أكاديمية التعلم
Academy Of Learning

الاختراق الأخلاقي وأساليب الحماية

دبلوم الأمن السيبراني

تحت إشراف
المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

❖ الأهداف التفصيلية للمقرر:

بنهاية هذا المقرر سيكون المتدرب قادراً وبكفاءة على أن:

- يحدد المصطلحات الأساسية المرتبطة بالمخترقين الأخلاقيين.
- يصف المراحل الخمس الاختراق الأخلاقي.
- يستخدم الأدوات Dmitry و whois و DNS record و Dig و nslookup في جمع المعلومات.
- يطبق أدوات المسح والتعداد المختلفة مثل ، Hping3,nc,telenet,nbstat.
- ينفذ هجوم للويب باستخدامBurp suite .
- يفحص نقاط الضعف في الشبكات اللاسلكية باستخدام الأمرNMA .
- يحدد منصات وهجمات الهواتف المتنقلة.
- يستخدم الأداة Netstat للكشف عن حصان طروادة.
- يحدد الإجراءات المضادة للبرامج الضارة والهندسة الاجتماعية باستخدام Social engineer Toolki.
- يستخدم اختبارات الاختراق وتقييمات الأمان وإدارة المخاطر.

❖ الفهرس

مقدمة في الاختراق الأخلاقي

الفصل الأول

في هذا الفصل سنتعرف على المواضيع التالية:

- الاختراق الأخلاقي
- بناء مختبر الأخلاق
- خطوات بناء مختبر الاختراق الافتراضي (عملي)

❖ الاختراق الأخلاقي

- **مفهوم الاختراق**

الاختراق هو الدخول غير المشروع إلى جهاز حاسب ما عن طريق ثغرات في نظام الحماية باستخدام برامج متخصصة يقوم بها محترفون أو هواة وذلك للحصول على البيانات أو تدميرها.

- **آلية الاختراق**

يعتمد الاختراق على السيطرة عن بعد عن طريق توفر برنامج على كل من جهازي المخترق وجهاز الهدف وتختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق.

- **مفهوم الاختراق الأخلاقي**

هو عملية أجراء فحص شامل لكل الأنظمة أو الأجهزة الموجودة في شركة أو مؤسسة ما , من اجل اكتشاف الثغرات التي يمكن استغلالها من قبل المخربين لإحداث اختراقات وسرقة للبيانات أو تخريبها والحاق أضرار جسيمة بالمؤسسات والعملاء وتعتمد على الخبرة في مجال الحاسب والشبكات والتي يتم توجيهها بشكل منهجي لاختراق نظام الحاسب أو الشبكة نيابة عن أصحابها لغرض إيجاد الثغرات الأمنية المتواجدة في الأنظمة المستهدفة ، وتعتبر مهنة ويقدم لها راتب شهري عند الشركات العالمية وهذا نتيجة انتشار الأخطار الأمنية حيث يقوم المخترق الأخلاقي بالتفكير بنفس الطريقة التي يفكر بها المخترق الغير أخلاقي ، حيث يختبر الاختراق الثغرات الأمنية ومن ثم معالجتها ويتم استخدام نفس المعرفة والأدوات التي يستخدمها المتسلل أو المخترق غير الأخلاقي , ولكن هنا تتم ممارسة الاختراق بطريقة قانونية ومشروعة لتقييم الموقف الأمني للنظام المستهدف , الفرق بينهما هو الهدف الذي يعتمده كل منهما من خلال عمله وبحثة وتجميع معرفته.

- **أهداف الاختراق الأخلاقي**

1. تامين الأنظمة
2. الدفاع ضد الهجمات المستقبلية
3. اكتشاف الثغرات البسيطة والمتقدمة
4. تقليل الوقت والجهود المطلوبة للاستمرار في مهاجمة الجهاز أو النظام ذاته بصورة متكررة

- **مصطلحات الاختراق**

فهم وتعريف المصطلحات جزءٌ مهم من مسؤوليات المخترق الأخلاقي، تتعلق هذه المصطلحات بكيفية تواصل مختصي الأمن الذين يعملون معًا في مجال الاختراق الأخلاقي.

- **التهديد Threat**

بيئةٌ أو وضع قد يقود إلى هجوم محتمل لأمن المعلومات في مؤسسةٍ ما، يبحث المخترقون الأخلاقيون عن التهديدات ويرتبونها حسب أولوياتها عندما يُجرون تحليلاً أمنيًا، يُعتبر المخترقون غير الأخلاقيون – هم وما يستعملونه من برمجيات وتقنيات الاختراق – تهديدات لأمن معلومات المؤسسة.

- **أداة الاستغلال Exploit**

يبحث المخترقون الغير أخلاقيون عن أدوات الاستغلال المناسبة لنظام حاسوبي لفتح ثغرة لهجوم ابتدائي، معظم أدوات الاستغلال هي أسطر برمجية قليلة تفتح ثغرات عند تنفيذها في نظام حاسوبي، ينشئ المخترقون الخبيرون أدوات الاستغلال الخاصة بهم، ولديهم مهارات برمجية ، العديد من برمجيات الاختراق لديها أدوات استغلال جاهزة يمكن تشغيلها ضد العديد من النظم الحاسوبية والشبكات، فأداة الاستغلال هي طريقة معرّفة لاختراق أمن نظام معلوماتي عن طريق ثغرة.

- **الثغرة Vulnerability**

خللٌ تشغيلي أو خطأ في التصميم المنطقي لبرمجية أو في تنفيذها، يمكن أن يقود إلى حدث غير متوقع وغير مرغوب فيه يؤدي إلى تنفيذ تعليمات مسيئة أو مخرِّبة للنظام، تُكتب تعليمات أداة الاستغلال لتستهدف ثغرة معيَّنة وتسبب خطأ في النظام بغرض استخراج بيانات مهمة.

- **هدف التقييم Target of Evaluation (TOE)**

هدف التقييم هو موضوع التحليل أو الهجوم الأمني، سواءٌ كان نظامًا، أم برنامجا، أم شبكة، يهتم المخترقون الأخلاقيون عادةً بأهداف التقييم ذات الأهمية المرتفعة؛ وهي النظم التي تحتوي على معلومات حساسة، مثل أرقام الحسابات أو كلمات المرور أو بيانات سرية أخرى، إن هدفَ المخترق الأخلاقي تجريبُ أدوات الاختراق على أهداف التقييم المهمة لتحديد الثغرات وسدها للحماية من أدوات الاستغلال ومن تسرب البيانات الحساسة.

- **Zero-day-vulnerability**

ثغرة الهجوم المكتشفة حديثا – ثغرة يوم الصفر ثغرة أمنية تم اكتشافها حديثا بدون برنامج إصلاحي أو حل لها للآن.

- **المهاجم Attaker**

هو الشخص الذي لديه مهارات ودوافع لاستغلال الثغرات الأمنية على نظام ما للوصول غير المشروع إليه.

- **الحمولة Payload**

تعليمات برمجية تحدد نتيجة استغلال الثغرات مثل فتح منافذ تكون موجودة داخل برنامج المهاجم.

- **الهجوم Attack**

يحدث الهجوم عندما تتم السيطرة على نظام اعتمادًا على ثغرة فيه، يُنفَّذ العديد من الهجمات عن طريق أدوات الاستغلال، يَستعمل المخترقون الأخلاقيون أدوات لاكتشاف النظم التي يمكن أن تكون معرضة لأداة استغلال بسبب نقاط ضعف في نظام التشغيل أو في تهيئة الشبكة أو في التطبيقات، وذلك لمنع هجوم معيَّن عليها.

- **اختراق Hacking**

هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، اختراق دخول غير مصرّح به إلى نظام إلكتروني.

- **اختبار الاختراق (Penetration Testing)**

يقصد بها قيام الشخص بمحاولة اكتشاف أي ثغرات موجودة في النظام، الموقع أو الجهاز المراد اختراقه بهدف وصوله لغايته والتي قد تكون إما لإغلاق هذه الثغرات أو لاستغلالها وإلحاق الضرر به.

- **البرمجيات الضارة Malware**

هو مصطلح عام يستخدم للتعبير عن البرمجيات الخبيثة كالفيروسات (Viruses) و الديدان (Worms).

- **Backdoor**

باب خلفي وهو 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.

- **حصان طروادة Trojan Horse**

تعني حصان طروادة وهو برنامج ضار يُحمَّل في المستضيف ويقوم بعمليات تشغيلية مطلوبة هو يقوم بما يشبه إخفاء النوايا حيث يحمله المستخدم ظناً منه أنه سيقوم بأمور معينة بينما هو يقوم بأمور أخرى كسرقة معلوماته الشخصية مثل كلمات سر حساباته وبطاقاته الائتمانية، ملفاته الشخصية، ومن هنا تأتي ضرورة تحميل البرامج من المواقع الرسمية لها.

- **الفيروسات Virus**

هو برمجية ضارة تصيب ملف ما أو برنامج وغيره ويحتاج إلى أن يتم تفعيله من قبل المستخدم من خلال قيامه بفتح الملف سواء بالنقر المزدوج عليه أو النقر على الرابط الموجود فيه وهو بدوره سيعمل وسيقوم هنا الفيروس بالتأثير على الملف.

- **الدودة Worm**

تعني دودة وتمتلك الديدان نفس القوة التدميرية للفايروس، ولكنها لا تحتاج لتدخل المستخدم للانتقال من هدف لآخر، بل تفعل ذلك بنفسها بشكل تلقائي، من الأفضل عدم استخدام الديدان في تجربة الاختراق حيث إنها غير قابله للتحكم بطبيعتها.

- **key-logger**

هو نظام يتجسس على ما يدخله المستخدم بواسطة لوحة المفاتيح ويرسله للمخترق ويعتبر أداة أساسية لمجربي الاختراق حيث تستخدم بصورة روتينية.

- **Botnet**

هو اختصار روبوت وهو عبارة عن شبكة من الأنظمة المخترقة يتم التحكم بها عن طريق جهاز حاسب واحد يسمى bot master.

- **Adware/Spyware**

هو برنامج مصمم لعرض إعلانات على جهاز الحاسب أو الهاتف الخاص بالمستخدم، مثل الإعلانات التي تظهر في عدة أماكن ولا يمكن إغلاقها ، هذه الإعلانات يتم التحكم بها Adware وهو ما يجعل المطور يحصل على المال من خلال ما يدعى الدفع لكل عرض أو مقابل النقرات وهو أمر يزعج المستخدمين لكن حين يقوم بجمع المعلومات ومراقبة النشاط الخاص بالمستخدمين من دون موافقتهم يكون حينها اسمه Spyware.

- **Target of evaluation**

استهداف للنظام أو البرنامج أو الشبكة التي توجد هذه الثغرة فيها.

- **Phishing**

رسائل احتيال إلكتروني يتم إرسالها إلى كميات كبيرة من إيميلات الأشخاص بشكل عشوائي بغرض سرقة حساباتهم أو بطاقات الائتمان أو كلمات المرور الخاصة.

- **Vishing**

يتم من خلال الاتصال بهاتف الهدف Voice Phishing.

- **APT اختصار لـ 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.

- **State Sponsored Attack**

هم المخترقين الذين يعملون تحت مظلة الأجهزة الحكومية والاستخباراتية التابعة لبلادهم ويتم دعمهم ماديا وخططيا وعدديا ومعلوماتياً من تلك الجهات.

- **Targeted Attack**

هو اختراق يستهدف شركة معينة وغرض هذا الاختراق دائما هو سرقة البيانات من الشركات.

- **Ransomware**

هو نوع من الفيروسات يجعل الحاسب الهدف غير صالح للاستخدام حتى يتم دفع مبلغاً معيناً من المال لإعادته إلى حالته الأصلية.

- **Social Engineering**

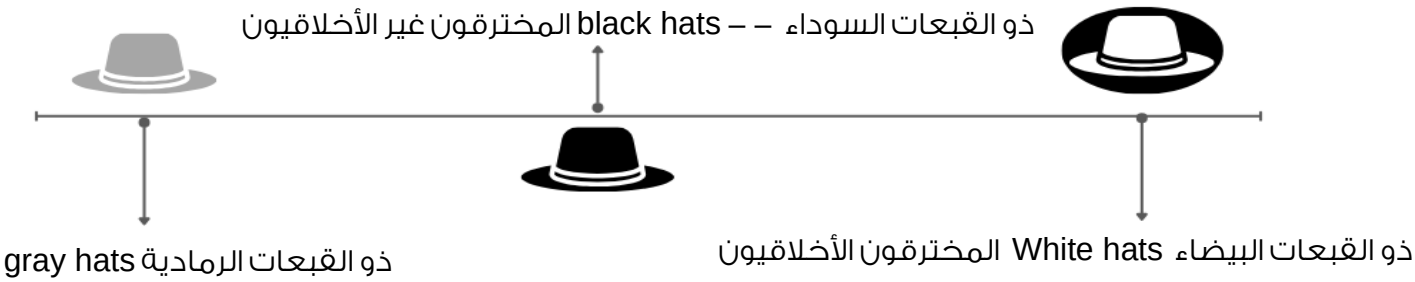
فن استخدام وخداع الشخص بحيث يقوم بشكل إرادي بكشف معلومات سرية أو بإعطاء المهاجم الفرصة للوصول للمعلومات السرية.

- **المخترق الأخلاقي**

المخترق الأخلاقيEthical Hacker يُعرف المتسللون الأخلاقيون أو المعروفون أيضاً باسم "القبعات البيضاء"، بأنهم خبراء أمنيون يقومون بإجراء التقييمات الأمنية ، يَستعمل المخترقُ الأخلاقي الأدوات البرمجيةَ والتقنيات ذاتها التي يستعملها المخترقون الغير أخلاقيون، ولكن هدف المخترق الأخلاقي هو إيجاد نقاط الضعف الأمنية في الشبكات والنظم الحاسوبية ، ومن ثم يمكن للمخترق الأخلاقي أن يطبق التصحيح أو التحديث المناسب لمنع المخترق الغير أخلاقي من النفاذ إلى البيانات ، لا تنتهي هذه الحلقة من التناوب بين دوري المخترق الأخلاقي والمخترق الغير أخلاقي، حيث تُكتشف نقاط ضعف جديدة في النظم الحاسوبية باستمرار، ومن ثم تستمر الشركات المطوّرة للبرمجيات بإنشاء التحديثات التي تخفّف خطرَ الهجوم.

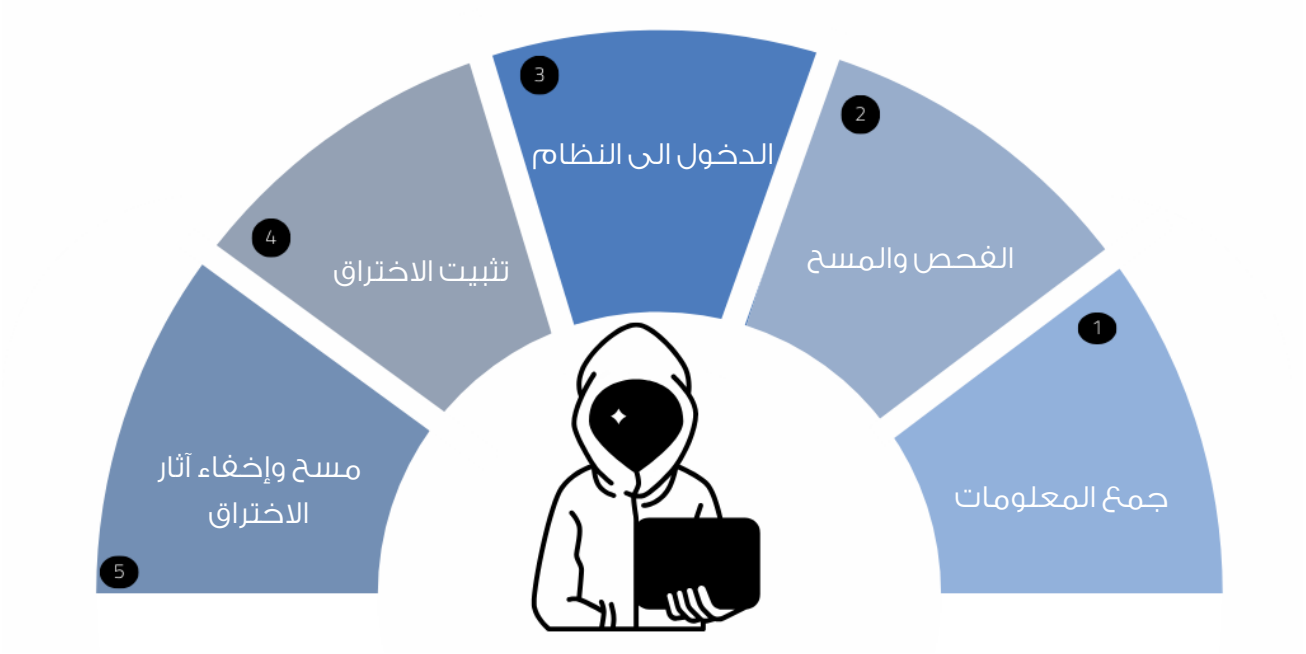
المخترقون الأخلاقيون هم عادةً محترفو الأمن أو مختبرو الاختراقات الشبكية الذين يستعملون أدواتهم ومهاراتهم الخاصة بالاختراقات بهدف الدفاع والحماية؛ فهم يختبرون أمن الشبكات والنظم للبحث عن نقاط الضعف، وذلك باستعمال الأدوات ذاتها التي قد يستعملها مخترق ما للسيطرة على الشبكة أو النظام.

- يمكن تصنيف المخترقين في ثلاث مجموعات



وهم عادةً مخترقون ذو نوايا حسنة ويعتبرون أنفسهم أخلاقيين، ولكنهم يُجرون اختبارات الاختراقات دون إذن من مالك البيانات ودون معرفته، ثم يعرضون نتائج عملهم واستعدادهم لسد الثغرات الأمنية، إلا أن طريقة عملهم تقابل بالرفض غالباً.

- **مراحل عملية الاختراق**



- **اختبار الاختراق**

هو محاكاة للهجمات المحتملة من قبل مخترقين الإنترنت على أنظمة المعلومات والبيانات الحساسة، نتيجة لهذه المحاكاة، يمكن للشركات القضاء على نقاط الضعف في أنظمتها وتصبح محمية من هجمات المخترقين، عادةً ما تكون الخطوط الرئيسية لاختبارات الاختراق في شكل اكتشاف التطبيقات أو البرامج التي تعمل في النظام، وتحليل وتقييم ما إذا كانت تحتوي على ثغرات أمنية.

- **فوائدها 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 يجب على المنظمة اتخاذ الاحتياطات اللازمة قبل مهاجمتها وليس بعد مهاجمتها حفاظا " على سمعتها وتجنبا" للخسائر المالية الكبيرة تشكل ضررًا كبيرًا للمنظمة عند مواجهة تسرب البيانات نتيجة لهجمات محتملة حيث يوجد قانون حماية البيانات الشخصية ، يتم تطبيق عقوبات مالية خطيرة على المنظمة ذات الصلة وتضر بسمعتها وتخضع المنظمات لاختبارات أمنية مختلفة وتكون ملزمة بشكل خاص بالحفاظ على سرية بيانات عملائها ، اختبار الاختراق Penetration Test يسمى أحيانا Pentest.

- **طرق اختبار الاختراق**

هناك ثلاث طرق من أجل أن يختبر المخترق نظام الاختراق في شركة ما، وهي:

- BlackBox

في هذه الطريقة يتم إعطاء المخترق فقط معلومات عن رابط الموقع أو عنوان الأهداف.

- GreyBox

في هذه الطريقة يتم اخذ معلومات بسيطة عن المستخدم مثل اسم المستخدم وكلمة المرور بشكل مبسط جداً ليس كمدير للموقع.

- Whitebox

هذه الطريقة فتعتبر من أسهل الطرق، حيث يتم إعطاء المخترق كافة المعلومات المتاحة والمطلوبة، **مثل:** بيانات مدير النظام، اسم المستخدم وكلمة المرور، حيث يتم تقديم كافة المعلومات التي يحتاجها المخترق، **يتم إجراء اختبار الاختراق في الحالات التالية:**

- تَطلب الامتثال التنظيمي إجراء تحليلات وتقييمات مجدولة بانتظام.
- إضافة تطبيقات أو بِنى تحتية جديدة للشبكات.
- إجراء ترقيات أو تعديلات كبيرة على البنية التحتية أو التطبيقات.
- تأسيس مكاتب في مواقع جديدة.
- تعديل سياسات المستخدمين النهائيين.
- تغيير تقنية المعلومات في الشركة بقدرٍ كبير.

أداء محاولات اختراق مصرح لها لأنظمة وتطبيقات الحاسبات والشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها.

- **وظيفة اختبار الاختراق الأمنية وكشف الثغرات المحتملة**

تكمن وظيفة اختبار الاختراق في حماية المواقع والبيانات والمعلومات الموجودة على الإنترنت، من خلال قيام مختبر الاختراق باختراق موقع ما بناء على طلب إدارة الموقع، وذلك للكشف عن الثغرات الأمنية للموقع، ما يساهم في حفظ كافة بيانات المستخدمين للموقع بعد ذلك.

يهدف اختبار الاختراق إلى الكشف عن الثغرات الأمنية ونقاط الضعف في البنية التحتية للبرمجيات وتقنية المعلومات، واستكشاف الآثار المحتملة لاستغلالها، وتقديم إرشادات قابلة للتنفيذ بشأن معالجتها، كل ذلك عن طريق محاكاة سيناريوهات الهجمات السيبرانية الحقيقية.

- **أنواع اختبار الاختراق**

عملية اختبار الاختراق لا تجري بطريقة واحدة، حيث يوجد عدة أنواع يتم استخدمها من قبل المختبرين تم تصنيفها **وفق الآتي:**

- **أولاً: الاختبار الخارجي External testing**

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.

- **ثانياً: الاختبار الداخلي Internal testing**

في الاختبار الداخلي، يقوم المختبِر بمحاكاة هجوم قد يحدث بواسطة شخص ضار من داخل المؤسسة

- **ثالثاً: الاختبار الأعمى Blind testing**

في الاختبار الأعمى، يُعطى الشخص الذي سيقوم بالاختبار فقط اسم المؤسسة المستهدفة.

- **رابعاً: اختبار التعمية المزدوجة Double-blind testing**

في اختبار التعمية المزدوجة، 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.

- **خامساً: الاختبار المستهدف Targeted testing**

في هذا السيناريو، يعمل كل من المختبِر وأفراد الأمن السيبراني معًا ويحافظون على تقييم بعضهم البعض لتحركاتهم، يعد هذا النوع من الاختبار تدريبًا قيمًا يزود فريق الأمن السيبراني بالمؤسسة بتعليقات في الوقت الفعلي من وجهة نظر المخترق.

- **اختيار أداة اختبار الاختراق المناسبة**

- **القوانين والمعايير DCI,DSS**

مجموعة إرشادية من معايير الدفع التي تحدد الحد الأدنى من المتطلبات الأمنية التي يجب تلبيتها لأي مزوّد خدمات يريد تخزين بيانات البطاقة الائتمانية أو معالجتها أو نقلها.

- يحدد معيار أمان بيانات صناعة بطاقات الدفع (PCI. DSS)
- التأكد من الحفاظ على أمان الشبكة التي تتم من خلالها المعاملات، ولذلك يجب استخدام جدران حماية قوية بشكل كافي لتقوم بدورها بفعّالية بدون أن تتسبّب بمتاعب إضافية لحاملي البطاقات أو البائعين.

❖ بناء مختبر الاختراق

إنشاء مُختبر اختراق افتراضي من أكثر التطورات التي يهتم بها الكثير من مسؤولي الأمن السيبراني لأن الكثير منهم جديد على المجال، فالأمر يحتاج إلى المُمارسة بإنشاء "مُختبر" لمُمارسة الاختراق بشكل سلمي تماماً،باستخدام تقنية المحاكاة التي تطورت تطورا سريعا مؤخرا مما أنتج برمجيات محاكاة جيدة جدا منها VirtualBox وVMWare وغيرهما الكثير.

❖ خطوات بناء مختبر الاختراق الافتراضي (عملي)

- **برنامج VirtualBox**

يتميز بإمكانيات كبيرة في أنظمة التشغيل، طورته شركة Oracle ويُمكن مختبري الاختراق من إنشاء وإدارة بيئات افتراضية لمحاكاة الاختراق الحقيقي دون تخريب البيئة الأساسية.

لا غنى عن هذه الأداة لصياغة بيئات اختبار خاضعة للرقابة، مما يسمح للمختبرين بتقييم نقاط الضعف دون تعريض الأنظمة الحية للخطر، من ناحية أخرى كالي لينكس، وهو نظام تشغيل مصمم لهذا الغرض، يزود مختبري الاختراق بمجموعة من الأدوات والموارد المتخصصة لإجراء تقييمات أمنية شاملة.

Kali Linux مهارة مهمة لاستكشاف منهجيات اختبار الاختراق المختلفة ومع ذلك، ينبغي أن يتم استخدام هذه الأدوات بشكل قانوني وفقًا لمبادئ الأخلاقيات السيبرانية وبإذن صريح من صاحب النظام أو المؤسسة ، يتم استخدام أدوات الهاكر والقرصنة في سياق الاختبارات الأمنية المعروفة أيضًا بالاختبارات القرصنة الأخلاقية أو الاختبارات الأمنية المؤسسية.

تتنوع أدوات الاختراق بحسب الغرض المخصص لها، وقد تشمل بعض الأمثلة على ذلك:

- أدوات اكتشاف الثغرات

تستخدم لاختبار الأمان والعثور على الثغرات في النظام أو التطبيقات المستهدفة مثل برامج اختبار الضعف وماسحات الأمان.

- أدوات الاختراق

تستخدم لاختراق الأنظمة والشبكات واختبار فعالية التدابير الأمنية المعمول بها، ومن أمثلة ذلك أدوات اختراق الشبكات والاختراق الاجتماعي.

- أدوات إعادة التجميع والاسترجاع

تستخدم لاستعادة المعلومات المحذوفة أو المشفرة وفحص محتوى الذاكرة وتحليل البرامج الضارة وفحص الحزم.

- أدوات التخمين والكسر

تستخدم لاختبار قوة كلمات المرور وتجربة مجموعة متنوعة من الاحتمالات للوصول غير المصرح به إلى النظام أو التطبيقات، تهدف استخدام هذه الأدوات بشكل مشروع ومن قبل المختصين إلى تحسين أمان النظام وتعزيز الوعي بالثغرات الأمنية المحتملة، ينبغي أن تكون مؤسسات ومحترفو الأمن السيبراني على دراية بأدوات الهاكر والقرصنة والتقنيات المستخدمة بهدف التصدي للتهديدات وتعزيز الأمن السيبراني في بيئتهم.

- **أدوات الاختراق**

هي برامج أو برامج متخصصة تستخدم لتحديد واستغلال نقاط الضعف في أنظمة الحاسب والشبكات، يتم استخدامها عادةً من قبل المتخصصين في الأمان السيبراني ومختبري الاختراق والمتسللين الأخلاقيين لاختبار أمان الأنظمة والتطبيقات.

يجب أن يتم استخدام أدوات الاختراق بشكل قانوني وفقًا للأطر القانونية والأخلاقيات السيبرانية، يتم استخدامها بشكل رئيسي في سياق الاختبارات الأخلاقية أو الاختبارات الأمنية المؤسسية، حيث يتم الحصول على إذن صريح من صاحب النظام أو المؤسسة قبل استخدام هذه الأدوات لاختبار الأمان وتحسينه، هناك أنواع من أدوات الاختراق المتاحة وتتنوع وظائفها وأغراضها وفقا للمهمة التي تقوم بها.

- **بعض الأنواع الشائعة الأخرى لأدوات الاختراق**

- **ماسحات الشبكة (Network Scanners):**

تستخدم لتحديد المضيفين والمنافذ المفتوحة على الشبكة، وتوفر معلومات حول تكوين الشبكة والأجهزة المتصلة بها.

- **أدوات تكسير كلمة المرور (Password Crackers):**

تستخدم لاستعادة كلمات المرور المفقودة أو المنسية، وتستخدم تقنيات مثل القوة الغاشمة والقواميس والهجمات المتقدمة لاختبار قوة وثغرات كلمات المرور.

- **أدوات الاستغلال (Exploitation Tools):**

تستخدم للاستفادة من نقاط الضعف المحددة في الأنظمة أو التطبيقات، وتسمح بتنفيذ شفرات خبيثة أو الحصول على وصول غير مصرح به إلى النظام.

- **مراقبة حركة الشبكة وتشم الحزم (Packet Sniffers):**

تستخدم لمراقبة حركة البيانات عبر الشبكة واستخراج المعلومات المرسلة والمستقبلة، ويمكن استخدامها للتجسس أو تحليل حركة البيانات لأغراض الاختبار والتحليل الأمني.

- **اكتشاف الجذور الخفية (Rootkit Detection):**

تستخدم للكشف عن الجذور الخفية والبرمجيات الضارة التي تختبئ في نظام التشغيل وتقوم بإخفاء أنشطتها ووجودها.

- **أدوات تحليل البرامج الضارة (Malware Analysis Tools):**

تستخدم لتحليل وفحص البرامج الضارة وفهم طريقة عملها وتأثيرها على الأنظمة، وتساعد في تطوير تقنيات الدفاع والكشف عن البرامج الضارة.

- **Install Oracle VM VirtualBox**
  - **أولا: تثبيت Virtual machine**

لإنشاء جهاز افتراضي وتثبيت Kali Linux عليه سوف يتم استخدام Oracle Virtual Box **عن طريق الخطوات التالية:**

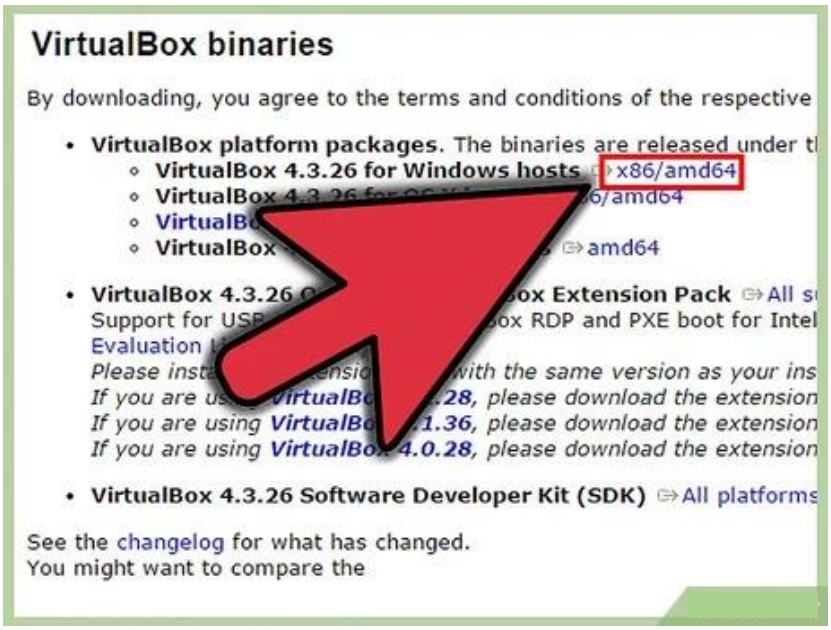
https://www.virtualbox.org

- كيفية التثبيت

١. **تثبيت برنامج VirtualBox**

يتم اختيار Windows hosts وتكملة خطوات المعالج حتى الانتهاء من التثبيت

١. تنزيل VirtualBox يمكنك تنزيل برنامج VirtualBox الخاص بشركة Oracle مجانًا من الموقع الإلكتروني الخاص بالمطوّر، احرص على تنزيل النسخة المناسبة لنظام التشغيل الذي تستخدمه، هناك العديد من الخيارات لنسخ نظام التشغيل Linux ، اختر الحزمة المناسبة لتوزيعة Linux التي تستخدمها، أو استخدم خيار كل التوزيعات إن لم تجد توزيعتك في القائمة.

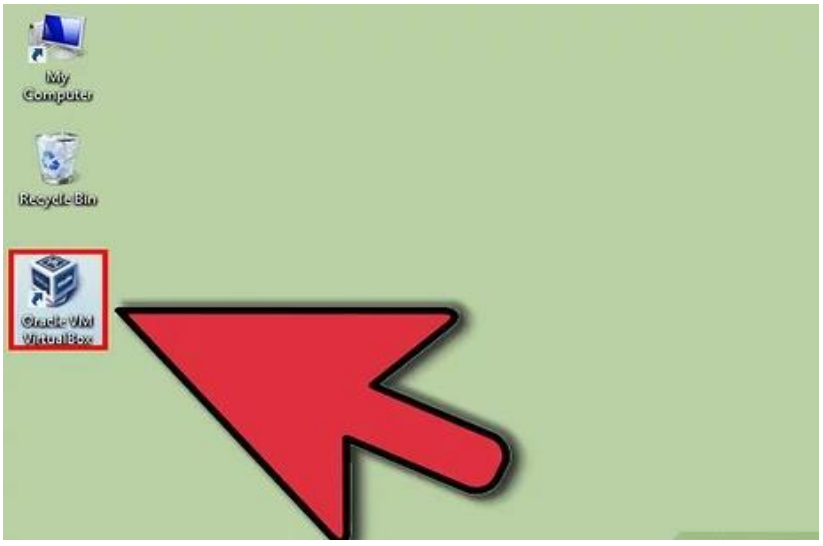


شكل (١) تثبيت برنامج VIRUALBOX

٢. ثبّت برنامج VirtualBox إن كنت تستخدم نظام التشغيل ويندوز، انقر نقرًا مزدوجًا على ملف التثبيت واتبع التعليمات لتثبيت البرنامج، إن كنت تستخدم نظام ماكنتوش، افتح ملف DMG الذي قمت بتنزيله واسحب ملف VirtualBox إلى مجلد التطبيقات.

اترك كل الخيارات على الوضع الافتراضي عند تثبيت البرنامج على نظام ويندوز.

شكل (٢) استكمال خطوات التثبيت



شكل (٣) الدخول على البرنامج

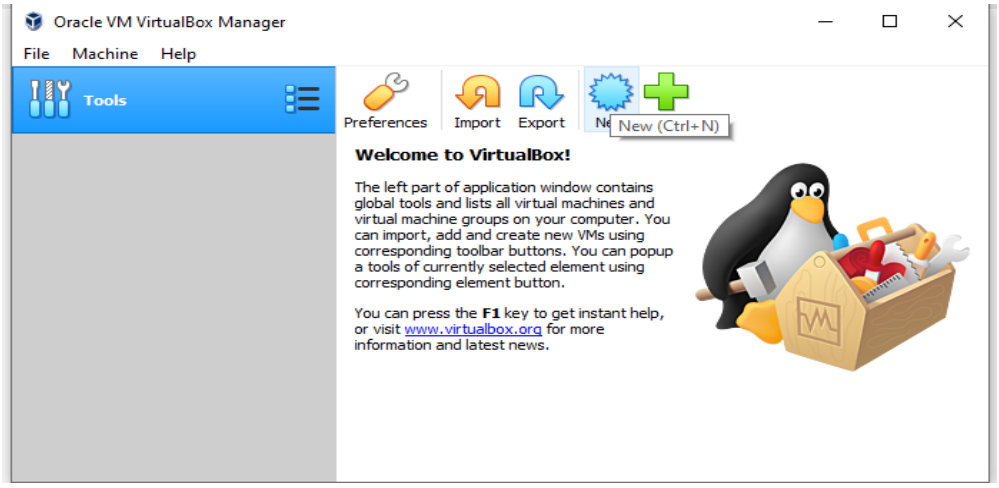
٣. شغّل البرنامج، يسمح لك برنامج VirtualBox أن تقوم بإدارة الأجهزة الافتراضية المختلفة بسهولة، كما يسمح لك أيضًا بإنشاء أجهزة أخرى، يمكنك تشغيل VirtualBox مباشرةً من برنامج التثبيت، أو تشغيله من أيقونة سطح المكتب.

٤. تحميل وتثبيت نظام kali Linux على نظام وهمي VirtualBox.

- **ما هو الكالي لينكس**

كالي لينكس أو kali Linux هو نظام تشغيل مثل ويندوز وماك أي تستطيع تنصيبها على الجهاز الشخصي كـ الويندوز، ولكن الهدف من نظام كالي هو لإجراء عمليات اختبار أمن المعلومات، واختبار الاختراق حيث تحتوي توزيعة كالي لينكس على المئات من الأدوات المتعددة المهام، تم تطويرها التوزيعة وتمويلها بواسطة شركة Offensive Security.

الضغط على أيقونة Oracle virtual BOX Manager على سطح المكتب يتم فتح شاشة يتم ظهور شاشة Oracle VM VirtualBox



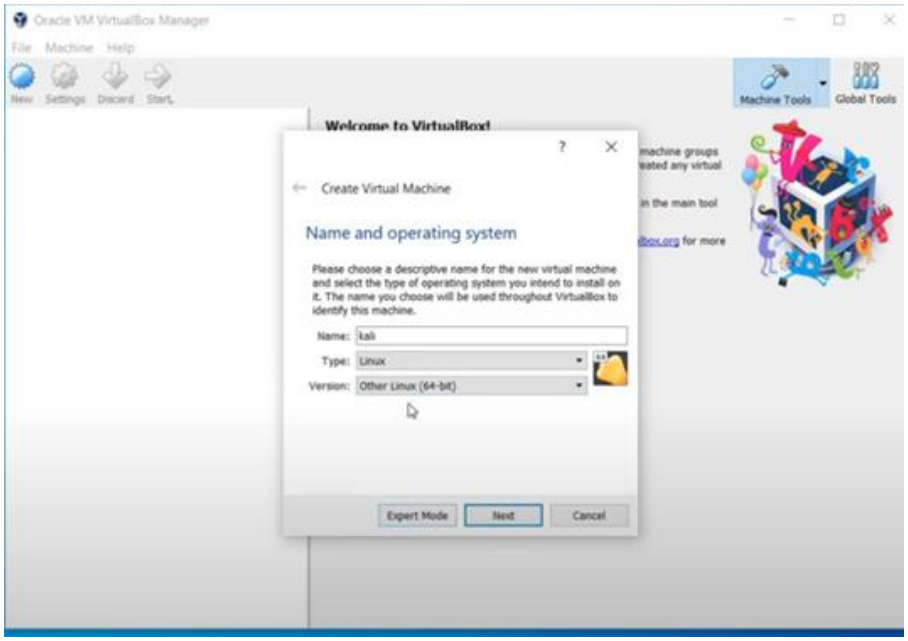
شكل (٤) الواجهة الأساسية

- **كيفية تثبيت كالي لينكس على برنامج النظام الوهمي VirtualBox**

١. افتح برنامج VirtualBox وانقر على New.

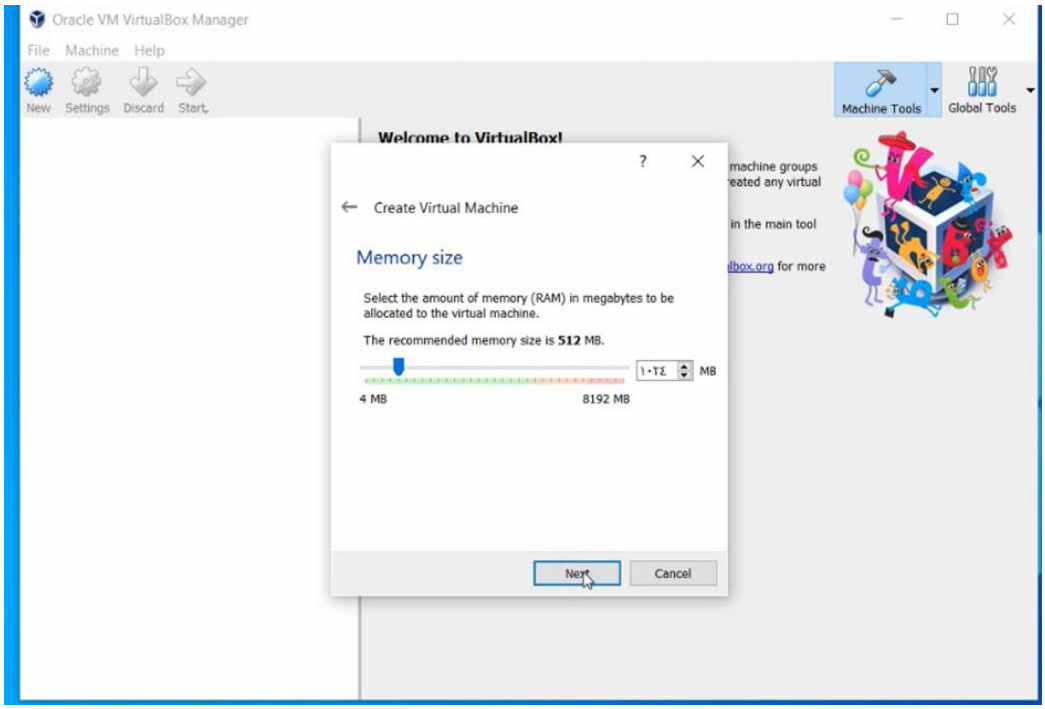
شكل (٥) الدخول على New 1

٢. الخانة الأولى أكتب اسم للنظام، مثل kali الخانة الثالثة اختار Linux ، الخانة الرابعة اختار نوع النسخة Other Linux 64 bit



شكل (٦) تسمية النظام

٣. نحد حجم الذاكرة الى 1024 MB ثم التالي

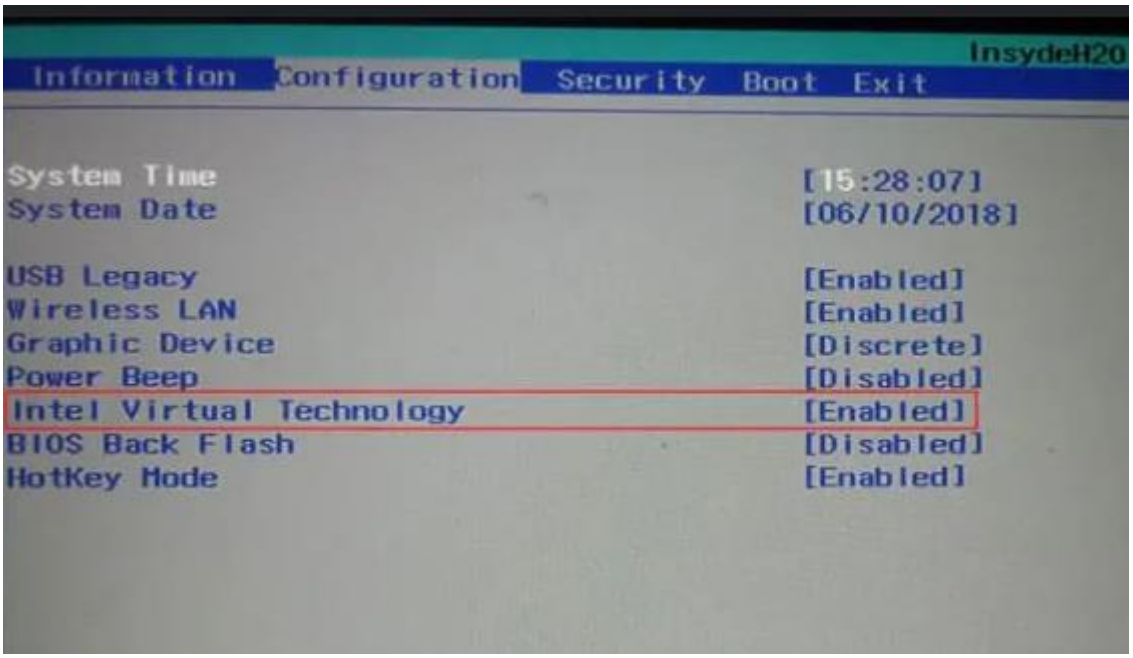


شكل (٧) ضبط حجم النظام

- **ملاحظة: في حال عدم ظهور النظام ٦٤بت**

عندما تحول تنصيب كالي لينكس ويكون نظام تشغيلك ٦٤ بت لكن تظهر لك رسالة أن نظامك ٣٢ بت **فالحل:**

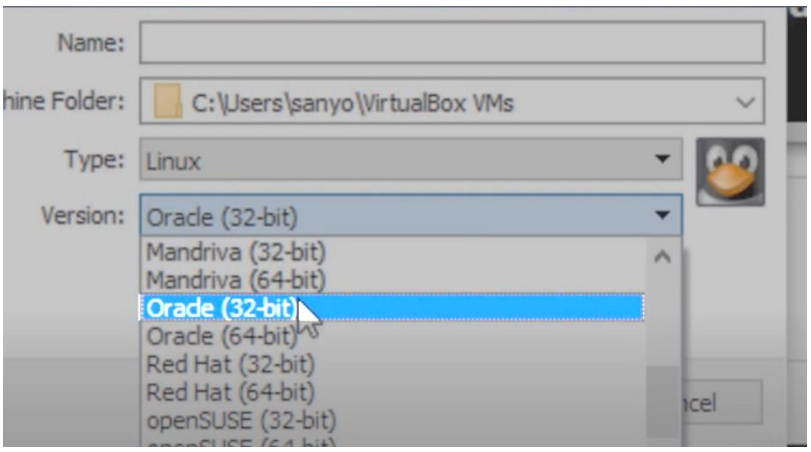
١. Configuration وتدخل الى intel virtual technology



شكل (٨) شاشة BIOS

٢. ستجدها disabled اجعلها enabled

٣. إعدادات – الكمبيوتر الشخصي – نوع النظام سيكون ٦٤ بت



شكل (٩) اختيار النظام في VB

٤. **الطريقة كالتالي:**

١. إعادة تشغيل الجهاز ثم الضغط على F2 باستمرار

- **ملاحظة:** بعض من المفاتيح المستخدمة للوصول إلى BIOS تتضمن مفاتيح **مثل:**
  - F1
  - F2
  - F10
  - Esc (Escape)
  - Del (Delete)

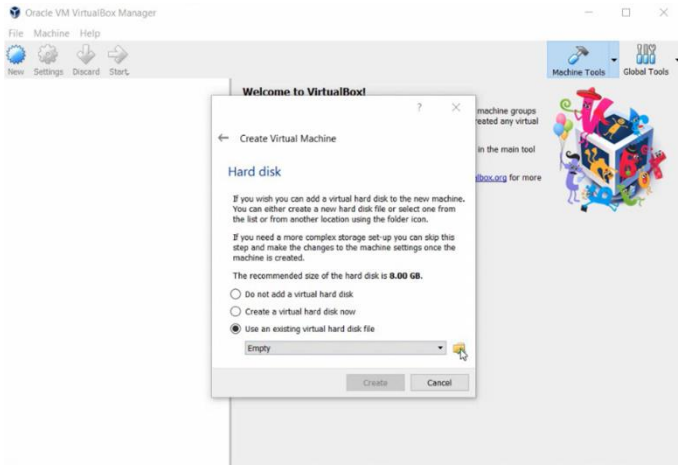
٥. من شاشة Bios نختار Configuration

٢. intel virtual technology

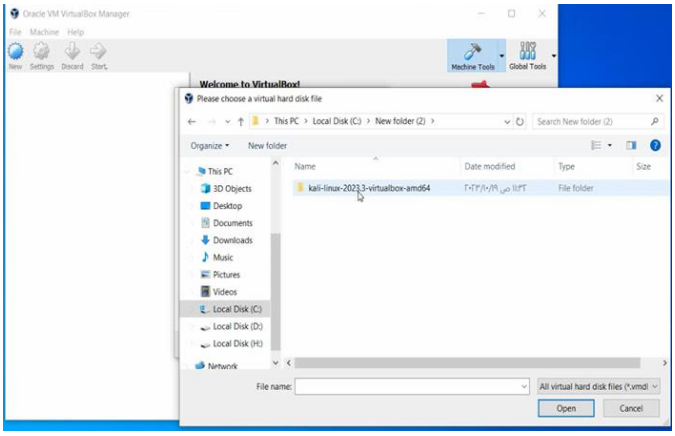
٣. ستجدها disabled_ اجعلها enabled

٤. ثم F10 حفظ وخروج

٦. سننتقل الى hard disk ثم نختار hard disk file virtual use and existing ثم نختار مكان image المطلوب (في المكان المخصص للحفظ على سبيل المثال سطح المكتب)

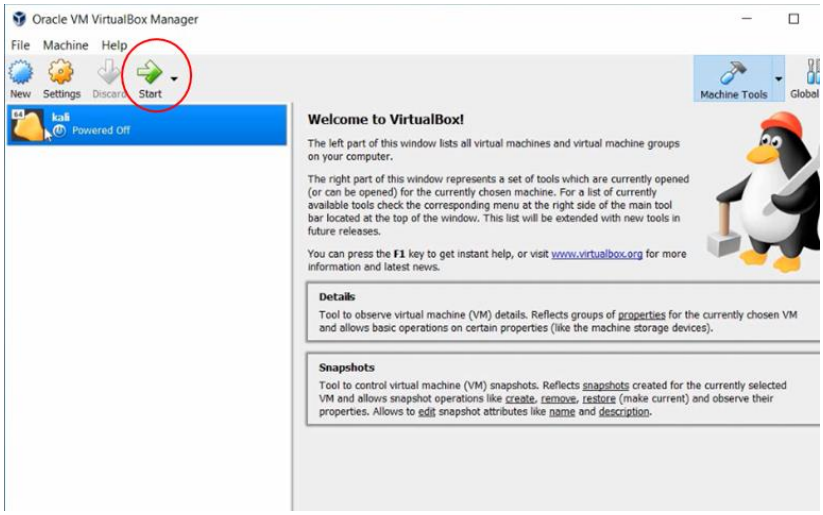


شكل (١٠) إضافة الصورة



شكل (١١) إضافة الصورة

٧. نختار النظام ثم نضغط start



شكل (١٢) اختيار start

٨. سيبدأ النظام بالإقلاع

٩. **ملاحظة:** اسم المستخدم وكلمة المرور: kali

- **Virtualization**

المحاكاة الافتراضية هي تقنية تتيح إنشاء تمثيلات افتراضية للخوادم والتخزين والشبكات والأجهزة المادية الأخرى، يحاكي البرنامج الافتراضي وظائف الأجهزة المادية لتشغيل عدة أجهزة افتراضية في الوقت نفسه على جهاز مادي واحد.

- **كيف تعمل الالة الافتراضية**

تقوم الآلة الافتراضية بإنشاء بيئة افتراضية تقع بين مستخدم الجهاز ومنصة التشغيل بحيث يستطيع المستخدم تشغيل البرامج المختلفة بدون الحاجة لوضع احتياجات كل منصة تشغيل، ويدعى البرنامج الحاسوبي المسؤول عن إدارة وتشغيل الآلات الافتراضية بمراقب الآلات الافتراضية.

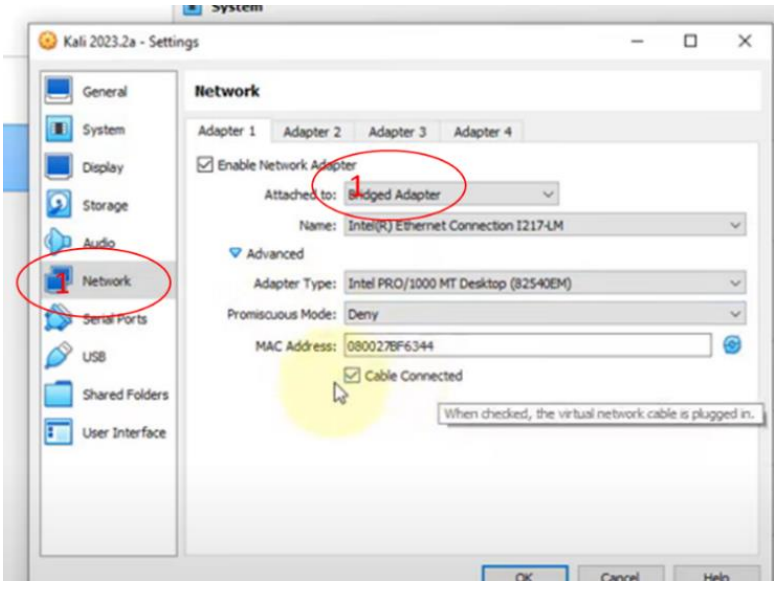
- **التعامل مع الكالي لينكس**

هو نظام تشغيل يحتوي على أدوات مثبتة لنا مسبقاً حتى نقوم بعمل اختبار اختراق ناجح، وهو نظام يستخدم من قبل الهاكرز لاختبار الأنظمة ومعالجة الثغرات الموجودة بها، وأيضا يستخدمه الهاكرز الغير أخلاقي مثل Ethical Hackers الأخلاقي وغيرهم من الهاكرز المخربين Black Hat Hackers أصحاب القبعات السوداء.

- **الان القيام بتعديل بعض الإعدادات في النظام من خلال الضغط:**

قائمة Settings ثم اختيار Network واختيار نوع كارت الشبكة ثم الضغط على موافق.

ضبط إعدادات بطاقة الشبكة اللاسلكية Wireless Adapter



لابد أن تتوافق مواصفات بطاقة الشبكة اللاسلكية Wireless Adapter مع عمليات تنفيذ اختبار الاختراق للشبكات اللاسلكية **التي تتطلب أن يكون:**

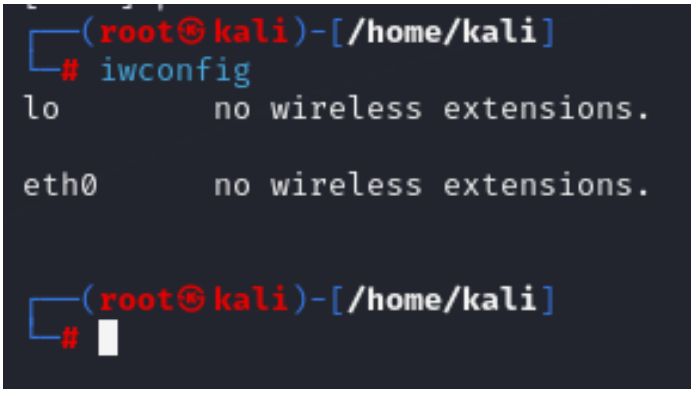
– متوافق مع IEEE 802.11b/g/n wi-fi Standard

– يدعم نمط المراقبة monitor mode الذي يسمح بالتصنت على wireless

تفعيل الـmonitor mode على Kali Linux :

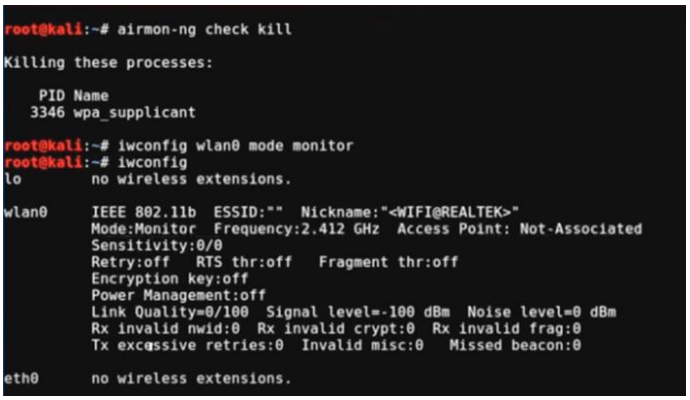
**ندخل على التيرمنال ونكتب الأمر التالي:

هو كرت البطاقة اللاسلكية Eth0



شكل (١٣) تعيين ip لكرت الشبكة1

نلاحظ أن الوضع أصبح " monitor mode" أصبح الكرت قادر على رؤية جميع الحزم



شكل (١٤) monitor mode1

– يدعم Packet Injection حقن الحزم.

- **طريقة التثبيت لـ virtualbox , kali Linux**
  - **كالي لينكس Kali Linux**

هو توزيعه من نظام التشغيل لينكس مخصصة لاختبار الاختراق والتدقيق في سلامة البيانات، كالي لينكس وهو يحتوي على أفضل الأدوات المستخدمة في عملية اختبار الاختراق أو الاختراق الأخلاقي.

- **مميزات نظام الكالي لينكس**

يمكن العمل مع كالي لينكس بعدة طرق مختلفة يمكن تثبيته على Virtual Machine داخل نظام ويندوز أو بالإمكان تثبيته كنظام رئيسي أو تثبيته بجانب ويندوز ويتم اختيار نظام التشغيل المطلوب أثناء عملية الإقلاع.

- **أدوات الكالي لينكس**

١. جمع المعلومات Information Gathering

يحتوي على أدوات الاستطلاع المستخدمة لجمع المعلومات والبيانات من الشبكة أو الجهاز الهدف.

٢. تحليل الثغرات Vulnerability Analysis

تحتوي على أدوات تخمين الثغرات في النظام الهدف وهذه الأدوات تستخدم بعد القيام بعملية الاستطلاع وجمع المعلومات عن الشبكة أو الجهاز الهدف.

٣. تحليل تطبيقات الويب Web Applications Analysis

تحتوي على الأدوات التي تستخدم في فحص واستغلال الثغرات في خوادم الويب.

٤. الهجمات على كلمة السر Password Attacks

تحتوي على الأدوات التي تقوم بهجمات القوة الغاشمة Brute force وهجمات تخمين كلمة السر بشكل Offline.

٥. الهجمات على الشبكات اللاسلكية Wireless Attacks

تحتوي على الأدوات المستخدمة في استغلال الثغرات الموجودة في بروتوكول الشبكات اللاسلكية 802.11 بالإضافة لأدوات استغلال ثغرات البلوتوث وثغرات RFID

٦. أدوات الاستغلال Exploitation Tools

تحتوي على الأدوات المستخدمة في استغلال الثغرات التي تم اكتشافها في النظام الهدف.

٧. التصنت وانتحال الشخصية Sniffing and Spoofing

تحتوي على أدوات التقاط حزم البيانات في الشبكة وأدوات تعديل حزم البيانات من أجل انتحال الشخصية.

٨. الهندسة العكسية Reverse Engineering

تحتوي على أدوات الهندسة العكسية وأدوات تحليل البرمجيات الخبيثة.

٩. التحليل الجنائي Forensics

تحتوي على الأدوات المستخدمة في مراقبة وتحليل بيانات وتطبيقات الشبكات وأدوات التحليل الجنائي الرقمي.

١٠. أدوات إعداد التقارير Reporting Tools

يمكن من خلالها تشغيل وإيقاف خدمات كالي لينكس مثل سيرفر الأباتشي.

- **تحديث الكالي لينكس**

يجب تحديث الكالي لينكس بشكل دائم للتأكد من أن نظام التشغيل الأساسي والتطبيقات في أحدث نسخة وأن التحديثات الأمنية مطبقة ويتم ذلك باستخدام الأمر.

١. يجب التعرف أولا على الأمر sudo حيث انه يقوم برفع الامتيازات عن المستخدم

(يقوم الأمر sudo مؤقتًا برفع الامتيازات التي تسمح للمستخدمين بإكمال المهام الحساسة دون تسجيل الدخول كمستخدم أساسي)

$sudo apt-get update

شكل (١٥) إدخال الأمر sudo 1

- **استخدام apt**

هي اختصار Advanced Packaging Tools وهي تقوم بالبحث في المستودع وتثبيت الحزمة المطلوبة أو تقوم بتحديثها ويمكن أن تستخدم للقيام بعملية الترقية upgrade لكامل النظام.

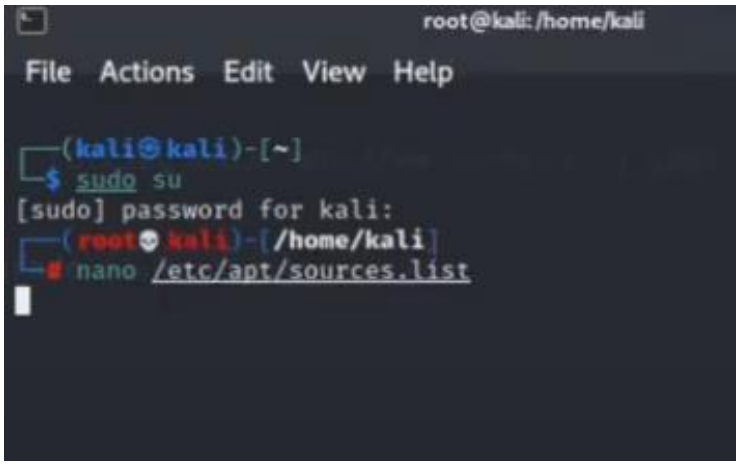
- **استخدامات أمر apt**

apt-get date –ا

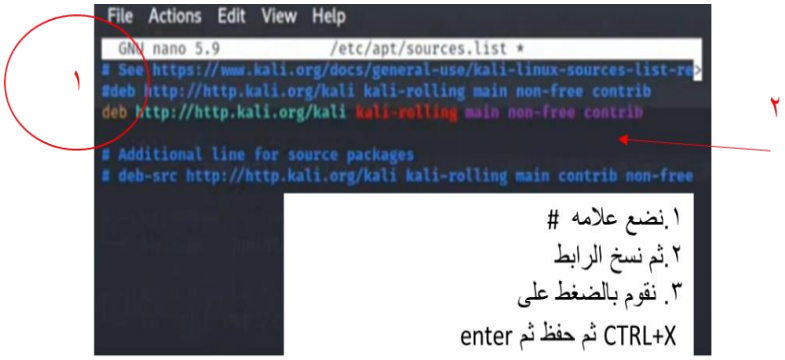
تستخدم من أجل تزامن ملفات الحزمة الحالية مع مصدرها المُعرف في ملف sources.list وعملية التحديث يجب أن تستخدم دائما قبل القيام بعملية الترقية upgrade or dist-upgrade

شكل (١٦) التسجيل كمستخدم كالي ا

" لحل مشكلة sources.list نقوم بالدخول على التيرمنال ومتصفح النظام لكالي لينكس ثم نسخ الرابط الاتي: https://www.kali.org/blog/kali-linux-2022-1-release/



شكل (١٧) حل مشكله المصدر



شكل (١٨) تثبيت الحزم

٢- apt-get upgrade

تستخدم لتثبيت أحدث نسخة من كل الحزم المثبتة على النظام وذلك من خلال المصادر المُعرفة في ملف sources.list .

" عملية الترقية لا تقوم بتغيير أو حذف الحزم التي لا يوجد نسخ جديدة منها ولا تقوم بتثبيت أي حزم جديدة غير موجودة مسبقا".

٣- apt-cache show<package name>

تستخدم لعرض معلومات عن حذمة معينة.

٤- apt-get remove< package name>

تستخدم لحذف حزمة معينة.

٥- apt-get dist – upgrade

تستخدم لترقية كل الحزم المثبتة على النظام وتقوم بإزالة الحزم التي لا تُستخدم من النظام.

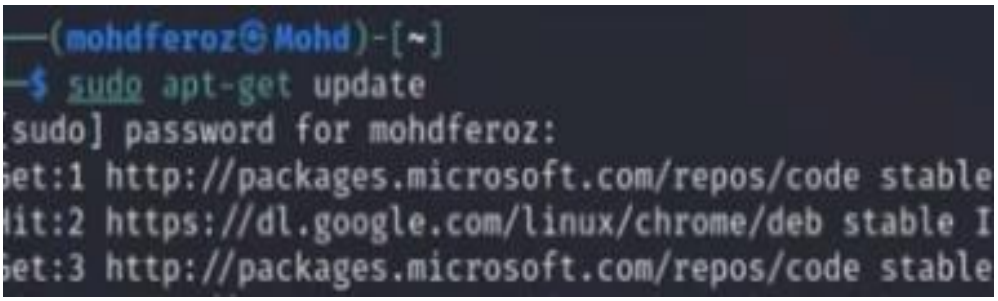
- **تثبيت أدوات إضافية على كالي لينكس**

يحتوي كالي لينكس على العديد من الأدوات، ولكن من المحتمل أن يتم الاحتياج لتثبيت أدوات إضافية لزيادة فعالية عملية اختبار الاختراق في بيئات معينة، **يوجد عدة طرق لتثبيت أدوات إضافية على كالي لينكس:**

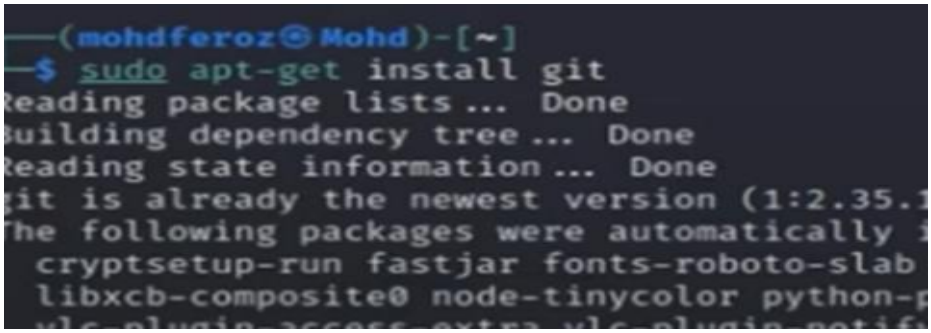
- التثبيت المباشر للأدوات

كل الأدوات الموجودة في مستودع كالي لينكس **Kali Linux repository** يتم تثبيتها من خلال الأمر:

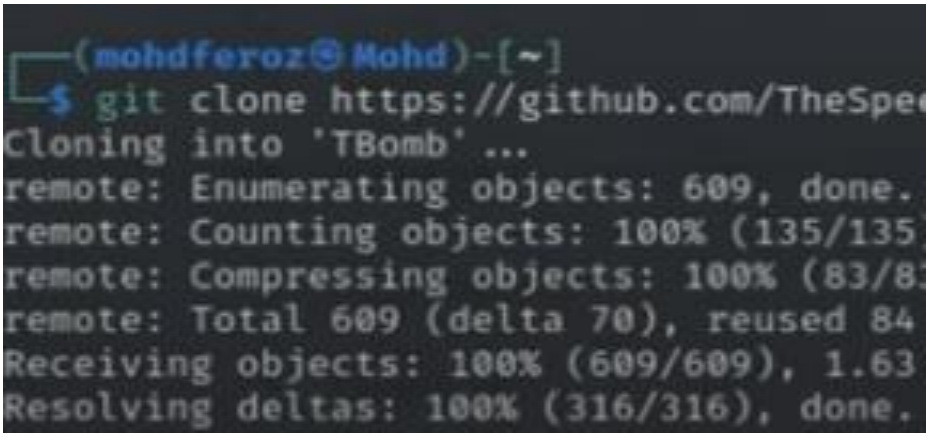
```
Apt-get install
```



شكل (١٩) تحديث للنظام



شكل (٢٠) تنزيل الحزمة



شكل (٢١) التثبيت من الرابط

- **بعض التطبيقات المقترحة**

  - **Apt-file**

هي command-line tool تستخدم للبحث داخل نظام APT packaging system وهي تسمح بعرض محتويات الحزمة بدون تثبيتها أو إحضارها.

  - **Gnome-tweak-tool**

تسمح للمستخدم بتغيير Themes وتغيير إعدادات سطح المكتب.

  - **OpenOffice**

هو مجموعة تطبيقات مفتوحة المصدر تستخدم لإنشاء وإدارة المستندات النصية.

  - **Scrub**

هو أداة حماية تقوم بحذف البيانات بشكل أمن عن طريق استخدام عدة أشكال لإعادة الكتابة فوق المساحة المخصصة للبيانات المحذوفة.

تمارين الفصل الأول

١. **اختار الإجابة الصحيحة فيما يلي:**

١. **هو الدخول غير المشروع إلى جهاز حاسب ما عن طريق ثغرات في نظام الحماية باستخدام برامج متخصصة يقوم بها محترفون أو هواة وذلك للحصول على البيانات أو تدميرها.**

أ- **الاختراق** ت- كالي لينكس

ب- النظام ث- الثغرات

٢. **ثغرة أمنية تم اكتشافها حديثا بدون برنامج إصلاحي أو حل لها للآن**

أ- **ثغرة يوم الصفر** ت- ثغرات الأيام

ب- ثغرة يوم الأول ث- ثغرة المتحرفين

٣. **هو الشخص الذي لديه مهارات ودوافع الاستغلال الثغرات الأمنية على نظام ما للوصول غير المشروع إليه.**

أ- **المهاجم** ت- المشفر

ب- المدافع ث- المصنف

٤. **مراحل عملية الاختراق**

أ- **جمع المعلومات** ت- تشفير البيانات

ب- جمع الاكواد ث- فك تشفير البيانات

٢. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	من أنواع اختبار الاختراق الاختبار الخارجي	√
٢.	$sudo apt-get update للتحديث	√
٣.	من مميزات نظام كالي لينكس سطح المكتب	×
٤.	اختيار الحجم المناسب للذاكرة للنظام ١٠٢٤	√
٥.	البرنامج VirtualBox يستخدم في الاختراق عن طريق إضافة kali Linux	√
٦.	يختبر الاختراق الثغرات الأمنية ومن ثم معالجتها ويتم استخدام نفس المعرفة والأدوات التي يستخدمها المتسلل أو المخترق غير الأخلاقي	√

الاستطلاع: جمع المعلومات للمخترقين الأخلاقيين

الفصل الثاني

في هذا الفصل سنتعرف على المواضيع التالية:

- الهدف من عملية الاستطلاع والتهديدات الناتجة منها
- الاستطلاع FootPrinting
- طرق عمليات الاستطلاع (عملي)
- أدوات FootPrinting
- التدابير المضادة والحماية من عمليات الاستطلاع (عملي)

- **مقدمة**

يقصد بمرحلة الاستطلاع **Reconnaissance** هو جمع المعلومات عن المنظمة الهدف أو بالتحديد شبكة المنظمة الهدف، فقبل أن يقوم المخترق باختراق نظام المعلومات في منظمة ما فإنه يقوم أولا بالتحضير والإعداد لهذا الاختراق من خلال جمع كل المعلومات الممكنة والمتوافرة عن شبكة المنظمة التي يريد اختراقها والمعلومات التي يتم تجميعها في مرحلة الاستطلاع:

- تساعده في أمور كثيرة مثل تحديد الأهداف ذات القيمة العالية في المنظمة المستهدفة.
- تحديد مواقع وجود المعلومات المطلوبة والحصول على بيانات يمكن من خلالها بدء الهجوم مثل عناوين **IP** للحواسب الموجودة في المنظمة.
- يجمع حسابات المستخدمين والمدراء وترجع أهمية هذه الحسابات إلى أن أنظمة التشغيل الشبكية تعتمد آلية أمان تسمى آلية التحقق من الصحة وبمقتضى هذه الآلية فإنه لا يمكن الدخول إلى أي نظام شبكي إلا بواسطة اسم المستخدم وكلمة المرور.

ومرحلة الاستطلاع تتميز بالسعة وعدم التحديد ويقوم فيها المخترق بجمع كل المعلومات عن المنظمة مهما كانت تبدو عديمة القيمة ويستخدم في ذلك مصادر مختلفة للمعلومات في شبكة الإنترنت أو على الواقع فهي نوع من البحث الشامل غير المحدد عن المعلومات.

يطلق على هذه العملية مصطلح **Reconnaissance** أو **Footprinting**

❖ الهدف من عملية الاستطلاع والتهديدات الناتجة منها

تهدف مرحلة الاستطلاع إلى تكوين نظرة شاملة لنظام الحاسب الآلي المستهدف والمنظمة التي ينتمي إليها ذلك النظام وذلك بغرض إيجاد طرق اقتحام النظام المعلوماتي للمنظمة والدخول إليه لسرقة المعلومات المهمة.

- **أهداف مرحلة الاستطلاع**

- جمع المعلومات عن بيئة النظام المعلوماتي المستهدف والبنية المعمارية التي يتكون منها.
- الكشف عن نقاط الضعف في النظام وأفضل الطرق لاستغلالها.
- التعرف على أكثر الجوانب الأمنية والتفاصيل الدقيقة للنظام الهدف مثل أنظمة الوصول عن بعد والمنافذ وأنواع الخدمات وطرق وأساليب الحماية والأمن والأنظمة الأمنية التي تتبعها المنظمة.

