الأكاديمية العربية الدولية

الأكاديمية العربية الدولية

المقررات الجامعية

www.aiacademy.info | care@aiacademy.info

كتاب
عالم القرصنه

بقلم: محمد سعد

حقوق التأليف

إخلاء المسؤولية

تستخدم المعلومات الواردة في هذا الكتاب للأغراض التعليمية فقط.
لا يتحمل منشئ هذا الكتاب بأي حال من الأحوال أي سوء استخدام للمعلومات قدمت. كل المعلومات المقدمة في هذا الكتاب تهدف إلى مساعدة القارئ تطوير موقف دفاع القراصنة وذلك لمنع الهجمات التي تمت مناقشتها. قطعا يجب أن تستخدم المعلومات المقدمة هنا للتسبب في أي نوع من الضرر مباشرة أو بشكل غير مباشر. كلمة "هاك" أو "القرصنة" تستخدم على نطاق واسع في جميع أنحاء هذا الكتاب
يجب اعتبار "الاختراق الأخلاقي" أو "القرصنة الأخلاقية" على التوالي.
تقوم بتنفيذ جميع المعلومات الواردة في هذا الكتاب على مسؤوليتك الخاصة.

جدول المحتويات

مقدمة

الفصل 1 مقدمة

ما هو الاختراق؟

تصنيف هاكر

المصطلحات الأساسية

القرصنة أسئلة وأجوبة

الفصل 2 - المفاهيم الأساسية

شبكة الكمبيوتر

شبكة المضيف

بروتوكول الشبكة

منفذ الشبكة

حزمة الشبكة

نظام اسم النطاق (DNS)

FIREWALL

مخدم بروكسي

الفصل 3 - مقدمة لينكس

لماذا لينكس؟

WINDOWS VS. LINUX

اختيار توزيع LINUX

تشغيل LINUX من قرص حقيقي

أساسيات لينكس

مراجع أخرى

الفصل 4 - البرمجة

لماذا البرمجة؟

أين يجب أن تبدأ؟

الفصل 5 - البصمة

ما هو التأليف؟

منهج جمع المعلومات

التدابير المضادة

الفصل 6 - المسح

اكتشاف الأنظمة الحية

أنواع الفحص

أدوات للمسح

نظام التشغيل بالإصبع

إيراز هويتك
التدابير المضادة
الفصل 7 - اختراق كلمات المرور
الهجوم الإجباري
الهجوم الوحشي بالقوة
قوس قزح الجدول
هجوم التصيد

التدابير المضادة
الفصل 8 - اختراق ويندوز
كسب الوصول إلى النظام
الإغراق على كلمات المرور
تحطيم كلمة المرور
التدابير المضادة
الفصل 9 - البرامج الضارة
متغيرات البرامج الضارة و التقنيات الشائعة
التدابير المضادة
الفصل 10 - إخفاء المعلومات
ويندوز يخفي السمة
NTFS البديل بيانات الجداول
إخفاء المعلومات
استخدام الأدوات لإخفاء المعلومات
الفصل 11 - استنشاق
أنواع الاستنشاق
تقنيات الاستنشاق الفعال
تسمم ذاكرة التخزين المؤقت DNS
رجل في منتصف الهجوم
أدوات للتطفل
التدابير المضادة
الفصل 12 - الحرمان من الخدمة
ما هو الهجوم على الخدمة (DOS)؟
الهجوم الموزع على الخدمة (DDOS)
التدابير المضادة
الفصل 13 - القرصنة اللاسلكية
أساسيات الشبكات اللاسلكية
الاستنشاق اللاسلكي

الخصوصية المكافئة السلكية (WEP)
الوصول المحمي بواسطة WPA) WI-FI)
الهجمات على الخدمة (DOS)
التدابير المضادة
الفصل 14 - نقاط الضعف في تطبيق الويب
أساسيات تطبيق الويب
أنواع نقاط الضعف في تطبيق الويب
أدوات لمسح الضعف
الفصل 15 - اختراق مستخدمي الانترنت
تقنيات الاختراق المشتركة
استنتاج

مقدمة

تهانينا على شرائك **" عالم القرصنه : دليل المبتدئين "**.
هذا الكتاب سوف يأخذك من خلال مفاهيم اختراق الكمبيوتر بطريقة بسيطة جدا و
من السهل اتباع الطريقة بحيث يجب على القراء الذين ليس لديهم معرفة مسبقة بالقرصنة
تكون قادرة على فهم بسهولة المفهوم. لتبدأ ، كل ما تحتاجه هو القليل من العمل
معرفة أجهزة الكمبيوتر ، ونظام التشغيل (ويندوز) واتصال بالإنترنت.
كثير من الكتب الشائعة التي قرأتها عن القرصنة الأخلاقية هي في الغالب مناسبة فقط
أولئك الذين لديهم بالفعل قدر كبير من المعرفة في هذا المجال. أيضا ، هذه
تنغمس الكتب كثيرًا في الجزء النظري الذي يقدم للقارئ الكثير من الأشياء غير الضرورية
التفسير ، وبالتالي إضافة إلى الجزء الأكبر من الكتاب. هذا قد يسبب القارئ ل
تفقد الاهتمام بالتدريج أو توقف عن القراءة في منتصف الطريق.
لذلك ، قررت الخروج بكتاب لا يتطلب معرفة مسبقة بالموضوع وهو كذلك
من السهل على القراء متابعة وفهم في كل نقطة. بدلا من حشو الكتاب
مع النوع التقليدي للفقرات من المحتوى ، أفضل عرض المواضيع بطريقة سهلة

اتبع الطريقة من خلال تضمين النقاط النقطية والرسوم التوضيحية والأمثلة العملية. هذا ممكن
أبقِ الكتاب نحيلًا ، لكنه لا يزال قادرًا على الاستجابة الفعالة لسعي القارئ
المعرفه. قررت أيضًا إسقاط المفاهيم والتقنيات القديمة من الكتاب
واحتفظ فقط بالأنشطة النشطة والممكنة في سيناريو اليوم الحالي.
عند الانتهاء من قراءة هذا الكتاب ، يجب أن تكون قادرًا على تطبيق المعرفة والمهارات
التي اكتسبتها بعدة طرق:
يمكنك *تبني عقلية الهاكر* والبدء في التفكير والرد على المواقف و
مشاكل تماما مثل القراصنة ستفعل. بعد كل شيء ، القرصنة هي مجرد عقلية أكثر من
مجموعة مهارة!
يجب أن تكون قادرًا بسهولة على *حماية نفسك* من جميع هؤلاء المتسللين الأشرار هناك
من خلال الحفاظ على أمان حساباتك عبر الإنترنت أو خادم الويب أو الشخصية الخاصة بك
الحاسوب.
يضع هذا الكتاب *الأساس* اللازم لبدء حياتك المهنية كقراصنة أخلاقيين
حيث يمكنك البدء في تطبيق المعرفة والمهارات في مهنتك.

كيفية استخدام هذا الكتاب؟

سيغطي هذا الكتاب مفاهيم اختراق الكمبيوتر لكل من *Windows* و *Linux*
أنظمة التشغيل. بالنسبة إلى الأمثلة العملية والرسومات التوضيحية التي تستند إلى Windows ،
فقد استخدمت
بلدي **ويندوز 8.1** الكمبيوتر. بالنسبة إلى الأمثلة المستندة إلى Linux ، استخدمت **Kali Linux**
1.0.9a مباشرة
DVD. نظرًا لأن معظم الأمثلة ليست خاصة بإصدار نظام التشغيل ، يمكنك ذلك
قم بتنفيذها على أي إصدار من نظامي التشغيل Windows و Linux مثبتين على جهاز الكمبيوتر
الخاص بك.
يتم وضع كل فصل بما في ذلك جميع المفاهيم الواردة في هذا الكتاب في التسلسل الهرمي

بطريقة حيث مفهوم واحد يشكل الأساس للآخر. هذا قد لا يكون صحيحا ل
كل فصل ولكن في كثير من الحالات المفاهيم التي نوقشت في الجزء السابق من الكتاب قد

يبدو لتشكيل العناصر الرئيسية في فهم المفاهيم اللاحقة. نتيجة لذلك
نوصي بقراءة هذا الكتاب بطريقة منظمة وعدم تخطي المفاهيم أو الفصول
ما بين أثنين.
خلال هذا الكتاب ، سيتم تقديم العديد من الأمثلة التوضيحية والتماثلية
والرسوم البيانية لافتة للنظر التي لن تجعل فقط عملية فهم كاملة
أسهل ، ولكن أيضا يجعل عملية التعلم متعة! آمل أن تكونوا مثل هذا الكتاب والتمتع به
المفاهيم المقدمة فيه.

الفصل 1 مقدمة

أراهن أن معظمكم متحمس جدًا للبدء. ولكن ، قبل أن ننتقل بالفعل إلى
تعلم كيفية الاختراق ، دعونا نبدأ في فهم معنى القرصنة حقا.

ما هو الاختراق؟

في مجال أمان الكمبيوتر ، يشير القرصنة ببساطة إلى فعل استغلال
ضعف موجود في نظام الكمبيوتر أو شبكة الكمبيوتر.
في أعمال أخرى ، فإن المتسلل هو شخص طور اهتمامًا عميقًا بالفهم
كيف يعمل نظام الكمبيوتر أو البرنامج ، حتى يتمكن من السيطرة على
الكمبيوتر عن طريق استغلال أي من نقاط الضعف الموجودة فيه.

تصنيف هاكر

بناءً على الموقف ومستوى المهارة التي يتمتعون بها ، يتم تصنيف المتسللين إلى ما يلي

أنواع:

القبعة البيضاء **القراصنة** : قراصنة *القبعة البيضاء* (المعروف أيضا باسم **القراصنة الأخلاقيين**) هو شخص ما

الذي يستخدم مهاراته فقط لأغراض دفاعية مثل اختبار الاختراق. هؤلاء

غالبًا ما يتم توظيف نوع من المتسللين من قبل العديد من المنظمات لضمان الأمن

نظم المعلومات الخاصة بهم.

القبعة السوداء **القراصنة** : القراصنة *القبعة السوداء* (المعروف أيضا باسم **المفرقع**) هو شخص يستخدم دائمًا مهاراته لأغراض هجومية. نية القراصنة القبعة السوداء هي ل

كسب المال أو الانتقام الشخصية عن طريق التسبب في ضرر لأنظمة المعلومات.

غراي هات **هاكر** : **هاكر *القبعة*** *الرمادية* هو شخص يقع بين *القبعة البيضاء*

و *قبعة سوداء* الفئة. هذا النوع من المتسللين قد يستخدم مهاراته سواء للدفاع أو

أغراض مسيئة.

Script Kiddie : A *kiddie* *سيناريو* هو المتسلل المتمني. هؤلاء هم الذين يفتقرون إلى

معرفة كيف يعمل نظام الكمبيوتر حقًا ولكن استخدم البرامج الجاهزة ،

الأدوات والبرامج النصية لاقتحام أجهزة الكمبيوتر.

المصطلحات الأساسية

قبل المضي قدما ، فيما يلي بعض المصطلحات الأساسية في

مجال القرصنة الذي يجب أن يكون على علم به:

الضعف: A *الضعف* هو ضعف الحالية التي يمكن أن تسمح للمهاجم

المساس بأمن النظام.

استغلال: إن *استغلال* وبطريقة محددة (قطعة من البرمجيات، مجموعة من الأوامر وغيرها) التي يستفيد من مشكلة عدم الحصانة الحالية لخرق أمان نظام تكنولوجيا المعلومات.

التهديد: A *التهديد* هو خطر محتمل يمكن أن يستغل نقطة ضعف الحالية ل

تسبب الضرر المحتمل.

الهجوم: إن *الهجوم* هو أي عمل يمس بأمن النظام. في أخرى

بعبارة أخرى ، إنه هجوم على أمان النظام مشتق من تهديد موجود.

القرصنة أسئلة وأجوبة

فيما يلي قائمة صغيرة ببعض *الأسئلة المتداولة* حول القرصنة:

كم من الوقت يستغرق لتصبح المتسلل؟

القرصنة ليست شيئًا يمكن إتقانه بين عشية وضحاها. يستغرق حقا بعض الوقت لفهم وتنفيذ المهارات التي وضعت في الواقع كنت في أحذية القراصنة.
لذلك ، لمن يريد أن يصبح متسللاً ، كل ما يتطلبه الأمر هو بعض الإبداع ، الرغبة في التعلم والمثابرة.

ما المهارات التي أحتاجها لكي أصبح متسللاً؟

أنا من أجل أن تصبح متسلل ، من الضروري أن يكون لديك فهم أساسي لكيفية يعمل نظام الكمبيوتر. على سبيل المثال ، يمكنك البدء باستخدام أساسيات نظام التشغيل ، شبكات الكمبيوتر وبعض البرمجة.
في هذه المرحلة الزمنية ، لا داعي للقلق بشأن هذا السؤال لأن هذا الكتاب سيستغرق من خلال كل هذه المفاهيم الضرورية لتأسيس المهارات التي تحتاج إلى امتلاكها القراصنة.

ما هي أفضل طريقة لتعلم القرصنة؟

كما ذكرنا سابقًا ، فإن أفضل طريقة لتعلم القرصنة هي البدء بالأساسيات. حالما تمتلك أنشأت المهارات الأساسية ، يمكنك أن تأخذها إلى أبعد من ذلك من خلال تصفح الكتب التي مناقشة المواضيع الفردية بطريقة مفصلة بكثير. لا تنس قوة الإنترنت عندما يتعلق الأمر باكتساب وتوسيع نطاق معرفتك.

الفصل 2 - المفاهيم الأساسية

الآن ، دعونا نبدأ في فهم بعض المفاهيم الأساسية التي لا غنى عنها في وضع الأساس لرحلتنا لتعلم كيفية اختراق. قبل القفز في الواقع
التدريب العملي على النهج ، فمن الضروري للغاية لأحد أن يكون لديك فهم شامل لل أساسيات شبكة الكمبيوتر ونموذج عملها. ستجد في هذا الفصل نبذة مختصرة وصف للمفاهيم والمصطلحات المختلفة المتعلقة بشبكات الكمبيوتر ،

التشفير والأمن.

شبكة الكمبيوتر

A *شبكة الكمبيوتر* هي مجموعة من اثنين أو أكثر من أجهزة الكمبيوتر مرتبطة معا بحيث يتم الاتصال بين أجهزة الكمبيوتر الفردية ممكن. بعض من الشائع
تشمل أنواع شبكات الكمبيوتر ما يلي:

شبكة محلية (LAN)

هذا هو نوع من شبكة الكمبيوتر حيث توجد أجهزة الكمبيوتر المترابطة للغاية على مقربة من بعضهم البعض يقولون على سبيل المثال ، داخل نفس المبنى.

شبكة واسعة النطاق (WAN)

هذا هو نوع من شبكة الكمبيوتر حيث يتم فصل أجهزة الكمبيوتر المتصلة بواسطة أ مسافة كبيرة (من بضعة كيلومترات إلى مئات الكيلومترات) ويتم توصيلها باستخدام خطوط الهاتف أو موجات الراديو.

الإنترنت

و *الإنترنت* هي أكبر شبكة التي تربط مختلف الشبكات المحلية والشبكات الواسعة. إنها النظام العالمي لمختلف شبكات الكمبيوتر المترابطة التابعة للحكومة أو
المنظمات الخاصة.

شبكة المضيف

A مضيف *شبكة* (أو يشار ببساطة إلى كمضيف) يمكن أن يكون أي جهاز كمبيوتر أو شبكة جهاز متصلا بشبكة الكمبيوتر. يمكن أن يكون هذا الكمبيوتر محطة طرفية أو خادم ويب
تقديم الخدمات لعملائها.

بروتوكول الشبكة

A *بروتوكول الشبكة* (أو إليها توا باسم بروتوكول) عبارة عن مجموعة من القواعد والاتفاقيات التي ضرورية للاتصال بين جهازين للشبكة. على سبيل المثال ، اثنان
يمكن لأجهزة الكمبيوتر على شبكة الاتصال فقط إذا وافقوا على اتباع البروتوكولات.

فيما يلي بعض بروتوكولات الشبكة الأكثر إحالةً:

بروتوكول الإنترنت (عنوان IP)

على *بروتوكول الإنترنت* عنوان (*IP* عنوان) هو رقم فريد المسندة إلى كل كمبيوتر أو الجهاز (مثل الطابعة) بحيث يمكن تعريف كل واحد منهم بشكل فريد على الشبكة.

أنواع عنوان IP:

خاص عنوان A **IP:** *عنوان IP الخاص* هو الذي تم تعيينه إلى جهاز كمبيوتر على شبكة محلية (LAN). مثال نموذجي لعنوان IP الخاص سيكون شيئًا ما مثل:

192.168.0.2

IP العامة العنوان: A *عنوان IP العام* هو الذي تم تعيينه إلى كمبيوتر متصلا بالإنترنت. مثال لعنوان IP العام سيكون مثل:

59.93.115.125

في معظم الحالات ، يتم توصيل الكمبيوتر بشبكة ISP باستخدام IP خاص. مرة الكمبيوتر موجود على شبكة ISP ، سيتم تعيين عنوان IP عام يستخدمه يتم التواصل مع الإنترنت ممكن.

كيفية البحث عن عنوان IP لجهاز الكمبيوتر؟

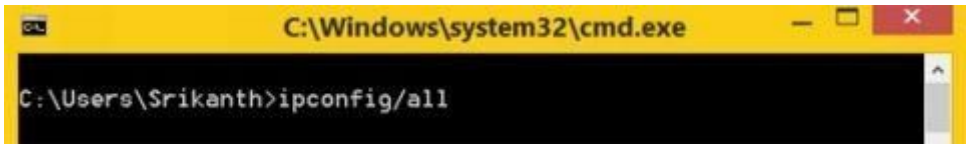
العثور على الملكية الفكرية العامة الخاصة بك هو في غاية البساطة. اكتب فقط "ما هو عنوان IP الخاص بي" على Google لمشاهدته

عنوان IP العام الخاص بك معروض في نتائج البحث.

الشكل 1.2

من أجل العثور على IP الخاص بك ، فقط افتح نافذة موجه الأوامر (اكتب **cmd** في "تشغيل" مربع) وأدخل الأمر التالي:

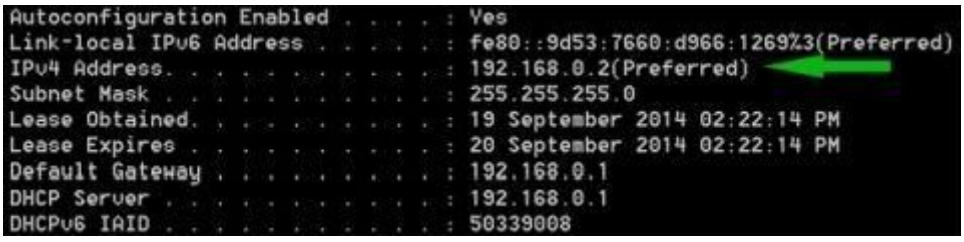
ipconfig / كافة



الشكل 2. 2

سيؤدي ذلك إلى عرض قائمة طويلة من التفاصيل حول أجهزة شبكة الكمبيوتر لديك ترتيب. لمشاهدة عنوان IP الخاص بك ، ما عليك سوى التمرير لأسفل للعثور على شيء باسم " IPv4"

العنوان "ليس سوى IP الخاص بك.



الشكل 2. 3

بروتوكول نقل النص التشعبي (HTTP)

يوفر *Hyper Text Transfer Protocol* معيارًا للاتصال بين الويب المتصفحات والخادم. انها واحدة من البروتوكول الأكثر استخداما على شبكة الإنترنت ل طلب مستندات مثل صفحات الويب والصور.

مثال: http://www.example.com

بروتوكول نقل الملفات (FTP)

و *بروتوكول نقل الملفات* يوفر معيارا لنقل الملفات بين البلدين أجهزة الكمبيوتر على الشبكة. يستخدم FTP على نطاق واسع في تنفيذ التحميل / التنزيل العمليات بين الخادم ومحطة العمل.

مثال: ftp://www.example.com

بروتوكول النقل الرئيسي البسيط (SMTP)

و *بروتوكول نقل البريد البسيط* يوفر معيارا لإرسال رسائل البريد الإلكتروني من واحد الخادم إلى آخر. تستخدم معظم أنظمة البريد الإلكتروني التي ترسل البريد عبر الإنترنت SMTP إلى تبادل الرسائل بين الخادم.

Telnet هو بروتوكول شبكة يسمح لك بالاتصال بالمضيفين عن بعد على الإنترنت أو على شبكة محلية. يتطلب برنامج عميل telnet لتطبيق البروتوكول باستخدام الذي تم تأسيس الاتصال مع الكمبيوتر البعيد.

في معظم الحالات تلنت يتطلب أن يكون لديك *اسم المستخدم* و *كلمة المرور* لإنشاء اتصال مع المضيف البعيد. في بعض الأحيان ، تسمح بعض الأجهزة المضيفة للمستخدمين أيضًا بإجراء

اتصال **كضيف** أو **الجمهور** .

بعد إجراء الاتصال ، يمكن للمرء استخدام الأوامر القائمة على النص للتواصل مع المضيف البعيد. بناء جملة استخدام الأمر telnet كالتالي:

منفذ telnet <اسم المضيف أو IP>

مثال: telnet 127.0.0.1 25

SSH (شل الآمنة)

SSH هو بروتوكول يشبه telnet والذي يسهل أيضًا الاتصال بالمضيفين عن بُعد الاتصالات. ومع ذلك ، SSH له اليد العليا على telnet من حيث الأمن. تلنت صمم في المقام الأول للعمل داخل الشبكة المحلية ، وبالتالي لا يعتني الأمان. من ناحية أخرى ، تمكن SSH من توفير أمان تام أثناء الاتصال المضيفين عن بعد على شبكة الاتصال البعيدة أو الإنترنت.

أقرب إلى SSH التلنت يستخدم أيضا برنامج العميل ويتطلب *اسم المستخدم* و *كلمة المرور* ل تأسيس اتصال مع المضيف البعيد.

منفذ الشبكة

قد يشغل جهاز كمبيوتر عدة خدمات عليه مثل HTTP (خادم الويب) ، FTP ، SMTP وهلم جرا. يتم تعريف كل من هذه الخدمات بشكل فريد بواسطة رقم يسمى منفذ *الشبكة* (أو يشار إليها ببساطة باسم *المنفذ*). إذا أراد الكمبيوتر الاستفادة من خدمة معينة من خدمة أخرى الكمبيوتر ، يجب عليه إنشاء اتصال به على رقم المنفذ الدقيق حيث الخدمة المقصودة قيد التشغيل.

على سبيل المثال ، إذا كانت المحطة تريد طلب مستند ويب من خادم بعيد باستخدام HTTP ، يجب عليه أولاً تأسيس اتصال بالخادم البعيد على المنفذ 80 (تشغيل خدمة HTTP على المنفذ 80) قبل وضع الطلب.

بعبارة بسيطة ، يمكن مقارنة أرقام المنافذ بأرقام الأبواب حيث يمنح كل باب الوصول إلى خدمة معينة على جهاز كمبيوتر. يعرض الجدول التالي قائمة بالشعبية الخدمات وأرقام المنافذ الافتراضية:

HTTP
80
FTP
21
SMTP
25
TELNET
23
SSH
22

الجدول 2. 1

حزمة الشبكة

تعد حزمة *الشبكة* (حزمة البيانات أو مخطط البيانات أو ما يسمى ببساطة الحزمة) وحدة أساسية من البيانات

إرسالها من مضيف إلى آخر عبر شبكة. عند البيانات (مثل البريد أو الرسالة أو ملف) يجب أن ينتقل بين مضيفين ، مجزأ في هياكل صغيرة تسمى الحزم وإعادة تجميعها في الوجهة لجعل قطعة البيانات الأصلية.

تتكون كل حزمة من البيانات المجزأة بالإضافة إلى المعلومات الضرورية التي سوف مساعدة لها الحصول على وجهتها مثل *IP المرسل* عنوان، ويقصد *IP المتلقي* عنوان، رقم *المنفذ المستهدف* ، *إجمالي* عدد *الحزم التي* تم قطع جزء البيانات الأصلي في *ورقم تسلسل* الحزمة معينة.

نظام اسم النطاق (DNS)

A *نظام اسم المجال* أو *خدمة اسم المجال* (DNS) هو بروتوكول شبكة وظيفته
هو تعيين أسماء النطاقات مثل "gohacking.com" إلى عنوان IP المقابل لها مثل
."104.28.6.51"

نظرًا لأن الإنترنت هي أم ملايين أجهزة الكمبيوتر التي تمتلك كل منها عنوان IP فريدًا
يصبح من المستحيل على الناس تذكر عنوان IP الخاص بكل كمبيوتر
انهم يريدون الوصول. لذلك ، من أجل جعل هذه العملية أكثر بساطة مفهوم المجال
تم تقديم الأسماء. ونتيجة لذلك ، يمكن للمستخدمين الوصول بسهولة إلى أي موقع ويب فقط عن طريق كتابة مواقعهم
أسماء النطاقات في أساس عنوان المتصفح مثل "google.com" أو "yahoo.com" بدون
الحاجة إلى تذكر عناوين IP الفعلية الخاصة بهم.
ومع ذلك ، منذ بروتوكول الشبكة يفهم فقط عنوان IP وليس المجال
أسماء ، فمن الضروري ترجمة اسم المجال مرة أخرى إلى عنوان IP المقابل لها
قبل تأسيس اتصال مع الخادم الهدف. هذا هو المكان الذي يأتي DNS فيه
مفيد.

مزود خدمة الإنترنت الخاص بك لديه خادم DNS الذي يحتفظ بسجل هائل من
أسماء النطاقات الحالية وعناوين IP المقابلة لها. في كل مرة تكتب عنوان URL
مثل "http://www.google.com" في شريط عنوان المتصفح ، سيستخدم جهاز الكمبيوتر الخاص بك
خادم DNS من مزود خدمة الإنترنت وترجمة اسم النطاق "google.com" إلى
عنوان IP المقابل لإجراء اتصال مع خادم جوجل. كل هذه العملية
سيحدث في جزء من الثانية وراء الكواليس وبالتالي يذهب دون أن يلاحظها أحد.

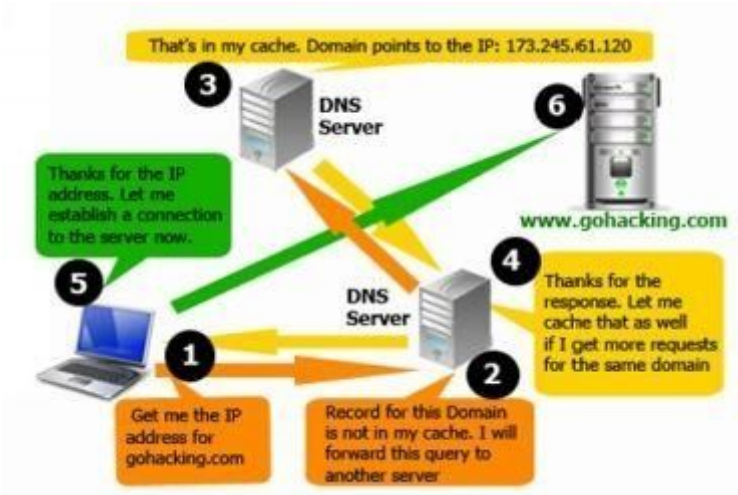
كيف يعمل DNS؟

دعنا نفهم عمل *نظام اسم المجال* باستخدام المثال التالي:
كلما قمت بكتابة عنوان URL مثل "http://www.gohacking.com" على متصفحك
شريط العناوين ، سيرسل جهاز الكمبيوتر الخاص بك طلبًا إلى *خادم الاسم المحلي* (ISP DNS)

الخادم) لحل اسم المجال إلى عنوان IP الخاص به. هذا الطلب هو في كثير من الأحيان يشار إليها باسم **استعلام DNS** .

سيتلقى خادم الاسم المحلي الاستعلام لمعرفة ما إذا كان يحتوي على المطابقة اسم وعنوان IP في قاعدة البيانات الخاصة به. إذا وجد ، يكون عنوان IP المقابل (الاستجابة) هو عاد. إذا لم يكن الأمر كذلك ، يتم تمرير الاستعلام تلقائيًا إلى خادم DNS آخر موجود في المستوى الأعلى التالي من التسلسل الهرمي DNS. تستمر هذه العملية حتى يصل الاستعلام إلى خادم DNS الذي يحتوي على الاسم المطابق وعنوان IP. عنوان IP (استجابة)

ثم يعود السلسلة بالترتيب العكسي إلى جهاز الكمبيوتر الخاص بك. الشكل التالي 2.4 يوضح العملية المذكورة أعلاه.



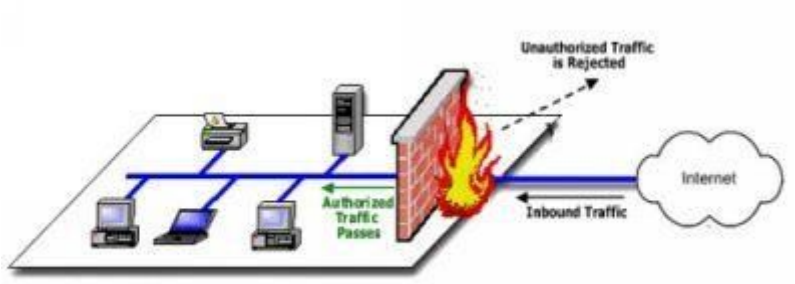
الشكل 2. 4

FIREWALL

جدران الحماية هي في الأساس حاجز بين جهاز الكمبيوتر الخاص بك (أو الشبكة) والإنترنت (العالم الخارجي). يمكن مقارنة جدار الحماية ببساطة بحارس الأمن الذي يقف عند مدخل منزلك وفلاتر الزوار القادمين إلى مكانك. قد يسمح لبعض يجب على الزائرين الدخول بينما يحرمون الآخرين الذين يشتبه في كونهم من المتسللين. وبالمثل جدار الحماية هو برنامج أو جهاز يقوم بتصفية المعلومات (الحزم) القادمة عبر الإنترنت إلى الكمبيوتر الشخصي أو شبكة الكمبيوتر.

كيف يعمل جدار الحماية؟

قد تقرر جدران الحماية السماح لحركة مرور الشبكة أو حظرها بين الأجهزة وفقًا للقواعد
التي تم تكوينها مسبقًا أو تعيينها بواسطة مسؤول جدار الحماية. معظم جدران الحماية الشخصية مثل
يعمل جدار حماية Windows على مجموعة من القواعد التي تم تكوينها مسبقًا والتي تعتبر أكثر
ملائمة
الظروف العادية ، بحيث لا يحتاج المستخدم إلى الكثير من القلق بشأن تكوين
جدار الحماية. يتضح تشغيل جدار الحماية في الشكل 2.5 أدناه.



الشكل 2. 5

جدران الحماية الشخصية سهلة التركيب والاستخدام ، وبالتالي يفضلها المستخدمون النهائيون
لتأمينها
أجهزة الكمبيوتر الشخصية الخاصة بهم. ومع ذلك ، من أجل تلبية الاحتياجات المخصصة شبكات
كبيرة و
تفضل الشركات تلك الجدران النارية التي لديها الكثير من الخيارات لتكوين.
على سبيل المثال ، قد تضع شركة قواعد جدار حماية مختلفة لخوادم FTP ، telnet
الخوادم وخوادم الويب. بالإضافة إلى ذلك ، يمكن للشركة التحكم في كيفية الموظفين
الاتصال بالإنترنت عن طريق حظر الوصول إلى بعض المواقع وتقييد نقل
الملفات إلى الشبكات الأخرى. وبالتالي ، بالإضافة إلى الأمان ، يمكن لجدار الحماية إعطاء الشركة أ
سيطرة هائلة على كيفية استخدام الناس لشبكتهم.
تستخدم جدران الحماية واحدًا أو أكثر من الطرق التالية للتحكم في الرسائل الواردة والصادرة
حركة المرور في الشبكة:
1. **تصفية الحزمة:** في هذه الطريقة ، يتم تحليل الحزم (قطع صغيرة من البيانات)
مجموعة من **المرشحات** . تحتوي عوامل تصفية الحزمة على مجموعة من القواعد التي تأتي مع
قبول ورفض الإجراءات
والتي تم تكوينها مسبقًا أو يمكن تهيئتها يدويًا بواسطة جدار الحماية

مدير. إذا تمكنت الحزمة من الوصول إليها من خلال هذه المرشحات ، فيُسمح بذلك للوصول إلى الوجهة ؛ وإلا يتم التخلص منها.

2. **التفتيش الدقيق:** هذه طريقة أحدث لا تحلل محتويات

الحزم. بدلاً من ذلك ، فإنه يقارن بعض الجوانب الرئيسية لكل حزمة بقاعدة بيانات مصدر موثوق. تتم مقارنة كل الحزم الواردة والصادرة ضد هذا قاعدة البيانات وإذا كانت المقارنة تعطي مطابقة معقولة ، ثم الحزم يسمح للسفر أبعد من ذلك. وإلا يتم تجاهلهم.

تكوين جدار الحماية:

يمكن تكوين جدران الحماية بإضافة عامل تصفية واحد أو أكثر استنادًا إلى العديد من الشروط المذكورة أدناه:

1. **عناوين IP: على** أي حال ، إذا قيل أن عنوان IP خارج الشبكة هو غير مواتية ، فمن الممكن ضبط مرشح لمنع كل حركة المرور من وإلى هذا عنوان IP. على سبيل المثال ، إذا تم العثور على عنوان IP معين ليكون أيضًا العديد من الاتصالات إلى خادم ، قد يقرر المسؤول حظر حركة المرور من هذا IP باستخدام جدار الحماية.
2. **أسماء النطاقات:** نظرًا لأنه من الصعب تذكر عناوين IP ، فهي عبارة عن طريقة أسهل وأكثر ذكاء لتكوين جدران الحماية من خلال إضافة المرشحات على أساس أسماء النطاقات. من خلال إعداد مرشح مجال ، قد تقرر شركة حظر الكل الوصول إلى أسماء مجالات معينة ، أو قد توفر الوصول فقط إلى قائمة أسماء النطاقات المختارة.
3. **المنافذ / البروتوكولات:** إذا كانت الخدمات التي تعمل على منفذ معين موجهة إلى المستخدمين العامين أو شبكة ، وعادة ما تبقى مفتوحة. وإلا يتم حظرها باستخدام جدار الحماية لمنع المتسللين من استخدام المنافذ المفتوحة لـ إجراء اتصالات غير مصرح بها.
4. **كلمات أو عبارات محددة:** يمكن تكوين جدار الحماية لتصفية واحد أو أكثر كلمات أو عبارات محددة بحيث تكون كل من الحزم الواردة والصادرة

الممسوحة ضوئيا للكلمات في التصفية.
على سبيل المثال ، يمكنك إعداد قاعدة جدار الحماية لتصفية أي حزمة
يحتوي على مصطلح مسيء أو عبارة قد تقرر حظرها
الدخول أو الخروج من الشبكة الخاصة بك.

الأجهزة مقابل جدار حماية البرامج:

توفر جدران الحماية للأجهزة مستوى أعلى من الأمان وبالتالي فهي مفضلة للخوادم حيث
الأمن له الأولوية القصوى. برامج جدران الحماية من ناحية أخرى أقل
باهظة الثمن ، وبالتالي يفضل في أجهزة الكمبيوتر المنزلية وأجهزة الكمبيوتر المحمولة.
عادة ما تأتي جدران الحماية للأجهزة كوحدة مدمجة في جهاز التوجيه وتوفر الحد الأقصى
الأمان لأنه يقوم بتصفية كل حزمة على مستوى الجهاز نفسه حتى قبل أن يتمكن من الدخول
حاسوبك. ومن الأمثلة الجيدة على جهاز التوجيه Linksys Cable / DSL.

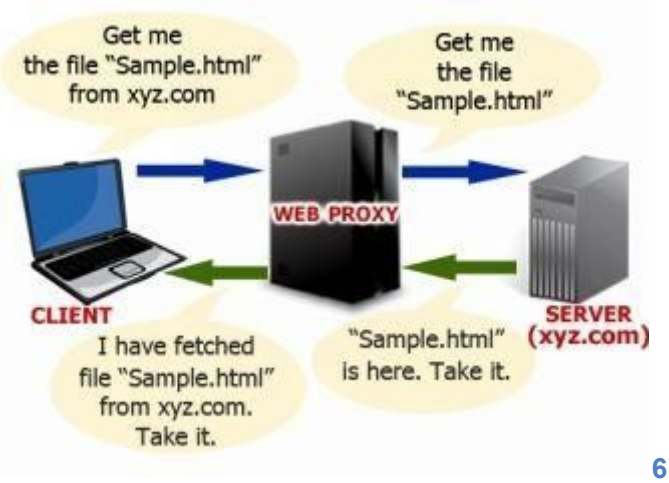
مخدم بروكسي

في شبكة الكمبيوتر ، يعد **الخادم الوكيل** أي نظام كمبيوتر يقدم خدمة تعمل
كوسيط بين الطرفين المتصلين ، العميل والخادم.
في وجود خادم وكيل ، لا يوجد اتصال مباشر بين العميل و
الخادم. بدلاً من ذلك ، يتصل العميل بالخادم الوكيل ويرسل طلبات الموارد
مثل مستند أو صفحة ويب أو ملف موجود على خادم بعيد. الخادم الوكيل
يعالج هذا الطلب عن طريق جلب الموارد المطلوبة من الخادم البعيد و
إعادة توجيه نفسه إلى العميل.

كيف يعمل الخادم الوكيل؟

يوضح الشكل 2.1 توضيحًا لكيفية عمل خادم وكيل.
كما هو موضح في المثال أدناه ، كلما يتصل العميل بخادم وكيل الويب و
يقدم طلبًا للموارد (في هذه الحالة ، "Sample.html") الموجودة على جهاز تحكم عن بُعد
الخادم (في هذه الحالة ، xyz.com) ، يقوم الخادم الوكيل بإعادة توجيه هذا الطلب إلى الخادم
الهدف على
نيابة عن العميل وذلك لجلب المورد المطلوب وتسليمه مرة أخرى إلى العميل.

يمكن أن يكون مثال العميل جهاز كمبيوتر يعمل بواسطة المستخدم ومتصل بالإنترنت.



الشكل 2. 6

يستخدم الخادم الوكيل على نطاق واسع لإخفاء عنوان IP أو أصل الإنترنت المستخدمين خلال نشاطهم. لأنه خادم الوكيل الذي يعالج الطلبات بين العميل والهدف ، يتم عرض عنوان IP الخاص بالخادم الوكيل فقط للخارج العالم وليس الفعلي. لذلك ، فإن معظم المتسللين استخدام خادم وكيل خلال الهجمات على هدفهم بحيث يكون من الصعب تتبعهم.

الفصل 3 - مقدمة لينكس

Linux هو نظام تشغيل يشبه UNIX وهو مفتوح المصدر ومتاح مجانًا تحميل. مقارنةً بنظام التشغيل Windows ، يعتبر Linux أكثر أمانًا واستقرارًا وموثوقية ، متعدد المستخدمين قادر ومتوافق مع كل من استخدام الخادم وسطح المكتب. هذا يجعلها واحدة من نظام التشغيل الأكثر شعبية بجانب ويندوز.

لماذا لينكس؟

بصفتك قراصنة أخلاقيا ، من الضروري للغاية أن يكون لديك فهم سليم لنظام Linux منصة ، واستخدامها والأوامر. Linux معروف على نطاق واسع بأنه "تشغيل المتسلل" النظام "وإذا كنت تتساءل لماذا ، الأسباب أدناه:

لأنه مجاني ، نظام تشغيل آمن ومستقر للغاية ، ملايين الخوادم على شبكة الإنترنت يعمل على لينكس.

بخلاف نظام التشغيل Windows الذي تم تصميمه على واجهة المستخدم الرسومية (GUI) ، تم تصميم Linux
على واجهة مستخدم الأوامر (CUI) وبالتالي توفر تحكمًا وتخصيصًا أكبر
خيارات للمتسللين.
تم تصميم بعض من أفضل البرامج النصية والقرصنة لنظام التشغيل Linux فقط.

WINDOWS VS. LINUX

مما لا شك فيه أن ويندوز هو نظام تشغيل سطح المكتب الأكثر شهرة المعروف به
سهولة الاستخدام وواجهة المستخدم الرسومية. نتيجة لذلك ، فإن معظم مستخدمي الكمبيوتر في
جميع أنحاء
العالم معتاد على نظام التشغيل ويندوز لكنه جديد على لينكس. إذا كنت كذلك
جديد إلى حد ما على Linux ويتساءلون ما هو الفرق بين Windows و Linux ،
هنا مقارنة سريعة بين الاثنين:

مقارنة بين ويندوز ولينكس

شبابيك

لينكس

المعروف عن سهولة الاستخدام وسهولة الاستخدام.

معروف بأمنه واستقراره ومرونته وسهولة حمله.

تستخدم على نطاق واسع لاستخدام سطح المكتب عن طريق المنزل والمكتب
المستخدمين.

تستخدم على نطاق واسع لاستخدام الخادم من قبل الشركات والشركات.

يعتمد نظام التشغيل بشكل أساسي على الرسوم البيانية
واجهة المستخدم (واجهة المستخدم الرسومية).

يعتمد نظام التشغيل بشكل أساسي على مستخدم الأوامر
واجهة (CUI).

مصمم للعمل مع مستخدم واحد فقط في كل مرة.

مصممة لدعم التشغيل المتزامن متعدد المستخدمين.

تم الإبلاغ عن أكثر من 70،000 فيروس لـ Windows
حتى الميعاد.

يتم الإبلاغ عن حوالي 80-100 فيروس فقط لنظام التشغيل Linux حتى الآن
وبالتالي أكثر أمانا.

نظرًا لأنه يعتمد على **واجهة المستخدم الرسومية** ، فمن السهل على المستخدمين التعلم
وتعمل.
نظرًا لأنه يستند إلى **CUI** ، يصعب على المستخدمين إلى حد ما
تعلم وتعمل.
يأتي كمنتج تجاري وبالتالي المتاحة
فقط عند الشراء.
يأتي كمصدر مفتوح وبالتالي فهو متاح مجانًا.
أمثلة على نظام التشغيل ويندوز القائم تشمل **ويندوز**
2000 و **XP** و **Vista** و **7** و **8.**
من أمثلة أنظمة التشغيل التي تستند إلى نظام Linux نظام التشغيل **Ubuntu** و **Fedora** و **Red**
هات ، *ديبيان* ، سينت أو إس إلخ.

