الجامعة الافتراضية السورية

SYRIAN VIRTUAL UNIVERSITY

أمن الشبكات والبنية التحتية المعلوماتية

الدكتور غسان سابا

ISSN: 2617-989X

Books

أمن الشبكات والبنية التحتية المعلوماتية

الدكتور غسان سابا

من منشورات الجامعة الافتراضية السورية

الجمهورية العربية السورية 2018

Network & IT Infrastructure Security

Ghassan Saba

Publications of the Syrian Virtual University (SVU)

Syrian Arab Republic, 2018

ISSN: 2617-989X

الفهرس

ISSN: 2617-989X

ISSN: 2617-989X

الفصل الأول: مقدمة عن أمن تقانات المعلومات

Introduction to IT security

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- وصف تحديات أمن المعلومات
- فهم أمن المعلومات ومناقشة أسباب أهميتها
- تعرف أنواع الهجمات المشهورة
- تعرف الخطوات المطلوبة للهجمات
- فهم المبادئ الخمسة اللازمة للدفاع

نسمع يومياً عن الهجمات الموجهة إلى الأنظمة المعلوماتية أو الحواسيب بأنواعها أو الأجهزة المحمولة أو الجوالة الموجودة في المؤسسات والمصارف والجامعات والمدارس وعند الأفراد. من الأمثلة المعروفة عن هذه الهجمات: حجب الخدمة أو سرقة الهوية أو البرامج الخبيثة Malware والتصيد Phishing وأدوات الجذر rootkits والأبواب الخلفية والهندسة الاجتماعية وشبكات البوتنت Botnets.

ولّدت الحاجة إلى الدفاع ضد هذه الهجمات اختصاصاً جديداً ضمن تقانات المعلومات يعرف تحت اسم أمن المعلومات Information Security والذي يركز على حماية المعلومات الالكترونية للمؤسسات وللأفراد.

يوجد حالياً صنفين رئيسين لوظيفة أمن المعلومات. وظيفة إدارة أمن المعلومات وتركز على الإدارة العامة وإدارة المخططات والسياسات والأشخاص. أما وظيفة تقنيات أمن المعلومات فهي تركز على تصميم وإعداد وتثبيت وصيانة أجهزة الحماية.

1. تحديات حماية المعلومات

الأنواع المختلفة للهجمات الممكن أن تتأثر بها المعلومات وطبيعتها تجعل وجود حل بسيط يضمن أمن المعلومات أمناً كاملاً شبه مستحيل.

1.1. الهجمات الأمنية Security Attacks

يزداد عدد الهجمات الناجحة باضطراد يوماً بعد يوم وتزداد معه الموازنات المخصصة للحلول الأمنية. نبين فيما يلي التطور الحالي فيما يخص الهجمات الأمنية:

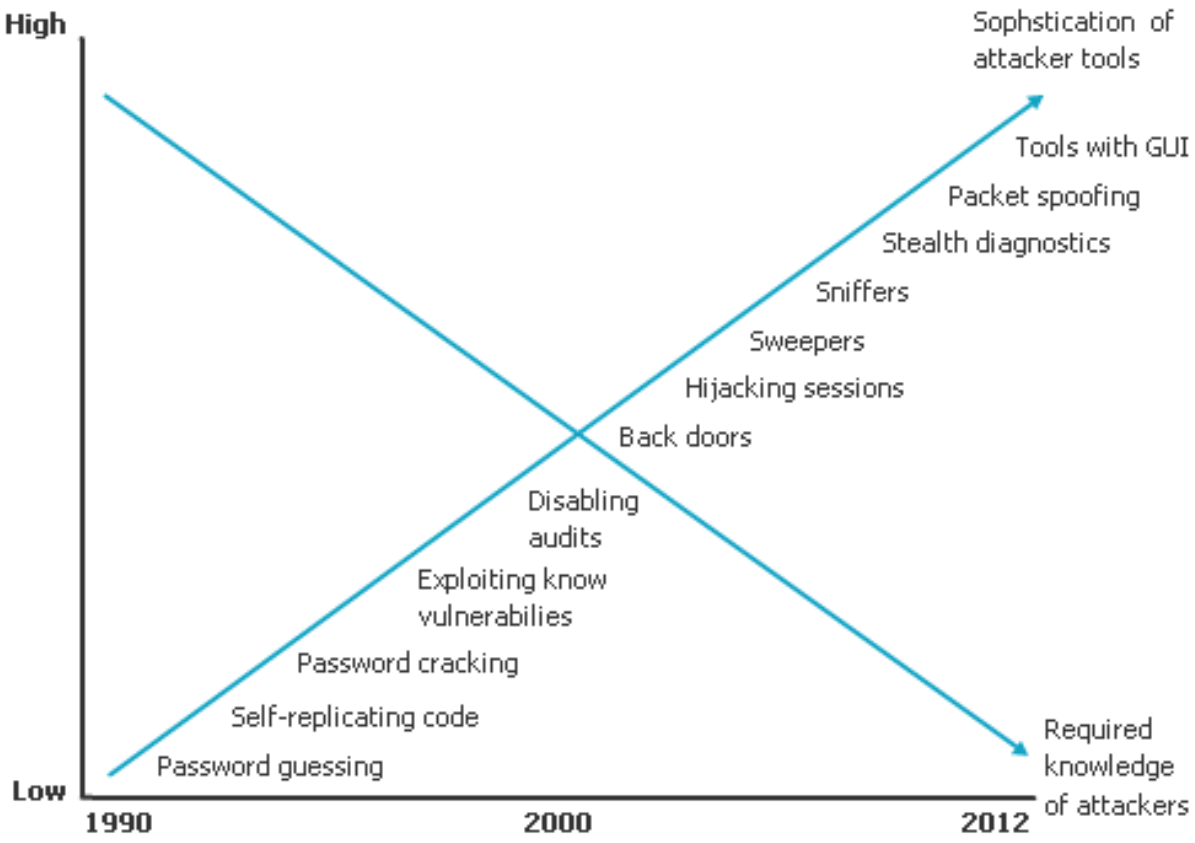
- تعتبر هجمات مضادات الفيروسات المزيفة Fake anti-virus attacks مسؤولة عن نصف البرامج الخبيثة المحملة عن طريق إعلانات الوب.
- الهجمات على مصارف الإنترنت باستخدام البرامج الخبيثة.
- يتجه المهاجمون حالياً إلى الاعتماد على وحدات المعالجة البيانية GPU بدلاً عن CPU نظراً لسرعة المعالجة فيها والتي يمكن أن تصل لحد 2 Teraflop. يمكن استخدام هذه الوحدات لكسر كلمات المرور حيث يعتقد بعض الباحثين بإمكانية كسر كلمات المرور المؤلفة من 12 محرفاً أمراً قريباً إذا لم يكن قد حصل فعلاً.
- لا يتم تصحيح جميع الثغرات الأمنية المكتشفة في البرمجيات.
- يزداد يومياً عدد عمليات الاحتيال التي تتم عن طريق البريد الالكتروني غير المرغوب به SCAM والتي أصبحت تحتل المركز الأول من ضمن عمليات الاحتيال عبر الإنترنت.
- حوالي 10% من الهواتف الذكية مصاب بفيروس أو برنامج خبيث على الأقل.

2.1. صعوبات مكافحة الهجمات

يوجد مجموعة من الصعوبات التي تصعّب تطبيق الحلول الأمنية، نذكر منها:

- الأجهزة الموجودة دائماً على الخط. غالبية الحواسيب وأجهزة الهواتف الذكية موصولة دائماً إلى الأنترنت الأمر الذي يسهل اختراقها.
- المعدل المتزايد للهجمات. يستطيع المهاجم باستخدام الأدوات الحديثة مهاجمة آلاف الأنظمة لاكتشاف نقاط الضعف وبدء الهجمات بسرعة كبيرة. حتى أن بعض الأدوات تبادر إلى الهجوم بدون تدخل المستخدم.
- تطور أكبر للهجمات. الأمر الذي يصعب اكتشاف الهجمات وبالتالي مكافحتها. بعض الهجمات تظهر بشكل مختلف في كل مرة بينما غيرها يتخفى على شكل حركات مرور طبيعية.
- توافر وبساطة أدوات المهاجمة. لا تتطلب الأدوات الحالية لشن الهجمات معارف وخبرات متقدمة لدى المهاجم بالبرمجة وبالشبكات وبأنظمة التشغيل حتى أن بعض هذه الأدوات يأتي مزوداً بواجهات بيانية GUI. يكون معظم هذه الأدوات مجاني أو تكون أسعارها زهيدة.

- اكتشاف أسرع للثغرات باستخدام الأدوات الحديثة.
- تأخير تصحيح الثغرات وسوء إدارة توزيع التصحيحات على المستخدمين
- الهجمات الموزعة. يمكن للمهاجم التحكم بعشرات الآلاف من الحواسيب لمهاجمة مخدم واحد أو شبكة ما. يجعل هذا النوع من الهجمات إمكانية مكافحته عن طريق توقيف المصدر شبه مستحيلة.



الشكل 1: تناقص المعارف المطلوبة مع تزايد تعقيد الهجمات

2. ما هو أمن المعلومات؟

لنبدأ بتعريف أمن المعلومات وأهمية حماية المعلومات ومن هم المهاجمون.

1.2. تعريف أمن المعلومات

يستخدم مصطلح أمن المعلومات Information security عادةً لوصف مهام حماية المعلومات بشكلها الرقمي. يمكن أن تكون هذه المعلومات قيد المعالجة ضمن وحدة المعالجة المركزية أو مخزنة على قرص صلب أو منقولة باستخدام شبكة ما.

يمكن فهم أمن المعلومات من خلال تعريف أهدافه وطرق تحقيقه. يضمن أمن المعلومات أولاً التحقيق السليم لإجراءات الحماية (الأمن عن طريق الحماية). كما يهدف أمن المعلومات ثانياً إلى حماية المعلومة نفسها التي تزود قيمة للفرد أو للمؤسسة. يجب هنا تأمين ثلاثة أنواع من الحماية للمعلومات وهي: الخصوصية Confidentiality والسلامة Integrity والتوافر Availability التي تختصر بمصطلح CIA:

1. الخصوصية. يستطيع فقط الأشخاص المخولين أو المصرح لهم النفاذ إلى أو رؤية المعلومات الهامة.
2. السلامة. تضمن السلامة كون المعلومات صحيحة ولم يجر تغييرها من قبل شخص غير مخول أو برنامج خبيث.
3. التوافر. يضمن التوافر كون المعلومات متاحة للأشخاص المخولين حتى يستطيعون الاستفادة من قيمتها.

نحتاج، إضافةً إلى CIA، إلى تحقيق مجموعة أخرى من الحمايات لضمان أمن المعلومات. نذكر من بين هذه الحمايات: الاستيقان أو المصادقة Authentication والتفويض Authorization والمحاسبة Accounting أي ما يعرف بـ AAA:

1. الاستيقان. يضمن الاستيقان أو المصادقة التأكد من كون الفرد هو من يدعي كونه وليس منتحل شخصية. يُستخدم عادةً كلمة مرور لا يعرفها إلا الشخص نفسه للاستيقان من هويته.
2. التفويض. بعد أن يجري الاستيقان من هوية شخص ما فإنه يفوض (يسمح له) القيام بمجموعة من المهام.
3. المحاسبة. تسمح المحاسبة بتعقب الأحداث. كتسجيل من دخل إلى موقع وب ما؟ ومن أين؟ وفي أي وقت؟

تتمثل المهمة الثالثة لأمن المعلومات في حماية سلامة وخصوصية وتوافر المعلومات على الجهاز الذي يخزنها أو يتعامل معها أو ينقلها.

يجري تحقيق أمن المعلومات باستخدام ثلاثة مكونات كما هو موضح في الشكل 2. يجري حماية المعلومات والعتاد الصلب والبرمجيات والاتصالات من خلال ثلاث طبقات وهي المنتجات والأشخاص والإجراءات.

الشكل 2: مركبات أمن المعلومات

2.2. بعض المصطلحات المتعلقة بأمن المعلومات

مثله مثل أي موضوع متقدم, يمتلك أمن المعلومات مصطلحات خاصة به. نبدأ عادة بتحديد الأصول (الأشياء الثمينة) Assets بالنسبة للمؤسسة. يبين الجدول التالي وصفاً لبعض العناصر التي يمكن أن تمتلكها أي مؤسسة تعمل في مجال تقانات المعلومات وتقييماً لنوع كل عنصر: هل يعتبر شيء ثمين أو لا؟

اسم العنصر	الوصف	مثال	هل هو شيء ثمين؟
المعلومات	المعلومات التي تم جمعها وتصنيفها وتنظيمها وتخزينها وفق أشكال مختلفة	الزبائن والإنتاج والمبيعات والتسويق والمالية	نعم: يصعب جداً استبدالها
البرمجيات التطبيقية	البرمجيات التي تدعم إجراءات العمل للمؤسسة	التطبيقات المخصصة لتداول الأوامر ومعالجات النصوص	نعم: لأنها خاصة بالمؤسسة لا: لأنها متوفرة في الأسواق
برمجيات النظام	البرمجيات الأساسية لتشغيل التطبيقات	أنظمة التشغيل	لا: يمكن استبدالها بسهولة
المواد الفيزيائية	الحواسيب وتجهيزاتها وأجهزة الاتصالات والشبكات ووسائط التخزين والفرش والمكاتب	المخدمات والمسيرات والأقراص المدمجة	لا: يمكن استبدالها بسهولة
الخدمات	الاستعانة بخدمات من مصادر خارجية Outsourcing	اتصالات الصوت والمعطيات	لا: يمكن استبدالها بسهولة

الشكل 3: الأشياء الثمينة المتعلقة بأمن المعلومات

نحدد بعد ذلك التهديدات Threats المحيطة بالأشياء الثمينة مثل سرقة المعلومات أو تأخر نقلها.

نطلق على الشخص أو العنصر الذي يشكل مصدر تهديد بعميل التهديد Threat agent. يمكن أن يكون عميل التهديد أي شخص يحاول اختراق الشبكة المعلوماتية الآمنة أو حتى أي قوة طبيعية مثل الأعاصير أو الفيضانات التي يمكن أن تدمر البنية التحتية المعلوماتية والمعلومات بطبيعة الحال أو يمكن أن تكون برمجيات خبيثة تهاجم الشبكة الحاسوبية.

حتى نحمي المعلومات، يجب علينا تحديد الثغرات الأمنية أو نقاط الصعف Vulnerabilities. يمكن أن تكون الثغرة الأمنية هي عطل في برنامج ما ضمن نظام التشغيل يسمح لشخص غير مصرح له التحكم بالحاسوب دون معرفة مالك الحاسوب أو إذنه.

في حال نجح المهاجم بالتحكم بالحاسوب فإننا نقول أنه استغل الثغرة (الضعف) الأمنية Exploiting the security vulnerability.

يجب أن نحدد أيضاً مقدار الخطأ الذي يمكن التسامح معه.

المصطلح	مثال
الأصل Assets	قاعدة معطيات الموظفين
التهديد Threat	سرقة المعطيات
عميل التهديد Threat Agent	مهاجم أو فيروس أو فيضان
الضعف Vulnerability	عطل برمجي
تفادي الخطر Risk	تدريب المستثمرين

الشكل 4: مصطلحات أمن المعلومات

3.2. فهم أهمية أمن المعلومات

يشمل أمن المعلومات على منع سرقة المعطيات وإحباط سرقة الهويات وتجنب التبعات القانونية إزاء عدم حماية المعلومات والحفاظ على الإنتاجية وإحباط الإرهاب السبراني Cyberterrorism.

- منع سرقة المعلومات. تعتبر غالبية الشركات أن الهدف الاساسي للأمن المعلوماتي هو منع سرقة المعلومات مثل نتائج جديدة للبحث العلمي أو قائمة بالمستهلكين أو المعلومات الشخصية وأرقام بطاقات الائتمان.
- إحباط سرقة الهوية. تسرق المعلومات الشخصية مثل رقم بطاقة الضمان الاجتماعي لانتحال الشخصية وانشاء حساب مصرفي للشخص واستخدامه في شراء كميات كبيرة من البضائع.
- منع التبعات القانونية. يوجد العديد من القوانين التي تحمي خصوصية المعلومات الالكترونية. أي جهة تفشل في حماية هذا النوع من المعلومات تصبح عرضة للعقوبات المالية أو الجزائية.
- الحفاظ على الإنتاجية. عندما تتعرض شركة ما لهجوم فإن الانتاجية بشكل عام تتأثر سلباً أثناء الهجوم وفي فترة استعادة النظام إلى حالته السابقة.
- إحباط الإرهاب السبراني. يمكن تعريف الإرهاب السبراني بأنه أي هجوم متعمد ذو طابع سياسي ضد معلومات أو أنظمة حاسوبية أو برامج أو معطيات يسبب أذى لأهداف غير مقاتلة من قبل مجموعات دولية أو عملاء سريين. يمكن أن يطال الإرهاب السبراني الصناعة المصرفية لبلد ما أو المنشآت العسكرية أو محطات توليد الكهرباء أو مراكز مراقبة الحركات الجوية وشبكات المياه.

3. من هم المهاجمون؟

المخترقون أو القراصنة Hackers

كان يعرف المخترق سابقاً بأنه أي شخص يستخدم خبرات حاسوبية متقدمة لمهاجمة الحواسيب. أما المخترقون ذوو القبعات البيضاء White hat hackers فإنهم يهدفون إلى كشف الثغرات الأمنية دون سرقة أو تخريب المعلومات، بعكس المخترقون ذوو القبعات السوداء الذين يهدفون إلى استغلال الثغرات الأمنية لنشاطاتهم التخريبية.

حالياً، يستخدم المصطلح مهاجم attacker بدون التفريق في الهدف.

Script Kiddies

هم الأفراد الذين يريدون اختراق الحواسيب وخلق الأضرار بها دون أن يملكون المعرفة المتقدمة في الحواسيب أو أنظمة التشغيل أو الشبكات. لذلك يستخدمون برمجية مهاجمة آلية automated attack software (scripts) لتنفيذ العمليات الشريرة. 40% من الهجمات تتم حالياً عن طريق script kiddies.

الجواسيس Spies

هو أي شخص يتم التعاقد معه لاختراق حاسوب أو منظومة معلوماتية بهدف سرقة المعلومات. يختلف الجواسيس عن بقية المخترقين بأنهم يعرفون ضحيتهم مسبقاً ويعرفون طبيعة المعلومات المطلوب سرقتها دون لفت الانتباه لعملياتهم.

المطلعين insiders

يقصد بالمطلعين الأشخاص الداخليين والموثوقين مثل الموظفين والمتعاقدين والشركاء.

المجرمون السبرانيون Cybercriminals

هم شبكة من المهاجمون وسارقو الهويات ومرسلو البريد غير المرغوب spammers والمحتالون الماليين. يمكن وصفهم بأنهم مندفعين بشدة وأقل تجنباً للمخاطر وذو تمويل أفضل وأكثر عناده من المهاجمين العاديين. يجتمع المجرمون السبرانيون غالباً في منتديات على الخط تحت أرضية Underground تحمل أسماء مثل GarkMarket.org و theftservices.com بغية التجارة بالمعلومات وتنسيق الهجمات حول العالم.

يهدف المجرمون السبرانيون من هجماتهم إلى تحقيق الربح الأمر الذي يجعلهم أكثر خطورة وهجماتهم أكثر تهديداً.

الأرهابيون السبرانيون Cyberterrorists

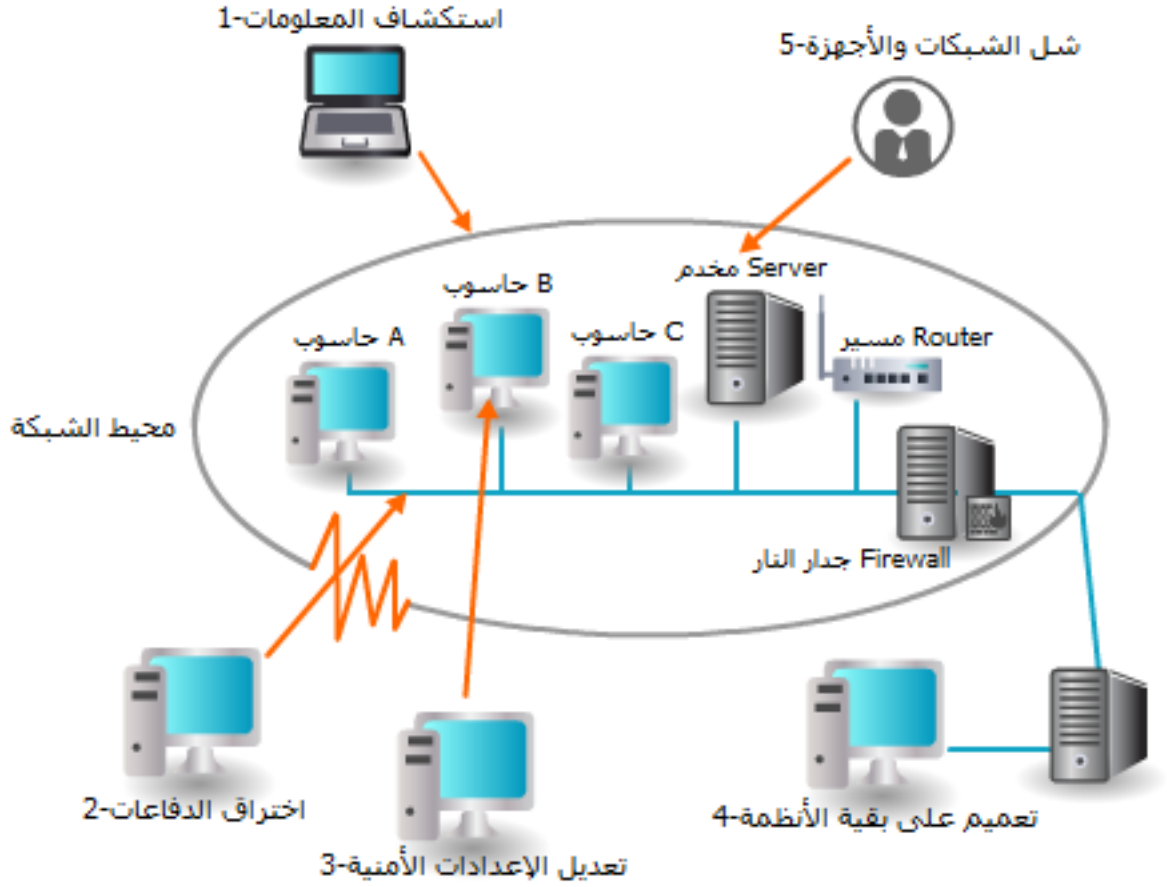
يكون هنا الهجوم على مستوى شبكة دولة ما أو بنية تحتية كاملة لبث الذعر بين المواطنين. يكون هنا المحرك الرئيسي للهجمات إما إيديولوجي أو حسب معتقداتهم ومبادئهم. الأهداف الأساسية للإرهاب السبراني:

- تشويه المعلومات الالكترونية (كمواقع الوب) ونشر معلومات مضللة وأكاذيب
- حجب الخدمات عن المستثمرين الشرعيين
- ارتكاب التطفل غير المسموح به على أنظمة وشبكات للتسبب بأعطال حرجة في البنية التحتية وإتلاف البيانات.

4. الهجمات والدفاع

خطوات الهجوم

يوجد أنواع متعددة للهجمات لكن يمكن تصنيف الهجمات عن طريق الخطوات الخمس التي تمر بها حسب ما هو موضح في الشكل التالي.



الشكل 5: خطوات تحقيق الهجوم

1. استكشاف المعلومات Probe for information. تتمثل الخطوة الأولى في الهجوم في استكشاف أي معلومة في النظام تفيد لاحقاً في تنفيذ الهجوم. يعتبر هذا النوع من الاستطلاع Reconnaissance ضروري لتزويد معلومات مثل نوع العتاد الصلب المستخدم وأرقام إصدارات البرمجيات والبرامج الثابتة firmware أو حتى معلومات شخصية عن المستخدمين يمكن الاستفادة منها في الخطوة التالية. من العمليات الممكن القيام بها في هذه الخطوة "ping sweeps" للشبكة لمعرفة عناوين IP الفعالة ومسح البوابات الفعالة port scan إضافةً إلى الاستعلامات التي تجيب برسائل الخطأ والتي تعطي معلومات هامة عن النظام.
2. اختراق الدفاعات. بعد جمع المعلومات والتعرف على نوع النظام، يمكن البدء بشن الهجمات لاختراق الدفاعات. يوجد أشكال مختلفة لهذا النوع من الهجمات.
3. تعديل الإعدادات الأمنية. بعد تحقيق الاختراق، يقوم المهاجم بتعديل الإعدادات الأمنية الأمر الذي يسمح له بإعادة النفاذ إلى النظام بسهولة أكبر.
4. تعميم على بقية الأنظمة. بعد اختراق النظام، يقوم المهاجم باستخدامه كقاعدة لمهاجمة بقية الشبكات والأنظمة بالطريقة نفسها.
5. شل الشبكات والأجهزة. إذا أراد المهاجم ذلك، فيمكن له تخريب الحاسوب المخترق عن طريق حذف أو تعديل ملفات نظام التشغيل الأساسية أو حقن برمجيات تمنع الحاسوب من العمل بشكل سليم.

5. الدفاع ضد الهجمات

مع أنه يوجد العديد من الدفاعات الممكنة لمقاومة الهجمات إلا أن هذه الدفاعات يجب أن تكون معتمدة على خمسة مبادئ أمنية أساسية: التقسيم الطبقي Layering والحد Limiting والتنوع Diversity والغموض Obscurity والبساطة Simplicity. تزود هذه المبادئ أساسيات بناء نظام آمن.

التقسيم الطبقي Layering

يجب خلق عدة طبقات أمنية لحماية أي نظام معلوماتي. حتى يستطيع المهاجم اختراق النظام الأمني هذا، يتوجب عليه اكتساب الخبرات والمهارات اللازمة لاختراق جميع الطبقات الأمنية الأمر الذي يجعل عملية الاختراق شديدة التعقيد. يؤمن التقسم الطبقي للأمن حماية شاملة ضد العديد من الهجمات.

الحد Limiting

الحد من إمكانية النفاذ إلى المعلومة يقلل التهديدات المحيطة بها. هذا يعني، أنه فقط الأشخاص الذين يستخدمون المعطيات يحق لهم النفاذ إليها. كما يجب الحد من نوع النفاذ المسموح بما يتوافق مع طبيعة العمل الذي سيجريه الشخص على المعطيات. فمثلاً، يمنح الطلاب فقط حق قراءة المعطيات التي يولدها قسم شؤون الطلاب بينما يمنح قسم الموارد البشرية حق رؤية رواتب الموظفين دون إمكانية تعديلها.

للحد من صلاحيات المستخدمين، يمكننا استخدام طرق تقانية كمنح سماحيات الملفات أو المجلدات أو استخدام طرق إجرائية (منع موظف من حذف وثيقة معينة).

التنوع Diversity

يرتبط التنوع ارتباطاً وثيقاً بفكرة التقسيم الطبقي. بما أنه يجب حماية المعلومات باستخدام عدة طبقات أمنية، فيجب أن تكون هذه الطبقات الأمنية مختلفة. هذا يعني أنه إذا استطاع مهاجم أن يخترق أحد الطبقات فهو لا يستطيع اختراق بقية الطبقات باستخدام التقنيات نفسها.

يمكن تحقيق التنوع في حماية الأنظمة المعلوماتية باستخدام أساليب عدة. مثلاً استخدام أجهزة حماية من مصنعين مختلفين (جداري نار على التسلسل كلٍ من مصنع). فعندما يخترق المهاجم لأحد الأجهزة الأمنية باستخدام مجموعة من المهارات والتقنيات، فإنه لا يستطيع اختراق الجهاز الآخر باستخدام المهارات والتقنيات نفسها.

الغموض Obscurity

يمكننا زيادة أمن أي نظام معلوماتي عن طريق إخفاء بعض المعلومات المتعلقة به. فمثلاً، عدم كشف نوع الحواسيب المستخدمة أو إصدارات أنظمة التشغيل أو نوع البرمجيات المستخدمة. فعندما لا يعرف المهاجم هذه المعلومات يصبح من الصعب عليه اختراق المنظومة المعلوماتية للمؤسسة لأن الثغرات الأمنية تكون مرتبطة عادةً بهذا النوع من المعلومات.

البساطة Simplicity

الأنظمة الأمنية المعقدة تكون عادة صعبة الفهم أو التشخيص أو التعامل مع مشاكلها. لذلك يجب أن تكون الأنظمة الأمنية بسيطة بحيث يسهل على الأشخاص الذين يتعاملون معها فهمها واستخدامها.

6. مشاريع عملية

1.6. مشروع 1: بعض المصادر على الإنترنت المتعلقة بأمن المعلومات

1. Refer to 41-internet-security-blogs-you-need-to-read.pdf file or use https://heimdalsecurity.com/blog/best-internet-security-blogs/
2. http://www.tomsguide.com/t/security/
3. https://security.googleblog.com/
4. http://www.pcadvisor.co.uk/security/
5. http://www.telegraph.co.uk/internet-security/
6. http://www.csoonline.com/news/
7. http://www.cnet.com/topics/security/
8. http://www.securityweek.com/
9. http://thehackernews.com/

2.6. مشروع 2: مسح البرمجيات الخبيثة باستخدام MS Windows Malicious Software Removal Tool

سنحاول في هذا المشروع تحميل وتشغيل برنامج مسح وإزالة البرامج الخبيثة من موقع Microsoft.

1. Open your browser and enter the URL www.microsoft.com/security/malwareremove/default.mspx
2. Click download the tool
3. Click download
4. Click save and save the program to the desired location on your local computer
5. When the download complete, click Run and follow the default installation instructions
6. When the Microsoft Windows Malicious Software Removal Tool dialog box appears, click Next.
7. Select Quick scan if necessary.
8. Click Next.
9. Depending on your computer, this scan may take several minutes. Analyze the results of the scan to determine if any malicious software was found in your computer by clicking View detailed results of the scan.
10. If any malicious software was detected, run the scan again and select Full scan.
11. Close all windows.

الفصل الثاني: البرامج الخبيثة Malware

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- فهم الفرق بين الفيروس والدودة
- تعرف أنواع البرامج الخبيثة التي تخفي وجودها
- تعرف أنواع البرامج الخبيثة المصممة من أجل الربح
- تعرف أنواع هجمات الهندسة الاجتماعية
- فهم هجمات الشبكات الاجتماعية الفيزيائية

يعتقد الكثيرون أن الهجمات على حواسبهم تأتي من برمجيات خبيثة MALicious softWARE (MALWARE). يخلق المهاجمون هذه البرامج لتتسلل بصمت عبر الحواسب بقصد الإيذاء. يمكن للبرمجيات الخبيثة (سنطلق عليها من الآن فصاعداً اسم برمجيثة) أن تعترض المعطيات أو تسرق المعلومات أو تشن الهجمات أو تتلف برمجيات الحاسب بحيث لا يعود يعمل بالشكل السليم.

نتغاضى أحياناً، عند التركيز على البرمجيثات، على الهجمات التي تعتمد الهندسة الاجتماعية. يمكن هنا خداع المستثمرين للبوح ببعض المعلومات أو لتنفيذ عمليات ما نتيجة عدم المبالاة أو الارتباك. في الواقع، يعتبر تجاوز الحمايات الأمنية باستخدام شخص ما أقل كلفة وأكثر نجاعةً من استخدام التقانات المتوفرة.

1. الهجمات باستخدام البرمجيثات

البرمجيثات هي برمجيات تدخل نظام حاسوبي دون معرفة المستثمر أو موافقته بقصد القيام بعمليات غير مطلوبة وعادةً مؤذية. البرمجيثات هو مصطلح عام يستخدم للدلالة على طيف واسع من البرامج المزعجة والمخربة. تتمثل إحدى الطرق لتصنيف البرمجيثات في تحديد هدفها الرئيسي. تهدف بعض البرمجيثات إلى انتشار العدوى بسرعة بينما يسعى بعضها الآخر إلى إخفاء الغرض منها. يهدف صنف آخر من البرمجيثات إلى تحقيق الربح المادي.

1.1. البرمجيثات التي تنتشر

يوجد نوعين من البرمجيثات التي تهدف بشكل أساسي للانتشار وهم الفيروسات Viruses والديدان Worms.

الفيروسات

فيروس الحاسوب هو رماز خبيث يعيد إنتاج نفسه داخل الحاسوب. عادةً، يُدخل الفيروس نفسه أولاً داخل أحد ملفات الحاسوب (الذي يمكن أن يكون ملف معطيات أو برنامج تنفيذي). في كل مرة يجري فيها تنفيذ البرنامج أو فتح الملف المصاب عن طريق المستثمر أو نظام التشغيل ينفذ الفيروس عملين: أولاً يحاول إعادة إنتاج نفسه reproduce itself عن طريق إدخال رمازه ضمن ملفات أخرى على الحاسوب نفسه، وثانياً، يفرغ حمولته الخبيثة ويقوم بتأدية عمل ما. نذكر من الأعمال التي يمكن أن يقوم بها الفيروس:

- التسبب بالتوقف المتكرر للحاسوب
- حذف الملفات من القرص الصلب
- صنع نسخ منه بغية استهلاك المساحات الفارغة من القرص الصلب
- إيقاف الإعدادات الأمنية للحاسوب
- إعادة تهيئة سواقة القرص الصلب

لا يستطيع الفيروس الانتقال آلياً إلى حاسوب آخر دون الاعتماد على أشخاص يقومون بنقله بدون قصد. مثلاً عند نسخ الملفات من حاسب لآخر عن طريق محرك فلاش USB أو عن طريق ملف مصاب ملحق Attachment لبريد الكتروني. عندما يصل الفيروس إلى حاسوب آخر، تبدأ العدوى.

يوجد عدة أنواع من الفيروسات الحاسوبية، نذكر منها:

- فيروس برمجي Program virus يصيب ملفات البرامج التنفيذية (الملفات ذات اللواحق exe. أو com.). عند تنفيذ البرنامج يجري تشغيل الفيروس.
- فيروس ماكرو macro virus يكتب ضمن سكريبت معروف تحت اسم ماكرو. الماكرو هو سلسلة من التعليمات التي يمكن تجميعها سويةً ضمن أمر واحد بغية أتمتة مجموعة معقدة أو مكررة من المهام. نحتاج إلى لغة ماكروية لكتابة الماكرو مثل فيجوال بيسك للتطبيقات VBA ويجري تخزينها ضمن وثيقة المستثمر (مثل وثيقة إكسل). عندما يجري فتح الوثيقة المصابة فإن تعليمات الفيروس الموجودة ضمنها تنفذ وتصيب الحاسوب.
- الفيروس المقيم resident virus هو الذي يجري تحميله ضمن ذاكرة RAM كل مرة يجري تشغيل الحاسوب وهو يصيب الملفات التي يجري فتحها من قبل المستثمر أو نظام التشغيل.
- فيروس الإقلاع boot virus يصيب سجل الإقلاع الرئيسي Master Boot Record (MBR) الموجود ضمن محرك القرص الصلب. يحوي MBR البرنامج الضروري لإقلاع الحاسوب وتوصيف تنظيم محرك الأقراص الصلبة (Partition Table). يهدف فيروس الإقلاع إلى إتلاف محرك القرص الصلب نفسه.
- الفيروس المرافق companion virus يضيف برنامج إلى نظام التشغيل هو تقليد خبيث لبرنامج نظامي. فمثلاً يمكن إضافة برنامج خبيث تحت اسم notepad.com بدلاً عن البرنامج النظامي notepad.exe. فعندما يحاول المستثمر استخدام البرنامج notepad عن طريق تنفيذ الأمر notepad بدون لاحقة فإن نظام التشغيل ينفذ البرنامج الخبيث notepad.com بدلاً عن البرنامج النظامي Notepad.exe.

الديدان

النوع الثاني من البرمجيثات الذي ينتشر هو الدودة. الدودة هي برنامج خبيث صمم للاستفادة من ضعف ما ضمن تطبيق أو نظام تشغيل بغية الدخول إلى الحاسوب. ما إن تستغل الدودة الثغرة الموجودة ضمن حاسوب ما فإنها تبحث مباشرةً عن حاسوب آخر يملك الثغرة نفسها. تستخدم الدودة الشبكات لإرسال نسخ عن نفسها إلى أجهزة أخرى مربوطة إلى الشبكة نفسها.

من العمليات التي يمكن أن تقوم بها الديدان حذف الملفات أو إضافة إمكانية تحكم المهاجم بالحاسوب عن بعد.

2.1. البرمجيثات التي تختفي

يوجد أنواع من البرمجيثات التي تهدف بشكل رئيسي إلى إخفاء وجودها عن المستثمر على عكس البرمجيثات سريعة الانتشار. نذكر من البرمجيثات الخفية الطروادي Trojan والجذور الخفية root kits والقنابل المنطقية logic bomb والأبواب الخلفية backdoors.

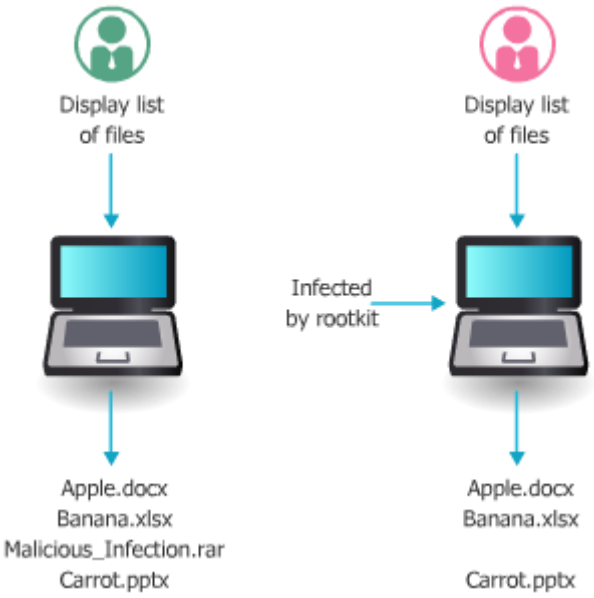
الطروادیات Trojans أو حصان طروادة

عند استخدام المصطلح حصان طروادة (أو الطروادي) مع الحواسيب فهو عبارة عن برنامج تنفيذي يهدف بشكل معلن إلى تحقيق وظيفة ما لكنه فعلاً يقوم بوظيفة أخرى (أو يقوم بالوظيفتين معاً). على سبيل المثال، يحمّل المستثمر برنامج معلن على أنه تقويم calendar لكن عندما ينفذ المستثمر البرنامج فإنه إضافةً إلى تنصيب برنامج التقويم، يقوم بمسح النظام لمعرفة أرقام البطاقات المصرفية المخزنة ضمنه وكلمات المرور ومن ثم يتصل عن طريق الشبكة بحاسب بعيد ويرسل هذه المعلومات إلى المهاجم. الطروادي هو إذاً برنامج تنفيذي يحوي رماز مخفي يستخدم للبدء بالهجوم.

الجذور الخفية rootkits

الجذر الخفي هو عبارة عن مجموعة من الأدوات البرمجية التي يستخدمها المهاجم لإخفاء العمليات التي تقوم بها مجموعة أخرى من البرمجيثات مثل الطروادیات والفيروسات والديدان أو إخفاء وجودها. تفعل الجذور الخفي ذلك عن طريق إخفاء أو حذف أثر سجلات الدخول log-in records أو معلومات الإدخالات Log entries أو الإجراءات المتعلقة بها. كما يمكن لها أن تغير نظام التشغيل ليتجاهل أي نشاط خبيث.

تتمثل إحدى الأساليب التي تتبعها الجذور الخفية في تعديل أو تبديل ملفات نظام التشغيل بإصدارات معدلة معمولة خصيصاً لتجاهل الأعمال الخبيثة. يظهر الشكل التالي مثال عن أحد أساليب عمل الجذور الخفية.



الشكل 1: أعراض الجذور الخفية

معالجة نظام التشغيل المصاب بالجذور الخفية يتطلب أولاً حذف الملفات المصابة ومن ثم نسخ ملفات أصلية مكانها. غير أن عملية حذف ملفات نظام التشغيل المصابة قد تجعل الحاسوب غير مستقر.

البرامج التي تستطيع اكتشاف الجذور الخفية تقارن عادةً محتوى ملفات نظام التشغيل مع المحتوى الأصلي. أي أنه يجب تشغيل برنامج الاكتشاف من وسط نظيف مثل القرص المضغوط أو محرك USB مخصص.

القنابل المنطقية Logic bombs

القنبلة المنطقية هي رماز حاسوبي يبقى نائماً حتى إطلاقه من قبل حدث منطقي محدد. ما أن يتم إطلاقه، فإنه يقوم بمجموعة من الأعمال الخبيثة. كمثال على القنابل المنطقية، إدخال رماز يعمل بتاريخ محدد ويقوم بحذف جميع سجلات الطلاب في جامعة ما.

استخدمت بعض الشركات النظامية القنابل المنطقية للتحقق من دفع قيمة البرمجيات التي تطورها. إذا لم يتم الدفع في تاريخ محدد، فإن القنبلة المنطقية تمنع البرنامج من العمل مجدداً وفي بعض الحالات تحذف جميع ملفات البرنامج.

من الصعوبة بمكان اكتشاف القنابل المنطقية قبل انطلاقها وذلك لأنها تكون غالباً مضمنة ضمن برامج كبيرة.

الأبواب الخلفية Backdoors

الباب الخلفي هو رماز برمجي قادر على منح حق النفاذ لبرنامج أو لخدمة بشكل يتجاوز أي حماية أمنية موضوعة. خلق باب خلفي شرعي من قبل مطوري البرامج هو ممارسة معروفة للنفاذ إلى برنامج أو جهاز دورياً بدون تعقيدات طلب كلمات المرور أو أي اجراءات أمنية أخرى. تكون النية عادة بحذف الباب الخلفي عند انتهاء تطوير البرنامج لكن غالباً ما يترك الباب الخلفي مفتوحاً الأمر الذي يسهل عملية الاختراق من قبل المهاجمين.

إضافةً إلى ما سبق، فإن البرمجيثات التي يرسلها المهاجمون يمكن أن تتصّب أبواب خلفية على حاسوب. هذا يسمح للمهاجم بالعودة في أي وقت لاحق وتجاوز الإعدادات الأمنية.

3.1. البرمجيثات ذات التوجه الربحي

يهدف النوع الثالث من البرمجيثات إلى تحقيق الربح المادي للمهاجمين. يشمل هذا النوع على البوتنت botnets وبرمجيات التجسس spyware وبرمجيات الإعلانات adware ومسجلات المفاتيح keyloggers.

البوتنت Botnets

يعتبر تحكم المهاجم بالحاسب البعيد من أهم أهداف البرمجيثات. يطلق على الحاسوب المصاب robot (bot) اسم الزومبي. يطلق على الشبكة المنطقية التي تجمع آلاف أو حتى مئات الآلاف من الحواسيب الزومبي التي يتحكم بها مهاجم ما اسم البوتنت. طبعاً لا يكون مستخدم الزومبي مدركاً لاشتراكه ضمن البوتنت.
يبين الجدول التالي بعض الهجمات الممكن شنها باستخدام شبكات البوتنت.

نوع الهجوم	الوصف
البريد غير المرغوب spamming	يمكن لشبكة بوتنت مؤلفة من آلاف الزومبي أن تسمح لمهاجم بإرسال كميات هائلة من البريد غير المرغوب أو للحصول على قوائم للعناوين البريدية الالكترونية.
نشر البرمجيثات	يمكن استخدام البوتنت في عملية نشر البرمجيثات وخلق زومبيات وبوتنت جديدة؛ يستطيع الزومبي تحميل وتنفيذ ملف مرسل من قبل المهاجم.
التلاعب بالتصويت الالكتروني على الخط	بما أن كل زومبي يمتلك عنوان IP خاص به الأمر الذي يعطيه مصداقية عند التصويت الالكتروني. يمكن التلاعب أيضاً بالألعاب على الخط بالطريقة نفسها.
حجب الخدمات	تستطيع البوتنت إغراق مخدم وب بآلاف الطلبات لدرجة لا يمكن له أن يجاوب الطلبات الشرعية.

تاريخياً، كان يجري التحكم بشبكات البوتنت عن طريق بروتوكول Internet Relay Chat (IRC) لكن حالياً يستخدم بروتوكول Hypertext Transport Protocol (HTTP). تمرير أوامر التحكم عبر HTTP يصعب اكتشافها أو حجبها. إضافةً إلى ذلك، فإن بروتوكول HTTP يجعل عملية التحكم والسيطرة Command and Control (C&C) أسهل وذلك عن طريق توجيه الزومبي للدخول إلى موقع يتبع للمهاجم أو تحت تصرفه. يُعرف المهاجم باسم راعي البوتنت botnet herder.
تعتبر شبكة البوتنت القاعدة المثالية للمهاجمين:

- تعمل الزومبي في الخلفية بدون أي دليل على وجودهم
- تسمح شبكة البوتنت بإخفاء مسار الراعي (المهاجم). أي أن أي تعقب رجعي Traceback يقود فقط إلى حواسب شبكة البوتنت.

- يمكن أن تبقى البوتنت فعالة لفترات تصل إلى عدة سنوات
- نمو عدد المستثمرين الدائمين على الخط يجعل قابلية الوصول إلى الزومبي متاحة بشكل دائم.

يوجد عدد كبير من شبكات البوتنت حالياً. تحوي إحدى الشبكات التي يتحكم بها راعي أوروبي مليون ونصف زومبي. يتوقع أحد الخبراء الأمنيين أنه بين 7 و 25 بالمئة من جميع الحواسيب الموجودين على الإنترنت تتبع لشبكة بوتنت ما.

برمجيات التجسس Spyware

برمجية التجسس هو مصطلح عام مستخدم لوصف البرمجية التي تتجسس على المستخدمين عن طريق جمع المعلومات عنهم بدون أذنهم الأمر الذي ينتهك خصوصيتهم. يتم تحقيق هذه البرمجيات بشكل يضعف تحكم المستخدم، مثل:

- استخدام موارد النظام بما يشمل على البرامج المنصبة على حواسبهم
- جمع واستخدام وتوزيع معلومات شخصية أو حساسة
- أي تغييرات جوهرية تؤثر على خبرة المستخدم أو خصوصيته أو أمن النظام

تقوم برمجيات التجسس بإحدى العمليات التالية: الإعلان أو جمع المعلومات الخاصة أو تغيير إعدادات الحاسوب. نذكر من التقانات التي تستخدمها برمجيات التجسس:

- برمجيات التحميل الآلي المستخدمة لتحميل وتنصيب البرامج دون أذن المستخدم
- تقانات التعقب السلبية التي تجمع المعلومات عن نشاطات المستخدم دون تنصيب أي برنامج
- برمجيات تعديل النظام
- برمجيات التعقب المستخدمة لمراقبة سلوك المستخدم أو جمع معلومات عنه

بالإضافة إلى انتهاك خصوصية المستخدم، يمكن لبرمجيات التجسس أن تؤثر سلباً على الحاسوب نفسه:

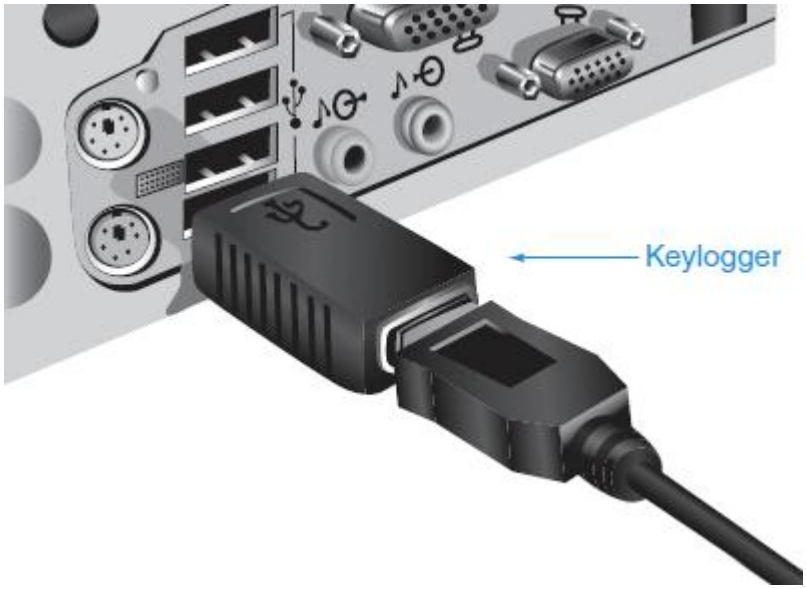
- أداء أخفض للحاسوب
- عدم استقرار النظام
- إضافة شريط أدوات أو قوائم جديدة على متصفح الإنترنت
- إضافة اختصارات جديدة
- اختطاف الصفحة الرئيسية
- زيادة عدد النوافذ الفجائية pop–ups خاصة الإعلانية

البرمجيات الإعلانية Adware

البرمجية الإعلانية هي عبارة عن برنامج لإيصال الإعلانات بطريقة غير متوقعة وغير مطلوبة من المستخدم. يمكن أن يصيب البرنامج الإعلاني الحاسوب عن طريق فيروس أو دودة أو طروادي. ما أن يتم تنصيب البرنامج الإعلاني حتى يبدأ بعرض شريط الإعلانات أو نوافذ الإعلانات الفجائية أو فتح نافذة وب جديدة ضمن المتصفح.

تقوم بعض البرمجيات بتعقب نشاطات المستخدمين على الإنترنت وإرسال تقرير عن هذه النشاطات إلى طرف ثالث بدون معرفة المستخدم. فمثلاً عندما يدخل مستخدم إلى موقع مختص ببيع السيارات فإن البرنامج الإعلاني Adware يصنف المستخدم على أنه مهتم بشراء سيارة جديدة. يمكن أن يباع هذا النوع من المعلومات إلى معلنو السيارات الذين يرسلون رسائل نظامية إلى المستخدم تعلن عن أنواع وأسعار سياراتهم أو يمكن أن يتصلوا بهم هاتفياً.

مسجلات المفاتيح Keyloggers



يلتقط مسجل المفاتيح أي ضغطة مفاتيح يقوم بها المستخدم على لوحة المفاتيح ثم يسجلها. يمكن للمهاجم أن يستفيد من هذه المعلومات أو أن يتم إرسالها إلى موقع بعيد. يبحث المهاجم عن الأنواع المفيدة من المعلومات ضمن النصوص الملتقطة مثل كلمات المرور وأرقام بطاقات الإئتمان والمعلومات الشخصية.

يمكن أن يكون مسجل المفاتيح برنامج أو جهاز صلب.

مسجلات المفاتيح البرمجية لا تستدعي الوصول الفيزيائي إلى الحاسوب وإنما يمكن تحميلها وتنصيبها عن طريق فيروس أو طروادي. تستطيع هذه البرمجيات إرسال النصوص الملتقطة إلى المهاجم بشكل دوري باستخدام الإنترنت. لا يمكن اكتشاف هذه البرامج بسهولة نظراً لمقدرتها على التخفي.

4.1. هجمات الهندسة الاجتماعية Social engineering attacks

لا نحتاج دائماً إلى التقانة لمهاجمة الأنظمة المعلوماتية. الهندسة الاجتماعية هي طريقة لجمع المعلومات المطلوبة لشن هجوم بالاعتماد على مواطن ضعف الأفراد. يمكن أن تتضمن هجمات الهندسة الاجتماعية على المقاربات النفسية أو الإجراءات الفيزيائية.

المقاربات النفسية

يعتمد العديد من هجمات الهندسة الاجتماعية على علم النفس الذي هو مقاربة عقلية وعاطفية عوضاً عن الفيزيائية. تعتمد الهندسة الاجتماعية في صميمها على تلاعب المهاجم الذكي بطبيعة الإنسان في سبيل إقناع الضحية بتزويد المعلومات أو القيام بفعل ما. تشمل الأساليب الأساسية في الإقناع على الإطراء والنفاق ingratiation والامتثال (أي شخص آخر يفعل نفس الشيء) والود. يحاول المهاجم إقناع الضحية بإمكانية الوثوق به.

بما أن جميع المقاربات النفسية تتطلب الاتصال من نوع شخص لشخص، فإن المهاجم يستخدم مجموعة متنوعة من التقنيات لاكتساب الثقة بدون التحرك بسرعة حتى لا يثير الشكوك.

تشمل المقاربات النفسية للهندسة الاجتماعية على التمثيل impersonation والتصيد phishing والبريد غير المرغوب spam والخدع hoaxes.

التمثيل

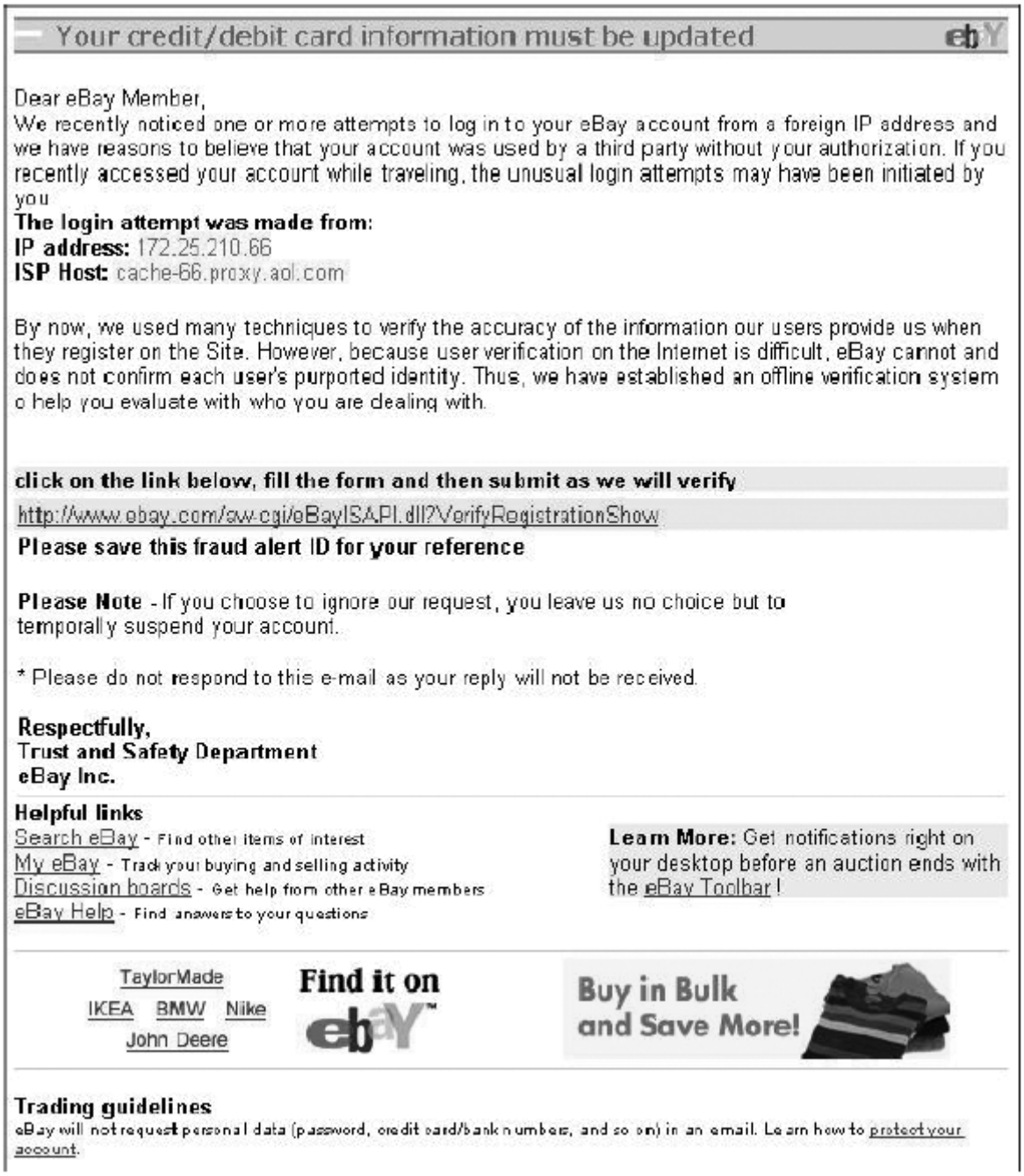
وفق الهندسة الاجتماعية يعني خلق شخصية خيالية ولعب دور هذا الشخص للضحية. كتمثيل دور مسؤول الدعم الفني الذي يتصل بالضحية ويدعي وجود مشكلة في الشبكة ومن ثم يطلب منه اسم المستخدم وكلمة المرور لإعادة تهيئة الحساب.

الأدوار المشهورة التي يتم تأديتها هي عامل الإصلاح أو الدعم الفني أو مدير النظام أو أي طرف ثالث موثوق أو موظف زميل. يمثل المهاجم عادةً دور شخص صاحب سلطة نظراً لخوف الضحية من عدم إجابة شخص من هذا النوع.

التصيد

من أكثر أشكال الهندسة الاجتماعية شهرةً. يجري التصيد عن طريق إرسال رسالة إلكترونية أو عرض إعلان على الوب يدعي كذباً كونه قادماً من شركة شرعية في محاولة لخداع المستخدم لكشف معلومات خاصة. يُطلب من المستخدم الجواب برسالة إلكترونية أو يتم توجيهه إلى أحد مواقع الوب حيث يتم الطلب منه تحديث معلوماته الشخصية مثل كلمات المرور أو رقم بطاقات الإئتمان أو أرقام حساباته المصرفية أو غيرها. يكون موقع الوب في هذه الحالة مزيف وهو معد لسرقة المعلومات التي يدخلها المستخدم.

يعود أحد أسباب نجاح عمليات التصيد إلى كون رسائل البريد الالكتروني الموجهة أو مواقع الوب تظهر كأنها شرعية. يظهر الشكل التالي موقع وب مستخدم للتصيد.


Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar!

TaylorMade
IKEA BMW Nike
John Deere
Find it on ebay
Buy in Bulk and Save More!

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account.

الشكل 2: رسالة التصيد

لاحظ أن الرسالة تحمل الشعار نفسه والألوان نفسها والعبارات نفسها المستخدمة عند الشركة الأصلية الأمر الذي يصعب عملية اكتشاف كونها مزيفة.

يوجد بعض الأشكال الأخرى للتصيد، نذكر منها:

- التزييف Pharming. بدلاً من الطلب من المستخدم ليزور موقع وب، التزييف يعيد توجيه المستخدم آلياً إلى الموقع المزيف. يمكن تحقيق هذا التوجيه عن طريق التسلل إلى مخدمات توجيه حركات المرور أو مخدمات الأسماء.

- التصيد الموجه Spear phishing. بينما يتطلب التصيد إرسال ملايين الرسائل العامة، فإن التصيد الموجه يهدف إلى مجموعة محددة من المستخدمين. في التصيد الموجه، تكون الرسالة مخصصة للمستقبلين عن طريق وضع الاسم وغيره من المعلومات الشخصية في سبيل جعل الرسالة تبدو شرعية أكثر.
- الحواتة Whaling. تعتبر الحواتة (صيد الحيتان) من أشكال التصيد الموجه. فبدلاً عن البحث عن الأسماك الصغيرة، الحواتة تبحث عن الأسماك الكبيرة؛ أي الأثرياء الذين لديهم أموالاً طائلة في حساباتهم المصرفية. في هذا النوع من التصيد، يمكن للمهاجم استثمار وقتاً أكبر لضبط رسائله بدقة كبيرة الأمر الذي يزيد فرص النجاح.
- التصيد بالهاتف Vishing. يجري هنا التصيد باستخدام الهاتف Voice phishing بدلاً عن البريد الالكتروني. فمثلاً، يقوم المهاجم بالاتصال بالضحية الذي يسمع رسالة مسجلة تزعم أنها قادمة من مصرف الضحية حيث تعلمه بأن حسابه المصرفي عاني من مشاكل تزوير أو أي عملية غير عادية. يُطلب من الضحية بعد ذلك الاتصال برقم محدد. بعد أن يتصل الضحية يسمع تعليمات آلية تطلب منه إدخال رقم البطاقة المصرفية أو رقم الحساب المصرفي أو أي معلومات أخرى على لوحة مفاتيح الهاتف.