تتميز مرحلة الاستطلاع بالشمولية و السعة ،بمعنى أنه لا يوجد معلومات محددة يجب البحث عنها خلال هذه المرحلة بل يقوم بإجراء البحث عن كل المعلومات المتاحة و عليه أن يلتقط كل معلومة عن النظام الهدف سواء كانت على شكل أجزاء صغيرة و مقتطفات أو على شكل مجموعات متكاملة وسواء بدت له تافهة أو مهمة ، ثم يقوم بعد ذلك بتركيبها أو تجميعها مع بعضها ودراستها وتحليلها لأن المعلومات التي تبدو غير مهمة في هذه المرحلة قد تكون حاسمة في نجاح المراحل اللاحقة للدخول إلى النظام ،كما أن المعلومات التي تكون غير مفيدة بسبب أنها متفرقة تكون أكثر أهمية عند تجميعها و القاعدة في هذه المرحلة هي الشمولية في البحث و لكن مجموعات محددة من المعلومات **يجب أن يحصل عليها:**

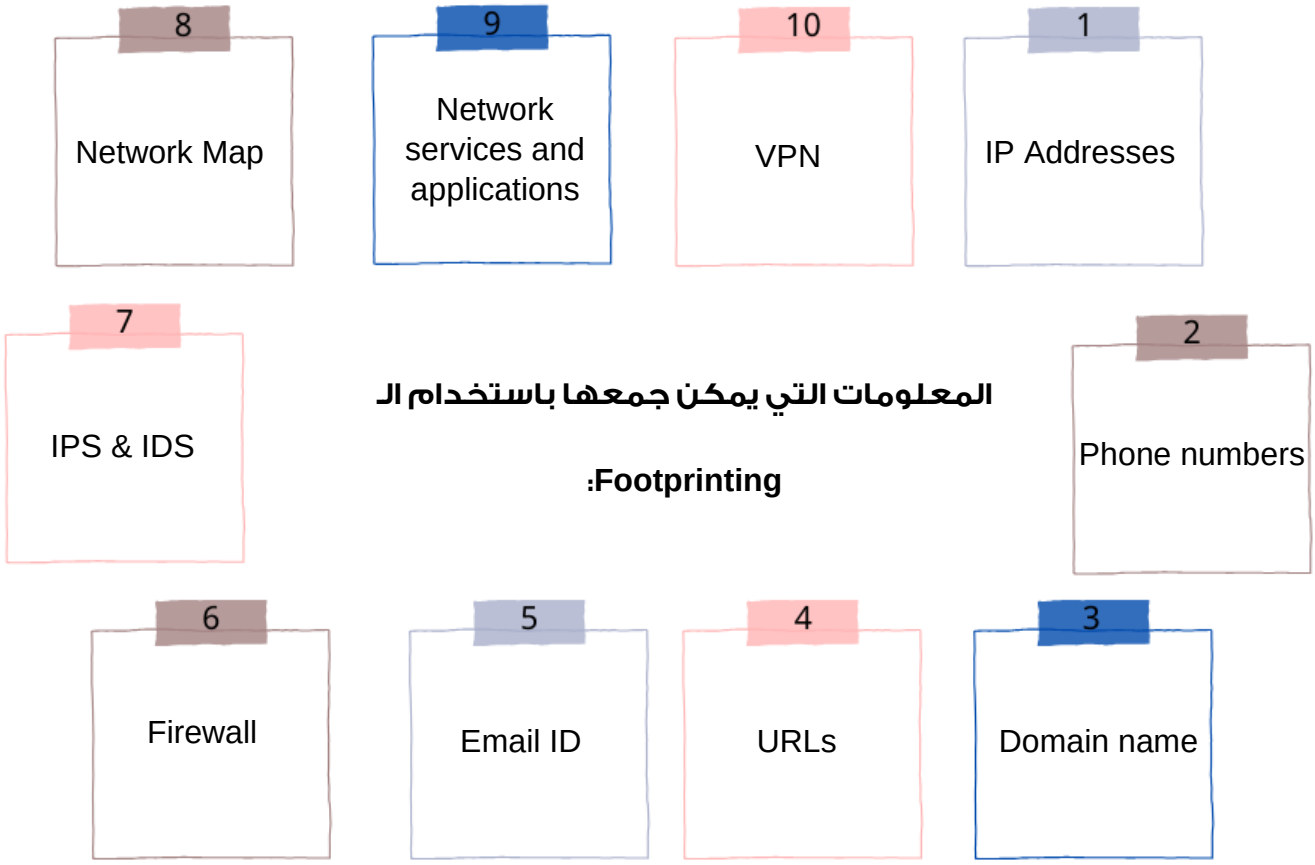
١	معلومات عن شبكة المنظمة	مثل اسم الميدان للمنظمة وأسماء الميادين للشبكات الداخلية الفرعية للمنظمة وعناوين **IP** ، كتل الشبكة، البروتوكولات والخدمات، جدار النار، موقع المنظمة على الإنترنت وخريطة الشبكة ومعماريتها.
٢	معلومات عن النظام	مثل نظام أو أنظمة التشغيل في المنظمة، بروتوكول **SMNP** نظام الوصول عن بعد، كلمات السر **PASSWORD**، أسماء المستخدمين والمجموعات، جداول الموجهات، آلية التحقق من الصحة.
٣	معلومات عن المنظمة	مثل تفاصيل الموظفين كالعناوين وأرقام الهواتف، دليل أسماء وهواتف المنظمة، موقع الويب الخاص بالمنظمة، عناوين البريد الإلكتروني.
٤	رسم خريطة للشبكة	تساعده على توجيه الهجوم باستخدام أداة مثل: **Tracert**

❖ الاستطلاع Footprinting

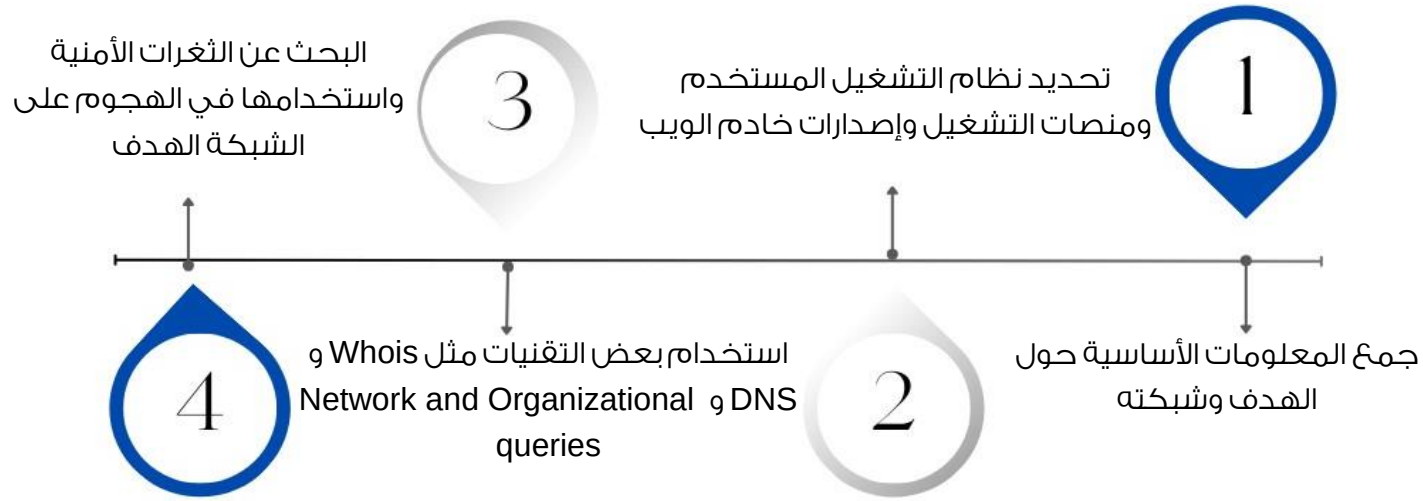
هو عبارة عن تقنيات تستخدم لجمع أكبر قدر من المعلومات حول نظام مستهدف معين لاستخدام تلك المعلومات في هجمات سيبرانية وذلك بطرق وأدوات مختلفة، **وللـ Footprinting نوعان:**

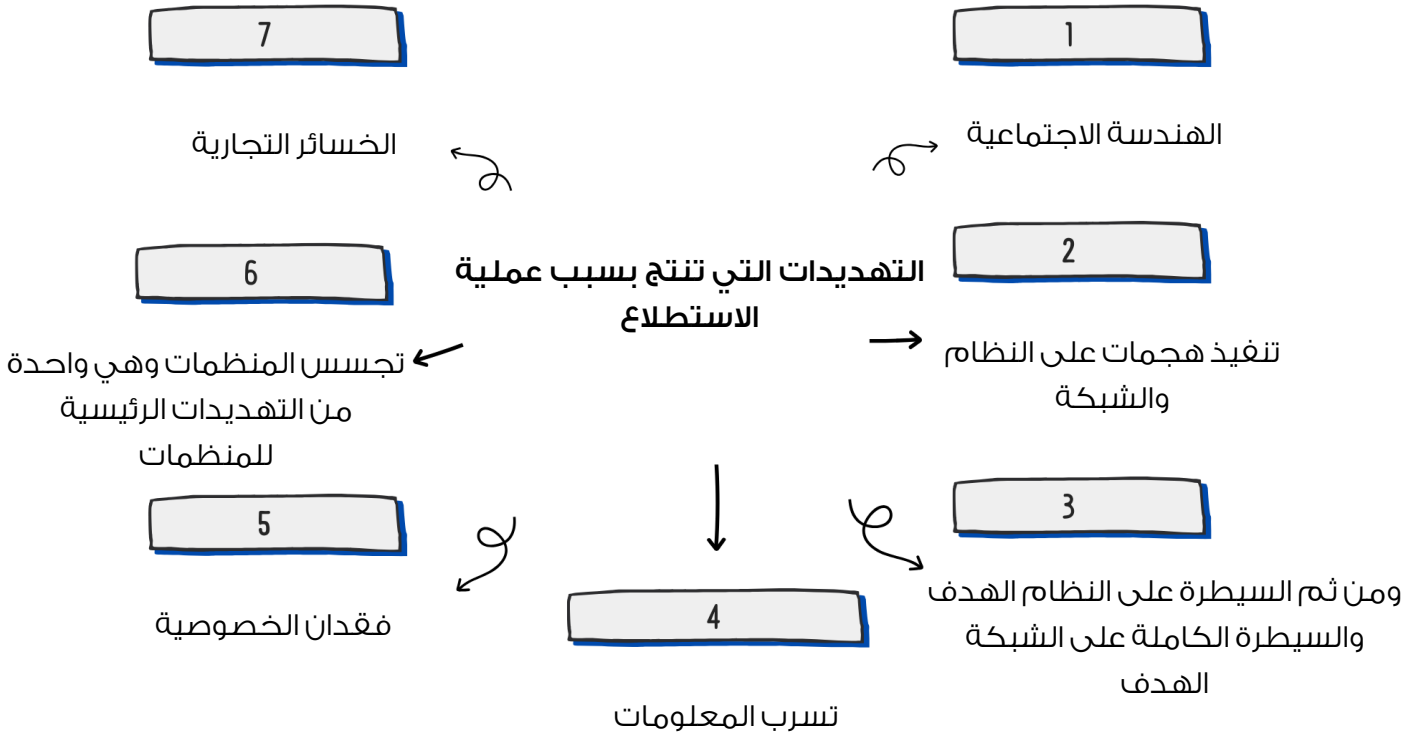
١. **Active Footprinting**: تتم العملية من خلال الاتصال المباشر بالنظام أو الجهاز المستهدف، وهنا يحتاج الأمر إلى قدرة عالية من التخفي لتجنب الاكتشاف من قبل أجهزة الـ **IPS and IDS**.

٢. **Passive Footprinting**: وهنا يقوم المهاجم بعملية جمع المعلومات عن جهاز أو نظام يقع عن بعد، حيث تتم هذه العملية من خلال جمع المعلومات من **Google search**، أو البحث في **archive.org**، ولا يحتاج هذا النوع إلى التخفي فهو يتم باستخدام أدوات بعيدة عن أن تصل إلى النظام الهدف أو أن تكتشف من قبل أجهزة كشف ومنع التسلل.



- **Footprinting في أربعة خطوات هي:**





الاستطلاع السلبي	جمع المعلومات دون التفاعل مع الهدف ولن تكون الجهة المستهدفة على علم بأن هناك من يجمع المعلومات عنها مثل جمع المعلومات من مواقع الإنترنت 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 و باستخدام هذا النوع يمكن تجميع المعلومات مثل نطاق الشبكة و عناوين **IP** للوصول للإنترنت و نظام التشغيل و تطبيقات الخوادم و بنية النظام و أنظمة كشف التسلل ويطلق عليه **Passive Information Gathering (OSINT)**.
الاستطلاع النشط	جمع المعلومات بالتفاعل مع الهدف بشكل مباشر، مثلا أن يقوم المخترق بتصفح الموقع الإلكتروني 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 الإنترنت والخدمات مما يعطي للمخترق مؤشرات عن إجراءات الأمن 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 **مثل:** ▪ **Shouler Surfing** هي تقنية يقف فيها المهاجم وراء الضحية ويلاحظ أنشطتها على جهاز الحاسب مثل ضربات المفاتيح أثناء إدخال أسماء المستخدمين وكلمات السر ويُستخدم هذا الأسلوب للحصول على كلمات السر والرموز الأمنية وأرقام الحسابات وبطاقة الائتمان. ▪ **Dumpster Diving** تقنية معروفة أيضا باسم **trashing** حيث يقوم المهاجم بالحصول على المعلومات من القمامة الخاصة بالمنظمة الهدف للحصول على معلومات مهمة وصناديق القمامة الخاصة بالطابعات وملاحظة لاصقة في مكاتب الموظفين.

❖ طرق عمليات الاستطلاع (عملي)

تحتوي توزيعة كالي لينكس على قائمة مليئة بالأدوات تحت عنوان **Information Gathering** مخصصة لعمليات الـ **Footprinting** ، يتم جمع المعلومات بتركيب البرنامج لان في هذه المرحلة بواسطة بعض أدوات الاختراق المتخصصة للبحث في الإنترنت وتنقسم أدوات جمع المعلومات بشكل عام إلى تطبيقات وإلى مواقع ويب وأساس عمل كل هذه الأدوات هو القيام بعمليات بحث مفتوحة في مصادر عامة على شبكة الإنترنت مثل الأخبار والمقالات والمجموعات الإخبارية وشركات التسجيل وخوادم أسماء النطاقات ، وتوجد في كل الأدوات المخصصة لجمع المعلومات خطوات محددة يقوم بها المخترق سواء كان يستخدم أداة أو برامج معينة أو كان يستخدم موقع من مواقع الويب الخاصة بالبحث.

الخطوات هي:

١. الدخول على المواقع أو البرنامج وفي حالة الموقع يقوم المخترق بكتابة اسم الموقع على محرك البحث أو نسخ الرابط على المتصفح ثم فتح صفحة الموقع وفي حالة البرنامج يتم تنزيل أو تركيب البرنامج أولا ثم فتح صفحة البرنامج

٢. كتابة اسم المنظمة على نافذة البحث المختارة في صفحة الموقع أو البرنامج وضغط زر البحث.

٣. يقوم الموقع أو البرنامج بالبحث وإحضار البيانات والمعلومات المتوفرة في الإنترنت عن المنظمة الهدف على شكل تقرير.

٤. يقوم المخترق بمراجعة تقرير المعلومات وتحليله ودراسته واستخلاص المعلومات المفيدة منه مثل عناوين **IP** وأرقام الموظفين وأرقام الهواتف ونظام التشغيل وحسابات المستخدمين وخادم أسماء النطاق.

٥. يقوم المخترق بهذه الخطوات في عدة برامج ومواقع وينتقل بين الأدوات والمواقع المختلفة بحثا عن أكبر قدر من المعلومات.

٦. يقوم المخترق بحفظ هذه المعلومات إما الكترونيًا في مجلد أو ملف أو كتابتها وتسجيلها على الأوراق.

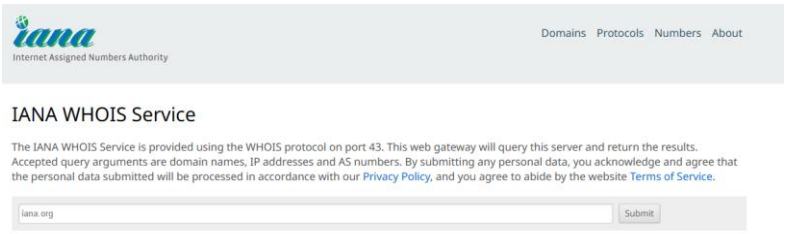
- تطبيق عملي

Footprinting Tools:

- " الموقع الأول "

١. نقوم بالدخول على الموقع: https://www.iana.org/whois

تلك الأداة هي عبارة Website يقدم معلومات حول Domain Name معين تتم هذه الخدمة من خلال مؤسسة الـ IANA حيث يتم استخدام بروتوكول WHOIS على Port 43، يقدم معلومات مثل (Email ID، Domain Owner، Phone Numbers) وغيرها كما هو مبين في الصورة التالية:



شكل (٢٢) واجهة موقع

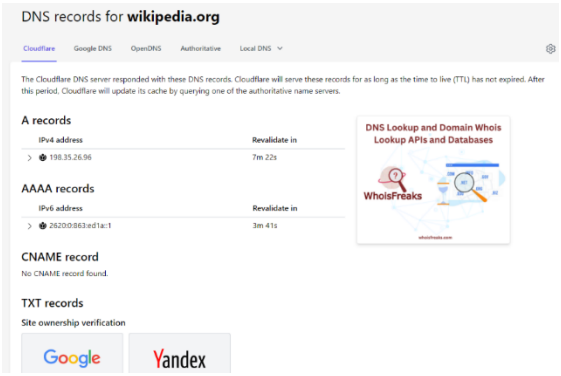
```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.publicinterestregistry.org

domain:       ORG

organisation: Public Interest Registry (PIR)
address:      11911 Freedom Drive,
address:      10th Floor, Suite 1000
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Director of Operations, Compliance and Customer Support
organisation: Public Interest Registry (PIR)
address:      11911 Freedom Drive,
address:      10th Floor, Suite 1000
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 889 5778
fax-no:       +1 703 889 5779
e-mail:       ops@pir.org

contact:      technical
name:         Senior Director, DNS Infrastructure Group
organisation: Donuts Inc.
address:      10500 NE 8th Street, Suite 750
address:      Bellevue WA 98004
```

شكل (٢٣) المعلومات المخرجة من الموقع

- "الموقع الثاني "

١. نقوم بالدخول على الموقع: https://www.nslookup.io/

هي عبارة عن موقع إلكتروني يعرض لك تسجيلات الـ DNS أو DNS Records الخاصة بـ Domain معين ، على سبيل المثال نقوم بالدخول على موقع ويكيبيديا.



شكل (٢٤) DNS

- **محركات البحث**

هو برنامج حاسب مصمم للمساعدة في العثور على مستندات مخزنة في شبكة الإنترنت، 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 الأنترنت والعديد من محركات البحث تسمح بالحصول على المعلومات عن المنظمة الهدف مثل تفاصيل الموظفين وصفحات تسجيل الدخول وباستخدام هذه المعلومات يمكن للمخترق بناء استراتيجية الهجوم لاختراق شبكة المنظمة المستهدفة **أمثلة على محركات البحث:**

- www.google,com , www.bing.com , www.yahoo.com

حيث يمكن كتابة اسم المنظمة الهدف والحصول على المعلومات.

- http://www.zabasearch.com

zabasearch هو محرك بحث عن الأفراد يوفر معلومات مثل العنوان ورقم الهاتف و الموقع الحالي في الولايات المتحدة ويسمح للبحث عن الأفراد بأسمائهم.

- http://www.wink.com

wink peaple search هو محرك بحث عن الأفراد و هي توفر معلومات عن الأفراد بالاسم و الموقع.

- http://www.peoplelookup.com

peoplelookup هو محرك بحث عن الأفراد و مواقعهم ويستخدم قاعدة بيانات من السجلات العامة.

- **المواقع الإلكترونية**

يوجد عدد من المواقع التي تتواجد في الإنترنت، الموقع الأهم للبحث هو موقع المنظمة الهدف وتعتبر صفحة المنظمة على الإنترنت مستودع لكثير من المعلومات المهمة عنها والمفيدة لعملية الاختراق ويوجد البحث في موقع المنظمة ثم البحث في بعض المواقع الأكثر شهرة الخاصة بجمع المعلومات.

١. البحث في موقع المنظمة

تتضمن كثير من المعلومات عن بنية نظام الحاسب المتبع فيها **ومن أهم المعلومات التي يحصل عليها المخترق من خلال موقع المنظمة على الإنترنت:**

١. البرمجيات المستخدمة وإصدارتها.
٢. نظم التشغيل المستخدمة.
٣. معلومات الاتصال مثل أسماء وأرقام الهواتف وعناوين البريد الإلكتروني وموقع المشرف.
٤. خوادم الويب المستخدمة وإصداراتها ومنصة السكريبت.
٥. الموقع الجغرافي للمنظمة الهدف.
٦. سياسة الأمن أو الخصوصية التي تشير إلى أنواع الآليات الموضوعة.
٧. الارتباطات إلى خوادم أخرى والكينونات والمنظمات المرتبطة.
٨. شيفرة المصدر HTML وأكواد الإنشاء والتي من خلالها يحصل على كثير من المعلومات مثل العناوين الداخلية والروابط وبنية نظام الملفات والمخلدات ويقوم المخترق بالعمل على نسخ الموقع الإلكتروني للمنظمة الهدف إلى جهازه لكي يتمكن من دراسة الموقع باستخدام أداة HTTRACK التي تقوم بنسخ الموقع الإلكتروني كاملا وتحميله إلى مجلد محلي في جهاز المخترق بكافة صفحاته وملفاته وتقوم هذه الأداة ببناء كافة المجلدات وصفحات HTML و الصور والملفات الخاصة بالموقع في المجلد المحلي الخاص بالمخترق ليقوم بتحليل مكونات الموقع والحصول على أكبر قدر من المعلومات .

٢. البحث في موقع Netcraft

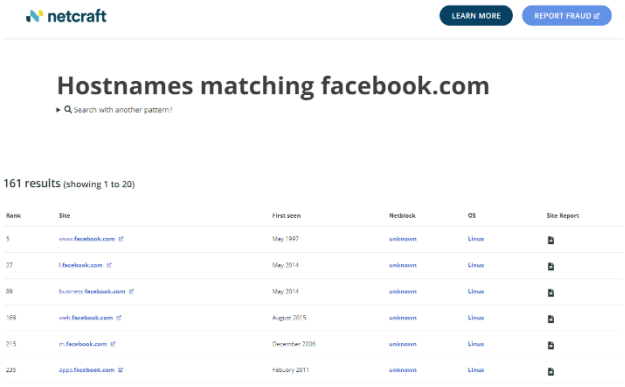
هو أحد مواقع البحث عن المعلومات حول المنظمات ويقدم هذا الموقع كثيرا من المعلومات ومن أهمها تحديد نظام التشغيل لخادم الويب الخاص بالمنظمة، لاستخدام هذا الموقع يتم القيام يتم فتح هذا الموقع وكتابة اسم المنظمة الهدف في الحقل what is والضغط على زر البحث ويظهر تقرير بالمعلومات عن المنظمة ومن أهمها نوع نظام تشغيل الويب وعناوين IP وتحديد خوادم أسماء النطاقات DNS.

٣. البحث عن الأفراد

مثل استخدام مواقع السجل العام للعثور على معلومات حول عناوين البريد الإلكتروني للأفراد وأرقام الهواتف وعناوين المنزل مثل **مواقع:** http://www.spokeo.com و http://pipl.com

- **مثال:** الدخول على موقع https://www.netcraft.com/tools/

ثم الانتقال الى DNS Search



شكل (٢٥) واجهة netcraft

- ZoomInfo:هو دليل استخدام رجل الأعمال التي يمكن أن يجد الاتصالات التجارية والسير الذاتية.

http://www.zoominfo.com

- Any who هو موقع يساعد في العثور على معلومات عن الأفراد والمؤسسات الخاصة بهم ومواقعهم على الإنترنت و مع مساعدة رقم الهاتف يتم عرض كل المعلومات.

http://www.anywho.com

- كما يمكن البحث عن الأفراد في مواقع التواصل الاجتماعي مثل https://www ، linkedin.com .
- facebook وهو يسمح بالبحث عن الأفراد والأصدقاء والمعلومات والصور والفيديوهات

https://www.facebook.com

- **جوجل**

- مُختبر الاختراق يمكن أن يدخل مصطلحات بحث خاصة للحصول على المعلومات التي يرغب بها ، كما يمكنه أن يكشف العلامات التجارية لجدران الحماية وبرامج مكافحة الفيروسات المستخدمة في المنظمات الهدف وفي بعض الأحيان يوفر مخططات الشبكة التي يمكن بواسطتها توجيه الهجوم ، كما يمكن حصول معلومات عن الموقع الجغرافي من موقع مثل http://www.google.com/earth و https://maps.google.com حيث يمكن استخدام هذه المعلومات من قبل المهاجمين للوصول الغير مصرح به إلى المباني والشبكات السلكية، وغير لاسلكية، والنظم، وغيرها.

- **مثال**

١. earth.google.com هي أداة تسمح للمهاجمين بإيجاد المكان و التكبير لاكتشافه والوصول إلى صور 3D بتفاصيل عالية الجودة.

٢. maps.google.com توفر خرائطها عرض الشوارع وصور المباني والمناطق المحيطة بها ويستخدمها المهاجمون للعثور على أو تحديد مداخل المباني والكاميرات الأمنية والبوابات وقياس المسافات بين الأهداف المختلفة.

كما توفر google finance الكثير من المعلومات المفيدة مثل القيمة السوقية لأسهم المنظمات ونبذة عن المنظمة وبعض التفاصيل الأخرى عن المنافسين ويمكن المهاجمين الاستفادة من المعلومات للهجوم على المنظمة.

- **Google alerts**

https://www.google.com/alerts

تنبيهات جوجل هي محتوى خدمة المراقبة تقوم بطريقة تلقائية بإعلام المستخدمين عن موضوع معين حسب اختيار المستخدم ويتم تخزينها بواسطة خدمة تنبيهات جوجل ومن أجل الحصول على هذه التنبيهات لابد من تسجيل البريد الإلكتروني أو رقم الهاتف فيستغلها المهاجم من خلال جمع هذه المعلومات، نتائج البحث تخزن في google cache مما يعرضه دائما للهجوم وهو يعرض من غير قصد معلومات مهمة عن موقع ما نتيجة الإعدادات الخاطئة لمختلف خوادم الويب.

- **Google hacking**

هو فن إنشاء عمليات بحث معقدة من خلال محرك البحث جوجل للعثور على الثغرات الأمنية في ملفات الإعداد والأكواد التي تستخدمها المواقع فإذا استطاع المهاجم بناء الاستعلامات المناسبة فإنه يستطيع الحصول على بيانات قيمة عن المنظمة المستهدفة عن طريق رسائل الخطأ تحتوي على معلومات مهمة، الملفات التي تحتوي على كلمات السر، الصفحات التي تحتوي على بوابات الدخول، الصفحات التي تحتوي على بيانات الشبكة، تحذيرات ونقاط ضعف النظام.

- **Whois**

للبحث 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 الإنترنت فمؤسسة Icon تطلب من كل منظمة أن تقوم بتسجيل الاسم الخاص بها لتضمن أن منظمة واحدة فقط تستخدم هذا الاسم وعندما تقوم أي منظمة بتسجيل اسمها فإنها تقدم معلومات تودع في قواعد بيانات Whois ومن أهم هذه المعلومات اسم الميدان أو المجال أي اسم المنظمة على الإنترنت، عناوين IP ، اسم الشخص القائم بالتسجيل و أرقام الهواتف وعناوين البريد الإلكتروني الخاص به ، معلومات الاتصال الإداري الأخرى، أسماء الخوادم و أسماء خوادم DNS ، معلومات عن مسؤولي المنظمة و عناوينهم و أرقامهم .

وتقوم آلية البحث في Whois باستيراد هذه المعلومات وغيرها من سجلات التسجيل وإحضارها إلى من يطلبها وعرض تقرير كامل بمعلومات عن المنظمة المكتوبة في خانة البحث.

- **DNS معلومات**

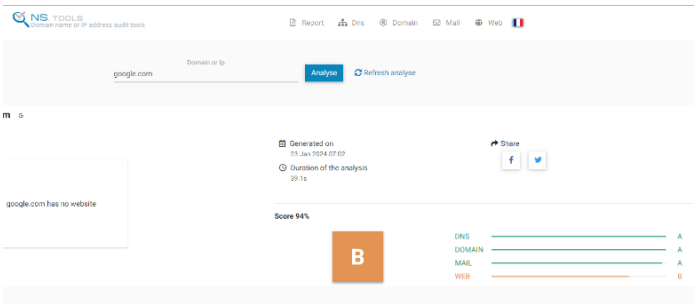
خادم DNS يحتوي على ملف نصي يسمى الملف HOST وأهمية هذا الملف أنه يحتوي على العنوان الإلكتروني لكل حاسب في المنظمة وعلى عنوان IP المقابل له وتعتبر خوادم DNS هي المكان الرسمي الذي تخزن فيه المعلومات التي تتعلق بكل الأجهزة التابعة لشبكة المنظمة وهي المصدر الرسمي للمعلومات عنها ومن أهم هذه المعلومات الاسم أو العنوان الإلكتروني لكل حاسب وهو يتكون من اسم الحاسب واسم المجال.

ويخزن معلومات أسماء المضيفات وأرقام IP الخاصة بها في سجلات تسمى موارد وتشمل سجلات الموارد في خادم DNS عدة أنواع رئيسية من أهمها سجل A HOST الذي يتضمن اسم وعنوان الخادم ورقم IP الخاص به وفي حال تلقي سجل A طلب السؤال عن اسم معين فإنه يعيد إليه رقم IP الخاص بهذا الاسم وسجل PTR والذي يعالج طلبات لمعرفة الاسم أو العنوان الإلكتروني الخاص برقم IP معين حيث إنه يرد باسم أو عنوان الحاسب أو الخادم المطابق لعنوان IP أي أنه يقوم بعملية عكسية لسجل A وهي التحويل من IP إلى الاسم.

- **البحث في DNS**

المواقع التي تقوم بعملية بحث عن DNS وتؤمن معلومات عن الـServer هي:

١. الموقع https://ns.tools/dnsstuff.com



شكل (٢٦) واجهة ns

٢. الدخول على الموقع / www.netcraft.com

يتم استخراج المعلومات من خادم DNS بطريقتين البحث في المواقع والأدوات والقيام بعمليات نقل المنطقة.

- البحث في المواقع

يوجد عدد من المواقع التي توفر إمكانية البحث في خوادم DNS مثل مواقع DNS- IP TOOL ، DNS STUFF -TOOLS ويتميز موقع IP TOOLS بوجود خيارات وخصائص للبحث تتضمن البحث في كل أنواع سجلات DNS فيمكن للمخترق عند دخوله إلى صفحة الموقع أن يضع اسم المنظمة في خانة البحث ثم يقوم بتحديد خيار أي سجل من سجلات DNS من القائمة المنسدلة مثل سجل A أو سجل MX ثم يضغط زر البحث وعندئذ يعيد الموقع كامل المعلومات عن المنظمة التي يتضمنها السجل المحدد.

- عملية نقل المنطقة

تعمل المنظمات على نشر خوادم ثانوية من DNS إلى جانب خادم DNS الرئيسي من أجل تخفيف الحمل عن الخادم الرئيسي وعن شبكة المنظمة و الذي ينشئ نتيجة تكرار طلبات التحميل لملف قاعدة بيانات DNS من قبل الحواسيب التابعة للشبكة ويحتفظ خادم DNS الثانوي بنسخة كاملة من قاعدة البيانات الموجودة في الخادم الرئيسي التابع للمنظمة ولكن هذه النسخة هي للقراءة فقط و غير قابلة للتعديل أو التحديث ولذلك فإن الخادم الثانوي يقوم بتحديث قاعدة البيانات الموجودة فيه دوريا من الخادم الرئيسي من أجل استيعاب التعديلات والإضافات الجديدة في الأسماء والأرقام.

يقوم المخترق بانتحال شخصية الخادم الثانوي ويقوم بتحميل نسخة كاملة من قاعدة بيانات الخادم الرئيسي لـ DNS على أساس أنها لتحديث قاعدة البيانات في الخادم الثانوي، ولكنها في الواقع تذهب إليه ويحصل على قاعدة بيانات الـ DNS الكاملة للمنطقة ويستخدم المخترق في هذه العملية عدداً من الأدوات مثل الأداة Dig والأداة Nslookup وبمجرد أن يقوم المخترق بتحميل نسخة الـ DNS فإنه يصبح لديه كافة أسماء وأرقام ip لأجهزة الشبكة الداخلية ومخطط كامل لبنية الشبكة.

- **استخراج معلومات DNS باستخدام http://www.dnsquerirs.com**

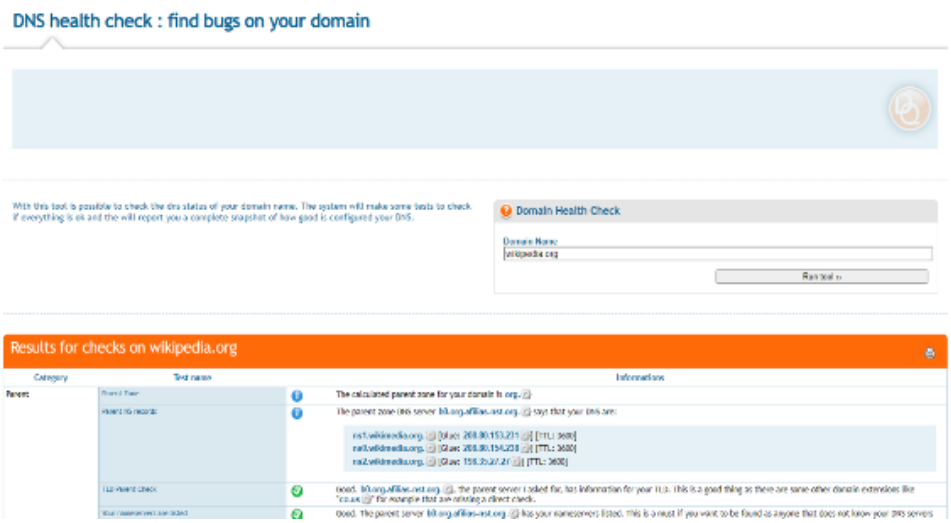
هي أداة تسمح بتنفيذ أي استعلام عن DNS باستخدام اسم المجال Domain بالذهاب للموقع يتم كتابة اسم موقع مثل microsoft.com في خانة perform DNS query ثم الضغط على Run tool.

- **مثال على استخراج معلومات DNS باستخدام :**

١. **الدخول على موقع : https://dnsquery.org/**

شكل (٢٧) واجهة dnsquary

٢. **الدخول على موقع:** https://www.dnsqueries.com/en/



شكل (٢٨) المعلومات

- **الشبكات**

طريقة العمل داخل الشبكات هي طريقة العميل –الاتصالات و خادم Client – Server وهي أساس العمل في المنظمات الكبيرة وفيها يتم تخصيص حاسب بمواصفات عالية كخادم للحواسب الأخرى المرتبطة بالشبكة ولا يقتصر دوره على الاحتفاظ بقواعد البيانات والمعلومات فقط بل يتم ربط جميع موارد الشبكة ووصلها به مثل الطابعات والاتصالات والملفات والأقراص الصلبة ويكون لكل حاسب مرتبط بالشبكة أن يحصل على أي من هذه الموارد من خلال طلبها من الحاسب الخادم Server الذي يتولى إيصاله بقواعد البيانات أو توفير خدمة تحميل ملف و غيرها .

محرك البحث shoden.io يوفر معلومات عن أجهزة الشبكة وهذا يسمح للمهاجم بالبحث عن الجهاز لمعرفة الثغرات الخاصة به.

يمكن بمساعدة الأداة Tracerouteفي معرفة عناوين IP للأجهزة الوسيطة مثل أجهزة التحويل، جدار الحماية، مما يمكن المهاجم من رسم تخطيط الشبكة من خلال تحليل نتائج الأداة Traceroute ، يوجد ثلاث شبكات تمنح الاتصال الغير مرئي لكل من العميل و الخادم **هم:** Tor , I2p ,Freenet.

❖ أدوات FootPrinting (عملي)

هي أدوات تستخدم لجمع أكبر قدر من المعلومات حول نظام مستهدف معين لاستخدام تلك المعلومات في هجمات سيبرانية **وذلك بطرق مختلفة مثل:**

- **Ping**

يستخدم البرنامج ping في معرفة ما إذا كان الحاسب الآلي متصلا بالأنترنت ويعمل وتقوم هذه الأداة بتوليد رسالة طلب اتصال وإرسالها إلى النظام الهدف وتسأل هذه الرسالة الحاسب الآلي الهدف ما إذا كان لازال متصلا وفي حالة ما إذا كان الهدف فعالا ومتصلا بالأنترنت فإنه يجيب برسالة نعم أما إذا كان الحاسب غير فعال إنه يأخذ مهلة ولا يرد وفي هذه الحالة إما أن يكون النظام الهدف في حالة إيقاف التشغيل أو في حالة عدم الاستجابة.

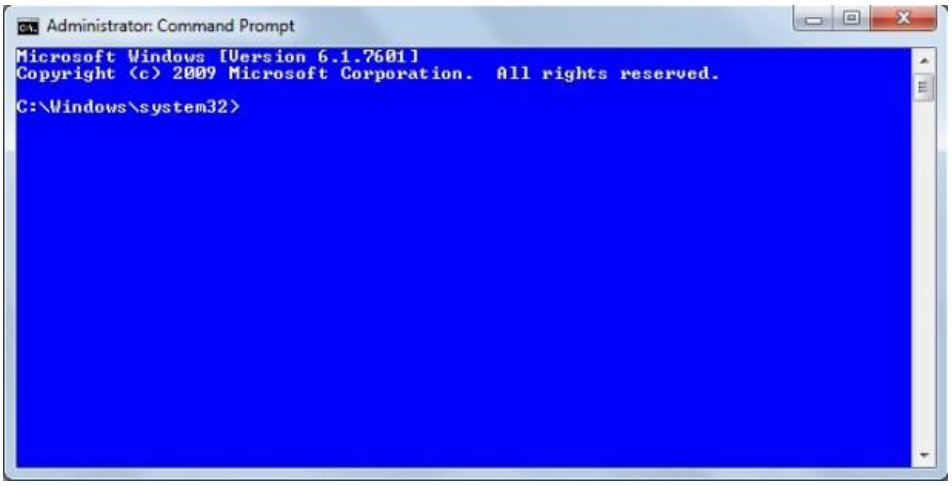
- **استخدام الأمر Ping**

- **لعمل فحص ذاتي للحاسب**

يتم استخدامها من قبل المخترقين لجمع المعلومات المهمة مثل عنوان IP ، الحد الأقصى لحجم الرزم وفي اختبار الاختراق من أجل التأكد من الوصول لجهاز حاسب في الشبكة.

- **لتطبيقه عمليا اتبع الخطوات الآتية:**

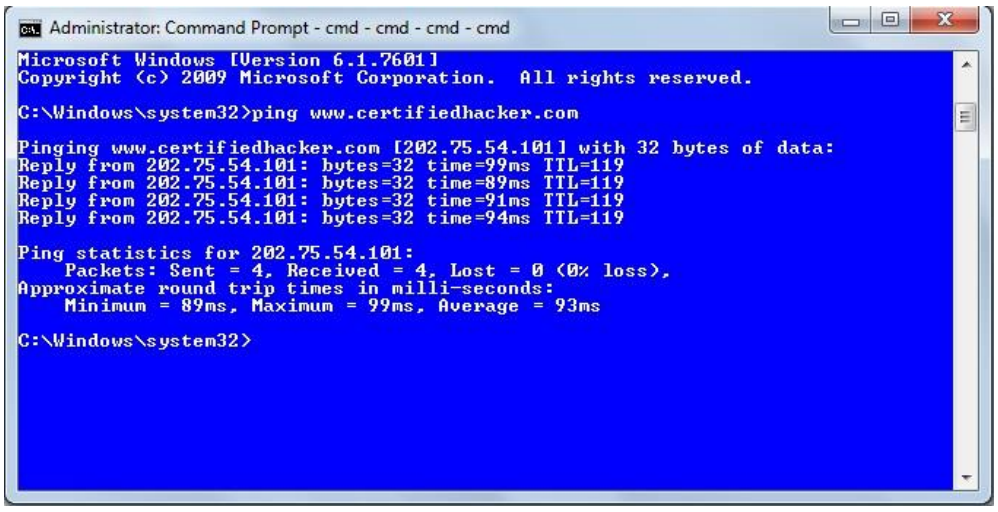
- افتح موجه الأوامر الخاص بك



شكل (٢٩) اتبع الخطوات ACM 1

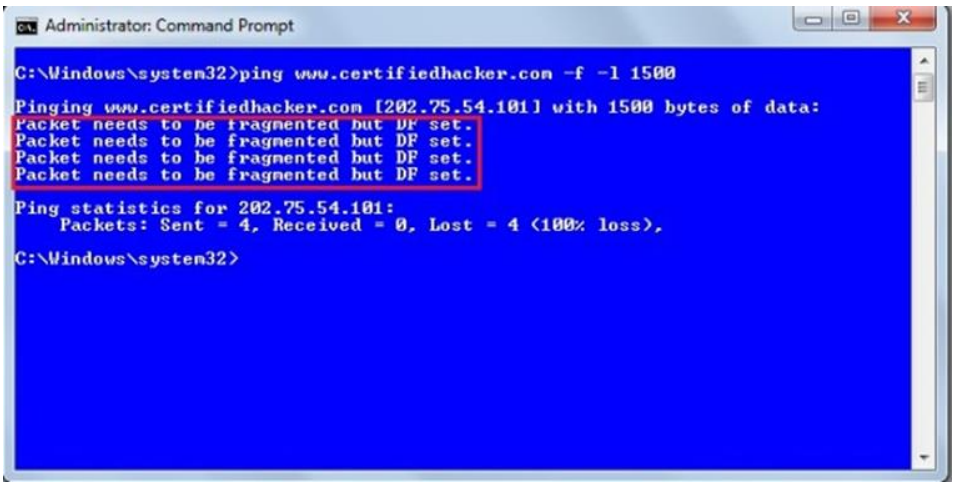
- اكتب ping متبوعًا بعنوان موقع الويب، هنا سوف نقوم بإجراء اختبار الاتصال بـ "Certifiedhacker.com

ثم اكتب "ping www.certifiedhacker.com " ثم اضغط على زر الإدخال



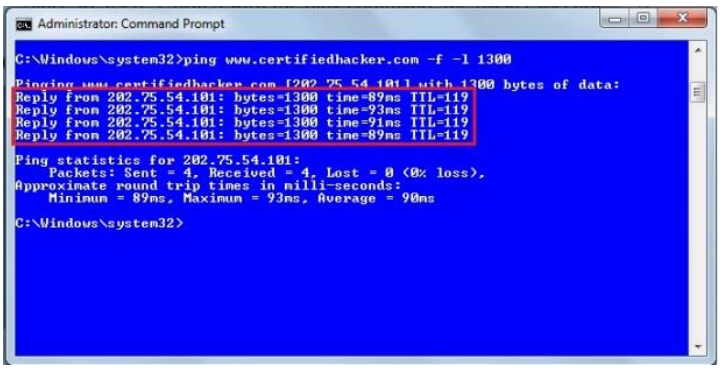
شكل (٢٩) اتبع الخطوات ACM ٢

- ستتلقى عنوان IP 202.75.54.101 لموقع www.certifiedhacker.com ، وإحصائيات Ping مثل الحزم المرسلة والمستلمة والمفقودة والوقت التقريبي لرحلة الذهاب والإياب.
- اكتشف الآن الحد الأقصى لحجم الإطار على الشبكة، في موجه الأوامر، اكتب



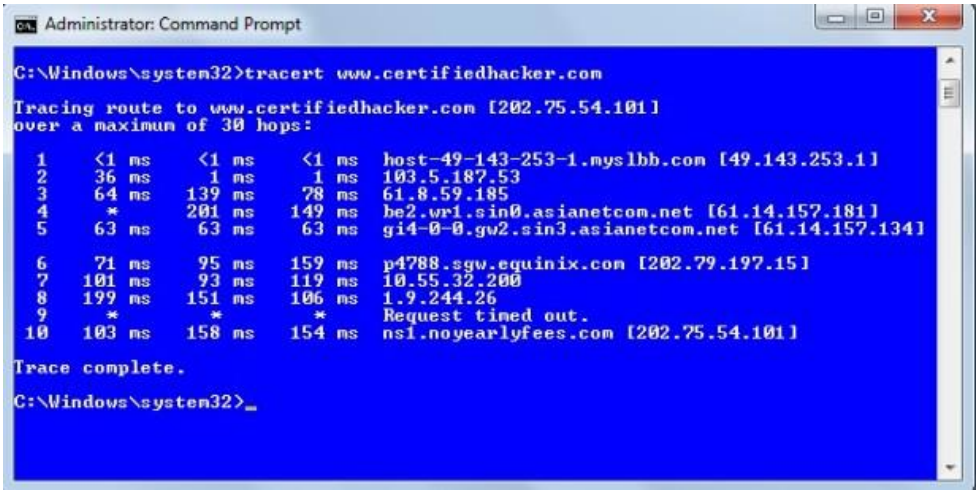
شكل (٢٩) اتبع الخطوات ACM ٣

- تتلقى الرسالة "يجب أن تكون الحزمة مجزأة ولكن تم ضبط DF" ، فهذا يعني أن الإطار كبير جدًا بحيث لا يمكن وضعه على الشبكة ويجب تجزئته ، وبما أننا استخدمنا المفتاح –f مع الأمر ping، لم يتم إرسال الحزمة، وأعاد الأمر ping هذا الخطأ.
- الآن دعونا نقوم بإجراء اختبار ping مع تقليل حجم الإطار إلى ١٣٠٠



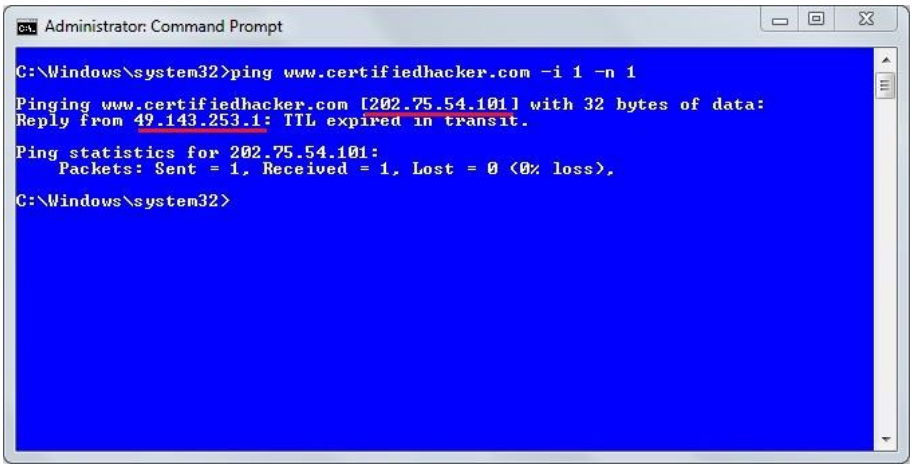
شكل (٢٩) اتبع الخطوات ACM ٤

- أثناء التنقل داخل جهاز التوجيه للايطار (TTL) ،
- الرد من جهاز التوجيه ٦١,٨,٥٩,١٨٥: انتهاء صلاحية المسار من جهاز Emulate Tracer (الإشارة للوصول ٠) نظرًا لانتهاء صلاحية الكمبيوتر الخاص بك

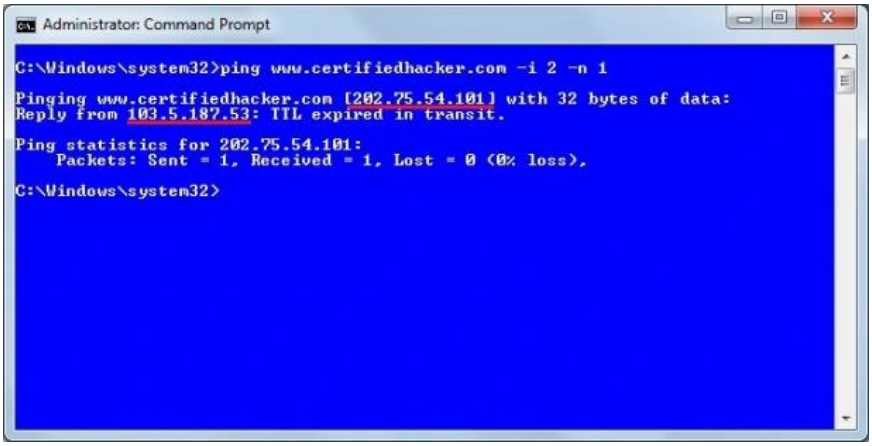


شكل (٢٩) اتبع الخطوات 5ACM

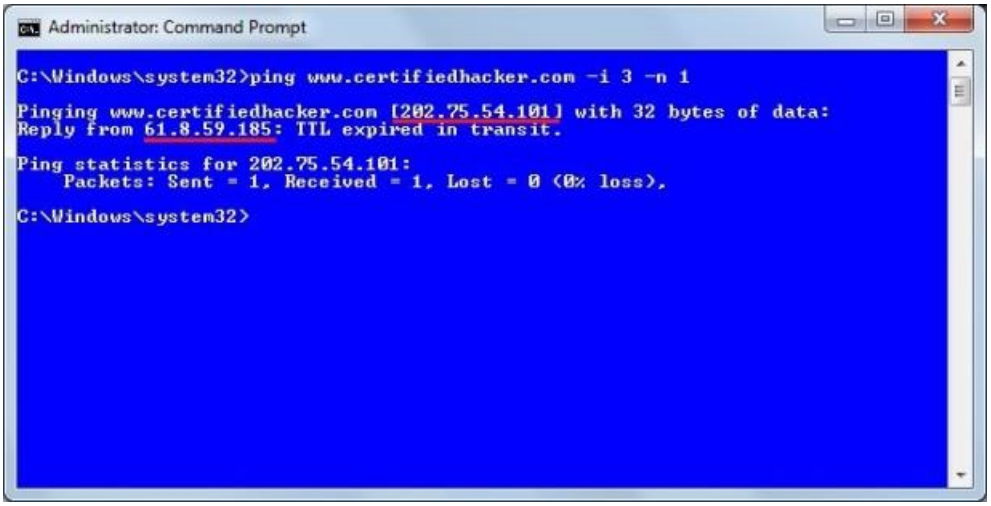
- في موجه الأوامر اكتب: استخدم n– 1 لإنتاج إرسال حزمة واحدة فقط (يجب أن تكون الاستجابة مشابهة للإخراج أدناه)



شكل (٢٩) اتبع الخطوات ٦ACM

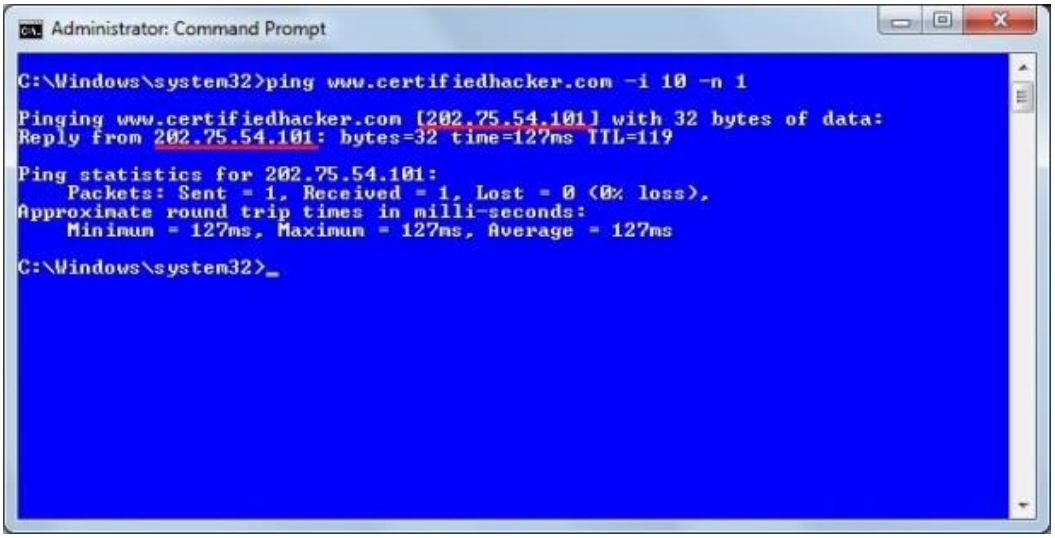


شكل (٢٩) اتبع الخطوات 7ACM



شكل (٢٩) اتبع الخطوات 8ACM

- لقد تلقينا الإجابة من نفس عنوان IP في خطوتين مختلفتين، هذا يحدد مرشح الحزم، لا تقلل بعض مرشحات الحزم من مدة البقاء (TTL) وبالتالي تكون غير مرئية.
- كرر الخطوة أعلاه حتى تصل إلى عنوان IP الخاص (في هذه الحالة ٢٠٢,٧٥,٥٤,١٠١)



شكل (٢٩) اتبع الخطوات 9 ACM

- **المعلومات التي تم جمعها:**
  - عنوان IP : 202.75.54.101
  - إحصائيات بينغ:
  - الحزمة المرسلة – ٤
  - تم استلام الحزمة – ٤
  - فقدان الحزمة – ٠
  - الوقت التقريبي لرحلة الذهاب والإياب – ٩٣ مللي ثانية
  - الحد الأقصى لحجم الإطار: ١٤٥٢ بايت
  - استجابة 10 : TTL قفزات

```
administrator@GFG19566-LAPTOP:~/practice$ ping www.google.com
PING www.google.com (142.250.194.100) 56(84) bytes of data.
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=1 ttl=116 time=1.60 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=2 ttl=116 time=1.15 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=3 ttl=116 time=1.17 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=4 ttl=116 time=1.14 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.136/1.264/1.599/0.193 ms
```

شكل (٣٠) تطبيق في كالي لينكس ping I

- **Dmitry**

أداة لديها القدرة على جمع أكبر قدر من المعلومات عن الهدف من هذه المعلومات النطاقات الفرعية subdomain، عناوين البريد الإلكتروني كما يمكن استخدام هذه الأداة لإجراء فحص tcp ويمكن استخدامها مع netcraft للحصول على المعلومات المستهدفة مثل نظام التشغيل وتفاصيل مضيف الويب وتفاصيل خدمة الاستضافة.

Application /Kali Linux /Information gathering /Live host Identification /dimitry

- **سجلات DNS**

DNS Records أو سجلات DNS هي عبارة عن مدخلات فردية تقدم تعليمات خاصة بالتعامل مع المعلومات التي يتم تداولها عبر الموقع ، مخصصة للتعامل مع معلومات محددة وغير قياسية.

- **Nslookup**

هو الأداة التي يمكن استخدامها للاستعلام من خوادم DNS والحصول على سجلات حول مختلف المضيفين وهو يعمل بطريقة مماثلة جدا بين مختلف أنظمة التشغيل ويستخدم من قبل المهاجمين للحصول على عنوان IP لمجال (Domain) معين.

```
#nslookup
>
```

- **كيفية جمع المعلومات عن طريق DNS**

لدينا مجموعة من الأدوات:

١. **nslookup**

وهي أداة موجودة في Windows وفي Linux ، عند التعامل مع nslookup لدينا طريقتان إما Interactive أو Noninteractive .

- **Interactive**

يقصد بها أن أكتب nslookup وأضغط Enter فأدخل بداخل أمر nslookup وبالتالي أبدأ بإعطائه بعض الأوامر لأقوم باستعلام وجمع معلومات و troubleshooting لـ DNS Server لو كتبت Microsoft.com : سيظهر لي بيانات، بشكل افتراضي عندما أكتب nslookup واسم الدومين الذي أريده سيرجع لي A records ، حيث A records يعيد لي عناوين IP المرتبطة مع الدومين الذي أريده.

سيظهر غالباً نوعان من الأجوبة: Authoritative و Nonauthoritative

- **Authoritative**

فلو فرضنا أن Microsoft.com بشكل منطقي لديها DNS Server رئيسي تضع داخله جميع المعلومات والتسجيلات الخاصة بالنطاقات لديها، سواء mail server أو web server أو dns server وغيرها داخل DNS.

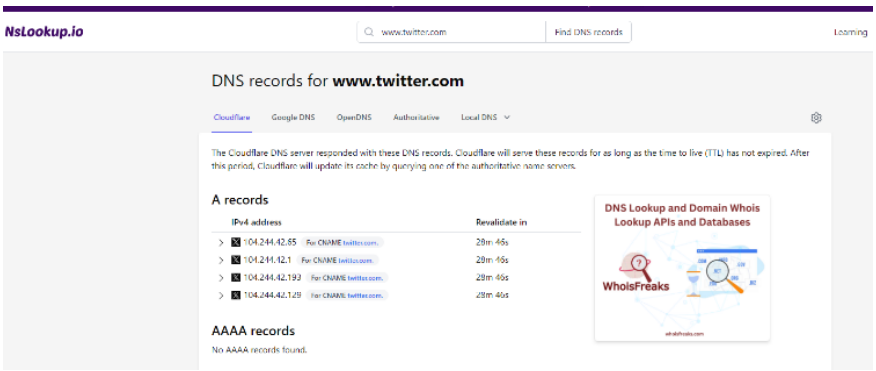
بما أن Microsoft لديها Server ومخزن عليه بيانات التسجيلات بشتى أنواعها فإن جاءت نتائج nslookup أو عملية DNS Footprinting من السيرفر الرئيسي فتكون Authoritative وهي عبارة عن إجابة كان من السيرفر الرئيسي الذي عليه بيانات الدومين المراد DNS Footprinting .

- **Non authoritative**

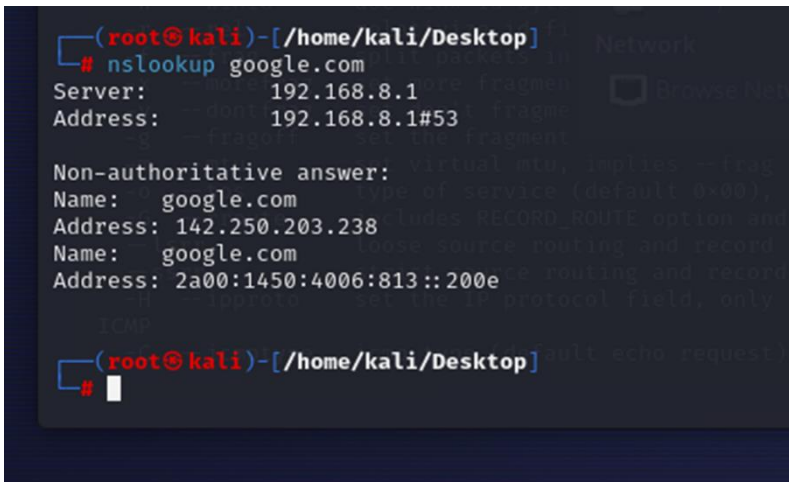
Non Authoritative هي معلومات DNS Server محفوظة في Cash.

- لو فرضنا أني داخل شبكة معينة في شركة وأريد أن أقوم بـ DNS Footprinting عن طريق nslookup أو غيرها من أدوات على Microsoft.com.
- منطقياً سأمر بـ Internet Server Provider كما قلنا في الدرس السابق، وهو يحاول أن يعمل داخل DNS Server الخاص به ويرى هل Microsoft.com لها نتائج أم لا.
- إن كان هناك نتائج سيرجع النتائج من عنده فهذه هي Non Authoritative.
- فإن استعلمت عن موقع ما ولم يجد DNS Server الذي تواصلت معه فيقوم DNS Server بالتواصل مع آخر، وبالنهاية يصل إلى Authoritative server .
- ويرد عليه ويقوم DNS Server بتخزينه لديه في الـ Cash ، مجرد تخزينه فأي شخص يطلب DNS microsodt.com سيجيبه من الـ Cash لتسريع العملية.
- وهذه النتيجة تكون Non Authoritative

https://www.nslookup.io/ يمكن الدخول على الموقع والتطبيق عمليا



شكل (٣١) DND , nslookup 1



شكل (٣٢) nslookup in kali

- **Noninteractive**

```
C:\>nslookup
Default Server:  terminator.movie.edu
Address:  192.249.249.3

> slate.mines.colorado.edu.
Server:  terminator.movie.edu
Address:  192.249.249.3

Non-authoritative answer:
Name:    slate.mines.colorado.edu
Address:  138.67.1.38
```

تشير هذه العبارة إلى أن خادم الأسماء غير معتمد للبيانات الموجودة في الإجابة (تذكر أن خادم الأسماء يكون مخوّلاً للبيانات عندما يكون خادمًا أساسيًا أو ثانويًا للمنطقة التي تحتوي على البيانات) **ستشاهد**

استجابة غير مخوّلة لأحد السببين:

الأول هو أن خادم الأسماء الذي استفسرت عنه لا يحتوي على البيانات التي كنت تبحث عنها وكان عليك الاستعلام عن خادم أسماء بعيد للحصول عليها، يعتبر خادم الاسم البعيد موثوقًا للبيانات (وهذا هو سبب الاستعلام عنها!) ويعيدها باستخدام مجموعة البت "الإجابة الموثوقة" في رأس رسالة DNS, يقوم خادم Microsoft DNS الذي استفسرت عنه بوضع هذه البيانات في ذاكرة التخزين المؤقت الخاصة به ويعيدها إليك والتي تم وضع علامة "غير موثوقة" عليها، إذا طلبت نفس البيانات مرة أخرى، فهذه المرة يمكن لخادم الأسماء الإجابة من ذاكرة التخزين المؤقت الخاصة به وسيضع علامة على البيانات كغير موثوقة؛ وهذا هو السبب الثاني الذي يجعلك ترى إجابة غير موثوقة.

لا يتم الإعلان عن الإجابات الموثوقة بواسطة nslookup : غياب الرسالة غير الموثوقة يعني أن الإجابة موثوقة.

لاحظ أننا أنهينا اسم النطاق بنقطة زائدة.

- **خادم Non-authoritative DNS Server**

لا تقوم خوادم DNS غير الموثوقة، والمعروفة أيضًا بخوادم DNS التخزين المؤقت، بتخزين سجلات DNS الرسمية للنطاقات، وبدلاً من ذلك يعملون كوسطاء بين العملاء وخوادم DNS الموثوقة، حيث يقومون بإعادة توجيه استعلامات DNS وتخزين الاستجابات مؤقتًا.

يقوم معظم مزودي خدمة الإنترنت (ISP) والمؤسسات بتشغيل خوادم DNS غير الرسمية الخاصة بهم للتعامل مع طلبات DNS من مستخدميهم، تقوم هذه الخوادم بتخزين سجلات DNS التي تتلقاها من الخوادم الموثوقة في ذاكرة تخزين مؤقت لفترة محددة (يتم تحديدها حسب مدة البقاء أو قيمة TTL لسجل DNS) لتحسين الأداء وتقليل زمن الوصول للاستعلامات اللاحقة.

على سبيل المثال: قمنا بالاستعلام عن سجلات DNS للنطاق tecadmin.net واستجاب خادم DNS المفتوح ٨,٨,٨,٨ من Google لهذا الاستعلام الذي لا يحتوي على ملف المنطقة الأصلي، تُعرف هذه الإجابة بأنها إجابة غير موثوقة.

```
$ nslookup tecadmin.net

الخادم: 8.8.8.8
العنوان: 53#8.8.8.8

إجابة غير موثوقة:
الاسم: tecadmin.net
العنوان: 104.27.189.217
الاسم: tecadmin.net
العنوان: 104.27.188.217
```

- **أدوات أخرى**

- **Netcraft**

يتعامل مع خادم الويب ومواقع استضافة تحليل حصة السوق والكشف عن نظام التشغيل.

- **Line Extractor**

هي أداة استخراج الروابط Links تسمح بالاختيار بين عناوين URL الداخلية والخارجية وتُنتج قائمة من العناوين المرتبطة في صورة URL أو قائمة HTML ويمكن استخدام في المواقع المنافسة.

- **Owasp**

هي أداة تعرض العناوين التي يمكن الحصول منها على معلومات مثل حالة الاتصال ونوع الاتصال ـ النطاقات المقبولة، خوادم الويب المستخدمة وإصداراتها.

- **eMailTrackerPro**

هي من أدوات الحصول على معلومات من خلال البريد الإلكتروني وهي أداة تسمح بتعقب البريد الإلكتروني واستخراج المعلومات منه مثل هوية المرسل وخادم البريد وعنوان IP المرسل وغيرها من المعلومات ويمكن استخدام هذه المعلومات لمهاجمة المنظمة الهدف كما يمكنه تحديد المدينة التي نشأ منها البريد الإلكتروني.

- **HTTrack Web Site Copier**

http://www.httrack.com

هي أداة لنسخ موقع ويب من على شبكة الأنترنت وهذه الأداة تسهل على المخترق عمله لأنها تعطيه الفرصة الكاملة لدراسة المحتوى الكامل لهذا الموقع.

- ملاحظة

مراءة المواقع Website Mirror

هي عملية تقوم بعمل نسخة طبق الأصل من الموقع الأصلي وتسمح بتحميل موقع ما على شبكة الإنترنت إلى مجلد محلي على أي جهاز حاسب و بناء كافة المجلدات وصفحات HTML ، الصور ، ملف ات الفيديو وغيرها من الملفات , **وهي مفيدة للأسباب التالية:**

- تصفح المواقع في الوضع offline
- إنشاء موقع احتياطي نسخة أصلية من موقع أصلي
- عمل استنساخ لموقع ما
- اختبار موقع ما أثناء تصميمه وتطويره
- توزيع الموقع على عدة خوادم

- **Hoovers**

http://www.hoovers.com

هي شركة للبحوث التجارية توفر تفاصيل كاملة عن المؤسسات والصناعات في جميع أنحاء العالم من خلال الإنترنت.

- **Fierce**

تستخدم لفحص Domain ويستخدم في العثور على عناوين IP في كالي لينكس

Applications /information gathering /DNS Analysis /fierce

- **اختبار الاختراق مرحلة الاستطلاع**

يتم إجراء اختبار الاختراق لتعزيز الأمن فيجب أثناء الاختبار جمع المعلومات المهمة مثل تفاصيل الخادم ونظام التشغيل من خلال عملية الاستطلاع وإجراء عملية تحليل النظام وشبكة الدفاعات عن طريق كسر أمنها مع صلاحيات كافية دون التسبب في أي ضرر والعثور على الثغرات ونقاط الضعف في الشبكات والنظام وفي تقرير اختبار الاختراق يتم توثيق كل تفاصيل هذه المرحلة وأساليب الاختراق المُستخدمة ونتائجها وتحديد تفاصيل سبب الضعف بجانب ذكر التدابير المُضادة لها .

يُستخدم لتحديد طبيعة معلومات المؤسسة المُتاحة على شبكة الإنترنت مثل هندسة الشبكات وأنظمة التشغيل والتطبيقات والمستخدمين ويحاول اختبار الاختراق في جمع المعلومات كأنه مهاجم قد يكون الهدف مجموعة محددة أو شبكة.

- **الخطوات المُتبعة في خطوات الاختراق**

١. يجب أن يتم تنفيذ الاختبار مع إذن بذلك وهو الحصول على الترخيص اللازم من الأشخاص المسؤولين.

٢. تحديد نطاق التقييم وهو شرط مُسبق لاختبار الاختراق وفيه يتم تحديد مجموعة من الأنظمة في الشبكة وذلك لفحصها والموارد التي يمكن استخدامها في الاختبار وبمجرد تحديدها يجب أن تُخطط لجمع المعلومات المهمة باستخدام تقنيات Footprinting

٣. إجراء Footprinting عن طريق محركات البحث مثل HTTrack web site copier.

٤. إجراء عملية الاستطلاع باستخدام البريد الإلكتروني باستخدام أداة free email tracker لجمع معلومات حول الموقع الفعلي للهدف لأداء الهندسة الاجتماعية والتي تساعد بدورها في رسم خرائط الشبكة للمنظمة الهدف.

٥. جمع المعلومات عن المنافسين باستخدام أدوات مثل SEC Info لاستخراج المعلومات حول المنافس.

٦. إجراء عملية الاستطلاع باستخدام قواعد whois للحصول على المعلومات مثل IP والاسم المسجل وتفاصيل الاتصال بهم.

٧. إجراء عملية الاستطلاع عن قواعد DNS لتديد الأجهزة في الشبكة وأداء هجمات الهندسة الاجتماعية.

٨. إجراء عمليات الاستطلاع عن الشبكة لإنشاء خريطة للشبكة الهدف.

٩. تنفيذ تقنيات الهندسة الاجتماعية مثل EAVESDROPPING , SHOULDER SURFING التي تساعد على جمع المعلومات الأكثر أهمية عن المنظمة الهدف وجمع تفاصيل عن الموظفين في المنظمة الهدف وأرقام الهواتف وعنوان البريد الإلكتروني .

١٠. توثيق جميع النتائج التي تم الحصول عليها في هذه المرحلة لتحليل الوضع الأمني والإشارة إلى التدابير المضادة لهذه الثغرات.

❖ التدابير المضادة والحماية من عمليات الاستطلاع (عملي)

إعداد جهاز المحول Router للحد من رد الطلبات عن الـ Footprinting .

- **للحد من عمليات الاستطلاع، يمكنك اتباع الخطوات التالية لإغلاق الراوتر:**

تعطيل WPS: يمكنك تعطيل WPS (واي فاي محمي بالضغط) على الراوتر، هذا يمنع الاستخدام غير المصرح به للشبكة اللاسلكية.

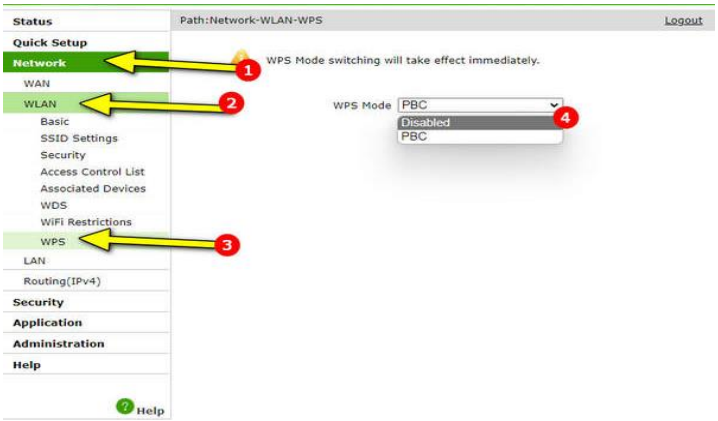
- **تطبيق عملي**

١. تقوم بالدخول على صفحة الراوتر بالضغط على الرابط التالي http://192.168.1.1/

٢. سوف يتطلب منك إدخال اسم المستخدم وكلمة السر، تقوم بإدخال admin في كلا الخانتين، ثم الضغط على زر Login .

شكل (٣٠-١) تسجيل الدخول ١

٣. من الشريط الأيسر تضغط على أعداد Network ومنها Wlan ثم الضغط على WPS ، الإن يمكنك قفل ثغرة WPS باختيار Disable ثم الضغط على زر الحفظ في الأسفل Save



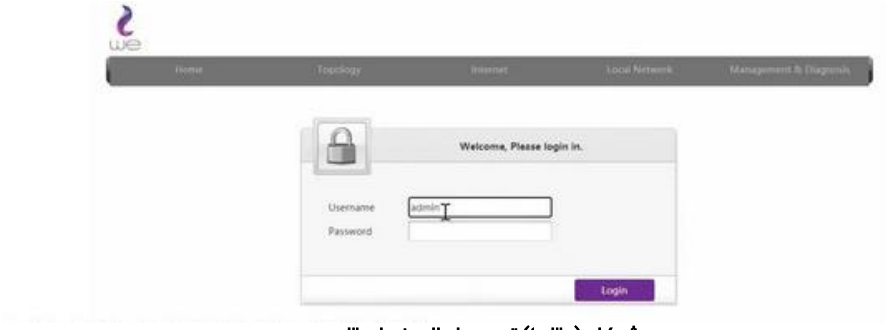
شكل (٣٠-١) تسجيل الدخول ٢

٤. بهذا سيتم إغلاق WPS في الراوتر Te Data وسوف تلاحظ إضاءة WPS على الراوتر قد انطفأ، وفيما يلي نستعرض شرح إغلاق ثغرة WPS في الراوتر الحديثة سواء WE أو غيره.

ملاحظة / يوجد طريقة أخرى للراوتر الجديد

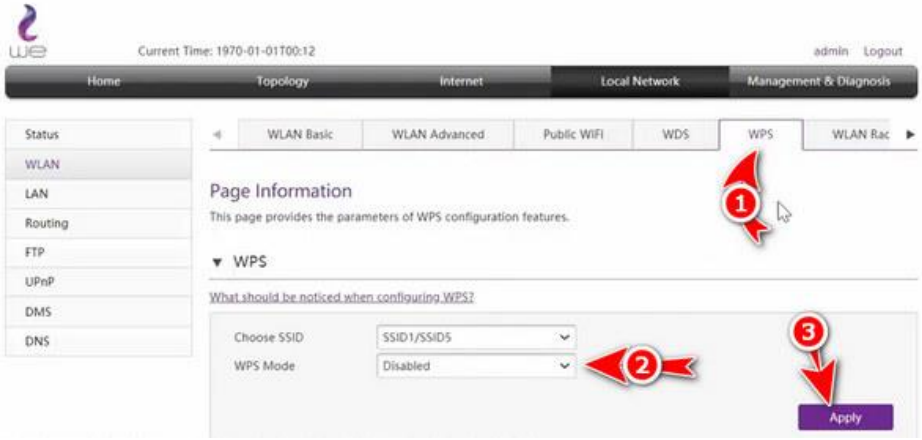
١. أولا يتوجب تسجيل الدخول لصفحة الراوتر بالضغط على الرابط : ١٩٢,١٦٨,١,١.

٢. تقوم بإدخال اسم المستخدم admin وكلمة السر الموجودة على ظهر الراوتر، ثم الضغط على زر تسجيل الدخول Login .



شكل (٣٠-١) تسجيل الدخول ٣

٣. تقوم بإدخال اسم المستخدم admin وكلمة السر الموجودة على ظهر الراوتر ، ثم الضغط على زر تسجيل الدخول Login .



شكل (٣٠-١) تسجيل الدخول ٤

٤. الإن يمكنك الغاء تفعيل WPS عبر اختيار Disabled أمام أعداد WPS Mode ثم الضغط على Apply لحفظ التغييرات .

٥. وبهذا تم إغلاق WPS في الراوتر وي الجديد.

○ تحديث كلمة المرور الافتراضية

قم بتغيير كلمة المرور الافتراضية للراوتر لزيادة الأمان.

١. اتصل براوتر الخاص بك.

٢. قم بتوصيل جهاز الكمبيوتر الخاص بك بالراوتر عبر كابل إيثرنت أو اتصال Wi-Fi.

٣. كيفية تغيير باسورد Wi-Fi وباسورد الراوتر.

٤. فتح متصفح الويب.

٥. قم بفتح متصفح الويب على جهاز الحاسوب الخاص بك (مثل Google Chrome أو Firefox أو Internet Explorer).

٦. ادخل عنوان IP للراوتر.

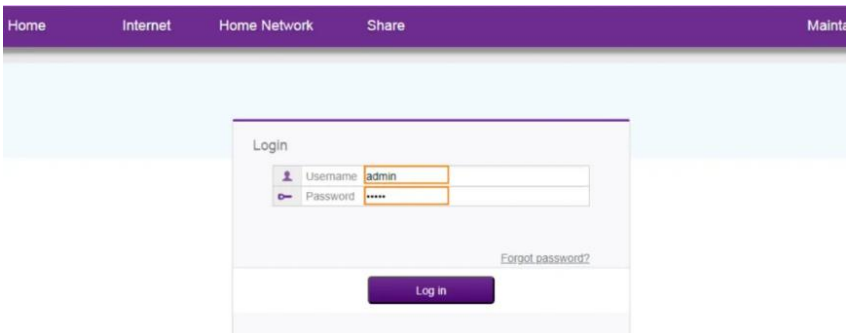
٧. قم بإدخال عنوان IP لجهاز الراوتر في شريط عنوان المتصفح، عادةً ما يكون العنوان هو ١٩٢,١٦٨,١,١ أو ١٩٢,١٦٨,٠,١.

ملاحظة/ إذا كنت غير متأكد من العنوان الصحيح، يمكنك العثور على هذه المعلومات في دليل الراوتر الخاص بك أو على مُلصق متواجد في ظهر جهاز الراوتر الخاص بك.

ملاحظة/ تخطي رسالة "Your connection is not private" (اتصالك غير آمن) وذلك عن طريق الضغط على Advanced ثم النقر بعدها على Proceed to 192.168.1.1 (unsafe)

٨. سيطلب منك بيانات تسجيل الدخول.

٩. مجرد الوصول إلى صفحة تسجيل الدخول للراوتر، ستحتاج إلى إدخال اسم المستخدم وكلمة المرور الحالية، هذه المعلومات الافتراضية موجودة في دليل الراوتر الخاص بك عادةً ما يكون اسم المستخدم "admin" وكلمة المرور "admin" أو "password"،



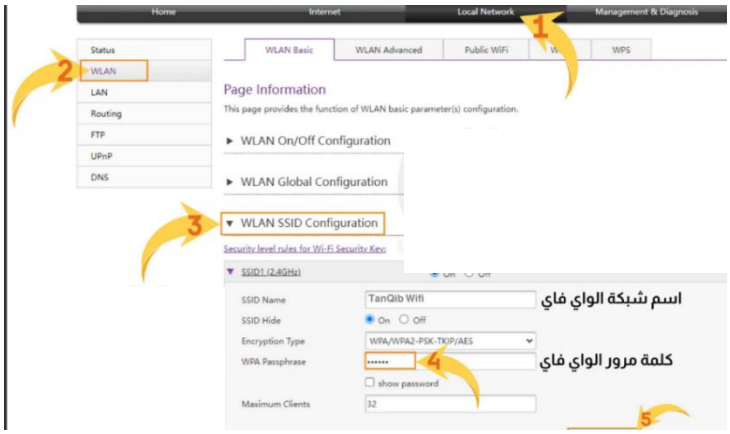
شكل (٣٠-٢) تسجيل الدخول 1

ملاحظة/ ومن الممكن أيضا أن تجد هذه المعلومات على مُلصق متواجد خلف جهاز الراوتر، أما إذا قمت بتغيير هذه المعلومات في وقت سابق

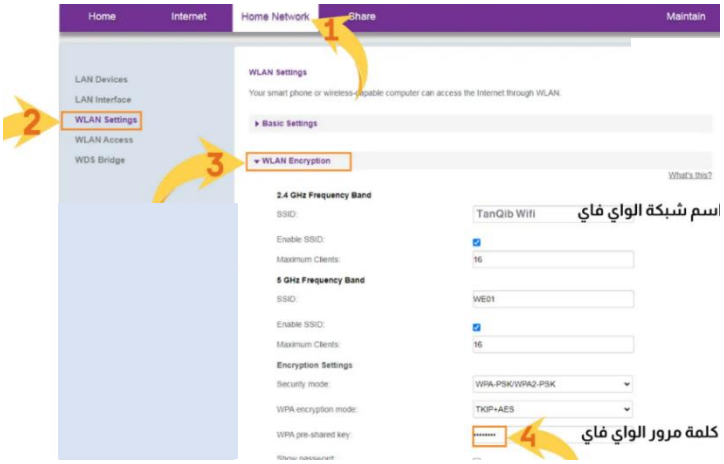
ونسيتها، فيجب عليك إعادة تعيين الراوتر إلى إعدادات المصنع الافتراضية (Factory Reset)، ولكن هذا سيؤدي إلى فقدان أي تغييرات قمت بها في الراوتر ومن المُحتمل تحتاج إلى الاتصال بخدمة العملاء.

١٠. تغيير كلمة المرور

بمجرد تسجيل الدخول بنجاح قمت بوضع صور لك لأكثر من راوتر، اختار المشابه لك في الإعدادات ابحث في قائمة الإعدادات عن قسم يسمى اذهب الى "Local Network" وبعدها نضغط على "WLAN" ثم "WLAN SSID Configuration"وعند WPA passphrase قم بوضع كلمة مرور Wi-Fi الجديدة لا تنسى الضغط على "Apply" لحفظ التغييرات.



شكل (٣٠-٢) تسجيل الدخول 2



شكل (٣٠-٢) تسجيل الدخول 3

ملاحظة/ قم بإعادة تشغيل الراوتر:

في بعض الأحيان قد تحتاج إلى إعادة تشغيل الراوتر لتفعيل الكلمة المرور الجديدة، تجد خيارًا لإعادة تشغيل الراوتر عادةً في قائمة الإعدادات، أو أيضا من الممكن أن تقوم بعمل ذلك من زر الكهرباء المتواجد في الراوتر.