اختيار توزيع LINUX

توزيع Linux عبارة عن مجموعة من البرامج والتطبيقات المترجمة حول
Linux kernel (المكون المركزي لنظام التشغيل). يمكنك الاختيار من بين مجموعة واسعة
مجموعة متنوعة من توزيعات لينكس مثل **أوبونتو** ، **فيدورا** أو **ديبيان** حيث يحتوي كل واحد منهم
مجموعة خاصة بهم من البرامج والتطبيقات ولكن تشترك في نواة لينكس المشتركة. ك
المبتدئين يمكنك اختيار أوبونتو لأنها سهلة التركيب وسهلة الاستعمال. يمكنك العثور على
رابط التحميل ودليل التثبيت من موقع أوبونتو الرسمي الذي يوجد به الرابط
المذكورة أدناه:

الموقع الرسمي لأوبونتو: http://www.ubuntu.com/

تشغيل LINUX من قرص حقيقي

هناك طريقتان لاستخدام نظام التشغيل Linux. واحد هو لتثبيت نظام التشغيل
إلى القرص الصلب تمامًا كما تفعل ذلك لنظام التشغيل Windows. ومع ذلك ، فإن هذه الطريقة
تتطلب
خبرة سابقة في تثبيت وتكوين أنظمة التشغيل. إذا كنت جديدا على
Linux أو ليس لديك خبرة سابقة في تثبيت نظام التشغيل ، يمكنك استخدام خيار القرص المباشر
مثل CD أو DVD لتشغيل واستخدام Linux. هذا في الواقع هو بديل جيد للتركيب
ويوفر طريقة سهلة لتشغيل Linux على نظامك دون تعديل أي من

الإعدادات السابقة ونظام الملفات الحالي. لكن هذا الخيار لا يحفظ عملك
عند إغلاق جهاز الكمبيوتر الخاص بك ، وبالتالي مناسبة فقط للاستخدام مثل الاختراق
الاختبار والتعلم.
أحد توزيعاتي المفضلة للاختراق والاختراق هو ***Kali Linux***. هذا هو
على أساس نظام دبيان جنو / لينكس ويأتي في شكل دي في دي مباشر مع
خيار لتثبيت كذلك. يمكنك تنزيل صورة *ISO* لإصدار DVD بحرية
من موقع Kali Linux الرسمي. الرابط إلى الموقع موضح أدناه:
موقع Kali: https://www.kali.org/downloads/
بعد اكتمال التنزيل ، يمكنك نسخ صورة ISO على قرص DVD باستخدام مجاني
برنامج مثل **إيمغبورن** . هذا يجب أن يوفر لك كالي دي في دي لايف للتمهيد. من اجلك
المرجع ، لقد استخدمت الإصدار 64 بت **1.0.9a** من Kali Linux live DVD في كل ما عندي
أمثلة وعروض خلال هذا الكتاب.

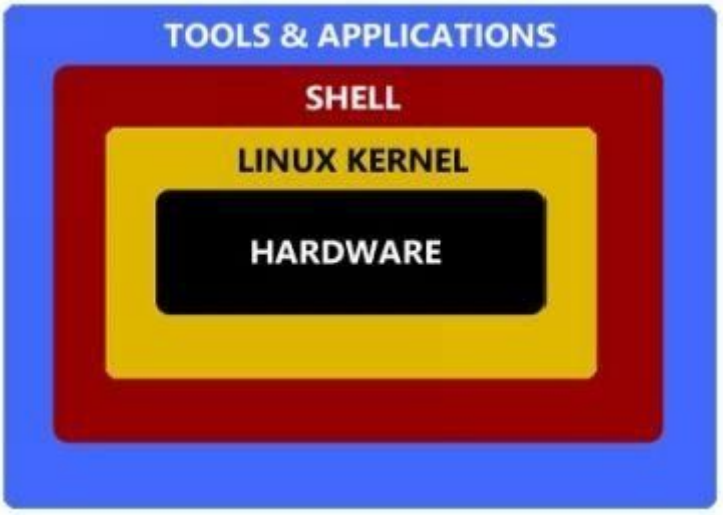
أساسيات لينكس

تم تطوير نظام التشغيل Linux في عام 1991 من قبل *Linus Torvalds* عندما كان طالبًا
جامعة هلسنكي ، فنلندا. نشر عن الكود المصدري الذي طوره في
مجموعة أخبار مينيكس. كانت التعليقات جيدة وبدأت شفرة المصدر في الانتشار
العالم عبر FTP وعلى مر السنين أصبح Linux نظام تشغيل مشهور جدًا.
اليوم ، العديد من برامج الشبكات الرائعة وأدوات الأمان والخوادم بما في ذلك DNS والبريد
الإلكتروني
وخادم الويب التي يجري تطويرها لنظام لينكس من قبل المبرمجين والمتسللين حول
العالمية.

نظام نظام لينكس

يتم تنظيم تشغيل Linux من حيث الطبقات التالية كما هو موضح في
الشكل أدناه:
تتكون **طبقة الأجهزة** من الأجهزة الفعلية مثل وحدة المعالجة المركزية والذاكرة والصلب
محرك الأقراص الخ

Kernel هو المكون الأساسي الذي يكمن في قلب نظام التشغيل
يتفاعل مباشرة مع الأجهزة باستخدام لغة الجهاز.

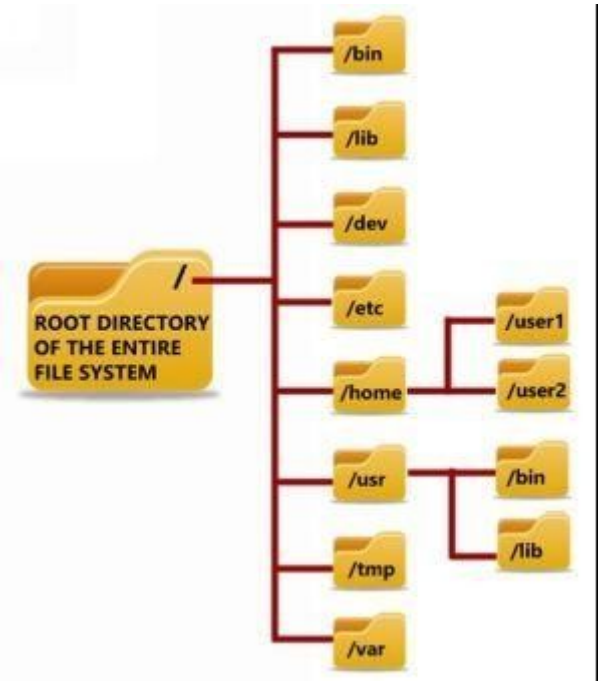


الشكل 3. 1

شل (أو مترجم الأوامر) يعمل كوسيط يأخذ الأوامر من
المستخدم ثم ينقلهم إلى النواة التي تنفذها في النهاية.
الأدوات والتطبيقات الموجودة على القشرة الخارجية وتمنح المستخدم معظم
وظائف نظام التشغيل.

هيكل دليل لينكس

A *بنية الدليل* هو الطريقة التي نظام الملفات وملفاته من التشغيل
يتم عرض النظام للمستخدم. أشخاص جدد على نظام التشغيل Linux و
غالبًا ما تجد بنية **نظام الملفات** الخاص بها مشكلة ومزعجة في التعامل معها
الملفات ومواقعها. لذلك ، دعونا نبدأ في استكشاف بعض المعلومات الأساسية حول
نظام ملفات Linux.
يحتوي أي توزيع Linux قياسي على بنية الدليل التالية كما هو موضح أدناه:



الشكل 3. 2

فيما يلي وصف موجز للغرض ومحتويات كل دليل:

/ - دليل الجذر

يبدأ كل ملف فردي ودليل نظام ملفات Linux من *الدليل الجذر* .

يمتلك المستخدم "root" فقط امتياز الكتابة لهذا الدليل.

/ بن - الثنائيات

يحتوي على الملفات الثنائية القابلة للتنفيذ اللازمة لتشغيل وإصلاح النظام. أيضا

يحتوي على ملفات وأوامر مطلوبة للتشغيل في وضع المستخدم الفردي مثل: *ls* و *ping* و *grep* وما إلى ذلك

/ lib - مكتبات النظام

يحتوي على مكتبات النظام ووحدات kernel المطلوبة لتشغيل النظام.

/ dev - ملفات الجهاز

يحتوي على ملفات متعلقة بالجهاز لجميع أجهزة النظام.

/ الخ - ملفات التكوين

يحتوي على ملفات التكوين المطلوبة من قبل جميع البرامج. كما أنه يحتوي على بدء و

البرامج النصية *إيقاف التشغيل* المستخدمة *لبدء* أو *إيقاف* البرامج الفردية.

/ الرئيسية - الدلائل الرئيسية

هذا يشكل "الدليل الرئيسي" للمستخدمين الفرديين لتخزين معلوماتهم الشخصية.

في كل مرة يتم إضافة مستخدم جديد ، يتم إنشاء دليل جديد باسم المستخدم الموجود أسفل "/الصفحة الرئيسية".

/ user - برامج المستخدم

يستخدم هذا الدليل لتخزين القابلة للتنفيذ ***الثنائيات*** ، ***وثائق*** ، ***التعليمات البرمجية المصدر*** ملفات و ***المكتبات*** لبرامج المستوى الثاني.

/ tmp - الملفات المؤقتة

يحتوي على ملفات مؤقتة للنظام والمستخدمين.

/ var - الملفات المتغيرة

يحتوي على ملفات من المتوقع أن يزداد حجمها. تتضمن أمثلة هذه الملفات ملفات *السجل* ، *طباعة طوابير* ، *ملفات القفل* و *الملفات المؤقتة* .

أوامر Linux

تتم كتابة جميع الأوامر في Linux بالأحرف الصغيرة وحساسة لحالة الأحرف. كل لينكس يجب كتابة الأمر وتنفيذه في نافذة تسمى " **المحاكي الطرفي** " أو يشار إليها ببساطة باعتبارها **محطة** . إنه برنامج مشابه *لموجه الأوامر* الخاص بـ Microsoft Windows حيث يمكن للمستخدم تشغيل الأوامر والحصول على النتائج المعروضة.

أ

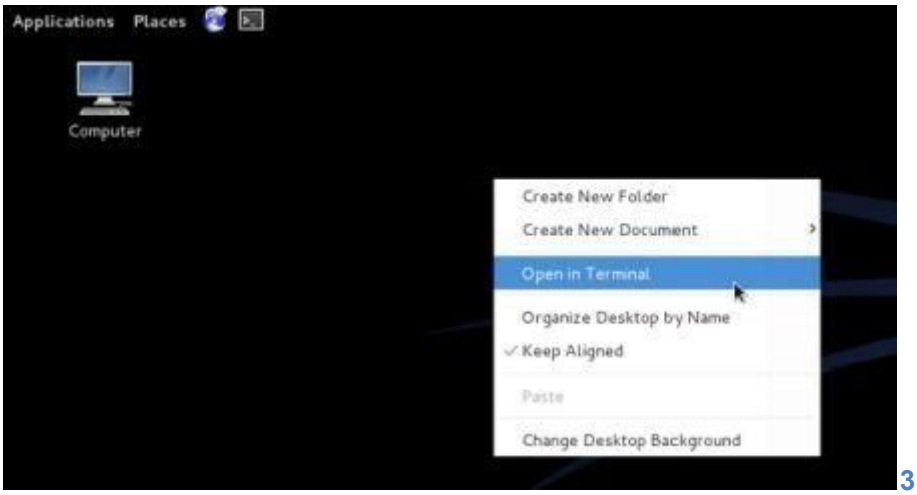
محطة تأخذ ببساطة أوامر المستخدم ، ويمررها إلى قذيفة للتنفيذ و يعرض النتائج مرة أخرى للمستخدم.

لتشغيل الأوامر في الجهاز ، يجب عليك أولاً تحميل Linux من Live قرص DVD الذي قمت بإنشائه. للقيام بذلك ، فقط أدخل Kali Linux DVD في محرك الأقراص ، التمهيد

من ذلك وحدد "خيار لايف". بمجرد الانتهاء من التشغيل يجب أن تشاهد سطح المكتب تحميلها على الشاشة.

لبدء نافذة المحطة ، فقط انقر **بزر** الماوس **الأيمن** على سطح المكتب وحدد الخيار

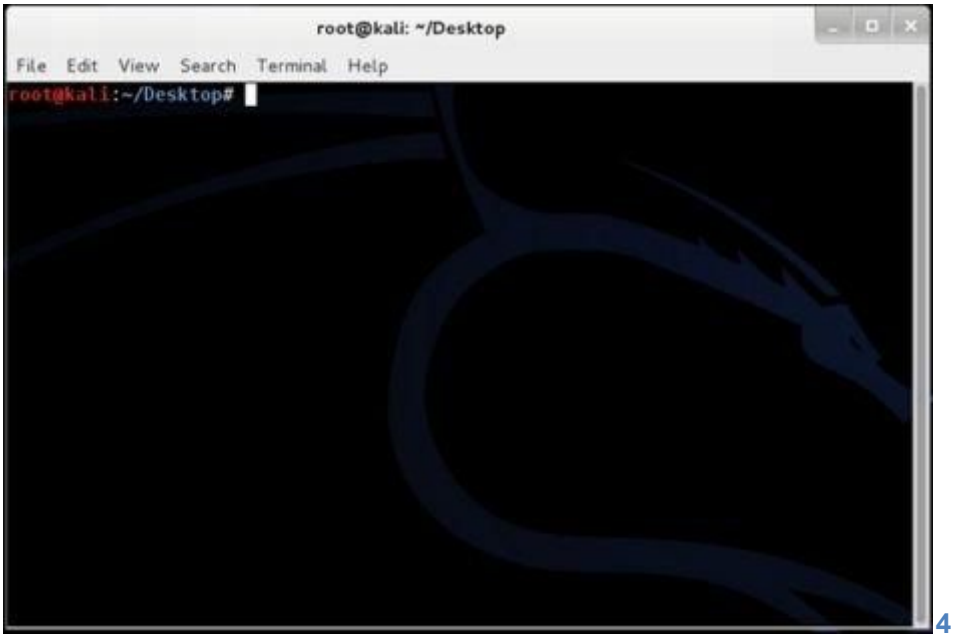
فتح في المحطة الطرفية كما هو موضح في لقطة أدناه 3.1:



الشكل 3. 3

بمجرد تحميل *نافذة الجهاز* ، يجب أن تكون قادرًا على بدء كتابة الأوامر. أ

ويرد لقطة من *نافذة المحطة* أدناه:



الشكل 3. 4

إنشاء الملفات

هناك نوعان من الأوامر لإنشاء ملفات: **لمسة** و **القط** . إليكم كيف سيكونون

مستخدم:

#لمسة عينة

هذا يخلق ملف فارغ يسمى "عينة". إذا كنت ترغب في إنشاء ملفات فارغة متعددة

بسرعة يمكن القيام به على النحو التالي:

 # لمس sample1 sample2 sample3 sample4 sample5

لتخزين بضعة أسطر من البيانات على الملف ، اكتب الأمر التالي فقط:

 # القط > عينة

عندما تضغط على المفتاح **Enter** ، ستجد المؤشر في وضع في انتظار السطر التالي بالنسبة لك لكتابة المحتوى الذي تريد تخزينه في ملف "عينة". فقط اكتب في السطر التالي:

هذا ملف عينة يحتوي على بعض نماذج النص.

بمجرد الانتهاء من ذلك، اضغط **على Ctrl + D** . هذا سيوفر المحتويات على الملف و يعيدك تلقائيًا إلى **#** المطالبة. الآن ، لعرض محتويات الملف "عينة" فقط اكتب الأمر كما يلي:

 # القط عينة

يجب أن يعرض هذا محتويات الملف كما هو موضح في اللقطة أدناه:

```
root@kali:~/Desktop# cat sample
This is a sample file containing some sample text.
root@kali:~/Desktop#
```

الشكل 3. 5

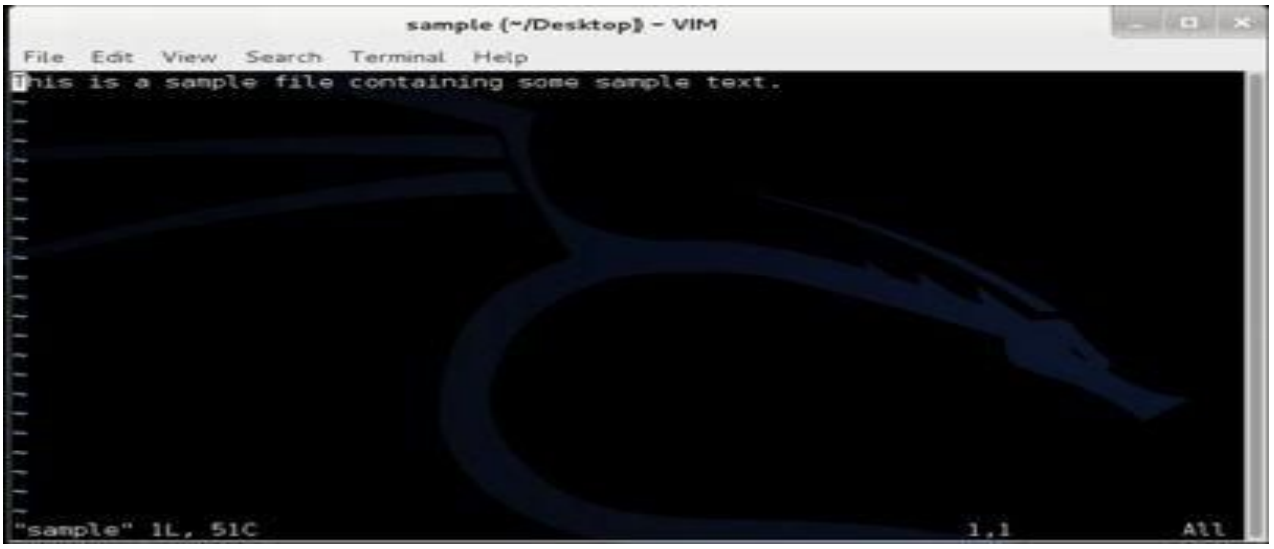
تحرير الملفات

لتحرير ملف معين يجب على المرء استخدام الأمر vi. من أجل تحرير ملف معين "عينة" الأمر كما يلي:

 # السادس عينة

عندما تكتب الأمر أعلاه وتضغط على مفتاح **Enter** ، سترى محتويات الملف "عينة" معروضة في نافذة vi Editor كما هو موضح في الشكل 3.6:

الشكل 3. 6

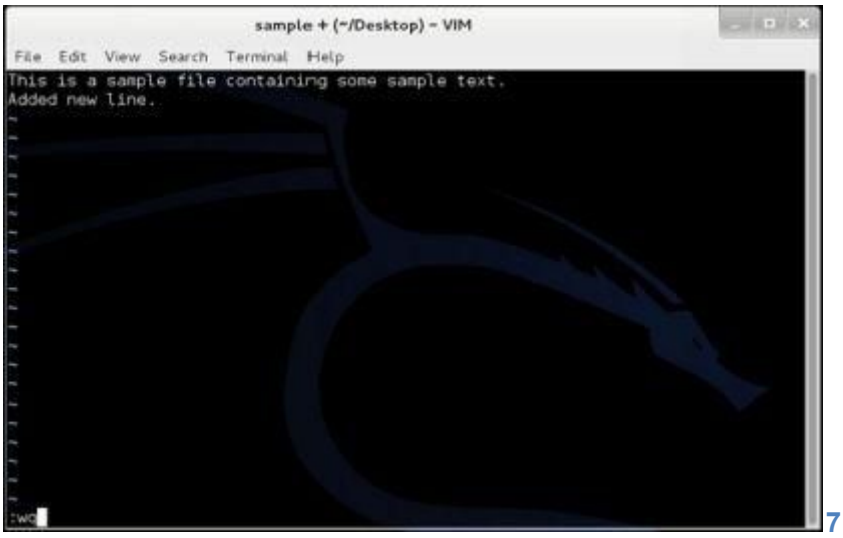


من أجل بدء عملية التحرير ، تحتاج إلى إدخال وضع **INSERT** عن طريق الضغط على المفتاح **ط** . الآن ، يجب أن يتحرك المؤشر بحرية داخل نافذة المحرر مما يتيح لك القيام بذلك التغييرات اللازمة على المحتوى. بمجرد الانتهاء من التحرير ، اضغط على مفتاح **Esc** .

الآن اكتب **: wq** كما هو موضح في اللقطة أدناه **واضغط** على **Enter** . و **ث** تقف على **الكتابة / حفظ**

و **q** لتقف على **الإقلاع** عن **التدخين** . سيؤدي هذا إلى حفظ التغييرات في ملفك ، وإغلاق محرر vi واتخاذ

عدت إلى موجه **#** . إذا كنت ترغب في الإقلاع دون حفظ التغييرات ، فاكتب فقط **: q!** بدلا من WQ : وضرب **أدخل** .



الشكل 3. 7

قائمة الملفات والدلائل

لعرض قائمة الملفات والدلائل ، فإن الأمر المستخدم هو **ls** . **ليرة سورية** هي لينكس أي ما يعادل الأمر **DIR** في ويندوز. لسرد الملفات والدلائل فقط اكتب بعد القيادة وضرب **أدخل** .

 # ليرة سورية

حذف الملفات والدلائل

في Linux ، يتم استخدام الأمر rm لحذف الملفات والدلائل. لحذف ملف استخدام القيادة كما هو موضح أدناه:

 # rm samplefile

عندما تضغط على **Enter** ، يُطلب منك تأكيد الحذف. فقط اكتب **y** واضغط على **Enter** مرة أخرى. يجب أن يكمل هذا حذف ملف "samplefile".

لحذف دليل وجميع محتوياته ، استخدم الأمر التالي:

 # rm- r sampledir

عندما تضغط على **Enter** ، يُطلب منك تأكيد الحذف. فقط اكتب **y** واضغط على **Enter** مرة أخرى. يجب أن يكمل هذا حذف دليل "sampledir" وجميع المحتويات داخله.

تسجيل الخروج

بمجرد الانتهاء من عملك ، يمكنك إغلاق نافذة المحطة الطرفية باستخدام **الخروج**

القيادة على النحو التالي:

 # الخروج

الاتصال بمضيف بعيد

لقد ناقشنا حتى الآن طرق تنفيذ الأوامر على كمبيوتر Linux الخاص بك.
ومع ذلك ، نظرًا لأن Linux هو نظام تشغيل متعدد المستخدمين ، يمكن للمستخدمين القيام بذلك
قم بالاتصال بجهاز كمبيوتر يعمل بنظام Linux حتى لو كان بعيدًا عن جهازه
موقعك. سنناقش في هذا القسم بعض الطرق التي يمكنك من خلالها الاتصال
إلى كمبيوتر بعيد وتنفيذ الأوامر على ذلك.
SSH (Secure Shell) هي الطريقة الأكثر شعبية وأسهل لإنجاز هذه المهمة. هذه
هو بروتوكول يسمح للعميل بالاتصال بمضيف بعيد وتنفيذ العمليات عليه.

SSH على لينكس

إذا كنت تستخدم جهاز كمبيوتر يعمل بنظام Linux ، فإن الاتصال بجهاز كمبيوتر آخر يعمل بنظام
Linux أمر سهل للغاية. مجرد
افتح نافذة *Terminal* واكتب الأمر التالي:

بناء جملة الأوامر: ssh اسم المستخدم @ المضيف

اسم المستخدم هنا يعني اسم المستخدم لحسابك على الكمبيوتر البعيد **والمضيف** يمكن أن يكون
على *اسم نطاق* مثل xyz.com أو *عنوان IP* من الكمبيوتر البعيد. الأتى
الأمثلة تجعل الأمر أكثر وضوحًا:

 # ssh john@xyz.com
 # ssh john@66.226.71.129
 # ssh root@xyz.com
 # ssh root@66.226.71.129

إذا كان المستخدم موجودًا على الجهاز المستهدف ، فسيتم إنشاء الاتصال وستكون كذلك
طلب إدخال *كلمة المرور* . بمجرد إدخال كلمة المرور وضرب **Enter** (كلمة المرور
سيتم الدخول غير مرئي لأسباب أمنية) ، سيتم منحك حق الوصول إلى الهدف
Linux Linux حيث يمكنك استخدام أي أمر على النحو الذي تمت مناقشته في
القسم السابق.

SSH على ويندوز

يمكنك الاتصال بجهاز Linux بعيد حتى لو كنت تستخدم جهاز كمبيوتر يعمل بنظام Windows.
يمكن القيام بذلك باستخدام برنامج مجاني صغير يسمى **PuTTY** وهو عميل SSH
ومحاكي محطة لنظام التشغيل Windows. يمكنك تنزيله من الرابط أدناه:

تنزيل المعجون: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

بعد التنزيل ، انقر نقرًا مزدوجًا على التطبيق **putty.exe** ، وأدخل **اسم المضيف** أو عنوان **IP**
عنوان الجهاز المستهدف ، حدد خيار **SSH** وانقر فوق الزر "فتح" كـ
هو مبين في لقطة أدناه:

الشكل 3. 8

يجب أن ينشئ هذا الاتصال بجهاز Linux البعيد ويطلب منك الدخول
و ودخول (اسم المستخدم) تليها *كلمة* (سوف تكون غير مرئية بسبب الوضع الأمني
الأسباب). بمجرد إدخال تفاصيل تسجيل الدخول الصحيحة ، ستتمكن من تنفيذها
الأوامر على الجهاز الهدف.

مراجع أخرى

لقد تناول هذا الفصل بعض المفاهيم الأساسية وأمثلة لينكس
نظام التشغيل وذلك لوضع الأساس لمزيد من التعلم الخاص بك. من أجل الظهور
باعتباره قراصنة محترف ، فمن الضروري أن يكون هناك فهم سليم على لينكس و
السيطرة على أوامرها. لهذا السبب ، لدي بعض التوصيات لمزيد من الخاص بك
المراجع.

فيما يلي قائمة ببعض مواقع الويب المفيدة لتوسيع معرفتك بنظام Linux:

لينكس الموقع الرسمي

تدريب مجاني على نظام Linux

قاعدة المعارف لينكس

لينكس التدريب البصري

فيما يلي قائمة ببعض الكتب العظيمة التي تستحق القراءة:

كيف يعمل لينكس

الفصل 4 - البرمجة

إن الحاجة إلى امتلاك المعرفة بالبرمجة كقراصنة هي واحدة من أكثر المواضيع التي نوقشت المواضيع في مجتمع القراصنة. على الرغم من توافر مجموعة متنوعة من الجاهزة الأدوات على الإنترنت قد قضت إلى حد كبير على الحاجة إلى البرمجة ، لا يزال الكثير منها يجادلون بأن امتلاك معرفة بالبرمجة يمكن أن يكون ميزة كبيرة للمتسلل.

لماذا البرمجة؟

في هذه المرحلة ، قد تسأل نفسك: "هل أحتاج إلى تعلم البرمجة؟"
من الصعب الإجابة عن السؤال لأن كل هذا يتوقف على الأهداف الفردية. في حين أن بعض الناس يكرهون
البرمجة وأحب التمسك بالأدوات المتاحة بسهولة ، وهناك عدد قليل من الذين يرغبون
لإعطاء البرمجة محاولة. تذكر أنه لا يزال من الممكن أن تكون متسللًا أخلاقيًا جيدًا إلى حد ما
دون معرفة أي برمجة على الإطلاق شريطة أن تتقن النظرية حقا
مفاهيم القرصنة ومعرفة كيفية استخدام الأدوات بشكل فعال.
ومع ذلك ، إذا كنت ترغب في أخذ نصيحتي الشخصية ، فما زلت أوصي بأن تتعلم بعضًا منها
أساسيات البرمجة بحيث يكون لديك فهم أفضل للحالات.
معرفة البرمجة يمكن أن توفر لك الفوائد المضافة التالية:
يمكنك رمز استغلال الخاص بك عن الثغرات المكتشفة حديثا دون الحاجة
لانتظار شخص ما لتطوير أداة.
يمكنك تعديل شفرة المصدر الحالية لتلبية الاحتياجات المخصصة الخاصة بك.
سيتم اعتبارك قراصنة أخلاقية النخبة في مجتمع القراصنة.
أخيرًا ، يمكنك تجنب الأشخاص الذين يصنفونك على أنه نص برمجي.

أين يجب أن تبدأ؟

إذا كنت جديد تمامًا في عالم برمجة الكمبيوتر ، فإن توصيتي هي

لتبدأ مع الأساسيات مثل تعلم لغات البرمجة مثل (Hyper **HTML** ، **C**
نص لغة توصيف النص)، **PHP** و **جافا سكريبت** . C هي لغة برمجة رائعة
للمبتدئين الذين يلعبون دورا بارزا في تأسيس الأساس لتعلم الآخرين
اللغات. فيما يلي بعض المواقع المتاحة مجانًا لتعلم لغة C:

جيم البرمجة

تعلم-C

C4Learn

بمجرد انتهائك من أساسيات C ، يصبح تعلم HTML و PHP و JavaScript
بسيطة الى حد كبير. فيما يلي مواقع الويب المتاحة مجانًا لتعلم HTML و PHP و
جافا سكريبت:

HTML دروس w3schools

PHP دروس w3schools

جافا سكريبت تعليمي w3schools

بالإضافة إلى الموارد المجانية ، يمكنك التفكير في شراء الكتب إذا كنت أكثر من ذلك
جادة في البرمجة. فيما يلي بعض الكتب العظيمة التي تستحق القراءة:

لغة البرمجة C

HTML و CSS: دليل المبتدئين

برمجة PHP

جافا سكريبت للمبتدئين

بمجرد اتخاذ القرار ، يمكنك البدء في تعلم وممارسة البرمجة ك
رحلة منفصلة دون الحاجة إلى التوقف عن متابعة دروس القرصنة الخاصة بك. على الأغلب
ظروف القرصنة الأخلاقية أو اختبار الاختراق مستقلة عن البرمجة و
وبالتالي يمكنك تعلمها في وقت واحد. إذا لم تكن مستعدًا بعد للبرمجة ، فأنت بذلك
قد يكمل قراءة هذا الكتاب ويقرر لاحقًا البرمجة.

الفصل 5 - البصمة

قبل أن تبدأ المتعة الحقيقية للقرصنة ، هناك خطوتان مهمتان في الذكاء

جمع عملية تعرف باسم *البصمة* و *المسح الضوئي* التي يتعين القيام بها من قبل القراصنة. هذه سوف الفصل التعامل مع الخطوة *الأولى* تسمى **البصمة** التي تعني ببساطة التجمع معلومات عن الهدف.

ما هو التأليف؟

تشير **البصمة** إلى عملية جمع المعلومات حول جهاز كمبيوتر معين نظام أو بيئة شبكة والشركة التي ينتمي إليها. هذا هو التحضيري مرحلة للمتسلل حيث يجمع أكبر قدر من المعلومات حتى يتمكن من إيجاد طرق ل تدخل في الهدف. يمكن أن تكشف البصمة عن نقاط الضعف في النظام المستهدف و تحسين الطرق التي يمكن استغلالها بها.

يجب القيام بالبصمة بطريقة بطيئة ومنهجية حيث يقضي القراصنة ٪90 من وقته في إعداد ملف تعريف أمان الهدف و 10٪ فقط شن الهجوم. يمكن أن يساعد تطبيق Footprinting في تحديد موقع القراصنة على نوع الهجوم هذا هو الأكثر ملاءمة للهدف.

منهج جمع المعلومات

لنفترض أنه إذا قرر أحد المتسللين اقتحام شركة مستهدفة ، فيمكنه القيام بذلك فقط بعد ذلك وضع مخطط للهدف وتقييم مواطن الضعف المحتملة. بناء على هذا المعلومات ، يمكن للمتسلل تنفيذ هجمات محتملة مثل اقتحام الشركة قاعدة البيانات ، اختراق موقعها على شبكة الإنترنت أو التسبب في الحرمان من الخدمة. وفيما يلي بعض من أنواع مختلفة من المعلومات التي يمكن للقراصنة جمعها قبل القيام في الواقع هجوم:

الحصول على معلومات اسم المجال

معلومات أساسية متنوعة حول موقع الويب الهدف (اسم المجال) مثل الاسم من لها *مالك* و *المسجل* ، *تاريخ تسجيلها* ، *تاريخ انتهاء الصلاحية* ، *خوادم الأسماء* المرتبطة، تفاصيل الاتصال المرتبطة به مثل *البريد الإلكتروني* ، *الهاتف* و *عنوان* يمكن العثور بها

إجراء **بحث Whois** . فيما يلي بعض المواقع الشعبية التي تتواجد فيها

يمكن إجراء بحث Whois على أي مجال للكشف عن معلومات الخلفية الخاصة به:

/http://www.whois.com/whois

/https://who.is

/http://whois.domaintools.com

أجرى تطبيق Whois Lookup عينة على "facebook.com" على **الموقع**

/http://www.whois.com/whois

يظهر المعلومات التالية:

الشكل 5. 1

العثور على عنوان IP وموفر الاستضافة

يمكن أن تكون المعلومات مثل عنوان IP الخاص بموقع الويب ومزود الاستضافة الخاص به للغاية

مهم. يمكن اكتشاف ذلك بسهولة باستخدام الموقع التالي:

/WhoIsHostingThis: http://www.whoishostingthis.com

ما عليك سوى زيارة الموقع أعلاه وإدخال اسم النطاق الذي تختاره للحصول على عنوان IP الخاص به

العنوان وكذلك اسم مزود الاستضافة الخاص به كما هو موضح أدناه.

الشكل 5. 2

كما ترون من اللقطة أعلاه ، يكشف استعلام على "facebook.com" عن عنوان *IP* الخاص به *العنوان* ، مزود *الاستضافة* وأيضًا خوادم *الأسماء* المرتبطة به.

العثور على عنوان IP الموقع

إن معرفة الموقع الفعلي لعنوان IP بسيط للغاية. فقط قم بزيارة التالي

موقع الويب وإدخال عنوان IP الهدف للكشف عن موقعه الفعلي:

IP2Location: http://www.ip2location.com/demo

لقطة من الاستعلام عينة لعنوان IP **173.252.120.6** على *ip2location.com* الموقع

هو مبين أدناه:

IP Address	173.252.120.6
Location	UNITED STATES, NORTH CAROLINA, FOREST CITY
Latitude & Longitude	35.334010, -81.865100 (35°20'2"N 81°51'54"W)
ISP	FACEBOOK INC
Local Time	10 Oct, 2014 04:53 AM (UTC -04:00)
Domain	FACEBOOK.COM
Net Speed	(COMP) Company/T1
IDD & Area Code	(1) 828
ZIP Code	28043
Weather Station	FOREST CITY (USNC0241)

الشكل 5. 3

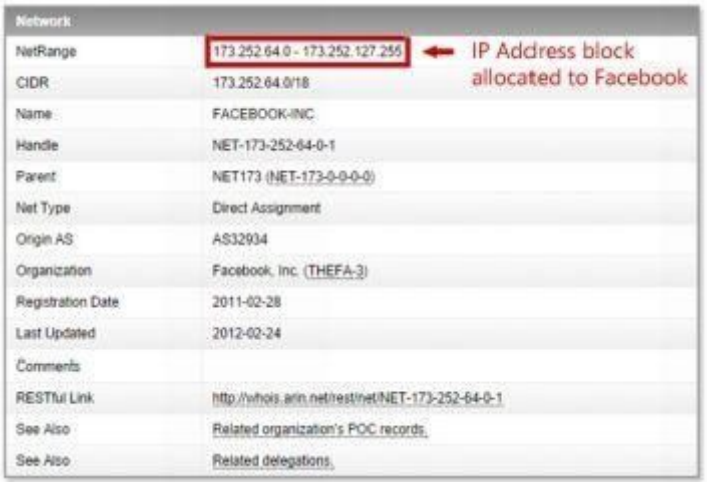
العثور على نطاق عنوان IP

بينما قد تحتوي المواقع الصغيرة على عنوان IP واحد ، فإن اللاعبين الكبار مثل Google و Facebook

و Microsoft لديها مجموعة من عناوين IP المخصصة لشركتهم للاستضافة مواقع وخوادم إضافية هذه المجموعة من المعلومات يمكن الحصول عليها من الموقع الرسمي **للسجل الأمريكي لأرقام الإنترنت (ARIN)** . عنوان URL لـ موقع ARIN مدرج أدناه:

موقع أرين: **https://www.arin.net/**

تفضل بزيارة عنوان URL أعلاه وأدخل *عنوان IP* لأي موقع ويب محدد في **" البحث "** تم العثور على مربع **Whois** في الركن الأيمن العلوي من صفحة الويب. هنا لقطة تظهر نتائج استعلام **نموذجي تم إجراؤه على** عنوان IP الخاص بـ **173.252.120.6** Facebook .



الشكل 5. 4

متتبع

Traceroute هي أداة تشخيص شبكة لتحديد المسار الفعلي (المسار) الذي المعلومات (الحزم) تأخذ للسفر من المصدر إلى الوجهة. المصدر سيكون لديك الكمبيوتر الخاص يسمى *المضيف المحلي* . يمكن أن تكون الوجهة أي مضيف أو خادم محلي شبكة أو الإنترنت.

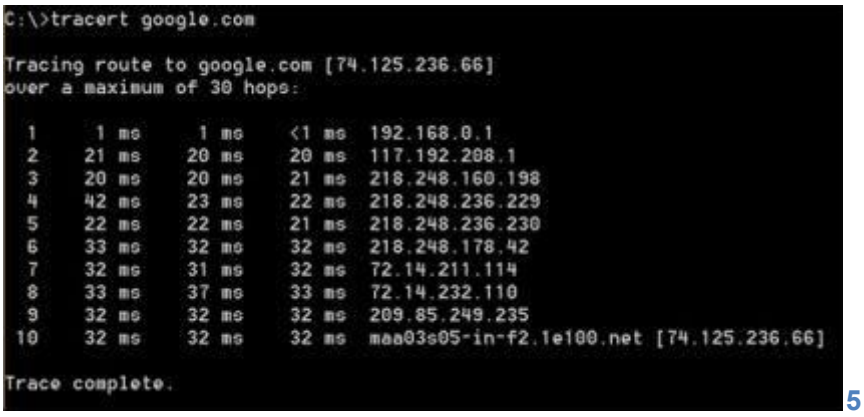
أداة التتبع متاحة على كل من Windows و Linux. بناء جملة الأمر لـ ويندوز هو على النحو التالي:

ترسرت الهدف المجال أو IP

بناء جملة الأمر لنظام Linux كما يلي:

تتبع الهدف المجال أو IP

عادة ، لن يتم نقل المعلومات من كمبيوتر إلى آخر في
قفزة واحدة. أنها تنطوي على سلسلة من العديد من أجهزة الكمبيوتر وأجهزة الشبكة تسمى *القفزات* إلى
نقل المعلومات من المصدر إلى الوجهة. يحدد Traceroute كل قفزة في تلك القائمة
ومقدار الوقت الذي يستغرقه السفر من قفزة إلى أخرى. لقطة من
يظهر أدناه تتبع "google.com" باستخدام كمبيوتر يعمل بنظام Windows:



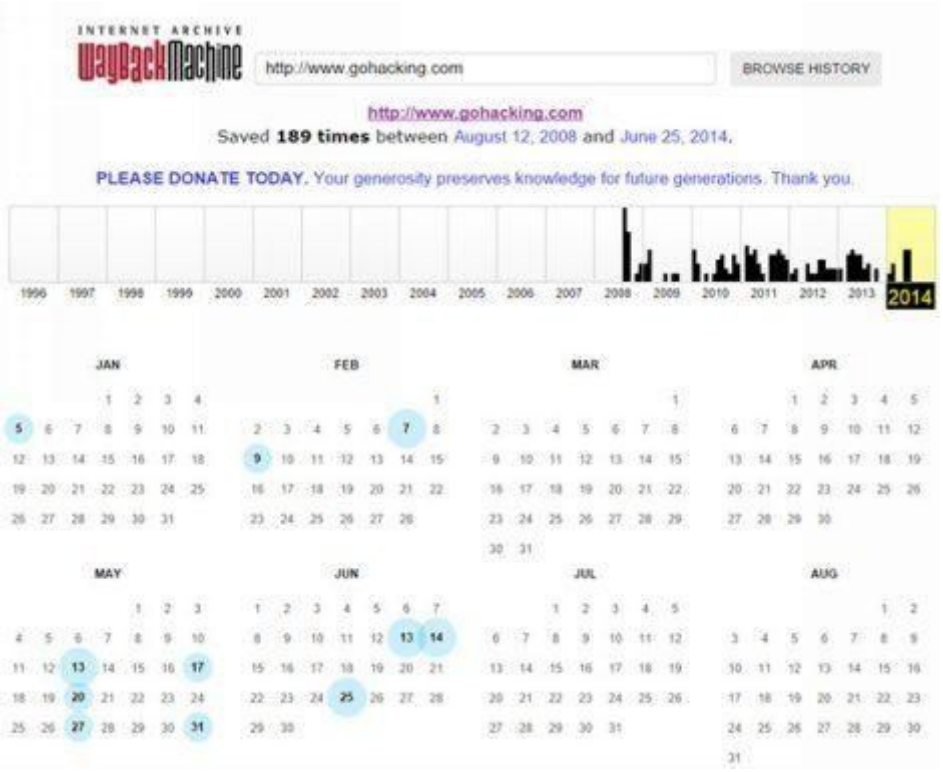
الشكل 5. 5

كما هو موضح في اللقطة أعلاه ، تحدد أداة التتبع جميع القفزات الموجودة في
المسار الذي تم عبوره بواسطة الحزم من المصدر إلى الوجهة. هنا **192.168.0.1** هو IP الخاص
و **117.192.208.1** هو عنوان IP العام للمصدر (جهاز الكمبيوتر الخاص بي).
74.125.236.66 هو
عنوان IP الوجهة (خادم جوجل). جميع عناوين IP المتبقية هو مبين في
ينتمي المصدر والوجهة إلى أجهزة الكمبيوتر التي تساعد في حمل المعلومات.

الحصول على أرشيف للموقع الهدف

يتيح لك الوصول إلى أرشيف الموقع الإلكتروني المستهدف معرفة كيف كان موقع الويب
خلال وقت إطلاقه وكيف تطورت وتغيرت مع مرور الوقت. سوف تفعلها
انظر أيضًا جميع التحديثات التي أجريت على الموقع ، بما في ذلك طبيعة التحديثات و
تواريخ. يمكنك استخدام أداة **WayBackMachine** للوصول إلى هذه المعلومات.
/WayBackMachine: http://archive.org/web

فقط استخدم الرابط أعلاه لزيارة موقع WayBackMachine واكتب عنوان URL الخاص بـ موقع الهدف. يجب أن تحصل على قائمة بأرشيفات الموقع المدرجة في الشهر بشهر وعلى أساس سنوي كما هو موضح في لقطة أدناه:



الشكل 5. 6

التدابير المضادة

أتمنى أن تكون على دراية الآن بالعديد من الطرق التي يمكنك تنفيذها بنجاح البصمة لجمع مجموعة كبيرة من المعلومات حول الهدف. بمجرد الانتهاء من ذلك تنظيم البيانات التي حصلت عليها من خلال عملية البصمة ، يمكنك الجلوس العودة وتحليلها لمعرفة نقاط الضعف المحتملة في أي من التقنيات المستخدمة في الموقع.

