال الداخلية، أو بالمستفيدين الآخرين عبر الشبكة الخارجية من أجل أن يستكمل صورة اتخاذ القرارات التي تكون أكثر كفاءة، وربما فاعلية بالاعتماد على هذه التكنولوجيا.

- **القيادة البشرية الإنسانية:**

فالقيادة الإلكترونية رغم اعتمادها على التقنية إلا أنها ذات محتوي إنساني كبير، وتتسم القيادة الإلكترونية القائمة على البعد البشري.

- **القيادة الذاتية:**

تركز القيادة الذاتية على عدد من المواصفات، يجب أن يتصف بها القادة من إدارة أعمال عبر الإنترنت، وهو ما يجعل قيادة الذات تتصف بالقدرة على تحفيز النفس، والتركيز على إنجازات المهمات ، والرغبة في المبادرة إلى المهارة العالية، ومرونة التكيف مع مستجدات البيئة المتغيرة.

o الرقابة الإلكترونية

تعرف الرقابة بشكلها التقليدي بأنها متابعة العمل وقياس الأداء والإنجاز الفعلي له ومقارنته بما هو مخطط باستخدام معايير رقابية، بحيث تحدد الإنجازات الإيجابية التي يجب تدعيمها والانحرافات السلبية التي يجب معالجتها تجنبها مستقبلاً وبالتالي تحقيق الأهداف المطلوبة

ومن أبرز الخصائص التي اتسمت بها الرقابة التقليدية هي أنها رقابة موجهة للماضي، وهذا ما يظهر واضحا والتنفيذ. ً في كون الرقابة هي المرحلة التي بعد التخطيط أما الرقابة الإلكترونية فإنها أكثر قدرة على معرفة المتغيرات الخاصة بالتنفيذ أوالً بأول وبالوقت الحالي، بالمعلومات التي تسجل فور التنفيذ تكون لدي المدير في نفس الوقت مما يمكنه من معرفة التغيرات قبل أو عند التنفيذ والاطلاع بالتالي على اتجاهات النشاط خارج السيطرة الاتخاذ ما يلزم من إجراءات التصحيح التي تصل في نفس الوقت إلى المسئولين عن التنفيذ.

- **أدوات الحكومة الإلكترونية**

• الأجهزة

• والمعدات.

• البرمجيات بمختلف أنواعها

- الاتصالات.
- نظم المعلومات.
- الكوادر البشرية.

الفصل الثالث
الأمن والسرية في الحكومة الإلكتروني

- **الأمن والسرية في الحكومة الإلكترونية**

يجب تحليل المخاطر التي قد تنجم من جراء عدم الاهتمام بموضوع أمن وسرية المعلومات ويشمل تحليل المخاطر جوانب عديدة منها:

الواقع والنوايا ومصادر الخطر بالإضافة إلى وسائل الهجوم الإلكتروني وكيفية تجنبها باعتماد إجراءات الوقاية والدفاع الإلكتروني وما ينتج عنه من تكلفة اقتصادية إضافية، ومن المهم تحديد أصول الحكومة الإلكترونية التي تحتاج إلى جهاز حماية فعال. فكثيًرا ما يستخدم مصطلح السرية ومصطلح الأمن تبادلياً، بينهما إلا أن الأمن والسرية قضيتان مختلفتان تماماً فالأمن هو بنية تحكم متمركزة على المنظمة أو الجهاز الحكومي كما تدل على ضوابط سبل الوصول وإضفاء الشرعية.

أما السرية بنية متمركزة على الفرد وهي عقد بين المنظمة والفرد بخصوص كيفية جمع المعلومات الشخصية عن الأفراد وظروفها والتعامل معها ومعالجتها من قبل المؤسسة أو المنظمة. وهنا البد من توافر عامل الثقة الذي يساعد الأفراد على تبادل البيانات بدقة دون تخوف من ضياعها أو تسربها، وهذا يتطلب من الجهات الحكومية وضع القوانين والأنظمة التي تضمن سرية المعلومات. فالهجوم على المعلومات وسرقة البيانات والملفات واختراق الأنظمة وبرامج الأنظمة وبرامج الحماية من أسباب تخوف المنظمات من التعاملات الإلكترونية.

- **الأمن المعلوماتي في الحكومة الإلكترونية**

أهداف العمل ونتائجه وأثار تعرضها لهجمات سواء كان ذلك من قبل الهواة المحترفين، لذلك فإنه يجب على كل المؤسسات والأجهزة الحكومية تأمين هذه المعلومات والبيانات على كافة المستويات التنظيمية. أمن البيانات هو حماية البيانات من حوادث التحوير والتدمير أو كشف المعلومات بدون تصريح. عن طريق تطوير وتنفيذ وصيانة برامج معدة لغرض حماية وإتاحة وسرية ومصداقية المعلومات. إذا أمن المعلومات هو حماية المعلومات والمحافظة على سرية المعلومات من الاختراقات والتهديدات غير المشروعة وغير القانونية التي قد تهدد المنشأة اقتصاديًا واجتماعًيا، ويوجد العديد من الوسائل التكنولوجية والإجراءات الإدارية للمحافظة على سرية المعلومات بحيث يتم تطبيق الوسائل الكفيلة من تداول المعلومات بين العاملين والموظفين المصرح لهم بالاطلاع عليها، والتأكد من أن محتويات السجلات والوثائق لم يتم تخريبها به أو تعديلها، معايير وإجراءات أمن المعلومات.

- **طبيعة المخاطر الإلكترونية**

هي الهجمات عبر الإنترنت للوصول غير المصرح به إلى أنظمة الكمبيوتر وسرقة البيانات أو تعديلها أو إتلافها وتنقسم إلى:

- مخاطر العنصر البشري

سبب أغلبية الهجمات والتهديدات هو العنصر البشري غير المدرب أو الواعي للمخاطر الكبيرة على البيانات في العالم كله. وهي تنتج عن طريق أخطار البشر مثل أعمال غير مقصودة أو إجراءات متعمدة مثل تحميل البرامج الخبيثة والوصول غير المصرح به إلى المعلومات السرية.

- مخاطر من الطبيعة البيئية

مثل الفيضانات والزلازل والأعاصير وينتج عنها تعطيل نظام الحاسب عن العمل وهي خارجة عن الإرادة البشرية وتتطلب تعاون العادة الخدمة وإصلاح الأعطال.

- المخاطر الناتجة عن الجرائم المعلوماتية

الجريمة الإلكترونية سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، وينتج عنها حصول المجرم على فوائد مادية ومعنوية مع تحميل الضحية خسارة مقابلة، وغالباً ما يكون هدف هذه الجرائم من أجل سرقة أو إتلاف معلومات، فالجريمة الإلكترونية هي مخالفة ترتكب ضد أفراد أو جماعات بدافع اجرامي، أو بنية الإساءة لسمعة الضحية بطريقة مباشرة أو غير مباشرة.

- **أنواع جهات الخطر**

تعمل أجهزة الحكومة الإلكترونية في فضاء مفتوح يتداخل فيه جمهورها الخارجي (مواطنون، مؤسسات، حكومات أخرى) مع جمهورها الداخلي (وزراء، موظفين..) وتصبح فيه أجهزة تلك الحكومة عرضة للعديد من أنواع الهجوم تحت دوافع مختلفة، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها وعبر أحد الموظفين الغاضبين أو من الخارج عبر مجموعات المخترقين أو أجهزة الاستخبارات في بلدان معادية وصولاً إلى المؤسسات التجارية الساعية إلى الحصول على معلومات تجارية تنافسية.

1- خطر المستخدم الشرعي:

المستخدم الشرعي هو المواطن أو صاحب المؤسسة الحاصل على إجازة من الحكومة في سبيل استعمال خدماتها الإلكترونية، وتكون الإجازة في معظم الأحوال عبارة عن تأكيد هوية المستخدم إلكترونياً عبر شبكة الحكومة بعد أن يكون قد تم تسجيله سابقاً وقد يحاول هذا المستخدم أن يوظف إمكانية دخوله إلى شبكة الحكومة من أجل تخريب الخدمات المتاحة في نطاق إجازته، وقد يحصل في بعض الأحيان يتمكن هذا المستخدم من الحصول على معلومات لا تخصه في حال وجود

عيوب فنية في تصميم الخدمة الإلكترونية المتاحة له. من ناحية أخرى، من الممكن لهذا المستخدم أن ينكر قيامه بخدمات معينة في حين تؤكد أنظمة الحكومة قيامه بها.

2- خطر موظفي الحكومة الإلكترونية:

تشكل هذه المجموعة خطراً كبيراً على أنظمة الحكومة في حال أرادت ذلك، ونظراً لما يملكه بعض الموظفين في الحكومة الإلكترونية من حقوق دخول إلى الشبكة واطالع على الأنظمة فمن الممكن لهم أن يقوموا بأعمال تخريبية تؤدي إلى إيقاف الخدمة الإلكترونية وقد يكون هؤلاء الأشخاص مدفوعين بدوافع مادية أو نفسية أو لمجرد عدم الرضا عن وضعهم الوظيفي داخل الحكومة.

3- خطر أجهزة المخابرات الخارجية:

من الممكن أن تعتمد أجهزة المخابرات الصديقة أو العدوة على حد سواء على الحصول على معلومات عن أشخاص أو مؤسسات أو حتى أجندات الحكومة الداخلية عبر تنفيذ هجمات إلكترونية بهدف اختراق النظام الأمني المعلوماتي للحكومة والدخول إلى مختلف الأنظمة فيها وقد توظف أجهزة المخابرات في هذه العملية كفاءات تقنية عالية وقادرة في كثير من الأحيان على اختراق أنظمة الحكومة الهدف.

4- خطر المؤسسات التجارية:

تسعى المؤسسات التجارية دوماً إلى تحقيق السبق الاقتصادي والإعلامي والتجاري على منافساتها من المؤسسات وقد تحاول هذه المؤسسات أن تخترق أنظمة الحكومة الإلكترونية من أجل الحصول على معلومات عن منافسيها في السوق عبر معلومات تجارية تنافسية تملكها الحكومة ولم يتم نشرها.

5- خطر المنظمات الإرهابية:

قد تحاول بعض المنظمات الإرهابية فرض أجنداتها السياسية على الحكومة عبر وسائل إرهابية عدة ومنها الحرب الإلكترونية، وربما تسعى إلى تعطيل خدمات الحكومة الإلكترونية من خلال هجوم إلكتروني مكثف قد يحدث في فترة زمنية قصيرة نسبياً، ويكمن خطر المنظمات الإرهابية في هذا المجال بكونها تتحرك من منطلقات تدميرية تكون فيها مصلحة البالد العليا نقطة هامشية أمام تحقيق أهدافها.

6- خطر مزودي البرمجيات والعتاد:

يمتلك مزودو البرمجيات القدرة على التلاعب بالشفرة البرمجية بحيث يتركون وراءهم أبواباً مفتوحة للأنظمة (Back Door) مما يمكنهم الحقاً من الدخول إلى تلك الأنظمة بطريقة غير شرعية وتجاوز بوابات يتركوا عيوباً الأمن المتاحة للجمهور، وعلى حد سواء يستطيع مزودو العتاد أن في أجهزة

الكمبيوتر والشبكات وغيرها عن قصد بحيث يسهل عليهم تجاوز الإجراءات الأمنية الإلكترونية للحكومة.

7- خطر الكوارث الطبيعية:

كما تؤثر الكوارث الطبيعية من زلازل وهزات أرضية وصواعق في الحركة العامة لأجهزة الحكومة ومستوى توافر خدماتها، فقد تلحق تلك الكوارث أضرار كبيرة بأنظمة الحكومة الإلكترونية وقد تؤدي في بعض الأحيان إلى شل الخدمات الإلكترونية للحكومة في حال أصابت مواقع تشغيل تلك الخدمات.

8- خطر عيوب التصميم والتشغيل:

تشمل عيوب التصميم والتشغيل في مختلف مكونات الحكومة الإلكترونية من الشبكات وطريقة تصميمها إلى البرمجيات المستخدمة وخوارزميات التشفير ومستوياتها وصولاً إلى أساليب وطرق التثبيت كالهوية الإلكترونية، وتقاس قوة جدار الأمن الإلكتروني الواقي بقوة الحلقة الأضعف في هذه المكونات بحيث يؤدي كسر تلك الحلقة الضعيفة إلى اختراق الجدار مهما كانت قوة مكوناته الأخرى. إن طريقة تصميم البنية التحتية لخدمات الحكومة الإلكترونية من الممكن أن يشكّل فارقاً مهماً في مستويات الأمن والسرية لتلك الخدمات، كما تعتمد الخدمات الإلكترونية على مبدأ " التوافر"(Availability) الذي يهدف بضرورة توفر الخدمة من خلال بدائل شبيهة في حال تم تدمير الخدمة الأصلية وفي حال لم يؤخذ هذا المبدأ بعين الاعتبار عند تصميم الخدمة فسوف تكون عرضة للانقطاع الحقاً.

9- خطر التكاثرية الأمنية:

في كثير من البلدان التي لا تملك مخططا عاماً (E- Master Government Master Plan) لتطبيقات الحكومة الإلكترونية على مستوى كافة الإدارات الرسمية والوزارات، تعمد إدارات تلك البلدان إلى تطبيق مفهومها الخاص بالأمن والسرية الإلكترونية بدون الأخذ بعين الاعتبار أية معايير أو مقاييس تضمن كفاءة وفعالية تطبيقاتها، ويؤدي هذا الأمر بالتالي إلى نوع من تناثر وتنوع تطبيق مفاهيم الأمن والسرية عبر الإدارات وقد يشكل ضعف تطبيق إدارة أو وزارة واحدة لمبدأ الحماية والأمن الحلقة الضعيفة في الجدار الواقي مما ينتج بالنهاية اختراق هذا الجدار.

10- خطر عدم الوعي بالمخاطر:

يمثل عدم وعي مدراء القمة وموظفيهم في الحكومة الإلكترونية بالمخاطر الخطر الأعظم على النموذج الإلكترو – حكومي فالذي ال يعي المخاطر لا يمكن أن يضع خطط الدفاع والطوارئ. لا يمكن ألي مشروع حكومة إلكترونية أن يزدهر وينجح بدون معالجة الأخطار المطروحة والجوانب المحيطة

بها، وربما من الأفضل للحكومة البقاء في فضائها المادي / الواقعي وعدم الشروع بدخول الفضاء الإلكترو – حكومي في حال لم تتسلح بأدوات الدفاع الإلكتروني المناسبة.

- **تقنيات الهجوم المتوقعة**

من المتوقع أن تقوم الجهات الـ مُعادية لعمليات هجوم تقليدية على منشآت الحكومة الإلكترونية من أجل تدمير بنيتها المعلوماتية وبالتالي شل قدرتها على اتخاذ القرارات الصائبة المطلوبة في الأوقات الحرجة والتي تركز بشكل أساسي على معلومات وبيانات مخزونة في أنظمة تلك الحكومة. وقد تلجأ الجهات المعادية إلى هذا الاختيار في حال استنفدت الخيارات التقنية الأخرى أو في حال لم تمتلك تلك الجهات القدرة التقنية والخبرات الهجومية الإلكترونية. وقد يشمل الهجوم على شبكات الاتصال ومكاتب الحكومة الإلكترونية

- **تقنيات أمن المعلومات**

هي مجموعة من استراتيجيات الأمن السيبراني التي تمنع الوصول غير المصرح به إلى الأصول التنظيمية مثل أجهزة الكمبيوتر والشبكات والبيانات. ويحافظ على سالمة وسرية المعلومات المهمة، ويمنع وصول المتسللين المتطورين إليها. تشمل أحدث التقنيات في مجال الأمن السيبراني الذكاء الاصطناعي (AI) والتعلم الآلي (ML)، والقياسات الحيوية السلوكية ، وهندسة الثقة الصفرية ، و Blockchain ، والحوسبة الكمية ، والأمن السحابي، وأمن إنترنت الأشياء.

الفصل الرابع
الحكومة الإلكترونية تنظيم وتطبيقات

- **البوابة الإلكترونية للحكومة الإلكترونية**

البوابات الإلكترونية هي همزة التواصل بين المنشأة والمستفيد، حيث أن البوابات الإلكترونية تعكس هوية وشعار المنشأة وتميزها بالهيكلية للمحتوى المعلوماتي، بدءا بالموضوعات الرئيسية وانتهاءً بالوظائف المرتبطة بشكل هرمي و تطبيق القواعد والتصنيفات الحديثة لتطوير وإدارة وتحديث المحتوى المعلوماتي وتميزها بالتفاعلية والتحديث الفوري والمستمر للمحتوى المعلوماتي، وربطها بأنظمة المعلومات وقواعد البيانات للمنشأة لتسهيل الحصول على المعلومات والخدمات الإلكترونية التي تقدمها المنشأة.