- **تعطيل DNS:** يمكنك تعطيل خدمة DNS على الراوتر لمنع التلاعب بتوجيهات الشبكة.

  - opendns

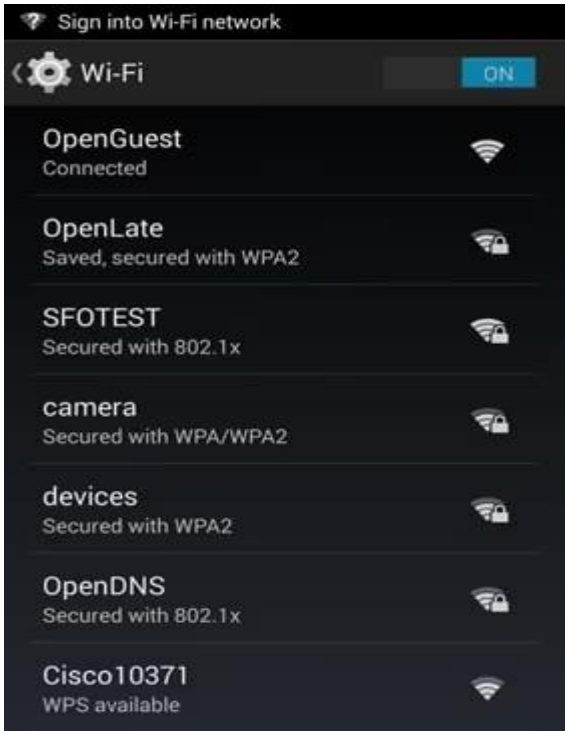
١. يتوجب عليك في البداية فتح الموقع الإلكتروني opendns.com وإنشاء حساب جديد عليه، والجدير بالذكر أن الـ DNS هو برتوكول خاص بالإنترنت يقوم بترجمة أسماء الصفحات بما يقابلها من عنوان IP الخاص بكل موقع، كما يقدم خدمة فلترة المحتوى للمستخدم.

٢. وتتميز هذه الخدمة بكونها مجانية ويطلق عليها اسم Family Shield وتستخدم بشكل شخصي أو في المنزل، ومن خلال عدة اختبارات وتجارب لها تبين أنها خدمة آمنة وموثوقة للغاية.

٣. لكي تتمكن من استخدام خدمة DNS Family Shield المجانية لحمايتك، يتوجب عليك استخدام خوادم DNS التالية على جهاز التوجيه (الراوتر) أو على كل جهاز متصل بالإنترنت.

208.67.222.123

208.67.220.123



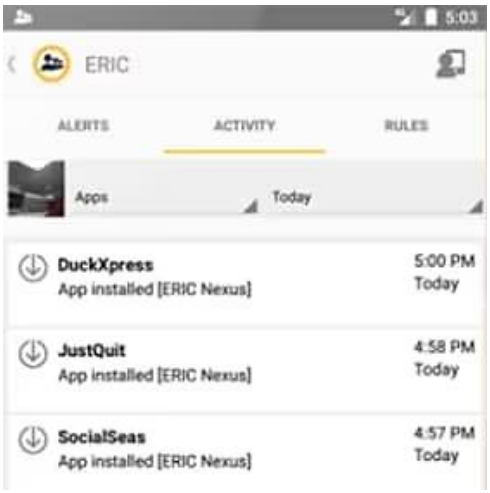
شكل (٣-٣٠) DNS

- **Norton Connect Safe**

تطبيق قواعد الوصول للشبكة اللاسلكية: يمكنك تحديد الأجهزة المسموح لها بالاتصال بالشبكة اللاسلكية ومنع الأجهزة الأخرى.

يعتبر Norton Connect Safe نظام خدمة DNS المجاني الثاني ويُنصح به لمنع الوصول إلى المحتوى الإباحي، ومن خلال عدة تجارب، تبين أن خدمة تصفية المحتوى هذه تعمل على حجب المواقع الإباحية المطلوبة، ولكنها بطيئة جدًا في التجاوب.

١. فإذا كنت ترغب في استخدام خدمات DNS نورتون لحماية عائلتك من المواقع غير الآمنة، سيتوجب عليك استخدام خوادم DNS التالية على جهاز التوجيه الخاص بك (الراوتر) أو على كل حاسب أو جهاز محمول تريد حمايته.



شكل (٣٠-٣) DNS1

- **تحديث البرامج الثابتة (Firmware):** تأكد من تحديث البرامج الثابتة للراوتر إلى أحدث إصدار لسد الثغرات الأمنية.

١. قم بزيارة موقع الدعم الخاص بشركة تصنيع الراوتر، إذا كان هناك إصدار أحدث من البرامج الثابتة متاح، يمكنك تنزيله من قسم الدعم على موقع الشركة.

٢. إذا لم يتم توفير رابط للتحميل، يمكنك البحث عن موقع الدعم عن طريق محرك البحث، على سبيل المثال، الدخول على الموقع الرسمي والبحث عن التحديث

٣. قم بتنزيل أحدث إصدار من البرامج الثابتة، قد يكون هناك ملف واحد أو عدة ملفات مختلفة للبرامج الثابتة، قم بتنزيل أحدث إصدار، سواءً بناءً على التاريخ أو الرقم.

- **إغلاق المنافذ غير الضرورية**

لإغلاق المنافذ غير الضرورية على الجهاز، **يمكنك اتباع الخطوات التالية:**

١. كانت بعض المنافذ المفتوحة في انظمة الويندوز ولا زالت نقطة عبور لأنواع عديدة من الديدان والفيروسات وحتى أحصنة طروادة ، لذلك من الضروري تعطيل بعض الخدمات غير الضرورية وغلق المنافذ القابلة للإصابة لسد الطريق أمام جميع التهديدات.

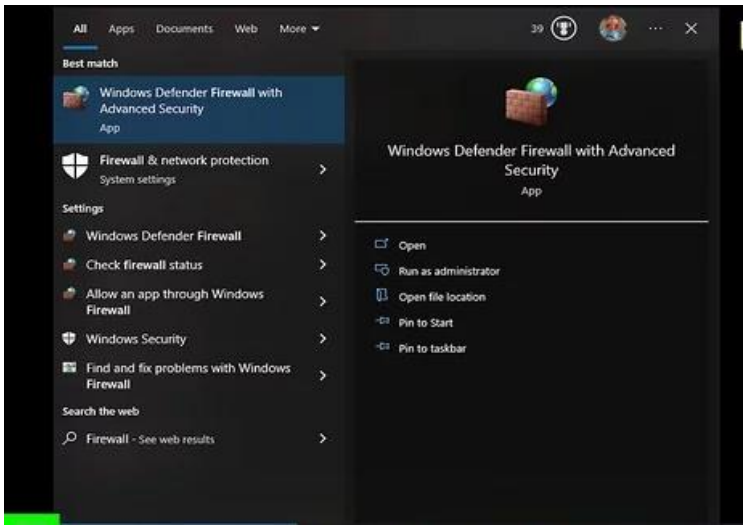
- أداة Windows Worms Doors Cleaner محمولة ولا تحتاج التثبيت، إضافة الى أنها خفيفة على الحاسوب وبمجرد تشغيل الأداة وإغلاق المنافذ وتعطيل الخدمات سيطلب من المستخدم إعادة تشغيل الحاسوب لتحدث التغييرات.
- واجهة أداة Windows Worms Doors Cleaner بسيطة جدا ولا تتطلب إعداد أي شيء، فهي تقوم بفحص السجل لاكتشاف الخدمات الممكنة والمنافذ المفتوحة القابلة للإصابة لتبقى الخطوة الأخيرة لدى المستخدم بالضغط على كلمتي Close و Disable.
- لتحميل الأداة: http://adf.ly/pJsvD أو http://adf.ly/pJt2S

شكل (٣٠-٤) Worms

- **ضبط إعدادات الجدار الناري Firewall**

الجدار الناري لجهاز الكمبيوتر مسؤول بصورة كبيرة عن حجب الاتصالات الواردة التي يمكن أن تضر جهازك، يمكنك عرض وتعديل إعدادات الجدار الناري على أي جهاز كمبيوتر، ولكن يفضل تطبيق الجدار الناري على أجهزة ويندوز حيث لا يحتاج مستخدمو نظام ماكنتوش إلى تفعيل أو استخدام الجدار الناري المضمّن عادة.

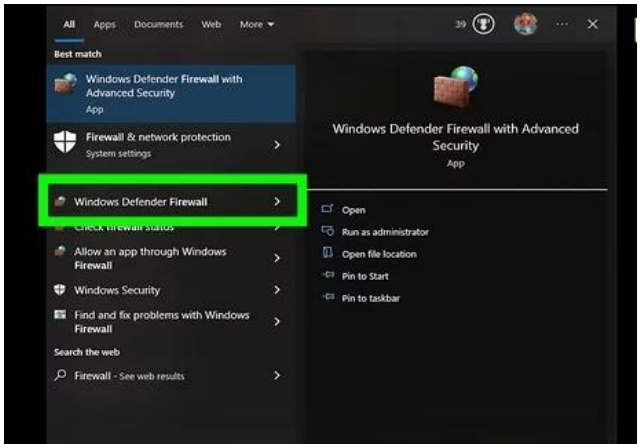
- **تفقد إعدادات الجدار الناري على نظام ويندوز**



شكل (٣٠-٥) firewall 1

١. افتح قائمة ابدأ، يوجد برنامج الجدار الناري الافتراضي في مجلد "النظام والأمان" بداخل لوحة التحكم على نظام ويندوز، ولكن يمكن الوصول إلى إعدادات الجدار الناري لنظام ويندوز بسهولة عن طريق استخدام شريط البحث في قائمة ابدأ.

٢. يمكنك أيضًا الضغط على زر ويندوز ⊞ Win لفتح قائمة ابدأ.



شكل (٣٠-٥) firewall 2

٣. انقر على خيار "الجدار الناري" يظهر هذا الخيار أعلى نافذة البحث.

شكل (٣٠-٥) firewall ٣

٤. راجع إعدادات الجدار الناري، يفترض أن ترى قسمين باسم "شبكات خاصة" و "شبكات عامة أو مضيفة" مع أيقونة درع أخضر إلى جوار كل منهما للدلالة على عمل الجدار الناري.

يؤدي النقر على أي من هذين القسمين إلى إظهار قائمة منسدلة تحتوي على تفاصيل الشبكات الخاصة أو العامة الحالية.

شكل (٣٠-٥) firewall ٤

٥. انقر على خيار "الإعدادات المتقدمة" يظهر هذا الخيار في الجهة اليسرى من القائمة الرئيسية ويؤدي النقر عليه إلى فتح قائمة الإعدادات المتقدمة للجدار الناري **التي تمكنك من تعديل الخيارات التالية:**

"قواعد الاتصالات الواردة": يسمح هذا الخيار بتحديد الاتصالات الواردة المسموح بها تلقائيًا.

"قواعد الاتصالات الصادرة": يسمح هذا الخيار بتحديد الاتصالات الصادرة المسموح تلقائيًا.

"قواعد أمان الاتصال": يسمح الخيار بتحديد قواعد رئيسية للاتصالات التي يسمح بها جهاز الحاسوب والاتصالات التي يحجبها.

"مراقبة": يقدم الخيار نظرة عامة على إرشادات المراقبة البسيطة للجدار الناري.

شكل (٥–٣٠) 5 firewall

٦. اخرج من قائمة الإعدادات المتقدمة بعد الانتهاء، لقد أنهيت بذلك تفقد إعدادات الجدار الناري على جهاز ويندوز، لاحظ إمكانية النقر على خيار "تفعيل وتعطيل الجدار الناري" من نفس قائمة الخيارات المحتوية على خيار الإعدادات المتقدمة، ويجب الحذر من تعطيل الجدار الناري عند الاتصال بشبكة عامة.

- **تقييم والحد من كمية المعلومات المتاحة قبل نشرها على شبكة الأنترنت**
  - منع محركات بحث الويب من التخزين المؤقت **Caching** لصفحات الموقع.

- **في تطبيق Chrome**

١. على هاتفك أو جهازك اللوحي المزوّد بنظام تشغيل Android، افتح تطبيق Chrome.

٢. في أعلى اليسار، انقر على "المزيد" المزيد.

٣. انقر على السجلّ ثم محو بيانات التصفح.

٤. في الأعلى، اختر نطاقًا زمنيًا، لحذف كل السجلّ، اختر كل الوقت.

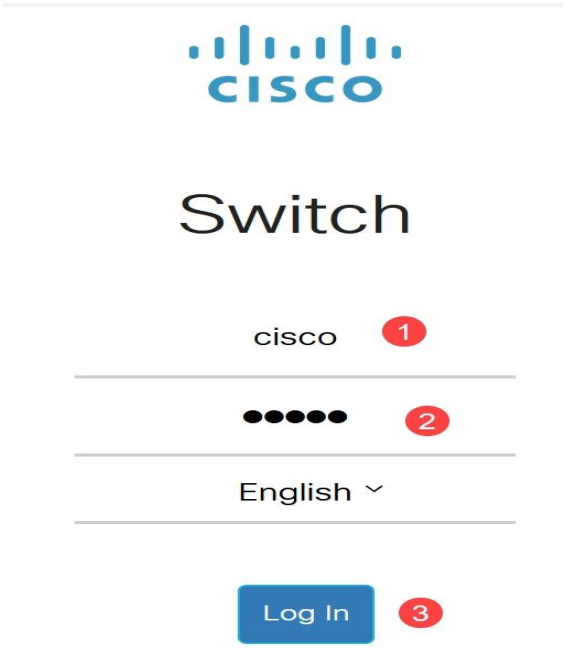
٥. بجوار "ملفات تعريف الارتباط وبيانات الموقع" و"صور وملفات ذاكرة التخزين المؤقت"، اختر المربّعين.

٦. انقر على محو البيانات.

  - تعطيل البروتوكولات غير المرغوب فيها

على سبيل المثال: تعطيل HTTP و HTTPS باستخدام واجهة مستخدم ويب

١. قم بتسجيل الدخول إلى المحول لديك من خلال إدخال اسم المستخدم وكلمة المرور وانقر فوق تسجيل الدخول.

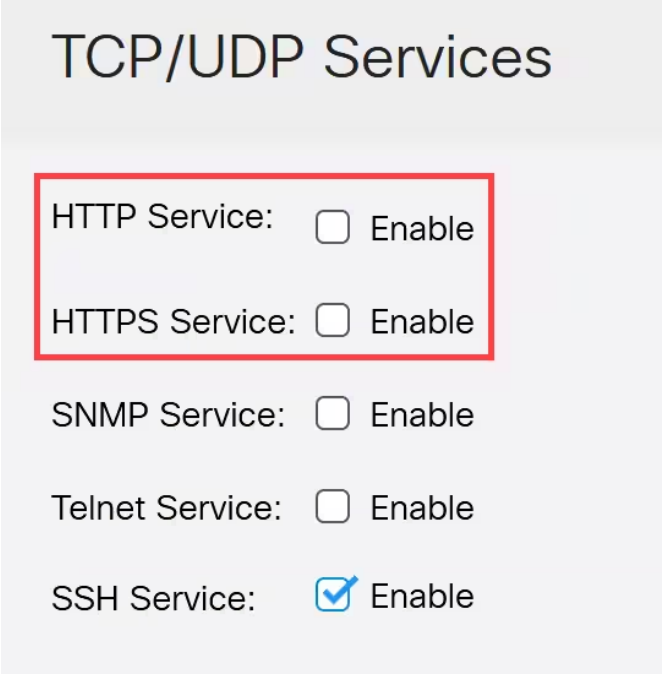


شكل (٦-٣٠) cisco 1

٢. انتقل إلى الأمان > خدمات TCP/UDP.

شكل (٣٠-٦) cisco 2

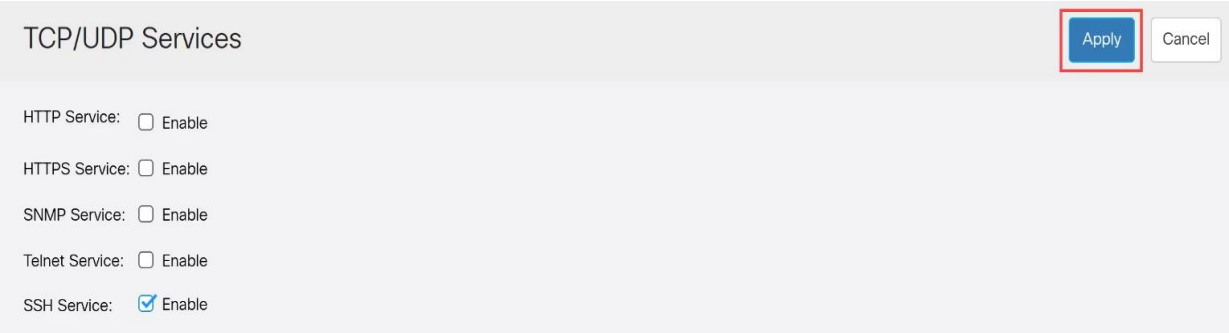
٣. قم بإلغاء تحديد الخانات الخاصة بخدمة HTTP وخدمة HTTPS.



شكل (٣٠-٦) cisco 3

ملاحظة / إذا كانت هناك حاجة إلى الوصول إلى سطر الأوامر عن بعد، فتأكد من تحديد المربع المجاور لخدمة SSH.

٤. انقر فوق تطبيق.

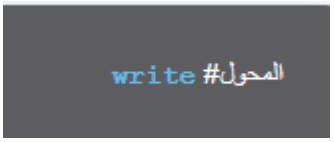


شكل (٦–٣٠) cisco 4

ملاحظة / سيفقد مستعرض الويب الوصول إلى واجهة مستخدم الويب ويجب إجراء تكوين إضافي باستخدام CLI عبر SSH أو منفذ وحدة التحكم (إذا كان المحول يحتوي على واحد).

٥. لحفظ التكوين، أدخل الأمر التالي باستخدام CLI (واجهة سطر الأوامر).

الأمر



٦. اضغط على Y للتأكيد.

- **تعطيل HTTP/HTTPS باستخدام CLI (واجهة سطر الأوامر)**

١. قم بتمكين خدمة SSH إذا كانت هناك حاجة إلى وصول سطر الأوامر البعيد ولم يتم تمكينه بالفعل من خلال إدخال:

```
switch(config)# ip ssh server
```

٢. أستخدم الأوامر التالية لتعطيل خدمات HTTP و HTTPS.

```
switch(config)# no ip http server
switch(config)# no ip http secure-server
```

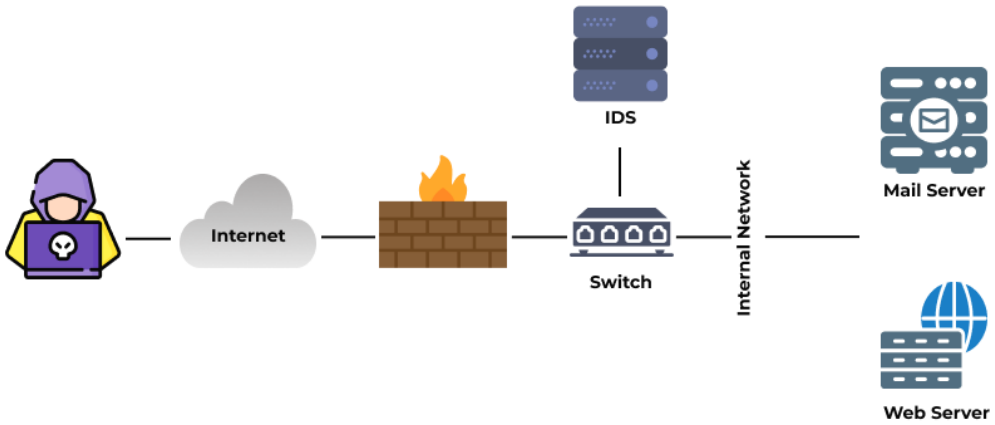
٣. لحفظ التكوين، أدخل

```
المحول# write
الكتابة فوق الملف [startup-config]... (Y/N) [N] ؟y
```

- **استخدام نظام كشف التسلل IDS**
  - **أولاً الـ IDS**

اختصاراً لـ Intrusion Detection System أو نظام كشف التطفُّل وهو نظام يتم وضعه في الشبكة لاكتشاف تهديدات الأمن السيبراني للمؤسسة وهو نظام للمراقبة والتنبيه فقط.

- **كيف يعمل؟**



1 IDS system

- يقوم بالبحث في الـ Traffic عن أي نشاط مشبوه وذلك عن طريق قائمة من الـ Signatures للتهديدات المعروفة ليقوم بالتعرف عليها إذا ما حدثت ويقوم بالإبلاغ وإنشاء تنبيه بوجود تسلل فيقوم فريق الأمن المسؤول بالتحقيق في الحادث واتخاذ الإجراءات اللازمة لمنع هذا التسلل أو الهجوم.

ملاحظة / يتم وضع الـ IDS خارج مسار الاتصال في الشبكة الداخلية (أي أن الـ Traffic لا يمر مباشرة به، ولكن يتم إرسال نسخة منه) ليعمل كنظام لكشف التطفل وليس لمنعه، والصورة السابقة توضح ذلك.

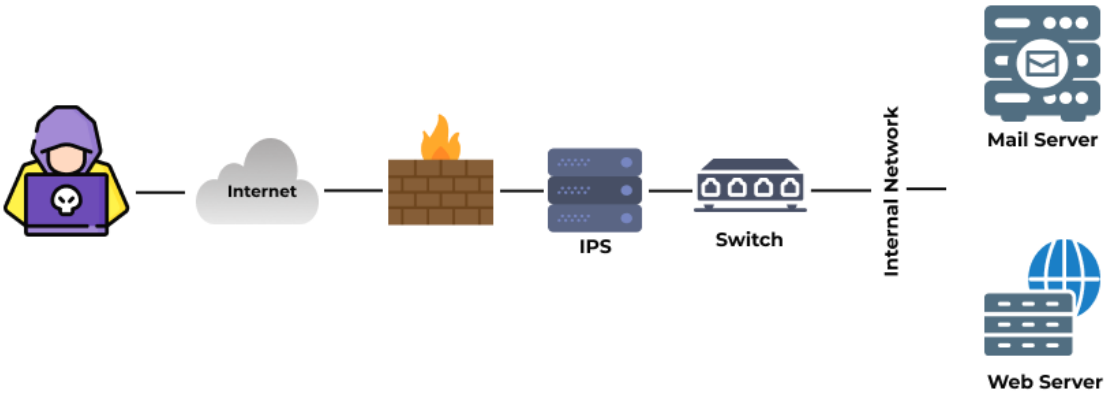
- **أنواع الـ IDS**

- **Network-based Intrusion Detection System (NIDS):** يتم وضعه لمراقبة الـ Traffic المار من وإلى الشبكة والكشف عن أي نشاط مشبوه.
- **Host-based Intrusion Detection System (HIDS):** يتم وضعه في أجهزة الكمبيوتر المتصلة بالشبكة (الداخلية)، لمراقبة الـ Traffic الذاهب من وإلي تلك الأجهزة حيث يمكنه اكتشاف الحزم الضارة "Network Packets" المرسلة في الشبكة الداخلية للمؤسسة، بما في الكشف عن أي جهاز مصاب يحاول التطفل علي الأجهزة الأخرى.
- **Anomaly-Based Intrusion Detection System (AIDS):** يعتمد هذا النوع علي طريقة ونظام معين حيث يتم تحليل الـ Traffic المستمر الخاص بالشبكة ويحلل النمط الخاص بها طبقاً للمعايير المحددة مسبقاً ويقوم بتنبيه المسئولين إلي السلوك غير المعتاد الذي يحدث في الـ Traffic، الأجهزة، الـ Ports، والبروتوكولات.
- **Signature-Based Intrusion Detection System (SIDS):** تعتمد تلك الأنظمة بشكل كبير علي قواعد البيانات التي تحتوي علي مجموعة كبير من التوقيعات "signatures" الخاص بهجمات أو تهديدات سابقة ومعروفة، فتقوم تلك الأنظمة القائمة علي الـ signatures بمراقبة جميع الـ Network Packets والكشف عن أي برمجيات خبيثة "Malwares" أو تهديدات محتملة من خلال تتطابق الـ signatures مع الأنشطة والبرمجيات الخبيثة التي تحدث.

- **ثانياً الـ IPS**

اختصاراً لـ Intrusion Prevention System أو نظام منع التطفل ويسمي أيضاً نظام الكشف عن التسلل ومنعه وهو نظام يتم وضعه في الشبكة لمنع أي هجوم أو تسلل محتمل بناءً على الخصائص المعطاة للـ Host والـ Signatures، على عكس الـ IDS يقوم الـ IPS باتخاذ الإجراءات اللازمة فيقوم بجمع المعلومات عنها والإبلاغ عنها ومحاولة منع ومعالجة تلك التهديدات وإيقافها.

- **كيف يعمل؟**



I IDS system

يقوم بتسجيل المعلومات التي تمت ملاحظتها وإخطار مسؤولي الأمن في المؤسسة بالأحداث التي تمت ملاحظتها، وإنشاء التقارير، كما يعمل على التصدي للتسلل ومحاولة إيقافه أو تغيير محتواه وذلك طبقاً لتقنيات مختلفة.

يتم وضعه في مسار الـ Traffic حيث يمر منه الـ Traffic ودوره أن يقوم بتحليله وكشف التسلل والتصدي له قبل وصول التهديد إلى الشبكة الداخلية.

- **أنواع الـ IPS**

- **Network-based intrusion prevention system (NIPS):** يقوم بمراقبة الشبكة بالكامل وتحليل الـ Traffic وكشف المشبوه منه ومنعه.

- **Host-based intrusion prevention system (HIPS):** يعمل على مراقبة الـ Traffic الخاص بجهاز معين وتحليله وكشف المشبوه منه ومحاولة التصدي له.

- **Network behavior analysis (NBA):** يفحص الـ Traffic الخاص بالشبكة لتحديد وكشف التهديدات التي تسبب تدفقات عالية في الشبكة كـ هجوم حجب الخدمة، وأشكال مختلفة من الـ Malwares وانتهاكات السياسة.

- **Wireless intrusion prevention system (WIPS):** يقوم بمراقبة الـ Traffic للشبكة اللاسلكية.

- **الاستنتاج:**

- الـ IDS لا يتم وضعه في مسار الـ Traffic فيقوم باكتشاف التهديد والإبلاغ عنه والتنبيه لكي يتم منعه.

- الـ IPS يتم وضعه في مسار الـ Traffic فيقوم بالكشف عنه والإبلاغ ومحاولة التصدي له أو تغيير محتواه وإسقاط الهجمات الضارة.

يمكن أن تعمل كلاً من أنظمة IPS و IDS معاً لتحقيق حماية كافية للتصدي للهجمات والتسلل الضار.

- **فصل مجموعة DNS الداخلية عن DNS الخارجية.**

هناك أدوات خاصة يمكن استخدامها لفصل مجموعة DNS الداخلية عن DNS الخارجية ، هذه الأدوات تساعد في تحقيق فصل فعال وسلس بين الشبكة المحلية والإنترنت العام ، **بعض الأدوات الشائعة:**

- **Bind:** هو خادم DNS مفتوح المصدر يستخدم على نطاق واسع في العديد من الشبكات. يوفر Bind إمكانية تكوين خوادم DNS الداخلية والخارجية وتحقيق الفصل بينهما.
- **Microsoft DNS:** هو خادم DNS يأتي مدمجًا مع أنظمة التشغيل Windows Server يوفر Microsoft DNS واجهة سهلة الاستخدام لتكوين خوادم DNS الداخلية والخارجية.
- **PowerDNS:** هو خادم DNS مفتوح المصدر يوفر ميزات متقدمة لإدارة DNS يمكن استخدام PowerDNS لتكوين خوادم DNS الداخلية والخارجية وتحقيق الفصل بينهما.
- **Dnsmasq:** هو خادم DNS و DHCP مفتوح المصدر يستخدم على نطاق واسع في الشبكات المنزلية والصغيرة ، يمكن استخدام Dnsmasq لتكوين خادم DNS داخلي وتوجيه طلبات الشبكة المحلية إلى خوادم DNS الخارجية.

- **استخدام طريقة split-DNS لحجب المعلومات الداخلية عن المستخدمين الخارجيين**
  - **بعض الأمثلة العملية لتطبيق split-DNS:**

- **حجب الوصول إلى موارد الشبكة الداخلية:** يمكن استخدام split-DNS لمنع المستخدمين الخارجيين من الوصول إلى موارد الشبكة الداخلية مثل الخوادم وقواعد البيانات الحساسة، عندما يحاول المستخدم الخارجي الوصول إلى عنوان IP داخلي، يتم توجيهه إلى عنوان IP خارجي بدلاً من ذلك.
- **توجيه حركة المرور إلى خوادم محددة:** يمكن استخدام split-DNS لتوجيه حركة المرور الخارجية إلى خوادم محددة. على سبيل المثال، يمكن توجيه حركة المرور الواردة من المستخدمين الخارجيين إلى خوادم ويب عامة، في حين يتم توجيه حركة المرور الداخلية إلى خوادم ويب داخلية.
- **تحقيق الأمان والحماية:** يعمل split-DNS على زيادة أمان البيانات وحماية البنية التحتية للشبكة، من خلال حجب المعلومات الداخلية عن المستخدمين الخارجيين، يتم تقليل فرصة الوصول غير المصرح به والاختراقات الأمنية.

يمكن تنفيذ split-DNS في شبكتك عن طريق إعداد خوادم DNS المناسبة، هناك عدة طرق لتنفيذها، **وفيما يلي خطوات عامة يمكن اتباعها:**

- قم بتحديد الموارد التي ترغب في حجبها عن المستخدمين الخارجيين في شبكتك الداخلية.
- قم بتكوين خادم DNS الخاص بك بحيث يقدم معلومات مختلفة للمستخدمين الداخليين والخارجيين.

ملاحظة / يمكنك تحقيق ذلك عن طريق تعيين سجلات DNS مختلفة لكل فئة من المستخدمين، للمستخدمين الداخليين، قم بتوجيههم إلى عناوين IP داخلية للموارد المطلوبة.

ملاحظة/ يمكنك تحقيق ذلك عن طريق تعيين سجلات DNS تشير إلى عناوين IP الداخلية، للمستخدمين الخارجيين، قم بتوجيههم إلى عناوين IP خارجية للموارد المطلوبة.

ملاحظة/ يمكنك تحقيق ذلك عن طريق تعيين سجلات DNS تشير إلى عناوين IP الخارجية، من المهم أن تتعاون مع مسؤولي الشبكة الخاصة بك لتنفيذ split-DNS بطريقة صحيحة وفعالة.

- **تشفير كلمات المرور وحماية المعلومات الحساسة**
  - **كلمات مرور المستخدم**

كلمات مرور المستخدم ومعظم كلمات المرور الأخرى (لا enable secrets) في ملفات تكوين Cisco IOS، يتم تشفيرها بمخطط ضعيف للغاية بواسطة المعايير المشفرة الحديثة.

على الرغم من أن Cisco لا تقوم بتوزيع برنامج فك تشفير، إلا أن هناك على الأقل برنامجين مختلفين لفك التشفير لكلمات مرور Cisco IOS متاحين للعامة على الإنترنت؛ الإصدار العام الأول من هذا البرنامج الذي تعلم Cisco أنه كان في أوائل عام ١٩٩٥ ، ونتوقع من أي مشفر هاو أن يتمكن من إنشاء برنامج جديد بأقل جهد ممكن.

  - **الـ enable سر و enable كلمة أمر**

يعرض الأمر enable password لم يعد من المستحسن استخدام الأمر، أستخدم enable secret لتحقيق مستوى أعلى من الأمان، المثيل الوحيد الذي enable password الأمر الذي يمكن اختباره هو عندما يكون الجهاز في وضع التمهيد الذي لا يدعم enable secret erasecat4000_flash..

  - **تمكين تجزئة الأسرار باستخدام خوارزمية MD5**

على قدر ما يعرفه أي شخص في Cisco، من المستحيل استعادة أمر enable secret استنادا إلى محتويات ملف تكوين (بخلاف هجمات القاموس الواضحة).

ملاحظة: لا ينطبق هذا إلا على كلمات المرور المعينة مع enable secret، وليس على كلمات المرور المعينة مع enable password والواقع أن قوة التشفير المستخدمة هي الفارق المهم الوحيد بين الأمرين.

- **تشفير كلمات المرور**

١. اختيار كلمة مرور قوية

استخدم كلمات مرور تتألف من مزيج من الأحرف الكبيرة، والصغيرة، والأرقام، والرموز، تجنب استخدام كلمات سهلة التخمين مثل تواريخ الميلاد أو الكلمات الشائعة.

٢. تحديث كلمات المرور بانتظام

قم بتغيير كلمات المرور بانتظام، على الأقل كل بضعة أشهر، لزيادة أمان حساباتك.

٣. عدم استخدام كلمة مرور واحدة للحسابات المتعددة

استخدم كلمات مرور فريدة لكل حساب لتجنب أن يتم تعريض الحسابات الأخرى في حالة اختراق أحدها.

٤. استخدام إدارة كلمات المرور

استخدم أدوات إدارة كلمات المرور مثل LastPass أو Password لتخزين وتوليد كلمات مرور قوية وتشفيرها.

٥. حماية المعلومات الحساسة

استخدام اتصال آمن (SSL/TLS): عند تبادل المعلومات الحساسة عبر الإنترنت، تأكد من أن المواقع التي تزورها تستخدم اتصال آمن.

٦. تشفير البريد الإلكتروني

استخدم خدمات البريد الإلكتروني التي تدعم التشفير مثل PGP/GPG لتأمين رسائل البريد الإلكتروني.

٧. تأمين الأجهزة

قفل جهاز الكمبيوتر والأجهزة الذكية بكلمة مرور أو نظام تعرفة البصمة لمنع وصول غير المصرح به.

٨. تنظيم الوثائق والملفات

قم بتنظيم المعلومات الحساسة في ملفات مؤمنة، وقم بحذف المعلومات التي لا تحتاجها بانتظام.

٩. التحقق الثنائي (Two-Factor Authentication)

قم بتفعيل خيار التحقق الثنائي حيثما كان ذلك ممكنًا، حيث يتم طلب رموز تحقق إضافية بجانب كلمة المرور.

١٠. تحديد الوصول

قم بتحديد الوصول إلى المعلومات الحساسة فقط للأشخاص الذين يحتاجون إليها.

- **القيام بعملية استطلاع دورية للكشف عن المعلومات المتاحة للجميع**
  - **كيفية القيام بعملية استطلاع دورية**

- **تحديد المصادر المناسبة:** قم بتحديد المصادر التي تحتوي على المعلومات المتاحة للجميع في مجال معين، يمكن أن تشمل هذه المصادر المواقع الإلكترونية، المجلات، الصحف، وقواعد البيانات العامة.
- **تحديد الجدول الزمني:** حدد تردد الاستطلاع الدوري، مثل مرة واحدة في الأسبوع أو مرة واحدة في الشهر، واحتفظ بتلك الجدولية للحصول على المعلومات المحدثة بشكل منتظم.
- **جمع المعلومات:** قم بزيارة المصادر المحددة واستخرج المعلومات المتاحة للجميع، يمكنك استخدام أدوات البحث المتاحة في هذه المصادر لتحديد المعلومات ذات الصلة.
- **تحليل المعلومات:** بعد جمع المعلومات، قم بتحليلها وتنظيمها بطريقة مناسبة، يمكن استخدام الأدوات والتقنيات المناسبة لتحليل البيانات واستخلاص النتائج الهامة.
- **توزيع النتائج:** قم بتوزيع النتائج والمعلومات المحدثة للأشخاص المعنيين، يمكن استخدام التقارير والعروض التقديمية لتوضيح النتائج والمعلومات بشكل فعال.

ملاحظة: يجب أن يتم تنفيذ الاستطلاع الدوري بشكل منتظم ومن قبل أشخاص مؤهلين لتحليل وتفسير البيانات المجمعة.

١. اختار الإجابة الصحيحة فيما يلي:

١. يعني جمع المعلومات دون التفاعل مع الهدف ولن تكون الجهة المستهدفة على علم بأن هناك من يجمع المعلومات عنها مثل جمع المعلومات من مواقع الأنترنت أو عن طريق الهندسة الاجتماعية

أ- الاستطلاع السلبي
ب- الاستطلاع الإيجابي
ت- الاستطلاع النشط
ث- الاستطلاع الغير نشط

٢. جمع المعلومات بالتفاعل مع الهدف بشكل مباشر، مثال أن يقوم المخترق بتصفح الموقع الإلكتروني 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 الإنترنت والخدمات

أ- الاستطلاع السلبي
ب- الاستطلاع الإيجابي
ت- الاستطلاع النشط
ث- الاستطلاع غير النشط

٣. من محركات البحث /

أ- www.google.com
ب- www.youtube.com
ت- www.wordspace.com
ث- www.masanger.com

٤. من محركات البحث عن الأشخاص

أ- Zabsearch
ب- Yahoo
ت- Youtube
ث- net

٥. who.is هو موقع لـ

أ- استخراج DNS
ب- استخراج IP
ت- استخراج DNA
ث- استخراج البيانات الافتراضية

٢. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	اختبار النطاق يكون من خلال الأمر ping	√
٢.	يتعامل مع خادم الويب ومواقع استضافة تحليل حصة السوق والكشف عن نظام التشغيل google	×
٣.	استخدام طريقة split-DNS لحجب المعلومات الداخلية عن المستخدمين الخارجيين	√
٤.	خادم DNS يحتوي على ملف نصي يسمى الملف HOST وأهمية هذا الملف أنه يحتوي على العنوان الإلكتروني لكل حاسب في المنظمة وعلى عنوان IP المقابل له وتعتبر خوادم DNS هي المكان الرسمي الذي تخزن فيه المعلومات التي تتعلق بكل الأجهزة التابعة لشبكة المنظمة وهي المصدر الرسمي للمعلومات عنها ومن أهم هذه المعلومات الاسم أو العنوان الإلكتروني لكل حاسب وهو يتكون من اسم الحاسب واسم المجال.	√
٥.	الكشف عن نقاط الضعف في النظام وأفضل الطرق لاستغلالها من طرق التنصيب	×

الفصل الثالث

المسح والتعداد Scanning and Enumeration

في هذا الفصل سنتعرف على المواضيع التالية:

- منهجية المسح (الفحص) Scanning
- الأدوات (عملي)
- تعداد Enumeration
- Banner Grapping Enumeration
- التدابير المضادة والحماية من عمليات الفحص والتعداد

❖ منهجية المسح (الفحص) Scanning

بعد جمع المعلومات لا يستطيع المخترق الوصول إلى أي حاسب آلي بعيد واختراقه إلا إذا كان هذا الحاسب متصلا بالأنترنت أو بشبكة المؤسسة التي ينتمي إليها، فالفكرة هي اكتشاف قنوات الاتصال لاستغلالها حيث يتم التعرف على الأنظمة المتصلة والقابلة للوصول عبر الإنترنت من خلال إرسال إشارة اتصال إلى عنوان IP للحاسب الهدف وفي حال إذا استجاب الحاسب الهدف لهذه الرسالة فسيعرف أن هذا الحاسب متصل وفعال ، كما أن في هذه المرحلة يمكن للمخترق العثور على طرق مختلفة لاختراق النظام المستهدف و اكتشاف المزيد من المعلومات مثل ما يستخدمه من نظام تشغيل وخدمات ، **و يوجد عدة أنواع للفحص و هي :**

١. فحص المنافذ **Port Scanning** : يستخدم في المنافذ و الخدمات، المنافذ تُمثل الأبواب و النوافذ لهذ النظام يستخدمها المتسلسلون و المخترقون للوصول إليه ، حيث المزيد من المنافذ المفتوحة تعني المزيد من نقاط الضعف و عدد أقل من المنافذ المفتوحة تعني المزيد من التأمين .

٢. فحص الشبكات **Network Scanning** : يستخدم في فحص عناوين IP فيتم فيها جمع معلومات حول عناوين IP التي تم جمعها من مرحلة الاستطلاع للوصول إليها عبر الشبكات و بنيتها و الخدمات التي تعمل عليها ، قبل الاختراق يلاحظ المخترق ويحلل الشبكة ليحصل على المعلومات المطلوبة لبناء استراتيجية الهجوم.

٣. فحص نقاط الضعف **Vulnerability Scanning**: يستخدم لفحص الضعف.

- **تحديد الأهداف**

هو التعرف على الحواسيب المتصلة التي تعمل على الشبكة والخدمات (التطبيقات والبرامج) التي تشغلها هذه الحواسيب والتي تُعد منافذ يمكن الدخول من خلالها إلى النظام **أي :**

- اكتشاف الأجهزة المتصلة، عنوان IP ، المنافذ المفتوحة التي تعمل على الشبكة.
- اكتشاف أنظمة التشغيل وبنية النظام المستهدف لأن المخترق سيبني الهجوم على أساس نقاط الضعف في نظام التشغيل.
- اكتشاف خدمة الشبكة مع كل منفذ.
- تحديد نقاط الضعف والتهديدات.

- **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 للانتظار، العديد من خدمات الشبكة المشتركة تعمل على أرقام منافذ قياسية تعطي المخترق مؤشر بوظيفة النظام الهدف.

بعد أن يتم التحقق من أن الحاسب الآلي الهدف متصل بالإنترنت، يقوم المخترق بعملية مسح المنفذ من أجل التعرف على الخدمات أو البرامج العاملة في الحاسب الآلي الهدف مثل خدمة Telnet أو خدمة ftp أو غير ذلك من الخدمات ويُمثل البرنامج أو الخدمة العاملة على النظام منفذا" مفتوحا للدخول إليه ثم بعد اكتشاف المنافذ المفتوحة يقوم المخترق باستغلال أي منفذ مفتوح لاختراق النظام المستهدف ، وتتم عملية مسح المنافذ باستخدام المخترق برنامج مخصص لمسح المنافذ ويرسل هذا البرنامج الموجود في حاسب المخترق إشارة اتصال SYN إلى المنفذ المحدد في الحاسب المستقبل وينتظر الجواب أو الرد من ذلك المنفذ ، إذا كان المنفذ في حالة إنصات أي جاهز للاتصال فإنه يُعيد جوابا برسالة موافقة ACK/ SYN ومعنى هذه الرسالة أن البرنامج أو الخدمة تعمل على المنفذ وجاهزة للاتصال أي أن المنفذ مفتوح للدخول أما إذا رد جهاز المستقبل برسالة RST/ACK فإن ذلك يعني إلى أن المنفذ لا ينصت أي مغلق بمعنى أن الخدمة أو البرنامج المحدد لا يعمل على النظام الهدف.

يتم مسح المنافذ لكل عنوان IP تم الحصول عليه من مرحلة الاستطلاع فاذا كان منفذ 80 مفتوح فإنه يحاول الاختراق من خلال هذا المنفذ.

- **التصنت**

هو الاستماع سرا إلى المحادثات بين الأفراد من خلال الهاتف أو محادثات الفيديو بدون علمهم ويشمل أيضا قراءة الرسائل السرية من وسائط الاتصال مثل الرسائل الفورية أو رسائل الفاكس لجمع المعلومات.

- **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

❖ الأدوات (عملي)

يوجد بعض الأدوات الخاصة بنظام كالي لينكس للكشف عن الأجهزة المتصلة **تكون تحت القائمة التالية:**

Live Host Identification/ Information Gathering/ Application.

مثل:

Arping – detect_sniffer – dmitrt – hping -Ncat

- **Arping**

كيفية مسح إدخال بروتوكول تحليل العنوان الواحد (ARP) في موجه باستخدام بروتوكول إدارة الشبكة البسيط (SNMP)

المتطلبات الأساسية // المكونات المستخدمة

١. مسح الإدخال ARP

لا يوجد أمر برنامج IOS Cisco software لمسح إدخال جدول ARP واحد، يعمل الأمر clear software cache-arp IOS Cisco على مسح الجدول بالكامل يمكنك استخدام بروتوكولSNMP مع كائن (IPnetToMediaType) ١,٣,٦,١,٢,١,٤,٢٢,١,٤ داخل جدول (IPnetToMediaTable) (1.3.6.1.2.4.22.) من قاعدة معلومات الإدارة (RFC MIB٢)

```
                                                                1.3.6.1.2.1.4.22.
                                                    ipNetToMediaTable OBJECT-TYPE
                                                      FROM RFC1213-MIB --
DESCRIPTION    "The IP Address Translation table used for mapping from IP addresses to
                                                                        ".physical addresses
                                    { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) 22 } =::


                                                                    1.3.6.1.2.1.4.22.1.4.
                                                    ipNetToMediaType OBJECT-TYPE
                                                      FROM RFC1213-MIB --
          { (SYNTAX          Integer { other(1), invalid(2), dynamic(3), static(4
                                                  MAX-ACCESS       read-create
                                                      STATUS           Current
                                                .DESCRIPTION     "The type of mapping
        Setting this object to the value invalid(2) has the effect of
                                                                              invalidating
        the corresponding entry in the ipNetToMediaTable.  That is, it
                                                                               effectively
disassociates the interface identified with said entry from the mapping
identified with said entry.  It is an implementation-specific matter as
                                                                                       to
        whether the agent removes an invalidated entry from the table.
                                                                              ,Accordingly
management stations must be prepared to receive tabular information from
                                                                                    agents
that corresponds to entries not currently in use.  Proper interpretation
                                                                                  of such
  ".entries requires examination of the relevant ipNetToMediaType object
            iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) ipNetToMediaTable(22) } =::
                                                                { ipNetToMediaEntry(1) 4
```

شكل (٣١) مسح الإدخال ARP

عندما تقوم بتشغيل عنصر (١,٣,٦,١,٢,١,٤,٢٢,١,٤) MIB،ipNetToMediaType ، إلى غير صالح=،٢ يمكنك حذف إدخال ARP واحد

```
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.172.16.98.45 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.7.172.16.96.1 = other(1

--<snip>--
```

عندما تقوم بتنفيذ **مجموعة snmpset** على إدخال ARP واحد، على سبيل المثال:

```
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.2 = dynamic(3
```

وتعيين قيمتها إلى 2=غير صحيحة، وفقا لتعريف قاعدة معلومات الإدارة:

```
snmpset 172.16.99.1 private ipNetToMediaType.1.172.16.98.2 i 2
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.2 = invalid(2
```

إذا قمت بتنفيذ **عملية سير** snmpwalk أخرى لكائن **ipNetToMediaType** MIB على الموجه، فأنت ترى هذا الإخراج:

```
snmpwalk 172.16.99.1 public .1.3.6.1.2.1.4.22.1.4

(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.1 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.172.16.98.36 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.172.16.98.37 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.1 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.101 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.254 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.172.16.98.41 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.172.16.98.45 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.7.172.16.96.1 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.7.172.16.96.31 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.7.172.16.96.40 = dynamic(3

--<snip>--
```

لم يعد الإخراج المستهدف في الإخراج.

شكل (٣٢) الإخراج لم يعد مستهدف

مثال

ملاحظة: تأكد من تكوين سلاسل مجتمع SNMP للقراءة فقط (RO)/للقراءة والكتابة (RW) على الموجه.

وفيما يلي إخراج **snmpwalk** لكائن **ipNetToMediaType** MIB على الموجه:

```
snmpwalk 172.16.99.1 public .1.3.6.1.2.1.4.22.1.4
```

```
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.1 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.2 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.172.16.98.36 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.172.16.98.37 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.1 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.101 = other(1
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.172.16.97.254 = dynamic(3
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.172.16.98.41 = dynamic(3
```

شكل (٣٣) مثال تكوين SNMP

لم يعد الإخراج المستهدف في الإخراج.

```
(ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.172.16.98.2 = dynamic(3
```

هنا شرح للمتغيرات المستخدمة أعلاه:

- 172.16.99.1 = عنوان IP الخاص بالموجه المستخدم في هذا المثال.
- خاص = سلسلة مجتمع RW SNMP للموجه
- عامة = سلسلة مجتمع RO SNMP للموجه
- 1.3.6.1.2.1.4.22.1.4. =معرف الكائن (OID) لكائن MIB **ipNetToMediaType**
- i = عدد صحيح كما هو محدد بناء الجملة في قاعدة معلومات الإدارة
- 2 (غير صالح)= قيمة كائن قاعدة معلومات الإدارة (MIB)

شكل (٣٤) شرح للمتغيرات المستخدمة

- **NMAP**

هي أداة تعداد معياريا ويتم استخدامها في البيئات الموزعة ويستخدم لاكتشاف المتصلين والخدمات على الشبكة مما يساعد في عمل مخطط للشبكة المستهدفة وتقوم هذه الأداة باختبار الشبكات وعرض الثغرات المفتوحة والأجهزة المتصلة على الشبكة ونوع جدار الحماية ونوع نظام التشغيل المستخدم وإصداره ويعتبر أداة قوية يستخدمه المخترقون وأيضا محللي الشبكات والذين يهدفون إلى اكتشاف الثغرات والأخطاء لتجنب أي عملية اختراق للأجهزة والشبكة.

هو أفضل وأقوى أدوات مسح المنافذ وأكثرها شهرة، وعند وضع عنوان IP في أداة NMAP وتشغيلها على النظام الهدف، تقوم NMAP بمسح المنافذ المشهورة والشائعة افتراضيا وتحديد خيار المسح لكل المنافذ في النظام الهدف فتقوم NMAP بمسح كل المنافذ الموجودة في النظام.

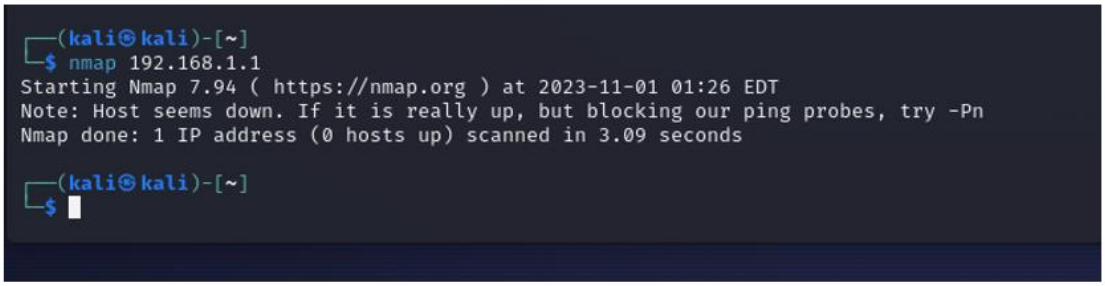
مخرجات NMAP يتضمن أنواعا متعددة من المعلومات من أهمها المنافذ المفتوحة والخدمات والبرامج العاملة عليها، حيث يتم استخدامها لإجراء فحوصات Ping حيث تقوم بتحديد المتصلين على الشبكة وترسل ICMP echo request لجميع المتصلين على الشبكة، إذا كان الجهاز متصلا فإنه يرسل رد ICMP ECHO وهذا الفحص مفيد لتحديد موقع الأجهزة المتصلة وتحديد إذا كان ICMP يمر من خلال جدار الحماية.

```
# NMAP    192.168.12.60
```

فكرة عمله في اكتشاف المنافذ في حالة المنافذ المفتوحة يعتمد على أسلوب THREE WAY HANDSHAKES يرسل المخترق عن طريق أداة Nmap حزمة مرفق بها رقم المنفذ لفتح جلسة TCP ثم يرد الجهاز الهدف من خلال المنفذ المفتوح ثم يغلق جهاز المخترق الاتصال عن طريق حزمة RST فيتم معرفة أنه يوجد منفذ مفتوح، في حالة المنفذ المغلق رد الجهاز يكون مختلفا، سيغلق الاتصال مباشرةً وبالتالي الجهاز الذي يتم فحصه يوقف الاتصال وهذا النوع من الفحص يتم اكتشافه بسهولة من قبل النظام المستهدف ويتم تسجيله في ملفات السجل LOG FILE.

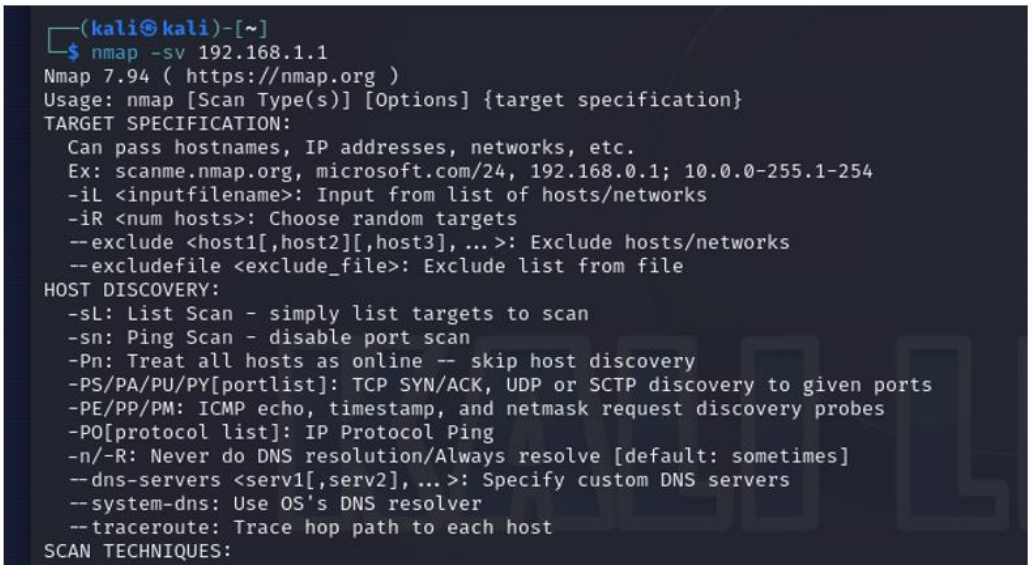
لمسح نطاق IPمحدد:

nmap <IP>



شكل (٣٥) مسح النطاق في كالي لينكس

لمسح المنافذ المفتوحة وتحديد الخدمات: nmap -sV <IP>



شكل (٣٦) مسح المنافذ والخدمات ا

- **Hping 3**

هي أداة لإنشاء حزم بيانات من أجل الحصول على إجابات من الأجهزة المتصلة في النظام الهدف والحصول على المسار الكامل للهدف وتجاوز أجهزة تصفية حزم البيانات وهي مترجم ومحلل لحزم TCP/IP وتدعم , ICMP , TCP,UDP وهي أيضا قادرة على التعقب Traceroute mode .

- **أهم ميزات الأداة**

- اختبار جدار الحماية وفحص قواعد وقوانينه.
- مسح متقدم للمنافذ.
- فحص منافذ الشبكة.
- اختبار الشبكة باستخدام بروتكولات مختلفة.
- اكتشاف نظم التشغيل على الشبكة المستهدفة.

```
# hping3    192.168.12.60  -S  -C 1  -P  25
```

S- : استخدام حزم من النوع SYN.

c- : يحدد كمية الحزم المطلوب إرسالها ، تم إرسال حزمة.

P- : لتحديد المنفذ المطلوب الإرسال إليه.

- تطبيق عملي

  - مثال لاستخدام hping3

استخدم وضع التتبع (--traceroute) وكن مطولا (-V) في وضع ICMP (-1) مقابل الهدف (www.example.com):

شكل (٣٧) استخدام haping3 ا

hping3 هي أداة شبكة قادرة على إرسال حزم ICMP/UDP/TCP مخصصة وعرض الردود المستهدفة مثلما يفعل ping مع ردود ICMP ، فهو يتعامل مع التجزئة وجسم وحجم الحزمة التعسفي، ويمكن استخدامه لنقل الملفات بموجب البروتوكولات المدعومة، باستخدام hping3، يمكنك اختبار قواعد جدار الحماية، وإجراء مسح للمنافذ (المخادعة)، واختبار أداء الشبكة باستخدام بروتوكولات مختلفة، واكتشاف مسار MTU، وتنفيذ إجراءات تشبه مسار التتبع بموجب بروتوكولات مختلفة، وأنظمة التشغيل عن بعد لبصمات الأصابع، ومراجعة مجموعات TCP/IP، وما إلى ذلك hping3 قابل للبرمجة باستخدام لغة Tcl.

الحجم المثبت: **٢٥٤ KB**

كيفية التثبيت: **sudo apt install hping3**

- **Arping**

تقوم بإرسال حزمة ARP (بروتوكول يستخدم في البحث عن MAC Address للأجهزة الموجودة في الشبكة الداخلية عن طريق IP Address) إلى الجهاز المحدد ثم يقوم بعرض النتائج.

```
# arping -c 4 192.168.12.60
```

-c : يحدد كمية الحزم المطلوب إرسالها ، تم استخدام ٤ حزم من النوعarp

❖ تعداد Enumeration

هي عملية لجمع معلومات معينة متعلقة بالنظام الهدف من خلال معرفة المنافذ المفتوحة ونظام التشغيل والخدمات التي تعمل والتطبيقات المدعومة.

بالنسبة لمُختبر الاختراق البيانات المُعادة تكشف الأجهزة المتصلة وهذا يُستخدم 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 الأنظمة بشكل أكبر.

- **أساسيات نظام Windows**

لمعرفة نظام التشغيل الذي يعمل في الشبكة الهدف وأساسياته يتم استخدام أداة NetCraft بفتح العنوان التالي **http://netcraft.com** وكتابة اسم المجال Domain الخاص بالشبكة المستهدفة، مثل استخدام microsoft.com.

- **تقنيات العد (عملي)**

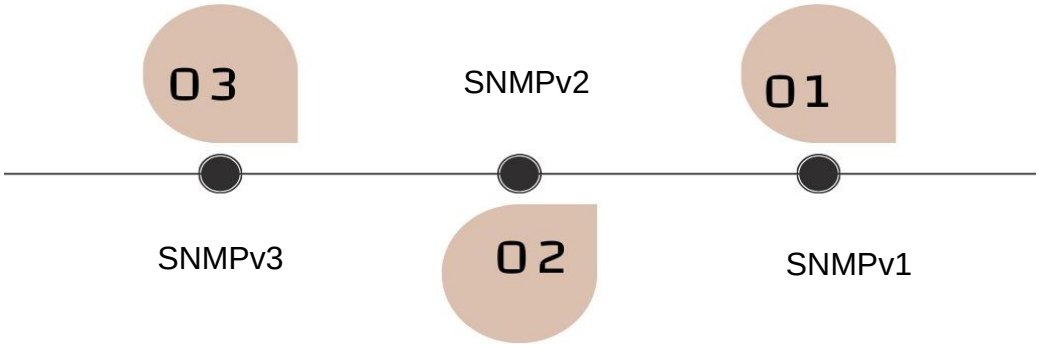
تقنيات للحصول على معلومات حول مشاركة موارد الشبكة وبيانات SNMP للحصول على معلومات حول مشاركة موارد الشبكة وبيانات SNMP، يمكن استخدام عدة تقنيات مختلفة، **من بينها:**

- **استخدام أدوات SNMP:** يمكن استخدام بروتوكول إدارة الشبكة البسيط (SNMP) وأدواته لجمع معلومات حول مشاركة موارد الشبكة وبيانات SNMP يمكن استخدام أدوات مراقبة الشبكة مثل Network Performance Monitor وغيرها للوصول إلى هذه البيانات.
- **استخدام تقنيات Honeypot:** يمكن استخدام تقنيات Honeypot لجذب المهاجمين ومراقبة أنشطتهم على الشبكة، هذا يمكن أن يوفر معلومات قيمة حول محاولات الوصول غير المصرح بها إلى موارد الشبكة.
- **تحليل حركة الشبكة والمرور:** يمكن استخدام تقنيات تحليل حركة الشبكة والمرور لفهم كيفية استخدام الموارد والبيانات على الشبكة، هذا يمكن أن يساعد في تحديد أي مشاركة غير مصرح بها للموارد.

- **تطبيق عملي لـ SNMP in kali Linux**

كيف يعمل الـ SNMP ؟

للـ SNMP ثلاث إصدارات مختلفة:



في الأصدر الثاني تم استبدال Get-Next بي Get-Bulk التي تستطيع تحمل معلومات أكبر بالإضافة لبعض أمور الأمن والسكيورتي والعديد من مميزات المراقبة وقد تم إصداره عام ١٩٩٧ أما الأصدر الثالث وهو المستخدم في وقتنا الحالي منذ عام ٢٠٠٤ فقد تم أضافة بعض الأمور **مثل:**

- Authentication
- Privacy
- access control

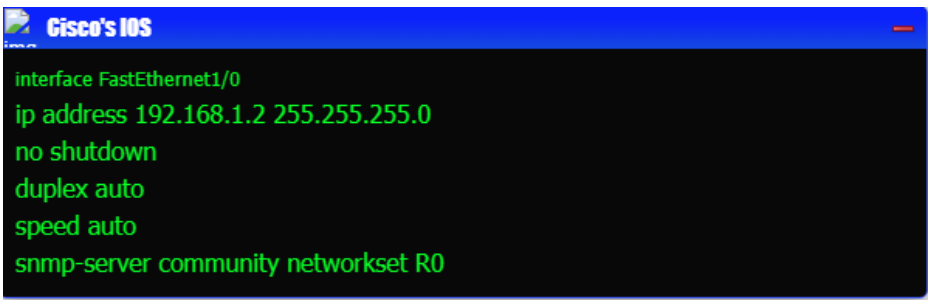
وبالنسبة للبرامج المستخدمة فهي كثيرة جدا ولكل برنامج له مميزاته الخاصة لكن يمكنك أن تحمل هذا البرنامج المجاني المفتوح المصدر الذي يعطيك حالة الترافيك التي تعبر من خلال الراوتر أو السويتش

http://oss.oetiker.ch/mrtg

ولتثبيته على ويندوز يحتاج الى مترجم بيرل تستطيع تحميله من هنا

http://strawberry-perl.googlecode.com/files/strawberry-perl-5.10.1.1.msi

بعد تثبيت بيرل تقوم بفك الضغط عن البرنامج على السي مباشرة وتذهب للراوتر(سيسكو) وتقوم بكتابة الأوامر التالية:



شكل (٢-٣٧) SNMP

بعدها من الدوس أدخل على الملف التالي:

شكل (٢-٣٧) SNMP ٢

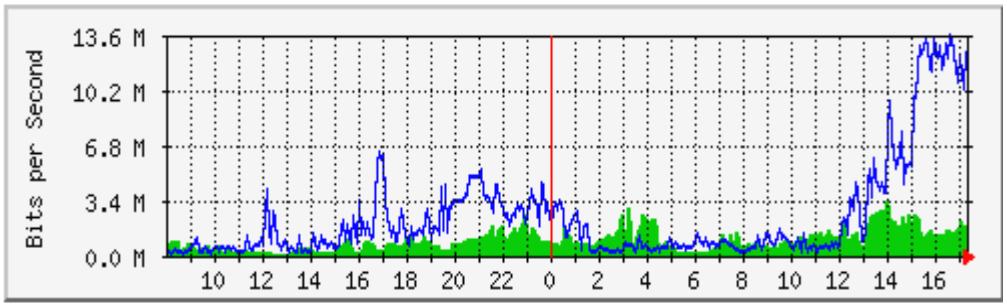
وقم بكتابة الأمر التالي:

شكل (٢-٣٧) SNMP ٣

ولتشغيل البرنامج أكتب هذا الأمر:

شكل (٢-٣٧) SNMP 4

قد تظهر بعض الأخطاء وهذا شيء طبيعي في حال قمت بتشغيله أول مرة وبعدها توجه الى C:wwwmrtg سوف تشاهد ملف Html قم بفتحه وشاهد الإحصائية للجهاز المراقب

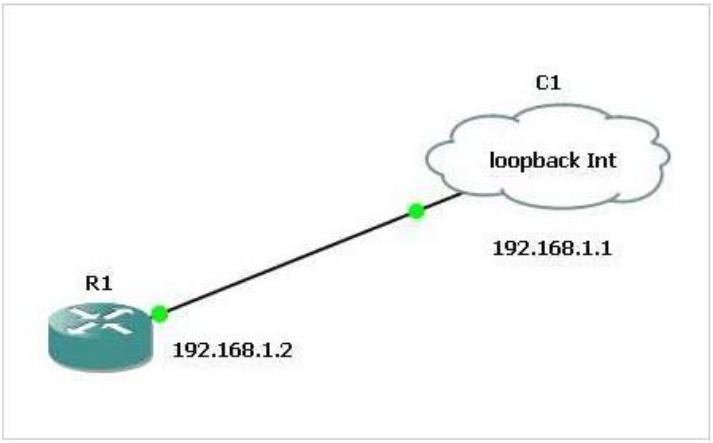


شكل (٢-٣٧) SNMP ٥

ولكي تقوم بتحديث النتائج قم مرة ثانية بتنفيذ الأمر السابق

شكل (٢-٣٧) SNMP ٦

ولو أردت تجربة الموضوع على GNS3 كل ما عليك أن تقوم بعمل Loopback Interface وتربطه مع الراوتر من خلال الغيمة وأعطي الـ Loopback الايبي ١٩٢,١٦٨,١,١ كما هو موضح بالصورة التالية



شكل (٢-٣٧) SNMP ٧

- **فحص الجداول IP والمستخدمين وقوائم سياسات كلمات المرور**

يمكن استخدام أدوات مثل (CMD) Command Prompt لفحص الجداول IP والمستخدمين وقوائم سياسات كلمات المرور على الشبكة.

- **استخدام أدوات إدارة الشبكة مثل CCNA:**

يمكن الاعتماد على الشهادات والتدريبات في مجال إدارة الشبكات مثل CCNA (Cisco Certified Network Associate) لتعلم كيفية الحصول على المعلومات المطلوبة وضمان أمان الشبكة.

- **تقنيات يمكن استخدامها للحصول على معلومات حول**

- مشاركة موارد الشبكة
- بيانات SNMP، إذا لم يتم تأمينها بشكل صحيح
- جداول IP
- أسماء المستخدمين للأنظمة المختلفة
- قوائم سياسات كلمات المرور

- **تعتمد التعدادات على الخدمات التي تقدمها الأنظمة، وأنواعها هي:**
  - **تعداد DNS (DNS ENUMERATION)**

من خلال عملية تعداد نقل المنطقة ينفذها المهاجم لتحديد خادم DNS وسجلات المنظمة المستهدفة يجمع معلومات قيمة عن الشبكة الهدف مثل أسماء المضيفين وأسماء الأجهزة وأسماء المستخدمين ولإجراء تعداد DNS يتم استخدام الأداة NSLOOKUP

  - **تعداد NTP (NTP ENUMERATION)**

من خلال تعداد NTP يمكن جمع معلومات مثل قوائم المضيفين (Lists of hosts) المتصلة بخادم NTP ، عناوين IP ، أسماء النظام ، نوع نظام التشغيل على أنظمة العميل في الشبكة , **ويتم تنفيذها باستخدام الأداة :** NTP SUITE.

  - **تعداد SNMP (SNMP ENUMERATION)**

لاستخدام SNMP في Kali Linux لأغراض عملية، **يمكنك اتباع الخطوات التالية:**

- **تثبيت أدوات SNMP :** تأكد من تثبيت أدوات SNMP على نظام Kali Linux الخاص بك ، يمكنك القيام بذلك عن طريق استخدام مدير الحزم لتثبيت أدوات SNMP الضرورية.
- **استخدم SNMPwalk** : SNMPwalk هو ماسح ضوئي قوي لـ SNMP يمكن استخدامه لجمع المعلومات من الأجهزة ذات سلاسل مجتمع SNMP التي يمكن تخمينها ، يمكنك استخدام SNMPwalk للتنقل بين سلسلة من الطلبات لجمع أكبر قدر ممكن من المعلومات من الخدمة.

- **فيما يلي مثال لكيفية استخدام SNMPwalk:**

```
snmpwalk -c public -v1 <target IP address<
```

استبدل <target IP address> بعنوان IP الخاص بالجهاز الذي تريد الاستعلام عنه.

تعداد SNMP : يمكنك إجراء تعداد SNMP باستخدام أدوات مثل snmp-check تتيح لك هذه الأداة تحديد منفذ SNMP والمجتمع والإصدار والخيارات الأخرى لجمع المعلومات من الأجهزة التي تدعم SNMP ،

- **فيما يلي مثال لكيفية استخدام snmp-check:**

```
snmp-check -c public -v1 <target IP address<
```

تعداد الخدمة: يمكنك أيضًا إجراء تعداد الخدمة لتحديد إصدار خدمة SNMP وسلسلة المجتمع، يمكن القيام بذلك باستخدام أدوات مثل NMAP مع البرامج النصية NSE.

- **فيما يلي مثال لكيفية تنفيذ تعداد الخدمة باستخدامNMAP :**

```
nmap -sV <target IP address<
```

تعداد SNMP هو عملية تعداد حسابات المستخدمين والأجهزة الموجودة على جهاز حاسب تم تمكين SNMP فيه.

- **أداة smtp-user-enum**

يحاول smtp-user-enum تخمين أسماء المستخدمين باستخدام خدمة SMTP.

- **تعداد LDAP (LDAP ENUMERATION)**

من خلال هذا التعداد يمكن الوصول إلى قوائم الدليل Active Directory وتستخدم من قبل المهاجمين للوصول إلى أسماء المستخدمين والعناوين.

❖ Banner Grabbing Enumeration

تقنيات يتم استخدامها من قبل المخترقين لمعرفة المعلومات المهمة **مثل:**

١. أنواع الأجهزة، فرضًا أنك ترغب في معرفة معلومات حول جهاز معين على الشبكة، يمكنك استخدام أدوات مثل Nmap لهذا الغرض.

- **استخدام Nmap**

يمكنك استخدام أداة Nmap مع خيار –0– للكشف عن نوع نظام التشغيل.

على سبيل المثال افترض أن لديك عنوان IP هدف هو 192,168,1,1 **يمكنك استخدام الأمر التالي:**

```
Copy code
nmap -O 192.168.1.1
```

هذا الأمر سيستخدم Nmap لفحص الجهاز الموجود على عنوان IP المعطى ومحاولة تحديد نوع نظام التشغيل المستخدم.

مثال / فرضًا أن لدينا عنوان IP هدف هو 192,168,1,100 ونريد معرفة نوع نظام التشغيل الذي يعمل عليه هذا الجهاز، **يمكننا استخدام Nmap بالأمر التالي:**

```
mathematica
nmap -O 192.168.1.1
```

عند تشغيل هذا الأمر، سيقوم Nmap بفحص الجهاز الموجود على عنوان IP المعطى ومحاولة تحديد نوع نظام التشغيل المستخدم، بعد اكتمال الفحص، ستظهر Nmap تقديرًا لنوع نظام التشغيل.

على سبيل المثال: إذا كان الجهاز يستخدم نظام تشغيل Linux، فقد تظهر نتيجة مشابهة للتالية:

```
Running: Linux 2.6.X
```

أو إذا كان الجهاز يستخدم نظام تشغيل Windows، **فقد تظهر نتيجة مشابهة للتالية :**

```
Running: Microsoft Windows XP
```

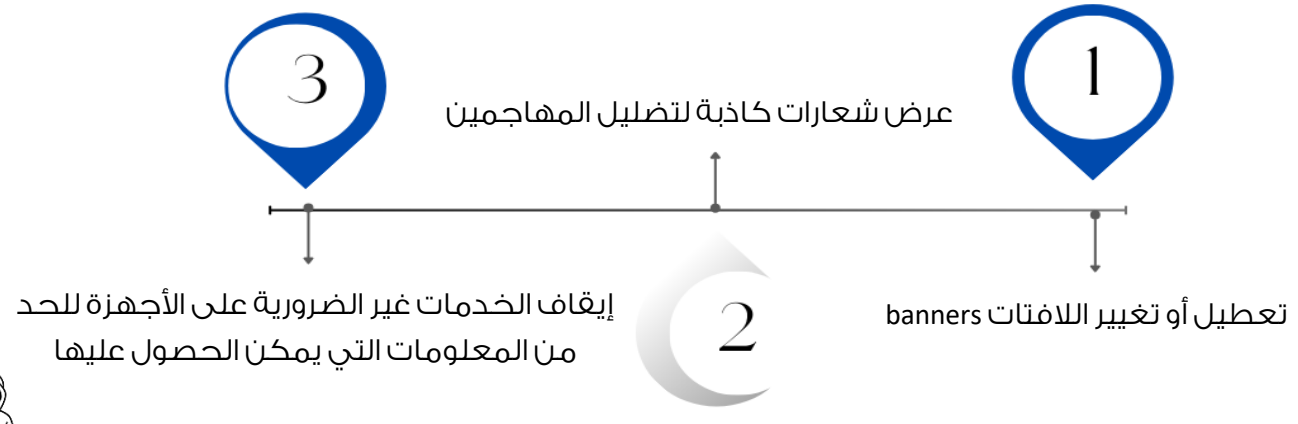
هذا المثال بسيط ويوضح كيفية استخدام Banner Grabbing لتحديد نوع نظام التشغيل باستخدام Nmap.

- **تذكر** دائماً أنه يجب استخدام هذه الأدوات بشكل قانوني وفي سياق اختبار الأمان أو بموافقة صاحب الجهاز.

٢. أنظمة التشغيل.

٣. إصدار التطبيقات المستخدمة من قبل الجهاز المستهدف مع مساعدة المعلومات التي تم جمعها فالمخترق يستغل الثغرات الأمنية التي لم يتم تحديثها من قبل تصحيحات الأمان Security patches ومن ثم إطلاق هجماته.

- **التدابير المضادة**



- **Telnet**

يعتبر من بروتوكولات TCP/IP للاتصال بأجهزة الحاسب البعيدة، كما أنه تطبيق من تطبيقات TCP/IP يتم استخدامه قي تشغيل برامج Telnet لكي يتم استخدام الحاسب بطريقة فعالة يتم الاتصال باستخدام تطبيق telnet الموجود على جهاز المتصل بالاتصال بتطبيق Telnet الموجود على الجهاز (الهدف)، وهو يعمل كبرنامج محاكاة يتم إرسال أي أوامر يقوم المتصل بكتابتها عبر الشبكة لكي يتم تنفيذها من قبل جهاز الحاسب البعيد.

- **لتشغيل telnet**

- Start /Run
- ثم كتابة telnet

- **Nbstat**

هي أداة تعرض قائمة بالاتصالات النشطة.

- **nbtstat في كالي لينكس**

الأمر nbtstat خاص بأنظمة Windows وغير موجود في Linux ، ومع ذلك، هناك أدوات بديلة متاحة في Kali Linux لوظائف مماثلة ، إحدى هذه الأدوات هي nbtscan، والتي تُستخدم لفحص خوادم أسماء NetBIOS على شبكة TCP/IP محلية أو بعيدة.

- **فيما يلي بعض التفاصيل حول nbtscan الأداة:**

- **استخدامها**

١	nbtscan هو برنامج مجاني يمكن استخدامه وتوزيعه وتعديله بموجب شروط GNU GPL 2+.
٢	يمكن استخدامه لفحص مجموعة من عناوين IP، ويوفر معلومات حول أسماء أجهزة كمبيوتر NetBIOS والخدمات المتاحة وأسماء المستخدمين الذين تم تسجيل دخولهم وعناوين MAC للأجهزة المقابلة.
٣	يمكن للأداة إنتاج تقارير تحتوي على عناوين IP ومعلومات اسم NetBIOS، والتي يمكن أن تكون مفيدة في اختبار الاختراق.

- مميزاتها

- **إخراج مطول:** يوفر جميع الأسماء المستلمة من كل مضيف.
- **تفريغ الحزم:** طباعة محتويات الحزمة بالكامل.
- **تنسيق الإخراج:** يمكن تنسيق الإخراج بتنسيق /etc/hosts أو lmhosts.
- **المهلة وعرض النطاق الترددي:** يسمح بتعيين مهلة الانتظار وتقييد الإخراج.
- **مخرجات متوافقة مع البرنامج النصي:** توفر مخرجات متوافقة مع البرنامج النصي بدون رؤوس الأعمدة والسجلات.