غالبًا ما يفشل العديد من مسؤولي الشبكة في تحديث البرامج والبرامج النصية الضعيفة قيد التشغيل على الخادم الخاص بهم إلى أحدث إصدار. هذا يمكن أن يفتح فرصة للمتسلل لاستغلالها والوصول إلى النظام. لذلك ، من المهم تحديد وتصحيح القائمة نقاط الضعف على أساس منتظم ، وكذلك الحد من كمية المعلومات الحساسة التي تسربت

إلى شبكة الإنترنت.

الفصل 6 - المسح

بعد جمع مجموعة متنوعة من المعلومات حول الهدف من خلال *البصمة* ، حان الوقت ل
الانتقال إلى الخطوة التالية تسمى ***المسح*** . المسح هو الخطوة الثانية في الاستخبارات
عملية جمع المتسللين حيث معلومات حول عناوين IP محددة ، والتشغيل
أنظمة ، يمكن الحصول على بنيتها والخدمات التي تعمل على أجهزة الكمبيوتر. مختلف
البصمة التي تجمع المعلومات بشكل سلبي من مصادر خارجية مختلفة ،
ينطوي *المسح الضوئي* على المشاركة النشطة مع الهدف للحصول على المعلومات.

اكتشاف الأنظمة الحية

الخطوة الأولى في عملية المسح هي تحديد ما إذا كان الهدف على قيد الحياة أم لا.
يمكن القيام بذلك باستخدام أداة **ping** المتوفرة بسهولة على كل من Windows و Linux
أجهزة الكمبيوتر. فقط افتح موجه الأوامر إذا كنت تستخدم نظام Windows أو نافذة المحطة
الطرفية إذا
أنت على Linux واكتب ping متبوعًا بعنوان IP المستهدف كما هو موضح أدناه:

```
ping 173.252.120.6
```

إذا كان الهدف على قيد الحياة وعبر الإنترنت ، فيجب أن تحصل على رد من الهدف أو إذا كان
الهدف هو
ليس على قيد الحياة ، سوف تحصل على رد يقول "لا يمكن العثور على طلب ping للمضيف".

غاضب IP الماسح الضوئي

يمكنك حتى تنفيذ الأمر ping لمجموعة من عناوين IP مرة واحدة باستخدام أداة لطيفة تسمى "
"Angry IP
الماسح الضوئي". إنها أداة ماسحة شبكة مفتوحة المصدر معبأة بالعديد من الأجهزة
ميزات مفيدة.
كل ما عليك القيام به هو إدخال *بدء* و *إنهاء* IP من النطاق الذي تريد
بينغ وانقر على زر "ابدأ" كما هو موضح في الشكل أدناه. هذا يجب أن أقول لك

أي من تلك IP المتاحة والتي ليست كذلك.

الشكل 6. 1

يتوفر Angry IP Scanner لكل من أنظمة تشغيل Windows و Linux ويمكن أن يكون كذلك

تم تنزيله من الرابط أدناه:

Angry IP Scanner: http://angryip.org/download/

أداة Ping عبر الإنترنت

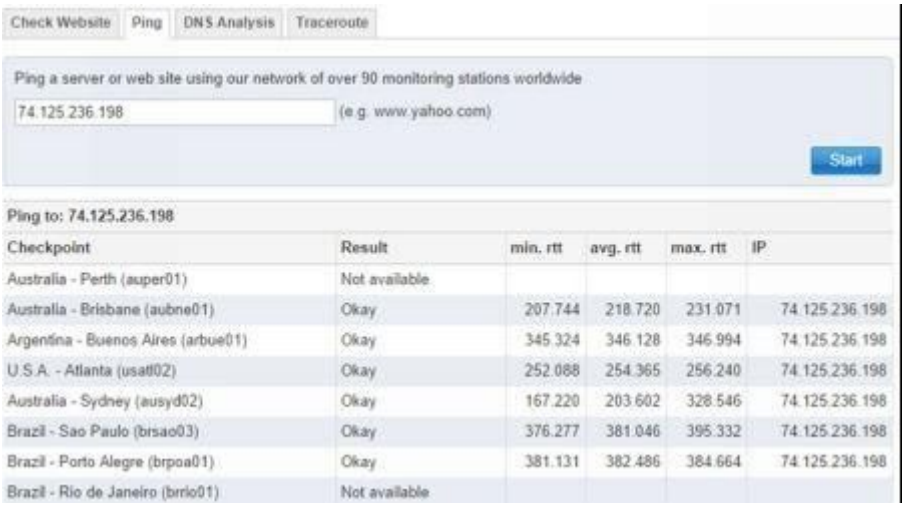
إذا كنت ترغب في تنفيذ الأمر ping للهدف باستخدام كمبيوتر جهة خارجية بدلاً من جهاز الكمبيوتر الخاص بك ، يمكنك ذلك

قم بذلك باستخدام أدوات عبر الإنترنت مثل **Just-Ping** التي تدق الهدف من 90 جغرافيًا مختلفًا المواقع في جميع أنحاء العالم. يمكنك الوصول إلى أداة Just-Ping من الرابط أدناه:

فقط بينغ: http://cloudmonitor.ca.com/en/ping.php

يوضح الشكل التالي 6.2 في الصفحة التالية عينة اختبار ping تم إجراؤها باستخدام

مجرد أداة **بينغ** :



الشكل 6. 2

أنواع الفحص

الآن ، دعونا نناقش واحدًا تلو الآخر بعض أنواع المسح المختلفة الموجودة.

ميناء المسح الضوئي

يتضمن **فحص المنفذ** إرسال سلسلة من الرسائل إلى الكمبيوتر الهدف لاكتشافها
أنواع خدمات الشبكة التي تعمل عليها. منذ يرتبط كل خدمة بئر
رقم المنفذ المعروف ، سيؤدي إجراء فحص المنفذ على الهدف إلى الكشف عن المنافذ الموجودة
افتح. لذلك ، عندما يقال إن المنفذ مفتوحًا ، يُقال إن الخدمة المرتبطة به نشطة
والجري ، وبالتالي فتح الفرصة للمهاجم لاقتحامها.
على سبيل المثال ، إذا أظهر فحص المنفذ على الهدف أن المنفذ 80 والمنفذ 25 مفتوحان ، فذلك
يعني أن
يعني أن الكمبيوتر الهدف به خدمة HTTP (خادم الويب) وخدمة SMTP (البريد الإلكتروني)
الخدمة) يعمل عليها على التوالي.

مسح الشبكة

يعد **فحص الشبكة** إجراءً لتحديد المضيفين النشطين على الشبكة المستهدفة أيضًا
لغرض مهاجمتهم أو لتقييم الأمن. بهذه الطريقة سيكون
ممكن للمتسلل لعمل قائمة بالمضيفين الضعفاء للهجوم المباشر أو لاستخدامهم
بشكل غير مباشر لمهاجمة المضيفين الآخرين.

مسح الثغرات الأمنية

يشمل **مسح الثغرات الأمنية** استخدام الأدوات الآلية المعروفة باسم *الثغرة الأمنية* *الماسحات الضوئية* لتحديد نقاط الضعف الأمنية لأنظمة الكمبيوتر في الشبكة بشكل استباقي.
ستقوم هذه الأدوات بمسح الهدف لمعرفة وجود عيوب معروفة موجودة
عرضة للاستغلال.

أدوات للمسح

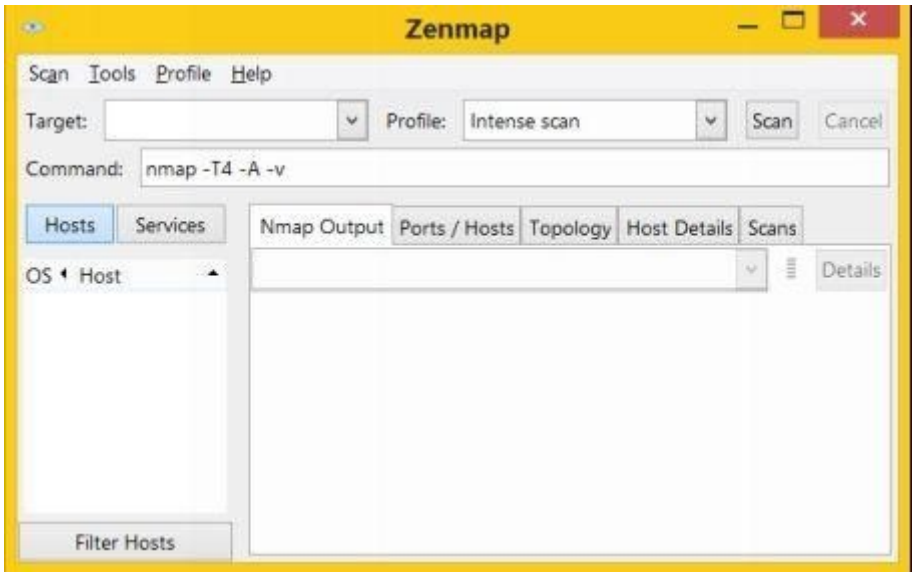
فيما يلي بعض الأدوات الشائعة المتاحة للمسح الضوئي:

NMAP

Nmap هي أداة مفتوحة المصدر مشهورة لاكتشاف الشبكة وتدقيق الأمان
يعمل على منصات مختلفة مثل Linux و Windows و Mac. انها تأتي أساسا في النموذج
واجهة سطر الأوامر ؛ ومع ذلك ، لتسهيل سهولة الاستخدام وهو متاح أيضا في
شكل واجهة المستخدم الرسومية يسمى **Zenmap** . بالنسبة لأجهزة Windows ، يمكنك تثبيت
"المثبت الذاتي"
إصدار *Nmap* الذي يأتي بتنسيق ".exe". رابط التحميل لنفسه في
المتاحة أدناه:

تنزيل Nmap: http://nmap.org/download.html

بعد تثبيت الأداة ، قم بتشغيل اختصار سطح المكتب لفتح نافذة *Zenmap* التي
عادة ما يبدو كما هو موضح أدناه:



الشكل 3. 6

"الهدف" احتياجات مربع لتكون مليئة الهدف *عنوان IP* أو *اسم النطاق* الذي تريد إجراء الفحص. كما يأتي قبل تحميلها مع 10 *ملامح المسح الضوئي* المختلفة التي يمكنك الاختيار من بينها.

مسح مكثف

يجب أن يكون نوع المسح سريعًا بشكل معقول حيث أنه يقوم بمسح منافذ TCP فقط. بالإضافة إلى ذلك

يجعل محاولة للكشف عن نوع نظام التشغيل والخدمات المختلفة وأرقام إصداراتها تعمل على الجهاز الهدف.

مسح مكثف بلاس UDP

إنه نفس *الفحص المكثف* كما هو موضح أعلاه ولكنه يشمل أيضًا مسح منافذ UDP.

مسح مكثف ، جميع منافذ TCP

على عكس *الفحص المكثف* العادي الذي يمسح فقط قائمة من 1000 منفذ شائع ، *يفحص* " *الفحص المكثف* ، جميع *منافذ TCP* " جميع المنافذ المتاحة 65535.

مسح مكثف ، لا بينغ

يستثني هذا الخيار تنفيذ الأمر ping للهدف من *الفحص المكثف* . يمكنك استخدام هذا الخيار عندما تعلم بالفعل أن الهدف متروك أو يقوم بحظر طلبات ping.

بينغ المسح الضوئي

سيؤدي هذا الخيار إلى تنفيذ الأمر ping للهدف فقط ولكنه لا يؤدي عملية مسح المنفذ من أي نوع.

مسح سريع

يقوم بمسح أسرع من *الفحص المكثف* عن طريق تحديد عدد منافذ TCP الممسوحة ضوئيًا على أعلى 100 منافذ TCP الأكثر شيوعا.

المسح السريع بلس

يضيف *Quick Scan plus* الكشف عن نظام التشغيل وقليلًا من ميزات الكشف عن الإصدار إلى *Quick scan* .

تتبع سريع

سيوضح لك هذا الخيار المسار الذي تتبعه الحزم للوصول إلى الهدف بدءًا من المضيف المحلي (المصدر أو الكمبيوتر الخاص بك).

مسح منتظم

سيؤدي ذلك إلى فحص منفذ ping و TCP لـ 1000 منفذ افتراضي على الهدف.

مسح بطيء شامل

سيحاول هذا الفحص جميع الخيارات الممكنة للكشف عن أكبر قدر ممكن من المعلومات حول استهداف. يستخدم ثلاثة بروتوكولات مختلفة: TCP و UDP و SCTP من أجل اكتشاف المضيفين.

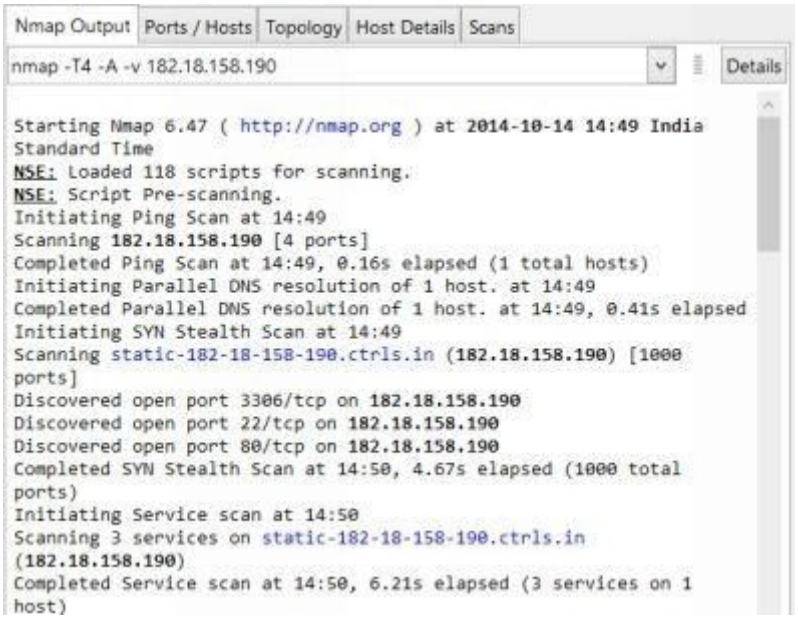
من بين جميع خيارات المسح العشرة ، أعتقد أن *الفحص المكثف* مناسب لأقصى درجة الظروف. ما عليك سوى ملء مربع "الهدف" ، وحدد ملف "الفحص المكثف" واضغط على "المسح"

زر. دعونا الآن نحلل ناتج نتيجة Nmap عن طريق تشغيله على هدف عينة.

بعد اكتمال الفحص ، تعرض علامة التبويب "إخراج Nmap" المخرجات الأولية لجميع عمليات المسح

عمليات مثل *التاريخ والوقت* الذي تم تنفيذه ، والنتائج من فحص *ping* ،

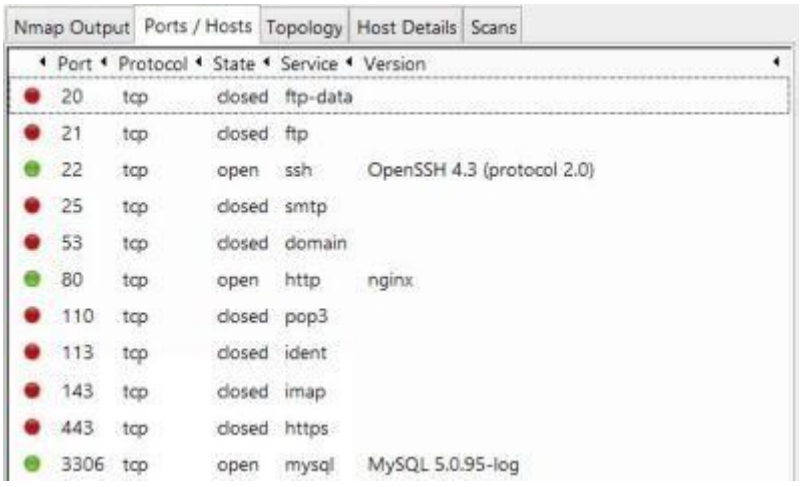
اكتشاف *المنافذ المفتوحة* ، *OS الهدف* و *النتائج* متتبع كما هو مبين أدناه:



الشكل 6. 4

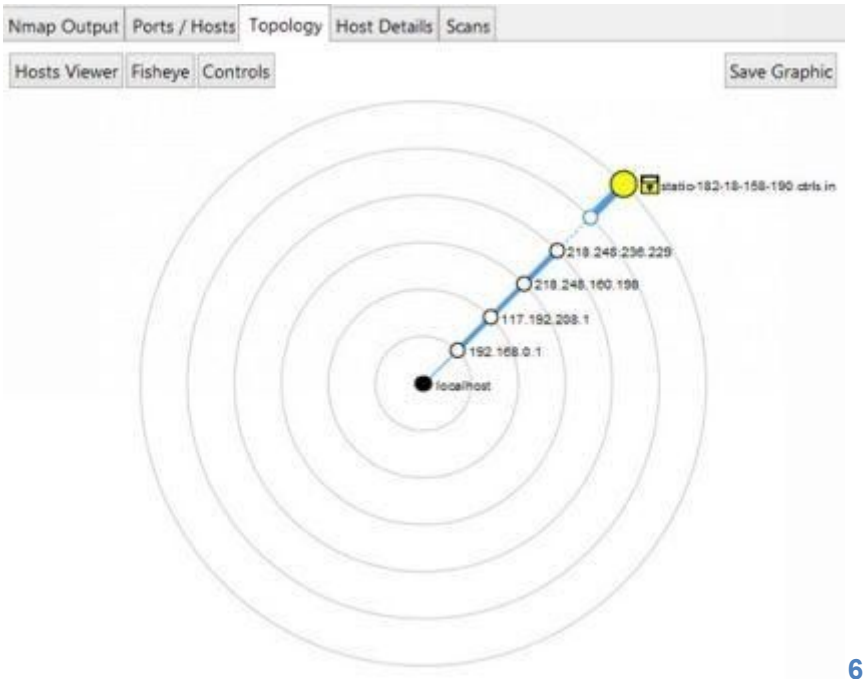
تقوم علامات التبويب الأخرى بتقسيم النتائج نفسها إلى طريقة منظمة لعرضها بطريقة أ أكثر سهولة الاستعمال بطريقة واجهة المستخدم الرسومية. تعرض علامة التبويب "الموانئ / المضيفين" قائمة

المنافذ المكتشفة ، وحالتها فيما إذا كانت مغلقة أم مفتوحة ، البروتوكول المرتبط والخدمات التي تعمل عليها. ويرد لقطة من عينة الإخراج أدناه:



الشكل 6. 5

تعرض علامة التبويب "الطوبولوجيا" نتيجة أمر *التتبع* بطريقة رسومية تظهر كل *قفزة* المشاركة في المسار.



الشكل 6. 6

تعرض علامة التبويب "تفاصيل المضيف" حالة المضيف واسمه وعدد المنافذ الممسوحة ضوئيًا ، مدة التشغيل ، وقت التمهيد الأخير ، نوع نظام التشغيل الذي يشتمل على رقم الإصدار الخاص به و العديد من التفاصيل الأخرى كما هو مبين في الشكل أدناه:

الشكل 6. 7

NetScanTools Pro

NetScanTools Pro هو برنامج رائع آخر لنظام Windows يحتوي على مجموعة قوية من

أكثر من 50 من أدوات الشبكة بما في ذلك الطرق الآلية واليدوية لاسترداد المعلومات من الهدف.

الشكل 8. 6

يمكنك استخدام "الأدوات الآلية" لأداء فحص المنفذ بسرعة والاستيلاء على الحيوية معلومات حول الهدف ، مثل سجلات DNS ، وبيانات Whois ، و Traceroute ، كل التفاصيل من

مكان واحد. من ناحية أخرى ، يحتوي قسم "الأدوات اليدوية" على أدوات فردية وضعت خصيصا لتوفير المزيد من السيطرة في عملية المسح للمستخدمين المتقدمين.

أدوات عبر الإنترنت

يمكنك أيضًا استخدام الأدوات المتوفرة عبر الإنترنت لإجراء فحص المنافذ واكتشافها معلومات عن الهدف. فيما يلي بعض الروابط المفيدة لشبكة الإنترنت

الأدوات التي تستحق الدراسة:

PenTest-أدوات

YouGetSignal

أدوات شعبية أخرى

فيما يلي قائمة ببعض الأدوات الشائعة الأخرى التي قد ترغب في استكشافها:

SuperScan

ipEye

نظام التشغيل بالإصبع

بصمة نظام التشغيل هي عملية الكشف عن نظام التشغيل للمضيف الهدف أو شبكة الاتصال. فيما يلي بعض أساليب بصمة نظام التشغيل الشائعة الاستخدام.

البصمات النشطة

البصمة النشطة هي الطريقة التي يتم بها إرسال الحزم المعدة خصيصًا إلى ويلاحظ النظام المستهدف والاستجابة. منذ أنظمة التشغيل المختلفة تستجيب ل الحزم المصدر بطرق مختلفة ، يمكن تحليل هذه الاستجابة لتحديد الهدف OS.

أحد الأمثلة البسيطة هو استخدام *أداة Nmap* كما تمت مناقشته في القسم السابق الذي يستخدم طريقة *البصمات النشطة* لتحديد نظام التشغيل الهدف.

الاستيلاء على لافتة

وتسمى طريقة أخرى شائعة الاستخدام لبصمات الأصابع النشطة **انتزاع الشعارات** . هذه يمكن القيام به باستخدام أداة بسيطة تسمى Telnet . **telnet** متاح بسهولة على نظام التشغيل Windows XP

والإصدارات السابقة. بالنسبة إلى أجهزة Windows Vista و 7 و 8 ، تحتاج إلى تنشيط بنيت أداة التلنت قبل أن تتمكن من استخدامه. ابحث فقط عن "كيفية تمكين التلنت على النوافذ" على Google للعثور على إرشادات مفصلة لتمكين عميل telnet على جهاز الكمبيوتر الخاص بك.

بمجرد قيامك بتمكين عميل telnet على جهاز الكمبيوتر الخاص بك ، تصبح عملية التقاط الشعارات جميلة

بسيط. فقط اكتب الأمر التالي في موجه الأوامر للكشف عن التشغيل

نظام يعمل على الهدف:

الهدف **telnet** المجال أو IP 80

سيؤدي هذا إلى فتح الاتصال مع الهدف. اكتب النص التالي تمامًا كما يلي **HEAD / HTTP / 1.1** واضغط على مفتاح **Enter** مرتين. هذا يجب أن يجلب النتائج حيث يوجد إمكانية ذكر نظام التشغيل المستهدف كما هو موضح في الشكل أدناه.

الشكل 6. 9

البصمة السلبية

البصمة السلبية هي تقنية تستخدم طرقًا غير مباشرة لتحديد الهدف

نظام التشغيل. على عكس البصمات النشطة التي ترسل الحزم إلى الهدف ، السلبي البصمة من ناحية أخرى تستخدم تقنية استنشاق لتحليل الشبكة المستهدفة حركة المرور وتحديد نظام التشغيل. إنه أقل دقة من البصمة النشطة.

يمكنك استخدام أدوات عبر الإنترنت مثل **Netcraft** لإجراء البصمات السلبية.

أداة **Netcraft:** http://toolbar.netcraft.com/site_report

ما عليك سوى زيارة الرابط أعلاه للوصول إلى أداة Netcraft وإدخال المجال المستهدف أو عنوان IP

عنوان لمعرفة نظام التشغيل المستهدف ، نقاط الضعف المحتملة ، تصنيف المخاطر و معلومات مفيدة أخرى.

إبراز هويتك

إخفاء الهوية الحقيقية لك أثناء عمليات مثل البصمة والمسح الضوئي أمر بالغ الأهمية ضروري كثيرًا حيث توجد فرصة حقيقية لاستهداف الهدف إليك. قليلا من ال الطرق التي يمكنك استخدامها لإخفاء هويتك موضحة أدناه.

باستخدام وكيل

يمكن استخدام خادم وكيل لإخفاء عنوان IP الحقيقي الخاص بك أثناء إجراء المسح الضوئي و محاولات اختراق على الهدف. نظرًا لأن عنوان IP يروي كل شيء عنك ، فإنه يخفيه باستخدام وكيل يمكن أن يكون فعالا للغاية في إخفاء أصلك.

على الرغم من توفر أنواع مختلفة من الوكلاء ، إلا أنني أوصي باستخدام VPN خدمة الوكيل لإخفاء عنوان IP الخاص بك. خدمات VPN سريعة وتوفر طرقًا موثوقة لا فقط لإخفاء عنوان IP الخاص بك ولكن أيضًا لحماية بياناتك وهويتك عبر الإنترنت.

فيما يلي بعض خدمات VPN الشائعة التي يمكنك تجربتها:

وكيل HideMyAss

وكيل VyprVPN

بدلاً من ذلك ، يمكنك أيضًا استخدام سلسلة من الوكلاء العامين لزيادة تعزيز التخفي العملية باستخدام أدوات مجانية مثل **Proxifier** و **SocksChain**. يرجى ملاحظة أن استخدام الجمهور

يمكن أن يبطئ الوكلاء سرعتك ومن ثم ينصح الوكلاء VPN بشكل أكبر
أفضل خدمة الغرض.
الطريقة الأخرى لإخفاء هويتك هي استخدام أدوات عبر الإنترنت لإجراء اختبار الاتصال والمسح الضوئي
استهداف. أثناء استخدام الأدوات عبر الإنترنت ، يكون عنوان IP الخاص بالخادم الذي يستضيف الأدوات هو
يتعرض للهدف وليس الذي ينتمي إلى المهاجم الفعلي.
بمجرد قيامك بجمع قائمة طويلة من المعلومات حول الهدف من خلال *البصمة*
و *المسح* ، فقد حان الوقت لتحليلها لمواطن الضعف المحتملة في التشغيل
النظام أو التقنيات أو الخدمات التي تعمل على الهدف. يمكنك الاستفادة مما يلي
مواقع الويب للعثور على معلومات حول أحدث مواطن الضعف والاستغلال:

1. http://www.securiteam.com
2. http://www.zone-h.org
3. http://www.securityfocus.com
4. http://www.packetstormsecurity.com

---

5. http://www.cybercrime.gov

التدابير المضادة

لقد تعلمت حتى الآن تقنيات مسح مختلفة لاكتشاف معلومات حول
استهداف. الآن دعونا نلقي نظرة على بعض التدابير المضادة التي يمكن للمرء اتخاذها لمنع حيوية المعلومات من تسرب في أيدي المهاجم.
تكوين خوادم الويب لمنع تسرب المعلومات.
تعطيل الخدمات والبروتوكولات غير المرغوب فيها / غير المستخدمة.
استخدم نظام كشف التسلل (IDS) للكشف عن عمليات فحص المنفذ وتسجيلها.

الفصل 7 - اختراق كلمات المرور

القرصنة هي واحدة من أكثر المواضيع سخونة والأكثر مناقشة على نطاق واسع في مجال

قرصنة الكمبيوتر. في عالم اليوم ، تلعب كلمات المرور وحدها دورًا رئيسيًا في تحديد أمان خادم الويب أو أي نظام كمبيوتر آخر. نتيجة لذلك ، اختراق كلمة المرور هي واحدة من أسهل وأحيانًا الطريقة الوحيدة للوصول إلى النظام. في هذا الفصل ، سيتم تعريفك على تقنيات القرصنة كلمة المرور المختلفة التي كثيرا ما المستخدمة في صناعة القرصنة.

بادئ ذي بدء ، سوف أخبركم ببعض التقنيات الواضحة والبسيطة والفعالة اختراق كلمات المرور:

1. **الهندسة الاجتماعية:** هذا النوع من التقنية ينطوي على التلاعب النفسي الناس في أداء الإجراءات التي تؤدي إلى الكشف عن سرية بهم معلومات. بمعنى آخر ، الهندسة الاجتماعية هي مجرد خدعة يلعبها القراصنة كسب ثقة الناس حتى يكشفوا عن كلمة المرور بأنفسهم.

السيناريو 1: قد يقوم المتسلل باستدعاء الشخص المستهدف بالتظاهر بنفسه كبنك المسؤول واطلب منه تأكيد كلمة المرور الخاصة به معتبرا أن هذا يجب أن يتم كجزء من ذلك من برنامج التحقق المستمر. في معظم الحالات ، يكون الشخص المستهدف على الطرف الآخر يعتقد هذا ويكشف كلمة المرور الخاصة به للمتسلل.

السيناريو 2: لتجنب الشك ، بدلاً من الطلب مباشرة من الضحية كشف كلمة المرور ، قد يحصل المتسلل على معلومات حيوية أخرى مثل "التاريخ" الميلاد "،" مكان الميلاد "،" تفاصيل المدرسة الثانوية "وما إلى ذلك من الشخص المستهدف. عن طريق

هذه التفاصيل ، يمكن للمتسلل بسهولة إعادة تعيين كلمة المرور والحصول على وصول غير مصرح به.

على الرغم من أن الهندسة الاجتماعية تبدو بسيطة ، فقد ثبت أن معظم الناس سوف تقع بسهولة ضحية لهذا الهجوم. نقص الوعي بين الناس هو السبب الرئيسي للنجاح وراء هذه الخدعة.

2. **التخمين:** بما أنه من المعروف أن معظم الناس يسهل عليهم تذكر كلمات مثل كلماتهم "اسم حيوان أليف" ، "رقم الهاتف" ، "اسم الطفل" وما إلى ذلك ككلمات المرور الخاصة بهم ، غالبًا ما تكون

ممكن للقراصنة لتخمين كلمة المرور بسهولة.

3. **تصفح الكتف:** هو فعل للتجسس على لوحة المفاتيح واحد من وراء الكتفين كشخص يكتب كلمة مروره. هذه التقنية تعمل بشكل جيد خاصة في المناطق المزدحمة مثل مقاهي الإنترنت وأجهزة الصراف الآلي حيث عادة ما يكون الناس غير مدركين ما يحدث وراء أكتافهم.

بعد فهم بعض تقنيات اختراق كلمة المرور البسيطة ، حان الوقت للتحرك إلى المستوى التالي. الآن ، دعونا نقفز إلى بعض الطرق الخطيرة التي يستخدمها المتسللون كلمات السر الكراك:

الهجوم الإجباري

A **القاموس الهجوم** هو نوع من كلمة المرور تكسير تقنية حيث قائمة طويلة من الكلمات من القاموس مرارًا وتكرارًا ضد الهدف حتى يتم العثور على التطابق الصحيح. هذه يمكن استخدام هذه التقنية لكسر كلمات المرور التي تحتوي على كلمات موجودة في القاموس. بشكل عام ، يعتمد نجاح الهجوم على القاموس على حقيقة أن معظم الأشخاص لديهم الميل لاستخدام سهل لتذكر كلمات المرور الموجودة في القاموس. ومع ذلك، إذا واحد يستخدم كلمة مرور قوية مع مزيج من الحروف الهجائية والأرقام أو إدخال اختلاف طفيف في الإملاء الفعلي سيجعل من المستحيل على القاموس الهجوم كسر هذه كلمات السر.

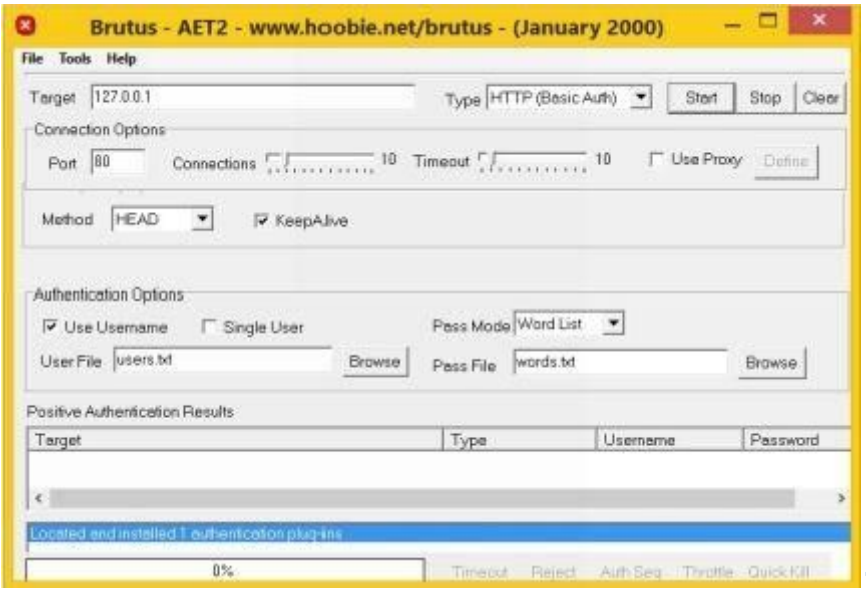
أحد أدواتي المفضلة لتنفيذ هجوم القاموس هو **Brutus** . إنه عن بعد عبر الإنترنت كلمة السر المفرقع التي تعمل على منصة ويندوز ويمكن تحميلها من الرابط التالي:

بروتوس تحميل: **http://www.hoobie.net/brutus/**

ملاحظة: من المعروف أن بعض برامج مكافحة الفيروسات تتعارض مع تطبيق *Brutus* . لذلك ، يوصى بتعطيل برنامج مكافحة الفيروسات مؤقتًا قبل تشغيل برنامج *Brutus* تطبيق.

الآن ، اسمحوا لي أن أقدم لكم عرضًا صغيرًا حول كيفية استخدام *Brutus* . هنا خطوة بخطوة إجراء:

1. بعد تنزيل الأداة من الرابط أعلاه ، قم بفك ضغط الحزمة إلى فراغ جديد مجلد.
2. قم بتشغيل ملف "BrutusA2.exe" لفتح التطبيق كما هو موضح في الشكل أدناه:



الشكل 7. 1

3. أدخل *عنوان IP* (أو *اسم المجال*) للخادم الهدف في الحقل "Target".

حدد نوع كلمة المرور التي تريد كسرها من حقل "الكتابة" أو أدخلها رقم المنفذ المخصص الخاص بك في حقل "المنفذ".

4. إذا كنت تعرف *اسم المستخدم* الذي تريد اختراق كلمة المرور الخاصة به ، ثم تحقق من خيار "مستخدم واحد" وأدخل *اسم المستخدم* في حقل "معرف المستخدم". ترك خلاف ذلك الإعدادات الافتراضية للعمل كما هي بحيث يتم تحميل *قائمة اسم المستخدم* من ملف "users.txt".
5. في حقل "وضع المرور" ، حدد خيار "قائمة الكلمات". في *قائمة من الكلمات* سوف يكون يتم تحميله من ملف "words.txt" بشكل افتراضي والذي يحتوي على حوالي 800 كلمة. إذا لديك ملف *TXT.* يحتوي على المزيد من الكلمات ، ثم يمكنك استخدامه عن طريق تحديد خيار "تصفح". كلما كانت القائمة أكبر ، كلما كانت فرص تكسير القرص أفضل

كلمه السر. فيما يلي مثال لكيفية *اسم المستخدم* و *كلمة المرور* قد تبدو قائمة مثل:

الشكل 7. 2

6. الآن ، اضغط على زر "ابدأ" لبدء عملية التكسير. سوف بروتوس محاولة كل كلمة في *قائمة كلمات المرور* لكل *اسم مستخدم* موجود في *قائمة اسم المستخدم* . سوف يستغرق بعض الوقت لإكمال العملية وإذا كنت محظوظًا ، فيجب أن تحصل على نتيجة *إيجابية* استجابة *المصادقة* وكلمة المرور متصدع كما هو مبين في الشكل أدناه:

الشكل 7. 3

ملاحظة: من الأفضل دائمًا *استخدام* بروكسي قبل محاولة عملية القرصنة هذه.

سيؤدي هذا إلى منع تخزين عنوان IP الحقيقي الخاص بك في سجلات الخادم البعيد و وبالتالي يقلل من فرص تتبعهم.

الهجوم الوحشي بالقوة

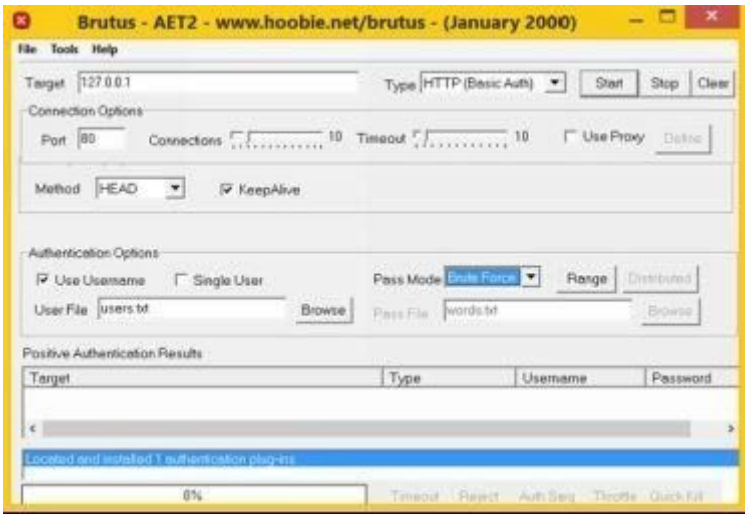
على عكس هجوم القاموس الذي يحاول فقط تلك الكلمات الموجودة في القائمة ، **الغاشمة هجوم القوة** من ناحية أخرى يحاول كل التقليب ممكن من الحروف الهجائية والأرقام و حتى الأحرف الخاصة حتى كلمة المرور الصحيحة إذا وجدت.

من الناحية النظرية ، من الممكن كسر أي كلمة مرور باستخدام هذا النهج ، ولكن ها هي المشكلة! هجوم *القوة الغاشمة* يستغرق وقتًا طويلاً للقضاء على كلمات المرور. الوقت يعتمد في الواقع على سرعة الكمبيوتر وتعقيد كلمة المرور.

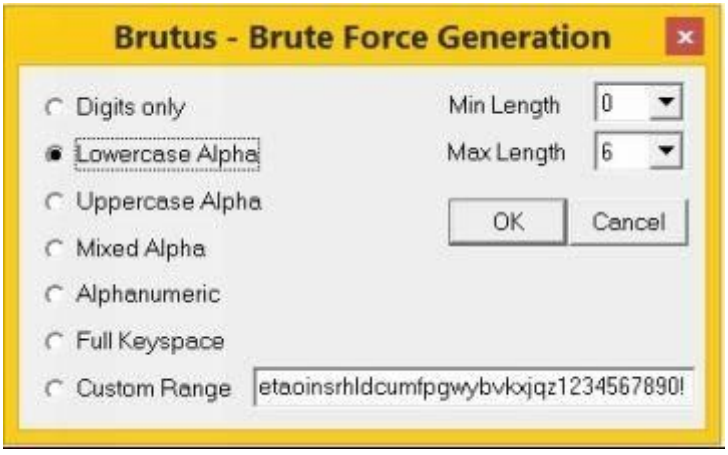
على سبيل المثال ، إذا كانت كلمة المرور الهدف صغيرة ولا تحتوي على أي أرقام أو أرقام خاصة الشخصيات ، فمن السهل إلى حد ما كسر هذه كلمات المرور باستخدام هذا النهج. ومع ذلك ، إذا كان كلمة المرور طويلة ، وتحتوي على أرقام أو حتى أحرف خاصة ، وقد يستغرق هذا النهج وقت طويل لإكمال. بالنسبة لبعض كلمات المرور المعقدة ، قد يستغرق نهج القوة الغاشمة حتى سنوات لإنهاء عملية تكسير لأن هناك مليارات من التباديل في محاولة.

فيما يلي كيفية تكوين برنامج *Brutus* لتجربة نهج القوة الغاشمة:

1. قم بتكوين "الهدف" و "النوع" و "المنفذ" بنفس الطريقة كما في حالة هجوم *القاموس* . ضمن "خيارات المصادقة" ، حدد "وضع المرور" كـ **القوة الغاشمة** وانقر على زر "النطاق" كما هو موضح في الشكل 7.4 أدناه:
2. بمجرد النقر فوق "النطاق" ، سترى عددًا من الخيارات لتحديدها مثل "الأرقام فقط" ، "أحرف صغيرة" ، "أحرف كبيرة" وهلم جرا. يمكنك أيضا تعيين على **طول مين** و **أقصى طول** لتضييق الخيارات هجوم القوة الغاشمة الخاص بك (الشكل 7.5).



الشكل 7. 4



الشكل 7. 5

في المثال أعلاه ، سيحاول Brutus جميع التباديل في الحروف الهجائية السفلية تتراوح من 0 إلى 6 أحرف في الطول. البحث عن خيارات مثل "Mixed Alpha" أو "أبجدي رقمي" وزيادة **الحد الأقصى للطول** سيزيد من النجاح معدل تكسير كلمة المرور ، وبالتالي يستغرق وقتًا أطول لإكماله.

3. بمجرد انتهاء تحديد النطاق ، انقر فوق "موافق" واضغط على زر "ابدأ". الغاشمة سوف تبدأ محاولة تكسير القوة وستستغرق أي مكان من بضع دقائق إلى بضع ساعات لإكمال. إذا كانت محاولة الكراك ناجحة ، يجب أن ترى *اسم المستخدم وكلمة المرور* المقابلة التي يتم عرضها على نافذة Brutus!

قوس قزح الجدول

و **الجدول قوس قزح** هو الجدول محسوبة مسبقا يحتوي على قائمة طويلة من التجزئة كلمة المرور لل
كلمات القاموس وكذلك التقليب الأبجدي الرقمي للكلمات. القراصنة في البداية
ينشئ قائمة طويلة من تجزئة كلمة المرور ويخزنها في جدول قوس قزح للاستخدام لاحقًا.
على الرغم من أن إنشاء طاولة قوس قزح يستغرق في البداية وقتًا طويلًا ويستخدم مساحة تخزين أكبر
مساحة ، بمجرد حسابها يمكن أن تقلل إلى حد كبير من الوقت المستغرق لتكسير كلمة المرور معالجة.
سيحتفظ أي نظام كمبيوتر يتطلب مصادقة كلمة المرور بجدول
أسماء المستخدمين وكلمات المرور في قاعدة البيانات الخاصة به. في حالة ما إذا تمكن القراصنة من سرقة هذا الجدول
من قاعدة البيانات ، سيكون بسهولة في وضع يمكنه من الوصول إلى عدد كبير من
حسابات على النظام المستهدف. لمنع حدوث ذلك ، يتم تخزين معظم الأنظمة
كلمات المرور بتنسيق التجزئة التشفير بدلاً من النص العادي.
على سبيل المثال ، عندما يكمل المستخدم عملية التسجيل على بوابة إلكترونية ، يكون النظام
قد يحول كلمة المرور الخاصة به إلى تنسيق التجزئة MD5 وتخزينها في جدول قاعدة البيانات الخاصة به. لنفترض إذا
لدى المستخدم كلمة **مروره كالسمكة الذهبية** ، ستكون علامة التجزئة MD5 على النحو التالي:
MD5 هاش: 861836f13e3d627dfa375bdb8389214e
بعد ذلك عندما يحاول المستخدم تسجيل الدخول إلى البوابة ، يتم تحويل كلمة المرور الخاصة به إلى
تنسيق التجزئة MD5 على الطاير ومقارنتها بعثرة التجزئة الموجودة في قاعدة البيانات
الطاولة. إذا تطابق كل من التجزئة ، يتم منح الوصول للمستخدم.
الآن ، حتى لو تمكن المتسلل من الوصول إلى قاعدة البيانات وسرقة كلمة المرور
الجدول ، وقال انه يرى سوى قائمة طويلة من التجزئة التشفير وليس كلمة المرور الفعلية.
هذا هو المكان الذي يأتي في متناول يدي *الجداول* . هاكر يمكن استخدام *الجداول قوس قزح* ل
مقارنة قائمة طويلة من التجزئة قبل حسابها مقارنة قائمة المسروقة من تجزئة كلمة المرور. إذا

تطابق التجزئة ، ستكون كلمة المرور هي الكلمة التي تم استخدامها في البداية لإنشاء التجزئة.