كما يعد توفير واجهة إلكترونية على الإنترنت للعملاء والمستفيدين من الجهود المبذولة لتطبيق التعاملات الإلكترونية الحكومية. ويمكن وضع معايير تكنولوجية مشتركة وبنية تحتية تمهد الطريق المزيد من الكفاءة داخل الحكومة ذاتها. مثل خفض الحواجز أيضا يمكن وصف موقع ويب بأنه بوابة رقمية، والنجاح الأولي لتصميم الموقع على شبكة القانونية والتكنولوجية للتعاون بين المنظمات. ولابد من توفر فيه المواصفات القياسية العالمية مثل:

- سهولة الدخول.
- مرونة الاستخدام.
- تنوع الخدمات.
- التفاعلية.
- التحديث المستمر للمعلومات.
- توفر الوسائط الرقمية المتعددة.
- بالإضافة إلى عدد ونطاق الارتباطات مع المواقع التوعية الأخرى وجودة المحتوى.
- إدارة الوثائق.
- ضمان أمن المعلومات والمعاملات والى غير ذلك من المواصفات المترابطة والمتكاملة.

- **الحكومة الإلكترونية والتجارة الإلكترونية والتسويق الإلكتروني**

الحكومة الإلكترونية كان لها تأثيرات اقتصادية ساعدت على تنمية التجارة إلكترونية التي تتطلب تواصل منظمات الاعمال التجارية مع مؤسسات الدولة وخاصة في مجال العالقة بين المنظمة والإدارة الرسمية وكذلك التسويق الإلكتروني الذي ُيعتبر من أهم ركائز النجاح ألي شركة تجارية تعتمد على التجارة الإلكترونية في عرض خدماتها أو بيع منتجاتها حيث يعد التسويق الإلكتروني جزء من التجارة الإلكترونية ألن التجارة سواء كانت تقليدية أو الكترونية فهي بحاجة إلى استراتيجيات التسويق لتتم معاملات البيع والشراء وعدم الربط بينهما يؤدي لفشل عملية التسويق. تقوم التجارة الإلكترونية بتسهيل الكثير من الأمور على العميل وقد بدأت بالانتشار بشكل واسع منذ بدء جائحة كورونا، وأصبح التوجه كبيراً للتجارة الإلكترونية على الصعيد المحلي والدولي، مما أدى الانتشارات على التسويق الإلكتروني بكافة تخصصاته والمرتبط بالتجارة

المواقع الإلكترونية التي تعتمد أسا الإلكترونية.

- **التجارة الإلكترونية**

تمثل التجارة الإلكترونية واحدا من موضوعي ما يسمى بالاقتصاد الرقمي، إذ يقوم الاقتصاد الرقمي على حقيقتين هما:

1- التجارة الإلكترونية

2- تقنية المعلومات

يتكون مصطلح التجارة الإلكترونية من مقطعين هما: (التجارة) وهي نشاط اقتصادي تجاري معروف عند الجميع، والذي يتم من خلاله تداول السلع والخدمات وفقا لقواعد ونظم متفق عليها.

و(الإلكترونية) التي يقصد بها عملية القيام بأداء النشاط التجاري من خلال استخدام تكنلوجيا المعلومات والاتصالات الحديثة وبخاصة شبكة الإنترنيت وغيرها.

- **التجارة الإلكترونية:**

هي تنفيذ كل ما يتصل بعمليات بيع وشراء السلع والخدمات والمعلومات من خلال استخدام شبكة الإنترنت او الأنظمة التقنية

مقارنة بين الوسائل التقليدية والإلكترونية في التجارة

أبعاد /عناصر المقارنة	الوسائل التقليدية	الوسائل الحديثة
المدى الجغرافي	ضيق	واسع
قطاعات العملاء	محدودة	كبيرة
الملائمة لظروف العميل	متوسطة	مرتفعة
سهولة الاستخدام	أكثر سهولة	تحتاج لمهارات خاصة
التكلفة	مرتفعة	تميل إلى الانخفاض
المدى الزمني	إطار محدود	مدار الساعة
العلاقة مع العميل	مباشرة / غير مباشرة	مباشرة
التعرف على الاستجابة	محدود /متوسط	مرتفع

- **أنماط التجارة الإلكترونية**

1- التجارة الإلكترونية من الاعمال إلى المستهلك: تشير الى التبادلات الإلكترونية بين المنظمات والعملاء إذ تقوم الشركات أو الموزعين بعرض وتسويق لمنتجاتها ولخدماتها للعملاء وبيعها لهم وتقديم الدعم والخدمات والاجابة عن استفساراتهم الكترونياً وتمثل بيع التجزئة الإلكتروني. ويتم التعامل بين المنظمة والافراد سواء على مستوى السوق المحلي أو الدولي، إذ يقوم الفرد بطلب المنتج من موقع المنظمة على شبكة الإنترنت ويدفع ثمنها بالبطاقة مثال ثم يحصل على المنتج مباشرة أو عن طريق البريد التقليدي إذا كان المنتج غير قابل للتسليم الكترونياً.

2- التجارة الإلكترونية من الاعمال إلى الاعمال: تشير إلى التبادلات التي تتم بين المنظمات كشراء المواد الاولية من الموردين. وتنسيق قنوات توزيع المنتجات والخدمات والاتصال والتنسيق مع جهات النقل والشحن وغيرها باستخدام التكنولوجيا الرقمية، ويشكل هذا النوع من التجارة أغلب معاملات التجارة الإلكترونية، إذ يستحوذ على ما يقارب (80%) من اجمالي حجم التجارة الإلكترونية في العالم.

3- التجارة الإلكترونية من المستهلك إلى الاعمال: تشير إلى اتصال العملاء على شكل مجموعات مع المنظمات باستخدام التكنولوجيا الرقمية لتحقيق مكاسب من خلال استخدام عروض خاصة

كخصم الكمية أو الحصول على منتجات بمواصفات وجودة عالية، إذ يستفيد العملاء من اجتماعهم معاً في تشكيل قوة اقتصادية يخاطبون من خلالها هذه المنظمات.

4- التجارة الإلكترونية داخل المنظمة: تتضمن استخدام المنظمة للتكنولوجيا الرقمية للقيام بنشاطها كتبادل المنتجات والخدمات والمعلومات بين وحدات المنظمة ودوائرها ودعم فرق العمل عبر وظائف اعمال. وتوزيع المراسلات والتعاميم الداخلية، وقد تتضمن تقديم عروض لبيع منتجاتها لأفرادها. وتتم هذه الممارسات داخل المنظمة عبر شبكة الأنترنت.

5- التجارة الإلكترونية بين المستهلك والمستهلك: يكون التعامل بين الافراد المستهلكين أنفسهم، وفيه عمليات البيع والشراء بين مستهلك ومستهلك أخر من خلال وضع إعلانات على الموقع الشخصي في الإنترنت بهدف بيع الأغراض الشخصية أو بيع الخبرات إلى الآخرين ويشمل ذلك المزادات الإلكترونية التي تتم فيها المعاملات التجارية بين الافراد. مثال ذلك قيام مستهلك ببيع منزل أو سيارة أو اي منتج أ خر لمستهلك آخر .

6- التجارة الإلكترونية بين الحكومة والمواطنين: تشكل التفاعل بين الحكومات ومواطنيها. الكترونيا والفكرة الرئيسة هنا هي تمكين المواطنين من طلب وتلقي السلع والخدمات والمعلومات التي تقدمها الحكومة والاجابة عن اي استفسارات من منازلهم أو سياراتهم أو اي مكان آخر في اي وقت خارج اوقات الدوام الرسمي ودون مراجعة دوائر الحكومة قدر الامكان مثل التقدم لطلب رخصة او هوية وتمكنه من دفع الضرائب الكترونيا واستلام المعونات أو الوثائق ومساعدتهم في الحصول على الوظائف ومن تطبيقات الحكومة الإلكترونية أيضاً تحويل المساعدات المالية إلى مواطنيها الكترونياً.

7- التجارة الإلكترونية بين الحكومة الاعمال: تشمل استخدام التكنولوجيا الرقمية في انجاز الإجراءات والمعاملات وعرض القوانين والأنظمة والتعليمات لأعمال قطاعات الاعمال المختلفة وبيع الاعمال الحكومية ومنتجاتها وخدماتها الكترونيا وتسعى الحكومة من خلال هذه المجموعة الى أتمته تفاعلاتها مع الاعمال من خلال تقديم المعلومات والخدمات للأعمال الكترونيا وادارة جمع الضرائب ، ومن اهم التطبيقات التدبير الإلكتروني للحكومة وتتمثل باستخدام الحكومة للإنترنت في البحث عن الموردين لشراء لوازمها واختيارهم ومتابعة تطبيق الاتفاقيات معهم ، والمشاركة في المزادات أو المناقصات الإلكترونية .

8- التجارة الكترونية بين الاعمال والحكومة: تضم كافة انواع العمليات التي تتم بين منظمات الاعمال والجهات الحكومية في إطار تنفيذ التعاقدات الموقعة بين الطرفين والتي بموجبها تنجز هذه المنظمات بنود هذه التعاقدات للوفاء بالتزاماتها تجاه تلك الجهات مثال ذلك توريد احتياجات تلك الجهات من الأجهزة والمعدات والمستلزمات وتنفيذ مقاولات بناء المباني الحكومية فتح طرق الصيانة بمختلف انواعها ...وغيرها.

9- التجارة الكترونية بين الحكومات: تتضمن استخدام التكنولوجيا الرقمية بين الحكومات المختلفة لتبادل المعلومات والخدمات والتسهيلات في إطار اتفاقات التبادل والمواثيق الدولية علاقات الدولة الثنائية والإقليمية.

10- التجارة الإلكترونية داخل الحكومة: تتضمن استخدام الدوائر والأجهزة الحكومية للتكنولوجيا الرقمية للقيام بنشاطاتها كتبادل السلع والخدمات والمعلومات بين هذه الدوائر، ودعم فرق العمل عبر الأجهزة الحكومية، وتوزيع المراسلات والتعميمات الداخلية وقد تتضمن تبادل المعلومات والتنسيق في الإجراءات وخطوات العمل لأفرادها أو اية نشاطات أخرى .

11- التجارة الإلكترونية بين الحكومة والموظفين: هنا تدعم الاعمال الإلكترونية رفع كفاءة الاتصالات بين الحكومة وموظفيها في الاماكن النائية والجغرافية المتباعدة وتقديم المعلومات والخدمات والامتيازات الداعمة للموظفين وعائلاتهم.

12- التجارة الإلكترونية غير الربحية: تحتوي على مختلف أنواع التطبيقات التجارية الإلكترونية تلك التي تتم في إطار الجمعيات الخيرية أو الدينية أو الاجتماعية والتي تكون غاياتها انسانية وتركز على خدمة المجتمع العام، أو شرائح محددة، او تخفيض التكاليف، او تحسين ادارة المنظمة.

- **الاشكال الأساسية للتجارة الإلكترونية بين منظمات الاعمال:**

1- اسواق التبادل الخاصة بتلبية احتياجات البيع والشراء لمنظمة واحدة. وتتم العمليات بين منظمة واحدة وعدة منظمات أو بين عدة منظمات ومنظمة واحدة وتصنف إلى:

أ– سوق المنظمة البائعة: Side-Seller

تقوم فيه منظمة واحدة بالبيع إلى عدد من المنظمات، وايضا تتم المزادات الإلكترونية

ب– سوق المنظمة المشترية: Side-Buyer

تقوم فيه منظمة واحدة بشراء احتياجاتها من عدة منظمات. وأيضا تتم فيه المناقصات الإلكترونية

2- أسواق التبادل العامة:Exchange Public

أعداد كبيرة من المنظمات البائعة والمنظمات المشترية، وتسمى أيضاً "المجتمعات الإلكترونية. E- Communities" وهي مملوكة ومدارة بواسطة جهة ثالثة.

3- التجارة الإلكترونية التعاونية:commerce-e Collaborative

يتم التعامل بهدف التعاون بين المنظمات في تصميم منتج ما، أو التشارك في تصنيعه.

- **مكونات نظام الشراء الإلكتروني: تتضمن الوحدات الوظيفية التالية:**

- وحدة إدارة الفهارس: إضافة المنتجات الجديدة للفهرس أو لتعديل مواصفات المنتجات الموجودة فيه.

– وحدة تخطيط العمليات التعاونية: تخطيط العمل التعاوني بين المنظمة المشترية وموردها

– وحدة الشراء من خلال الشبكة: دعم عمليات الشراء سواء الفورية او المتكررة

– وحدة معالجة طلبات الشراء: تمكين المنظمة المشترية من إصدار طلبات الشراء وارسالها عبر الشبكة وتنفيذ المناقصات.

- وحدة خدمة الوثائق: توثيق عمليات الشراء

– وحدة تقييم الأداء: تتبع أداء عمليات المشتريات والتحليل الإحصائي

– وحدة خدمة المعلومات: تمكين موظفي المشتريات من ارسال رسائل الكترونية واستقبالها.

– وحدة إدارة النظام: أدوات التحكم بأنشطة المشتريات.

- **الفوائد للمنظمات التي تقوم بالشراء:**

–الشراء من مكان واحد

– إجراء المقارنات بين السلع

– الحصول على خصومات

– عقد صفقة واحدة مع عدة موردين

–معلومات عن كافة التفاصيل دون قيود

–الوصول إلى الموردين الجدد

– سهولة إصدار طلبات الشراء

– التوصيل السريع للمنتجات.

– الشراء من أي مكان وأي وقت

- **المزايا للمنظمات البائعة:**

– قناة توزيع جديدة

– لا تتطلب وجود مخازن

– تقليل الاخطاء اثناء إعداد الطلبيات

– البيع على مدار الساعة واليوم

– الترويج للشركة

– تصريف البضاعة الزائدة

– الخروج للأسواق العالمية.

- **نماذج إيرادات الاسواق التبادلية:**

– تحصيل رسوم مقابل تنفيذ كل عملية تجارية

– رسوم لقاء الخدمات التي توفرها السوق

– رسوم اشتراك تدفع مرة واحدة في السنة

– أجور الإعلانات.

– مصادر ايرادات اخرى.

- **الخدمات التي توفرها السوق الإلكترونية التبادلية:**

خدمات دعم العمليات التجارية:

– تسجيل الاعضاء الجدد

– خدمات محركات البحث

– خدمات الاتصالات

– الحماية والسرية

– توفير البرمجيات

- **التجارة الإلكترونية التعاونية**

هي استخدام تطبيقات التجارة الإلكترونية لتمكين منظمات الاعمال من التعاون في تخطيط وتصميم وتطوير وادارة منتجاتها وإجراء البحوث عليها.

أمثلة التجارة الإلكترونية التعاونية:

- شركات بيع التجزئة والمنظمات المزودة لها
- بين الشركات الصناعية والشركات التي تزودها بالاحتياجات المادية
- بين عدة منظمات لتسريع دورة تصميم المنتجات وتطويرها.
- بين عدة منظمات لتنفيذ مشاريع مشتركة
- إمكانية الاتصال والعمل التعاوني بين منظمات الأعمال وموردها والجهات المشاركة في المشروع.

- **التسويق الإلكتروني**

مجموعة من الأنشطة التسويقية يمكن من خلالها تحديد احتياجات العملاء والمستهلكين ودراسة المنافسين ومن ثم الترويج للخدمة أو المُنتج ضمن خطط تسويقية مدروسة، ويكون تنفيذ هذه الأنشطة عبر منصات الإنترنت والأجهزة الرقمية مثل أجهزة الحاسوب والهواتف الذكية وغيرها. ولأن مفهوم التسويق الإلكتروني يتبع نهجًا خاصاً و أكثر مرونة وفعالية في عمليات التسويق من التسويق التقليدي، بدأ اتجاه الأعمال التجارية والشركات يتزايد نحوه بشكل كبير في تسويق السلع والخدمات.

- **جاهزية الحكومة الإلكترونية في المملكة العربية السعودية**

البوابة الوطنية

هي بوابة إلكترونية تمكن المواطنين والمقيمين والشركات والزوار من أي مكان الوصول إلى الخدمات الحكومية الإلكترونية في المملكة العربية السعودية وتنفيذ التعاملات بها بسرعة وكفاءة عالية، حيث تعتبر المدخل إلى الخدمات الإلكترونية الحكومية. كما تعد البوابة الوطنية منصة لنشر الأخبار والفعاليات المتعلقة بالخدمات الإلكترونية وبالجهات المقدمة لها، وهي بمثابة دليل للجهات الحكومية، بالإضافة لذلك هي توفر البوابة عددا كبيرا من روابط الأنظمة واللوائح والقوانين والخطط والمبادرات السعودية، ويستطيع مستخدم البوابة أن يجد قسم عن المملكة والذي تحتوي صفحاته على معلومات متكاملة عن المملكة العربية السعودية.

أبرز خدمات الحكومة الإلكترونية:

- منصة أبشر: وهي منصة تجمع كافة الخدمات المتعلقة بوزارة الداخلية السعودية، مثل خدمات الجوازات، والأمن العام، والمرور، والأحوال المدنية، وغيرها.
- منصة إيجار: وهي منصة إلكترونية تابعة لوزارة الإسكان السعودية، ومتخصصة بخدمات الإيجار تقدم حلولا تكاملية لقطاع الإسكان التجاري.
- تطبيق كلنا أمن: وهو تطبيق إلكتروني تابع لوزارة الداخلية السعودية، ويختص بالبالغات الأمنية والمرورية باستعمال الموقع والصور أو الفيديو أو الصوت.
- السجل التجاري الإلكتروني: مكّنت وزارة التجارة والاستثمار (السعودية) الأفراد من استخراج سجلات تجاريّة إلكترونياً دون الحاجة لمراجعة فروع الوزارة.
- لسحابة الإلكترونية الحكومية: وهي سحابة تقدم للقطاعات الحكومية خدمات جاهزة، من ناحية البنية التحتية أو منصات التكامل والربط البيني أو التطبيقات الوطنية المشتركة.