- **بعض الأمثلة على كيفية استخدام nbstat**

- عرض قائمة بالجهاز المحلي

يمكنك استخدام nbstat دون أي معلومات لعرض قائمة بالجهاز المحلي والاتصالات النشطة في شبكة NetBIOS , **يتم ذلك بالأمر التالي:**

```
nbstat
```

- عرض معلومات حول مستخدم محدد

يمكنك استخدام nbstat لعرض معلومات حول مستخدم محدد في الشبكة، على سبيل المثال، إذا كان اسم المستخدم هو "user1"، **يمكنك استخدام الأمر التالي:**

```
nbstat -a user1
```

- عرض قائمة بالموارد المشتركة في الشبكة

يمكنك استخدام nbstat لعرض قائمة بالموارد المشتركة في الشبكة، **يتم ذلك بالأمر التالي:**

```
nbstat -S
```

- **عرض إحصائيات الجدول المفتوح (Open Table Statistics):**

يمكنك استخدام nbstat لعرض إحصائيات الجدول المفتوح للاتصالات NetBIOS , **يتم ذلك بالأمر التالي:**

```
nbstat -n
```

هذه بعض الأمثلة على كيفية استخدام nbstat في نظام التشغيل Windows يرجى ملاحظة أن يجب تشغيل nbstat في سطر الأوامر في نظام Windows.

- **تثبيتها**

للتثبيت nbtscan على كالي لينكس، **يمكنك استخدام الأمر التالي:**

```
sudo apt install nbtscan
```

من المهم ملاحظة أنها nbtscan أداة قيمة لتعداد الشركات الصغيرة والمتوسطة وتدقيق أمان الشبكة، خاصة في بيئات Windows ومع ذلك، فمن الضروري استخدامها بطريقة مسؤولة، لأن استخدام هذه الأداة قد يولد قدرًا كبيرًا من حركة المرور، والتي يمكن تسجيلها بواسطة الأجهزة المستهدفة.

باختصار، على الرغم من أن nbtstat الأمر خاص بأنظمة Windows، فإن Kali Linux يوفر nbtscan الأداة كبديل لوظائف مماثلة في بيئات Linux.

بعد التثبيت، يمكنك استخدام nbtscan لفحص الشبكات للحصول على معلومات حول أسماء NetBIOS المشتركة والمستخدمين المسجلين الدخول، يمكنك استخدام الخيارات المختلفة مثل –h لطباعة أسماء بشرية للخدمات و –m لعدد إعادة الإرسال.

يمكنك أيضًا استخدام nbtscan لفحص نطاق محدد من العناوين IP أو مجموعة من العناوين، **على سبيل المثال:**

```
nbtscan -r 192.168.1.0/24
```

- **Superscan**

أداة Superscan تقوم بفحص المنافذ للاتصال القائم على TCP& Pinger وترجمة اسم المضيف وفحص نطاق IP مع خاصية التعدد وتقنيات غير متزامنة.

- **مميزاتها**

- دعم لنطاقات IP غير محدودة
- الكشف عن المضيف باستخدام أساليب ICMP متعددة
- فحص منافذ المصدر UDP
- ترجمة اسم المضيف Hostname resolving
- القدرة على التعداد لمضيف الويندوز
- فحص منافذ المصدر
- إنشاء تقرير بسيط HTML

- **Snmp Enumeration**

تعداد SNMP هو عملية تعداد حسابات المستخدمين والأجهزة الموجودة على جهاز حاسب تم تمكين SNMP فيه، تأتي خدمة SNMP مع كلمتي مرور، يتم استخدامهما لتكوين وكيل SNMP والوصول إليه من محطة الإدارة.

- **Netscan Tool Pro**

هو أداة للتحقيق يسمح باكتشاف الأخطاء والرصد والكشف عن الأجهزة الموجودة على الشبكة وعناوين IP والمنافذ **وباستخدام هذه الأداة يمكن إيجاد نقاط الضعف فهو يؤدي الفحوصات التالية على الشبكة:**

- رصد أجهزة الشبكة المتاحة.
- معرفة عناوين IP واسم الأجهزة والمجال والمنافذ.
- كما أنه يسمح باختبار عملية إرسال البريد الإلكتروني من خلال SMTP .

- **اختبار اختراق التعداد**

من خلال عملية التعداد فإن المخترق يقوم بجمع المعلومات المهمة عن المنظمة إذا كان مستوى الأمن ضعيف فمن المحتمل أن تواجه خسائر مالية نتيجة تسرب المعلومات يتم إجراء تعداد اختبار الاختراق بمساعدة المعلومات التي تم الحصول عليها من عمليات الاستطلاع ، يجب أن يقوم مُختبر الاختراق بإجراء الأساليب الممكنة من عمليات التعداد لضمان النطاق الكامل للاختبار **مثل:**

١. البحث في نطاق الشبكة
٢. حساب قناع الشبكة
٣. اكتشاف المضيف
٤. فحص المنافذ
٥. إجراء تعداد DNS
٦. إجراء تعداد SNMP
٧. إجراء تعداد LDAP
٨. إجراء التعداد NTP
٩. توثيق نتائج الاختبار وتحليل واقتراح التدابير المضادة لتحسين أمن المنظمة.

❖ التدابير المضادة والحماية من عمليات الفحص والتعداد

بتجنب تسرب المعلومات من خلال SNMP& DNS& SMTP & LPDA

١. إزالة SNMP أو إيقاف تشغيل الخدمة SNMP من النظام.

٢. تحديث إصدارات SNMP.

٣. تنفيذ الاختيار الأمني نهج المجموعة.

٤. تقييد الوصول إلى null session pipes & null session share وتصفية IPSEC.

٥. التشفير والمصادقة IPSEC.

٦. منع الوصول إلى المنافذ ١٦١.

٧. إعداد كافة أسماء الخوادم بعدم السماح للقيام بعملية نقل منطقة DNS إلى مضيفين.

٨. التأكد من أن ملفات المنطقة DNS لا تحتوي على HINFO.

٩. تعطيل خدمة Server Message Block (SMB) و هي خدمة تهدف إلى توفير الوصول المشترك إلى الملفات و المنافذ التسلسلية و الطابعات و الاتصال بين العقد على الشبكة.

١٠. تحديد اسم مستخدم مختلف عن عنوان البريد الإلكتروني الخاص بع وتمكين تأمين الحساب.

١١. استخدام تكنولوجيا SSL لتشفير حركة مرور LDAP.

١٢. استخدام المصادقة الأصلية لتقييد الوصول إلى المستخدمين المصرح لهم فقط.

١٣. ضبط إعدادات خادم SMPT بحيث تتجاهل رسائل البريد الإلكتروني لغير المصرح لهم، استجابات البريد الإلكتروني لا تشمل معلومات خادم البريد ومعلومات المضيف المحلي.

١٤. تنفيذ أدوات مراقبة الشبكة للكشف عن أنشطة المسح المشبوهة أو عمليات فحص المنافذ.

١٥. مراقبة السجلات وتحليلها بانتظام بحثًا عن محاولات الوصول غير العادية أو غير المصرح بها.

١٦. تثقيف الموظفين حول أهمية حماية المعلومات الحساسة والحذر عند مشاركتها عبر الإنترنت.

١٧. تنفيذ جدران الحماية وأنظمة كشف التسلل (IDS) لمنع أو التنبيه بشأن نشاط الشبكة المشبوه.

تمارين الفصل الثالث

١. **اختار الإجابة الصحيحة فيما يلي:**

١. **# hping3 192.168.12.60 S C 1 P 25 الجملة تستخدم لـ**

أ- المسح التعداد
ب- التنصت
ت- التحميل
ث- المضادات للاختراق

٢. **استخدام تكنولوجيا SSL لتشفير حركة مرور .....**

أ- LDPA
ب- **LDAP**
ت- LAPD
ث- APDL

٣. **اهم مميزات Hping 3**

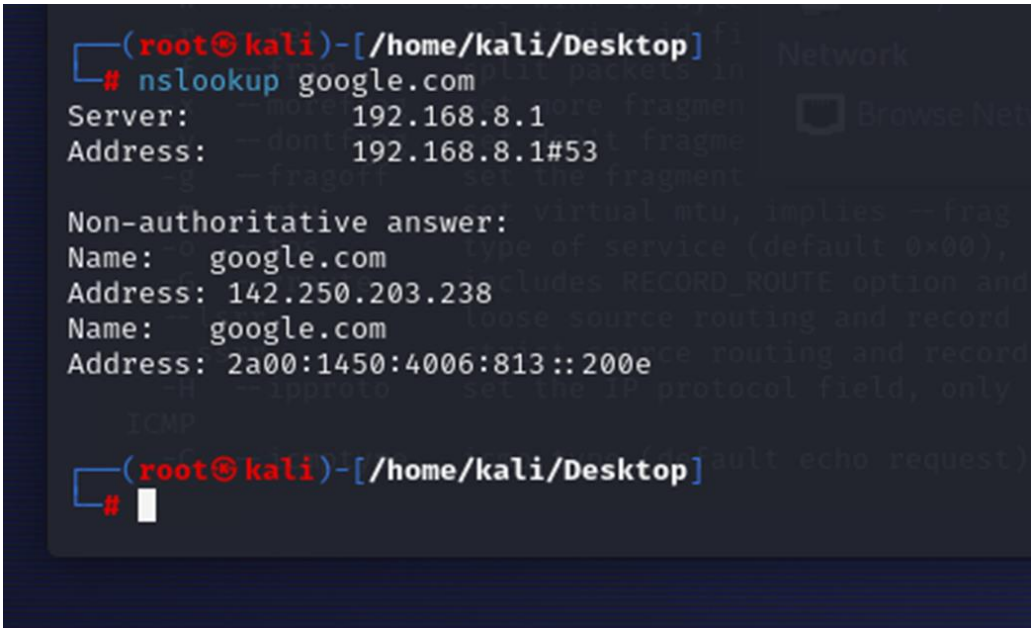
أ- فحص منافذ الشبكة
ب- فحص منافذ الأسلاك
ت- فحص التيمنان
ث- فحص النسخ للنظام

٢. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

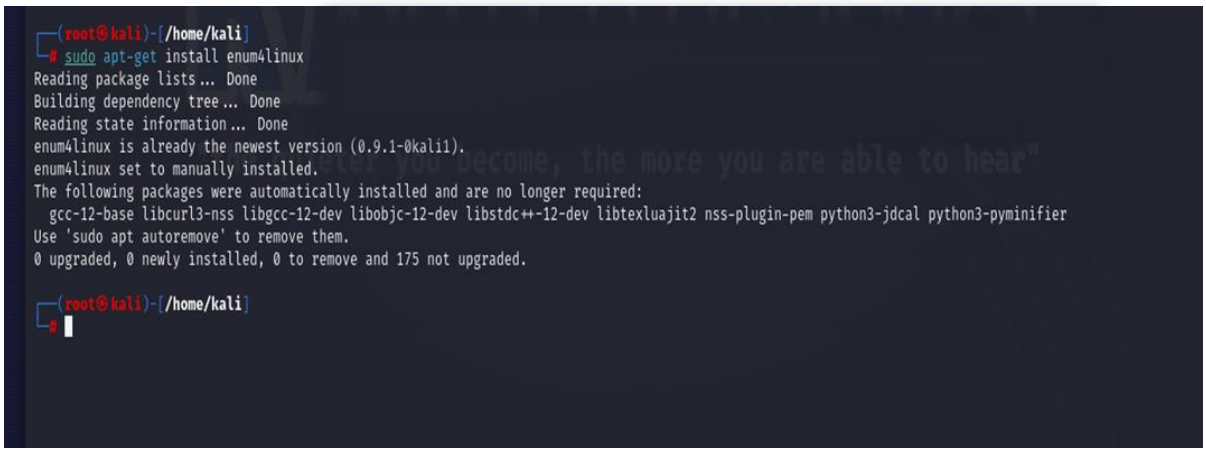
١.	بعد جمع المعلومات لا يستطيع المخترق الوصول إلى أي حاسب آلي بعيد واختراقه إلا إذا كان هذا الحاسب متصلا	√
٢.	يتم التعرف على الأنظمة المتصلة والقابلة للوصول عبر الإنترنت من خلال إرسال إشارة اتصال إلى عنوان IP للحاسب الهدف وفي حال إذا استجاب الحاسب الهدف لهذه الرسالة فسيعرف إن هذا الحاسب متصل وفعال	√
٣.	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 يلاحظ المخترق ويحلل الشبكة ليحصل على المعلومات المطلوبة لبناء استراتيجية الهجوم هو فحص المنفذ	×
٤.	لا يمكن استكشاف الثغرات لأن المخترق سيبني الهجوم على أساس نقاط الضعف في نظام التشغيل	×
٥.	لمسح نطاق IP محدد نستخدم الامر makdir	×

٣. طبق ما يلي عمليا:

١. استخدم الأمر **Nslookup** للاستعلام عن خوادم **DNS** لاسترداد معلومات حول أسماء النطاقات وعناوين **IP** وسجلات **DNS** الأخرى.



٢. استخدم الأمر (**enum4linux**) لتعداد المعلومات من أنظمة **Windows** و **Samba** ولاستخراج معلومات المستخدم والمجموعة من دلائل **LDAP**.



الفصل الرابع

التصنت والتهرب Sniffing and Evasion

في هذا الفصل سنتعرف على المواضيع التالية:

- التصنت Sniffing
- التصنت الإيجابي والسلبي
- بروتوكولات
- أدوات وتقنيات التصنت Sniffing (عملي)
- التقنيات والأدوات
- تهرب Evasion
- تقنيات التهرب وأنواعها
- الأجهزة المضادة
- Snort
- Firewall
- التدابير المضادة والحماية من عمليات التصنت والتهرب

❖ التصنت Sniffing

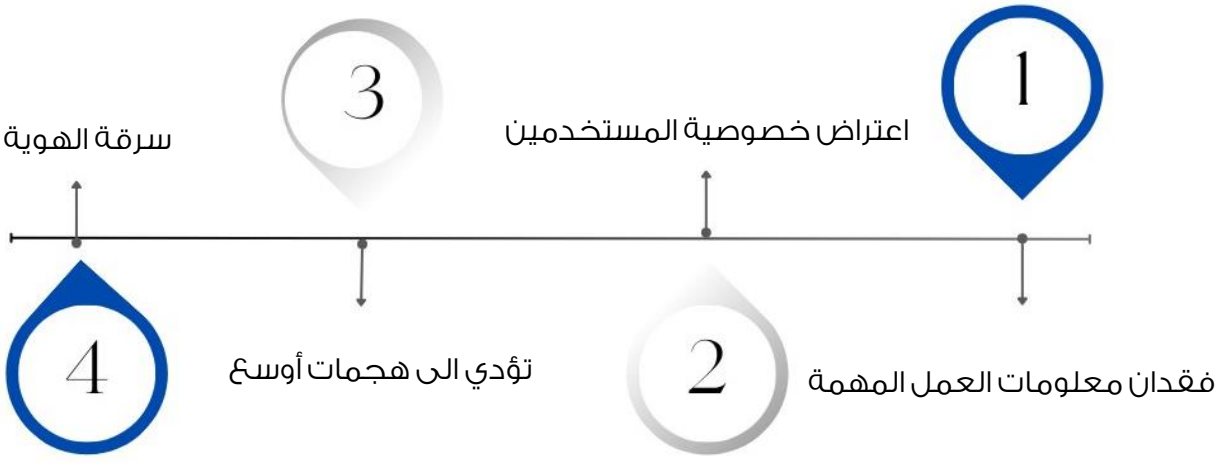
فهو عملية مراقبة والتقاط جميع الحزم التي تمر عبر شبكة معينة باستخدام أدوات التصنت، إذا كانت مجموعة من منافذ التبديل الخاصة بالمؤسسة مفتوحة، فيمكن لأحد موظفيها التعرف على حركة مرور الشبكة بالكامل.

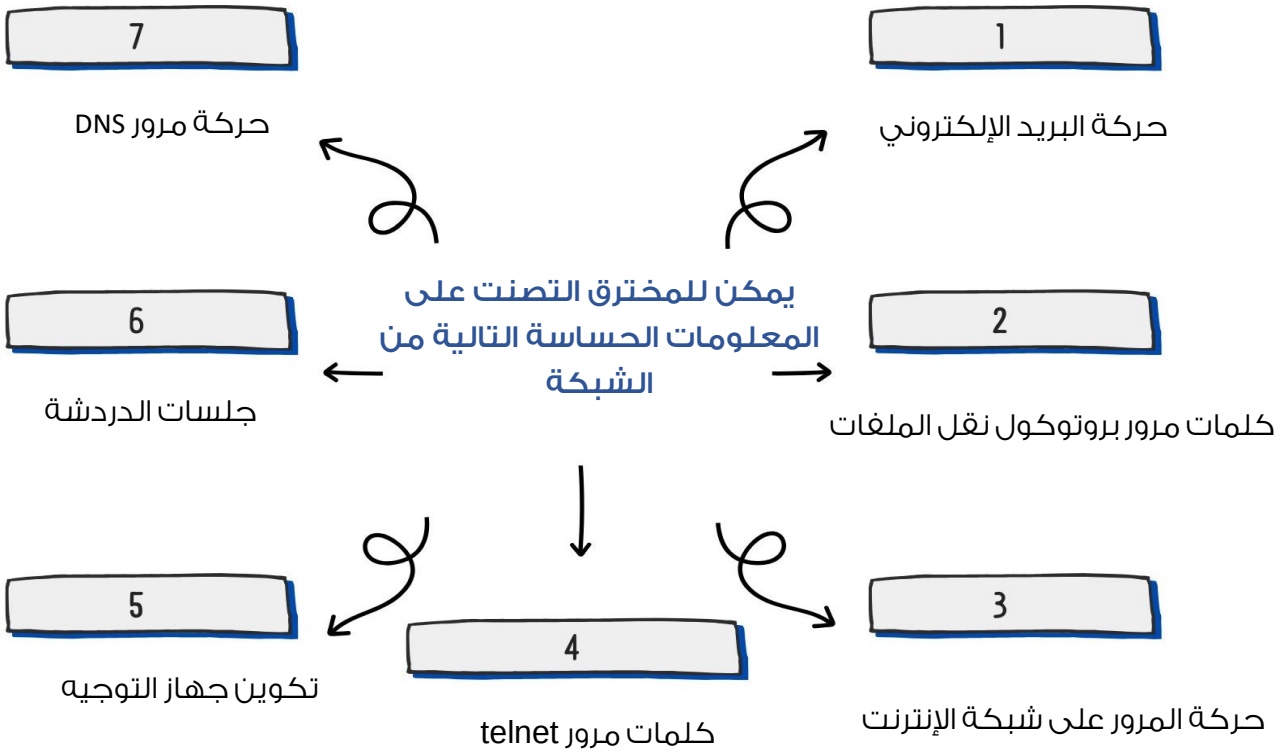
يمكن لأي شخص في نفس الموقع الفعلي الاتصال بالشبكة باستخدام كابل Ethernet أو الاتصال لاسلكيًا بتلك الشبكة والتصنت إجمالي حركة المرور.

بمعنى آخر، يسمح Sniffing برؤية جميع أنواع حركة المرور، سواء كانت محمية أو غير محمية، في الظروف المناسبة ومع وجود البروتوكولات الصحيحة، قد يتمكن الطرف المهاجم من جمع المعلومات التي يمكن استخدامها لمزيد من الهجمات أو التسبب في مشكلات أخرى لمالك الشبكة أو النظام.

وهو برنامج يقوم برصد البيانات المارة عبر شبكة الاتصال حيث يتم وضع Packet sniffer على الشبكة في الوضع promiscuous حتى يمكن التقاط وتحليل كل حركة مرور الشبكة وسرقة المعلومات من خلال التصنت عليها.

- **يمكن أن تؤدي هجمات التنصت إلى التالي:**





- **طريقة عمل التصنت**

عادةً ما يقوم المُتصنت بتحويل بطاقة واجهة الشبكة (NIC) الخاصة بالنظام الهدف إلى الوضع المختلط promiscuous بحيث يستمع إلى جميع البيانات المرسلة.

يشير الوضع المختلط إلى الطريقة الفريدة لأجهزة Ethernet، على وجه الخصوص، بطاقات واجهة الشبكة (NIC)، التي تسمح لبطاقة NIC باستقبال كل حركة المرور على الشبكة، حتى لو لم تكن موجهة إلى بطاقة NIC هذه ، افتراضيًا، تتجاهل بطاقة NIC كل حركة المرور غير الموجهة إليها، ويتم ذلك عن طريق مقارنة عنوان الوجهة لحزمة Ethernet مع عنوان الجهاز (المعروف أيضًا باسم MAC) الخاص بالجهاز ، في حين أن هذا منطقي تمامًا بالنسبة للشبكات، إلا أن الوضع غير المختلط يجعل من الصعب استخدام برامج مراقبة وتحليل الشبكة لتشخيص مشكلات الاتصال أو محاسبة حركة المرور ، يمكن للمتصنت مراقبة كل حركة المرور إلى جهاز الحاسب بشكل مستمر من خلال بطاقة واجهة الشبكة (NIC) عن طريق فك تشفير المعلومات المغلفة في حزم البيانات.

❖ التصنت الإيجابي والسلبي

يوجد نوعين من التصنت هما:

١. التصنت الإيجابي

في عملية التصنت الإيجابي، لا يتم غلق حركة المرور ومراقبتها فحسب، بل يمكن أيضًا تغييرها بطريقة ما وفقًا 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.

أي في يتم فحص عناوين المصدر والواجهة لحزم البيانات من قبل المحولات ومن ثم نقلها إلى الوجهة المناسبة مما يصعب عملية التصنت فيلجأ المهاجمون في التصنت الإيجابي بحقن حزم في حركة المرور للتصنت على الشبكة.

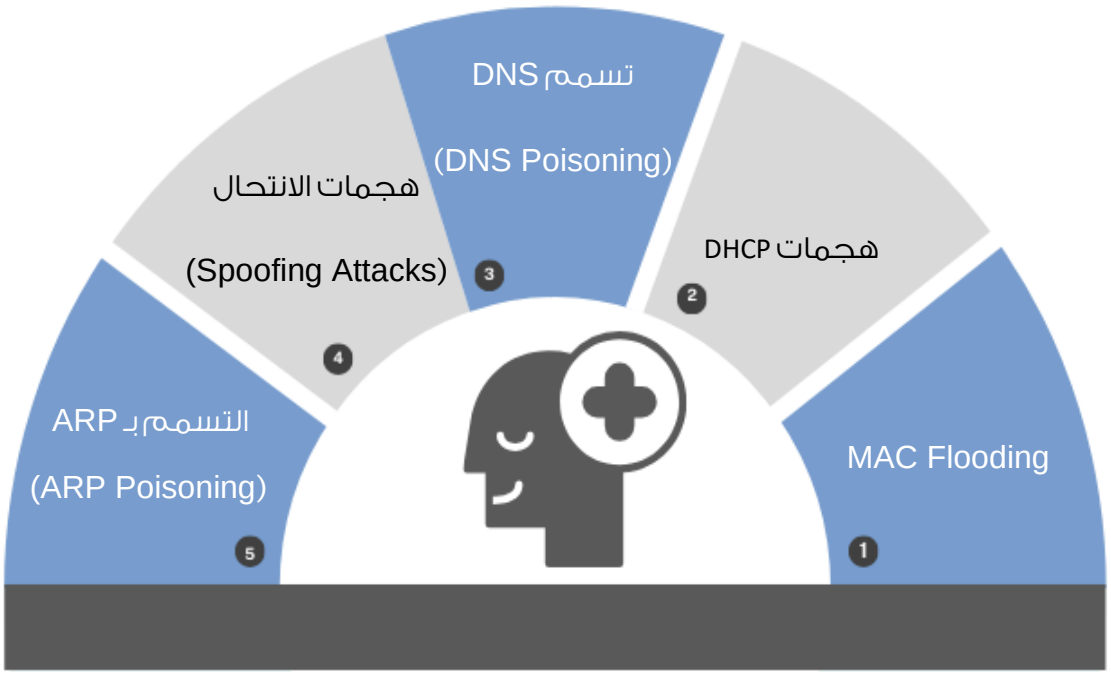
- **أنواع هجوم التصنت**

MAC Flooding	هو نوع من هجوم التصنت التي تغرق شبكة المبدلات بفيضانات من حزم البيانات وهي تقطع تدفق البيانات المعتادة بين المرسل والمستقبل الذي هو مشترك مع عناوين MAC بدلا من تمريرها من المرسل إلى المستقبل فإنها تخرج من كل المنافذ، يُمكن المهاجمين من مراقبة بيانات الشبكة، يمكن استخدام الأداة MAC flooding Tool Scapy .
DNS Poisoning	هي العملية التي يتم فيها إعادة توجيه المستخدم إلى موقع مزيف من خلال توفير بيانات وهمية إلى خادم DNS الموقع.
ARP Poisoning	هو الهجوم الذي يحاول فيه المهاجم ربط عنوان MAC الخاص به مع عنوان IP الضحية لكي يتم إرسال حركة المرور إلى عنوان IP ما إلى المهاجم. الأدوات ARP Poisoning Tool تستخدم في التصنت على كلمات المرور ورسائل البريد الإلكتروني وهي مصممة لالتقاط الحزم التي تمر عبر الشبكة واعتراض رسائل البريد الإلكتروني.

- **أنواع هجوم التصنت**

DHCP Attacks	**يوجد نوعين:** – DHCP STARVATION : وهي عملية مهاجمة خادم DHCP عن طريق إرسال كمية كبيرة من الطلبات. – Rogue DHCP Server Attack : يقوم المهاجم بتثبيت Rogue DHCP Server لانتحال صفة خادم DHCP مصرح به على الشبكة Rogue DHCP Server، ويبدأ تشغيل Rogue Server لمعالجة طلبات عملاء DHCP من أجل الحصول على إعدادات الشبكة باستخدام الأداة الموجودة في كالي لينكس Yersinia.
Password Sniffing	هو طريقة تستخدم لسرقة كلمات السر من خلال رصد حركة المرور التي تنتقل عبر الشبكة وبعدها يمكن للمهاجم السيطرة على الشبكة والوصول لحسابات المستخدمين.
Spoofing Attack	انتحال المهاجم لبيانات مستخدم أخر للوصول إلى موارد مقيدة MAC Spoofing Tool وهي أداة تسمح بتغيير عناوين MAC لأي بطاقة شبكة ويسمح باستعادة عنوان MAC الأصلي.

- **تقنيات التصنت الإيجابي**



٢. التصنت السلبي

في التصنت السلبي، يتم غلق حركة المرور، ولكن لا يتم تغييرها بأي شكل من الأشكال، التصنت السلبي يسمح بالاستماع فقط، لا يرسل حزم، بل يكتفي المُتصنت بالتقاط ومراقبة الحزم المُرسلة من الآخرين، ويعمل مع أجهزة Hub على جهاز المحور، يتم إرسال حركة المرور إلى جميع المنافذ، في الشبكة التي تستخدم لوحات الوصل لتوصيل الأنظمة، يمكن لجميع المضيفين على الشبكة رؤية حركة المرور، ولذلك، يمكن للمهاجم بسهولة التقاط حركة المرور من خلاله.

المحاور أصبحت قديمة تقريبًا في الوقت الحاضر، تستخدم معظم الشبكات الحديثة المحولات، وبالتالي، تزيل خطر التصنت السلبي، ولكن المحولات لاتزال عرضة للتصنت الإيجابي.

ممكن عن طريق التصنت السلبي

تثبيت حصان طروادة مع قدرات التصنت المدمجة معها على الجهاز (الهدف) لاختراقه وبمجرد الاختراق يمكن التصنت.

اختراق الشبكة (الهدف) ودمج جهاز المخترق في شبكة المنظمة (الهدف) وحينها يمكنه التقاط المعلومات المهمة عن المنظمة.

❖ بروتوكولات

لا يوجد أمان كامل في تصميم البروتوكولات وعادة يتم التصنت على هذه البروتوكولات للحصول على كلمة السر مثل البروتوكول Telnet مع التصنت يمكن للمهاجم التصنت على ضربات المفاتيح ومعرفة ما تم كتابته بما في ذلك اسم المستخدم وكلمة المرور المستخدمة، بروتوكول FTP يرسل كلمات المرور والبيانات في نص واضح عبر الشبكة وبالمثل في البروتوكولات POP& IMAP&HTTP

- **Arp**

Address Resolution Protocol بروتوكول تحليل العنوان (ARP) هو بروتوكول عديم الحالة يُستخدم لتحليل عناوين IP إلى عناوين MAC للجهاز، تقوم جميع أجهزة الشبكة التي تحتاج إلى الاتصال بالشبكة ببث استعلامات ARP في النظام لمعرفة عناوين MAC الخاصة بالأجهزة الأخرى، يُعرف تسمم ARP أيضًا باسم ARP Spoofing.

- **كيفية عمل ARP**

١. عندما يحتاج جهاز ما إلى الاتصال بجهاز آخر، فإنه يبحث عن جدول ARP الخاص به.

٢. إذا لم يتم العثور على عنوان MAC في الجدول، فسيتم بث طلب ARP_request عبر الشبكة.

٣. ستقوم جميع الأجهزة الموجودة على الشبكة بمقارنة عنوان IP هذا بعنوان MAC.

٤. إذا قام أحد الأجهزة الموجودة في الشبكة بتعريف هذا العنوان، فسوف يستجيب لطلب ARP_request بعنوان IP وMAC الخاص به.

٥. سيقوم الكمبيوتر الطالب بتخزين زوج العناوين في جدول ARP الخاص به وسيتم إجراء الاتصال.

- **انتحال ARP (ARP Spoofing)**

- يمكن تزوير حزم ARP لإرسال البيانات إلى جهاز المهاجم.
- يقوم انتحال ARP بإنشاء عدد كبير من طلبات ARP المزورة وحزم الرد لزيادة التحميل على المحول.
- يتم تعيين المفتاح في وضع إعادة التوجيه وبعد امتلاء جدول ARP باستجابات ARP المخادعة، يمكن للمهاجمين التعرف على جميع حزم الشبكة.
- يقوم المهاجمون بإغراق ذاكرة التخزين المؤقت لـ ARP للكمبيوتر المستهدف بإدخالات مزورة، وهو ما يُعرف أيضًا باسم التسمم، يستخدم تسميم ARP وصول Man-in-the-Middle لتسميم الشبكة.

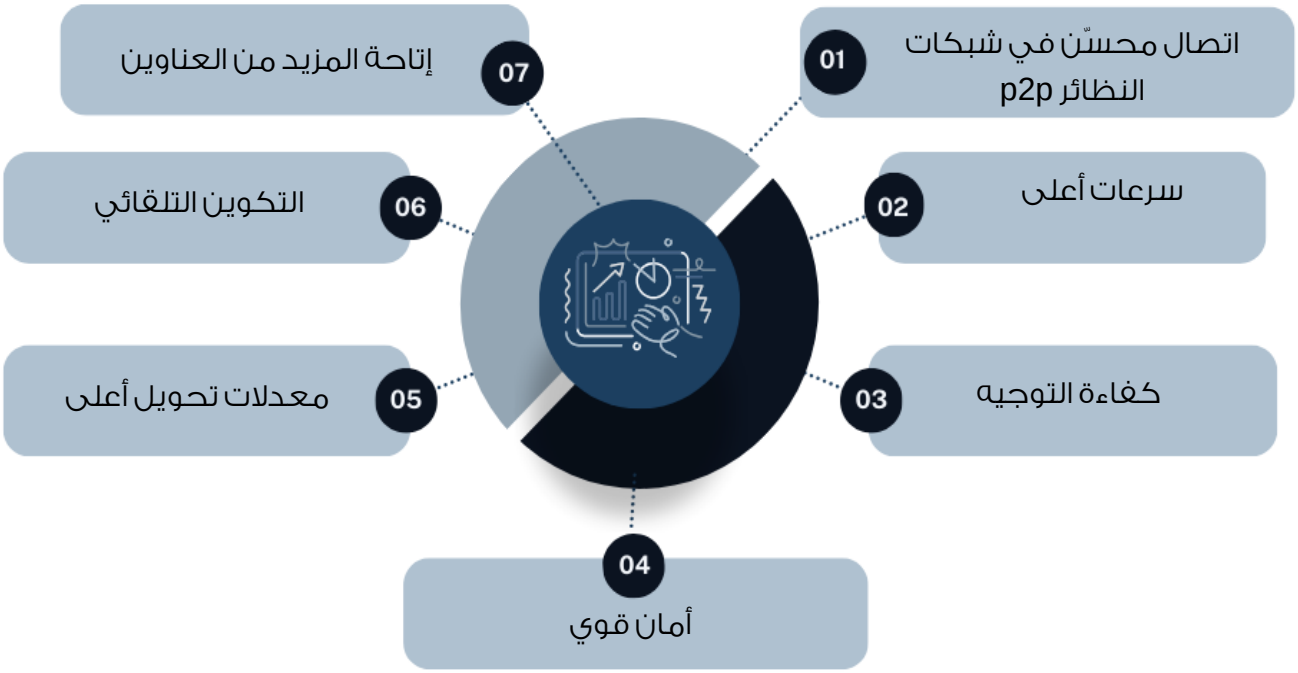
- **IPV6**

هو أحد إصدارات بروتوكول الإنترنت (IP) الذي يوفر مساحة عناوين IP أكبر لمستخدمي الإنترنت، هذا الإصدار يستخدم ١٢٨ بت للعنوان الواحد وبالتالي توفير عدد كبير من العناوين مما يعطي مساحة كبيرة لتوسيع التطبيقات المرتبطة بشبكة الإنترنت.

IPv6 هو عنوان من 128بت يحتوي على ثمانية خانات من أربعة أرقام مفصولة بنقطتين.

العنوان النموذجي يبدو كالتالي: 2018:0ab6:84a2:0000:0000:7a2b:0271:7435

- **مزايا IPv6**



❖ أدوات وتقنيات التصنت Sniffing

يمكن للمتصنت استخدام أي من أدوات التصنت هذه لتحليل حركة المرور على الشبكة وتحليل المعلومات:

1	2	3	4
تقنية MAC flooding	تقنية DHCP Attacks	تقنية ARP Poisoning	تقنية MAC Spoofing / Duplicating

❖ التقنيات والأدوات

يتم استخدام تقنية تحليل الشبكة وهو عملية تحليل المرور داخل الشبكة لتحديد مشاكل الأداء وتحديد الاختراقات الأمنية وتحليل بروتوكولات الشبكة وتحتاج الفهم السليم لبروتوكول الاتصال TCP/IP ومعرفة تركيب هياكل الحزم وكيفية تدفقها وكيفية تطبيق المرشحات للتركيز على حركة المرور المطلوبة وتحديد الحالات الغير عادية في حركة مرور الرزم باستخدام أدوات مثل Wireshark – TCP dump.

- **Wireshark**

إنها واحدة من أكثر أدوات التصنت على الحزم المعروفة والمستخدمة على نطاق واسع، فهو يقدم عدداً هائلاً من الميزات المصممة للمساعدة في تشريح وتحليل حركة المرور.

- **TCP dump**

وهو محلل حزم سطر الأوامر المعروف، فهو يوفر القدرة على اعتراض ومراقبة TCP/IP والحزم الأخرى أثناء الإرسال عبر الشبكة.

❖ تهرب Evasion

التهرب هو تجاوز دفاع تجاوز أنظمة الحماية والأمان من أجل تقديم استغلال أو هجوم أو أي شكل آخر من أشكال البرامج الضارة إلى شبكة أو نظام مستهدف، دون اكتشافه ويعد خطر جدا على الشبكة.

❖ تقنيات التهرب وأنواعها

1

تقنية استخدام تجزئة حزم التحقق على أن يتم جمعها مرة أخرى في حزمة واحدة بمجرد وصولها للجهاز الهدف.

2

استخدام تقنية توجيه المصدر هي تقنية يستطيع المهاجم تحديد الطريق المطلوب أن تتخذه الحزمة من خلال مخطط الشبكة وتحديد أفضل مسار.

3

تقنية التشفير لتمرير البرامج الضارة عبر أنظمة الحماية والتحليل الأمني دون الكشف عنها.

4

تقنيات تغيير خصائص البرامج الضارة لتجنب اكتشافها بواسطة الحلول الأمنية التي تعتمد على التوقيعات.

5

يستخدم المخترقون تقنيات التهرب هذه لتجاوز أنظمة مكافحة الفيروسات التقليدية وأنظمة كشف التسلل.

❖ الأجهزة المضادة

يتم تركيب الأجهزة المضادة من أجل تعزيز أمن المنظمة الهدف **باستخدام:**

١. أنظمة كشف التطفل IDSs

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 tools وواجهات التواصل مع مديري الأنظمة interfaces ، تجمع الحساسات البيانات وأنشطة المستخدمين وترسلها لأدوات التحليل وتحلل أدوات التحليل البيانات والأحداث الواردة إليها من الحساسات وعند وجود أي نتائج ترسل إلى واجهات التواصل مع مديري الأنظمة لإخطارهم بوجود شيء مريب و غير طبيعي .

٢. أنظمة منع التطفل Intrusion Prevention Systems IPSs

تكشف البيانات والأنشطة غير الطبيعية ثم تمنعها من الوصول إلى أهدافها فهي تقوم بخطوات استباقية لمنع المتطفل من الوصول إلى أهدافه وتقطع الاتصال وتوقف عمل الأجهزة في حالة وجود بيانات أو أنشطة مريبة على الشبكة.

٣. الشبكة الافتراضية الخاصة VPN

توفّر الشبكة الافتراضية الخاصة، أو ما يُعرَف بـــ VPN ، اتصالاً مشفّراً عبر الإنترنت من جهاز إلى شبكة، ويساهم هذا الاتصال المشفّر في توفير نقل آمن للبيانات الحساسة عبر الشبكة، وكذلك السماح للمستخدمين بالعمل عن بعد مع مؤسساتهم، حيث إنها تضمن منع التنصت على حركة المرور من قبل الأشخاص غير المصرح لهم بالدخول إلى الشبكة، لضمان خصوصية وسلامة المعلومات الحساسة من خلال المصادقة متعددة العوامل وفحص الامتثال لنقطة النهاية وتشفير جميع البيانات المرسلة.

❖ Snort

هو جهاز تسلل للحزم يفحص كل حزمة عن لاكتشاف حالات مشبوهة.

❖ Firewall

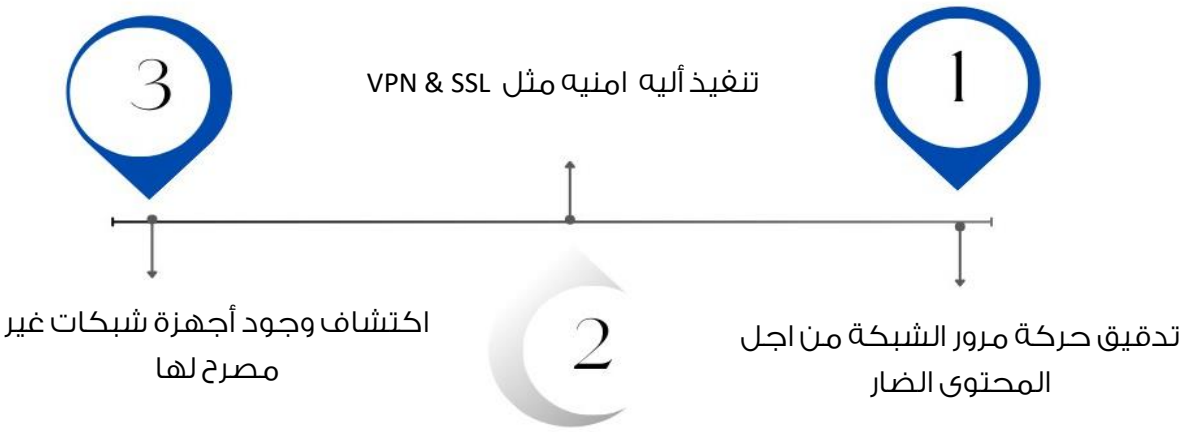
جدار الحماية هو جهاز أمان للشبكة يراقب حركة مرور الشبكة الواردة والصادرة ويقرر ما إذا كان سيتم السماح بحركة مرور معينة أو حظرها بناءً على مجموعة محددة من قواعد الأمان، كانت جدران الحماية بمثابة خط الدفاع الأول في أمن الشبكات فهي تنشئ حاجزًا بين الشبكات الداخلية الآمنة والخاضعة للرقابة والتي يمكن الوثوق بها والشبكات الخارجية غير الموثوق بها، مثل الإنترنت.

❖ التدابير المضادة والحماية من عمليات التصنت والتهرب

- تقييد الوصول الفعلي إلى وسائط الشبكة لضمان عدم إمكانية تثبيت Packet Sniffer.
- استخدام التشفير لحماية المعلومات السرية.
- إضافة عنوان MAC بشكل دائم للعبارة Gateway إلى ذاكرة التخزين المؤت ARP .
- استخدام عناوين IP ثابتة وجداول ARP ثابتة لمنع المهاجمين من إدخالات ARP المنتحلة للأجهزة على الشبكة.
- استخدام HTTPS بدلا من HTTP لحماية أسماء المستخدمين وكلمات المرور.
- إيقاف بث تحديد الشبكة (Network identification broadcasts) وتقييد الشبكة للمستخدمين المرخص لهم من أجل حماية الشبكة من أن يتم اكتشافها من أدوات sniffing واستخدام الإصدار Ipv6 بدلا من الإصدار Ipv4 .
- استخدام الـ switch بدلا من hub.
- استخدام كلمات المرور على المجلدات والخدمات المشتركة.
- تشفير التواصل بين جهاز الحاسب ونقطة الوصول اللاسلكية لمنع انتحال MAC
- استخدام جلسات مشفرة مثل SSH بدلا من Telnet والنسخ الآمن SCP بدلا من FTP ، SSL للاتصالات والبريد الإلكتروني لحماية المستخدمين.
- استخدام البروتوكول SSL/TLS.
- استخدام one-time passwords(OTPS).
- استخدام IP security.
- استخدام أدوات antisniff اللازمة لتحديد إذا ما كانت بطاقات الشبكة NIC تعمل في الوضع promiscuous mode.
- استرداد MAC مباشرةً من NIC بدلا من نظام التشغيل و هذا يمنع انتحال عنوان MAC.

- **أهداف اختبار اختراق التصنت**

تحديد ما إذا كانت الشبكة عُرضة لأي نوع من التصنت Sniffing بإجراء:



١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

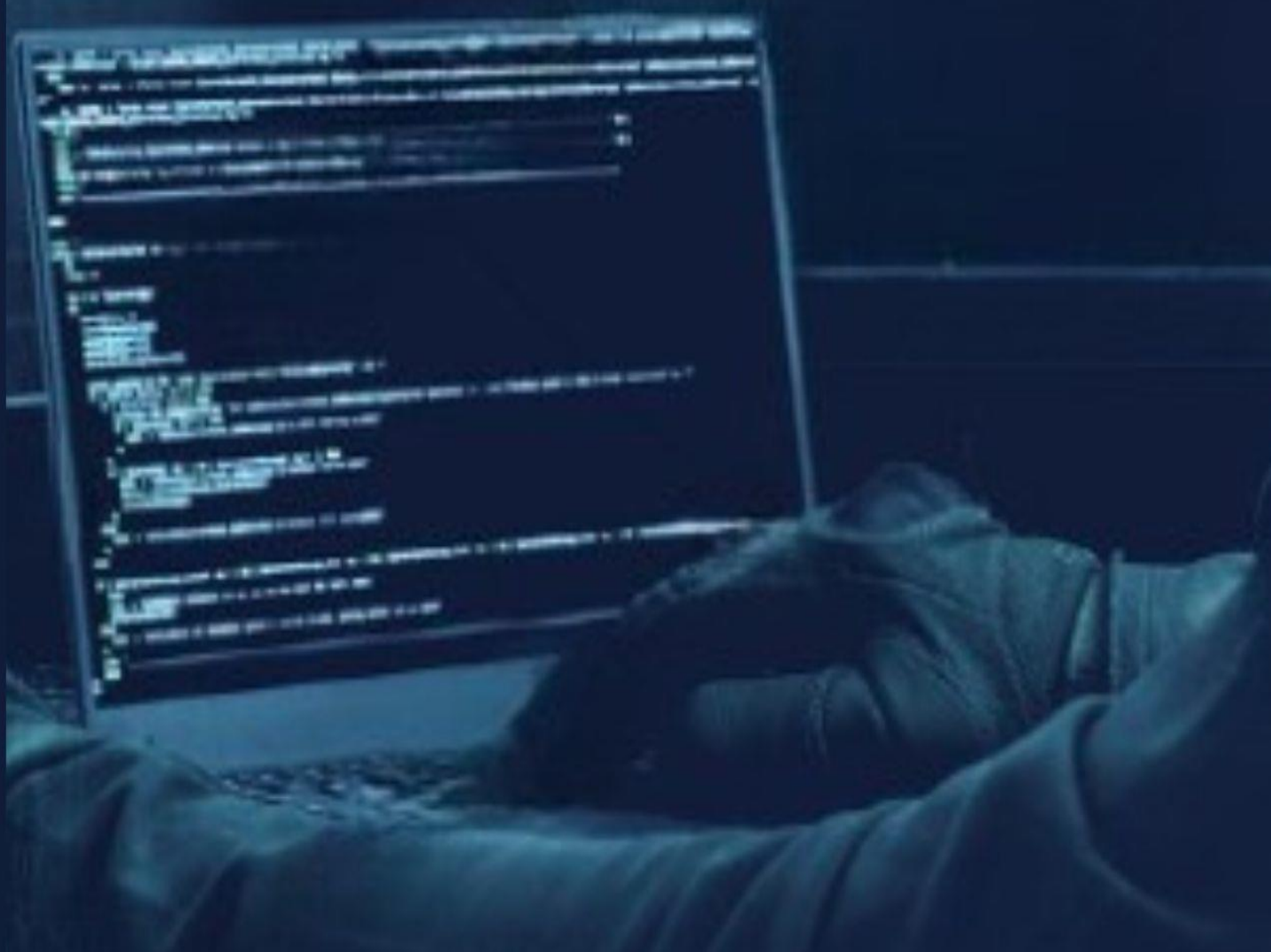
١.	يسمح Sniffing برؤية جميع أنواع حركة المرور	√
٢.	يمكن أن تؤدي هجمات التنصت الى سرقة الهوية	√
٣.	يمكن للمخترق التصنت على المعلومات الحساسة التالية من الشبكة	√
٤.	يوجد ست أنواع من أنواع التنصت	×
٥.	في التنصت الإيجابي لا يتم غلق حركة المرور	√
٦.	تستخدم معظم الشبكات الحديثة المحولات وبالتالي، تزيل خطر التصنت الإيجابي	×
٧.	من أدوات تحليل حركة المرور MAC Flooding	√
٨.	Attack Spoofing انتحال المهاجم لبيانات مستخدم أخر للوصول إلى موارد مقيدة	√
٩.	MACC هو أحد إصدارات بروتوكول الإنترنت (IP) الذي يوفر مساحة عناوين IP أكبر لمستخدمي	×
١٠.	IPv6 هو عنوان من ١٢٨ بت يحتوي على ثمانية خانات من أربعة أرقام مفصولة بنقطتين	√

اختراق أنظمة التشغيل

الفصل الخامس

في هذا الفصل سنتعرف على المواضيع التالية:

- منهجية أمان نظم التشغيل
- خطوات الاختراق
- المصادقة وكلمات المرور
- أدوات مهاجمة كلمات المرور (عملي)
- التدابير المضادة والحماية من عمليات المهاجمة



❖ 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، تقدم أنظمة التشغيل مزايا أمان عديدة منها لحماية سرية البيانات أثناء التخزين والنقل والمعالجة، وأخرى لضمان أمانتها أي عدم إجراء تعديل غير مرغوب به عليها أثناء تخزينها ونقلها ومعالجتها وأيضا لضمان توافرها وعدم خسارتها بفعل متعمد أو بشكل غير مقصود، كما تقدم أنظمة التشغيل إمكانية إدارة التحكم بالوصول إلى الموارد Access Controlوغيرها من ميزات الأمان التي تختلف بين نظام تشغيل وآخر.

إذا عند اختيار نظام التشغيل يجب معرفة ميزات الأمان التي يقدمها كل نظام تشغيل ومقارنتها مع ميزات الأمان في أنظمة التشغيل الأخرى لتكون هذه المعلومة عاملا إضافيا يجب أخذه بعين الاعتبار عند اختيار نظام التشغيل المناسب.

تستهدف أغلب التطبيقات الخبيثة نظام التشغيل نفسه، إذ أن ذلك يخولها إخفاء تواجدها عن المستخدم وبقية التطبيقات بما في ذلك برامج مضادات الفيروسات Antivirus Software ومضادات التطبيقات الخبيثة بشكل عام Antimalware والتي تتموضع في طبقة التطبيقات، ويتيح لها الوصول إلى العتاد مباشرة بما في ذلك القرص الصلب والشبكة ولوحة المفاتيح ...الخ ، معرفة المستخدم أو بقية التطبيقات ، وهذا يعني بدوره أن المخترقين يحاولون البحث عن ثغرات أمنية موجودة في أنظمة التشغيل لتقوم برمجياتهم الخبيثة باستغلالها ، أغلب المخترقين يختارون البحث عن الثغرات في أنظمة التشغيل الأكثر شيوعا، لكي يكون مردود اكتشافهم لثغرة أمنية يمكن لبرامجهم الخبيثة استغلالها عاليا.

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.

وبالتالي عند تقدير مستوى أمان نظام تشغيل ما، لا يكفي استخدام معايير مزايا الأمان التي يقدمها وإنما ينبغي أيضا بالإضافة لذلك مراجعة مستوى انتشاره وشيوعه في العالم.

- **كيف يحمي نظام التشغيل نفسه**

يمنع التشغيل الآمن البرامج الضارة من النوع المعقد والخطير مثل مجموعات البرامج الضارة المخفية من التحميل عند بدء تشغيل جهاز الحاسب، حيث تستخدم مجموعات البرامج الضارة المخفية أذونات نظام التشغيل نفسها ويبدأ تشغيلها قبل النظام مما يعني أن بإمكانها إخفاء نفسها.

- **مزايا الأمان في نظام التشغيل**

١. إدارة حسابات المستخدمين

تعني أن نظام التشغيل يتيح إمكانية إنشاء عدد من حسابات المستخدمين على الحاسب، وأن نظام التشغيل يتيح التحكم بالوصول Access Control كل من هذه الحسابات.

٢. تحديثات الأمان **Security Updates**

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

٣. حالة الدعم التقني

تقوم الجهة المصدرة لنظام التشغيل بتقديم الدعم التقني لنظام التشغيل الذي يتضمن إصدار التحديثات، لسد الثغرات الأمنية بعد اكتشافها، عادة ما تقوم الجهة المصدرة لنظام التشغيل بتقديم الدعم هذا لعدد محدد من السنوات يتوقف بعدها الدعم ويتوقف معه إصدار تحديثات الأمان، وبالتالي تعد أنظمة التشغيل التي وصلت لنهاية عمرها الافتراضي end of life أنظمة تشغيل غير آمنة، ويتوجب على مستخدميها الانتقال لنظام تشغيل مازال مدعوما من الجهة المصدرة.

تختلف أنظمة التشغيل بعضها عن بعض بالنسبة للدعم التقني في عدة نقاط منها:

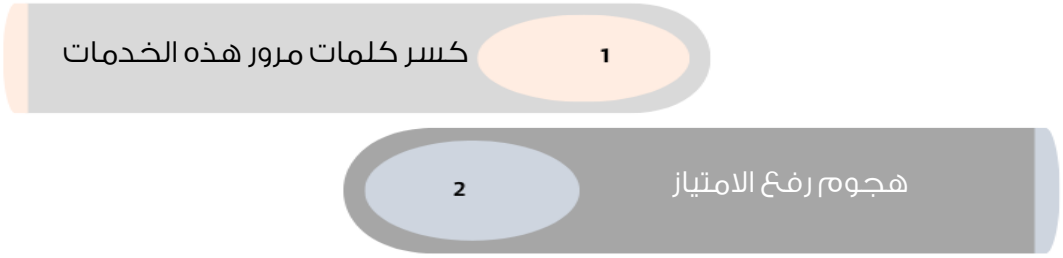
- مدة الدعم التقني أي عمر نظام التشغيل.
- سرعة إصدار التحديثات الأمنية بعد اكتشاف الثغرات.
- مصداقية الجهة المصدرة ودرجة تحملها للمسؤولية.

❖ خطوات الاختراق

من خلال مراحل الاستطلاع والمسح يكون المُخترق قد تمكن من جمع معلومات كثيرة ومهمة عن الهدف ومن أهمها معلومات عن حسابات المستخدمين والمجموعات والتطبيقات والخدمات والاتصال عن بعد ونوع أنظمة التشغيل وهذه المعلومات هي اللازمة للدخول للنظام والسيطرة على موارده وتتضمن أنظمة التشغيل ويندوز وأنظمة التشغيل الأخرى برامج معروفة التي توفر وظيفة الاتصال عن بعد مثل برنامج telenet وبرنامج خادم الملفات FTP وهي تكون مدمجة في أنظمة التشغيل الحديثة.

برامج الاتصال عن بعد مكونة من مكونين برمجيين، المكون الأول يسمى العميل Client وهو يوجد في جهاز المستخدم والمكون الثاني يسمى الخادم Server و يوجد في خادم المؤسسة وهو يطلب من المستخدم اسمه وكلمة المرور لكي يمكنه من إنشاء الاتصال والدخول إلى Server ، و إذا كان المخترق قد حصل على لائحة حسابات المستخدمين من خلال مراحل الاستطلاع والتعداد فإنه يكتب اسم المستخدم ثم يقوم بمحاولة تخمين كلمة المرور من أجل أن يتمكن من الدخول على النظام الهدف فإذا نجح في تخمين كلمة المرور باستخدام أي أداة من أدوات كسر كلمة المرور فإنه سيتمكن من الدخول إلى النظام الهدف وهذا الدخول لا يتيح للمستخدمين العاديين الوصول للمعلومات المهمة لأن أنظمة التشغيل تحصر حقوق الوصول إلى الملفات والمعلومات المهمة لمدير الشبكة فقط الذي يمنح صلاحيات الوصول للمستخدمين حسب أعمالهم لذلك يلجأ لهجوم رفع الامتياز.

- **يتم الاختراق عبر خدمات الاتصال عن بعد عن طريق خطوتين رئيسيتين:**



❖ المصادقة وكلمة المرور

يوفر الأمان آلية للتحقق من هوية المستخدم أو العملية للسماح له باستخدام النظام.

يوفر الوصول الى النظام للمستخدمين المصرح لهم فقط.

❖ أدوات مهاجمة كلمات المرور (عملي)

إذا اكتشف المُخترق أن أحد المنافذ مفتوحة في هذا النظام أي أن خدمة ما من خدمات الاتصال عن بعد في حالة عمل وتصنت على هذا المنفذ فيقوم بمهاجمتها ومحاولة الاتصال بها فإنه بعد كتابة اسم المستخدم يحاول كسر كلمة السر باستخدام أشهر الأدوات وهي Cain , Hydra وتعتمد هذه الأدوات على تجربة تركيبات مختلفة من اسم المستخدم وكلمة المرور محفوظة في ملف عندها والمُخترق يقوم بتسجيل عنوان ip للنظام الهدف و نوع الخدمة المطلوب الاتصال بها وعند ذلك ترسل الأداة تركيبة من اسم المستخدم و كلمة المرور إلى الخدمة فإذا كانت التركيبة خاطئة يتم عرض رسالة خطأ ويفشل الدخول فتقوم الأداة بإرسال تركيبة أخرى ويتكرر ذلك إلى أن تنجح الأداة في العثور على كلمة المرور الصحيحة أو تستنفذ كل التخمينات الموجودة فيها .

تكسير كلمة المرور Password Cracking هو مصطلح يستخدم لتحديد عملية اكتساب الاستخدام الغير مصرح به لدخول الشبكة والنظام أو الموارد التي يتم تأمينها مع كلمة المرور عن طريق تخمينها، أدوات تكسير كلمة المرور تسمح لإعادة تعيين كلمات مرور لمسؤول غير معروف أو مدير الشبكة أو في حالة نسيانها من قبل المستخدم.

تمكن استخدام تقنية هجوم القاموس حيث يتم فيه تحميل ملف Dictionary إلى تطبيق كسر كلمات المرور الذي يستخدم ضد حسابات المستخدمين وهو ملف نصي يحتوي على عدد من كلمات القاموس، ويستخدم البرنامج كل كلمة في القاموس للعثور على كلمة السر.

- **يتم مهاجمة كلمات المرور باستخدام أدوات مثل:**

- **Hydra**

أداة Hydra هي 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 Brute Force القوة الغاشمة وأداة لمهاجمة أنظمة البريد الإلكتروني، موجود في كالي لينكس Password Attacks /Online Attacks /Hydra.

- **الأوامر الأساسية**

```
hydra -l [username] -p [password] [target] [protocol]
```

يقوم هذا الأمر بتنفيذ هجوم التخمين على كلمات المرور باستخدام قائمة من كلمات المرور المحتملة ويستخدم اسم المستخدم المُعطى للدخول إلى النظام.

```
hydra -l [username] -P [password list file] [target] [protocol]
```

يقوم هذا الأمر بتنفيذ هجوم التخمين على كلمات المرور باستخدام كلمة المرور المعينة ويستخدم اسم المستخدم المُعطى للدخول إلى النظام.

```
hydra -L [user list file] -P [password list file] [target] [protocol
```

يقوم هذا الأمر بتنفيذ التخمين على كلمات المرور باستخدام قائمة من أسماء المستخدمين وقائمة من كلمات المرور هجوم باستخدام قائمة من أسماء المستخدمين وقائمة من كلمات المرور المحتملة

```
hydra -M [target list file] -l [username] -P [password list file] [protocol]
```

يقوم هذا الأمر بتنفيذ هجوم التخمين على كلمات المرور باستخدام قائمة من أسماء المستخدمين وقائمة من كلمات المرور باستخدام قائمة من الأهداف ويستخدم اسم المستخدم المُعطى للدخول إلى الأهداف.

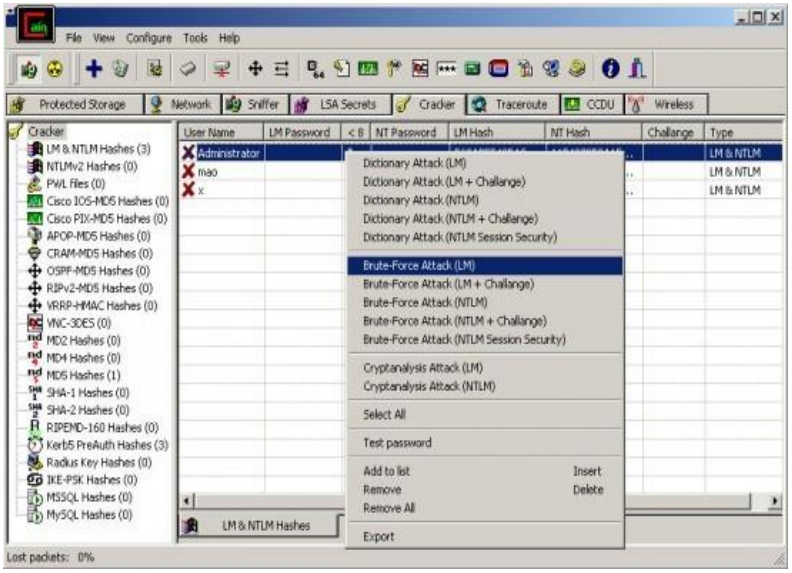
```
hydra -S -l [username] -P [password list file] [target] [protocol]
```

يقوم هذا الأمر بتنفيذ هجوم التخمين على كلمات المرور بشكل متسلسل أي يتم تجربة كل كلمة مرور على كل مستخدم قبل الانتقال إلى المستخدم الذي يليه.

```
Example : Hydra -L users.txt -P password.txt
ftp://127.0.0.1

* -L path of usernames list.
* -P path of passwords list.
* ftp:// the protocol type.
* We can also use -vV to display the
results directly.
```

شكل (٣٨) هجمات التخمين

- برنامج Cain



شكل (٣٩) واجهة CAIN

Cain هي واحدة من أفضل أدوات الاختراق لاختراق كلمات المرور واستعادة كلمة المرور لنظام التشغيل Windows.

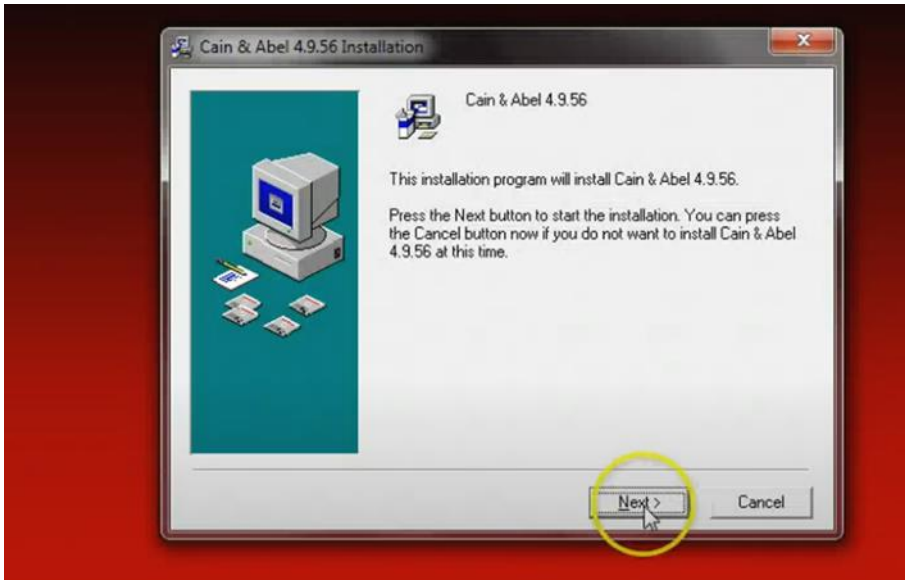
Cain واجهة المستخدم الرسومية للبرنامج بسيطة للغاية وسهلة الاستخدام ، ولكن لديها قيود على التوافر، الأداة متاحة فقط للأنظمة القائمة على widows.

- **خطوات التطبيق العملي**

استخدام برنامج Cain لمعرفة كلمة سر الشبكات على سبيل المثال الشبكات المنزلية.

١. الدخول على الرابط

https://ar.softmedal.com/download.php?file=cain-abel



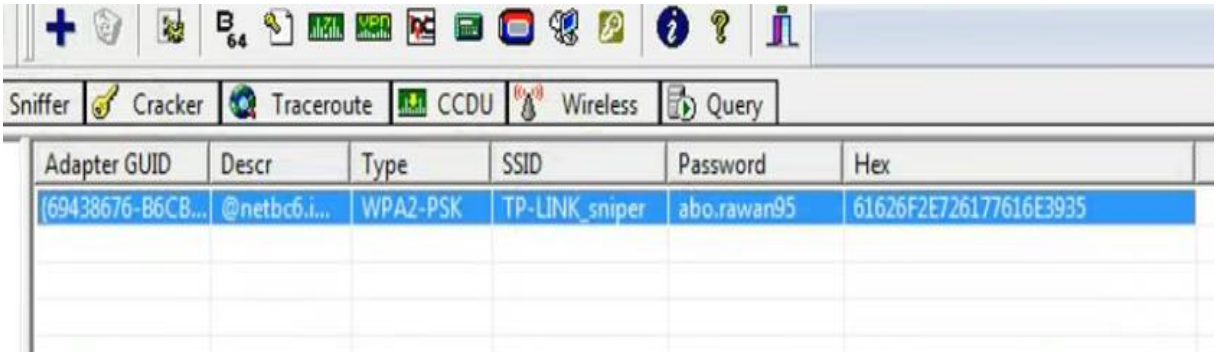
شكل (٤٠) تثبيت البرنامج

- نستكمل خطوات التنصيب وبعد الانتهاء نفتح البرنامج

١. نقوم بالدخول على wireless password

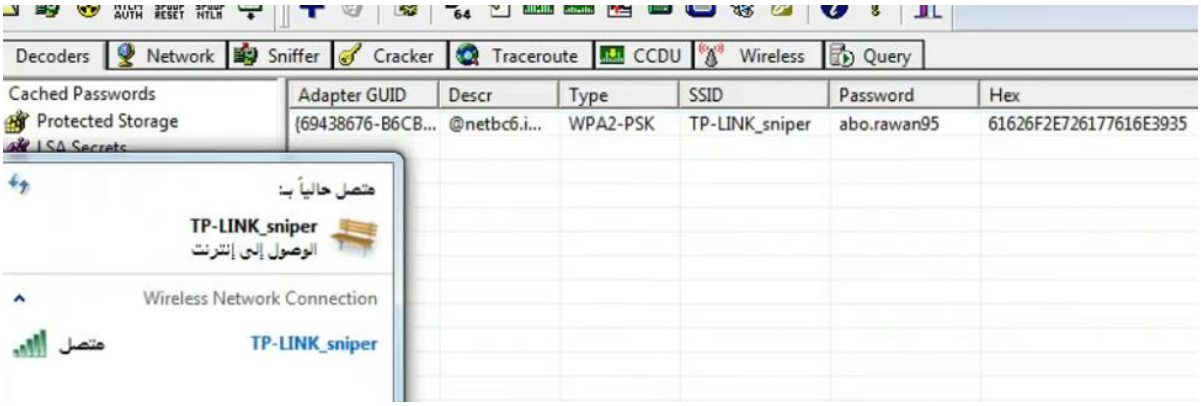
٢. ثم نضغط على الأمر press the+button on the toolbar to etc

٣. ثم نختار علامة الزائد



شكل (٤١) الدخول على الشبكة

٤. ثم نقوم بالدخول على شبكتنا ونتحقق



شكل (٤٢) نتحقق من شبكة المنزل

- **تصعيد الامتياز وتنفيذ التطبيقات**

بمجرد استغلال الثغرات الأمنية بنجاح في نظام معين، قد يحاول المختبرين استخدام النظام المخترق لإطلاق عمليات استغلال لاحقة على موارد داخلية أخرى، وتحديداً من خلال محاولة تحقيق مستويات أعلى من التصريح الأمني ووصول أعمق إلى الأصول والمعلومات الإلكترونية عبر تصعيد الامتيازات.

فبعد أن يتمكن من الدخول إلى النظام الهدف فإنه يعمل على رفع حسابه إلى امتياز مدير النظام إما من خلال إضافة نفسه إلى مجموعة المدراء أو من خلال إنشاء حساب مدير جديد وتسمى هذه العملية بهجوم رفع الامتياز وبمجرد أن يحصل المُخترق على امتياز مدير فإن جميع موارد النظام وملفاته المهمة تصبح في متناول يده ويستطيع تنفيذ التطبيقات ، بعد ذلك يهدف إلى الاستيلاء على الأجهزة الأخرى في بيئة الشبكة بهذه الامتيازات الإضافية التي حصل عليها، وفي النهاية امتيازات المستخدم الأعلى مستوى مثل مسؤول النطاق أو مسؤول قاعدة البيانات.

- **Metasploit**

هو أداة استغلال مفتوحة المصدر Metasploit framework (msf) ، يؤمن هيكلية منظمة لعملية الاستغلال ويسمح للمطورين باستخدام وتطوير ومشاركة الاستغلالات مع بعضهم البعض.

- **يمكن تثبيتها عن طريق الأمر**

```
apt update; apt install metasploit-framework
```

- **الأوامر الأساسية المستخدمة في Metasploit**

- **Search**

تُستخدم للبحث عن الاستغلال في database & MSF

Metasploit يحتوي على العديد من الأوامر التي يمكن استخدامها للبحث عن الموديولات والثغرات المتاحة.

- **هنا بعض الأوامر البحثية الشائعة في Metasploit**

search <term>: يستخدم هذا الأمر للبحث عن الموديولات والثغرات المتاحة في Metasploit ، يمكنك استخدام هذا الأمر للبحث عن موديولات معينة أو ثغرات ذات صلة بمصطلح محدد ، على سبيل المثال، يمكنك استخدام search flash للبحث عن ثغرات تتعلق ببرنامج Flash Player.

grep <pattern>: يستخدم هذا الأمر للبحث عن نص محدد في نتائج الأوامر السابقة في Metasploit. يمكنك استخدام هذا الأمر للتركيز على النتائج التي تحتوي على نص معين، على سبيل المثال، يمكنك استخدام grep http للبحث عن النتائج التي تحتوي على كلمة "http".

search -f <filetype>: يستخدم هذا الأمر للبحث عن ملفات معينة في النظام ، يمكنك استخدام هذا الأمر للبحث عن ملفات معينة بناءً على نوع الملف ، على سبيل المثال، يمكنك استخدام search -f *.jpg للبحث عن جميع ملفات الصور بامتداد JPG.

- **Use**

تُستخدم لاختيار الاستغلال الملائم.

- **لبدء استخدام أداة Metasploit في Kali Linux، يمكنك اتباع الخطوات التالية:**

- قم بفتح واجهة سطر الأوامر في Kali Linux.
- اكتب MSF console واضغط على مفتاح Enter لبدء واجهة Metasploit.
- بمجرد فتح واجهة Metasploit، ستظهر لك شاشة ترحيبية تحتوي على معلومات حول الإصدار الحالي لـ Metasploit.

يمكنك استخدام الأوامر التالية للتنقل واستخدام Metasploit:

help: يعرض قائمة بالأوامر الأساسية في Metasploit مع وصف لكل أمر.

search <term>: يستخدم للبحث عن الموديلات والثغرات المتاحة في Metasploit.

use <module>: يستخدم لتحديد واستخدام وحدة Metasploit المحددة.

set <option> <value>: يستخدم لتعيين قيمة لخيار محدد في وحدة Metasploit.

exploit: يستخدم لتنفيذ الهجوم المحدد في وحدة Metasploit.

يمكنك استكشاف المزيد من الأوامر والوحدات المتاحة في Metasploit وفقًا لاحتياجاتك الخاصة.

- **Show payload**

تُستخدم لاستعراض payloads المتوفرة من أجل الاستغلال.

- **Set payload**

تستخدم لاختيار payload المطلوب.

- **Show options**

تُستخدم لاستعراض الاختيارات الضرورية التي يجب إعدادها كجزء من payload المختار.

- **Set**

تُستخدم لتخصيص قيمة لكل الاختيارات المطلوبة.

تعد مجموعة أدوات المهندس الاجتماعي (SET) أداة قوية مفتوحة المصدر متوفرة في Kali Linux

لتنفيذ هجمات الهندسة الاجتماعية.

- **خطوات استخدام أمر SET في Kali Linux**

- افتح المحطة في كالي لينكس.
- اكتب setoolkit واضغط على Enter لتشغيل مجموعة أدوات المهندس الاجتماعي، سيؤدي هذا الأمر إلى فتح قائمة SET، حيث يمكنك تحديد خيارات الهجوم المختلفة.
- بمجرد ظهور قائمة SET، يمكنك التنقل عبر متجهات وخيارات الهجوم المختلفة باستخدام القائمة المتوفرة، توفر قائمة SET واجهة سهلة الاستخدام لتنفيذ العديد من هجمات الهندسة الاجتماعية، مثل التصيد الاحتيالي وجمع بيانات الاعتماد والمزيد.
- اتبع التعليمات التي تظهر على الشاشة لتحديد ناقل الهجوم المطلوب وتكوين معلمات الهجوم، سترشدك قائمة SET خلال عملية إعداد الهجوم.
- بعد تكوين الهجوم، سيقوم SET بإنشاء الملفات والحمولات الضرورية لمتجه الهجوم المحدد، وسوف يزودك بالمعلومات والخيارات المطلوبة لمواصلة الهجوم.
- اتبع التعليمات المقدمة من SET لتنفيذ هجوم الهندسة الاجتماعية، كن حذرًا وتأكد من حصولك على التفويض المناسب والإذن القانوني قبل تنفيذ أي هجوم.

يرجى ملاحظة: أن هجمات الهندسة الاجتماعية يجب أن يتم تنفيذها فقط لأغراض أخلاقية، مثل اختبار الاختراق والتقييمات الأمنية. إن إساءة استخدام تقنيات الهندسة الاجتماعية أمر غير قانوني وغير أخلاقي.

تذكر دائمًا الحصول على الترخيص المناسب واتباع الإرشادات القانونية والأخلاقية عند استخدام مجموعة أدوات المهندس الاجتماعي أو أي أداة أمنية أخرى.

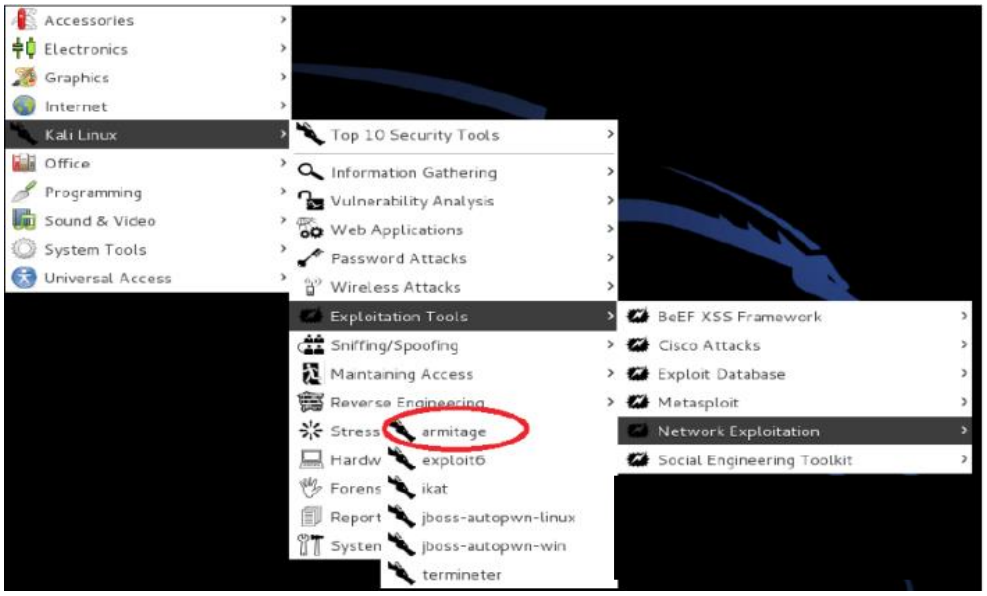
- **Exploit**

تُستخدم لإرسال الاستغلال إلى النظام الهدف.

- **Shell code**

- هو الكود الذي يقوم بإنشاء remote shell تتصل مع جهاز مُختبر الاختراق.
- مُختبر الاختراق يقوم بإنشاء ملف خبيث يحتوي على shell code ويقوم بإرساله إلى الهدف عبر البريد الإلكتروني أو بأي طريقة أخرى باستخدام الهندسة الاجتماعية أو الوصول المادي للجهاز الهدف وعندما يقوم الهدف بفتح الملف فإن مُختبر الاختراق يمكنه الوصول إلى النظام الهدف عن بعد.
- Shell code يمكن أن تُضاف أو تُدمج مع برنامج عادي من أجل فتح باب خلفي backdoor في الجهاز الهدف.
- مُختبر الاختراق يستخدم ملف لبرنامج معروف ويقوم بحقن أو دمج shell code في هذا البرنامج وعندما يقوم الهدف بفتح هذا الملف فإن مُختبر الاختراق يمكنه الوصول والتحكم بجهاز الهدف عن بعد.
- Metasploit تسمح بإنشاء shell code التي يمكن أن تُستخدم من أجل اختبار الحماية في النظام الهدف.
    - **لفتحها في كالي لينكس**

Start /Kali Linux /Exploitation tools /Network Exploitation Tools أما لاستخدام الواجهة الرسومية بتم استخدام armitage



شكل (٤٣) armitage

- **Metasploit تطبيق عملي**

تماشيًا مع سياسة خدمات شبكة Kali Linux ، لا يتم تشغيل أي خدمات شبكة، بما في ذلك خدمات قاعدة البيانات، عند التمهيد كإعداد افتراضي، لذلك هناك بضع خطوات يجب اتخاذها لتشغيل Metasploit مع دعم قاعدة البيانات.

الطريقة السريعة / سيكون لديك كل شيء جاهزًا للعمل، من خلال بدء تشغيل خدمة PostgreSQL وإعدادها فقط، **عن طريق القيام بما يلي:**

```
kali@kali:~$ sudo msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
kali@kali:~$
```

يمكنك أيضًا أن تخطو خطوة أخرى إلى الأمام من خلال القيام sudo msfdb run بنفس الشيء كما هو مذكور أعلاه، وكذلك البدء msfconsole بعد ذلك.