على عكس نهج *القوة الغاشمة* حيث يتم حساب التجزئة في كل محاولة ، *قوس قزح* نهج *الجدول* من ناحية أخرى يستخدم قائمة محسوبة مسبقا من التجزئة للمقارنة مباشرة لهم ضد تجزئة كلمة المرور الحالية. كما الوقت اللازم لحساب التجزئة على يتم تقليل كل محاولة ، نهج *الجدول قوس قزح* يستغرق وقتا أقل بكثير ل أكمل عملية التكسير.

سيتم مناقشة مثال عملي لنهج *جدول قوس قزح* في الفصل التالي حيث نتناول موضوع تكسير كلمات مرور Windows.

هجوم التصيد

الخداع هو شكل من أشكال الهندسة الاجتماعية التي يستخدمها المتسللين لجمع المعلومات الحساسة معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان عن طريق طرح باسم شخص موثوق به أو منظمة.

عادةً ما ترسل حيل الخداع رسالة بريد إلكتروني إلى المستخدمين الذين يطلبون شخصيتهم المعلومات ، أو إعادة توجيهها إلى موقع ويب حيث يُطلب منهم إدخال بياناتهم الشخصية معلومات.

في معظم الحالات ، يوجه البريد الإلكتروني المخادع الضحايا إلى اتباع رابط يؤدي إلى موقع ويب حيث سيتعين عليهم إدخال تفاصيل تسجيل الدخول الخاصة بهم أو معلومات سرية أخرى. في في الواقع ، هذا الموقع هو موقع مزيف تم إنشاؤه بواسطة المتسلل (يشار إليه غالبًا على أنه مضلل موقع الويب) وهو نسخة طبق الأصل من الأصل أو يبدو مشابهًا. عندما الضحية يقوم بإدخال تفاصيل تسجيل الدخول الخاصة به / بها على صفحة مزيفة يتم سرقتها فعليًا من قِبل القراصنة.

على سبيل المثال ، قد يقوم المتسلل بإرسال بريد إلكتروني يدعي أنه كان يظهر من البنك الذي يحتفظ فيه الضحية بحساب واطلب منه / لها تحديث بيانات تسجيل الدخول من خلال بعد الرابط الموجود في البريد الإلكتروني. يذكر البريد الإلكتروني أن عملية التحديث هذه إلزامي وسيؤدي عدم القيام بذلك إلى إغلاق الحساب المصرفي. ك

ردا على ذلك ، ينقر الضحية على الرابط حيث سيتم نقله إلى صفحة تسجيل الدخول المزيفة يشبه الأصلي واحد. ومع ذلك ، عندما يتم إدخال تفاصيل تسجيل الدخول ، فهي سجلت وتخزينها على الموقع الإلكتروني للوصول في وقت لاحق من قبل القراصنة. يبقى الضحية غير مدركين للعملية بأكملها ولكن القراصنة يتمكن من اختراق كلمة المرور بمهارة.

التدابير المضادة

بعد معالجة بعض أساليب تكسير كلمة المرور الشائعة ، دعونا الآن نلقي نظرة على بعض التدابير المضادة التي يمكن اتخاذها لحماية أنفسنا من أعلاه الهجمات المذكورة.

هندسة اجتماعية

الإجراءات اللازمة لحماية نفسك من هجمات *الهندسة الاجتماعية* بسيطة للغاية ومباشرة إلى الأمام. لا تكشف مطلقًا عن كلمة مرورك أو أي معلومات شخصية أخرى أي شخص عبر الهاتف أو البريد الإلكتروني. قد يحاول المهاجمون إقناعك بالتظاهر بأنك شخص الشخص المفوض الذي يمكنك مشاركة التفاصيل الشخصية معه. لكن تذكر ذلك كلمات المرور تعني فقط إدخالها على صفحات تسجيل الدخول وليس مشاركتها مع أي شخص على الاطلاق.

التخمين وتصفح الكتف

تأكد دائمًا من أن كلمة مرورك لا تحتوي على أسماء الحيوانات الأليفة وتاريخ الميلاد والأسرة أسماء الأعضاء أو أي شيء يسهل تخمينه. هذا موصى به تحتوي كلمة مرورك على مزيج من الكلمات والأرقام التي يصعب تخمينها الشخصيات.

بقدر ما يتعلق الأمر *بتصفح الكتف* ، يمكنك تجنب ذلك عن طريق التأكد من ذلك لا أحد خلفك يراقب حركة أصابعك على لوحة المفاتيح عندما أنت تكتب كلمة المرور.

هجوم القاموس

لحماية نفسك من هجوم *القاموس* ، كل ما عليك القيام به هو التأكد من أن لديك كلمة المرور لا تحتوي على كلمات من القاموس. وهذا يعني ، كلمة المرور الخاصة بك ليست كذلك

شيء مثل "التفاح" ، "اللوتس" أو "المانجو". بدلا من استخدام الكلمات التي ليست في
قاموس. يمكنك أيضًا استخدام عبارة مثل **str0ngpAss ؟؟** كلمة المرور الخاصة بك بحيث لا
يمكن
يكون متصدع باستخدام نهج الهجوم القاموس.

هجوم القوة الغاشمة وجدول قوس قزح

غالبًا ما تصبح هجمات *القوة الغاشمة* ناجحة عندما تكون كلمات المرور قصيرة. هذا يعني،
من خلال الحفاظ على كلمة المرور لفترة كافية ، يمكنك أن تجعل من الصعب على المهاجم كسرها.
عادةً ما تعتبر كلمة المرور التي يبلغ طولها 8 أحرف طويلة بما يكفي وآمنة
في الماضي. ومع ذلك ، ليس هذا هو الحال في سيناريو اليوم الحالي كما الحديث
أجهزة الكمبيوتر لديها قدرات معالجة عالية السرعة لتجربة الآلاف من التخمينات في الثانية الواحدة.
لذلك ، من أجل جعل كلمة مرورك محصنة ضد الهجمات بالقوة الغاشمة ، تأكد من أنها أكبر
من 8 أحرف وهي مجموعات من الحروف الهجائية والأرقام والأحرف الخاصة.
يمكنك تجنب هجوم جدول قوس قزح على كلمات المرور الخاصة بك عن طريق جعلها طويلة جدًا.
إذا كان لديك
كلمة المرور أكثر من 12 أو 14 حرفًا ، وستكون مضيعة للوقت للغاية
إنشاء الجداول لهم. هذا ينبغي أن تبقيك محمية من هذه الهجمات.

هجوم التصيد

يمكنك تجنب هجوم التصيد الاحتيالي باتباع الإرشادات المذكورة أدناه:
لا ترد على رسائل البريد الإلكتروني المشبوهة التي تطلب منك تقديم معلوماتك الشخصية.
إذا لم تكن متأكدًا مما إذا كان طلب البريد الإلكتروني مشروعًا ، فقم بالتحقق من ذلك عن طريق
الاتصال
البنك / الشركة المعنية. دائما استخدام أرقام الهواتف المطبوعة على
السجلات المصرفية أو البيانات وليس تلك المذكورة في البريد الإلكتروني المشبوه.
لا تستخدم الروابط الموجودة في البريد الإلكتروني أو الرسائل الفورية أو محادثة الدردشة لإدخال
موقع الكتروني. بدلاً من ذلك ، اكتب دائمًا عنوان URL لموقع الويب على شريط عنوان المتصفح
للوصول الى موقع على شبكة الانترنت.

تستخدم مواقع الويب الشرعية دائمًا اتصالًا آمنًا (*https: //*) على تلك الصفحات التي
الغرض منه هو جمع معلومات حساسة مثل كلمات المرور أو أرقام الحسابات أو
تفاصيل بطاقة الائتمان. سترى أيقونة قفل في شريط عنوان المتصفح الخاص بك
يشير إلى اتصال آمن. في بعض المواقع مثل "PayPal" الذي يستخدم
شهادة التحقق الممتدة ، يتحول شريط العناوين إلى اللون **الأخضر** كما هو موضح أدناه:

الشكل 7. 6

حتى إذا كانت صفحة تسجيل الدخول غير آمنة (https: //) ، فقد يكون موقع الويب الهدف مستمراً
شرعية. ومع ذلك ، ابحث عن الأخطاء الإملائية مثل ، **www.papyal.com**
www.payapl.com
أو **paypal.somethingelse.com** بدلاً من الموقع الشرعي **www.paypal.com** و
تأكد من إدخال تفاصيل تسجيل الدخول فقط على صفحة الويب الشرعية.

الفصل 8 - اختراق ويندوز

نظرًا لكونه أحد أنظمة التشغيل الأكثر شهرة في العالم ، فإن Windows لديه وجوده
على تقريبا كل نظام الكمبيوتر اليوم. لذلك ، في مجال فهم القرصنة الأخلاقية
تقنيات اختراق أنظمة Windows تصبح مهمة للغاية. دعونا الآن ننظر
في بعض هذه التقنيات باستخدام والتي يمكنك إدارة بنجاح لاختراق أي
كمبيوتر ويندوز.

كسب الوصول إلى النظام

الوصول إلى حساب مستخدم محمي بكلمة مرور خاصةً الحساب
تشكل "امتيازات المسؤول" العنصر الرئيسي في اختراق Windows. وفيما يلي
الطريقتان المهمتان اللتان تستخدمهما يمكنك الوصول إلى أي حساب محمي عليهما
ويندوز دون معرفة كلمة المرور.

إعادة ضبط كلمة مرور Windows

إذا كنت ترغب في الوصول إلى جهاز كمبيوتر يعمل بنظام Windows بحسابه بكلمة مرور ،
إعادة تعيين كلمة المرور خيار سهل. يخزن Windows جميع معلومات حسابه و

كلمات المرور المشفرة في ملف يسمى "SAM". من خلال تعديل ملف "SAM" من الممكن إعادة تعيين كلمة المرور لأي حساب مستخدم بما في ذلك كلمة "المسؤول". تستطيع قم بتنفيذ هذه المهمة باستخدام أداة مفتوحة المصدر صغيرة تعرف باسم **Offline NT & Password** **محرر التسجيل** . تعمل هذه الأداة في وضع عدم الاتصال ، مما يعني أنك بحاجة إلى إيقاف التشغيل والإقلاع

الكمبيوتر الهدف باستخدام قرص مضغوط أو جهاز USB مثل محرك الإبهام. الأداة لديها الميزات التالية:

أنت **لا** تحتاج إلى معرفة كلمة المرور القديمة لوضع واحدة جديدة.

تتيح لك هذه الأداة **إعادة تعيين** كلمة المرور لأي حساب مستخدم.

يمكن لهذه الأداة أيضًا اكتشاف **وإلغاء** *قفل* حسابات المستخدمين *المقفلة* أو *المعطلة* .

يمكنك تنزيل الأداة من الرابط أدناه:

تنزيل: /http://pogostick.net/~pnh/ntpasswd

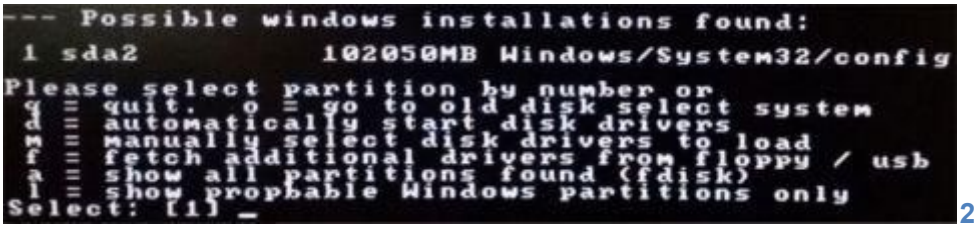
تتوفر موارد لإنشاء قرص مضغوط قابل للتمهيد وجهاز USB قابل للتنزيل بشكل منفصل. كلاهما يعمل بشكل مشابه وهو مسألة راحتك. ومع ذلك ، في هذا كتاب سأقدم عرضًا توضيحيًا لإصدار USB لإعادة تعيين كلمة المرور الحالية. إلى قم بإنشاء محرك أقراص USB قابل للتمهيد ، وقم بتنزيل وإلغاء ضغط نسخة USB من الأداة من الرابط أعلاه باتباع الإرشادات البسيطة الواردة في ملف **readme.txt** .

بمجرد امتلاك جهاز USB القابل للتمهيد في يدك ، قم بتوصيل الجهاز والتمهيد منه.

تأكد من قيامك بتمكين خيار تمهيد USB وتعيين أولوية التمهيد الأعلى لـ جهاز USB الخاص بك في BIOS. إرشادات خطوة بخطوة لإكمال إعادة تعيين كلمة المرور وترد العملية أدناه:

الشكل 8. 1

بمجرد تشغيل الأداة من جهاز USB ، يجب أن تشاهد الشاشة مشابهة للشاشة واحد هو مبين أعلاه. فقط اتبع تعليمات الشاشة وستكتشف الأداة تلقائيًا القسم الذي تم تثبيت Windows عليه. عادة ما يتم تحميل الخيارات الصحيحة مسبقًا قوس مربع كما هو موضح في لقطة أدناه. لذلك ، فقط اضغط على مفتاح **الإدخال** يجب عمل.

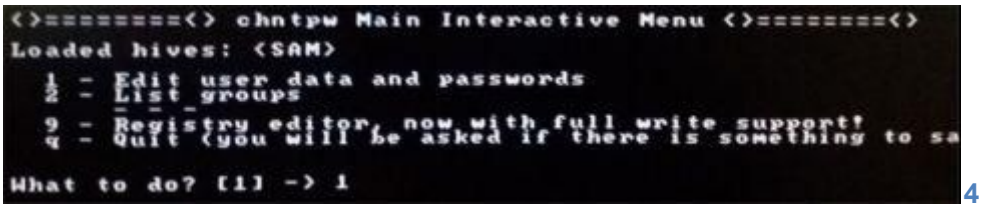


الشكل 8. 2

في الخطوة التالية ، سيُطلب منك "تحديد أي جزء من السجل ليتم تحميله". انت تحتاج لتحديد الخيار - **1** وهو "بقية كلمة المرور [sam]" والتي يتم تحميلها افتراضيًا كما هو موضح أدناه. لذلك فقط اضغط على **Enter** للمتابعة.

الشكل 8. 3

في الخطوة التالية ، حدد الخيار **1 -** وهو "تحرير بيانات المستخدم وكلمات المرور" كما هو موضح أدناه وضرب **أدخل** .



الشكل 8. 4

الآن ، يجب أن ترى قائمة "أسماء المستخدمين" وحالة "المسؤول" الخاصة بهم يتم عرضها.

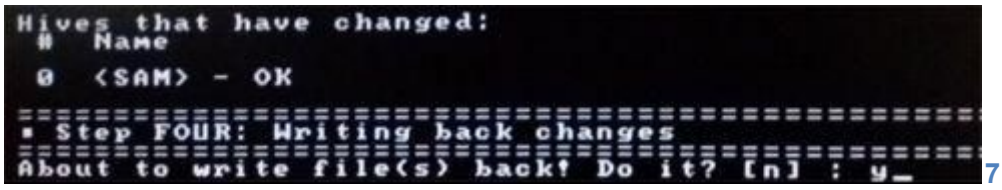
حدد المستخدم الذي لديه امتياز المسؤول واضغط على **Enter** .

الشكل 8. 5

في الشاشة التالية سيُطلب منك الاختيار من قائمة الخيارات التي قد ترغب فيها
أداء على المستخدم المحدد. هنا ، ما عليك سوى اختيار الخيار - **1** وهو "مسح (فارغ) المستخدم
كلمة المرور "وضرب **Enter** .

الشكل 8. 6

هذا يجب إعادة تعيين كلمة المرور لحساب المستخدم لجعلها فارغة ، بحيث التالي
عند إعادة تشغيل Windows ، يجب أن تكون قادرًا على تسجيل الدخول تلقائيًا كما لو كان هناك
لم يتم تعيين كلمة مرور لحساب المستخدم هذا.
الآن استقال تحرير المستخدم بالضغط **ف** وضرب **أدخل** حتى أن تنتقل إلى الشاشة حيث
سيُطلب منك تأكيد "إعادة كتابة التغييرات" إلى ملف SAM. هذه الخطوة هي جدا
المهم حيث تحتاج إلى الصحافة **ذ** وضرب **أدخل** كما هو موضح في اللقطة أدناه. اذا أنت
عن طريق الخطأ اضغط **Enter** مع الاحتفاظ بالخيار الافتراضي وهو **n** ، ستفشل عملية إعادة
الضبط
والإجراء كله يجب أن يتكرر مرة أخرى من البداية. لذلك ، تغيير
الخيار الافتراضي من **n** إلى **y** قبل الضغط على مفتاح **Enter** مهم للغاية.



الشكل 8. 7

سيؤدي هذا إلى إكمال عملية إعادة التعيين حيث ستتم إزالة كلمة المرور الحالية وتعيينها لتفريغ. افصل جهاز USB واضغط على **CTRL + ALT + DEL** لإعادة تشغيل الجهاز الحاسوب. الآن ، يجب أن يسمح لك Windows بتسجيل الدخول إلى النظام دون الإصرار على الدخول

كلمة السر.

استعادة كلمة المرور بعد الخرق

تعد إعادة تعيين كلمة المرور خيارًا رائعًا للوصول بسهولة إلى كلمة المرور الحسابات المحمية. ومع ذلك ، تحتوي هذه الطريقة على عيب واضح عند إعادة تعيين كلمة المرور العملية دائمة. سيتعرف مسؤول الجهاز المستهدف بسهولة حول خرق الأمان لأنه بعد ذلك لن يتم طلب كلمة مرور أثناء عملية تسجيل الدخول.

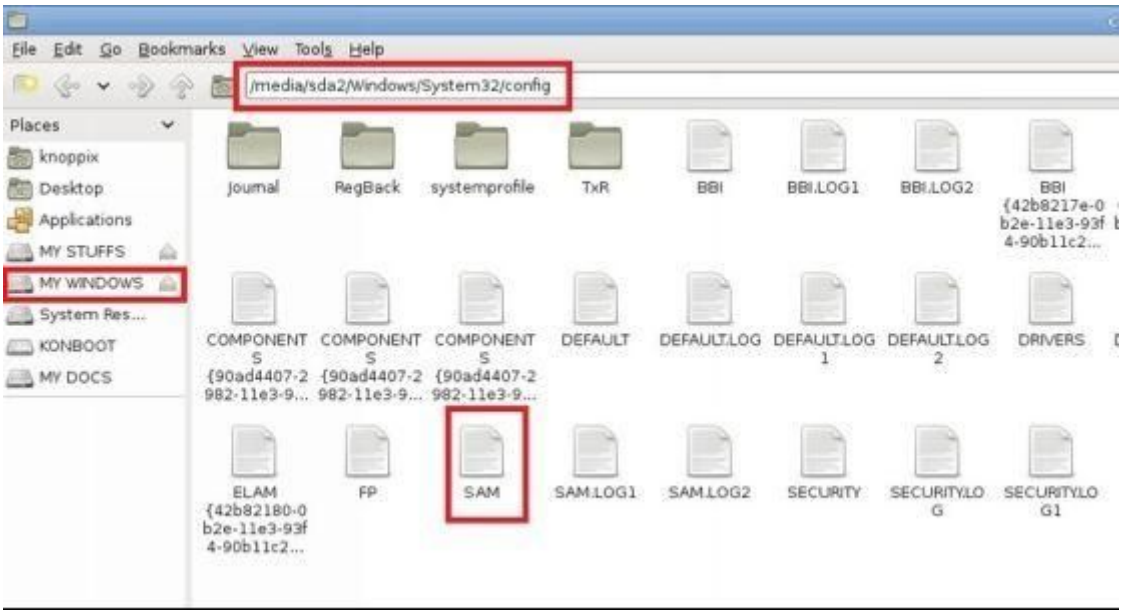
للتغلب على هذا العيب ، سيتعين علينا استخدام وسيلة لاستعادة كل شيء مرة أخرى طبيعي بمجرد اكتمال الغرض من الاختراق. لهذا علينا أن نأخذ نسخة احتياطية من ملف **SAM** الأصلي قبل تعديله في عملية إعادة تعيين كلمة المرور واستعادتها بأمان مرة أخرى لجعل كل شيء يبدو طبيعيا.

يوجد ملف **SAM** في محرك الأقراص المثبت عليه Windows (عادةً **:C**) ضمن المسار التالي: **\ config \ system32 \ windows** . يمكنك الوصول بسهولة إلى هذا الموقع عن طريق التمهيد

الكمبيوتر من **Kali Linux** DVD مباشرة. بمجرد تحميل **Kali** DVD ،

انقر فوق "رمز الكمبيوتر" الموجود على سطح المكتب لفتح نافذة المستكشف. الآن، انتقل إلى الموقع أعلاه للعثور على ملف **SAM** وإعادته إلى موقع مختلف مثل محرك أقراص مختلف أو إلى جهاز USB الخاص بك.

الشكل 8. 8



الآن أعد تشغيل النظام وأجري عملية إعادة تعيين كلمة المرور كما تمت مناقشته مسبقًا. ذات مرة لقد انتهيت من عملك ، أعد تشغيل النظام مرة أخرى باستخدام **Kali** DVD وانتقل إلى موقع ملف **SAM** . إعادة تسمية الملف الموجود إلى **SAM.OLD** واستعادة الأصل ملف **SAM** من موقع النسخ الاحتياطي. هذا يجب أن يعيد كل شيء إلى طبيعته و تجنب الشك.

تجاوز عملية مصادقة Windows

في القسم السابق ، ناقشنا كيفية إعادة تعيين كلمة المرور للوصول إليها النظام. ولكن هناك طريقة ذكية أخرى للوصول إلى نظام Windows بواسطة تجاوز بصمت عملية المصادقة نفسها. يتم ذلك عن طريق تطبيق مؤقت التغييرات على نواة ويندوز على الطاير (أثناء التشغيل) لتعطيل المصادقة معالجة. تتيح لك أداة تسمى **Kon-Boot** إنجاز هذه المهمة. يمكنك تنزيله من الرابط أدناه:

/Kon-Boot: http://www.piotrbania.com/all/kon-boot

Kon-Boot هي أداة مفيدة تتيح لك إدخال أي مستخدم Windows محمي بكلمة مرور حساب دون الحاجة إلى إدخال كلمة المرور أثناء عملية تسجيل الدخول. الأداة تسمح

لك لإنشاء قرص مضغوط قابل للتمهيد أو محرك أقراص USB. بمجرد تشغيل الكمبيوتر الهدف من هذا

جهاز قابل للتمهيد ، سيتم تعديل أجزاء Windows kernel تقريبًا لتحميل التشغيل
النظام في وضع خاص حيث لن يتم إصرارك على إدخال كلمة المرور. ال
ميزة هذه الأداة هي أن جميع التغييرات مؤقتة وتختفي بعد إعادة التشغيل ، لذلك
أن كل شيء يبدو طبيعيا بعد ذلك ولا يثير الشك في إمكانية
اختراق امني.

الإغراق على كلمات المرور

بعد فهم بعض التقنيات للوصول إلى النظام دون معرفة
كلمة المرور ، لقد حان الوقت للمضي قدماً بخطوة واحدة ومعرفة وسيلة لكسر
كلمة المرور الفعلية نفسها. إذا كان مطلوبًا للوصول إلى النظام المستهدف عدة مرات
على مدار فترة ما ، من المستحسن دائمًا كشف كلمة المرور عن طريق تكسيرها حتى تتمكن من كشفها
يمكن بسهولة تسجيل الدخول إلى النظام عن طريق إدخال كلمة المرور وبالتالي القضاء على الحاجة إلى
إعادة تعيين كلمة المرور في كل مرة تريد الوصول إليها.
يتم تحويل كلمات مرور حساب مستخدم Windows إلى تنسيق تجزئة يسمى
تجزئة **NTLM (إدارة LAN LAN)** . هذا التجزئة **NTLM** جنبا إلى جنب مع ملف تعريف المستخدم
يتم تخزين التفاصيل في ملف خاص يسمى **Security Accounts Manager** أو **SAM** .
و **SAM**
يتم تشفير الملف بشكل أكبر باستخدام *syskey* المخزن في ملف يسمى **SYSTEM** . على حد سواء
توجد SAM و **SYSTEM** في محرك الأقراص حيث تم تثبيت Windows (عادةً C :)
تحت المسار التالي: **\ windows \ system32 \ config** .
من أجل كسر كلمة المرور ، من الضروري استخراج تجزئة **NTLM** والمستخدم

تفاصيل حسابات المخزنة في ملف **SAM** من النظام الهدف الذي يعرف باسم الإغراق. يتم نقل التفاصيل الملقاة إلى جهاز كمبيوتر المتسلل وكلمة المرور متصدع باستخدام أداة تكسير كلمة المرور حاليا. فيما يلي طريقتان لتفريغ تجزئة كلمة المرور:

الإغراقات مع وصول المسؤول

إذا كان لديك وصول المسؤول إلى النظام الذي تريد تفريغ كلمة المرور تجزئة ، يمكنك استخدام أداة مفيدة تسمى **PWDUMP** . هذا سطر أوامر مفتوح المصدر أداة لتفريغ كلمة المرور بسرعة تجزئة على ملف نصي. يمكن تنزيل الأداة من الرابط أدناه:

/PWDUMP: http://www.tarasco.org/security/pwdump_7

هذه أداة صغيرة جدًا يقل حجمها عن ميغابايت ويمكن نقلها إلى الهدف الموقع في محرك أقراص USB الإبهام. لتفريغ التجزئة ، ما عليك سوى فتح موجه الأوامر باستخدام حقوق المسؤول ، انتقل إلى موقع الأداة (PwDump7.exe) وقم بتشغيل الأمر التالي:

PwDump7.exe >> targetfilename.txt

كما هو موضح في اللقطة أدناه ، أقوم بتشغيل **PwDump.exe** من إبهامي USB محرك الأقراص (**M :**) وإلقاء تفاصيل التجزئة في ملف يسمى **hash.txt** . يجب أن يحصل هذا الملف تم إنشاؤه في نفس الدليل الذي يعمل منه **PwDump.exe** .

الشكل 8. 9

و **hash.txt** يحتوي الملف على قائمة حسابات المستخدمين الموجودة على الجهاز وعلى التجزئة **NTLM** المقابلة كما هو مبين أدناه:

الشكل 8. 10

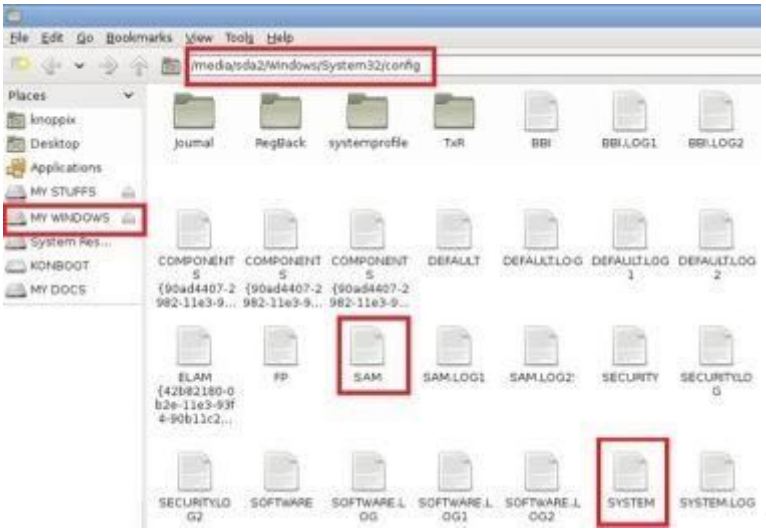
الإغراقات دون وصول المسؤول

يوضح القسم السابق كيفية تفريغ تجزئة كلمة المرور عندما يكون لديك بالفعل وصول المسؤول إلى الجهاز الهدف. ماذا لو لم يكن لديك وصول المسؤول؟

في هذه الحالة ، يمكنك استخدام **Kali Linux** Live DVD لتشغيل النظام وتحميل لينكس. من هنا ، قم بالوصول إلى محرك الأقراص المثبت عليه نظام التشغيل Windows وانتقل إلى

\ config \ system32 \ windows ** . من هنا انسخ الملفين **SAM و **SYSTEM** إلى ملفك

جهاز USB بحيث يمكنك حملهم إلى جهاز الكمبيوتر الخاص بك لتكسير كلمة المرور في وضع عدم الاتصال.



الشكل 8. 11

تحطيم كلمة المرور

بعد إلقاء علامات تجزئة كلمة المرور بنجاح ، يمكننا الآن كسرها بسهولة باستخدام أدوات وأساليب مختلفة كما هو مذكور أدناه:

باستخدام قوس قزح الجداول

كما نوقش في الفصل السابق ، يحتوي جدول قوس قزح على قائمة محسوبة مسبقًا

التجزئة التي يمكن مقارنتها على الفور مع كلمة مرور ملقاة التجزئة لكسر
كلمه السر. هذا هو حتى الآن أفضل وأسرع طريقة لكسر ويندوز بنجاح
كلمه السر. لهذا سنستخدم أداة مفتوحة المصدر تسمى **Ophcrack** التي يمكن أن تكون
تم تنزيله من الرابط أدناه:

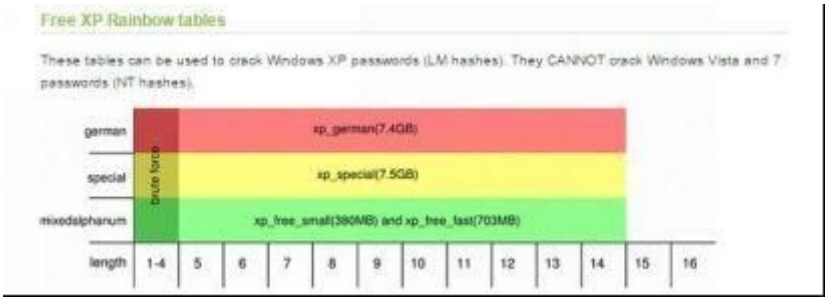
موقع Ophcrack: http://ophcrack.sourceforge.net/

من الرابط أعلاه ، قم بتنزيل الإصدار القابل للتثبيت من **Ophcrack** (وليس القرص المضغوط المباشر
الإصدار) وتثبيته على نظامك. أثناء عملية التثبيت ، عندما يكون الخيار
يأتي لتنزيل جداول قوس قزح وإلغاء تحديدها جميعًا وتثبيت البرنامج فقط. أنه
دائما أفضل لتحميل الجداول قوس قزح بشكل منفصل.

الشكل 8. 12

بمجرد تثبيته على نظامك ، انتقل إلى **موقع Ophcrack الإلكتروني** من أعلاه
الرابط وانقر على **الجداول** في قائمة التنقل. هنا يجب أن ترى قائمة قوس قزح
الجداول التي يمكنك تحميلها.

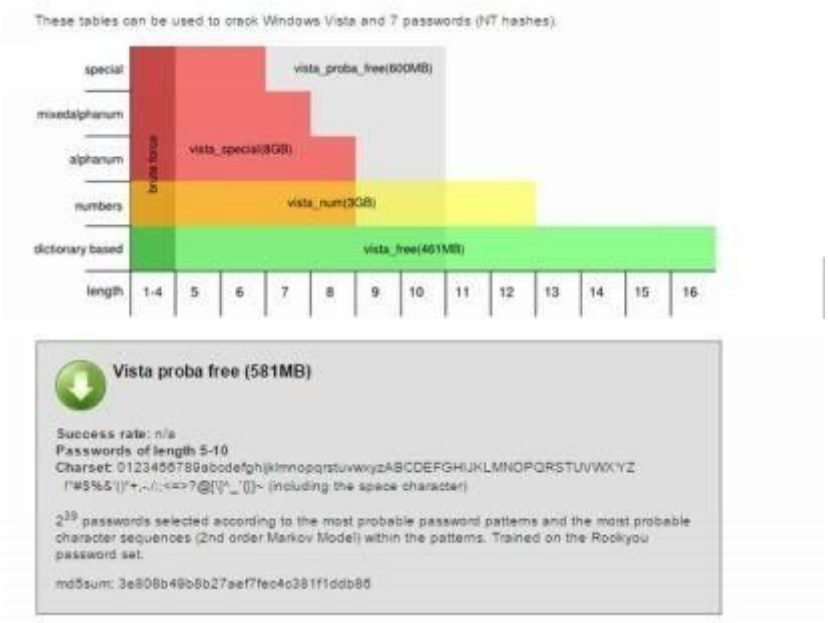
إذا كنت ترغب في كسر كلمات مرور *نظام التشغيل Windows XP* وتنزيل أنظمة التشغيل السابقة
الجداول من قسم **التجزئة LM** . لأنظمة التشغيل بعد XP مثل *ويندوز*
Vista و *7* و *8* قم بتنزيل الجداول من قسم **تجزئة NT** .



الشكل 8. 13

الشكل 8. 14

الشكل 8. 15



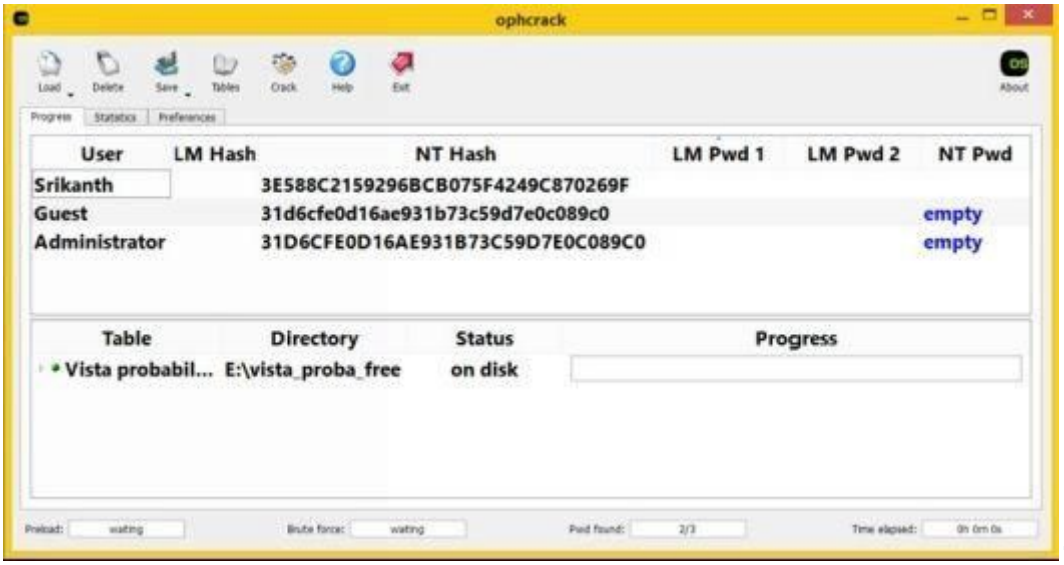
الشكل 8. 16

كما هو موضح في اللقطات أعلاه ، حيث تزيد مجموعة الأحرف من حجم الجدول أكبر. أكبر الجدول أعلى فرصة للتشقق ناجحة. يمكنك تحميل واحد يلائم احتياجاتك. لأغراض العرض التوضيحي ، أستخدم "Vista proba free "table على جهاز Windows 8 الخاص بي مع **Ophcrack** . هنا دليل خطوة بخطوة حول كيفية استخدام هذه الأداة للقضاء على كلمات المرور.

1. افتح أداة **Ophcrack** بالنقر المزدوج فوق الرمز الموجود على سطح المكتب.
2. من نافذة **Ophcrack** الرئيسية ، انقر على زر "Tables" وحدد الجدول الذي لقد قمت بتنزيلها من القائمة. الآن انقر على زر "تثبيت" ، قم بتحميل المجلد الذي يحتوي على الجداول التي تم تنزيلها وانقر فوق "موافق".

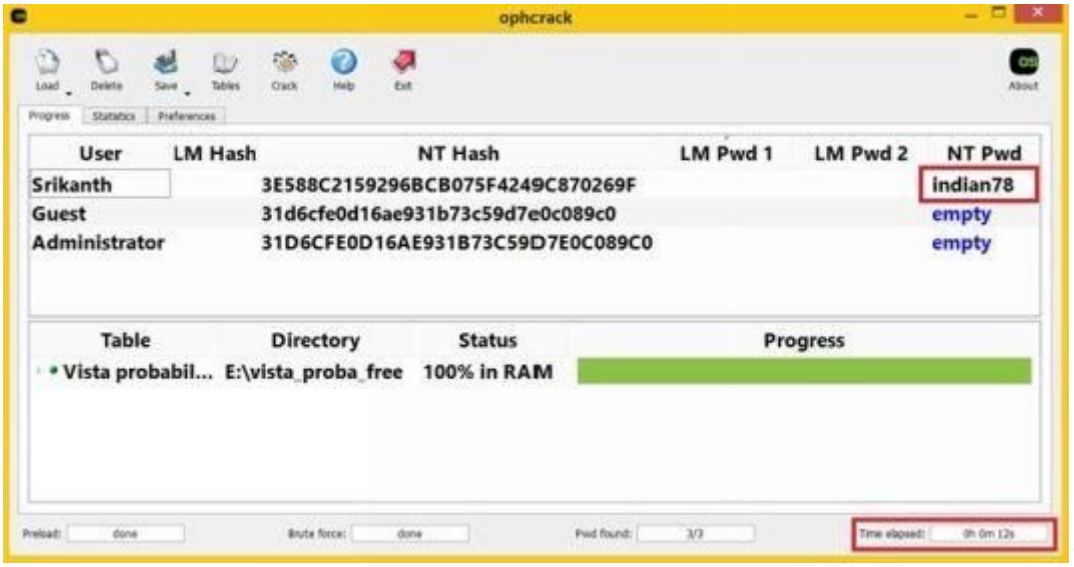
الشكل 8. 17

3. بعد ذلك ، لتحميل تجزئة كلمة المرور التي تم إلقاؤها ، انقر فوق الزر "تحميل" ، حدد "ملف PWDUMP" الخيار وتحميل ملف **hash.txt** الحصول عليها عن طريق تشغيل أداة PWDUMP على الجهاز الهدف. إذا كان لديك ملفات **SAM** و **SYSTEM** بدلاً من **hash.txt** ، يمكنك اختيار الخيار **SAM المشفر** بدلاً من "ملف PWDUMP" وحدد المجلد الذي يحتوي على هذين الملفين.



الشكل 8. 18

4. عندما يتم تحميل كل شيء وجاهزة كما هو موضح في لقطة أعلاه ، انقر على زر "الكراك" وموقعه بصبر. سوف تتخذ عملية تكسير من أي مكان بين بضع دقائق إلى بضع ساعات لإكمال اعتمادا على حجم الجدول وقوة كلمة المرور. إذا نجحت ، ستكون كلمة المرور المتصدعة عرض جنبا إلى جنب مع الوقت المستغرق للقضاء على النحو المبين أدناه:



الشكل 8. 19

إذا لم تنجح في تكسير كلمة المرور ، يمكنك تجربة قوس قزح مختلف الجدول الذي يغطي المزيد من الأحرف وكلمات المرور الطويلة.

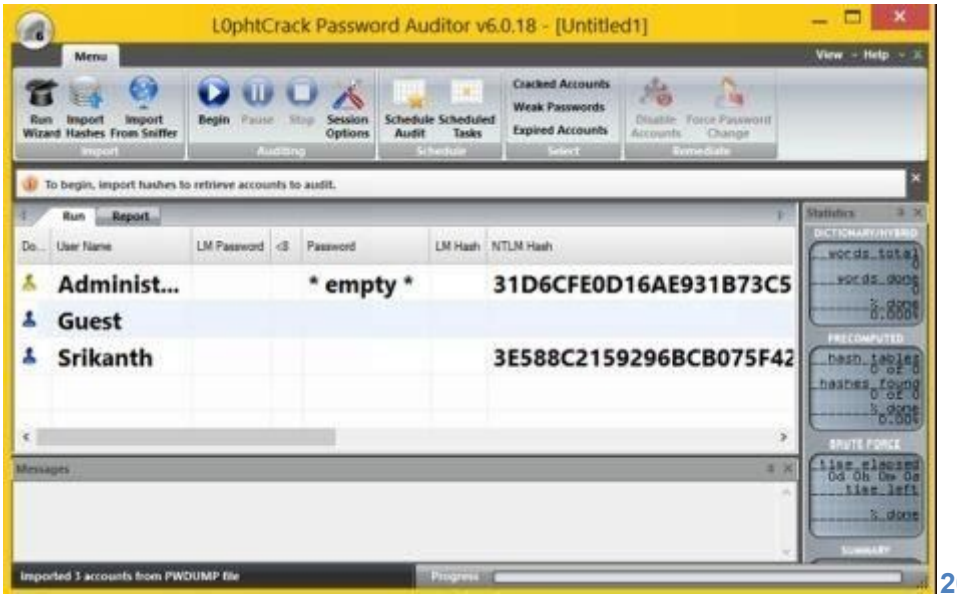
باستخدام القوة الغاشمة النهج

على الرغم من أن استخدام طاولات قوس قزح هو إلى حد بعيد أسرع وأفضل طريقة للتصدع كلمات المرور ، قد لا يكون ناجحًا لكلمات المرور الطويلة والقوية مثل جداول التجزئة لهذه كلمات المرور يصعب العثور عليها. لذلك ، يصبح نهج القوة الغاشمة أمرًا لا مفر منه في ظل هذه مواقف. لكن تذكر أن الأمر قد يستغرق وقتًا طويلًا جدًا يتراوح بين بضع ساعات إلى ساعات قليلة

أيام لاستكمال عملية تكسير. منذ **Ophcrack** ليست فعالة جدا لل الغاشمة نهج القوة ، سوف نستخدم أداة قوية أخرى تسمى **L0phtCrack** وهو متاح من الرابط أدناه:

L0PhtCrack Download: http://www.l0phtcrack.com/download.html

بعد تثبيت **L0phtCrack** ، انقر على زر "استيراد التجزئة" من النافذة الرئيسية إلى تحميل التجزئة. لديك خيار تحميل التجزئة من كل من "ملف PWDUMP" كما كذلك "ملف SAM".



الشكل 8. 20

انقر على زر "خيارات الجلسة" لتكوين خيارات تدقيق مختلفة مثل هذه كما هجمات القاموس والقوة الغاشمة. يمكنك تمكين أو تعطيل هجمات محددة وكذلك تخصيص مجموعة الأحرف وطول كلمة المرور وخيارات النطاق لنهج القوة الغاشمة. يمكن أن يؤدي تكوين خيارات التدقيق بحكمة إلى تجنب التأخير الزمني غير الضروري وبالتالي

تسريع عملية تكسير كلمة المرور.