- **الحكومة الإلكترونية المتنقلة**

الثورة في عالم الهواتف الذكية و الأجهزة الذكية دفع الخبراء إلى التفكير بتطوير الخدمات الإلكترونية التي تقدمها الحكومة الإلكترونية واستغلال انتشار الأجهزة الذكية حيث ظهر مفهوم الحكومة الإلكترونية المتنقلة كامتداد للحكومة الإلكترونية حيث يتم باستخدام جميع أنواع التكنولوجيا والخدمات والتطبيقات و الأجهزة اللاسلكية و المتنقلة لتحسين الفوائد التي تعود على الأطراف المشاركة في الحكومة الإلكترونية بما في ذلك المواطنون و الشركات و جميع وحدات الحكومة و بذلك تصل الخدمات الحكومية الرقمية إلى المواطنين والمسؤولين أثناء تنقلهم من دون الارتباط بمكان حول العالم حيث يمكن للحكومة الإلكترونية المتنقلة توفير الوقت والجهد لمواطنيها بحصولهم على الخدمات العامة الحكومية على هواتفهم.

- **الرؤية المستقبلية للحكومة الإلكترونية**

قدمت رؤية السعودية 2030 وعداً بتوسيع نطاق الخدمات الإلكترونية المقدمة، لتشمل الخدمات الصحية والتعليمية. كما وعدت بتحسين جودة الخدمات الإلكترونية المتوافرة حالياً.

الأسئلة

1. هي قدرة الأجهزة والهيئات الحكومية على إتاحة المعلومات وتقديم الخدمات الحكومية فيما بينها وبين المواطنين ومنظمات الأعمال والجهات الأخرى التي تتعامل معها بأسلوب سهل ويسر وسريع وأكثر مرونة وفي أي وقت 24 ساعة يوميًا طوال الأسبوع			
الحكومة الإلكترونية	البوابة الوطنية	الإدارة الإلكترونية	الرقابة الإلكترونية
2. تتضمن فوائد الحكومة الإلكترونية من وجهة نظر المواطن وهو تحقيق قدرًا من الشفافية من خلال الإتاحة الشاملة والمتساوية لمعظم المعلومات			
صح	خطأ		
3. تتضمن فوائد الحكومة الإلكترونية من وجهة نظر الحكومة أو المنظمات الحكومية وهي تتيح لها الاستجابة السريعة لطلبات السوق من خلال التفاعل مع العملاء.			
صح	خطأ		
4. وهي الخدمات المتخصصة لموظفي الحكومة، وقد تستخدم الحكومة شبكة اتصال داخلية للتفاعل مع موظفيها فيما يتعلق بمعلومات الموارد البشرية والتقاعد والإصدارات الجديدة			
G2C	G2B	G2E	G2G
5. هي شكل من أشكال التعاملات الإلكترونية الحكومية التي تتم بين الحكومة والمواطن			
G2C	G2B	G2E	G2G
6. هي منظومة متكاملة تهدف إلى تحويل العمل الإداري العادي من إدارة يدوية إلى إدارة باستخدام الحاسب وذلك بالاعتماد على نظم معلوماتية قوية تساعد في اتخاذ القرار الإداري			
الإدارة التقليدية	الإدارة الالكترونية	الرقابة الإلكترونية	التخطيط لإلكتروني
7. من أهداف الإدارة الإلكترونية تبسيط الإجراءات وسرعة الإنجاز ورفع المستوى			
صح	خطأ		
8. من فوائد الإدارة الإلكترونية إدارة أعمال المؤسسة التي تشمل التخطيط والتنفيذ والتقييم والمتابعة وإدارة العملاء			
صح	خطأ		
9. من متطلبات الإدارة الالكترونية التي تسهل عمل الإدارة الإلكترونية وتضفي عليها المشروعية والمصداقية وكافة النتائج القانونية المترتبة عليها.			
وجود التشريعات والنصوص القانونية	توفير الامن الالكتروني والسرية	توفر الإرادة السياسية	الكوادر البشرية
10. من متطلبات الإدارة الالكترونية الوسائل التي يستطيع الأفراد بواسطتها التواصل معها ومنها أجهزة الكمبيوتر الشخصية والمحمولة والهاتف الشبكي			
توافر مستوى مناسب من التمويل	توافر الوسائل الإلكترونية	توفر الإرادة السياسية	توافر عدد لا بأس به من مزودي الخدمة
11. التقسيم الإداري هو عبارة عن قاعدة تجميع المراكز والأنشطة والوظائف في إدارات وأقسام و الخبرة و أوجدت التقسيمات الإدارية على أساس			
المنتج	العاملين	المهام	الكوادر البشرية
12. واجهت ..... في السابق تحديين أساسيين تمثلا في المهام والعاملين، ومع تطور الفكر الإداري تحولا إلى مدخلين هما: المدخل المرتكز على المهام والمدخل المرتكز على العاملين			

الرقابة الالكترونية	التنظيم الالكتروني	القيادة الالكترونية	التخطيط كتروني
13. هي..... تتمثل في مجموعة اللوائح والسياسات والقواعد والإجراءات المكتوبة التي توجه العاملين وتحدد يقة استجابتهم في تأدية أعمالهم			
الرسمية	المركزية واللامركزية	الهيكل التنظيمي	التقسيم الإداري
14. القيادة الالكترونية تحدد بثلاث مداخل أساسية			
صح	خطأ		
15. خط السلطة المستمر الذي يمتد من مستويات التنظيم العليا إلى مستويات التنظيم الدنيا			
التقسيم الإداري	سلسلة الأوامر	الرسمية	الهيكل التنظيمي
16. يقصد به تحقيق الحماية لمحتوى الرسائل أو البيانات ضد محاولات التغيير أو التعديل أو المحو			
الموثوقية	السرية	الخصوصية	تأمين البيانات
17. يرتبط بالأنظمة التقنية والشبكية والأجهزة والبرامج المستخدمة في التطبيقات الإلكترونية			
البعد التقني	البعد الإنساني	البعد المؤسسي	البعد البيني
18. الإجراءات غير الفنية (المادية والادارية) لحماية الحكومة الالكترونية مثل البصمة الالكترونية			
صح	خطأ		
19. ينتج عنها حصول المجرم على فوائد مادية ومعنوية مع تحميل الضحية خسارة مقابلة			
مخاطر العنصر البشري	مخاطر من الطبيعة البيئية	المخاطر الناتجة عن جرائم المعلوماتية	مخاطر أجهزة خابرات
20. الفيضانات والزلازل والأعاصير مثال للمخاطر من الطبيعة البيئية			
صح	خطأ		
21. القدرة على التلاعب بالشفرة البرمجية بحيث يتركون وراءهم أبوابًا مفتوحة الأنظمة (Back Door)			
خطر المؤسسات التجارية	خطر مزودي البرمجيات والعتاد	خطر أجهزة خابرات الخارجية	خطر عدم الوعي مخاطر
22. هو المواطن أو صاحب المؤسسة الحاصل على إجازة من الحكومة واستخدام خدماتها الالكتروني			
خطر المستخدم الشرعي	خطر أجهزة المخابرات	خطر المنظمات هابية	خطر مزودي رمجيات
23. يعتبر من أهم ركائز النجاح لاي شركة تجارية			
الحكومة الالكترونية	التجارة الالكترونية	التسويق الالكتروني	مراكز الخدمات
24. من أوجه المقارنة بين الوسائل التقليدية انها .....والوسائل الحديثة ..... من حيث التكلفة في التجارة			
مرتفعة – تميل الى الانخفاض	منخفضة – مرتفعة	متوسطة – مرتفعة	محدودة – مرتفعة
25. من أوجه المقارنة بين الوسائل التقليدية انها .....والوسائل الحديثة ..... من حيث المدى الجغرافي في التجارة			
محدودة – كبيرة	ضيق – واسع	مباشر – غير مباشر	واسع – اطار حدود
26. التبادلات الالكترونية بين المنظمات والعملاء اذ تقوم الشركات أو الموزعين بغرض تسويق منتجاتها			
التجارة الالكترونية من الاعمال الى ستهلك	التجارة الالكترونية من المستهلك ى الاعمال	التجارة الالكترونية خل المنظمة	التجارة الالكترونية ى الحكومة مواطنين
27. يتم التعامل بهدف التعاون بين المنظمات في تصميم منتج ما او التشارك في تصنيعه			

سوق المنظمة البائعة	التجارة الالكترونية التعاونية	سوق المنظمة شترية	أسواق التبادل امة
28. التجارة الالكترونية تشمل نوعين من العمليات			
صح	خطأ		
29. هو الشراء عند الحاجة وبالأسعار السائدة في ذلك الوقت			
الشراء الفوري	التزود الالكتروني	أسواق شامله	أسواق متخصصة
30. تقوم فيه منظمة واحدة بالبيع الى عدد من المنظمات وايضاً تتم المزادات الالكترونية			
سوق المنظمة البائعة	سوق المنظمة المشترية	أسواق التبادل العامة	التجارة الالكترونية عاونية
31. هي بوابة الالكترونية تمكن المواطنين والمقيمين و الشركات و الزوار من أي مكان الوصول الخدمات			
الحكومة الالكترونية	الحكومة الالكترونية المتنقلة	البوابة الوطنية	الأسواق التبادلية
32. من ابرز خدمات الحكومة الالكترونية السحابة الالكترونية الحكومية			
صح	خطأ		
33. كانت بدايات فكرة الحكومة الإلكترونية في الواليات المتحدة الأمريكية بصدور قانون الضمان الاجتماعي			
1935م	1937م	1955م	1958م
34. مزايا نموذج سوق الجهة المشترية (طرق الشراء الالكتروني)			
تقييم الموردين	الشراء من المورد مباشرة	تحقيق إيرادات اعلى	تقليل تكلفة الشراء
35. هو يحول من التخطيط الزمني المنقطع (وضع التقارير الفصلية) إلى التخطيط المستمر			
التخطيط الالكتروني	تقسيم العمل الإداري	المعلومات الرقمية	التنظيم الالكتروني
36. من مبادئ الحكومة الالكترونية تقليل الاعتماد على العمل الورقي في المعاملات الحكومية.			
صح	خطأ		
37. من معايير وإجراءات أمن المعلومات التحقق من هوية المستخدم			
صح	خطأ		
38. من قواعد المعلومات السرية استخدام كلمات مرور معقدة			
صح	خطأ		
39. تخطيط العمل التعاوني بين المنظمة المشترية وموردها			
وحدة إدارة الفهارس	وحدة تخطيط العمليات التعاونية	وحدة الشراء من لال الشبكة	وحدة معالجة بات الشراء
40. من فوائد التجارة الالكترونية بين منظمات الاعمال			
زيادة انتاجية العاملين في إدارات شتريات والبيع	شبكات الاتصال و ادواتها	توفير البرمجيات	أجور الإعلانات
41. من نظريات الحكومة الالكترونية المبدأ الاجرائي			
صح	خطأ		
42. عبارة عن سلسلة متتابعة من التجارب والمشروعات السابقة لكثير من الدول			
مشروع التعاملات الإلكترونية حكومية	الحكومة	مبادئ الحكومة كترونية	الإدارة الالكترونية

ملخص لمقرر الاختراق الأخلاقي وأساليب الحماية

الفصل الأول
مقدمة في الاختراق الأخلاقي

- مفهوم الاختراق :

الدخول غير المشروع إلى جهاز حاسب ما عن طريق ثغرات في نظام الحماية باستخدام برامج متخصصة يقوم بها محترفون او هواة وذلك للحصول على البيانات أو تدميرها

- آلية الاختراق:

السيطرة عن بعد عن طريق توفر برنامج على كل من جهازي المخترق والجهاز الهدف وتختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق

- مفهوم الاختراق الأخلاقي:

هي عملية إجراء فحصًا شاملاً للأنظمة والأجهزة في شركة أو مؤسسة بهدف اكتشاف الثغرات الأمنية. يتم تنفيذ هذا العمل بشكل قانوني وأخلاقي.

- أهداف الاختراق الأخلاقي :

1. اكتشاف الثغرات البسيطة والمتقدمة
2. تأمين الأنظمة
3. الدفاع ضد الهجمات المستقبلية
4. تقليل الوقت والجهود المطلوبة لاستمرار في مهاجمة الجهاز أو نظام ذاته بصورة مكررة .

- مصطلحات الاختراق:

Malware : مصطلح عام يستخدم للتعبير عن البرمجيات الخبيثة كالفيروسات (Viruses) و الديدان (Worms)

THREAT : بيئة أو وضع قد يقود إلى هجوم محتمل لأمن المعلومات في مؤسسة ما.

Attacker : هو الشخص الذي لديه مهارات و دوافع الاستغلال الثغرات الأمنية على نظام ما للوصول غير المشروع إليه

Exploit : أداة الاستغلال هي طريقة معّرفة الاختراق أمن نظام معلوماتي عن طريق ثغرة.

Vulnerability : خلل تشغيلي أو خطأ في التصميم المنطقي لبرمجية أو في تنفيذها، يمكن أن يقود إلى حدث غير متوقع وغيرٌ مرغوب فيه يؤدي إلى تنفيذ تعليمات مسيئة أو مخّربة للنظام.

Worm : تمتلك الديدان نفس القوة التدميرية للفايروس و لكنها لا تحتاج لتدخل المستخدم لانتقال من هدف آخر بل تفعل ذلك بنفسها بشكل تلقائي.

Virus : برمجية ضارة تصيب ملف ما أو برنامج و غيره و يحتاج إلى أن يتم تفعيله من قبل المستخدم من خلال قيامه بفتح الملف سواء بالنقر المزدوج عليه أو النقر على الرابط

Social Engineering : فن استخدام وخداع الشخص بحيث يقوم بشكل إرادي بكشف معلومات سرية أو بإعطاء المهاجم الفرصة للوصول للمعلومات السرية

Payload : تعليمات برمجية تحدد نتيجة استغلال الثغرات مثل فتح منافذ تكون موجودة داخل برنامج المهاجم

Targeted Attack : اختراق يستهدف شركة معينة وغرض هذا الاختراق دائما هو سرقة البيانات من الشركات

Vulnerability Day-Zero : ثغرة أمنية تم اكتشافها حديثا بدون برنامج إصلاحي أو حل لها للآن

Backdoor : برنامج يبقى مشغلاً على النظام المخترق بهدف التنصت دون أن يلاحظ أحد وجوده وهو يسهل الدخول لاحقاً من دون الحاجة إلى تكرار اختراق الثغرات من جديد

Ransomware : نوع من الفيروسات يجعل الحاسب الهدف غير صالح للاستخدام حتى يتم دفع مبلغًا معيناً من المال لإعادته إلى حالته الأصلية

Phishing /Vishing : رسائل احتيال إلكتروني يتم إرسالها إلي كميات كبيرة من إيميلات الأشخاص بشكل عشوائي أو من خلال الاتصال على هاتف الهدف

State Sponsored Attack : المخترقين الذين يعملون تحت مظلة الأجهزة الحكومية والاستخباراتية التابعة لبلادهم ويتم دعمهم ماديا وخططاً و عددياً ومعلوماتياً من تلك الجهات

Botnet : عبارة عن شبكة من الأنظمة المخترقة يتم التحكم بها عن طريق جهاز حاسب واحد. يسمى bot master

key-logger : نظام يتجسس على ما يدخله المستخدم بواسطة لوحة المفاتيح و يرسله للمخترق و يعتبر أداة أساسية لمجربي الاختراق حيث تستخدم بصورة روتينية.

Target of Evaluate : التحليل أو الهجوم الأمني، سواء كان نظامًا أو برنامجًا أو شبكة.

تجريب أدوات الاختراق على أهداف التقييم المهمة لتحديد الثغرات وسدها للحماية

Advanced Persistent Threat : تطلق على المخترقين الذين يقومون باستخدام برمجيات متطورة ومتقدمة تسمح لهم بالبقاء داخل شبكات الشركات وأجهزتها لمدة طويلة جدا دون أن يتم اكتشافهم .

key-logger : نظام يتجسس على ما يدخله المستخدم بواسطة لوحة المفاتيح ويرسله للمخترق ويعتبر أداة أساسية لمجربي الاختراق حيث تستخدم بصورة روتينية.