- **MSFDB**

للمساعدة في التفاعل مع أجزاء مختلفة من تكوين Metasploit هناك msfdb:

```
kali@kali:~$ sudo msfdb

Manage the metasploit framework database

  msfdb init     # start and initialize the database
  msfdb reinit   # delete and reinitialize the database
  msfdb delete   # delete database and stop using it
  msfdb start    # start the database
  msfdb stop     # stop the database
  msfdb status   # check service status
  msfdb run      # start the database and run msfconsole

kali@kali:~$
```

شكل (٤٤) تكوين msfdb ا

يرجى ملاحظة: هذه نسخة مختلفة يتم msfdb شحنها مع المشروع الافتراضي

ابدأ تشغيل خدمة Kali PostgreSQL

يستخدم Metasploit PostgreSQL كقاعدة بيانات خاصة به لذا يجب تشغيله أولاً:

```
kali@kali:~$ sudo msfdb start
[+] Starting database
kali@kali:~$
```

شكل (٤٥) تشغيل DB

يمكنك التحقق من تشغيل PostgreSQL عن طريق التحقق من مخرجات ss -antالمنفذ ٥٤٣٢ والتأكد من أنه يستمع إليه، أو باستخدام sudo msfdb status:

```
kali@kali:~$ sudo msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sun 2021-02-07 02:15:42 EST; 4s ago
    Process: 157089 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 157089 (code=exited, status=0/SUCCESS)

Feb 07 02:15:42 kali systemd[1]: Starting PostgreSQL RDBMS...
Feb 07 02:15:42 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND     PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 157071 postgres    5u  IPv6 647182      0t0  TCP localhost:5432 (LISTEN)
postgres 157071 postgres    6u  IPv4 647183      0t0  TCP localhost:5432 (LISTEN)


UID          PID    PPID  C STIME TTY      STAT   TIME CMD
postgres  157071       1  1 02:15 ?        Ss     0:00 /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=

[i] No configuration file found
kali@kali:~$
```

شكل (٤٦) PostgreSQL

- **تهيئة قاعدة بيانات Metasploit Postgre SQL**

مع تشغيل PostgreSQL , نحتاج بعد ذلك الى إنشاء قاعدة بيانات MSF وتهيئتها:

```
kali@kali:~$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
kali@kali:~$
```

قم بتشغيل msfconsole في كالي

الآن بعد أن تم تشغيل خدمة PostgreSQL وتهيئة قاعدة البيانات، يمكنك تشغيل msfconsole والتحقق من اتصال قاعدة البيانات باستخدام الأمر db_status كما هو موضح أدناه:

```
kali@kali:~$ msfconsole -q
msf6 >
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

شكل (٤٧) الاتصال بقاعدة البيانات ا

- **إخفاء الملفات وتغطية المسارات**

بمجرد كسر المهاجم النظام بنجاح فإنه يحاول إخفاء نفسه من أن يتم اكتشافه أو تتبعه وبالتالي يحاول تغطية جميع المسارات أو السجلات التي يتم إنشاؤها أثناء ممارسته أو محاولة وصوله للنظام والأجهزة والشبكات المستهدفة وهنا يقوم بحذف جميع الآثار التي قد تم تسجيلها في الجهاز المراد اختبار الاختراق عليه، ومنها حذف ملف الـ "logs" لجدار الحماية، سواء كان الجدار الأساسي في الـ Windows أو كان مثبت أيضاً، ويتم في هذه المرحلة استخدام عدة أدوات لحذف الآثار بشكل كامل.

اما المخترق غير الأخلاقي فيقوم بمسح أثاره على الجهاز، حتى لا يتم اكتشافه من طرف صاحب النظام المستهدف فالمخترق يلجأ لمسح أي دليل على وجوده ومحو سجلات التسلل وتتبع الملفات فهو يقوم بمسح الأدلة التي تدل على الحفاظ على الوصول والتهرب لأنه إذا تمكن من حذف المسارات فإنه له إعادة تسجيل الدخول إلى النظام والتثبيت الخفي للحصول على المعلومات المهمة للمستخدمين.

قد لا يستطيع المُخترق في حذف السجل كامل لأنه يتطلب امتيازات مدير الشبكة التي تمكنه من حذف السجلات لأحداث الاختراق وبالتالي يخفي نفسه من أن يتم اكتشافه بالتعديل.

يستخدم المخترق الأداة rootkits لتعطيل وتجاهل كافة السجلات الموجودة التي تكشف عن وجود هجوم.

- **Covering Tracks tool**

- **MRU-Blaster**

هو برنامج يسمح بتنظيف أكثر القوائم المستخدمة مؤخرا على النظام وملفات الإنترنت المؤقتة ويوفر معلومات كاملة عن أسماء ومواقع الملفات الأخيرة المستخدمة ويعالج تنظيف " المسارات المستخدمة " وآثار البرامج التي تتركها البرامج المستخدمة، الموقع http://www.brightfort.com

- **CCleaner**

هي أداة تنظيف وينظف أثار تفاصيل تصفح الإنترنت من خلال جهاز الحاسب ويمحو المسارات الخاصة بالمهاجم والأنشطة على الإنترنت الموقع http://www.piriform.com

- **Disabling Auditing : Auditpol**

هي جزء من مجموعة أدوات NT resource kit والتي يمكن استخدامها لمعرفة حالة تدقيق نظام التشغيل يحتاج المُخترق إلى تثبيت الأداة في مسار WINNT وتأسيس جلسة عمل فارغة Null Session إلى الجهاز الهدف **ثم تشغيل الأمر:**

```
C:\auditpol \\ <ip address of target>
```

سوف يكشف حالة التدقيق الحالية للنظام ويمكن أن يختار تعطيل التدقيق بواسطة"

```
C:\auditpol \\ <ip address of target>/disable
```

هذا الإجراء سوف يقوم بالعديد من التغيرات في مختلف ملفات السجلات التي تسجل الأحداث.

- **إخفاء الملفات**

يقوم المهاجمون أيضا بإخفاء الملفات الخبيثة داخل الملفات الأخرى Rootkits يمكن استخدامها لإخفاء الملفات عن المستخدمين وغالبا ما تكون ناجحة في التلاعب حتى من برامج مكافحة الفيروسات، ويمكن أن تستخدم في عدة أهداف منها تصعيد الامتيازات وتسجيل ضربات المفاتيح وتركيب backdoors ولديها القدرة على اعتراض وتعديل الاستجابات من قبل نظام التشغيل أي هي تهدف لإخفاء الملفات أو البرامج والحفاظ على الوصول المخفي، ويقوم **المهاجم يوضعها في النظام باستخدام الطرق التالية:**

- منافذ الأجهزة.
- من خلال الهندسة الاجتماعية بتثبيتها على أجهزة الشبكات للمنظمة أو أجهزة الحاسب العامة.
- تغليفها في برامج الألعاب.

- **هجوم Zero-day**

للكشف عنها يجب الفحص بانتظام لمنافذ النظم للتأكد من عدم وجود منافذ للنظام وغير معروفة مفتوحة وتحليل ملف السجل والنسخ الاحتياطي للبيانات، إنشاء بصمة للملفات واستخدام برامج فحص سلامة ملفات النظام، واستخدام أدوات مثل Rootkit Revealer للكشف عنه وعن الملفات الخفية، McAfee Stinger.

- **برامج التجسس Spyware**

هي برامج تسمح للمهاجمين بالحصول على معلومات حول أنشطة المستخدم أو جميع المعلومات الشخصية عنه وهي تسمح بالتسجيل الحي لسطح المكتب البعيد ومراقبة وتسجيل أنشطة الإنترنت وتسجيل استخدام برمجيات بالتوقيت وتسجيل ضربات مفاتيح المستخدمين، **ويوجد العديد من البرامج مثل:** - Internet Spyware – Email Spyware-Screen Capturing Spyware- Audio Spyware -Video Spyware- Print Spyware- GPS spyware

Remote Desktop Spy – usb spyware

وبرامج أخرى مثل: All in One Keylogger – The Best Keylogger – iMonitorPC

- **اختبار اختراق النظام**

يجب محاولة كسر كلمة للنظام عن طريق اتباع الخطوات التالية:

١- تحديد نظام كلمة السر المحمية.

٢- تنفيذ هجوم القاموس.

٣- تنفيذ هجوم القوة الغاشمة.

٤- استخدام البرامج الضارة أو التجسس لسرقة كلمة السر.

٥- استخدام تقنية الهندسة الاجتماعية للحصول على كلمة السر.

٦- استخدام shoulder surfing لسرقة كلمة المرور.

٧- محاولة تسجيل الدخول باستخدام أسماء المستخدمين التي تم تعدادها وكلمات المرور التي تم كسرها.

٨- تشغيل خدمات المستخدمين التي تم الاستيلاء على حساباتهم.

٩- استخدام أدوات تصعيد الامتياز.

١٠-التحقق من تثبيت برنامج مكافحة الفيروسات على النظام الهدف.

١١-التحقق من تثبيت جدار الحماية وإعداداته والبرامج المضادة للتجسس على النظام الهدف.

١٢-التحقق من بيئة تأمين الأجهزة في المبنى.

١٣-تثبيت Keylogger برنامج على النظام من أجل تسجيل ضربات المفاتيح.

١٤-استخدام spyware من أجل رصد الأنشطة على النظام.

١٥-تثبيت برنامج rootkits الخاص بالمحافظة على الوصول الخفي.

١٦-تنفيذ تقنيات الكشف القائم على السلامة للكشف عن rootkit.

١٧-استخدام برنامج مكافحة rootkits.

١٨-تعطيل التدقيق لتغطية المسارات.

١٩-التعديل في ملفات السجل event log files.

٢٠-استخدام أدوات تغطية المسارات.

٢١-توثيق النتائج في التقرير مع التدابير المضادة.

❖ التدابير المضادة والحماية من عمليات المهاجمة

١. أداء تحديثات نظام التشغيل العادية.

٢. تفعيل جدار الحماية Firewall.

٣. تشفير محركات الأقراص.

٤. استخدام كلمات مرور قوية للحسابات على الإنترنت.

٥. استخدام خيار شبكة الضيوف.

٦. إعداد رمز مرور قوي لتأمين الأجهزة والاستفادة من ميزات الأمان العالية التي توفرها الطرق البيو مترية.

٧. استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة والتجسس تحديثها بانتظام.

٨. تحديد الموظفين ذوي المسؤوليات.

٩. نشر التوعية بالهندسة الاجتماعية وطرق الحماية منها.

١٠. الحماية من برنامج Keyloggers.

هو برنامج يلتقط ويسجل جميع ضربات المفاتيح سراً بما في ذلك كلمات المرور التي يتم كتابتها على لوحة مفاتيح الحاسب.

وللحماية منها يجب:

- تقييد الوصول الفعلي لأجهزة الحاسب المهمة.
- فحص دوري لواجهة لوحة المفاتيح لضمان عدم وجود مكونات إضافية يتم توصيلها بكبل لوحة المفاتيح.
- إغلاق أبواب الغرف التي يوجد بها خوادم مركز البيانات.
- استخدام برنامج Zemana Antilogger

١١. تقييد امتيازات الدخول للتأمين من هجوم تصعيد الامتياز وتنفيذ مصادقة متعددة العوامل وجعل المستخدمين وتشغيل التطبيقات على الأقل امتياز.

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	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.	√
٢.	يمنع التشغيل الآمن البرامج الضارة من النوع المعقد والخطير مثل مجموعات البرامج الضارة المخفية.	√
٣.	من مزايا الاختراق " تحديثات الأمان Security Updates " .	×
٤.	المصادقة بالوجهة (يوفر الوصول إلى النظام للمستخدمين المصرح لهم فقط) .	×
٥.	يحاول المخترق كسر كلمة المرور باستخدام البرنامج Ipconfig.	×

٢. **اختار الإجابة الصحيحة فيما يلي:**

١. **يمكن تنفيذ اختبار الاختراق عن طريق تنفيذ .....**

أ- القوة الغاشمة
ب- القوة الجبرية
ت- القوة الاختراقية
ث- القوة التشفيرية

٢. **يمكن تنظيف اثار المتصفح من خلال البرنامج .....**

أ- CCleaner
ب- Linux
ت- Open office
ث- Oracle

٣. **Metasploit framework (msf) هي أداة استغلال ..... المصدر**

أ- مفتوحة المصدر
ب- مغلقة المصدر
ت- مفصلة المصدر
ث- ممتدة المصدر

٣. طبق ما يلي عمليا :

١. ابدأ تشغيل خدمة Kali PostgreSQL

```
kali@kali:~$ sudo msfdb start
[+] Starting database
kali@kali:~$
```

٢. تهيئة قاعدة بيانات Metasploit PostgreSQL مع تشغيل PostgreSQL ، نحتاج بعد ذلك إلى إنشاء قاعدة بيانات MSF وتهيئتها

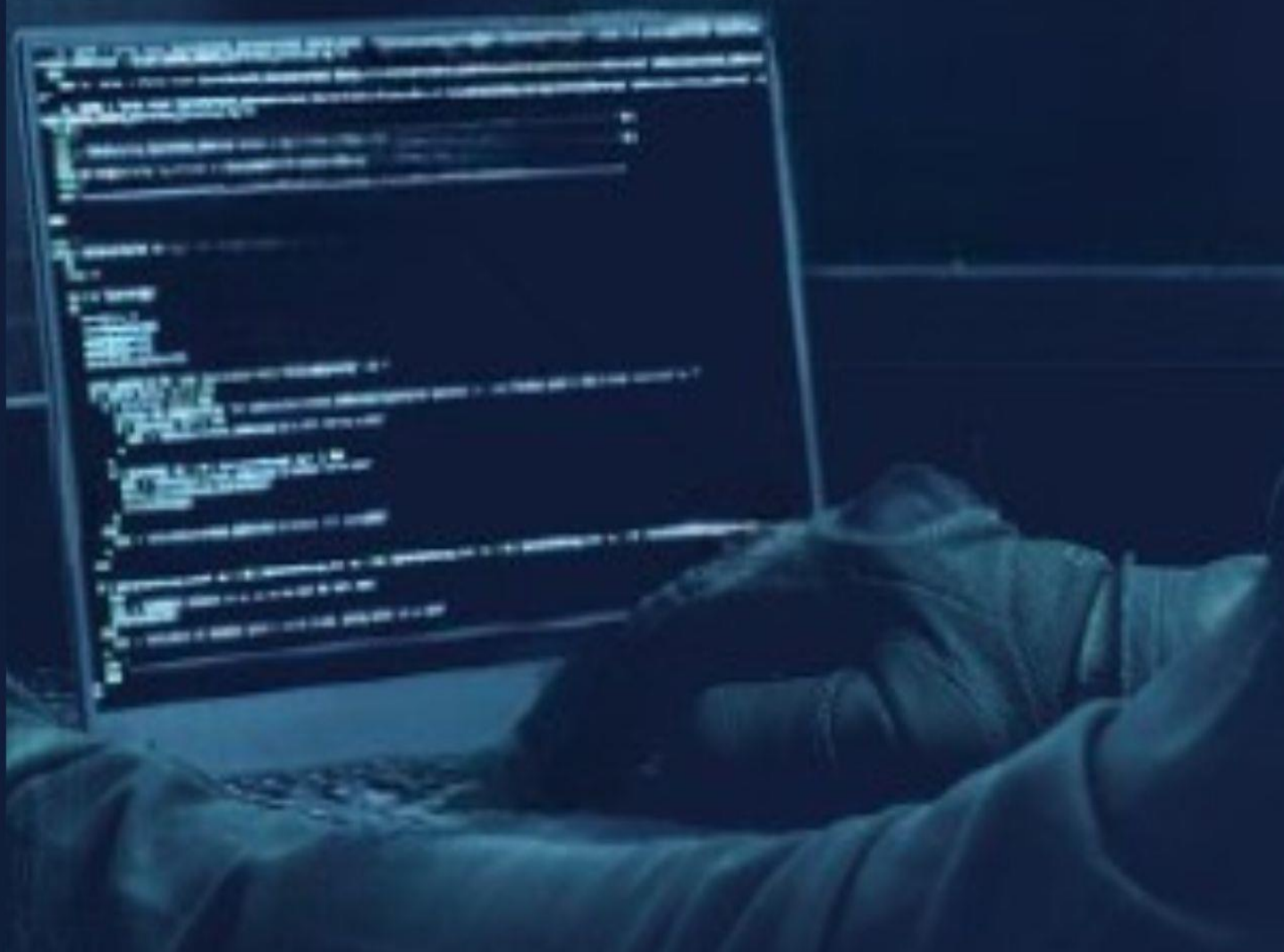
```
kali@kali:~$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
kali@kali:~$
```

اختراق الويب والتطبيقات

الفصل السادس

في هذا الفصل سنتعرف على المواضيع التالية:

- خوادم الويب
- منهجية الهجوم وأدوات الهجوم (عملي)
- مهاجمة تطبيقات الويب (عملي)
- أدوات اختراق تطبيقات الويب
- التدابير المضادة والحماية من عمليات اختراق خوادم وتطبيقات الويب (عملي)



❖ 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 الإعدادات الافتراضية دون إعادة ضبطها للتوافق مع إعدادات الأمان.

أما تطبيقات الويب Web application 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 خادم الويب**

هو Software يعمل داخل نظام التشغيل الخادم Server والذي يسمح للاتصال بالوصول إلى تطبيق الويب.

أكثر الخوادم انتشارا هي:

- Internet Information Services (IIS) وهو يعمل على أنظمة ويندوز.
- Apache Server وهو يعمل على أنظمة لينكس.

هذه الخوادم تملك بنية مجلدات عادية مثل أي جهاز حاسب وهذه المجلدات تكون داخل تطبيق الويب عند تثبيت IIS WEB SERVER يكون بنية المجلد الافتراضي C:\Inetpub\wwwroot حيث كل تطبيق سيملك مجلده الخاص داخل wwwroot .

نظام التشغيل لينكس مختلف في بنية الملفات، ولكن معظم تطبيقات الويب تكون داخل /var/www يوجد العديد من المجلدات في Linux web server مرتبطة باختبار اختراق الويب مثل مجلد /etc./shadow يحتوي على الهاش الخاص بكلمة السر لكل مستخدم للنظام والمجلد /use/lib يحتوي على ملفات غير مُعدة لتكون ملفات تنفيذية من قبل المستخدم أو من قبل Shell scripts وتستخدم من قبل التطبيق وتكون داخل هذا المجلد.

- /var/ هذا المجلد يحتوي على الملفات الخاصة بقاعدة البيانات وسجلات النظام و الكود المصدر لتطبيق الويب نفسه.
- /bin/ هذا المجلد يحتوي على البرامج التي يحتاجها النظام ليعمل مثل shell, ls, grep وبرامج مساعدة أخرى .
- Bin هي اختصار إلى binary معظم تعليمات نظام التشغيل تكون على شكل ملفات منفصلة.
- HTTP هو بروتوكول يستخدم للتفاعل والاتصال مع تطبيق الويب ولا يوجد اعتبار للحماية أو الخصوصية عند استخدامه فأي مستخدم يمكنه أن يطلب وتطبيق الويب يجيب بشكل مستقل ودون أي معرفة بأي طلبات سابقة ولكن تطبيق الويب يحفظ مسار طلب المستخدم وبدون استخدام cookies يمكن أن يطلب من المستخدم إعادة تسجيل الدخول خلال كل خطوة عمل وكان هذا غير عملي فتم استخدام مفهوم الجلسة session حيث يقوم التطبيق بحفظ مسار طلبات المستخدم بعد قيامه بعملية تسجيل الدخول وهي عامل من عوامل تعرض تطبيقات الويب للهجوم ولذلك يتم استخدام https لأنه يمنع بعض أنواع الهجمات.
- يتم الحصول على https عندما يستخدم http بروتوكول SSL/TLS والذي يضاف إلى طلب وإجابة http وتعتبر من أفضل طرق الحماية من هجمات الرجل في المنتصف وهي تؤمن اتصال خاص ومحمي بين المتصفح وتطبيق الويب.
- استخدام https يعني الاتصال مع تطبيق الويب عبر قناة اتصال مشفرة.
- دورة أو حلقة http هي الطلب request من متصفح المستخدم والإجابة response العائدة من خادم الويب.
- المتصفح يرسل طلب يحتوي على بارامترات خاصة بدخول المستخدم وخادم الويب يرسل إجابة يتم توجيهها إلى مصدر الطلب.
- تطبيق الويب يمكن أن يعمل بالاعتماد على قيمة البارامترات لذلك فهي أول هدف يقوم مُختبر الاختراق بمهاجمته باستخدام قيم للبارامترات لاستغلال تطبيق الويب وخادم الويب.

- **طرق الهجوم على خادم الويب**

١. 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.

تشكل هجمات XSS تهديدًا أمنيًا خطيرًا، حيث يمكن استخدامها لسرقة معلومات مهمة أو القيام بأنشطة احتيالية أو حتى السيطرة على متصفح المستخدم.

- **هناك نوعان رئيسيان من هجمات XSS :**

١. هجمات XSS انعكاسية

هجمات XSS العاكسة تحدث عندما يتم حقن الشفرة الخبيثة في الصفحة ثم تنعكس فورًا على المستخدم، دون تخزينها على الخادم.

٢. 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.

- تطبيق هجمات XXS عمليا

  - هجمة الcross site scripting (xss)

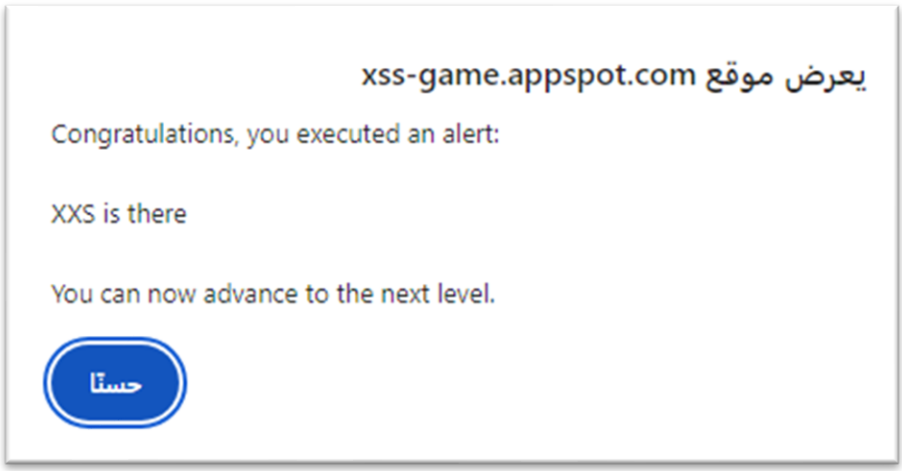
١. يمكن الدخول على الموقع الاتي وتجربه الهجمة xxs

https://xss-game.appspot.com/level1

شكل (٤٨) موقع appspot 1

٢. اكتب الجملة الأتية

```
<script>alert("XXS is there ")</script>
```



شكل (٤٩) نتيجة تنفيذ الهجوم 1

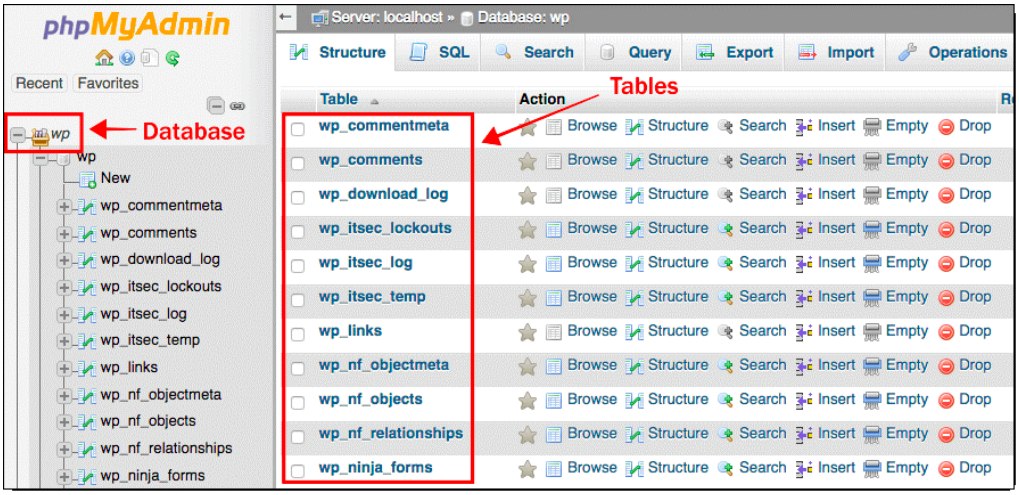
٢- حقن SQL

- 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 SQL.
- 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 بيانات SQL ، قد يكون من الصعب منع هذا النوع من الهجوم،

- **ما هي أدوات اختبار الثغرات المتاحة لتنفيذ هجمات حقن SQL؟**

- **SQLMap:** أداة شهيرة وقوية تستخدم لاختبار الثغرات في تطبيقات قواعد البيانات وتنفيذ هجمات حقن SQL بشكل آلي.
- **Burp Suite:** برنامج شامل لاختبار الأمان يحتوي على العديد من الأدوات، بما في ذلك أدوات لاختبار حقن SQL.
- **Acunetix:** أداة متقدمة لاختبار الأمان تدعم اكتشاف واستغلال ثغرات حقن SQL وتوفر تقارير مفصلة عن الثغرات المكتشفة.
- **Nessus:** أداة شهيرة لاختبار الأمان تستخدم لتحليل الثغرات واكتشاف ثغرات حقن SQL وتقديم توصيات لتصحيحها.
- **Vega:** أداة مفتوحة المصدر تستخدم لاختبار الأمان واكتشاف ثغرات حقن SQL وتوفر تقارير مفصلة عن الثغرات المكتشفة.

إذا كان القصد هو الإضرار بموقعك عن طريق حذف المحتوى من قاعدة البيانات الخاصة بك، فهذا يسمى **Blind SQL injection attack**.

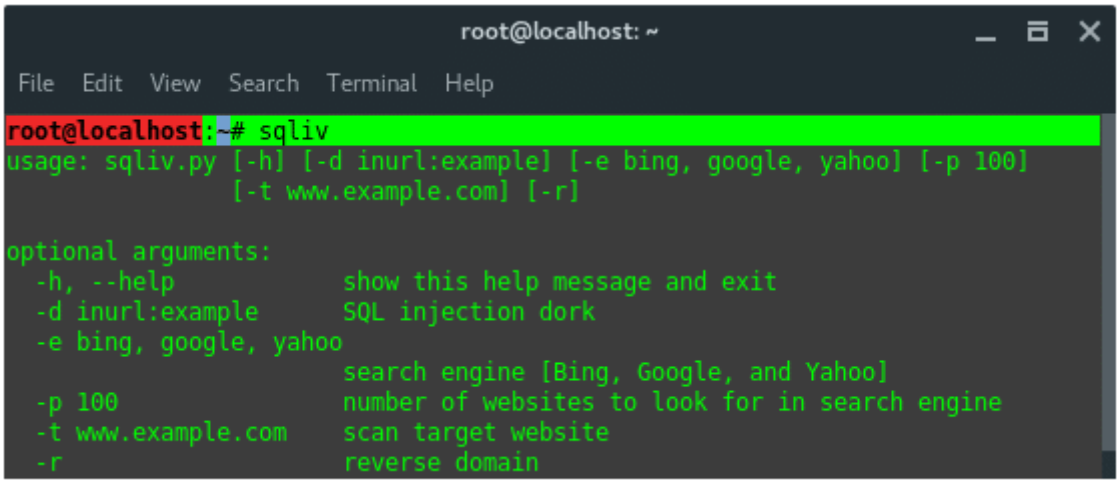


شكل (٥٠) SQL injection

- الخطوة ١: تثبيت **SQLiv** على كالي لينكس

اكتب الأوامر أدناه في جهازك الطرفي لتثبيت SQLiv:

بمجرد تثبيت SQLiv في نظام Kali Linux الخاص بك، يتم تخزينه في المسار /usr/bin/sqliv ، والتي يمكنك الاتصال بها مباشرة من المحطة عن طريق كتابة "sqliv"



شكل (٥١) تثبيت SQLLiv

- **مميزات SQLIv:**

١. **البحث التلقائي عن الثغرات:** SQLiv يقوم بالبحث التلقائي عن الثغرات في المواقع الويب باستخدام تقنيات SQL Injection ، يعني هذا أنه يمكنه اكتشاف النقاط الضعيفة في قواعد البيانات بشكل آلي دون تدخل يدوي.

٢. **دعم متعدد لقواعد البيانات:** يمكن لـ SQLiv التعامل مع قواعد بيانات مختلفة مثل MySQL و PostgreSQL و Microsoft SQL Server و Oracle و SQLite وغيرها، مما يجعلها ملائمة للاختبار في مجموعة متنوعة من البيئات.

٣. **التخصيص الشامل:** يوفر SQLiv خيارات تخصيص متقدمة تتيح للمستخدمين تحديد طريقة البحث والتصفية للنتائج وتحديد البيانات المستهدفة بشكل دقيق.

٤. **تقارير شاملة:** يمكن لـ SQLiv إنشاء تقارير شاملة بعد الاختبار تحتوي على النتائج والتحليلات المهمة، مما يساعد في فهم الثغرات واتخاذ الإجراءات اللازمة لتصحيحها.

٥. **سهولة الاستخدام:** تم تصميم واجهة المستخدم لـ SQLiv بطريقة تجعلها سهلة الاستخدام حتى بالنسبة لأولئك الذين ليسوا خبراء في اختبار الاختراق، مما يسهل عملية اكتشاف الثغرات وتقديم التقارير.

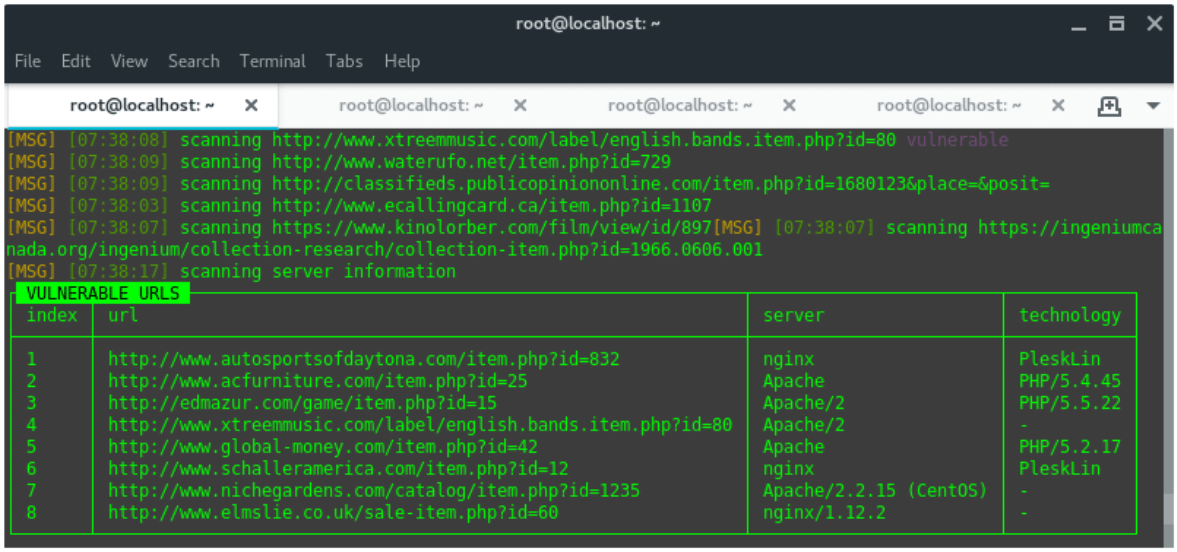
٦. **التحديثات الدورية:** يتم تحديث SQLiv بانتظام لمواكبة آخر التطورات في مجال أمان المعلومات وتقنيات اختراق قواعد البيانات، مما يضمن أنها تظل فعالة وموثوقة في الاستخدام العملي.

- **الخطوة ٢: العثور على الثغرات الأمنية في حقن SQL**

سوف نستخدم Google Dorking لمسح والعثور على فجوة إدخال SQL في الأهداف، لنأخذ فكرة بسيطة، ونسمح لـ SQLiv بفحص كل هدف على حدة والبحث عن ثغرة أمنية في التجارة الإلكترونية في نمط عنوان URL التالي "item.php?id=".

ملاحظة / للعثور على أنماط أخرى، ما عليك سوى البحث في Google عن "قائمة google dork".

SQLiv بالنقر إلى الصفحة الأولى في محرك البحث، والذي يبلغ ١٠ مواقع على Google لكل صفحة، وبالتالي، نحدد هنا الوسيطة –p 100 للتخطي إلى ١٠ صفحات (١٠٠ موقع) ، استنادًا إلى المعلومات المذكورة أعلاه، **حصلنا على نتيجة لعناوين URL الضعيفة التي تبدو كما يلي:**



شكل (٥٢) عناوين URL ا

لقد وجدنا ثمانية من مائة عنوان URL تم فحصها وتعتبر عرضة لهجوم حقن SQL ، احفظ عناوين URL في محرر النصوص لمزيد من الخطوات.

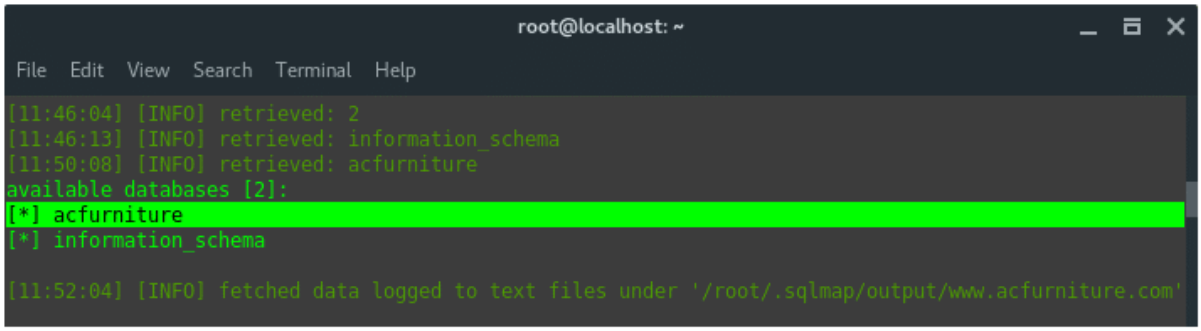
- **الخطوة ٣: حقن SQL باستخدام SQLMAP**

بمجرد حصولنا على هدف واحد على الأقل عرضة لحقن SQL، نقوم بعد ذلك بتنفيذ الهجوم باستخدام SQL Map ، وأغتنم واحدا منهم ليكون عينة هنا أولاً، نحتاج إلى الكشف عن اسم قاعدة البيانات، حيث يوجد داخل قاعدة البيانات جداول وأعمدة تحتوي على البيانات.

أ. عنوان URL المستهدف:

http://www.acfurniture.com/item.php?id=25

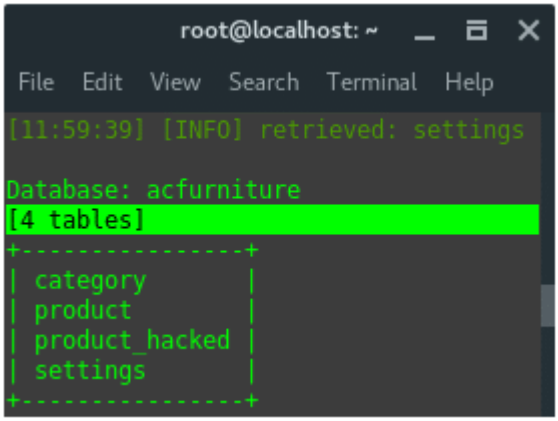
لذا، فإن الأمر المترجم سيبدو كما يلي:



شكل (٥٣) شاشة المترجم ١

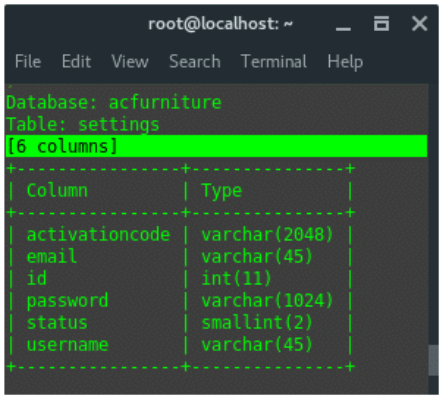
حصلنا على اسم قاعدة البيانات " acfurniture ".

ب. تعداد اسماء الجداول



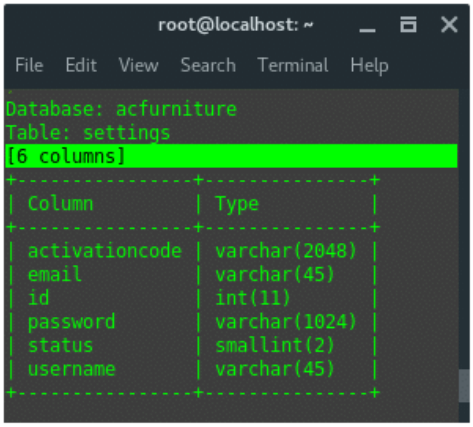
شكل (٥٤) اسماء الجداول

ج. تعداد الأعمدة



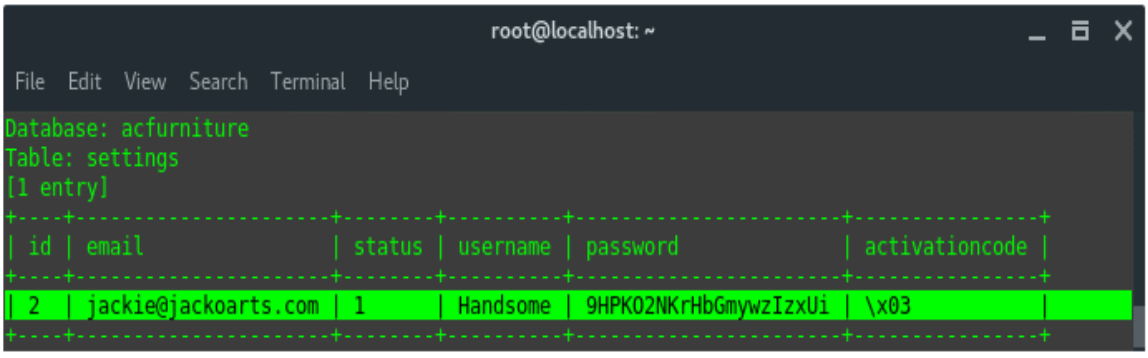
شكل (٥٥) الاعمدة !

يجب أن يبدو الإخراج كما يلي:



شكل (٥٦) النتيجة !

د. تفريغ البيانات



شكل (٥٧) تغريق البيانات !

٣- هجمات DDoS

- هجوم DDoS ، أو 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.
- غالبًا ما تُستخدم هجمات DDoS لإزالة مواقع الويب أو الخدمات عبر قد يكون من الصعب الدفاع ضدها.

٤- الهجمات القائمة على كلمة المرور

الهجوم المستند إلى كلمة المرور هو أي هجوم إلكتروني يحاول اختراق كلمة مرور المستخدم، هناك العديد من الهجمات المستندة إلى كلمة المرور الشائعة، فيما **يلي بعض أكثرها شيوعًا:**

- **هجمات القوة الغاشمة**

يحاول فيه المهاجم إدخال عددًا كبيرًا من كلمات المرور المحتملة حتى يعثر على الكلمة الصحيحة، يمكن منع ذلك باستخدام كلمات مرور قوية والحد من عدد محاولات تسجيل الدخول الفاشلة.

- **هجمات القاموس**

يستخدم المهاجم قائمة بالكلمات الشائعة وكلمات المرور لمحاولة تخمين كلمة المرور الصحيحة، يمكن منع ذلك باستخدام كلمات مرور قوية ليست كلمات شائعة.

- **هجمات الهندسة الاجتماعية**

يستخدم فيه المهاجم الخداع والخداع لحمل شخص ما على الكشف عن كلمة المرور الخاصة به، يمكن منع ذلك من خلال تدريب المستخدمين على عدم الكشف عن كلمات المرور الخاصة بهم لأي شخص.

٥- هجمات التصيد

- هجوم التصيد هو نوع من الهجمات الإلكترونية المصممة لسرقة البيانات المهمة، مثل بيانات اعتماد تسجيل الدخول أو المعلومات المالية.
- غالبًا ما يتم تنفيذ هجمات التصيد الاحتيالي عن طريق إرسال رسائل بريد إلكتروني يبدو أنها من مصدر شرعي، مثل أحد البنوك أو موقع الويب الذي تعرفه الضحية.
- سيحتوي البريد الإلكتروني على رابط يؤدي إلى موقع ويب مزيف مصمم لخداع الضحية لإدخال تفاصيل تسجيل الدخول أو المعلومات المالية.
- قد يكون من الصعب اكتشاف هجمات التصيد، حيث يمكن أن تبدو رسائل البريد الإلكتروني مقنعة للغاية، ومع ذلك، هناك بعض العلامات التي يمكن البحث عنها، مثل القواعد النحوية أو الأخطاء الإملائية، والشعور بالإلحاح في البريد الإلكتروني.

❖ منهجية الهجوم وأدوات الهجوم (عملي)

العديد من الهجمات تتم من خلال اختراق خوادم ومواقع الويب وهذه الهجمات هي الأكثر انتشاراً في الفترة الحالية.

- **منهجية عملية اختبار اختراق الويب مقسمة إلى أربعة مراحل**

- **منهجية الهجوم على موقع الويب يمكن أن يتم من خلال**

١. استهداف خادم الويب

الخادم هو جهاز بمواصفات عالية يقوم باستضافة موقع أو عدد من مواقف 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.

٢. استهداف موقع الويب

مواقع الويب يمكن أن تحوي على ثغرات برمجية والتي يمكن للمهاجم استغلالها وتعديل أو تخريب محتوى الموقع وأشهر هذه الثغرات هي SQL injection and XSS.

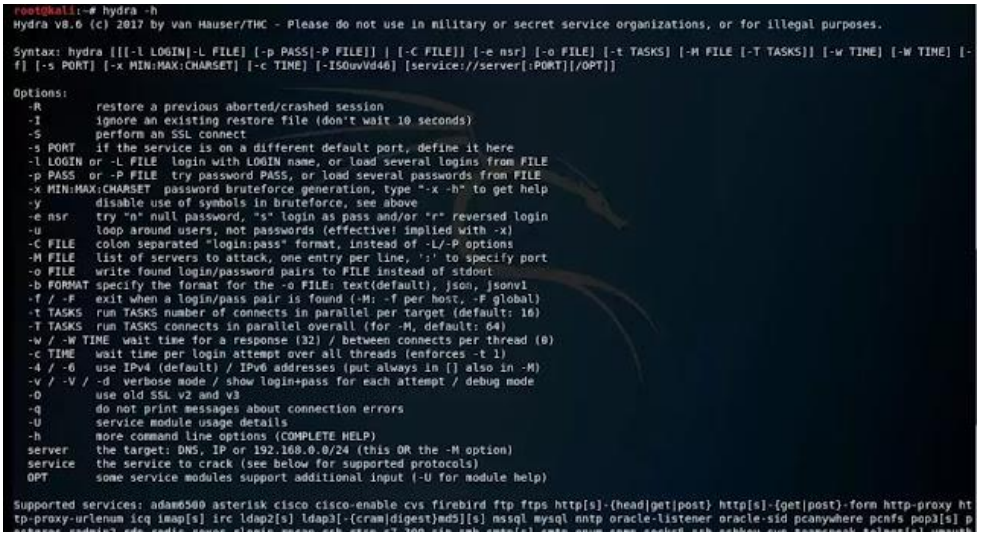
٣. استهداف المستخدم

يتم ذلك باستخدام الهندسة الاجتماعية كمحاولة لخداع مدير الموقع أو مستخدمي الموقع من اجل الحصول على معلومات تسجيل الدخول الخاصة بهم.

- **الثغرات**

١. ثغرات المصادقة وإدارة الجلسة

- عملية المصادقة تسمح بتسجيل الدخول إلى موقع الويب بينما إدارة الجلسة تتبع الطلبات والإجابات التي تتم خلال عملية التصفح.
- عملية المصادقة authentication وعملية إدارة الجلسة لم تؤخذان بعين الاعتبار عندما تم إيجاد بروتوكول HTTP ، لسوء الحظ فإن المصادقة وإدارة الجلسة تحوي على ثغرات كثيرة في العديد من مواقع الويب.
- هجوم المصادقة الأكثر شيوعاً يتم من خلال أدوات تسمح بتخمين كلمة السر باستخدام القوة الغاشمة brute force للتخمين على معلومات تسجيل الدخول مثل الأداة xHydra (موجودة بشكل تلقائي في Kali) ولها واجهة رسومية بسيطة ومن السهل التعامل معها.
- لا يوجد الكثير من السرية في هذا النوع من الهجوم، ولكنه ناجح جداً لأن معظم المستخدمين مازالوا يستخدمون كلمات سر ضعيفة.
- Hydra عبارة عن أداة تكسير تسجيل دخول متوازية تدعم العديد من البروتوكولات للهجوم، إنه سريع ومرن للغاية، ومن السهل إضافة وحدات جديدة ، تتيح هذه الأداة للباحثين والمستشارين الأمنيين إظهار مدى سهولة الوصول غير المصرح به إلى النظام عن بعد.



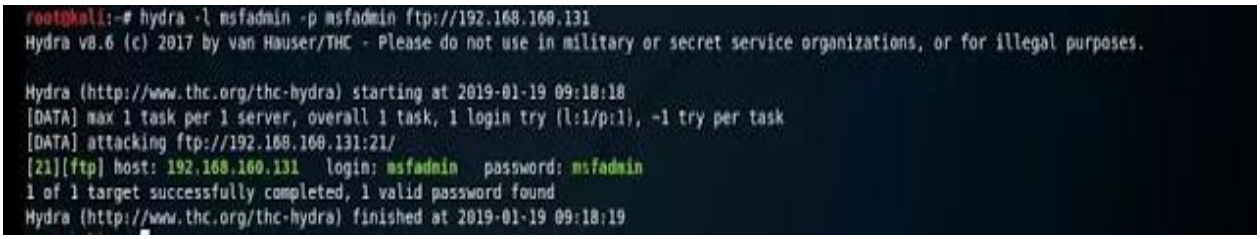
شكل (٥٨) اداة hydra ا

نحتاج إلى اسم مستخدم لقائمة أسماء المستخدمين وكلمة مرور أو قائمة كلمات مرور لتسجيل الدخول إلى خدمات الويب، يمكننا العثور على ملفات قائمة الكلمات في الدليل /usr/share/wodlists الخاص بـ Kali Linux.

إذا أردنا إنشاء قوائم كلمات مخصصة، فيمكننا استخدام crunch ، لتسجيل الدخول إلى بروتوكول نقل الملفات في المضيف المحلي لدينا **يمكننا استخدام الأمر التالي:**

hydra -l اسم المستخدم –

ftp://192.168.xx.xx كلمة المرور p اسم المستخدم –l- hydra

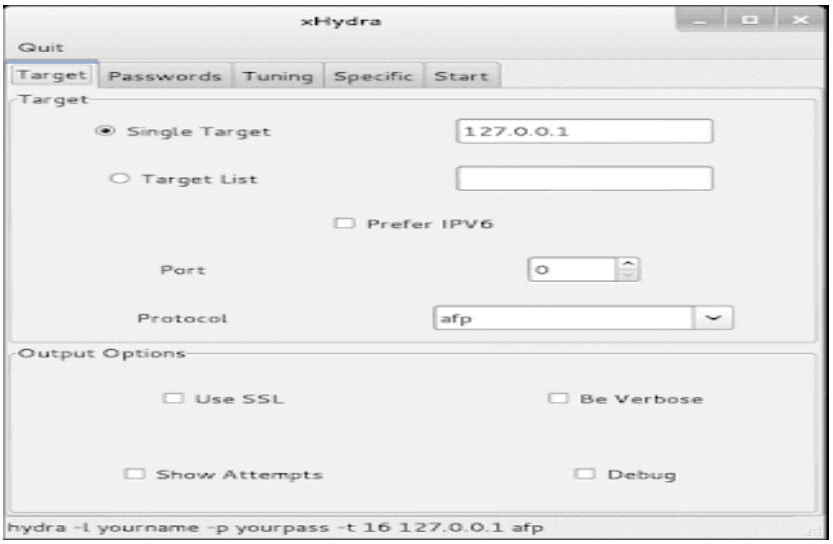


شكل (٥٩) hydra

لقد استخدمنا هنا العلامتين l- و p- لاسم مستخدم وكلمة مرور واحدة، ولكن يمكننا أيضًا استخدام L- و P- لقوائم الكلمات الخاصة باسم المستخدم وكلمة المرور.

hydra -L /path/of/usernames.txt -P /path/of/pasword.txt ftp://192.168.1.1

- هناك نسخة رسومية من هيدرا، تسمى xHydra ، كما أنه يأتي مثبتًا مسبقًا على جهاز Kali Linux الخاص بنا.
- يمكنك فتح xHydra من محطة Kali Linux باستخدام أمر xhydra .



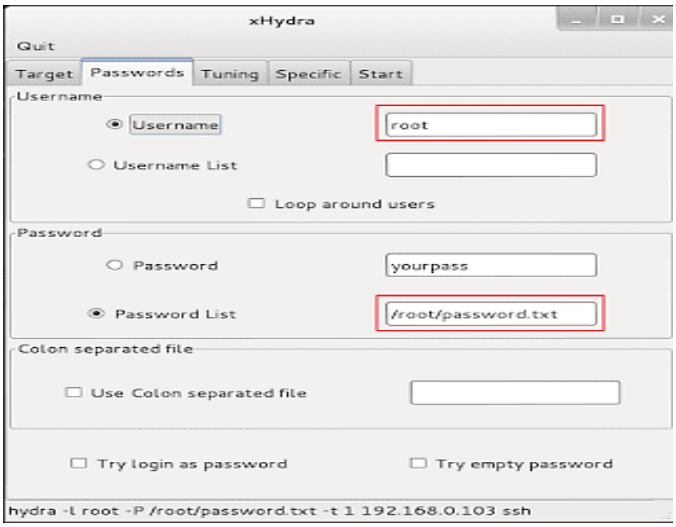
شكل (٦٠) hydra 1

- لقطة الشاشة أعلاه هي علامة التبويب المستهدفة لـ xhydra. دعنا نتعرف على جميع علامات التبويب وأنها تعمل.
- الهدف – حدد الهدف
- كلمات المرور – حدد خيارات كلمة المرور وقوائم الكلمات
- الضبط – حدد مدى السرعة التي يجب أن تعمل بها الهيدر ، تتوفر أيضًا خيارات توقيت أخرى.
- محدد – للاختبار على أهداف محددة مثل المجال، وكيل https وما إلى ذلك.
- البدء – بدء وإيقاف الهجوم ويظهر الإخراج.

في لقطة الشاشة التالية، اخترنا هدفًا وبروتوكولًا في علامة التبويب الهدف

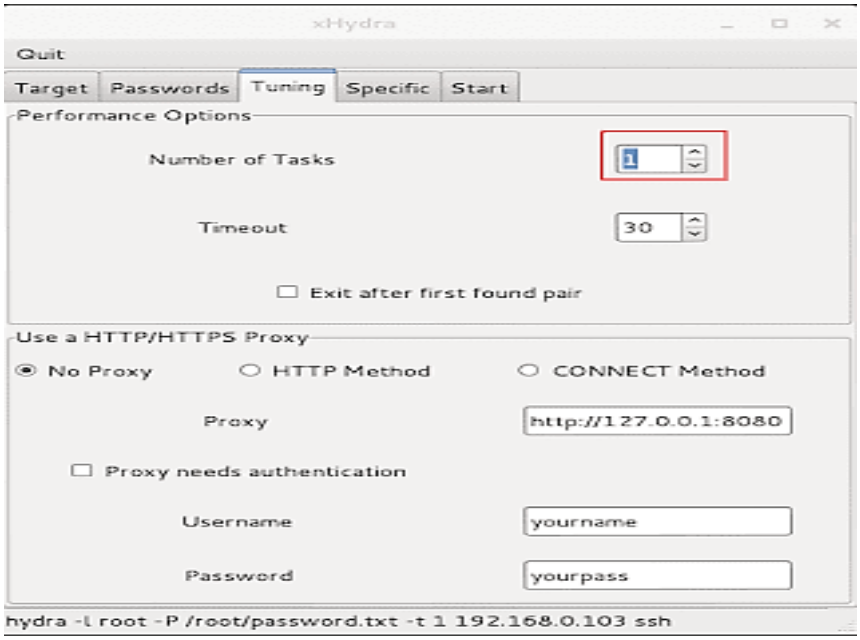
ثم في علامة التبويب كلمات المرور يمكننا إدخال اسم المستخدم أو قائمة أسماء المستخدمين وكلمة

المرور أو قائمة كلمات المرور، تحقق من example في لقطة الشاشة التالية:

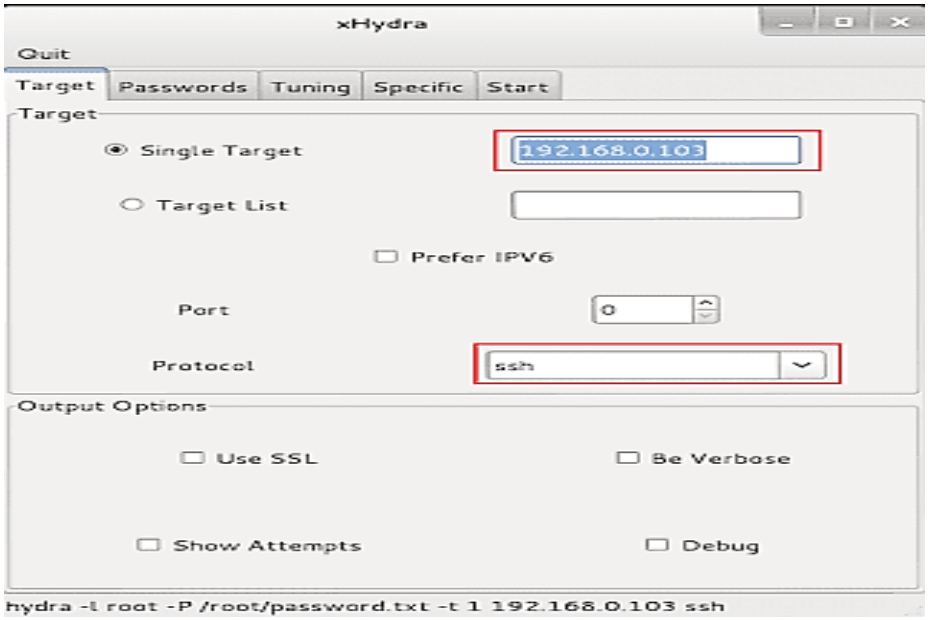


شكل (٦١) مهام xhydra 1

ثم تأتي علامة التبويب ضبط، نضع ١ في حقل " عدد المهام "



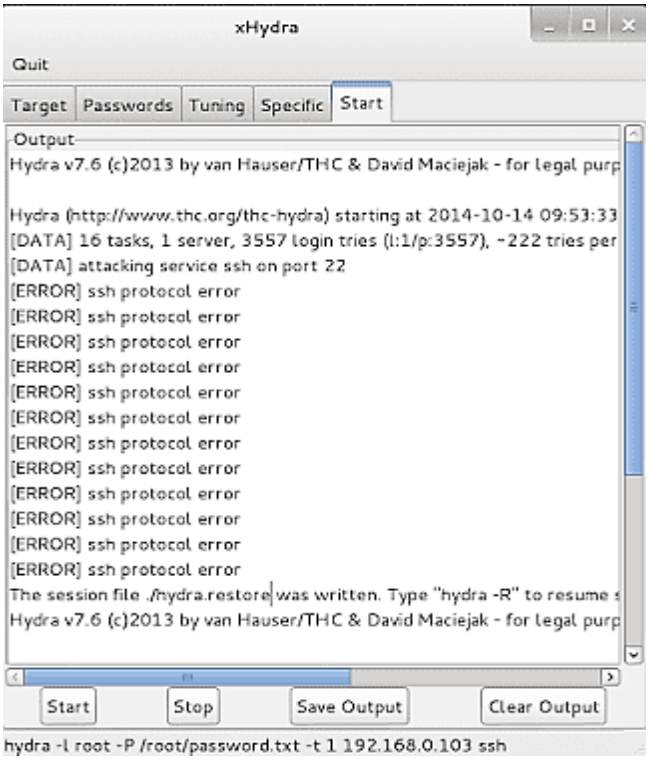
شكل (٦٢) مهام xhydra 2



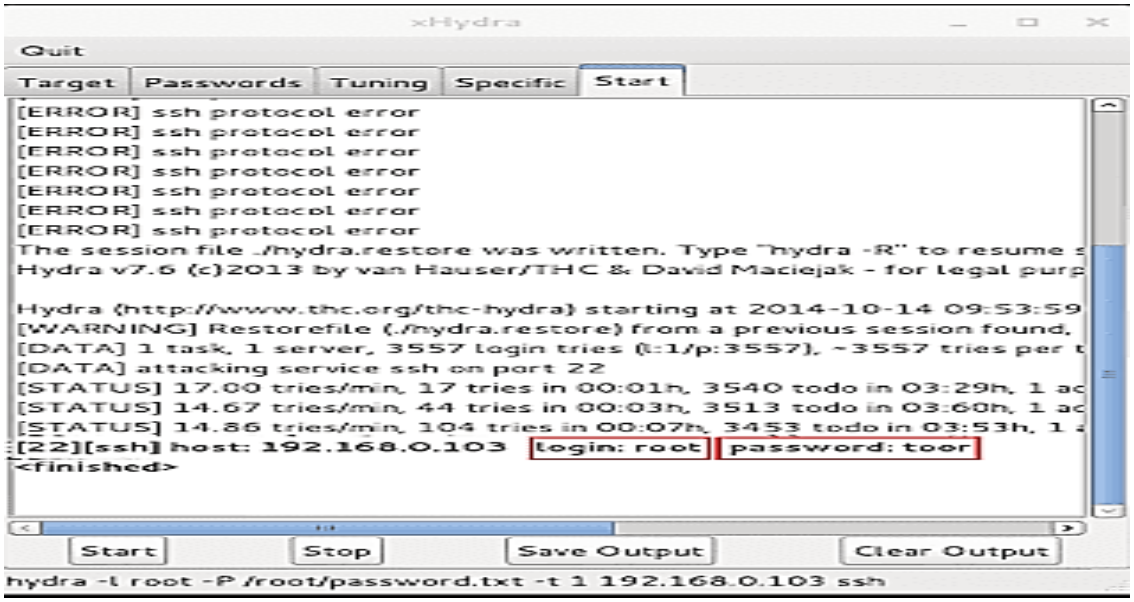
شكل (٦٣) مهام xhydra ٣

ثم ننتقل إلى علامة التبويب "ابدأ" ونختار خيار البدء في الزاوية اليسرى السفلية، لقطة الشاشة هي التالية/

مهاجمة إدارة الجلسة **يمكن فقط من خلال إحدى الطريقتين:**



شكل (٦٤) مهام xhydra ٤



شكل (٦٥) مهام xhydra 5

ثم ستبدأ العملية، عندما يقوم xHydra باختراق SSH، يمكننا رؤية اسم المستخدم وكلمة المرور أدناه،

كما هو موضح في لقطة الشاشة التالية:

```
┌──(kali㉿DESKTOP-SK08UEQ)-[/mnt/c/Users/RAJ/Desktop/javascript]
└─$ hydra -L user.txt -P pass.txt 192.168.29.135 ssh -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p
[DATA] attacking ssh://192.168.29.135:22/
[22][ssh] host: 192.168.29.135   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-
```

- مهاجمة آلية توليد معرف الجلسة.
- مهاجمة آلية استخدام معرف الجلسة وآلية تسليمها من قبل موقع الويب.
- مهاجمة آلية توليد معرف الجلسة صعب جداً لأن آلية توليد إدارة الجلسة تكون متضمنة داخل مخدم الويب الذي يقوم بإنشاء معرف الجلسة ومن الصعب جداً تخمينها.
- الهجوم الأكثر شيوعاً يتم من خلال اختبار كيفية استخدام معرف الجلسة من قبل الموقع وهذا النوع من الهجوم لا يتطلب منك فهم عملية توليدها، بل يركز على الوصول اليها وطريقة استخدامها.
- المهاجم يقوم بسرقة معرف الجلسة وإعادة استخدامها.
- هذه هي الطريقة التي يمكننا بها فرض كلمات المرور عبر الإنترنت باستخدام hydra وxHydra في Kali Linux هذه أداة قديمة جدًا ومفيدة لمختبري الاختراق.
- الأداة Firesheep وهي عبارة عن إضافة add-on خاصة بالإصدارات القديمة من المتصفح Firefox تسمح للمهاجم بالتقاط حزم البيانات اللاسلكية والحصول على معرف الجلسة الخاصة بالفيس بوك ومن ثم يقوم المهاجم بحقن المعرف في متصفحه ويمكنه الدخول إلى حساب الضحية بدون معرفة كلمة السر وهذه الطريقة يمكن أن تعمل مع مواقع التواصل الاجتماعي الأخرى.

٢– ثغرة تجاوز المسار Directory Traversal

تتم عملية تخصيص المساحات التخزينية للمواقع الإلكترونية ضمن المخدم المضيف أثناء إعداد وتشغيل مخدم الويب، يعمل كل موقع ضمن المساحة المخصصة له والتي تحتوي على الرمزات الخاصة بالموقع والصور والملفات بالإضافة إلى قواعد البيانات وملفات الموقع الأخرى، تحدث ثغرة تجاوز المسار عندما يتم إعداد مخدم الويب بحيث يسمح للمستخدم (المهاجم) بالتنقل بين مجلدات الموقع الإلكتروني.

يجب ضبط إعدادات المواقع الإلكترونية بحيث لا تتمكن من محاولة الوصول إلى موارد أو بيانات خارج حدود المساحة التخزينية المخصصة لكل موقع وذلك لأن هذه الموارد والبيانات ستكون حتماً مخصصة لمواقع أخرى.

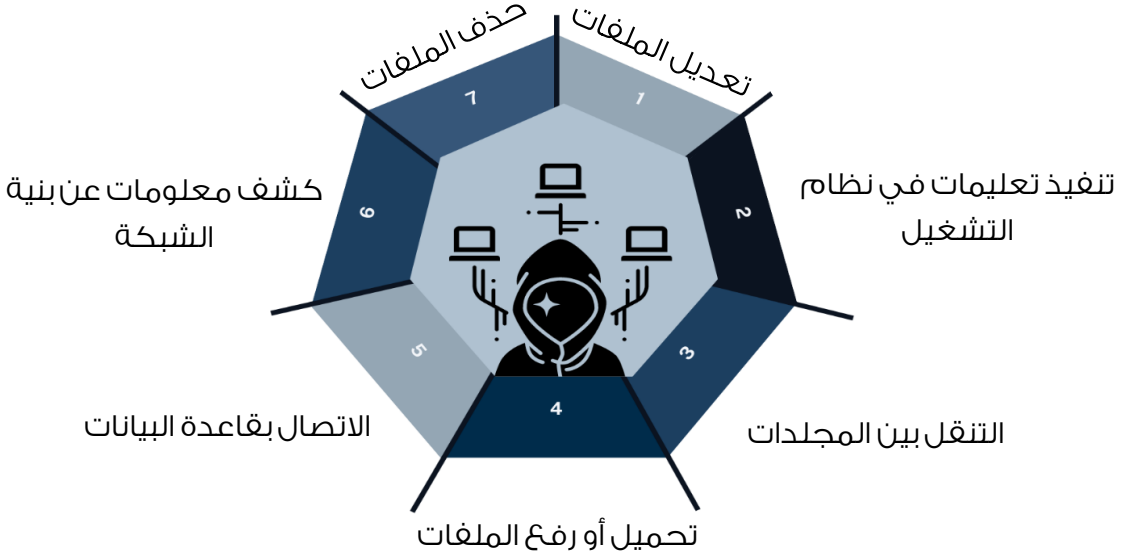
إذا استطاع المهاجم الوصول إلى خارج حدود المساحة المخصصة للموقع والوصول إلى المصادر الأخرى على مخدم الويب فهذا يسمى هجوم تجاوز المسار.

٣–ثغرة رفع الملفات File Inclusion

في حال وجود هذه الثغرة فإن المهاجم يستطيع رفع shell عبارة رمزا 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.

- يجب أن يكون الرمز مكتوب بلغة يدعمها مخدم الويب (php or asp).
- إذا كان المخدم الهدف يدعم PHP فيجب استخدام رمزا مكتوب بهذه اللغة.

وهي تسمح للمهاجم القيام ومن بعد بالأمور التالية:



٤– ثغرة الإعداد 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 أكثر صعوبة عندما لا تؤمن الحماية منع الوصول الغير مسموح به للموقع.

- **امثله على هذه الثغرة التي يمكن أن تكون في خادم الويب:**

الحماية الفعالة تتطلب إعدادات محمية تعرف وتنفذ على الموقع وعلى إطار العمل وعلى خادم الويب وعلى خادم قاعدة البيانات وعلى نظام التشغيل، كل هذه الإعدادات يجب أن تعرف وتنفذ بدل من إعدادات الحماية الافتراضية، وهذا يتضمن كل البرامج التي تتعامل مع البيانات ومكتبات الرمز البرمجي الذي يستخدمه التطبيق، بالإضافة إلى تطبيق سياسية صارمة تحدد الأشخاص المسموح لهم بالوصول إلى الخادم أو إدارة موقع الويب.

- **OWASP**

- هي أداة لفحص نقاط الضعف والثغرات في تطبيقات الويب أو المواقع وهي عبارة عن أداة مفتوحة المصدر مبرمجه بلغة Java .
- استهداف موقع testphp.vulnweb.com : وهو موقع لتجارب اختبار الاختراق.

١. اختيار الأداة وهي موجودة بقسم Web application analysis

٢. تظهر واجهة البرنامج – اختيار Automated Scan

٣. في هذه المرحلة يتم إضافة رابط الموقع المستهدف http://testphp.vulnweb.com/ او رقم الـ IP الخاص بالنظام والضغط على Attack.

٤. يبدا الفحص ويظهر عدة أشياء **مثل:**

أ– كم متبقي من الفحص.

ب– الروابط التي تم فحصها.

ت– عدد الثغرات الموجودة بالموقع.

- **تقسم الثغرات بالأداة الى ٤ أقسام حسب الألوان:**
  - احمر = خطير
  - برتقالي = متوسط
  - اصفر = ضعيف
  - ازرق = للتنبيه فقط

٥. بعد انتهاء الفحص تظهر نتائج جميع الثغرات بالموقع بقسم التنبيهات (Alerts) ومقسمة حسب الأخطر.

٦. تجربة ثغرة XSS يظهر تفاصيل الثغرة بالرابط المحدد.

٧. تجربة ثغرةSQL injection مع إضافة علامة تنصيص لنهاية الرابط.

- **OWASP**

OWASP هو اختصار لـ Open Web Application Security Project وتعني مشروع أمان تطبيق الويب المفتوح، وهي مؤسسة أو مشروع غير ربحي تأسست عام ٢٠٠١ تقوم بتكريس جهودها على هدفها الوحيد وهو تحسين ورفع كفاءة أمان التطبيقات، حيث أن لديها ٣٢٠٠٠ متطوع في جميع أنحاء العالم يقومون بإجراء بحوثهم الأمنية، وتتضمن مشاريعهم عدداً من برامج التطوير والأدوات مفتوحة المصدر والفعاليات والمؤتمرات، ولكن قد يكون مشروعهم الأكثر شهرة هو OWASP Top 10.

تعد OWASP Top 10 قائمة لتصنيف أهم ١٠ ثغرات لتطبيقات الويب، حيث يتم تصنيف المخاطر بناء على مدى خطورة الثغرات، كما أنها أيضاً تقوم بإعطاء بعض النصائح لكيفية تجنب مثل هذه الثغرات، وذلك ما يساعد مختبري الاختراق والمطورين أثناء عملهم مما يقلل انتشار هذه الثغرات الأمنية.

قامت OWASP بنشر قائمة Top 10 لأول مرة عام ٢٠٠٣ كما أنها تقوم بتحديثها كل عامين أو ثلاث سنوات لتعكس التطورات في أمن تطبيقات الويب، حيث بالنسبة للعديد تُعد المرجع الأول لاختبار اختراق تطبيقات الويب، كما أنها تُعد قائمة إرشادات مهمة أثناء عملية التطوير، حيث يعتبر دمجها في عملية تطوير التطبيقات (SDLC) من الممارسات الجيدة لضمان إنتاج تطبيقات ذات كفاءة أمنية مضاد للثغرات الأمنية الشائعة.

آخر تحديث للقائمة تم إصداره في العام ٢٠٢١ ويحتوي على:

- **Broken Access Control**

يكون هدف أنظمة التحكم في الوصول (Access Control) في ضمان وصول المستخدمين الشرعيين فقط إلى البيانات أو الوظائف المطلوبة، ولكن ماذا يحدث إذا وصل مستخدم لا يحق له الوصول إلى تلك البيانات؟ هذا هو الـ Broken Access Control فهي نقطة ضعف تسمح لمستخدم لا يحق له الوصول لتلك البيانات بتجاوز عناصر التحكم، على سبيل المثال الوصول لبيانات مستخدم آخر عن طريق تغير الـ ID الخاص بالمستخدم.

- **Failures Cryptographic**

خصوصية البيانات وأمنها لا تقدر بثمن للمحافظة على ثقة المستخدمين، يحدث فشل التشفير (Cryptographic Failures) أو كما كان يعرف في قائمة OWASP Top 10 للعام ٢٠١٧ بـ (Sensitive Data Exposure) عند الحفاظ على البيانات دون تشفير (Plain Text) أو استخدام خوارزميات تشفير ضعيفة قابلة للكسر أو على سبيل المثال تكرار استخدام الـ (Salt Value) عند تشفير كلمات المرور.

- **Injection**

عدم الثقة بمدخلات المستخدمين حيث تصبح ثغرات الحقن (Injection) خطراً يهدد أمان تطبيق الويب، تمكن ثغرات الحقن المهاجمين بإدخال بيانات واستعلامات ضارة تؤدي لإتاحة الوصول إلى بيانات حساسة، وأشهر مثالين على هذا النوع هما الـ XSS Injections & SQL.

- **Insecure Design**

بينما تتعامل العديد من الثغرات الأمنية مع أخطاء في التنفيذ، هنا يختلف الوضع لتصف هذه الثغرة فشلاً في التصميم لعدم وجود ضوابط الأمان أو الضوابط غير الفعالة، حيث يتم إنشاء التطبيق دون مراعاة لأي معايير أمنية.

- **Misconfiguration Security**

للإعدادات الأمنية غير المكتملة العديد من الأمثلة مثل وجود منافذ (Ports) مفتوحة غير ضرورية أو عدم حذف الحسابات الافتراضية أو رسائل الأخطاء التي تحتوي على كثير من المعلومات التي قد يساء استخدامها.

- **Vulnerable and Outdated Components**

تتعرض تطبيقات الويب لهذا النوع من الثغرات عند استخدام مكونات ومكاتب برمجية غير محدثة أو غير مدعومة من قبل المطورين مما يجعل تطبيق الويب عرضة للهجمات التي تقوم باستغلال تلك المكونات.

- **Identification and authentication failures**

تطلب العديد من تطبيقات الويب إثباتاً للهوية للتحقق من المستخدم لتسمح له باستخدام خدامتها، هنا يأتي خطر فشل التحقق من الهوية مما يسمح للمهاجم الوصول لكلمات المرور والجلسات، وذلك يحدث عند استخدام عملية مصادقة ضعيفة للهوية أو عدم استخدام مصادقة متعددة العوامل (MFA).

- **Software and Data Integrity Failures**

يعتمد العديد من تطبيقات الويب على الـ Plugins وLibraries وCDNs والتي ربما قد تكون من مصادر غير موثوق فيها والتي تقوم بإرسال التحديثات تلقائياً دون الرجوع لتطبيق الويب ليتأكد من سلامة التحديثات، ذلك ما قد يؤدي إلى وجود تحديثات ضارة تعرض تطبيق الويب وسلامة بياناته.

- **Failures Security Logging and Monitoring**

يؤدي الافتقار إلى سجلات الأمان والمراقبة للسماح بمرور اختراقات أمنية دون أي ملاحظة، مما يؤدي إلى فشل فرق التحقيق والاستجابة للحوادث لعدم وجود سجلات أو عدم وجود المحتوى الكافي الذي يتم تخزينه في السجلات أو أن السجلات تعرضت للحذف أو التعديل نتيجة عدم تأمينها بشكل كاف.

- **Server-Side Request Forgery (SSRF)**

عند القيام بإرسال طلب مزور عن طريق السيرفر لـ End Point غير متوقعة دون التحقق من صحة الـ URL، قد تكون بداخل السيرفر واستخدامه كجهة موثوق فيها أو خارجه للوصول إلى معلومات لا يجب الوصول إليها، رغم أن ثغرات الـ SSRF نادرة نسبياً إلا أن لها تأثيراً كبيراً إذا تم التعرف عليها واستغلالها.

- **NMAP**

أداة تُستخدم لمسح المنفذ، كالي لينكس يحتوي على أداة NMAP التي تُستخدم للتعرف على المنافذ المفتوحة و للتعرف على نظام التشغيل والخدمات المثبتة على الأجهزة البعيدة وهي الأداة الأكثر شهرة للقيام بعملية فحص المنافذ Port Scanning ويوجد العديد من أنواع الفحص التي تستطيع هذه الأداة القيام بها، عند معرفة عنوان خادم الويب الهدف IP Address بتنفيذ الأمر