الرسائل غير المرغوبة Spam

تزداد كمية الرسائل غير المرغوبة باضطراد. تؤثر هذه الرسائل على الإنتاجية إضافةً إلى كونها مصدراً أساسياً للمهاجمين لتوزيع الفيروسات ومسجلات المفاتيح والطروادیات وغيرها من البرمجيثات. من أشكال الرسائل غير المرغوبة spam يوجد الرسائل الفورية غير المرغوبة Instant Messaging (spim).

يعود السبب الرئيسي لإرسال كميات كبيرة من الرسائل إلى كونها عمليات مربحة. فهي لا تكلف المرسل spammer أي شيء فعلياً لإرسال ملايين الرسائل يومياً. فإذا استلموا نسبة ضئيلة من الأجوبة للمنتج موضوع الرسالة فإنهم يحصلون على ربح كبير. يجب هنا اعتبار النفقات التالية:

- عناوين البريد الالكتروني. يستخدم المرسلون spammers برمجيات خاصة لتوليد عناوين البريد الالكتروني التابعة لمزود خدمات أنترنت معروف. كما يمكن للمرسل أن يشتري قوائم بريدية جاهزة وصحيحة (سعر 10 مليون عنوان هو حوالي 100 دولار)
- التجهيزات ووصلات الإنترنت. يعتمد السبامر على حاسب محمول عادي ويستأجر غرفة في فندق مزود بوصلات إنترنت سريعة كمحطة لشن الهجمات. كما يمكن للمهاجم أن يستأجر زمن من مهاجم آخر (40 دولار بالساعة) لاستخدام شبكة مكونة من عدة آلاف الحواسب المصابة لشن الهجوم.

بفرض أن السبامر أرسل 6 مليون رسالة في يوم واحد لمنتج يباع بمبلغ 50 $ ويكلف فقط 5 $ وبفرض أن 0.001 من المستقبلين للرسالة اشتروا المنتج فإن السبامر يحقق ربحاً قدره 270.000 $.

بما أن مخدمات البريد الالكتروني باتت تستخدم مصفيات السبام spam filters التي تبحث عن كلمات محددة مثل Viagra أو Investments وتتعرف على هذه الرسائل، توجه السبامر إلى طريقة أخرى لإرسال الرسائل تعرف باسم image spam حيث يرسلون النصوص على شكل صور لتجاوز مصفيات النصوص. تحوي هذه

الرسائل نص عادي بلا أي معنى محدد لخداع مصفيات النصوص وذلك لأنه يجري استبعاد الرسائل التي تحوي صور بدون أي نص عادةً.

الخدع Hoaxes

يستطيع المهاجمون استخدام الخدع كمرحلة أولى من الهجوم. الخدعة هي تحذير خاطئ غالباً ما يكون مضمناً ضمن رسالة الكترونية تزعم كونها قادمة من مدير النظام المعلوماتي. تدعي الرسالة وجود فيروس ضار على الإنترنت وأنه على المستقبل حذف ملفات معينة أو تغيير الإعدادات الأمنية (إضافةً إلى توجيه الرسالة إلى الغير). تغيير الإعدادات يتيح للمهاجم اختراق الحاسب. أما حذف الملفات فيجعل الحاسب غير مستقر الأمر الذي يتطلب الاتصال برقم الهاتف الموجود ضمن الرسالة الخدعة hoax e-mail طلباً للمساعدة من المهاجم.

5.1. الإجراءات الفيزيائية

تستفيد هذه الهجمات من ردة فعل المستخدم الفيزيائية التي يمكن أن ينتج عنها أمناً أقل. أهم نوعين لهذه الهجمات هما الغوص في القمامة Dumpster Diving والتمرير Tailgating.

الغوص في القمامة

يتطلب الغوص في القمامة البحث ضمن حاويات القمامة لإيجاد معلومات يمكن أن تفيد في الهجوم. من المعلومات التي يمكن الحصول عليها باستخدام هذه الطريقة:

- المفكرات الشخصية التي تفيد في معرفة من هم خارج البلد في لحظة معينة
- بعض التجهيزات الحاسوبية زهيدة الثمن مثل ذواكر USB أو الأقراص الصلبة القديمة
- المذكرات التي تفيد المهاجم عند التمثيل
- المخططات التنظيمية التي تفيد في معرفة أصحاب القرار وأصحاب السلطة
- دليل الهاتف
- كتيبات السياسات الأمنية تفيد في معرفة مستوى السياسات الأمنية المطبقة في المؤسسة
- كتيبات أنظمة التشغيل

التمرير Tailgating

تستثمر الشركات مبالغ كبيرة لتجهيز الأبواب بأجهزة دخول متطورة تسمح فقط للأشخاص المسموح لهم بالدخول عن طريق استخدام البصمات أو بطاقات دخول وغيرها. تكمن المشكلة في هذا النوع من الأجهزة في أنها لا تستطيع التحكم بعدد الأشخاص الذين يدخلون عندما يسمح بالدخول أو يفتح الباب. أي عندما يسمح لموظف ما بالدخول فإنه يستطيع أن يدخل معه من يريد. يعرف هذا التصرف بالتمرير Tailgating.

2. تمارين عملية

1.2. منع الكتابة على محرك ذاكرة USB

بما أن البرمجيثات يمكن أن تنتشر عبر الحواسب عن طريق محركات ذاكرة USB، لذلك سنستخدم أداة للتحكم بسماحيات الكتابة على قرص فلاش نوع USB. ستحمل وتنصب أداة منع الكتابة على قرص فلاش USB.

1. Go to URL www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker.
2. Click download Thumbscrew
3. Open Thumbscrew.exe
4. Insert a USB flash drive
5. Make the USB flash drive write-protected (read-only)
6. Try to move a file to USB drive

2.2. مسح الحاسب ضد أدوات الجذور Rootkits

1. Download and install rootkitremover.exe from McCafe web site
2. Run rootkitremover.exe

3.2. استخدام IE SmartScreen filter

1. شغل Internet Explorer 9
2. شغل SmartSCree من Tools>Safety>Turn on SmartScreen Filter
3. أذهب إلى الموقع www.svuonline.org
4. أضغط Tools>Safety>Check this web site
5. ما هي نتيجة الاختبار المعادة؟

الفصل الثالث: الهجمات على التطبيقات والشبكات

Application and Network Attacks

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعرف ومناقشة الأنواع المختلفة لهجمات تطبيق الوب
- شرح آلية عمل هجمات إغراق الصوان Buffer Overflow
- تعرف أهم أنواع حجب الخدمة
- فهم هجمات الاعتراض والتسمم

بعد مناقشة البرمجيثات في الفصل السابق، سنتابع في هذا الفصل مناقشة التهديدات والثغرات الأمنية التي تتعرض لها بعض التطبيقات والشبكات.

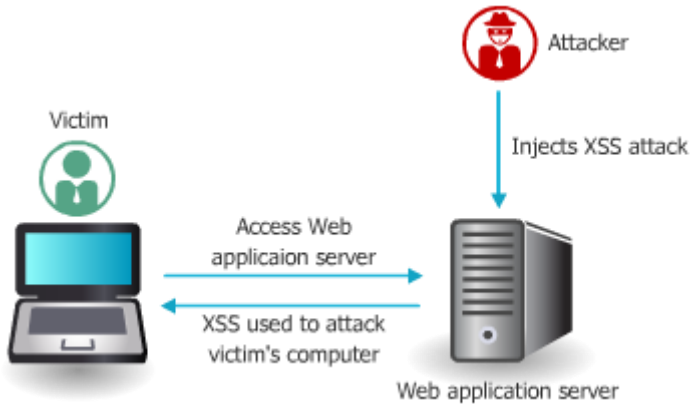
1. الهجمات على التطبيقات

نذكر، من أهم الهجمات التي تنمو بسرعة، الهجمات على التطبيقات. تعرف معظم هذه الهجمات وفق مصطلح هجمات اليوم صفر Zero-day attack أي أنها تستغل نقاط ضعف غير معروفة وليس للمستخدم أي وقت (صفر يوم) للتحضير أو للدفاع عن الهجوم. لعل الهجمات على تطبيق الوب والهجمات من طرف الزبون وإغراق الصوان من أشهر الهجمات على التطبيقات.

1.1. الهجمات على تطبيق الوب

بما أنه لا تجري تصفية محتويات طرود تطبيق HTTP ضمن أجهزة الحماية المستخدمة مثل جدران النار، يستخدم المهاجمون هذا البروتوكول للتركيز على عيوب بعض برمجيات تطبيقات الوب. تعتبر الأوامر النصية عبر المواقع Cross-site scripting وحقن SQL وحقن التحكمات/اجتياز الدليل من أهم هذه الهجمات.

Cross-site scripting (XSS) يقوم هنا المهاجم بحقن نص أوامر Script ضمن مخدم تطبيق الوب الذي سيوجه الهجمة إلى الزبون. يجري هنا استخدام المخدم كمنصة لشن الهجوم على بقية الحواسب الذين يدخلون إلى المخدم. يبين الشكل التالي هجوم XSS.



الشكل 1: هجوم XSS

عندما يزور الضحية موقع وب محقون، تُرسل التعليمات الخبيثة إلى متصفح الزبون وتنفذ عنده. بما أن متصفح الزبون غير قادر على التمييز بين الرمازات الصالحة وبين نصوص XSS فسوف ينفذ جميع الرمازات المستقبلة من موقع الوب مثل JavaScript و HTML و Adobe flash.

يتطلب تنفيذ هجوم XSS موقع وب بخاصتين: يقبل مدخلات المستثمر بدون التحقق منها ويستخدم هذه المدخلات كجواب غير مرمز من المستثمر.

بما أن هذه الهجمات مختصة بالتطبيقات بشكل عام فهي تخرج عن إطار هذا المقرر.

2.1.الهجمات من طرف الزبون

تهدف الهجمات من طرف الزبون إلى استغلال نقاط ضعف تطبيقات الزبون التي تتفاعل مع مخدم مخترق أو تعالج معطيات خبيثة. في هذه الحالة، يقوم الزبون بفتح اتصال مع مخدم الأمر الذي ينتج عنه الهجوم.
يُعتقد أن مجرد فتح برنامج الزبون وحتى وإن لم يقم بالاتصال ببرنامج التطبيق لا يعرضه للخطر. بيد أن هذا الاعتقاد غير صحيح لأن الزبون عادةً يدخل آلياً إلى مخدم نفاذ بعيد الأمر الذي يعرضه لخطر هجوم محتمل.
تشمل أهم الهجمات من طرف الزبون على التلاعب بالترويسات والكوكيز والمرفقات واختطاف الجلسة والإضافات الخبيثة.

التلاعب بالترويسة Header Manipulation

تعتبر ترويسة HTTP جزءاً من طرد HTTP وهي تهتم بخصائص متصفح الزبون ومخدم الوب. يجري نقل المعطيات كنتيجة رسالة طلب HTTP من قبل المتصفح متبوعاً برسالة جواب HTTP من قبل المخدم. يشمل حقل الترويسة على اسم الحقل متبوعاً بنقطتين ":" ومن ثم قيمة الحقل. يبين الجدول التالي بعض حقول HTTP وقيمها.

اسم حقل HTTP	المصدر	مثال	وصف
Referer	متصفح الوب	Referer: http://google.com	عنوان المواقع الذي قدم منه الطلب
Accept-language	متصفح الوب	Accept-Language: en-us, en;	اللغات المقبولة
Server	مخدم الوب	Server: Apache	نوع مخدم الوب
Set-Cookie	مخدم الوب	Set-cookie: UserID=Bob;Max-Age=1800; Version=1	إضافة كوكي إلى المتصفح

الجدول 1: بعض حقول ترويسة HTTP

يمكن هنا للمهاجم تغيير محتويات الترويسات القادمة من الزبون ليشن الهجوم. من الأمثلة على هجمات التلاعب بترويسة HTTP، نذكر:

- المحيل Referer. تستخدم بعض المواقع هذا الحقل للتأكد من كون الطلب قادم من موقع محدد. يستطيع هنا المهاجم تعديل هذا الحقل لتجاوز إجراء الحماية هذا.

- Accept-Language. تمرر بعض تطبيقات الوب هذه المعلومة مباشرةً إلى قاعدة المعطيات الأمر الذي يساعد في هجمات من نوع SQL injection.

الكوكيز والملفات المرفقة

لا يحتفظ مخدم الوب بأي معلومات عن حالة الزبون بعد تخديمه. فإذا طلب الزبون الغرض نفسه مرتين متتاليتين، يكون المخدم غير قادر على معرفة ذلك وسيعيد له الغرض المطلوب كل مرة. لذلك يعرف بروتوكول HTTP بأنه عديم الحالة Stateless protocol. لكن مخدم الوب، في بعض الحالات، يحتاج إلى التعرف على المستثمرين ومتابعتهم بغية توجيه المحتوى حسب المستثمر مثلاً. لذلك تقوم مخدمات HTTP باستخدام cookies. تسمح الكوكيز، حسب المعيار [RFC 6265]، للمواقع بمتابعة المستثمرين. كما أن معظم مواقع الإنترنت التجارية الحالية تستخدم الكوكيز.

تتألف تقنية الكوكيز من أربعة مكونات:

- وضع الكوكي ضمن سطر ترويسة رسالة الجواب
- وضع ترويسة الكوكي ضمن رسالة الطلب
- يحتفظ متصفح الإنترنت بالكوكي ويقوم بإدارتها
- يقوم مخدم الوب بإضافة مدخل ضمن قاعدة المعطيات خاصة بهذه الكوكي

عندما يجري انشاء الكوكي لدى متصفح الزبون، فقط الموقع الذي أنشأ الكوكي يحق له قراءتها.

يوجد عدة أنواع من الكوكيز:

- كوكي الطرف الأول First-party cookie. يخلقها موقع الوب الذي يشاهده المستثمر حالياً. عندما يزور المستثمر الموقع نفسه مرةً أخرى فإنه يرسل الكوكي للموقع.
- كوكي الطرف الثالث. تضع بعض المواقع كوكيز إضافية تكون موجهة لطرف ثالث مثل الذين يضعون إعلانات ضمن الموقع ويريدون تسجيل تفضيلات المستخدمين. يستخدم هذا النوع من الكوكيز لوضع الإعلانات المناسبة لكل مستخدم.
- كوكي الجلسة Session cookie. تخزن كوكي الجلسة ضمن RAM عوضاً عن القرص الصلب وتستمر حتى انتهاء زيارة الموقع. تنتهي صلاحية هذا النوع من الكوكي عندما يغادر المستخدم موقع الوب أو عندما لا يقوم المستخدم بأي نشاط خلال فترة من الزمن.
- الكوكي الآمنة Secure cookie. تستخدم عندما يزور المتصفح مخدماً يستخدم اتصالاً آمناً. تكون هنا الكوكي مشفرة بين المستخدم وبين المخدم.
- فلاش كوكي. لا يمكن حذف هذه الكوكي مثلها مثل بقية الكوكيز وتتميز بسعتها التي تتجاوز سعة الكوكي العادية.

يمكن أن تشكل الكوكيز خطراً أمنياً وخطراً آخر متعلق بالخصوصية. فيمكن سرقة كوكيز الطرف الأول ومن ثم انتحال شخصية المستخدم. بينما تفيد كوكيز الطرف الثالث في تعقب عادات المستخدم عند التصفح أو عند الشراء.

الملفات المرفقة Attachments مع البريد الإلكتروني، يمكن استغلالها لنشر الفيروسات والديدان والطرواديات وغيرها من البرمجيثات.

اختطاف الجلسة Session Hijacking

من الأهمية بمكان بالنسبة لمستخدم يزور تطبيق وب آمن مثل تطبيقات التجارة الإلكترونية التحقق منه بحيث نمنع أي مهاجم من التسلل إلى الجلسة القائمة بين المستخدم والموقع ومن ثم طلب غرض ما على حساب المستخدم الضحية. يدعى هذا النوع من التحقق علامة الجلسة Token Session الذي هو عبارة عن سلسلة محارف عشوائية تنسب للجلسة. يقوم المستخدم بإضافة علامة الجلسة إلى كل طلب لاحق إلى المخدم.

اختطاف الجلسة هو عبارة عن هجوم يحاول فيه المهاجم انتحال شخصية الضحية عن طريق استخدام علامة الجلسة التابعة له. يجري تحقيق هذا الهجوم عن طريق سرقة علامة الجلسة بالتنصت على حركة المرور بين الطرفين أو عن طريق سرقة الكوكي الخاص بعلامة الجلسة باستخدام XSS أو أي هجوم آخر يستطيع من خلاله المهاجم من معرفة ملف كوكي علامة الجلسة من حاسب المستخدم.

يوجد خيار آخر للمهاجم يتمثل في تخمين علامة الجلسة. يمكن أن يحدث هذا الأمر إذا استطاع المهاجم جمع عدة علامات جلسات وكانت خوارزمية توليد العلامات غير عشوائية تماماً.

الإضافات الخبيثة Malicious Add-ons

الإضافات هي برامج تزود وظائف إضافية لمتصفح الوب. تعرف أيضاً تحت اسم توسعات Extensions أو Plug-ins. يمكن أن تشكل بعض هذه الإضافات مثل MS ActiveX Control التي تملك نفاذ كامل على نظام تشغيل MS Windows تهديداً أمنياً للحاسوب.

هجمات إغراق الصوان Buffer Overflow

يمكن أن يحدث إغراق الصوان عندما يحاول إجراء ما تخزين معطيات ضمن ذاكرة RAM خارج حدود الصوان المسموحة بها. تغرق كمية المعطيات الإضافية أمكنة التخزين المجاورة وفي بعض الحالات يمكن أن يتوقف الحاسوب عن العمل. تجدر الإشارة هنا إلى أن هجمات إغراق الصوان قد تتسبب في اختراق الحاسوب أيضاً.

2. الهجمات الشبكية

يعتبر الهجوم على الشبكة من أولويات المهاجمين وذلك كون استغلال نقطة ضعف واحدة ضمن الشبكة يمكن أن يكشف مجموعة كبيرة من التجهيزات الموصولة إلى الشبكة للمهاجم. نذكر، من الهجمات على الشبكات، حجب الخدمة والاعتراض والتسميم والهجمات على حقوق المستثمرين.

1.2. حجب الخدمة Denial of Service (DoS)

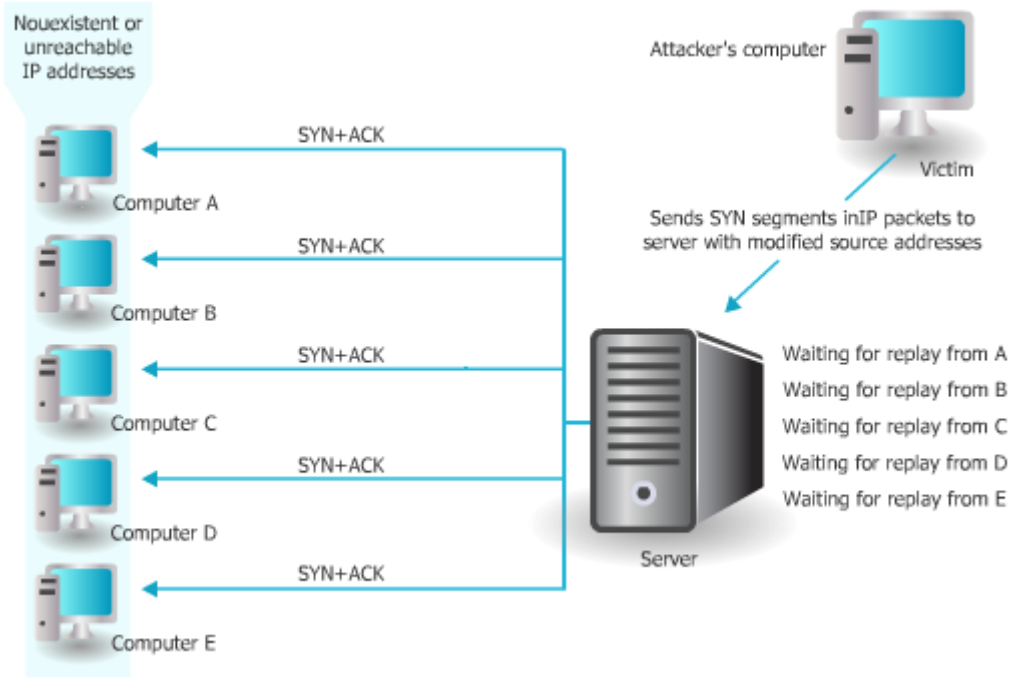
يحاول هجوم حجب الخدمة منع نظام ما من تأدية وظائفه الطبيعية. غالباً ما يقصد بحجب الخدمة المحاولة المتعمدة لمنع المستثمرين من النفاذ إلى النظام.

يوجد عدة أنواع من هجمات حجب الخدمة. فهجوم إغراق ping يستخدم بروتوكول رسائل التحكم بالأنترنت Internet Control Message Protocol (ICMP) لإغراق الضحية بالطرود. تُستخدم الأداة ping للتأكد من وجود اتصال على مستوى بروتوكول IP بين جهازين يستخدمان بروتوكولات TCP/IP. ترسل الأداة ping رسالة ICMP من نوع echo ويجاوب الطرف الثاني (المطلوب اختبار الاتصال معه) برسالة echo response. عند الهجوم باستخدام الأداة ping، يقوم المهاجم بإرسال عدد كبير من رسائل ping بسرعة كبيرة أيضاً لمخدم وب مثلاً الذي ينشغل بالرد على هذه الرسائل ولا يصبح لديه الموارد الكافية لمعالجة طلبات الاتصال الشرعية من الزبائن.

يوجد هجوم حجب خدمة آخر يعرف باسم هجوم الحوت Smurf attack حيث يحاول المهاجم خداع الأجهزة الأخرى لتجاوب على طلبات مزيفة. يقوم المهاجم بتعميم broadcast طلب ping على جميع الحواسيب الموجودة على الشبكة بعد تغيير عنوان IP المصدر لكل طلب جديد بعنوان لأحد المخدمات الموجودة أو الضحية (تدعى عملية انتحال عنوان IP للغير بغش العنوان Spoofed IP address). هنا يظهر أن المخدم المصدر يطلب من بقية الحواسب مجاوبته، الأمر الذي يمنعه من متابعة مهامه بالشكل المطلوب.

أما هجوم إغراق فتح الاتصال SYN flood فهو يستغل إجراءات تأسيس اتصال TCP. قبل أن يستطيع زبون الوب من طلب صفحة ما من موقع الوب أو أي تطبيق يعمل فوق TCP يجب تأسيس اتصال TCP بين الزبون والمخدم. تمر فترة تأسيس الاتصال عبر ثلاث مراحل: (1) يرسل الزبون مقطع (طرد) SYN يحوي على عنوانه وعلى عنوان المخدم ورقم البوابات المستخدمة للاتصال؛ (2) يجاوب المخدم بإرسال مقطع SYN+ACK لتأكيد موافقته على طلب فتح الاتصال ويخصص بعض الموارد لهذا الاتصال؛ (3) ينتظر المخدم فترة زمنية لاستلام مقطع ACK من الزبون للانتقال إلى مرحلة تبادل المعطيات.

في هجوم من نوع إغراق SYN على مخدم وب مثلاً يرسل المهاجم مقاطع SYN ضمن طرود IP إلى المخدم. في كل مقطع جديد، يغير المهاجم عنوان IP المصدر إلى عنوان غير موجود أو غير قابل للوصول إليه. بعد إرسال SYN+ACK لكل مقطع، ينتظر المخدم استلام ACK الذي لن يأتي. بعد فترة من استلام مقاطع SYN وتخصيص موارد لكل طلب تأسيس اتصال فإن موارد المخدم تستنفذ ويصبح غير قادر على تأسيس اتصال مع زبائن شرعيين. يوضح الشكل التالي مبدأ عمل هجوم إغراق SYN.



الشكل 2: هجوم إغراق SYN

يوجد، من أشكال هجمات حجب الخدمة، حجب الخدمة الموزع DDOS. يجري هنا، عوضاً عن شن الهجوم من خلال حاسب واحد، استخدام المئات أو الآلاف من حواسب الزومبي المشكلة لشبكة بوتنت لإغراق المخدم بالطلبات. هذا يصعّب عملية منع الطرود القادمة من مصدر الهجوم. أغلب هجمات حجب الخدمة الحالية تتبع أسلوب DDoS.

2.2. الاعتراض Interception

تصمم بعض الهجمات على أساس اعتراض اتصالات الشبكة. نذكر من أهم هجمات الاعتراض رجل المنتصف وهجمات الإعادة.

رجل المنتصف Man-in-the-Middle (MITM)

لنفرض السيناريو التالي: يأخذ عدنان علامة ضعيفة في مادة الرياضيات؛ يرسل المعلم رسالة إلى أهل عدنان لإخبارهم بهذه الحقيقة وبأنه يريد إجراء لقاء معهم للتباحث في أمر أبنهم؛ يعترض عدنان الرسالة ويكتب عوضاً عنها رسالة أخرى موجهة من المعلم إلى الأهل تفيد في تفوق ابنهم في مادة الرياضيات؛ يرسل عدنان أيضاً رسالة من الأهل إلى المعلم يعتذر فيها عن حضور اللقاء بعد تزوير توقيع ولي الأمر. يكون، حسب هذا السيناريو، عدنان قد نفذ هجوم رجل في المنتصف عن طريق اعتراض رسالة شرعية وتزوير رسالة جواب مزيفة للمرسل.

يمكن ارتكاب هذا النوع من الهجمات في الشبكات أيضاً. يظهر هنا أن حاسبين يتبادلان الرسائل فيما بينهما لكن في طبيعة الأمر فإن تبادل الرسائل يتم مع حاسب ثالث في المنتصف لا يدركان بوجوده بينهما كما هو موضح في الشكل التالي.

الشكل 3: هجوم رجل المنتصف

يمكن أن يكون هجوم رجل المنتصف فاعل active أو سلبي passive. في الهجم السلبي، يلتقط المهاجم المعطيات المنقولة ويسجلها ومن ثم يرسلها إلى الوجهة النظامية دون أن يكتشف أمرة. بينما في الهجوم الفاعل، يجري التقاط المعطيات وتعديلها قبل إرسالها إلى الوجهة.

الإعادة Replay

يشبه هجوم الإعادة هجوم رجل المنتصف السلبي. بينما يرسل المهاجم المعطيات مباشرةً إلى الوجهة، ففي حالة الإعادة يحتفظ المهاجم بنسخة من المعطيات قبل توجيهها إلى الوجهة. يجري استخدام هذه النسخة في زمن لاحق.

كمثال بسيط عن هجوم الإعادة، يمكن لرجل المنتصف التقاط معلومات تسجيل الدخول بين الحاسب والمخدم. ما أن تنتهي الجلسة، يحاول رجل المنتصف الدخول عن طريق إعادة إرسال معلومات التسجيل الملتقطة والمحفوظة عنده.

التسميم Poisoning

يوجد نوعين من الهجمات التي تحقن السم داخل شبكة ما لتسهيل اختراقها وهما تسميم ARP وتسميم DNS.

تسميم بروتوكول حل العناوين Address Resolution Protocol (ARP Poisoning). يعمل بروتوكول حل العناوين على المقابلة بين عنوان IP وعنوان فيزيائي أو MAC على شبكة محلية. أي بفرض أن حاسب يعرف عنوان IP لحاسب آخر ويريد التخاطب معه. يجب على المرسل معرفة العنوان الفيزيائي للحاسب الوجهة. هنا يأتي دور بروتوكول ARP الذي يسمح للحاسب المصدر بإرسال تعميم على الشبكة يضع فيه عنوانيه الفيزيائي و IP إضافةً إلى عنوان IP للحاسب الوجهة ويطلب العنوان الفيزيائي للوجهة. بما أن الإطار معمم على الشبكة فإن جميع الأجهزة ستشاهد الإطار ويقوم الحاسب الوجهة بعد التعرف على عنوان IP الخاص به بإرسال إطار جواب يحمل عنوانه الفيزيائي. تخزن هذه التقابلات ضمن ذاكرة خابية ويمكن الاستفادة منها لاحقاً دون إعادة طلب حل للعناوين. أضف إلى ذلك أن أي حاسب يشاهد طلب ARP request يقوم بحفظ العنوانين الفيزيائي والمنطقي (IP) للمرسل.

يستطيع المهاجم تعديل العنوان الفيزيائي الموجود ضمن الذاكرة الخابية بشكل يصبح العنوان المنطقي يؤشر إلى حاسب آخر. يعرف هذا الهجوم باسم تسميم ARP. يبين الجدول التالي محتويات الذاكرة الخابية قبل وبعد التعديل.

Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.2 & 00-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.3& 00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.4 & 00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

الشكل 4: هجوم تسميم ARP

يوجد مجموعة من الأدوات التي تتيح تسميم الذاكرة الخابية عن طريق إرسال رسائل ARP reply مزورة.
يمكن أن يفيد هذا النوع من الهجمات في سرقة المعلومات الموجهة إلى عنوان IP محدد أو منعه من الوصول إلى الإنترنت في حال استطاع المهاجم تغيير العنوان الفيزيائي للعبارة الافتراضية أو تحقيق رجل المنتصف أو حجب الخدمة عن طريق إعطاء حاسب الضحية عنوان فيزيائي غير موجود.
تسميم مخدم الأسماء Domain Name System (DNS poisoning). تلعب مخدمات الأسماء دوراً هاماً في عمل الإنترنت وذلك لأنها تسمح بالتحويل من الأسماء مثل www.hiast.edu.sy إلى عناوين IP مثل 91.144.9.40. بسبب أهمية هذه المخدمات باتت عرضة للهجمات. إذا استطاع المهاجم تغيير عنوان IP لمخدم ما بعنوان آخر مزيف باتت جميع الاتصالات الواردة إلى المخدم الضحية موجهة إلى حاسب المهاجم.
يمكن تنفيذ تغيير عناوين IP في موقعين: في ملف جدول المضيف المحلي Local host table أو مخدم نطاقات الأسماء الخارجي.
ما تزال TCP/IP تستخدم جدول المضيف المحلي الذي يوضح الملف التالي مثالاً عنه.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
```

```
#       ::1             localhost

127.0.0.1       genuine.microsoft.com
127.0.0.1       mpa.one.microsoft.com
127.0.0.1       sls.microsoft.com
204.15.20.80    www.facebook.com
```

يوجد هذا الملف في نظام Windows 7 وفق المسار التالي:

```
C:\Windows\System32\Drivers\etc\hosts
```

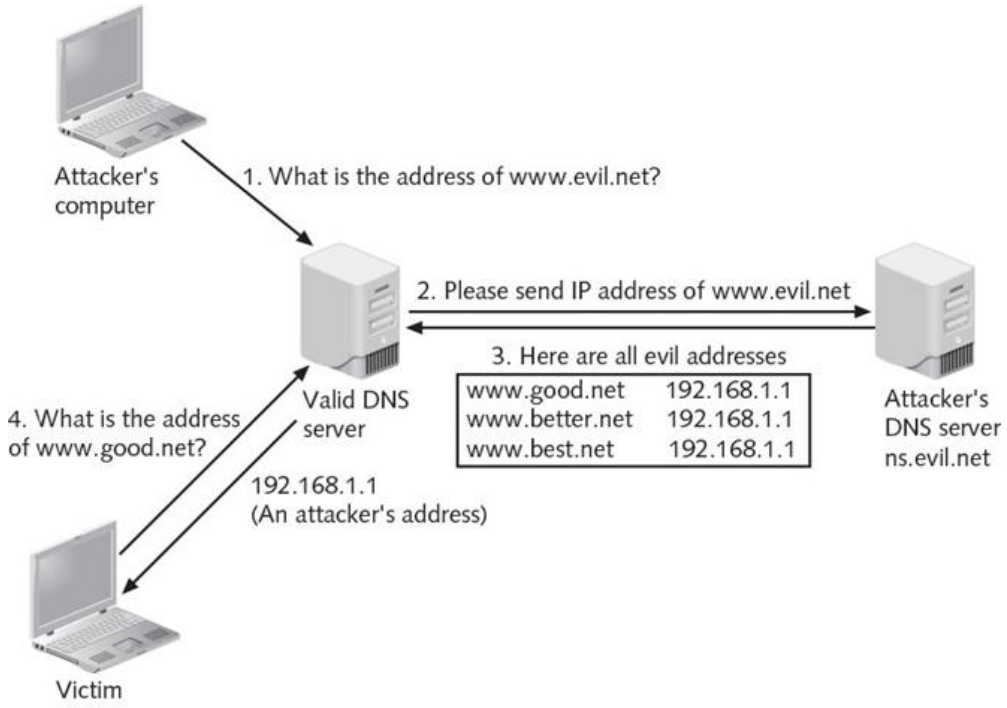
عندما يدخل المستثمر اسم نطاق ما فإن TCP/IP تبحث أولاً ضمن Local host لعلها تجد سجلاً موافقاً للاسم المطلوب. في حال عدم وجود سجل مناسب ضمن المضيف المحلي يجري الاتصال بمخدم نطاق الأسماء الخارجي. يحاول المهاجم تعديل المعلومات ضمن الملف المحلي عن طريق إضافة مدخلات توجه المستثمر إلى عناوين IP خاصة بمواقعهم بحيث إذا أدخل مثلاً المستثمر اسم الموقع www.paypal.com فإنه سيوجه إلى موقع المهاجم الذي يبدو شكله مطابقة للموقع الأصلي.

الموقع الثاني الذي يمكن مهاجمته هو مخدم نطاق الأسماء الخارجي. لا حاجة هنا للمهاجم لاختراق مخدم الأسماء نفسه إذ يمكن له استخدام مقاربة أسهل.

تجري عملية تسميم مخدم نطاق الأسماء من خلال مهاجم يملك اسم النطاق www.evil.net ومخدم الأسماء ns.evil.com على الشكل التالي:

1. يرسل المهاجم طلب إلى مخدم أسماء نظامي يطلب فيه حل الاسم www.evil.net.
2. بما أن مخدم الأسماء النظامي لا يعرف الجواب فإنه سيطلب من مخدم الأسماء ذو الصلاحية أي ns.evil.net الذي هو المخدم المسؤول عنه المهاجم.
3. يرسل مخدم الأسماء عنوان IP المطلوب إضافةً إلى جميع السجلات الموجودة لديه (نقل منطقة zone transfer) إلى مخدم الأسماء النظامي الذي يقبلهم.
4. سيقوم مخدم الأسماء النظامي من الآن فصاعداً بالإجابة على طلبات الحل باستخدام السجلات المزيفة التي استقبلها من المعاجم.

ينجح هذا الهجوم في حالة عدم تحقق مخدم الأسماء النظامي من السجلات القادمة من مخدم المهاجم على أنها قادمة من مخدم ذو صلاحية Authoritative.



الشكل 5: تسميم DNS

يمكن استخدام بروتوكول DNS أيضاً لشن هجوم حجب خدمة موزع على مخدم ما. يعرف هذا النوع من الهجمات باسم هجوم حجب خدمة موزع ومنعكس Distributed Reflection DoS attack. يستخدم المهاجم مخدمات DNS مفتوحة وعودية ويرسل لها طلبات كثيرة عن طريق شبكة بوتنت بغية حل عناوين بعد وضع عنوان المخدم الضحية كعنوان مصدر لطلبات الحل. تكون الطلبات معمولة بشكل تولد أجوبة طويلة (تعرف هذه الطريقة بالتضخيم Amplification أي سؤال صغير يولد جواب كبير). جميع رسائل الحل ستوجه إلى المخدم الضحية الذي سيتأثر أداؤه لدى استقبالها ومعالجتها.

الهجوم على حقوق النفاذ Access rights

حقوق النفاذ هي عبارة عن امتيازات تمنح للمستثمرين للنفاذ إلى الموارد البرمجية والعتادية. مثل منح شخص ما حقوق قراءة ملف بينما يمنح شخص آخر حقوق تعديله أو حذفه أيضاً. من أهم الهجمات التي تركز على حقوق النفاذ تصعيد الامتيازات Privilege Escalation والنفاذ المتعدي Transitive access.

- تصعيد الامتيازات. يستطيع نظام التشغيل أو بعض التطبيقات حصر امتيازات المستثمر في الوصول إلى وظائف محددة. تصعيد الامتيازات هي عملية استغلال ضعف برمجي للوصول إلى موارد ممنوعة عنه.

يوجد نوعان لتصعيد الامتيازات. الأول حينما يحاول مستثمر ممنوح امتيازات قليلة تصعيد امتيازاته. أما الثاني فهو عندما ينفذ مستثمر ذو امتيازات محدودة إلى وظائف باستخدام امتيازات مستثمر آخر.

- النفاذ المتعدي. يجري هنا استغلال الالتباس الذي يحصل عند عدم وضوح الصلاحيات الممنوحة لمجموعة مستثمرين ينفذون وظائف متكاملة على مجموعة من الملفات. أو بشكل آخر استغلال علاقة الثقة بين ثلاث أطراف.

3. تمارين عملية

1.3. خلق HTTP Header

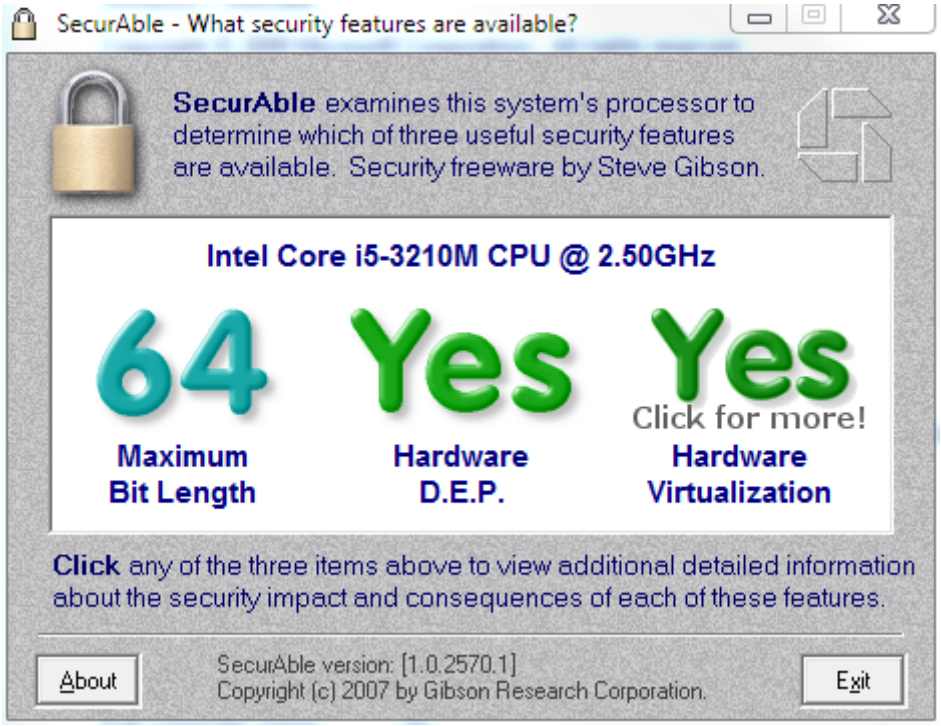
ستحاول في خذا التمرين تعديل حقل referer باستخدام أداة توليد ترويسة HTTP.

1. set your Web browser to go to www.httpdebugger.com/tools/View HttpHeaders.aspx to access the MadeForNet HTTP debugger
2. Under HTTP(S) URL: enter http://www.svuonline.org.
3. Under Content Type: enter text/html.
4. Under Referer: enter http://www.google.com
5. Click Submit. Note that the Referer field is changed.
6. Close all windows.

2.3. ضبط Windows لمنع تنفيذ المعطيات Data Execution Prevention (DEP)

يهدف هذا التمرين إلى أعداد برنامج منع تنفيذ المعطيات الذي يمنع المهاجم من شن هجمات إغراق الصوان أو تنفيذ أي برمجية خبيثة وذلك عن طريق تحديد أجزاء الذاكرة التي تحوي فقط المعطيات وليس رمازات تنفيذية.

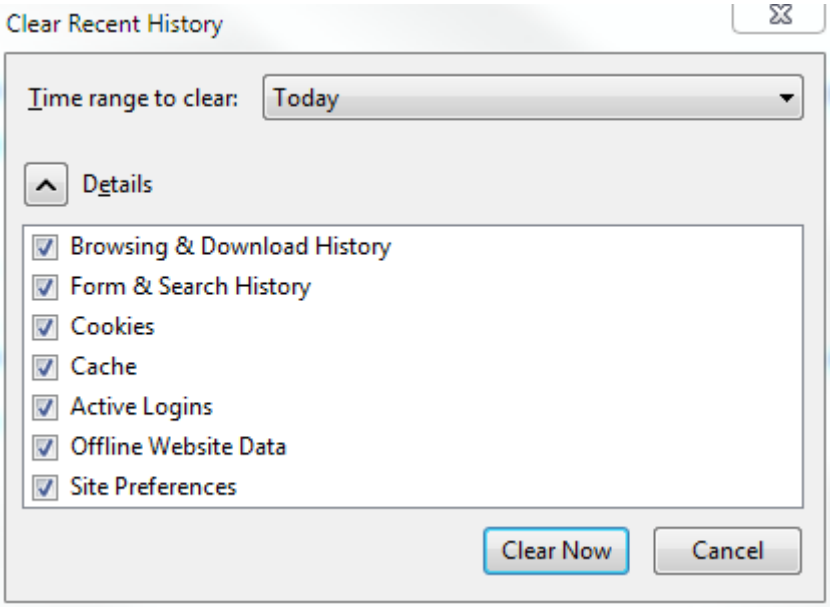
1. Use your Web browser to go to www.grc.com/securable
2. Click Download now and follow the default settings to install the application on your computer
3. Double-click SecurAble to launch the program, as shown in next Figure
4. If it reports that Hardware D.E.P. is “No,” then that computer’s processor does not support NX
5. Checking the DEP settings in Microsoft Windows 7
6. Click Start and Control Panel
7. Click System => system protection => Advanced Tab => performance setting
8. Click the Data Execution Prevention tab
9. Click "Turn on DEP for all programs and services except those I select:"
10. Click OK
11. Restart your computer



الشكل 6: نتائج برنامج Securable

3.3. ضبط الإعدادات الأمنية والخصوصية ضمن Firefox

1. Start Firefox
2. Click Options
3. Click Privacy
4. Click Clear your recent history
5. Select Time range to clear and what you are going to clear
6. Click clear now
7. Click remove individual cookies
8. Double-click on a cookie to show details and then click Remove selected



الشكل 7: Clear recent history

الفصل الرابع: تقدير الضعف وتخفيف المخاطر
Vulnerability assessment and risk mitigation

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعرف مفهوم تقييم الضعف وشرح سبب أهميته
- تعرف تقنيات وأدوات تقييم الضعف
- شرح الفرق بين مسح نقاط الضعف واختبار الاختراق
- تعرف تقنيات تخفيف أثر الهجمات أو ردعها

قلة من الشركات هي التي تتساءل عن مقدار ضعف الأنظمة الأمنية المعلوماتية التي تمتلكها. يتولد غالباً شعور زائف بالأمن بعد شراء تجهيزات أمنية غالية وتنصيب أحدث البرمجيات. تتمثل المشكلة الحقيقية في كون العديد من الشركات لا تشعر بالهجمات إلى في وقت متأخر يمكن أن يصل لعدة أسابيع وهناك جزءاً آخر لا يشعر بتاتاً بالهجمات.

الحقيقة المعروفة هي أن جميع الأنظمة الحاسوبية والمعلومات المحتواة ضمنها هي عرضة للهجمات. يجمع جميع خبراء الأمن المعلوماتي على أن الأمر ليس متعلق بهل سيتم التسلل عبر المواقع الدفاعية؟ وإنما متعلق **بمتى؟**.

بمعنىً آخر، يجب على كل مؤسسة التفكير بأماكن ضعف أنظمتها المعلوماتية وتقييم الطرق التي يمكن أن يتبعها المهاجم لاختراق الدفاعات الموضوعة حول هذه الأنظمة وتحديد الخطوات الاستباقية للدفاع ضد المهاجمين.

1. تقييم الضعف

تعتبر المعلومات من أهم الأشياء الثمينة التي تمتلكها أي مؤسسة. تتمثل الخطوة الأولى في حماية المعلومات في تقييم أماكن ضعف المعلومات. يمكن استخدام أدوات وتقنيات متنوعة لتقييم مستوى الضعف الموجود.

1.1. ما هو تقدير الضعف؟

تقدير الضعف هو تقييم منظم ومنهجي لمقدار تعرض الأصول للمهاجمين أو للقوى الطبيعية أو أي مكون آخر يمكن أن يكون مؤذياً. تقدير الضعف هو محاولة للتعرف على ما يجب حمايته (التعرف على الأصول) وما هي الضغوطات التي تتعرض لها (تقييم التهديدات) وما هي قابلية تعرض الحماية الحالية (تقييم الضعف) وما هي الأضرار التي يمكن أن تلحق نتيجة التهديدات (تقدير الأخطار) وماذا يمكن عمله (تخفيف أثر الأخطار).

التعرف على الأصول Asset Identification

تعرف الأصول (جمع أصل) بأنها أي شيء ذي قيمة تمتلكه شركة أو مؤسسة، بينما يعرف التعرف على الأصول بأنه عملية جرد هذه الأشياء. تمتلك أي مؤسسة أشكال مختلفة من الأصول. أهم شكلين هما الأشخاص (موظفين وزبائن وشركاء ومتعاقدين وبائعين) والأصول الفيزيائية (أبنية وسيارات وأجهزة غير حاسوبية). الآن، أصبحت عناصر تقانات المعلومات أصول رئيسية. تشمل هذه الأصول على المعطيات (جميع المعلومات المستخدمة والمتراسلة) والعتاديات (حواسب مكتبية ومخدمات وأجهزة شبكية ووصلات اتصال) والبرمجيات (برامج تطبيقية وأنظمة تشغيل وبرمجيات حماية). تتمثل الخطوة الأولى المصيرية في إنشاء جرد بالأصول المعلوماتية. بعد جرد الأصول، من الأهمية بمكان تحديد قيمة نسبية لكل مادة. لتحديد قيمة المادة، يمكن أن نلجأ إلى عوامل مثل مدى أهمية الأصل لتحقيق أهداف المؤسسة وما هي الإيرادات التي يولدها وما هي صعوبة تبديله وما هو انعكاس فقدان هذا الشيء على المؤسسة؟ بعض المؤسسات تستخدم قيم رقمية من "1" كأقل قيمة إلى "5" كأعلى قيمة وتنسبها للأصول. على سبيل المثال، يمكن إعطاء مخدم تطبيقات وب الذي يستقبل ويعالج الأوامر على الخط القيمة "5" وذلك لأن أساس عمل الشركة معتمد عليه. بينما يمكن إعطاء قيمة "2" لحاسب مكتبي يستخدمه موظف ما لأن فقدان هذا الحاسب لا يؤثر على العمل اليومي للشركة ولا يشكل تهديد أمني جدي.

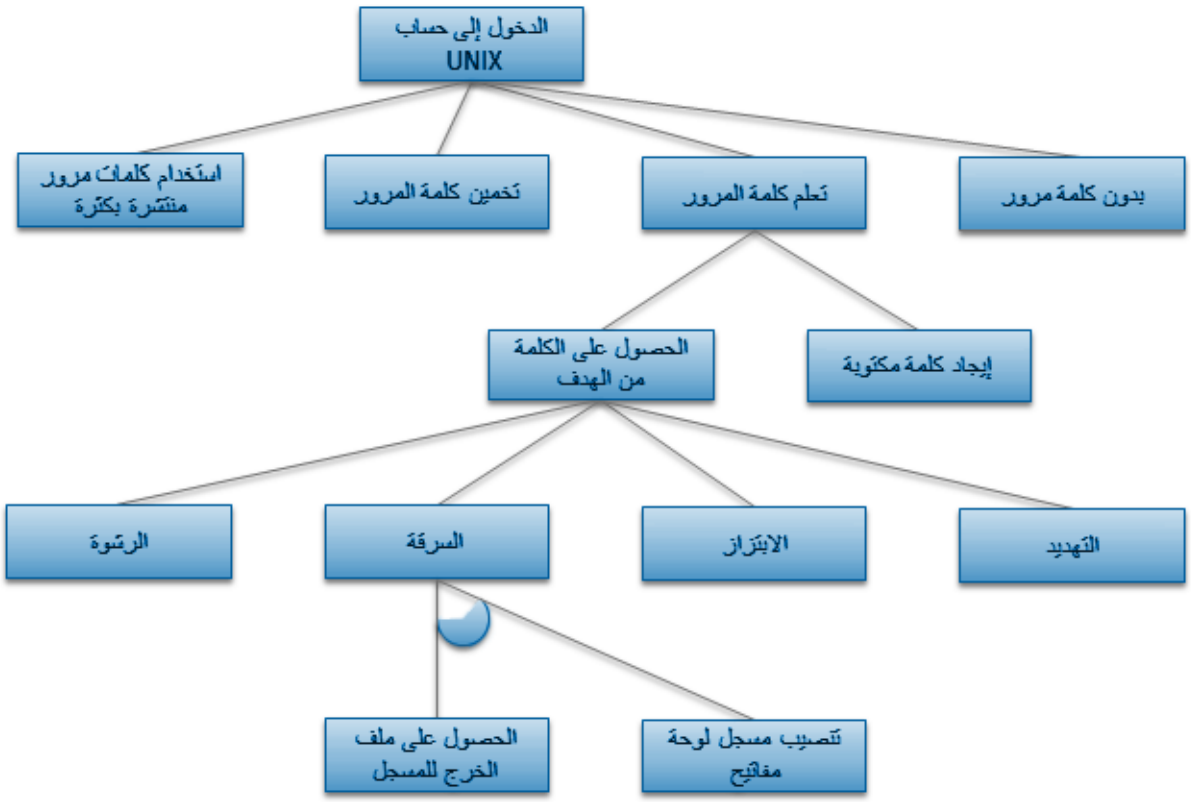
تقييم التهديدات Threat evaluation

بعد عملية جرد الأصول، يجب تحديد التهديدات المحتملة على الأصول والقادمة من عملاء التهديدات (وهم أي شخص أو شيء قادر على تنفيذ تهديد على الأصل). يوضح الجدول التالي بعض عملاء التهديدات الشائعين.

صنف التهديد	مثال
كوارث طبيعية	تخريب المعطيات عن طريق حريق أو فيضان أو هزة أرضية
انتهاك حقوق الملكية الفكرية	قرصنة برمجية أو الاعتداء على حقوق التأليف والنشر
التجسس	جاسوس يسرق الجدول الزمني للإنتاج
الابتزاز	اعتراض موظف البريد واعتراض الرسائل
الأعطال العتادية والأخطاء	توقيف جدار النار لجميع حركات مرور الشبكة
الأخطاء البشرية	موظف يفقد حاسبه المحمول في موقف السيارات
التخريب أو التدمير	مهاجم يزرع دودة تحذف جميع الملفات
مهاجمة البرمجيات	اختراق البرمجيات أو العتاديات عن طريق فيروس أو دودة أو حجب الخدمة عنها
الأعطال البرمجية والأخطاء	وجود علة ما تمنع البرنامج من العمل بشكل سليم
القدم التقني	برنامج لا يعمل ضمن نظام تشغيل بإصدار حديث
السرقة	سرقة حاسب مكتبي من غرفة غير مقفولة
انقطاع الخدمات	قطع التيار الكهربائي

الجدول 1: وكلاء التهديد الشائعون

قد يكون تحديد التهديدات التي يمكن أن تشكل مخاطراً على الأصول إجراءً معقداً. تعرف إحدى المقاربات لتحقيق هذه المهمة تحت اسم نمذجة التهديد threat modeling. تهدف نمذجة التهديد إلى فهم من هم المهاجمون ولماذا يهاجمون وما نوع الهجوم المزمع تنفيذه بشكل أفضل. باستخدام نمذجة التهديد، يجري بناء سيناريوهات لأنماط التهديدات التي يمكن للأصول أن تواجهها. أحد أهم الأدوات المستخدمة في نمذجة التهديدات هي بناء شجرة الهجوم. تزود شجرة الهجوم صورة مرئية للهجمات التي يمكن أن تحدث لأصل ما. بعد رسمها كبنية شجرة مقلوبة، تظهر شجرة الهجوم هدف الهجوم ونمطه والتقنيات المستخدمة في الهجوم.
يبين الشكل التالي شجرة الهجوم المتعلقة بكسر كلمة مرور حساب يونيكس.



الشكل 1: شجرة الهجوم لسرقة كلمة مرور حساب يونيكس

تقييم الضعف Vulnerability appraisal

بعد جرد الأصول وتحديد التهديدات يمكن طرح سؤال من نوع "ما هي نقاط الضعف الحالية التي يمكن أن تعرض الأصول لهذه التهديدات؟" الذي يعرف باسم تقييم الضعف. تأخذ هذه العملية لقطة عن الأمن الحالي للمؤسسة.

ليست عملية كشف نقاط ضعف أصل ما سهلة كما تبدو. يجب هنا اختبار كل أصل من خلال كل تهديد. كما يمكن لتهديد واحد أن يكشف عدة ثغرات أو نقاط ضعف. فمثلاً، إذا اعتبرنا حالة الخطأ البشري في إعداد جهاز شبكي، فيمكن لنقاط الضعف أن تكون:

- عدم إعداد البرامج الثابتة firmware بشكل سليم مما يمنع المستثمرين من النفاذ إلى الجهاز.
- الإعداد الخاطئ يمنع الجهاز من العمل بشكل سليم.
- يمكن أن يمنح مدير الشبكة صلاحيات المدير لمستثمر غير مصرح له.

تقدير المخاطر Risk Assessment

يتطلب تقدير المخاطر تحديد الأضرار التي يمكن أن تحدث نتيجة هجوم ما ودرجة احتمالية كون نقطة ضعف هي من المخاطر على المؤسسة.

تحديد الأضرار يتعلق بشكل أساسي بنوع الهجوم الممكن حدوثه. اعتماداً على نقاط الضعف التي تعرفنا عليها ضمن مرحلة تقييم الضعف يمكن تحليل تأثير الهجوم. لا تطرح جميع نقاط الضعف مخاطر شديدة. تتمثل إحدى الطرق في تحديد شدة المخاطر في قياس تأثير نقطة الضعف فيما لو تم استغلالها. يبين الجدول التالي مثالاً عن قياس نقاط الضعف.

التأثير	الوصف	مثال
لا تأثير No impact	لا تؤثر نقطة الضعف هذه على المؤسسة	سرقة فأرة مرتبطة بحاسب مكتبي ضمن المؤسسة
تأثير طفيف Small impact	نقاط الضعف ذات التأثير الطفيف يمكن أن تنتج إزعاجاً محدوداً زمنياً يحل عادةً بتغيير إجرائي	تعطل نوع محدد من الأقراص الصلبة يتطلب تأمين أقراص صلبة احتياط واختبارها دورياً
تأثير كبير Significant impact	نقطة ضعف يمكن أن ينتج عنها فقدان الإنتاجية بسبب التوقف عن العمل أو نفقات مالية للتخفيف من حدتها	يمكن تصنيف حقن برمجيثة ضمن الشبكة كنقطة ضعف ذات تأثير كبير
تأثير رئيسي Major impact	لها تأثير كبير وسلبي على الإيرادات	سرقة معلومات متعلقة بآخر أبحاث الإنتاج والتطوير من خلال باب خلفي
تأثير كارثي Catastrophic impact	يمكن أن توقف المؤسسة عن العمل أو تؤثر في إمكانية تأدية عملها تأثيراً كبيراً	إعصار يدمر فرع للمؤسسة وجميع معطياتها

الجدول 2: مقياس تأثير الضعف

يمكننا بعد ذلك تحديد الخسارة المادية جراء الهجوم والتي يمكن أن تفيد أيضاً في تحديد مدى تأثير الضعف. يوجد صيغتين لحساب الخسارة المتوقعة جراء المخاطر. توقع الخسارة الوحيد Single Loss Expectancy (SLE) التي هي عبارة عن قيمة الخسارة المالية المتوقعة كل مرة يقع الخطر. نحسب SLE عن طريق حساب جداء قيمة الأصل AV مع عامل التعرض Exposure Factor (EF) الذي هو نسبة من قيمة الأصل التي ستتضرر نتيجة المخاطر.

$$SLE = AV * EF$$

على سبيل المثال، بفرض أنه لدينا بناء شركة ما قيمته 800,000,000 ل.س، 40% ستتضرر نتيجة مخاطر زلزال. يكون توقع الخسارة الوحيد هو:

$$SLE = 800.000.000 * 0.40 = 32,000,000$$

أما توقع الخسارة السنوي Annualize Loss Expectancy (ALE) فهو الخسارة المادية المتوقعة جراء وقوع مخاطر ما على أصل خلال سنة واحدة. وهو جداء توقع الخسارة الوحيد بنسبة الحدوث السنوية Annualized Rate of Occurrence (ARO) الذي هو نسبة وقوع المخاطر خلال سنة واحدة.

$$ALE = SLE * ARO$$

فإذا توقعت شركة التأمين وقوع زلزال واحد خلال 200 سنة فإن ARO = 0,005 فتكون :

$$ALE= 32,000,000 * 0,005 = 160,000$$

الخطوة التالية هي تخمين احتمالية وقوع المخاطر المتعلق بنقطة الضعف. تستعمل بعض المؤسسات معلومات تاريخية ومشاهدات حالية لإنشاء نظام ترتيب. يجري هنا ترتيب الضعف على مقياس من 1 إلى 10 حيث القيمة 10 تدل على الاحتمال الكبير بينما تدل القيمة 1 على كون الاحتمال بعيد.

تخفيف المخاطر Risk mitigation

ما أن يتم تحديد المخاطر وترتيبها يجب علينا في الخطة النهائية تحديد ماذا سنفعل إزاء المخاطر. إن استبعاد المخاطر نهائياً أمراً غير ممكن تحقيقه عملياً أو يمكن أن يكون مكلفاً مادياً أو بشرياً. فيجب علينا افتراض بعض درجات المخاطر. يجب أن لا تطرح المؤسسة سؤالاً من نوع "كيف يجب علينا استبعاد جميع المخاطر؟" وإنما يجب على السؤال أن يكون من الشكل "ما هي كمية المخاطر المقبولة التي نستطيع أن نتسامح معها؟" تملك كل مؤسسة ثلاثة خيارات عند التصدي لمخاطر ما.

أولاً، يمكن أن تسعى المؤسسة لتقليل المخاطر Diminish the risk. أي اتخاذ خطوات استباقية لخفض احتمال وقوع الأضرار أو خفض خطورة الأضرار. مثلاً، يمكن أن تسعى مؤسسة ما لاعتماد عتاديات آمنة لتقليل احتمال اختراق مهاجم للشبكة.

ثانياً، تتمثل المقاربة الثانية في نقل المخاطر Transfer the risk عن طريق جعل طرف آخر مسؤول عن المخاطر. مثال، التعاقد مع طرف آخر ذو إمكانيات أكبر لتزويد الخدمة أو المنتج. تعرف هذه العملية بالتعهيد الخارجي outsourcing. فيمكن هنا تعهيد خدمات الوب إلى طرف ثالث يكون مسؤولاً عن انشاء وإدارة وتأمين وحماية موقع الوب. يمكننا هنا اعتبار التأمين من أنواع نقل المخاطر أيضاً.

ثالثاً، قبول المخاطر Accept the risk. في هذه الحالة لا نفعل شيئاً ونترك كل شيء كما هو. مثال على هذه المقاربة، شركة توزع حواسب محمولة على موظفيها بغية تحسين الإنتاجية. يمكن أن يستغل موظف هذه المبادرة

لنسخ معطيات الشركة الهامة ونقلها إلى شركة منافسة. في هذه الحالة، يمكن للشركة أن تتحمل مخاطر توزيع الحواسب المحمولة بدون أن تجازف بتقليل الإنتاجية جراء سحبها من الموظفين.

نلخص في الجدول التالي خطوات إدارة المخاطر.

عملية التعرف على المخاطر	الخطوة
التعرف على الأصول	جرد الأصول تحديد القيمة النسبية لكل أصل
التعرف على التهديدات	تصنيف التهديدات
تقييم الضعف	تعيين نقاط الضعف ضمن الأصول استخدام أدوات تقدير الضعف
تقدير المخاطر	تقدير تأثير الضعف على المؤسسة حساب توقع الخسارة تقدير احتمال وقوع خطر الضعف
تخفيف المخاطر	إقرار آلية العمل مع المخاطر: تقليل أو نقل أو قبول

الجدول 3: خطوات التعرف على المخاطر

2. تقنيات التقدير Assessment Techniques

يمكن استخدام مجموعة متنوعة من التقنيات لتقدير الضعف. تشمل هذه التقنيات على تبليغات خط الأساس Baseline reporting والتقنيات المرتبطة بتطوير البرمجيات.

تبليغات خط الأساس من منظور أمن المعلومات هي عبارة عن لائحة مرجعية عن الأنظمة التي يجب تقييمها وتدقيقها أمنياً. يلخص خط الأساس الاعتبارات الأمنية الأساسية لنظام ويشكل نقطة الانطلاق باتجاه أمن أكثر صلابة.

تبليغات خط الأساس هي عبارة عن مقارنة الحالة الحالية للنظام مع خط الأساس. يجب ملاحظة أي اختلاف ومعالجته بشكل سليم.

تطوير البرمجيات. يجب هنا الاهتمام بالأمور الأمنية أثناء تطوير البرمجيات وليس بعد استثمارها.

3. أدوات التقدير

يوجد مجموعة متنوعة من الأدوات التي تقوم بتقدير الضعف. من بين هذه الأدوات ما يسمح بمسح البوابات أو تحليل البروتوكولات أو مسح الضعف ومصايد honeypots و honeynets.

1.3. اكتشاف المضيفين Host Discovery

تتمثل الخطوة الأولى في التعرف على شبكة ما Network reconnaissance في تخفيض نطاق عناوين IP إلى قائمة بالمضيفين الفعالين أو الهامين. يجب أولاً معرفة نطاق عناوين IP التي تستخدمها المؤسسة ومن ثم مسح هذا النطاق باستخدام أي أداة موجودة لمعرفة العناوين الفعالة. معرفة نطاق العناوين المخصص لمؤسسة ما يجري عن طريق استخدام الأدوات nslookup أو dig والتي تسمح بالاستفسار من مخدم أسماء.

أسهل طريقة لاكتشاف عنوان مضيف هي باستخدام أمر ping (ICMP echo and echo reply) وانتظار الجواب. لكن للأسف مديرو الشبكات يحجبون حالياً خدمة الإجابة على طلب Ping. كحل بديل يمكن استخدام TCP SYN Ping أو TCP ACK ping الذي يحاول تأسيس اتصال مع مضيف ما على بوابة محددة أو إرسال إقرار ACK لاتصال غير موجود. مجرد رد الطرف الآخر برسالة من أي نوع تعني أنه موجود.

2.3. ماسحي البوابات Port scanners

تستخدم الإنترنت عناوين IP للوصول إلى الحاسب أو المخدم الوجهة ومن ثم تستخدم أرقام البوابات للوصول إلى البرنامج التطبيقي أو الإجرائية المسؤولة عن تطبيق ما. يتكون رقم البوابة من 16 بت أي أن قيمته تكون محصورة بين 1 و 65,535. تم تخصيص أرقام البوابات من 1 إلى 1023 للبروتوكولات المعروفة Well-known مثل بروتوكول HTTP وبروتوكول SMTP.

يوضح الجدول التالي بعض البروتوكولات المعروفة وأرقام البوابات المخصصة لها.

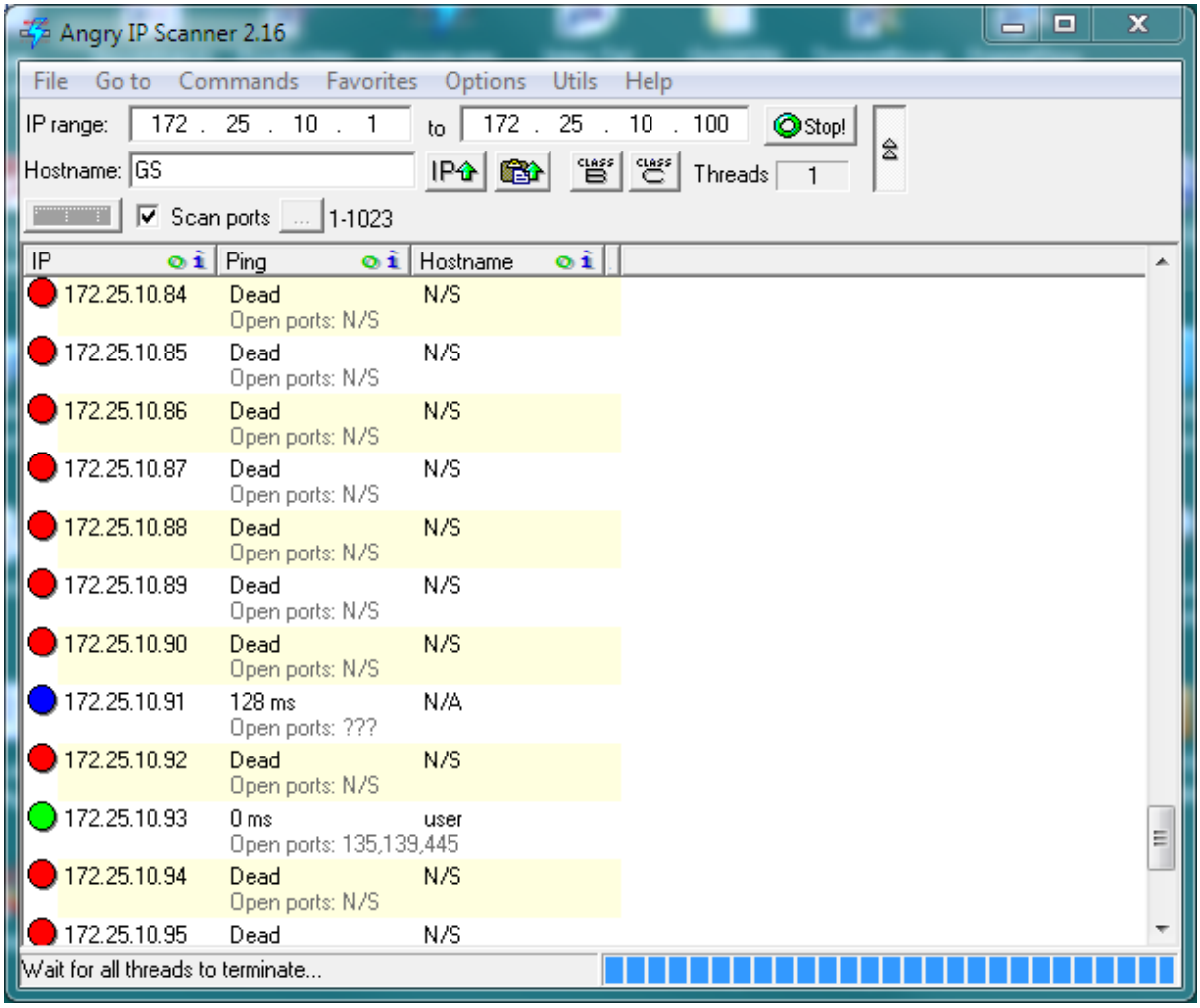
Protocol	Port number
File Transfer Protocol (FTP)	20 (data) and 21 (Control)
Secure Shell (SSH), Secure Shell Transfer Protocol (SFTP), Secure Copy(SCP)	22
Telnet	23
Trivial File Transfer Protocol (TFTP)	69
HyperText Transfer Protocol (HTTP)	80
NetBIOS	139
HyperText Transfer Protocol Secure (HTTPS)	443
FTP Secure (FTPS)	989 (data) and 990 (Control)

الجدول 4: البوابات الافتراضية لبعض التطبيقات الشبكية المشهورة

بما أن البوابة ترتبط بخدمة ما، فإذا استطاع المهاجم معرفة كون بوابة ما مفتوحة فإنه سيعرف ما هي الخدمة المتاحة ومن ثم يوجه هجومه إلى هذه الخدمة. عندما تريد مؤسسة ما أن تقوم بتقدير الضعف فإنها تستخدم برمجيات مسح البوابات لمعرفة حالة كل بوابة. يوجد ثلاث حالات للبوابات:

- مفتوحة Open. هذا يعني أنه يوجد تطبيق مرتبط بهذه البوابة وهو يتنصت عليها بغية الرد على الطلبات. تقوم طبقة النقل (TCP أو UDP) المثبتة ضمن نظام التشغيل بتوصيل الطرود الواصلة عبر هذه البوابات إلى التطبيقات المرتبطة معها كما تقبل طلبات تأسيس الاتصال معها.
- مغلقة Closed. لا يوجد تطبيق مرتبط أو يتنصت على هذه البوابة. يعيد نظام التشغيل جواباً من نوع "لا يوجد خدمة على هذه البوابة" ولا تسمح بتأسيس أي اتصال مع هذه البوابة.
- محجوبة Blocked. هذا يعني أن نظام التشغيل لن يرد على أي طلب بخصوص هذه البوابة.

يوجد العديد من الأدوات التي تمكن مسح البوابات، يوضح الشكل التالي لقطة من الأداة Angry IP Scanner.



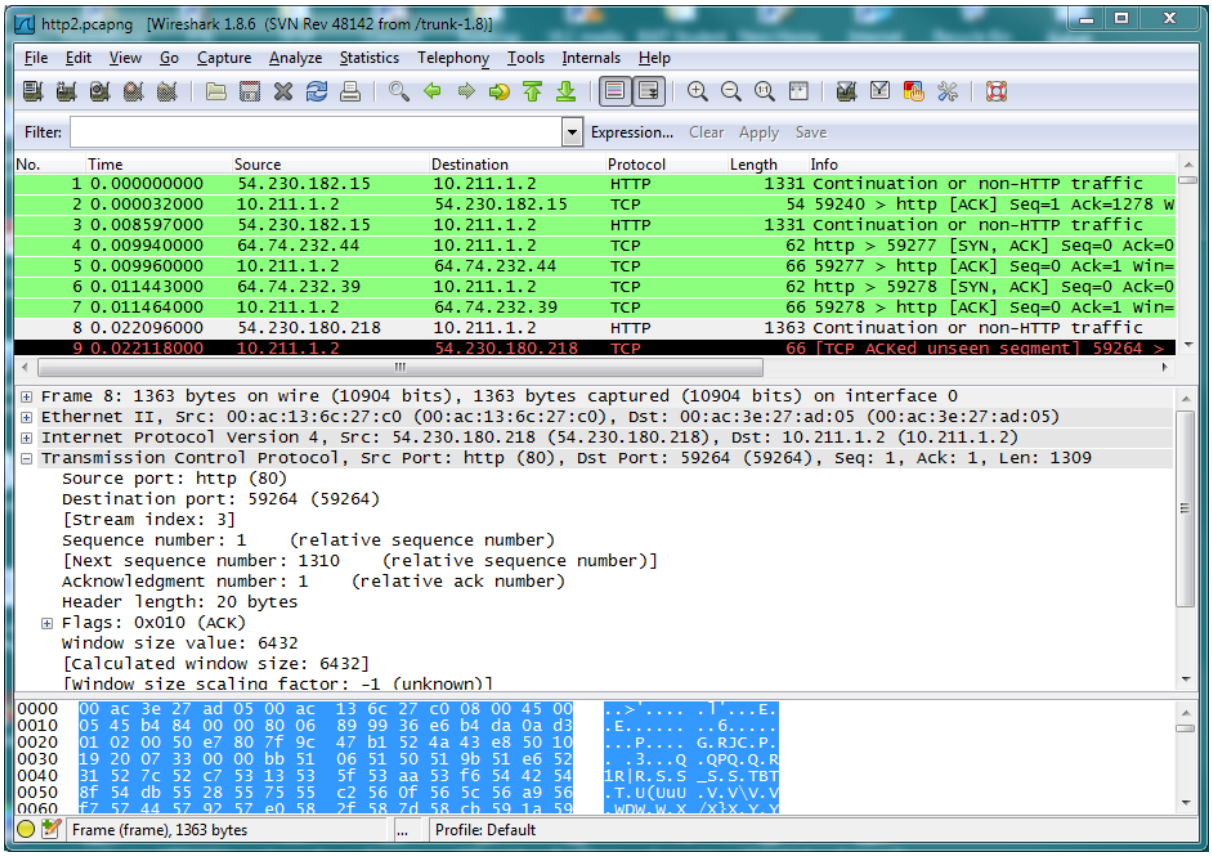
الشكل 2: مسح العناوين والبوابات

محلل البروتوكولات Protocol Analyzer

يمكن التقاط حركة المرور على شبكة ما باستخدام جهاز متخصص لتحليل البروتوكولات أو برنامج لتحليل البروتوكولات يعمل على حاسب. محلل البروتوكولات (يدعى أيضاً الشمّام sniffer) هو جهاز عتادي أو برمجية تقوم بالتقاط الطرود وتفك ترميزها وتحلل محتواها.

تُستخدم محللات البروتوكولات بشكل واسع من قبل مديري الشبكات لمراقبة الشبكة. نذكر من استخداماتها:

- استكشاف وحل مشاكل الشبكة Network troubleshooting. يمكن لمحللات لبروتوكولات اكتشاف مشاكل الشبكة مثل أخطاء العنونة وأخطاء إعدادات البروتوكولات.
- توصيف حركة مرور الشبكة Network traffic characterization. يستطيع محللو البروتوكولات رسم صورة لما يجري في الشبكة.
- تحليل الأمن. يمكن اكتشاف هجمات حجب الخدمة أو أي نوع آخر من الاستغلال للثغرات عن طريق محللي البروتوكولات.



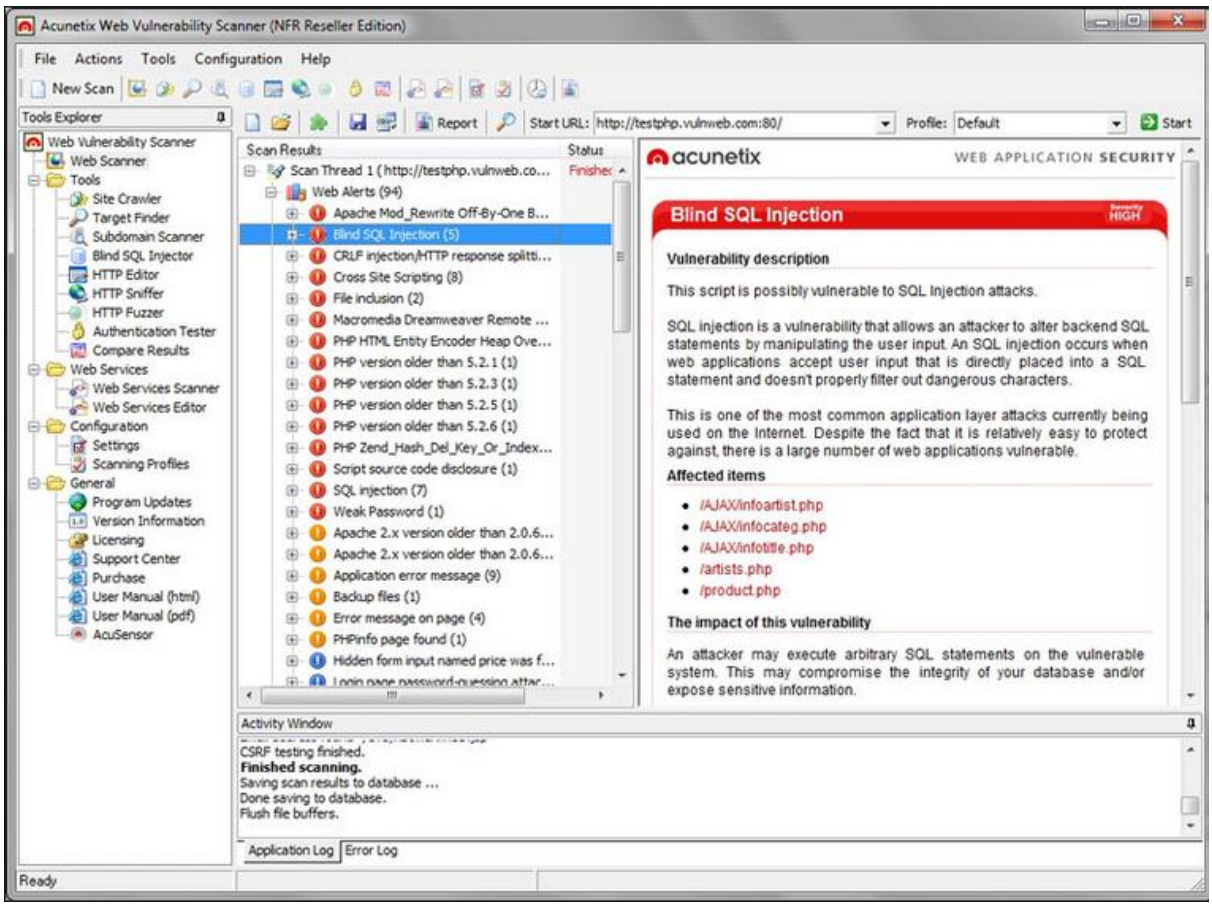
الشكل 3: محلل البروتوكولات wireshark

يتمتع محلل الطرود بمزايا هامة تجعل منه أداة أساسية للمهاجم. عندما يجري تشغيل محلل البروتوكولات، فإنها تضع بطاقة الشبكة على نمط Promiscuous mode أي التقاط جميع الطرود وحتى وإن لم تكن موجهة إلى

هذه البطاقة. فإذا توفر محلل بروتوكولات لمهاجم ما فإنه يستطيع معرفة ترويسات جميع الطرود المتبادلة ومحتوياتها،. فيمكن على سبيل المثال للمهاجم أن يعيد تجميع ملف يجري نقله على الشبكة ويقرأ رسائل البريد الالكتروني ويشاهد محتويات صفحات الوب ويشاهد كلمات المرور غير المشفرة.

ماسحات الضعف Vulnerability scanners

هو تسمية عامة تطلق على مجموعة من الأدوات المستخدمة للبحث عن أماكن الضعف في الشبكات أو أنظمة التشغيل أو التطبيقات. الشكل التالي يوضح الأداة Acunetix المستخدمة لإبراز أماكن ضعف مواقع الوب.



الشكل 4: ماسح أماكن ضعف مواقع الوب Acunetix

من الأدوات الشهيرة في مسح أماكن الضعف Network Mapper (NMAP). كان أول إصدار لهذه الأداة عام 1997 ثم ما لبثت أن تطورت وأصبحت من أهم أدوات المسح الأمنية المجانية والمفتوحة المصدر المستخدمة من قبل ملايين المستخدمين حول العالم. من أهم خدماتها: اكتشاف الشبكة وتدقيق النواحي الأمنية فيها إضافةً إلى استخدامها من قبل بعض مديرو الشبكات لجرد التجهيزات الشبكية وترقية الخدمات حسب جدول زمني ومراقبة الحواسب المضيفة أو الخدمات. يستطيع NMAP اكتشاف الحواسب والمخدمات وأنظمة التشغيل وإصداراتها والخدمات والتطبيقات وإصداراتها وأنواع جدران النار أو مصفيات الطرود المستخدمة وغيرها.

يستخدم مدير الشبكة ماسح الضعف للحصول على بعض الخدمات، مثل:

- التحذير عند إضافة نظام جديد إلى الشبكة
- اكتشاف اختراق تطبيق ما أو انهياره
- اكتشاف تنفيذ مسح بوابات أو مسح عناوين داخلي
- اكتشاف البوابات العاملة بلحظة معينة
- التعرف على التطبيقات والمخدمات التي تستضيف أو تنقل المعلومات الحساسة
- الحفاظ على سجل بكافة جلسات الشبكة
- تحديد نوع نظام التشغيل لكل نظام فعال في الشبكة
- تعقب أماكن ضعف تطبيقات الزبائن والمخدمات
- تعقب الأنظمة التي تتصل مع أنظمة داخلية أخرى

أوعية العسل Honeypots وشبكات العسل Honeynets

وعاء العسل هو حاسب يوضع عادةً في منطقة ذات متطلبات أمنية محدودة ويجهز ببرمجيات ومعطيات غير ذات قيمة تظهر على أنها أصلية غير أنها تكون مقلدة عن معطيات حقيقية. يعد وعاء العسل عن قصد بثغرات أمنية بغية استقبال المهاجمين. يهدف وعاء العسل إلى خداع المهاجم حتى يكشف التقنيات التي يستخدمها بشكل يجعل من السهل مقارنتها مع أنظمة الإنتاج الحالية للتأكد من إمكانية إحباط الهجوم.

بشكل مشابه لوعاء العسل، فإن شبكة العسل هي شبكة ذات ثغرات أمنية مقصودة معدة لاستقبال المهاجمين بغية اكتشاف تقنياتهم والاستفادة منها في تقوية الحماية الأمنية للشبكة. تحوي شبكة العسل وعاء عسل أو أكثر.

4. مسح الضعف واختبار الاختراق Penetration Testing

تعتبر تقنيات مسح الضعف واختبار الاختراق من أهم تقنيات تقدير الضعف. بالرغم من أنه يجري الخلط بين النوعين السابقين من العمليات لكن كل منهم يلعب دوراً في كشف الثغرات الأمنية.

1.4. ما هو مسح الضعف؟

مسح الضعف هو عبارة عن استخدام برمجية تنفذ بحث آلي (مسح) لنظام لاكتشاف أي ضعف أمني ومن ثم يولد تقريراً يحوي هذه الاكتشافات. تقارن نتيجة المسح هذه مع خط أساس بحيث يجري التحقيق في أي تغيير حاصل (كفتح بوابة جديدة أو إضافة خدمة). يجب إجراء مسح الضعف على الأنظمة الموجودة وخاصةً عند نشر أجهزة جديدة؛ تمسح الأجهزة الجدية مباشرة ومن ثم تضاف إلى الجداول الزمنية لمسح جميع التجهيزات.
يعمل مسح الضعف بشكل سلبي اي أنه لا يحاول استغلال نقاط الضعف المكتشفة وإنما فقط توليد تقرير عنها.
يجري تحقيق مسح الضعف من داخل المؤسسة ويجب أن لا تؤثر على سير عمل الشبكة أو التجهيزات.

2.4. اختبار الاختراق

يجري تصميم اختبار الاختراق pentest لاستغلال نقاط الضعف المكتشفة في النظام. يعتمد اختبار الاختراق على مهارات ومعرفة وبراعة المختبر. عادةً، يكون المختبر هو متعاقد مستقل غير مرتبط بالمؤسسة لكن يملك خبرة معلوماتية جيدة وعلى دراية بطبيعة عمل المؤسسة. يكون المختبرون خارج المحيط الأمني للمؤسسة ويمكن أن يعطلون عمل الشبكة أو التجهيزات.
الناتج النهائي لعملية اختبار الاختراق هو تقرير يدلل على طبيعة المعطيات التي اخترقت وكيف تم الاختراق؟ ولماذا؟. يفصل التقرير طريقة الهجوم التي اتبعت وقيم المعطيات المستغلة. يمكن أيضاً تزويد حلول للمشاكل المكتشفة لكن عادةً تقع مسائل حل المشاكل الأمنية على عاتق المؤسسة.
يمكن أن يستخدم مختبرو الاختراق أحد ثلاث تقنيات. تتفاوت كل تقنية حسب درجة المعرفة التي يمتلكها المختبر إزاء تفاصيل الأنظمة قيد التقييم:

- الصندوق الأسود Black box. في اختبار الصندوق الأسود، ليس لدى المختبر أي معرفة ببنية الشبكة المختبرة. يجب على المختبر تحديد مواقع وأنواع الأنظمة والأجهزة قبل البدء بالاختبار. هذا الاختبار يقلد بشكل دقيق الهجمات الخارجية الفعلية.
- الصندوق الأبيض White box. في اختبار الصندوق الأبيض، يملك المختبر معرفة عميقة عن الشبكة والأجهزة المطلوب اختبارها بما يشمل على مخططات الشبكات وعناوين IP وحتى الرماز المصدري لبعض التطبيقات.
- الصندوق الرمادي Gray box. في اختبار الصندوق الرمادي، يجري تزويد المختبر ببعض المعلومات المحدودة.

يقارن الجدول التالي ميزات كل من مسح الضعف واختبار الاختراق.

الميزة	مسح الضعف	اختبار الاختراق
التكرار frequency	عند إضافة تجهيزات جديدة أو على الأقل مرة بالشهر	مرة بالسنة
الأهداف	اكتشاف ثغرات معروفة لم تعالج بعد	إيجاد المخاطر التجارية على سير العمل
المختبر	تقني محلي	استشاري خارجي مستقل
الموقع	من الداخل	من الخارج
تعطل العمل	لا يوجد	محتمل
الأدوات	برمجيات مؤتمتة	مهارات ومعارف المختبر
التكلفة	منخفضة	عالية
التقرير	مقارنات شاملة بين الثغرات الحالية وخط الأساس	مختصرة تحلل طريقة نجاح الهجوم والأضرار
القيمة	اكتشاف الضعف في الأجهزة والبرمجيات	وقائي لتقليل المخاطر التجارية

الجدول 5: ميزات مسح الضعف واختبار الاختراق

5. تخفيف الهجمات وردعها Mitigating and Deterring attacks

مع أنه يوجد مجموعة متنوعة من الهجمات لكن يوجد تقنيات معيارية يمكن استخدامها لتخفيف الهجمات وردعها. تشمل هذه التقنيات على انشاء وضعيات أمنية وتكوين الضوابط والتصليد وإعداد التقارير.

1.5. انشاء وضعيات أمنية Security Posture

من العناصر التي يمكن اعتبارها عند انشاء وضعية أمنية:

- ضبط خط أساس ابتدائي.
- مراقبة أمنية متواصلة.
- المعالجة.

2.5. وضع الضوابط

من العوامل الهامة في تخفيف الهجمات أو ردعها هو وضع الضوابط. تستطيع بعض الضوابط اكتشاف الهجمات لكن لا يمكنها منعه مثل كاميرا المراقبة التي تسجل دخول شخص إلى موقع ما بينما تستطيع ضوابط خرى أن تمنع الهجمات مثل وضع حارس أمني على باب الدخول لمنع الأشخاص غير المخولين من الدخول.
يجب أيضاً تحديد الضوابط التي تحكم آلية العمل عند حدوث الأعطال. فمثلاً ما هي الحالة التي يجب أن ينتقل لها جدار النار عندما يتعطل هل يسمح بمرور جميع الطرود أو يمنعها؟
من الأهمية بمكان هنا تحديد الضوابط السليمة بغية تزويد المستوى الأعلى من الأمن للمؤسسة.

3.5. التصليد Hardening

يهدف التصليد إلى إزالة أكبر قدر ممكن من المخاطر الأمنية وجعل النظام أكثر أمناً. يوجد أنواعاً متعددة من التقنيات المستخدمة لتصليد الأنظمة. تذكر منها:

- حماية الحسابات بكلمات المرور
- تعطيل الحسابات غير الضرورية
- تعطيل الخدمات غير الضرورية
- حماية واجهات الإدارة والتطبيقات

4.5. إعداد التقارير reporting

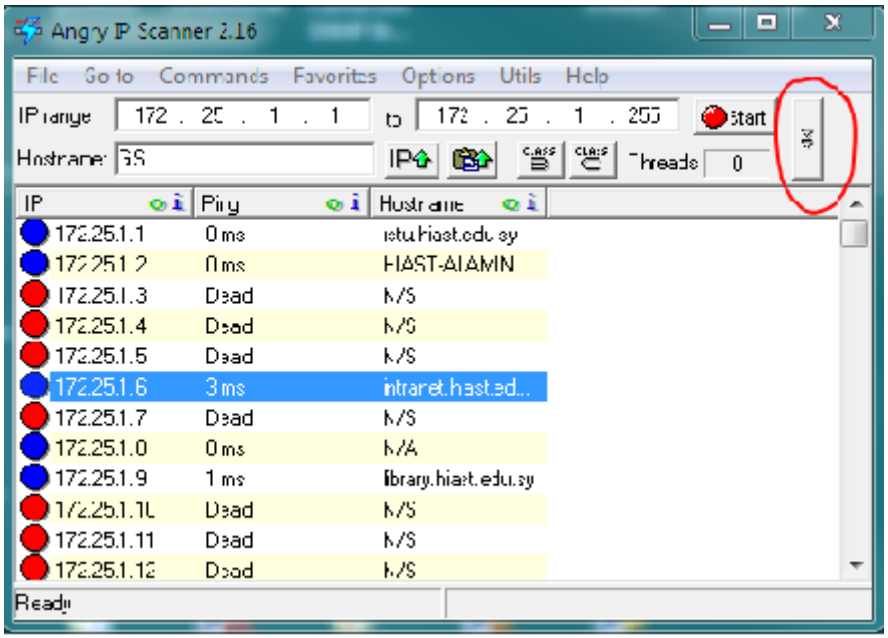
من المهم تزويد المعلومات عن الأحداث التي تقع حتى نستطيع متابعتها ومعالجتها. يمكن أن تأخذ التقارير شكل الإنذارات alarms أو التحذيرات alerts التي تردد رسالة محددة للتنبيه عن حدث معين قيد الحصول. مثلاً، يمكن أن يؤشر تحذير ما على محاولة إدخال كلمة مرور خاطئة لمستثمر لعدة مرات. ويمكن أن تكون الإنذارات أكثر شمولاً عن طريق الإنذار مثلاً عن محاولة تخمين كلمات مرور عدة مستثمرين في نافذة زمنية صغيرة.

6.تمارين عملية

1.6. استخدام ماسح عناوين وبوابات

سنستخدم في هذا التمرين ماسح العناوين والبوابات Angry IP Scanner لمعرفة عناوين IP المستخدمة في شبكة ما ومن ثم اختيار عنوان IP ما واختبار البوابات المفتوحة.

1. Run ipscan.exe
2. Depending on your network range, select a range from 192.168.1.1 to 192.168.1.255
3. Click start
4. A list of alive hosts will be in blue color
5. how many alive host, you find?
6. Select your own host
7. Click show/hide additional controls at the far right as shown in the following figure:



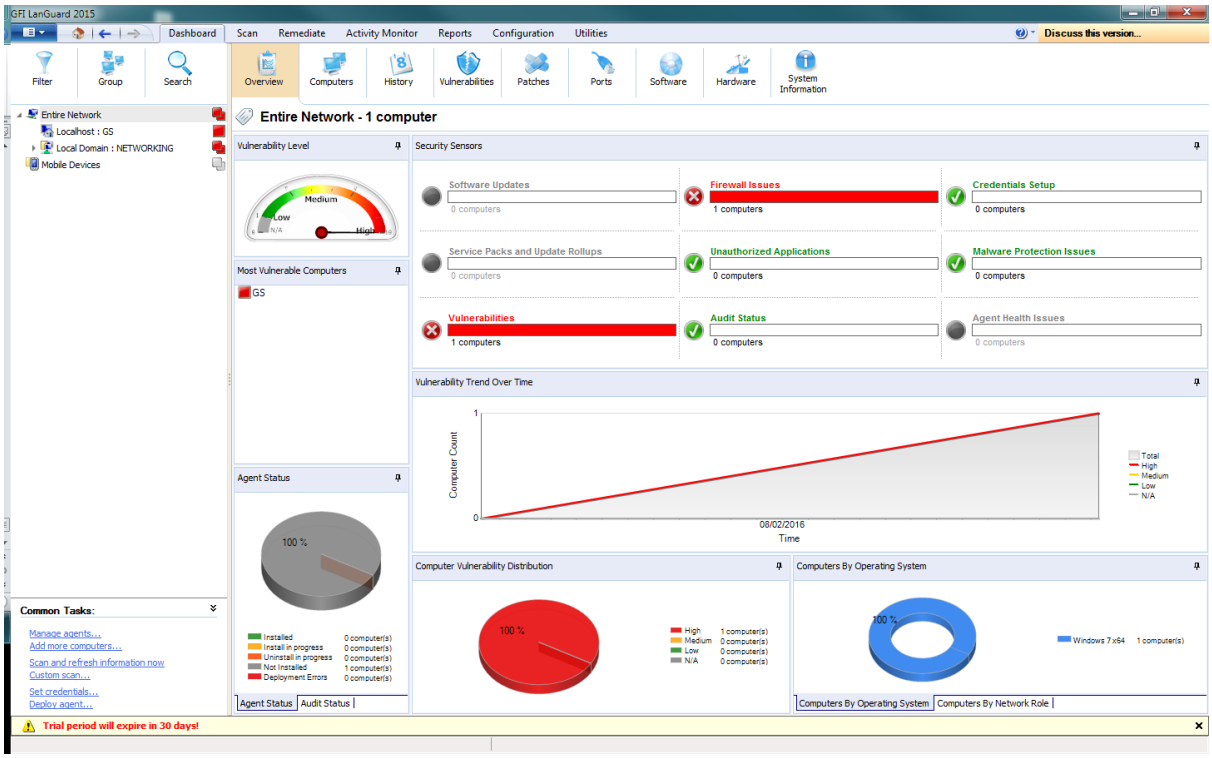
8. Enter the IP address of your host in the IP range
9. Click select TCP ports to be scanned
10. Enter range between 1 and 1023
11. Click start

12. What ports are open in your host? and what are the service for each open port?

2.6. استخدام ماسح الضعف GFI LANGuard

ستقوم هنا بتحميل وتنصيب أداة GFI LANGuard.

1. Launch GFI LANGuard
2. Click Quick scan
3. Click scan this computer and then click next
4. Click currently logged on user and then click Scan
5. The scanning in progress … screen appear as show in next figure.

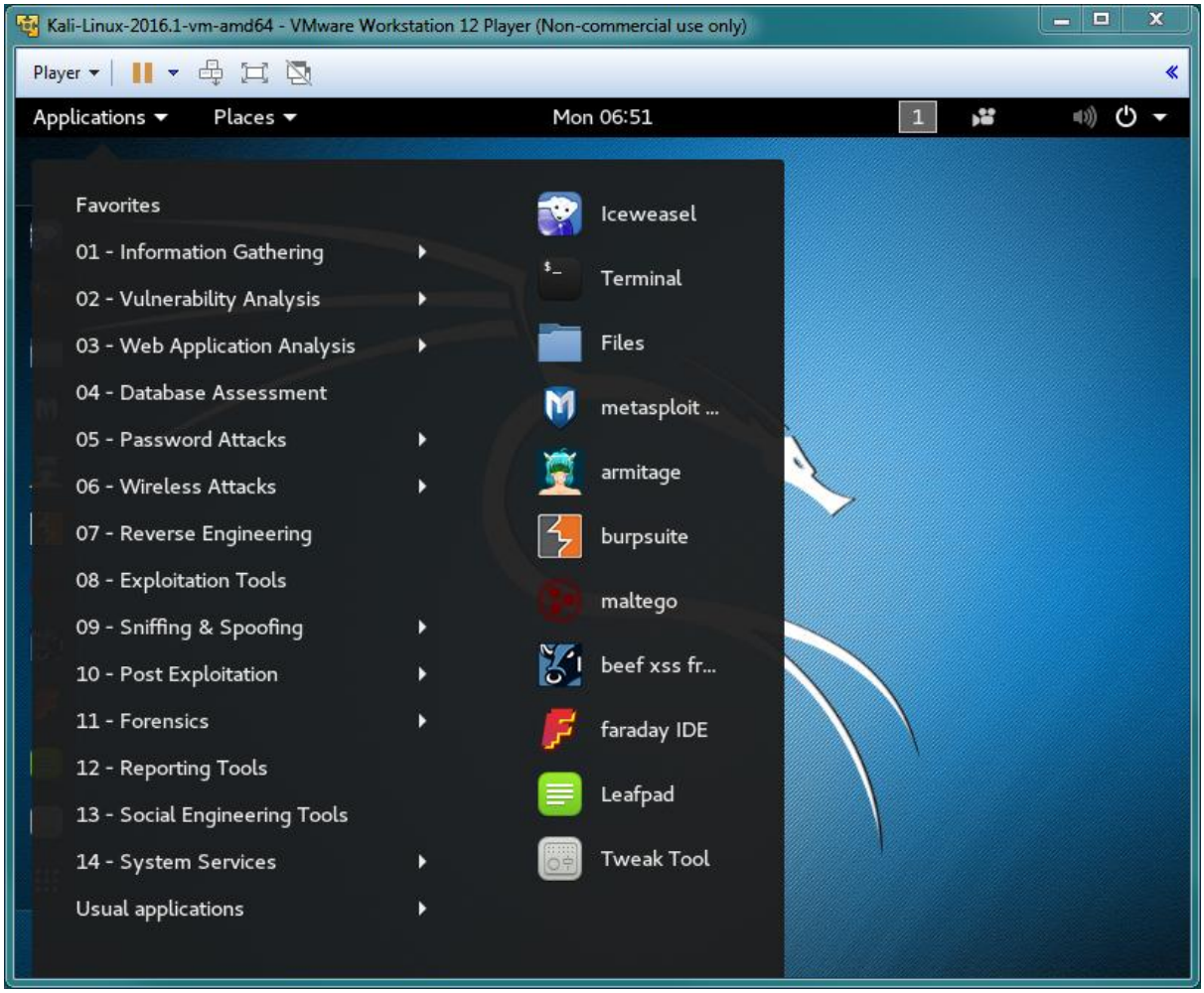


6. When the scan is complete click OK.
7. Click analyze scan results
8. Expand the items in Scan Results Overview to display the detail in the Scan Results Details window. What information can you gather from this scan? Would you consider it helpful? In what way?
9. Close all windows.

3.6. استخدام Kali Linux Vmware

كالي لينوكس هي الجيل الجديد من توزيعة BackTrack Linux لتنفيذ اختبار الاختراقات وتدقيق الإعدادات الأمنية للشبكات والحواسب. من الأدوات التي تقدمها الأداة المجانية كالي:

- جمع المعلومات Information Gathering
- تحليل الضعف Vulnerability Analysis
- الهجمات على الشبكات اللاسلكية Wireless Attacks
- تطبيقات الوب
- أدوات الاستغلال
- أدوات قضائية Forensic tools
- اختبار التحمل Stress Testing
- التنصت والشم Sniffing & spoofing
- الهجوم على كلمات المرور
- الحفاظ على النفاذ
- الهندسة العكسية
- أدوات توليد التقارير
- اختراق العتاديات Hardware Hacking


Kali-Linux-2016.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications
Places
Mon 06:51
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Iceweasel
Terminal
Files
metasploit ...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad
Tweak Tool

الفصل الخامس: أمن الشبكات
Network Security

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعرف أنواع الأجهزة المختلفة لتحقيق أمن الشبكات وشرح طريقة استخدام كل منها
- تعريف ترجمة عناوين الشبكات والتحكم بالنفاذ الشبكي
- شرح طريقة تعزيز الأمن من خلال تصميم الشبكة

يعتبر أمن الشبكات ضروري جداً للحفاظ على سلامة المعلومات. عندما يجري تصميم ومن ثم كتابة تطبيق ما، لا يتم أخذ الأمن والوثوقية بعين الاعتبار. هذا يعني أنه أصبحت مسؤولية الشبكة لحماية هذا التطبيق. أضف إلى ذلك أن بمجرد نفاذ مهاجم ما إلى شبكة حاسوبية فإنه يصبح قادراً على النفاذ إلى جميع الحواسيب والمخدمات وأجهزة التخزين الأمر الذي يجعل الشبكة مكوناً أساسياً في عمليات التخطيط الأمنية للمؤسسة.

1. الأمن من خلال الأجهزة الشبكية

يمكننا تأمين مستوى قاعدي من الأمن باستخدام ميزات الأمن التي تقدمها الأجهزة الشبكية.

1.1. الأجهزة الشبكية المعيارية

يمكننا تصنيف الأجهزة الشبكية المعيارية على أساس الطبقة التي يعمل بها كل جهاز مقارنةً بالنموذج المعياري Open Systems Interconnection (OSI). تشمل الأجهزة حسب التصنيف المعياري المجمعات Hubs والمبدلات Switches والمسيرات Routers وموازنات العبء Load Balancers.

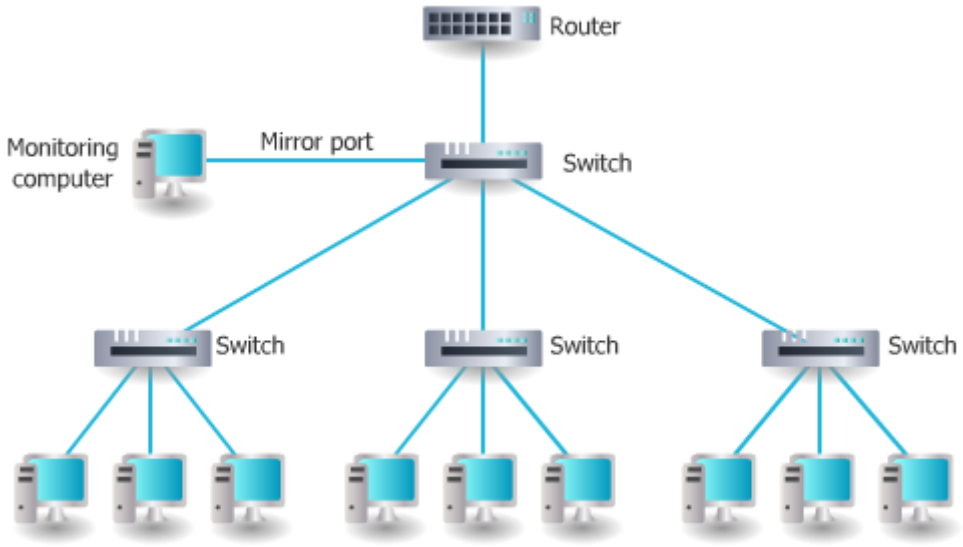
المجمعات Hubs

تعمل المجمعة على المستوى الفيزيائي حيث تسمح بربط عدة حواسب مع بعضها البعض باستخدام أزواج مجدولة أو ألياف ضوئية ضمن شبكة إيثرنت. تستقبل المجمعة إطار ما وتعيد إرساله على بقية البوابات دون أن تعرف أي معلومة متعلقة بالعناوين الفيزيائية أو المنطقية (تسمى مكرر متعدد البوابات). بما أن المجمعة تعيد إرسال الإشارات الكهربائية المستقبلة على جميع البوابات فإنها يمكن أن تشكل مخاطرة أمنية. يكفي المهاجم أن يصل حاسبه إلى أحد بوابات المجمعة أو أن يتنصت على أحد الحواسب الأخرى باستخدام محلل البروتوكولات حتى يصبح قادراً على فك ترميز جميع محتويات الأطر المارة في الشبكة.

المبدلات Switches

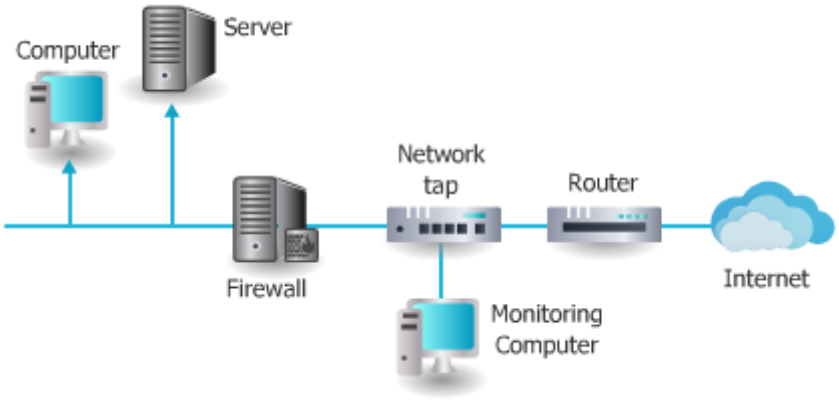
على عكس المجمعة، تعمل المبدلة على المستوى الثاني أي طبقة وصلة المعطيات Data-link layer وهي قادرة على قراءة عنوان المرسل وعنوان الوجهة الفيزيائيين (أو MAC addresses) ومن ثم توجيه الإطار المستقبل على البوابة التي تقع عليه الوجهة كما أن المبدلة تملك ألية التعلم الذاتي Auto-learning تمكنها من ربيط كل عنوان فيزيائي مع البوابة الموصولة عليه. تقدم المبدلة أداءً أمنياً أفضل من المجمعة لأن وضع محلل بروتوكولات على إحدى بواباتها تمكّن فقط من التقاط الطرود الموجهة إلى تلك البوابة.

مع أن المبدلة تحد من عملية تعميم الأطر على بقية البوابات إلا أن مدير النظام يحتاج في بعض الأحيان لمراقبة أداء بطاقات الشبكة ومعرفة البطاقات المعطلة كتلك التي تولد أطراً غير سليمة. لذلك تكون بعض المبدلات القابلة للإدارة مزودة بميزة انعكاس البوابات Port mirroring حيث يستطيع مدير الشبكة إعداد المبدلة بشكل يسمح بتوجيه جميع حركات المرور لبوابة أو لعدة بوابات أو لجميع البوابات إلى بوابة مراقبة معروفة. يبين الشكل التالي ميزة انعكاس البوابات.



الشكل 1: انعكاس البوابات

تتمثل الطريقة الثانية في مراقبة حركات المرور في تنصيب فرعة شبكية network tap. الفرعة الشبكية هي عبارة عن جهاز منفصل يمكن وضعه بين جهازين شبكيين مثل مبدلة أو مسير أو جدار نار لمراقبة حركات المرور. يبين الشكل التالي مثالاً عن فرعة شبكية موضوعة بين جدار نار ومبدلة.



الشكل 2: الفرعة الشبكية

يوضح الجدول التالي أنواع الهجمات التي يمكن أن تتعرض لها شبكة ما.

نوع الهجوم	الوصف	الدفاع
إغراق العناوين الفيزيائية MAC flooding	يمكن للمهاجم إغراق جدول العناوين الفيزيائية للمبدلة بعناوين مزيفة الأمر الذي يجبره على التصرف كمجمعة	استخدام مبدلة قادرة على إغلاق البوابات ذات العدد الكبير من العناوين
انتحال العناوين الفيزيائية	إذا امتلك جهازان عنوان فيزيائي واحد فيمكن للمبدلة توجيه الأطر لأحد الأجهزة فقط حسب إعدادات ARP. يمكن للمهاجم تغيير عنوانه ليطابق عنوان جهاز آخر.	تكوين المبدلة بحيث تسمح بربط بوابة واحدة لكل عنوان فيزيائي
تسميم ARP	يمكن للمهاجم إرسال أطر ARP مزيفة بحيث ينتحل عنوان جهاز آخر وبالتالي يستقبل الطرود الموجهة لها	استخدام طرق اكتشاف تزوير ARP
انعكاس البوابات	يربط المهاجم جهازه ببوابة الانعكاس لمبدلة	تأمين المبدلة في غرفة مقفولة
فرعة شبكية	يصل المهاجم فرعة شبكية إلى الشبكة لاعتراض الأطر	حصر الوصول الفيزيائي للشبكة

الجدول 1: حماية المبدلة

المسيرات Routers

يعمل المسير على مستوى طبقة الشبكة (الطبقة الثالثة) وهو قادر على توجيه الطرود عبر الشبكات من خلال البحث، ضمن جدول توجيه موجود عنده، عن عنوان الوجهة، الموجود في ترويسة طبقة الشبكة، ومن ثم إرسال الطرد إلى الشبكة التالية باتجاه الوجهة. يمكن للمسيرات القيام ببعض الوظائف الأمنية مثل تصفية الطرود Packet Filtering.

موازنات العبء Load Balancers

موازنة العبء هي تقانة مساعدة في توزيع العمل ضمن الشبكة. أي يمكن توزيع الطلبات المستقبلة على مجموعة من المخدمات بدلاً عن مخدم واحد وبطريقة شفافة بالنسبة للمستخدم. تقدم موازنات العبء الميزات التالية:

- تقليل احتمال إرهاق مخدم واحد
- تخصيص كل حاسب شبكي بمعدل نقل أمثلي
- تقليل توقف الشبكة