Spyware/Adware : برنامج مصمم لعرض إعلانات على جهاز الحاسب أو الهاتف الخاص بالمستخدم حين يقوم بجمع المعلومات ومراقبة النشاط الخاص بالمستخدمين من دون موافقتهم يكون حينها اسمه Spyware

- **أنواع المخترقون :**
- القبعة الرمادية : مخترقون ذو نوايا حسنة لكن دون إذن من مالك البيانات ودون معرفته .
- القبعة البيضاء: المخترقون الأخلاقيون
- القبعة السوداء : المخترقون الغير الأخلاقيون
- **مراحل عملية الاختراق:**
- جمع المعلومات
- الفحص والمسح
- الدخول إلى النظام
- تثبيت الاختراق
- مسح واخفاء آثار الاختراق
- **مفهوم اختبار الاختراق:**

قيام الشخص بمحاولة اكتشاف أي ثغرات موجودة في النظام، الموقع أو الجهاز المراد اختراقه بهدف وصوله لغايته والتي قد تكون إما إغلاق هذه الثغرات أو استغلالها وإلحاق الضرر به

الهدف من اختبار الاختراق:

حماية المواقع والبيانات والمعلومات الموجودة على الأنترنت

فوائده للمنظمات: يتم تقديم تقرير مفصل للمنظمات حول نقاط الضعف في أنظمتها، ونتيجة لهذا التقرير، يمكن للمنظمات إغلاق نقاط الضعف في أنظمتها، وتقوية أنظمتها ، وتصبح محمية من الهجمات المحتملة.

- **يوجد طُرق عديدة لاختبار الاختراق وهي 3 أساسية:**

- الصندوق الابيض: اسهل الطرق، حيث يتم إعطاء المخترق كافة المعلومات المتاحة، مثل بيانات مدير النظام
- الصندوق الرمادي: يتم أخذ معلومات بسيطة عن المستخدم كـ اسمه وكلمة المرور وليس مدير للموقع
- الصندوق الاسود: يتم إعطاء المخترق فقط معلومات عن رابط الموقع أو عنوان الأهداف

- **أنواع اختبار الاختراق:**

Testing Internal

يقوم المختبِر بمحاكاة هجوم قد يحدث بواسطة شخص ضار من داخل المؤسسة.

Testing External

تستهدف اختبارات الاختراق الخارجية أصول الشركة المرئية على الإنترنت، مثل تطبيق الويب نفسه، موقع الشركة على الويب، وخوادم البريد الإلكتروني . الهدف من هذا الاختبار هو الوصول إلى البيانات القيمة واستخراجها.

Testing Double-blind

ليس لدى أفراد الأمن السيبراني معرفة مسبقة بالهجوم المحاكي، سيكون الأمر كما هو الحال في البيئة الحقيقية، لن يكون لديهم أي وقت لتعزيز دفاعاتهم قبل محاولة الاختراق.

Testing Blind

يعطى الشخص الذي سيقوم بالاختبار فقط اسم المؤسسة المستهدفة.

Testing Targeted

في هذا السيناريو، يعمل كل من المختبِر وأفراد الأمن السيبراني معاً ويحافظون على تقييم بعضهم البعض لتحركاتهم يعد هذا النوع من الاختبار تدريباً قيماً يزود فريق الأمن السيبراني بالمؤسسة بتعليقات في الوقت الفعلي من وجهة نظر المخترق.

الفصل الثاني
الاستطلاعFootprinting

- الاستطلاع Footprinting :

يقصد بمرحلة الاستطلاع هو جمع المعلومات عن المنظمة المستهدفة أو بالتحديد شبكة المنظمة المستهدفة فقبل أن يقوم المخترق باختراق نظام المعلومات في منظمة ما فإنه يقوم أولا بالتحضير والاعداد لهذا الاختراق من خلال جمع كل المعلومات الممكنة و المتوافرة عن شبكة المنظمة التي يريد اختراقها و المعلومات التي يتم تجميعها في مرحلة الاستطلاع تساعده في أمور كثيرة مثل تحديد الاهداف ذات القيمة العالية في المنظمة المستهدفة و تحديد مواقع وجود المعلومات المطلوبة و الحصول على بيانات يمكن من خلالها بدء الهجوم مثل عناوين IP للحواسب الموجودة في المنظمة.

ومرحلة الاستطلاع Footprinting تتميز بالسعة وعدم التحديد و يقوم فيها المخترق بجمع كل المعلومات عن المنظمة مهما كانت تبدو عديمة القيمة و يستخدم في ذلك مصادر مختلفة للمعلومات في شبكة الانترنت أو على الواقع فهي نوع من البحث الشامل غير المحدد عن المعلومات يطلق على هذه العملية مصطلحReconnaissance أوFoot printing

الهدف من عملية الاستطلاع والتهديدات الناتجة منها:

تهدف مرحلة الاستطلاع إلى تكوين نظرة شاملة لنظام الحاسب الآلي المستهدف والمنظمة التي ينتمي إليها ذلك النظام و ذلك بغرض إيجاد طرق اقتحام النظام المعلوماتي للمنظمة و الدخول إليه لسرقة المعلومات المهمة.

- تتميز مرحلة الاستطلاع Footprinting بـ:

1. الشمولية
2. السعة

- خطوات الاستطلاع Footprinting :

1. جمع المعلومات الاساسية حول الهدف وشبكته.
2. تحديد نظام التشغيل المستخدم ومنصات التشغيل وإصدارات خادم الويب.
3. استخدام بعض التقنيات مثل Whois وDNS
4. البحث عن الثغرات الامنية واستخدامها في الهجوم على الشبكة الهدف.

- التهديدات التي تنتج بسبب عملية الاستطلاع:

1. الهندسة الاجتماعية
2. تنفيذ هجمات على النظام والشبكة
3. تسرب المعلومات
4. فقدان الخصوصية
5. تجسس المنظمات
6. الخسائر التجارية

- أنواع الاستطلاع Footprinting :

1. الاستطلاع النشط

جمع المعلومات بالتفاعل مع الهدف بشكل مباشر، مثال أن يقوم المخترق بتصفح الموقع الالكتروني الخاص بالهدف وهذا سيظهر للهدف بأن هناك من يتصفح موقعه ويجمع المعلومات عنه بدون اختراق لأنه يتطلب التخاطب مع مكونات الشبكة لاكتشاف الحواسيب الشخصية وعناوين الانترنت والخدمات مما يعطي للمخترق مؤشرات عن إجراءات الامن المطبقة، ولكن يزيد من فرصة الإمساك بالمخترق أو الشك بوجوده والمخترق هنا يقوم بالتركيز على موظفي المنظمة الهدف للحصول على المعلومات منهم باستخدام تقنية الهندسة الاجتماعية.

2. الاستطلاع السلبي

يعني جمع المعلومات دون التفاعل مع الهدف ولن تكون الجهة المستهدفة على علم بأن هناك من يجمع المعلومات عنها مثل جمع المعلومات من مواقع الانترنت أو عن طريق الهندسة الاجتماعية والمصادر المفتوحة المجانية للمعلومات تعتبر من أسهل الطرق في جمع المعلومات عن الهدف وهي تشير إلى عملية جمع المعلومات من المصادر المفتوحة أي من المصادر العامة المتاحة وهذا النوع قانوني مثل الصحف والمجلات والتليفزيون ومواقع التواصل الاجتماعي.

- تعريف محركات البحث:

هو برنامج حاسب مصمم للمساعدة في العثور على مستندات مخزنة في شبكة الانترنت، ويسمح للمستخدم أن يطلب المحتوى الذي يقابل معايير محددة ويستدعي قائمة بالمراجع التي توافق هذا المعيار، تستخدم محركات البحث الفهارس لتنفذ العمليات بسرعة ومحركات البحث على شبكة الانترنت و العديد من محركات البحث تسمح بالحصول على المعلومات عن المنظمة الهدف مثل تفاصيل الموظفين .

- تعريف Whois :

البحث في موقع Whois وهو عبارة عن قواعد بيانات متعددة تتضمن معلومات التسجيل الخاصة بالمنظمة وتعتمد آلية البحث في Whois على استيراد المعلومات من سجلات تسجيل أسماء وأرقام الانترنت.

- **أدوات Foot Printing :**

Ping

يستخدم البرنامج ping في معرفة ما إذا كان الحاسب الالي متصلا بالإنترنت ويعمل وتقوم هذه الاداة بتوليد رسالة طلب اتصال وإرسالها إلى النظام الهدف و تسأل هذه الرسالة الحاسب الالي الهدف ما إذا كان لازال متصلا و في حالة ما إذا كان الهدف فعالا و متصلا بالإنترنت.

Dmitry

أداة لديها القدرة على جمع أكبر قدر من المعلومات عن الهدف من هذه المعلومات النطاقات الفرعية subdomain

سجلات DNS

هي عبارة عن مدخلات فردية تقدم تعليمات خاصة بالتعامل مع المعلومات Records DNS أو DNS التي يتم تداولها عبر الموقع سجلات مخصصة للتعامل مع معلومات محددة وغير قياسية.

Nslookup

هو الاداة التي يمكن استخدامها لاستعلام من خوادم DNS والحصول على سجلات حول مختلف المضيفين.

الفصل الثالث
المسح والتعداد Enumeration and Scanning

- منهجية المسح(الفحص)Scanning

بعد جمع المعلومات لا يستطيع المخترق الوصول إلى أي حاسب آلي بعيد واختراقه إلا إذا كان هذا الحاسب متصلا بالإنترنت أو بشبكة المؤسسة التي ينتمي إليها

فالفكرة هي اكتشاف قنوات الاتصال للاستغلال هذه القنوات حيث يتم التعرف على الانظمة المتصلة والقابلة للوصول عبر الانترنت من خلال إرسال إشارة اتصال إلى عنوان IP لحاسب الهدف وفي حال إذا استجاب الحاسب الهدف لهذه الرسالة فسيعرف أن هذا الحاسب متصل و فعال.

كما أن في هذه المرحلة يمكن للمخترق العثور على طرق مختلفة الاختراق النظام المستهدف واكتشاف المزيد من المعلومات.

- يوجد عدة أنواع للفحص وهي:

1. فحص المنافذ Scanning Port

يستخدم في المنافذ والخدمات، المنافذ تُمثل الأبواب و النوافذ لهذ النظام ويستخدمها المتسللون و المخترقون للوصول إليه حيث المزيد من المنافذ المفتوحة تعني المزيد من نقاط الضعف و عدد أقل من المنافذ المفتوحة تعني المزيد من الأمان.

2. فحص الشبكات Scanning Network

يستخدم في فحص عناوين IP فيتم فيها جمع معلومات حول عناوين IP التي تم جمعها من مرحلة الاستطلاع للوصول إليها عبر الشبكات وبنيتها والخدمات التي تعمل عليها قبل الاختراق.

3. فحص نقاط الضعف Scanning Vulnerability

يستخدم لفحص الضعف.

- منهجية المسح(الفحص)Scanning

1. تحديد الأهداف: هو التعرف على الحواسيب المتصلة التي تعمل على الشبكة و الخدمات و التطبيقات و البرامج التي تشغلها هذه الحواسيب والتي تُعد منافذ يمكن الدخول من خلالها إلى النظام أي:

-اكتشاف الاجهزة المتصلة ، عنوان IP ، المنافذ المفتوحة التي تعمل على الشبكة

-اكتشاف أنظمة التشغيل و بنية النظام المستهدف لا ن المخترق سيبني الهجوم على أساس نقاط الضعف في نظام التشغيل.

-اكتشاف خدمة الشبكة مع كل منفذ.

-تحديد نقاط الضعف و التهديدات.

2. مسح المنفذ

المنفذ هو قناة اتصال للبيانات التي يسمح جهاز الحاسب تبادل البيانات مع جهاز أخر، برمجيات واستخدام منافذ متعددة في وقت واحد يسمح للاتصال دون الحاجة الانتظار.

3. التنصت

هو الاستماع سرا إلى المحادثات بين الافراد من خلال الهاتف أو محادثات الفيديو بدون علمهم ويشمل أيضا قراءة الرسائل السرية من وسائط الاتصال مثل الرسائل الفورية أو رسائل الفاكس لجمع المعلومات.

4. فحص الضعف

هو عملية البحث عن الثغرات في الخدمات التي تعمل باستخدام أدوات معينة مثل Nmap ، Hping أي هو عملية التحقق من وجود منافذ TCP, UDP مفتوحة على الجهاز.

- تعدادEnumeration

هي عملية لجمع معلومات معينة متعلقة بالنظام الهدف من خلال معرفة المنافذ المفتوحة ونظام التشغيل والخدمات التي تعمل والتطبيقات المدعومة بالنسبة لمختبر لاختراق البيانات المعادة تكشف الاجهزة المتصلة وهذا يستخدم من أجل التعرف على الهدف قبل الهجوم . أي (جمع المعلومات) بإنشاء اتصال نشط مع الضحية ومحاولة اكتشاف أكبر قدر ممكن من نواقل الهجوم، والتي يمكن استخدامها لاستغلال الانظمة بشكل أكبر.

تقنيات يمكن استخدامها للحصول على معلومات حول:

- مشاركة موارد الشبكة
- بيانات SNMP ، إذا لم يتم تأمينها بشكل صحيح
- جداولIP
- أسماء المستخدمين للأنظمة المختلفة
- قوائم سياسات كلمات المرور

تعتمد التعدادات على الخدمات التي تقدمها الأنظمة. و أنواعها هي:	
تعدادDNS (DNS ENUMERATION)	ينفذها المهاجم لتحديد خادم DNS و سجلات المنظمة المستهدفة يجمع معلومات قيمة عن الشبكة الهدف مثل أسماء المضيفين و الأجهزة والمستخدمين
تعدادNTP (NTP ENUMERATION)	جمع معلومات مثل قوائم المضيفين (Lists of hosts) المتصلة بخادم NTP، عناوينIP، أسماء النظام ، نوع نظام التشغيل على أنظمة العميل في الشبكة
تعداد SNMP (SNMP ENUMERATION)	عملية تعداد حسابات المستخدمين والأجهزة الموجودة على جهاز حاسب تم تمكينSNMP فيه
تعداد LDAP (LDAP ENUMERATION	الوصول إلى قوائم الدليل Active Directory و تستخدم من قبل المهاجمين للوصول إلى أسماء المستخدمين و العناوين

- تقنية Banner Grappling Enumeration

تقنيات يتم استخدامها من قبل المخترقين لمعرفة المعلومات المهمة مثل أنواع الاجهزة ، أنظمة التشغيل إصدار التطبيقات المستخدمة من قبل الجهاز المستهدف مع مساعدة المعلومات التي تم جمعها فالمخترق يستغل الثغرات الامنية التي لم يتم تحديثها من قبل تصحيحات الامان (patches Security ومن ثم إطلاق هجماته.

الفصل الرابع
التصنت والتهرب Evasion and Sniffing

- التصنت:

عملية مراقبة والتقاط جميع الحزم التي تمر عبر شبكة معينة باستخدام أدوات التصنت.

- طريقة عمل التصنت:

عادةً ما يقوم المُتصنت بتحويل بطاقة واجهة الشبكة (NIC) الخاصة بالنظام الهدف إلى الوضع المختلط بحيث يستمع إلى جميع البيانات المرسلة.

- يمكن أن تؤدي هجمات التنصت إلى:
- فقدان معلومات العمل المهمة.
- اعتراض خصوصية المستخدمين
- تؤدي إلى هجمات أوسع
- سرقة الهوية
- التصنت على المعلومات الحساسة التالية من الشبكة:
- التصنت الإيجابي والسلبي
- حركة البريد الإلكتروني
- كلمات مرور بروتوكول نقل الملفات
- حركة المرور على شبكة الإنترنت
- كلمات مرورtelnet
- تكوين جهاز التوجيه
- جلسات الدردشة
- حركة مرورDNS

- أنواع التنصت

1 – التصنت السلبي

في التصنت السلبي، يتم غلق حركة المرور، ولكن لا يتم تغييرها بأي شكل من الأشكال .يسمح بالاستماع فقط. لا يرسل حزم، بل يكتفي المتصنت بالتقاط و مراقبة الحزم المرسلة من الآخرين ، و يعمل مع أجهزةHub

طريق التصنت السلبي:

- تثبيت حصان طروادة
- اختراق شبكة الهدف

2– التصنت الإيجابي

عملية التصنت الإيجابي، لا يتم غلق حركة المرور ومراقبتها فحسب، بل يمكن أيضا تغييرها بطريقة ما وفقاً لما يحدده الهجوم. يتم استخدام التصنت الإيجابي للتصنت على الشبكة القائمة على المحول. يتضمن ذلك حقن حزم دقة العنوان(ARP) في الشبكة المستهدفة لإغراقها في جدول الذاكرة القابلة للعنونة(MAC) لمحتوى المحول تقوم (MAC) بتتبع المضيف المتصل بأي منفذ.

طرق التصنت الإيجابي:

- MAC Flooding
- هجمات DHCP
- تسمم DNS (DNS Poisoning)
- هجمات الانتحال(Spoofing Attacks)
- التسمم بـARP (ARP Poisoning)

- الأجهزة المضادة:

أنظمة كشف التطفلIDSs

الهدف منها التقاط أي شيء مريب أو مشكوك فيه يحدث في الشبكة والتنبيه على ذلك بشكل رسالة على الشاشة الخاصة بمدير النظام أو بريد الكتروني فهي تقوم بفحص البيانات وسجلات الأحداث وكشف أي بيانات غير طبيعية والتنبيه عليها وتتكون من الحساسات Sensors وأدوات التحليل Analyzing toolsوواجهات التواصل مع مديري الأنظمةinterfaces .