```
#Nmap -sV -O -p- 127.0.0.1
```

-sV ← لتحديد الإصدار Version الخاص بالخدمات المكتشفة.

-O ← تعطي معلومات متعلقة بنظام التشغيل كنوع النظام أو إصداره.

-p- ← للقيام بعملية فحص لكل المنافذ.

127.0.0.1 ← عنوان IP Address للهدف.

نتيجة تنفيذ هذا الأمر هو معرفة الخدمات التي تعمل على خادم الويب للبحث عن الثغرات والقيام باستغلالها.

وإحدى طرق استخدام Nmap هي الطريقة التي تتضمن scripts للقيام بعملية بحث مخصصة من خلال طلب script يؤمن معلومات معينة عن الهدف المطلوب ويمكن استدعاء الـ sript من خلال إضافة Sript<--script name> إلى أمر Nmap.

ناتج عملية فحص المنافذ التي تقوم بها Nmap يمكن أن تربط بشكل مباشر مع العملية التي يتم فيها استخدام Nessus & Nikto للبحث عن الثغرات في خادم الويب.

- **Metasploit**

أداة تستخدم لاستغلال خادم الويب وتمكن من تنسيق خدمات تقييم أمن تطبيقات الويب والشبكات ومستخدمي البريد الإلكتروني واختبار قواعد البيانات.

- **Wfetch**

هي أداة تعرض الطلب والاستجابة بحيث يمكن فهم الاتصال بسهولة، يمكن استخدامها لإنشاء طلبات HTTP تختبر أداء مواقع الويب الجديدة أو مواقع الويب التي تحتوي على عناصر جديدة، مثل صفحات الخادم النشطة (ASP) أو البروتوكولات اللاسلكية وهي تساعد على حل المشاكل المتعلقة بالتفاعل مع متصفح خادم الويب.

❖ مهاجمة تطبيقات الويب (عملي)

مرحلة الاستطلاع والفحص لتطبيق الويب تؤمن تفاصيل ومعلومات حول المصادر مثل الصفحات والملفات والمجلدات والروابط والصور المكونة لتطبيق الويب ويوجد أجزاء من المعلومات التي يمكن أن تُستخدم خلال عملية استغلال تطبيق الويب.

القيام بعملية استطلاع تطبيق الويب تتضمن اكتشاف كل مصدر يتفاعل معه التطبيق، فقط المصادر التي تم اكتشافها خلال عملية الاستطلاع سوف يتم فحصها، **والأدوات المستخدمة في عملية استطلاع تطبيق الويب تتضمن:**

- بروكسي اعتراض لكشف كل طلب HTTP/S مُرسل من المتصفح وكل إجابة يتم إرسالها من تطبيق الويب، Spiderinf tool لجعل الطلبات بشكل أوتوماتيكي لتطبيق الويب.
- باحث عن ثغرات مخصص لتطبيقات الويب للبحث في المصادر المُكتشفة لتحديد الثغرات.
- أداة brute forcing لاكتشاف المجلدات الأكثر استخداما في تطبيق الويب والتي يمكن أن تكتشف المزيد من المصادر.

- **أساسيات بروكسي الويب**

مهم في عملية اختبار اختراق الويب ويجب إعداد البروكسي ليعمل في المتصفح، فالمتصفح المُستخدم يرسل طلبات إلى تطبيق الويب والتطبيق يرد بإرسال الإجابات إلى المتصفح عند استخدام الإنترنت.

البروكسي يسمح برؤية دورة العمل هذه من طلبات وإجابات لأن البروكسي يكون بين المتصفح وتطبيق الويب ويتحكم بتدفق البيانات من الطلبات والإجابات.

عند القيام بإعداد البروكسي يمكن فحص كل طلب وكل إجابة تمر من خلاله ويمكن اعتراض وتغيير قيم البارامترات المستخدمة في هذه العملية وهي عملية في استغلال تطبيقات الويب.

كما يتم استخدام بروكسي الويب لحفظ تاريخ أو لفهرسة كل الطلبات والإجابات التي تمر من خلاله.

- **هجمات التطبيق**

نقاط الضعف في تطبيقات الويب التي تعمل على الخادم توفر مسار واسع من الهجوم **منها:**

- **اجتياز الدليل "Directory Traversal"** وهو استغلال HTTP والتي يكون من خلالها المهاجم يستطيع الوصول إلى المجلدات المقيدة وتنفيذ الأوامر خارج المجلد الجذري لخادم الويب.
- **Parameter /Form Tampering** ويهدف هذا الهجوم على التعامل مع المعلمات المتبادلة بين العميل و الخادم من أجل تعديل بيانات التطبيق مثل ورق اعتماد المستخدم و كمية المنتجات.
- **Cookie Tampering** يتم الهجوم عند إرسال ملفات cookies من جانب العميل إلى الخادم ويمكن تعديلها باستخدام أدوات خاصة.
- **Command Injection Attacks** هو هجوم يقوم فيه المهاجم بتغيير محتوى صفحة الويب باستخدام الكود وعن طريق تحديد حقول تفتقر القيود الصالحة.
- **Buffer Overflow Attacks** تم تصميم معظم تطبيقات الويب للحفاظ على كميات من البيانات ، إذا تم تجاوز هذا يحدث عطل للتطبيق ويستخدم المهاجم هذه الميزة.
- **Cross-Site Scripting** هي طريقة من المهاجم لحقن HTML tags في موقع على شبكة الإنترنت الهدف.
- **هجوم الحرمان من الخدمة (DoS)** وفيها يهدف المهاجم إلى إنهاء عمليات موقع على شبكة الإنترنت أو خادم لجعله غير متاح لوصول المستخدمين.
- **Unvalidated Input anf File injection Attacks** هي هجمات تقوم بتحميل unvalidated input أو حقن الملفات إلى تطبيق ويب.
- **Cross-site request forgery (CSRF) Attacks** في هذا الهجوم تقوم صفحة ويب خبيثة بطلب من متصفح الويب المستخدم بإرسال الطلبات إلى الموقع على شبكة الإنترنت الخبيثة حيث يتم تنفيذ إجراءات ليست للمستخدم وهو خطير في حالة المواقع المالية.
- **SQL Injection Attacks** هو تقنية لحقن أكواد تستخدم ثغرة أمنية موجودة في قاعدة بيانات للهجمات.
- **Session Hijacking** هو هجوم يستغل المهاجم آلية الرقابة لجلسة المستخدم الصالحة الحقيقية للوصول إلى أجزاء موثقة من تطبيق الويب.

على سبيل المثال، أثناء القيام بفحص رصيد البطاقة الائتمانية أو سداد الفواتير أو التسوق في متجر عبر الإنترنت، عادةً ما يستهدف مخترقو الجلسات جلسات المتصفح أو تطبيقات الويب، حيث يمكن للمهاجم الذي يقوم باختطاف الجلسة بعد ذلك القيام بأي شيء يمكن القيام به على الموقع، في الواقع، يخدع أحد.

- **ثغرات SQL injection**

SQL injection هي أقدم ثغرات مواقع الويب ومازالت منتشرة حتى الإن وتعتبر من اكبر المخاطر على مواقع الويب.

- **ثغرات SQL injection تحدث لسببين:**

١. ضعف في عملية تنقيح دخل المستخدم (المبرمج لم يقم بعملية تصفية لمتغير الدخل).

٢. البيانات والتحكم مدمجان في نفس قناة النقل.

الضعف في عملية تنقيح دخل المستخدم تسمح للمهاجم بالقفز من الجزء الخاص بالبيانات (السلسلة النصية الموجودة بين إشارات تنصيص مفردة) إلى حقن تعليمات تحكم (مثل SELECT, UNION, AND, OR).

تتم عملية تدفق المعلومات في بنية مؤلفة من ثلاث صفوف هي: المستخدم، خادم الويب، خادم قاعدة البيانات.

١. المستخدم يرسل طلب إلى خادم الويب.

٢. خادم الويب يقوم بتضمين طلب المستخدم ضمن عبارة SQL ويرسلها كطلب (استعلام) إلى خادم قاعدة البيانات.

٣. يقوم خادم قاعدة البيانات بتنفيذ طلب SQL بدون أن يعرف منطق التطبيق، فقط يقوم بتنفيذ الطلب ويعيد النتيجة إلى خادم الويب.

٤. يقوم خادم الويب بإنشاء صفحة HTML بشكل ديناميكي بالاعتماد على الإجابة القادمة اليه من خادم قاعدة البيانات ويرسلها إلى المستخدم.

٥. خادم الويب وخادم قاعدة البيانات منفصلان، خادم الويب فقط يقوم بإنشاء طلب SQL ويترجم النتيجة ويعرضها للمستخدم أما خادم قاعدة البيانات فهو يستقبل طلب SQL ويعيد النتيجة إلى خادم الويب وهذا مهم جداً من أجل استغلال ثغرات SQL injection لأن التحكم بعبارة SQL وجعل خادم قاعدة البيانات يعيد بيانات مهمة مثل أسماء المستخدمين وكلمة السر.

رسائل الخطأ المختلفة الصادرة عن خوادم قواعد البيانات والتي يتم الحصول عليها من خادم الويب عندما القيام باختبار ثغرة SQL injection .

- **الخطوات التالية تبين كيفية حدوث خطأ SQL injection وكيف يتعامل خادم الويب معه**

١. المستخدم يرسل طلب لمحاولة معرفة إذا كانت ثغرة SQL injection موجودة في هذا التطبيق، في هذه الحالة المستخدم يرسل القيمة أو الاسم مضافاً اليه علامة تنصيص مفردة.

٢. سيقوم خادم الويب بتضمين بيانات المستخدم ضمن طلب SQL إلى خادم قاعدة البيانات، في هذا المثال فإن عبارة SQL التي سينشئها خادم الويب سوف تحتوي على دخل المستخدم وعلامة التنصيص المفردة المضافة من قبل المستخدم بالإضافة إلى علامة تنصيص مفردة أخرى يقوم التطبيق بإضافتها.

٣. خادم قاعدة البيانات يستقبل طلب SQL غير سليم ويعيد رسالة خطأ إلى خادم الويب.

٤. يستقبل خادم الويب رسالة الخطأ من خادم قاعدة البيانات ويرسلها كإجابة على شكل HTML إلى المستخدم.

سيتم إعادة النتيجة في الخطوة الرابعة بإحدى هذه الطرق:

- SQL error يعرض على متصفح المستخدم.
- SQL error يخفي في مصدر صفحة الويب لأغراض تصليح الأخطاء.

- إعادة التوجيه إلى صفحة أخرى

HTTP error code 500 (خطأ داخلي بالخادم) أو HTTP redirection code 302

- التطبيق يتعامل مع الخطأ بشكل فوري ويظهر انه لا يوجد نتيجة أو يظهر صفحة خطأ عام.
- مُختبر الاختراق يستطيع استغلال ثغرة حقن الكود من خلال تقديم دخل يدوي خبيث يجعل تطبيق الويب يقوم بعمل غير مسموح به كعرض معلومات مهمة مثل الأسماء وكلمات السر أو تنفيذ تعليمات النظام مثل إضافة حساب مدير.
- هجوم حقن الكود من أخطر أنواع الهجمات التي تتعرض لها تطبيقات الويب بسبب قوة تأثيرها وعدد المستخدمين الذي مازالت الثغرة منتشرة في تطبيقاتهم، هجوم حقن الكود يتم نتيجة لنقص في إجراءات الحماية.
- تطبيقات الويب تصنع من قبل مبرمج وبالتالي حدوث أخطاء هو أمر وارد وهذه الأخطاء هي سبب لوجود الثغرات.

- **بعض أنواع الحقن في تطبيقات الويب**

١. حقن طلبات Structured query language (SQL)

٢. حقن طلبات Lightweight directory access protocol (LDAP)

٣. حقن طلبات XML path language (XPATH)

٤. حقن تعليمات نظام التشغيل

هجوم الحقن هو القيام بالهجوم أثناء التفاعل مع تطبيق الويب كمستخدم مصرح له وهذا يعني أن البيانات الخاصة به وإجابات تطبيق الويب سوف تبدو مماثلة للطلبات الأخرى غير الخبيثة.

المهاجم يستطيع إنشاء دخل خبيث ويدخله في صندوق البحث لاستغلال ثغرة SQL injection مع المحافظة على كتابة الدخل بين علامات التنصيص لكي لا تظهر رسالة خطأ.

مثال كلاسيكي على هذا الاستغلال هو إدخال التالي إلى صندوق البحث:

Ahmed'OR 1=1'#

- هذا الدخل سيبنى عبارة SQL التالية وإرسالها إلى المترجم ليقوم بتنفيذها

```
SELECT * FROM users WHERE UserName='Ahmed'OR 1=1'#
```

إشارة # هي inline comment تجعل المترجم يتجاهل كل شيء بعدها نتيجة عبارة SQL لهذا الرمز المحقون **هي:**

```
Select * From users Where username='Ahmed'OR 1=1
```

أصبح الدخل (Ahmed) بين علامتي التنصيص فالعلامة الأولى تكون مكتوبة مسبقاً من قبل المبرمج والعلامة الثانية تم إدخالها بعد الدخل.

- إشارة التنصيص (') التي يتم أضافتها إلى نهاية دخل المستخدم من قبل التطبيق سيتم تجاهلها بسبب وجود # التي هي inline comment.

لن يتم عرض اسم المستخدم Ahmed فقط، بل سيتم عرض كل المستخدمين الموجودين لأن ١ = ١ دائماً محققة.

- يمكنك أيضا حقن سلسلة نصية وترك علامة التنصيص معلقة **كالتالي:**

```
'Ahmed'OR 'a'='a
```

يتم تحديد أين ستضاف علامة التنصيص (') وبالتالي النتيجة ستكون عبارة SQL صحيحة وستصبح **كالتالي:**

```
Select * FROM users WHERE UserName='Ahmed' OR 'a'='a'
```

- **هجوم SQL injection**

سوف يتم استخدم بيئة DVWA (موقع ويب تجريبي يحوي على ثغرات) لمحاولة استخراج اسم المستخدم وهاش كلمة السر الخاص بمدير الموقع.

- **إيجاد ثغرة SQL injection**

إشارة التنصيص المفردة ستؤدي إلى خلل في صيغة التعليمة والموقع سوف يرد برسالة خطأ، يمكننا محاولة معرفة إذا كان DVWA يحوي على ثغرة SQL injection من خلال استخدام نفس الطريقة أي إدخال إشارة تنصيص مفردة (') في User ID textbox ، أو بدل ذلك سوف يتم القيام بإدخال سلسلة نصية مع إشارة تنصيص مفردة **كالدخل التالي:**

Damn Vulnerable Web Application

البرنامج:

PHP/MySQL web application

الرابط:

/https://sourceforge.net/projects/dvwa.mirror

في هذا الموقع كل دخل المستخدم يكون مغلف بين مجموعتين من إشارات التنصيص المفردة (ليست إشارة تنصيص مزدوجة).

- لعرض محتوى العامودين user and password من جدول قاعدة البيانات **يتم إدخال العبارة التالية:**

Ahmed' and 1=1 union select null, concat (user, 0x0a, passoword) from users#

- النتائج التي سوف تظهر هي القيم التي يسعى المخترق للحصول عليها.
- سوف يتم الحصول على اسم وكلمة السر لكل مستخدم في قاعدة البيانات.
- كلمات السر لن تظهر كنص صريح، سوف تكون على شكل hash ومن السهل جداً كسر هذا النوع من الهاش وهو بالتحديد من نوع MD5 hash لأنه عبارة عن ٣٢ رقم ستة عشري.
- لمعرفة نوع الهاش يمكن استخدام أداة Hash-ID وهي تساعد على معرفة نوع الهاش الذي يكون أكبر من ٥٠ حرف أو رقم وهذه الأداة موجودة بشكل تلقائي بنظام Kali , أو استخدام أداة مثل John the Ripper (JtR) أو للاختصار فقط John لكسر الهاش والحصول على كلمة بشكل نص صريح.
- استخدام هذه الأداة سهل جداً، فقط يتم نسخ ولصق الأسماء وكلمات السر إلى ملف نصي وتقديمه للأداة ثم انتظار إظهار النص الصريح لكلمة السر لكل مستخدم.

- **أدوات حقن الـ SQL**
  - **أداة Sqlmap**

هي أداة لحقن تعليمات وأوامر SQL موجودة في نظام كالي لينكس وهي تقوم بشكل تلقائي باكتشاف واستغلال ثغرات حقن SQL injection وتملك محرك بحث خارجي وعدة خيارات تمنح المهاجم مجال أكبر لتنفيذ الهجوم ضد تطبيقات الويب وهي أداة مفتوحة المصدر و مجانية وتُستخدم في اختبار الاختراق وتحليل الأمان لتطبيقات ومواقع الويب التي تعتمد على قواعد البيانات ، يمكن استخدام الأداة لاستكشاف واستغلال ثغرات الأمان المتعلقة ، بقواعد البيانات وتنفيذ الأوامر SQL الخبيثة وذلك بهدف معرفة مدى قابلية هذه التطبيقات للاختراق وحمايتها من مثل هذه الهجمات.

- **Sqlmap تستخدم إشارات مثل:**

-u	تستخدم لتحديد عنوان url الهدف للصفحة المصابة بالثغرة.
--cookies	تستخدم لتحديد cookies الخاصة بالجلسة للوصول إلى التطبيق أثناء عملية الهجوم.
-b	لعرض banner الخاص بقاعدة البيانات.
--current-db	لعرض نظام إدارة قاعدة البيانات الحالية. لعرض نظام إدارة قاعدة البيانات للمستخدم الحالي.
--string	لتأمين قيمة نصية لتعريف الإيجابيات الخاطئة.
--users	لعرض مستخدمي نظام إدارة قاعدة البيانات.
-U	لتحديد مستخدم إدارة قاعدة البيانات لتضمينه بالهجوم.
--Privileges	لعرض صلاحيات المستخدم.
--dbs	لعرض أسماء كل قواعد البيانات الموجودة في خادم قاعدة البيانات.
-D	لتحديد أي قاعدة بيانات كهدف.
--tables	لعرض كل الجداول في قاعدة البيانات الهدف.
-T	لتحديد الجدول الهدف.

❖ أدوات اختراق تطبيقات الويب

هي تقنيات مستخدمة من قبل المهاجمين في كسر كلمات المرور ومهاجمة خادم الويب.

- **Burp suite**

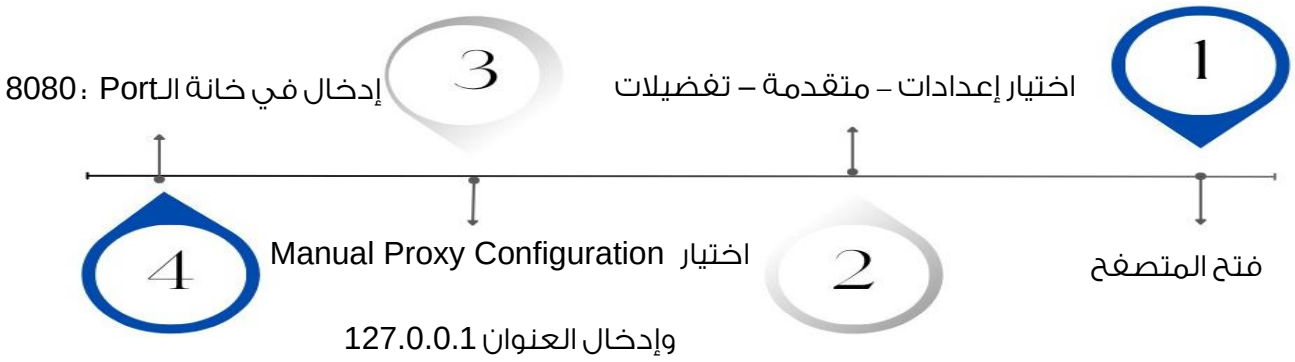
يستخدم في اختطاف الجلسة Session Hijacking من خلال التعرف على الجلسة الحالية للمستخدم الهدف والاستيلاء عليها من قبل المهاجم بمجرد تأسيس المستخدم مصادقة الاتصال مع الخادم كما إنها أداة ضرورية في أي عملية اختبار اختراق الويب وهو يستخدم كبروكسي خاص للمخترق وهو موجود بنظام كالي لينكس بشكل تلقائي.

يتم استخدام عدة أدوات في Burp suite خلال عملية الاختراق ويمكن الوصول لها من favorite bar.

- **إعداد Burp Proxy**

من أجل الحصول على كل طلبات وإجابات HTTP/S يجب القيام بإعداد المتصفح لاستخدام بروكسي

من خلال الخطوات التالية:



- **Cookie Digger**

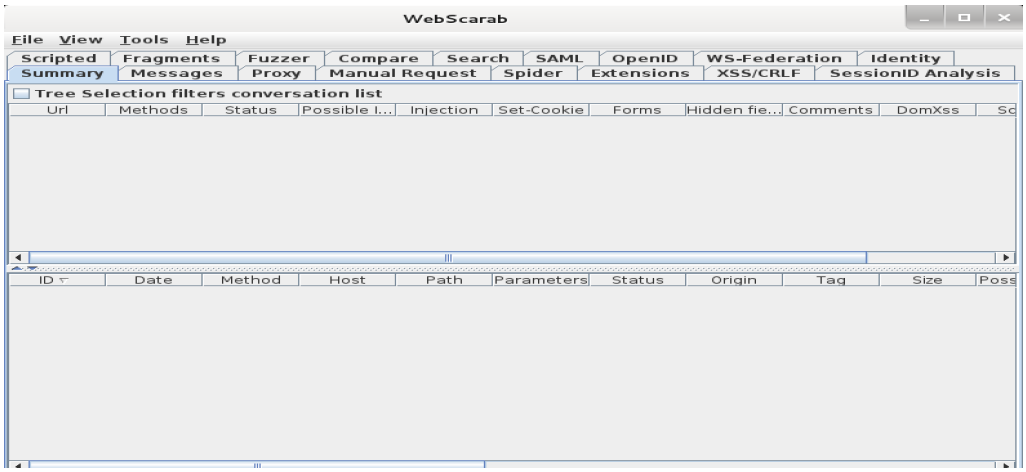
- يساعد Cookie Digger في تحديد إنشاء ملفات تعريف الارتباط الضعيفة والتطبيقات غير الآمنة لإدارة الجلسة بواسطة تطبيقات الويب.
- تعمل الأداة من خلال جمع وتحليل ملفات تعريف الارتباط الصادرة عن تطبيق ويب لعدة مستخدمين.
- تقارير الأداة عن إمكانية التنبؤ لملف تعريف الارتباط وما إذا كانت المعلومات الهامة، مثل اسم المستخدم وكلمة المرور، مضمنة في قيم ملف تعريف الارتباط.

يمكن عمل لها Download: https://cookiedigger.apponic.com/

- **WebScarab**

أداة WebScarab يتم تشفير عنوان URL عن طريق استبدال كافة الأحرف غير المسموح بها بعلامة % متبوعة برقمين سداسيين عشريين ، تمثل هاتان القيمتان السداسية العشرية القيم الرقمية للحرف في مجموعة أحرف ASCII ، على سبيل المثال، المسافة غير مقبولة في عنوان URL ويتم استبدالها بعلامة "٢٠%" أو علامة "+" أثناء التشفير ، وبالمثل، يتم استبدال علامة $ بـ "٢٤%".اة تقوم بإنشاء بروكسي بين المتصفح وبين الموقع ، وتعديل البيانات التي ايتم إرسالها ، كما تقوم أيضا بتسجل كل الحركات على المتصفح ، ويمكنك ربطها بالعديد من المتصفحات مثل Firefox و chrome والعديد .

يمكن من خلال الأداة عمل تحليل ومحاولة اكتشاف ثغرات تطبيقات الويب ويوجد الكثير من الأدوات المفيدة في الأداة.



شكل webscarab (61)

❖ التدابير المضادة والحماية من عمليات اختراق خوادم وتطبيقات الويب (عملي)

١. استخدام ملف جدار حماية تطبيق الويب (WAF) لتصفية التعليمات البرمجية الضارة.

٢. استخدام التحقق من صحة الإدخال، مما يعني فحص إدخال المستخدم بحثًا عن تعليمات برمجية ضارة قبل معالجتها بواسطة الخادم.

٣. استخدام تشفير الإخراج، والذي يحول الأحرف الخاصة إلى معادلات كيان HTML الخاصة بهم.

٤. التحقق الدائم من صحة إدخال المستخدم قبل إدخاله في قاعدة البيانات الخاصة.

٥. استخدام الاستعلامات ذات المعلمات متى أمكن.

٦. مراقبة قاعدة البيانات الخاصة لأي نشاط غريب.

٧. يمكن استخدام خدمة حماية DDoS ، والتي ستعيد توجيه حركة المرور بعيدًا عن الخادم الخاص بالهدف أثناء الهجوم.

٨. يمكن أيضا استخدام شبكة توصيل المحتوى (CDN) مثلCloudflare ، والتي ستوزع المحتوى الخاص بالهدف عبر شبكة من الخوادم بحيث لا يؤدي هجوم على خادم واحد إلى تدمير موقع الويب بالكامل.

٩. وضع سياسات كلمات مرور قوية، هذا يعني طلب كلمات مرور قوية وفريدة من نوعها لجميع الحسابات، وتغييرات منتظمة لكلمات المرور.

١٠. استخدام مدير كلمات المرور أداة لإنشاء كلمات مرور آمنة وإدارتها وتخزينها.

١١. تنفيذ المصادقة الثنائية (2FA) للمطالبة بجزء إضافي من المعلومات قبل السماح بالوصول إلى الحساب.

١٢. تحديث جميع البرامج والأنظمة بأحدث تصحيحات الأمان ومراقبة أنظمتك بحثًا عن أي نشاط مشبوه.

١٣. الحماية من هجمات التصيد الاحتيالي، بفتح رسائل البريد الإلكتروني من مصادر موثوقة فقط.

١٤. عدم النقر على أي روابط أو تفتح أي مرفقات، الحذر من أي رسائل بريد إلكتروني أو مواقع إلكترونية تطلب معلومات شخصية.

- **التدابير المضادة والحماية من عمليات اختراق خوادم وتطبيقات الويب (عملي)**

١٥. التأكد من موقع الويب، بالبحث عن https: // في عنوان URL قبل إدخال أي معلومات مهمة.

١٦. تحديث برنامج مكافحة الفيروسات الخاص بك محدث للمساعدة في حماية الحاسب من البرامج الضارة.

١٧. تحديث مواقع الويب وبرامجها باستمرار، إنشاء موقع الويب احتياطيًا واستخدم سياسات كلمات مرور قوية واستخدم جدار حماية لتطبيق الويب.

١٨. تدقيق المنافذ على الخادم بانتظام لضمان أن الخدمة الغير آمنة أو غير الضرورية ليست نشطة على خادم الويب الهدف.

١٩. تقليل حركة مرور البيانات الواردة إلى منفذ HTTP 80 أو 443 HTTPS(SSL).

٢٠. تعطيل خدمة قوائم الدليل.

٢١. مراقبة والتحقق من كل سجلات خدمات الشبكة وسجلات خادم قواعد البيانات.

- **باستخدام الأداة WebCruiser**

من أدوات أمن خادم الويب تقوم بفحص المواقع الكبيرة والمعقدة والتطبيقات على شبكة الإنترنت لمعالجة نقاط الضعف على شبكة الإنترنت وتعمل على تحديد نقاط الضعف في التطبيق، الموقع

http://sec4app.com

- **استخدم الأداة Snort**

باستخدام (Snort)، يمكن لمسؤولي الشبكة اكتشاف هجمات رفض الخدمة (DoS) وهجمات (DDoS) الموزعة وفحص المنفذ الخفي، ينشئ (Snort) سلسلة من القواعد التي تحدد نشاط الشبكة الضار وتحدد الحزم الضارة وترسل تنبيهات إلى المستخدمين، كما تحدد لغة قاعدة (Snort) حركة مرور الشبكة التي يجب جمعها وما يجب أن يحدث عندما تكتشف الحزم الضارة.

تم تصميم أداة الحماية (Snort) لاكتشاف أنواع مختلفة من الاختراق ويستخدم لغة قواعد مرنة لتحديد أنواع حركة مرور الشبكة التي يجب جمعها، لكي يعمل Snort بشكل صحيح.

- **مميزات Snort**

هناك العديد من الميزات التي تجعل (Snort) مفيدًا لمديري الشبكة لمراقبة أنظمتهم واكتشاف النشاط الضار، **وتشمل هذه:**

١. مراقبة حركة المرور في الوقت الحقيقي

يمكن استخدام (Snort) لمراقبة حركة المرور التي تدخل وتخرج من الشبكة، ستقوم بمراقبة حركة المرور في الوقت الفعلي وإصدار تنبيهات للمستخدمين عندما يكتشف الحزم أو التهديدات التي يحتمل أن تكون ضارة على شبكات بروتوكول الإنترنت (IP).

٢. تسجيل الحزم

يتيح (Snort) تسجيل الحزم من خلال وضع مسجل الحزمة الخاص به، مما يعني أنه يسجل الحزم على القرص، في هذا الوضع، يجمع (Snort) كل حزمة ويسجلها في دليل هرمي بناءً على عنوان (IP) للشبكة المضيفة.

٣. تحليل البروتوكول

يمكن لـ (Snort) إجراء تحليل البروتوكول، وهو عبارة عن عملية تسلل للشبكة تلتقط البيانات في طبقات البروتوكول لتحليل إضافي، يتيح ذلك لمسؤول الشبكة إجراء فحص إضافي لحزم البيانات التي يُحتمل أن تكون ضارة،

- **أنظمة الترميز URL-HTML**

هي طرق لتحويل الرموز والحروف غير المألوفة أو المحظورة في عناوين URLوفي مستندات HTML إلى مجموعة محددة من الرموز التي يمكن فهمها وتفسيرها بواسطة المتصفح.

- **يوجد العديد من أنظمة الترميز**

١. URL (Percent Encoding)

ترميز URL هو عملية تحويل عنوان URL إلى تنسيق صالح تقبله متصفحات الويب.

٢. HTML (HTML Encoding)

HTML هي اختصار يرمز إلى (Hyper Text Markup Language) ، ومعناها لغة توصيف أو ترميز النص الفائق ، كما أنها لغة الترميز القياسية لإنشاء صفحات الويب، وتطبيقات هجينة تعمل على الهواتف المحمولة كذلك تطبيقات تعمل على أنظمة التشغيل ويندوز أو لينكس أو أواس أو ماك.

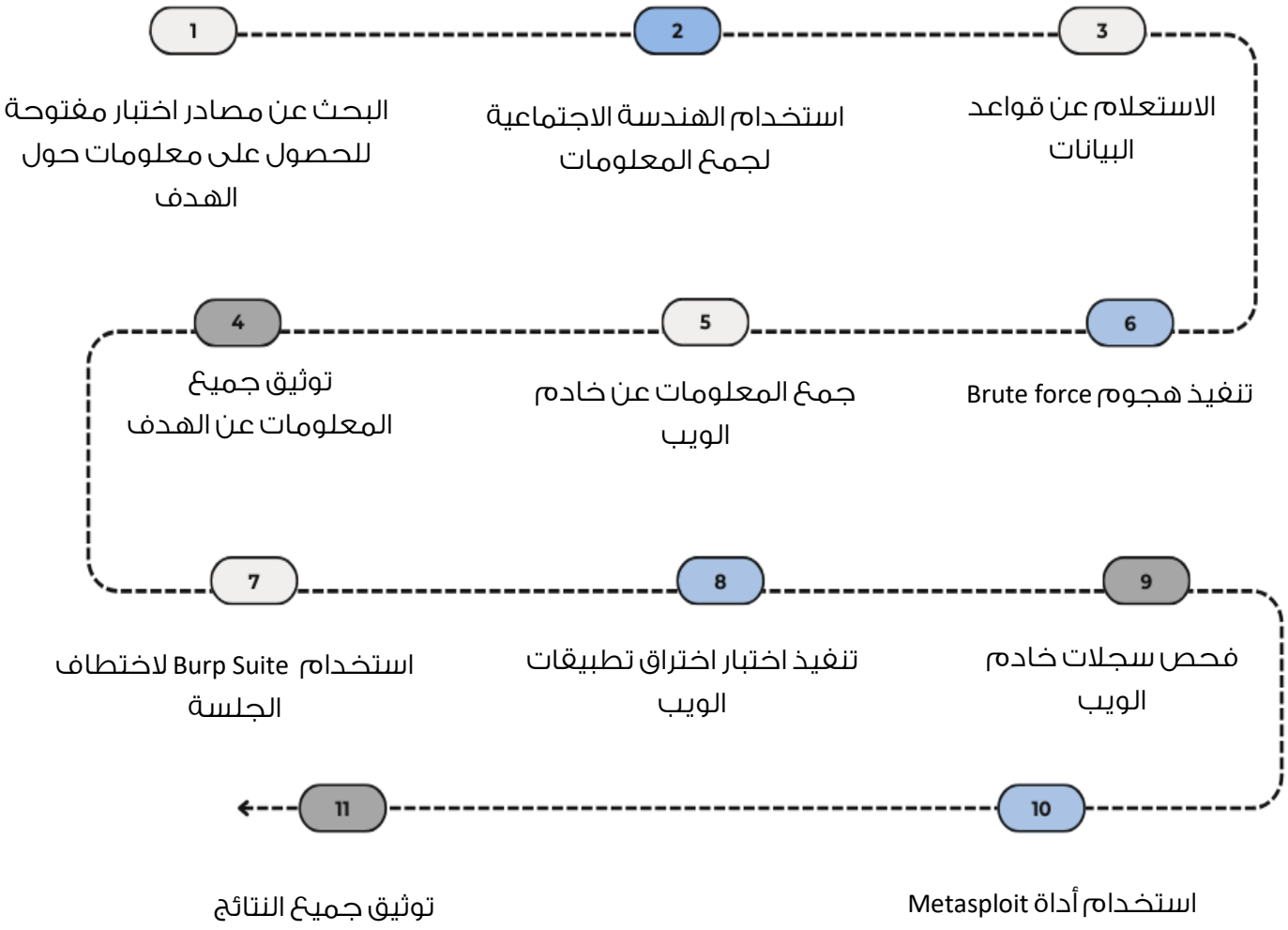
- **WEB Application Firewalls**

WAF (جدار حماية تطبيق الويب) هو شكل محدد لجدار حماية التطبيق الذي يقوم بتصفية حركة مرور HTTP ومراقبتها وحظرها من وإلى خدمة ويب، من خلال فحص حركة مرور HTTP ، يمكن أن يمنع الهجمات من استغلال نقاط الضعف المعروفة في تطبيق الويب ، مثل حقن SQL والبرمجة النصية للمواقع المشتركة وإدراج الملفات وتكوين نظام غير لائق.

يساعد WAF على وضع قواعد وإدارتها لتجنب تهديدات الإنترنت،بما في ذلك عناوين IP ورؤوس HTTP ونص HTTP وسلاسل URI والاسكربتات عبر المواقع (XSS) وحقن SQL والثغرات الأخرى المحددة.

- **اختبار اختراق الويب**

يساعد على تحديد وتحليل وتقديم تقرير عن نقاط الضعف مثل ضعف التوثيق وأخطاء الأعداد ونقاط الضعف المتعلقة بخادم الويب وهو مفيد في تحديد البنية التحتية للويب والتحقق من وجود ثغرات أمنية للعمل على إصلاحها **والخطوات هي:**

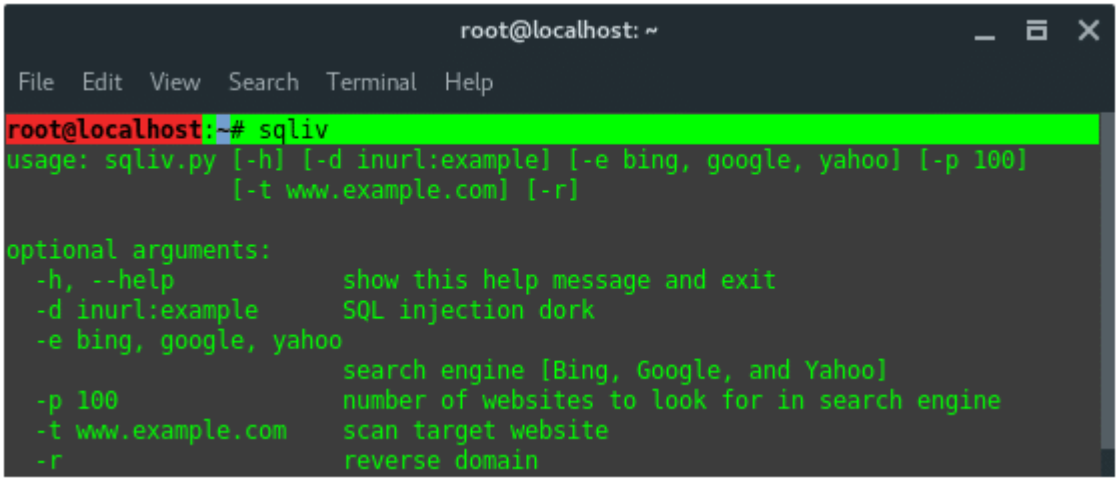


١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	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 الإعدادات الافتراضية دون إعادة ضبطها للتوافق مع إعدادات الأمان.	√
٢.	Internet Information Services (IIS) و هو يعمل على أنظمة اللينكس	×
٣.	هجمات XSS انعكاسية من أنواع الهجمات على خادم الويب	√
٤.	(Nmap) هي إداة لفحص نقاط الضعف والثغرات في تطبيقات الويب أو المواقع وهي عبارة عن اداة مفتوحة المصدر مبرمجه بلغة Java	×
٥.	تنقسم الثغرات على حسب الألوان	√
٦.	يساعد Cookie Digger في تحديد إنشاء ملفات تعريف الارتباط الضعيفة والتطبيقات غير الآمنة لإدارة الجلسة بواسطة تطبيقات الويب.	√
٧.	هجوم DoS ، أو 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.	×
٨.	يمكن القيام بذلك عن طريق إغراق الهدف بطلبات من أجهزة حواسيب متعددة، أو باستخدام جهاز حاسب واحد لإرسال عدد كبير من الطلبات	√
٩.	(ثغرة يوم الصفر) هذه الثغرة تصنف بشكل خاص للتعامل مع الحماية (الضعف في الحماية) وهي متعلقة بنظام التشغيل و خادم الويب ونظام إدارة قاعدة البيانات، هذه المخاطر تصبح اكثر صعوبة عندما لا تؤمن الحماية منع الوصول الغير مسموح به للموقع.	×

٢. طبق ما يلي عمليا:

ا- قم بتثبيت sqliv

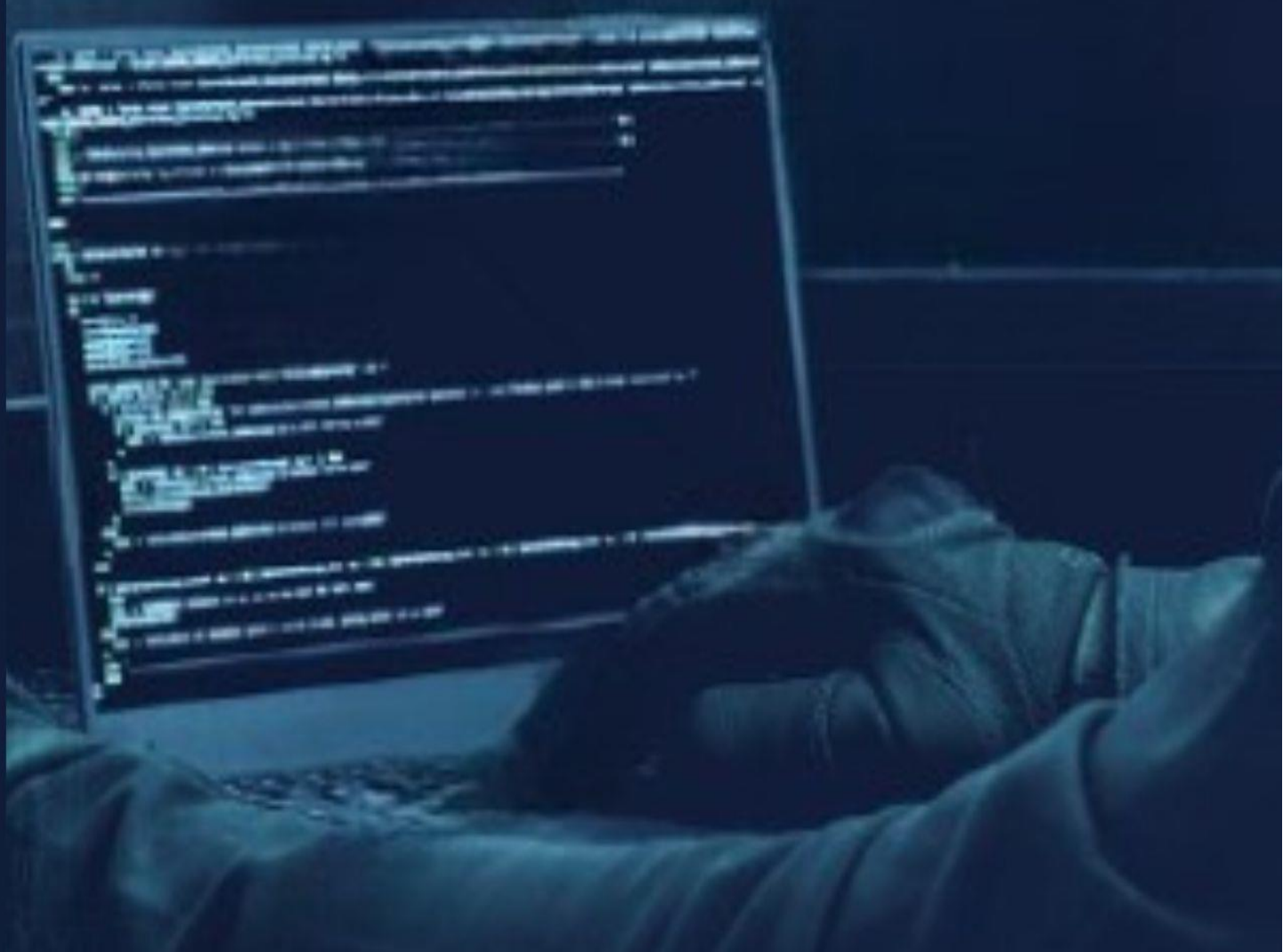


اختراق الشبكات اللاسلكي

الفصل السابع

في هذا الفصل سنتعرف على المواضيع التالية:

- تشفير الشبكات اللاسلكية
- أدوات كسر التشفير (عملي)
- طرق اختراق الشبكة اللاسلكية
- أدوات اختراق الشبكة اللاسلكية
- التدابير المضادة والحماية من عمليات اختراق الشبكات اللاسلكية



- **تعريف الشبكات اللاسلكية**

الشبكات اللاسلكية هي نوع من الشبكات الحاسوبية التي تعمل على نقل المعلومات بين العُقَد من دون استخدام الأسلاك.

- **اختبار الاختراق**

اختبار الاختراق يتم عبر سلسلة من الخطوات لإيجاد الثغرات ونقاط الضعف في الشبكة اللاسلكية **وهي:**

١. الاستطلاع لاكتشاف الأجهزة اللاسلكية وجمع المعلومات

- يوجد العديد من أدوات اكتشاف الشبكات اللاسلكية المتوفرة مجانا على الإنترنت **مثل:**

Insider ,Netsurveyor , NetStumble,Visstumber ,Wavestumbler

٢. فحص وجود جهاز لاسلكي

- إذا تم اكتشاف شبكة لاسلكية يتم فحص تقنية التشفير المستخدمة أو غير مشفرة.
- تحديد فيما إذا كانت الشبكة تستخدم تشفير WEP أو أي نوع أخر.

٣. الهجوم بكسر هذا التشفير واختراق الشبكة.

- **أهداف اختبار اختراق الشبكات**

١. **فحص التحكم بالحماية:** لفحص والتحقق من فعالية الحماية للشبكة اللاسلكية.

٢. **كشف سرقة البيانات:** إيجاد سلسلة من البيانات المهمة عن طريق التقاط حركة المرور sniffing traffic.

٣. **إدارة نظام المعلومات:** جمع معلومات عن بروتوكولات الحماية وقوة الشبكة والأجهزة المتصلة يتم ذلك باستخدام أدوات اكتشاف الشبكات اللاسلكية و Port Scanner فحص المنافذ.

٤. **منع المخاطر والإجابة:** تؤمن وصول شامل للخطوات التي يمكن أن تتم لمنع الاستغلال.

٥. **تحسين البنية التحتية:** تحسين عتاد الأجهزة والشبكات والبرمجيات.

٦. **اكتشاف المخاطر الأمنية:** تحديد التهديدات ونقاط الضعف التي تهدد المنظمة.

- **مصادر تهديد الشبكات اللاسلكية**

- عدم إلمام المستخدمين بتفعيل إجراءات الحماية ومن أمثلة ذلك ترك تسمية الشبكة حسب الموزع الأصلي دون تغيير مما يسهل على المهاجم الاشتراك في الشبكة اللاسلكية.
- وفرة البرامج المجانية لتحديد الشبكات الغير مؤمنة والغير مرئية.
- التقاط تسمية الشبكة عن طريق برامج خاصة للكشف وتخمين كلمة المرور للشبكات اللاسلكية.
- اعتماد الشبكات اللاسلكية على الطيف الكهرومغناطيسي في الفضاء مما أدى إلى التهديد عن طريق التصنت والتقاط الإشارات.
- التشويش.
- الاختراق عبر تسمية جهاز المخترق باسم نقطة التغطية اللاسلكية.

- **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.

عندما تكون نقطة الوصول Access Point بشكل broadcast يعتبر نمط غير أمن ويمكن ضبطها على عدم النشر، في هذه الحالة يكون المستخدم على معرفة مسبقة باسم SSID ويقوم بضبطه في جهازه حتى يتمكن من الاتصال بالشبكة اللاسلكية، ولكن حتى إخفاؤه لا يؤمن الشبكة لأنه يظهر على شكل صريح داخل الرزمة Packet.

- **المصادقة بالنظام المفتوح Open system authentication في الشبكات اللاسلكية**

الجهاز الأول يرسل authentication management frame وهو الذي يحتوي على مُعرف الجهاز المُرسل لكي يحصل على المصادقة والاتصال مع الجهاز الأخر.

الجهاز الأخر هو نقطة الوصول Access Point يقوم بفحص SSID المرسل من قبل الجهاز الأول ويرد بإطار authentication verification frame إذا كان SSID صحيح يتم إرسال إطار تأكيد المصادقة إلى الجهاز الأول (المستخدم) حتى يستطيع الاتصال بالشبكة اللاسلكية أو الجهاز المطلوب.

❖ تشفير الشبكات اللاسلكية

الانتشار لهذه التقنية يتطلب العناية بتطبيق الإجراءات الأمنية لحماية الشبكات اللاسلكية، وإهمال هذا الجانب قد يعرض بيانات المستخدم والأنظمة المتصلة بالشبكة اللاسلكية لمخاطر كبيرة من المخترقين والمتسللين الى داخلها، أهم طرق الحماية تتركز في تشفير الشبكات اللاسلكية ويوجد أكثر من نظام (أو ما يسمى بروتوكول التشفير) وهي ذات قوة حماية مختلفة.

- **أنظمة التشفير المستخدمة في الشبكات اللاسلكية لجعلها أكثر أمانًا**

○ WEP

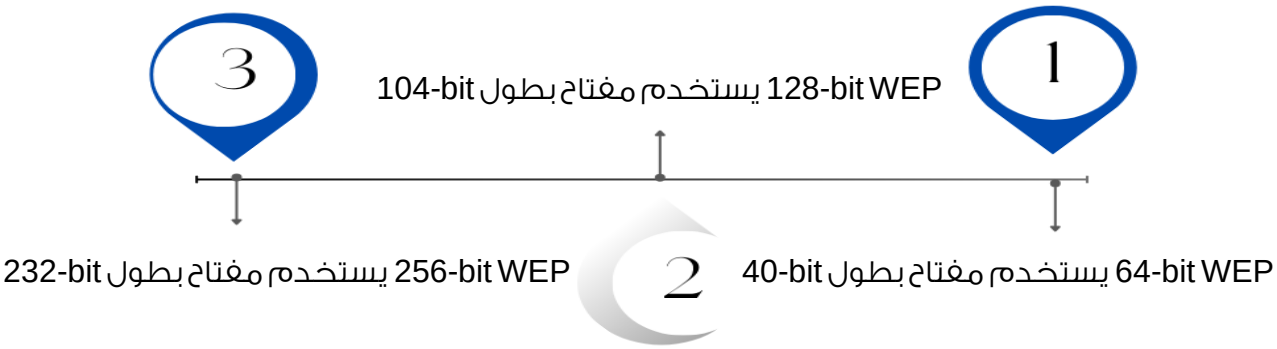
كانت المحاولة الأولى لتوفير الحماية للشبكة اللاسلكية، كان الهدف هو إضافة مستوى أمان إلى الشبكات اللاسلكية عن طريق تشفير البيانات، لن يتمكن المعترضون من التعرف على البيانات اللاسلكية إذا تم اعتراضها نظرًا إلى أنها قد تم تشفيرها، ومع ذلك، ستكون الأنظمة المصرح بها على الشبكة قادرة على التعرف على البيانات وفك تشفيرها، والسبب في هذا يرجع إلى أن الأجهزة الموجودة على الشبكة تستخدم لوغاريتم التشفير نفسها..

نظام التشفير WEP يعتبر الأضعف من بين أنظمة التشفير لأنه سهل الاختراق ولا ينصح الخبراء بالاعتماد عليه في عملية التشفير للبث اللاسلكي ، وهو بروتوكول لمصادقة المستخدم وتشفير البيانات وهو اختصار للجملة (Wired Equivalency Protocol) وهذا النوع من التشفير من اقدم البروتوكولات المستخدمة في تشفير الشبكات اللاسلكية، إلا انه يعاني من نقطة ضعف كبيرة، فبإمكان أي مخترق محترف أن يكسر هذا البرتوكول خلال فترة قصيرة، وينصح باستخدام بروتوكول (WEP) مع مفتاح طوله ١٢٨ بت، لأنه يوفر حماية افضل من المفتاح الأقصر ٦٤ بت، ويتم إنشاء المفتاح في نقطة الوصول ومن ثم يمكن نسخه لأي جهاز يتم توصيله بالشبكة اللاسلكية، ويسمى هذا النوع من المفاتيح مفتاح التشفير المشترك (PSK).

- **دور WEP في الاتصال اللاسلكي**

- الخصوصية حيث يحمي من التجسس على الشبكة اللاسلكية.
- التحكم بالوصول يحدد من يستطيع الوصول المصرح به إلى الشبكة اللاسلكية.
- سلامة البيانات فهو يعتمد على مفتاح سري يُستخدم لتشفير الحزم قبل إرسالها، جهاز المستخدم ونقطة الوصول ACCESS POINT يتشاركون في هذا المفتاح وتتم عملية فحص السلامة للتأكد من أن حزم البيانات لم تتبدل أثناء عملية الإرسال.
- يشفر البيانات فقط.

- **طول WEP وطول المفتاح السري**



- **عيوب WEP**

- طريقة لتوزيع مفاتيح التشفير.
- من السهل اكتشاف النص من عدد من الرسائل المشفرة بنفس المفتاح.
- يستخدم RC4 الذي صمم ليستخدم للتشفير مرة واحدة وهو غير مُعد لتشفير عدة رسائل فالمهاجم يراقب حركة مرور البيانات ويكتشف طرق مختلفة للعمل مع رسائل النص الصريح وبمعرفة النص المشفر والنص الصريح يستطيع حساب مفتاح التشفير.
- يحلل المهاجم حركة مرور البيانات التي قام بالتقاطها ويقوم بكسر مفتاح WEP بمساعدة أدوات مثل AirSnort &WEPCrack.
- طريقة توليد المفاتيح المستخدمة من قبل المُصنعين قابلة للهجوم.
- طريقة تخطيط المفاتيح أيضا قابلة للهجوم.

- **WPA**

هو اختصار للجملة (WI-FI Protected Access)

تم ابتكار هذا البروتوكول في عام ٢٠٠٣، وكان بمثابة البديل الذي قدمته Wi-Fi Alliance لمعيار WEP ، وقد كانت تجمعه مع WEP أوجه تشابه، ولكنه أدخل تحسينات بخصوص كيفية التعامل مع مفاتيح الأمان والطريقة التي يتم التصريح بها للمستخدمين ،بينما يوفر معيار WEP لكل نظام مصرح له المفتاح نفسه، يستخدم WPA بروتوكول سلامة المفتاح المؤقت (TKIP) الذي يغير المفتاح الذي تستخدمه الأنظمة ديناميكيًا ، ومن شأن هذا أن يحول دون قيام المهاجمين بإنشاء مفتاح التشفير الخاص بهم لمطابقة المفتاح الذي تستخدمه الشبكة الآمنة ، تم استبدال معيار تشفير بروتوكول سلامة المفتاح المؤقت (TKIP) لاحقًا بمعيار التشفير المتقدم (AES).

بالإضافة إلى ذلك، يضمن بروتوكول WPA فحوصات سلامة الرسائل لتحديد ما إذا كان المهاجم قد استولى على حزم البيانات أو قام بتغييرها، كانت المفاتيح المستخدمة بواسطة معيار WPA بطول ٢٥٦ بت، وهي زيادة كبيرة عن مفاتيح ٦٤ بت و١٢٨ بت المُستخدمة في نظام WEP ، لكن على الرغم من هذه التحسينات، تعرضت عناصر WPA للاستغلال، ما أدى إلى ابتكار WPA2.

- **WPA/2**

تم ابتكار معيار WPA/2 في عام ٢٠٠٤ وكان بمثابة إصدار تمت ترقيته من معيار WPA يعتمد معيار WPA/2 على آلية شبكة الأمان القوية (RSN) **ويعمل على وضعين:**

١. الوضع الشخصي أو المفتاح المشترك مسبقًا - (WPA2-PSK) والذي يعتمد على رمز مرور مشترك للوصول وعادةً ما يُستخدم في البيئات المنزلية.

٢. وضع المؤسسة - (WPA/2-EAP) وهذا أكثر ملاءمة للاستخدام المؤسسي أو التجاري كما يوحي الاسم، يستخدم كلا الوضعين بروتوكولCCMP ، وهو اختصار لعبارة بروتوكول رمز مصادقة رسائل سلسلة كتلة شفرة وضع العداد، يعتمد بروتوكول CCMP على لوغاريتم معيار التشفير المتقدم (AES)التي توفر مصادقة الرسالة والتحقق من سلامتها ، يعد بروتوكول CCMP أقوى وأكثر موثوقية من بروتوكول سلامة المفتاح المؤقت (TKIP) الأصلي الخاص بمعيار WPA ، ما يجعل من الصعب على المهاجمين اكتشاف الأنماط.

لكن WPA/2 لا يزال يعاني من العيوب، رغم ذلك، فهو، ، عُرضة لهجمات إعادة تثبيت المفتاح (KRACK) يستغل هجوم إعادة تثبيت المفتاح (KRACK) نقطة ضعف في WPA/2 ، ما يسمح للمهاجمين بالظهور كشبكة مستنسخة وإجبار الضحية على الاتصال بشبكة ضارة بدلاً من ذلك ، وهذا يتيح للمتسلل فك تشفير جزء صغير من البيانات التي قد يتم تجميعها لفك مفتاح التشفير ، ومع ذلك، يمكن تزويد الأجهزة بالتصحيحات، ولا يزال WPA/2 يعدّ أكثر أمانًا من WEP أو WPA .

❖ أدوات كسر التشفير (عملي)

إطار عمل اختبار اختراق الشبكات اللاسلكية هو اكتشاف الأجهزة اللاسلكية، ثم الاتصال بالشبكة والحصول على معلومات أكثر دقة، إذا كانت الشبكة الهدف تستخدم تشفير مثل WEP ,WPA,WPA2 سيتم محاولة كسر هذا التشفير **باستخدام :**

- **القوة الغاشمة** Brute Force

هجوم القوة العمياء هو نوع من الهجوم الذي يعتمد على النص المشفر فقط، وتتم فيه محاولة تجربة كل المفاتيح المحتملة لفك النص المشفر ، وهو الأسلوب الأساسي لمحاولة استخدام كل مفتاح بدوره حتى يمكن التعرف على المفتاح الصحيح وفيه يحاول المهاجم إنتاج كل مفتاح تشفير واحد للبيانات حتى يتم الكشف عن المعلومات المطلوبة وتحليل الشفرات، هو هجوم القوة الغاشمة على التشفير عن طريق اختبار جميع المفاتيح الموجودة في محاولة لاسترداد النص العادي الذي استخدم لإنتاج التشفير وهذه العملية تستغرق وقت طويل ولكن في النهاية يتم العثور على كل كلمات السر.

- **من بين الأدوات المستخدمة في Kali Linux لهجمات القوة الغاشمة على SSH:**

- Patator: يمكن استخدام أداة Patator لاختبار الهجمات بالقوة الغاشمة على SSH ، يمكن استخدامها لتجربة مجموعة من كلمات المرور المحتملة من قاموس مثل rockyou.txt.
- Medusa: هي أداة قوية لاختبار الهجمات بالقوة الغاشمة على SSH وغيرها من البروتوكولات ، يمكن استخدامها لتجربة مجموعة من أسماء المستخدمين وكلمات المرور المحتملة.
- Hydra: هي أداة شهيرة لاختبار الهجمات بالقوة الغاشمة على SSH وغيرها من البروتوكولات ، يمكن استخدامها لتجربة مجموعة من أسماء المستخدمين وكلمات المرور المحتملة.

- **كيفية استخدام القوة الغاشمة لـ SSH في كالي لينكس**

- Aircrack

باستخدام الأداة aircrack-ng يمكن للمخترق كسر التشفير واستخراج مفتاح التشفير WEP من Ivs وذلك بعد التقاط 50000 Ivs

١. إعداد بطاقة الشبكة اللاسلكية في نمط المراقبة Monitor mode على القناة Channel 1

```
root@kali:~#airmon-ng  start wlan0 1
```

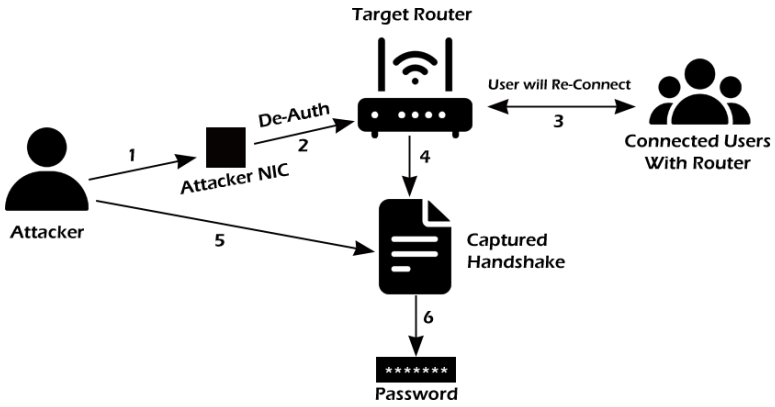
من الكالي لينكس يتم كتابة الأمر

```
# aircrack-ng   -b  MAC address   output.cap
```

-b لتحديد عنوان MAC للـAccess point

output.cap اسم الملف الذي يتم الحفظ فيه ، عند نجاح العملية يظهر مفتاح التشفير.

- **الآن نرى كيف يتم استخدام المنهجية في سيناريو الهجوم في العالم الحقيقي بمساعدة الرسم البياني الموضح أدناه.**



شكل (٦٢) القوة الغاشمة ١

يقوم المهاجم أولاً بتكوين بطاقة واجهة الشبكة الخاصة به، وهذا يعني أن بطاقة واجهة الشبكة مضبوطة على وضع المراقبة ويمكنها إجراء حقن الحزم.

ثم يتم استخدام بطاقة واجهة الشبكة التي تم تكوينها بشكل صحيح لتنفيذ هجوم إلغاء المصادقة، ثم يقوم العميل الذي تم إلغاء مصادقته بإعادة الاتصال بنقطة الوصول، وهذا يسمح لنا بالتقاط المصافحة الرباعية.

نقوم بعد ذلك بتنفيذ هجوم القوة الغاشمة أو هجوم القاموس على المصافحة التي تم التقاطها ، بمجرد اكتمال الهجوم، نحصل على كلمة المرور التي تم فك تشفيرها.

○ Aircrack-ng

Aircrack-ng عبارة عن مجموعة شاملة من الأدوات لتقييم أمان شبكات Wi-Fi ، ويركز على الجوانب المختلفة لأمن Wi-Fi، **بما في ذلك:**

- **المراقبة:** التقاط الحزم وتصدير البيانات إلى ملفات نصية للمعالجة الإضافية بواسطة أدوات خارجية.
- **الهجوم:** تتضمن هجمات حقن الحزم هجمات إعادة التشغيل وإلغاء المصادقة وإنشاء نقاط وصول زائفة، من بين أمور أخرى.
- **الاختبار:** التحقق من قدرات بطاقات Wi-Fi وبرامج التشغيل (الالتقاط والحقن).
- **التكسير:** تكسير WEP وWPA PSK (WPA 1 و٢)
- تعتمد جميع الأدوات على سطر الأوامر، مما يسمح بالكثير من البرمجة النصية، استفادت مجموعة كبيرة ومتنوعة من واجهات المستخدم الرسومية من هذه الميزة، وهو متاح لأنظمة التشغيل Linux و Windows و macOS و FreeBSD وOpenBSD و NetBSD و Solaris وحتى eComStation 2.
- سنستخدم أدوات airmon-ng، و airodump-ng، و aireplay-ng، و Aircrack-ng من مجموعة Aircrack-ng ، **واستخدامها :**

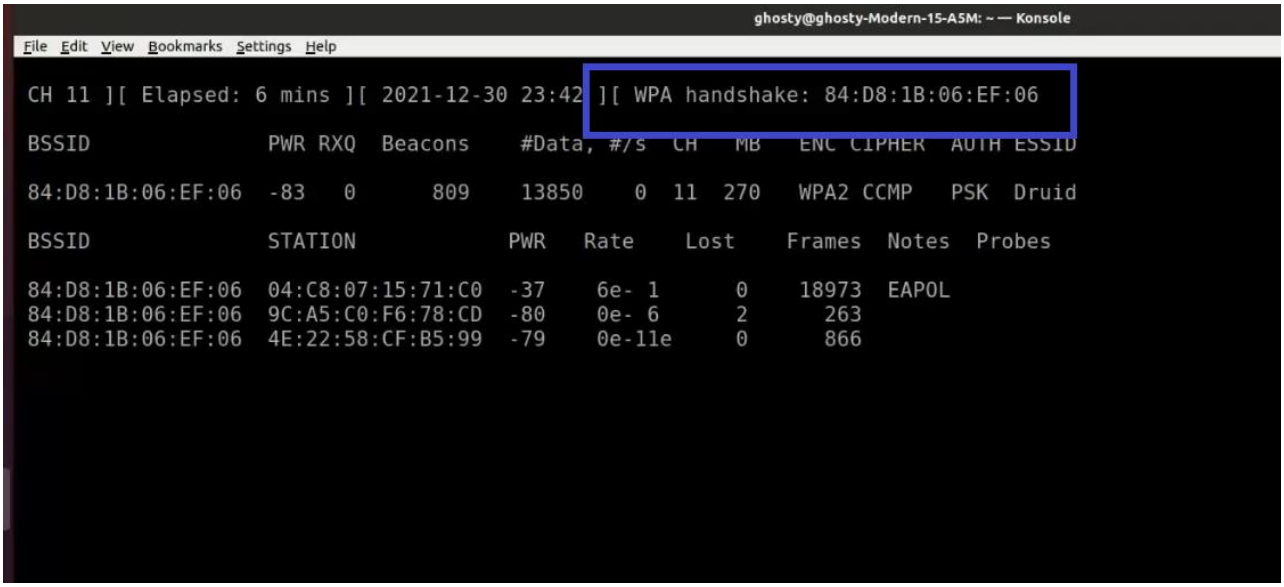
- **Airmon-ng : وضع المراقبة**

يتم استخدام Airmon-ng لإدارة أوضاع الامتدادات اللاسلكية، للتعرف على اتصال لاسلكي، يجب عليك تبديل بطاقتك اللاسلكية من وضع المراقبة إلى وضع المراقبة، وهو ما يتم باستخدام airmon-ng ، يسمح وضع المراقبة لبطاقتك بالاستماع إلى جميع الحزم الموجودة في الهواء ، عادةً، سيتم "سماع" الحزم المخصصة لك فقط بواسطة بطاقتك ، يمكننا لاحقًا التقاط مصافحة WPA/WPA2 رباعية الاتجاهات من خلال الاستماع إلى كل حزمة.

شكل (٦٣) airmon I

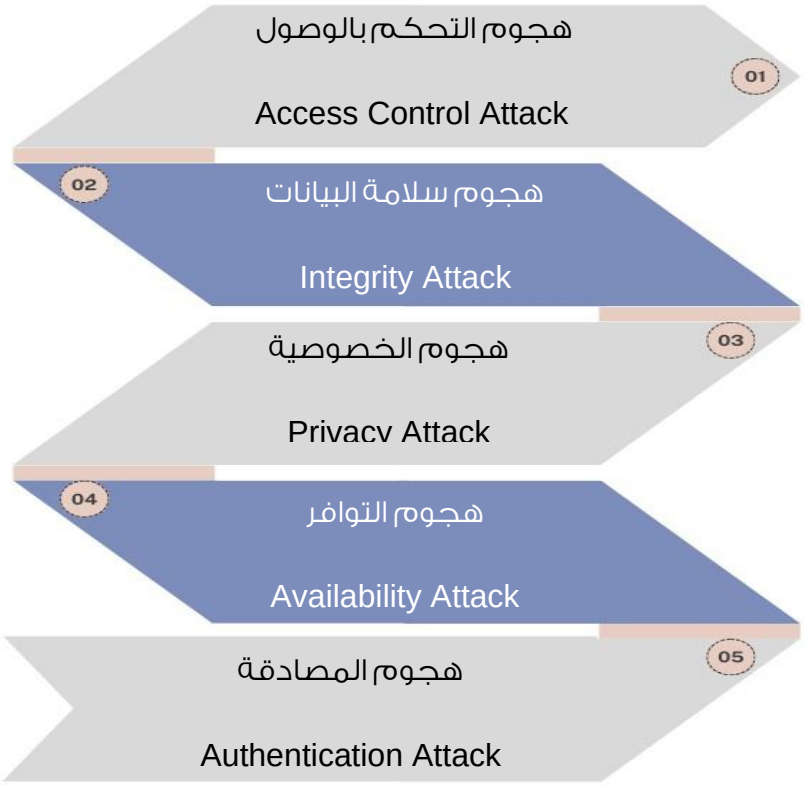
- **Airodump-ng: مصافحة المصادقة**

Airodump-ng عبارة عن أداة لاسلكية يمكنها جمع البيانات من عدة نقاط وصول لاسلكية ، يتم استخدامه للبحث عن نقاط الوصول القريبة وتسجيل المصافحات.



شكل (٦٣) airmon 2

❖ طرق اختراق الشبكة اللاسلكية



❖ أدوات اختراق الشبكة اللاسلكية

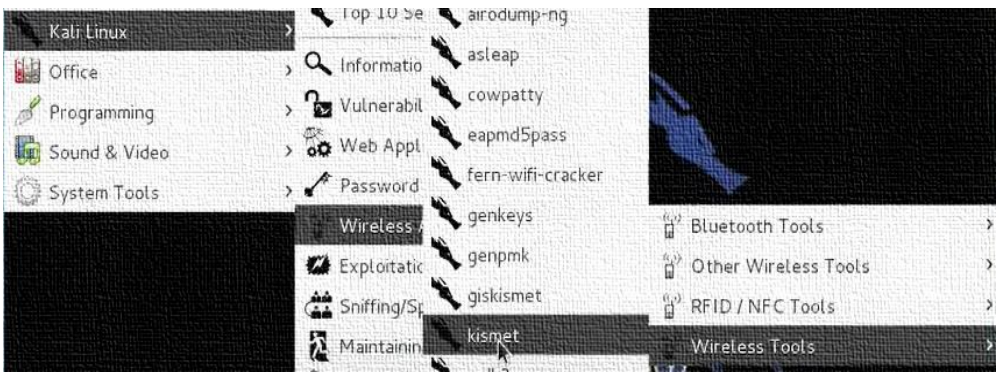
يوجد العديد من أدوات اختراق الشبكات اللاسلكية التي يمكن استخدامها لاختبار أمنها **مثل:**

- **Kismet**

هي تستخدم في هجوم التجسس وتقوم بفك تشفير البيانات للحصول على المعلومات المهمة Kismet هو عبارة عن كاشف للشبكات ونظام اكتشاف الحزمة ونظام اكتشاف التطفل للشبكات اللاسلكية ٨٠٢,١١ ، ستعمل Kismet مع أي بطاقة لاسلكية تدعم وضع المراقبة.

لتنفيذ الأمر

Application Menu /Kali Linux / Wireless Attacks / 802.11 wireless Tools /Kismet



شكل (٦٤) wireless tools ١

- **Wardriving**

Wardriving هو هجوم إلكتروني حيث يجد المتسللون نقاط وصول ضعيفة لشبكة Wi-Fi ، وفيها يقوم المهاجم بالتجول ومعه جهاز اللابتوب wi-fi enabled laptop ليحدد ويكتشف الشبكات اللاسلكية المفتوحة ثم يتم إرسال لها طلب تحقق Probe Request أو بالاستماع إلى beacons frames ويستطيع بعد ذلك المهاجم الوصول إلى الشبكة باستخدام الأدوات مثل : NetStumbler

- **NetStumbler**

أحد أفضل البرامج التي يمكن الاعتماد عليها، في الحصول على كلمة السر الخاصة بالشبكات اللاسلكية المفتوحة.

❖ التدابير المضادة والحماية من اختراق الشبكات اللاسلكية

يوجد العديد من التدابير المضادة والحماية من الاختراق وهي:

١. تجنب استخدام كلمة المرور الافتراضية والحماية باسم مستخدم وكلمة سر جديدة، يجب أن يستخدم المستخدم كلمة مرور قوية لا تقل عن ٨ حروف خليط بين أرقام وحروف ورموز.

٢. استخدام إحدى طرق تشفير الشبكات اللاسلكية: WEP أو WAP أو WPA2

٣. تغيير معُرف الشبكة اللاسلكية SSID بتعطيل خيار الإعلان عن معرف نقطة الوصول (Broadcasting SSID)

٤. وضع نقطة الوصول Access Point في مكان مناسب بحيث تضمن تغطية المكان المراد تغطيته وتقليل نسبة تسرب الذبذبة خارج النطاق المطلوب حتى لا يتمكن المهاجمين بالاتصال بالشبكة.

٥. تحديد قائمة بالأجهزة القادرة على الارتباط بنقطة الوصول وذلك من خلال تسجيل عنوان بطاقة الشبكة (MAC) في نقطة الوصول.

٦. تحديث نظام تشغيل نقطة الاتصال وتثبيت منتج فعّال للحماية من البرامج الضارة الحفاظ على تحديث منتج الحماية من البرامج الضارة.

٧. التأكد من موثوقية الشبكات اللاسلكية التي يتم الاتصال بها.

٨. عدم الاتصال بالشبكات اللاسلكية المفتوحة وتعطيل هذه الخدمة في إعدادات الشبكة اللاسلكية.

- **استخدام الأداة Nmap**

تُستخدم لفحص الشبكات اللاسلكية والتدقيق الأمني لاكتشاف المضيفين والخدمات على الشبكة من خلال تحليل الاستجابات للحزم والطلبات المختلفة.

- **استخدام الأداة Comm view**

أداة للمراقبة في حالة الاتصال بشبكة لاسلكية، هو مفيد لحماية الشبكة اللاسلكية من الاختراق، ويحتوي على القدرة على تحليل رزم المعلومات والتحكم في تدفق البيانات ويعرض البرنامج قائمة باتصالات الشبكة، **يُستخدم في:**

- فحص الهواء لمحطات Wi-Fi ونقاط الوصول.
- التقاط حركة المرور WLAN 802.11a و ٨٠٢,١١b و ٨٠٢,١١g.
- تحديد مفاتيح WEP أو WPA لفك تشفير الحزم المشفرة.
- عرض مفصل لكل العقد وإحصاء لكل قناة.
- مشاهدة مفصلة لاتصالات و الإحصاءات للـ IP : عناوين IP، ports ، الجلسات.
- إعادة بناء جلسات TCP.
- تكوين أجهزة الإنذار التي يمكن أن ينبه بالأحداث الهامة، مثل الحزم المشبوهة، وارتفاع استخدام عرض النطاق الترددي، وعناوين غير معروفة، نقاط الوصول المارة.
- مشاهدة خرائط بروتوكول "pie".
- مراقبة استخدام عرض النطاق الترددي.
- تصفح الحزم الملتقطة وفك الشفرة في الوقت الحقيقي.
- البحث عن سلاسل أو hex في الحزم الملتقطة.

تمارين الفصل السابع

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

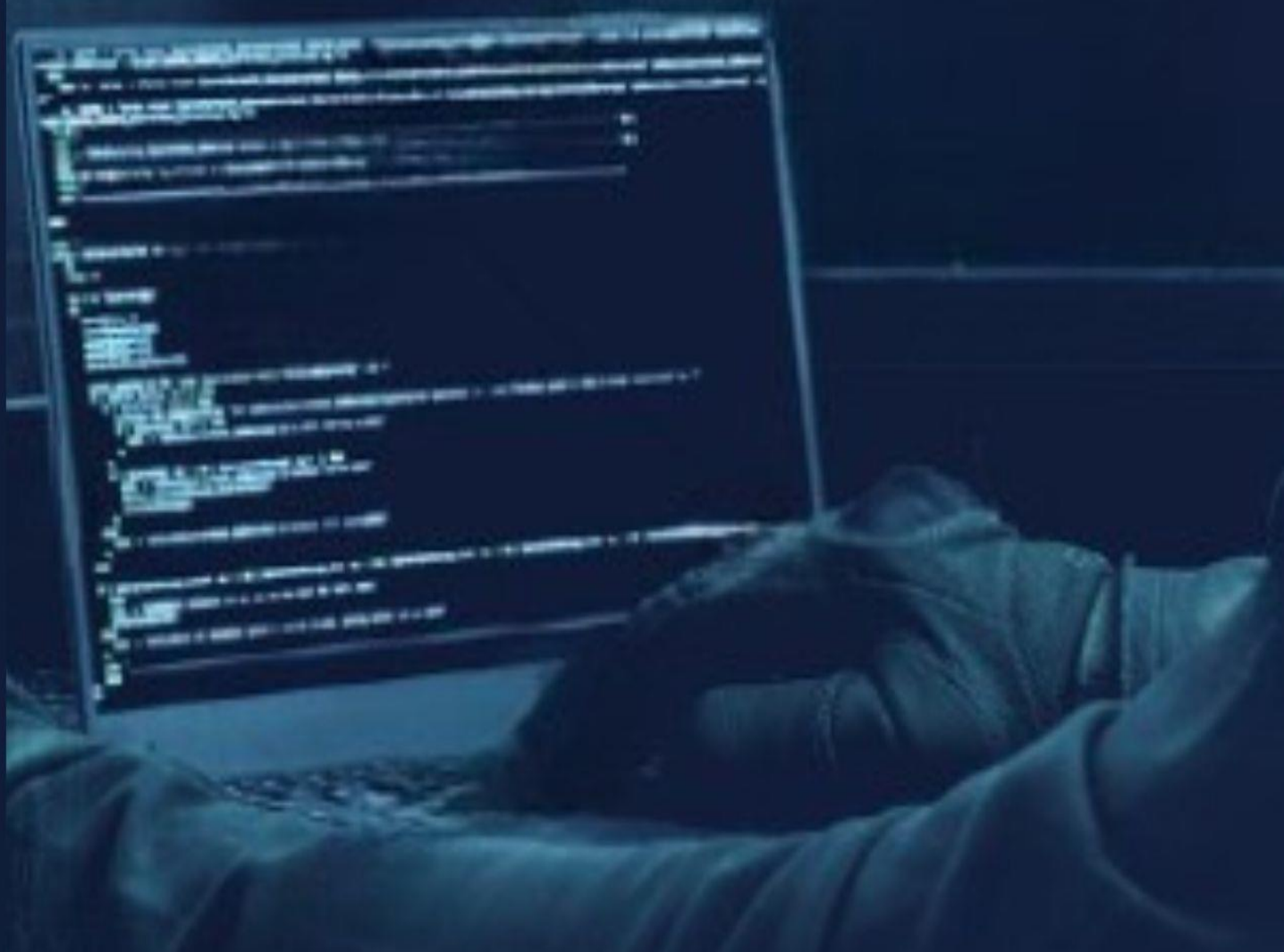
١.	(شبكة الإنترنت) هي نوع من الشبكات الحاسوبية التي تعمل على نقل المعلومات بين العُقَد من دون استخدام الأسلاك	×
٢.	اختبار الاختراق يتم عبر سلسلة من الخطوات لإيجاد الثغرات ونقاط الضعف في الشبكة اللاسلكية	√
٣.	يوجد العديد من أدوات ا كتشاف الشبكات اللاسلكية المتوفرة مجانا على الإنترنت مثل : NetStumble	√
٤.	من أهداف اختبار الاختراق (تحسين البنية التحتية تحسين عتاد الأجهزة والشبكات والبرمجيات)	√
٥.	التشفير من مصادر تهديد المخترق الأخلاقي	×
٦.	(WI-FI Protected Access) للجملة اختصار وهو WIPAs	×
٧.	من طرق اختراق الشبكة اللاسلكية (هجوم الخصوصيةAttack PRO)	×
٨.	من التدابير لمضادة لاختراق لشبكات استخدام إحدى طرق تشفير الشبكات اللاسلكية : WEP	√
٩.	استخدام (NMAP) تُستخدم لفحص الشبكات اللاسلكية والتدقيق الأمني الاكتشاف المضيفين والخدمات على الشبكة من خلال تحليل الاستجابات للحزم والطلبات المختلفة.	√
١٠.	(Kismet) تستخدم في هجوم التجسس وتقوم بفك تشفير البيانات للحصول على المعلومات المهمة	√

اختراق الأجهزة المتنقلة

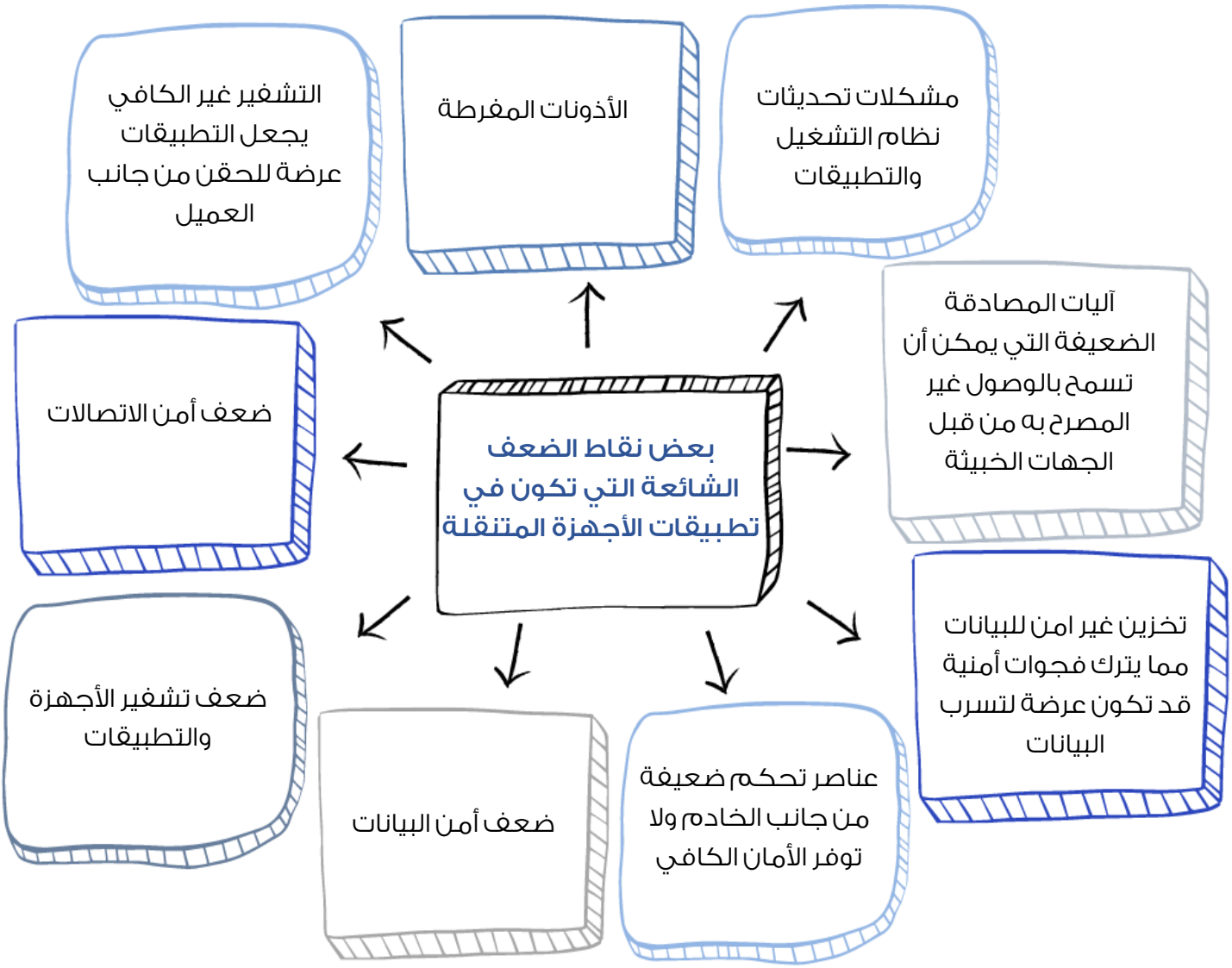
الفصل الثامن

في هذا الفصل سنتعرف على المواضيع التالية:

- نقاط الضعف والمخاطر المتنقلة
- منصات وهجمات الهواتف المحمولة



❖ نقاط الضعف والمخاطر المتنقلة



- **المخاطر الرئيسية المتعلقة بأمن الأجهزة المتنقلة**

١. فقدان الجهاز المتنقل يعرض المستخدم للخطر عن طريق التصيد الاحتيالي المحتمل.

٢. اختراق التطبيق أو اختراقه عند قيام المستخدم بتحميل تطبيقات الجهاز وتثبيتها، يطلب بعضها وصولاً أو امتيازات إضافية مثل الوصول إلى موقعه وجهات الاتصال وسجل التصفح لأغراض تسويقية، ولكن من ناحية أخرى، يوفر الموقع إمكانية الوصول إلى جهات الاتصال الأخرى أيضًا، العوامل الأخرى المثيرة للقلق هي أحصنة طروادة والفيروسات وما إلى ذلك.

٣. تعد سرقة الهواتف الذكية مشكلة شائعة لأصحاب الهواتف الذكية مثل أجهزة iPhone أو Android ، يمثل خطر وقوع بيانات الشركة، مثل بيانات اعتماد الحساب والوصول إلى البريد الإلكتروني في أيدي مهاجم التكنولوجيا تهديدًا.

٤. التعديل عن طريق تطبيق آخر.

٥. محاولات الاختراق غير المكتشفة.

٦. فقدان البيانات.

٧. فقدان السمعة – في حالة اختراق حساب البريد الإلكتروني الخاص بالعمل، يمكن للمتسلل إرسال رسائل مزيفة إلى جهات الاتصال الأخرى، قد يؤدي هذا إلى الإضرار بسمعة المنظمة.

٨. سرقة الهوية من الجهاز المتنقل.

٩. التصيد من خلال رسائل SMS.

- **استخدام الأداة OWASP**

تستخدم لاختبار أمان تطبيقات الأجهزة المتنقلة، عند الحديث عن أمان الأجهزة، يتم بناء أنواع الثغرات الأمنية على OWASP وهي منظمة خيرية غير ربحية في الولايات المتحدة، تأسست في ٢١ أبريل ، OWASP هي منظمة دولية وتدعم مؤسسة OWASP جهود OWASP حول العالم ، بالنسبة للأجهزة المتنقلة، لدى OWASP 10 تصنيفات للثغرات الأمنية.

١. **الاستخدام غير السليم للنظام الأساسي**

تغطي هذه الفئة إساءة استخدام إحدى ميزات النظام الأساسي أو الفشل في استخدام ضوابط أمان النظام الأساسي، وقد يتضمن أذونات النظام الأساسي، أو إساءة استخدام TouchID، أو Keychain، أو أي عناصر تحكم أمنية أخرى تشكل جزءًا من نظام تشغيل الجهاز المتنقل، يوجد عدة طرق يمكن أن تواجه بها تطبيقات الجهاز المتنقل هذه المخاطر.

٢. **البيانات غير الآمنة**

تغطي هذه الفئة تخزين البيانات غير الآمن وتسرب البيانات غير المقصود.

٣. **الاتصالات غير الآمنة**

يغطي هذا المصافحة الضعيفة، وإصدارات SSL غير الصحيحة، والتفاوض الضعيف، والاتصال النصي الواضح للأصول المهمة، وما إلى ذلك.

٤. **المصادقة غير الآمنة**

تلتقط هذه الفئة مفاهيم مصادقة المستخدم النهائي أو إدارة الجلسة السيئة، **وهذا يشمل:**

- الفشل في تحديد هوية المستخدم على الإطلاق عندما يكون ذلك مطلوبًا.
- الفشل في الحفاظ على هوية المستخدم عندما يكون ذلك مطلوبًا.
- نقاط الضعف في إدارة الجلسة.

٥. **التشفير غير الكافي**

هذه الفئة مخصصة للمشكلات التي تمت فيها محاولة التشفير، ولكن لم يتم تنفيذها بشكل صحيح.

٦. التفويض غير الآمن

هذه فئة لالتقاط أي إخفاقات في التفويض (وهي تختلف عن مشكلات المصادقة، إذا لم يقم التطبيق بمصادقة المستخدمين في منح الوصول إلى بعض الموارد أو الخدمة عندما يكون الوصول المصادق عليه والمصرح به مطلوبًا، فهذا يعني فشل المصادقة وليس فشل الترخيص.

٧. جودة كود العميل

فئة مشاكل التنفيذ على مستوى التعليمات البرمجية في عميل الأجهزة المتنقلة، وهذا يختلف عن أخطاء الترميز من جانب الخادم، قد يؤدي هذا إلى مثل تجاوز سعة المخزن المؤقت، ونقاط الضعف في سلسلة التنسيق، والعديد من الأخطاء الأخرى على مستوى التعليمات البرمجية حيث يكون الحل هو إعادة كتابة بعض التعليمات البرمجية التي تعمل على الجهاز المحمول.

٨. Code Tampering

تغطي هذه الفئة التصحيح الثنائي، وتعديل الموارد المحلية، وربط الطريقة، وتعديل الطريقة، وتعديل الذاكرة الديناميكية.

بمجرد تسليم التطبيق إلى الجهاز المتنقل، تكون التعليمات البرمجية وموارد البيانات موجودة هناك، يمكن للمهاجم إما تعديل التعليمات البرمجية مباشرةً، أو تغيير محتويات الذاكرة ديناميكيًا، أو تغيير أو استبدال واجهات برمجة تطبيقات النظام التي يستخدمها التطبيق، أو تعديل بيانات التطبيق وموارده، يمكن أن يوفر هذا للمهاجم طريقة مباشرة لتخريب الاستخدام المقصود للبرنامج لتحقيق مكاسب شخصية أو مالية.

٩. الهندسة العكسية

تتضمن هذه الفئة تحليل الملف الثنائي الأساسي النهائي لتحديد الكود المصدري والمكتبات والخوارزميات والأصول الأخرى، تمنح البرامج مثل IDA Pro وHopper وotool وأدوات الفحص الثنائية الأخرى للمهاجم نظرة ثاقبة على الأعمال الداخلية للتطبيق، ويمكن استخدام هذا لاستغلال نقاط الضعف الناشئة الأخرى في التطبيق، بالإضافة إلى الكشف عن معلومات حول الخوادم الخلفية وثوابت التشفير والأصفار والملكية الفكرية.

١٠. وظائف غريبة

في كثير من الأحيان، يقوم المطورون بتضمين وظائف الباب الخلفي المخفية أو غيرها من عناصر التحكم في أمان التطوير الداخلي التي لا يُقصد إصدارها في بيئة الإنتاج، مثل تعطيل المصادقة الثنائية أثناء الاختبار.

- تطبيقها عمليا

لبدء استخدام OWASP ZAP في Kali Linux، يمكنك اتباع الخطوات التالية:

- قم بفتح الترمينال في Kali Linux.
- اكتب الأمر "owasp-zap" واضغط على مفتاح الإدخال.
- ستظهر واجهة OWASP ZAP على الشاشة، ويمكنك الآن استخدامها لاختبار تطبيقات الويب وتحليل الثغرات.

- **كيفية التثبيت**