بمجرد الانتهاء من تحميل التجزئات وتكوين الخيارات ، انقر فوق

زر "ابدأ". هذا سيبدأ عملية تكسير والوقت المستغرق لكسر

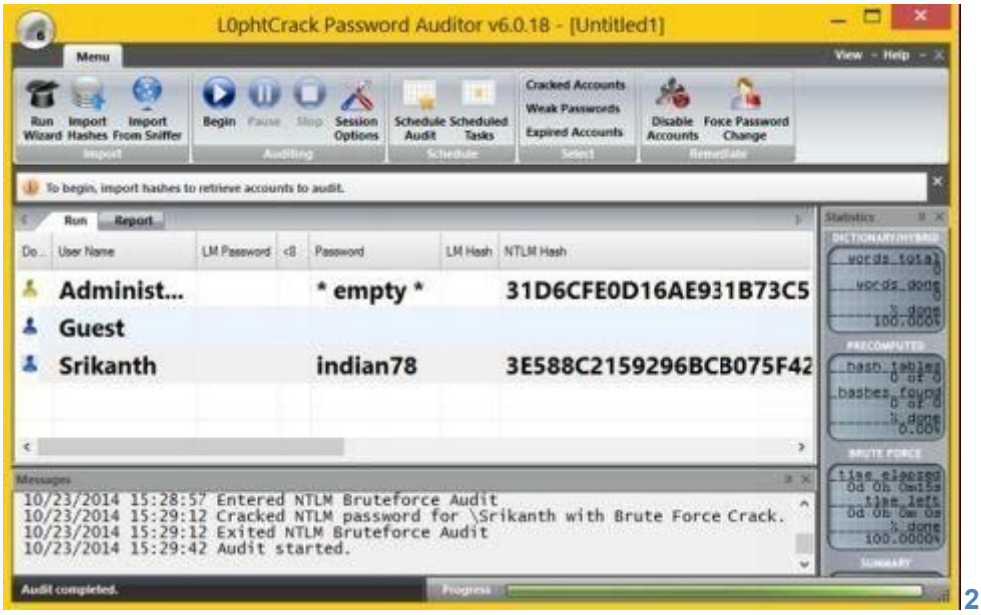
كلمة المرور تعتمد على عوامل مختلفة مثل قوة كلمة المرور (طول + وجود

الأحرف الأبجدية الرقمية + الخاصة) ، ونوع الهجوم (القاموس ، القوة الهجينة أو الغاشمة) و

سرعة جهاز الكمبيوتر الخاص بك.

في حالة نجاح عملية تكسير كلمة المرور ، يجب أن تشاهد كلمة مرور التكسير التالية

إلى اسم المستخدم في نافذة **L0phtCrack** كما هو موضح أدناه:



الشكل 8. 21

استنشاق كلمات المرور على الشبكة

إذا كان جهاز الكمبيوتر الخاص بك موجودًا على شبكة مثل المكتب أو المدرسة ، فمن الممكن الاستيراد عن بُعد

تجزئة كلمة المرور لأجهزة الكمبيوتر الأخرى على الشبكة دون الحاجة إلى الحصول على المادية الوصول إليهم. تسمى هذه الطريقة استنشاق و 6 **L0phtCrack** وما فوق يدعم هذا اختيار.

لاستنشاق كلمة مرور التجزئة من أجهزة الكمبيوتر الأخرى ، ما عليك سوى النقر على "استيراد من الشم"

زر على النافذة الرئيسية. إذا تم اكتشاف أكثر من واجهة شبكة واحدة ، فإن "اختيار"
يسمح لك مربع حوار واجهة الشبكة باختيار الواجهة التي تستنشقها. بعد
عند اختيار الواجهة الخاصة بك ، يظهر مربع الحوار "SMB Packet Capture Output"
أينما كنت
بحاجة إلى النقر على "بدء استنشاق".
إذا تم التقاط التجزئة ، يتم عرضها على الفور في مربع الحوار بعد ذلك
يمكنك الضغط على "Stop Sniffing" والنقر فوق الزر "استيراد" لتحميل علامات تجزئة كلمة
المرور
تكسير.

التدابير المضادة

من أجل تأمين جهاز الكمبيوتر الخاص بك الذي يعمل بنظام Windows من كل تلك الهجمات
المحتملة كما هو مذكور في
هذا الفصل ، فيما يلي بعض الإجراءات المضادة التي تحتاج إلى اتباعها:
لا تسمح للغرباء بالوصول إلى جهاز الكمبيوتر الخاص بك أثناء غيابك.
إذا كان الكمبيوتر موجودًا على شبكة عامة ، مثل المدرسة أو المكتب ، فيمكنك حماية كلمة المرور
تلك الحسابات مع وصول المسؤول وإعطاء حسابات محدودة فقط للمستخدمين.
استخدم دائمًا كلمة مرور قوية يصعب تخمينها. كلمات مرور قوية تحتوي على مزيج
من الأحرف الأبجدية الرقمية والخاصة التي طويلة بما يكفي لتجنب الجدول قوس قزح
والقوة الغاشمة النهج.
تعطيل الوصول إلى محركات أقراص CD / DVD وأجهزة USB على الشبكات العامة.
قم بتهيئة BIOS لتعطيل التمهيد من USB و CD / DVD والأجهزة المحمولة الأخرى.
حماية كلمة مرور BIOS جهاز الكمبيوتر الخاص بك بحيث لا يكون من الممكن للمهاجمين
لتعديل إعداداتها والوصول إليها.

الفصل 9 - البرامج الضارة

البرامج الضارة هي مصطلح جماعي يستخدم لتمثيل الفيروسات والديدان وبرامج التجسس وغيرها من البرامج الضارة
البرامج هناك على شبكة الإنترنت. بكلمات بسيطة ، أي برنامج مخصص
للتسبب في ضرر مباشر أو غير مباشر لنظام الكمبيوتر ويشار إلى البرمجيات الخبيثة.
يمكن أن تتسبب بعض البرامج الضارة في مشاكل خطيرة مثل تدمير ملفات النظام ،
مما تسبب في تعطيل لتشغيل الكمبيوتر أو جمع معلومات حساسة في حين
قد لا يكون للآخرين سوى تأثير خفيف مثل إعادة توجيه المواقع لتحميل المواد الإباحية
المحتوى أو مزعج المستخدمين مع النوافذ المنبثقة واللافتات.

متغيرات البرامج الضارة والتقنيات الشائعة

بمجرد وصول المتسلل إلى الهدف ولديه امتيازات المسؤول عليه ،
فيما يلي بعض برامج البرامج الضارة التي يمكنه استخدامها للسيطرة بشكل أكبر على
النظام:

فيروس الكمبيوتر

كما نعلم جميعًا ، هذا هو نوع البرامج الضارة التي أصبحت ذات شعبية كبيرة وواحدة من
الموضوع الأكثر مناقشة على نطاق واسع في مجال أمن الكمبيوتر. A **فيروس** هو عادل
برنامج كمبيوتر مصمم للتحكم غير المصرح به للكمبيوتر المصاب
وذلك للتسبب في ضرر لبيانات النظام أو تدهور أدائها.

طريقة التشغيل:

تعمل فيروسات الكمبيوتر عن طريق ربط أنفسهم بملف أو برنامج موجود بالفعل
وتكرر نفسها لتنتشر من كمبيوتر إلى آخر. في معظم الحالات ، فإنها تميل إلى
تصيب الملفات القابلة للتنفيذ التي هي جزء من البرامج الشرعية. لذلك ، كلما كان الملف المصاب
يتم تنفيذه على جهاز كمبيوتر جديد ، ويتم تنشيط الفيروس ويبدأ العمل به
مزيد من التكرار أو التسبب في تلف النظام المقصود.
لا يمكن للفيروس أداء مهمته المتمثلة في الأذى والتكرار إلا إذا سمح له بالتنفيذ.

هذا هو السبب في أن الفيروسات غالباً ما تختار ملفاً قابلاً للتنفيذ كمضيف لها والحصول على المرفقات
لهم. تصنف الفيروسات بشكل رئيسي إلى نوعين:

غير المقيم الفيروسات: هذا النوع من الفيروسات سوف تنفذ جنبا إلى جنب مع المضيف ، وتنفيذ العمل اللازم لإيجاد وإصابة الملفات الأخرى المحتملة وفي النهاية ينقل
السيطرة مرة أخرى إلى البرنامج الرئيسي (المضيف). سيتم تشغيل الفيروس على طول مع ذلك من مضيفها.

الفيروسات المقيمة: في حالة الفيروسات المقيمة ، كلما تم تشغيل البرنامج المصاب بواسطة المستخدم ، يتم تنشيط الفيروس ، ويقوم بتحميل وحدة النسخ المتماثل الخاصة به في الذاكرة ثم ينقل التحكم مرة أخرى إلى البرنامج الرئيسي. في هذه الحالة ، لا يزال الفيروس نشطًا في الذاكرة في انتظار فرصة للعثور على الملفات الأخرى وتصيبها حتى بعد الرئيسية
تم إنهاء البرنامج (المضيف).

الأضرار الناجمة:

من المعروف أن الفيروسات تتسبب في تدمير البيانات والبرامج. في بعض الحالات ، أ الفيروس قد لا يفعل أي شيء آخر غير مجرد تكرار نفسه. ومع ذلك ، فهي مسؤولة عن باستخدام جزء كبير من موارد النظام مثل وحدة المعالجة المركزية والذاكرة مما يؤدي إلى تدهور أداء الكمبيوتر.

ديدان

الديدان هي برامج كمبيوتر مستقلة ذات نية خبيثة تنتشر من واحدة
الكمبيوتر إلى آخر. خلافا للفيروسات ، والديدان لديها القدرة على العمل بشكل مستقل و وبالتالي لا نعلق أنفسهم على برنامج آخر.

طريقة التشغيل:

غالبًا ما تستخدم الديدان شبكة كمبيوتر لنشر نفسها من خلال استغلال الأمان
نقاط الضعف الموجودة داخل أجهزة الكمبيوتر الفردية. في معظم الحالات ، والديدان هي مصممة فقط لتنتشر دون التسبب في أي تغيير خطير في نظام الكمبيوتر.

الأضرار الناجمة:

على عكس الفيروسات ، الديدان لا تسبب ضررا لملفات النظام وغيرها من المهم البرامج. ومع ذلك ، فهي مسؤولة عن استهلاك عرض النطاق الترددي وبالتالي مهينة أداء الشبكة.

أدوات الإدارة عن بعد (RATs)

A **أداة الإدارة عن بعد** (**RAT**) هو قطعة من البرمجيات التي تسمح القراصنة ل السيطرة عن بعد على النظام المستهدف لتنفيذ الأوامر وتنفيذ العمليات عليه. بمساعدة RATs ، يمكن للمتسلل التحكم في النظام المستهدف كما لو كان لديه جسديًا الوصول إليها.

طريقة التشغيل:

يمكن تثبيت RAT يدويًا بواسطة المهاجم عندما يحصل على وصول المسؤول إلى النظام. يمكن أيضًا ربطها ببرامج ضارة أخرى مثل حصان طروادة تسليمها إلى النظام المستهدف. بمجرد تثبيت RAT يمكن أن تسمح على الفور للمتسلل ل السيطرة عن بعد على النظام.

الأضرار الناجمة:

بمساعدة RAT ، يمكن للمهاجم تنفيذ العمليات التالية على الهدف النظام:

مشاهدة أنشطة الشاشة الحية والتقاط لقطات.

قراءة / كتابة / تحميل / تنزيل الملفات والمجلدات.

تثبيت / إلغاء تثبيت برامج ضارة إضافية.

تعديل السجل مثل إضافة / تحرير / حذف الإدخالات.

قم بإيقاف تشغيل / إعادة تشغيل النظام.

كما ترون من القائمة أعلاه ، لا توجد أي عملية لا يمكن للمهاجم القيام بها أداء باستخدام RAT. بعض الأمثلة من **RATs** شعبية تشمل **PsTools**، رادمن و غمين.

ضربة المفتاح قطع الاشجار

برنامج **تسجيل ضغط المفاتيح** (أو المعروف ببساطة باسم **keylogger**) هو برنامج مصمم ل سجل كل ضغط المفاتيح المكتوب على لوحة مفاتيح الكمبيوتر.

طريقة التشغيل:

يمكن تثبيت برنامج keylogger يدويًا من خلال الوصول الفعلي إلى النظام أو

عن بعد باستخدام برامج أخرى مثل RAT. بمجرد اكتمال التثبيت ، كلوغر
يعمل في وضع التخفي الكامل عن طريق إخفاء نفسه من أماكن معروفة مثل
مجلد البرامج ، علبة النظام ، إضافة / إزالة البرامج ، مدير المهام وما إلى ذلك بحيث الضحايا
سيبقى الكمبيوتر غير مدرك لوجوده.

الأضرار الناجمة:

سيقوم كلوغر بالتقاط كل ضغطة على لوحة مفاتيح الكمبيوتر بما في ذلك
كلمات المرور ، تسجيلات البنك ، تفاصيل بطاقة الائتمان ، رسائل البريد الإلكتروني ، محادثة
الدردشة وما إلى ذلك وتخزين
يسجل في مكان آمن بحيث لا يمكن الوصول إليه إلا للمهاجمين. يمكن لبعض keyloggers أيضا
إرسال السجلات عبر البريد الإلكتروني أو تحميلها على حساب FTP الخاص بالقراصنة.
بعض من قطع الاشجار ضربة المفتاح شعبية تشمل **كلوغر النخبة**، **بالطاقة كلوغر** و
كلوغر الفعلي .

برامج التجسس

برامج التجسس هي نوع من البرامج الضارة التي يمكنها جمع معلومات حول أنشطة
الكمبيوتر الهدف دون علم مستخدميها. معظم برامج التجسس تأتي أيضا
محملة مسبقا مع كلوغر مما يجعلها أكثر قوة. هذا النوع من البرامج
غالبًا ما يتم تثبيتها بواسطة مالك أو مسؤول الكمبيوتر من أجل مراقبة
أنشطة المستخدمين على ذلك. يمكن أن يكون أحد الوالدين يحاول مراقبة طفله أو طفلها
صاحب شركة تحاول مراقبة موظفيها. لسوء الحظ ، يمكن أن تستخدم أيضا من قبل
المتسللين والمجرمين للتجسس على مستخدمي الآلات المستهدفة.

طريقة التشغيل:

تم تصميم Spywares للعمل في وضع خفي تمامًا بحيث يكون وجوده
مخفية تماما عن مستخدمي الكمبيوتر. بمجرد تثبيت ، فإنها تراقب بصمت جميع

أنشطة الكمبيوتر مثل ضغطات المفاتيح ، نشاط الويب ، لقطات الشاشة ، رسائل البريد الإلكتروني ، الرسائل الفورية

سجلات وما إلى ذلك يتم تخزين هذه السجلات سرا للوصول في وقت لاحق أو تحميلها على الإنترنت بحيث

مثبت برنامج التجسس يمكنه الوصول إليهم.

الأضرار الناجمة:

بصرف النظر عن المراقبة ، لا تسبب برامج التجسس أي ضرر للكمبيوتر. ومع ذلك، في في بعض الحالات ، قد يتعرض الكمبيوتر المتأثر للتدهور في أدائه.

سنيبيرسبي، **SpyAgent** و **WebWatcher** هي بعض الأمثلة على برامج التجسس الشائعة البرامج.

الجذور الخفية

Rootkit هو نوع خاص من البرامج الخبيثة التي صممها القراصنة لإخفاء بعض برامج مثل برامج التجسس وكلوغرز وغيرها من العمليات من الطرق العادية للكشف وذلك لتمكين الوصول المتميز المستمر إلى الكمبيوتر الهدف.

طريقة التشغيل:

غالبًا ما يتم تثبيت Rootkits بواسطة المهاجم بمجرد حصوله على وصول إلى مستوى المسؤول إلى الهدف. تعمل الجذور الخفية عن طريق تعديل نواة نظام التشغيل نفسه يجعل من الصعب حقا الكشف عنها.

الأضرار الناجمة:

تتسبب Rootkits في أضرار جسيمة للنظام لأنه يعدل نواة نظام التشغيل عمليات. ما لم تتم إزالته بالكامل ، يمكن أن يكون خطيرًا جدًا.

حصان طروادة

و **حصان طروادة** أو ببساطة كما دعا **حصان طروادة** هو نوع من البرامج الضارة التي التنكر نفسه كشيء مشروع أو مفيد. الغرض الرئيسي من حصان طروادة هو الحصول على ثقة المستخدم من خلال إخفاء نفسه كبرنامج مفيد أو أداة مساعدة أخرى ، بحيث يحصل على إذن ليتم تثبيتها. ولكن من النهاية الخلفية ، تم تصميمه لمنح غير مصرح به

السيطرة على الكمبيوتر إلى المتسلل عن طريق تثبيت RAT أو برامج التجسس أو Rootkit.

طريقة التشغيل:

لا يعتمد حصان طروادة على المضيف للقيام بعملياته. لذلك ، على عكس الكمبيوتر
فيروس ، فإنه لا يميل إلى إرفاق ملفات أخرى. غالبًا ما يتم إخفاء طروادة كفيديو
برامج الترميز ، والشقوق البرمجيات ، keygens وغيرها من البرامج المماثلة تحميلها من غير موثوق بها
مصادر. لذلك ، يجب على المرء أن يكون حذرا حول تلك المواقع غير الموثوق بها التي تقدم مجانا التحميلات.
أحد الأمثلة الأكثر شيوعًا هو **Trojan** **DNSChanger** الذي تم تصميمه لاختطافه
خوادم DNS لأجهزة الكمبيوتر الضحية. تم توزيعه من قبل بعض المارقة
المواقع الإباحية مثل برنامج ترميز الفيديو اللازم لعرض المحتوى عبر الإنترنت.

الأضرار الناجمة:

من المعروف أن أحصنة طروادة تسبب مجموعة متنوعة من الأضرار مثل سرقة كلمات المرور وتفاصيل تسجيل الدخول وسرقة الأموال الإلكترونية وتسجيل ضربات المفاتيح وتعديل أو حذف الملفات ،
مراقبة نشاط المستخدم وهلم جرا.

التدابير المضادة

فيما يلي بعض الإجراءات المضادة التي يمكنك اتخاذها لمنع البرامج الضارة
الهجوم على الأنظمة الخاصة بك:
قم بنشر جدار حماية ثنائي الاتجاه يدير حركة المرور الواردة والصادرة.
قم بتثبيت برنامج مكافحة فيروسات جيد وحافظ عليه محدثًا. تشغيل النظام الكامل بشكل دوري بمسح للكشف عن كلوغر وبرامج التجسس والجذور الخفية وإزالتها.
مواكبة على جميع تصحيحات البرامج الأمنية. استخدام التحديثات التلقائية للحفاظ على
نوافذ مصححة لأحدث التهديدات ونقاط الضعف.
قم بتثبيت برامج أمان إضافية مثل برامج مكافحة التجسس ومكافحة keyloggers ومكافحة

الجذور الخفية.
تشغيل بأقل امتياز. تسجيل الدخول كمسؤول فقط عند الحاجة. لأخف وزنا
أنشطة مثل تصفح الإنترنت وقراءة رسائل البريد الإلكتروني لتسجيل الدخول باستخدام حساب له وصول محدود.
مسح البرامج غير المعروفة باستخدام برنامج مكافحة فيروسات محدث قبل تثبيتها
على النظام الخاص بك.
احصل على نسخ احتياطية دورية من نظامك بحيث يحدث في حالة فقد البيانات أو تلفها
البرامج الضارة التي يمكن أن تعود بسهولة إلى تاريخ سابق لحالة العمل العادية.

الفصل 10 - إخفاء المعلومات

بمجرد أن يتمكن المتسللون من الوصول إلى النظام والسيطرة عليه ، فإن الخطوة التالية قد يحاولون القيام بها
القيام به هو إخفاء بعض الملفات الهامة والمعلومات المتعلقة بها. قد يقرر المتسلل إخفاء الملفات للتنفيذ في وقت لاحق أو استخدام نظام الضحية للخطر لتخزين المعلومات سرا بذلك
أنه يمكن الوصول إليها في وقت لاحق وإرسالها إلى الوجهة النهائية حيث يهدف إلى الذهاب. في سنناقش هذا الفصل بعض التقنيات الشائعة لإخفاء الملفات والمعلومات
على النظام. لنبدأ بالأشياء البسيطة ونتقدم تدريجياً إلى أكثر تعقيدًا
التقنيات.

يندوز يخفي السمة

يعد استخدام السمة المخفية المدمجة في Windows الطريقة البسيطة والأسهل للاختباء بها الملفات والمجلدات على النظام. لتمكين السمة المخفية ، فقط اتبع التعليمات كما
المعطى أدناه:

1. انقر بزر الماوس الأيمن على الملف أو المجلد الذي تنوي إخفاءه واختر "خصائص" من القائمة المنبثقة.
2. في نافذة "الخصائص" ، ضمن قسم "السمات" ، حدد مربع الاختيار

"مخفي" وانقر على "موافق".
هذا سيجعل الملف أو المجلد المحدد غير مرئي. لعرض الملفات والمجلدات المخفية
اتبع التعليمات أدناه:
1. افتح "لوحة التحكم" بالنقر فوق الزر "ابدأ"
2. انقر الآن على "المظهر والتخصيص" ثم على "خيارات المجلد".
3. قم بالتبديل إلى علامة التبويب "عرض" ، حدد الخيار "إظهار الملفات والمجلدات ومحركات الأقراص المخفية" ضمن
"الإعدادات المتقدمة" وانقر على "موافق".
هذا يجب إظهار كافة الملفات والمجلدات المخفية. ومع ذلك ، فإن عيب هذه الطريقة
هو أن معظم المستخدمين يدركون هذا ، وبالتالي يمكن بسهولة كشف الملفات المخفية. في
من أجل مواجهة هذا العيب ، بعض أساليب إخفاء المعلومات المتقدمة
مشروح بالاسفل.

NTFS البديل بيانات الجداول

دفق البيانات البديلة (ADS) هو دفق مخفي Windows معتمد على ملف NTFS
النظام المستخدم لتخزين البيانات الوصفية لملف مثل السمات ، وعدد الكلمات ، والوصول و
تعديل الوقت وما إلى ذلك عندما يتم إنشاء ملف على نظام الملفات NTFS ، ويندوز
تلقائيا بإنشاء إعلانات لذلك. حتى في سرد الدليل فقط الملف الفعلي مرئي
ولكن يتم الاحتفاظ إعلاناتها مخفية.
من الممكن إضافة إعلانات إضافية إلى ملف موجود لتخزين المعلومات المخفية فيها
ذلك. يستخدم المتسللون غالبًا هذه التقنية لتخزين الأكواد الخبيثة في الأنظمة المخترقة
دون علم الضحايا.
افترض إذا كنت تريد إخفاء المعلومات داخل صورة أو أي ملف آخر ، فما عليك سوى اتباع
الخطوات المذكورة أدناه:
1. افتح موجه أوامر Windows.
2. اكتب الأمر التالي واضغط على Enter.

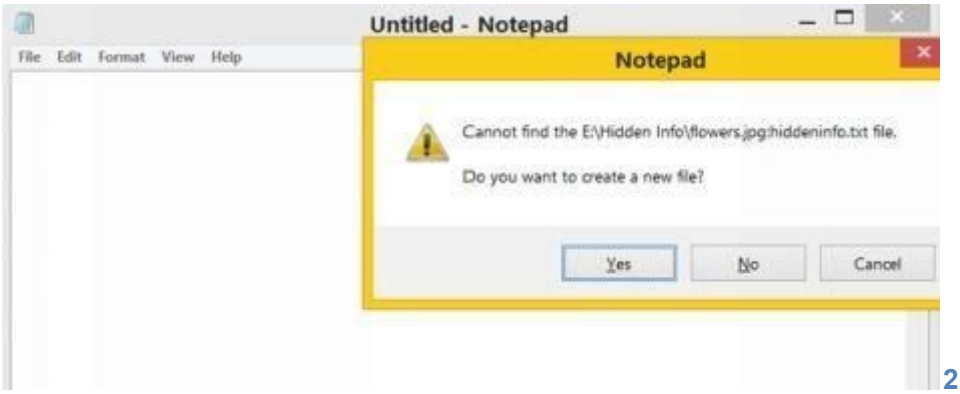
بناء جملة الأوامر: اسم ملف **المفكرة** : ADS-name

مثال القيادة: **notepad** flowers.jpg: hiddeninfo

الشكل 10. 1

كما هو مبين في لقطة أعلاه ، أنا أصدر الأمر أعلاه على **flowers.jpg** موجودة داخل المجلد المسمى " **المعلومات المخفية"** .

3. الآن سيقوم Windows بإنشاء **إعلانات** جديدة للملف المحدد وفتحه في جديد المفكرة مع نافذة رسالة "هل تريد إنشاء ملف جديد؟" كما هو موضح أدناه.



الشكل 10. 2

4. انقر فوق "نعم" ، واكتب المحتوى الذي تريد إخفاءه عليه وبمجرد وجودك القيام به حفظ وإغلاق المفكرة.

5. الآن ، سيتم تخزين كل رسائلك السرية في **إعلانات** جديدة تسمى **hiddeninfo** بالداخل ملف **الزهور** .

بالنسبة إلى العالم الخارجي ، فإن ملف **flowers.jpg** هو مجرد ملف للصور ولكن المتسلل وحده يعلم ذلك

يحتوي على بيانات مخفية داخله. حتى إذا تم نقل الملف إلى نظام آخر (NTFS فقط) ، فإنه لا يزال يحمل المعلومات المخفية جنبا إلى جنب معها.

لعرض المعلومات المخفية ، كل ما عليك فعله هو كتابة الأمر نفسه **كمفكرة**

flowers.jpg: hiddeninfo في موجه الأوامر. هذا سيفتح **الإعلانات** الواردة داخل ملف **flowers.jpg** في مفكرة تعرض كل النص المخفي الذي كان في السابق مخزن.

تقنية **ADS** لها عيب صغير! إذا تم نسخ هذا الملف أو نقله إلى ملف مختلف نظام مثل **FAT32** ، سيتم إسقاط جميع المعلومات **ADS** ومخفية سيتم فقدان المعلومات.

إخفاء المعلومات

إخفاء المعلومات هو وسيلة لإخفاء البيانات حيث يتم إخفاء الرسائل السرية داخل ملفات الكمبيوتر مثل الصور وملفات الصوت ومقاطع الفيديو وحتى الملفات القابلة للتنفيذ ، بحيث

لن يعلم أحد سوى الخالق بوجود معلومات خلسة فيه.

قد تتضمن معلومات إخفاء المعلومات أيضًا استخدام التشفير حيث تكون الرسالة أولاً مشفرة قبل أن يتم إخفاؤها في ملف آخر. عموما ، يبدو أن الرسائل شيء آخر مثل صورة أو صوت أو فيديو بحيث وجود بيانات سرية فيه لا يزال غير متوقع.

الميزة الرئيسية لعلم إخفاء المعلومات عن طرق إخفاء المعلومات الأخرى هي أنه لن تنشأ الشكوك حتى لو كانت الملفات في أيدي طرف ثالث. مختلف التشفير الذي يشفر المعلومات فقط ، يستخدم إخفاء المعلومات كل من التشفير و غموض البيانات في ملف عادي. وهذا يجعل من الصعب الكشف عن إخفاء المعلومات كملفات تبدو طبيعية تماما من الخارج.

تنفذ أدوات إخفاء المعلومات خوارزميات ذكية لتضمين المشفرة بعناية رسائل نصية أو بيانات ثنائية داخل ملفات أكبر أخرى مثل صورة أو صوت أو فيديو أو ملف تنفيذي. ستقوم بعض الأدوات بتضمين البيانات المشفرة في نهاية ملف آخر بحيث ستكون هناك مساحة كافية لتخزين البيانات الأكبر.

هناك العديد من أدوات إخفاء المعلومات المتاحة على الإنترنت ، لكن القليل منها فقط قادر على العمل

لا تشوبه شائبة. لم أجد أي أداة تعمل بشكل مثالي على البيانات الصغيرة والكبيرة. إلى مواجهة هذه المشكلة ، تمكنت من تطوير أداة خاصة بي يمكن أن تعمل بشكل مثالي جميع أنواع الملفات وجميع حجم البيانات. لقد قمت بتسمية الأداة باسم **StegoMagic** . تستطيع قم بتنزيله من الرابط التالي.

تحميل StegoMagic

يحتوي ملف zip على إصدارين من ***StegoMagic*** : ***إصدار*** واحد لتشفير الرسائل النصية والآخر لتشفير الملفات الثنائية. يمكن استخدام ***StegoMagic_TXT*** لإخفاء النص الرسائل في ملفات أخرى مثل صورة أو ملف صوتي. ***StegoMagic_BIN*** يمكن استخدامها ل إخفاء ملف ثنائي في آخر مثل ملف قابل للتنفيذ داخل صورة أو صورة داخل ملف فيديو وهلم جرا.

الشكل 10. 3

مع ***StegoMagic*** ، ليس هناك قيود على حجم ونوع الملف الذي أنت عليه تنوي الاختباء. على سبيل المثال ، يمكنك إخفاء مقطع فيديو بحجم 1 جيجابايت في صورة بحجم 1 ميغابايت أو إخفاء ملف قابل للتنفيذ داخل مستند WORD. الأداة جميلة مباشرة للاستخدام ولا يتطلب أي فهم خاص للمفهوم.

في نهاية عملية التشفير ، سيتم إنشاء مفتاح فك التشفير السري و نفس الشيء مطلوب أثناء عملية فك التشفير.

كيفية استخدام StegoMagic؟

افترض أنك تريد إخفاء رسالة **نصية** داخل. ملف **صورة JPG** :

1. **ضع ملف صورة .JPG والملف النصي (.txt) في نفس المجلد مثل ذلك of *StegoMagic_TXT.exe***
2. قم بتشغيل ***StegoMagic_TXT.exe*** (مع حقوق المسؤول) واتبع الشاشة تعليمات لتضمين الرسالة النصية داخل صورة JPG.
3. قم بتدوين ***مفتاح فك التشفير السري*** .
4. الآن يمكنك إرسال هذه الصورة إلى صديقك عبر البريد الإلكتروني. لفك تشفير الخفية رسالة ، يجب على صديقك تحميل **ملف JPG** على أداة ***StegoMagic*** واستخدامه و ***مفتاح فك التشفير السري*** .

استخدام الأدوات لإخفاء المعلومات

يمكنك أيضًا استخدام العديد من الأدوات والبرامج مفتوحة المصدر لإخفاء الملفات المهمة و المجلدات على نظام معين. فيما يلي قائمة ببعض الأدوات المفيدة التي يمكنك استخدامها:

1. إخفاء مجلد الحرة

هذه أداة مجانية لنظام التشغيل Windows يمكنها إخفاء أي عدد من المجلدات وصنعها الذهاب غير مرئية تماما للآخرين. لديك أيضا خيار لحماية كلمة المرور برنامج لسلامة إضافية.

2. الحكيم مجلد المخفي

Wise Folder Hider هو برنامج مجاني يستخدم لإخفاء مجلد (**مجلدات)ك** الشخصية أو الملف (الملفات) الخاص بك إلى في مكان آخر على جهاز الكمبيوتر الخاص بك أو في الأجهزة القابلة للإزالة ، وبهذه الطريقة يمكنك حماية جهازك الخصوصية مع كلمات المرور باتباع الخطوات السهلة.

3. WinMend مجلد المخفية

WinMend Folder Hidden هو أداة إخفاء للملفات / المجلدات المجانية. مع ضمان المطلق سلامة النظام ، يمكن لهذا التطبيق إخفاء الملفات والمجلدات بسرعة على الأقسام المحلية و / أو

على الأجهزة القابلة للإزالة. سيتم إخفاء الملفات / المجلدات المخفية بأمان سواء كان محرك الأقراص
الوصول إليها في نظام تشغيل آخر على نفس الكمبيوتر أو إعادة تثبيته على آخر
الحاسوب. يمكنك تعيين كلمة مرور لهذا التطبيق. البيانات المخفية يمكن عرضها و
غير مخفي فقط عندما يقوم المستخدم بإدخال كلمة مرور صالحة.

الفصل 11 - استنشاق

يشير **استنشاق** (يطلق عليه أيضًا **استنشاق الحزمة**) إلى استخدام جهاز أو برنامج ل
التقاط المعلومات الحيوية من حركة مرور الشبكة السلكية أو اللاسلكية باستخدام اعتراض البيانات
تقنية. الهدف من الاستنشاق هو سرقة معلومات مختلفة مثل كلمات مرور
تطبيقات مثل البريد الإلكتروني و FTP والمحتويات في البريد الإلكتروني ومحادثات الدردشة
والملفات الموجودة
نقل من نظام إلى آخر وهلم جرا.
البروتوكولات التي ترسل وتستقبل البيانات بتنسيق خام بدون تشفير هي بسهولة
عرضة لهجوم استنشاق. فيما يلي قائمة ببعض البروتوكولات الشائعة
عرضة لاستنشاق:

Telnet: ضغطات المفاتيح بما في ذلك أسماء المستخدمين وكلمات المرور.
HTTP: البيانات المرسلة بنص واضح.
SMTP: كلمات المرور والبيانات المرسلة بنص واضح.
FTP: كلمات المرور والبيانات المرسلة بنص واضح.
POP: كلمات المرور والبيانات المرسلة بنص واضح.

أنواع الاستنشاق

يتم تصنيف الاستنشاق بشكل أساسي إلى نوعين على النحو التالي:

استنشاق السلبي

استنشاق السلبي بسيط إلى حد ما والذي ينطوي فقط على الاتصال بالشبكة المستهدفة و
في انتظار وصول الحزم إلى مضيفك لاستنشاقها. هذا النوع من استنشاق يعمل فقط

في بيئة شبكة غير مخزنة حيث يتم ربط المضيفين الفرديين
باستخدام **محور** .
في نوع لوحة الوصل من بيئة الشبكة ، يتم إرسال حركة المرور (الحزم) من جميع المضيفين إلى جميع المنافذ
على الشبكة. هذا يجعل من الممكن لجهاز الكمبيوتر الخاص بالقراصنة اعتراض و
حزم الشم التي تنتمي إلى أجهزة الكمبيوتر الأخرى على نفس الشبكة.
من أجل تنفيذ استنشاق السلبي ، سوف هوك القراصنة ببساطة ربط جهاز الكمبيوتر المحمول الخاص به إلى
شبكة وتشغيل برنامج استنشاق لالتقاط بصمت الحزم التي تصل إلى ميناءه.
نظرًا لأن الاستنشاق السلبي يعمل ببساطة عن طريق استغلال الثغرات الموجودة لدى unswitched
شبكات دون إجراء تعديلات إضافية ، غالبا ما يكون من الصعب الكشف عنها.

استنشاق نشط

استنشاق نشط هو الذي يتم تنفيذه في كثير من الأحيان على بيئة شبكة تبديل.
هنا يتم ربط المضيفين الفرديين على الشبكة باستخدام **رموز التبديل** التي تحافظ على السجل من عناوين MAC (عناوين الأجهزة) لجميع المضيفين المتصلين بها. مع هذه المعلومات يمكن للمفتاح تحديد النظام الذي يجلس على أي منفذ بحيث عندما تكون الحزم
تلقى يتم تصفيتها بذكاء وإعادة توجيهها فقط إلى المنافذ المقصودة.
هذا يجعل الحزمة استنشاق صعبة للغاية على شبكة تبديل كما حركة المرور من الجميع المضيفين لا يتدفق إلى جميع المنافذ على الشبكة. ومع ذلك ، لا يزال من الممكن بنشاط حزم شم على الشبكات بتبديل باستخدام تقنيات مثل **التسمم ARP** و **MAC الفيضانات** التي تناقش أدناه.

تقنيات الاستنشاق الفعال

نظرًا لأن معظم شبكات الكمبيوتر تستخدم اليوم مفاتيح بدلاً من لوحات الوصل ، فإن عملية الاستنشاق النشطة تثبت ذلك
أكثر جدوى في ظل ظروف عملية. وفيما يلي بعض من المهم

التقنيات المستخدمة في *استنشاق نشط* :

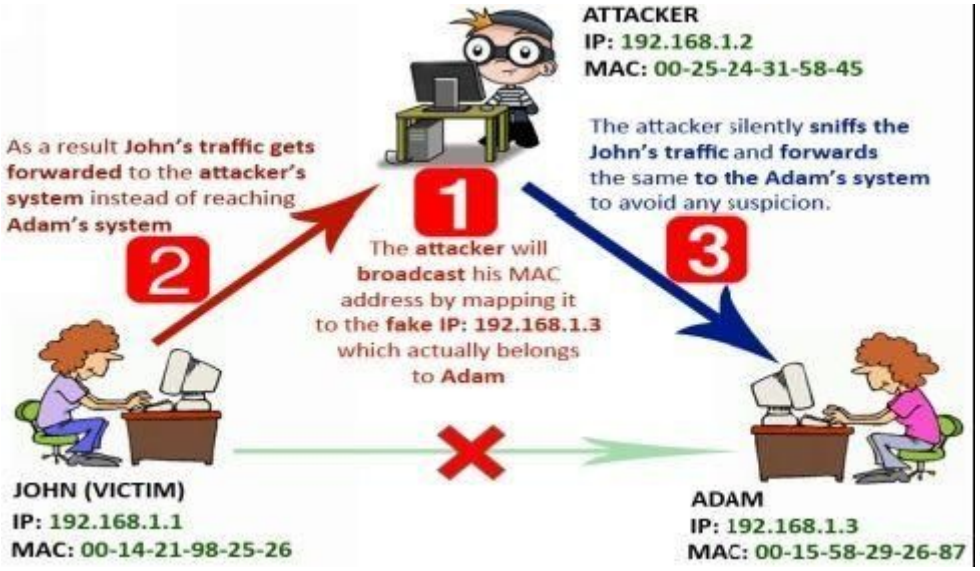
تسمم ARP

قبل الخوض في عملية **التسمم ARP** ، دعونا أولاً نحاول أن نفهم ما **ARP** يعني في الواقع.

ما هو ARP؟

ARP الذي يمثل **بروتوكول تحليل العنوان** هو المسؤول عن تحويل *IP* *العنوان* إلى *عنوان* فعلي يسمى *عنوان MAC* في الشبكة. كل مضيف على الشبكة يحتوي على عنوان MAC المرتبط به وهو مضمن في مكون الجهاز الخاص به كما **NIC** (وحدة تحكم واجهة الشبكة). يتم استخدام عنوان MAC هذا لتحديد جسديا المضيف على الشبكة والحزم إلى الأمام لذلك.

عندما يريد أحد المضيفين إرسال بيانات إلى آخر ، فإنه يبث رسالة ARP إلى عنوان IP العنوان الذي يطلب العنوان الفعلي المقابل له. المضيف مع عنوان IP في يرد الطلب بعنوانه الفعلي وبعدها يتم توجيه البيانات إليه. هذه يتم تخزين طلب ARP مؤقتًا وتخزينه في جدول ARP لتسهيل عمليات البحث الإضافية. لذلك ، **التسمم ARP** (المعروف أيضا باسم **خداع ARP**) هو المكان الذي يذهب القراصنة ويتلوث الإدخالات في جدول ARP لإجراء اعتراض البيانات بين جهازين في شبكة الاتصال. لهذا ، عندما يرسل مضيف مصدر رسالة ARP يطلب فيها MAC عنوان المضيف الهدف ، يقوم المتسلل ببث عنوان MAC الخاص بجهازه حتى يتسنى للجميع يتم توجيه الحزم له وليس المضيف الهدف المقصود لتلقي. ال يوضح الشكل التالي توضيحًا لكيفية إجراء التسمم ARP.



الشكل 11. 1

كما هو مبين في المثال أعلاه **جون** ، **آدم** و **المهاجم** جميعا ثلاثة نفس

شبكة الاتصال. يقرر جون إرسال رسالة إلى آدم حيث يعرف حاسوبه عنوان IP

عنوان آدم كما 192.168.1.3 ولكن لا يعرف عنوان MAC الخاص به. لذلك سوف تبث

رسالة ARP تطلب عنوان 192.168.1.3 MAC. ولكن ، سوف المهاجم

تسمم جدول ذاكرة التخزين المؤقت لـ ARP عن طريق خداع عنوان IP الخاص بـ Adam ورسم خريطة له (المهاجم)

عنوان MAC إلى. نتيجة لذلك ، يتم توجيه حركة مرور John إلى كمبيوتر المهاجم

حيث يستنشق كل المعلومات الحيوية ويرسلها إلى آدم نفسه

كل شيء يبدو طبيعيا.

أدوات للتسمم أبريل

فيما يلي بعض الأدوات التي يمكن استخدامها لتنفيذ تسمم ARP:

1. Ettercap

هذه أداة أمان شبكة مفتوحة المصدر تستخدم لأداء الاستنشاق

الهجمات المتوسطة على الشبكة المحلية. انها قادرة على اعتراض حركة مرور الشبكة و

التقاط المعلومات الحيوية مثل كلمات المرور ورسائل البريد الإلكتروني. وهو يعمل عن طريق وضع الشبكة

واجهة الجهاز في وضع مختلط وتسمم إدخالات ARP من الأجهزة المستهدفة

لاستنشاق حركة المرور حتى على بيئة الشبكة التبديل. يمكن تنزيله من الرابط أدناه:

تنزيل Ettercap: http://ettercap.github.io/ettercap/

2. نايتوك

هذه هي أداة بسيطة لأداء خداع ARP واستنشاق كلمة المرور. لديها القدرة لالتقاط كلمات المرور من نماذج تسجيل الدخول على الويب المنفذة على بروتوكولات مثل HTTP و FTP و SMTP و POP. يمكن تنزيله من الرابط أدناه:

تحميل Nightawk: https://code.google.com/p/nighthawk/

الفيضانات MAC

فيضان MAC هو نوع آخر من تقنيات الاستنشاق المستخدمة في شبكة مبدلة البيئة التي تنطوي أساسا فيضان التبديل مع العديد من لا لزوم لها الطلبات. منذ رموز التبديل لديها قدرات الذاكرة والمعالجة محدودة لتعيين MAC عناوين الموانئ المادية ، يحصلون على الخلط ويضرب قيودهم.

عندما تضغط رموز التبديل على قيودها ، فإنها ستقع في حالة مفتوحة وتبدأ في العمل بشكل عادل مثل المحور. وهذا يعني ، يتم توجيه كل حركة المرور إلى جميع المنافذ مثلما هو الحال في حالة شبكة غير مخزنة حتى يتمكن المهاجم من استنشاق المعلومات المطلوبة بسهولة.