أنظمة منع التطفل IPSs

تكشف البيانات والأنشطة غير الطبيعية ثم تمنعها من الوصول إلى أهدافها فهي تقوم بخطوات استباقية لمنع المتطفل من الوصول إلى أهدافه و تقطع الاتصال و توقف عمل الأجهزة في حالة وجود بيانات أو أنشطة مريبة على الشبكة.

الشبكة الافتراضية الخاصةVPN

توفّر اتصالا مشفّراً عبر الإنترنت من جهاز إلى شبكة، ويساهم ذلك في توفير نقل آمن للبيانات الحساسة عبر الشبكة، وكذلك السماح للمستخدمين بالعمل عن بعد مع مؤسساتهم، حيث إنها تضمن منع التنصت على حركة المرور .

- التقنيات الحماية من عمليات التصنت والتهرب:

Snort

هو نظام كشف تسلل للحزم يفحص كل حزمة عن لاكتشاف حالات مشبوهة

Firewall

جهاز أمان للشبكة يراقب حركة مرور الشبكة الواردة والصادرة ويقرر ما إذا كان سيتم السماح بحركة مرور معينة أو حظرها بناءً على مجموعة محددة من قواعد الأمان.

الفصل الخامس
اختراق انظمة التشغيل

- منهجية أمان نظم التشغيل

المقصود بمنهجية أمان نظام التشغيل هو الخطوات أو التدابير المحددة المستخدمة لحماية نظام التشغيل من التهديدات، أو الفيروسات، أو الفيروسات المتنقلة، أو البرامج الضارة، أو عمليات اختراق المهاجمين عن بُعد.

كما تشمل منهجية أمان نظام التشغيل جميع تقنيات التحكم الوقائي في حالة تعرض أمان نظام التشغيل للخطر.

- أمان نظام التشغيل

هو عملية ضمان سلامة نظام التشغيل وسريته وتوافره.

- كيف يحمي نظام التشغيل نفسه

يمنع تشغيل البرامج الضارة من النوع المعقد والخطير

- مزايا الأمان في نظام التشغيل

1– إدارة حسابات المستخدمين

2– تحديثات الامان Updates Security

3–حالة الدعم التقني

- خطوات الاختراق في نظام التشغيل

يتم الاختراق عبر خدمات الاتصال عن بعد عن طريق خطوتين رئيسيتين:

1– كسر كلمات مرور هذه الخدمات

2– هجوم رفع الامتياز

- المصادقة وكلمة المرور

1– يوفر الامان آلية للتحقق من هوية المستخدم أو العملية للسماح له باستخدام النظام.

2– يوفر الوصول إلى النظام للمستخدمين المصرح لهم فقط.

- أدوات مهاجمة كلمات المرور

بعد كتابة اسم المستخدم يحاول كسر كلمة السر باستخدام أشهر الادوات و هي Hydra ، Cain و تعتمد هذه الادوات على تجربة تركيبات مختلفة من اسم المستخدم و كلمة المرور محفوظة في ملف عندها و Ip للنظام المخترق يقوم بتسجيل عنوان الهدف و نوع الخدمة المطلوب الاتصال بها و عند ذلك ترسل الاداة تركيبة من اسم المستخدم و كلمة المرور إلى الخدمة فإذا كانت التركيبة

خاطئة يتم عرض رسالة خطأ و يفشل الدخول فتقوم الأداة بإرسال تركيبة أخرى ويتكرر ذلك إلى أن تنجح الأداة في العثور على كلمة المرور الصحيحة أو تستنفذ كل التخمينات الموجودة فيها.

- الادوات:

Cain :

Cainهي واحدة من أفضل أدوات الاختراق لاختراق كلمات المرور واستعادة كلمة المرور لنظام التشغيل Windowsواجهة المستخدم الرسومية للبرنامج بسيطة للغاية وسهلة الاستخدام. ولكن لديها قيود على التوافر، الاداة متاحة فقط على windows.

Hydra:

أداة Hydraهي أداة اختبار تخمين كلمات المرور المستخدمة في أنظمة Linux و Windows والبروتوكولات المختلفة مثل FTP و SSH و Telnet و SMB وغيرها. وهي تستخدم أسلوب هجوم Force Brute القوة الغاشمة وأداة لمهاجمة أنظمة البريد الالكتروني.

- التدابير المضادة والحماية من عمليات المهاجمة:
- أداء تحديثات نظام التشغيل العادية
- تفعيل جدار الحماية Firewall
- تشفير محركات الاقراص
- استخدام كلمات مرور قوية للحسابات على الانترنت
- استخدام خيار شبكة الضيوف
- إعداد رمز مرور قوي لتأمين الاجهزة والاستفادة من ميزات الأمان العالية التي توفرها الطرق البيو مترية.
- استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة والتجسس تحديثها بانتظام
- تحديد الموظفين ذوي المسؤوليات.
- نشر التوعية بالهندسة الاجتماعية وطرق الحماية منها
- الحماية من برنامج Keyloggers
- تقييد امتيازات الدخول للتأمين

الفصل السادس

اختراق أنظمة الويب والتطبيقات

- خوادم الويب:

هو الجهاز الذي يستضيف تطبيق الويب وهو هدف للمهاجم لأنه يحتوي على منافذ Ports مفتوحة وثغرات بالإضافة إلى أخطاء في إعدادات نظام التشغيل أو وجود الاعدادات الافتراضية دون إعادة ضبطها للتوافق مع إعدادات الامان.

أما تطبيقات الويب application Web فهو برنامج مبني بالاعتماد على الويب ليؤدي وظيفة تعتمد على التفاعل مع المستخدم وعندما يتفاعل المستخدم مع موقع الويب ليقوم بمهمة مثل تسجيل الدخول أو التسوق أو التفاعل من خلال مواقع التواصل الاجتماعي.

- بنية خوادم الويب:

هو برمجية Software تعمل داخل نظام التشغيل الخادم Server والذي يسمح للاتصال بالوصول إلى تطبيق الويب.

أكثر الخوادم انتشارا هي:

• IIS (Services Information Internet) وهو يعمل على أنظمة ويندوز.

• Server Apache وهو يعمل على أنظمة لينكس.

- **طرق الهجوم على خوادم الويب:**

1– عبر موقع البرمجة:

البرمجة النصية عبر المواقع (XSS)هو نوع من الهجوم يسمح للمهاجمين بحقن تعليمات برمجية ضارة في صفحة ويب. ثم يتم تنفيذ هذا الرمز من قبل المستخدمين الذين يزورون الصفحة، مما يؤدي إلى تنفيذ الشفرة الضارة للمهاجم.

- **هناك نوعان رئيسيان من هجمات XSS:**

1– هجمات XSS انعكاسية

هجمات XSS العاكسة تحدث عندما يتم حقن الشفرة الخبيثة في الصفحة ثم تنعكس فورًا على المستخدم دون تخزينها على الخادم.

2 – هجمات XSS المستمرة

تحدث عندما يتم إدخال الشفرة الضارة في الصفحة ثم تخزينها على الخادم، حيث سيتم تنفيذها في كل مرة يتم فيها الوصول إلى الصفحة.

2– حقن SQL:

حقن SQL هي تقنية حقن التعليمات البرمجية التي تستغل ثغرة أمنية في برنامج موقع الويب. الضعف موجود عندما لم يتم التحقق من صحة إدخال المستخدم بشكل صحيح قبل أن يتم تمريرها إلى قاعدة بيانات. هذا يسمح للمهاجم تنفيذ التعليمات البرمجية الخبيثة SQL مما يُمكنه من معالجة البيانات أو حذفها، أو حتى التحكم في خادم قاعدة البيانات. يعد حقن SQL مشكلة أمنية خطيرة ويمكن استخدامه لمهاجمة أي موقع ويب يستخدم قاعدة بياناتSQL قد يكون من الصعب منع هذا النوع من الهجوم.

3– هجمات DDoS

هجوم الرفض الموزع للخدمة: هو نوع من الهجمات الإلكترونية التي تسعى إلى زيادة تحميل النظام بالطلبات مما يجعله غير قادر على العمل بشكل صحيح. يمكن القيام بذلك عن طريق إغراق الهدف بطلبات من أجهزة حواسيب متعددة، أو باستخدام جهاز حاسب واحد لإرسال عدد كبير من الطلبات. غالبا ما تُستخدم هجمات DDoS لا زاله مواقع الويب أو الخدمات عبر قد يكون من الصعب الدفاع ضدها

4– الهجمات القائمة على كلمة المرور

الهجوم المستند إلى كلمة المرور هو أي هجوم إلكتروني يحاول اختراق كلمة مرور المستخدم. وهناك العديد من الهجمات المستندة إلى كلمة المرور الشائعة. منهجية الهجوم على موقع الويب يمكن ان يتم من خلال:

1– استهداف خادم الويب:

الخادم هو جهاز بمواصفات عالية يقوم باستضافة موقع أو عدد من مواقع الويب، المهاجم يحاول استهداف الخادم من خلال البحث عن ثغرات محتملة في نظام التشغيل الخاص بالخادم أو ثغرات في البرامج التي تعمل على الخادم ومحاولة استغلالها ومن ثم الوصول إلى الملفات الخاصة بالموقع والتعديل عليها أو تخريبها.

2– استهداف موقع الويب:

مواقع الويب يمكن ان تحوي على ثغرات برمجية والتي يمكن للمهاجم استغلالها وتعديل أو تخريب محتوى الموقع وأشهر هذه الثغرات هي XSS and injection SQL.

3– استهداف المستخدم:

يتم ذلك باستخدام الهندسة الاجتماعية كمحاولة لخداع مدير الموقع أو مستخدمي الموقع من اجل الحصول على معلومات تسجيل الدخول الخاصة بهم.

- الثغرات:

1– ثغرات المصادقة وإدارة الجلسة

عملية المصادقة تسمح بتسجيل الدخول إلى موقع الويب بينما إدارة الجلسة تتبع الطلبات والاجابات التي تتم خلال عملية التصفح.

2– ثغرة تجاوز المسار Traversal Directory

تتم عملية تخصيص المساحات التخزينية للمواقع الالكترونية ضمن المخدم المضيف أثناء إعداد وتشغيل مخدم الويب يعمل كل موقع ضمن المساحة المخصصة له والتي تحتوي على الرموز الخاصة بالموقع والصور والملفات بالإضافة إلى قواعد البيانات وملفات المواقع الاخرى

3– ثغرة رفع الملفات Inclusion File

في حال وجود هذه الثغرة فإن المهاجم يستطيع رفع shell عبارة عن رمز برمجي صغير يمكن رفعه إلى مخدم الويب من خلال موقع مصاب بهذه الثغرة وهو يؤمن للمهاجم وصول لمخدم الويب ويسمح له بتنفيذ التعليمات عن بعد.

4– ثغرة الاعداد الخاطئ للحماية

هذه الثغرة تصنف بشكل خاص للتعامل مع الحماية (الضعف في الحماية) وهي متعلقة بنظام التشغيل وخادم الويب ونظام إدارة قاعدة البيانات، هذه المخاطر تصبح اكثر صعوبة عندما لا تؤمن الحماية منع الوصول الغير مسموح به للموقع.

- اختبار اختراق الويب

يساعد على تحديد وتحليل وتقديم تقرير عن نقاط الضعف مثل ضعف التوثيق وأخطاء الاعداد ونقاط الضعف المتعلقة بخادم الويب وهو مفيد في تحديد البنية التحتية للويب والتحقق من وجود ثغرات أمنية للعمل على إصلاحها: الخطوات هي:

1– البحث عن مصادر اختبار مفتوحة للحصول على معلومات حول الهدف

2– استخدام الهندسة الاجتماعية لجمع المعلومات

3– الاستعلام عن قواعد البيانات

4– توثيق جميع المعلومات عن الهدف

5– جمع المعلومات عن خادم الويب

6– تنفيذ هجوم force Brute

7– استخدام Suite Burp لاختطاف الجلسة

8– تنفيذ اختبار اختراق تطبيقات الويب

9– فحص سجلات خادم الويب

10– استخدام أداة Metasploit

11– توثيق جميع النتائج

- التدابير المضادة والحماية من عمليات اختراق خوادم وتطبيقات الويب:

1. استخدام ملف جدار حماية تطبيق الويب (WAF) لتصفية التعليمات البرمجية الضارة.
2. استخدام التحقق من صحة الادخال، مما يعني فحص إدخال المستخدم بحثًا عن تعليمات برمجية ضارة قبل معالجتها بواسطة الخادم.
3. استخدام تشفير الاخراج والذي يحول الاحرف الخاصة إلى معادلات كيان HTML الخاصة بهم.
4. التحقق الدائم من صحة إدخال المستخدم قبل إدخاله في قاعدة البيانات الخاصة.
5. استخدام الاستعلامات ذات المعلمات متى أمكن.
6. مراقبة قاعدة البيانات الخاصة لاي نشاط غريب
7. يمكن استخدام خدمة حماية DdoS ، والتي ستعيد توجيه حركة المرور بعيًدا عن الخادم الخاص بالهدف أثناء الهجوم.
8. يمكن أيضا استخدام شبكة توصيل المحتوى (CDN)مثلCloudflare ، والتي ستوزع المحتوى الخاص بالهدف عبر شبكة من الخوادم بحيث الى يؤدي هجوم على خادم واحد إلى تدمير موقع الويب بالكامل.
9. وضع سياسات كلمات مرور قوية.
10. استخدام مدير كلمات المرور أداة لإنشاء كلمات مرور آمنة وإدارتها وتخزينها.

الفصل السابع
الشبكات اللاسلكية

- تعريف الشبكة:

هي نوع من الشبكات الحاسوبية التي تعمل على نقل المعلومات بين العُقَد من دون استخدام الأسلاك.

- أهداف اختبار اختراق الشبكات:
  - فحص التحكم بالحماية
  - منع المخاطر والاجابة
  - كشف سرقة البيانات
  - تحسين البنية التحتية
  - إدارة نظام المعلومات
  - اكتشاف المخاطر الأمنية
- مصادر تهديد الشبكات اللاسلكية:
  - التقاط تسمية الشبكة
  - الاختراق عبر تسمية جهاز المخترق باسم نقطة التغطية اللاسلكية
  - عدم إلمام المستخدمين بتفعيل إجراءات الحماية
  - التشويش
  - وفرة البرامج المجانية
  - مُعرف مجموعة الخدمة :

Service Set Identifier (SSID)

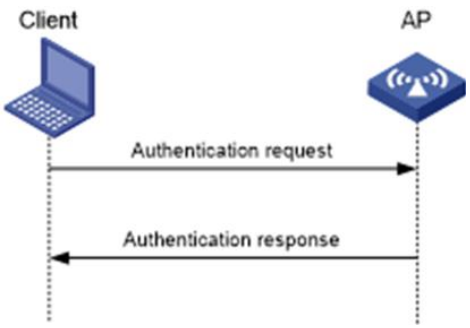
هو الاسم الذي يُعرف الشبكة اللاسلكية وبشكل افتراضي،

هو جزء من Packet header ويرسل عبر الشبكة اللاسلكية المحلية

مثال:"My WiFi Connection"

  - المصادقة بالنظام المفتوح :

Open system authentication في الشبكات اللاسلكية



- تشفير الشبكات اللاسلكية:

إهمال تطبيق الإجراءات الأمنية لحماية الشبكة يعرض بيانات المستخدم والأنظمة المتصلة للمخاطر، لذلك يجب حمايتها بأنظمة التشفير (بروتوكول التشفير).

بروتوكول التشفير	WEB	WPA	WPA/2
اختصارل	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2
نبذة	أول محاولة لتأمين الشبكات اللاسلكية عن طريق تشفير البيانات لمنع الوصول غير المصرح به. ومع ذلك، يُعتبر ضعيفًا وسهل الاختراق.	تم تقديم WPA كتحسين لـ WEP. يشمل آليات مثل TKIP(بروتوكول سلامة المفتاح المؤقت) وفي وقت لاحق، AES(المعيار المتقدم للتشفير)، مما يوفر ميزات أمان أفضل للشبكات اللاسلكية.	إصدار محسن لـWPA . يستخدم CCMP(وضع العداد مع بروتوكول تشفير سلسلة كتلة ورمز مصادقة الرسائل) للتشفير، مما يوفر أمانًا أقوى
نوع التشفير	RC4	TKIP ثم (AES)	AES
طول المفتاح	64 بت (أو 128 بت) أو 265 بت	256 بت (تحسين عن WEP)	256 بت (أقوى تشفير)
تحسينات في سلامة الرسائل	لا	نعم	نعم
مشكلات وعيوب	سهولة الكسر وضعف RC4 طريقة توزيع مفاتيح التشفير من السهل اكتشاف النص	عرضة للاستغلال	عرضة لهجوم إعادة تثبيت المفتاح (KRACK)

- أدوات كسر التشفير (عملي):

Aircrack–brute force

- طرق اختراق الشبكة اللاسلكية:

1– هجوم التحكم بالوصول

2– هجوم سلامة البيانات

3– هجوم الخصوصية

4– هجوم التوافر

5– هجوم المصادقة

يوجد العديد من أدوات اختراق الشبكات اللاسلكية التي يمكن استخدامها لاختبار أمنها مثل:

Kismet

تستخدم في هجوم التجسس وتقوم بفك تشفير البيانات للحصول على المعلومات المهمة

Wardriving

هجوم إلكتروني حيث يجد المتسللون نقاط وصول ضعيفة لشبكةWIFI لتفيد الأمر: Application Menu /Kali Linux / Wireless Attacks / 802.11 wireless Tools / Kismet

Net Stumbler

أحد أفضل البرامج التي يمكن الاعتماد عليها، في الحصول على كلمة السر الخاصة بالشبكات اللاسلكية المفتوحة.