```
sudo apt install zaprox
```

```
sudo apt install owasp-mantra-ff
```

١. **owasp-zap**

```
root@kali:~# owasp-zap -h
Found Java version 17.0.9
Available memory: 14909 MB
Using JVM args: -Xmx3727m
```

شكل (٦٥) Owasp 1

الحزم الخاصة بالأداء

```
root@kali:~# owasp-mantra-ff -h
firefoxportable:Debug/Info: 0=./OWASP Mantra
firefoxportable:Debug/Info: dir=/usr/share/owasp-mantra-ff
firefoxportable:Debug/Info: Current Dir=/usr/share/owasp-mantra-ff/Mantra
Welcome to the Linux version of firefox 18.0 in portable mode. Feedback is NOT disabled.
firefoxportable:Debug/Info: Profile Directory already exists!
firefoxportable:Debug/Info: firefox is now closed.
firefoxportable:Debug/Info: firefoxportable is now closed.
```

شكل (٦٥) Owasp 1

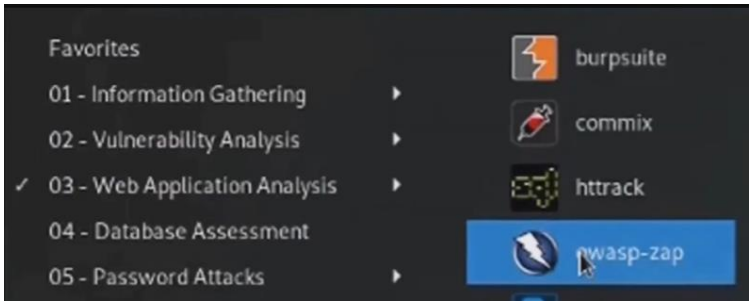
٢. **Zaproxy لمعرفه جميع استخداماتها**

```
root@kali:~# zaproxy -h
Found Java version 17.0.9
Available memory: 14909 MB
Using JVM args: -Xmx3727m
Usage:
        zap.sh [Options]
Core options:
        -version                Reports the ZAP version
        -cmd                    Run inline (exits when command line options complete)
        -daemon                 Starts ZAP in daemon mode, i.e. without a UI
        -config <kvpair>        Overrides the specified key=value pair in the configur
        -configfile <path>      Overrides the key=value pairs with those in the specif
        -dir <dir>              Uses the specified directory instead of the default on
        -installdir <dir>       Overrides the code that detects where ZAP has been ins
        -h                      Shows all of the command line options available, inclu
        -help                   The same as -h
        -newsession <path>      Creates a new session at the given location
        -session <path>         Opens the given session after starting ZAP
        -lowmem                 Use the database instead of memory as much as possible
```

شكل (٦٦) Zaproxy

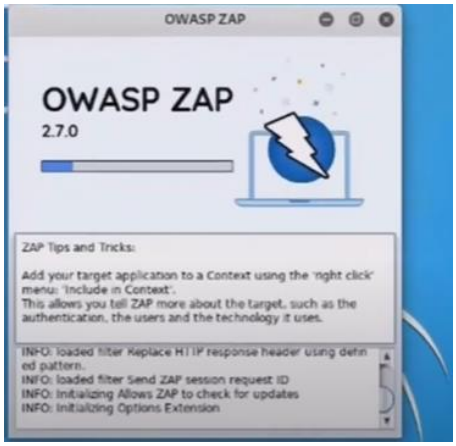
- تطبيق عملي للبحث عن ثغرة امنيه باستخدام الأداة لاختبار الأمان OWASP-ZAP

١. الدخول على الأداة



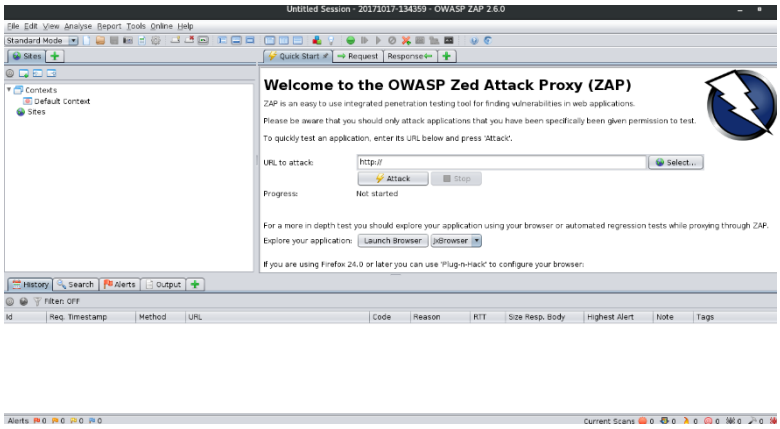
شكل (٦٥) Owasp ٢

٢. نتبع التعليمات الآتية



شكل (٦٥) Owasp ٣

٣. ستظهر لنا الشاشة الآتية :

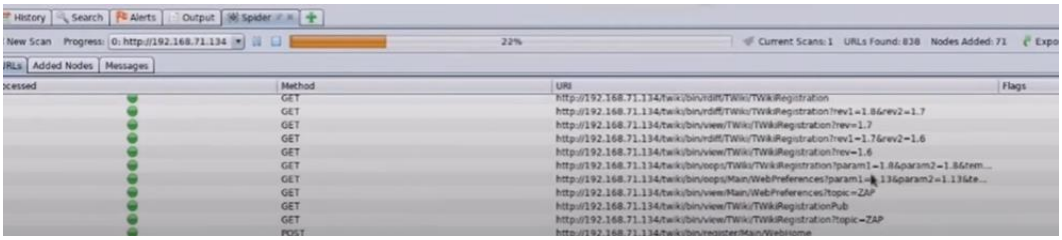


شكل (٦٥) Owasp 4

٤. نقوم بإدخال عنوان Ip هنا ثم الضغط على attack

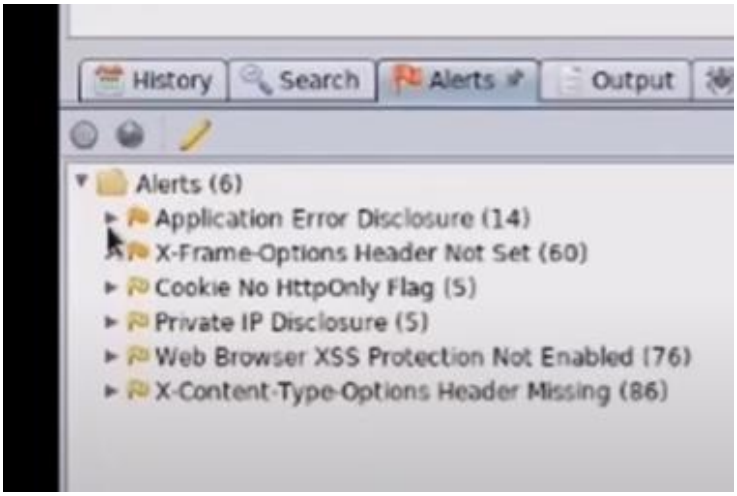
شكل (٦٥) Owasp ٥

٥. سيتم تشغيله من خلال جمع الروابط وعرض وسيتم عرض جميع الثغرات الأمنية



شكل (٦٥) Owasp ٦

٦. سنرى الثغرات الأمنية في خانه **alert**

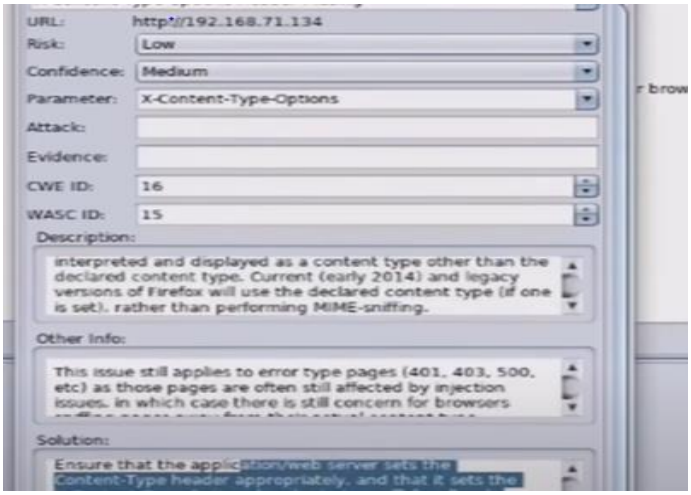


شكل (٦٥) Owasp ٧

٧. **المخرجات**

- error للتطبيقات
- تصنيفهم حسب الألوان

ملاحظة // يمكنني الدخول ومشاهدة الثغرة ووصفها وموقع لحلها



شكل (٦٥) Owasp 8

- يمكن إيقافها من خلال الضغط على **stop**

- **استخدام الأداة IP scanner**

هو ماسح للمنافذ ويقوم بتحليل شبكة الاتصال ويقوم البرنامج بإظهار جميع أجهزة الشبكة، مما يمنح الوصول إلى المجلدات المشتركة والتحكم عن بعد في الأجهزة المتنقلة، وهو برنامج سهل الاستخدام ويعمل كإصدار محمول، لذا فإنه يجب أن يكون الخيار الأول لكل مسؤول شبكة.

- **استخدام الأداة NetStumbler**

تستخدم الأداة في اختراق شبكة Wi-Fi للأجهزة المتنقلة بهدف الوصول غير المصرح به إلى موارد الجهاز والتصنت عليه.

- تثبيت واستخدام أداة NetStumbler

لتثبيت أداة NetStumbler واستخدامها، يمكنك اتباع الخطوات التالية:

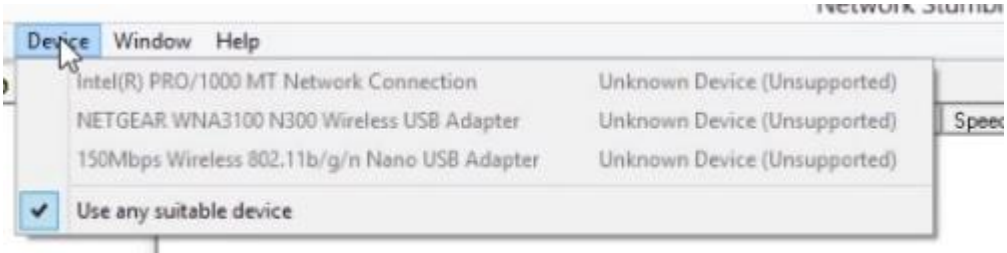
- قم بتنزيل أحدث إصدار من NetStumbler لنظام التشغيل Windows من موقعه الرسمي أو من مصادر موثوقة مثل Uptodown.
- بعد تنزيل البرنامج، قم بتشغيل ملف التثبيت واتبع التعليمات على الشاشة لإكمال عملية التثبيت.
- بمجرد تثبيت NetStumbler، قم بتشغيل البرنامج.
- ستظهر لك واجهة البرنامج التي تعرض قائمة بالشبكات اللاسلكية المحيطة بك وحالتها.
- يمكنك استخدام NetStumbler لتحليل شبكات الـ Wi-Fi المحيطة بك، وتحديد قوة الإشارة، وتحديد المواقع، والتحقق من تكوينات الشبكة، وكشف التداخلات اللاسلكية، وكشف نقاط الوصول غير المصرح بها، وتحديد الاتجاه الذي يجب أن توجهه الهوائيات لتحسين تغطية الشبكة.

ملاحظة: يجب أن تكون لديك نظام التشغيل Windows لاستخدام NetStumbler، ويجب أن تتبع القوانين واللوائح

- **تطبيق عملي**

ملاحظة: هي أداة صعبه تطبيقها عمليا بمكن تطبيقها على شرائح معينة من الأجهزة لأنها أداة قديمة جدا.

١, الدخول على البرنامج والتشيك على الأجهزة



شكل (٦٦) استعراض الاجهزة ١

٢. استعرض لي ٣ أجهزة وجميعها غير مناسبه (يمكن تصنيفها من خلال SSID أو التشفير او من خلال ESS)

٣. إذا كانت مجموعه الأجهزة قليله يمكن أن تكون أجهزة WIFI – قديمة جدا

٤. سنحصل على جهاز netgear Wi-Fi نريد العمل على جهاز ويندوز ٨ فأعلى لكن لا يوجد جهاز مناسب لبطاقات شبكة مناسبة " يمكن تشغيل network tumbler ويوجد ماسحات أخرى لويندوز "

٥. الدخول على الموقع الاتي : ١

https://www.metageek.com/inssider/

٦. الدخول على الموقع الاتي : ٢

http://www.wifichannelscanner.com/ **"يحتاج ترخيص"** أو أي موقع أخر يمكن الاستفادة منه لأجراء عمليات البحث.

- **نبدأ بتحميل البرنامج**

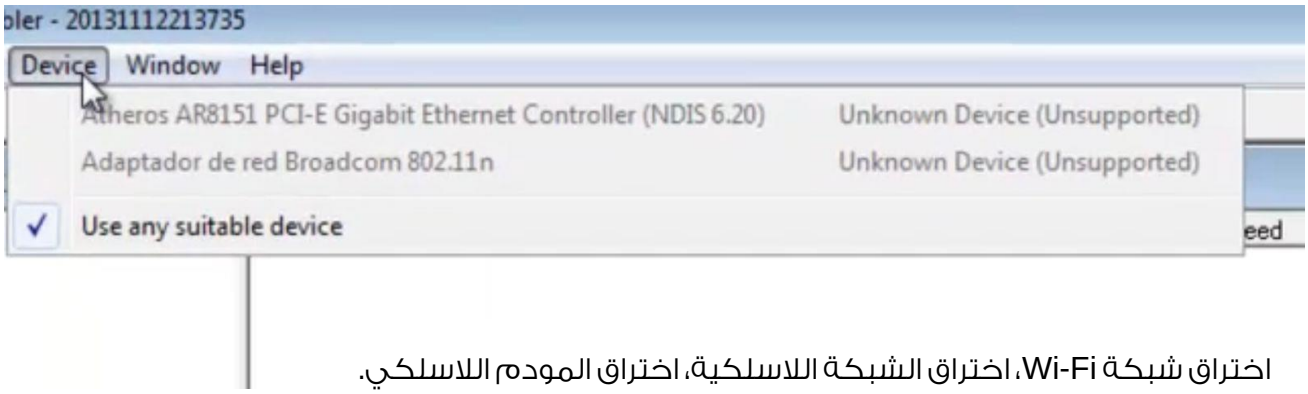
https://netstumbler.ar.uptodown.com/windows/download

NetStumbler لفحص الشبكات اللاسلكية؟

١. قم بتنزيل NetStumbler وتثبيته.

٢. قم بتشغيل NetStumbler بعد ذلك سيبدأ تلقائيًا في فحص الشبكات اللاسلكية من حولك.

٣. بمجرد اكتماله، سترى القائمة الكاملة للشبكات اللاسلكية من حولك **كما هو موضح في اللقطة أدناه:**



- اختراق شبكة Wi-Fi، اختراق الشبكة اللاسلكية، اختراق المودم اللاسلكي.
- قائمة الشبكات اللاسلكية التي تم فحصها بواسطة NetStumbler.
- هناك سترى أعمدة مختلفة مثل MAC وSSID وSPEED وVENDOR وTYPE وغير ذلك الكثير...

٤. حدد الآن أي شخص من عنوان MAC الذي ترغب في اختراقه وتريد استكشاف المزيد حول ذلك ، إذا قمت بالنقر فوق عنوان MAC الخاص بإحدى الشبكات اللاسلكية المكتشفة ضمن القنوات، فسوف ترى رسمًا بيانيًا يوضح قوة إشارة الشبكة اللاسلكية، كلما زاد اللون الأخضر وقلت المساحات، فهذا يشير إلى قوة الإشارة بشكل أفضل.

٥. كما ترون، يوفر NetStumbler أكثر من مجرد اسم (SSID) للشبكة اللاسلكية، فهو يوفر عنوان MAC ورقم القناة ونوع التشفير وغير ذلك الكثير، يتم استخدام كل هذه الأشياء عندما نقرر أننا نريد الدخول إلى الشبكة الآمنة عن طريق فك التشفير.

- **هناك نوعان من طرق التشفير الأكثر شيوعًا التي تستخدمها الشبكات اللاسلكية**

١. WEP (الخصوصية السلكية المكافئة) – لم يعد WEP آمنًا بعد الآن، تم اكتشاف العديد من العيوب التي تسمح للمتسللين باختراق مفتاح WEP بسهولة ، سأشرح كيفية اختراق WEP في البرنامج التعليمي التالي حتى يستمرا في القراءة.

٢. WAP (بروتوكول التطبيقات اللاسلكية) – يعد WAP الخيار الأكثر أمانًا والأفضل حاليًا لتأمين شبكتك اللاسلكية ، لا يمكن اختراقه بسهولة مثل WEP لأن الطريقة الوحيدة لاسترداد مفتاح WAP **هي**:

- استخدام القوة الغاشمة أو هجوم القاموس، إذا كان مفتاحك آمنًا بدرجة كافية، فلن ينجح هجوم القاموس، وقد يستغرق الأمر عقودًا.

❖ منصات وهجمات الهواتف المحمولة

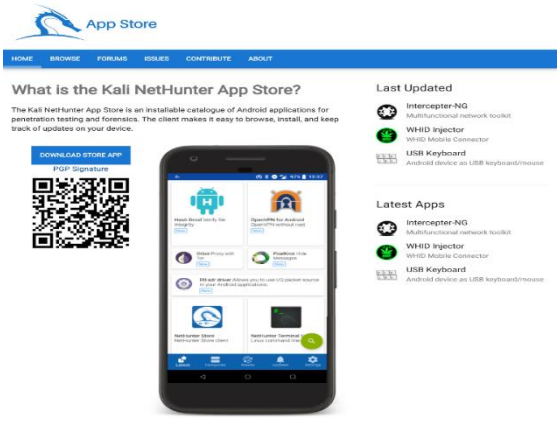
يوجد تقنيات ومنصات يستخدمها المتسلل للوصول إلى جهاز متنقل، تساعد هذه التقنيات المتسللين على استغلال ثغرات النظام ، العديد من تقنيات الهجوم هذه تستفيد من العنصر البشري و الاستخدام السيئ لموارد الجهاز المتنقل – فيمكن أن يتعرض لحمولة زائدة بحيث لا يتمكن المستخدم من الوصول إلى خدماته الأصلية ، ويستخدمها المتسلل لتوصيل جهاز أو شبكة أخرى كما يتم تنفيذ الهجوم على الجهاز ببرامج التجسس المحمولة وتثبيت الباب الخلفيBackdoor وكسر كلمات المرور وتجاوز آليات التشفير وسرقة المعلومات، ترسل برامج التجسس محتوى مثل رسائل البريد الإلكتروني والرسائل المشفرة إلى الجهاز.

- **WiHack**

تم تصميم أدوات الاختراق اللاسلكية، للمساعدة في الهجوم على الشبكات اللاسلكية خدمة الـ Wi-Fi والعديد من هذه الشبكات اللاسلكية محمية بكلمة مرور، ويلزم معرفة كلمة المرور للاتصال بالإنترنت.

- **يوجد العديد من الأدوات الشائعة لاختراق شبكات Wi-Fi**
  - **أداة Kali NetHunter**

Kali NetHunter مخصصة للهواتف ، وعبارة عن منصة مجانية ومفتوحة المصدر لاختبار اختراق الأجهزة المحمولة لأجهزة Android، تعتمد على Kali Linux.

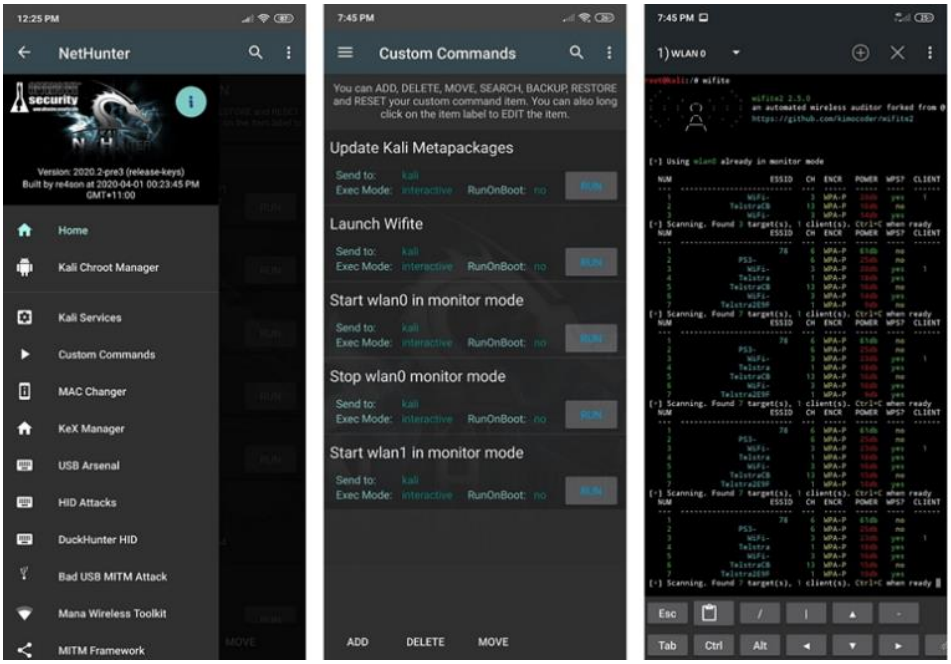


شكل (٦٧) واجهة تحميل البرنامج 1

- **متجر تطبيقات كالي NetHunter**

كلا الإصدارين المتجذرين يوفران أدوات وخدمات إضافية، يمكن للنواة المخصصة توسيع هذه الوظيفة عن طريق إضافة برامج تشغيل إضافية للشبكة وأجهزة USB بالإضافة إلى دعم حقن Wi-Fi لشرائح Wi-Fi محددة.

رابط التحميل: https://store.nethunter.com/



شكل (٦٨) NetHunter |

تطبيق Kali NetHunter متاح في كلا الإصدارين المعتمدين (NetHunter Lite وNetHunter)، بالإضافة إلى أدوات اختبار الاختراق المضمنة في Kali Linux، يدعم NetHunter أيضًا العديد من الفئات الإضافية، مثل HID Keyboard Attacks وهجمات BadUSB وهجمات Evil AP MANA وغيرها الكثير.

- **التطبيق العملي**

كيف تبدأ استخدام Kali Nethunter ؟

تنصيب Kali Nethunter على الهاتف الذكي ليس بالعملية السهلة، فهو ليس بتنصيب تطبيق ثم تنصيبه والبدء في استخدامه، لا يمكن تنصيب نظام Kali Nethunter إلا عن طريق سطر الأوامر Termux في الهاتف الذكي، إن لم تعرف ما هو Termux " **يرجى قراءة الملاحظة الآتية:**

ملاحظة:

تطبيق Termux هو تطبيق للأندرويد، يوفر لك التطبيق منصة Terminal مبنية على اللينكس في هاتفك الذكي، استخدام التطبيق لا يحتاج الى الروت ويشتغل مباشرة، يمكنك من خلال Termux في الهاتف إجراء أيٍ من العمليات الاعتيادية التي تقوم بها في اللينكس، كمثال على ذلك تنصيب برمجيات عن طريق امر apt-get، أو تنصيب أيضا تطبيقات و برامج من خلال GitHub عبر إجراء أمر git clone، الى جانب تنصيب أدوات اللينكس الأخرى للموبايل، يتيح لك التطبيق تنصيب مجموعة من الحزم (Packages) التي توفر لك استخدامات للعديد من البرمجيات اللينكساوية على هاتفك الأندرويد، كما يمكنك تحديث هذه الحزم او البرمجيات بإستخدام Termux، يتميز بالصرامة و القوة و الواجهة المحببة لكل عشاق نظم اللينكس، وعلى عكس تطبيقات أخرى مشابهة (مثل Connectbot) فإستخدام Termux واسع الحيلة ويمكن استخدامه للعديد من الأغراض لإدارة هاتفك، استخدام تطبيق Termux منوط باللينكس بشكل كبير، أي أن البرمجيات التي ستقوم بتنصيبها من خلاله أو التي ستتعامل معها لا تتضمن واجهة جرافيكية في الغالب، و ستتعامل مع أغلبها مع سطر أوامر اللينكس.

- **كيفية البدء في استخدام تطبيق Termux ؟**

١. رابط تحميل البرنامج https://termux.dev/en/

٢. بعد أن تقوم بتحميله وتنصيبه في هاتفك الذكي، تقوم بالنقر عليه، سيُظهر لك التطبيق شاشة سوداء وهي عبارة عن سطر الأوامر (Command Line)

- **بعض الحزم المميزة التي يمكنك تنصيبها واستخدامها:**

- **حزمة تأثير The Matrix :** من منا يكره المصفوفة او The Matrix، كلنا نريد الحصول على بعض التأثيرات الخاصة بها في هاتفنا أليس كذلك ؟ هذه الحزمة المسلية تستطيع أن توفر لك هذا الأمر، قم تشغيل تطبيق Termux **ثم أكتب الأمر التالي:**

```
pkg install cmatrix
```

ثم بعدها لتشغيل هذا التأثير تقوم بكتابة:

سطر cmatrix ثم النقر على Enter

وستجد أن هاتفك أصبح مصفوفات متساقطة، يمكنك الغاءه بالخروج من التطبيق، مجرد حزمة بسيطة ومسلية لا أقل ولا أكثر.

- **تحديث التطبيق والحزم:** قد يصادف ألا يشتغل لديك التطبيق، أو أن بعض الحزم لم تعد تشتغل بعدما كانت تشتغل سابقا بشكل جيد، في هذه الحالة توجب عليك تحديث التطبيق والحزم أيضا، لتحقيق ذلك نقوم بتنفيذ الأمر apt-get update ، هو نفسه الموجود أيضا في اللينكس، سيقوم هذا الأمر بالتحقق من الحزم وتطبيق Termux و يقوم بتحديثها إن توافر أي تحديث لها.

- **حزمة Figlet :** تسمح لك حزمة Figlet بتكوين كتابة مهيكلة لأي عبارة تقوم بإضافتها، على سبيل المثال في الجانب قمنا بهيكلة اسم Aqua Web،

لفعل ذلك نقوم بتحميل حزمة Figlet عن طريق الأمر:

```
pkg install figlet ،
```

ثم بعدها نقوم باستخدامها عن طريق الأمر:

figlet aqua web، مع تغير عبارة aqua web بالعبارة التي تريد.

- **حزمة Python :** اغلب برمجيات الاختراق والحزم تستخدم الـ Python و الـ Ruby بشكل كبير، لذلك قد تود تنصيب حزمتيهما حتى تستطيع تنفيذ أكواد باستخدام اللغتين، لفعل ذلك نقوم بتنفيذ الأمر pkg install python ، هذا الخيار سيسمح لنا بتنصيب مدير الحزم الخاص بالـ python كذلك و هو الـ pip، بعدها سيمكننا البحث عن برمجيات تم ابتكارها بالبايثون واستخدامها عن طريق تنفيذ الأمر pip install في الـ Termux .
- **حزمة الـ Ruby :** كحال الـ Python، نقوم بتنفيذ أمر pkg install ruby ، الذي بدوره سيوفر لنا مدير الحزم الخاص بالـ Ruby و هو Gem، بعدها سيمكنك تشغيل برمجيات أيضا تعتمد على الـ Ruby أو حزم خاصة بها باستخدام الـ Termux .

ما رأيك بتنصيب الـ Metasploit في هاتفك؟

نعم يمكنك فعل ذلك عبر الـ Termux كذلك، تقوم أولا بتنصيب حزمة الـ curl عن طريق الأمر pkg install curl، ثم نقوم بجلب الـ Metasploit من رابطها عن طريق الـ curl بتنفيذ الأمر curl -LO https://raw.githubusercontent.com/Hax4us/Metasploit_termux/master/metasploit.sh ، انتظر قليلا (أو كثيرا) حتى يتم تنصيبها ، بعدها نقوم بإعطاء المنفذ لتشغيل الـ metasploit عبر أمر chmod 777 metasploit.sh ، ثم نقوم بتشغيل الميتاسبلويت عن طريق أمر ./metasploit.sh.

- قم بتنصيبهما بالطبع على هاتفك الذكي

في تطبيق Kali NetHunter Store، ابحث عن تطبيق آخر باسم NetHunter Kex ثم قم بتنزيله من المتجر الآن كل العمل سيتم عبر سطر الأوامر Termux وذلك عبر تنفيذ مجموعة من الأوامر اتباعًا والتي سنتركها لك بالطريقة التالية:

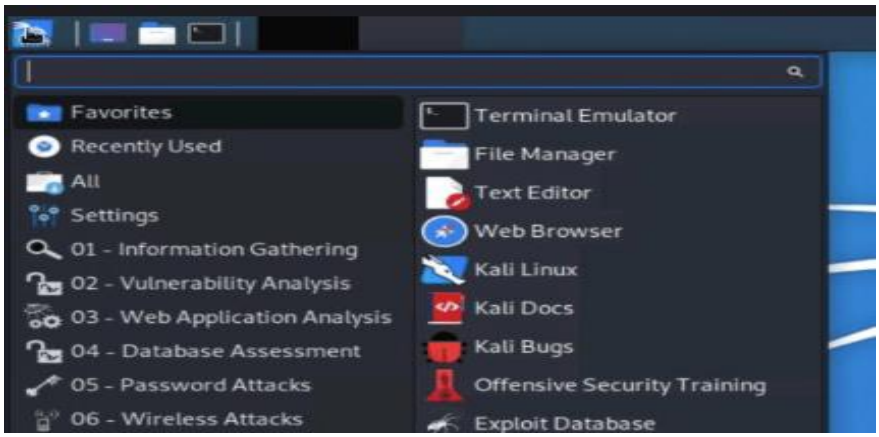
```
1 - apt upgrade // to upgrade termux
2 - apt update   // to update packages
3 - apt install wget // to install wget command
4 - wget -O nethunterInstaller https://offs.ec/2MceZWr  // to download nethunter
5 - chmod +x nethunterInstaller // permission to install nethunter

6 - ./nethunterInstaller // install nethunter
```

شكل (٦٩) Termux termainal 1

- **لنسخ الاكواد من هنا**

تطبيقه من خلال الكالي لينكس

١. نقوم بفتح التير منال



شكل (٦٩) Termux termainal ٢

٢. قم بتثبيت تطبيق NetHunter-Store من store.nethunter.com

٣. من متجر NetHunter، قم بتثبيت Termux وعميل NetHunter-KeX ولوحة مفاتيح Hacker

ملاحظة: قد لا يتغير الزر "تثبيت" إلى "مثبت " في عميل المتجر بعد التثبيت – فقط تجاهله، قد يبدو بدء تشغيل برنامج termux لأول مرة متوقفًا أثناء عرض كلمة "التثبيت" على بعض الأجهزة – ما عليك سوى الضغط على زر الإدخال.

٤. افتح برنامج Termux واكتب:

```
kali@kali:~$ termux-setup-storage
kali@kali:~$ pkg install wget
kali@kali:~$ wget -O install-nethunter-termux https://offs.ec/2MceZWr
kali@kali:~$ chmod +x install-nethunter-termux
kali@kali:~$ ./install-nethunter-termux
```

شكل (٧٠) termux steup ا

- **الاستخدام**

افتح Termux واكتب واحدًا مما يلي:

Command	To
`nethunter`	start Kali NetHunter command line interface
`nethunter kex passwd`	configure the KeX password (only needed before 1st use)
`nethunter kex &`	start Kali NetHunter Desktop Experience user sessions
`nethunter kex stop`	stop Kali NetHunter Desktop Experience
`nethunter <command>`	run in NetHunter environment
`nethunter -r`	start Kali NetHunter cli as root
`nethunter -r kex passwd`	configure the KeX password for root
`nethunter -r kex &`	start Kali NetHunter Desktop Experience as root
`nethunter -r kex stop`	stop Kali NetHunter Desktop Experience root sessions
`nethunter -r kex kill`	Kill all KeX sessions
`nethunter -r <command>`	run `<command>` in NetHunter environment as root

شكل (٧١) أوامر Termux ا

- **Bluediving**

http://bluediving.sf.net

لفتح اتصالات Bluetooth وWi-Fi يسمح بالتنصت واعتراض نقل البيانات ويوجد أدوات عبارة عن مجموعة اختراق بلوتوث التي تنفذ هجمات مختلفة.

Bluediving عبارة عن مجموعة من برامج اختراق البلوتوث ، فهو ينفذ هجمات مثل Bluebug وBlueSnarf وBlueSnarf++ وBlueSmack وميزات مثل انتحال عنوان Bluetooth.

- مثال
  - **اختبار اختراق الأندرويد**

يهدف اختبار اختراق الهاتف المحمول أو Android إلى اكتشاف الثغرات الأمنية والتأكد من أن تطبيقات الهاتف المحمول ليست عرضة للهجمات.

- **أهمية اختبار اختراق Android**

تُستخدم تطبيقات Android الحديثة للأغراض التجارية والرعاية الصحية، والخدمات المصرفية، والتعليم والمزيد، وبصرف النظر عن احتواء تطبيقات الهاتف المحمول هذه على معلومات المهمة، فإنها تحتوي أيضًا على ثغرات أمنية، يمكن لمختبري الاختراق والمطورين العثور على نقاط الضعف هذه وإصلاحها والتخفيف من المخاطر الأمنية.

يتعامل مفهوم Mobile Security مع حماية الأجهزة المتنقل من الهجمات المحتملة من الأجهزة المحمولة الأخرى، أو البيئة اللاسلكية التي يتصل بها الجهاز.

  - **اختبار الاختراق اللاسلكي**

تعد منهجية اختبار قلم تطبيقات الهاتف المحمول بمثابة اختبار لتحليل محيط الأمان داخل بيئة الهاتف المحمول للحصول على نظرة ثاقبة حول نقاط الضعف والاختناقات ومتجهات الهجوم في التعليمات البرمجية المصدر قبل حدوثها، يساعد اختبار الاختراق على زيادة الأمن السيبراني عبر تطبيقات الهاتف المحمول.

- **أهمية اختبار اختراق تطبيقات الهاتف المحمول**

الكثير من يعتمدون على تطبيقات الهاتف المحمول ، توفر تطبيقات الهاتف المحمول الراحة وتمكنهم من أن يكونوا أكثر إنتاجية، مما يجعل الجهاز المحمول جزءاً أساسيًا من العمليات التجارية اليومية ، ومع ذلك، مع الراحة تأتي المخاطر الأمنية، ونظرًا للحجم الكبير من البيانات التي تتم معالجتها من خلال تطبيقات الهاتف المحمول، فهي هدف رئيسي للهجمات السيبرانية ، يعد اختبار قلم تطبيقات الهاتف المحمول أمرًا مهمًا لإدارة الأمان عبر منصات التطبيقات هذه ، نظرًا لأنه يتم العثور على ثغرات أمنية جديدة يوميًا، الشركات دائما في حالة من الاستباقية لضمان أن تطبيقات الهاتف المحمول الخاصة بها آمنة من الهجمات الإلكترونية الحديثة وتقليل فرصة البرامج الضارة أو برامج التجسس أو أي خرق أمني آخر.

- **اختبار الاختراق لجهاز أندرويد**

الخطوات الأساسية في جهاز Android OS هي كما يلي :

الخطوة ١ : قم بتجذير نظام التشغيل بمساعدة أدوات مثل SuperOneClick وSuperboot من أجل تحميل البرنامج :

/ https://superoneclick-download.soft112.com/https://www.malavida.com/en/soft/superoneclick

- **لاستخدام SuperOneClick، اتبع الخطوات التالية:**

- قم بتنزيل SuperOneClick من مصدر موثوق مثل موقع XDA Developers.

SuperOneClick هو برنامج مجاني لتجذير أجهزة Android تم تطويره بواسطة XDA Developers، ويتميز بتطبيق توصيل سهل الاستخدام لمعظم موديلات هواتف Android.

- **تمكين تصحيح أخطاء USB على هاتف Android الخاص بك**

- انتقل إلى الإعدادات > التطبيقات > التطوير وقم بتمكين تصحيح أخطاء USB.
- قم بتوصيل هاتفك بالكمبيوتر باستخدام كابل USB.
- افتح SuperOneClick على جهاز الكمبيوتر الخاص بك.
- اتبع الإرشادات التي يقدمها البرنامج لعمل روت لهاتف Android الخاص بك.
- قد تختلف الخطوات المحددة وفقًا لطراز هاتفك وإصدار SuperOneClick الذي تستخدمه.

يرجى ملاحظة **أن عمل روت لهاتف Android الخاص بك يمكن أن يلغي الضمان الخاص بك وقد يكون له مخاطر مرتبطة به، تأكد من فهم الآثار المترتبة والمضي قدما بحذر.**

ملاحظة: من المهم تنزيل SuperOneClick من مصدر موثوق به واتباع التعليمات بعناية، توخي الحذر دائمًا عند عمل روت لجهازك، حيث من المحتمل أن يؤدي ذلك إلى تلف جهازك وإبطال الضمان الخاص بك.

- الحصول على حق الوصول الإداري إلى نظام التشغيل والتطبيقات.

الخطوة ٢: تنفيذ هجوم DoS من أجل إجراء اختبار التحمل للتطبيقات أو نظام التشغيل.

الخطوة ٣: التحقق من وجود نقاط الضعف في متصفحات الويب، التحقق بشكل أساسي من وجود خطأ في البرمجة النصية عبر التطبيقات في متصفح Android.

الخطوة ٤: التحقق من وجود ثغرات أمنية واحدة من أفضل الأدوات المستخدمة لهذا هي sqlmap الموجودة في توزيعة كالي لينكس.

الخطوة ٥: القيام بتعديل معلومات المستخدمين واستبدالها.

يعد اختبار اختراق Android، أو اختبار الاختراق، ممارسة أمنية حيوية تتضمن اختبار تطبيقات Android لتحديد نقاط الضعف المحتملة، يقوم متخصصو الأمن بمحاكاة سيناريوهات الهجوم الواقعية على التطبيق في بيئة خاضعة للرقابة.

- **فيما يلي دليل خطوة بخطوة لاستخدام SuperOneClick:**

- قم بتنزيل SuperOneClick من مصدر موثوق، مثل موقع XDA Developers.
- تأكد من تنزيل الإصدار المناسب لجهاز الكمبيوتر الذي يعمل بنظام Windows.
- تمكين تصحيح أخطاء USB على هاتف Android الخاص بك.
- انتقل إلى الإعدادات > حول الهاتف > اضغط على "رقم الإصدار" سبع مرات لتمكين خيارات المطور.
- ارجع إلى الإعدادات > خيارات المطور > تمكين تصحيح أخطاء USB.
- قم بتوصيل هاتف Android الخاص بك بالكمبيوتر باستخدام كابل USB.
- قم بتشغيل تطبيق SuperOneClick على جهاز الكمبيوتر الخاص بك.
- في واجهة SuperOneClick، انقر فوق الزر "Root" لبدء عملية التجذير.

اتبع التعليمات التي تظهر على الشاشة والتي يقدمها البرنامج، انتظر حتى تكتمل العملية.

قد ترى مطالبة تشير إلى إكمال عملية التجذير بنجاح، أعد تشغيل هاتف Android الخاص بك بعد إجراء عملية الروت، يوصى بهذه الخطوة لضمان سريان التغييرات.

- **يرجى ملاحظة** أن الخطوات المحددة قد تختلف قليلاً حسب طراز هاتفك وإصدار SuperOneClick الذي تستخدمه، من المهم اتباع التعليمات التي يقدمها لك البرنامج بعناية وتوخي الحذر عند عمل روت لجهازك.

تمارين الفصل الثامن

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	تخزين غير آمن للبيانات مما يترك فجوات أمنية قد تكون عرضة لتسرب البيانات هي من نقاط الضعف المتنقلة	√
٢.	(Netstambler) هو ماسح للمنافذ ويقوم بتحليل شبكة الاتصال ويقوم البرنامج بإظهار جميع أجهزة الشبكة، مما يمنح الوصول إلى المجلدات المشتركة والتحكم عن بعد في الأجهزة المتنقلة.	×
٣.	(OWSAP) تستخدم لاختبار أمان تطبيقات الأجهزة المتنقلة	√
٤.	(WE-Wi-Fi) خدمة Wi-Fi منتشرة ، العديد من هذه الشبكات اللاسلكية محمية بكلمة مرور، ويلزم معرفة كلمة المرور للاتصال بالإنترنت.	×
٥.	لفتح اتصالات Bluetooth وFi-Wi يسمح بالتنصت واعتراض نقل البيانات ويوجد أدوات عبارة عن مجموعة اختراق بلوتوث التي تنفذ هجمات مختلفة نستخدم Bluediving	√
٦.	يهدف اختبار اختراق الهاتف المحمول أو Android إلى اكتشاف الثغرات الأمنية والتأكد من أن تطبيقات الهاتف المحمول ليست عرضة للهجمات	√
٧.	يتعامل مفهوم Mobile Security مع حماية الأجهزة المتنقل من الهجمات المحتملة من الأجهزة المحمولة الأخرى، أو البيئة اللاسلكية التي يتصل بها الجهاز	√
٨.	Kali NetHunter عبارة عن منصة مجانية ومفتوحة المصدر لاختبار اختراق الأجهزة المحمولة لأجهزة Android، تعتمد على Kali Linux.	√
٩.	ملاحظة أن عمل روت لهاتف Android الخاص بك يمكن أن يلغي الضمان الخاص بك وقد يكون له مخاطر مرتبطة به، تأكد من فهم الآثار المترتبة والمضي قدما بحذر	√

٢. **طبق ما يلي عمليا :**

١. **لتثبيت ZAPROX نستخدم**

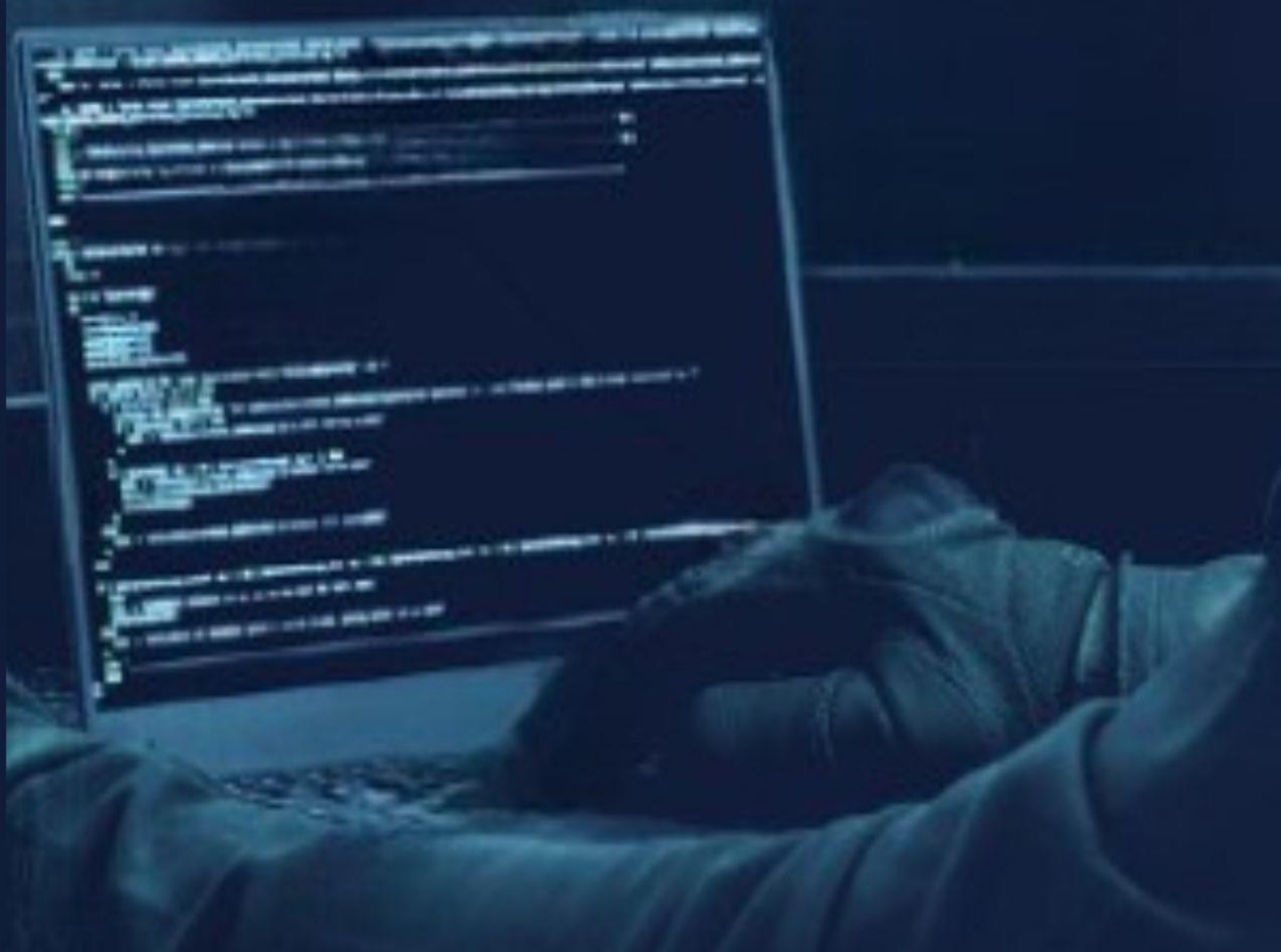
```
sudo apt install zaprox
```

اختراقات البرامج الضارة للحواسيب

الفصل التاسع

في هذا الفصل سنتعرف على المواضيع التالية:

- مفاهيم حصان طروادة وأنوعها
- هجمات Dos (Denial of service)
- اختطاف الجلسة Session Hijacking
- تحليل البرامج الضارة
- التدابير المضادة ضد البرامج الضارة



❖ مفاهيم حصان طروادة وأنواعها

من أخطر و أشد أنواع الاختراقات الأمنية المعلوماتية و يعتبر شفرة برمجية و هذه الشفرة تكون منقسمة إلى قسمين ، القسم الأول يتم إرسالها للجهاز الهدف (الضحية) و القسم الثاني شفرة برمجية تتحكم به حسب تعليمات في جهاز المهاجم و تتحكم في كافة موارد النظام الرئيسي لجهاز الضحية و يمكن أن يقوم بسرقة جميع ما يوجد في الجهاز من معلومات سرية وغير سرية ويعتمد على ثغرات خلفية أمنية و تعمل أحيانا على تخريب أجهزة الحاسبات الشخصية و لا يمكن إصلاح بعضها إلا بإعادة تثبيت نظام التشغيل مرة أخرى بعد مسح كافة معلومات النظام السابق المصاب وتقوم هذه الشفرة المصدرية البرمجية بنسخ جميع الضربات الكهربائية من مفاتيح الضحية وتحتفظ بها كسجلات وترسلها للشفرة الأخرى لجهاز المهاجم ويختلف هذا النموذج عن غيره بأنه لا يحتاج إلى الانتشار بين الملفات فقط يلصق نفسه بملفات النظام حيث يعمل فورا معه وينتقل إلى ذاكرة الجهاز الرئيسية ليقوم بعمله كما تم برمجته مسبقا".

- **أنواع أحصنة طروادة**

١. أحصنة طروادة المتسللة

إنها واحدة من أبسط أنواع أحصنة طروادة، ولكن من المحتمل أن تكون هي الأكثر خطورة ، وهذا لأن بإمكانها إما تحميل مختلف أنواع البرمجيات الضارة على جهاز الضحية وهي تقوم بدورها كمنفذ للوصول للجهاز ، أو على الأقل التأكد من جعل جهاز الحاسب عرضة للهجوم ، يتم إعداد Bot Net عن طريق التسلل في أغلب الأحيان ، وعندئذ، يصبح جهاز الحاسب جزءًا من شبكة خبيثة تُستخدم لإطلاق الهجمات ، كما يمكن للتسلل أن يسمح بتنفيذ الأوامر والتعليمات البرمجية على جهاز الضحية أو مراقبة حركة المرور على الويب فيه.

٢. أحصنة طروادة الحاملة/المنزّلة للبرمجيات الضارة

يعد برنامج Emotet الخبيث أحد أشهر أحصنة طروادة المحملة بالبرمجيات الضارة، والذي أصبح الآن غير ضار، ولكنه، على العكس من حصان طروادة المتسلل، لا يمكنه تنفيذ أي تعليمة برمجية على جهاز الحاسب بنفسه، بل إنه يجلب معه برامج ضارة أخرى، منها على سبيل المثال Trojan Trickbot المهدد للخدمات المصرفية، و Ryuk المخصص لطلب الفدية وعلى ذلك ، فإن أحصنة الطروادة المحملة بالبرمجيات الضارة تشبه تلك المنزّلة لها، ويكمن الفرق في أن أحصنة التنزيل تحتاج إلى مورد شبكي لجلب البرامج الضارة من الشبكة ، لكن الأحصنة المحمَّلة تحتوي هي نفسها على مكونات خبيثة أخرى داخل حزمة البرنامج ، ويمكن تحديث النوعين كليهما من أحصنة طروادة عن بعد في السر من قبل المبرمجين المسؤولين.

٣. أحصنة طروادة المهددة للخدمات المصرفية

تعد أحصنة طروادة المهددة للخدمات المصرفية أحد أكثر أنواع أحصنة طروادة انتشارًا، ونظرًا للقبول المتزايد للخدمات المصرفية عبر الإنترنت، فضلاً عن إهمال بعض المستخدمين، فإن هذه البرمجيات تعد طريقة واعدة للمهاجمين للحصول على الأموال بسرعة، وهدفهم هو الحصول على بيانات اعتماد الوصول إلى الحسابات المصرفية.

٤. أحصنة طروادة الموزعة للحرمان من الخدمات(DDoS)

في هذه الهجمات، يتم إغراق الخادم أو الشبكة بسيل من الطلبات، الأمر الذي يتم عادةً بواسطة الروبوتات.

٥. البرامج الزائفة لمكافحة الفيروسات من أحصنة طروادة

تتسم البرامج الزائفة لمكافحة الفيروسات من أحصنة طروادة بطابع خاص، إذ يتعرض كل جهاز تهاجمه لمشكلة خطيرة، بدلاً من أن يتم حمايته، فمن خلال اكتشافها الفيروسات المزعومة، تهدف إلى التسبب في حالة من الذعر بين المستخدمين المطمئنين وإقناعهم بشراء حماية فعَّالة من خلال دفع رسوم، ولكن بدلاً من استخدام برنامج مسح فيروسات مفيد، يواجه المستخدم المزيد من المشكلات فقط، حيث يتم نقل بيانات الدفع الخاصة به إلى منشئ أحصنة طروادة.

٦. حصان طروادة لص الألعاب

يسرق هذا النوع من البرامج معلومات حساب المستخدم من اللاعبين عبر الإنترنت.

٧. أحصنة طروادة للمراسلة الفورية(IM)

تسرق أحصنة طروادة للمراسلة الفورية معلومات تسجيل الدخول وكلمات المرور الخاصة ببرامج المراسلة الفورية مثل ICQ و MSN Messenger و AOL Instant Messenger و Yahoo Pagerو Skype وما إلى ذلك.

٨. أحصنة طروادة لطلب الفدية

بإمكان هذا النوع من أحصنة طروادة تعديل البيانات على الحاسب بحيث لا يعمل الحاسب بشكل صحيح أو يتعذّر استخدام بيانات معينة، ولن يقوم المجرم باستعادة أداء الحاسوب أو إلغاء حظر بيانات الضحية إلا بعد أن يدفع الفدية المالية التي طلبها.

٩. أحصنة طروادة عبر الرسائل النصية القصيرة(SMS)

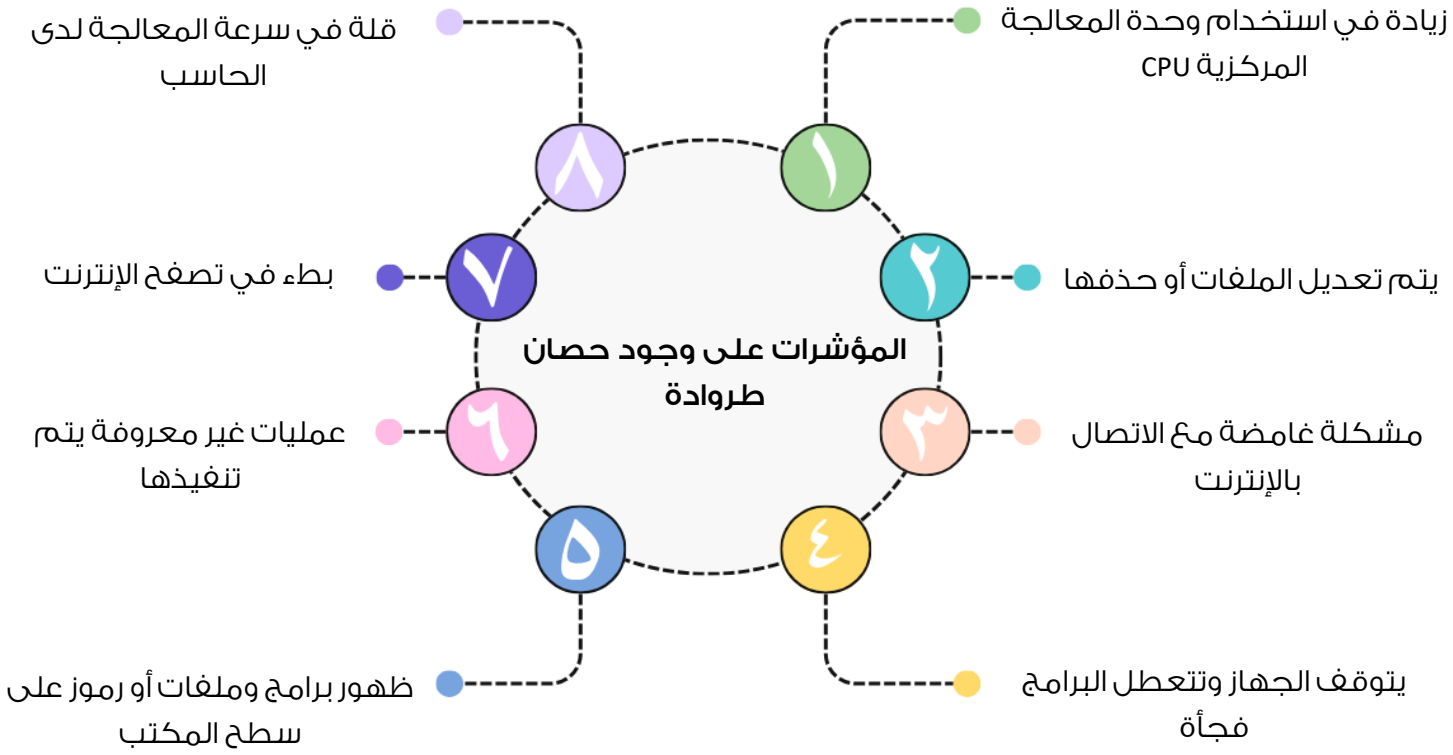
قد يشكل تهديدًا كبيرًا، يمكن أن تعمل أحصنة طروادة عبرSMS ، مثل برنامج Android الضار Faketoken، بطرق مختلفة، على سبيل المثال، يرسل Faketoken رسائل SMS جماعية إلى أرقام دولية متسببًا في تكلفة باهظة، ويتنكر داخل النظام كتطبيق SMS قياسي، ويتعين على مالك الهاتف الذكي دفع تكاليف ذلك.

١٠. أحصنة طروادة التجسسية

بإمكان أحصنة طروادة التجسسية مراقبة كيفية استخدام الضحية للحاسوب، على سبيل المثال، عن طريق تتبع البيانات التي يدخلها عبر لوحة المفاتيح أو تصوير لقطات للشاشة أو الحصول على قائمة بالتطبيقات قيد التشغيل.

١١. أحصنة طروادة للعثور على البريد

بإمكان هذه البرامج الحصول على عناوين البريد الإلكتروني من حاسوب الضحية.



- **أدوات الكشف عن حصان طروادة (عملي)**

يوجد الكثير من الأدوات التي تكشف وجود البرامج الخبيثة من أجهزة الحاسب:

- **Netstat**

من الأدوات المشهورة في عرض معلومات الشبكة، يتعامل ويراقب حركة المرور للمعلومات الواردة والصادرة في الشبكة وهو مهم لمديري الشبكات لتحديد عناوين الإنترنت والبرامج التي يتصل معها الجهاز، حيث يمكن لمدير الأمن السيبراني ملاحظة أي برنامج خبيث متصل بالجهاز وتحديد مكانه في الجهاز لإزالته بالشكل الصحيح.

اسم netstat مشتق من العبارة Network and Statistics ، وهو اسم لبرنامج يستخدم في سطر الأوامر في أنظمة التشغيل لتزويد المستخدم بالمعلومات والإحصائيات المتعلقة بالشبكة وكل ما يتعلق بها، من بينها منافذ الشبكة المفتوحة البروتوكولات مثل UDP و TCPوعناوين IP المتصل، يتواجد هذا الأمر افتراضيًا في موجه أوامر الويندوز وطرفيه نظام لينكس، وقد يختلف من ناحية التعامل معه بين هذه الأنظمة في أشياء بسيطة ، لكنه يحقق نفس الغرض المطلوب، أيضًا إن netstat هي أداة تستخدم في سطر الأوامر فقط ولا توجد لها واجهة رسومية.

- **استخدام Netstat**

١. في ويندوز

الذهاب إلى سطر الأوامر، الذهاب إلى ابدأ ، كتابة CMD كتابة netstat والضغط على Enter .

٢. في كالي لينكس