أدوات لفيضان MAC

EtherFlood هو أداة سهلة الاستخدام ومفتوحة المصدر لتنفيذ فيضانات MAC في تبديل بيئة الشبكة. تم ذكر رابط التنزيل EtherFlood أدناه:

تنزيل EtherFlood: http://ntsecurity.nu/toolbox/etherflood/

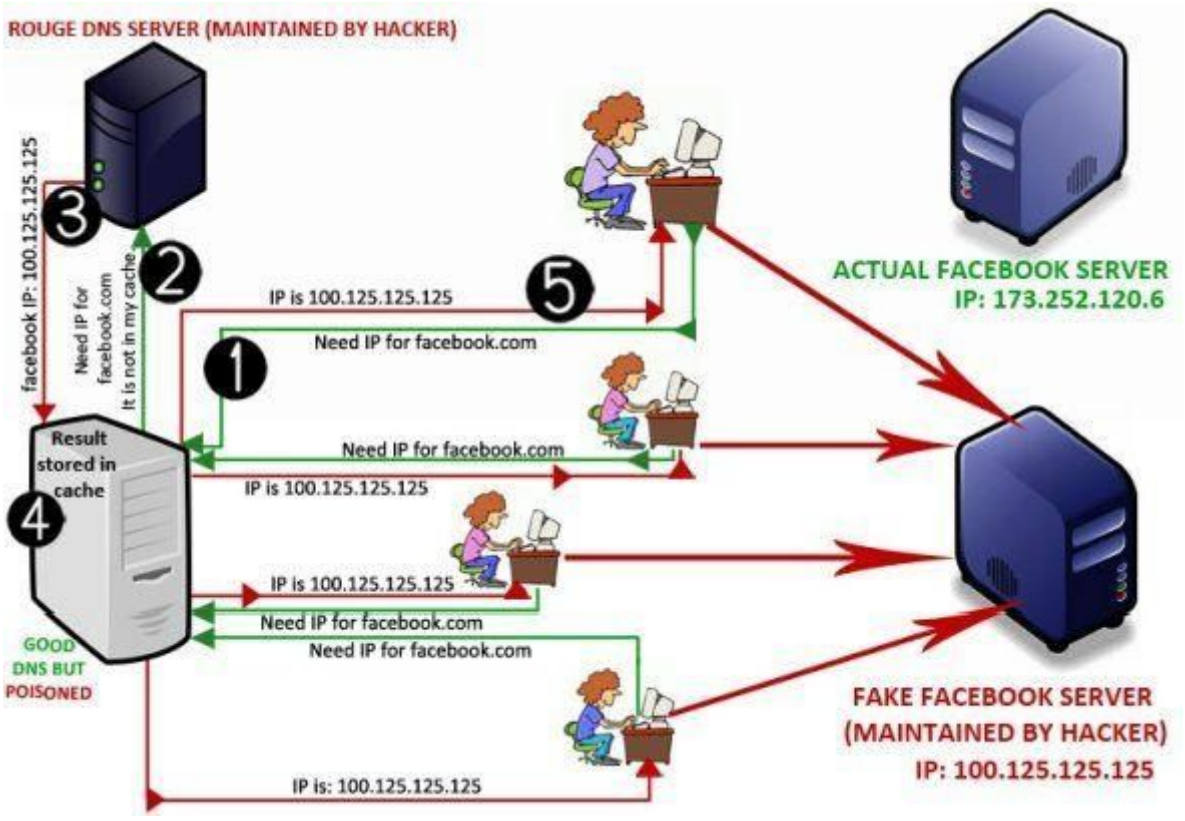
تسمم ذاكرة التخزين المؤقت DNS

تسمم ذاكرة التخزين المؤقت DNS (المعروف أيضًا باسم **خداع DNS**) هو تقنية مشابهة لـ *ARP*

التسمم حيث يتم تلوث ذاكرة التخزين المؤقت لمحلل نظام اسم المجال (DNS) إدخال البيانات التلاعب فيه. لذلك ، كلما حاول المستخدمون الوصول إلى المواقع ، فإن خادم DNS المسموم يقوم بإرجاع عنوان IP غير صحيح وبالتالي توجيه المستخدمين إلى

أجهزة الكمبيوتر المهاجم.
DNS مسؤول عن تعيين أسماء المجال القابلة للقراءة البشرية إلى
عناوين المقابلة. من أجل تحسين سرعة القرار ، خوادم DNS في كثير من الأحيان
مخبأ نتائج الاستعلام التي تم الحصول عليها سابقا. قبل التخزين المؤقت أو إعادة توجيه الاستعلام
النتائج ، خادم DNS لديه للتحقق من صحة الاستجابة التي تم الحصول عليها من خوادم أخرى
لجعل
تأكد من أنه جاء من مصدر موثوق.
ومع ذلك ، يتم تكوين بعض الخوادم بميزات أمان أقل حيث لا تعمل
التحقق من صحة مصدر الاستجابة بشكل صحيح. يمكن للقراصنة استغلال هذه الثغرة الأمنية ل
إدخال سجلات ضارة إلى ذاكرة التخزين المؤقت DNS لإعادة توجيه مجموعة كبيرة من الإنترنت
المستخدمين لأجهزة الكمبيوتر الخاصة بهم. عندما يُقال أن ذاكرة التخزين المؤقت لنظام أسماء
النطاقات (DNS) قد تسممت ، فإنها ستؤثر على كل ذلك
مستخدمو الإنترنت الذين قاموا بتكوين أنظمتها لاستخدامها كخادم DNS الخاص بهم. ال
يوضح الشكل التالي عمل هجوم تسمم ذاكرة التخزين المؤقت DNS.

الشكل 11. 2



كما هو موضح في الشكل أعلاه ، سيقوم المستخدم بتقديم طلب إلى خادم DNS لحله "facebook.com". نظرًا لأن خادم DNS لا يحتوي على IP في ذاكرة التخزين المؤقت الخاصة به ، فإنه يعيد توجيه

نفس الطلب إلى خادم DNS المقبل. الآن ، خادم DNS روج يلتقط الطلب و

الردود باستخدام عنوان IP مزيف للاستعلام "facebook.com". دون التحقق من صحة في الواقع

استجابة ، يقوم خادم DNS بإعادة توجيه النتيجة إلى المستخدم ويخزن النتيجة أيضًا في مخبأ. نتيجة لذلك ، يتم تسميم ذاكرة التخزين المؤقت.

يتم توجيه المستخدم الآن نحو خادم "Facebook" **المزيف الذي** يديره القراصنة

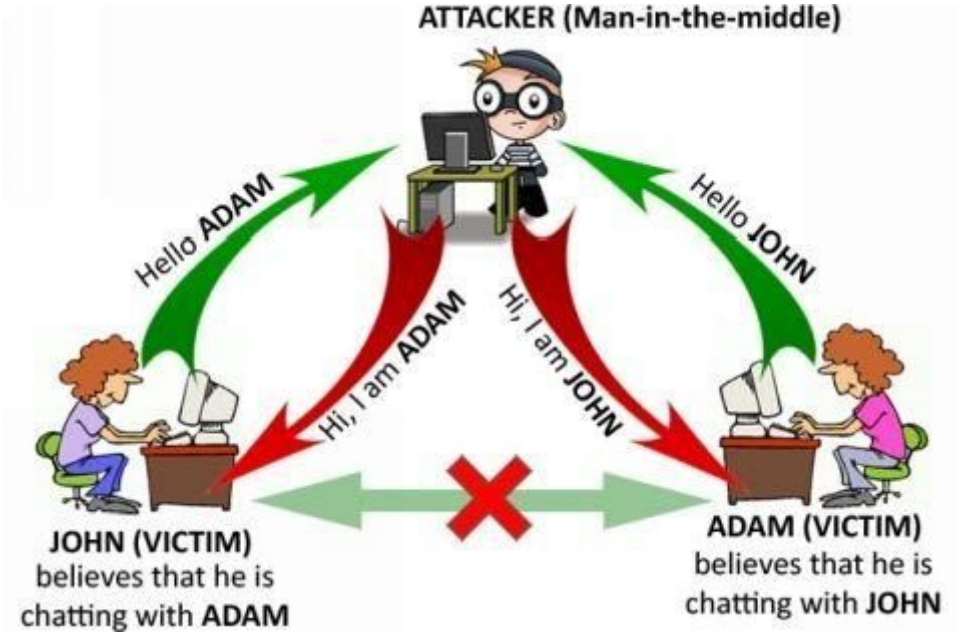
بدلا من الحقيقي. جميع الطلبات اللاحقة من المستخدمين الآخرين لـ "facebook.com" هي تم الرد عليها أيضًا من قِبل خادم نظام أسماء النطاقات المخترق باستخدام بيانات ذاكرة التخزين المؤقت المسمومة.

وبهذه الطريقة ، يمكن للمتسلل اختراق مجموعة كبيرة من الأشخاص واختطافهم معلوماتهم الشخصية مثل كلمات المرور ورسائل البريد الإلكتروني وتسجيلات الدخول البنكية وغيرها من البيانات القيمة.

رجل في منتصف الهجوم

يشار إلى **رجل في الوسط** بنوع من الهجوم حيث يعترض المهاجم على استمرار التواصل بين مضيفين في الشبكة مع القدرة على شم البيانات أو التلاعب في الحزم المتبادلة بين طرفين متواصلين. هذا الهجوم هو تشبه إلى حد ما تلك الموضحة في الشكل 11.1 من القسم السابق.

مثال جيد آخر على هجوم الرجل في الوسط هو التنصت النشط الذي تم تنفيذه من قبل المهاجم من خلال إجراء اتصالين مستقلين مع الضحايا لجعلهم نعتقد أنهم يتحدثون مع بعضهم البعض. لكن المحادثة بأكملها هي في الواقع يسيطر عليها المهاجم كما هو موضح في الشكل التالي 11.3.



الشكل 11. 3

أدوات للتطفل

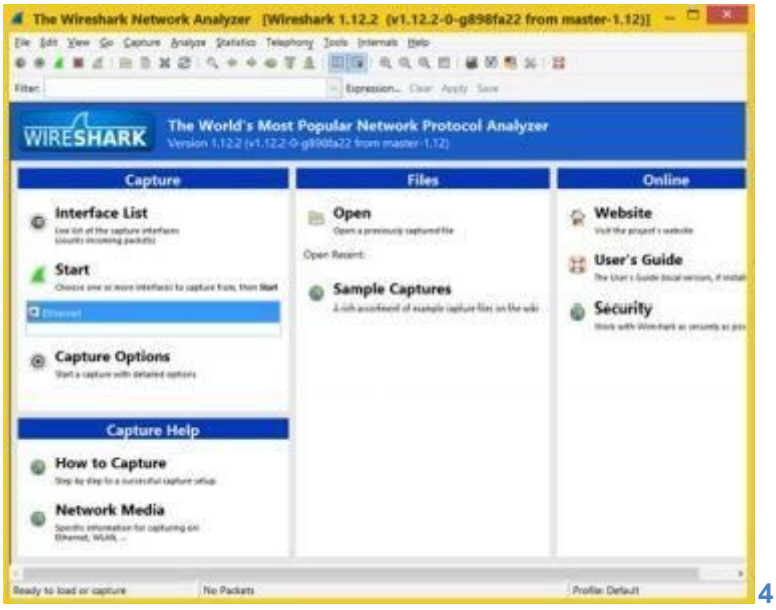
بعد أن نذهب إلى حد بعيد في المفاهيم النظرية لاستنشاق ، دعونا الآن ننظر في بعض أدوات الاستنشاق الشائعة وتعلم كيفية استخدامها لتنفيذ أنواع مختلفة من الهجمات.

يريشارك

Wireshark هو برنامج مجاني لتحليل الرزم مفتوح المصدر يستخدم للشبكة استكشاف الأخطاء وإصلاحها والتحليل. وهو متاح لتشغيل كل من ويندوز ولينكس أنظمة ويمكن تحميلها من الرابط التالي:

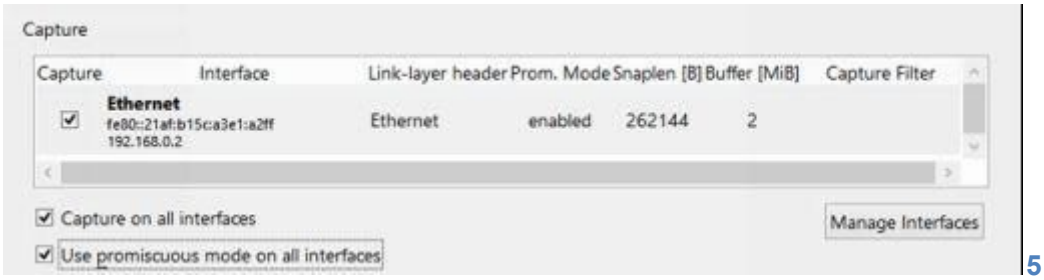
تحميل WireShark: https://www.wireshark.org/download.html

بمجرد تثبيت **WireShark** على كمبيوتر يعمل بنظام Windows ، ابدأ تشغيل البرنامج من خلال تشغيله مع امتيازات المسؤول.



الشكل 11. 4

من خيارات القائمة ، انقر فوق "التقاط" وحدد "خيارات" من القائمة المنسدلة قائمة طعام. سيعرض هذا قائمة بأجهزة الواجهة المتاحة للاستنشاق.



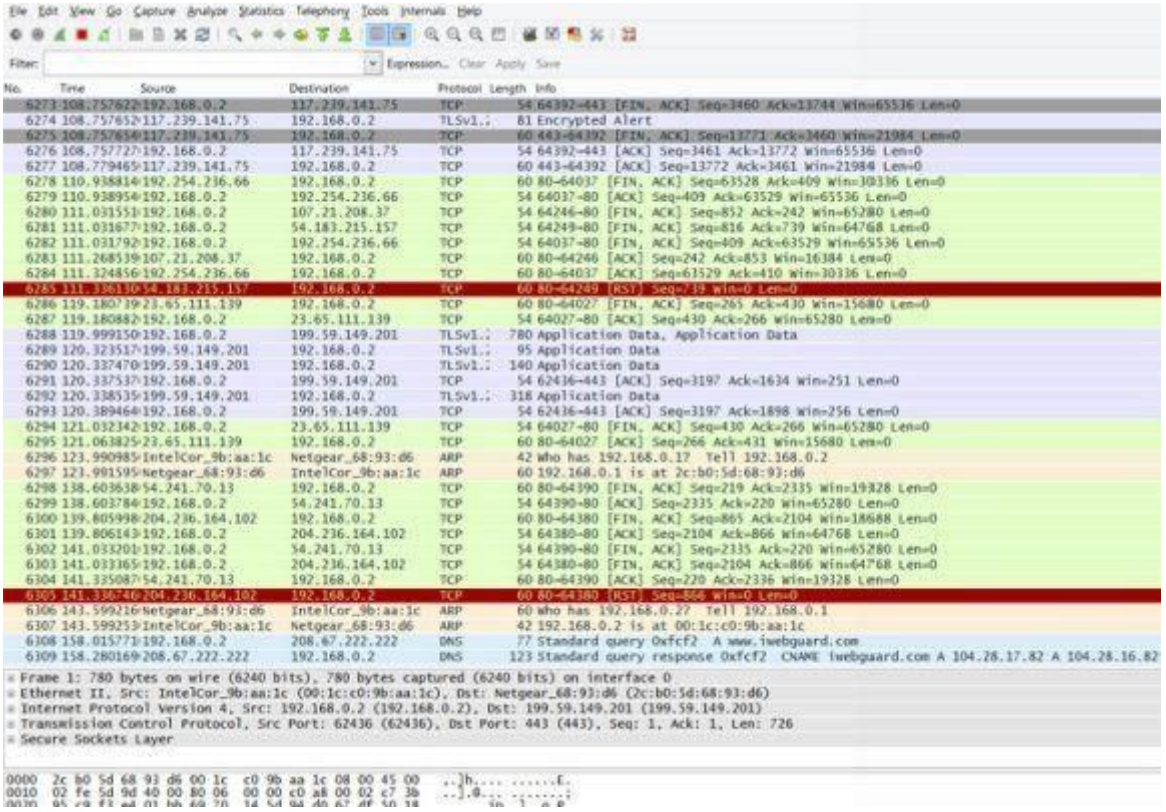
الشكل 11. 5

يمكنك إما اختيار جهاز معين أو اختيار الالتقاط على جميع الواجهات. أيضا جعل تأكد من تنشيط "الوضع المختلط". عند الانتهاء ، انقر فوق الزر "ابدأ"

لبدء عملية استنشاق.

سيبدأ هذا في التقاط كل حركة المرور الواردة والصادرة على الشبكة كما هو موضح في الشكل 11.6 أدناه:

الشكل 11. 6



قم بتشغيل هذه الأداة طالما أردت وعندما تشعر أنك قد انتهيت من الالتقاط

بيانات كافية ، قم بإيقاف عملية الاستنشاق عن طريق الضغط على زر "إيقاف" المعروض باللون الأحمر

اللون في الأعلى.

من أجل تحليل البيانات التي تم التقاطها ، سوف تضطر إلى تعيين عوامل تصفية لتصفية نوع البيانات التي تبحث عنها. على سبيل المثال ، إذا كان أحد يبحث عن التقاط كلمات المرور من نماذج تسجيل الدخول التي يتم إرسالها عادة باستخدام طريقة طلب HTTP POST ، يمكنك تعيين عامل التصفية كـ **"http.request.method == "POST** . هذا سيساعدك على تضييق نتائجك و

تجد ما تبحث عنه.

بمجرد تعيين عامل التصفية ، انقر بزر الماوس الأيمن على النتيجة المرغوبة التي تريد تحليلها وتحديدها

"اتبع TCP Stream". سيؤدي ذلك إلى فتح دفق TCP بأكمله في نافذة جديدة. هنا يمكنك تحليل البيانات بعناية لمعرفة كلمة المرور التي أدخلها المستخدمون في نماذج تسجيل الدخول غير المشفرة كما هو موضح في نموذج لقطة أدناه.

الشكل 11. 7

يمكنك استخدام عوامل تصفية مختلفة لتحليل أنواع مختلفة من البيانات. على سبيل المثال إذا كنت تريد

لتحليل نتائج FTP ، اضبط المرشح كـ **ftp** واتبع تدفق TCP.

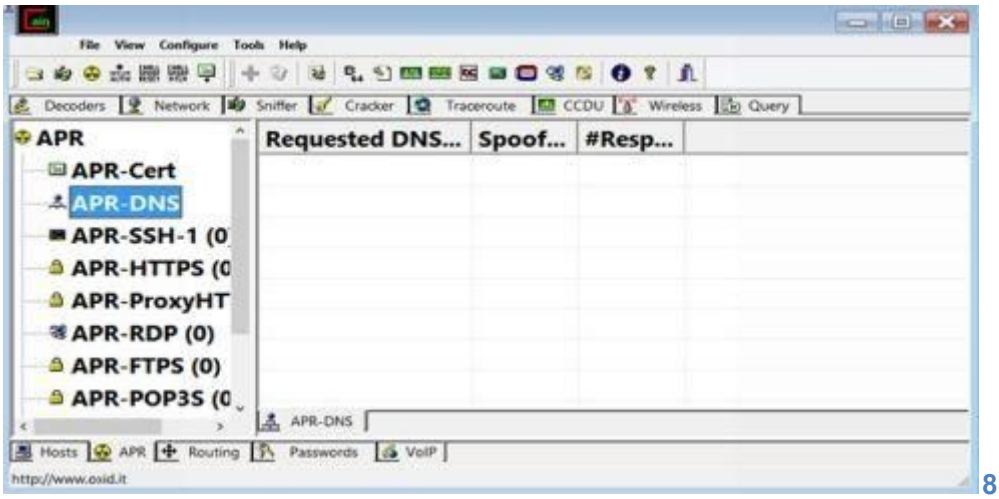
قابيل وهابيل

هذا هو آخر الشم شبكة قوية والتي لديها العديد من الميزات المضمنة الأخرى مثل

تكسير كلمة المرور والتسمم ARP والخداع MAC. يثبت كأداة الكل في واحد ل

تنفيذ هجمات مختلفة مثل استنشاق ، هجوم رجل في منتصف وذاكرة التخزين المؤقت ARP

تسمم.



الشكل 11. 8

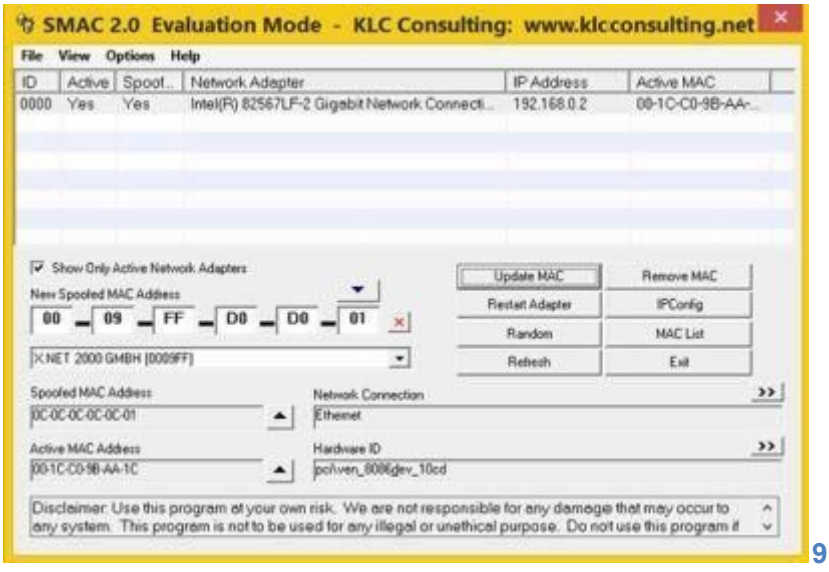
يمكنك تنزيل هذه الأداة من الرابط التالي:

قم بتنزيل Cain & Abel: http://www.oxid.it/cain.html

SMAC

SMAC هي أداة مفيدة تتيح لك محاكاة ساخرة لعنوان MAC على جهازك. عن طريق هذه الأداة من الممكن تعيين عنوان MAC الذي تختاره بحيث تخدع الآخرين بسهولة آلات على الشبكة لإرسال المعلومات الخاصة بهم إلى جهازك.

تُظهر اللقطة التالية أداة SMAC قيد التنفيذ:



الشكل 11. 9

فيما يلي رابط التنزيل لـ SMAC:

تنزيل SMAC: http://www.klcconsulting.net/smac/

التدابير المضادة

بعد معرفة طرق الاستنشاق المختلفة والأدوات المستخدمة لتنفيذها ، إنها كذلك الوقت لإلقاء بعض الضوء على التدابير المضادة المحتملة التي يمكن اتخاذها لمنع هذا الهجمات على شبكتك.

تقييد الوصول المادي إلى الشبكة للمستخدمين غير المقصودين. هذا سوف يوقف المهاجم من تثبيت حزمة الشم على الشبكة.

استخدم التشفير على الشبكة حتى إذا تمكن المهاجم من استنشاق الحزم ، وقال انه لن يكون قادرا على رؤية المعلومات في شكل نص عادي.

إضافة عنوان MAC الخاص بالبوابة إلى ذاكرة التخزين المؤقت لـ ARP بشكل دائم المهاجم من ARP خداع البوابة.

في حالة وجود شبكة صغيرة باستخدام عناوين IP ثابتة وجداول ARP الثابتة سوف تمنع المتسللين من إضافة إدخالات ARP المخادعة.

في حالة وجود شبكة كبيرة تثبيت رموز التبديل التي تأتي مع ميزات أمان المنفذ الذي يجعل من المستحيل محاكاة ساخرة.

استخدم أدوات مثل **Arpwatch** أو **IDS** (نظام كشف التسلل) لمراقبة و الكشف عن أنشطة الاستنشاق على الشبكة.

الفصل 12 - الحرمان من الخدمة

في هذا الفصل ، سنلقي نظرة فاحصة على ما هو بالضبط **رفض الخدمة (DoS)** الهجمات ، وأنواعها المختلفة والأدوات المستخدمة لتنفيذها. في السنوات الأخيرة ، دوس لقد نمت الهجمات ببساطة من مجرد إزعاج إلى تهديدات أكثر جدية وتميزًا لمواقع الأعمال والتجارة الإلكترونية. هذا هو نوع الهجوم الذي لديه المتسللين تم استخدامه بنجاح لإسقاط موفري خدمات الإنترنت الرئيسيين مثل *Yahoo!* و *eBay* و لاعبين كبار آخرين. لذلك ، وجود فهم واضح لهجمات DoS وعملهم يبدو المبدأ أساسيًا للغاية لأي شخص يحتاج إلى التفوق في مجال الأخلاقيات القرصنة.

ما هو الهجوم على الخدمة (DOS)؟

و **رفض الخدمة (دوس)** الهجوم هو محاولة لجعل نظام أو خدمة أو شبكة غير قابل للاستخدام بالكامل للمستخدمين المقصودين أو يبطئ من أدائه بشكل ملحوظ الحمولة الزائدة مواردها.

في معظم الحالات ، إذا كان المهاجم غير قادر على الوصول غير المصرح به إلى النظام المستهدف يقرر في النهاية تنفيذ هجوم DoS بمحاولة تعطل موارده. في أعقاب يمكن أن يؤدي هجوم DoS إلى خسائر مالية خاصة إذا كان موقع الويب أو الخادم المتأثر هو المرتبطة بأنشطة التجارة الإلكترونية. قد يؤثر أيضًا على شهرة الشركة أو المنظمة التي أصبحت ضحية للهجوم لأن هناك فرصة واضحة للناس فقدان الثقة في استخدام خدماتها.

أهداف هجمات حجب الخدمة

الهدف من هجوم DoS ليس الحصول على وصول غير مصرح به إلى النظام ولكن إلى منع المستخدمين الشرعيين من خدمتها من الوصول إليها. لإنجاز هذا ، مهاجم قد تستخدم وسائل مختلفة مثل:

محاولة **إغراق حركة المرور** إلى الشبكة المستهدفة لجعلها غير قابلة للوصول إليها المستخدمين المستهدفين.

محاولة **تعطيل الاتصالات** بين جهازين على الشبكة والتي قد يؤدي إلى الحرمان من الخدمة.

محاولة **منع فرد معين** من الوصول إلى الخدمة أو **تعطيلها فقط خدمة محددة** من الوصول إليها.

هل تقنيات الهجوم

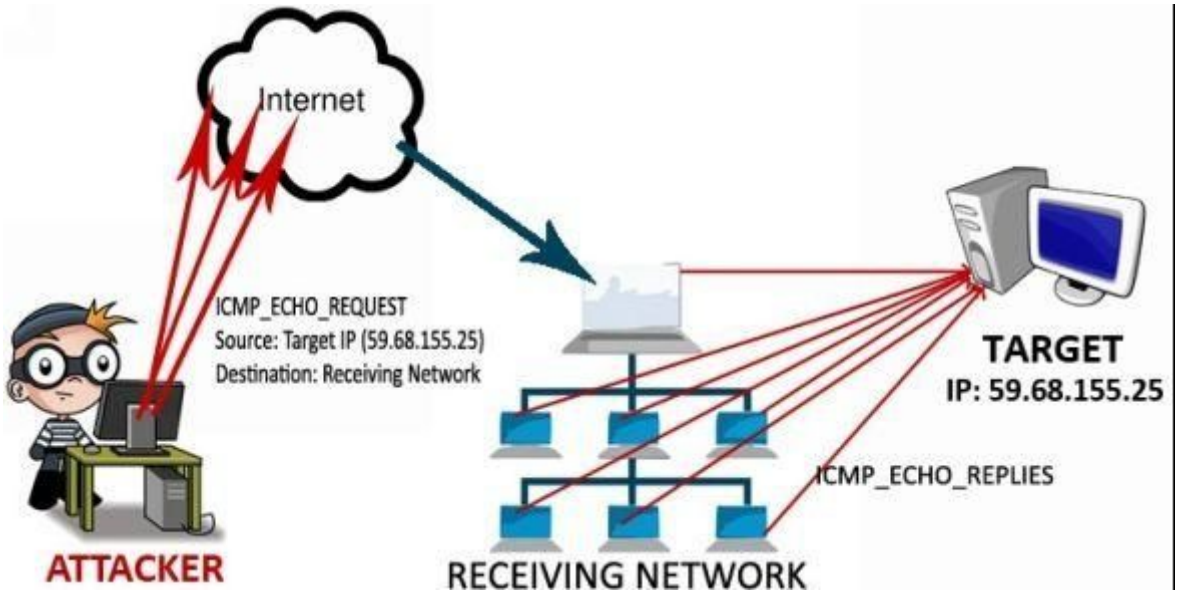
فيما يلي بعض الأساليب الشائعة المستخدمة في هجوم رفض الخدمة:

1. هجوم سنفور (فيضان ICMP)

في هذا النوع من هجمات حجب الخدمة ، يقوم المهاجم ببث قدر كبير من التحكم في الإنترنت بروتوكول رسائل (ICMP) صدى طلب الحزم لشبكة الكمبيوتر مع IP المخادعة عنوان المضيف الهدف (الضحية). سيؤدي ذلك إلى إغراق المضيف الهدف بالكثير من ردود ping

(ردود صدى ICMP) من الشبكة مما يجعل من المستحيل التعامل معها. يوجد ايضا متغير من هجوم smurf يسمى هجوم **fraggle** حيث يتم استخدام حزم UDP بدلاً من حزم ICMP. يوضح الشكل التالي آلية هجوم الحوت:

الشكل 12. 1



2. بينغ الموت (POD)

في هذا النوع من الهجوم ، يرسل المهاجم عن قصد حزمة IP أكبر من المسموح بها حجم 65.535 بايت. نظرًا لأن الحجم يتجاوز الحد الأقصى المسموح به ، يتم تقسيمه عبر حزم IP متعددة تعرف باسم الأجزاء ويتم إرسالها إلى المضيف الهدف. ومع ذلك ، عندما يحاول الهدف إعادة تجميع الحزمة في نهايتها ، وتضيف الأجزاء إلى أكثر من حجم المسموح به من 65535 بايت. عدم القدرة على التعامل مع الحزم كبيرة الحجم ، التشغيل سيقوم النظام بتجميد أو إعادة تشغيل أو ببساطة تعطل وبالتالي تسبب في جميع الخدمات التي تعمل عليه ل

تصبح غير متوفرة للمستخدمين الشرعيين.

بهذه الطريقة ، يصبح المهاجم ناجحًا في التسبب في رفض الخدمة باستخدام الأمر **ping** تقنية **الموت** .

3. هجوم دمعة

ينطوي هجوم الدمعة على إرسال أجزاء IP ذات حمولة كبيرة وتداخل

قيمة الإزاحة خاصة في الجزء الثاني أو الأحدث. إذا كان نظام التشغيل المتلقي هو غير قادر على تجميع الحزم وفقا لذلك ، يمكن أن يؤدي إلى تعطل النظام.

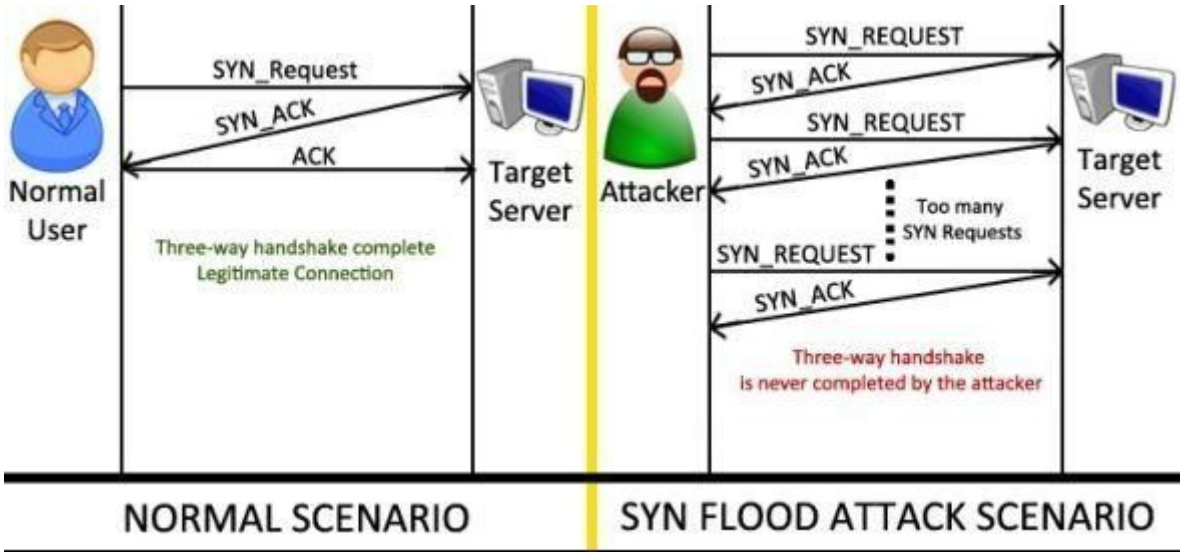
4. SYN الفيضان الهجوم

يستغل هجوم الفيضان SYN ضعف معروف في تسلسل اتصال TCP يسمى "المصافحة الثلاثية". وفقًا لهذا ، يرسل المضيف **طلب SYN** إلى الهدف الخادم الذي يستجيب مع **SYN-ACK** العودة إلى المضيف. وأخيرا المضيف الطالبة يرسل **استجابة ACK** مرة أخرى إلى الخادم الذي يكمل التعارف الثلاثي عملية لتأسيس الاتصال.

ومع ذلك ، في حالة حدوث هجوم SYN ، يتم إرسال عدد كبير من طلبات TCP SYN وهمية إلى الخادم الهدف ولكن استجابة SYN-ACK المرسلة من الخادم لم تتم الإجابة عنها. في بعض الأحيان قد يستخدم المهاجم عنوان IP المخادع أثناء إرسال طلب SYN. لكل طلب SYN من المهاجم ، يخصص خادم الضحية الموارد والاحتفاظ بها في انتظار ACK من المصدر الطالب (المهاجم). لأنه لم يتم تلقي ACK ، يحصل غمرت الخادم مع كمية كبيرة من اتصالات نصف مفتوحة مما يؤدي إلى

استنفاد الموارد مما أدى إلى رفض الخدمة. يتضح الهجوم الفيضانات SYN في الشكل التالي.

الشكل 12. 2



أدوات لهجمات الخدمة

الآن ، دعونا نلقي نظرة على بعض الأدوات الشائعة المستخدمة في هجمات حجب الخدمة.

1. Slowloris

Slowloris هي أداة **مصممة** لنظام التشغيل Linux وتستهدف المضيفين الذين يشغلون خوادم الويب مثل

أباتشي ، *Tomcat* ، *dhttpd* و *GoAhead* . تعمل هذه الأداة عن طريق إرسال الكثير من HTTP

رؤوس إلى الخادم الهدف ولكن لا يكمله. تم تصميم Slowloris لإنزال أ

استهداف خادم الويب من جهاز واحد عن طريق الاحتفاظ بأكبر عدد ممكن من الاتصالات به.

سيؤدي هذا في النهاية إلى تجاوز الحد الأقصى للاتصالات التي يمكن لخادم الويب الهدف

التعامل مع ذلك مما يؤدي إلى رفض الخدمة للاتصالات المشروعة الأخرى.

2. QSlowloris

تعمل هذه الأداة على نفس مبدأ Slowloris ولكن لديها مستخدم رسومي

واجهة لسهولة الاستخدام ويعمل على منصة ويندوز.

3. بيلوريس

PyLoris هي في الأساس أداة اختبار للخوادم ولكن يمكن أيضًا استخدامها لتنفيذ هجمات DoS.

يمكن أن تستهدف بروتوكولات مختلفة بما في ذلك *HTTP* و *FTP* و *SMTP* و *IMAP* و *Telnet* .

4. LOIC (المدار المنخفض أيون المدفع)

LOIC عبارة عن أداة لاختبار إجهاد الشبكة مفتوحة المصدر وأداة DoS. الفيضانات الخادم الهدف

مع كمية كبيرة من حزم TCP أو UDP مما يؤدي إلى رفض الخدمة.

الهجوم الموزع على الخدمة (DDOS)

يحدث هجوم رفض الخدمة الموزع عندما ينشأ الهجوم على المضيف الهدف

من أنظمة متعددة للخطر. قبل شن الهجوم ، المهاجم

تنازل أنظمة متعددة من شبكة أو أكثر باستخدام أحصنة طروادة وغيرها

التقنيات. تُعرف هذه الأنظمة **المشوهة** باسم **الزومبي** حيث يستخدم المهاجم

لهم لشن هجوم DDoS على الهدف النهائي.

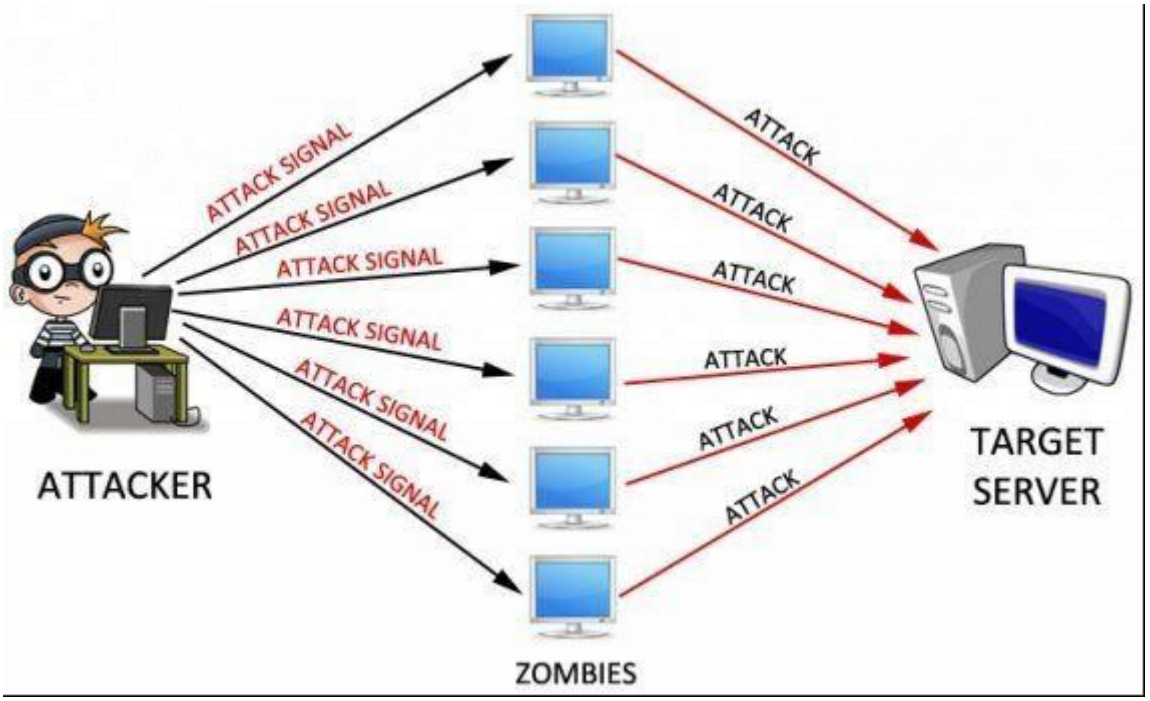
مزايا الحرمان الموزع من الخدمة هو أنه منذ استخدام أنظمة متعددة ،

يمكن بسهولة غمرت الهدف مع الكثير من حركة المرور في نهاية المطاف مما تسبب في هبوطه. أ

يمكن الحصول على فهم أكثر وضوحًا باستخدام الشكل التالي 12.3 الذي يوضح

الآلية المتورطة في هجوم DDoS نموذجي.

الشكل 12. 3



خصائص هجوم DDoS

بالمقارنة مع هجوم حجب الخدمة ، فإن DDoS هو هجوم منسق واسع النطاق على الهدف باستخدام عدد كبير من الأنظمة المسبقة للخطر (الزومبي).

هجوم DDoS يعمل تحت مستويين. الهدف النهائي الذي يتعرض لهجوم مباشر هو المعروف باسم "الضحية الرئيسية" في حين يشار إلى الكسالى المستخدمة لمهاجمته باسم "الضحايا الثانوية".

حيث أن الهجوم ينشأ من مواقع متعددة للشبكات ويتضمن عددًا كبيرًا من الكسالى ، وغالبا ما يكون من الصعب الكشف عنها أو منعها.

يمكن بسهولة حظر هجوم DoS البسيط الذي ينشأ من عنوان IP واحد على مستوى جدار الحماية. لكن هجوم DDoS الذي ينشأ من العشرين إلى الثلاثين

ألف أنظمة مختلفة (عناوين IP) من الصعب للغاية الكشف عنها.

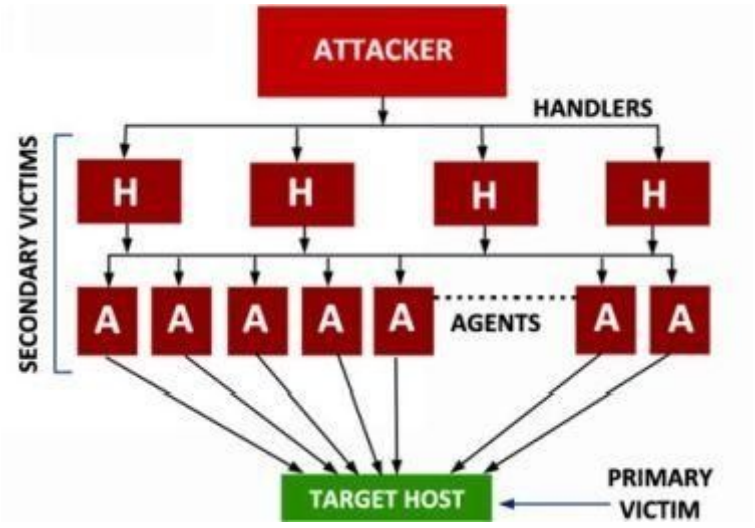
حتى لو قامت الشركة بعمل تخمين وتدير حظر عناوين IP متعددة في جدار الحماية الخاص به ، هناك فرصة واضحة للتأثير سلبًا على المستخدمين الحقيقيين كما هو من الصعب التمييز بين حركة المرور الحقيقية والخبيثة.

آلية هجوم DDoS

الآن ، دعونا نلقي نظرة على بعض نماذج هجمات DDoS الموجودة عادة:

وكيل معالج نموذج

وكيل نموذج عامل هي واحدة من آليات DDoS شعبية حيث المهاجم
التصاميم بذكاء الهجوم بطريقة هرمية وذلك لتحسين فعاليته و
أيضا جعل من الصعب اكتشاف وتتبع الظهر.
في المستوى الأول ، يقوم المهاجم بتسوية مجموعة من أجهزة الكمبيوتر ويقوم بتثبيت معالج البرنامج عليها. في المستوى الثاني ، يقوم المهاجم بتسوية مجموعة كبيرة أخرى من يشار إلى أجهزة الكمبيوتر التي يشار إليها عادةً باسم "الوكلاء" أو "الزومبي" والتي يتحكم فيها "معالجات".