- التدابير المضادة والحماية من اختراق الشبكات اللاسلكية:

1– تجنب استخدام كلمة المرور الافتراضية والحماية باسم مستخدم وكلمة سر جديدة.

2– استخدام أحد طرق تشفير الشبكات اللاسلكية.

3– تغير معرف الشبكة اللاسلكية بتعطيل SSID خيار الاعلان عن معرف نقطة الوصول.

4– وضع نقطة الوصول Access Point في مكان مناسب بحيث تضمن تغطية المكان المراد تغطيته.

5– تحديد قائمة بالأجهزة القادرة على الارتباط بنقطة الوصول.

6– تحديث نظام تشغيل نقطة الاتصال وتثبيت منتج فعال للحماية من البرامج الضارة.

7– التأكد من موثوقية الشبكات اللاسلكية التي يتم الاتصال بها.

8– عدم الاتصال بالشبكات اللاسلكية المفتوحة وتعطيل هذه الخدمة في إعدادات الشبكة اللاسلكية.

9– استخدام أداة Nmap لفحص الشبكات وتحديد الاجهزة المتصلة والخدمات التي تعمل.

10– استخدام أداة Comm view أداة للمراقبة في حال الاتصال بشبكة لاسلكية. لها القدرة على تحليل رزم المعلومات والتحكم في تدفق البيانات ويعرض البرنامج قائمة باتصالات الشبكة.

الفصل الثامن
اختراق الاجهزة المتنقلة

- نقاط الضعف والمخاطر المتنقلة:

1. أمن الأجهزة المتنقلة

- فقدان الجهاز المتنقل
- اخترق التطبيق او اختراقه عند تحميله
- سرقة الهواتف الذكية
- فقدان البيانات والسمعة
- سرقة الهوية

2. تطبيقات الأجهزة المتنقلة

- تخزين غير آمن للبيانات
- آليات المصادقة ضعيفة
- ضعف أمن البيانات والاتصالات وتشفير الاجهزة
- الاذونات المفرطة
- مشكلات تحديثات نظام التشغيل والتطبيقات

3. نقاط الضعف والمخاطر المتنقلة

أداة	OWASP	IP Scanner	NetStumbler
الغرض	أمان التطبيقات	فحص الشبكة وتحديد الأجهزة	اكتشاف وتحليل شبكات Wi-Fi
التركيز	تطبيقات الويب والأجهزة	شبكات الكمبيوتر	شبكات Wi-Fi اللاسلكية
النوع	مجتمعي	فحص الشبكة	تحليل شبكات Wi-Fi
المثال	مشروع OWASP AppSensor	Nmap	NetStumbler
المجال الرئيسي للاستخدام	أمان تطبيقات الويب	أمان الشبكات	تحليل شبكات Wi-Fi

يتم بناء أنواع الثغرات الأمنية على OWASPوهي منظمة خيرية غير ربحية في الولايات المتحدة، لدى OWASP 10 تصنيفات للثغرات الأمنية .

التصنيف	الوصف
استخدام غير سليم للنظام الأساسي	يشمل سوء استخدام ميزات النظام الأساسي أو عدم استخدام ضوابط الأمان بشكل صحيح، مثل أذونات النظام وتقنيات التحقق مثل TouchID.
بيانات غير آمنة	يتعامل مع تخزين وتسريب البيانات غير المحمية بشكل صحيح على الأجهزة المحمولة.
اتصالات غير آمنة	يشمل الهجمات على ضعف المصافحة، وإصدارات SSL غير الصحيحة، والتفاوض الضعيف، والاتصال النصي الواضح للأصول المهمة.
مصادقة غير آمنة	يلتقط مفاهيم مصادقة المستخدم وإدارة الجلسة السيئة، مثل فشل تحديد هوية المستخدم أو الحفاظ عليها، ونقاط الضعف في إدارة الجلسة.
تشفير غير كافٍ	يتناول مشاكل تنفيذ التشفير بشكل غير صحيح، حيث تكون محاولات التشفير موجودة ولكنها غير فعالة.
تفويض غير آمن	يتعامل مع إخفاقات في عمليات التفويض، مثل فشل المصادقة أو الترخيص السليم.
جودة كود العميل	يتناول مشاكل في تنفيذ التعليمات البرمجية على مستوى التعليمات البرمجية للعميل على الأجهزة المحمولة.
Code Tampering التلاعب في الكود	يشمل تحليل الملف الثنائي لتعديل التعليمات البرمجية أو الموارد المحلية بشكل غير مصرح به، مما يتيح للمهاجم فرصة لتخريب الاستخدام المقصود للتطبيق.
الهندسة العكسية	يتعامل مع تحليل الملف الثنائي النهائي لتحديد الكود المصدري والمكتبات والخوارزميات والأصول الأخرى، مما يمنح المهاجم رؤية داخلية للتطبيق وفرصة للكشف عن نقاط الضعف.
وظائف غريبة	يتعامل مع وظائف الباب الخلفي المخفية أو عناصر التحكم في أمان التطوير التي لا يُفترض إصدارها في بيئة الإنتاج.

- Bluediving

لفتح اتصالات Bluetooth و Wi Fi يسمح بالتنصت واعتراض نقل البيانات و يوجد أدوات عبارة عن مجموعة اختراق بلوتوث التي تنفذ هجمات مختلفة مثل: انتحال عنوان Bluetooth

- Wi Hack اختراق شبكات (Wi-Fi)

تقنية تستخدم لاختراق شبكات Wi-Fi المحمية بكلمة مرور، وتساعد في الوصول غير المصرح به إلى شبكات الإنترنت. أداة Kali NetHunter وهي مخصصة للهواتف.

الفصل التاسع
اختراقات البرامج الضارة للحواسيب

- حصان طروادة

من أخطر وأشد أنواع الاختراقات الأمنية المعلوماتية، وهي نوع من برامج الحاسوب الضارة التي تتنكر كبرمجية غير ضارة أو مفيدة لكي تقوم بالدخول إلى الأنظمة والتحكم فيها بشكل سري.

أنواع حصان طروادة	الوصف
أحصنة طروادة المتسللة	تقوم بتحميل برامج ضارة على جهاز الضحية وتعمل كمنفذ للوصول إلى الجهاز أو تجعله عرضة للهجوم. قد تُعد جزءًا من **Bot Net.**
أحصنة طروادة المحملة للبرمجيات الضارة	تجلب برامج ضارة مثل **Emotet** وغيرها، وتعمل على نشر التهديدات داخل النظام.
أحصنة طروادة المهددة للخدمات المصرفية	تستهدف سرقة بيانات اعتماد الوصول إلى الحسابات المصرفية.
أحصنة طروادة الموزعة للحرمان من الخدمات **(DDoS)**	تستخدم لإغراق الخوادم أو الشبكات بسيل من الطلبات، مما يؤدي إلى تعطيل الخدمات.
برامج زائفة لمكافحة الفيروسات من أحصنة طروادة	تتظاهر بكونها برامج مكافحة فيروسات لكنها في الواقع تسبب مشاكل وتسهم في احتيال المستخدمين.
حصان طروادة لص الألعاب	يسرق معلومات حسابات اللاعبين عبر الإنترنت.
أحصنة طروادة للمراسلة الفورية **(IM)**	تسرق بيانات تسجيل الدخول وكلمات المرور من برامج المراسلة الفورية.
أحصنة طروادة لطلب الفدية	يقوم بتعديل البيانات على الحاسوب لجعله غير قابل للاستخدام، ويطلب فدية لاستعادة الوضع الطبيعي.
أحصنة طروادة عبر الرسائل النصية **(SMS)**	تُرسل رسائل **SMS** الضارة مثل **Faketoken** التي تتسبب في تكاليف باهظة للمستخدمين.
أحصنة طروادة التجسسية	تراقب استخدام الحاسوب وتسجل بيانات لوحة المفاتيح أو تأخذ لقطات للشاشة.
أحصنة طروادة للعثور على البريد	تجمع عناوين البريد الإلكتروني من حاسوب الضحية.

- المؤشرات لوجود حصان طروادة:
- زيادة في استخدام وحدة المعالجة المركزية CPU
- قلة في سرعة المعالجة لدى الحاسب
- يتوقف الجهاز وتتعطل البرامج فجأة
- مشكلة غامضة مع الاتصال بالإنترنت
- ظهور برامج وملفات أو رموز على سطح المكتب يتم تعديل الملفات أو حذفها

- ادوات كشف حصان طروادة:

Netstat

هو اختصار لكلمة" Network Statistics" أداة مشهورة تُستخدم في سطر الأوامر لعرض معلومات حول حركة المرور في الشبكة.

يعتبر مهمًا لمديري الشبكات لتحديد الاتصالات والبرامج المتصلة بالجهاز.

Netstat

يساعد مديري الأمان السيبراني في رصد برامج الضارة وتحديد موقعها لإزالتها بشكل صحيح.

Tcpvie

يتيح رؤية جميع اتصالات بروتوكولات UDP & TCP ويعطي تقرير عن حالة الاتصال واسم العملية المرتبطة بها مع إمكانية إنهاء اتصال أي عملية يتم الشك في طبيعة عملها.

- التدابير المضادة ضد البرامج الضارة:

Trojan Hunter

جميع أنواع البرامج الضارة مثل أحصنة طروادة وبرامج التجسس وبرامج الإعلانات المتسللة وبرامج الاتصال ويعمل على إزالتها

Ems iSOFT

هو برنامج يكتشف التهديدات الجديدة بشكل فعال قبل أن يتم اختراق جهاز الحاسب

McAfee

هو برنامج يستخدم لتجنب الرسائل النصية الاحتيالية باستخدام الحماية المدعومة بالذكاء الاصطناعي. ويمكنه حظر الروابط الخطرة إذا تم القيام بالنقر فوقها عن طريق الخطأ، كما يقوم بالتنبيه إذا ا كتشف روابط احتيالية.

الفصل العاشر
اختراقات الهندسة الاجتماعية

- تقنيات الهندسة الاجتماعية

تعريف الهندسة الاجتماعية:

أنها نوع من التقنيات التي يستخدمها المجرمون الالكترونيون بهدف استدراج المستخدمين غير المرتابين لإرسال بياناتهم السرية وإصابة حواسيبهم ببرامج ضارة.

اسباب خطورة الهندسة الاجتماعية:

أكثر ما يجعل الهندسة الاجتماعية خطيرة والسبب في أنها محط اهتمام الشركات هو أنها تعتمد على الاخطاء البشرية، بدلا من الثغرات في البرامج وأنظمة التشغيل حيث أن الاخطاء التي يقوم بها المستخدمون الشرعيون من الصعب ملاحظتها أو التنبؤ بها مما يجعل التعرف عليها ومنعها أكثر صعوبة من التسلل المستند إلى البرامج الضارة.

يمتلك مهاجمو الهندسة الاجتماعية هدفا من هدفين:

التخريب: يكون هذا بتعطيل أو إتلاف البيانات لإحداث ضرر أو لمجرد الإزعاج

السرقة: الاستلاء على الاشياء الثمينة مثل المعلومات أو الوصول أو المال. ومن أشهر أساليبها استغلال الشائعات وطباع وشخصية البشر وضعف الخبرة التقنية للضحية وانتحال الشخصية واستغلال السمعة الجيدة لتطبيقات معينة ليحمل فيها ملفات خبيثة و خيانة الثقة و الاقناع المباشر و الغير مباشر و استغلال الانترنت.

يقوم عمل الهندسة الاجتماعية على ما يلي:

1– جمع المعلومات: هذه هي المرحلة الاولى من أجل الحصول على معلومات أ كثر عن الضحية المقصودة ويتم جمع المعلومات من مواقع المنظمة ومنشورات أخرى وأحيانًا عن طريق التحدث إلى ُمستخدمي النظام المستهدف للتواصل معهم.

2– خطة الهجوم: يحدد المهاجمون كيفية تنفيذ الهجوم، وما هي الادوات والوسائل التي يمكن استخدامها في الهجوم.

3– أدوات الاستحواذ: تتضمن برامج الحاسب التي سيستخدمها المهاجم عند بدء الهجوم.

4– الهجوم: استغلال نقاط الضعف في النظام المستهدف أو الافراد.

5– استخدام المعرفة المكتسبة: وذلك من خلال المعلومات التي تم تحصيلها من الافراد أو المؤسسات.

2–الهجمات البشرية:

هو استخدام الاساليب والمهارات البشرية مثل الاساليب الكلامية أو النفسية الايحائية أو الاعلانية لتوجيه عقل وتفكير الهدف(الضحية) إلى ما يريد المهاجم والاستفادة منه بأكبر قدر ممكن بدون أن يشعر لكسب معلومات ذات قيمة كبيرة عن النظام باستخدام معلومات قليلة لكسب ثقته دون الاعتماد على التقنية لانهم يستخدمون مهارات التعامل مع البشر لاستغلالهم .

وفيما يلي الطرق التي تؤديها الهندسة الاجتماعية القائمة على البشر:

– التظاهر بأنه المستخدم النهائي للمشروع

– التظاهر بأنه مستخدم وهمي

– يتنكر في زي الدعم الفني

3– الهجمات الحاسوبية:

استخدام وسائل خداعية تعتمد على التقنية بشكل مباشر تمكنه من سحب المعلومات من الهدف (الضحية) مثل إنشاء مواقع توظيفية مزيفة أو مواقع تحميل برامج بشرط أن ُيدخل المستخدم بياناته الطرق المستخدمة هي:

– التصيد (Phishing)

– البريد الوهمي

– هجمات النافذة المنبثقة

4– الهجمات المعتمدة على الهاتف المحمول:

يستخدم المهاجم الهاتف المحمول لشن هجمات بأسلوب الهندسة الاجتماعية حيث يقوم بالاتصال بالهدف(الضحية)مدعيا أن شخص له صلاحيات ويقوم تدريجيا بسحب المعلومات من الضحية كأن يدعي أنه من فريق الدعم الفني للمنظمة ويريد معرفة بعض المعلومات. أو التي تتم عن طريق المساعدة من تطبيقات الهاتف المحمول حيث يقوم المهاجمون بإنشاء تطبيقات خبيثة مع مميزات جذب وأسماء مشابهة لتلك التطبيقات المشهورة ونشرها في المتاجر للتطبيقات وعندما يقوم المستخدم بتحميلها فإنه يتم مهاجمته من قبل البرمجيات الخبيثة الطرق هي:

– نشر التطبيقات الخبيثة

– تطبيقات الامن الوهمية

– استخدام رسائل SMS

- التدابير المضادة والحماية من عمليات الهندسة الاجتماعية

تعتبر الهندسة الاجتماعية من الثغرات الامنية التي يعب منعها لأنها تعتمد على طبيعة البشر ولذلك يجب توعيتهم وتدريبهم باستمرار من خطرها باتخاذ تدابير مضادة للحماية منها **مثل:**

• الحرص على الخصوصية وعدم نشر المعلومات الشخصية.

• تجنب الرسائل التي تطلب معلومات شخصية.

• عدم فتح الرسائل مجهولة المصدر.

• استخدام مرشحا جيِّدا للرسائل العشوائية.

• التخلص من الأوراق المهمة بتمزيقها بواسطة الالة المخصصة بذلك قبل وضعها في النفايات.

• عدم مشاركة كلمة السر مع الأخرين أو تركها على المكتب.

• يجب التحقق من هوية أي شخص يطلب معلومات عن الجهاز أو الحساب أو أي معلومات شخصية عن موظف ما .

- اختبار اختراق الهندسة الاجتماعية:
- هو اختبار قوة العوامل البشرية في أمن المؤسسة.
- الخطوات المتبعة في إجراء الاختبار

1– الحصول على إذن

2– تحديد نطاق الاختبار

3– الحصول على قائمة رسائل البريد الالكتروني والاتصالات من الاهداف المحددة سابقا

4– جمع رسائل البريد الالكتروني وتفاصيل اتصال للعاملين في المنظمة المستهدفة

5– جمع المعلومات باستخدام تقنيات Footprinting

6– إنشاء مخطط قائم على المعلومات

7– توجيه رسائل بريد الكتروني إلى موظف لطلب معلومات شخصية

8– إرسال ومراقبة رسائل البريد الالكتروني مع المرفقات الخبيثة لاستهداف الضحية

9– إجراء اتصال هاتفي بالهدف وانتحال شخصية ما ثم السؤال عن معلومات مهمة

10– الاتصال بالهدف وانتحال شخصية مشرف الدعم الفني

11– محاولة دخول المنظمة كمدقق خارجي

12– محاولة التصنت و surfing shoulder على الانظمة و المستخدمين

13– توثيق جميع النتائج في التقرير

الفصل الحادي عشر

التقييم الأمني

- منهجية اختبار الاختراق الأخلاقي

هي نهج منظم لتحديد واستغلال نقاط الضعف في النظام وتتضمن العملية عدة مراحل وتُمكن اتباع هذه المنهجية في تحديد نقاط الضعف المحتملة في أمان النظام وتقديم توصيات للمعالجة و سد الثغرات و يجب على المُخترق الأخلاقي عدم الإغفال عن أي مورد للمعلومات، يجب أن يتم اختبار جميع مصادر المعلومات الممكنة للبحث عن نقاط الضعف و ليس فقط مصادر المعلومات.