```
# netstat -a | mo
```

- **Tcpview**

يتيح رؤية جميع اتصالات بروتوكولات TCP & UDP ويعطي تقرير عن حالة الاتصال واسم العملية المرتبطة بها مع إمكانية إنهاء اتصال أي عملية يتم الشك في طبيعة عملها.

هذه الأداة تراقب كل الاتصالات الشبكية (TCP or UDP) التي تجريها العملية أو البرنامج وتقوم بعرض عنوان الجهة الأخرى التي قام البرنامج بالاتصال بها وعلى أي منفذ تم ذلك ولكنها لا توضح البيانات المرسلة أو القادمة، يتم عمل لها Download.

❖ هجمات Dos (Denial of service)

هي نوع الهجمات الشبكية وينتج عنها تعطيل خدمات الشبكة عن طريق إغراق الخادم Server بالطلبات المسموحة بقصد تعطيله عن التجاوب مع طلبات المستخدمين.

❖ اختطاف الجلسة Session Hijacking

يقوم المخترق بتعيين معرف جلسة مستخدم للمستخدم "للضحية المعروفة" على سبيل المثال، سوف يقوم المخترق بإرسال بريد إلكتروني إلى الضحية المعروفة مع رابط يحتوي على معرف جلسة معينة، إذاً اتبع الضحية هذا الرابط، يمكن للمتسلل استخدام تلك الجلسة والوصول إلى الجهاز.

❖ تحليل البرامج الضارة

دراسة تلك البرمجيات الخبيثة عن طريق تحليل مكوناتها المختلفة ودراسة سلوكها على نظام التشغيل، وفهم كيفية عمل هذه البرمجيات كمحاولة لكشف من قام بإنشاء هذه البرمجية أو كشف الهدف من نشرها واستخدامها.

عند تحليل برمجية خبيثة معينة عند اكتشافها وكانت تقوم بمحاولة اتصال عكسي مع عنوان IP معين ، من خلال هذا العنوان يمكن تحديد هوية الشخص الذي قام بإنشاء أو استخدام هذه البرمجية، لا يتطلب أن يكون محلل برمجيات خبيثة مخترقاً محترفاً، ولكن يجب أن تكون لديه مهارات برمجية قوية.

- **تصنيف عملية التحليل**

١. Static Analysis

عملية دراسة البرمجية بدون تنفيذها، محاولة إيجاد أكبر قدر من المعلومات بدون تنفيذ هذه البرمجية من خلال فحص الرمز البرمجي المصدري إذا أمكن ذلك.

٢. Dynamic Analysis

عملية دراسة البرمجية الخبيثة أثناء وبعد تنفيذها وتحليل التفاعل مع النظام والعمليات الخاصة التي قامت هذه البرمجية بإنشائها أو الاعتماد عليها

عند تحليل أي برمجية خبيثة يجب استدعاء عمليات النظام ومعرفة ما هي البارامترات التي تقوم البرمجية بتمريرها للتوابع الخاصة بعمليات النظام.

هذه البارامترات يمكن أن تكشف معلومات مهمة عن هذه البرمجية، كما يجب مراقبة مصادر النظام لمعرفة مدى استهلاك البرمجية الخبيثة لمصادر النظام مثل الذاكرة Ram عن طريق إنشاء نسخة احتياطية لسجلات النظام قبل تشغيل البرمجية الخبيثة ومن ثم استخدام أداة معينة لتقوم بالمقارنة واكتشاف التغيرات التي تمت بسبب تشغيل هذه البرمجية ومعرفة التغيرات التي تُحدثها البرمجية الخبيثة في سجلات النظام Windows Registry مفيد جدا في عملية إزالة هذه البرمجية من النظام المصاب بها.

عملية تحليل البرمجية الخبيثة يجب أن تتم في بيئة تجريبية آمنة Virtual Machine معزولة بشكل كامل عن الشبكة.

أدوات تحليل البرمجيات الخبيثة Idapro هي الأدوات المفيدة في عملية تحليل البيانات وهي تعطي صورة عن العمليات التي تتم على النظام **ومنها:**

Idapro	هي أداة لتحليل الكود الثنائي، قادر على إنشاء خرائط لتنفيذ البرنامج لإظهار التعليمات الثنائية التي يتم تنفيذها بالفعل بواسطة المعالج في تمثيل رمزي يسمى لغة التجميع. طورته شركة Hex-Rays، ويستخدم في الهندسة العكسية للكود الثنائي، بصفته أداة فك ومصحح أخطاء، فإنه يمكّن المستخدمين من التعمق في التفاصيل المعقدة للملفات القابلة للتنفيذ، بما في ذلك الملفات التنفيذية والمكتبات المشتركة وملفات الكائنات والبرامج الثابتة.
Virus total	تأسست Virus Total في عام ٢٠٠٤ كخدمة مجانية تحلل الملفات وعناوين URL بحثًا عن الفيروسات والديدان وأحصنة طروادة وأنواع أخرى من المحتوى الضار. هدفها هو جعل الإنترنت مكانًا أكثر أمانًا من خلال التعاون بين أعضاء صناعة مكافحة الفيروسات والباحثين والمستخدمين النهائيين من جميع الأنواع.

❖ التدابير المضادة ضد البرامج الضارة

يجب أن يكون هناك برامج مضادة لأحصنة طروادة وأفضل تلك البرامج المضادة لها التي تصطادها وتكتشفها قبل تحميلها **هي:**

- **Trojan Hunter**

هو ماسح متقدم للبرامج الضارة يكتشف جميع أنواع البرامج الضارة مثل أحصنة طروادة وبرامج التجسس وبرامج الإعلانات المتسللة وبرامج الاتصال ويعمل على إزالتها.

- **الخصائص الرئيسية**

- مسح الذاكرة لاكتشاف أي نسخة معدلة من بنية معينة لحصان طروادة.
- فحص السجل للكشف عن آثار أحصنة طروادة في السجل.
- مسح Ini file للكشف عن آثار أحصنة طروادة في ملفات التكوين.
- مسح المنافذ للكشف عن منافذ طروادة المفتوحة.

لعمل Download يتم الذهاب إلى الموقع https://trojanhunter.informer.com

- **Emsisoft**

هو برنامج يكتشف التهديدات الجديدة بشكل فعال قبل أن يتم اختراق جهاز الحاسب.

لعمل Download يتم الذهاب إلى الموقع https://www.emsisoft.com/en/

- **McAfee**

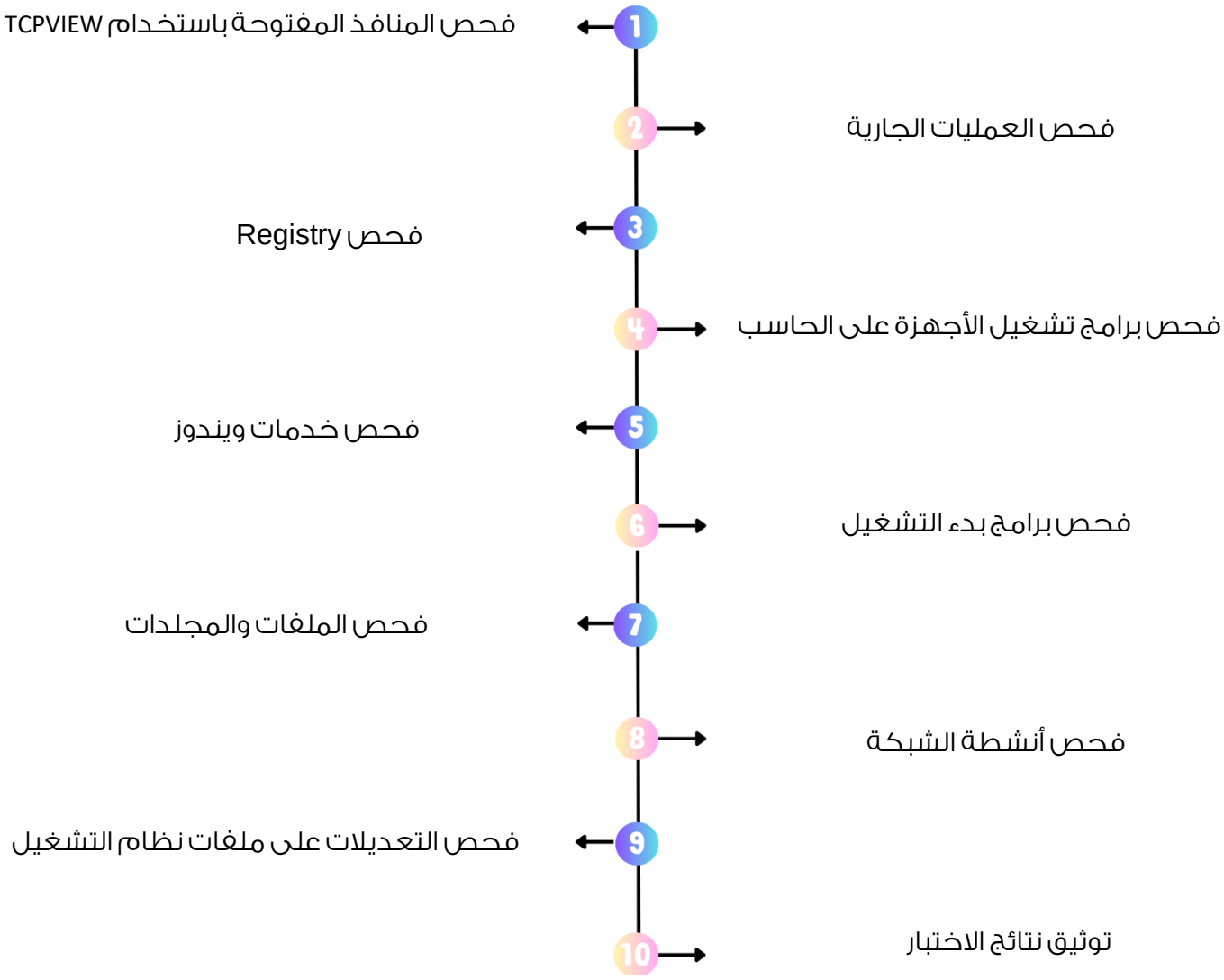
هو برنامج يستخدم لتجنب الرسائل النصية الاحتيالية باستخدام الحماية المدعومة بالذكاء الاصطناعي، ويمكنه حظر الروابط الخطرة إذا تم القيام بالنقر فوقها عن طريق الخطأ، كما يقوم بالتنبيه إذا اكتشف روابط احتيالية، يحظر الروابط الخطرة من رسائل البريد الإلكتروني والنصوص ووسائل التواصل الاجتماعي إذا قمت بالنقر فوقها عن طريق الخطأ.

لعمل Download يتم الذهاب إلى الموقع https://www.mcafee.com

- **اختبار الاختراق**

يجب اتباع نفس الاستراتيجيات التي يتبعها المهاجم لاختبار النظام أو الشبكة ضد طروادة ويجب تنفيذ كل ما هو متاح من تقنيات الهجوم لمعرفة الثغرات ونقاط الضعف والإشارة إلى التدابير المضادة التي تجعل المنظمة بشكل أقوى.

- **خطوات الاختبار**



بمجرد الانتهاء من الاختبار من الممكن الحصول على أحصنة طروادة للتحليل والتحقق من وجوده وفي التحقق من وجوده يجب عزل الجهاز فورا قبل أن ينتقل للأجهزة الأخرى والتأكد ما إذا كان يتم تحديث برامج مكافحة الطروادة.

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	من أنواع احصنه طروادة الأحصنة المتسلسلة	√
٢.	بإمكان هذا النوع من أحصنة طروادة تعديل البيانات على الحاسب بحيث لا يعمل الحاسب بشكل صحيح أو يتعّذر استخدام بيانات معينة، ولن يقوم المجرم باستعادة أداء الحاسوب أو إلغاء حظر بيانات الضحية ألا بعد أن يدفع الفدية المالية التي طلبه (أحصنة SMS)	×
٣.	في هذه الهجمات، يتم إغراق الخادم أو الشبكة بسيل من الطلبات، الأمر الذي يتم عادًة بواسطة الروبوتات (أحصنة DDOS)	√
٤.	هي نوع الهجمات الشبكية وينتج عنها تعطيل خدمات الشبكة عن طريق إغراق الخادم Server بالطلبات المسموحة بقصد تعطيله عن التجاوب مع طلبات المستخدمين (هي هجمات DOS)	√
٥.	من خطوات اختبار الاختراق (فحص العمليات الجارية)	√
٦.	يوجد الكثير من الأدوات التي تكشف وجود البرامج الخبيثة من أجهزة الحاسب منها (NET>DO)	×
٧.	(Idapro) هي أداة لتحليل الكود الثنائي، قادر على إنشاء خرائط لتنفيذ البرنامج إظهار التعليمات الثنائية التي يتم تنفيذها بالفعل بواسطة المعالج في تمثيل رمزي يسمى لغة التجميع.	√
٨.	يجب أن يكون هناك برامج مضادة أحصنة طروادة وأفضل تلك البرامج المضادة لها التي تصطادها وتكتشفها قبل تحميلها هي (Trojan Hunter)	√
٩.	(Emsisoft) هو برنامج يكتشف التهديدات الجديدة بشكل فعال قبل أن يتم اختراق جهاز الحاسب	√
١٠.	(360 total) 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 اكتشف روابط احتيالية ، يحظر الروابط الخطرة من رسائل البريد الإلكتروني والنصوص ووسائل التواصل الاجتماعي إذا قمت بالنقر فوقها عن طريق الخطأ	×

الفصل العاشر

اختراقات الهندسة الاجتماعية

في هذا الفصل سنتعرف على المواضيع التالية:

- تقنيات الهندسة الاجتماعية
- الهجمات البشرية
- الهجمات الحاسوبية
- الهجمات المعتمدة على الهاتف المحمول
- الأدوات
- الأمن المادي والأدوات المادية
- التدابير المضادة والحماية من عمليات الهندسة الاجتماعية

❖ تقنيات الهندسة الاجتماعية

الهندسة الاجتماعية نوع من التقنيات التي يستخدمها المجرمون الإلكترونيون بهدف استدراج المستخدمين غير المرتابين لإرسال بياناتهم السرية، وإصابة حواسيبهم ببرامج ضارة، أو فتح روابط إلى مواقع مصابة، بالإضافة إلى ذلك، قد يحاول المتطفلون استغلال نقص معرفة المستخدم؛ فبفضل سرعة تقدم التكنولوجيا، قد لا يدرك الكثير من المستهلكين والموظفين القيمة الحقيقية للبيانات الشخصية، وقد يجهلون الطريقة المثلى لحماية هذه المعلومات.

تشير الهندسة الاجتماعية إلى جميع التقنيات التي تهدف إلى التحدث عن هدف في الكشف عن معلومات محددة أو القيام بعمل معين لأسباب غير مشروعة، على الرغم من وجود هذا النوع من الخداع دائمًا، إلا أنه تطور بشكل كبير مع تقنيات تكنولوجيا المعلومات والاتصالات.

أكثر ما يجعل الهندسة الاجتماعية خطيرة والسبب في أنها محط اهتمام الشركات هو أنها تعتمد على الأخطاء البشرية، بدلاً من الثغرات في البرامج وأنظمة التشغيل، حيث إن الأخطاء التي يقوم بها المستخدمون الشرعيون من الصعب ملاحظتها أو التنبؤ بها، ممّا يجعل التعرف عليها ومنعها أكثر صعوبة من التسلل المستند إلى البرامج الضارة.

- **بشكل عام يمتلك مهاجمو الهندسة الاجتماعية هدفًا من هدفين:**

١. التخريب

يكون هذا بتعطيل أو إتلاف البيانات لإحداث ضرر أو لمجرد الإزعاج.

٢. السرقة

الاستيلاء على الأشياء 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 وخيانة الثقة والإقناع المباشر والغير مباشر واستغلال الإنترنت ،أما الآثار المترتبة على تقنية الهندسة الاجتماعية، فهي خطيرة لأنها تُتيح للمهاجم الحصول على ما يحتاجه من المعلومات المهمة لتنفيذ الهجوم من خلال خداع الآخرين لكسر الإجراءات الأمنية والحصول على كلمات المرور للدخول إلى النظام ويوجد عدة أنواع من هجمات الهندسة الاجتماعي مثل الهجمات البشرية والهجمات الحاسوبية والهجمات المعتمدة على الهاتف المحمول وغيرها .

شكل (٧٢) Social Engineering attack ا

يقوم عمل الهندسة الاجتماعية على ما يلي:

١. جمع المعلومات

هذه هي المرحلة الأولى، من أجل الحصول على معلومات أكثر عن الضحية المقصودة، ويتم جمع المعلومات من مواقع المنظمون، ومنشورات أخرى وأحيانًا عن طريق التحدث إلى مُستخدمي النظام المُستهدف، (التواصل معهم).

٢. خطة الهجوم

يحدد المهاجمون كيفية تنفيذ الهجوم، وما هي الأدوات والوسائل التي يمكن استخدامها في الهجوم.

٣. أدوات الاستحواذ

نتضمن برامج الحاسب التي سيستخدمها المُهاجم عند بدء الهجوم.

٤. الهجوم

استغلال نقاط الضعف في النظام المُستهدف، أو الأفراد.

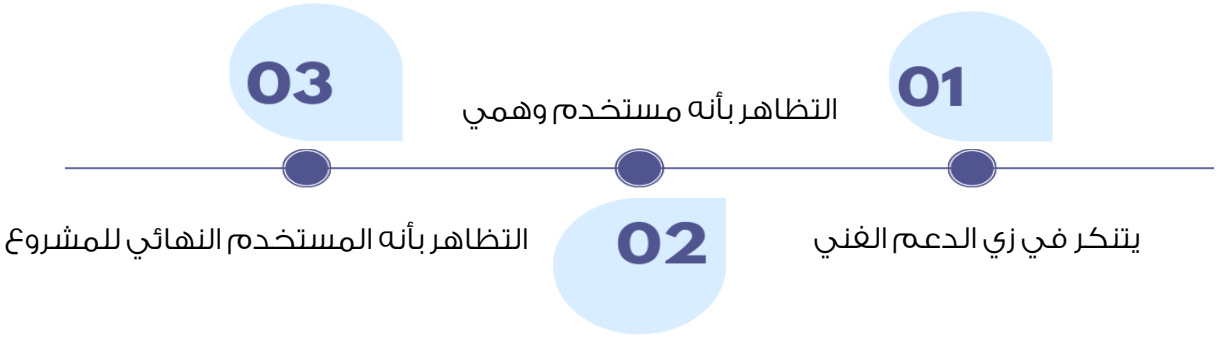
٥. استخدام المعرفة المكتسبة

وذلك من خلال المعلومات التي تم تحصيلها من الأفراد أو المؤسسات.

❖ الهجمات البشرية

هو استخدام الأساليب والمهارات البشرية مثل الأساليب الكلامية أو النفسية الإيحائية أو الإعلانية 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 لأنهم يستخدمون مهارات التعامل مع البشر لاستغلالهم.

- **وفيما يلي الطرق التي تؤديها الهندسة الاجتماعية القائمة على البشر**



❖ الهجمات الحاسوبية

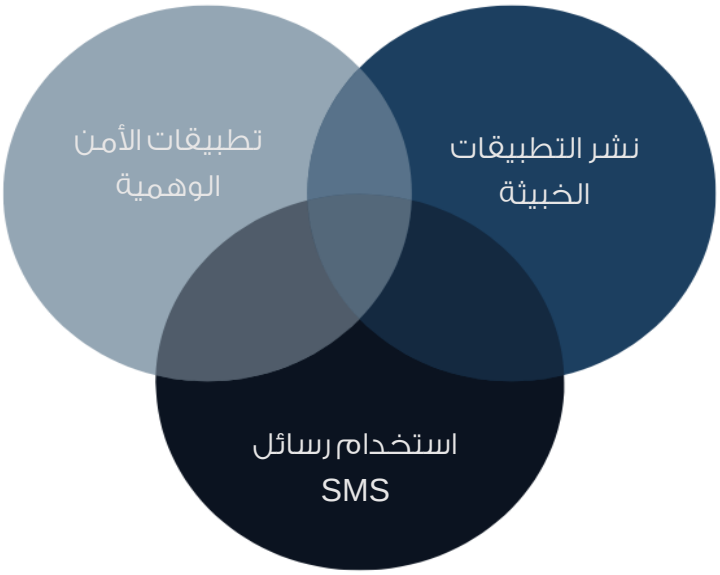
استخدام وسائل خداعية تعتمد على التقنية بشكل مباشر تمكنه من سحب المعلومات من الهدف (الضحية) مثل إنشاء مواقع توظيفية مزيفة أو مواقع تحميل برامج بشرط أن يُدخل المستخدم بياناته.

- **الطرق المستخدمة**

❖ الهجمات المعتمدة على الهاتف المحمول

يستخدم المهاجم الهاتف المحمول لشن هجمات بأسلوب الهندسة الاجتماعية حيث يقوم بالاتصال بالهدف (الضحية) مُدعيا 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 المستخدمة**



❖ الأدوات

1. الإنترنت ومواقع التواصل الاجتماعي ومن خلال تزوير البريد الإلكتروني وتزييف صفحات الويب

2. الظهور بمظهر صاحب سلطة

3. جذب الهدف لامتلاك شيء ذات قيمة

4. الهواتف

5. استغلال أخلاق حسنة مثل رد الجميل

6. النفايات بالبحث فيها والحصول على أوراق بها معلومات مهمه

7. الرسائل الاصطيادية

8. الإعلانات الوهمية

9. مكان العمل

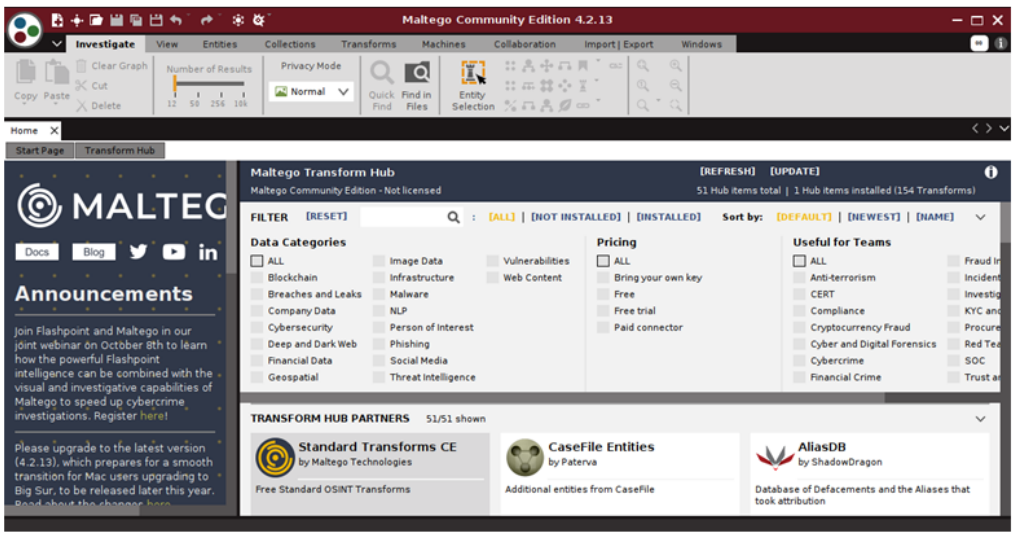
- **استخدام الأداة (عملي)**

  - **Maltego**

كالي لينكس يحتوي على هذه الأداة الخاصة بالاستطلاع والبحث عن المعلومات وهي تعمل بشكل أوتوماتيكي ،وهي أداة مفتوحة المصدر وتُستخدم بجمع المعلومات وتعداد واكتشاف الأجهزة المتصلة واكتشاف عناوين البريد الإلكتروني ومجموعات التواصل الاجتماعي وأرقام الهواتف في حال وجودها ، وهي تتعامل مع الهندسة الاجتماعية وتُمكن المهاجم من صناعة مخططات متعددة لاختراق عقلية الضحية وتُمكنه من استنتاج واستخراج المعلومات المهمة، ولاستخدام هذه الأداة يتم كتابة هذه الأداة في Terminal لكالي لينكس أو اختيارها من قائمة أدوات كالي لينكس.

وعندما يتم فتح الأداة لأول مرة يجب التسجيل فيها وإجراء عملية التحقق عبر الإيميل بعدها يتم فتح الواجهة الرسومية وهي تصور البيانات المجمعة على شكل رسم بياني مناسبة لتحليل الروابط .

يمكن إضافة أي نوع من المعلومات في Maltego، سواء كانت معلومات خاصة بأجهزة الضحية كعناوين الـ IP ومعلومات الاتصال، أو روابط حساباته، أو معلوماته الشخصية، ويمكن ربطها مع بعضها البعض والتخطيط والاستنتاج بناءً على كل تلك المعلومات.

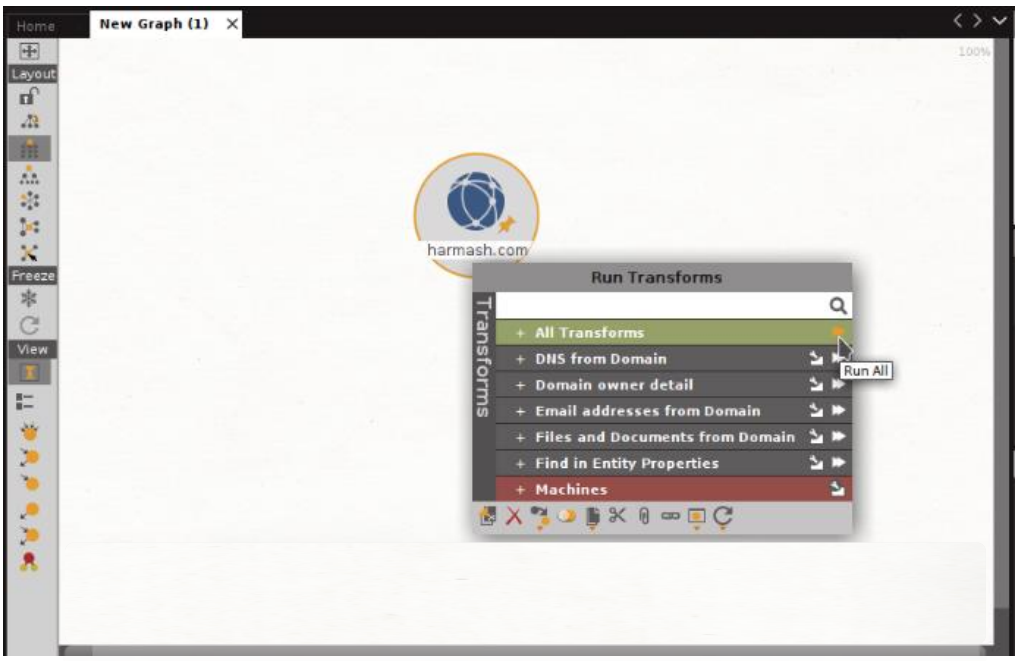


شكل (٧٣) MAltego 1

لبدء العمل بها يتم الضغط على إشارة + في الأعلى أي فتح Graph جديد ، يظهر في الجانب الأيسر بعض الكيانات التي يمكنك البدء بها، بسحب كيان إلى صفحة الـ Graph ثم البدء بالتعمق به، يمكنكم البدء باسم المجال، الشركة أو الشخص، يوجد الكثير من الكيانات للبدء بها مثل عنوان البريد الإلكتروني وغيره.

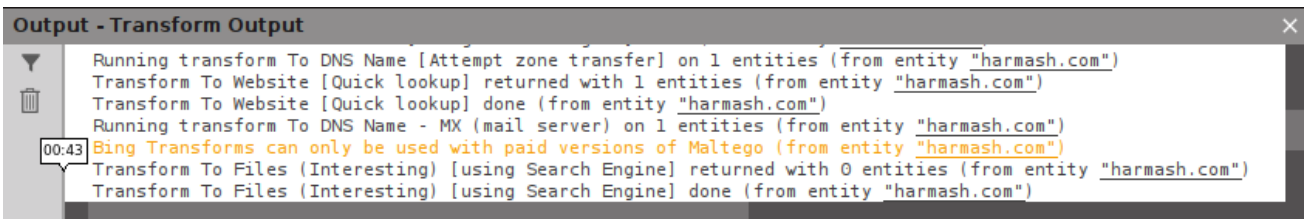
قم بالنقر عليه بواسطة الزر الأيمن كي تظهر لك قائمة من التحويلات مرتبطة بـ DNS, تفاصيل مالك الدومين، الإيميلات الموجودة في هذا الدومين وغيرها من المعلومات.

يمكنك الحصول على الكثير من المعلومات ذات الصلة من خلال البدء بالدومين, لجعل العملية سهله قم بالنقر على All Transforms كما في الصورة التالية:

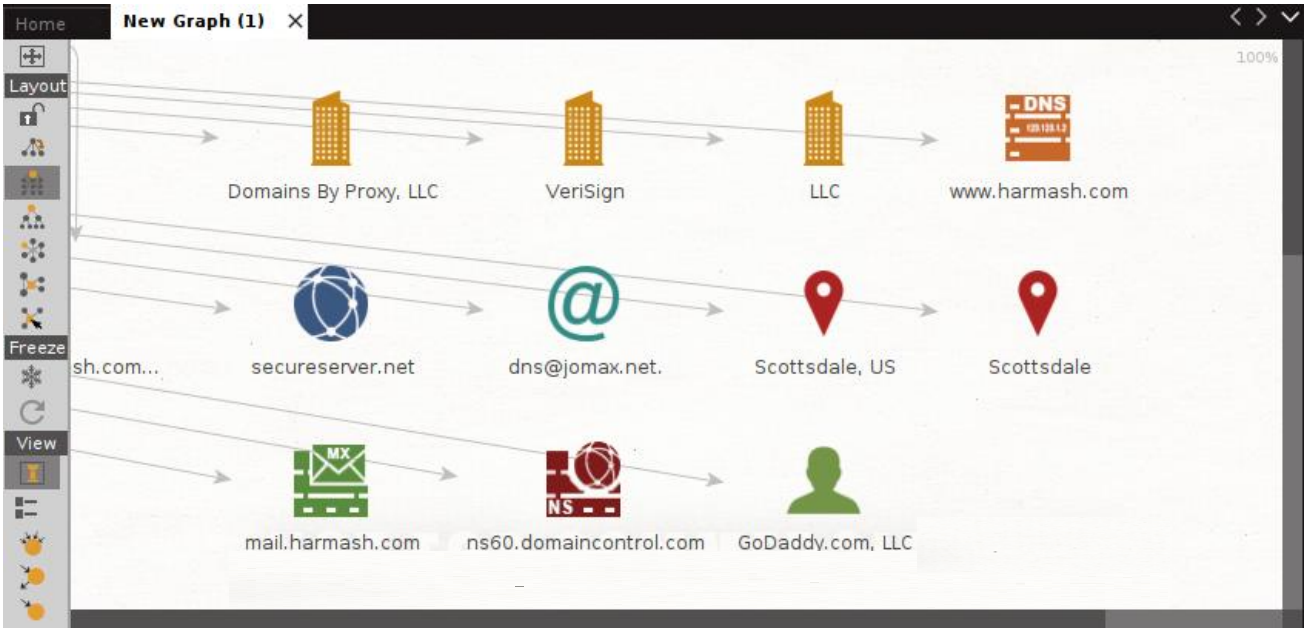


شكل (٧٤) MAltego Graph

وسوف نرى أيقونة سير العملية في الأسفل هكذا :



وحالما ينتهي سيحّمل لنا واجهة بيانات معقدة كالتالي ولكنها مفيدة للغاية:



سوف يعطينا بعض البيانات المرتبطة بهذا الدومين من سجلات DNS المرتبطة به, بعض المواقع الإلكترونية المرتبطة به, سجلات MX, موقع الدومين وعناوين الإيميل المرتبطة بالدومين إلخ..

يمكنك الضغط مرتين على أي معلومة حصلت عليها لرؤية التفاصيل.

- **التصيد Phishing**

هذا الهجوم يتم من خلال إنشاء صفحة تسجيل الخول الخاصة بموقع مثل الفيس بوك ولكن في الصفحة المزورة يتم تغيير بعض البارامترات ليتم إرسال بيانات تسجيل الدخول الخاصة بالهدف إلى مُختبر الاختراق ومن ثم إعادة توجيه الهدف إلى صفحة الموقع الأصلية، ويمكن القيام بهذه العملية بشكل يدوي من خلال نسخ الكود المصدري لصفحة تسجيل الدخول الخاصة بالموقع ومن ثم التعديل عليها ورفعها إلى موقع استضافة، وإرسال رابط هذه الصفحة إلى الهدف أو القيام بهذه العملية بشكل أوتوماتيكي باستخدام أداة Social Engineer Toolkit.

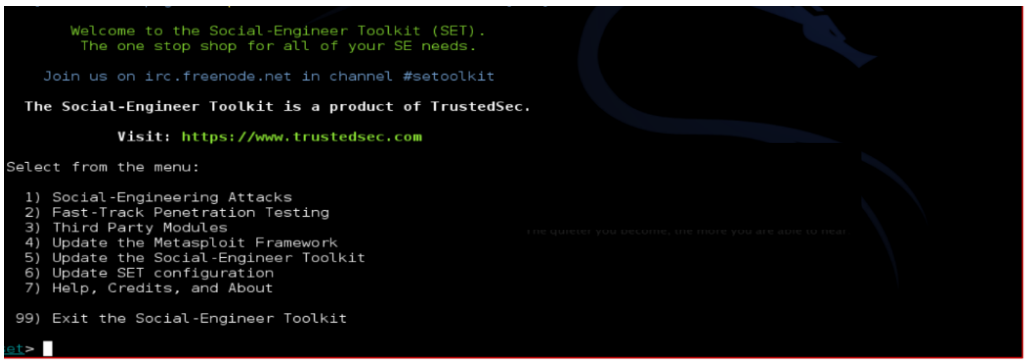
- **Social engineer Toolkit**

هذه الأداة تم إنشاؤها من قبل مؤسس TrustedSec وهي أداة مفتوحة المصدر مكتوبة بلغة بايثون ومُعدة للقيام بعمليات اختبار الاختراق عن طريق الهندسة الاجتماعية، SET هي الاختصار لها.

- تُستخدم من قبل مختبري الحماية من أجل القيام بعملية فحص لحماية المنظمة الهدف.
- هذه الأداة موجودة بشكل تلقائي في نظام كالي لينكس ويمكن استخدامها بكتابة الأمر:

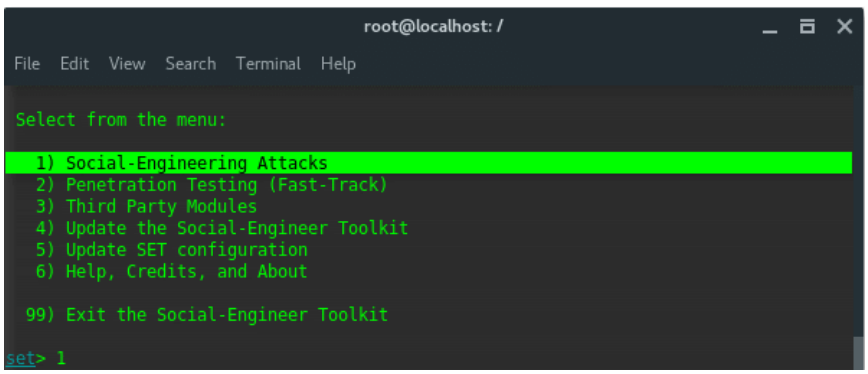
```
# setoolkit
```

تظهر الشاشة التالية:



شكل (٧٥) SET ١

يتم اختيار Social -Engineering Attacks تظهر الشاشة التالية لاختيار نوع الهجوم



❖ الأمن المادي والأدوات المادية

يؤدي الأمن المادي دورا أساسيا في الأمن السيبراني فهي تحمي أجهزة الحاسب والبرامج والشبكات والبيانات والمُعدات من المخاطر المادية المباشرة كالوصول إليها من قبل الأشخاص غير المصرح لهم وفي المناطق غير المسموح بها، بالإضافة لحمايتها من الكوارث والأخطار الطبيعية كالفيضانات والحرائق والزلازل والبراكين **باستخدام الأدوات المادية التالية:**

١. أنظمة التحكم بالدخول

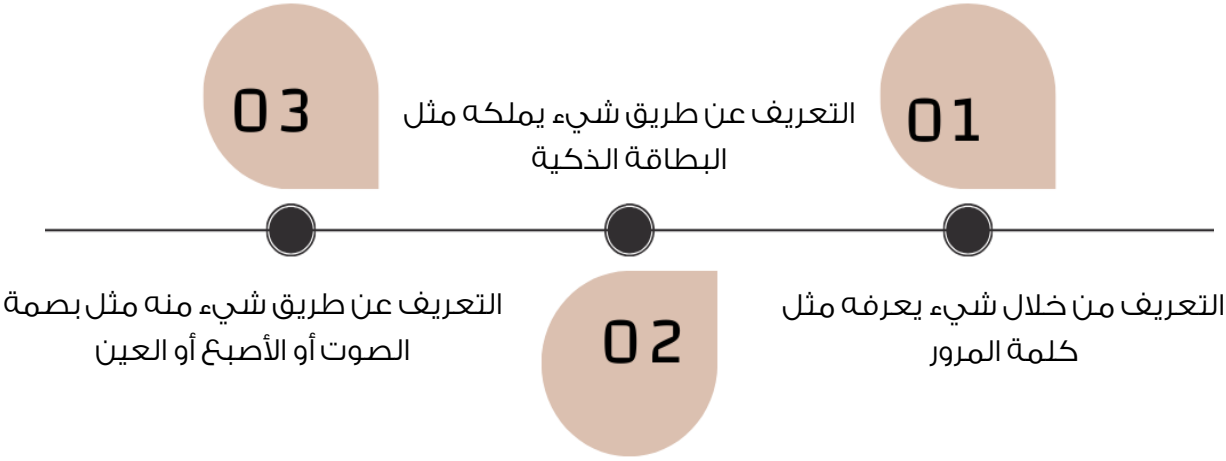
هي مجموعة من التقنيات والأجهزة التي تتحكم بالدخول للمبنى الذي يوجد به البيانات المهمة للمنظمة والحواسيب التي تحتوي عليها (مراكز البيانات) والوثائق والملفات المهمة حتى لا يتم سرقتها أو تخريبها

ومن هذه التقنيات:

١. الحواجز الفيزيائية مثل الأسوار الخارجية التي تُحيط بالمبنى الخارجي ومثبت عليه أجهزة إنذار والأبواب التي يتم إغلاقها بأقفال أو آلية وتكون مؤمنة ومراقبة.

٢. المقاييس الحيوية هي طريقة آلية لوضع هوية تعتمد على الخصائص المادية التي يصعب تزييفها مثل بصمات الأصابع أو أنماط شبكية العين أو الصوت وهي فريدة لكل شخص وتستخدم في تعريف الشخص.

- **طرق عملية التعريف**



٢. أنظمة المراقبة المرئية

تعتمد على تقنية كاميرات المراقبة الخاصة بالتسجيل والتحكم عن بعد بوضعها في أماكن خاصة ومحددة ليتم مراقبة المكان مثل على أسوار المبنى أو داخل غرف مركز البيانات وفوق الأبواب ليتم الاستفادة منها عند حدوث أي اختراق أمني.

٣. أنظمة الإنذار

تعتمد هذه الأنظمة على توزيع حساسات تقوم بمراقبة خصائص معينة وإعطاء الإنذارات عند مستويات محددة لإعطاء الإنذارات عند حدوث خطر معين في المبنى، مثل صفارات حدوث الحريق أو محاولة اختراق الأبواب.

❖ التدابير المضادة والحماية من عمليات الهندسة الاجتماعية

تعتبر الهندسة الاجتماعية من الثغرات الأمنية التي يجب منعها لأنها تعتمد على طبيعة البشر ولذلك يجب توعيتهم وتدريبهم باستمرار من خطرها باتخاذ تدابير مضادة للحماية **منها مثل:**

١. الحرص على الخصوصية وعدم نشر المعلومات الشخصية.

٢. تجنب الرسائل التي تطلب معلومات شخصية.

٣. عدم فتح الرسائل مجهولة المصدر.

٤. استخدام مرشحًا جيدًا للرسائل العشوائية.

٥. التخلص من الأوراق المهمة بتمزيقها بواسطة الآلة المخصصة بذلك قبل وضعها في النفايات.

٦. عدم مشاركة كلمة السر مع الآخرين أو تركها على المكتب.

٧. يجب التحقق من هوية أي شخص يطلب معلومات عن الجهاز أو الحساب أو أي معلومات شخصية عن موظف ما.

٨. عدم استخدام نفس كلمة المرور لحسابات مختلفة، إذا حصل هجوم هندسة اجتماعية على كلمة مرور حساب على وسائل التواصل الاجتماعي، حتى يتمكن المهاجمون من فتح جميع الحسابات الأخرى أيضًا.

٩. توفير الضمانات التقنية وغير التقنية من قبل المنظمة التي يُمكن تنفيذها لخفض المخاطر المُرتبطة بالهندسة الاجتماعية إلى مستُوى مقبول، باللجوء إلى إضافة طبقات مُتعددة لمُخططاتها الأمنية حتى إذا فشلت الآلية في الطبقة الخارجية، هناك آلية واحدة في الطبقة الداخلية يمكن أن يُساعد في منع تهديد قد يتحول إلى كارثة (التخفيف من حدة المخاطر)، وهذا المفهوم المعروف بالدفاع متُعدد الطبقات أو الدفاع في العمق.

١٠. تدريب الموظفين والأفراد بإقامة دورات تدريبية تشرح لهم مفهوم الهندسة الاجتماعية وأساليبها والآثار المترتبة عنها وكيفية التصدي لها.

١١. ينبغي أن يشتمل هذا التدريب على عروض توضيحية للطرق التي قد يحاول المهاجمون من خلالها تطبيق الهندسة الاجتماعية على الموظفين، على سبيل المثال، محاكاة سيناريو ينتحل فيه مهاجم شخصية موظف بنكي يطلب من الشخص المستهدف أن يؤكد معلومات حسابه، وقد يتمثل سيناريو آخر في مدير كبير (تم نسخ أو انتحال عنوان بريده الإلكتروني) يطلب من الشخص المستهدف إرسال مدفوعات مالية إلى حساب معيّن.

١٢. يساعد التدريب على تعليم الموظفين الدفاع ضد هذه الهجمات وفهم سبب أهمية دورهم المؤسسي في إطار الثقافة الأمنية.

١٣. عمليات مُراجعة الحسابات: المُنظمات التي لها نشاط عليها التحقق من التقيد بسياسة الأمن، والتي تشمل العناصر الهامة المُتعلقة بأمن الأشخاص والمُنظمة.

١٤. اتباع السياسة الأمنية: وهي سياسة مكتوبة بشكل جيد، وينبغي أن تشمل النهج التقني وغير التقني ، وينبغي إدماج كل منظمة الأمن في أهدافها التشغيلية و التأكد من اتباعها.

١٥. التأكد من إعدادات المتصفح وإغلاق النوافذ المنبثقة.

١٦. تجنب المشاركة في الاستبيانات التي تكون من مصادر غير موثوقة.

١٧. عدم فتح الروابط.

١٨. عدم الإفصاح عن أي معلومات شخصية أو مالية عن طريق الهاتف أو البريد الالكتروني.

١٩. تحميل برنامج مكافحة الفيروسات وتحديث باستمرار.

٢٠. استخدام المصادقة المتعددة العوامل.

٢١. التحذير وبشكل مُستمر وبكافة الوسائل من خطر الإشاعة وتداولها، كونها تُشكل صيداً سهلا لبعض الذين يبحثون عن استثمارها في تحقيق مصالحه.

- **اختبار اختراق الهندسة الاجتماعية**

هو لاختبار قوة العوامل البشرية في أمن المؤسسة.

- **الخطوات المتبعة في إجراء الاختبار**

١. الحصول على إذن.

٢. تحديد نطاق الاختبار.

٣. الحصول على قائمة رسائل البريد الإلكتروني والاتصالات من الأهداف المحددة سابقا.

٤. جمع رسائل البريد الإلكتروني وتفاصيل اتصال العاملين في المنظمة المستهدفة.

٥. جمع المعلومات باستخدام تقنيات Footprinting.

٦. إنشاء مخطط قائم على المعلومات.

٧. توجيه رسائل البريد الإلكتروني إلى موظف لطلب معلومات شخصية.

٨. إرسال ومراقبة رسائل البريد الإلكتروني مع المرفقات الخبيثة لاستهداف الضحية.

٩. إجراء اتصال هاتفي بالهدف وانتحال شخصية ما ثم السؤال عن معلومات مهمة.

١٠. الاتصال بالهدف وانتحال شخصية مشرف الدعم الفني.

١١. محاولة دخول المنظمة كمدقق خارجي.

١٢. محاولة التصنت و shoulder surfing على الأنظمة و المستخدمين.

١٣. توثيق جميع النتائج في التقرير.

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	الهندسة الاجتماعية نوع من التقنيات التي يستخدمها المجرمون الإلكترونيون بهدف استدراج المستخدمين غير المرتابين إرسال بياناتهم السرية، وإصابة حواسيبهم ببرامج ضارة، أو فتح روابط إلى مواقع مصابة، بالإضافة إلى ذلك، قد يحاول المتطفلون استغلال نقص معرفة المستخدم؛ فبفضل سرعة تقدم التكنولوجيا، قد يدرك الكثير من المستهلكين والموظفين القيمة الحقيقية للبيانات الشخصية، وقد يجهلون الطريقة المثلى لحماية هذه المعلومات.	√
٢.	(الهجمات البشرية) هو استخدام الأساليب والمهارات البشرية مثل الأساليب الكلامية أو النفسية الإيحائية أو الإعلانية 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 ألنهم يستخدمون مهارات التعامل مع البشر استغلالهم.	√
٣.	(الهجمات التشجيرية) 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 يُدخل المستخدم بياناته.	×
٤.	السرقة الاستيلاء على الأشياء الثمينة مثل المعلومات أو الوصول أو المال.	√
٥.	(جمع المعلومات) يحدد المهاجمون كيفية تنفيذ الهجوم، وما هي الأدوات والوسائل التي يمكن استخدامها في الهجوم.	×
٦.	يستخدم المهاجم الهاتف المحمول لشن هجمات بأسلوب الهندسة الاجتماعية حيث يقوم بالاتصال بالهدف(الضحية) مُدعيا أن شخص له صالحيات 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 يحدد المهاجمون كيفية تنفيذ الهجوم، وما هي الأدوات والوسائل التي يمكن استخدامها في الهجوم.	√

٢. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

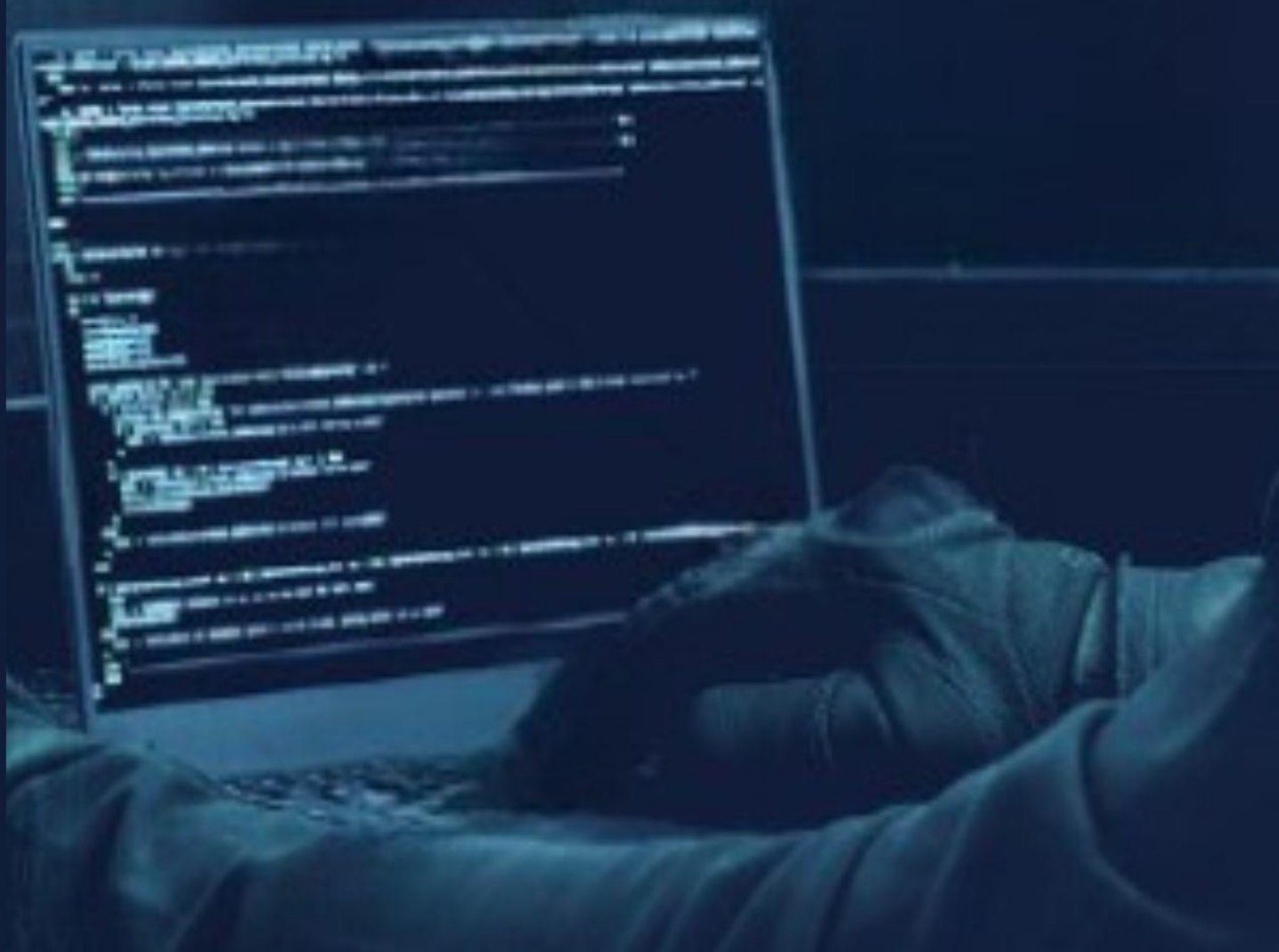
٧.	التصيد هذا الهجوم يتم من خلال إنشاء صفحة تسجيل الدخول الخاصة بموقع مثل الفيس بوك، ولكن في الصفحة المزورة يتم تغيير بعض البارامترات ليتم إرسال بيانات تسجيل الدخول الخاصة بالهدف إلى مُختبر الاختراق ومن ثم إعادة توجيه الهدف إلى صفحة الموقع الأصلية ويمكن القيام بهذه العملية بشكل يدوي من خلال نسخ الكود المصدري لصفحة تسجيل الدخول الخاصة بالموقع ومن ثم التعديل عليها ورفعها إلى موقع استضافة وإرسال رابط هذه الصفحة إلى الهدف أو القيام بهذه العملية بشكل أوتوماتيكي باستخدام أداة.	√
٨.	أنظمة الإنذار تعتمد على تقنية كاميرات المراقبة الخاصة بالتسجيل والتحكم عن بعد بوضعها في أماكن خاصة ومحددة ليتم مراقبة المكان مثل على أسوار المبنى أو داخل غرف مركز البيانات وفوق الأبواب ليتم الاستفادة منها عند حدوث أي اختراق أمني.	×
٩.	التدابير المضادة والحماية من عمليات الهندسة الاجتماعية (عدم فتح الروابط).	√
١٠.	اختبار اختراق الهندسة الاجتماعية هو الاختبار قوة العوامل البشرية في أمن المؤسسة.	√

التقييم الأمني

الفصل الحادي عشر

في هذا الفصل سنتعرف على المواضيع التالية:

- المنهجية والخطوات
- التقييم الأمني
- مخرجات تقيم الأمان
- القواعد الإرشادية
- المزيد من المصطلحات



❖ المنهجية والخطوات

اختبار الاختراق هو محاولة اكتشاف ضعف النظام بهدف تحديدها والإبلاغ عنها للمسؤولين في المنظمة، ولإجراء اختبار اختراق أخلاقي ناجح يجب على المخترق الأخلاقي إتباع منهجية صارمة.

استخدام العملية المنهجية يساعد في فهم وتحليل سلامة الدفاعات الحالية في كل مرحلة من مراحل الاختبار.

- **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 وسد 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 و يجب أن يتم اختبار كل آلية وبرنامج يستعملهم في عمله واتباع منهجية اختبار الاختراق وهي جمع المعلومات وتحليل الثغرات وإجراء الاختبار من الخارج ومحاولة اختبار اختراق الشبكة الداخلية واختراق الموجهات وأجهزة الشبكة و اختبار جدران الحماية و اختبار أجهزة منع التسلل (IDS) و إجراء اختبار الشبكات اللاسلكية واختبار هجوم منع الخدمة وكسر كلمات المرور واختبار الهندسة الاجتماعية واختراق الأجهزة النقالة واختبار مواقع الويب وتطبيقاته واختبار اختراق الأنظمة و اختبار وجود أحصنة طروادة و الفيروسات و البرامج الضارة الأمن واختبار البريد الإلكتروني والتحقق من الأمن المادي واختبار تأمين المباني والأجهزة وتوفير منهج شامل لخطوات إعداد التي يمكن اتخاذها لمنع الاستغلال أي يحاول المخترق الأخلاقي يحاول أن يحدد ما يمكن أن يعرفه المهاجم أو المتسلل عن النظام المستهدف من خلال مرحلة جمع المعلومات ، وخلال مرحلة الاستطلاع والمسح يحاول معرفة ما الذي يمكن أن يفعل المهاجم بهذه المعلومات وكيف يمكن استغلالها ، وفي مرحلة الوصول و المحافظة هل يستطيع أن يثبت وجود مهاجم و اختراق للنظام وفي المرحلة الأخيرة يقيم الأمن حسب المعايير و النتائج و التدابير .

- **الخطوات**

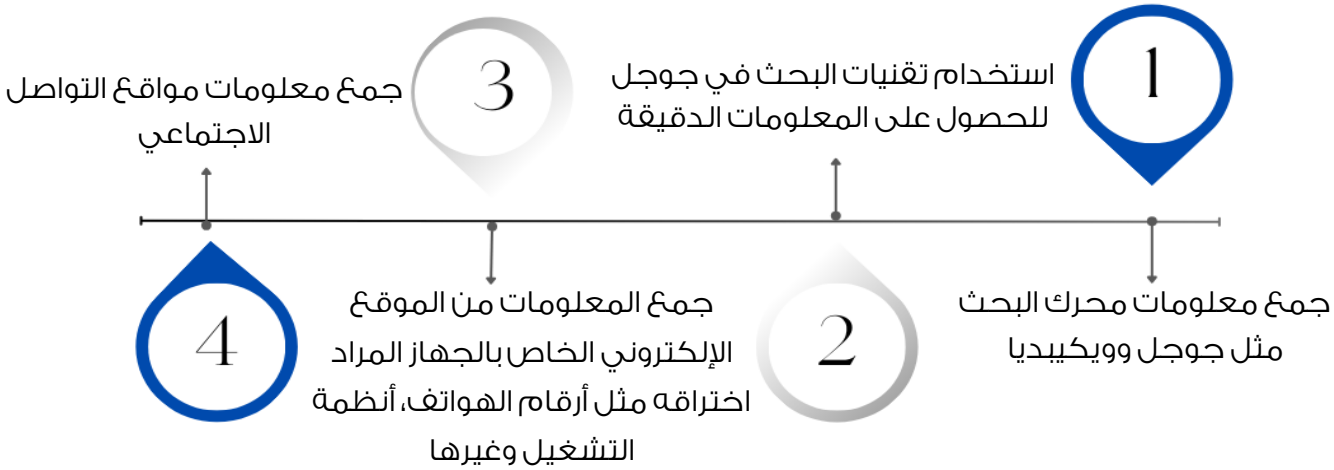
١- الاستطلاع

هو جمع أكبر قدر ممكن من المعلومات حول النظام أو الشبكة المستهدفة بهدف تحديد نقاط الدخول المحتملة الى النظام.

- **منهجية جمع المعلومات**

خلال مراحل Footprinting ، على المخترق القيام بعدة خطوات ، **لذلك يجب أن يكون لديه عدة خطوات**

منهجية يتبعها :



٢- المسح

استخدام أدوات لفحص النظام أو الشبكة المستهدفة بحثا عن نقاط الضعف مثل المنافذ المفتوحة والخدمات قيد التشغيل ومعلومات تشغيل النظام.

٣- التعداد

تحديد وجمع المعلومات حول المستخدمين والمجموعات والموارد على النظام المستهدف والهدف منها هو تحديد نقاط الدخول المحتملة إلى النظام التي يمكن استغلالها.

٤- تقييم الضعف

تتضمن تحليل المعلومات التي تم جمعها لتحديد نقاط الضعف المحتملة في النظام وتحديد أولويات الثغرات بناء على شدتها واحتمال تعرضها للاستغلال.

٥- الاستغلال

بعد تحديد الثغرات الأمنية يتم محاولة استغلالها للوصول إلى النظام أو الشبكة المستهدفة.

٦- الإبلاغ

تتضمن هذه المرحلة توثيق نقاط الضعف التي تم تحديدها خلال المراحل السابقة والإبلاغ عنها للمسؤولين وإعداد التقارير بالمعلومات اللزمة بالتدابير المضادة لإصلاح الثغرات وتعزيز امن 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.

ويعد الاستطلاع أحد أنشطة التقييم الأمني الفعالة التي ترسم خرائط للبنية التحتية لخدمة المؤسسة من خلال تحديد الاتصالات التي تشكل الشبكة، وتحتاج المؤسسة دائمًا إلى إجراء فحوصات على البنية التحتية للشبكة باستخدام مجموعة من الأدوات باستخدام هذه الأدوات يمكن تحليل البيانات التي تمر على الشبكة، ومتابعة حزم البيانات، والفحص المفصل على الشبكة، واكتشاف الخدمات التي تعمل في البنية التحتية، وما إذا كانت الخدمة بها ضعف خاص.

يعتمد اختبار الاختراق على أفضل ممارسات الأمن السيبراني بحيث يتضمن تنفيذ متطلبات الأمان المناسبة وتنفيذ وتحليل المخاطر ونمذجة التهديد ومراجعات الكود وقياس الأمان التشغيلي.

يعتبر اختبار الاختراق أخطر وأشد أشكال التقييم الأمني ويتم معالجتها بواسطة محترفين مؤهلين ويتم إجراؤه باستخدام Pentest لتقييم جميع مكونات البنية التحتية للشبكة والتطبيقات وأنظمة التشغيل ووسائط الاتصال والأمن المادي وتقييم أجهزة أمن الشبكات مثل جدران الحماية وأجهزة التوجيه والتحويل وخوادم الويب.

❖ 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:

١. 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.

٢. قائمة بالتغييرات التي نفَّذَها فريق العمل في النظام في أثناء الاختبار.

٣. بروتوكول الاختبار بما في ذلك الوسائل والأدوات المُستخدمة، والأجزاء المفحوصة، والمشكلات المُكتشفة في النظام.

٤. توصيات قابلة للتنفيذ لمعالجة المشكلات الأمنية المُكتشفة في النظام.

❖ القواعد الإرشادية

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:**

01 البقاء قانونياً وذلك عبر الحصول على الموافقة المناسبة قبل الوصول وإجراء التقييم الأمني

02 تحديد النطاق، تحديد نطاق التقييم بحيث يظل عملهم المخترق الأخلاقي قانونياً وضمن الحدود المعتمدة للمؤسسة.

03 الإبلاغ عن نقاط الضعف عن طريق إخطار المؤسسة بكافة نقاط الضعف التي تم اكتشافها أثناء التقييم وتقديم المشورة العلاجية لحل هذه الثغرات الأمنية.

04 احترام حساسية البيانات فاعتمادا على حساسية البيانات، قد يتعين على المتسللين الأخلاقيين الموافقة على اتفاقية عدم إفشاء، بالإضافة الى الشروط والأحكام الأخرى التي تتطلبها المؤسسة التى تم تقييمها.

05 يقوم بالاختبار أكثر من مرة ليتم التأكد من قوة نظام الحماية.

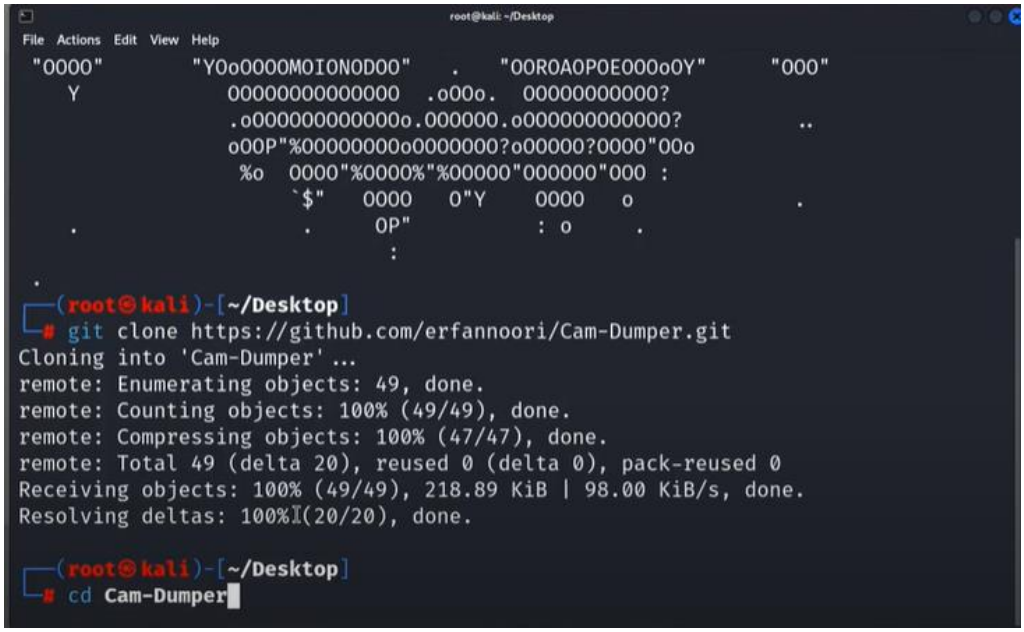
❖ المزيد من المصطلحات

٠١.	تقرير	Report
٠٢.	المنهجية	Methodology
٠٣.	رواية	Narrative
٠٤.	اكتشاف	Discovery
٠٥.	نطاق الهدف	Target scop
٠٦.	نتائج	Results
٠٧.	العلاج	Remediation
٠٨.	حالة	State
٠٩.	ملخص تنفيذي	Executive summary
٠١٠.	تقييم التقرير	Report Evaluation
٠١١.	قائمة تدقيق	Checklist
٠١٢.	الخطوط العريضة للتقرير	Report outline
٠١٣.	التقرير والتوثيق	Report and Documentation

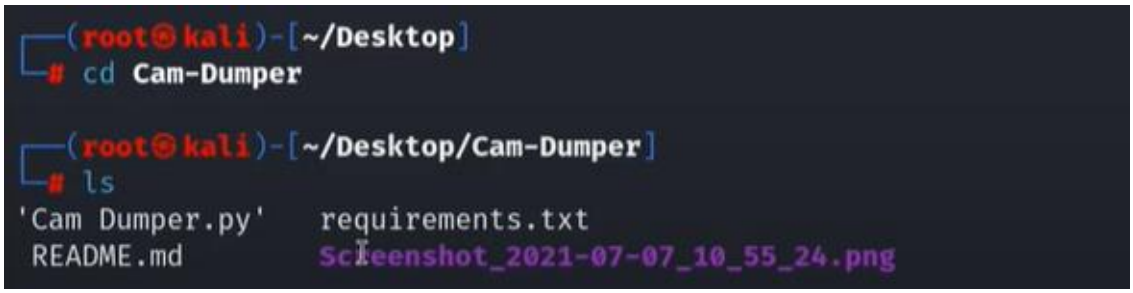
- إثراء علمي " تطبيق اختراق الكاميرات"

اتبع الخطوات التالية:

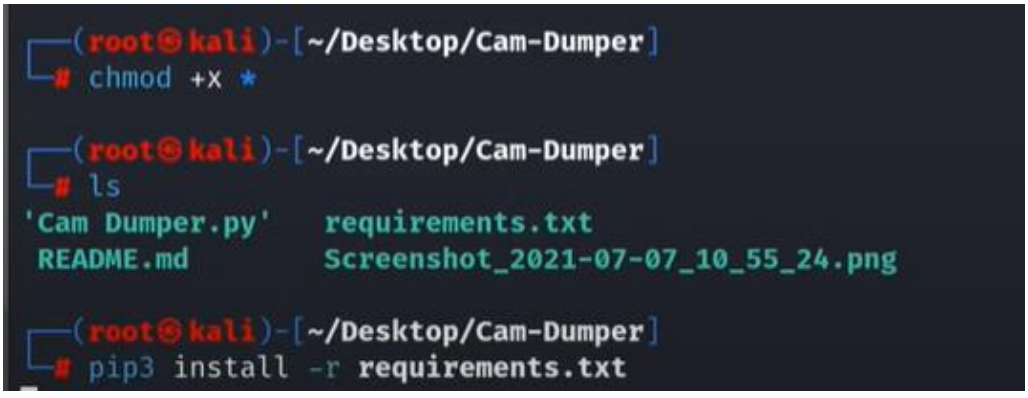
١.



٢.



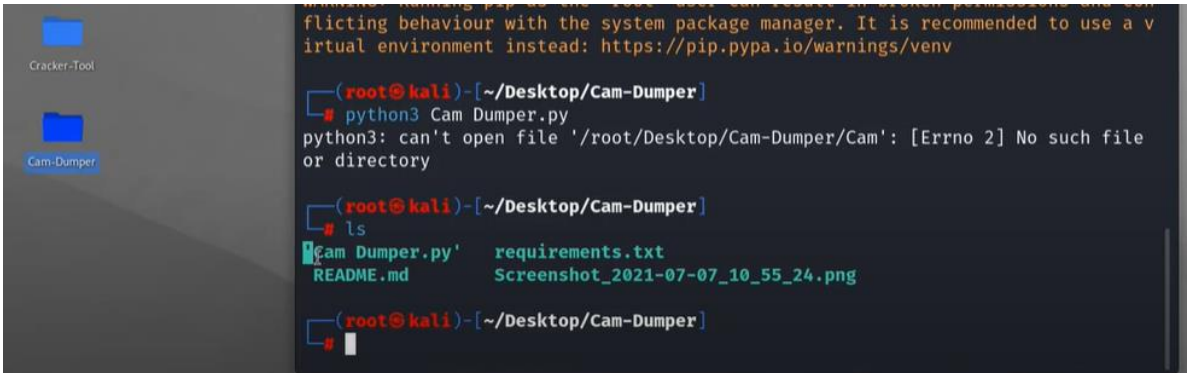
٣.

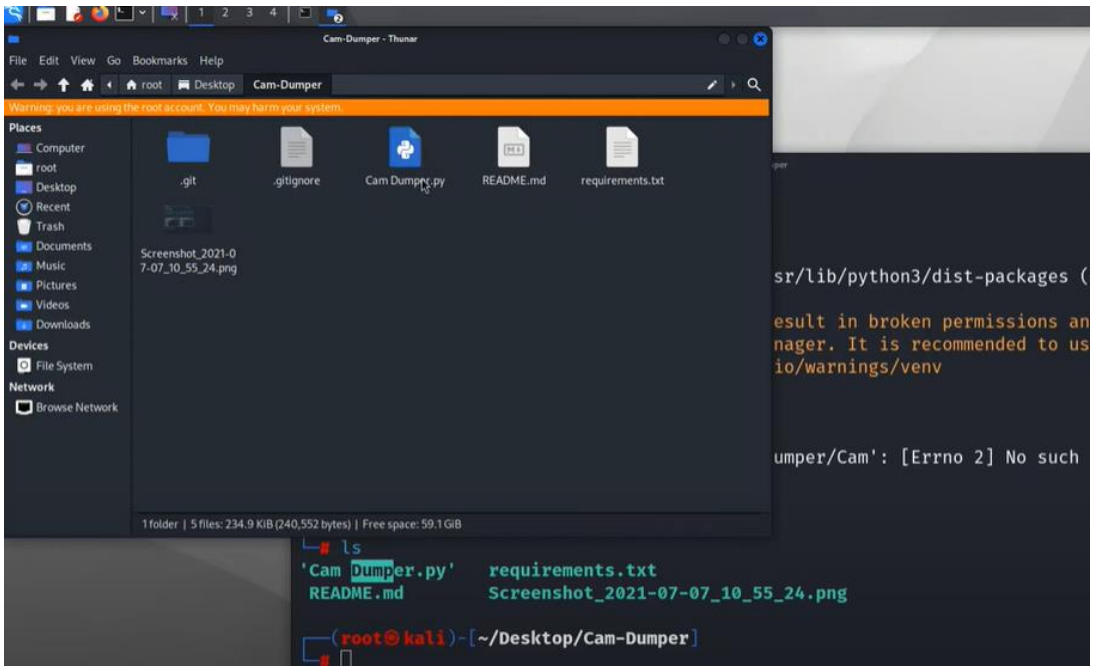


٤.

```
┌──(root㉿kali)-[~/Desktop/Cam-Dumper]
└─# pip3 install -r requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from
-r requirements.txt (line 1)) (2.31.0)
WARNING: Running pip as the 'root' user can result in broken permissions and con
flicting behaviour with the system package manager. It is recommended to use a v
irtual environment instead: https://pip.pypa.io/warnings/venv

┌──(root㉿kali)-[~/Desktop/Cam-Dumper]
└─# pip install colorama
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (0.4.6
)
```

٥.

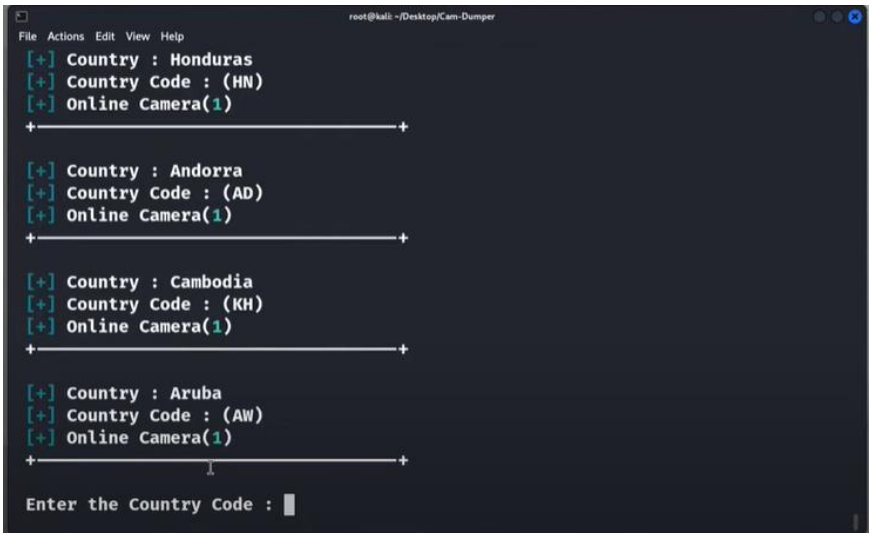




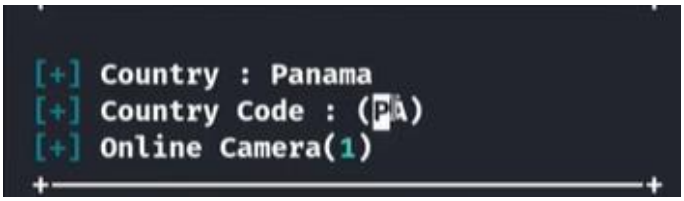
٦.

```
┌──(root㉿kali)-[~/Desktop/Cam-Dumper]
└─# ls
CamDumper.py  README.md  requirements.txt  Screenshot_2021-07-07_10_55_24.png

┌──(root㉿kali)-[~/Desktop/Cam-Dumper]
└─# python3 CamDumper.py
```

٧.

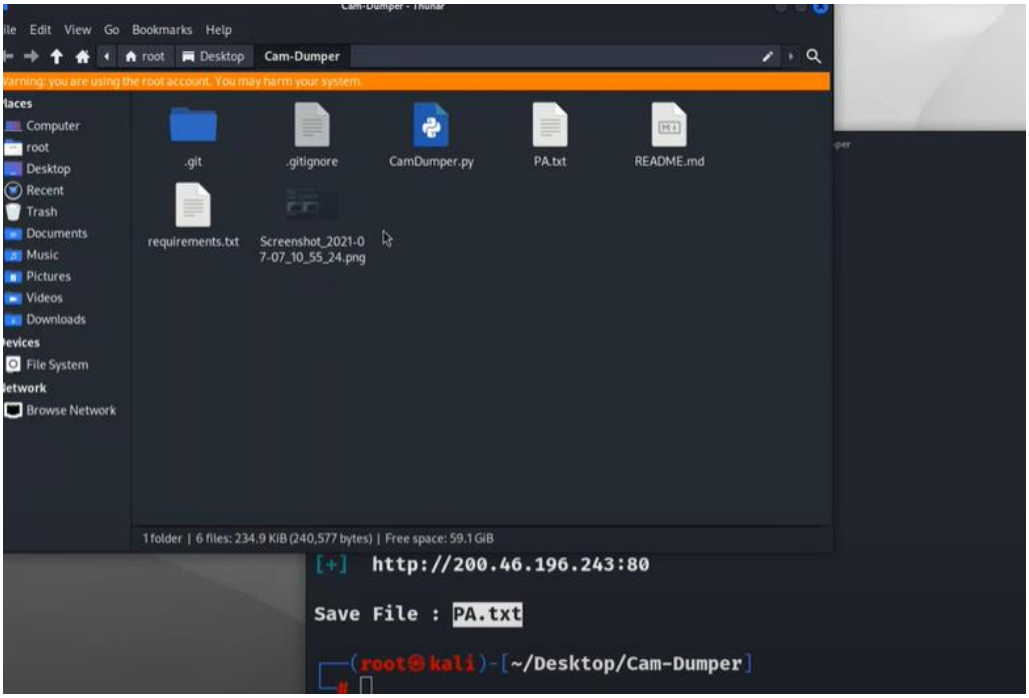


٨.

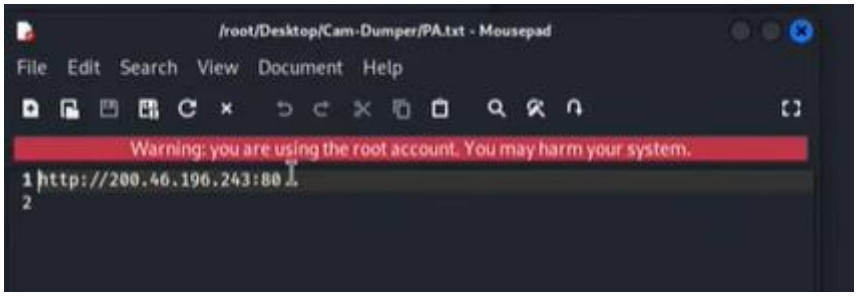


٩.

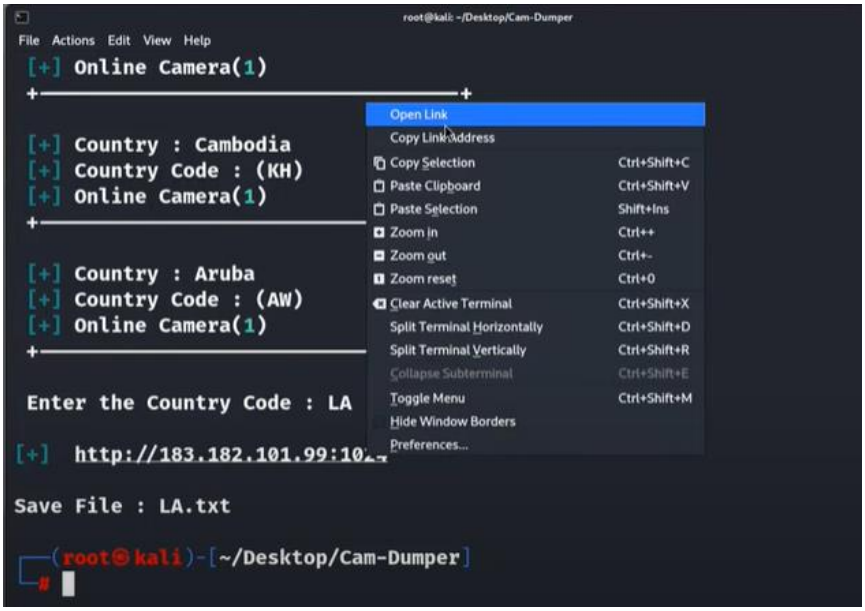
.١٠


File Edit View Go Bookmarks Help
root
Desktop
Cam-Dumper
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
.git
.gitignore
CamDumper.py
PA.txt
README.md
requirements.txt
Screenshot_2021-07-07_10_55_24.png
1 folder | 6 files: 234.9 KiB (240,577 bytes) | Free space: 59.1 GiB
[+] http://200.46.196.243:80
Save File : PA.txt
(root㉿kali)-[~/Desktop/Cam-Dumper]

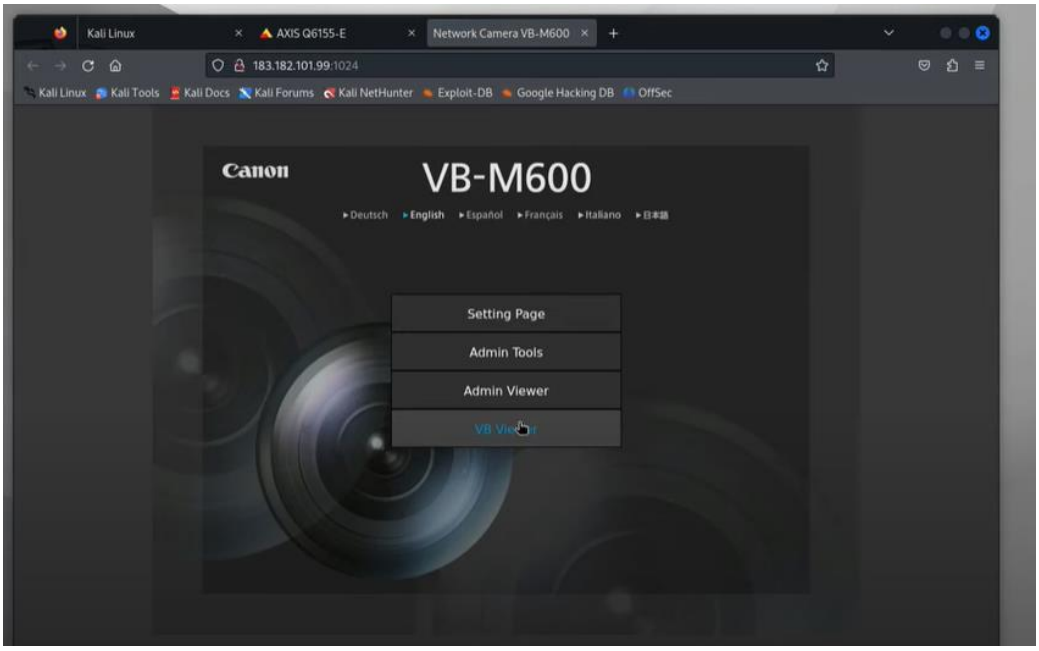
.١١


/root/Desktop/Cam-Dumper/PA.txt - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
1 http://200.46.196.243:80
2

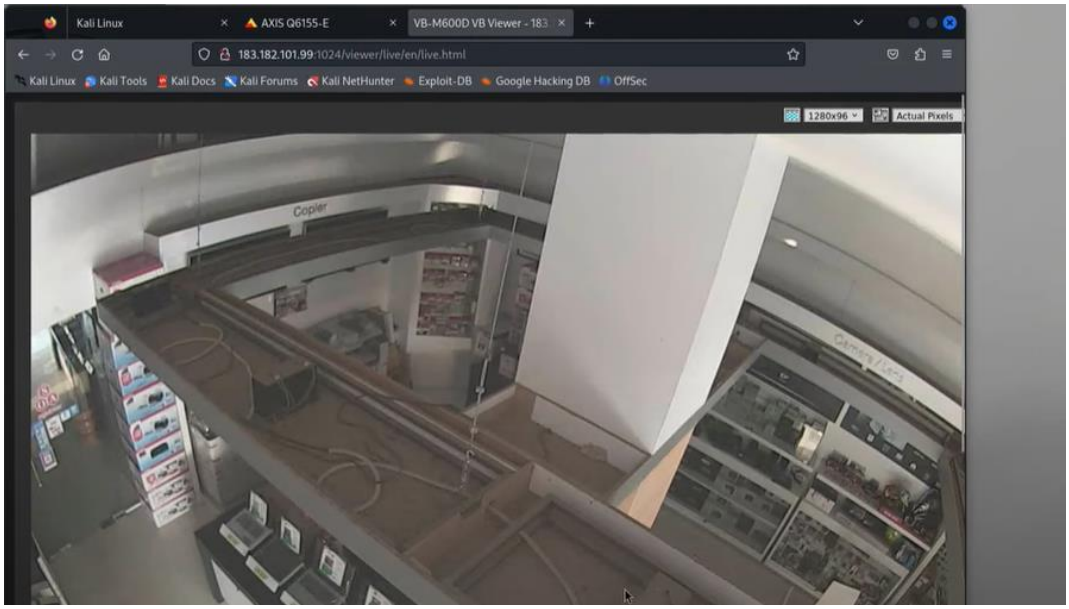
.١٢


root@kali: ~/Desktop/Cam-Dumper
File Actions Edit View Help
[+] Online Camera(1)
[+] Country : Cambodia
[+] Country Code : (KH)
[+] Online Camera(1)
[+] Country : Aruba
[+] Country Code : (AW)
[+] Online Camera(1)
Enter the Country Code : LA
[+] http://183.182.101.99:10
Save File : LA.txt
(root㉿kali)-[~/Desktop/Cam-Dumper]
Open Link
Copy Link Address
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...

١٣.


Kali Linux
AXIS Q6155-E
Network Camera VB-M600
183.182.101.99:1024
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Canon
VB-M600
Deutsch English Español Français Italiano
Setting Page
Admin Tools
Admin Viewer

١٤.


Kali Linux
AXIS Q6155-E
VB-M600D VB Viewer - 183
183.182.101.99:1024/viewer/live/en/live.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1280x96
Actual Pixels
Copier

تمارين الفصل الحادي عشر

١. **ضع علامة (√) أمام العبارات الصحيحة وعلامة (×) أمام العبارات الخاطئة:**

١.	اختبار الاختراق هو محاولة اكتشاف ضعف النظام بهدف تحديدها والإبلاغ عنها للمسؤولين في المنظمة ولإجراء اختبار اختراق أخلاقي ناجح يجب على المخترق الأخلاقي اتباع منهجية صارمة	√
٢.	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 وسد الثغرات ويجب على المُخترق الأخلاقي عدم الأغفال عن أي مورد للمعلومات (منهج التشفير)	×
٣.	هو جمع أكبر قدر ممكن من المعلومات حول النظام او الشبكة المستهدفة بهدف تحديد نقاط الدخول المحتملة الى النظام (منهجية جمع المعلومات)	×
٤.	استخدام أدوات لفحص النظام او الشبكة المستهدفة بحثا عن نقاط الضعف مثل المنافذ المفتوحة والخدمات قيد التشغيل ومعلومات تشغيل النظام (المسح)	√
٥.	بعد تحديد الثغرات الأمنية يتم محاولة استغلالها للوصول الى النظام او الشبكة المستهدفة (الاستغلال)	√
٦.	يشير التقييم الأمني الى العمليات والإجراءات والأدوات المستخدمة لكشف ما إذا كانت المنظمة تعاني من بعض نقاط الضعف التي يمكن ان يستغلها المهاجمين	√
٧.	نقاط الضعف الموجودة حاليا للبيئة المستهدفة بإعداد قائمة بالثغرات الأمنية ونقاط الضعف المكتشفة في النظام وتصنيفها حسب مدى سهولة استغلالها ومدى الضرر الذي قد يلحق بالنظام والأعمال التجارية قائمة بالتغييرات التي نفذها فريق العمل في النظام في أثناء الاختبار	√
٨.	يتبع المخترقون مفاهيم إرشادات أساسية مثل: البقاء قانونيا وذلك عبر الحصول على الموافقة المناسبة قبل الوصول وإجراء التقييم الأمني	√
٩.	خلال مراحل Footprinting على المخترق القيام بعدة خطوات لذلك يجب ان يكون لدية عدة خطوات منهجية يتبعها أولها : جمع معلومات محرك البحث مثل جوجل وويكيبيديا	√
١٠.	يقوم بالاختبار أكثر من مرة ليتم التأكد من قوة نظام الحماية	√

❖ المراجع

.١	Matt Walker , 2018, CEH Certified Ehical Haker,Mc Graw Hill,
.٢	Raphael Hertzog,Jim O'Gorman and Mati Ahron,2017, Kali Linux Revealed ,Offsec Press
.٣	(Arnaud Rebilout, 2021)
4.	(https://isecur1.rssing.com/chan-30079129/all_p1.html, 2014)
.٥	(https://www.youtube.com/watch?v=rFEgAaAi84g, 2022)
.٦	(https://www.malavida.com/en/soft/superoneclick/, 2016)
.٧	(اوامر لينكس الأساسية و المهمة التي عليك معرفتها) Linux Command Line -
.٨	(Hacker, 2023; offsec, 2024)
.٩	(offsec, 2024)
.١٠	(Brewin, 2012)
.١١	(المحترف، ٢٠٢٤)
.١٢	(LavishT@TWC; LavishT@TWC)
.١٣	(InfoSec, 2023)
.١٤	(Arnaud Rebilout, 2021)
.١٥	(العصيفير, ٢٠٢٣)
.١٦	(isecuri1ty, 2018)
.١٧	(لعصيفير, n.d.)
.١٨	(offsec, n.d.)
.١٩	(kailliunx, n.d.)
.٢٠	(Khadijah, 2013)

أكاديمية التعلم
Academy Of Learning

تحت إشراف

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

9200031 37

aol.edu.sa

aolksa