يمكن تشغيل موازنات العبء ضمن برنامج على حاسوب أو تخصيص جهاز لهذه العملية (جهاز موازنة العبء). يأخذ موازن العبء بالحسبان مجموعة من العوامل مثل عدد الاتصالات المفتوحة عند كل مخدم أو نسبة انشغال المعالجات في كل مخدم أو الأداء الكلي للمخدم.

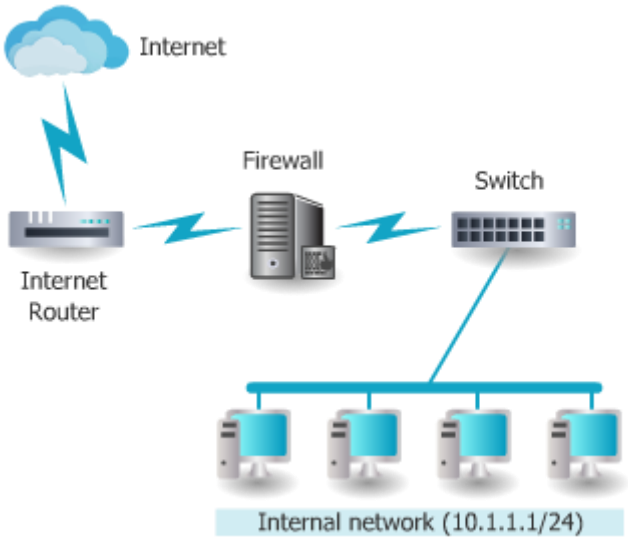
بما أن موازن العبء يقع قبل المخدمات فهو قادر على اكتشاف بعض أنواع الهجمات مثل حجب الخدمة.

2.1. عتاديات أمن الشبكات

مع أن الأجهزة الشبكية المعيارية تستطيع تقديم درجة من الأمن غير أن الأجهزة المصممة خصيصاً للأمن تقدم درجة أعلى من الحماية. نذكر من هذه الأجهزة جدران النار Firewalls والمخدمات الوكيلة Proxy servers ومصفيات الرسائل غير المرغوبة spam filters ومركزات الشبكات الخاصة الافتراضية VPN concentrators ومصفيات محتويات الإنترنت Internet content filters وعبّارات أمن الوب Web Security Gateways وأنظمة اكتشاف التسلل ومنعه IDS/IPS وتطبيقات تشمل جميع الخدمات.

جدران النار Firewalls

يوجد نوعين من جدران النار: الشخصي والشبكي. جدار النار الشخصي هو عبارة عن برنامج يعمل على الحاسب المحلي لتصفية حركات المرور الشبكية من وإلى الحاسب. أما جدار النار الشبكي فهو يصفي الطرود قبل دخولها إلى الشبكة. يقع جدار نار الشبكة عادةً خارج المحيط الأمني للشبكة ويعتبر خط الدفاع الأول كما هو موضح في الشكل التالي.



الشكل 3: توضع جدار النار

عندما يستقبل جدار النار طرداً ما فإنه إما يسمح له بالمرور أو يوقفه Block عن طريق تجاهله أو المطالبة (يسأل عن العملية المطلوب فعلها). يعمل جدار النار على أساس القواعد Rule-based أو على أساس التطبيقات applications-based. عندما يعمل جدار النار على أساس القواعد فإنه يستخدم مجموعة من التعليمات الفردية للتحكم بالفعل. القاعدة هي مجموعة من المعلومات النصية التي تحدد عنوان الشبكة ورقم البوابة المسموح لهم/ غير المسموح لهم بالدخول. فمثلاً تسمح قاعدة ما لمستخدم من داخل الشبكة بإرسال طلب صفحة وب من مخدم وب خارجي. كما تسمح لمخدم الوب بإرسال الصفحة كجواب على الطلب السابق. يلخص الجدول التالي بعض محتويات القواعد.

وصف القاعدة	شرح عنها	التصفية
Source address = any	عنوان IP للمخدم غير المعروف مسبقاً	لا يوجد تصفية لأننا لا نعرف عناوين IP للمخدمات بشكل مسبق
Destination address = internal IP address	عنوان IP للحاسب الموجهة له الصفحة	تسمح هذه القاعدة للطرود الموجهة إلى عناوين محددة ضمن الشبكة المحلية بالمرور عبر جدار النار
Port = 80	هذا يعني أن البوابة رقم 80 مفتوحة	لا يوجد بوابات أخرى مفتوحة

الجدول 2: قاعدة مخصصة للاتصال مع مخدم وب

تحدد كل قاعدة لجدار النار ما يجب فعله مع كل طرد مستقبل. تخزن القواعد ضمن ملف أو عدة ملفات نصية يقرأها جدار النار عند الإقلاع. يعتبر هذا النوع من جدران النار ساكن وذلك لأن جدار النار لا يمكن أن يفعل شيئاً من خارج إعدادات القواعد الأمر الذي يجعله سهل الإعداد لكن غير مرن في التأقلم مع التغيرات.

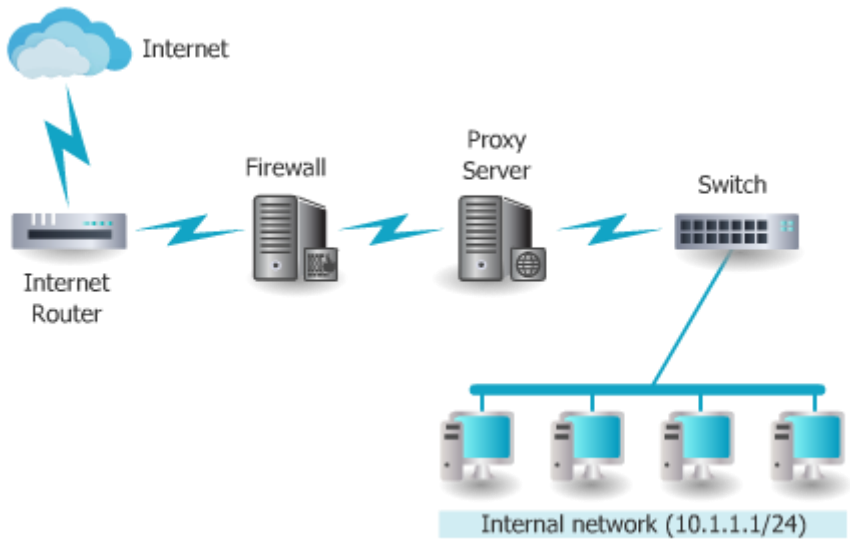
في حالة جدار نار على أساس التطبيقات، فإنه يحد من نفاذ التطبيقات إلى نظام التشغيل عن طريق التحكم بتنفيذ الملفات أو بمعالجة المعطيات من قبل التطبيقات.

تجري عملية تصفية الطرود من قبل جدار النار بطريقتين: تصفية المعطيات عديمة الحالة Stateless Packet filtering حيث تجري تصفية كل طرد قادم حسب الشروط التي وضعها مدير النظام. أما في حال تصفية المعطيات حسب الحالة Stateful packet filtering فيحتفظ جدار النار بسجل عن حالة الاتصال بين الحاسب المحلي والمخدم الخارجي ويأخذ قراراً اعتماداً على حالة الاتصال وعلى الشروط الموضوعة. فمثلاً عند استخدام جدار نار حسب الحالة فإنه يمكننا تحديد أن تأسيس الاتصال يتم من قبل الحاسب المحلي وتقبل الطرود المستقبلة من الطرف الخارجي بعد تأسيس الاتصال. هذه القاعدة غير ممكنة في حالة جدار نار عديم الحالة.

تعتبر جدران نار تطبيقات الوب حالة خاصة من جدران النار. يتم هنا البحث بشكل أعمق في الطرود التي تحمل حركات مرور تطبيقات الوب (أي HTTP) على أساس تطبيقات الطبقة 7. يمكن لهذا النوع من جدران النار توقيف مواقع وب محددة أو هجمات يمكن أن تستغل نقاط ضعف معروفة ضمن برمجيات الزبائن.

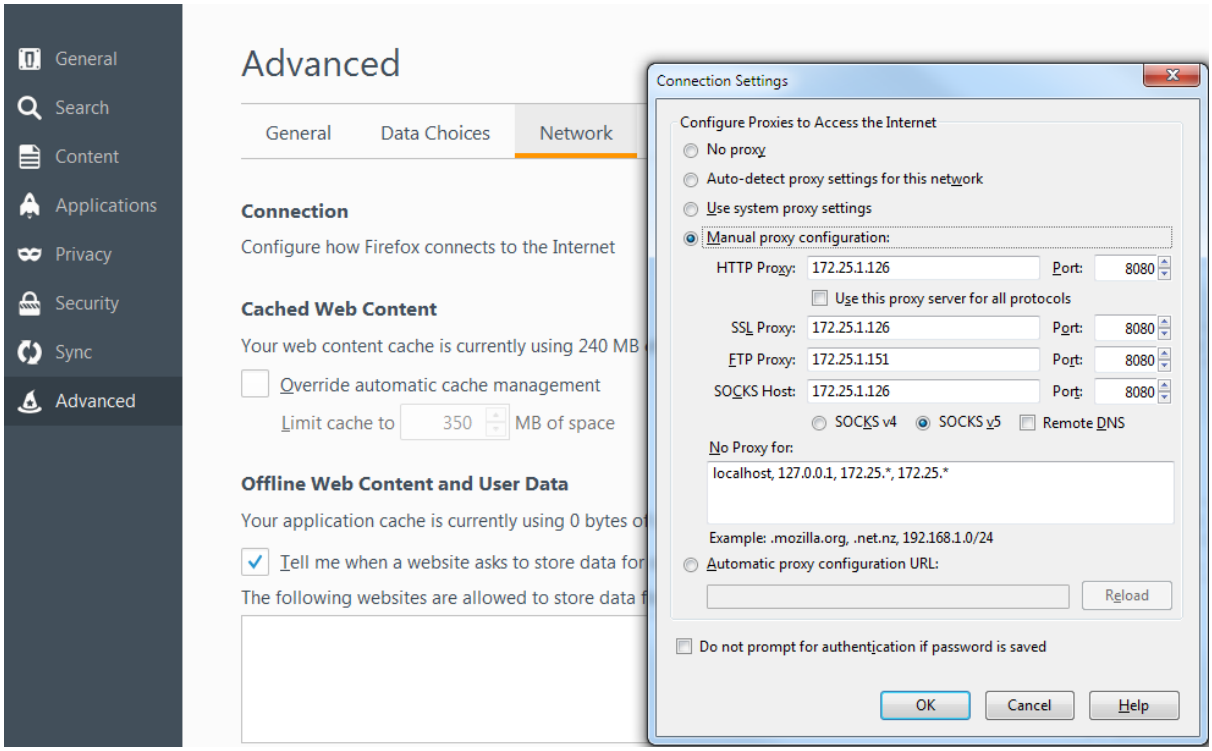
المخدمات الوكيلة Proxies

المخدم الوكيل هو حاسب أو برنامج تطبيقي يقوم باعتراض طلبات المستخدم القادمة من الشبكة الداخلية المحمية ومن ثم يعالج هذا الطلب بدلاً عن المستخدم. يوضح الشكل التالي آلية عمل المخدم الوكيل.



الشكل 4: المخدم الوكيل

عندما يطلب المستخدم الداخلي ملف ما أو صفحة وب من مخدم خارجي فإن الاتصال يكون مباشراً مع المخدم الخارجي في حال عدم وجود المخدم الوكيل. أما في حالة وجود المخدم الوكيل، فإن اتصال الزبون وإرسال الطلب يجري مع المخدم الوكيل الذي يختبر وجود جواب للطلب ضمن ذاكرة خابية Cache (أي يعمل المخدم الوكيل كمخدم تخبئة أيضاً). في حال وجود نسخة من الجواب ضمن الذاكرة الخابية فإن المخدم الوكيل يرسلها للمستخدم وإلا فإنه يتصل بمخدم الوب الخارجي باستخدام عنوان الإنترنت الخاص به ويطلب الصفحة. عندما يستقبل المخدم الوكيل الصفحة المطلوبة فإنه يعيد توجيهها إلى المستخدم بعد وضع نسخة منها ضمن الخابية. يجري إعداد الاتصال مع المخدم الوكيل من خلال متصفح الإنترنت كما هو موضح في الشكل التالي.



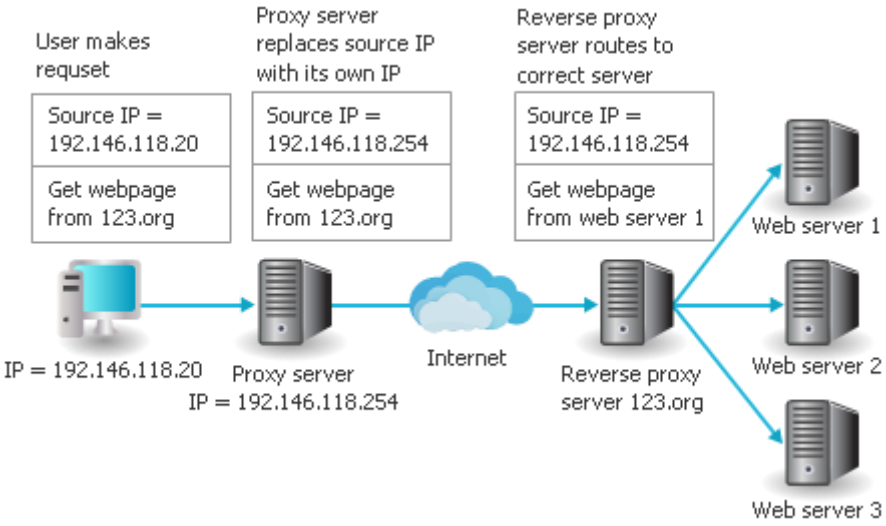
الشكل 5: إعدادات المخدم الوكيل ضمن متصفح موزيلا فاير فوكس

يفيد المخدم الوكيل في تحقيق ما يلي:

- زيادة سرعة التحميل بسبب تخبئة المعطيات
- تخفيض التكاليف عن طريق تقليل سعة الوصلة المطلوبة
- تحسين الإدارة عن طريق توقيف مواقع الوب غير المرغوبة أو توقيف صفحات محدد منها
- تأمين حماية أمنية أعلى وذلك لأن المخدم الوكيل يخفي العنوان الحقيقي للزبون كما أنه يعمل كوسيط عند استقبال الأجوبة على طلبات المستخدمين أي أنه يستقبل أي برمجيثة قبل أن تصيب المستخدم.

تجدر الإشارة إلى وجود مخدمات وكيلة شفافة لا يعلم المستخدم بوجودها ولا تتطلب أية إعدادات.

كما يوجد أيضاً مخدمات وكيلة عكسية تهدف إلى حماية المخدمات وليس المستخدمين أي أنها تربط إلى المخدمات وتستقبل الطلبات عوضاً عنها وتوجهها إلا المخدمات ولا يشعر المستخدم بوجودها.



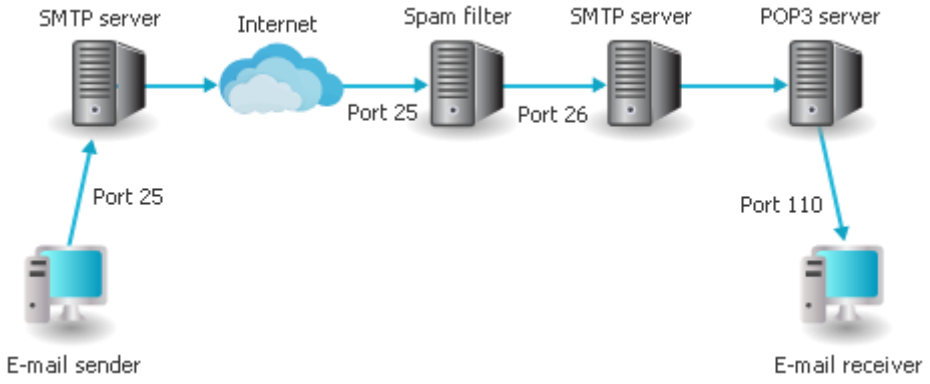
الشكل 6: المخدم الوكيل العكسي

مصفيات البريد غير المرغوب Spam filters

نظراً لخطورة رسائل البريد غير المرغوبة وحجمها الهائل، تسعى المؤسسات لاستخدام مصفيات الرسائل غير المرغوبة لتوقيف هذه الرسائل قبل أن تصل للمستخدم.

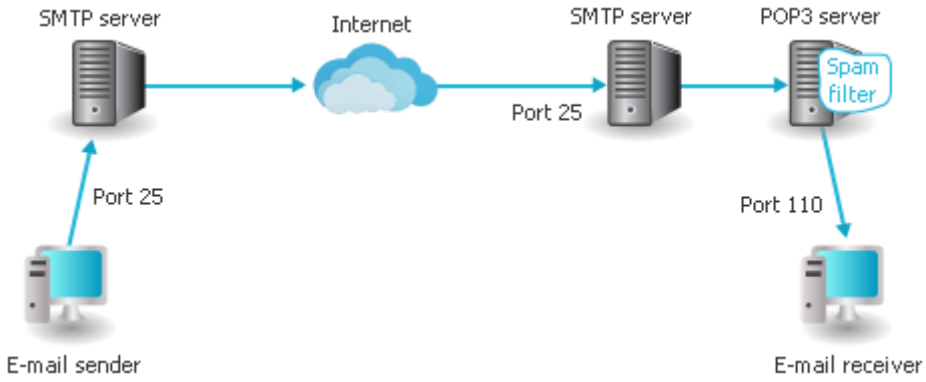
يوجد طريقتين لتحقيق تصفية الرسائل غير المرغوبة:

- تثبيت مصفي البريد غير المرغوب مع مخدم SMTP. يمكننا هنا تشغيل مخدم SMTP ومصفي البريد غير المرغوب على الحاسوب نفسه أو على حاسوبين مختلفين. يجري إعداد المصفي للتنصت على البوابة 25 لاعتراض جميع الرسائل المستقبلة وتوجيه الرسائل النظامية إلى مخدم SMTP الذي يتنصت على بوابة أخرى وذلك بعد حذف البريد غير المرغوب. هذا الإعداد يجنب مخدم SMTP إعلام المرسل عن عدم إمكانية إرسال الرسالة. يبين الشكل التالي هذه الطريقة.



الشكل 7: مصفي البريد مع مخدم SMTP

- تثبيت مصفي البريد غير المرغوب على مخدم POP3. تعني هذه الطريقة أن جميع الرسائل غير المرغوبة ستمر عبر مخدم SMTP وتصل إلى علب بريد المستخدمين. هذا يؤدي إلى الحاجة إلى أماكن تخزين أكبر وسعات اتصال أوسع ونسخ احتياطي ومن ثم حذف. يبين الشكل التالي آلية عمل هذه الطريقة.



الشكل 8: مصفي البريد المزعج مع مخدم POP3

يوجد طريقة أخرى لتصفية البريد المزعج تتمثل في التعاقد مع طرف ثالث يقوم بعملية التصفية. يجري هنا تحويل جميع الرسائل إلى مصفي البريد غير المرغوب الخارجي حيث يتم تصفيتها وإعادة إرسالها إلى المؤسسة.

مركزات الشبكات الخاصة الافتراضية Virtual Private network (VPN) Concentrators

تستخدم الشبكات الخاصة الافتراضية شبكة عامة غير آمنة مثل الإنترنت وتحولها إلى شبكة خاصة آمنة. تفعل ذلك عن طريق تشفير جميع المعطيات المارة بين الجهاز البعيد وبين الشبكة. هذا يضمن عدم قابلية المعطيات للقراءة في حال اعتراضها من قبل طرف ثالث. يوجد نوعين شائعين لشبكات VPN. شبكات VPN للنفاذ البعيد Remote-access VPN وهي من نوع اتصال مستخدم مع شبكة محلية. النوع الثاني هو شبكات VPN موقع لموقع Site-to-site VPN حيث يجري وصل مواقع مع بعضها باستخدام VPN.

تحقق اتصالات VPN عن طريق الاتصال بين النقاط النهائية Endpoints. النقطة النهائية هي نهاية النفق بين أجهزة VPN. يمكن أن تكون النقطة النهائية عبارة عن برمجية ضمن حاسوب محلي أو جهاز مخصص كمركّز VPN (يجمع مئات أو آلاف اتصالات VPN) أو مضمن ضمن جهاز شبكي مثل جدار النار. يمكن أن نحتاج في بعض الحلات إلى برامج خاصة بالزبون الذي يريد الاتصال بشبكة VPN حسب نوع النقاط النهائية المستخدمة. تعالج الأجهزة التي تحوي نقاط نهائية مضمنة داخلها إعدادات أنفاق VPN والتغليف والتشفير عند النقطة النهائية. هنا لا تحتاج أجهزة الزبون إلى برمجيات خاصة حيث تكون جميع عمليات VPN شفافة بالنسبة لهم.

يمكن أن تكون شبكات VPN برمجية أو عتادية. شبكات VPN البرمجية، أي النقاط النهائية هي برمجيات تعمل على الأجهزة نفسها، وتؤمن درجة عالية من المرونة في إدارة حركات المرور لكنها لا تملك الأداء والأمن الذي

تحققه الشبكات العتادية. تكون الشبكات العتادية أكثر أمناً وذات أداء أفضل وتزود مرونة أعلى من الشبكات البرمجية.

مصفيات محتوى الإنترنت Internet Content Filter

تراقب مصفيات محتوى الإنترنت حركات مرور الإنترنت وتعطل النفاذ إلى مواقع أو ملفات محددة. يجري عرض صفحة الوب إذا كانت تمتثل إلى محددات المصفي. يمكن هنا تحديد الصفحات غير المرغوبة عن طريق URL أو باستخدام كلمات مفتاحية كما يمكن أيضاً منع أنواع محددة من المحتوى مثل الموسيقى والفيديو.

عبّارات أمن الوب Web Security Gateways

تقوم عبّارات أمن الإنترنت بتعطيل المحتويات الخبيثة بالزمن الحقيقي لحظة ظهورها (حتى بدون معرفة أن المحتوى قادم من صفحة خبيثة). تختبر عبّارات أمن الإنترنت المحتوى من خلال التصفية على مستوى التطبيقات. على سبيل المثال، يمكن لعبّارات أمن الإنترنت تعطيل المحتويات التالية:

- أغراض من نوع ActiveX
- البرمجيات الإعلانية Adware والتجسسية Spyware
- الكوكيز
- المرسلات الفورية Instant Messengers
- مشاركة الملفات من نوع ند للند P2P
- استغلال السكريبتات
- الهجمات باستخدام رمازات TCP/IP خبيثة

كشف وتجنب التسلل Intrusion Detection and Prevention

يمكن الدفاع عن الشبكات بشكل فاعل Active أو بشكل سلبي Passive. الدفاع السلبي مثل استخدام جدار النار لتعطيل الهجمات على أساس القواعد الموضوعة أو الإعدادات الأمنية أو استخدام مصفي وب لتعطيل المواقع الخبيثة بينما الدفاع الفاعل مثل استخدام نظام كشف التسلل فهو قادر على كشف الهجوم أثناء وقوعه.

يمكن لأنظمة كشف التسلل استخدام منهجيات مختلفة لمراقبة الهجمات كما يمكن إعداد نظام كشف التسلل على مضيف محلي أو على الشبكة.

منهجيات المراقبة. تقتضي المراقبة اختبار حركات المرور الشبكية والنشاطات والسلوك لكشف حالات الشذوذ الأمنية. هناك أربع منهجيات مراقبة: المراقبة المعتمدة على الشذوذ والمراقبة المعتمدة على التوقيع والمراقبة المعتمدة على السلوك والمراقبة الإرشادية.

يجري تصميم المراقبة المعتمدة على الشذوذ Anomaly-based monitoring لكشف الشذوذ الإحصائي. يتم أولاً بناء خط أساس Baseline للنشاطات العادية خلال وقت محدد. عندما يلاحَظ انحراف كبير عن خط الأساس يجري تشغيل الإنذار أو التحذير المناسبين. من ميزات هذه المنهجية أنها تستطيع كشف الشذوذ بسرعة ودون الحاجة لمعرفة أسبابه. لكن هذه المنهجية تبقى عرضةً للإنذارات الخاطئة False Positives أي تلك الإنذارات التي تحدث دون وجود مبرر لها وذلك لأن النشاطات الطبيعية يمكن أن تتغير بسرعة أو مع مرور

الزمن. إضافةً إلى الإنذارات الخاطئة، يمكن أن تسبب هذه المنهجية حمل معالجة كبير على النظام الذي يشغلها. أخيراً، بما أن هذه المنهجية تعتمد على بناء خط أساس، فهي تبقى عرضةً للهجمات طالما خط الأساس لم ينجز بعد.

أما المنهجية المعتمدة على التوقيع Signature-based monitoring (بصمة خاصة بكل هجوم) فتعتمد على التدقيق في حركات مرور الشبكة والنشاطات المختلفة والاتصالات والبحث عن نماذج معروفة وذلك بشكل قريب من آلية عمل مضادات الفيروسات. تتطلب هذه المنهجية النفاذ إلى قواعد معطيات للتواقيع محدثة بشكل متواصل إضافة إلى تعريف آلية المقارنة المطلوبة لاكتشاف التسلل. من سيئات هذه المنهجية كون قواعد معطيات التواقيع تزداد باستمرار وأن تعديل صغير في الهجوم يجعل توقيعه السابق غير مفيد.

تسعى المراقبة عن طريق السلوك Behavior-based monitoring إلى تجاوز حدود المنهجيتين السابقتين عن طريق العمل بشكل استباقي ومتأقلم عوضاً عن العمل بشكل تفاعلي. تأخذ هذه المنهجية الأعمال والإجرائيات العادية كقياس. تحلل هذه المنهجية الإجراءات والتطبيقات التي تعمل ضمن نظام ما بشكل متواصل وتحذر المستخدم عند اكتشاف أي فعل غير طبيعي ويقوم المستخدم بتعطيل أو بالسماح بهذا الفعل. لا نحتاج هنا إلى تحديث قواعد معطيات التواقيع باستمرار أو بناء خط أساس إحصائي قبل البدء بالمراقبة. يفيد أيضاً هذا النوع من المراقبة في كشف الهجمات الحديثة.

تستند المراقبة الإرشادية Heuristic monitoring على تقنيات معتمدة على الخبرات Experience-based techniques. تحاول الإجابة على السؤال التالي: هل ستفعل هذه شيئاً ضاراً إذا سُمح لها بالتنفيذ؟ تستخدم هذه المنهجية خوارزمية لتحديد وجود تهديد.

أنواع أنظمة كشف التسلل

يوجد نوعان رئيسيان لأنظمة كشف التسلل وهما المضيف HIDS والشبكي NIDS. النظام المضيف HIDS هو تطبيق برمجي يعمل على مضيف محلي يستطيع كشف الهجوم أثناء حدوثه. يجري تنصيب المضيف عند كل حاسب مطلوب حمايته سواء كان مكتبي أو مخدم. يعتمد المضيف على عملاء Agents مثبتة على النظام المطلوب حمايته. تعمل هذه العملاء بشكل وثيق مع نظام التشغيل لمراقبة واعتراض الطلبات في سبيل تجنب الهجمات. تراقب HIDS عادةً الوظائف التالية:

- استدعاءات النظام System calls. استدعاء النظام هو تعليمة تقاطع البرنامج قيد التنفيذ وتطلب خدمة من نظام التشغيل.
- النفاذ إلى نظام الملفات File System access. يتأكد أن جميع استدعاءات طلب فتح الملفات هي شرعية وليست نتيجة نشاطات خبيثة.
- إعدادات تسجيلات النظام System Registry settings. يراقب HIDS سجلات نظام Windows التي تحوي معلومات التكوينات المتعلقة بالبرامج والحاسب ويتعرف على أي تعديل غير مسموح به.
- دخل/خرج المضيف Host input/output. يراقب HIDS كل اتصالات الدخل والخرج بحثاً عن أي نشاط خبيث. فمثلا، إذا كان نظام ما لا يستخدم الرسائل الفورية، وفي لحظة ما حاول النظام اتصال IM فإن HIDS سيكشف هذا الخطر على أنه نشاط شاذ.

نذكر من سيئات HIDS أنه غير قادر على مراقبة حركات المرور الشبكية غير الموجهة للنظام المراقب وأنه يخزن جميع سجلات الأثر Log file بشكل محلي كما أنه يسبب ضغط كبير على الموارد المحلية الأمر الذي يسبب ببطء النظام.

على الجانب الآخر، يراقب نظام كشف التسلل الشبكي NIDS الهجمات على الشبكة. يجري هنا وضع حساسات Sensors على بعض التجهيزات الشبكية مثل المسيرات أو جدران النار لتجميع المعلومات عن حركات المرور الشبكية وتوليد التقارير عنها وإرسالها إلى جهاز مركزي.

نذكر من التقنيات التي يمكن أن يستخدمها NIDS:

- التحقق من مكدس البروتوكولات Protocol stack verification عن طريق كشف طرود IP, TCP, UDP, ICMP غير النظامية
- التحقق من بروتوكولات التطبيقات Application protocol verification عن طريق التحقق من بعض سلوكيات البروتوكولات غير الصحيحة
- خلق سجلات موسعة Create extended logs عن طريق تسجيل الأحداث غير العادية بغية تمريرها لمحلل التسجيلات.

ما أن يتم كشف الهجوم، يمكن لنظام NDIS التصرف بطرق مختلفة. يقوم النظام السلبي passive NDIS بتشغيل إنذار وتسجيل الحدث ضمن Log. يمكن أن يشمل الإنذار إرسال بريد الكتروني أو رسالة SMS لمدير الشبكة أو قرع إنذار صوتي. أما النظام الفاعل active NIDS فيقوم إضافة إلى ما سبق بفعل ما. يمكن أن يتمثل الفعل في إعادة تشكيل جدار النار لتعطيل الطرود القادمة من عنوان إنترنت محدد أو تشغيل برنامج آخر لمعالجة الحادث أو انهاء جلسة TCP.

يمكننا اعتبار أن نظام تجنب التسلل الشبكي NIPS مشابه لنظام كشف تسلل شبكي فاعل من حيث كشف الهجوم واتخاذ ما يلزم لتعطيله. لكن الفارق الرئيسي بينهما هو مكان التواجد. فنظام NIDS يملك حساسات تراقب حركات المرور الداخلة والخارجة من جدار النار وتبلغ جهاز مركزي للتحليل. أما نظام NIPS فهو يوجد في نسق جدار النار نفسه الأمر الذي يسمح له بالقيام بفعل سريع لتعطيل الهجوم.

أدوات أمن شبكات من نوع الكل في واحد

بما أن أجهزة حماية الشبكات متنوعة ومن الصعوبة بمكان تشغيلها جميعاً في شبكة واحدة لذلك ظهرت أدوات أمن شبكات من نوع الكل في واحد. تسعى هذه الأدوات لتأمين طيف واسع من الحماية الأمنية للشبكات في أداة واحدة. كما يمكننا أيضاً دمج هذه الأدوات ضمن بعض أنواع الأجهزة الشبكية كالمبدلات أو المسيرات التي تعالج جميع الطرود المارة بالشبكة للحصول على ما يعرف بالأمن الشبكي المتكامل.

2. الأمن من خلال تقانات الشبكات

يمكننا أيضاً تأمين الشبكة عن طريق التقانات الشبكية. من هذه التقانات ترجمة عناوين الشبكة Network Address Translation (NAT) والتحكم بالنفاذ الشبكي Network Access Control (NAC).

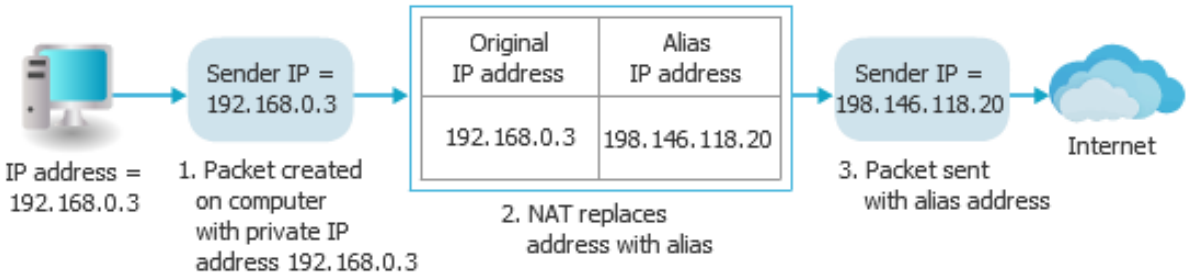
1.2. ترجمة عناوين الشبكة NAT

تسمح تقانة ترجمة عناوين الإنترنت إلى استخدام عناوين خاصة للنفاذ إلى الإنترنت. عناوين الإنترنت الخاصة كما هو موضح في الشكل التالي هي مجموعة من العناوين غير المخصصة لأي مستخدم أو مؤسسة ويمكن أن يستخدمها أيٍ كان في الشبكات الخاصة. تعمل العناوين الخاصة مثلها مثل العناوين الاعتيادية ضمن الشبكات الداخلية لكن إذا حصل وخرج طرد منها إلى الإنترنت فإن المسيرات تستبعدها.

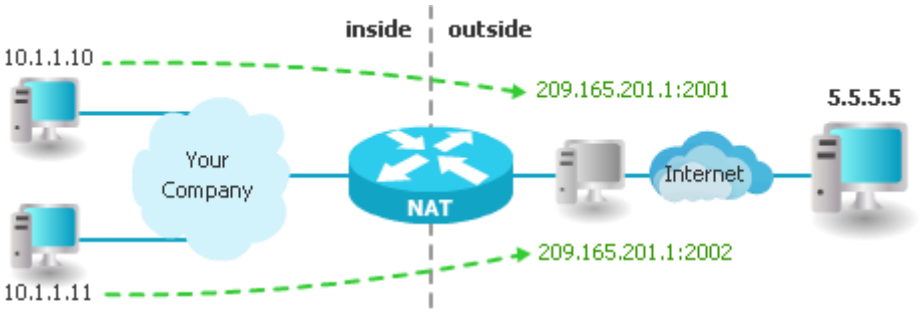
Class	Beginning address	Ending address	Number of addresses
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

الجدول 3: عناوين IP الخاصة

عند خروج طرد ما من الشبكة الخاصة، يقوم جهاز NAT باستبدال عنوان الإنترنت الخاص بالمصدر بعنوان عام Public IP address كما هو موضح في الشكل التالي. يحافظ برنامج NAT على جدول مقابلة بين العناوين الخاصة وتلك العامة. عندما يستقبل برنامج NAT طرداً ما يقلب العملية ويضع العنوان الخاص بدلاً عن العنوان العام. يمكن أيضاً استخدام Port Address Translation (PAT) كأحد أشكال الترجمة (الشكل 10)، فبدلاً عن تخصيص عنوان عام لكل عنوان خاص، يجري هنا استخدام عنوان IP عام وحيد لكن مع رقم بوابة TCP مصدر مختلفة TCP Source Port. هذا يسمح باستخدام عنوان عام وحيد لمجموعة مستخدمين في الوقت نفسه.



الشكل 9: ترجمة عناوين الشبكة NAT



PAT table:

	inside local		inside global		outside global	
proto	addr	prot	addr	proo	addr	prot
TCP	10.1.1.10	3001	209.165.201.1	2001	5.5.5.5	80
TCP	10.1.1.11	4003	209.165.201.1	2002	5.5.5.5	25

الشكل 10: PAT

تمتلك تقانة NAT ميزتين. أولاً، تخفي العناوين الداخلية للشبكة وثانياً، تسمح لمجموعة من الأجهزة باستخدام عنوان IP عام وحيد.

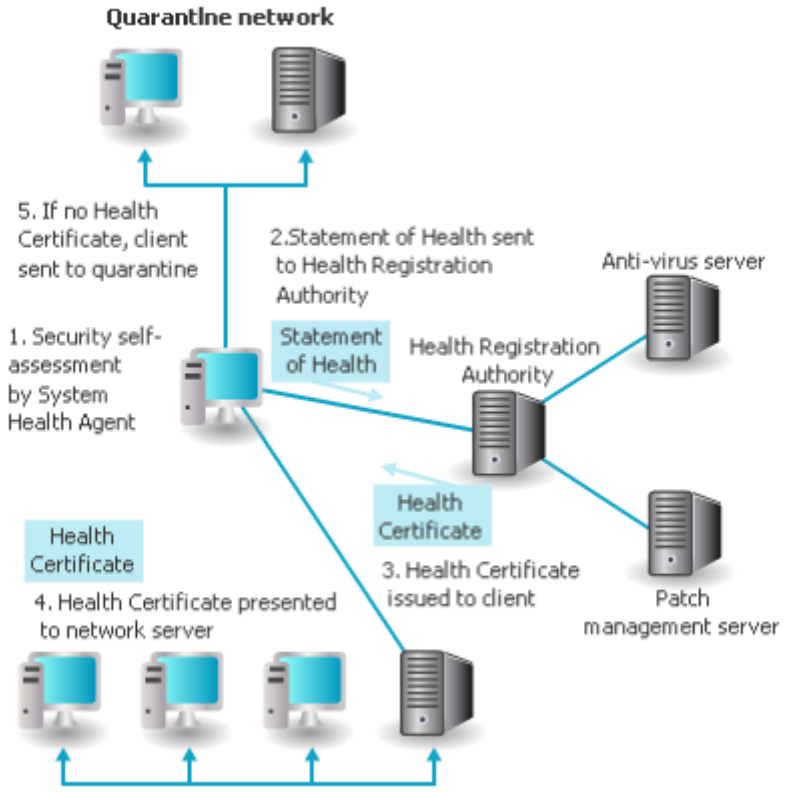
2.2. التحكم بالنفاذ الشبكي NAC

عند استخدام التحكم بالنفاذ الشبكي يجري فحص حالة أي نظام أو جهاز شبكي قبل السماح له بالانضمام إلى الشبكة. أي جهاز يفشل في تحقيق مجموعة محددة من الضوابط، كشرط احتوائه على برنامج مضاد للفيروسات مجهز بأخر تحديث لقاعدة المعطيات أو على جدار ناري برمجي مفعل، يسمح له فقط بالاتصال بشبكة خاصة (حجر quarantine) لتصحيح أماكن العيوب الأمنية. بعد تصحيح هذه العيوب يسمح للجهاز بالانضمام إلى الشبكة العادية. تهدف هذه العملية إلى منع أي جهاز غير آمن من نقل العدوى إلى بقية الأجهزة عبر الشبكة.

يبين الشكل 11 مثالاً عن عملية تحكم بالنفاذ الشبكي باستخدام مصطلحات حماية النفاذ الشبكي لمايكروسوفت:

1. ينفذ الزبون تقدير ذاتي باستخدام عميل صحة النظام System Health Agent (SHA) لتحديد مدى إمكانية إصابته.
2. يُرسل التقدير، المعروف باسم بيان الصحة Statement of Health، إلى مخدم، يعرف باسم سلطة تسجيل الصحة Health Registration Authority (HLA). يفرض هذا المخدم السياسات الأمنية للشبكة كما يتكامل مع بعض السلطات الخارجية مثل مخدمات مضادات الفيروسات وإدارة التصحيحات Patches في سبيل استخلاص معلومات التكوين الحالية.
3. إذا تمت الموافقة على الزبون من قبل HRA، يصدر له شهادة صحية Health Certificate.
4. تقدم الشهادة الصحية لمخدمات الشبكة لإثبات أنه تمت الموافقة على الشروط الأمنية للزبون
5. إذا لم تتم الموافقة على الزبون، يتم ربطه مع شبكة حجر لتصحيح العيوب الأمنية الموجودة عنده ومن ثم الربط إلى الشبكة.

تستخدم NAC إحدى طريقتين لتوجيه الزبون إلى شبكة الحجر أولاً ثم إلى شبكة الإنتاج. تتمثل الطريقة الأولى في استخدام مخدم بروتوكول تكوين المضيف الديناميكي Dynamic Host Configuration Protocol (DHCP). يمنح الزبون عنوان تابع لشبكة الحجر أولاً ثم بعد تصحيح العيوب يمنح عنواناً يتبع لشبكة الإنتاج. أما في الطريقة الثانية فتستخدم طريقة يتبعها المهاجمين وهي تسميم ARP. يتم هنا التلاعب بجدول ARP ضمن حاسوب الزبون ليتم ربطه مع شبكة الحجر.



الشكل 11: منصة عمل التحكم بالنفاذ الشبكي

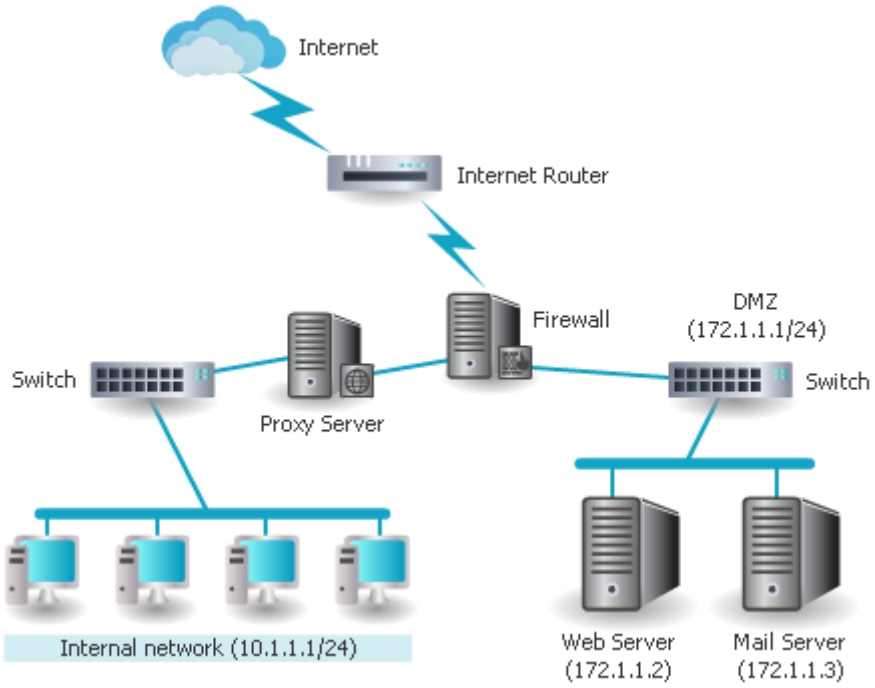
3. الأمن من خلال عناصر تصميم الشبكة

يمكن أن توفر عناصر تصميم الشبكة أساساً آمناً لمقاومة المهاجمين. تشمل هذه العناصر على خلق منطقة منزوعة السلاح DMZ وتجزئة الشبكات واستخدام الشبكات المحلية الافتراضية والنفاذ البعيد.

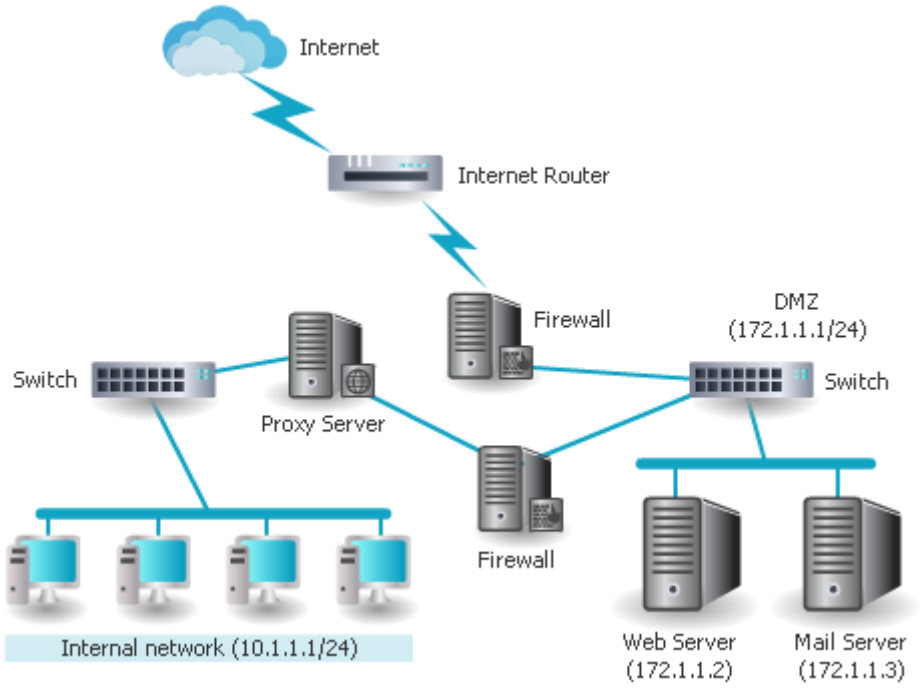
1.3. المنطقة منزوعة السلاح Demilitarized Zone (DMZ)

يستخدم مصممو الشبكات مفهوم DMZ في سبيل السماح للمستثمرين الخارجيين غير الموثوقين بالنفاذ إلى بعض الموارد مثل موقع الوب أو مخدم البريد الالكتروني. تعمل منطقة DMZ كشبكة مستقلة توضع خارج محيط الشبكة الداخلية المحمية؛ يستطيع المستثمرون الخارجيون غير الموثوقين النفاذ إلى شبكة DMZ فقط دون إمكانية النفاذ إلى الشبكة الداخلية المحمية.

يوضح الشكل 12 منطقة DMZ تحوي مخدم وب ومخدم بريد الكتروني قابلين للوصول من الزبائن الخارجية. يجري، ضمن هذا التكوين، استخدام جدار نار واحد مزود بثلاث واجهات شبكية: واجهة مع الإنترنت وثانية مع الشبكة الداخلية والثالثة مع منطقة DMZ. يجعل هذا التكوين جدار النار نقطة تعطل وحيدة في الشبكة. إذا أردنا تحقيق تصميم أكثر أمناً وموثوقية يمكننا استخدام جداري نار كما هو موضح في الشكل 13 حيث يحتاج المهاجم إلى اختراق جداري نار للوصول إلى الشبكة الداخلية.



الشكل 12: منطقة DMZ بجدار نار وحيد



الشكل 13: منطقة DMZ بجداري نار

2.3. تجزئة الشبكات Subnetting

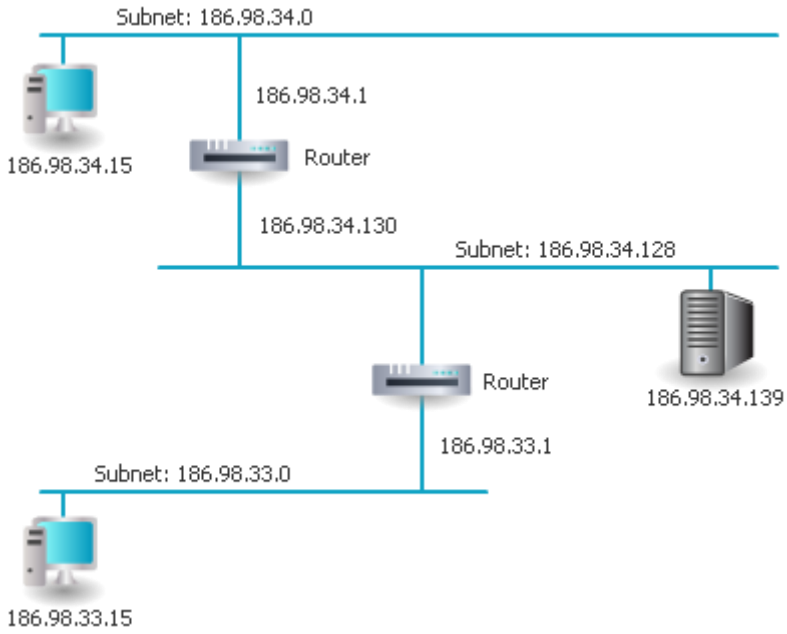
تستخدم الإنترنت عناوين IP مكونة من 32 بت. يتألف عنوان IP من جزأين: جزء خاص برقم الشبكة NetID وجزء خاص برقم الحاسوب ضمن الشبكة HostID. فمثلاً، يكون معرف الشبكة في العنوان 192.168.1.23 هو الجزء 192.168.1 بينما معرف الحاسب يكون الجزء 23. هذا التقسيم بين أرقام الحواسيب وأرقام الشبكات كان يتم عادةً على الحدود بين البايتات (أي يكون كل جزء من مضاعفات البايت) وهو ما يعرف بالعنونة الصفية Classful addressing. تم، في عام 1985، إدخال تقنيان محسنة للعنونة سمحت بتجزئة عنوان IP في أي مكان ضمن 32 بت. تعرف هذه التقنية بتجزئة الشبكات Subnetting أو Subnet address. عند استخدام التجزئة، يصبح عنوان IP مؤلفاً من ثلاثة أقسام: شبكة وشبكة جزئية ومضيف. يمكن لشبكة ما أن تحوي عدة شبكات جزئية وكل شبكة جزئية تتصل بمسير مختلف وتحوي عدة مضيفين. يبين الجدول التالي بعض فوائد التجزئة.

الفائدة	الشرح
تقليل حركة المرور	يجري التعميم داخل الشبكات الجزئية فقط
المرونة	التحكم بعدد الشبكات الجزئية والمضيفين في كل شبكة مع إمكانية التعديل لاحقاً
تحسين استخدام العناوين	تخفيض العناوين المهدورة
تأثير ضئيل على المسيرات الخارجية	لا تحتاج المسيرات الواقعة خارج المؤسسة لتحديث معلوماتها عند تجزئة الشبكة وذلك لأنه فقط المسيرات الداخلية الموصولة مباشرة إلى هذه الشبكات الجزئية تحتاج إلى معلومات التجزئة
انعكاس الشبكات الفيزيائية	يمكن تشكيل الشبكات الجزئية بطريقة تعكس علاقة التجاور الفيزيائي

الجدول 4: فوائد تجزئة الشبكات

يمكن للتجزئة أن تحسن أمن الشبكات أيضاً وذلك لأننا نضع كل مجموعة من الحواسب ضمن شبكة جزئية معزولة عن غيرها. يستطيع مدير النظام تحديد من يحق له النفاذ إلى أي شبكة جزئية. وبما أن كل جهاز يعرف الشبكة الجزئية التي ينتمي لها ويعرف أرقام الشبكات الجزئية الأخرى فيمكن لهذا الجهاز أن يعرف من عنوان المصدر إلى أي شبكة جزئية ينتمي المرسل وإذا كان العنوان خارجياً فيمكن توقع أن يكون مهاجماً. يبين الشكل التالي مثالاً عن تجزئة الشبكات.

تفيد أيضاً تجزئة الشبكات في إخفاء البنية الداخلية وطريقة تقسيم الشبكات عن الخارج الأمر الذي يصعب مهمة المخترق.



الشكل 14: مثال عن تجزئة الشكات

3.3. الشبكات المحلية الافتراضية VLANs

تسمح المبدلات المستخدمة في الشبكات المحلية بتقطيع الشبكة إلى مجموعات منطقية تعرف باسم شبكات محلية افتراضية VLANs. تسمح هذه الطريقة بتجميع مجموعة من المستخدمين المتناثرين حول الشبكة منطقياً مع بعضهم حتى ولو كان كل منهم متصل مع مبدلة مختلفة. هذا من شأنه تقليل حركة المرور الشبكية وتزويد درجة من الأمن مشابهة لما تزوده تجزئة الشبكات؛ تكون الشبكات المحلية الافتراضية معزولة عن بعضها وتناقل المعلومات الحساسة محدود بشبكة افتراضية الأمر الذي يحسن الأمن.

يتم تبادل الطرود ضمن شبكات VLANS بطريقتين. في حال كون المرسل والمستقبل موصولين على المبدلة نفسها فإن المبدلة تؤمن عملية تبادل الطرود بين الأجهزة التي تنتمي لشبكة افتراضية واحدة. أما في حال كون المرسل والمستقبل غير موصولين على المبدلة نفسها، فيجري استخدام بروتوكول وسم خاص الذي يمكن أن يكون مملوك من قبل شركة ما أو معياري مثل البروتوكول IEEE 802.1Q. يضيف هذا الأخير سمة (حقل بطول 16 بت) إلى الإطار تحمل رقم الشبكة الافتراضية للمرسل.

لا يمكن الاتصال بين جهازين ينتميان إلى شبكتين مختلفتين دون المرور ضمن مسير يحقق التسيير بين الشبكات الافتراضية.

4.3. النفاذ عن بعد Remote access

شاع مؤخراً نفاذ المستثمرين إلى شبكاتهم المحلية عن بعد. فالبعض يؤدي عمله من المنزل مباشرةً والبعض الآخر يسافر للقاء الزبائن البعيدة مثل مندوبي المبيعات أو الأشخاص الذين يكونون بعيدين عن مكاتبهم لحضور مؤتمر ما. تؤمن المؤسسات عادةً إمكانية نفاذ هؤلاء عن بعد إلى الموارد المحلية كما لو أنهم يتصلون بشكل مباشر من مكاتبهم. من الأهمية بمكان تأمين هذا النوع من الاتصالات وخاصة كون وصلات الاتصال وتجهيزاتها غير مدارين أو محميين من قبل المؤسسة.

يقصد بالنفاذ عن بعد استخدام أي نوع من التجهيزات والبرمجيات بغرض تمكين مستثمر بعيد من النفاذ إلى شبكة داخلية محلية. عادةً يجري استخدام تقنيات VPN لمنح المستخدمين البعيدين الوظائف والصلاحيات الموجودة على الشبكة الداخلية.

4. تمارين عملية

تنصيب SoftEther VPN Client

1. Go to the URL: www.vpngate.net/en/download.aspx
2. Download and install SoftEther VPN Client + VPN Gate Client Plugin
3. During installation and when prompted, Select " SoftEther VPN Client" and press next
4. Launch SoftEther VPN Client
5. If you access the Internet through proxy server, type Proxy settings and enter required information
6. Double-click VPN Gate Public VPN Servers
7. Follow the instruction until you have a valid Tunnel with the selected VPN server
8. Go to cmd and type ipconfig /all | more and verify that you have been assigned a new IP address

الفصل السادس: إدارة شبكة آمنة
Administering a Secure Network

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- التعرف على وظائف بروتوكولات الشبكات الشائعة
- فهم كيف يمكن تطبيق مبادئ إدارة الشبكة
- تعرف أنواع جديدة من تطبيقات الشبكات وطرق تحقيق آمنها

مع أن التصميم الجيد للشبكة واستخدام التقانات والأجهزة المناسبة، التي تعلمناها في الفصل السابق، هما من الخطوات المطلوبة لحماية المعلومات غير أنها غير كافية إذ نحتاج أيضاً إلى إدارة الشبكة بشكل سليم لصونها من الهجمات. نحتاج هنا إلى تحقيق إجراءات إدارية صارمة.

1. بروتوكولات الشبكات الشائعة

1.1. بروتوكول إيثرنت Ethernet Protocol

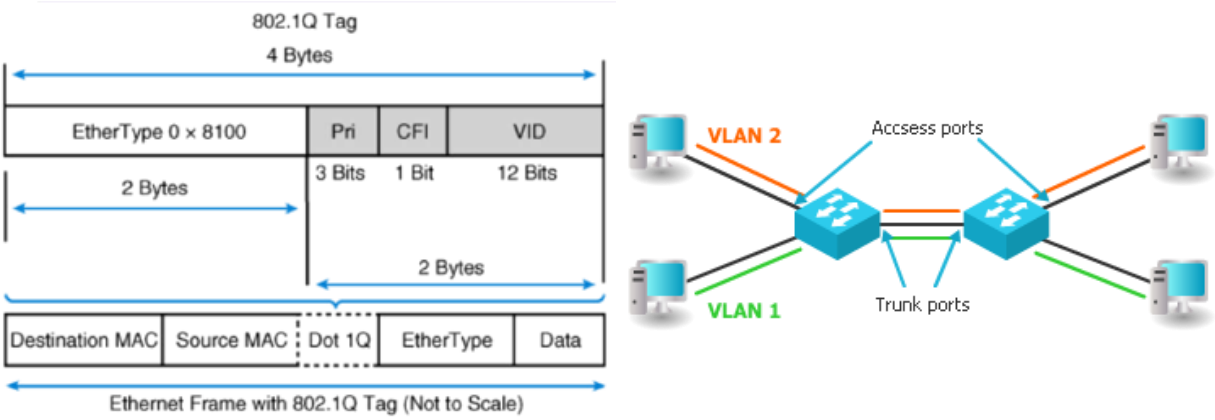
تعتبر شبكة إيثرنت الشبكة المهيمنة على عالم الشبكات السلكية بعد خروج معظم الشبكات الأخرى مثل Token Ring و النقل غير المتزامن ATM من الخدمة.

تعرّف شبكة إيثرنت طيف واسع من التقنيات: منها ما يتعلق بوسائط النقل الفيزيائية ومنها ما يتعلق بالتحكم بوسيط النقل MAC عن طريق استخدام بروتوكول التنصت على الحامل والنفاذ المتعدد مع كشف التصادمات CSMA/CD ومنها ما يتعلق بتحديد صيغة الإطار والحقول المؤلفة له أو الأجهزة المستخدمة (مجمعة أو مبدلة) إضافةً إلى تحديد آليات توجيه الأطر وبروتوكول شجرة التغطية والعنونة.

الشبكات المحلية الافتراضية VLANs

رأينا سابقاً كيف يمكن تقسيم الشبكة إلى عدة شبكات جزئية (مجموعات منطقية) بغية عزل حركات المرور على المستوى الثاني. يعطى لكل شبكة جزئية وسم tag خاص بها وتقوم المبدلات بتوجيه الأطر إلى الشبكات الجزئية حسب الوسم الموجود في كل إطار.

يجري تحقيق الشبكات الافتراضية، حسب المعيار 802.1Q، من خلال إضافة مجموعة من الحقول طولها 4 بايتات وأهمها معرف الشبكة الافتراضية VID المكون من 12–bit كما هو موضح في الشكل التالي.



الشكل 1: وسم أطر VLANS وفق المعيار 802.1Q

يجب هنا تعريف بوابات كل مبدلة كبوابة نفاذ Access port أو كبوابة جذع Trunk port:

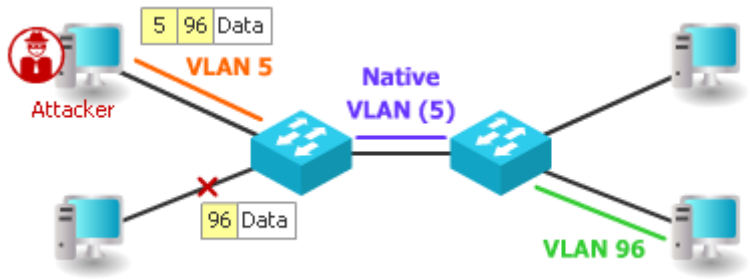
- تضيف بوابات النفاذ الوسوم إلى الأطر
- تمزج البوابات الجذعية مجموعة شبكات افتراضية مع بعضها.

يمكن، في حال تجاوز عدد الشبكات الافتراضية القيمة 4096، استخدام المعيار 802.1ad (QinQ) الذي يسمح بتكديس وسوم الشبكات الافتراضية.

يسمح معيار 802.1Q بنقل الأطر مع أو بدون وسم على البوابات الجذعية وذلك عن طريق اعتبار كل إطار بدون وسم ينتمي إلى الشبكة الافتراضية الأصلية Native VLAN.

الهجمات على الشبكات المحلية الافتراضية VLANs

- القفز بين الشبكات الافتراضية VLAN hopping. يهدف هذا الهجوم إلى خداع المبدلات لتوجيه طرود المهاجم إلى الشبكة الافتراضية الخاطئة إما بسبب الضبط الخاطئ للمبدلات خاصةً مع وجود الشبكة الافتراضية الأصلية.
- القفز بين الشبكات المتداخل Nested VLAN hopping (Tag stack). يضيف المهاجم وسم آخر موجه إلى شبكة داخلية (96) فوق وسم الشبكة الأصلية (5). عندما يصل الطرد إلى المبدلة الأولى تحذف أول وسم (5) وترسل الإطار إلى البوابة الجذع. تلاحظ المبدلة الثانية أن الوسم هو (96) فتوجه الإطار إلى الحاسب الموصول إلى الشبكة (96) كما هو موضح في الشكل التالي.



الشكل 2: القفز بين الشبكات المتداخل

يمكن مكافحة هذا الهجوم عن طريق عدم ضم أي بوابة من بوابات المبدلات إلى الشبكة الأصلية Native VLAN وحذف الشبكة الأصلية من البوابة الجذع وفرض على جميع الأطر على البوابات الجذعية أن تحمل وسم.

- بروتوكول التجذيع الديناميكي Dynamic Trunking Protocol (DTP). DTP هو بروتوكول لأتمتة بعض إعدادات التحكم بالشبكات الافتراضية مثل إنشاء بوابة جذع بين مبدلتين والتفاوض على المتحولات المطلوبة مثل نوع التغليف ونظام أرقام الشبكات الافتراضية. يمكن أن يستغل المهاجم هذا البروتوكول عن طريق إرسال طرود DTP إلى المبدلة وخداعه لينضم إلى شبكة افتراضية ما. يجب هنا عدم ترك بوابات المبدلات المواجهة للمستخدمين بنمط الضبط الديناميكي.

- بروتوكول تجذيع الشبكات الافتراضية VLAN Trunk Protocol (VTP). يقوم هذا البروتوكول بنشر معلومات إعدادات الشبكات الافتراضية من مبدلة إلى بقية المبدلات الأمر الذي من شأنه عدم تكرار الإعدادات نفسها على جميع المبدلات. يمكن للمهاجم أن يتلاعب بمحتويات طرود VTP لحذف شبكة ما (حجب خدمة) أو إضافة شبكة افتراضية على جميع المبدلات (إغراق المبدلات).

بروتوكول شجرة التغطية Spanning Tree Protocol (STP)

حتى يعمل التوجيه في شبكة إيثرنت بكفاءة يجب أن لا تحوي طبولوجيا الشبكة على حلقات. يهدف بروتوكول STP الذي يعمل بين المبدلات إلى تحويل الطبولوجيا إلى شجرة خالية من الحلقات. يقوم البروتوكول أولاً بانتخاب جذر للشجرة (المبدلة ذات أدنى رقم معرف وفي حال التعادل أقل رقم عنوان MAC). يقوم الجذر بحساب شجرة أقصر الطرق إلى بقية المبدلات (الجسور حسب المعيار). تقوم كل مبدلة بتعطيل البوابات البعيدة عن الجذر(أي التي لا تنتمي إلى شجرة أقصر الطرق).

يعتبر بروتوكول STP عرضة للهجمات التالية:

- تولي مهام الجسر الجذر root bridge. يرسل المهاجم طرود Bridge Protocol Data Unit (BPDU) بأدنى قيمة (32767) ويختار عنوان MAC ذو قيمة دنيا أيضاً الأمر الذي سيمح بانتخابه جذراً. يستطيع المهاجم بعد أن يصبح جذراً التحكم بحركات المرور أو اعتراضها (رجل في المنتصف). يوجد طريقتين لمعالجة هذا الهجوم: حراسة الجذر root guard وحراسة طرود BPDU على المبدلات.
- إغراق المبدلات بطرود BPDUs. الأمر الذي يسبب زيادة عبء المعالجة عند المبدلات وبالتالي حجب الخدمة.

التعلم الذاتي في المبدلات Switch Learning

تتعلم المبدلة من حركة الأطر التي تستقبلها عناوين MAC للأجهزة الموصولة معها. يفيد ذلك في بناء جدول توجيه خاص بها يقابل عنوان MAC مع البوابة التي تصل إلى هذا العنوان. يوجد نوعين من الهجمات على جدول التوجيه: إغراق MAC وخداع MAC. عندما تمتلئ ذاكرة RAM الخاصة بجدول التوجيه فتقوم بعض أنواع المبدلات بكتابة العناوين الجديدة مكان القديمة. يقوم المهاجم بتوليد عدد كبير من الطرود بعناوين MAC غير موجودة الأمر الذي يغرق ذاكرة المبدلة ويحولها إلى مجمعة (لأن جميع العناوين المخزنة تصبح غير صالحة). تعمم المجمعة جميع الطرود مما ينعكس سلباً على الأداء وعلى الخصوصية.

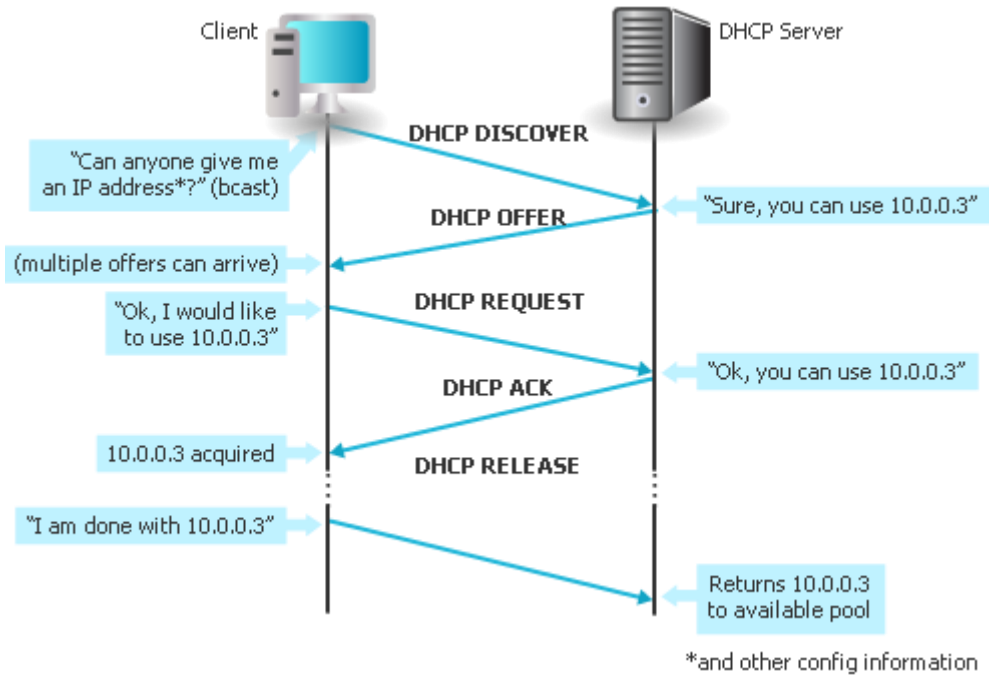
أما هجوم خداع عناوين MAC Spoofing فيتم من خلال استخدام عنوان فيزيائي MAC لمضيف آخر الأمر الذي يحجب الخدمة عن الضحية ويحول حركة المرور إلى المهاجم الذي يتجاوز جميع القيود الموضوعة على أساس عنوان MAC.

يمكن صد هذا النوع من الهجمات عن طريق إعداد المبدلات لتحذير إداريّ الشبكة عند انتقال عناوين الماك أو عن طريق استخدام أمن البوابات Port Security الذي يربط عنوان الماك ببوابة محددة ولا يقبل أطر من عناوين ماك أخرى أو مراقبة حركات المرور على البوابات وتعطيل البوابات التي تولد عدد من الطرود يتجاوز المحدد له.

2.1. الهجمات على العنونة Attacks on Addressing

بروتوكول ضبط العناوين تلقائياً Dynamic Host Configuration Protocol (DHCP)

يستخدم بروتوكول DHCP لتوزيع عناوين IP وعناوين مخدمات الأسماء وعنوان العبارة الافتراضية للمضيفين. يتنصت الزبون على بوابة UDP رقم 68 بينما يتنصت المخدم على البوابة رقم 67. يتم منح العنوان لفترة محددة Lease time. تتم عملية منح العناوين بعدة خطوات كما هو موضح في الشكل التالي.

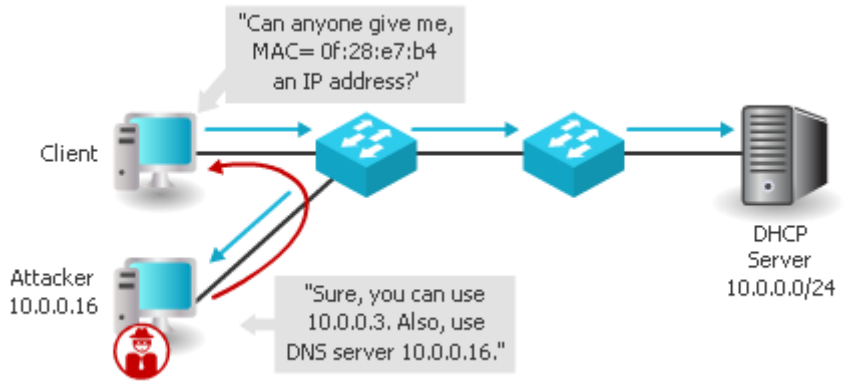


الشكل 3: خطوات عمل DHCP

بما أنه جرى تصميم بروتوكول DHCP دون مراعاة الجوانب الأمنية أو المصادقة فأي مضيف يطلب عنوان يحصل عليه كما أنه لا تجري المصادقة على المخدم نفسه.

ففي هجوم استنفاذ النطاق Scope Exhaustion، يسعى الزبون الخبيث إلى استنفاذ كامل نطاق العناوين عن طريق توليد عدد كبير من طلبات DHCP الأمر الذي من شأنه منع زبون شرعي من الحصول على عنوان IP أي حجب الخدمة عنه.

أما في هجوم مخدم DHCP المزيف Rogue DHCP Server فيقوم المخدم المخادع بتقديم عرض للزبون الأمر الذي يسمح بالتحكم به فيما بعد.

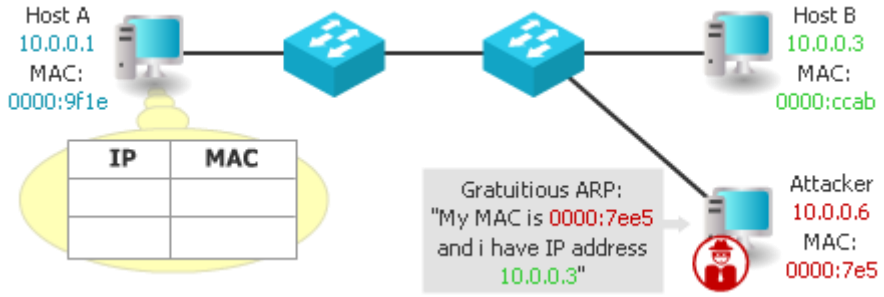


الشكل 4: تزييف مخدم DHCP

يمكن تخفيف أثر هذا الهجوم عن طريق تحديد عدد عناوين MAC لبوابة محددة أو عدم السماح لمضيفين من توليد أنواع محددة من طرود DHCP مثل DHCPOffer و DHCPAck باستخدام جدار نار أو مسير مركزي يتجسس على طرود DHCP ويتعلم الارتباطات MAC–IP.

بروتوكول حل العناوين ARP

يقوم بروتوكول ARP بعملية اقتران بين عنوان IP وعنوان MAC. باستخدام خداع ARP، يمكن للمهاجم إرسال جواب ARP مزيف يحمل عنوان IP للعقدة الضحية الأمر الذي يسمح له باعتراض حركة المرور المتوجهة للضحية وكذلك الأمر بالنسبة للحركة القادمة من الضحية من خلال إعادة الهجوم على المصدر.



الشكل 5: خداع بروتوكول حل العناوينARP Spoofing

يمكن صد هذا الهجوم من خلال منع طرود ARP المجانية Gratuitious ARP أو عن طريق تخزين اقترانات MAC–IP من قبل المبدلات والتي تم تعلمها من طرود ARP وإسقاط الطرود التي لا تحترمها أو باستخدام أنظمة كشف التسلل IDS.

3.1. بروتوكول رسائل التحكم بالإنترنت ICMP

يعتبر بروتوكول Internet Control Message Protocol (ICMP) أحد البروتوكولات الأساسية في TCP/IP. تستخدم الأجهزة ICMP لإرسال معلومات متعلقة بالتحديثات أو بالأخطاء إلى بقية الأجهزة. يستخدم بروتوكول ICMP أيضاً لنقل رسائل الاستفسارات.

تحوي رسالة ICMP 3 حقول:

- النوع Type (8-bit). يعرف الصنف العام لرسالة ICMP. فمثلاً النوع 3 هو مخصص لوجهة غير قابلة للوصول Destination unreachable بينما يخصص النوع 12 لحالة مشكلة موسط Parameter problem. يوجد حالياً 13 قيمة مختلفة لهذا الحقل.
- رماز Code (8-bit). يعطي هذا الحقل معلومات محددة عن حقل النوع. يبين الجدول التالي أهم قيم هذا الحقل المستخدمة مع النوع رقم 3.
- اختبار المجموع Checksum (16-bit). يستخدم هذا الحقل لاختبار تكامل الرسالة.

Type 3 Code value	Description
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
5	Source route failed
6	Destination network unknown