- الخطوات هي:

1. الاستطلاع

هو جمع أكبر قدر ممكن من المعلومات حول النظام أو الشبكة المستهدفة بهدف تحديد نقاط الدخول المحتملة إلى النظام.

1. منهجية جمع المعلومات

خلال مراحل Footprinting ، على المخترق القيام بعدة خطوات لذلك يجب أن يكون ما هي لديه عدة خطوات

منهجية يتبعها:

•جمع معلومات محرك البحث مثل جوجل وويكيبيديا.

•استخدام تقنيات البحث في جوجل للحصول على المعلومات الدقيقة.

•جمع معلومات مواقع التواصل الاجتماعي.

•جمع المعلومات من مواقع الإلكتروني الخاصة بالجهاز مراد اختراقها، مثل أرقام الهواتف، أنظمة التشغيل وغيرها.

2. المسح

استخدام أدوات لفحص النظام أو الشبكة المستهدفة بحثا عن نقاط الضعف مثل المنافذ المفتوحة والخدمات قيد التشغيل ومعلومات تشغيل النظام.

3. التعداد

تحديد وجمع المعلومات حول المستخدمين والمجموعات والموارد على النظام المستهدف والهدف منها هو تحديد نقاط الدخول المحتملة إلى النظام التي يمكن استغلالها.

4. تقييم الضعف

تتضمن تحليل المعلومات التي تم جمعها لتحديد نقاط الضعف المحتملة في النظام وتحديد أولويات الثغرات بناء على شدتها واحتمال تعرضها للاستغلال .

5. الاستغلال

بعد تحديد الثغرات الأمنية يتم محاولة استغلالها للوصول إلى النظام أو الشبكة المستهدفة.

6. الإبلاغ

تتضمن هذه المرحلة توثيق نقاط الضعف التي تم تحديدها خلال المراحل السابقة والإبلاغ عنها للمسؤولين وإعداد التقارير بالمعلومات اللازمة بالتدابير المضادة لإصلاح الثغرات وتعزيز أمن المنظمة.

- التقييم الأمني

يشير التقييم الأمني إلى العمليات والإجراءات والأدوات المستخدمة لكشف ما إذا كانت المنظمة تعاني من بعض نقاط الضعف التي يمكن أن يستغلها المهاجمين وهو مسح أمني أو عملية دراسة تغطي جميع خدمات المؤسسة، بما في ذلك البنية ويتمثل ناتج التقييم في توصيات تتعلق بنشر الضوابط الأمنية أو تعزيزها أو إعادة هيكلتها للتخفيف من خطر استغلال نقاط الضعف من قبل المهاجمين والاختبار والتحقق من صحة وكفاءة الحماية الأمنية والضوابط أثناء تطبيقها.

- مخرجات تقييم الأمان

يتكون الناتج من اختبار الاختراق تقرير عن نتائج الاختبار ونقاط الضعف مفصلة وتدابير الوقاية والاقتراحات وفي العادة تكون مطبوعة لضمان الأمان مقسم إلى عدة أقسام تتناول:

- نقاط الضعف الموجودة حاليا للبيئة المستهدفة بإعداد قائمة بالثغرات الأمنية ونقاط الضعف المُكتشفة في النظام وتصنيفها حسب مدى سهولة استغلالها ومدى الضرر الذي قد يلحق بالنظام والأعمال التجارية.
- قائمة بالتغييرات التي نفَّذَها فريق العمل ف ي النظام في أثناء الاختبار.
- بروتوكول الاختبار بما في ذلك الوسائل والأدوات المُستخدمة، والأجزاء المفحوصة، والمشكلات المُكتشفة في النظام.

- القواعد الارشادية

الاختراق الأخلاقي هو ممارسة قانونية ويجب إجراؤه فقط بإذن من المسؤول في المنظمة ومن المهم اتباع الإرشادات الأخلاقية المناسبة وعدم استغلال نقاط الضعف المكتشفة لأغراض ضارة والاحتفاظ بأسرار المنظمة وعدم الإفصاح للأخرين عن نقاط الضعف المكتشفة إلا في التقارير الرسمية للمسؤولين الاستخدام القانوني والأخلاقي لأدوات الاختراق هو جزء مهم من مجال الأمن السيبراني. يجب أن يكون الاستخدام لهذه الأدوات في إطار القوانين المحلية والدولية ويجب الحصول على إذن صريح قبل استخدامها لأي أغراض تتعلق بالاختبار أو التحليل الأمني.

- يتبع المخترقون مفاهيم إرشادات أساسية مثل:

البقاء قانونياً وذلك عبر الحصول على الموافقة المناسبة قبل الوصول وإجراء التقييم الأمني

- تحديد النطاق ،تحديد نطاق التقييم بحيث يظل عملهم المخترق الأخلاقي قانونياً وضمن الحدود المعتمدة للمؤسسة
- الإبلاغ عن نقاط الضعف عن طريق إخطار المؤسسة بكافة نقاط الضعف التي تم ا كتشافها أثناء التقييم وتقديم المشورة العلاجية لحل هذه الثغرات الأمنية
- احترام حساسية البيانات فاعتمادا على حساسية البيانات، قد يتعين على المتسللين الأخلاقيين الموافقة على اتفاقية عدم إفشاء، بالإضافة إلى الشروط والأحكام الأخرى التي تتطلبها المؤسسة التي تم تقييمها.

الأسئلة

1. هو الدخول غير المشروع إلى جهاز حاسب ما عن طريق ثغرات في نظام الحماية باستخدام برامج خصصة يقوم بها محترفون او هواة وذلك للحصول على البيانات أو تدميرها			
الاختراق	التجسس	تقييد الأمان	الأمان
2. هو عملية إجراء فحص شامل لكل الانظمة أو الاجهزة الموجودة في شركة أو مؤسسة ما، من أجل تشاف الثغرات التي يمكن استغلالها من قبل المخربين لأحداث اختراقات وسرقة للبيانات أو تخريبها وإلحاق أضرار سيمة بالمؤسسات والعملاء .			
الاختراق الأخلاقي	الاختراق الغير أخلاقي	الاختراق المتعمد	الاختراق ير متعمد
3. من أهداف الاختراق الاخلاقي			
الدفاع ضد الهجمات المستقبلية	الدفاع عن الهجمات ستقبلية	زيادة الوقت والجهد	زيادة كلفة
4. يتم إجراء اختبار الاختراق في حالة تعديل سياسات المستخدمين النهائيين فقط ؟			
صح	خطأ		
5. من أهداف الاختراق الاخلاقي تأمين الانظمة ؟			
صح	خطأ		
6. خالد موظف في شركة ما، واشتد الخلاف بينه وبين مديره، فأراد خالد تدمير نظام الشركة. فأي طرق تبار الاختراق سيتبعها ؟			
WhiteBox	GreyBox	BlueBox	BlackBox
7. كل الادوات المخصصة لجمع المعلومات لها خطوات محددة ؟			
صح	خطا		
8. باستخدام تقنيات التعداد يمكن الحصول على أسماء المستخدمين للأنظمة المختلفة وجداول IP ؟			
صح	خطا		
9. نوع من أنواع الفحص، يستخدم في فحص عناوين IP ؟			
فحص الشبكات	فحص المنافذ	فحص الضعف	فحص وة
10. نوع من أنواع هجوم التصنت يتم فيها توجيه المستخدم إلى موقع مزيف من خلال توفير بيانات وهمية			

DNS Poisoning	Mac Flooding	Arp Poisoning	DHCP tack

11. بروتوكول عديم الحالة يستخدم لتحليل عناوين IP إلى عناوين MAC للجهاز

ARP (Address Resolution Protocol)	FTP (File Transfer Protocol)	Post office (Protocol POP)	Telnet

12. من مميزات Ipv6؟

كفاءة التوجيه	إتاحة عناوين محدودة	سرعات أقل	أمان خفض

13. Wiresharkهو محلل حزم سطر الأوامر المعروف، فهو يوفر القدرة على اعتراض ومراقبة IP/TCP والحزم خرى أثناء الارسال عبر الشبكة

صح	خطأ		

14. عندما يقوم النظام بقطع الاتصال وتوقف عمل الاجهزة عند الاشتباه بنشاط مريب في الشبكة فأن هذا ن ؟

أنظمة منع التطفل	أنظمة كشف التطفل	أنظمة مرور الشبكة	Firewall

15. في التصنت السلبي، يمكن تغيير حركة مرور الشبكة بالطريقة التي يريدها المهاجم ؟

صح	خطا		

16. يستخدم التعداد LDAP للوصول إلى ؟

قوائم الدليل Directory Active	جمع المعلومات المتصلة بخادم NTP	جمع المعلومات تصلة بخادم SNMP	سجلات نظمة ستهدفة

17. عملية اختبار الاختراق تجري بطريقة واحدة مهما تعددت الانواع ؟

صح	خطأ		

18. من التدابير المضادة والحماية من عمليات المهاجمة لأنظمة التشغيل تشغير محركات الأقراص فقط ؟

صح	خطأ		

19. ما هو الغرض من منهجية أمان نظام التشغيل ؟

حماية نظام التشغيل من التهديدات فيروسات	تعزيز أداء نظام التشغيل	تطوير ميزات جديدة ظام التشغيل	تحسين ميم واجهة ستخدم

20. أداة اختبار تخمين كلمات المرور المستخدمة في أنظمة Linux و Windows؟

Hydra	Nmap	IP Scanner	Cain

21. ماذا يضمن أمان نظام التشغيل

سلامة وسرية نظام التشغيل	التوافق والتوسعية لنظام شغيل	توفر وتوافق نظام شغيل	كفاءة سهولة تخدام نظام شغيل
22. يتم الاختراق عبر خدمات الاتصال عن بعد عن طريق خطوتين رئيسيتين: كسر كلمات مرور هذه الخدمات			
هجوم رفع الامتياز	هجوم اختراق الخصوصية	هجوم سلامة انات	هجوم وافر
23. من التدابير المضادة والحماية من عمليات الهندسة الاجتماعية ؟			
التخلص من الاوراق المهمة بتمزيقها سطة الآلة المخصصة بذلك قبل عها في النفايات	نشر المعلومات الشخصية ى مواقع التواصل الاجتماعي	فتح رسائل مجهولة صدر	مشاركة مات السر مع ملاء
24. كيف تختلف هجمات الهندسة الاجتماعية عن تقنيات الاختراق التقليدية ؟			
تستغل علم النفس البشري وتلاعب فراد	تكون فعالة فقط ضد ظمة القديمة	تستهدف البنية حتية بدلا من الافراد	تعتمد فط على كنولوجيا، ون تدخل شري
25. أين يعمل برنامج خادم الويب؟			
داخل نظام تشغيل الخادم	داخل متصفح الويب	داخل جهاز العميل	داخل جهاز جيه الشبكة
26. التحقق الدائم من صحة إدخال المستخدم قبل إدخاله في قاعدة البيانات الخاصة، تعتبر من التدابير ضادة والحماية من عمليات اختراق خوادم وتطبيقات الويب ؟			
صح	خطا		
27. استهداف المستخدم من منهجية الهجوم على موقع الويب وذلك من خلال			
الهندسة الاجتماعية	استخدام أدوات الاختراق	المصارحة	عن طريق دة توجيه كة الشبكة
28. أنواع هجمات البرمجة النصية عبر المواقع (XSS) يُسمى:			

هجمات انعكاسية ومستمرة	هجمات انعكاسية ومنقطعة	هجمات انعكاسية بته	هجمات كاسية وارية
.29 استخدام خوارزميات التشفير القوية يعد مثالا على الهندسة الاجتماعية من خلال انتحال الشخصية			
صح	خطأ		
.30 أيهما هو أحد أشهر خوادم الويب المستخدمة على نطاق واسع ؟			
خدمات معلومات الانترنت (IIS)	بروتوكول إدارة الشبكة سيطة (SNMP)	بروتوكول نقل لفات (FTP)	بروتوكول ل النص ائق (HTTP)
.31 ما الذي يمكن أن يجعل خادم الويب عرضة للثغرات ؟			
الاعدادات الافتراضية دون إعادة بطها	إعدادات نظام التشغيل كل صحيح	استخدام توكولات الأمان	اتصال رنت بطيء
.32 ما هو الضعف الرئيسي الذي يسمح بحدوث حقن SQL؟			
عدم التحقق الكافي من البيانات	تشفير قاعدة بيانات ضعيف	نقص في موارد الخادم	حماية جدار حماية غير كافية
.33 ما هو هدف هجمات DDoS؟			
تحميل النظام وتعطيل تشغيله	الحصول على وصول غير مصرح به إلى الخادم	حذف البيانات الحساسة	سرقة كلمات مرور المستخدم
.34 ما هي العواقب المحتملة لوقوع ضحية لهجوم الهندسة الاجتماعية ؟			
الكشف عن المعلومات الشخصية حساسة.	انخفاض سعة تخزين الجهاز	زيادة استخدام طاق الترددي للشبكة.	الفقدان ؤقت تصال نترنت
.35 من أهداف اختبار اختراق الشبكة، ويتم فيها تحسين عتاد الاجهزة والشبكات والبرمجيات ؟			
تحسين البنية التحتية	اكتشاف المخاطر الامنية	إدارة نظام علومات	كشف رقة البيانات

ملخص لمقرر مقدمة في الأدلة الجنائية الرقمية
Introduction to Digital Forensics

الفصل الأولى
العلوم الجنائية المتعلقة بالحاسب الآلي

تعريف العلوم الجنائية المتعلقة بالحاسب الآلي:

فرع من فروع العلوم الجنائية الرقمية، تتعلق العلوم الجنائية المتعلقة بالحاسب الآلي وبالأدلة المستخلصة من الحاسب الآلي وسائط التخزين الرقمية، الهدف هو فحص الوسائل الرقمية للتحديد والتعريف Identifying والحفاظ Preserving واسترجاع واسترداد Recovering وتحليل Analyzing وإظهار حقائق واراء حول البيانات الرقمية Information Digital.

مفهوم التحقيق الجنائي الرقمي:

هو دراسة الحقائق الجنائية الرقمية للتحقق من وجود جريمة الكترونية وإثبات ذنب المجرم، التحقيق الجنائي الرقمي يمكن أن يشتمل البحث والمقابلة والاستجواب وجمع الأدلة وحفظها وعدة أساليب مختلفة للتحقيق.

أهداف التحقيق الجنائي الرقمي

1. استعادة البيانات والمواد ذات الصلة وتقديمها كدليل
2. معرفة دوافع الجريمة
3. معرفة هوية الجاني
4. رسم مسرح الجريمة
5. الحصول على البيانات لاستخراج الأدلة والتحقق منها
6. التعرف على الأدلة
7. إنتاج تقرير جنائي حاسوبي
8. حفظ الأدلة

تعريف معمل التحقيق الجنائي الرقمي

معمل التحليل الجنائي الرقمي هو المكان الذي يتم نقل الأدلة من مسرح الجريمة إليه ليتم عمل نسخ منها وتحليليها وحفظها.

1. الحماية المادية : معدات لإغلاق الباب تلقائيا باستخدام بطاقات يتم من خلالها تسجيل كامل المعلومات أو ببصمة اليد أو بصمة العين للفتح.

2. البرامج : يجب أن يحتوي الجهاز المخصص لتحليل البيانات على برامج تحليل البيانات فقط ولابد أن تكون البرامج أصلية مأخوذة من المصدر مباشرتا حتى تعتمد من المحكمة.
3. المعدات طقم كامل يمكن شراؤه يحتوي على العديد من الأدوات والأسلاك الموصلات.

تعريف المعمل الجنائي الرقمي المتنقل

يكون عبارة عن حقيبة بها معدات لهذا الغرض وتراعي المعايير.

تعريف أدوات التحقيق الجنائي الرقمي

الأدوات فهي عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد على واجهة رسومية يستخدم في تحليل أجهزة الحاسب والهواتف الذكية والمعدات اللازمة لحفظ وتأمين الأدلة.

Autopsy هو عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد على واجهة رسومية يستخدم في تحليل أجهزة الكمبيوتر والهواتف الذكية.

ExifTool :هو برنامج مجاني ومفتوح المصدر للتعامل مع بيانات الصور الرقمية يمكن استخدامها لقراءة وكتابة العناصر.

Kit Forensic : أداة قوية قادرة على استعادة كلمات المرور لأكثر من ٣٤٠ نوع من أنواع الملفات.