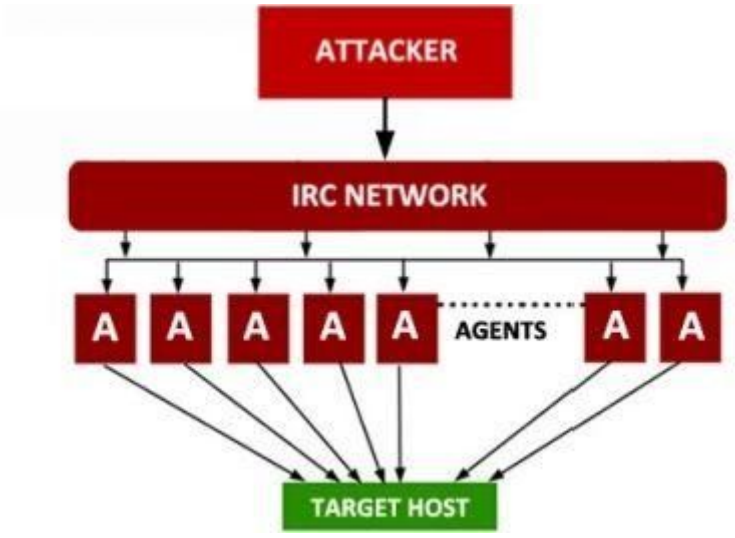


الشكل 12. 4

لذلك ، أثناء الهجوم ، يجلس المهاجم بذكاء في أعلى التسلسل الهرمي السيطرة على المعالجات التي بدورها تشرع الوكلاء (الزومبي) لمهاجمة المضيف المستهدف (ضحية). بما أن المهاجم يختبئ بأمان في الخلفية ، فإن هذا النوع من الهجوم يجعله من الصعب حقا تتبع مرة أخرى إلى المصدر.

نموذج IRC القائم

يشبه **النموذج القائم على IRC** "نموذج معالج الوكلاء" الذي تمت مناقشته أعلاه ولكن فقط الفرق هو أن المهاجم يستفيد من شبكة "دردشة الإنترنت (IRC)" بدلا من معالجات للاتصال الوكلاء.



الشكل 12. 5

ميزة هذا النموذج هي أن المهاجم يمكنه استخدام منفذ IRC الشرعي بسهولة ربط نفسه للعملاء وبدء الهجوم. أيضا ، كمية هائلة من حركة المرور على IRC الشبكة تجعل من الصعب على مسؤول الشبكة تتبع وجود المهاجم على الخادم.

أدوات لهجمات DDoS

فيما يلي بعض الأدوات الشائعة المستخدمة في تنفيذ هجمات DDoS:

1. ترينو

تعد **Trinoo** أداة شائعة لهجمات DDoS ولديها سجل في إزالة المواقع الكبيرة مثل ياهو! وهي مصممة لتسبب هجمات DDoS منسقة على الهدف من مختلف المواقع. تستخدم هذه الأداة بشكل أساسي مشكلة عدم حصانة "تجاوز سعة المخزن المؤقت عن بُعد" للأنظمة الحصول على تثبيت واستخدامها في وقت لاحق كما الكسالى.

2. DDoSim

DDoSim المعروف أيضا باسم *Layer 7 DDoS simulator* هو أداة ممتازة لتنفيذ DDoS الهجوم على الهدف من خلال محاكاة العديد من الكسالى. هذه الكسالى خلق TCP الكامل اتصال إلى الهدف باستخدام عناوين IP عشوائية. يمكن أن يؤدي أيضا HTTP القائمة هجمات DDoS مع كل من طلبات صالحة وغير صالحة.

3. تور المطرقة

هذا هو أداة أخرى لطيفة DDoS مكتوبة في بيثون. إنها أداة فعالة للغاية لديها القدرة على إنزال الأجهزة التي تشغل خوادم Apache و IIS في وقت قصير جدًا. ميزة هذه الأداة هي أن لديها القدرة على العمل من خلال شبكة TOR (شبكة مجهولة) للحفاظ على الهجوم بأكمله مجهول.

4. دافوسيت

تعتبر **Davoset** أداة رائعة أخرى لتنفيذ هجمات DDoS. يجعل من استخدام

ضعف "إساءة استخدام الوظيفة" على المواقع لاستخدامها كزومبي وسبب ضرر DDoS الهجمات على الهدف.

التدابير المضادة

بعد استكشاف قدر لا بأس به من المعلومات حول أنواع مختلفة من هجمات DoS ، الآلية والأدوات المختلفة المستخدمة في تنفيذها ، دعونا الآن ننظر في بعض التدابير المضادة التي يمكن للمرء اتخاذها لوقف أو تخفيف مثل هذه الهجمات من الحدوث على الأنظمة.

باستخدام **IDS** (نظام كشف التسلل) و **IPS** (نظام منع التسلل)

يمكن أن يكون ذا ميزة كبيرة عندما يتعلق الأمر بالكشف عن DoS / DDoS والوقاية منها الهجمات في مرحلة مبكرة.

عناوين IP في القائمة السوداء التي تم العثور عليها هي مصدر هجوم DoS محتمل.

تصفية الدخول: تأكد من أن الحزم الواردة تأتي من صالحة مصدر.

تصفية الخروج: تفحص جميع الحزم الصادرة بحثًا عن بيانات ضارة قبل ذلك في الواقع ترك الشبكة.

نظرًا لأنه من الممكن التزوير بسهولة لعنوان IP لحزم DDoS الواردة ، فهناك فرصة جيدة ألا تمثل الحزم مصدرًا صالحًا. لذلك ، تكوين جدار الحماية لإسقاط الحزم التي لا تمثل عنوان مصدر صالح.

ضع جدارًا ناريًا أو حزمة شم يقوم بتصفية كل حركة المرور الواردة التي لا تحتوي على عنوان IP الأصلي.
زيادة النطاق الترددي أو الموارد المتاحة لمنع الخدمات من الذهاب أسفل بسرعة أثناء الهجوم.
موازنة التحميل: استخدم بنية خادم متعددة وتوازن التحميل الوارد على كل خادم. هذا يمكن أن يساعد في تحسين الأداء وكذلك تخفيف آثار هجمات DDoS.

الفصل 13 - القرصنة اللاسلكية

استخدام الشبكات اللاسلكية أصبحت شعبية متزايدة في هذه الأيام بسبب مرونة التشغيل وتكلفة منخفضة الإعداد. الشبكات اللاسلكية مثل الشبكات المحلية اللاسلكية تسمح للمستخدمين
الوصول إلى موارد الشبكة من أي مكان في الحرم الجامعي باستخدام الأجهزة المحمولة مثل أجهزة الكمبيوتر المحمولة
والأجهزة اللوحية. وهذا يوفر قدرا كبيرا من المرونة للطلاب والموظفين ، وبالتالي القضاء على الحاجة إلى التمسك دائما مكاتبهم أثناء وقت عملهم.
ومع ذلك ، على الجانب الآخر من جميع مزاياها تكمن القضايا الأمنية الرئيسية. اكثر فأكثر بدأت الشركات الآن في استخدام التقنيات اللاسلكية في شبكتهم ، وهذه الأمان
قضايا يضع العمل على مخاطر عالية. على عكس الشبكات السلكية والتكنولوجيا اللاسلكية لا يحد من الوصول المادي إلى شخص غريب مثل المتسلل. اليوم ، بكل سهولة
الأدوات المتاحة يمكن بسهولة للمتسلل من اختراق الثغرات في اللاسلكي
نظام الأمن والوصول إلى الشبكة.
في هذا الفصل سوف نلقي نظرة على بعض نقاط الضعف الشائعة الموجودة في تقنية الشبكات اللاسلكية ، طرق استغلالها للوصول إلى الوصول وأيضًا
تدابير مضادة لمنعهم.

أساسيات الشبكات اللاسلكية

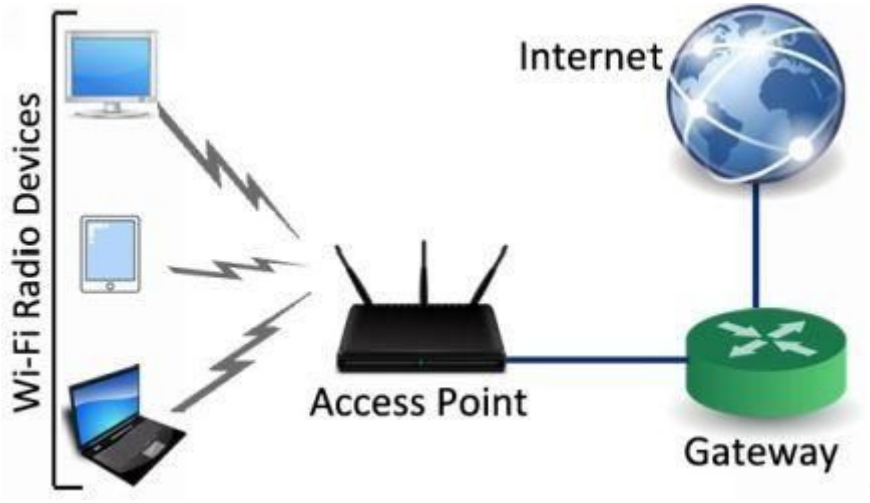
قبل القفز إلى القرصنة الفعلية ، دعونا نذهب من خلال بعض المفاهيم الأساسية لل الشبكات اللاسلكية.

يتم تمثيل المعيار اللاسلكي بشكل شائع كـ **802.11** ويستخدم لإعداد اللاسلكي شبكات المناطق المحلية (**WLAN)** في بيئات مثل المدارس والمكاتب. 802.11 يحتوي المعيار على 3 بروتوكولات رائدة (أو ملحقات) كما يلي:

1. **802.11a** - يوفر سرعة أعلى (تصل إلى 54 ميغابت في الثانية) ، والمزيد من القنوات وأقل التدخلات.
2. **802.11b** - يُعرف هذا البروتوكول أيضًا باسم **"Wi-Fi"** . هذا هو المعيار الذي كان يستخدم في معظم النقاط الساخنة واي فاي.
3. **802.11g** - يشبه هذا البروتوكول 802.11b ولكنه يوفر أسرع بكثير انتقال.

مكونات الشبكة اللاسلكية

تتكون الشبكة اللاسلكية من المكونات الأساسية الثلاثة التالية:



الشكل 13. 1

1. **جهاز راديو Wi-Fi:** يمكن أن يكون أي جهاز به بطاقة لاسلكية (NIC) مضمنة مثل جهاز كمبيوتر محمول أو جهاز لوحي أو كمبيوتر شخصي مزود بتقنية Wi-Fi أو هاتف محمول.
2. **نقطة الوصول:** هذا هو الجهاز الذي يسمح لأجهزة راديو Wi-Fi بالاتصال شبكة لاسلكية باستخدام معايير Wi-Fi. و **AP** ثم لديه اتصال سلكي ل

جهاز التوجيه. ومع ذلك ، تأتي معظم أجهزة التوجيه الحديثة الآن مع **APs** المدمج للقضاء على تحتاج لجهاز إضافي.

---

3. **البوابة:** يتم توصيل أجهزة التوجيه بالبوابات التي تقوم بعد ذلك بتوصيل الكل شبكة إلى الإنترنت.

الكشف عن الشبكات اللاسلكية (القيادة للحرب)

للكشف عن شبكة لاسلكية مثل *نقطة وصول Wi-Fi* ، يمكنك بدء التجوال في حديقة التكنولوجيا ، منطقة وسط المدينة أو ببساطة من خلال جدران المبنى الخاص بك باستخدام جهاز قادر على استخدام Wi-Fi (مثل أجهزة الكمبيوتر المحمولة وأجهزة النخيل) مع "قيادة الحرب"

البرمجيات. فيما يلي بعض برامج القيادة الشهيرة للحرب:

Netstumbler: هذه أداة تستند إلى نظام التشغيل Windows والتي يمكنها اكتشاف اللاسلكي الشبكات وأيضا بمناسبة موقفهم مع GPS.

MiniStumbler: هذا إصدار محمول من *NetStumbler* يمكن تثبيته على أجهزة الكمبيوتر المحمولة.

Vistumbler: هذه أداة أخرى مفيدة للتشغيل الحربي لتشغيل Windows الأنظمة.

Kismet: هذه أداة استنشاق لاسلكية قائمة على نظام Linux ولديها أيضًا القدرة على أداء القيادة الحرب.

واي فاي الماسح الضوئي: هذا هو أداة Windows المستندة إلى واجهة المستخدم الرسومية للكشف عن جميع APs المتاحة في

محيطك.

يرجى ملاحظة أن جميع بطاقات الشبكة اللاسلكية (NIC) ليست نفسها وبعضها قد لا يكون كذلك متوافق مع أدوات الحرب المذكورة أعلاه. في هذه الحالة سوف تضطر إلى استخدام البرنامج الذي يأتي مع بطاقة NIC اللاسلكية للكشف عن نقاط الوصول.

الاستنشاق اللاسلكي

لا يختلف **الاستنشاق اللاسلكي** عن "الاستنشاق السلكي" الذي ناقشناه بالفعل في الفصل السابق ولكن الفرق الوحيد هنا هو أن يتم تنفيذ هذا واحد على بيئة لاسلكية. في هذه الحالة يكون البروتوكول المستخدم لاستنشاق 802.11. منذ الراديو الموجات متعددة الاتجاهات ، يمكن بسهولة تنفيذ هجوم "رجل في الوسط" والتقاط جميع الحزم من حركة المرور اللاسلكية المتاحة في النطاق الخاص بك.

تكوين بطاقات لاسلكية لوضع مختلط

يسمح **الوضع المختلط** لـ NIC (بطاقة واجهة الشبكة) بالتقاط جميع الشبكة حركة المرور التي تصل إليها بدلاً من التقاط فقط تلك المقصود بها بطاقة واجهة الشبكة. ما لم يتم تكوين بطاقتك اللاسلكية للعمل في وضع مختلط ، فإن ذلك غير ممكن لأداء الاستنشاق اللاسلكي.

لا تدعم معظم بطاقات الشبكة اللاسلكية الوضع المختلط على تشغيل Windows النظام وبالتالي على المرء استخدام Linux لأداء الاستنشاق اللاسلكي بنجاح. اذا أنت لا تزال ترغب في أداء استنشاق على ويندوز ، يمكنك استخدام نوع خاص من بطاقة لاسلكية المعروفة باسم **AirPcap** وهي مكلفة للغاية مقارنة بتلك العادية. بطاقات AirPcap يمكن استخدامها على ويندوز مع برامج استنشاق مثل "بريشارك"و" قابيل و هابيل"، لكن بالنسبة لجميع البطاقات الأخرى ، يجب استخدام منصة Linux.

أدوات لاستنشاق اللاسلكية

دعونا نلقي نظرة على بعض الأدوات المستخدمة على نطاق واسع لأداء الاستنشاق اللاسلكي:

إيثار ريال

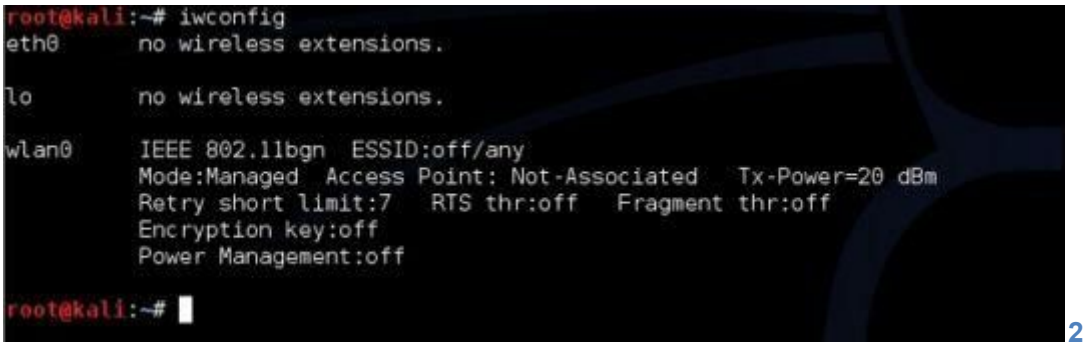
Wireshark هو أحد أدوات استنشاق الحزم المفضلة لدي لأنه سهل الاستخدام ويدعم واجهة المستخدم الرسومية. على الرغم من أنه يعمل على Windows ، إلا أنني أستخدم نظام التشغيل Linux في بلدي

مظاهرة استنشاق لاسلكية كوضع مختلط غير معتمد على Windows منصة. أنا أستخدم **TP-LINK TL-WN722N** لهذا العرض التوضيحي لأنه متوافق تمامًا مع كالي لينكس الذي أقوم بتشغيله. إذا كان لديك بطاقة لاسلكية مختلفة أو تحتاج إلى شراء واحدة ، يرجى التأكد من أنه متوافق مع نواة لينكس أنك سوف تكون استخدامه على. منذ كالي لينكس هي معبأة مع Wireshark وجميع الأدوات المفيدة الأخرى هناك

لا حاجة لتثبيته بشكل منفصل. اتبع الإرشادات أدناه لإجراء عينة لاسلكية استنشاق:

1. قم بنسخ جهاز الكمبيوتر الخاص بك من قرص DVD الخاص بـ Live Kali Linux.
2. بمجرد تحميل Linux ، قم بتوصيل بطاقة USB اللاسلكية.
3. افتح نافذة "Terminal" واكتب الأمر التالي:

إيوكنفيغ



الشكل 13. 2

4. إذا كانت بطاقتك اللاسلكية متوافقة ، يجب أن ترى جهازك مدرجًا كما هو موضح في أعلاه لقطة باسم "wlan0".
5. الخطوة التالية هي وضع البطاقة في وضع المراقبة (الوضع المختلط). إلى عن على هذا ، اكتب الأمر التالي:

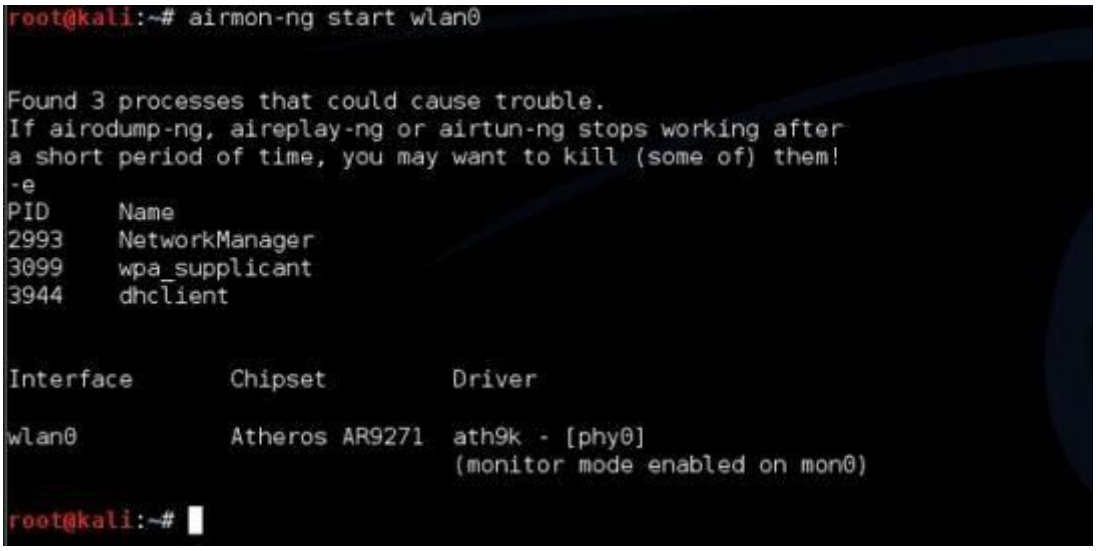
airmon-ng start wlan0

على جهاز الكمبيوتر الخاص بي ، يتم سرد البطاقة اللاسلكية باسم "wlan0". لذلك ، لقد دخلت " wlan0"

في الأمر. إذا كان الكمبيوتر الخاص بك يحتوي على قائمة مختلفة مثل "wlan1" أو "wlan2" ، فأنت بحاجة إلى استبدال نفسه في الأمر أعلاه.

6. بعد تنفيذ الأمر بنجاح ، سينشئ جهاز الكمبيوتر الخاص بك جهازًا افتراضيًا جديدًا بطاقة لاسلكية وتمكين "وضع الشاشة" في ذلك. في حالتي ، "mon0" كما هو موضح في

لقطة أدناه.



الشكل 13. 3

7. حان الوقت الآن لاستخدام Wireshark لبدء التقاط الحزم. لبدء Wireshark ،
انقر فوق **التطبيقات -> Kali Linux -> أفضل 10 أدوات أمان -> wireshark** as

---

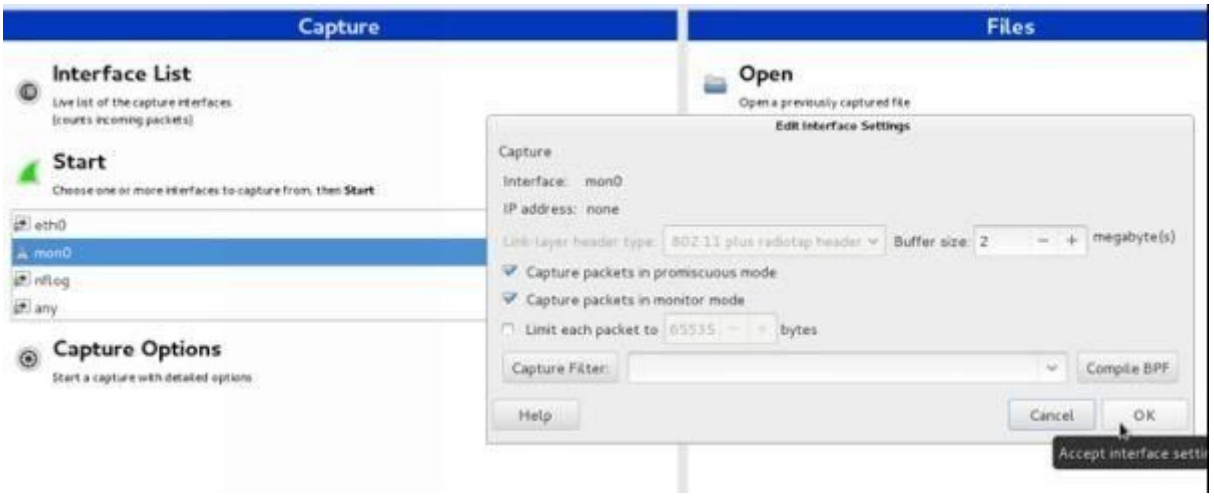
ظاهر أدناه:

الشكل 13. 4

8. الآن ، من نافذة Wireshark الرئيسية ، حدد "mon0" من **قائمة الواجهة** ،
انقر نقرًا مزدوجًا فوقه واختر خيارًا لالتقاط الحزم في "الوضع المختلط"

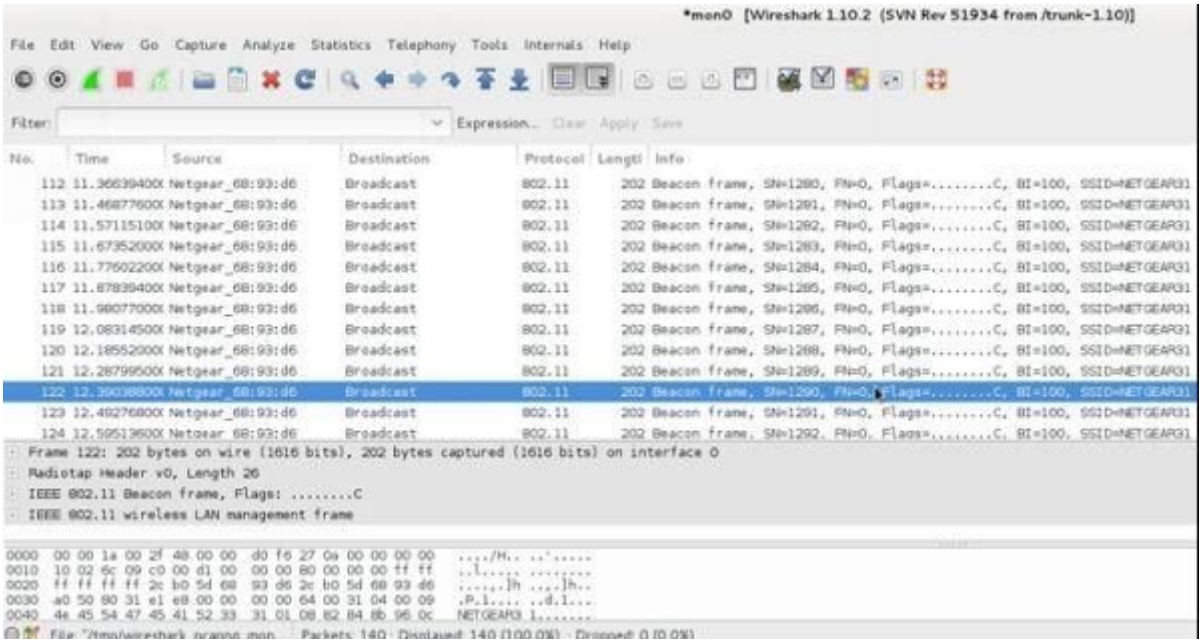
و "وضع الشاشة". التالي انقر على **موافق** .

الشكل 13. 5



9. بمجرد الانتهاء ، انقر فوق الزر "ابدأ" لبدء استنشاق. هذا يجب التقاط الحزم من جميع الشبكات اللاسلكية المتاحة القريبة. اللقطة التالية يظهر التقاط حزمة عينة:

الشكل 13. 6



فيما يلي بعض أدوات الاستنشاق اللاسلكية الأخرى التي تستحق الدراسة:

أثيري

هذا هو أداة أخرى تعتمد على نظام Linux تعمل على كل من الشبكات السلكية واللاسلكية.
يأتي كأداة اختبار أمان مضمّنة في Kali Linux.

OmniPeek اللاسلكي

OmniPeek عبارة عن حزمة أدوات شم 802.11 تجارية مع الكثير من الميزات المفيدة لـ شبكة الرصد. وهي تعمل على منصة ويندوز.

الخصوصية المكافئة السلكية (WEP)

WEP هو مكون من شبكات WLAN 802.11 المصممة لتوفير سرية
البيانات في الشبكات اللاسلكية. على عكس الشبكات السلكية حيث يمكن الحد من المادية
الوصول فقط للمستخدمين الموثوق بهم ، الأمر نفسه غير ممكن في حالة وجود شبكة لاسلكية.
لذلك ، للتغلب على هذا القيد ، هناك نوع خاص من التشفير يسمى WEP هو
تستخدم لمنع المهاجمين من اعتراض البيانات اللاسلكية.
ومع ذلك ، هناك ضعف واضح في نظام الأمان WEP يمكن استغلاله.
بمجرد التقاط حزم بيانات كافية وإتاحة الوقت الكافي لها ، يمكن للمهاجم التصدع بسهولة
مفتاح WEP المستخدم للتشفير وذلك لفك تشفير جميع المعلومات مرة أخرى إلى البيانات الخام.

تكسير تشفير WEP

تُستخدم الأدوات التالية بشكل شائع لتكسير مفتاح / كلمة مرور تشفير WEP:

ايركراك-NG

هذه أداة شائعة الاستخدام على Linux للقضاء على مفاتيح تشفير 802.11 WEP. إنها
أداة سطر الأوامر التي تأتي كميزة مضمنة في حزمة Kali Linux ويمكن أن تكون بسهولة
المستخدمة عن طريق تحميله من دي في دي الحية. لأنه يأخذ قائمة طويلة من الأوامر و
إجراءات للقضاء على كلمات مرور WEP ، لقد قررت حذف التجريبي للتكسير
عملية من هذا الكتاب. ولكن لا يزال بإمكانك Google عن "كيفية كسر تشفير WEP"
العثور على العديد من الإجراءات خطوة بخطوة التي تصف عملية التكسير الفعلية.

WEPCrack

WEPCrack هي أداة شائعة أخرى لتكسير المفاتيح السرية 802.11. هذه هي الأداة الأولى ل
قدم عرضًا عامًا حول كيفية استغلال تشفير WEP.

الوصول المحمي بواسطة WPA) WI-FI)

WPA هو معيار أمان لاسلكي آخر تم تطويره بشكل أساسي لمعالجة
أوجه القصور في WEP. يستخدم WPA معيار تشفير مختلف أفضل من ذلك
من WEP ومصمم كترقية البرنامج.
ومع ذلك ، يسمح وجود ثغرة في ميزة الأمان هذه تسمى (**Wi-Fi Protected Setup**
WPS)
كلمات مرور WPA المكسورة باستخدام نهج القوة الغاشمة. تحتوي معظم نقاط الوصول على
WPS
تمكين افتراضيا ، وبالتالي لا تزال عرضة للخطر.

تكسير كلمات مرور WPA

فيما يلي عرض تفصيلي لتكسير كلمة مرور WPA باستخدام أداة **Reaver**
الذي يأتي مع كالي لينكس.

1. قم بتشغيل جهاز الكمبيوتر الخاص بك باستخدام Kali Live DVD وأيضاً قم بتوصيل USB اللاسلكي
بطاقة.

2. افتح نافذة المحطة الطرفية واكتب الأمر **iwconfig** للتأكد من أن لديك
تم اكتشاف البطاقة.

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

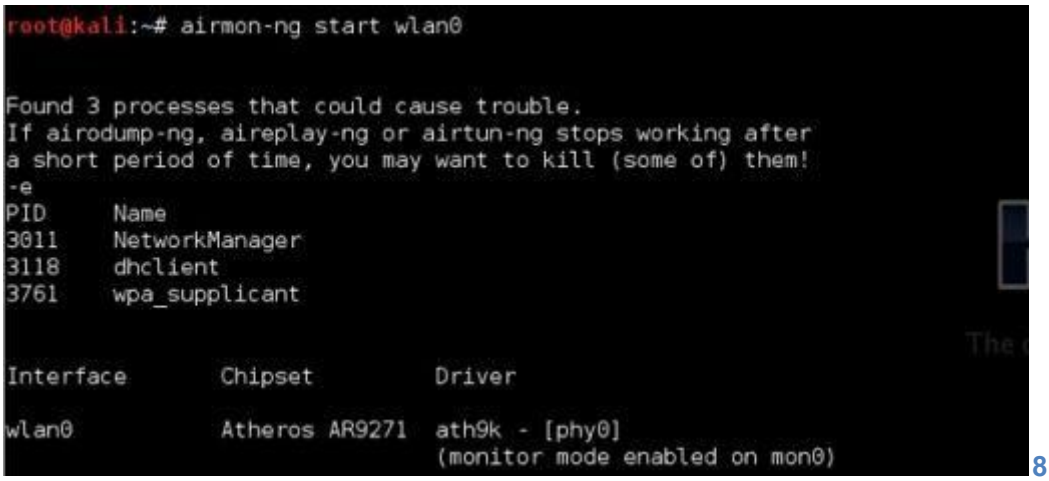
الشكل 13. 7

3. بمجرد أن ترى بطاقتك مدرجة (wlan0) كما هو موضح أعلاه ، اكتب الأمر التالي
لوضع بطاقتك في "وضع المراقبة" والبدء في استخدامها.

airmon-ng start wlan0

يجب أن ينشط هذا "وضع المراقبة" لبطاقتك. على جهاز الكمبيوتر الخاص بي هو عليه

ممكّن في "mon0" كما هو موضح في الصورة أدناه.



الشكل 13. 8

4. الآن اكتب الأمر التالي لاكتشاف نقاط الوصول الممكنة الممكّنة لـ WPS.

l mon0 -C-

يجب أن يقوم هذا بإجراء مسح وقائمة بجميع نقاط الوصول القريبة كما هو موضح أدناه.

بمجرد اكتشاف نقاط الوصول ، اضغط على **Ctrl + C** لإيقاف عملية المسح.

الشكل 13. 9

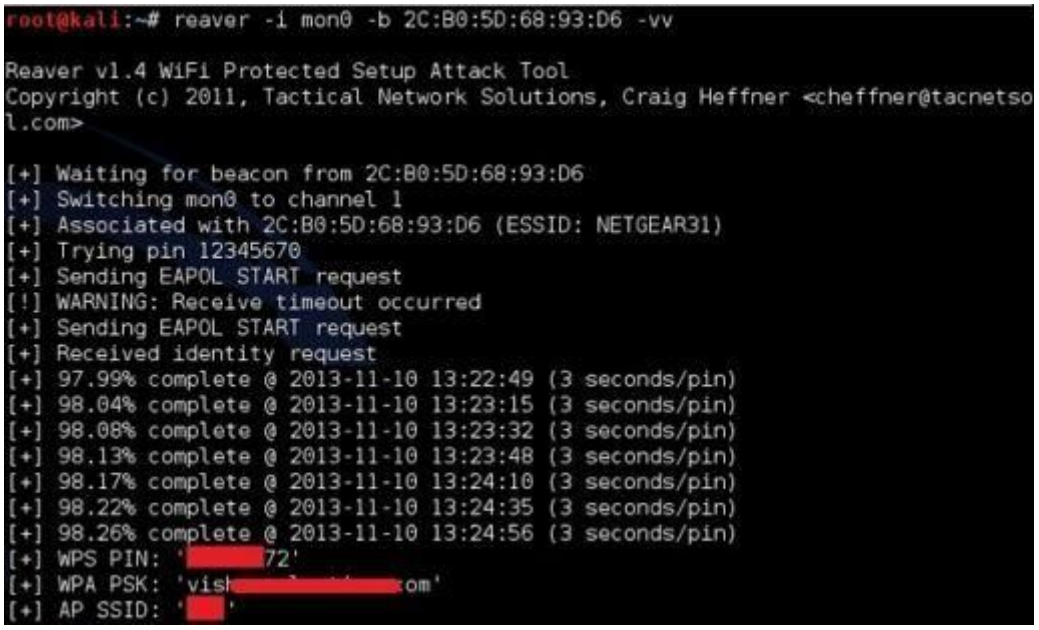
5. كما هو مبين أعلاه ، هناك قائمة واحدة والتي تظهر نقطة وصول ضعيفة مع ESSID" **NETGEAR31**" . الآن إصدار الأمر التالي لأداء القوة الغاشمة الهجوم على الهدف.

ريفر -vv- i mon0 -b 2C: B0: 5D: 68: 93: D6

يرجى ملاحظة أنه سيتعين عليك استبدال "2C: B0: 5D: 68: 93: D6" بـ **BSSID** الهدف AP في قضيتك.

6. سوف تستغرق عملية التكسير بضع ساعات حتى تكتمل وإذا سارت الأمور على ما يرام

يجب أن تشاهد رقم التعريف الشخصي المتقطع وكلمة المرور في النتائج كما هو موضح أدناه لمحة:



الشكل 13. 10

أدوات أخرى لتكسير WPA

فيما يلي بعض أدوات تكسير WPA الأخرى التي يمكنك تجربتها:

coWPAtty: هذه أداة تعتمد على نظام Linux وتستخدم نهج القاموس وقبل ملفات التجزئة المحسوبة (على غرار جداول قوس قزح) للقضاء على عبارات مرور WPA.

Hashcat: هذا هو واحد من أسرع أداة تكسير كلمة المرور القائمة على وحدة المعالجة المركزية التي تستخدم أساليب مختلفة مثل القاموس ، والقوة الغاشمة وأنواع الهجينة من الهجمات. يأتي لكل من أنظمة تشغيل Windows و Linux.

الهجمات على الخدمة (DOS)

تماما مثل الشبكات السلكية ، والشبكات اللاسلكية هي أيضا عرضة لرفض الخدمة الهجمات. منذ الشبكات المحلية اللاسلكية تستخدم موجات الراديو على الترددات العامة لإرسال واستقبال

حركة المرور ، فمن السهل استخدام حركة المرور الأخرى من نفس النطاق للتسبب في تداخل. إذا كان
فشل المهاجم في الوصول إلى الشبكة ، فقد يستخدم DoS كخيار أخير لمهاجمة
شبكة الاتصال. تتسبب هجمات حجب الخدمة في إسقاط كافة الاتصالات الموجودة بالشبكة
يمنع أيضًا حدوث اتصالات جديدة مما يؤدي إلى حدوث شبكة WLAN تقريبًا
غير صالح للاستخدام.

أدوات اللاسلكي لا

يحتوي Kali Linux على عدد قليل من الأدوات والميزات المدمجة التي تسبب هجمات DoS على شبكات WLAN.
تعمل معظم هذه الأدوات عن طريق إرسال حزم إلغاء المصادقة بدلاً من المصادقة
الحزم للوصول إلى نقاط مما يؤدي إلى إسقاط الشبكة جميع الاتصالات الموجودة.
هناك طريقة أخرى لإغراق الشبكة من خلال إرسال طلبات المصادقة إلى APs مع
رموز الحالة غير المناسبة أو أجهزة MAC العميل العشوائية.
تتضمن بعض الأدوات الشائعة **للدائرة** اللاسلكية **Void11** و **Fatajack** و **FakeAP** (لـ
خداع أو إنشاء عدد كبير من نقاط الوصول المزيفة في محاولة لإرباك العملاء).

التدابير المضادة

فيما يلي بعض الإجراءات المضادة التي يمكن استخدامها لمنع حدوث ذلك
الهجمات على شبكة لاسلكية:
تصفية عنوان MAC: تستخدم هذه الميزة قائمة محددة مسبقًا من عناوين MAC الخاصة بـ
بطاقات NIC اللاسلكية للعملاء المسموح لهم بالاتصال بالشبكة. بهذه الطريقة
ممكن لمنع الغرباء من الوصول إلى الشبكات المحلية اللاسلكية.
SSID المخفي: منع AP من إيقاف بث SSID الخاص به يجعله غير مرئي
وبالتالي لا يمكن الوصول إليها للمهاجمين.
WPA بدلاً من WEP: نظرًا لأن WEP لديه مشكلات أمنية معروفة جيدًا ، فهي آمنة دائمًا
لاستخدام معايير تشفير بديلة مثل WPA أو WPA2 عبر WEP.
تعطيل WPS: نظرًا لأن WPS (إعداد Wi-Fi المحمي) يقال إنها بها عيوب ، مما يتيح لها ذلك

يجعل WPA عرضة للخطر. لذلك ، من الضروري تعطيل WPS يدويًا
ميزة حيث يتم تفعيلها مسبقًا في معظم أجهزة التوجيه افتراضيًا.
جدار الحماية: يساعد استخدام جدار حماية ذي قواعد قوية على تصفية حركة المرور غير المصرح بها و
منع هجمات القوة الغاشمة.

الفصل 14 - نقاط الضعف في تطبيق الويب

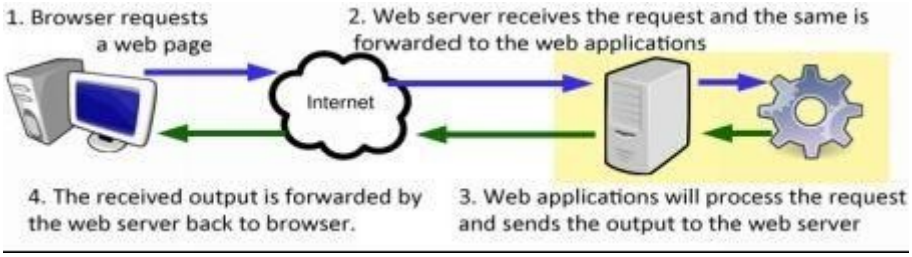
يسمح الضعف في تطبيقات الويب للمتسللين بتنفيذ هجمات ضارة مختلفة مثل
اختطاف الحسابات ، وسرقة الهويات ، والوصول إلى المعلومات السرية وغيرها
على. سنبحث في هذا الفصل في بعض نقاط الضعف الشائعة الموجودة على الويب
التطبيقات وطرق استغلالها.

أساسيات تطبيق الويب

تطبيق الويب هو برنامج عميل / خادم يعمل على جهاز كمبيوتر ويتفاعل مع
المستخدمين أو الأنظمة الأخرى التي تستخدم بروتوكولات مثل HTTP. معظم تطبيقات الويب هي عادة
مكتوبة باستخدام لغات البرمجة مثل Java و PHP و Perl و Microsoft .NET وما إلى ذلك.
يحتوي كل خادم على العديد من تطبيقات الويب التي يتم تشغيلها باستخدامه والذي يمكن تنفيذه
الاتصال ذهابًا وإيابًا بين العميل والخادم لتنفيذ المهام
مثل تنفيذ استعلامات قاعدة البيانات واسترجاع الملفات وما إلى ذلك. توضح الخطوات التالية
عمل تطبيقات الويب على الخادم:

1. يقدم العميل طلبًا لصفحة ويب عن طريق كتابة عنوان URL الخاص به على المتصفح.
2. يتلقى خادم الويب الهدف هذا الطلب ويعيد توجيهه إلى الويب
التطبيقات الموجودة عليه.
3. ستقوم تطبيقات الويب بمعالجة طلب جلب جميع المعلومات اللازمة
مطلوب للإخراج (مثل الاستعلام عن قاعدة البيانات ، ومعالجة الصور وما إلى ذلك) ويرسل
مرة أخرى إلى خادم الويب.

4. يقوم خادم الويب بإعادة توجيه الإخراج إلى متصفح العميل الطالب.



الشكل 14. 1

أنواع نقاط الضعف في تطبيق الويب

الآن ، دعونا نناقش بعض أنواع الثغرات المختلفة الموجودة على الويب
التطبيقات ، وكيفية عملها وطرق استغلالها.

البرمجة النصية للمواقع المشتركة (XSS)

البرمجة النصية للمواقع المشتركة (والمعروفة أيضًا باسم **XSS**) هي نوع من الهجمات التي تحقن البرامج النصية الضارة
(مثل JavaScript و ActiveX و VBScript و Flash وما إلى ذلك) في صفحات الويب الضعيفة في الموقع.
يتم تخزين هذا البرنامج النصي الضار على موقع الويب نفسه وعندما يزور المستخدمون هذا الموقع أو
تصفح صفحاته التي يتم تشغيل البرنامج النصي من جانب العميل لبدء الهجوم. بسيط
الكلمات XSS هي نوع من الهجوم الذي يستغل موقعًا ضعيفًا ويستخدمه كوسيط
لتنفيذ هجمات على المستخدمين النهائيين.

المفاهيم الأساسية لل XSS

XSS هو هجوم قائم على الويب يتم تنفيذه على تطبيقات الويب الضعيفة.
في هجمات XSS ، يكون الهدف النهائي أو الضحية هو المستخدم النهائي وليس المستضعف تطبيق.
هنا ، يتم استخدام صفحة الويب أو التطبيق الضعيف كقناة للوصول إلى
الهدف النهائي من هو المستخدم النهائي.

تأثير هجوم XSS

عندما ينجح المهاجمون في استغلال ثغرات XSS ، يمكنهم القيام بما يلي

الأنشطة على جانب العميل:

الوصول إلى ملفات تعريف الارتباط للجلسة واختطاف حسابات المستخدمين.

انتشار الديدان والفيروس وأحصنة طروادة.

الوصول إلى ملفات المستخدم النهائي والدلائل.

التحكم عن بعد في نشاط متصفح المستخدم.