7	Destination host unknown
9	Communication with destination network administratively prohibited
12	Host unreachable for type of service

الجدول 1: قيم الرماز للنوع 3 destination unreachable

يمكن للطالب العودة إلى الملف المرفق ICMP Types and codes لمعرفة جميع الأنواع والرمازات المستخدمة.

تستخدم عدة أنوع من الهجمات بروتوكول ICMP:

- اكتشاف الشبكات Network Discovery. يمكن للمهاجم استخدام ICMP كخطوة أولى من خطوات التعرف لاكتشاف معلومات عن الحواسيب الموجودة ضمن شبكة محددة. يمكن للمهاجم هنا استخدام الأداة ping لإرسال رسالة ICMP echo request لعنوان البث Broadcast للشبكة ومن ثم أرسال طلب من نوع address mask request لحاسب ما لمعرفة قناع الشبكة المستخدم.
- هجوم الحوت لحجب الخدمة Smurf DoS attack. يستطيع المهاجم إرسال رسالة ICMP echo request (ping) لعنوان البث في الشبكة لكن بعد استخدام عنوان الضحية كعنوان مرسل Source address. جميع الأجوبة سترسل إلى الحاسب الضحية الأمر الذي يوقفه عن العمل أو يؤثر على أدائه ووظائفه.
- هجوم إعادة توجيه ICMP. يتم هنا إرسال رسالة من نوع ICMP redirect للضحية تسأل الضحية لتوجيه رسائله عن طريق مسير آخر خبيث أو مستغل من قبل المهاجم.
- Ping of Death. يجري هنا إرسال رسالة ICMP مشوهة تتجاوز طول طرد IP المسموح به إلى الضحية الأمر الذي يؤدي إلى تعطل الحاسب.

4.1. بروتوكول إدارة الشبكات المبسط SNMP

يستخدم بروتوكول إدارة الشبكات المبسط Simple Network Management Protocol (SNMP) من قبل غالبية مصنعي الأجهزة الشبكية وهو بروتوكول شائع جداً لإدارة هذه التجهيزات. فهو يسمح لمدير الشبكة بإدارة ومراقبة وإعداد التجهيزات الشبكية وحتى الحاسوبية عن بعد. يعمل SNMP عن طريق تبادل رسائل إدارة بين التجهيزات.

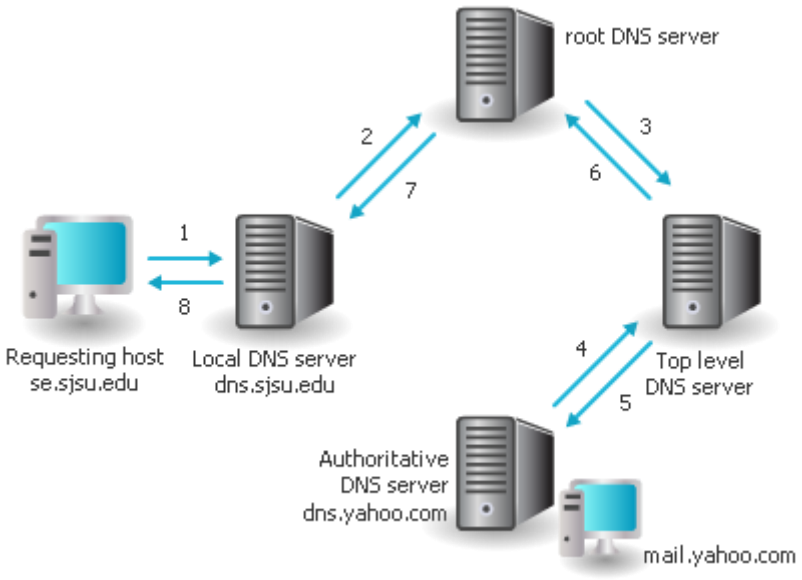
يجب على كل جهاز مُدار أن يعرف وكيل agent أو خدمة تنتظر أوامر محددة ومن ثم تنفذها. تتم حماية هؤلاء الوكلاء عن طريق كلمة مرور تعرف باسم community string تهدف إلى منع المستثمرين غير المصرح لهم من السيطرة على هذه الأجهزة. يوجد نوعان من community string : قراءة فقط تسمح بمشاهدة معلومات من الوكلاء أو قراءة وكتابة تسمح بتغيير إعدادات عند الوكلاء.

يوجد عدة نقاط ضعف أمنية متعلقة باستخدام Community string في الإصدارين الأول والثاني من SNMP. أولاً، القيمة الافتراضية لسلسلة المجتمع كانت هي public في حالة القراءة و private في حالة القراءة والكتابة. فإذا لم يغير مدير الشبكة هذه القيم الافتراضية يكون قد فتح الباب للمهاجمين للسيطرة على أجهزة الشبكة. أيضاً يجري نقل سلسلة المجتمع على الشبكة بدون تسفير الأمر الذي يتيح لمهاجم مزود بمحلل بروتوكولات وموصول على الشبكة معرفة سلاسل المجتمع المستخدمة.

تم عام 1998 إصدار النسخة الثالثة SNMPv3 لتفادي نقاط الضعف هذه عن طريق استخدام اسم مستخدم وكلمة مرور إضافةً إلى التشفير.

5.1. نظام أسماء النطاقات DNS

نظام أسماء النطاقات Domain Name System (DNS) هو بروتوكول مسؤول عن حل (مقابلة) عنوان IP (مثل العنوان 213.78.2.44) إلى اسم مقابل له (www.someplace.com). نظام DNS هو عبارة عن قاعدة معطيات تراتبية أو شجرية تحوي اسم كل موقع على الإنترنت وعنوانه. تقسم قاعدة المعطيات هذه وتوزع على مجموعة من المخدمات الموجودة على الإنترنت، يعتبر كل مخدم مسؤولاً عن منطقة أو عدة مناطق مختلفة من الإنترنت. يبين الشكل التالي خطوات البحث ضمن قاعدة DNS.



الشكل 6: البحث ضمن DNS lookup

يتم البحث عن عنوان الموقع mail.yahoo.com وفق الخطوات التالية:

الخطوة 1. يرسل الحلال resolver الموجود على حاسب الزبون رسالة حل DNS إلى مخدم DNS المحلي المعرف عند الزبون.

الخطوة 2. إذا لم يكن العنوان المطلوب متوفراً في الذاكرة الخابية للمخدم المحلي فإنه يرسل الطلب بدوره إلى المخدم الجذر root server أو إلى المخدم العلوي com. إذا كان يعرف عنوانه.

الخطوة 3. بما أن المخدم الجذر لا يعرف العنوان المطلوب فيوجه الطلب إلى المخدم النطاق العلوي com.

الخطوة 4. بما أن المخدم العلوي com. لا يعرف العنوان المطلوب فيوجه الطلب إلى المخدم المسؤول dns.yahoo.com

(ذو السلطة authoritative)

الخطوة 5. بما أن المخدم dns.yahoo.com هو صاحب السلطة فإنه سيرسل حتماً جواباً إلى المخدم com. يحمل

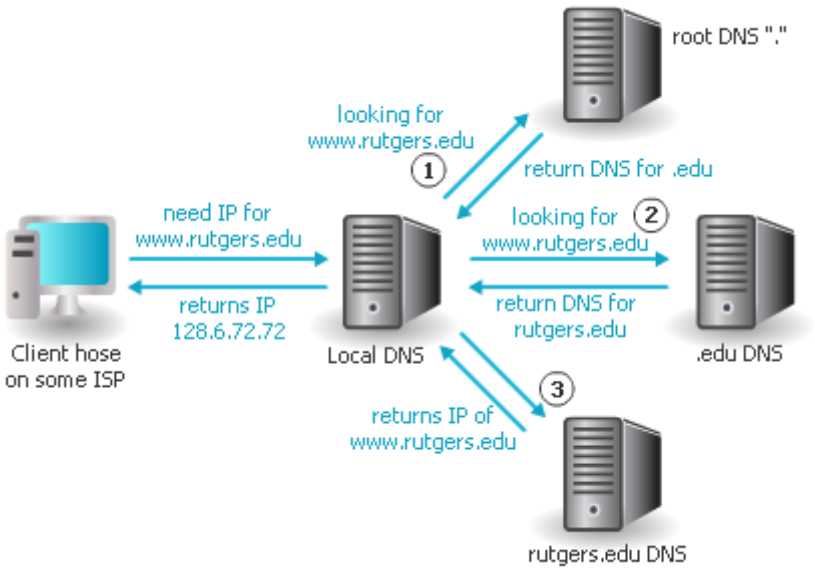
العنوان المطلوب أو رسالة خطأ.

الخطوة 6. يخزن المخدم com. نسخة من الجواب ضمن الخابية ومن ثم يعيد توجيهه إلى المخدم الجذر

الخطوة 7. يخزن المخدم الجذر "." نسخة من الجواب في الخابية ويعيد توجيه الرسالة إلى المخدم المحلي

الخطوة 8. المخدم المحلي بعد تخزين الجواب ضمن الخابية يعيد الجواب إلى الزبون.

يدعى هذا النوع من الحل بالحل العودي recursive وذلك لأن مهمة الاتصال بالمخدم التالي وفق التراتبية تقع على عاتقه. بينما في الحل التكراري Iterative يقوم كل مخدم بإرسال عنوان IP للمخدم التالي وفق التراتبية إلى المخدم المحلي الذي يقوم بالاتصال عوضاً عنه كما هو موضح في الشكل التالي.



الشكل 7: الحل التكراري ضمن DNS

من الهجمات التي يمكن أن تتعرض لها مخدمات DNS، نذكر تسميم DNS حيث يتم تغيير عناوين IP للوجهة بعناوين مزيفة الأمر الذي يسمح بتوجيه حركة المرور إلى العنوان المزيف. لتجنب تسميم مخدمات DNS يجب استخدام الإصدار الأخير من مخدم Berkeley Internet Name Domain (BIND) الذي يتجاهل أي سجل DNS غير متعلق بالاستفسار حصراً. كما يمكن استخدام إصدار آخر من DNS يعرف باسم Domain Name System Security Extensions (DNSSEC) يعتمد على إجراءات متقدمة لتحديد مصداقية المعطيات المستقبلة.

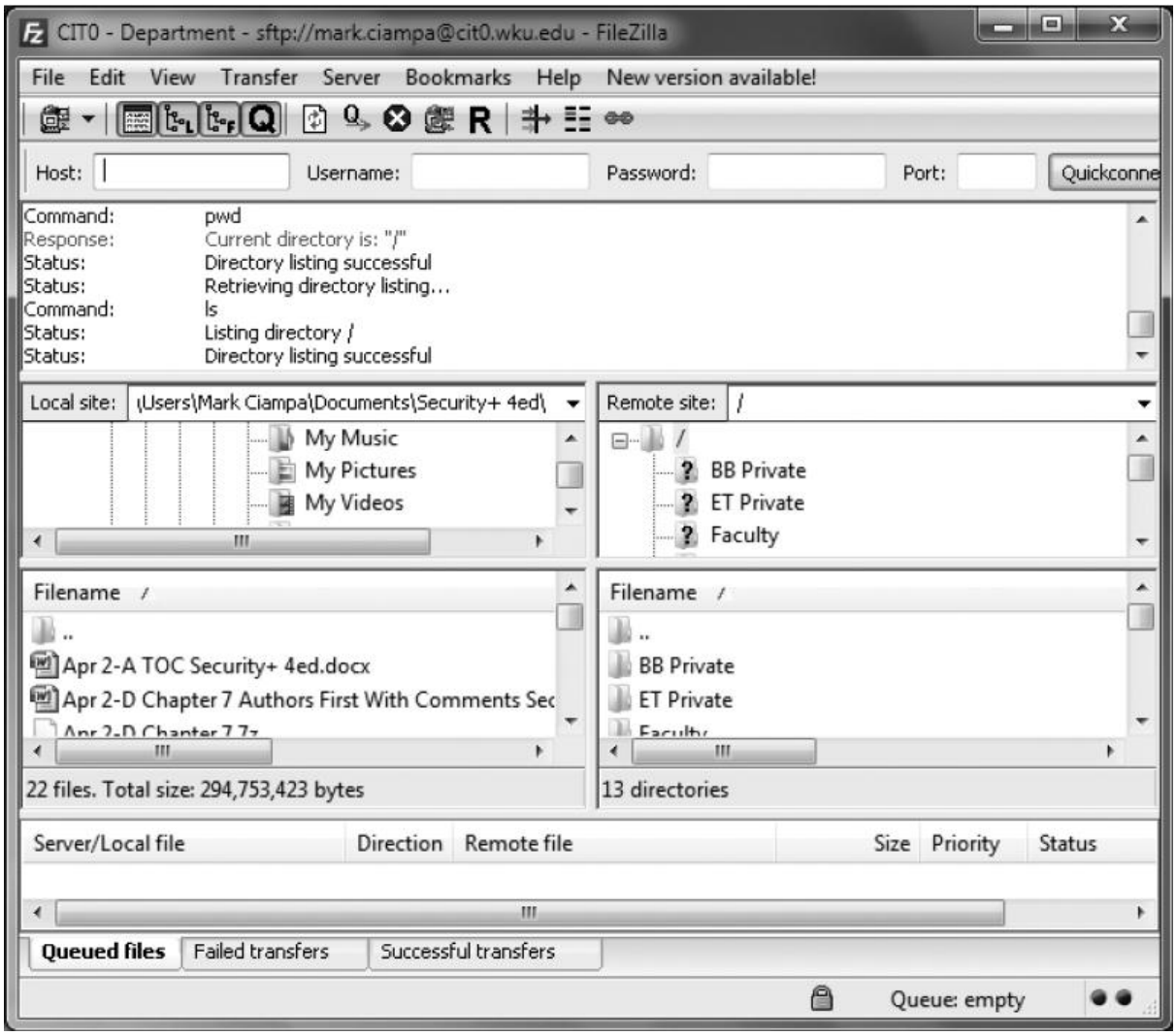
النوع الآخر من الهجمات على DNS هو عكس هجوم التسميم؛ فبدلاً من إرسال نقل منطقة Zone transfer إلى مخدم DNS نظامي، فإن المهاجم يطلب من المخدم النظامي أن يرسل له ملف المنطقة الخاصة به معروفة باسم DNS transfer. هذا يفيد المهاجم في معرفة جميع السجلات الداخلية التي يخدمها مخدم DNS.

6.1. بروتوكولات نقل الملفات

بروتوكول FTP

يستخدم عادةً بروتوكول File Transfer Protocol (FTP) لنقل الملفات بطريقة غير آمنة. يوجد عدة طرق لاستخدام FTP على حاسوب محلي:

- من سطر الأوامر cmd. يجري هنا التعامل مع بروتوكول FTP من سطر الأوامر باستخدام أوامر مثل ls أو get أو put
- باستخدام متصفح وب. عن طريق بدء URL بالسابقة ftp:// بدلاً عن http://
- باستخدام زبون ftp. يمكن هنا تنصيب زبون FTP مستقل يقوم بعرض الملفات المحلية والبعيدة كما هو موضح في الشكل التالي. يمكن سحب وإفلات الملفات بين الموقعين.



الشكل 8: زبون FTP مستقل

يشكل استخدام FTP من خلف جدار نار مجموعة من التحديات. يستخدم FTP بوابتين: بوابة TCP رقم 21 لتبادل أوامر التحكم وبوابة TCP رقم 20 لتبادل المعطيات. في حالة استخدام نمط FTP الفعال Active mode، يقوم الزبون بفتح اتصال تحكم مع المخدم على البوابة 21 ومن ثم يطلب الزبون نقل ملف من المخدم بعد إرسال أمر PORT الذي يحدد رقم البوابة التي يتنصت عليها الزبون لاستقبال الملف. يقوم المخدم بمحاولة فتح اتصال معطيات حيث تكون البوابة المصدر هي 20 والبوابة الوجهة هي التي حددها الزبون. بما أن المبادرة إلى الاتصال تجري من طرف المخدم، فإن جدار النار سيتجاهل هذا الطلب ويتعذر تأسيس اتصال المعطيات مع الزبون. لتجنب هذه المشكلة، يمكن استخدام نمط FTP السلبي FTP Passive mode حيث يرسل الزبون أمر PASV بدلاً عن PORT ويرد المخدم بإرسال رقم البوابة التي يستطيع الزبون تأسيس اتصال معها.

يعاني بروتوكول FTP من مجموعة من نقاط الضعف. أولاً، لا يستخدم بروتوكول FTP التشفير أي أن جميع المعلومات المتبادلة بين الطرفين مثل أسماء المستخدمين وكلمات المرور والملفات نفسها تكون بالنص الواضح

الأمر الذي من شأنه السماح لمهاجم مزود بمحلل بروتوكولات ويتنصت على الاتصالات أن يكشف محتويات الطرود المتبادلة. ثانياً، يعاني هذا البروتوكول من إمكانية شن هجوم من نوع رجل في المنتصف MITM حيث يستطيع المهاجم اعتراض المعطيات المتبادلة وتغييرها قبل إعادة توجيهها إلى الوجهة.

يوجد خياران لحماية بروتوكول FTP. استخدام بروتوكول FTPS الذي يعمل فوق طبقة Secure Socket Layer (SSL) ويقوم بتشفير أوامر التحكم المرسلة على البوابة 21 مع إمكانية تشفير طرود المعطيات على البوابة 20.

يتمثل الخيار الآخر في استخدام Secure FTP (SFTP). على عكس بروتوكول FTPS الذي هو مزيج من FTP و SSL/TLS فإن SFTP هو بروتوكول متكامل يستخدم بوابة TCP وحيدة ويقوم بتشفير وضغط أوامر التحكم والمعطيات.

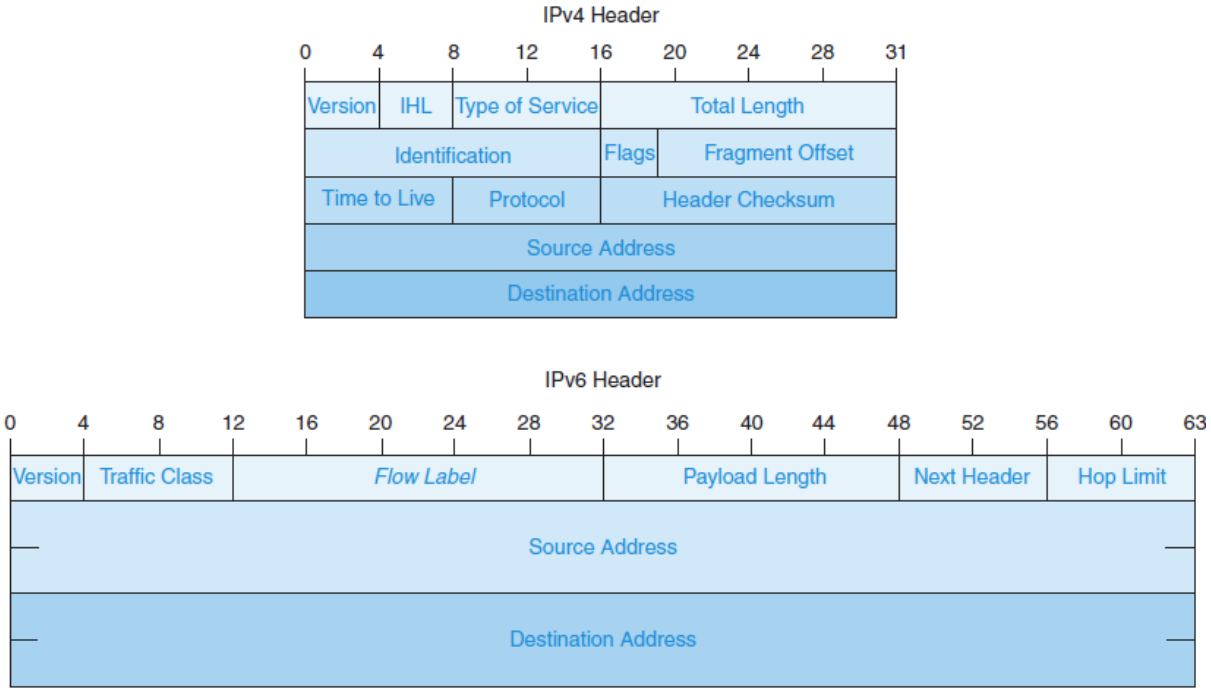
بروتوكول النسخ الآمن SCP

Secure Copy Protocol (SCP) هو بروتوكول مستخدم لنسخ الملفات بطريقة آمنة. يعتبر SCP إصدار محسن عن Remote Copy Protocol (RCP). يقوم بروتوكول SCP بتشفير الملفات والأوامر وهو يعمل بشكل رئيسي على مخدمات يونيكس ولينوكس.

7.1. بروتوكول IPv6

الإصدار الحالي من بروتوكول IP هو v4. يعاني IPv4 من مشكلتين أساسيتين: عدد العناوين الكلي لم يعد قادراً على استيعاب عدد الأجهزة المطلوب وصلها إلى الإنترنت بالإضافة إلى الضعف الأمني الذي يعرضه للهجوم.

يحل بروتوكول IPv6 المشكلتين السابقتين ويضيف مجموعة أخرى من التحسينات. يبين الشكل التالي مقارنة بين ترويستي IPv4 و IPv6.



الشكل 9: ترويستي IPv4 و IPv6

يملك بروتوكول IPv6 عدة تحسينات أمنية. فبروتوكولات التشفير أصبحت مكوناً أساسياً في IPv6 وتمت إضافة ترويسات خاصة بالاستيقان لمنع التلاعب بمحتويات بروتوكول IPv6.

2. مبادئ إدارة الشبكات

تزيد إدارة الشبكات الآمنة من صعوبة إدارة الشبكات. لذلك من الأهمية بمكان، عند إدارة الشبكات الآمنة، اتباع مقاربة إدارية معتمدة على القواعد الإجرائية والتقنية. يمكن تعريف القواعد الإجرائية على أنها التوجيهات الرسمية والإلزامية للسلوك. إن القواعد الإجرائية هي التي تفرض القواعد التقنية كإعداد جدار نار أو مخدم وكيل للتوافق مع التوجيهات الإجرائية.

يقع على مسؤولية مدير الشبكة اتباع القواعد الإدارية المفروضة. يشمل هذا عادةً على القواعد التقنية المرتبطة بالأجهزة الأمنية وتصميم الشبكة وحماية البوابات.

1.2. أمن الأجهزة

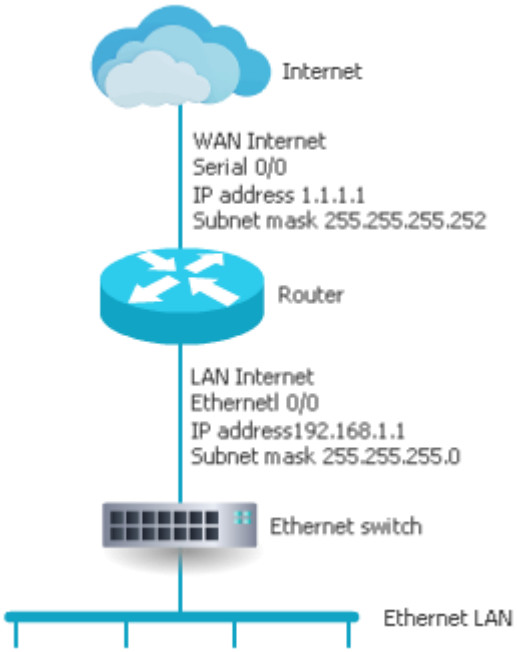
نذكر من الوظائف التي يمكن أن تتضمنها إدارة الأجهزة الإعداد الآمن للمسيرات وتحقيق حارس الإغراق وتحليل سجلات الأجهزة.

الإعداد الآمن للمسيرات

يعتبر المسير Router من المكونات الرئيسية في الشبكات. يعمل المسير على مستوى الطبقة الثالثة (طبقة الشبكة) وهو مسؤول عن توجيه الطرود عبر مجموعة من الشبكات. بما أن الطرود تمر عبر المسير، فيمكن أن يؤدي بعض المهام الأمنية مثل تلك المتعلقة بتصفية الطرود على المستوى الثالث. من هنا تأتي أهمية إعداد المسير بعناية لتأمين الحماية اللازمة للشبكات الموصولة إليه.

يبين الجدول التالي أهم الإعدادات المطلوبة لتأمين المسيرات.

المهمة	الشرح
توثيق التصميم	يجب انشاء مخططات الشبكة بشكل يُظهر واجهات المسير على الشبكات المحلية والواسعة على حد سواء (انظر الشكل المقابل)
استخدام أسماء معبرة للمسيرات	تساعد التسمية المعبرة للمسيرات في تقليل أخطاء توجيه الأوامر إلى مسيرات أخرى وخاصةً كون اسم المسير يظهر عندما يكون طور التكوين
تأمين جميع البوابات	يجب تأمين جميع بوابات المسير سواء الفيزيائية مثل console port و Auxiliary port والبوابات الداخلة من المواقع البعيدة مثل VTY
وضع كلمة مرور مدير قوية	يعمل مدير النظام في نمط privileged mode مع تحكم كامل بالمسير لذلك يجب استخدام كلمات مرور قوية
إجراء التعديلات من بوابة Console	يجب إجراء جميع التعديلات على المسير من بوابة الكونسول وليس عن بعد باستخدام telnet مثلاً. يتم بعد ذلك تخزين الإعدادات على سواقة شبكية آمنة كنسخة احتياط وليس على حاسب محمول أو سواقة USB



الجدول 2: مهام تأمين إعدادات المسيرات

حارس الإغراق Flood Guard

تعتبر هجمات حجب الخدمة DoS و DDoS من أخطر أنواع الهجمات. رأينا سابقاً طريقة استخدام TCP SYN لإغراق مخدم ما بطلبات تأسيس اتصال قادمة من عناوين IP مزيفة الأمر الذي يؤثر على أداء المخدم أو يعطله نهائياً.

يُستخدم حارس الإغراق كأحد وسائل الدفاع ضد هذا النوع من الهجوم. حارس الإغراق هي ميزة تتحكم بمقدار تحمل جهاز ما لطلبات خدمة لم يتم الرد عليها وتساعد في تجنب هجمات حجب الخدمة. يستطيع مدير الشبكة تحديد العتبة العليا للعدد الأعظمي لطلبات تأسيس الاتصال التي يستطيع الجهاز تحملها. عند الوصول إلى العتبة العليا يجري اعتراض أي طرد جديد موجه إلى أحد المخدمات واسقاطه. يمكن العثور على حارس الإغراق في تجهيزات مثل جدران النار وأجهزة كسف و/أو تجنب التسلل IDS/IPS.

تحليل السجلات Log analysis

تحوي السجلات الأحداث التي تقع وهي تعتبر هامة جداً إذا كانت متعلقة بأمن الحواسيب. يمكن أن تكون عملية مراقبة هذه السجلات مفيدة لمعرفة طريقة حدوث الهجوم ولمعرفة إذا تمت مقاومته بنجاح. يمكن تصنيف السجلات المتعلقة بأمن النظام ضمن الحواسيب ضمن صنفين: سجلات نظام التشغيل وسجلات تطبيق الأمن. أما أجهزة الشبكة العتادية فهي تولد سجلات تعكس حالة كامل الشبكة. في حال كان الجهاز الذي يولد السجلات هو جهاز متخصص بالأمن كجدار النار فمن الممكن العثور على معلومات أمنية محددة ضمن هذه السجلات.

نذكر من أنواع سجلات الأجهزة الأمنية:

- الأنظمة الشبكية لكشف التسلل NIDS والأنظمة الشبكية لتجنب التسلل NIPS. يسجل هذا النوع من الأنظمة معلومات أمنية تفصيلية متعلقة بالتصرفات المشبوهة وبالأفعال التي قام بتنفيذها جهاز NIPS لتعطيل هذه الهجمات.
- أنظمة أسماء النطاقات DNS. يخزن مخدم الأسماء سجلات متعلقة بجميع الطلبات التي تم استلامها بما فيها الطلبات الخاطئة أو رسائل التنبيه.
- المخدمات الوكيلة Proxy servers. تخزن المخدمات الوكيلة جميع عناوين URL التي تم النفاذ إليها من خلالها.
- جدران النار Firewalls. يمكن أن تفيد سجلات جدار النار في إيجاد عناوين IP جديدة تحاول استكشاف الشبكة وبناء على ما سبق تحديد ضرورة وضع قواعد أمنية أشد لمنع المهاجم. تعتبر سجلات جدران النار التي تزود معلومات أساسية فقط محدودة الفائدة كما يبينه الشكل 10. يفضل هنا السجلات التي تزود معلومات تفصيلية كما هو وضح في الشكل 11.

Outgoing Log Table Refresh

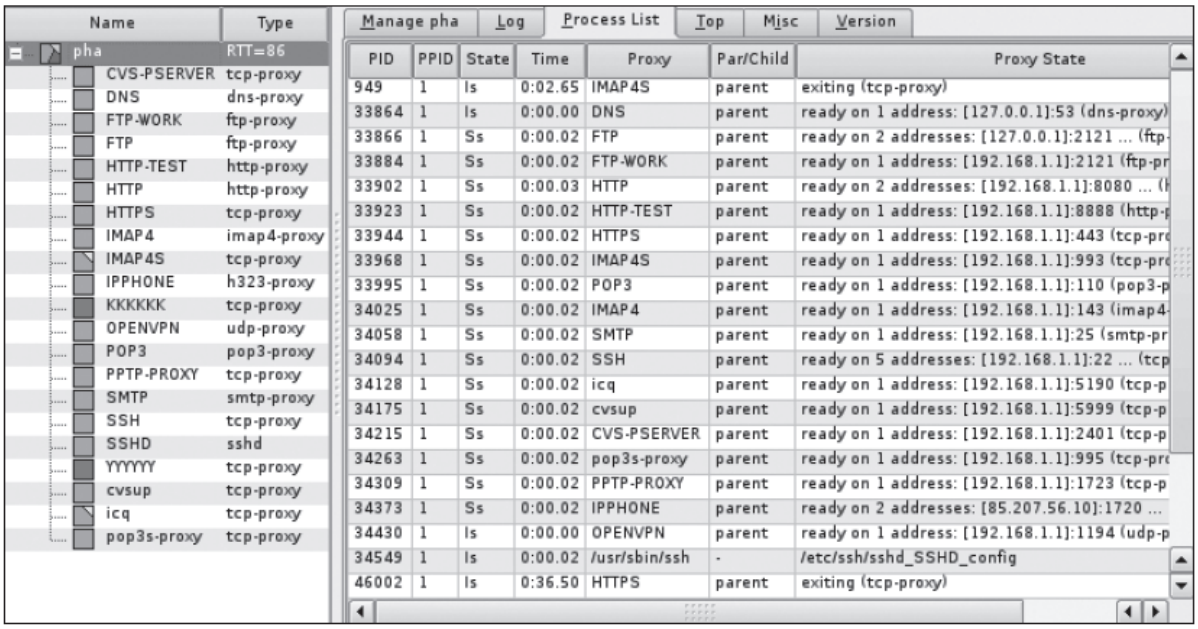
LAN IP	Destination URL/IP	Service/Port Number
192.168.1.136	161.6.18.93	https
192.168.1.136	207.115.11.17	pop3
192.168.1.136	207.115.11.17	smtp
192.168.1.136	207.115.11.17	pop3

Close

الشكل 10: سجل جدار نار أساسي

أما بالنسبة لنوع المعلومات الواجب فحصها ضمن سجلات جدار النار فهي:

- عناوين الإنترنت التي تم رفضها وإسقاط طرودها. تفيد هذه المعلومات في معرفة المؤسسة أو الموقع التي قدمت منها الطرود المرفوضة الأمر الذي يسهل على مدير جدار النار عملية الاتصال بمالك هذه المؤسسة لتوضيح سبب قيام أشخاص ينتمون لها في توليد طرود استكشاف أو طرود مرفوضة على الشبكة.
- استكشاف البوابات التي لا يوجد خدمات تطبيقية مرتبطة بها. عادةً، قبل أن يحاول مهاجم ما تنصيب برنامج طروادي على حاسب ما بغية خلق باب خلفي فإنه يقوم باستكشاف كون البوابة التي يعمل عليها هذا الطروادي مخصصة لتطبيق آخر على الحاسب الضحية. لذلك، يمكن أن تفيد سجلات جدار النار في مقارنة البوابات المفتوحة غير المعروف هدفها مع البوابات التي تستخدمها برامج الأبواب الخلفية الشائعة.



الشكل 11: سجلات جدار نار تفصيلية

- الطرود المسيرة من المصدر Source-routed packets. أي طرد يحمل عنوان مصدر داخلي لكن جرى توليده من خارج الشبكة يمكن أن يدل على محاولة مهاجم غش (تزييف) عنوان داخلي في سبيل النفاذ إلى الموارد الداخلية.
- اتصالات خارجة مشبوهة. كشف اتصال خارجي لمخدم وب عام يمكن أن يدل على أن مهاجم ما استطاع شن هجمات على مواقع أخرى من خلال المخدم.
- الدخول الفاشل. عند اكتشاف عدة محاولات دخول login فاشلة من نطاق ما، يجب خلق قاعدة جديدة تمنع أي اتصال من هذا النطاق.

2.2. إدارة تصميم الشبكة

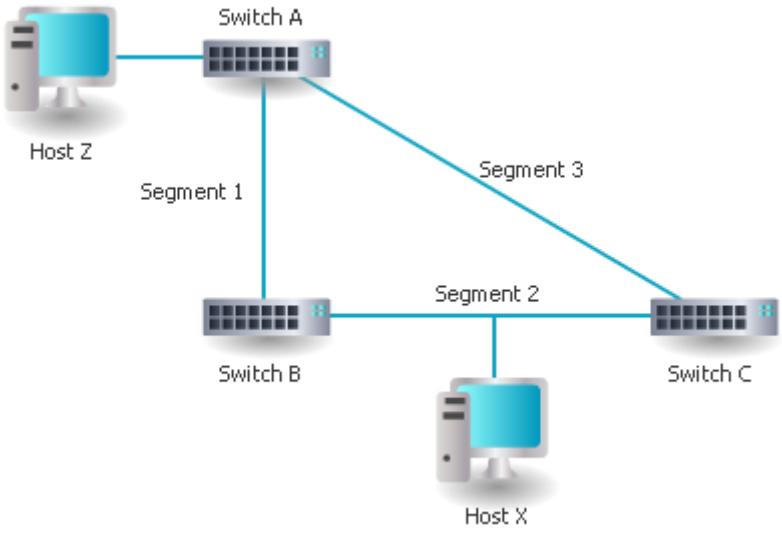
نحتاج إضافةً إلى تأمين الأجهزة الشبكية إلى اتباع مبادئ أساسية في إدارة تصميم الشبكة لضمان أمن الشبكة. نستخدم هنا فصل الشبكات والحماية من الحلقات وإدارة الشبكات المحلية الافتراضية.

فصل الشبكات Network Separation

يقصد بفصل الشبكات منع أجزاء تنتمي إلى شبكة محمية من الاتصال بالشبكات الخارجية أو غير المحمية لتجنب تجسير الشبكات Network Bridging (كمنع الشبكة الخاصة بالطلاب مثلاً من الدخول إلى الشبكة المخصصة لشؤون الطلاب). يمكن تحقيق فصل الشبكات فيزيائياً عن طريق وصل حواسب الطلاب إلى مبدلات ومسيرات مختلفة.

الحماية من الحلقات Loop protection

يبين الشكل 12 مثالاً عن تشكيل حلقة مكونة من 3 وصلات بين 3 مبدلات. ففي حالة عدم استخدام بروتوكول شجرة التغطية Spanning Tree Protocol (STP) عند هذا المبدلات فإن ظاهرة عاصفة البث Broadcast storm يمكن أن تحدث إذا أرسل المضيف Z رسالة إلى المضيف X وكانت المبدلات الثلاثة لا تعرف البوابة الموصولة إلى المضيف X. يمكن لهذه الظاهرة أن تغرق الشبكة في ثوان معدودة وتجعلها غير مستقرة بسبب دوران الإطار في الشبكة إلى اللانهاية.



الشكل 12: عاصفة البث

إدارة الشبكات المحلية الافتراضية VLANs

استخدام الشبكات المحلية الافتراضية VLANs يسمح بتجزئة الشبكة الكلية إلى عدة مجموعات منطقية تربط كل شبكة جزئية افتراضية مستخدمين متباعدين جغرافياً ومتناثرين حول الشبكة الكلية (كل مستخدم موصول على مبدلة مختلفة) الأمر الذي يقلل حركات المرور ويزيد الأمن.

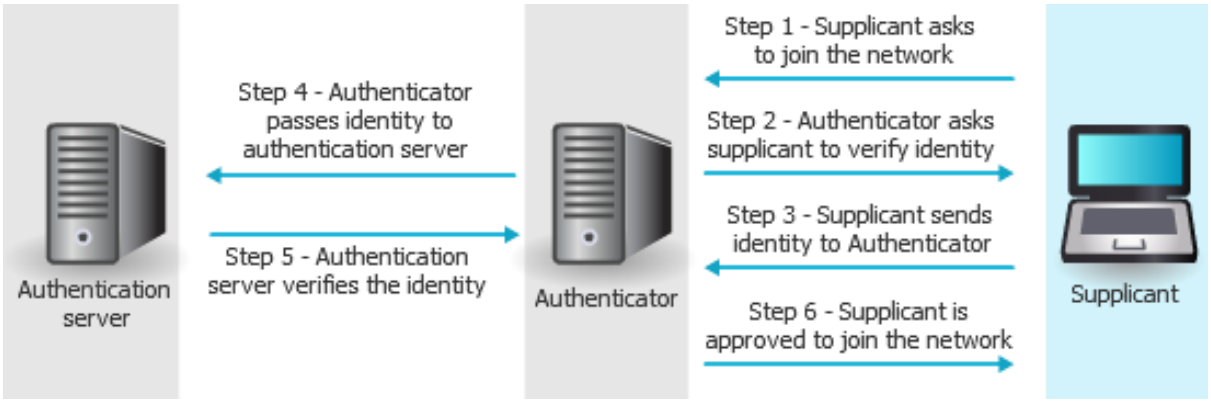
يوجد عدة مبادئ عامة لإدارة VLANs:

- يجب أن لا تتواصل VLAN مع أخرى إلى عن طريق مسير
- إعداد بوابات المبدلات الحرة على أنها تتبع unused VLAN
- يجب تغيير أسماء VLANs الافتراضية
- إعداد بوابات المبدلات التي تمرر طرود VLAN الموسومة tagged بشكل يسمح بتوجيه سمات محددة
- يجب عدم وضع الأجهزة العامة مثل مخدمات تطبيقات الوب ضمن شبكة VLAN خاصة

أمن البوابات Port security

يعتبر تأمين البوابات خطوة هامة في إدارة الشبكات. يمكن تأمين البوابات عن طريق تعطيل البوابات غير المستخدمة وتقييد عناوين MAC وتصفيتها وباستخدام IEEE 802.1x.

- تعطيل البوابات غير المستخدمة. يمكن هنا مثلاً تعطيل البوابات غير المستخدمة على المبدلة. تسمح أي مبدلة لا تستخدم بروتوكول أمن البوابات لأي مهاجم استطاع أن يرتبط ببوابة غير مستخدمة من تحقيق هجمات على الشبكة. يجب على مدير الشبكة النفاذ على جميع المبدلات وتعطيل البوابات غير المستخدمة فيها.
- تقييد وتصفية عناوين MAC. تصفي هذه العملية عناوين Media Access Control (MAC) القادمة إلى مبدلة ما وتحد العدد الأعظمي لها. يمكن تعريف بوابة مبدلة للسماح بعنوان MAC وحيد ومحدد مسبقاً يستطيع الاتصال بهذه البوابة الأمر الذي يسمح لمضيف واحد فقط بالاتصال بالمبدلة عن طريق هذه البوابة.
- بروتوكول IEEE 802.1x. يقدم هذا البروتوكول المعياري أعلى درجات حماية بوابات المبدلات. يتم هنا تحقيق الاستيقان حسب البوابة Port-based authentication. يمنع هذا البروتوكول مرور أي طرد عبر أي بوابة حتى يتم التحقق من هوية الزبون المتصل إلى البوابة عن طريق معلومات اعتماده المخزنة على مخدم استيقان. هذا يمنع أي جهاز غير مصادق عليه من استقبال أي طرد قبل إتمام عملية التحقق من الهوية. كما أنه يحد النفاذ إلى مخدم الاستيقان لمنع تعرض هذا المخدم إلى أي نوع من الهجمات. يبين الشكل 8 خطوات الاستيقان التي يتبعها بروتوكول 802.1x.

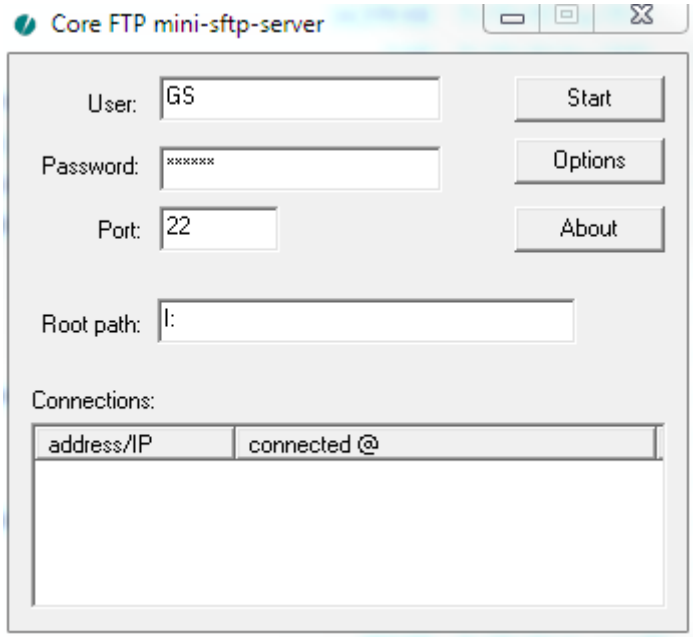


الشكل 13: إجراءات بروتوكول IEEE 802.1x

3. تمارين عملية

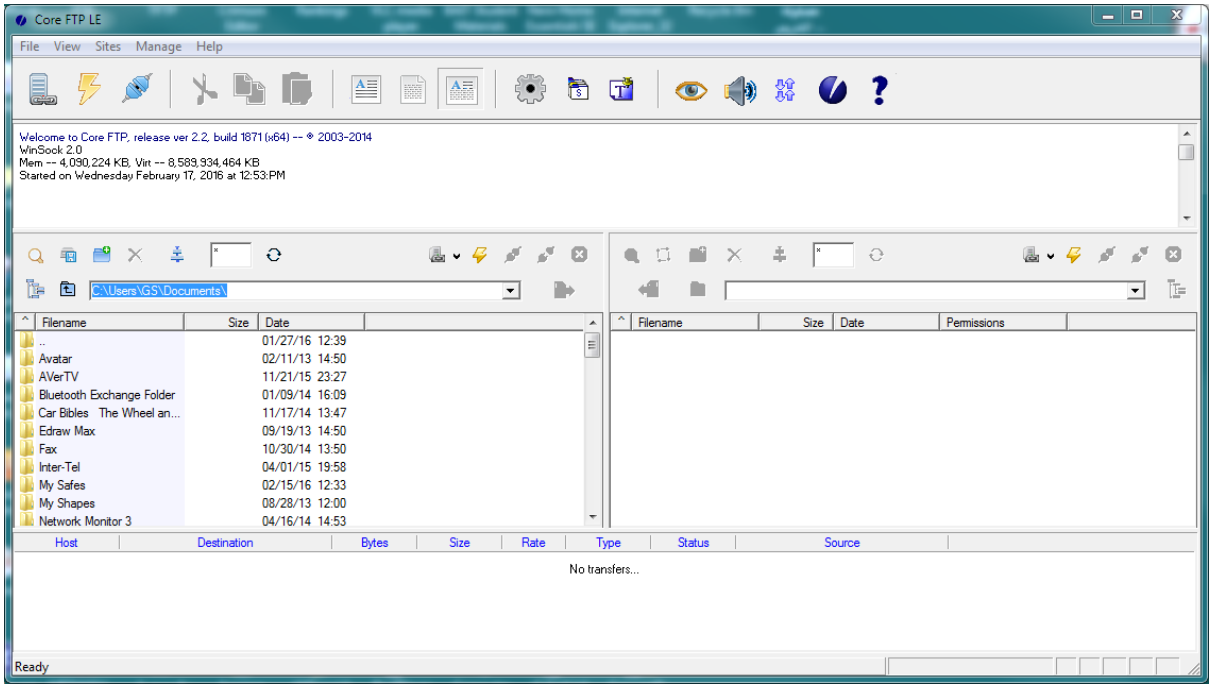
1.3. استخدام مخدم وزبون FTPS

1. Go to www.coreftp.com/server/index.html (for SFTP mini server)
2. Download CoreFTP server (32 or 64 bit depending on your machine)
3. run msftpsrvr.exe

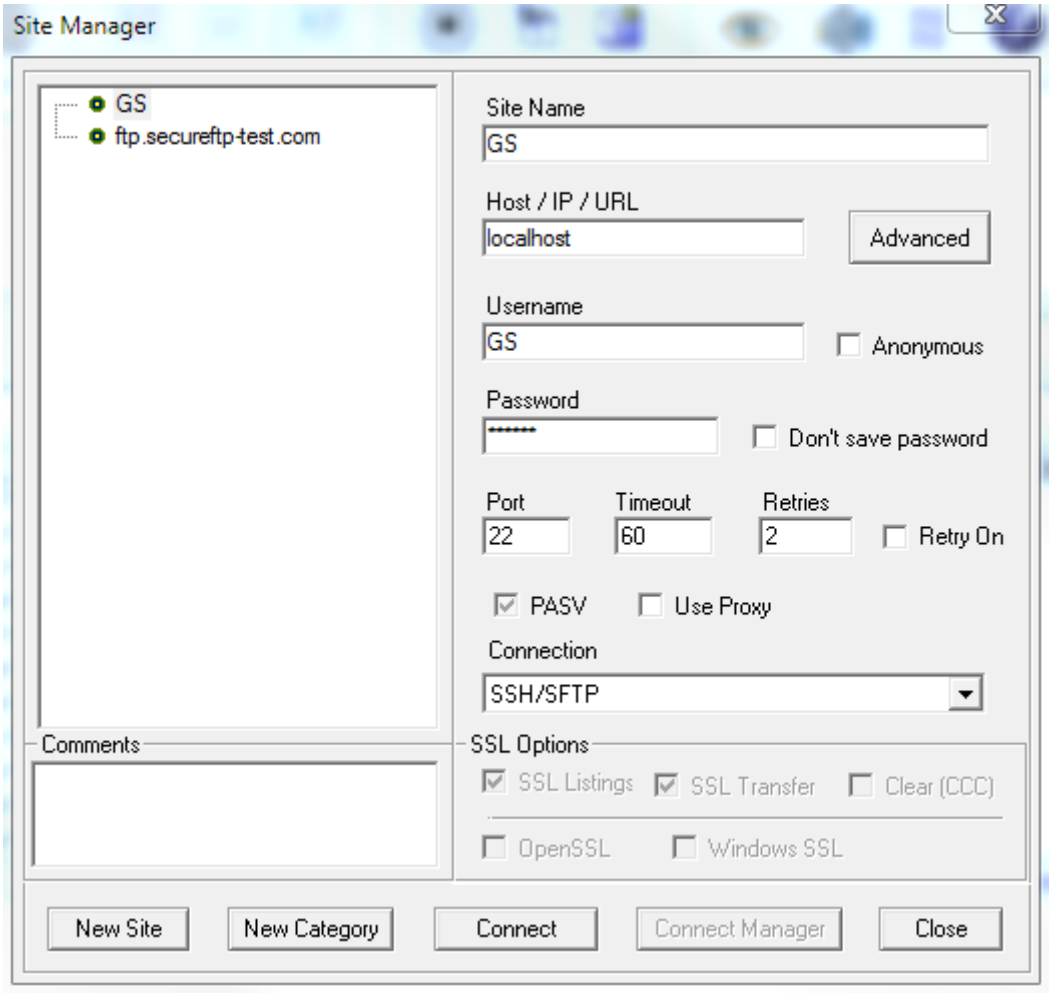


الشكل 14: Core FTP mini-sftp-server

4. Enter user name and password
5. Define a Root path (root directory for SFTP server)
6. Click Start
7. Go to www.coreftp.com/download.html (for SFTP client)
8. Download Core FTP MSI installs LE version
9. Run setup64.msi
10. Launch Core FYP LE (you 'll see a windows as below)



11. Click Sites > Site Manager
12. Enter the parameters as per next windows but after putting your site name instead of GS



13. Click Connect
14. You can now copy securely copy files between the two locations

2.3. استخدام مخدم أسماء أسرع

إذا كان مخدم الأسماء الذي تستخدمه بطيء، فإنك ستعاني من بطئ في تصفح الإنترنت. سنحاول في هذا التمرين مقارنة أداء مجموعة من مخدمات الأسماء بغرض اختيار أسرع مخدم مجاني بالقرب منك بحيث يسمح لك بتسريع الإنترنت.

1. Find and download Namebench tool
2. Extract and set-up the tool
3. Run namebench
4. Scroll through the list of DNS servers and note the differences among them

الفصل السابع:أمن الشبكات اللاسلكية
Wireless Network security

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- شرح أنواع الهجمات على الشبكات اللاسلكية
- فهم نقاط ضعف معيار IEEE 802.11 وثغراته الأمنية
- تعرف طرق تأمين الشبكات اللاسلكية

مع انتشار الشبكات اللاسلكية وتغلغلها في حياتنا اليومية، لم يعد هناك حاجة لوصل الحاسوب فيزيائياً إلى إحدى المبدلات كما أصبح بالإمكان الحركة أثناء تبادل المعلومات أو الاتصال بالإنترنت من أي بقعة.
أصبحت الشبكات اللاسلكية موجودة في كل مكان كما أن أجهزة الهاتف الذكية التي تجاوز مبيعاتها الأجهزة الحاسوبية المحمولة باتت تتصل عن طريق الشبكات اللاسلكية.
لقد كانت الشبكات اللاسلكية عرضةً للهجمات بسبب طبيعة البث اللاسلكي وبسبب ضعف الأجيال الأولى منها.
سنغطي في هذا الفصل الجوانب الأمنية المتعلقة بالشبكات اللاسلكية.

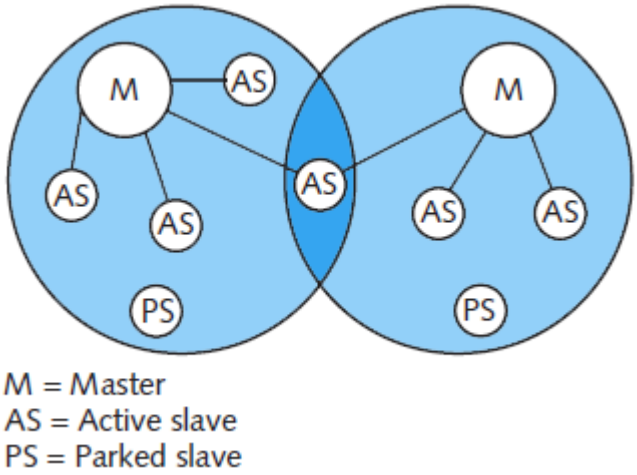
1. الهجمات اللاسلكية

الهجمات على أجهزة بلوتوث

تسمح تقانة البلوتوث بوصل المستثمرين لاسلكياً لمسافات محدودة. تعتبر بلوتوث من تقانات الشبكات الشخصية Personal Area Network (PAN) المصممة لتبادل المعطيات على مسافة قصيرة جداً. تستخدم غالبية أجهزة البلوتوث راديو من الصف 2 التي تغطي حتى 10 متر بمعدل نقل معطيات يصل إلى 1 Mbps.

يعرف بلوتوث نوعين من الطبولوجيات. يعرف الأول باسم بيكونت Piconet. عندما يقترب جهازان يعملان بتقانة بلوتوث من بعضهما مسافة كافية فإنهما يتصلان مع بعضهما آلياً. يصبح أحد الأجهزة هو السيد Master الذي يتحكم بحركات المرور ويصبح الجهاز الآخر العبد slave الذي يتلقى الأوامر من السيد. تعرف الأجهزة العبدة المتصلة بشبكة بيكونت والتي ترسل الأطر بالعبيد النشطين active slaves بينما العبيد الذين لا يرسلون شيئاً فهم عبيد واقفين parked slaves.

في حال وجود عدة بيكونت في نفس الرقعة الجغرافية، يمكن لأحد الأجهزة أن يشارك في شبكتي بيكونت أو أكثر في الوقت نفسه. تسمى الطبولوجيا التي تحوي عدة بيكونت متصلة مع بعضها بالشبكة المبعثرة Scatternet كما هو موضح في الشكل 1.



الشكل 1: شبكة بلوتوث مبعثرة Scatternet

إن الطبيعة الوضعية Ad hoc لشبكات بيكونت و scatternet تجعلها عرضةً للهجمات. من أهم الهجمات التي تستهدف شبكات بلوتوث نذكر Bluejacking و Bluesnarfing.

Bluejacking

يتمثل هذا الهجوم في إرسال رسالة بدون دعوة لجهاز بلوتوث. يمكن أن تكون الرسالة نصية أو صورة أو فيديو أو صوتية. يعتبر هذا النوع من الهجمات المستخدم عادةً غي نشر الإعلانات مزعج أكثر منه ضار بسبب عدم سرقة المعلومات.

Bluesnarfing

يهدف هذا الهجوم إلى سرقة معلومات خاصة منقولة بين هاتف ذكي وحاسوب محمول. يقوم المهاجم في هذه الحالة بنسخ رسائل البريد الالكتروني والتقويمات ولوائح الاتصال والصور والفيديو الموجودة في الهاتف المحمول عن طريق الاتصال بالجهاز دون علم صاحب هذا الجهاز.

لتجنب هذا النوع من الهجمات يجب تعطيل البلوتوث إذا لم تكن له حاجة أو عند التواجد في غرفة مع أشخاص غير معروفين. أو يمكن وضع جهاز البلوتوث في وضعية غير قابل للاكتشاف undiscoverable حيث يكون البلوتوث مفعل لكن غير قابل للاكتشاف.

2. هجمات الشبكات اللاسلكية المحلية

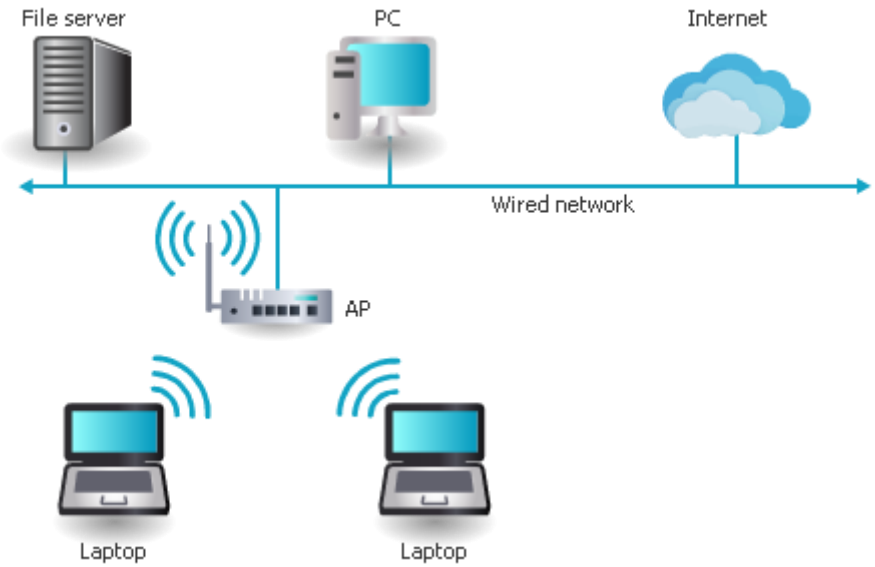
يشرف معهد Institute of Electrical and Electronics Engineer (IEEE) على وضع معايير الشبكات المحلية اللاسلكية مثلها مثل معايير الشبكات المحلية. تعرف معايير الشبكات المحلية اللاسلكية بالاسم IEEE 802.11x حيث x هو متحول من القيم المعروفة التي يأخذها هي a, b, g, n والتي تدل على رقم الإصدار. أحدث الإصدار الأخير 802.11n المصدق عليه عام 2009 تغييرات جذرية وقفزة نوعية على الإصدارات السابقة تتمثل في:

- معدل النقل. يمكن أن يصل معدل نقل المعطيات إلى 600 Mbps.
- منطقة التغطية. مضاعفة مساحة التغطية الداخلية والحصول على ثلاثة أضعاف التغطية الخارجية.
- التداخل. تقليل التداخل باستخدام ترددات متنوعة.
- الأمن. يحقق الإصدار أعلى مستوى أمني.

تعتمد الشبكات اللاسلكية على نقاط النفاذ Access Points (Aps). تتألف نقطة النفاذ من ثلاثة أجزاء أساسية:

- هوائي ومرسل/مستقبل راديوي
- برمجيات تجسير خاصة لربط الأجهزة اللاسلكية بالأجهزة الأخرى
- واجهة شبكة سلكية للسماح بالربط مع شبكة سلكية

تقوم نقطة النفاذ بوظيفتين. أولاً، هي تعمل كمحطة قاعدية تستقبل الإشارات اللاسلكية من بقية الأجهزة اللاسلكية وتعيد توجيهها إلى بقية الأجهزة. ثانياً، تعمل كجسر بين الشبكات السلكية واللاسلكية كما هو مبين في الشكل 2.



الشكل 2: نقطة النفاذ ضمن شبكة لاسلكية

تحوي نقطة النفاذ المعيارية (أو المستقلة) الذكاء الكافي لتحقيق عمليات الاستيقان والتشفير والإدارة المطلوبين لتخديم مختلف الأجهزة اللاسلكية المربوطة معها. يجري، في المكاتب الصغيرة أو المنازل، استخدام نوعاً آخر من نقاط النفاذ يحقق أيضاً وظائف إضافية مثل جدار النار ومسير ومخدم DHCP وغيرها. يمكن أن نطلق عليها اسم عبّارات لاسلكية سكنية Residential Wireless gateway أو كما هي معروفة في الأسواق تحت اسم مسير لاسلكي wireless router.

نظراً لطبيعة عمل الشبكات اللاسلكية فقد اعتبرت كهدف ثمين للمهاجمين. لا يحتاج المهاجم هنا إلى الوصل مع كبل الشبكة السلكية حتى يستطيع اعتراض حركة المرور وإنما يكفيه اعتراض حركات المرور اللاسلكية غير المشفرة وقراءة محتوياتها وسرقة المعلومات الهامة منها مثل كلمات المرور أو حتى تغيير محتوى الرسائل أيضاً. كما يستطيع المهاجم المزود بمشوش ترددات لاسلكية radio frequency jammer من حجب الخدمة وتوقيف الشبكة عن العمل.

يوجد، من أشكال الهجمات على الشبكات اللاسلكية، اكتشاف الشبكة والهجوم على الطيف الترددي والهجوم الذي يتطلب نقاط نفاذ.

1.2. اكتشاف الشبكة

يقصد هنا اكتشاف وجود الشبكة اللاسلكية. تبث نقطة النفاذ على فترات زمنية منتظمة (كل 100 ميكرو ثانية) إشارة (يطلق عليا اسم إطار Beacon) تعلن عن وجودها وتزود بعض المعلومات الضرورية للأجهزة التي تريد الانضمام إلى الشبكة اللاسلكية. يستمع كل جهاز لاسلكي يريد الانضمام إلى شبكة ما إلى هذه الأطر (مسح scanning). بالنسبة للمهاجم، فهو ينتظر هذه الإشارات Beaconing لاكتشاف الشبكات اللاسلكية وتجميع معلومات عنها. تعرف هذه العملية باسم war driving أو Wireless location mapping.

يمكن للمهاجم اكتشاف الشبكة باستخدام هاتف ذكي أو بطاقة شبكة لاسلكية خارجية مع هوائي خارجي موصولين إلى حاسب محمول مزودين ببرمجيات خاصة تعرض معلومات تفصيلية عن كل شبكة مكتشفة.

بعد اكتشاف الشبكة اللاسلكية، تأتي عملية توثيق وجودها والإعلان عن موقعها ليتاح للآخرين استخدامها (تعرف هذه العملية باسم War Chalking). يجري حالياً الإعلان عن مواقع الشبكات اللاسلكية على مواقع الوب.

2.2. الهجوم على الطيف الترددي

يجري هنا استخدام محلل بروتوكولات لاسلكي وتوليد التداخلات.

محلل البروتوكولات اللاسلكي

يعمل محلل البروتوكولات اللاسلكي على اعتراض حركة المرور اللاسلكية وفك ترميزها وتحليل محتويات الطرود المارة. لكن التقاط حركة المرور اللاسلكية تتطلب وضع بطاقة الشبكة اللاسلكية في نمط مناسب. يمكن أن تعمل بطاقة الشبكة اللاسلكية وفق واحد من ستة أنماط: سيد Master عندما تعمل البطاقة كنقطة نفاذ ومُدار managed عندما تعمل المحطة كزبون عادي ومكرر repeater و mesh ووضعي ad-hoc ومراقبة monitor. يجب وضع بطاقة الشبكة في نمط المراقبة Monitor mode حتى تستطيع التقاط الأطر بدون الارتباط مع نقطة النفاذ.

التداخل

يمكن أن يشكل أي جهاز مصدر تداخل مع بقية الأجهزة الأمر الذي يعيق حركة المرور اللاسلكية. يمكن للمهاجمين استخدام تداخلات الإشارات الراديوية عن قصد لإغراق الطيف الترددي بإشارات تحجب خدمة الإرسال عن المستثمرين العاديين.

الهجوم باستخدام نقاط النفاذ

يمكن شن نوعين من الهجمات باستخدام نقاط النفاذ: نقاط النفاذ المخادعة والتوأم الشرير.

- نقطة النفاذ المخادعة rogue AP. هي عملية وصل وإعداد نقطة نفاذ غير شرعية من قبل مستثمر داخلي إلى شبكة المؤسسة الداخلية الأمر الذي يسمح لمهاجم بالنفاذ إلى الشبكة الداخلية وتجاوز بعض الإعدادات الأمنية للمؤسسة.
- التوأم الشرير evil Twins. هي عملية وصل وإعداد نقطة نفاذ غير شرعية من قبل المهاجم. تصمم نقطة النفاذ هذه لتقليد نقاط النفاذ الشرعية بحيث يمكن لمستثمر داخلي الانضمام إلى نقطة النفاذ هذه دون أن يعرف حقيقتها. يصبح باستطاعة المهاجم الآن التقاط حركات مرور المستثمرين المنضمين إلى نقطة النفاذ.

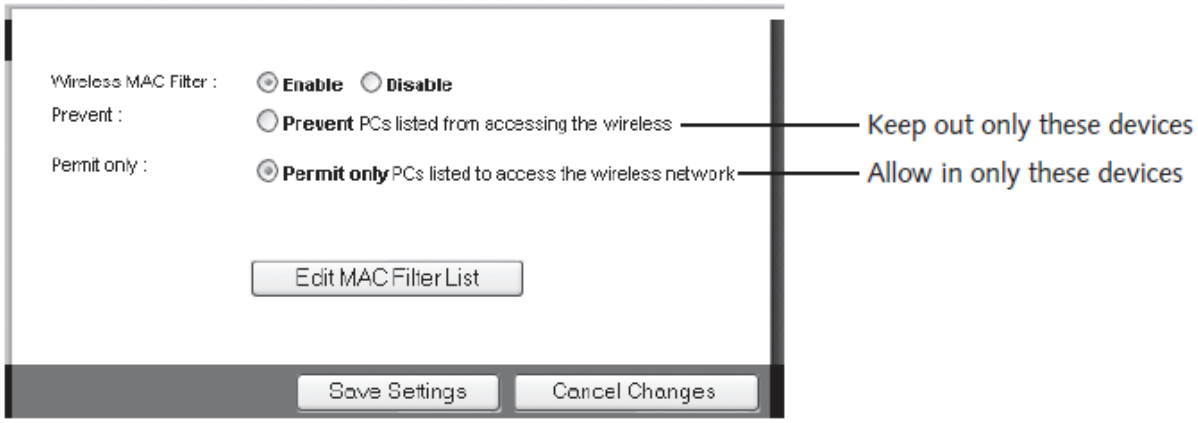
3. نقاط الضعف الأمنية في معيار IEEE 802.11

وضع معهد IEEE مجموعة من الحمايات لبروتوكول IEEE 802.11 وترك البعض الآخر لمصنعي المكونات اللاسلكية. أدى ذلك إلى انتشار مجموعة من نقاط الضعف وبالتالي مجموعة من الهجمات. يمكن تصنيف نقاط الضعف هذه إلى تصفية عناوين MAC وبث SSID وتشفير WEP.

1.3. تصفية عناوين MAC

تكمن إحدى الطرق في التحكم بالنفاذ إلى شبكة لاسلكية في تحديد عناوين الماك المسموح لها النفاذ عن طريق نقطة النفاذ. بما أن نقطة النفاذ هي النقطة المركزية التي تمر من خلالها جميع حركات الشبكة اللاسلكية فهي المكان المناسب لتحقيق التصفية هذه.

يجري هنا إدخال مجموعة من عناوين MAC إلى برنامج إدارة نقطة النفاذ بشكل يسمح أو يمنع دخول هذه العناوين إلى الشبكة كما هو مبين في الشكل 3.



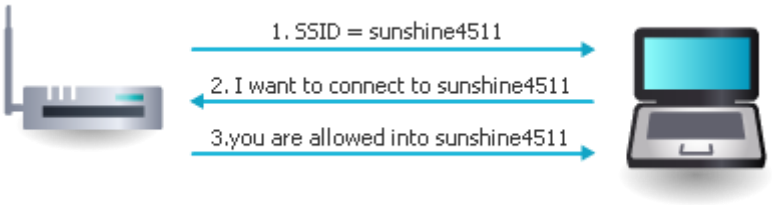
الشكل 3: تصفية عناوين MAC

تعاني هذه التقنية من عدة ثغرات أمنية. أولاً، يجري تبادل عناوين MAC بين نقطة النفاذ والأجهزة اللاسلكية بصيغة غير مشفرة. يمكن لمهاجم مزود بمحلل بروتوكولات لاسلكي رؤية عنوان MAC لجهاز مصرح له النفاذ واستبدال عنوانه بهذا العنوان.

تعود الثغرة الأمنية الثانية في تصفية عناوين MAC إلى التحدي الكبير المتمثل في إدارة عدد كبير من عناوين MAC. عندما تملك مؤسسة ما عدد كبير من المستخدمين، فإنه يجب متابعة دخول مستخدمين جدد وخروج بعض المستخدمين من الشبكة الأمر الذي يشكل عبء إداري كبير. لهذا السبب، تصبح تصفية عناوين MAC غير عملية في المؤسسات الكبيرة والديناميكية.

2.3. بث معرف الشبكة SSID

يجب المصادقة على الجهاز اللاسلكي قبل السماح للمستخدم بالنفاذ إلى الشبكة. يعرف أحد أنواع الاستيقان (أو المصادقة) المعرفة ضمن 802.11 باستيقان النظام المفتوح Open System Authentication. يكتشف الجهاز اللاسلكي نقطة نفاذ لاسلكي عن طريق مسح الطيف الترددي واستقبال إطار Beacon من نقطة النفاذ. يحوي إطار Beacon معلومات كثيرة عن الشبكة اللاسلكية أهمها معدل النقل الذي تدعمه نقطة النفاذ واسم الشبكة اللاسلكية المعروف بمعرف مجموعة الخدمة(SSID) Service Set Identifier. SSID هو سلسلة محارف يصل طولها حتى 32 محرفاً. بعد أن تستقبل نقطة النفاذ طلب الارتباط Association request من الجهاز اللاسلكي، تقوم بمقارنه SSID الموجود في الطلب مع SSID الخاص بها وفي حال التطابق يجري فتح الارتباط كما هو موضح في الشكل 4.



الشكل 4: استيقان النظام المفتوح

يعتبر هذا النوع من الاستيقان ضعيفاً لأنه يعتمد على عامل استيقان وحيد هو معرف SSID. يلزم المهاجم معرفة SSID حتى يستطيع أن ينفذ إلى الشبكة. يوجد عدة طرق تسمح للمهاجم باكتشاف SSID، مثل البحث عن SSID لجهاز مصادق عليه ضمن الشبكة. تتمثل الطريقة الأسهل في اكتشاف معرف SSID في انتظار بثه من قبل نقطة النفاذ.

تشجع بعض المصادر الأمنية على إعداد نقطة النفاذ بحيث لا تضع معرف SSID ضمن إطار Beacon الذي يجري بثه. هنا يتحتم على المستخدم إدخال معرف SSID يدوياً. تخفي هذه الطريقة اسم الشبكة عن المستخدمين لكنها تعاني من بعض القيود:

- يمكن اكتشاف معرف SSID من أطر الإدارة التي ترسلها نقطة النفاذ عن طريق محلل بروتوكولات لاسلكية.
- يمكن أن يمنع إخفاء معرف SSID مستخدم من التجوال بين الشبكات اللاسلكية.
- لا تدعم جميع نقاط النفاذ إمكانية إخفاء معرف SSID.

بروتوكول WEP

بروتوكول Wireless Equivalent Privacy (WEP) هو بروتوكول أمني 802.11 مصمم للسماح للأطراف المخولين فقط برؤية محتويات الطرود المتبادلة. يعتمد بروتوكول WEP على التشفير بمفتاح سري بين الجهاز ونقطة النفاذ. ينتج مفتاح التشفير عن تركيب المفتاح السري مع شعاع بدائي مكون من 24 بت يتغير بعد تشفير كل طرد.

نظراً لصغر طول الشعاع البدائي المكون من 24 بت (أي حوالي 16 مليون قيمة ممكنة) فإن نقطة النفاذ ستستخدم القيمة نفسها للشعاع بعد مدة زمنية لا تتجاوز 7 ساعات. استغل المهاجمين هذه الثغرة للسيطرة على بروتوكول WEP.

4. الحلول الأمنية للشبكات اللاسلكية

1.4. استخدام WPA

تهدف Wi-Fi Protected Access (WPA) إلى حماية الأجهزة اللاسلكية الحالية والمستقبلية. WPA هي مجموعة جزئية من معايير IEEE 802.11i وتقوم بعمليات التشفير والمصادقة.

بروتوكول TKIP للتشفير

تستبدل WPA بروتوكول WEP بتقانة تشفير تدعى Temporal Key Integrity Protocol (TKIP). تستخدم TKIP مفتاح تشفير بطول 128-bit ويجري توليد مفتاح لكل طرد. تستخدم TKIP أيضاً حقل اختبار تكامل الرسالة Message Integrity Check (MIC) للتحقق من عدم تغيير محتويات الطرد.

المصادقة بمفتاح مسبق المشاركة PSK

يمكننا تحقيق مصادقة WPA باستخدام IEEE 802.1x أو باستخدام تقانة Preshared Key (PSK). بعد إعداد نقطة النفاذ، يتم المشاركة على مفتاح مسبق بين نقطة النفاذ وجميع الأجهزة اللاسلكية التي تدعم PSK. عندما يحاول جهاز ما الاتصال بالشبكة اللاسلكية، يقوم بإدخال قيمة المفتاح المشترك.

يستخدم PSK جملة مرور Passphrase لتوليد مفتاح التشفير. لا تدخل جملة المرور ضمن مفتاح التشفير لكنها تستخدم كنقطة انطلاق لتوليد مفتاح التشفير.

يمكن إضافة WPA كتحديث برمجي على الجهاز اللاسلكي وتحديث بنية ثابتة Firmware update على نقطة النفاذ.

بالرغم من التحسينات التي أضافها بروتوكول WPA على بروتوكول WEP إلا أنه لا يزال يعاني من بعض المشاكل الأمنية فيما يتعلق بإدارة المفاتيح وجمل المرور.

2.4. باستخدام WPA2

تعتمد WPA2 على النسخة النهائية من المعيار IEEE 802.11i لعام 2004. يشفر WPA2 المعطيات باستخدام معايير التشفير المتقدمة Advanced Encryption Standards (AES) ويدعم PSK و IEEE 802.1x للمصادقة.

3.4. خطوات أمنية أخرى

يمكن حماية شبكة محلية لاسلكية باتباع مجموعة أخرى من الخطوات مثل تموضع الهوائيات والتحكم بمستوى الطاقة وأدوات اكتشاف نقاط النفاذ المخادعة.

تموضع الهوائيات

توضع نقاط النفاذ عادة في مركز منطقة التغطية المطلوبة. ينصح عند تثبيت نقطة النفاذ أن تكون مرتفعة قدر الإمكان بشكل يعرِّض الإشارات الراديوية إلى أقل عدد من العوائق الطبيعية ولمنع اللصوص من سرقة الجهاز. يجب أيضاً وضع نقطة النفاذ وهوائياتها بشكل يقلل قدر الإمكان من وصول الإشارة إلى خارج محيط المؤسسة.

التحكم بمستوى الطاقة

عندما تتمتع نقطة النفاذ بإمكانية التحكم بمستوى الطاقة يصبح بالإمكان تعيير الطاقة بحيث أقل قدر من الإشارة يتجاوز محيط المؤسسة.

أدوات اكتشاف نقاط النفاذ المخادعة

تشكل نقاط النفاذ المخادعة ثغرة أمنية كبيرة لأي مؤسسة لذلك لا بد من اكتشاف هذا النوع من نقاط النفاذ وتعطيلها. تستخدم غالبية المؤسسات المراقبة المتواصلة للترددات الراديوية في الهواء. نحتاج في هذه الحالة إلى جهاز خاص يدعى بالمسبار اللاسلكي Wireless probe.

يوجد أربعة أنواع من المسبار اللاسلكي:

- مسبار جهاز لاسلكي. يمكن استخدام أي جهاز مزود ببطاقة شبكة لاسلكية مثل الحاسوب المحمول كمسبار لاسلكي. يستطيع هذا الجهاز مسح الترددات اللاسلكية دورياً وإرسال القيم الناتجة إلى قاعدة معطيات مركزية. فعند استخدام عدد كبير من الأجهزة المحمولة كمسبار كل في منطقته، يمكن أن نكتشف بدقة عالية نقاط النفاذ المخادعة.
- مسبار سطح المكتب. نستخدم هنا بطاقة شبكة لاسلكية خارجية للوصل مع جهاز حاسوب مكتبي للقيام بالعمليات السابقة نفسها.
- مسبار نقطة النفاذ. تأتي بعض نقاط النفاذ مجهزة بإمكانية اكتشاف نقاط النفاذ الجارة والمخادعة والتي يمكن استخدامها لهذا الغرض.
- مسبار متخصص. يعمل كجهاز متخصص لمراقبة طيف الترددات اللاسلكية. يشبه المسبار التخصصي نقطة النفاذ في الشكل لكن يختلف عنها بطريقة العمل.

ما أن، تصل قائمة نقاط النفاذ إلى قاعدة المعطيات المركزية، تقوم برمجيات إدارة الشبكات اللاسلكية بمقارنة نقاط النفاذ مع قائمة نقاط النفاذ الموافق عليها. في حال كان جهاز ما لا ينتمي إلى القائمة فيتم اعتباره كجهاز مخادع ويتم تعطيل بوابة المبدلة المتصل إليها عن طريق برنامج الإدارة اللاسلكي.

الشبكات المحلية اللاسلكية الافتراضية Wireless VLANs

مثلها مثل الشبكات المحلية الافتراضية، يمكن لمؤسسة ما تقسيم الشبكة اللاسلكية إلى شبكة خاصة بالموظفين وأخرى خاصة بالضيوف. شبكة الموظفين تتيح لهم النفاذ إلى قاعدة معطيات المؤسسة وملفاتها بينما شبكة الضيوف تتيح لهم النفاذ إلى الإنترنت والملفات العامة. يستخدم الموظفون معرف SSID=employee ويستخدم الضيوف المعرف SSID=Guest. كما يمكن أيضاً مشاركة الشبكة الافتراضية اللاسلكية مع الشبكة الافتراضية السلكية.