خطوات عملية التحقيق الجنائي الرقمي

Preservation: الأدلة محفوظة على نفس الحالة التي وجدت بها

Acquisition: الحصول على تلك الأدلة

Analysis: تحليل تلك الأدلة ومعرفة نوع المعلومات التي تم الحصول عليها

Discovery: عزل البيانات و اكتشاف ما يكون متعلق بالقضية

التوثيق Documentation

العرض : Presentation

دور المحقق:

هو فقط جمع الأدلة واستخراج الحقائق ويجب أن يتحلى بالأخلاقيات المهنية ويعمل على تقديم الحقائق فقط وليس إدانة أي شخص ، ويتم وضع خطة عمل التحقيق من خلال:

1. **التخطيط للتحقيق** وضع خطة عمل مناسبة لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات للتصدي للجريمة.
2. **إجراءات التحقيق:** أساليب المواجهة والاستجواب مع عرض الحالة ودراستها.
3. **تجميع المعلومات وتحليلها.**
4. **أساليب المعمل الجنائي.**

معوقات التحقيق الجنائي الرقمي:

أولا : معوقات تتعلق بصعوبة استخلاص الأدلة الجنائية الرقمية مثل:

- الطبيعة الغير مرئية للدليل الجنائي الرقمي
- سهولة تدمير ومحو الدليل الجنائي الرقمي
- إعاقة الوصول إلى الدليل الجنائي الرقمي
- ضخامة البيانات المطلوب فحصها

ثانياً : المعوقات المتعلقة بجهات التحقيق :

الصعوبات تتعلق بجهة التحقيق، منها نقص المعرفة الفنية لدى سلطات التحقيق، ولدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي.

المقصود بالدليل الجنائي الرقمي

قد يكون صورة رقمية Image أو مطبوعة من أصل رقمي أو يكون متناً Text لموضوع أو رسالة أو غيرها Message

أماكن وجود الدليل الرقمي

– الأقراص الصلبة – أدوات التخزين – سجلات النظام – البريد الإلكتروني – المحادثات – قواعد البيانات– الهواتف .

الفصل الثاني
أساسيات التحليل الجنائي الرقمي

الهدف من التحليل الجنائي الرقمي :

– إنتاج تقرير جنائي حاسوبي وتقديمه بكل إجراءاته منذ البداية إلى النهاية.

– معاينة مسرح الجريمة.

– حفظ كل الأدلة بنسخ عديدة في أماكن سرية.

خطوات التحليل الجنائي الرقمي:

1. الوصول للموقع: عند الوصول لمكان الجريمة يجب على المحقق القيام بعملية توثيق دقيقة لكل الأحداث والعمليات الجارية والأشخاص الموجودين في مكان الجريمة.
2. الحصول على الأدلة الرقمية: للحصول على الأدلة الرقمية يتم القيام بعملية الفحص من خلال الفحص البصري لتحديد حالة الجهاز الهدف ومكان وجوده والبيئة المحيطة به ثم القيام بنسخ الملفات قبل بدء الفحص والقيام بعمل صورة طبق الأصل ليتم العمل عليها.
3. .تحديد مكان الأدلة الرقمية: عند الانتهاء من عملية الفحص يتم تحديد المكان أو الملف الذي يحتوي على الدليل الجنائي الرقمي وتوثيقه وقد يكون الدليل في قواعد البيانات مثل SQL Server Oracle جهاز الحاسب هو تاريخ تصفح الانترنت أو الملفات المحذوفة.
4. حماية الأدلة الرقمية: بعد الحصول على الأدلة يجب على المحقق المحافظة على سلامتها حتى لا يتم التعديل عليها أو تخريبها وعمل صورة طبق الأصل منها عن طريق أدوات التحليل الجنائي الرقمي.
5. نقل الأدلة الرقمية: إذا كان الدليل الرقمي موجود في جهاز حاسب أو في جهاز موبايل يتم نقل هذا الجهاز إلى المختبر ويجب التأكد من منع الاتصال بهذا الجهاز أثناء عملية النقل.
6. .تخزين الأدلة الرقمية: يجب أن يتم تخزين الأدلة في بيئة أمنة لا يمكن الوصول إليها من قبل أشخاص غير مصرح لهم من المهم أن تكون معزولة عن الحقول الكهرومغناطيسية ومحمية من الحرائق وبعيدة عن أنابيب المياه وأن يكون المكان مغلق.
7. إجراء التحقيق: وهي الإجراءات التي يتم تنفيذها عند ثبوت ووقوع الجريمة وتحديد شخصية مرتكبيها بعد العمل على إدارة عمليات المعاينة لمسرح الجريمة.
8. إعداد التقارير: التقرير النهائي يكون مدرج فيه كل شيء متعلق بالقضية.

9. الاستجابة وتجهيز الأدوات: الاستجابة هو ردت الفعل عن وقوع الحادثة المعلوماتية وتتضمن عملية الاستجابة الوصول لموقع الحادث وتصوير الأدلة وتأمين مسرح الجريمة ونقل الأدلة إلى مختبر (معمل) الجنائي الرقمي.

الفصل الثالث
عملية الفحص والحصول على الأدلة الجنائية الرقمية

أماكن وجود الدليل الرقمي:

يوجد كثير من البرامج التي تساعد المحلل الجنائي الرقمي منها:

1. برنامج إذن التفتيش Computer Scorch Warrant Program : هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها.
2. قرص بدء تشغيل جهاز الحاسب Bootable CD : هو قرص يمكن المحقق من تشغيل الجهاز إذا كان محمي بكلمة سر.
3. برنامج معالجة الملفات مثل tree Pro Gold : هو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة.
4. برامج اتصالات مثل LANtastic هو برنامج يستطيع ربط جهاز حاسب المحقق بجهاز المتهم لنقل منه المعلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

أدوات الجرائم الالكترونية:

1. الطابعات الالكترونية.
2. تقنية الباركود الالكترونية.
3. البرامج الخبيثة والفيروسات.
4. وسيط الكتروني لا سلكي.
5. الكاميرات وخط يربطها بوسائل التجسس.
6. برامج خاصة بنسخ المعلومات على أجهزة الحواسيب.

تعريف النموذج المرجعي OSI :

هو نموذج تم تطويره بواسطة منظمة المعايير الدولية " OSI " وإنه يعطي إطار عمل شبكي متعدد الطبقات يصور كيف يجب أن يتم الاتصال بين الأنظمة غير المتجانسة ولها سبع طبقات مترابطة.

الفصل الرابع
المحكمة الرقمية

مفهوم المحكمة الرقمية:

المحكمة الرقمية تحتاج الى اعداد مكاني يتطلب وجود جهاز حاسب الي حديث لاستعراض ما هو مسجل، وشاشة عرض متسعة توضع في مكان يشاهده كل من في القاعة بشكل واضح.

مفهوم القاضي الرقمي:

هو القاضي البشري، لكنه هو الذي يطبق القوانين الخاصة بمستجدات التعاملات الرقمية، والحكومة الإلكترونية، والتجارة الإلكترونية، والتوقيع الرقمي، والمستندات الرقمية، وجرائم النصب الرقمية والسرقة والقتل بالوسائل الرقمي.

مفهوم التوقيع الالكتروني بالمحكمة:

هو ما يوضع على محرر الكتروني ويتخذ شكل حروف، أو ارقام، أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.

أنواع التوقيع الالكتروني بالمحكمة:

1. التوقيع الاجرائي: يسمى هذا التوقيع بالتوقيع المكود أو المشفر، وهو عدة خطوات منطقية متتالية يمكن من خلالها التعريف بالشخص، ويحكمها مفتاحان أحدهما يعرف بالمفتاح الشخصي أو السري ويمكن الوصول اليه من خلال المفتاح عام. ومن امثلتها التوقيعات المستخدمة في بطاقات الائتمان.
2. التوقيعات البيومترية: وهي تعرف بالتوقيعات القياسية وهي خاصية من خواص الإنسان مثل قرنية العين – بصمة الاصبع . بصمة الصوت – بصمة الوجه – بصمة الدم .
3. التوقيعات البيولوجية: وهي خاصة بالشخص والتي توقع بخط اليد ويتم نقلها بإحدى وسائل النقل الى جهاز الكمبيوتر لتسجيل رقميا باستخدام الوسائل التالية:

الماسح الضوئي – الفاكس – الادخال على سطح حساس – الادخال بالكاميرا الرقمية بقلم رقمي.

مفهوم المجرم المعلوماتي

هو المتهم أمام هذه المحكمة وهو الذي يسئ استعمال أجهزة الحاسب والشبكة المعلومات الدولية والشبكات الأخرى بإحدى الطرف التي تعد جريمة يعاقب عليها القانون.

الأسئلة

1. تعرف ادوات التحقيق الجنائي الرقمي انها عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد على جهة رسومية.			
صح	خطأ		
2. تتعدد أهداف التحقيق الجنائي الرقمي ومنها الحصول على البيانات لاستخراج الأدلة والتحقق منها.			
صح	خطأ		
3. القاضي الرقمي هو القاضي البشري، لكنه هو الذي يطبق القوانين الخاصة بمستجدات التعاملات الرقمية، حكومة الإلكترونية، والتجارة الإلكترونية، وجرائم النصب الرقمية والسرقة والقتل بالوسائل الرقمي.			
صح	خطأ		
4. من الصعوبات التي تتعلق بجهة التحقيق نقص المعرفة الفنية لدى سلطات التحقيق.			
صح	خطأ		
5. التوقيعات البيولوجية تسمى بالتوقيع المكود أو المشفر.			
صح	خطأ		
6. يعتبر التوثيق والعرض من خطوات عملية التحقيق الجنائي الرقمي			
صح	خطأ		
7. يمكننا العثور على الدليل الرقمي في قواعد البيانات والمحادثات.			
صح	خطأ		
8. أداة قوية قادرة على استعادة كلمات المرور لأكثر من 340 نوع من أنواع الملفات.			
Autopsy	ExifTool	Kit Forensic	FTK Imager
9. دراسة الحقائق الجنائية الرقمية للتحقق من وجود جريمة الكترونية وإثبات ذنب المجرم.			
التحقيق الجنائي الرقمي	التوقيع الرقمي	ادوات التحقيق الجنائي	معمل التحقيق الجنائي
10. المكان الذي يتم فيه نقل الأدلة من مسرح الجريمة إليه ليتم عمل نسخ منها وتحليليها وحفظها.			
معمل التحليل الجنائي الرقمي	ادوات التحليل الجنائي الرقمي	الدليل الجنائي الرقمي	الادلة الجنائية
11. احدى خطوات عملية التحقيق الجنائي ..... وهي تحليل تلك الأدلة ومعرفة نوع المعلومات التي تم حصول عليها.			
Analysis	Acquisition	Presentation	Preservation
12. إنتاج تقرير جنائي حاسوبي وتقديمه بكل إجراءاته منذ البداية إلى النهاية يعتبر الهدف من :			
التحليل الجنائي الرقمي	الوصول للموقع	مسرح الجريمة	حماية الادلة الرقمية
13. بصمة الاصبع مثال على :			
التوقيع الاجرائي	التوقيعات البيومترية	التوقيعات الرقمية	التوقيعات المعلوماتية
14. هو المتهم أمام المحكمة والذي يسئ استعمال أجهزة الحاسب والشبكة الدولية والشبكات الأخرى بإحدى طرق التي تعد جريمة يعاقب عليها القانون .			
اللص	المجرم المعلوماتي	القاضي الرقمي	التوقيع الالكتروني
15. تحتاج الى اعداد مكاني يتطلب وجود جهاز حاسب آلي حديث لاستعراض ما هو مسجل ، وشاشة عرض متسعة توضع في مكان يشاهده كل من في القاعة بشكل واضح.			

المحكمة الرقمية	التوقيع الرقمي	القاضي الرقمي	العقود

16. برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها.

برنامج إذن التفتيش	قرص بدء تشغيل جهاز الحاسب	برنامج معالجة الملفات	برامج اتصالات

17. نموذج تم تطويره بواسطة منظمة المعايير الدولية ويعطي إطار عمل شبكي متعدد الطبقات يصور كيف يجب يتم الاتصال بين الأنظمة غير المتجانسة ولها سبع طبقات مترابطة

نموذج النقل	نموذج التطبيقات	نموذج الجلسة	النموذج المرجعي OSI

18. فرع من فروع العلوم الجنائية الرقمية يهدف الى فحص الوسائل الرقمية للتحديد والتعريف والحفاظ واسترجاع استرداد وتحليل وإظهار حقائق وآراء حول البيانات الرقمية.

العلوم الجنائية المتعلقة بالحاسب الآلي	القاضي الرقمي	المجرم المعلوماتي	العلوم الجنائية المتعلقة بنموذج التطبيقات

19. عبارة عن صورة رقمية Image أو مطبوعة من اصل رقمي أو يكون متناً Text لموضوع أو رسالة Message أو غيرها.

مسرح الجريمة	الدليل الجنائي الرقمي	المجرم المعلوماتي	المحكمة الرقمية

20. وضع خطة عمل مناسبة لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر وضع التصورات للتصدي للجريمة.

التخطيط للتحقيق	التوقيع الالكتروني	الوصول للموقع	أساليب المعمل الجنائي

21. عباره عن معدات لإغلاق الباب تلقائيا باستخدام بطاقات يتم من خلالها تسجيل كامل المعلومات أو ببصمة اليد وبصمة العين للفتح .

الملفات	البرامج	التحقيق الجنائي	الحماية المادية

22. أثناء ..... يقوم المحقق بعملية توثيق دقيقة لكل الأحداث والعمليات الجارية والأشخاص الموجودين في مكان الجريمة.

الوصول للموقع	مراقبه الشبكات	حماية الأدلة الرقمية	البرامج

23. هو فقط يقوم بجمع الأدلة واستخراج الحقائق ويجب أن يتحلى بالأخلاقيات المهنية ويعمل على تقديم الحقائق فقط وليس إدانة أي شخص.

دور المحقق	دور المجرم المعلوماتي	دور اللص	دور الباحث

24. توقيعات خاصة بالشخص والتي توقع بخط اليد ويتم نقلها بإحدى وسائل النقل الى جهاز الكومبيوتر لتسجل رقمياً.

التوقيعات البيولوجية	التوقيع الاجرائي	محاذير التوقيع الإلكتروني	التوقيعات المعلوماتية

25. عبارة عن حقيبة بها معدات لهذا الغرض وتراعي المعايير.

المعمل الجنائي الرقمي المتنقل	المعمل الجنائي الرقمي	الوصول للموقع	مسرح الجريمة

26. عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد على واجهة رسومية يستخدم في تحليل أجهزة الكومبيوتر والهواتف الذكية.

Autopsy	ExifTool	Kit Forensic	FTK Imager

27. يعتبر من أهداف التحقيق الجنائي الرقمي

معرفة هويّة الجاني	معرفة اسم المحقق	معرفة التاريخ والوقت	معرفة القاضي الرقمي

28. تعتبر من أدوات الجرائم الالكترونية			
تقنية الباركود الالكترونية	جدار الحماية	المتصفح	الهندسة الاجتماعية
29. قرص يمكّن المحقق من تشغيل الجهاز إذا كان محمي بكلمة سر.			
قرص بدء تشغيل جهاز الحاسب	قرص معالجة الملفات	قرص الاتصالات	قرص إذن التفتيش
30. يوضع على محرر الكتروني ويتخذ شكل حروف، أو ارقام، أو رموز، أو إشارات، أو غيرها ويكون له طابع منفرد يسمح تحديد شخص الموقع ويميزه عن غيره			
الدفاع الرقمي	التوقيع الإلكتروني	المحضر الرقمي	المجرم المعلوماتي
31. هي ان يقوم المحقق بالمحافظة على سلامة الأدلة حتى لا يتم التعديل عليها أو تخريبها وعمل صورة طبق الأصل منها			
حماية الأدلة الرقمية	المعمل الجنائي الرقمي	اجراء التحقيق	اعداد التقارير
32. لابد ان تكون في بيئة أمنة ، ولا يمكن الوصول إليها من قبل أشخاص غير مصرح لهم ومن المهم أن تكون معزولة عن الحقول الكهرومغناطيسية ومحمية من الحرائق وبعيدة عن أنابيب المياه وأن يكون المكان مغلق			
تخزين الأدلة الرقمية	إجراء الاستجابة	اجراء التحقيق	اعداد التقارير
33. الإجراءات التي يتم تنفيذها عند ثبوت ووقوع الجريمة وتحديد شخصية مرتكبيها بعد العمل على إدارة عمليات المعاينة لمسرح الجريمة			
إجراء التحقيق	إجراء الاستجابة	إجراء الوصول للموقع	مراقبه الشبكات
34. يدرج به كل شيء متعلق بالقضية وكل الملفات التي تم اكتشافها وتحليلها وذكر طريقة اكتشاف الدليل الرقمي والأدوات التي تم استخدامها في هذه العملية.			
القاضي الرقمي	إجراء التحقيق	أساليب المعمل الجنائي	إعداد التقارير
35. من المعوقات التي تتعلق بصعوبة استخلاص الأدلة الجنائية الرقمية			
ضخامة البيانات المطلوب فحصها.	عدم وجود ادلة	مراقبه الشبكات	اتصال الشبكات

متمنين لكم التوفيق والنجاح الدائم