سيناريو XSS

دعونا نفترض أن أحد المتسللين يكتشف ثغرة أمنية في XSS في أحد تطبيقات الويب من موقع كبير مثل *facebook.com* . القراصنة يستغل هذا الضعف ويحقن أ شفرة ضارة على إحدى صفحات الويب على Facebook. كلما زار المستخدمون هذه الصفحة ،

تعمل الشفرة الخبيثة على متصفحها وتسرق ملف تعريف ارتباط الجلسة وترسل ذلك المعلومات مرة أخرى إلى القراصنة. سيستخدم المهاجم الآن ملف تعريف الارتباط هذا لاختطاف المستخدم

الدورة وسهولة الوصول إلى حسابه / صفحتها على Facebook.

XSS التدابير المضادة

اليوم ، تعتمد المواقع الحديثة اعتمادًا كبيرًا على تطبيقات الويب المعقدة لتقديم ديناميكية مخرجات المحتوى بناءً على الاحتياجات والأفضليات الخاصة بالمستخدم. على عكس المواقع الثابتة ، هو عليه

لا يمكن لمواقع الويب الديناميكية ممارسة سيطرة كاملة على كيفية إنتاجها

يتم تفسيرها من قبل العميل. قد يفتح هذا إمكانية وجود XSS

نقاط الضعف في تطبيق ويب واحد أو أكثر يستخدمه موقع الويب الديناميكي. يمكنك أن تأخذ الإجراءات المضادة التالية لإيقاف هجمات XSS على مواقع الويب الخاصة بك:

التحقق من صحة جميع البيانات الواردة إلى تطبيقات الويب بدقة قبل التنفيذ.

اعتماد سياسة أمنية صارمة لمنع الناس من تقديم البرامج النصية مباشرة إلى الخادم.

تصفية بيانات الإدخال لإزالة أي من البرامج النصية الموجودة فيه قبل معالجتها.

حقن SQL

تستخدم تطبيقات الويب قواعد البيانات لتخزين البيانات اللازمة لمواقع الويب لتقديم معلومات محددة المحتوى للزوار وتقديم معلومات مفيدة أخرى. قواعد البيانات قد تحتوي أيضا على غيرها معلومات حيوية مثل بيانات اعتماد المستخدم والوثائق المالية وبيانات المستخدم المحددة و العديد من المعلومات السرية الأخرى. كلما المستخدمين الشرعيين تقديم طلب لعرض أو تعديل هذه المعلومات ، يتم استخدام استعلامات SQL (وتسمى أيضا أوامر SQL) عن طريق الويب
تطبيق لجلب أو تعديل البيانات المخزنة في قواعد البيانات.

حقن SQL هو نوع من الهجوم حيث يحاول المهاجم تمرير أمر SQL نفسه (بدلاً من البيانات النصية) من خلال تطبيق الويب للتنفيذ بواسطة قاعدة بيانات الواجهة الخلفية.
هنا يقوم المهاجم بحقن أوامر SQL المعدة خصيصًا لإدخال حقول مثل البحث المربعات وحقول تسجيل الدخول ونماذج الملاحظات وما إلى ذلك والتي تهدف إلى تلقي بيانات صالحة. إذا كان الويب
فشل التطبيقات في التحقق من صحة الإدخال بشكل صحيح قبل تمريره إلى قاعدة البيانات ، هذا يجوز له منح الوصول غير المصرح به للمهاجم والسماح له بمشاهدة أو تعديله
المعلومات من قاعدة البيانات.

المفاهيم الأساسية للحقن SQL

حقن SQL عبارة عن ثغرة أمنية في البرامج تحدث عند إرسال مدخلات بيانات المستخدم مباشرة إلى مترجم SQL للتنفيذ دون التحقق من الصحة المناسبة.
يستخدم المهاجمون حقول الإدخال لتمرير استعلامات SQL المعدة خصيصًا في محاولة للخداع المترجم لتنفيذ الأوامر غير المقصودة في قاعدة البيانات.

تأثير حقن SQL الهجوم

عند النجاح ، قد يسمح هجوم حقن SQL للمتسلل بتنفيذ ما يلي
أنشطة:

تجاوز مصادقة المستخدم والحصول على وصول غير مصرح به.
الوصول إلى أجزاء مهمة من قاعدة البيانات وعرض البيانات غير المقصودة.
إضافة أو إزالة إدخالات جديدة إلى قاعدة البيانات.

في بعض الأحيان يكون من الممكن حتى مسح محتويات قاعدة البيانات تمامًا.

مثال حقن SQL

دعونا نفترض وجود صفحة تسجيل دخول مصممة للسماح للمستخدمين بالوصول إلى قيود مساحة الموقع عند التصديق على أوراق اعتمادهم. عندما يدخل مستخدم حقيقي له "اسم المستخدم" و "كلمة المرور" في حقل تسجيل الدخول ، ينفذ تطبيق الويب استعلام SQL في الخلفية على قاعدة بيانات تحتوي على قائمة بأسماء المستخدمين وكلمات المرور. إذا كان يقال إن زوج "اسم المستخدم - كلمة المرور" المطابق يمنح المستخدم حق الوصول ؛ غير ذلك الدخول محظور.

لنفترض عندما يقوم مستخدم حقيقي بإدخال بيانات اعتماده على النحو التالي:

اسم المستخدم: توم

كلمة المرور: pass2000

سيكون استعلام SQL المستخدم لتنفيذ هذه المطابقة شيئًا كما يلي:

```
SELECT * من المستخدمين WHERE اسم المستخدم = 'توم' و كلمة المرور = 'pass2000 "
```

هنا استعلام SQL أعلاه يحاول العثور على صف في قاعدة البيانات عن طريق مطابقة "اسم المستخدم، كلمة السر" الزوج باستخدام **منطقي و** المشغل. و **و** عوائد المشغل **صحيح** فقط عندما يتطابق كل من المعاملات (اسم المستخدم وكلمة المرور). الوصول خلاف ذلك سيتم رفض.

تخيل ما سيحدث عندما يكتشف متسلل ثغرة أمنية في حقن SQL في هذا الصدد صفحة تسجيل الدخول. وقال انه ضخ أمر SQL وضعت خصيصا في حقل تسجيل الدخول باسم يتبع:

اسم المستخدم: توم

كلمة المرور: 'أو' 1 '=' 1

تطبيق الويب الضعيف يمر ببساطة البيانات في حقل كلمة المرور دون التحقق من الصحة الصحيح ، وبالتالي يحصل على تفسير ذلك باعتباره أمر SQL بدلا من العادي بيانات النص. الآن ، سيكون استعلام SQL المستخدم لتنفيذ هذه المطابقة شيئًا كما يلي:

```
SELECT * من المستخدمين WHERE اسم المستخدم = 'توم' و كلمة المرور = " أو " 1 '=' 1 '
```

هنا **المشغل المنطقي أو** يحمل **TRUE** حتى لو كان واحد من معاملاته يطابق. في تطابق هذه الحالة **'1' = '1'** ، وبالتالي يُمنح المتسلل الوصول إلى المنطقة المحظورة لـ

الموقع. بهذه الطريقة ، الضعف حقن SQL يساعد القراصنة على تجاوز نظام المصادقة والحصول على وصول غير مصرح به إلى النظام.

حقن SQL التدابير المضادة

اعتماد تقنية التحقق من صحة الإدخال لتعقيم إدخال المستخدم قبل تمريره إلى تطبيقات قاعدة البيانات للتنفيذ.

يجب منح المستخدمين أقل إذن عندما يُسمح لهم بالوصول إلى قاعدة البيانات.

يجب عدم السماح لتطبيقات الويب بالوصول إلى قاعدة البيانات باستخدام المسؤول الامتيازات. بدلاً من ذلك ، استخدم حسابًا محدودًا عند الوصول إلى قواعد البيانات عبر الويب التطبيقات.

حقن القيادة

حقن الأوامر (المعروف أيضا باسم **حقن قذيفة**) هو نوع من الهجوم حيث المهاجم يستغل تطبيقات الويب الضعيفة لحقن الرموز الخبيثة في الواجهة الخلفية التطبيقات من أجل السعي للوصول غير المصرح به إلى البيانات أو موارد الشبكة. هذا الهجوم يشبه إلى حد كبير الهجوم حقن SQL المذكورة أعلاه.

تستخدم صفحات الويب الديناميكية تطبيقات الويب لتقديم بيانات خاصة بالمستخدم وتنفيذ أخرى عمليات ديناميكية مثل استرداد محتويات الملف ، وإرسال رسائل البريد الإلكتروني وما إلى ذلك هذه الشبكة

تستخدم التطبيقات بدورها البرامج الأساسية مثل البرامج النصية للكتل والتشغيل

يدعو النظام لإكمال طلبات وإجراءات محددة.

إذا فشلت تطبيقات الويب مثل حقول النماذج في تعقيم بيانات إدخال المستخدم قبل اجتياز نفسه بالنسبة للتطبيقات الخلفية ، يمكن للمهاجم استغلالها بسهولة لأداء الأوامر

هجوم الحقن.

حقن الأوامر المضادة التدابير

فيما يلي بعض الإجراءات المضادة التي يمكن استخدامها لمنع الأمر

هجمات الحقن:

قم بالتعقيم الصحيح والتحقق من صحة بيانات إدخال المستخدم لإزالة أي من البيانات الموجودة محتوى ضار.

طلبات البنية بحيث يتم التعامل مع جميع المعلمات الموفرة كبيانات بدلاً من
يحتمل أن يكون محتوى قابل للتنفيذ.

تأكد من تجريد شخصيات محتملة الخطورة مثل الفواصل المنقوطة والأنابيب
(|) وعلامات (&) من إدخال المستخدم قبل تمريرها على الأساس
البرامج.
إذا كان ذلك ممكنًا ، تجنب تمرير وسائط معينة للمستخدم إلى برامج نظام التشغيل.

تجاوز سعة المخزن المؤقت

يعد تجاوز سعة المخزن المؤقت (المعروف أيضًا باسم **تجاوز سعة المخزن المؤقت**) نوعًا من
أنواع الاستغلال التي تستفيد منها
التطبيقات الضعيفة التي تنتظر معالجة مدخلات المستخدم. يقال تطبيق ويب
لتكون عرضة لهذا النوع من الهجوم عند التطبيق ، أثناء كتابة البيانات إلى
المخزن المؤقت يتجاوز الحد المخزن المؤقت والكتابة إلى الذاكرة المجاورة.

المفاهيم الأساسية لتجاوز المخزن المؤقت

يحدث تجاوز سعة المخزن المؤقت عندما يكون حجم بيانات إدخال المستخدم أكبر من حجمه
المخصص
حجم المخزن المؤقت والتطبيق يتجاوز حدود المخزن المؤقت الخاص به عند كتابة الإدخال
إلى الذاكرة.
الهدف هو تشغيل تجاوزات المخزن المؤقت في التطبيقات الضعيفة من خلال مدخلات ذلك
صممت لتنفيذ أكواد ضارة أو تغيير التدفق الطبيعي للبرنامج
التدفق الذي يحدده القراصنة.

أنواع تجاوزات المخزن المؤقت

يمكن تصنيف هجمات تجاوز سعة المخزن المؤقت في نوعين رئيسيين كما يلي:

الهجمات على كومة

الهجمات على المكدس

يعمل الهجوم على أساس كومة الذاكرة المؤقتة مساحة الذاكرة التي يتم تخصيصها بشكل حيوي إلى
البرنامج ، ولكن صعوبة المشاركة في تنفيذ مثل هذه الهجمات تجعلها نادرة. على ال

الهجمات الأخرى القائمة على المكدس هي الأسهل ، وبالتالي يتم تنفيذها على نطاق واسع من قبل المهاجمين.

كومة تجاوز سعة المخزن المؤقت مثال

المكدس هو ذاكرة كمبيوتر تستخدم عندما تستدعي إحدى الوظائف داخل البرنامج وظيفة أخرى. تحتوي هذه المجموعة على بيانات ، متغيرات محلية (متغيرات خاصة بوظيفة) ، وظيفة الحجج والأهم من ذلك عنوان المرسل للتعليمات للعودة عند واحد انتهاء وظيفة. بمعنى آخر ، عندما تستدعي "FunctionA" "FunctionB" ، تحتاج وحدة المعالجة المركزية إلى ذلك

تعرف إلى أين أعود عندما ينتهي "FunctionB" من مهمته وعنوان الإرجاع هذا (العودة إلى يتم تخزين "FunctionA") في المكدس.

خذ بعين الاعتبار نموذج التعليمات البرمجية التالي:

وظيفة باطلة A ()

}

functionB (ReadUserName (مأخذ التوصيل)) ؛

{

وظيفة باطلة B (اسم شار *)

}

[char name_arr [10 ؛

strcpy (name_arr ، الاسم) ؛

{

في المثال أعلاه ، يقرأ **functionA** السلسلة (اسم المستخدم) من من المستخدم و يمررها إلى **functionB** لنسخ نفسها إلى المخزن مؤقت ([name_arr [10) التي الحجم المخصص هو 10 بايت. عندما يدخل المهاجم اسم إدخال ابتكر بذكاء حجمه أكبر من 10 بايت ، يمكن أن تتجاوز البيانات أجزاء الذاكرة تعيين إلى "name_arr" مما أدى إلى تجاوز سعة المخزن المؤقت. تذكر أن كومة أيضا يحتوي على عنوان المرسل لـ **functionA** عند اكتمال **functionB** تنفيذه. عندما تجاوزات المخزن المؤقت ، يمكن للمهاجم معالجة المكدس لتعيين عنوان المرسل الخاص به إلى نشير حيث يوجد برنامجه الخبيث في المخزن المؤقت. بهذه الطريقة ، يمكن للمهاجم استغلال

مكدس تجاوز مشكلة عدم الحصانة في تطبيقات الويب لتنفيذ رموزه الضارة و السيطرة على النظام.

تجاوز المخزن المؤقت التدابير المضادة

التحقق من صحة طول إدخال البيانات في النماذج قبل تمريرها إلى الوظائف.

ممارسة عادات الترميز آمنة ومأمونة عند التعامل مع المخازن المؤقتة.

استخدم أدوات مثل **Stack Shield** و **Stack Guard** لأنظمة Linux للدفاع ضدها كومة هجمات الفائض.

دليل السفر

دليل اجتياز هو نوع من مشكلة عدم حصانة HTTP المستخدمة من قبل المتسللين للوصول إلى الدلائل المقيدة ونظام الملفات على خادم الويب. يحدث هجوم اجتياز الدليل بسبب عدم قدرة خوادم الويب على التحقق من / تصفية مدخلات المستخدم. تطوير تطبيقات الويب باستخدام لغات البرمجة مثل PHP و Python و Perl و Apache و ColdFusion عرضة عادة لهذا النوع من الهجوم.

المفاهيم الأساسية ل عبور الدليل

يمكن استخدام مهاجمين مشكلة عدم الحصانة هذه استعراض الدلائل والملفات الموجودة خارج وصول التطبيق العادي.

هذا النوع من الهجوم يكشف بنية الدليل وخادم الويب الأساسي والتشغيل نظام الجهاز الضعيف.

يسمح الهجوم للمتسلل بالوصول إلى الصفحات المحظورة والمعلومات السرية على النظام.

دليل عبور التدابير المضادة

التحقق من صحة مدخلات المستخدم من المتصفحات.

استخدم عوامل تصفية لحظر عناوين URL التي تحتوي على أوامر ورموز الهروب يشيع استخدامها من قبل المهاجمين.

حدد حقوق الوصول إلى المناطق المحمية في موقع الويب لتقييد المستخدم العادي التمكن من.

حافظ على تحديث برنامج خادم الويب بأحدث التصحيحات والتحديثات.

أدوات لمسح الضعف

فيما يلي بعض الأدوات الشائعة التي يمكن استخدامها للعثور على نقاط الضعف في الويب التطبيقات.

Acunetix: هذا هو الماسح الضوئي الضعف تطبيق ويب على مستوى المؤسسة و أداة اختبار الاختراق المتاحة لأجهزة ويندوز.

W3af: هذا هو أداة الهجوم ومراجعة التطبيقات مفتوحة المصدر لنظام التشغيل BSD ، Linux ، أجهزة ماك وويندوز.

Vega: يتم استخدام هذه الأداة للعثور على تطبيق الويب الذي يتم العثور عليه بشكل شائع وإصلاحه

نقاط الضعف مثل XSS ، حقن SQL وأكثر. إنها أداة مفتوحة المصدر مكتوب فيها جافا ومتاحة لأنظمة تشغيل Windows و Linux.

Arachni: هذه أداة قوية مفتوحة المصدر تستخدمها أجهزة اختبار الاختراق والنظام المسؤولون لتقييم أمن تطبيقات الويب. الأداة متاحة ل

منصات لينكس وماك.

X5S **X5S:** هي أداة قوية مصممة للعثور على نقاط الضعف في البرمجة النصية للمواقع تطبيقات الويب.

الفصل 15 - اختراق مستخدمي الإنترنت

بسبب الزيادة السريعة في عدد مستخدمي الإنترنت في السنوات الأخيرة ، الخبيثة بدأ المتسللون الآن في استهداف المستخدمين الفرديين لهجومهم. جانب العميل عديدة نقاط الضعف مثل عيوب المتصفح وانعدام الوعي الأمني بين الإنترنت

المستخدمين جعلتهم هدفا سهلا للمتسللين. في هذا الفصل دعونا نلقي نظرة على بعض طرق شائعة لاختراق مستخدمي الإنترنت وكذلك التدابير المضادة لمنعهم.

أهداف اختراق مستخدمي الإنترنت

يستهدف المتسللون المستخدمين الفرديين لمجموعة متنوعة من الأسباب كما هو مذكور أدناه:

للوصول إلى المعلومات السرية مثل تفاصيل بطاقات الائتمان والبنك
تسجيلات الدخول ، معلومات الحساب الخ
للسيطرة على حسابات المستخدم عبر الإنترنت مثل البريد الإلكتروني والفيسبوك وغيرها من الشبكات الاجتماعية
حسابات الشبكة.
لكسب إيرادات الإعلانات عن طريق دفع المستخدمين بقوة إلى الإعلانات عبر الإنترنت مثل كما لافتات والنوافذ المنبثقة.
لاستخدام المستخدمين الفرديين لمهاجمة أنظمة أخرى مثل التسبب في هجوم DDoS.
في بعض الأحيان حتى للمتعة أو المواهب الاستعراضية بين مجتمع القراصنة.

تقنيات الاختراق المشتركة

فيما يلي بعض التقنيات الشائعة الاستخدام لاختراق المستخدمين الفرديين على الإنترنت:

اختطاف الجلسة (اختطاف ملفات تعريف الارتباط)

نظرًا لأن صفحات الويب لا تحتوي على ذكريات ، فيجب عليها استخدام وسيلة لتحديد الهوية والتوثيق
المستخدمين الفرديين الذين يصلون إلى صفحات الويب. خاصة عندما يصل الناس إلى قيود الصفحات أو المنطقة الآمنة التي تتطلب مصادقة كلمة المرور ، يحتاج الموقع إلى وسيلة تذكر المستخدمين بشكل فردي بعد تسجيلات الدخول الناجحة. على سبيل المثال ، عندما يسجل الناس
في حساب Facebook الخاص بهم (عن طريق إدخال كلمة المرور) ، يمكنهم الوصول إلى عدة مواقع مختلفة
الصفحات حتى يتم تسجيل الخروج أخيرًا. سيكون من غير العملي مطالبة المستخدمين بإعادة إدخال كلمة المرور
في كل مرة يصلون إلى صفحة مختلفة.

ملفات تعريف ارتباط الجلسة

لذلك ، لتذكر المستخدمين الفرديين ، تخزن مواقع الويب ملفًا صغيرًا يسمى **الجلسة**
ملف تعريف الارتباط على جانب العميل (في متصفح المستخدم) والذي يحتوي على مصادقة فريدة

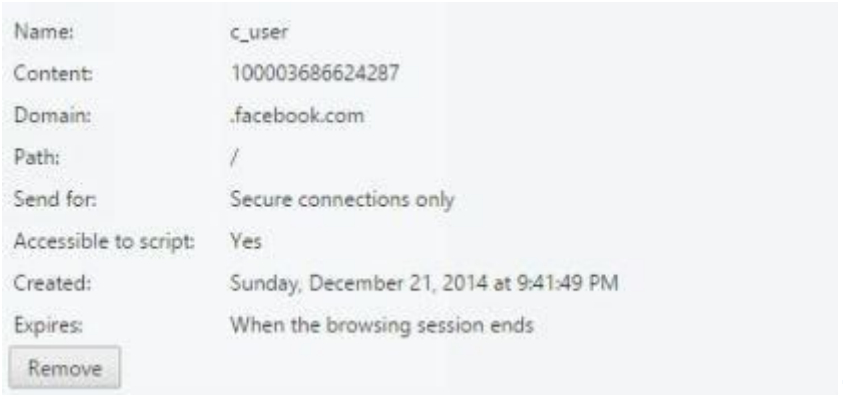
معلومات حول جلسة المستخدم النشطة. تساعد ملفات تعريف الارتباط هذه في تحديد المستخدمين الفرديين
في جميع أنحاء الموقع. عندما يضرب المستخدم زر تسجيل الخروج أو يغلق المتصفح ،
يقال الجلسة تنتهي.
لذلك ، عندما يتمكن أحد المتسللين من سرقة ملفات تعريف الارتباط الخاصة بجلسة نشطة ، فقد يقوم بحقنها
متصفحه للحصول على غير مصرح به لأي حساب على الإنترنت مثل رسائل البريد الإلكتروني ، وسائل الإعلام الاجتماعية
حسابات وهلم جرا. تُعرف هذه التقنية **باختطاف الجلسة** (يشار إليها أيضًا باسم
اختطاف ملفات تعريف الارتباط أو **سرقة ملفات تعريف الارتباط**).

جلسة اختطاف تجريبي

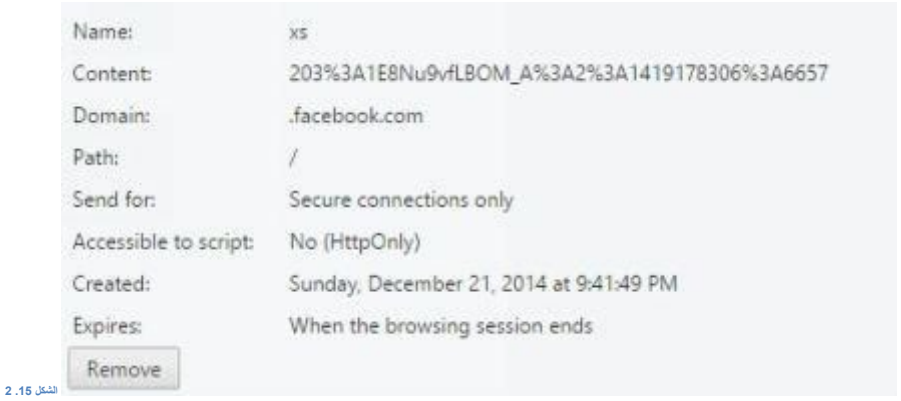
في ما يلي عرض توضيحي لجلسة اختطاف نموذجية أجريت على نموذج Facebook
الحساب. هنا قد يستخدم المتسلل تقنيات مختلفة مثل *البرمجة النصية عبر المواقع (XSS)* أو
استنشاق الحزمة لسرقة ملفات تعريف ارتباط جلسة المستخدم الهدف.
على الرغم من أن Facebook يخزن العديد من ملفات تعريف الارتباط في المتصفح بعد تسجيل الدخول بنجاح ، هناك
هما فقط ملفات تعريف الارتباط الهامة التي تحتوي على بيانات المصادقة لتحديد نشط
جلسة. فيما يلي أسماء هذين الملفين:

1. **c_user**
2. **XS**

من أجل اختطاف جلسة نشطة ، يجب على المرء الوصول إلى محتويات الاثنين أعلاه
بسكويت. فيما يلي لقطات من نماذج البيانات الموجودة في هذين الملفين:



الشكل 15. 1



الشكل 15. 2

بمجرد وصولك إلى محتويات ملفات تعريف الارتباط **للجلستين** أعلاه " **c_user"** و " **xs"** حان الوقت لحقنهم في متصفحك والوصول إلى Facebook المستخدم المستهدف الحساب. امتداد فايرفوكس يسمى "**مدير ملفات تعريف الارتباط المتقدم** "يجعل هذا العمل كثيرًا بساطة. يوفر خيارًا لإضافة وتعديل ملفات تعريف الارتباط المخزنة على Firefox. هنا خطوة بخطوة

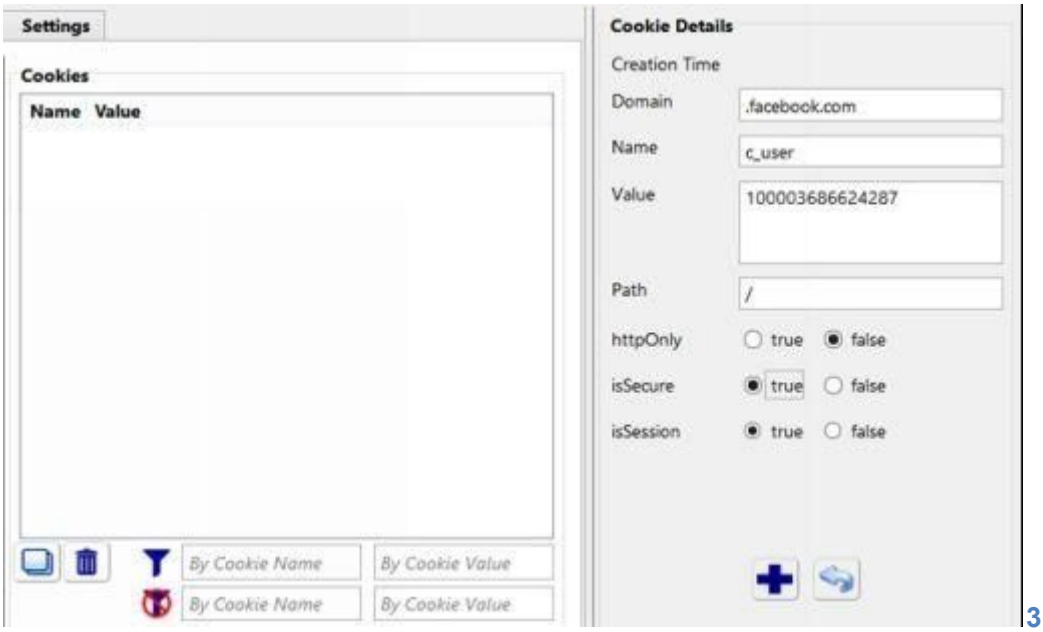
إرشادات خطوة لحقن ملف تعريف الارتباط في متصفح Firefox:

تثبيت الوظيفة الإضافية **Advanced Cookie Manager** لمتصفح Firefox وافتحه بالنقر فوق الرمز الموجود في شريط الأدوات.

انتقل إلى علامة التبويب "إدارة ملفات تعريف الارتباط" وانقر على زر "إضافة ملفات تعريف الارتباط".

لإنشاء ملف تعريف الارتباط " **c_user** " ، قم بملء جميع التفاصيل تمامًا كما هو موضح أدناه لقطة نتوقع لحقل "القيمة" الذي يجب استبداله بالمحتوى من

ملف تعريف الارتباط المختطف. بمجرد الانتهاء من ذلك ، انقر على زر "إضافة".

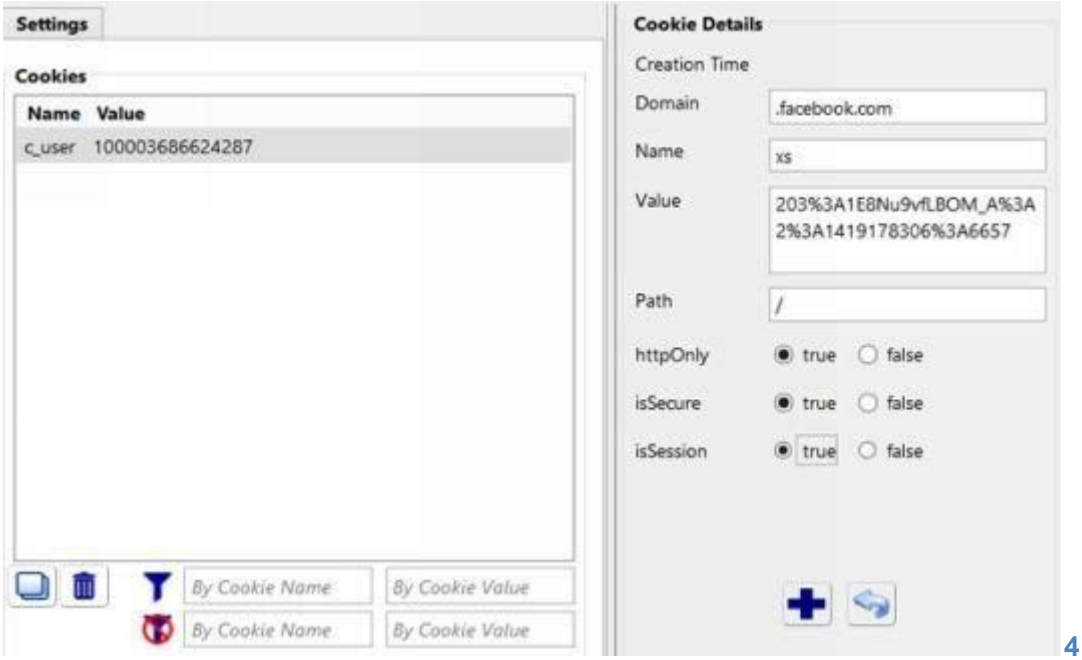


الشكل 15. 3

مرة أخرى ، انقر فوق الزر "إضافة ملف تعريف الارتباط" لإنشاء ملف تعريف الارتباط " **xs** " بنفس الطريقة. بعد

ملء التفاصيل كما هو موضح أدناه انقر على زر "إضافة". لا تنسى أن تحل محل

حقل "القيمة" مع المحتوى من ملف تعريف الارتباط "xs" المختطف:



الشكل 15. 4

بعد الانتهاء من إنشاء هذين الملفين ، أغلق "ملف تعريف الارتباط المتقدم"

مدير "وتحميل صفحة الفيسبوك. يجب أن يتم تسجيل الدخول تلقائيًا إلى
حساب المستخدم المستهدف حيث لديك حق الوصول الكامل.
بمجرد تسجيل الدخول ، يمكنك الوصول إلى الحساب طالما كانت جلسة المستخدم الهدف
نشيط. هذا يعني أنه يمكنك الوصول إلى الحساب بالتوازي من جهاز الكمبيوتر الخاص بك حتى
يضرب المستخدم زر "تسجيل الخروج" على جهاز الكمبيوتر الخاص به.

دورة اختطاف الإجراءات المضادة

فيما يلي بعض الإجراءات المضادة لمنع اختطاف الجلسة على جهازك
الحاسوب:
استخدم معايير التشفير مثل SSL (HTTPS) لمنع اختطاف ملفات تعريف الارتباط عبر الحزمة
استنشاق.
استخدم برنامج مستعرض حديث لمنع استغلال المستعرضات.
قم بتكوين المتصفح لإيقاف تشغيل البرامج النصية التي لم يتم التحقق منها وتجنب استخدام المتصفح
أيضًا
المكونات الإضافية من مصادر غير موثوق بها.

البريد الإلكتروني القرصنة

القرصنة عبر البريد الإلكتروني هي واحدة من الموضوعات الساخنة السائدة في مجال القرصنة
الأخلاقية. القراصنة
يمكن الوصول إلى مجموعة واسعة من المعلومات الخاصة حول المستخدم المستهدف إذا كان مدير
لاختراق حساب البريد الإلكتروني الخاص به. بعض الطرق الممكنة لاختراق حسابات البريد
الإلكتروني هي
مشروح بالاسفل.

ال keylogging

إن استخدام برنامج تجسس مثل keylogger هو أسهل طريقة لاختراق بريد إلكتروني أو أي
كلمة مرور الحساب الأخرى عبر الإنترنت. كل ما عليك فعله هو مجرد تثبيت برنامج
keylogger على

الكمبيوتر حيث من المحتمل أن يصل المستخدم المستهدف إلى حساب البريد الإلكتروني الخاص به من. هؤلاء

برامج التجسس مصممة للعمل في وضع التخفي الكلي ، وبالتالي يبقى

مخفية تماما عن المستخدمين العاديين. بمجرد تسجيل ضغطات المفاتيح ، يمكنك فتحها

البرنامج باستخدام مزيج مفتاح التشغيل السريع أو كلمة المرور لعرض السجلات. تحتوي السجلات جميع ضغطات المفاتيح المكتوبة على لوحة مفاتيح الكمبيوتر بما في ذلك أسماء المستخدمين و كلمات السر.

برامج كلوغر الحديثة مثل SpyAgent ،Realtime-Spy و SniperSpy الدعم

ميزة المراقبة عن بعد حيث يمكنك عرض السجلات حتى من موقع بعيد.

لدى البعض منهم أيضًا ميزة لإرسال السجلات عبر البريد الإلكتروني و FTP.

على الرغم من أن كلوغرز يستطيعون جعل عملية القرصنة أكثر بساطة ، إلا أنهم يمتلكون القليل منها

عيوب. يجب تثبيت معظم هذه البرامج يدويًا على الكمبيوتر الهدف

التي تحتاج إلى الوصول المادي إليها. أيضا ، هناك فرصة لمكافحة برامج التجسس

برامج الكشف عن وحذف تثبيت keylogger على الكمبيوتر.

الخداع

الخداع هو أسلوب شائع وفعال للغاية يستخدمه المهاجمون لاختراق البريد الإلكتروني

والحسابات الأخرى عبر الإنترنت. معظم مستخدمي الإنترنت يسقطون فريسة ويصبحون ضحايا

لهذا النوع من الهجوم. ومع ذلك ، لتوجيه هجوم تصيد ، يجب أن يكون لدى المرء أساسية على الأقل

معرفة HTML والبرمجة.

الخطوات المتضمنة في هجوم التصيد الاحتيالي:

يقوم المتسلل أولاً بإنشاء نسخة متماثلة من صفحة تسجيل الدخول الهدف مثل Gmail و Yahoo! أو

أي حساب آخر عبر الإنترنت.

تم تصميم هذه الصفحة لإرسال جميع معلومات تسجيل الدخول (اسم المستخدم وكلمة المرور) على شكل حقول إلى قاعدة بيانات محلية بدلاً من الموقع الفعلي. سوف هاكر استخدام

لغة برمجة مثل PHP وقاعدة بيانات مثل MySQL لإنجاز ذلك.
بمجرد دمج الصفحة في البرنامج النصي وقاعدة البيانات ، يقوم المتسلل بتحميل المحتوى بالكامل
الإعداد لخادم استضافة لجعل صفحة الخداع متصلة.
يختار المتسلل *نطاقاً متطابقاً* (مثل *gmail-account.com* ، *gamil.com* ،
yahoo-mail.com وما إلى ذلك) لصفحة التصيد الخاصة به لتجنب أي شك.
بمجرد أن تعمل صفحة التصيد الاحتيالي وتعمل ، يقوم المتسلل بتوجيه الناس إلى هذا التصيد
الاحتيالي
صفحة عن طريق نشر رابط التصيد عبر البريد الإلكتروني و Internet Messenger
والمنتديات.
نظرًا لأن صفحات الخداع تبدو مماثلة تمامًا للصفحات الحقيقية ، يدخل الأشخاص في تسجيل
الدخول
التفاصيل على هذه الصفحات حيث يتم سرقتها ويتم تخزينها في المخترق
قاعدة البيانات.

اختطاف الجلسة

كما نوقش سابقًا ، من الممكن الوصول إلى حساب بريد إلكتروني خلال الجلسة
اختطاف. بسرقة ملفات تعريف الارتباط الخاصة بجلسة نشطة وحقنها في مكان واحد
متصفح ، فمن الممكن للوصول إلى حساب البريد الإلكتروني المستهدف. ومع ذلك ، إذا كان الهدف
يغلق المستخدم جلسته الحالية من خلال تسجيل الخروج ، ولن تتمكن بعد الآن من الوصول إلى
الحساب. أيضًا ، بخلاف تدوين المفاتيح والتصيد ، لا تمنحك هذه الطريقة
كلمة مرور الحساب الهدف وبالتالي لن تتمكن من إعادة الوصول إليه في وقت لاحق
زمن.

فتح كلمات المرور المخزنة

يفضل معظم المستخدمين تخزين تفاصيل كلمة المرور الخاصة بالبريد الإلكتروني والحسابات
الأخرى عبر الإنترنت في
متصفح لتمكين الوصول السريع. في بعض الأحيان تسجيل الدخول تفاصيل عملاء البريد الإلكتروني
دون اتصال مثل
يتم تخزين Outlook أيضًا على الكمبيوتر. هذا يجعلهم عرضة للقراصنة. **Nirsoft و**

يوفر حفنة من الأدوات المجانية لاستعادة كلمات المرور المخزنة على Windows. تستطيع
قم بتنزيل الأدوات من الرابط أدناه:

تنزيل: http://www.nirsoft.net/password_recovery_tools.html

البريد الإلكتروني القرصنة التدابير المضادة

فيما يلي بعض الإجراءات المضادة التي يمكنك اعتمادها لمنع بريدك الإلكتروني و
حسابات أخرى عبر الإنترنت من الاختراق:

قم بتثبيت برنامج جيد لمكافحة الفيروسات ومكافحة برامج التجسس على جهاز الكمبيوتر الخاص بك والاحتفاظ بها
حتى الآن.
حماية كلمة المرور لنظام التشغيل الخاص بك بحيث لا يمكن لأحد الوصول إلى جهاز الكمبيوتر الخاص بك في
غيابك.
قم دائمًا بإجراء فحص للبرامج الضارة قبل تثبيتها.
تجنب الوصول إلى حساباتك في الأماكن العامة مثل المقاهي الإلكترونية.
تأكد من تشغيل HTTPS عند الوصول إلى رسائل البريد الإلكتروني الخاصة بك.
لا تنقر فوق الروابط الموجودة في بريدك الإلكتروني أو المنتدى للدخول إلى صفحة تسجيل الدخول. في حين أن
اكتب دائمًا عنوان URL لموقع الويب في شريط عنوان المتصفح وتأكد أيضًا
يتم تمكين HTTPS على صفحة تسجيل الدخول الخاصة بك.
تجنب تخزين تفاصيل تسجيل الدخول الخاصة بك على المتصفح إلا إذا كنت المستخدم الوحيد على الحاسوب.

طرق أخرى لاختراق مستخدمي الإنترنت

فيما يلي بعض طرق القرصنة الأخرى الشائعة في الممارسة:

JavaScript: نظرًا لأن معظم التطبيقات من جانب العميل مكتوبة بلغة JavaScript ، فهي أيضًا
يجعل أداة رائعة للمتسللين لكتابة برامج ضارة للاستغلال
نقاط ضعف المتصفح. نظرًا لنقص الوعي الأمني بين المستخدمين ، يمكنهم ذلك

من السهل أن ينخدع في إدخال معلومات حساسة أو الانتقال إلى الخبيثة
المواقع. ويمكن أيضا أن تستخدم لتنفيذ هجمات أخرى مثل البرمجة النصية عبر المواقع و
التصيد.

البرامج الضارة: يعد استخدام البرامج الضارة طريقة شائعة أخرى لاختراق مستخدمي الإنترنت.
قراصنة
استفد من البرامج الضارة مثل فيروسات وحصان طروادة لإنجاز مهمتها
عن طريق التأثير على عدد كبير من الناس. ومن الأمثلة الشائعة على هذا الهجوم استخدام
" DNSChanger " طروادة التي طالت الملايين من مستخدمي الإنترنت عن طريق خطف بهم
خوادم DNS.

المراسلة الفورية: يمكن للمهاجمين أيضًا استهداف مستخدمي الرسائل الفورية من خلال إرسالهم
غير المرغوب فيهم
العروض في شكل ملفات وروابط. هذا قد تضليل المستخدمين في التثبيت
البرامج الضارة أو الانتقال إلى مواقع الويب الضارة.

استنتاج

أود أن أهنئ مجهودك لإنجازه من خلال الكتاب بأكمله. على مدار
مسار هذا الكتاب الذي تم عرضه على تقنيات القرصنة المختلفة و
مفاهيم الأمان التي وضعت أساسًا قويًا لتقديم نفسك كمتسلل أخلاقي.
ومع ذلك ، كما يوحي اسم هذا الكتاب نفسه ، هذه مجرد بداية. في مجال ال
أمن المعلومات ، هناك دائمًا مساحة وحاجة لتعلم أشياء جديدة والبحث عنها
لتوسيع المعرفة يبقى إلى الأبد. تذكر ، تقنيات القرصنة في الوقت الحاضر
قد لا تعمل من أجل المستقبل! كما تحصل اكتشاف نقاط الضعف الجديدة القديمة الحصول عليها
مرمم. لذلك ، يجب أن يكون لديك متسلل أخلاقي دائمًا تحديثًا عن آخر أمان
الأخبار ونقاط الضعف المكتشفة حديثا.

قراءة متعمقة

من أجل تسهيل الأمر للمبتدئين والقراء لأول مرة ، قمت بتسهيل بعض
المواضيع في الكتاب. ومع ذلك ، يمكن توسيع كل منها ومناقشتها في الكثير

طريقة أعمق. يمكنك دائمًا اختيار موضوعك المفضل من الكتاب والبدء في التعلم
المزيد عن ذلك.
واحدة من أفضل طريقة لتوسيع المعرفة من خلال شراء كتاب عن موضوع معين و
متابعة ذلك. بالإضافة إلى ذلك ، يمكنك معرفة المزيد عن المواضيع الفردية من خلال الانضمام عبر
الإنترنت
المجتمعات حيث يمكنك مناقشة مشاكلك وإيجاد حلول سريعة من الخبراء.
فيما يلي مجموعة من بعض الروابط المفيدة التي تساعد على توسيع نطاق معرفتك
موضوع:
HackThisSite: واحد من أفضل المواقع التي توفر منصة ممتازة للتعلم والاختبار و
توسيع مهارات القرصنة الخاصة بك.
قراصنة Hellbound: موقع آخر يوفر معلومات متعمقة حول مختلف
مواضيع متعلقة بالأمان.
Astalavista: هذا مكان رائع للتعرف على أحدث مآثر الأمان والاختراق
التقنيات ، رمز تكسير وأكثر من ذلك.
هاك المنتديات: هنا يمكنك مناقشة والتفاعل مع مجموعة كبيرة من يشبهه
الأشخاص والخبراء لإيجاد المعلومات والحلول لمختلف الموضوعات والمشاكل

البرمجة وتطوير الشبكة.

اقتراحات وردود الفعل

أتمنى أن تكون قد وجدت هذا الكتاب غني بالمعلومات وأنك راضي عن الطريقة التي تسير بها
الأمور
قدم. إذا كان لديك أي أسئلة أو تعليقات أو ملاحظات لا تتردد في الاتصال
مع عنوان بريدي الإلكتروني المذكور أدناه:

البريد الإلكتروني: mohmedsaad6464@gmsil.com

تحياتي الحارة،

محمد سعد


محمد سعد
2020
mohmed saad
2020