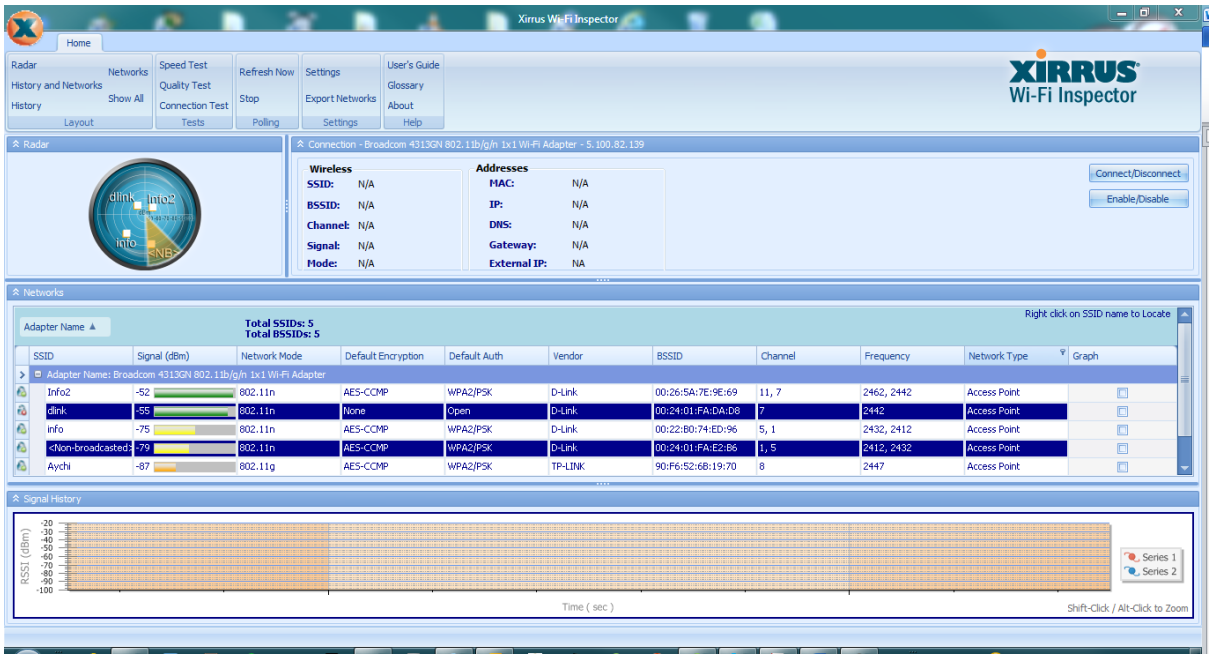
يمكن إعداد الشبكات الافتراضية بإحدى طريقتين. إما عن طريق المبدلة، بما أن كلAP موصولة إلى بوابة مختلفة من المبدلة أو المبدلات فيمكن تحديد الشبكة الافتراضية على هذا الأساس. الطريقة الأخرى الأكثر مرونةً تعتمد على نقطة النفاذ نفسها لفصل الأطر. تسمح هذا الطريقة لنقطة النفاذ بالانتماء إلى عدة شبكات افتراضية وترسل معطيات إلى بقية الشبكات الافتراضية. يمكن لنقاط النفاذ التي تعتمد Wireless VLANs أن تدعم حتى 16 SSID أو أكثر (أي عدة VLANs).

5. تمارين عملية

1.5. استخدام أداة مراقبة لاسلكية

يهدف هذا التمرين إلى مسح الطيف الراديوي للبحث عن الشبكات اللاسلكية الموجودة ومعرفة خصائصها.

1. Go to URL www.xirrus.com/free-tools
2. Download WI-FI INSPECTOR
3. Install the tool
4. Run xirrus Wi-fi inspector
5. The tool display information as per next figure.

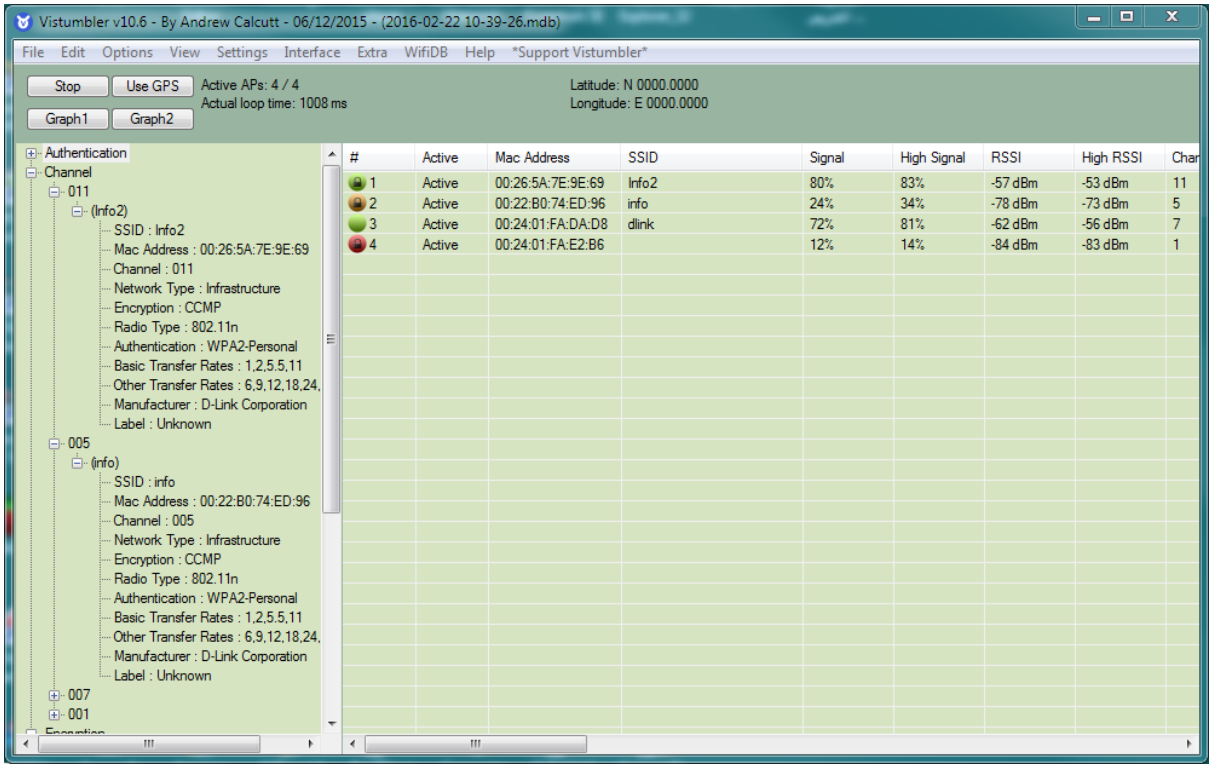


الشكل 5: نافذة Wi-Fi inspector

2.5. الحصول على معلومات تفصيلية أكثر عن الشبكات اللاسلكية

سنستخدم في هذا التمرين أداة متقدمة أكثر وهي vistumbler التي تقدم معلومات أكثر.

1. Go to URL www.vistumbler.net/index.html
2. Download and install the EXE file
3. Click scan Aps
4. In the left pane, expand the options under the various headings (Authentication, Channel, Encryption, Network Type, and SSID), as illustrated in Figure 6. Which information would be useful to an attacker? How could it be used?
5. In the right pane, click one of the WLANs to select it.
6. Click graph1
7. Notice that the signal strength of that WLAN is graphed. Click Graph2. How is this same information displayed differently?
8. Select another WLAN in the bottom pane. Note how its information is graphed.
9. Click No Graph to return to the main screen.
10. One of the features of Vistumbler is its ability to use audio and text-to-speech information so that the location and strength of WLANs can be detected without the need to constantly monitor the screen. Be sure that the speakers on the laptop computer are turned on.
11. Click Options.
12. Click Speak Signals. Now Vistumbler will “speak” the percentage of signal strength.
13. Now carry the laptop away from the AP and note the changes. How would this be helpful to an attacker?
14. Explore the other Vistumbler options.

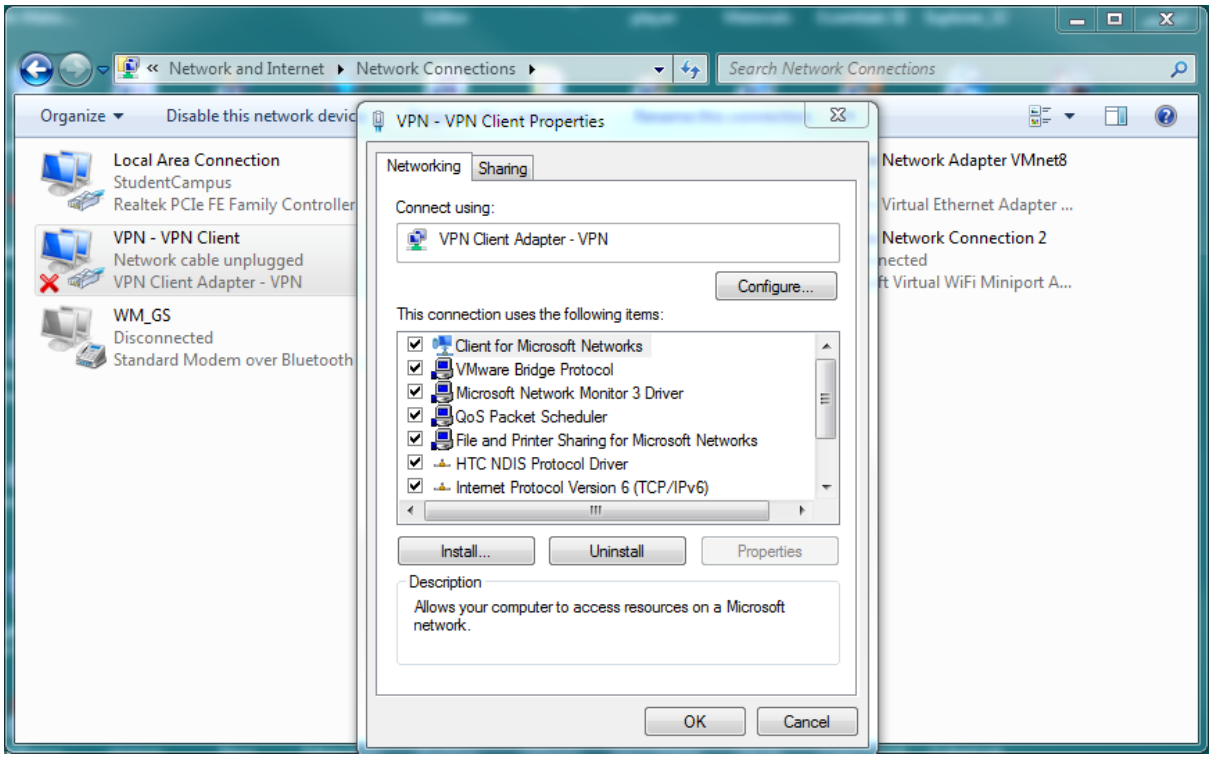


الشكل 6: نافذة Vistumbler

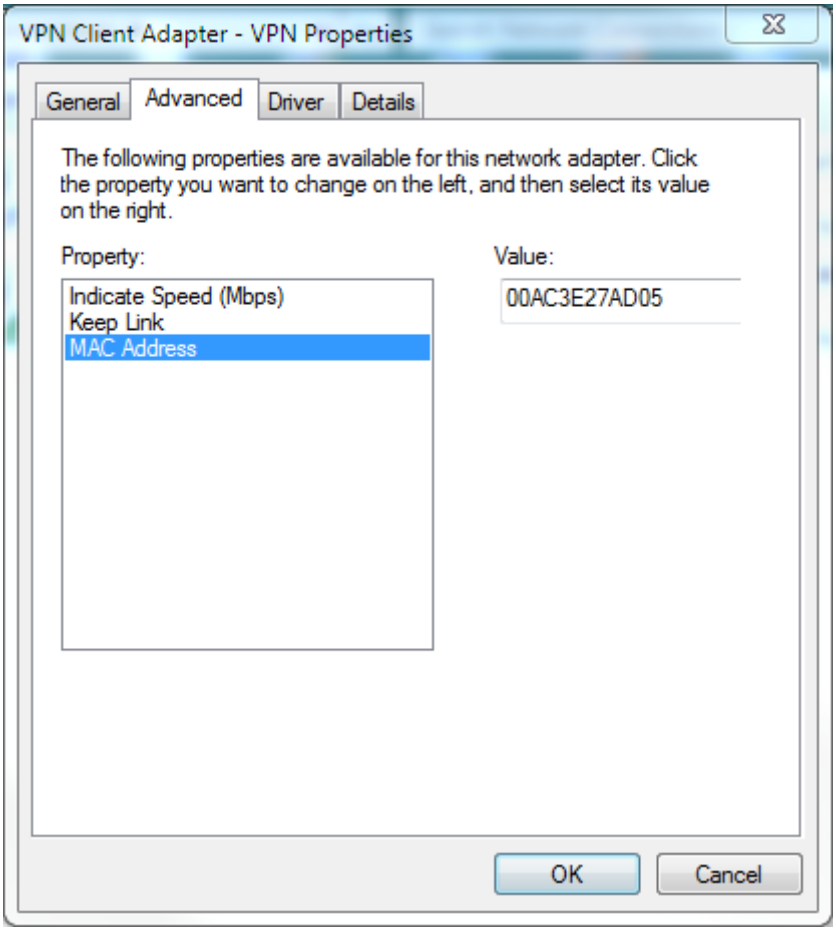
3.5. تغيير عنوان MAC

يهدف هذا التمرين إلى تغيير عنوان MAC لأحد بطاقات الشبكة الموجودة على الحاسب.

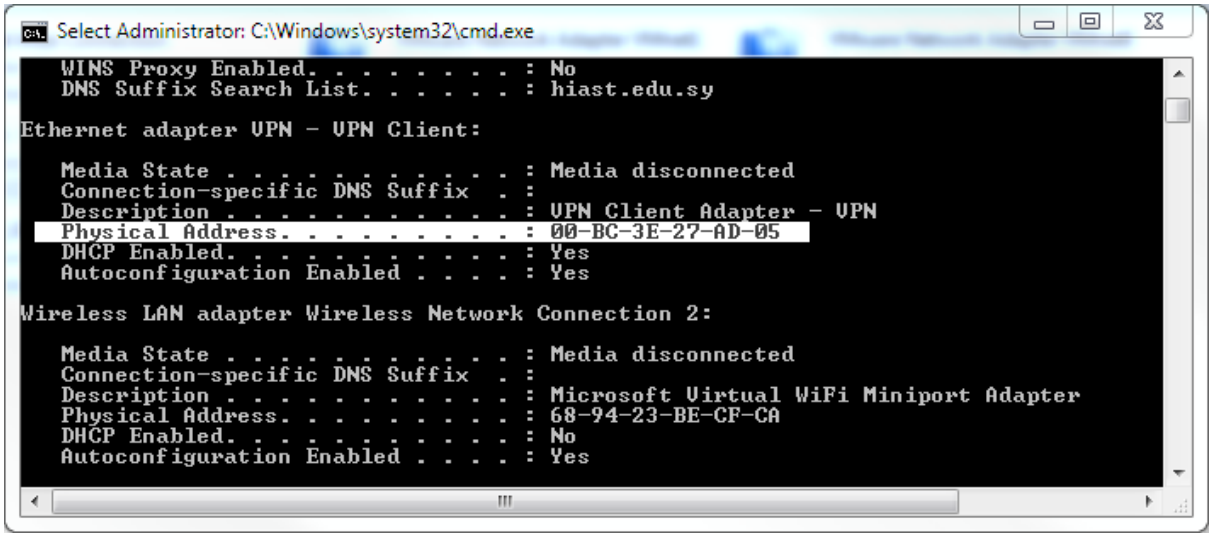
1. Go to Control Panel\Network and Internet\Network Connections
2. Double-click on an adapter icon to show properties (I'll use VPN adapter)



3. Click configure then select Advanced
4. Select MAC Address



5. I will replace the first A with B so MAC address will be 00BC3E27AD05
6. Go to cmd and type ipconfig /all|more

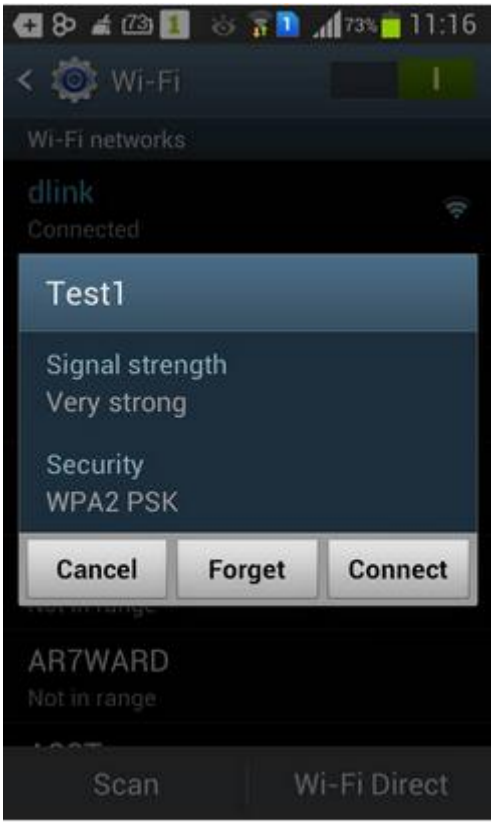


7. Go back to MAC configuration and set the MAC address to its original value

4.5. إعداد مسير لاسلكي افتراضي

أضافت مايكروسوفت وظيفة إلى Windows 7 تتمثل باستضافة شبكة لاسلكية Wireless Hosted Network، عن طريق تعريف عدة بطاقات لاسلكية افتراضية Virtual WiFi ونقطة نفاذ برمجية. يساعد ذلك في المشاركة على اتصال واحد للحاسب المحمول مع بقية أجهزة الشبكة. يمكن أن يستخدم المهاجم هذه الطريقة لتعريف نقطة نفاذ مخادعة Evil Twin.

1. Make sure your wireless adapter is on
2. Go to cmd and type the following (N.B., type ssid and key of your choice)
3. netsh wlan set hostednetwork mode=allow ssid=Test1 key=Test12345
4. netsh wlan start hostednetwork
5. Now, you have an Access Point fully functional
6. Open your wireless connection on your mobile phone, you find the Test1 hotspot as in the next figure



5.5. استخدام تعليمات netsh ضمن Windows 7

تفيد تعليمات netsh في عرض إعداد الشبكات لاسلكية والخصائص الأمنية لها إضافةً إلى إمكانية تغيير بعض الإعدادات.

ندخل إلى netsh عن طريق cmd –> netsh

بعد ذلك يمكننا طلب التعليمات التالية:

1. Run cmd
2. Type netsh
3. Type wlan (the prompt will be as netsh wlan>)
4. show drivers
5. show interfaces
6. show settings
7. Show networks
8. Show profiles
9. Disconnect

الفصل الثامن:مبادئ التحكم بالنفاذ
Access Control Basics

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعرف التحكم بالنفاذ وفهم نماذجه المختلفة
- مناقشة أساليب التحكم بالنفاذ المنطقية
- مناقشة الأنواع المختلفة للتحكم بالنفاذ الفيزيائي
- تعرف خدمات المصادقة

عندما يريد أي شخص الدخول إلى إحدى الشبكات الاجتماعية أو إلى مخدم البريد الالكتروني أو إلى الشبكة الداخلية للشركة التي يعمل بها فإنه يدخل عادةً اسم مستخدم وكلمة مرور. تفيد هذه المعلومات في التحقق من شخصية المستخدم أو المصادقة Authentication. عند النجاح في الدخول إلى الشبكة، يمنح المستخدم مجموعة من الصلاحيات حسب طبيعة عمله في الشركة. تسمى عملية منح الصلاحيات للمستخدم بالتفويض Authorization.

1. ما هو التحكم بالنفاذ؟

التحكم بالنفاذ هو قبول أو عدم قبول استخدام موارد محددة. مع أن مفهوم التحكم بالنفاذ مستخدماً للتعبير عن النفاذ الفيزيائي عبر أبواب مزودة بأجهزة خاصة (كقراءة بصمة الشخص والتعرف عليه قبل فتح باب الدخول له) أو وضع سور معدني حول الشركة يجبر الأشخاص على الدخول من البوابة الرئيسية للشركة غير أن ما يهمنا هنا هو إعطاء أذن النفاذ إلى المعطيات والأجهزة ضمن نظام معلوماتي. يوجد أربعة نماذج للتحكم بالنفاذ إضافةً إلى مجموعة من الممارسات المستخدمة لفرض التحكم بالنفاذ.

1.1. مصطلحات التحكم بالنفاذ

المصادقة Authentication هي التحقق من كون الشخص هو من يدعي كونه عن طريق تقديم معرفات خاصة به مثل كلمة مرور أو بصمة أو أي طريقة أخرى للمصادقة. التفويض Authorization هي عملية إعطاء الأذن للقيام بفعل محدد مثل الدخول إلى النظام.

يلخص الجدول التالي الخطوات التي يقوم بها مستخدم ما للقيام بفعل ما.

الفعل	الوصف	مثال
التعريف Identification	مراجعة الثبوتيات	إدخال اسم المستخدم
المصادقة	التحقق أن الثبوتيات حقيقية	إدخال كلمة المرور
التفويض	منح الأذن بالدخول	السماح للمستخدم بالدخول
النفاذ	منح الحق بالنفاذ إلى موارد محددة	يمنح المستخدم الحق بالنفاذ إلى معطيات محددة

الجدول 1: الخطوات الأساسية في التحكم بالنفاذ

بوجد اصطلاحات أخرى لوصف كيف يفرض نظام حاسوبي التحكم بالنفاذ.

- الغرض Object. الغرض هو مورد محدد مثل ملف أو جهاز عتادي.
- الفاعل Subject. الفاعل هو مستخدم أو إجراء يعمل نيابةً عن المستخدم الذي يحاول النفاذ إلى الغرض.
- العملية Operation. هو الفعل الذي يقوم به الفاعل (المستخدم) على الغرض. كمحاولة مستخدم حذف ملف ما.

يُمنح الأفراد أدوار نفاذ مختلفة حسب الموارد والأغراض. يلخص الجدول 2 هذه الأدوار.

الدور	الوصف	المهام	مثال
المالك Owner	شخص مسؤول عن المعلومة	تحديد المستوى الأمني اللازم للمعطيات وتفويض المهام الأمنية المطلوبة	تحديد إمكانية قراءة الملف SALARY.XLS من قبل مديري القسم
الإداري أو الأمين Administrator or custodian	الفرد الذي عين له الماك القيام بالأعمال اليومية	يراجع دورياً الإعدادات الأمنية ويحافظ على سجلات النفاذ الخاصة بالمستخدمين النهائيين	وضع ومراجعة الإعدادات الأمنية للملف SALARY.XLS
المستخدم النهائي	المستخدم الذي ينفذ إلى المعلومات حسب مسؤولياته الروتينية	اتباع التوجيهات الأمنية التي تضعها المؤسسة دون محاولة تجاوزها	فتح ملف SALARY.XLS

الجدول 2: الأدوار ضمن التحكم بالنفاذ

يبين الشكل 1 إجراءات التحكم بالنفاذ ومصطلحاته.

الشكل 1: إجراءات التحكم بالنفاذ ومصطلحاته

2.1. نماذج التحكم بالنفاذ

نموذج التحكم بالنفاذ هو معيار يقدم منصة عمل معرفة مسبقاً تساعد مطوري البرمجيات والعتاديات الذين يحتاجون إلى تحقيق التحكم بالنفاذ ضمن تطبيقاتهم أو أجهزتهم.

ما أن يتم تطبيق نموذج التحكم بالنفاذ، حتى يستطيع المديرون وضع الإعدادات الأمنية على أساس المتطلبات التي فرضها المالك، الأمر الذي يسمح للمستخدمين النهائيين بالقيام بأعمالهم.

يوجد أربعة نماذج رئيسية للتحكم بالنفاذ: التحكم بالنفاذ الإلزامي والتحكم بالنفاذ التقديري والتحكم بالنفاذ على أساس الدور والتحكم بالنفاذ على أساس القواعد.

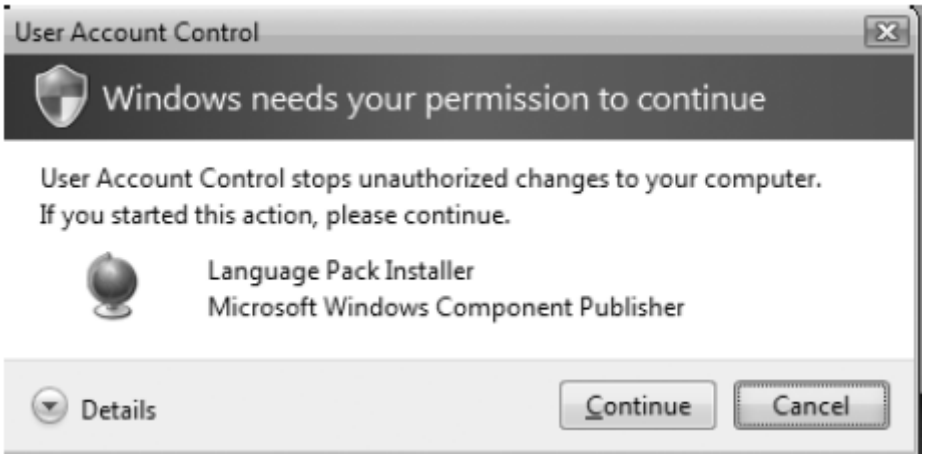
التحكم بالنفاذ الإلزامي Mandatory Access Control (MAC)

يعتبر هذا النموذج الأكثر تقييداً. نجد هذا النموذج في الأنظمة العسكرية حيث تعتبر الناحية الأمنية شديدة الأهمية. يشمل التحكم الإلزامي عنصرين:

- لصيقة Label. يجري هنا اعتبار كل مكون على أنه غرض (حاسب محمول أو ملف أو مشروع) ويعين له لصيقة تصنيفية. تُظهر هذه اللصيقة الأهمية النسبية للغرض مثل خصوصي أو سري أو سري للغاية. يعين للمستخدمين (الفاعلين) لصيقات امتياز (تسمى تصريح).
- مستويات. يجري هنا استخدام تراتبية معتمدة على اللصيقات للأغراض والفاعلين. فمثلاً، سري للغاية ذو مستوى أعلى من سري الذي هو بدوره أعلى من خصوصي.

يمنح نموذج MAC الأذونات عن طريق مطابقة لصيقات الغرض مع لصيقات الفاعل على أساس مستوى كل منهما. فلتحديد إمكانية فتح مستخدم لملف ما تجري مطابقة لصيقة المستخدم مع لصيقة الملف. يجب أن يمتلك الفاعل مستوىً مساوٍ أو أعلى من مستوى الغرض حتي يمتلك حق النفاذ إليه. فإذا كانت لصيقة الغرض هي سري للغاية والفاعل يمتلك لصيقة تفويض من نوع سري فهو لا يستطيع النفاذ إلى الغرض. لا يستطيع الفاعلون تغيير الإعدادات الأمنية للأغراض أو لبقية الفاعلين.

يمكن رؤية تطبيق محدود لنموذج MAC في نظام تشغيل Windows 7 الذي يحوي أربعة مستويات أمنية هي منخفض Low ومتوسط medium ومرتفع High ونظام system. تعمل الإجراءات غير العادية (دون صلاحيات مدير النظام) في المستوى المتوسط. تحتاج بعض العمليات مثل تثبيت تطبيق جديد من قبل مستخدم ما يملك تصنيف أقل من المطلوب (مثل مستخدم عادي) مستوىً أعلى (كالمستوى عالي) لقبول عملية التثبيت. تستدعي هذه العملية تدخل إجرائية User Account Control (UAC). يطلب UAC من المستخدم إدخال كلمة مرور مدير نظام ذو مستوىً أعلى حتى يستطيع تثبيت التطبيق كما هو كوضح في الشكل 2.

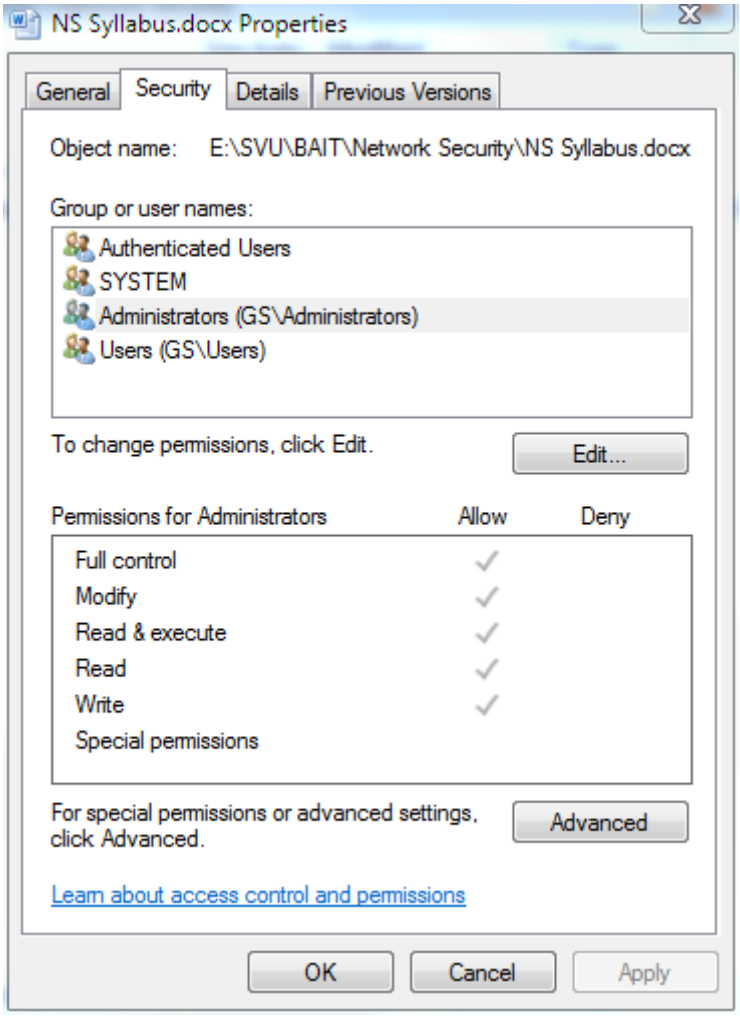


الشكل 2: صندوق حوار التحكم بحساب المستخدم UAC

التحكم بالنفاذ التقديري Discretionary Access Control (DAC)

يعتبر التحكم بالنفاذ التقديري الأقل تقييداً. حسب النموذج التقديري، لكل غرض مالك owner قادر على التحكم الكلي بالغرض. لدى المالكين الحرية الكاملة في خلق الأغراض الخاصة بهم والنفاذ إليها. بالإضافة إلى ذلك، يمنح المالك الأذونات إلى الفاعلين للنفاذ إلى الأغراض التي يملكونها.

يُستخدم النموذج التقديري DAC ضمن أنظمة التشغيل مثل يونيكس ومايكروسوفت ووينـدوز. يبين الشكل 3 نوع التحكم لدى مالك الملف.



الشكل 3: التحكم بالنفاذ التقديري

يعاني DAC من نقطتي ضعف: تتجلى النقطة الأولى في اعتماده على قرار المستخدم النهائي في وضع المستوى الأمني للغرض، الأمر الذي قد ينتج عنه منح أذن غير مناسب لفاعل ما أو منح أذن لفاعل غير مسموح له النفاذ. أما نقطة الضعف الثانية فتعود إلى كون الأذن الممنوح لفاعل ما يرثه أي برنامج يشغله الفاعل. يستغل المهاجمون نقاط الضعف هذه بسبب امتلاك المستخدمون النهائيون مستويات عليا من الامتيازات. ففي حالة تشغيل برمجيثة على حاسوب مستخدم، ستعمل البرمجيثة في نفس سياق امتيازات المستخدم العالية.

التحكم بالنفاذ على أساس الدور Role Based Access Control (RBAC)

يتم هنا التحكم بالنفاذ على أساس العمل الوظيفي للمستخدم داخل المؤسسة. يجري هنا منح الأذونات حسب الدور ومن ثم يجري توزيع كل مستخدم إلى دور محدد. يوضع كل غرض ضمن نمط محدد يسمح للمستخدمين من دور معين بالنفاذ إليه. فمثلاً، يمكننا خلق دور باسم Business_Manager يحدد امتيازات المستخدمين الذين سينتمون إلى هذا الدور. يرث كل مستخدم منتمٍ إلى دور ما جميع أذونات الدور.

تجدر الإشارة هنا إلى أن الدور مختلف عن المجموعات فيمكن لمستخدم أن ينضم إلى عدة مجموعات بنفس الوقت لكن يحدد له دور واحد فقط كما أنه من غير الممكن منح مستخدم أذونات لا يتمتع بها الدور المحدد له.

التحكم بالنفاذ على أساس القاعدة Rule Based Access Control

يستطيع نموذج التحكم بالنفاذ على أساس القاعدة منح الأدوار إلى الفاعلين ديناميكياً اعتماداً على مجموعة من القواعد التي قام بوضعها الأمين أو إداري النظام. يعرف هذا النموذج، من هذا المنظور، وفق التحكم بالنفاذ على أساس الأدوار والقواعد RB-RBAC. فعندما يريد مستخدم ما النفاذ إلى غرض، يختبر النظام القواعد الموجودة ضمن الغرض لإقرار قبول النفاذ.

يُستخدم عادةً التحكم على أساس القواعد لإدارة نفاذ المستخدمين إلى نظام أو أكثر، حيث يمكن لتغيرات الأعمال أن تستدعي تطبيق القواعد التي تحدد تغيرات النفاذ. فمثلاً، عندما يريد مستخدم من شبكة 1 أن ينفذ إلى غرض من شبكة 2 فيمكن للمسير الذي يفصل بين الشبكتين تحديد الدور المناسب لهذا المستخدم. يحوي هذا المسير مجموعة من قواعد التحكم بالنفاذ ويمكن أن يعين دوراً محدداً للمستخدم على أساس عنوان شبكته أو البروتوكول المستخدم. هذا الدور سيحدد فيما إذا كان يحق للمستخدم النفاذ إلى الغرض أو لا. لا يستطيع المستخدمون تغيير القواعد هنا؛ فقط الأمناء أو الإداريون يستطيعون وضع القواعد.

3.1. أفضل ممارسات التحكم بالنفاذ

تشمل أفضل الممارسات على فصل المسؤوليات وتدوير الوظائف والأقل امتيازاً والحجب الضمني والإجازات الإلزامية.

فصل المسؤوليات Separation of duties

من المبادئ الأساسية في الأنظمة المعلوماتية عدم إعطاء شخص واحد تحكماً كاملاً. تتطلب ممارسة فصل المسؤوليات، تقسيم أي إجراء، يمكن أن يؤدي تطبيقه بشكل مخادع إلى ثغرة أمنية، بين أثنين أو أكثر من الأفراد. فمثلاً، إذا وجد شخص واحد يقوم بمسؤوليات المالك والأمين بنفس الوقت فإن هذا الشخص يصبح لديه صلاحيات كاملة على جميع الإعدادات الأمنية للنظام.

تدوير الوظائف Job rotation

الطريقة الثانية لمنع امتلاك شخص واحد قدرة كبيرة من التحكم هي في تدوير الوظائف. هذا يعني أنه يتم تدوير مجموعة من الأشخاص على مجموعة من الوظائف.

الأقل امتيازاً Least privilege

يقصد بالأقل امتيازاً في التحكم بالنفاذ تخصيص أقل قدراً من الأذونات التي تكفي لتأدية وظيفة ما. يفيد ذلك في تقليل السطح المعرض للهجمات عن طريق استبعاد الامتيازات غير الضرورية.

يجب تطبيق الأقل امتيازاً على المستخدمين وعلى الإجراءات التي تعمل ضمن النظام على حدٍ سواء. يوجد عدة خيارات لمنح الامتيازات بطريقة آمنة. ففي أنظمة لينوكس أو يونيكس على سبيل المثال، يمكن لإداري النظام أن يمنح مستخدم محدد أو مجموعة حق النفاذ إلى أوامر من المستوى الأعلى دون كشف كلمة مرور الجذر root لهؤلاء الأشخاص. يكفي المستخدم إدخال الأمر sudo (super user do) الذي يطلب منه كلمة المرور الشخصية ويؤكد الطلب لتنفيذ الأمر.

أما في بيئة ويندوز 7 مثلاً، يمكن للمستخدم العادي الضغط على زر الفأرة اليمين واختيار Run as administrator لترقية الامتيازات الممنوحة له.

الحجب الضمني Implicit deny

يعني الحجب الضمني في التحكم بالنفاذ أنه إذا لم يتحقق شرط ما يتم رفض طلب النفاذ. فمثلاً، إذا كان لدينا جدار نار معرف عليه مجموعة من قواعد النفاذ المعلنة واستقبل طرد لا يحقق أي من القواعد فإنه يرفض هذا الطلب بسبب الحجب الضمني (أي طرد لا يحقق أحد القواعد هو مرفوض).

الإجازات الإلزامية Mandatory vacations

يجب على مقترف عمليات الاحتيال، في الكثير من الحالات، أن يكون موجوداً فيزيائياً بشكل يومي لمواصلة عملية الاحتيال أو الحفاظ على سريتها. تفيد الإجازات الإلزامية في التصدي لهذا النوع من العمليات. بالنسبة للمستخدمين في المواقع الحساسة، يمكن العودة إلى سجلات تدقيق نشاطاتهم عندما يكونون في إجازات طويلة.

2. تحقيق التحكم بالنفاذ

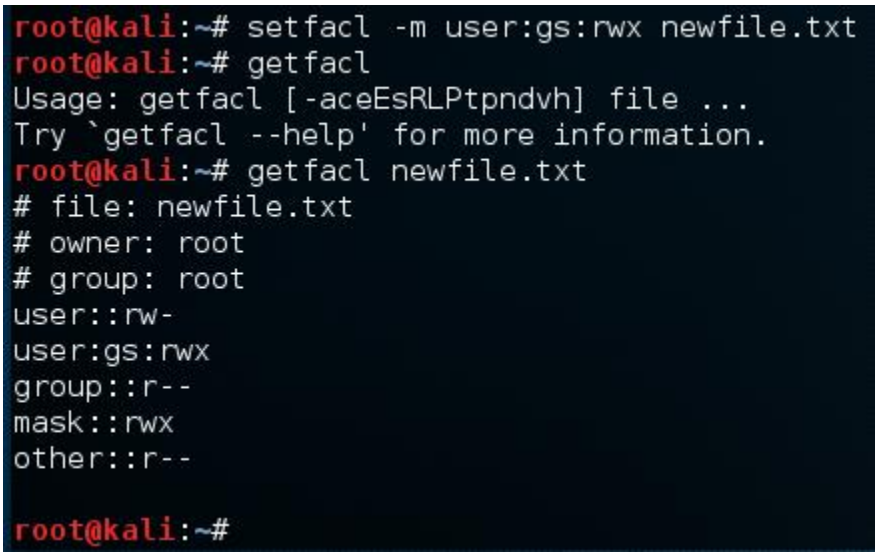
يوجد عدة تقانات لتحقيق التحكم بالنفاذ. نذكر منها قوائم التحكم بالنفاذ ونهج المجموعات وتقييد الحسابات.

1.2. قوائم التحكم بالنفاذ Access Control Lists (ACLs)

قائمة التحكم بالنفاذ هي مجموعة من الأذونات المربوطة بغرض. تحدد هذه القائمة الفاعلين الذين يستطيعون النفاذ إلى الغرض والعمليات التي يستطيعون القيام بها عليه.

مع أن قوائم التحكم بالنفاذ هي معدة لأي نوع من الأغراض إلى أن استخدامها يشمل عادةً ملفات أنظمة التشغيل. فمثلاً، يمكن تعريف قائمة التحكم بالنفاذ ضمن نظام لينوكس باستخدام الأمرين getfacl و setfacl كما هو موضح في الشكلين 4 و5.

الشكل 4: أذونات لينوكس



الشكل 5: أذونات لينوكس

2.2. نهج المجموعات Group policy

يُستخدم نهج المجموعات عادةً في الشركات الكبيرة لفرض التحكم بالنفاذ عن طريق تقييد أفعال المستخدمين التي يمكن أن تشكل خطراً أمنياً، مثل تغيير الحقوق لبعض المجلدات أو تحميل ملف تنفيذي. يمكن أن يتحكم نهج المجموعات بالدخول والخروج من النظام وبإعدادات متصفحات الإنترنت وإعدادات سجلات ويندوز Registry settings وغيرها. يعتمد نظام ويندوز على نهج المجموعات لأنها تؤمن إدارة وإعداد مركزيين للحواسب وللمستخدمين عن طريق المجلد النشط Active Directory (AD).

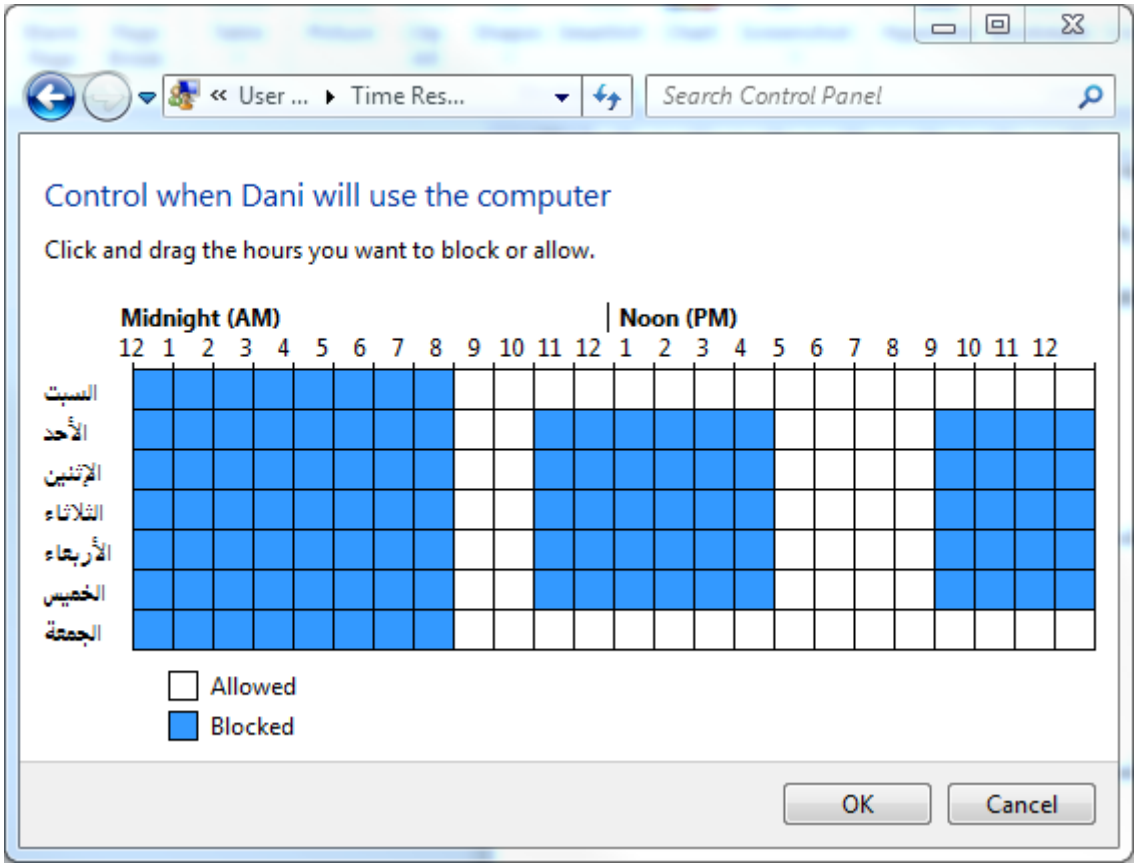
3.2. تقييد الحسابات Account restrictions

يوجد طريقة أخرى لفرض التحكم بالنفاذ عن طريق تقييد حسابات المستخدمين. يمكن هنا التقييد على أساس الوقت أو على أساس مدة صلاحية الحساب.

التقيد على أساس الوقت Time of day

يجري استخدام هذه الطريقة لتحديد الساعات التي يمكن أن يدخل فيها المستخدم إلى النظام (كوقت العمل الفعلي بين الساعة 8 صباحاً و17 عصراً).

يمكن استخدام هذه الطريقة في ويندوز من خلال إعداد نهج المجموعات (انظر الشكل 6).



الشكل 6: تحديد ساعات العمل ضمن نظام ويندوز

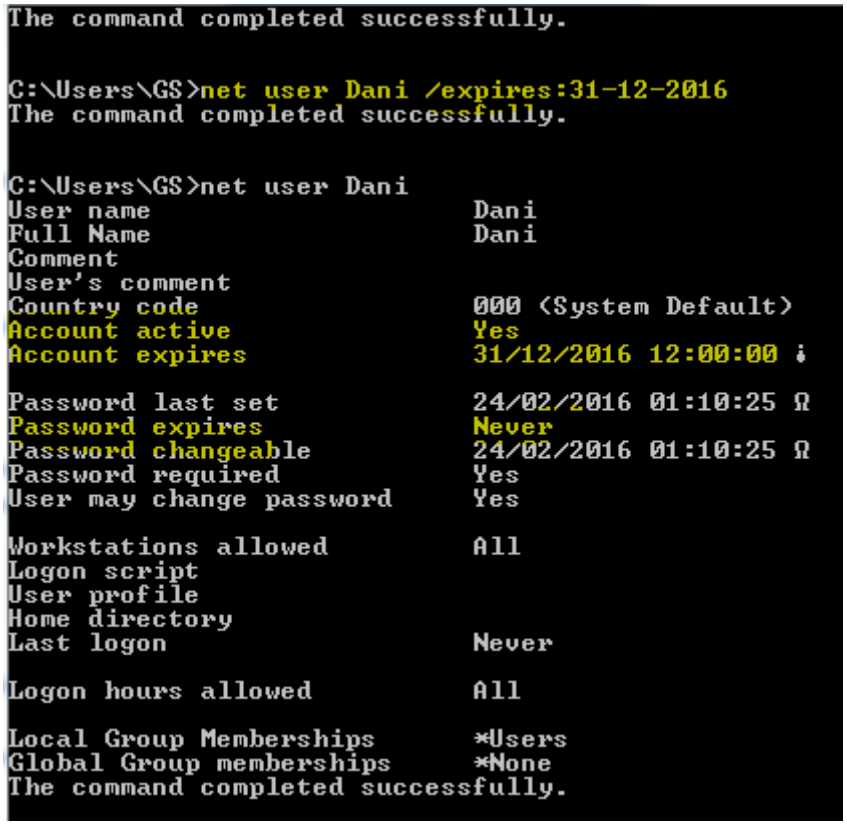
مدة صلاحية الحساب Account Expiration

الحساب اليتيم هو الحساب الذي يبقى نشط بعد مغادرة الموظف صاحب الحساب الشركة بينما الحساب الهامد Dormant هو الحساب الذي لم يتم الدخول إليه منذ مدة طويلة. يمكن أن يشكل هذا النوع من الحسابات خطراً أمنياً. فيمكن لموظف مطرود من الشركة أن يحاول أن ينتقم منها عن طريق سرقة بعض المعلومات الحساسة أو حذفها عن طريق حسابه. أما الحسابات الهامدة، فهي تعطي المهاجم فرصة لاستغلالها بدون أن ينتبه صاحب الحساب أو إداري النظام إلى ذلك.

تم التوصل إلى مجموعة من التوصيات للتعامل مع هذا النوع من الحسابات وهي تشمل:

- انشاء تدابير رسمية. من الأهمية بمكان تعريف تدابير رسمية تعطل حسابات الموظفين الين غادروا الشركة أو استقالوا منها.
- انهاء النفاذ مباشرةً. يجب انهاء أي نوع من النفاذ للموظفين الذين غادروا الشركة.
- مراقبة سجلات log. تفيد السجلات في منع الموظفين من استخدام حسابات هامدة بدلاً عن حساباتهم الأصلية.

يمكن أن تفيد مدة صلاحية الحسابات في معالجة الحسابات اليتيمة أو الهامدة. نحدد لكل حساب مدة زمنية قبل أن تنتهي صلاحيته. انتهاء صلاحية الحساب غير انتهاء صلاحية كلمة المرور. فالحساب عندما تنتهي صلاحيته يصبح غير مفعل. يمكن تحديد مدة صلاحية الحساب بشكل معلن عن طريق تحديد عدد أيام الفاعلية أو تاريخ انتهاء الصلاحية أو في حال لم يتم الدخول إلى الحساب لفترة طويلة. يبين الشكل 7 طريقة تحديد مدة صلاحية حساب المستخدم Dani باستخدام الأمر net user.



الشكل 7: تحديد صلاحية الحساب ضمن ويندوز 7

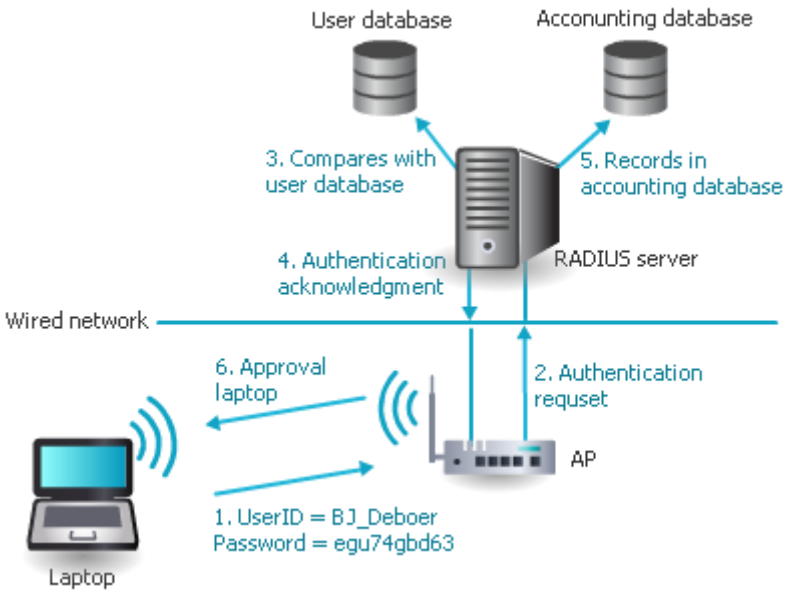
3. خدمات المصادقة Authentication Services

المصادقة هي عملية التحقق من كون المستخدم هو من يدعي كونه عن طريق تقديم إثباتات تؤكد هويته. يمكن تقديم خدمات المصادقة على شبكة من خلال مخدم Authentication, Authorization, and Accounting (AAA) مخصص أو من خلال مخدم مصادقة. من مخدمات AAA المعروفة هناك RADIUS و Kerberos و TACACS و LDAP.

1.3. مخدم RADIUS

طور مخدم Remote Authentication Dial In User Service (RADIUS) عام 1992 وسرعان ما أصبح معيار الواقع وتم اعتماده من قبل غالبية مصنعي الأجهزة الشبكية. زبون RADIUS هو جهاز مثل نقطة النفاذ اللاسلكي مسؤول عن إرسال ثبوتيات المستخدمين وموسطات الاتصالات في صيغة رسائل RADIUS إلى مخدم راديوس. يقوم المخدم بالمصادقة ومن ثم التفويض على الطلبات القادمة من الزبائن ويعيد رسالة جواب. ترسل أجهزة الزبون أيضاً رسائل متعلقة بالمحاسبة accounting messages إلى المخدم. تكمن قوة هذه الخدمة في كون الرسائل لا تتم بين الجهاز اللاسلكي وبين المخدم الأمر الذي يمنع المهاجمين من اختراق المخدم والتأثير على الوضعية الأمنية له.

يبين الشكل 8 الخطوات التفصيلية التي تتم بين جهاز لاسلكي يحقق المعيار IEEE 802.1x وبين مخدم المصادقة.



الشكل 8: مصادقة RADIUS

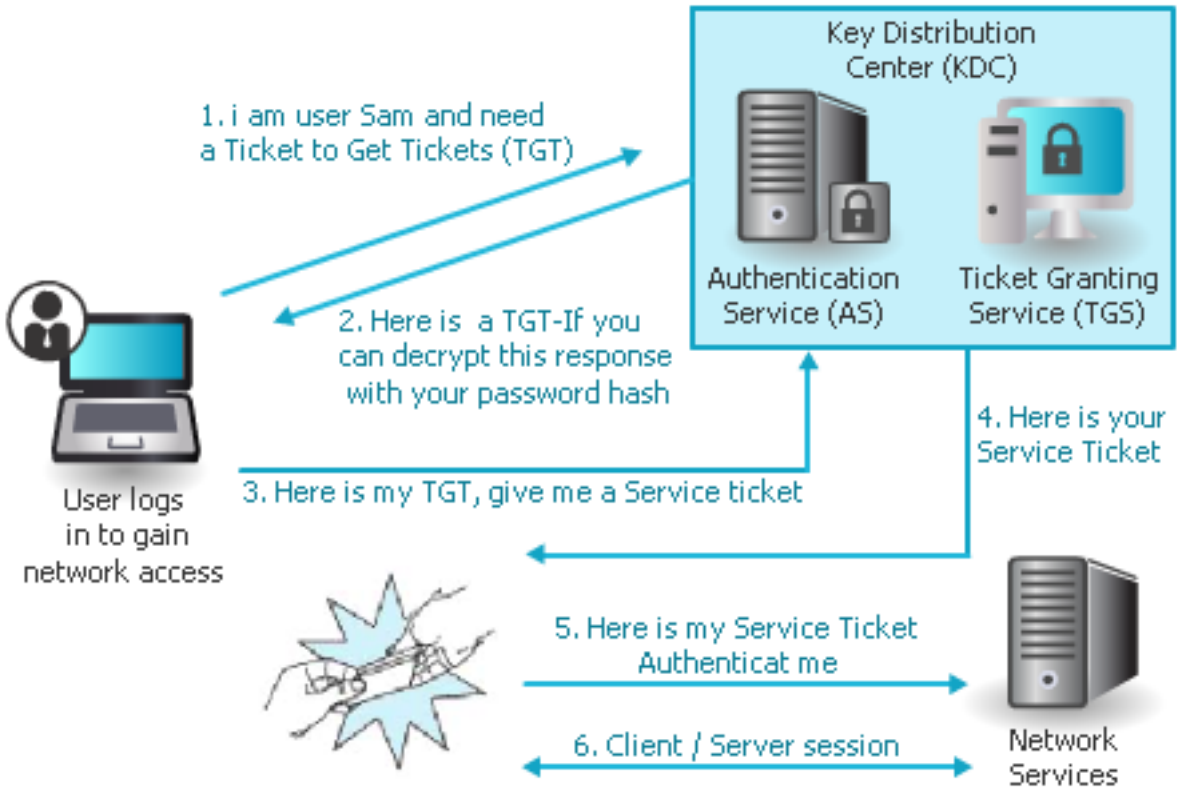
1. يرسل الجهاز اللاسلكي الملتمس Supplicant طلب إلى نقطة النفاذ في سبيل النفاذ إلى الشبكة اللاسلكية. تطلب نقطة النفاذ من المستخدم إدخال الاسم وكلمة المرور.
2. تخلق نقطة النفاذ، التي تعمل كجهة مصادقة، طرد معطيات يدعى طلب المصادقة Authentication request. يحمل هذا الطرد معلومات تعريف عن هوية نقطة النفاذ طالبة الخدمة واسم المستخدم وكلمة المرور. يقوم الزبون (أي نقطة النفاذ) بتشفير كلمة المرور قبل إرسال الطلب إلى مخدم RADIUS. يتم التواصل بين زبون ومخدم RADIUS إما على الشبكة المحلية أو باستخدام شبكة واسعة.
3. عندما يستقبل مخدم RADIUS الطلب، يقوم بالتأكد من هوية نقطة النفاذ المرسلة للطلب ومن ثم فك تشفير طرد المعلومات للتوصل إلى اسم المستخدم وكلمة المرور. تمرر هذه المعلومات إلى قاعدة معطيات أو إلى ملف نصي يحوي اسماء المستخدمين وكلمات المرور للتأكد من صحتها.
4. في حال كان اسم المستخدم وكلمة المرور صحيحين، يرسل مخدم RADIUS إقرار مصادقة يحوي معلومات عن نظام شبكة المستخدم ومتطلبات الخدمة. أما في حال كون المعلومات السابقة غير صحيحة فيتم توجيه رسالة رفض إلى نقطة النفاذ. يرسل مخدم RADIUS ايضاً مفتاح مصادقة أو توقيع للتعريف عن نفسه إلى زبون RADIUS.
5. إذا كانت المحاسبة مفعلة ضمن مخدم RADIUS فيتم خلق مدخلة في قاعدة معطيات المحاسبة.
6. عندما تستقبل نقطة النفاذ معلومات المصادقة من المخدم وتتأكد منها فإنها تفعل الإعدادات اللازمة للسماح للجهاز اللاسلكي بالنفاذ إلى الشبكة.

2.3. خدمة Kerberos

يتم استخدام كيربوروس للتحقق من هوية مستخدمي الشبكات واستخدامه شائع في الجامعات والمؤسسات الحكومية. يستخدم كيربوروس التشفير والمصادقة لضمان الأمن.

يجري استدعاء كيربوروس عندما يريد مستخدم النفاذ إلى خدمة شبكية تتطلب المصادقة. يُزوَد المستخدم بتذكرة Ticket من مخدم كيربوروس للمصادقة. تحوي هذه التذكرة معلومات مرتبطة بالمستخدم. يقدم المستخدم هذه التذكرة إلى الشبكة للنفاذ إلى الخدمات. تفحص الخدمة التذكرة للتأكد من هوية المستخدم وقبول النفاذ في حال نجاح عملية الفحص. من ميزات تذاكر كيربوروس أنها صعبة النسخ بسبب التشفير وأنها تحمل معلومات محددة عن المستخدم وتحصر الأفعال التي يمكن للمستخدم القيام بها وتنتهي صلاحيتها بعد عدة ساعات أو بعد يوم كامل. تتم عمليات إصدار التذاكر وتقديمها ضمن نظام كيربوروس بشكل داخلي وشفاف بالنسبة للمستخدمين.

يبين الشكل التالي خطوات تبادل التذاكر ضمن نظام كيربوروس.



الشكل 9: تبادل التذاكر ضمن نظام كيربوروس

3.3. خدمة TACACS

تعتبر تاكاكس Terminal Access Control Access Control System (TACACS) الشبيهة براديوس، خدمة مصادقة شائع استخدامها ضمن أجهزة نظام تشغيل يونيكس التي تتصل فيما بينها عن طريق توجيه ثبوتيات المستخدمين إلى مخدم مركزي. يمكن أن يكون المخدم المركزي قاعدة معطيات تاكاكس أو ملف كلمات مرور كتلك المستخدمة في لينوكس مع دعم لبروتوكول تاكاكس.

نظام تاكاكس هو نظام خاص مملوك لشركة Cisco الذي طور عدة إصدارات منها XTACACS و TACACS+ المتوافر حالياً.

يوجد بعض الاختلافات بين راديوس وتاكاكس يلخص الجدول التالي أهمها.

الميزة	RADIUS	TACACS+
بروتوكول النقل	UDP	TCP
المصادقة والتفويض	موحدة	منفصلة
الاتصال	غير مشفر	مشفر
التفاعل مع Kerberos	لا	نعم

الجدول 3: مقارنة بين RADIUS و TACACS+

4.3. خدمة Lightweight Directory Access Protocol (LDAP)

خدمة الدليل هي قاعدة معطيات مخزنة على الشبكة وتحوي معلومات عن المستخدمين مثل أسمائهم وعناوين بريدهم الالكترونية وأرقام هواتفهم واسماء الدخول وغيرها والأجهزة الشبكية. تتابع خدمة الدليل جميع الموارد الموجودة على الشبكة وامتيازات المستخدمين على هذه الموارد وتمنع أو تمنح النفاذ إلى هذه الموارد اعتماداً على معلومات خدمة الدليل. تسهل خدمة الدليل منح الأذونات أو الامتيازات لمستخدمي الشبكة.

عرفت المنظمة العالمية للمعايير ISO معياراً لخدمة الدليل يعرف تحت اسم X.500. يهدف X.500 إلى معيرة طريقة تخزين المعطيات بشكل يسمح لأي حاسوب بالدخول إليها. فهو يزود إمكانية البحث عن المعلومة حسب الاسم (خدمة الصفحات البيضاء) إضافةً إلى التصفح والبحث عن المعلومات حسب التصنيف (خدمة الصفحات الصفراء). توضع المعلومات ضمن قاعدة معلومات الدليل Directory Information Base (DIB). يتم ترتيب المكونات ضمن الدليل DIB على شكل شجري يطلق عليه اسم شجرة معلومات الدليل Directory Information Tree (DIT). كل مدخلة هي غرض مُسمى Named object ويحوي مجموعة من السمات Attributes. يجري تعريف لكل سمة نوع وقيمة أو أكثر. يعرِّف الدليل السمات الإلزامية والخيارية لكل صف من الأغراض. يمكن لكل غرض مسمى أن يحوي صف أغراض واحد أو أكثر مرتبط معه.

يعرِّف X.500 بروتوكولاً يسمح لتطبيق الزبون بالنفاذ إلى دليل X.500 يعرف باسم بروتوكول النفاذ إلى الدليل Directory Access protocol (DAP). بما أن بروتوكول DAP هو ضخم جداً ويصعب تحميله وتشغيله على حاسوب شخصي، يستعاض عنه ببروتوكول Lightweight DAP (LDAP) أو X.500 Lite الذي هو مجموعة جزئية منه يعمل باستخدام TCP/IP.

يسمح LDAP لأي تطبيق يعمل على أي منصة عمل ممكنة من الحصول على معلومات من الدليل. بما أن بروتوكول LDAP هو بروتوكول مفتوح فلا يحتاج أي تطبيق إلى معرفة نوع مخدم LDAP. يوجد حالياً الكثير من مخدمات LDAP التي تم تحقيق محركها عن طريق أنظمة قواعد معطيات علاقاتية وتتصل عن طريق وثائق Extensible Markup Language (XML) المتبادلة باستخدام بروتوكول HTTP.

من مشاكل بروتوكول LDAP أنه عرضه لهجوم حقن LDAP وذلك لأنه لا يتم تصفية مدخلات المستخدمين الأمر الذي يسمح للمهاجم باسترجاع معلومات من قاعدة معطيات LDAP أو تغيير محتوياتها.

4. تمارين عملية

1.4. تفعيل IEEE 802.1x

سنفعّل في هذا التمرين IEEE 802.1.x على حاسب ويندوز 7 مزود ببطاقة شبكة محلية. يجب هنا الدخول كإداري نظام.

1. Enable the Wired AutoConfig service from start=> run services.msc
2. Select standard tab
3. Scroll down to Wired AutoConfig and right-click it and click start
4. Go to control panel
5. Click Network and Sharing Center
6. In the left pane, click change adapter settings
7. Double-click the network interface card being used.
8. Click Properties.
9. If you are prompted by UAC, enter the password or click Yes.
10. Click Authentication.
11. Click Enable IEEE 802.1X authentication if necessary.
12. If necessary, under Choose a network authentication method, select Microsoft Protected EAP (PEAP).
13. Click Additional Settings and view the different IEEE 802.1X options.
14. Click Cancel.
15. Click OK.

2.4. استكشاف التحكم بحسابات المستخدمين UAC غير المنتهية

تزود ويندوز 7 خيارات متعددة للتحكم بحسابات المستخدمين. سنحاول إعدادها واختبارها.

1. Click the Start button and then click Control Panel.
2. Click Action Center
3. click Change User Account Control Settings.
4. The User Account Control Settings dialog box is displayed. move the slider up to the higher level of Always notify.
5. Click OK.
6. In the Control Panel menu, under System, click Remote settings then Allow remote Assistance connections to this computer.
7. The UAC confirmation box is displayed. Click No.
8. In the Control Panel menu, under Action Center, click Change User Account Control Settings.
9. The User Account Control Settings dialog box is displayed. Move the slider down to the lowest level of Never notify.
10. Click OK.
11. In the Control Panel menu, under System, click Allow remote access. What happens?
12. Return to the Control Panel menu and under Action Center, click Change User Account Control Settings.
13. Change the account settings to Notify me only when programs try to make changes to my computer.
14. Now try to click Allow remote access. What happens?
15. Return to the Control Panel menu, and under Action Center, click
16. Change User Account Control Settings.
17. Change the account settings to Notify me only when programs try to make changes to my computer (do not dim my desktop).
18. Now try to click Allow remote access. What happens?
19. Return to the Control Panel menu, and under Action Center, click Change User Account Control Settings.
20. The User Account Control Settings dialog box is displayed. Move the slider up to the higher level of Always notify.
21. Click OK.

الفصل التاسع:المصادقة وإدارة الحسابات

Authentication and Account Management

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعرف الأنواع الثلاثة للمصادقة
- شرح آلية وأهداف الدخول الوحيد
- فهم إجراءات إدارة الحسابات وكلمات المرور
- تعريف أنظمة التشغيل الموثوقة

المصادقة، في الأنظمة المعلوماتية، هي إجرائية التأكد من كون الشخص الذي يحاول النفاذ إلى مورد ما هو أصلي Authentic.

1. ثبوتيات المصادقة Authentication Credentials

لنأخذ السيناريو التالي: يركن موظف ما سيارته في الموقف المخصص للشركة التي يعمل بها ومن ثم يقفل باب السيارة باستخدام المفتاح أو جهاز التحكم عن بعد؛ يدخل من الباب الرئيسي للشركة حيث يتعرف عليه حارس المبنى ويتركه يدخل؛ عندما يصل إلى القسم الذي يعمل فيه يقوم بإدخال رمز دخول يعرفه على جهاز لكي يفتح له باب الدخول إلى القسم.

لقد استخدم الموظف في هذا السيناريو ثلاثة أنواع من المصادقة. أولاً، قفل السيارة بمفتاح يملكه. ثانياً، تعرف حارس المبنى عليه أو على ما يكون. ثالثاً، أدخل رمز الدخول الذي يعرفه.

فإذاً ، يمكننا تحقيق لمصادقة (أو الاستيقان) بالاعتماد على ما يعرفه الشخص أو على ما يملكه أو على ما يكون.

1.1. ماذا تعرف What You Know؟: كلمات المرور

تعتمد غالبية الأنظمة على إدخال اسم المستخدم للتعريف عنه ومن ثم إدخال كلمة المرور التي لا يعرفها إلى المستخدم للمصادقة عليه. كلمة المرور هي مجموعة من المحارف والأرقام التي يجب أن لا يعرفها إلا المستخدم الذي وضعها. يعتبر النفاذ باستخدام اسم وكلمة مرور من أكثر أنواع المصادقة انتشاراً في أيامنا هذه.

بالرغم من انتشارها الواسع، غير أن كلمات المرور تؤمن حماية ضعيفة وهي عرضة لمجموعة متنوعة من الهجمات، الأمر الذي يتطلب تقويتها.

ضعف كلمات المرور

يعود ضعف كلمات المرور إلى ذاكرة المستخدم التي يمكن أن تحفظ مجموعة محددة من الأشياء. تضفي كلمات المرور عبئاً إضافياً على ذاكرة الإنسان من منظورين. أولاً، يصعب حفظ كلمات المرور الطويلة والمعقدة. وثانياً، يجب على المستخدمين حفظ كلمات مرور لمجموعة من الحسابات المختلفة مثل مواقع التواصل الاجتماعي وعلب البريد الالكتروني والحسابات المصرفية وحسابات العمل. يملك الإنسان وسطياً حوالي 15 كلمة مرور.

تزدار الصعوبة عندما تضع السياسات الأمنية مدة صلاحية لكلمة المرور أو تمنع استخدام كلمات مرور سابقة أو قريبة منها.

الهجمات التي تشن على كلمات المرور

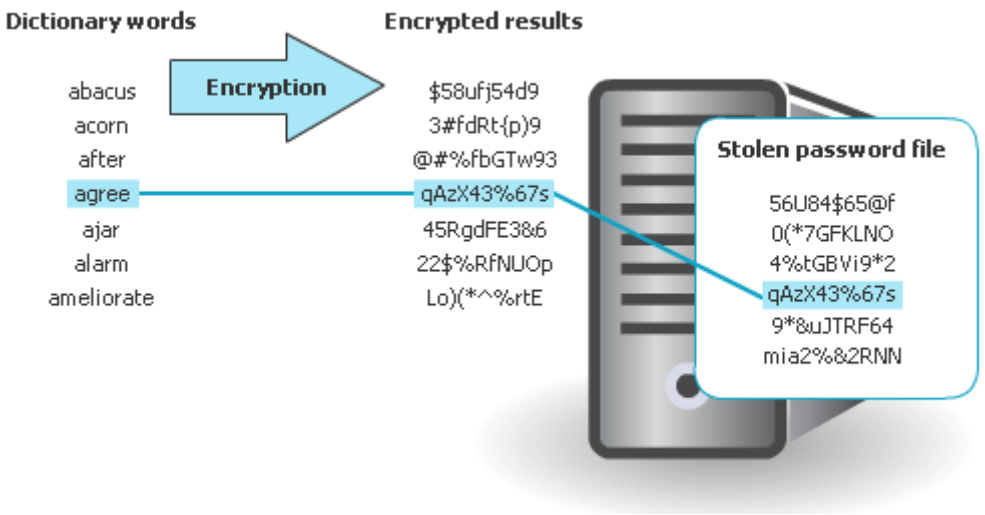
- الهندسة الاجتماعية. مثل التصيد أو مراقبة المستخدم عندما يدخل كلمة المرور Shoulder Surfing أو الغوص في حاويات القمامة.
- الالتقاط. يوجد عدة تقنيات تسمح بالتقاط كلمات المرور. عند الإدخال باستخدام مسجلات ضغطات المفاتيح أو عند النقل باستخدام رجل في المنتصف أو هجوم الإعادة. أو باستخدام محلل بروتوكولات لاكتشاف كلمات المرور عند نقلها.
- إعادة الضبط Resetting. إذا استطاع المهاجم الوصول إلى حاسب الضحية فيمكنه تصفير كلمة المرور ومن ثم إعادة وضع كلمة مرور جديدة. يجب هنا إقلاع الحاسوب من قرص مضغوط CD أو محرك فلاش USB يمتلك نظام تشغيل مختلف وبرنامج يسمح بإعادة ضبط كلمات المرور.
- الحزر على الخط online guessing. يحاول هنا المهاجم حزر كلمة المرور عند ظهور صندوق حوار إدخال ثبوتيات الضحية. طبعاً هذه الطريقة غير عملية إذا كانت كلمة المرور طويلة ومعقدة.
- كسر كلمات المرور خارج الخط Offline cracking. يلجأ المهاجمون، بسبب عدم فعالية الحزر على الخط، إلى تقنية كسر كلمات المرور. يتم عادةً تخزين كلمات المرور بشكل مشفر على ملف ضمن نظام التشغيل. عندما يدخل مستخدم إلى النظام ويدخل كلمة المرور فإنه يتم تشفيرها ومقارنتها مع كلمات المرور الموجودة ضمن الملف المشفر ويسمح للمستخدم بالدخول في حال التطابق. يلجأ المهاجمون إلى سرقة ملف كلمات المرور المشفرة وتحميله ضمن حاسوبهم. يحاول المهاجم بعد ذلك مقارنة كلمات المرور المشفرة مع كلمات يقوموا بتوليدها وتشفيرها وعند وجود تطابق يكونوا قد اكتشفوا كلمة مرور.

يوجد عدة تقنيات لكسر كلمات المرور خارج الخط. إحداها هو استخدام هجوم القوة القاسية الآلي Brute force حيث يتم توليد جميع كلمات المرور الممكنة باستخدام جميع تراكيب الأحرف letters والأرقام والمحارف characters ومن ثم تشفيرها ومطابقتها مع ملف كلمات المرور المشفرة. عند تنفيذ برنامج يقوم بكسر كلمات المفاتيح بالقوة القاسية، يقوم المهاجم بإدخال المتغيرات التالية المتعلقة بنوع كلمات المرور المطلوب توليدها:

- طول كلمة المرور. الطول الأصغري والأعظمي لكلمات المرور المطلوب توليدها (مثل ولد كلمات مرور محصور طولها بين 1 و 12 حرف).
- مجموعة المحارف Character set. هي مجموعة الأحرف والأرقام والمحارف والرموز التي تتألف منها كلمة المرور.
- اللغة. تسمح بعض البرامج باختيار لغات متعددة.
- النموذج Pattern. يمكن تخفيض زمن الاكتشاف إذا كنا نعرف جزء من كلمة المرور. يمكن هنا استخدام محارف مثل "?" للاستعاضة عن رمز واحد والمحرف "*" للاستعاضة عن مجموعة مكونة من عدة محارف. فإذا كنا نعرف أن كلمة المرور مكونة من ستة محارف وأول محرفين هما xt فيمكن إدخال النموذج xt????.

- القفزات Skips. بما أن غالبية كلمات المرور هي مشتقة من كلمات اللغة، فيمكن ضبط بعض برامج القوة القاسية للقفز عن (إهمال) تراكب الأحرف عديم المعنى مثل (xrtjuh) وتوليد تراكبات مفهومة مثل widesky و bluesky.

يوجد نوع آخر من الهجمات خارج الخط لكسر كلمات المفاتيح يعرف باسم هجوم القاموس Dictionary attack. يقوم المهاجم هنا باستخدام كلمات من القاموس لتوليد كلمات المرور ومن ثم تشفيرها ومقارنتها مع ملف كلمات المرور المشفرة كما هو موضح في الشكل التالي:



الشكل 1: هجوم القاموس

يوجد شكل آخر لهجوم القاموس يعرف باسم الهجوم الهجين، حيث يتم تغيير كلمات القاموس عن طريق إضافة أرقام إلى نهاية كلمة المرور المولدة أو كتابة كلمات المرور بالمقلوب أو إضفاء تغيير بسيط على الكلمات أو إضافة محارف خاصة مثل &,% ,!, #, $, @.

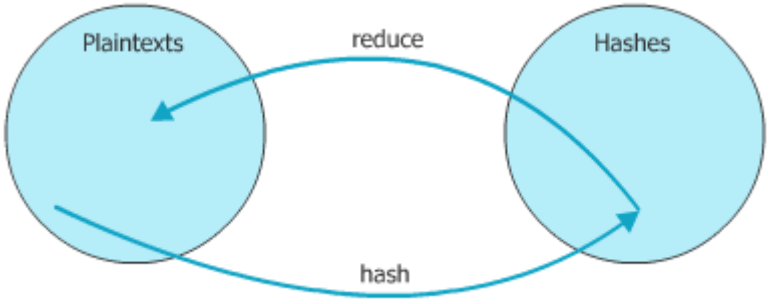
يفضل المهاجمون حالياً استخدام جداول قوس قزح Rainbow tables التي هي ملفات تحوي كلمات مرور مشفرة ومسبقة التوليد. تكمن الفكرة وراء جداول قوس قزح في تقليل حجوم التخزين عن طريق زيادة الاعتماد على وحدة المعالجة المركزية.

تكون كلمات المرور ضمن الملف مهشرة ولا يوجد تابع يعيد كلمة المرور من القيمة المهشرة. لذلك يوجد طريقتين لتحقيق هذه العملية:

1. تهشير كل نص صريح ممكن واحد تلو الآخر حتى نصل إلى الهاش.
2. تهشير كل نص صريح ممكن واحد تلو الآخر مع تخزين كل هاش مولد ضمن جدول مفرز بحيث يمكن البحث عن هاش ضمنه دون توليد الهاش مرة أخرى.

الطريقة الأولى تتطلب وقتاً طويلاً بينما تتطلب الطريقة الثانية حجم تخزين كبير. جداول قوس قزح هي حل وسط بين الطريقتين. حتى نستطيع فهم جداول قوس قزح لا بد من التطرق لتوابع الاختزال Reduction function.

تابع الاختزال يأخذ قيمة هاش ويولد نص صريح لها (عكس تابع التهشير). انتبه أن تهشير نص صريح ومن ثم اختزاله لا يعيد نفس القيمة أي أن تابع الاختزال ليس مقلوب تابع التهشير.



الشكل 2: تابع الاختزال وتابع التهشير

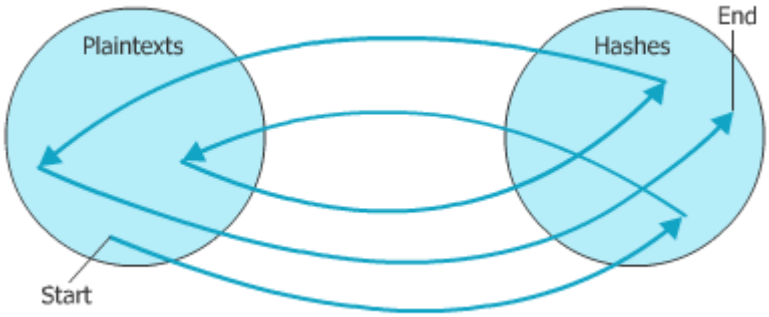
بفرض أن مجموعة النصوص الصريحة هي {6}[0123456789] أي أننا نريد توليد جدول قوس قزح لجميع الأرقام المكونة من ست مرتبات باستخدام تابع التهشير MD5(). يمكن أن تكون قيمة الهاش لنص صريح كما يلي:

MD5("493823") -> "222f00dc4b7f9131c89cff641d1a8c50"

أما بتابع الاختزال فيمكن أن يأخذ نتيجة التهشير السابقة كدخل ويكون خرجه أول ستة أرقام منه، أي:

R("222f00dc4b7f9131c89cff641d1a8c50") -> "222004"

جدول قوس قزح هو عبارة عن سلاسل Chains تنتج عن التطبيق المتتابع للتهشير والاختزال تبدأ من نص صريح معين وتنتهي بهاش معين. يخزن الجدول فقط نقطة البداية (النص الصريح الذي يختار عشوائياً) ونقطة النهاية (الهاش الذي قررنا التوقف عنده).



الشكل 3: إحدى سلاسل جدول قوس قزح

بعد تخزين عدة سلاسل يصبح شكل جدول قوس قزح على الشكل التالي:

```
iaisudhiu –> 4259cc34599c530b1e4a8f225d665802
oxcvioix –> c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf –> 3cd696a8571a843cda453a229d741843
[…]
sodifo8sf –> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

يمكننا الآن الاستفادة من السلاسل. لدينا قيمة هاش ولا نعرف النص الصريح المقابل له ونريد أن نعرف إذا كان الهاش موجوداً ضمن إحدى السلاسل المولدة. نتبع الخوارزمية التالية:

1. بدء حلقة لا نهائية
2. نبحث عن الهاش ضمن القيم الموجودة في آخر كل سلسلة، إذا وجدنا الهاش نتوقف عن البحث.
3. إذا لم يكن الهاش موجوداً نقوم باختزال الهاش إلى نص صريح ومن ثم تهشير النص الصريح هذا.
4. العودة إلى 2
5. إذا تطابق الهاش مع إحدى قيم الهاش النهائية، فإن السلسلة التي ضمنها تم التطابق تحوي الهاش الأصلي.

يمكننا الآن البدء من النص الصريح الموجود في بدء السلسلة المكتشفة وتطبيق الهاش والاختزال حتى نصل إلى الهاش المطلوب والنص الصريح المقابل له (أي الخطوة ما قبل الأخيرة).

الدفاع عن كلمات المرور

يتطلب الدفاع عن كلمات المرور خطوتين: أولاً خلق كلمات مرور قوية وثانياً إدارة كمات المرور بشكل سليم.

- خلق كلمات مرور قوية. تقود معرفة طرق شن الهجمات على كلمات المرور إلى استشراف صرورة توليد كلمات مرور قوية. معظم كلمات المرور تحوي كلمة جذر (ليس بالضرورة مأخوذة من القاموس لكنها منطوقة) ومرفق الذي هو لاحقة نهائية (في 90% من الحالات) أو بادئة (10% من الحالات) مثل SVU12 أو 2016SVU. يقوم برنامج كسر كلمات المرور أولاً باختبار 1000 كلمة مرور معروفة (مثل 123456 و paswword1). إذا لم ينجح، يقوم بإعادة التجربة بعد إضافة 100 لاحقة نهائية إلى كلمات المرور المعروفة (مثل 1 و 4u و abc). هذا يولد 100,000 تركيبة ممكنة قادرة على كسر حوالي 25% من جميع كلمات المرور. بعد ذلك، يستخدم البرنامج 5000 كلمة من كلمات القاموس الشائعة و10,000 اسم و 100,000 من كلمات القاموس الشاملة وتراكيب تتدرج من النماذج اللفظية من القاموس phonetic pattern إلى تغيير كلمات القاموس باستخدام الأحرف الصغيرة (أكثر استخداماً) أو الكبيرة إلى استخدام أحرف كبيرة في البداية (ثاني أكثر شيوعاً) أو جميع الأحرف كبيرة ثم وضع المحارف اللاحقة بالحروف الكبيرة. يقوم البرنامج أيضاً بتبديل الأحرف الشائعة مثل وضع $ مكان s ووضع @ مكان a ووضع 3 مكان E وهكذا. أخيراً، يستخدم البرنامج مرفقات مختلفة مع الكلمة الجذر مثل:

- جميع تراكيب رقمين
- التاريخ منذ 1900 وحتى الآن
- جميع تراكيب 3 أرقام
- رمز واحد (#, $, %)
- رقم واحد ثم رمز واحد
- جميع تراكيب رمزين

يساعد فهم خطوات كسر كلمات المرور في تشكيل التوجيهات التالية عند خلق كلمات المرور:

- لا تستخدم كلمات المرور التي تتكون من كلمات من القاموس أو كلمات لفظية
- لا تستخدم أعياد الميلاد أو أسماء من أفراد العائلة وأسماء الحيوانات أو العناوين أو أي معلومة شخصية
- لا تكرر المحارف مثل (zzz) أو استخدام تسلسلات مثل (abc, 123)
- لا تستخدم كلمات مرور قصيرة. يفضل أن يكون طول كلمة المرور 12 محرفاً على الأقل.

- إدارة كلمات المرور. تتمثل إحدى طرق منع كسر كلمات المرور في تجنب سرقة الملف الذي يحوي كلمات المرور المهشرة. يوجد عدة دفاعات ضد سرقة هذا الملف:
  - عدم ترك الحاسوب يعمل دون حضور أحد حتى ولو كان ضمن مكتب مقفل.
  - لا تضبط الحاسوب ليقلع من القرص المضغوط أو أي جهاز آخر
  - حماية ROM BIOS بكلمة مرور
  - قفل حاوية الحاسوب فيزيائياً بحيث لا يمكن فتحه.

كما تشكل الإدارة السليمة لكلمات المرور ما يلي:

- تغيير كلمات المرور بشكل متكرر
- لا تستخدم كلمات مرور قديمة
- لا تكتب كلمات المرور في أي مكان
- ضع كلمة مرور مختلفة لكل حساب
- استخدم كلمة مرور مؤقتة عند الحاجة لإعطائها لشخص آخر محتاج إلى النفاذ إلى حسابك وغير كلمة المرور حالما تنتهي عملية النفاذ
- لا تسمح للحاسوب بالتوقيع عنك آلياً أو بتخزين كلمات المرور
- لا تدخل كلمات المرور لحواسيب موجودة في أماكن عامة أو أي حاسب آخر يمكن أن يكون مصاب
- عدم إدخال كلمة مرور إذا كنت متصلاً بشبكة لاسلكية غير مشفرة

يمكن جعل كلمات المرور قوية عن طريق استخدام محارف خاصة غير موجودة على لوحة المفاتيح أو استخدام محارف من النوع non-keyboard characters. يمكن خلق هذه المحارف باستخدام الضغطات Alt + number من لوحة الأرقام وليس من أعلى لوحة المفاتيح فمثلاً ALT + 0163

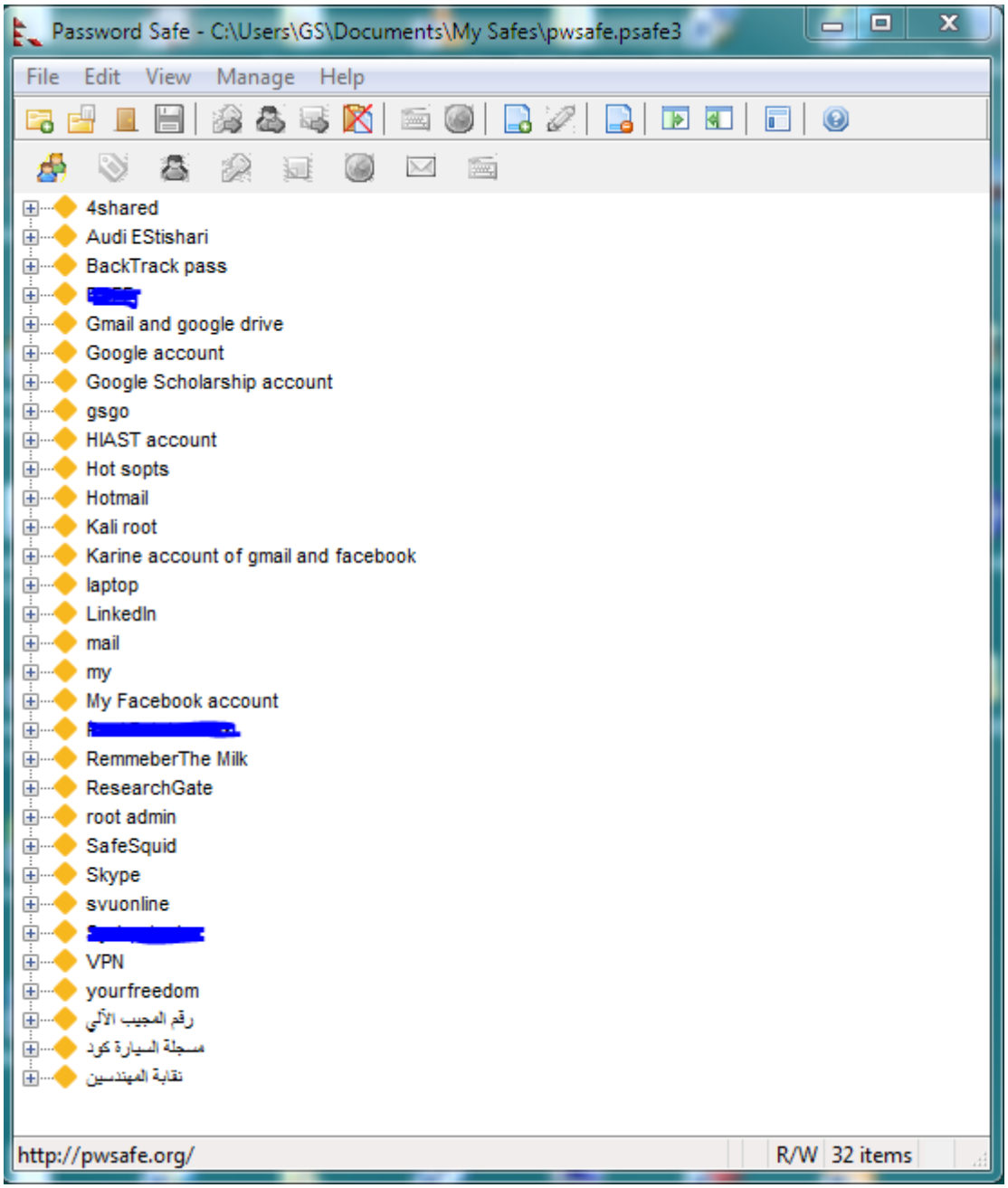
تنتج الرمز £. حتى تحصل على قائمة بالمحارف بدون لوحة المفاتيح نفذ الأمر run => charmap.exe (انظر الشكل التالي).

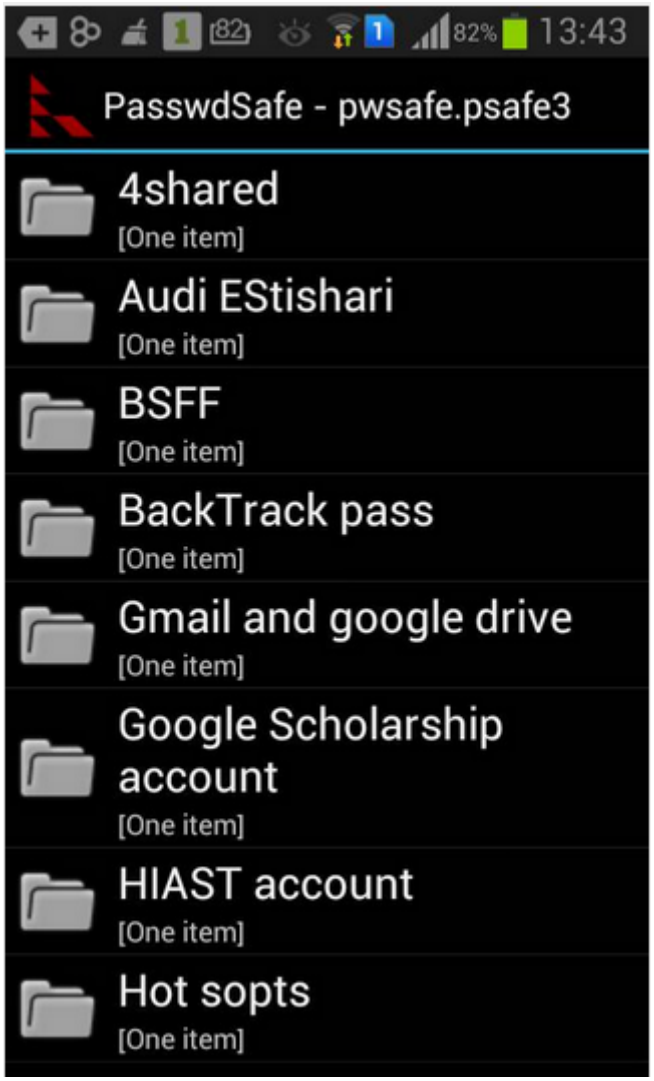
ملاحظة: لا تدعم بعض أنظمة التشغيل أو بعض التطبيقات طريقة الإدخال هذه كما أن الدخول إلى حساب باستخدام الهواتف المحمولة يصبح غير ممكناً.

الشكل 4: خريطة محارف ويندوز

- ملحقات كلمات المرور. تتمثل إحدى الطرق المتبعة لتسهيل حفظ أو إدارة كلمات المرور المتعددة في استخدام ميزة Autocomplete التي تدعمها بعض متصفحات الإنترنت مثل IE و Firefox والتي تخزن نسخة مشفرة ضمن ملف السجلات. طريقة الإدارة الثانية هي باستخدام تطبيق لإدارة كلمات المرور Password Management Application يسمح بتخزين عدة كلمات مرور ضمن ملف مشفر. يلزم المستخدم هنا تذكر كلمة مرور واحدة للدخول إلى هذا التطبيق ومن ثم مشاهدة أي كلمة مرور مخزنة أو استخدام copy–paste للصقها عندما نفتح تطبيق يطلب كلمة مرور. من البرامج التي تساعد في إدارة كلمات المرور Password Safe الذي يقدم، إضافةً إلى إدارة كلمات المرور إمكانية مزامنة كلمات المرور مع نفس البرنامج على الهاتف الذكي. يوجد عدة أنواع من هذه التطبيقات، منها

ما يجب تثبيته على كل حاسب شخصي أو هاتف محمول ومنها ما يمكن حمله ضمن سواقة فلاش ومنها ما يتم الدخول عليه على الخط عبر الإنترنت.





الشكل 5: واجهة تخاطب برنامج Password Safe على الحاسوب وعلى الهاتف الذكي

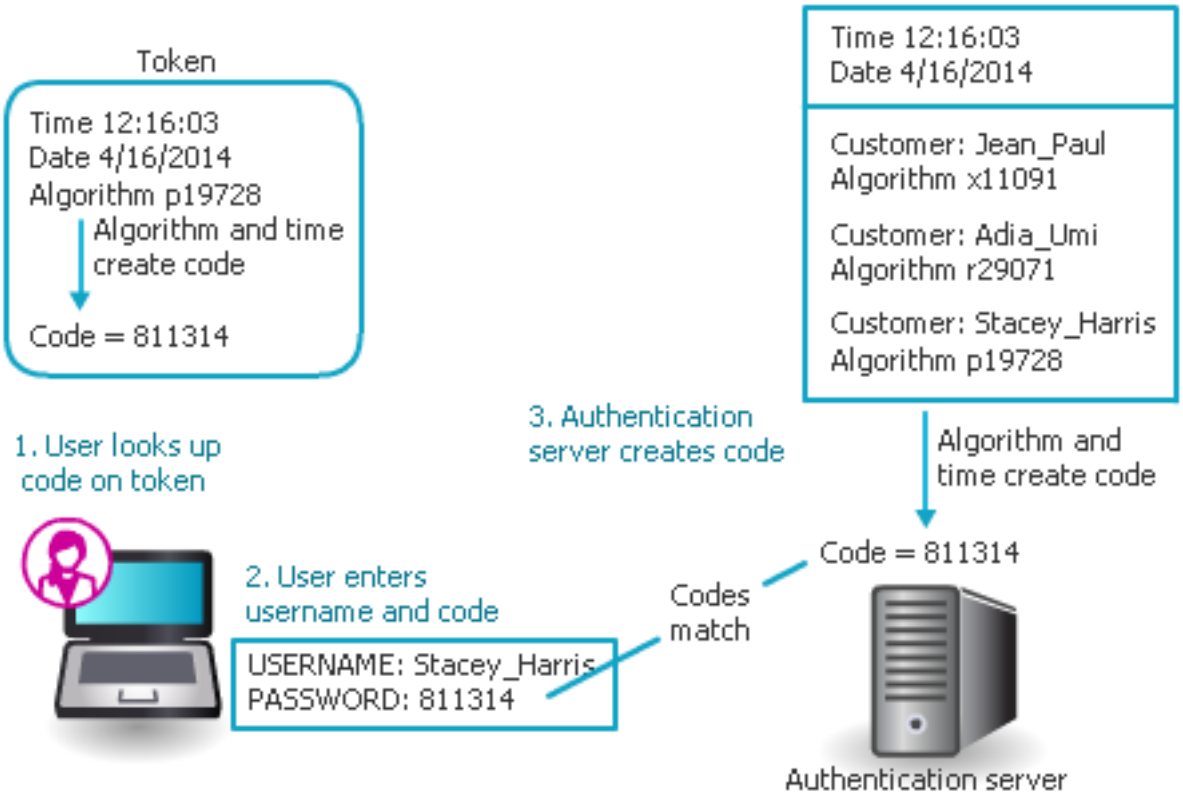
2.1. ماذا تملك: القطع والبطاقات What You Have: Tokens and cards

النوع الآخر من الثبوتيات التي يستطيع مستخدم ما تقديمها تأتي على قطع أو بطاقات يملكها.

القطع Tokens

يحسِّن استخدام القطع من المستوى الأمني للمصادقة بشكل ملحوظ. القطعة هي إجمالاً جهاز صغير (يمكن وضعه ضمن حمالة مفاتيح) مزود بشاشة عرض كما في الشكل 6. تتشارك القطعة مع مخدم مصادقة مركزي خوارزمية فريدة (أي لكل مستخدم خوارزمية مختلفة). تولد القطعة رمزاً كل 30 أو 60 ثانية ويكون هذا الرمز صالحاً لمدة محددة تعرض على الشاشة. عندما يريد المستخدم الدخول فإنه يدخل اسم المستخدم والرمز الذي يظهر على شاشة القطعة. ما أن يستقبل مخدم المصادقة المعلومات السابقة، فإنه يبحث عن الخوارزمية المقابلة للمستخدم ويولد رمزاً خاصاً به ويقارنه مع الرمز المستقبل من المستخدم حتى يسمح للمستخدم بالدخول في حال تطابق الرمزين كما هو موضح في الشكل 7. لا يحتاج المستخدم، في هذه الطريقة، إلى حفظ كلمة المرور وإنما يكفيه امتلاك القطعة.

الشكل 6: قطعة Token



الشكل 7: توليد الرمز ومقارنته

تتميز القطع بعدة محاسن مقارنةً بكلمات المرور. أولاً، تكون كلمات المرور ساكنة ولا تتغير طالما المستخدم لم يقم بذلك؛ هذا الأمر يمنح المهاجم وقتاً كبيراً نسبياً حتى يستطيع تحقيق هجومه وكسر كلمة المرور. في الطرف المقابل، كلمة المرور التي تولدها القطعة لها مدة حياة قليلة جداً (حوالي الدقيقة) وهي تتغير باستمرار لذلك يطلق عليها اسم كلمة المرور لمرة واحدة one-time password (OTP). فإذا استطاع المهاجم معرفة كلمة المرور، فلديه فقط 60 ثانية ليشن هجومه. تطلب بعض القطع انتظار بعض الوقت وإعادة إدخال الرمز الجديد لضمان عدم سرقة الرمز. هذا النوع من كلمات المرور لا يحمي ضد سرقة القطعة نفسها التي وإن حصلت يستطيع المستخدم اتخاذ إجراءات مباشرة لحماية معلوماته على عكس سرقة كلمات المرور التي يمكن أن تحصل دون علم المستخدم.

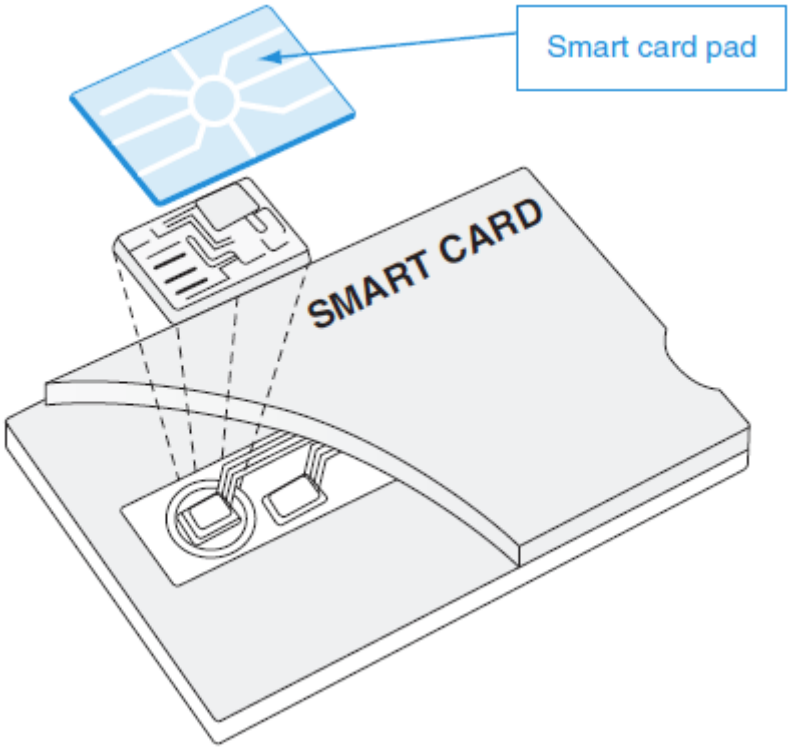
يوجد بعض أنواع القطع التي تطلب كلمة مرور أيضاً (كتلك المستخدمة في الجامعة الافتراضية) وهذا ما يسمى بالمصادقة متعددة العوامل Multifactor authentication. يطلب نوع ثالث من القطع من المستخدم خلق رقم شخصي PIN الذي يراكب مع الرمز المولد لتكوين رمز مرور passcode (مثلاً، PIN=1346 و Code=22497 فإن المستخدم يدخل رمز الدخول 134622496).

نظراً للانتشار الواسع لأجهزة الهواتف الذكية، بدأت هذه الأجهزة تحل محل القطع. يمكن هنا إرسال الرمز إلى هاتف المستخدم من خلال تطبيق ما على الجهاز أو من خلال إرسال رسالة قصيرة SMS.

تجدر الإشارة هنا إلى تطبيق Google Authenticator الذي يعمل بطريقة مشابهة للقطع لكن توليد الرمز يتم من خلال تطبيق ضمن جهاز الهاتف الذكي ومن ثم إرسال الرمز واسم المستخدم وكلمة المرور إلى موقع Google للمصادقة عليه للدخول إلى خدمات Google.

البطاقات Cards

يوجد عدة أنواع من البطاقات التي يمكن استخدامها. فالبطاقات الذكية، كما هو موضح في الشكل 8، تحوي رقاقة دارة متكاملة IC chip قادرة على تخزين معلومات يمكن استخدامها أثناء عملية المصادقة.



الشكل 8: بطاقة ذكية

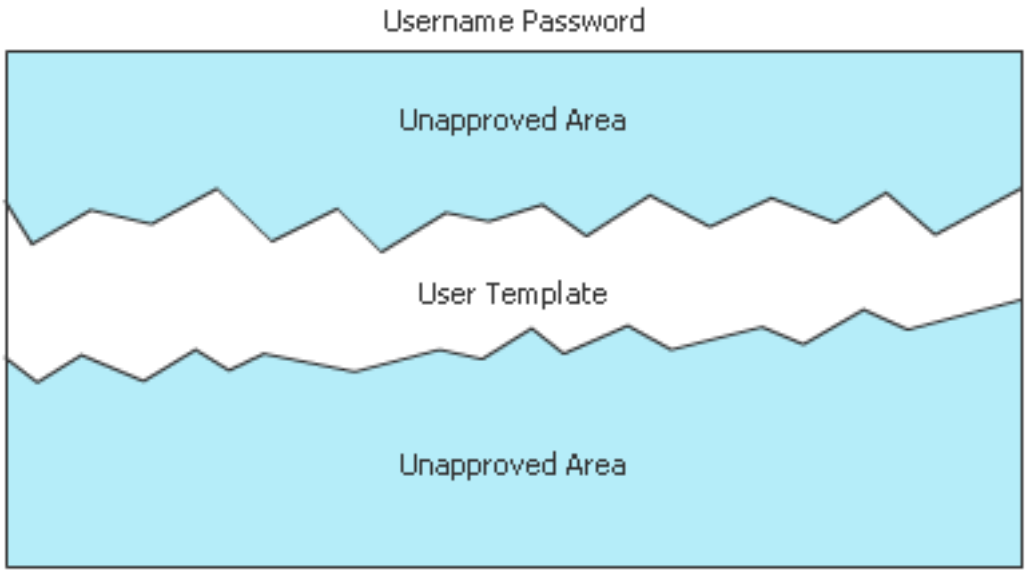
ما تكون: المعلومات الحيوية What You Are: Biometrics

يتعلق الصنف الثالث من المصادقة بميزات وخصائص الشخص الحيوية. هذا النوع من "ما تكون" يشمل المعلومات الحيوية المعيارية والمعلومات الحيوية السلوكية والمعلومات الحيوية الإدراكية.

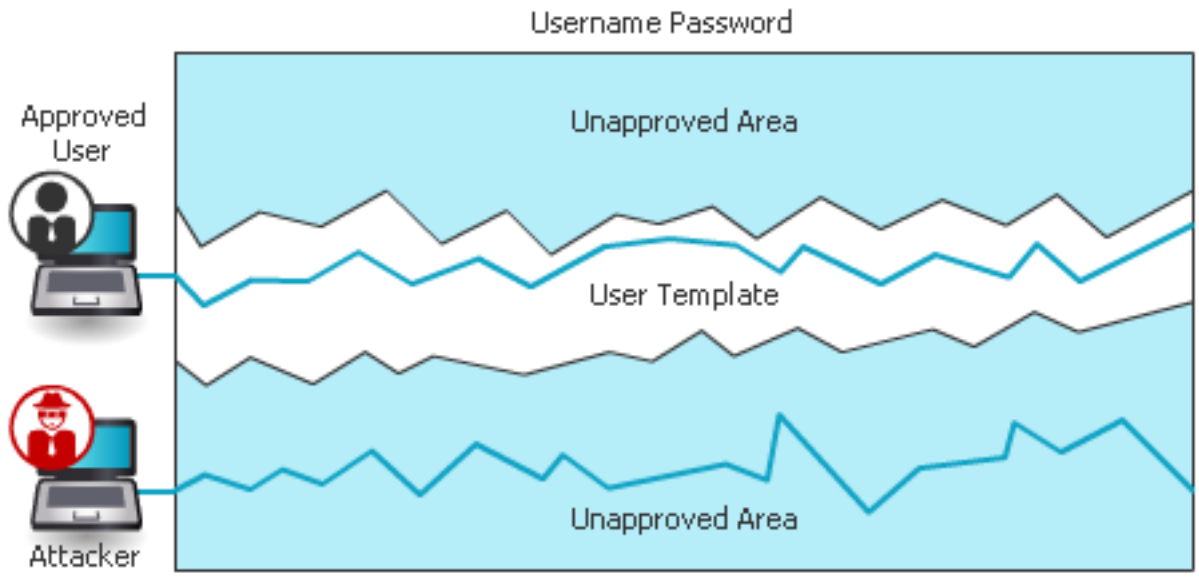
- المعلومات الحيوية المعيارية. تعتمد على بصمات الشخص أو على أي خصائص فيزيائية متعلقة بالشخص مثل الوجه أو اليدين أو العيون (القزحية والشبكية) للمصادقة. المشكلة الأساسية مع هذا النوع من التقانة هو الكلفة العالية. أجهزة مسح وقراءة البصمات مرتفعة الكلفة ويجب شراء أجهزة متعددة منها. أضف إلى ذلك إمكانية عدم قبول مستخدم شرعي أو قبول مستخدم غير شرعي. كما يمكن قهر

هذه التقانة عن طريق رفع بصمة شخص آخر من الزجاج أو تصوير القزحية أو تسجيل صوت الضحية ومن ثم خداع القارئ.

- المعلومات الحيوية السلوكية Behavioral Biometrics. تتم هنا المصادقة من خلال الأفعال العادية التي يقوم بها الإنسان. أكثر ثلاث سلوكيات واعدة هي ديناميكية ضربات المفاتيح والتعرف على الصوت والبصمة الحاسوبية.
  - ديناميكية ضربات المفاتيح Keystroke dynamics. تحاول هذه الطريقة التعرف على إيقاع ضربات المفاتيح للمستخدم الفريدة. يتم هنا استخدام متحولين هما زمن الثبات Dwell time وهو الزمن الفاصل بين الضغط على مفتاح و تحريره وزمن الحركة Flight time وهو الزمن بين الضغطات. يجري هنا جمع عدة عينات لضغطات المستخدم لتشكيل نموذج template كما هو موضح في الشكل 9. عندما يدخل المستخدم الاسم وكلمة المرور فإنهما يرسلا مع متحولات ضغطات المفاتيح لهما. يتم قبول الدخول في حال تطابق كلمة المرور ومتحولات ضغطات المفاتيح مع المعلومات المخزنة مسبقاً ضمن مخدم مصادقة (انظر الشكل 10).

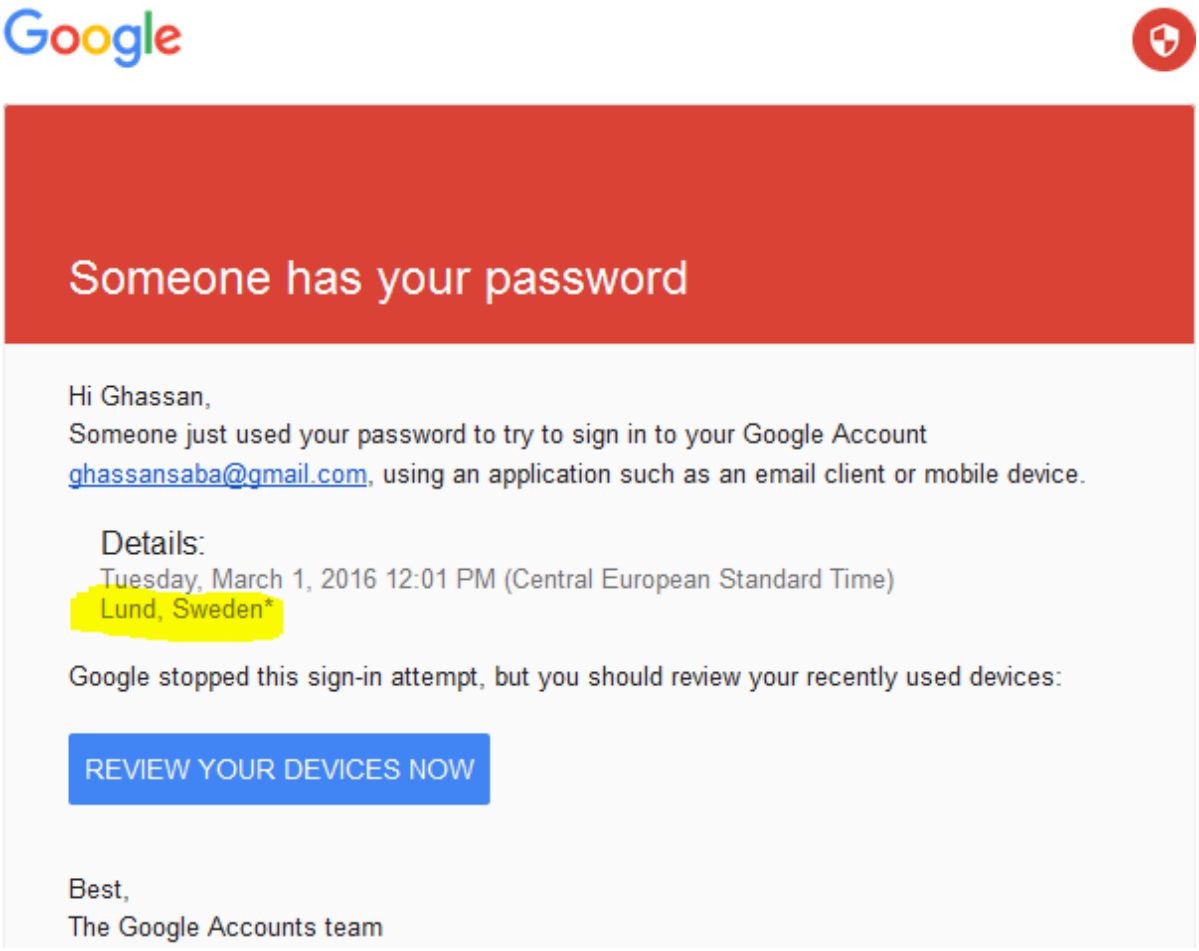


الشكل 9: نموذج الإدخال



الشكل 10: المصادقة وفق ديناميكية ضغطات المفاتيح

- التعرف على الصوت voice recognition. تتم هنا المصادقة على أساس خصائص الصوت الفريدة عند كل مستخدم وتوليد نموذج صوتي لكل مستخدم.
- بصمات الحاسوب computer footprint. يدخل المستخدم عادةً إلى حسابه المصرفي من مكان محدد وبوقت معروف وأي دخول إلى الحساب من مكان بعيد وبأوقات مشبوهة (مثل الساعة 2 صباحاً) يمكن أن تعطي مؤشراً على محاولة اختراق. من المعلومات التي يمكن استخدامها لتشكيل البصمة الحاسوبية الموقع الجغرافي والساعة ومزود خدمة الإنترنت المستخدم وبعض إعدادات الحاسوب الأساسية. يمكن هنا عند تجاوز بعض هذه المعلومات منح المستخدم نفاذاً محدوداً بدلاً عن النفاذ الكامل. يعاني المستخدمون الذين يعتمدون على شبكات خاصة افتراضية VPN للدخول إلى بعض المواقع من مشاكل دخول إلى خدمات Goggle و Facebook بسبب كون الموقع الجغرافي للمستخدم يتغير حسب مخدم VPN الذي يستخدمه (انظر الشكل 11).



الشكل 11: رسالة من Gmail بسبب الدخول باستخدام VPN من السويد

- المعلومات الحيوية المعرفية Cognitive Biometrics. تعتمد المعلومات الحيوية المعرفية على إمكانات التمييز وإجراءات التفكير والفهم لدى المستخدم. تعتبر هذه الطريقة سهلة بالنسبة للمستخدمين لأنها تعتمد على تذكر أحداث من الحياة الطبيعية كما تصعب عملية شن الهجوم. كأمثلة على المعلومات الحيوية المعرفية الطلب من المستخدم التعرف على الوجوه أو سؤال المستخدم أسئلة متعلقة بحادثة معينة حصلت ضمن حدث ما خلال تقضية إجازة أو أثناء حفل الزفاف (مثال، كم كان عمرك عندما تزوجت؟ أو عندما تخرجت؟)

2. تسجيل الدخول الوحيد Single Sign-on

تتجلى المشكلة الأساسية في استخدام كلمات المرور في حاجة المستخدم إلى عدة كلمات مرور لعدة منصات عمل وأنظمة تشغيل الأمر الذي يؤدي بالمستخدم في النهاية إلى استخدام كلمة مرور واحدة لجميع الحسابات تكون سهلة الكسر. يكمن الحل لهذه المشكلة في توفير اسم مستخدم وكلمة مرور واحدة للمستخدم يستخدمها للدخول إلى جميع الحسابات.

هذه هي الفكرة وراء إدارة الهوية Identity Management التي هي استخدام ثبوتيات مصادقة واحدة مشارك بها على جميع الشبكات. عندما تكون الشبكات مملوكة لمؤسسات مختلفة فيطلق عليها اسم إدارة الهوية الموحد Federated Identity Management (FIM). يعتبر الدخول الوحيد SSO أحد تطبيقات FIM حيث نستخدم ثبوتيات مصادقة واحدة للدخول إلى عدة حسابات أو تطبيقات.

يوجد عدة تحقيقات لما يعرف باسم نظام Web-based FIM مثل Windows Live ID و OpenID و OAuth.

1.2. هوية Windows Live ID

تطورت هوية Windows Live ID من Net Passport. إلى Microsoft Passport Network حتى أخذت الاسم الحالي عام 2006. تعتمد هذه الطريقة على خلق اسم مستخدم وكلمة مرور على مخدم مركزي كما تعتمد أيضاً على توليد كوكيز عامة مشفرة محدودة زمنياً ولصيقة هوية مشفرة أيضاً وتخزينهما عند حاسوب المستخدم بغية المصادقة من أي موقع وب يعتمد هوية ويندوز. يقوم موقع الوب، بعد المصادقة، بتوليد كوكيز أخرى محلية ومشفرة ومحدودة زمنياً. لم تتلق هوية ويندوز الدعم اللازم لتصبح FIM فبقيت معتمدة لدى شركة مايكروسوفت والشركات التي تدور في فلكها.

2.2. هوية OpenID

هوية OpenID هي عبارة عن FIM غير مركزية ومفتوحة المصدر ولا تحتاج إلى تثبيت أي برنامج على حاسوب المستخدم. هوية OpenID هي عبارة عن نظام يعتمد URL-based. الهوية هي URL مدعومة باسم مستخدم وكلمة مرور. تزود OpenID وسيلة للتحقق من كون المستخدم يملك URL محددة.

خطوات خلق واستعمال OpenID هي التالية:

1. يذهب المستخدم إلى موقع مجاني يزود حسابات OpenID مثل MyOpenID.com ويخلق حساب باسم (Me) وكلمة مرور. يصبح لدى المستخدم الحساب Me.myopenid.com.
2. عندما يزور المستخدم موقع وب مثل BuyThis.com الذي يطلب منه تسجيل الدخول فبإمكان المستخدم اختيار استعمال OpenID حيث يدخل اسم المستخدم me.myopenid.com.
3. يوجه الموقع BuyThis.com المستخدم إلى MyOpenID.com حيث يطلب منه إدخال كلمة المرور لتحقيق المصادقة ولتأكيد أنه يثق بالموقع BuyThis.com.

4. يعيده موقع Myopenid.com إلى BuyThis.com بعد أن تمت المصادقة عليه.

يحوي OpenID بعض نقاط الضعف، أهمها كونه يعتمد على تسيير معرف URL إلى المخدم الصحيح الأمر الذي يتعلق بمخدم DNS الذي يمكن أن يحوي ثغرات أمنية. لذلك لا يعتبر نظام OpenID قوياً كفايةً للتطبيقات المصرفية أو التجارة الالكترونية وإنما للتطبيقات الأقل أمناً.

3.2. هوية Open Authorization (OAuth)

يسمح OAuth، المفتوح المصدر، للمستخدمين بمشاركة موارد موجودة ضمن موقع مع موقع ثانٍ دون توجيه ثبوتياتهم إلى الموقع الثاني كما يسمح أيضاً لعدة تطبيقات بمشاركة المعطيات عبر المواقع.

3. تمارين عملية

1.3. تحميل وتثبيت تطبيق إدارة كلمات المرور

يهدف هذا التمرين إلى استخدام تطبيق يسمح بتخزين كلمات المرور وحمايتها عن طريق كلمة مرور واحدة.

1. Go to the URL http://filehippo.com/download_password_safe/download/95213d54679efcab7b09c2ea6283d52d/ and download the file pwsafe.exe (11.5 MB)
2. Install the program and launch it
3. Try adding some accounts
4. Download Password Safe APK file from http://www.apkpro.org/2015/12/password-safe-416-apk.html
5. Install it on you android phone
6. Try to synchronize accounts between the two operating systems

2.3. التعامل مع تطبيق إدارة كلمات المرور يعتمد متصفح الإنترنت

تكمن مشكلة تطبيقات إدارة كلمات المرور في الحاجة إلى تشغيل التطبيق كل مرة تحتاج فيها إلى كلمة مرور لحساب ما وبالتالي إعادة كتابة كلمة مرور للتطبيق بشكل متكرر علماً أن إبقاء التطبيق مفتوحاً يشكل ثغرة أمنية. التطبيقات المعتمدة على المتصفح تسترجع كلمات لمرور آلياً دون تدخل المستخدم.

1. Use your Web browser to go to lastpass.com and click Free – Download LastPass
2. Download LastPass (Free version 32- or 64-bit)
3. after the program has downloaded, run the program and follow the instructions
4. select create LastPass account for me when prompted and enter required fields
5. Be sure that Yes, let me choose which items I want imported into LastPass is selected. Click Next.
6. If LastPass finds any passwords stored in your Web browser, you can import them. Click Next when finished.
7. Click No, do not remove any insecure items. Click Next.
8. Click Done.
9. Click OK.

ستقوم الآن باستخدام LastPass.

1. Launch your Web browser.
2. Notice that you now have a LastPass button at the top of the screen.
3. Click LastPass.
4. Enter your Master Password and then click Login.
5. Point your Web browser to a Web site you frequently use that requires you to enter your username and password.
6. Enter your username and password. Notice that LastPass now asks Should LastPass remember this password? Click Save Site.
7. When the Add LastPass Site window opens, enter Test for the group and click Save Site.
8. Log out of the Web site.
9. Point your Web browser again to that site. Notice that this time your username and password are already entered for you. Log on to this site.
10. Log out of the Web site.
11. Now log into two other Web sites and record their passwords in LastPass.
12. Close the Web browser.
13. Reopen the Web browser and click the LastPass icon on the toolbar. Notice that you are still logged in.
14. Revisit the two Web sites in Step 11 for which you recorded your LastPass information. What happens when you go to these sites?

3.3. استخدام المعلومات الحيوية المعرفية

1. Use your Web browser to go to www.passfaces.com/demo.
2. Under First Time Users, enter the requested information and then click Enroll.
3. Click Click to continue.
4. Accept demo and then click OK.
5. When asked, click Next to enroll now.
6. When the Enroll in Passfaces dialog box opens, click Next.
7. You will then be asked to think of associations with the first face (who they may look like or who they may remind you of). Follow each step with the faces and then click Next after each face.

8. When the Step 2 Practice Using Passfaces dialog box opens, click Next.
9. You will then select your faces from three separate screens, each of which has nine total faces. Click the face (which is also moving as a hint).
10. Continue to the end of demo

4.3. كسر كلمات المرور باستخدام قوائم قوس قزح

1. Go to www.fileformat.info/tool/hash.htm يحوي خوارزمية للتهشير
2. Under String hash, enter the simple password pass123 in the Text: line.
3. Click Hash
4. Scroll down the page and copy the MD4 hash of this password
5. Open a new tab on your web browser and go to https://crackstation.net/
6. Paste the MD4 hash of *pass123* into the text box and the required Captcha then click crack Hashes
7. How long did it take this online rainbow table to crack this hash?
8. Try a more complicated password such as 12applesauce

5.3. ديناميكية ضربات المفاتيح

1. Go to www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/65
2. Download, uncompress, and run the application
3. Click parameter => Password and type Pass123go or any other password
4. Register yourself and click Execution Mode
5. Point to Enroll User and enter your name
6. Under Password: type Pass123go and monitor the graphs
7. Now change the color of graphs and run the test again
8. Go to Execution Mode => Verify (user name)
9. Try to type the password differently and note the result
10. Let someone else attempt to type your password and note the result.

الفصل العاشر: أساسيات التعمية
Basic Cryptography

بعد الانتهاء من هذا الفصل، سيكون باستطاعتك القيام بما يلي:

- تعريف التشفير
- شرح وفهم التهشير وخوارزميات التشفير المتناظرة وغير المتناظرة
- تعرف أماكن استخدام التشفير

نحتاج عادةً ، إضافة إلى أجهزة حماية المعلومات مثل جدار النار، إلى تشفير المعلومات الهامة بغية منع المهاجم من قراءة المعلومات حتى ولو تمكن من الحصول عليها إذا لم يكن يعرف مفتاح التشفير المستخدم. نحتاج أيضاً إلى التشفير عندما ننقل المعلومات عبر الشبكات لمنع المتطفلين من معرفة محتوياتها فيما لو كانوا يتجسسون على الاتصال. يفيد التشفير في تحقيق غايات أخرى سندرسها في هذا الفصل.

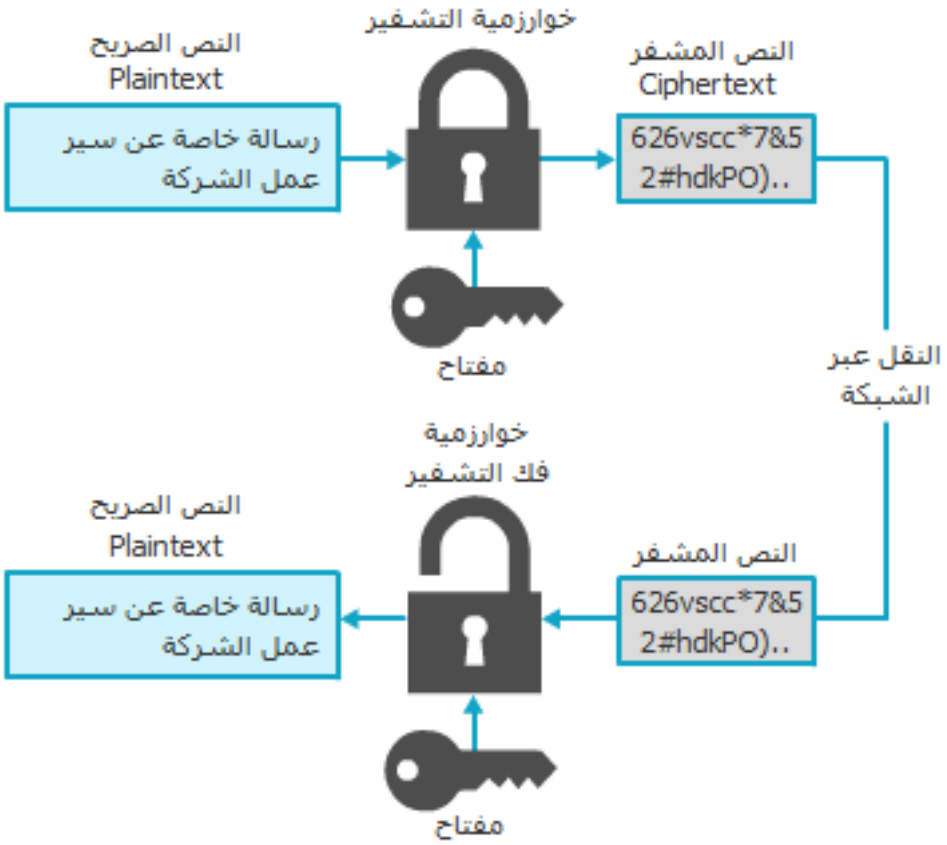
ملاحظة: سنستخدم مصطلح التعمية للدلالة على Cryptography ومصطلح التشفير للدلالة على encryption.

1. تعريف التعمية

يتطلب تعريف التعمية فهم ما هي التعمية وماذا يستطيع أن يفعل وكيف يفيد في حماية المعطيات.

1.1. ما هي التعمية؟

التعمية هي علم تحويل المعلومات إلى شكل آمن لا يستطيع شخص غير مصرح له النفاذ إليها. يطلق على المعطيات غير المشفرة اسم النص الواضح Cleartext وهي معطيات قابلة للقراءة مباشرةً بدون أي خوارزمية فك تشفير. النص الصريح Plaintext هو نص واضح مطلوب تشفيره باستخدام خوارزمية رياضية أو ناتج عن فك تشفير نص مشفر. المفتاح key هو قيمة رياضية تدخل إلى الخوارزمية لتوليد النص المشفر Ciphertext أو المعطيات المشفرة. عندما نريد استرجاع النص الصريح من النص المشفر، نستخدم خوارزمية ومفتاح فك تشفير. يبين الشكل 1 إجرائيات التشفير وفك التشفير.



الشكل 1: التشفير وفك التشفير

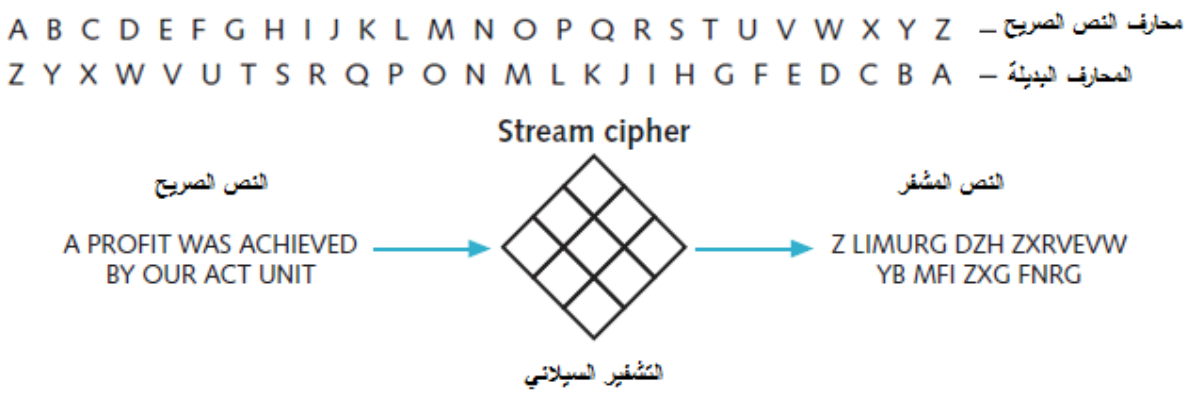
2.1. التعمية والأمن

تؤمن التعمية حماية أمنية أساسية للمعلومات لأن إمكانية الوصول إلى المفتاح تكون عادةً محدودة. يمكن أن تؤمن التعمية خمسة أنواع من الحماية:

- الخصوصية Confidentiality. تحمي التعمية خصوصية المعلومات بحيث فقط المصرح لهم يستطيعون رؤيتها.
- السلامة Integrity. يمكن أن تؤمن التعمية سلامة المعلومات من التعديل عن طريق طرف ثالث.
- المتاحية Availability. يمكن أن تؤمن التعمية متاحية المعطيات بحيث يستطيع الأشخاص المصرح لهم والذين يملكون المفتاح من الاطلاع عليها عندما يريدون.
- المصادقة Authentication. يمكن المصادقة على هوية المستخدمين عن طريق التعمية.
- عدم الإنكار Non-repudiation. يمكن أن تفرض التعمية عدم الإنكار. يقصد هنا عملية التحقق من كون مستخدم ما نفذ فعل ما وعدم إنكاره له.

2. خوارزميات التعمية

تتمثل إحدى الاختلافات الرئيسية في خوارزميات التشفير في كمية المعطيات الممكن معالجتها في لحظة ما. تستخدم بعض الخوارزميات التشفير السيلاني stream cipher حيث يتم استبدال كل محرف بمحرف آخر وفي بعض الحالات بعدة محارف. يعد تشفير الاستبدال Substitution cipher من أبسط انواع التشفير السيلاني. يبين الشكل 2 مثال بسيط عن هذا النوع من التشفير.



الشكل 2: التشفير الاستبدالي

يمكننا تعقيد التشفير الاستبدالي عن طريق مقابلة كل حرف بعدة حروف فمثلاً الحرف F يصبح ILS وهكذا.

النوع الآخر من الخوارزميات يستخدم التشفير الكتلي Block cipher. هنا تجري معالجة كتلة كاملة من المعطيات في مرة ما. يجري هنا تقسيم النص الصريح إلى عدة كتل مكونة من 8 إلى 16 بايت مثلاً ومن ثم يتم تشفير كل كتلة بشكل مستقل.

تم مؤخراً إدخال نوع ثالث يعرف بالتابع الإسفنجي Sponge function. يأخذ التابع الإسفنجي سلسلة من أي طول ويولد سلسلة أخرى حسب الطول المطلوب.

يوجد، بشكل عام، ثلاثة أصناف لخوارزميات التعمية وهم خوارزميات التهشير Hash وخوارزميات التعمية المتناظرة Symmetric وخوارزميات التعمية غير المتناظرة Asymmetric.

1.2. خوارزميات التهشير

تخلق خوارزمية التهشير بصمة رقمية فريدة لمجموعة معطيات ويطلق على العملية وحيدة الاتجاه اسم التهشير Hashing. تمثل هذه البصمة محتوى المعطيات (يطلق عليها تعابير مختلفة مثل Digest, hash). مع أن التهشير يعتبر من خوارزميات التعمية إلا أنه لا يخلق نصاً مشفراً يستخدم لاحقاً عند فك التشفير. فعملية التهشير هي وحيدة الاتجاه بمعنى أنه لا يمكننا عكسها والحصول على المعطيات من الهاش. يستخدم التهشير لأغراض المقارنة.

يمكن اعتبار تابع تهشير آمناً إذا تمتع بالخصائص التالية:

- الطول الثابت. أي أن طول خرج تابع التهشير يكون ثابتاً مهما كان طول معلومات الدخل.
- فريد Unique. لا يجب أن تولد مجموعتين مختلفتين من المعطيات الهاش نفسه (تعرف الحالة بالتصادم Collision). كما أن تغيير محرف واحد في معطيات الدخل سيولد خرجاً مختلفاً تماماً عن الخرج السابق.
- أصلي Original. يجب أن يكون من المستحيل إنتاج مجموعة معطيات لها هاش مرغوب أو سابق التحديد.
- آمن Secure. عدم إمكانية عكس الهاش للحصول على النص الأصلي.

يجري استخدام التهشير لاختبار سلامة رسالة أو محتوى ملف ما من التعديل. فمثلاً بعد وضع ملف على موقع وب يتم إرفاق ملف الهاش الخاص به. عندما يحمِّل المستخدم الملف والهاش من الموقع يقوم بحساب الهاش للملف ومقارنته بالهاش الأصلي للتأكد من سلامة الملف.

يعتبر رماز مصادقة الرسائل المهشرة Hashed Message Authentication Code (HMAC) تحسيناً على الهاش يؤمن حماية إضافية. يتم هنا توليد رماز مصادقة الرسالة Message Authentication Code (MAC) يضم مفتاح سري مشترك يعرفه فقط المرسل والمستقبل يرفق مع الرسالة. عندما يستلم المستقبل الرسالة فهو يعرف أنها قادمة من المرسل لأنه يعرف المفتاح السري. هذا يفيد في المصادقة على مرسل الرسالة مع العلم أن MAC لا يشفر محتوى الرسالة. تقوم خوارزمية HMAC بعملية التهشير على الرسالة والمفتاح السري.

أشهر خوارزميات التهشير هي ملخص الرسالة Message Digest وخوارزمية التهشير الآمنة Secure Hash Algorithm (SHA).

ملخص الرسالة Message Digest (MD)

تعتبر خوارزمية MD من أشهر خوارزميات التهشير المعروفة وهي تحوي ثلاثة إصدارات. فخوارزمية MD2 تأخذ نص صريح مهما كان طوله وتولد ملخص Digest بطول 128 bits. تقسم MD2 المعطيات إلى مقاطع مؤلفة من 128 bits وفي حال كون الرسالة أقل من 128 bits فإنه يجري إضافة حشوة إليها. لا يعتبر تهشير MD2 آمناً في وقتنا الحالي.

أما تهشير MD4 الذي طور عام 1990 فهو بطول 128 bits أيضاً لكن طول المقاطع هنا يصبح 512 bits. لا يستخدم MD4 بشكل واسع بسبب وجود بعض العيوب فيه.

النسخة الحالية للخوارزمية هي MD5 والتي حاولت تجاوز عيوب MD4. يجري هنا استخدام مقاطع ذات طول 512 bits مع إضافة بتات حشو عند اللزوم. يستخدم تابع التهشير 4 متحولات بطول 32 bits لكل متحول على التسلسل وبطريقة دائرية لتوليد قيمة يتم ضغطها للحصول على الملخص. مع هذه التحسينات الأمنية إلا أن الخوارزمية تعتبر غير آمنة كفاية ويجب استخدام خوارزميات أكثر أمناً.

خوارزمية التهشير الآمنة Secure Hash Algorithm (SHA)

تعتبر عائلة خوارزميات SHA أكثر أمناً من عائلة MD. الإصدار الأول SHA-0 جرى استبعاده مباشرةً بسبب عيوب فيه. تم تطوير SHA-1 عام 1993 بشكل يشابه تصميم كلٍ من MD4 و MD5 لكنه يولد ملخص بطول 160 bits بدلاً عن 128 bits. يحشو SHA-1 الرسائل الأقل من 512 bits باستخدام أصفار ورقم طبيعي يدل على الطول الأصلي للرسالة.

الإصدار الثاني SHA-2 يأتي بعدة أنواع لكن أهمها SHA-512/256 حيث يكون طول الملخص 256 bits. يعتبر SHA-2 تابع تهشير آمناً.

تم اعتماد SHA-3 في آب 2015 بعد عدة جولات من المنافسة بين عدة مرشحين. SHA-3 يعتمد البناء الإسفنجي 224 bits إلى 512 bits.

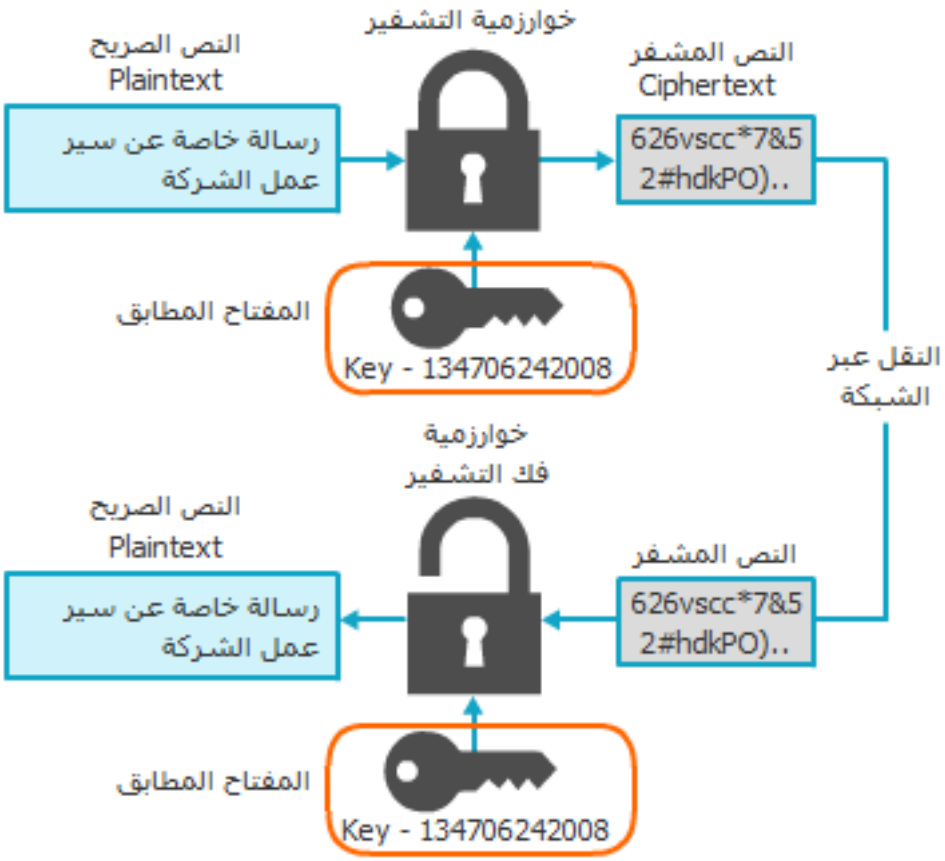
يبين الجدول التالي خرج بعض توابع التهشير.

Hash	Digest
MD2	c4b4c4568a42895c68e5d507d7f0a6ca
MD4	9a5b5cec21dd77d611e04e10f902e283
MD5	0e41799d87f1179c1b8c38c318132236
SHA-1	299b20adfec43b1e8fade03c0e0c61fc51b55420
SHA-256	133380e0ebfc19e91589c2feaa346d3e679a7529fa8d03617fcd661c997d7287
SHA-3	c298d1ec129b04495f399cbc5c44b8023e213ebe27b78f689046a72e436e0e0 1d47302bbc8a857695594106d63571b95933a67b389802ceb2ef9b078297cfcc3

الجدول 1: خرج بعض توابع التهشير

2.2. خوارزميات التعمية التناظرية

تستخدم خوارزميات التعمية التناظرية المفتاح نفسه للتشفير ولفك التشفير لذلك يجب الحفاظ على سرية مفتاح التشفير لمنع أي مهاجم من معرفة محتويات الملفات المتبادلة بين طرفين. يطلق على هذا النوع من التعمية اسم التعمية بالمفتاح الخاص. يوضح الشكل 3 آلية التشفير بالمفتاح الخاص.



الشكل 3: آلية التعمية المتناظرة

يمكن أن تفيد التعمية بالمفتاح الخاص في الحفاظ على خصوصية المعطيات وسلامتها ومتاحيتها.

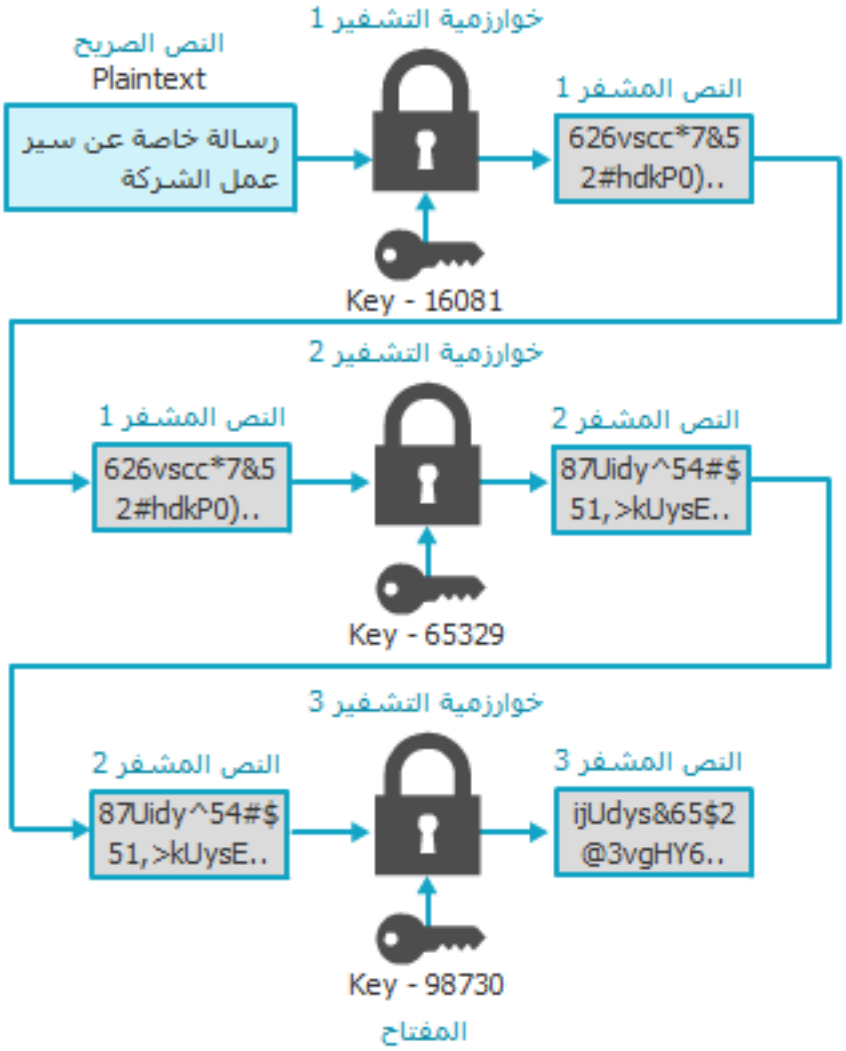
من أشهر خوارزميات التعمية بالمفتاح المتناظر (الخاص) معيار تشفير المعطيات DES ومعيار تشفير المعطيات الثلاثي 3DES ومعيار التشفير المتقدم AES وغيرهم.

معيار تشفير المعطيات Data Encryption Standard (DES)

يعتمد DES التشفير الكتلي مع مفتاح بطول 56–bitوهو يقسم النص الصريح إلى كتل بطول 64–bit وينفذ الخوارزمية 16 مرة. يوجد أربعة أنماط لتشفير DES. لقد تم كسر خوارزمية التشفير DES عدة مرات ولا تعتبر آمنة في وقتنا الحالي.

معيار تشفير المعطيات الثلاثي 3DES

يستخدم 3DES ثلاث جولات من التشفير بدلاً عن جولة واحدة كانت موجودة ضمن DES أي أن عدد التكرارات الكلية تصبح 48 بدلاً عن 16 كما هو موضح في الشكل 4. لزيادة أمن الخوارزمية، يجري استخدام مفاتيح مختلفة لكل جولة.



الشكل 4: 3DES

معيار التشفير المتقدم Advanced Encryption Standard (AES)

اعتمدت خوارزمية التشفير AES (المعروفة أيضاً باسم Rijndael) من قبل الحكومة الأمريكية بعد منافسة من عدة جولات لتحل محل خوارزمية DES.

تقسم خوارزمية AES النص الصريح إلى كتل طول كل منها 128-bit وتقوم بثلاث خطوات على كل كتلة. ضمن الخطوة 2، يتم تنفيذ عدة جولات يتعلق عددها بطول المفتاح: 9 جولات لمفتاح بطول 128-bit و11 جولة لمفتاح بطول 192-bit و13 جولة لمفتاح بطول 256-bit المعروف بخوارزمية AES-256. يتم في

كل جولة، استبدال البايتات وإعادة ترتيبها ومن ثم تحقيق بعض عمليات الضرب الخاصة حسب الترتيب الجديد. لم ينجح أي هجوم على خوارزمية AES حتى الآن.

بقية الخوارزميات

يوجد مجموعة متنوعة من خوارزميات التشفير التناظري مثل عائلة (RC) Rivest Cipher. أحدث هذه الإصدارات هو RC6 وهو يملك 3 أطوال للمفاتيح (128 و 192 و 256 بت) وينفذ 20 جولة على كل كتلة.

أما خوارزمية تشفير المعطيات العالمية (IDEA) International Data Encryption Algorithm فهو يعتمد التشفير الكتلي الذي يعالج 64-bit باستخدام مفتاح بطول 128-bit مع 8 جولات. تعتبر هذه الخوارزمية آمنة أيضاً.

هناك أيضاً خوارزمية بلوفيش Blowfish الكتلية التي تستخدم كتل بطول 64-bit ومفاتيح بأطوال مختلفة من 32 إلى 448 بت. لا يوجد حتى الآن عيوب في هذه الخوارزمية ويوجد لها تحديث يعرف باسم Twofish لكنها غير معروفة مثل سابقتها.

الحشو لمرة واحدة One-time pad (OTP) يراكب النص الصريح مع مفتاح عشوائي. هذه الطريقة غير قابلة للكسر رياضياً كما أنها لا تتطلب استخدام الحاسوب.

الحشو هو عبارة عن سلسلة طويلة من الأحرف العشوائية. يتم تركيب هذه الأحرف مع النص الصريح لتوليد النص المشفر. حتى يستطيع فك التشفير، يجب أن يملك المستقبل نسخة عن السلسلة العشوائية لعكس العملية. يجب هنا استخدام الحشو مرة واحدة فقط ومن ثم حذفها. يوضح الجدول التالي إحدى طرق استخدام OTP.

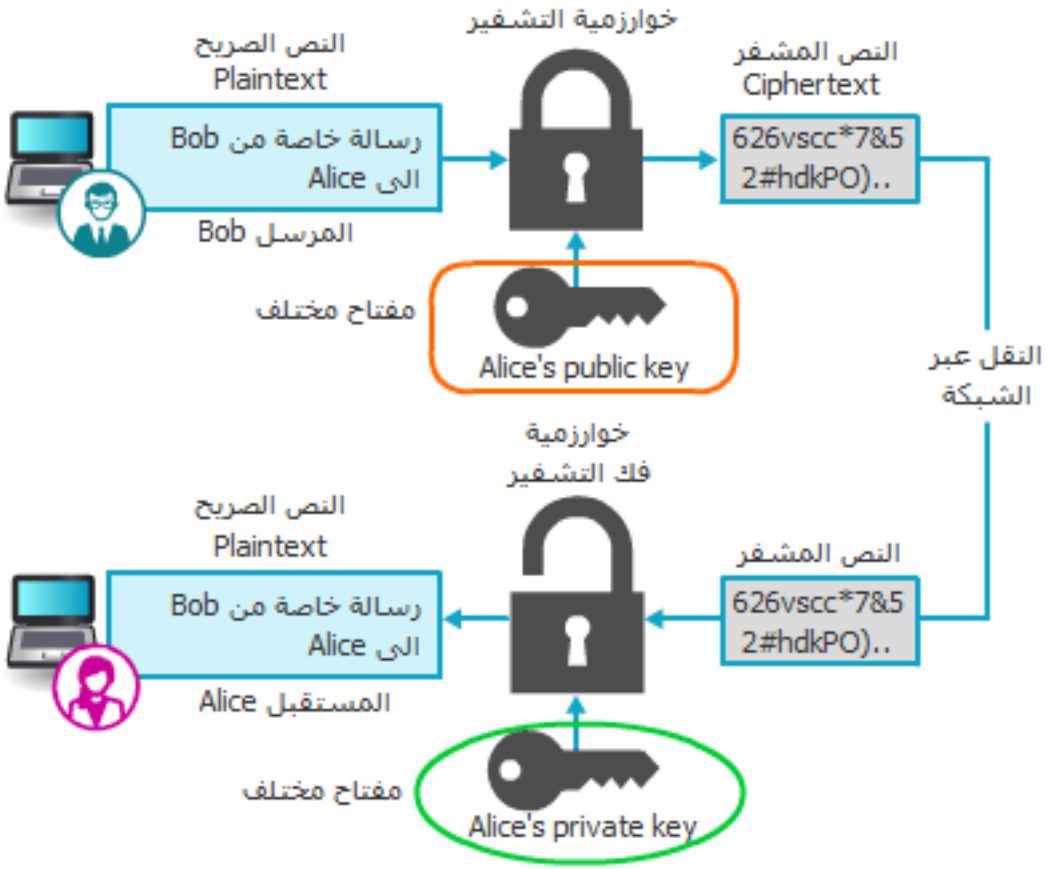
Plaintext	Position in alphabet	Pad	Position in alphabet	Calculation	Result
S	19	C	3	19+3−1=21	U
E	5	B	2	5+2−1=6	F
C	3	Y	25	3+25−1=1(wrap 26)	A
R	18	F	6	18+6−1=23	W
E	5	E	5	5+5−1=9	I
T	20	A	1	20+1−1=20	T

الجدول 2: آلية عمل OTP

3.2. خوارزميات التعمية غير التناظرية

تعاني خوارزميات التعمية التناظرية من مشكلة أساسية تتمثل في تبادل المفاتيح. أو كيف يستطيع المستخدم A من إرسال المفتاح المشترك إلى المستخدم B دون أن تكون عملية تبادل المفاتيح عرضة للاعتراض من قبل طرف ثالث؟

التشفير غير المتناظر (أو التشفير بالمفتاح العام) يستخدم مفتاحين عوضاً عن مفتاح واحد. يكون المفتاحان مرتبطين رياضياً وهم معروفين كمفتاح عام Public key ومفتاح خاص Private key. المفتاح العام معروف للجميع ويمكن توزيعه بحرية بينما يكون المفتاح الخاص معروف فقط من قبل الشخص الذي يملكه. عندما يريد Bob إرسال رسالة مشفرة إلى Alice فإنه يستخدم مفتاحها العام لتشفير الرسالة. تستخدم Alice مفتاحها الخاص لفك تشفير الرسالة. يبين الشكل5 آلية عمل التشفير غير المتناظر.



الشكل 5: التشفير غير المتناظر

يوجد عدة مبادئ هامة تتعلق بالتشفير غير المتناظر وهم:

- زوج المفاتيح key pairs. نحتاج هنا إلى زوج من المفاتيح لتحقيق التشفير غير المتناظر.
- المفتاح العام. لا تحتاج المفاتيح العامة إلى الحماية.

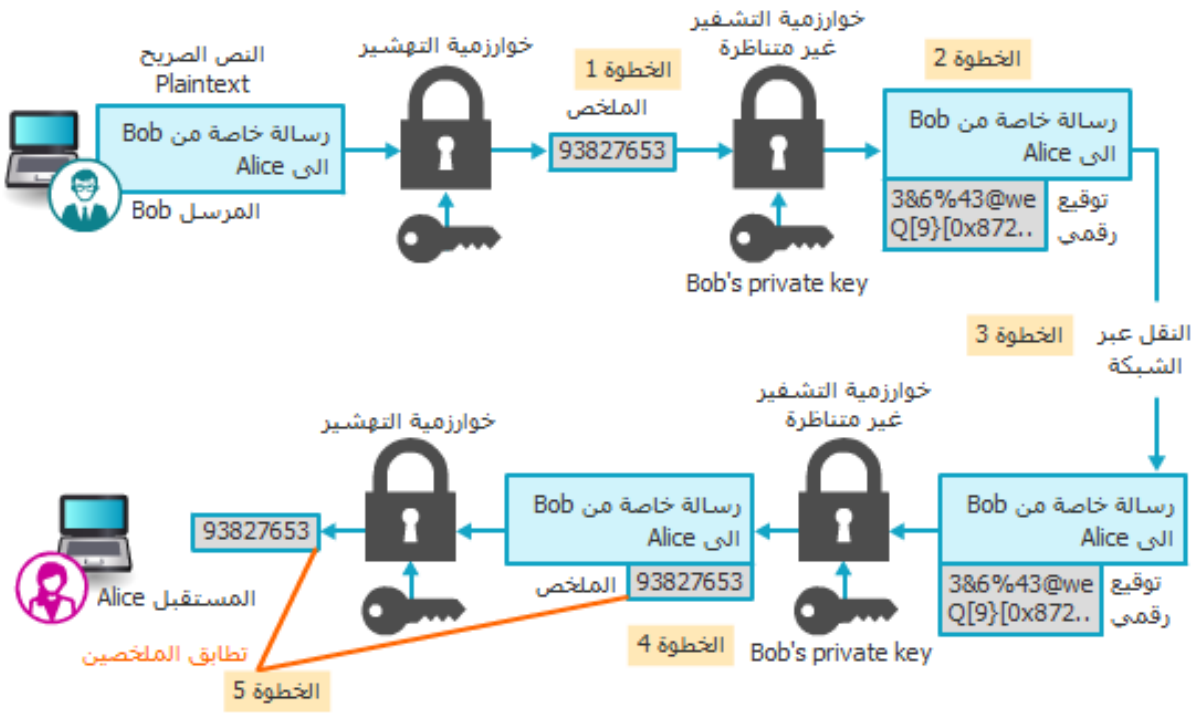
- المفتاح الخاص. يجب الحفاظ على المفاتيح الخاصة سرية وعدم مشاركتها مع أحد.
- في الاتجاهين. إذا تم تشفير نص بالمفتاح العام فيمكن فك تشفيره بالمفتاح الخاص والعكس بالعكس.

يمكن استخدام التشفير غير المتناظر لتوليد توقيع رقمي للرسالة للتحقق من هوية المرسل مثل التوقيع اليدوي على الوثائق الذي يفيد في التحقق من المرسل. يمكن أن يفيد التوقيع الرقمي في:

- التحقق من المرسل.
- منع المرسل من إنكار ملكيته للرسالة. لا يمكن للمرسل إنكار عدم إرساله للرسالة بسبب تزوير توقيعه مثلاً.
- إثبات سلامة الرسالة. هذا يعني إثبات عدم حدوث أي عبث بالرسالة بعد التوقيع.

تمر خطوات التوقيع الرقمي بما يلي:

1. بعد خلق الرسالة، يولد بوب ملخص digest لها.
2. يقوم بوب بتشفير الملخص باستخدام مفتاحه الخاص. يصبح الملخص المشفر هو التوقيع الرقمي للرسالة.
3. يرسل بوب الرسالة والتوقيع الرقمي إلى أليس.
4. عندما تستقبلهم أليس، تقوم بفك تشفير التوقيع الرقمي باستخدام المفتاح العام لبوب ورؤية الملخص الصريح. أما إذا لم تستطع أليس فك التشفير فهذا يعني أن الرسالة غير قادمة من بوب.
5. تقوم أليس بعد التحقق من أن المرسل هو بوب بتهشير الرسالة بنفس الخوارزمية التي استخدمها بوب ومقارنة نتيجة التهشير مع الملخص الذي أرسله بوب. إذا كانت نتيجة المقارنة مطابقة فهذا يعني أن الرسالة لم يُعبث بها بعد التوقيع. يبين الشكل 6 تسلسل هذه الخطوات.



الشكل 6: التوقيع الرقمي

تجدر الملاحظة هنا أن التوقيع الرقمي لا يشفر الرسالة فإذا كان بوب يريد أن يشفر الرسالة أيضاً فيجب عليه استخدام المفتاح العام لأليس.

يمكن أن يؤمن التشفير بالمفاتح العام الخصوصية والسلامة والمتاحية وعدم الإنكار والأصالة.

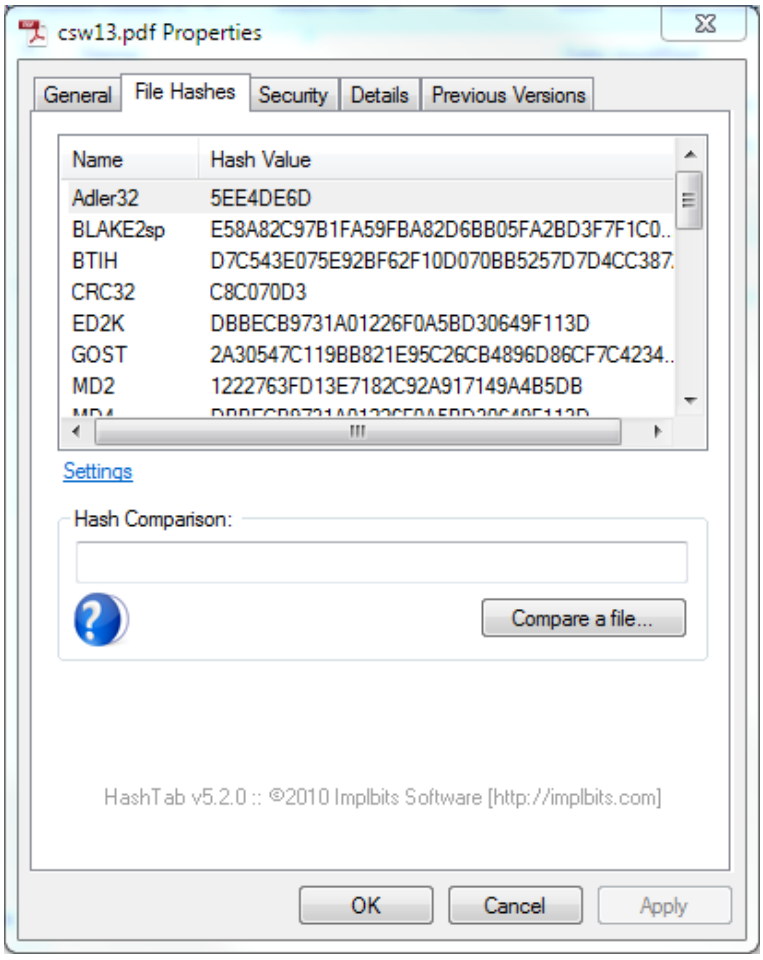
تعتبر خوارزمية RSA من أشهر خوارزميات التشفير غير المتناظر وهي معتمدة في العديد من المنتجات.

3. تمارين عملية

1.3. التعامل مع مولد هاش

سنعمل في هذا التمرين على تحميل برنامج لتوليد الهاش ومقارنتها.

1. Go to implbits.com/Products/HashTab
2. Download a copy of the program for Windows
3. Install it and run it
4. Click Open Windows Explorer.
5. Click once on a file and then right-click.
6. Click Properties.
7. Notice that there is a new tab, File Hashes. Click this tab to display the digests for this file, as illustrated in the next figure.



الشكل 7: استخدام Hashes Tab

8. Click Settings.
9. Click the Select All button.
10. Click OK.
11. Scroll through the different digests generated.
12. Click Compare a file.
13. Navigate to another file and then click Open.
14. A digest is generated on this file. What tells you that the digests are not the same?

2.3. استخدام برنامج لتشفير ملفات قرص

1. Go to https://veracrypt.codeplex.com/
2. Download the tool (actual version is 1.17)
3. Install veraCrypt.exe
4. Launch VeraCrypt
5. Click Create Volume button
6. A VeraCrypt volume can be in a file (called a container), in a partition or drive. Be sure that Create an encrypted file container isselected.
7. Click Next.
8. Under Volume Type, be sure that Standard VeraCrypt volume is selected. Click Next.
9. Under Volume Location, click Select File.
10. Enter VeraCrypt Encrypted Volume next to File name and select the location for this file. Click Save.
11. Click Next.
12. Under Encryption Algorithm, be sure that AES is selected. Click Next.
13. Under Volume Size, enter 50 and be sure that MB is selected. Click Next.
14. Under Volume Password, read the requirements for a password and then enter a strong password to protect the files. Enter it again under Confirm and then click Next.

15. When the Volume Format dialog box displays, move your mouse as randomly as possible within the window for at least 30 seconds. The mouse movements are used to strengthen the encryption keys.
16. Click Format. It is now creating the VeraCrypt Encrypted Volume container. When it is finished, click OK.
17. Click Exit.
18. Now you must mount this container as a volume. Select a drive letter that is not being used by clicking on it.
19. Click Select File.
20. Navigate to the location where you saved the VeraCrypt Encrypted Volume container and then click Open.
21. Click Mount.
22. When prompted, enter your VeraCrypt container password and then click OK. The volume will now display as mounted. This container is entirely encrypted, including file names and free space, and functions like a real disk. You can copy, save, or move files to this container disk and they will be encrypted as they are being written. Minimize this window.
23. Copy a file to this drive.
24. Open the document from your VeraCrypt container. Did it take any longer to open now that it is encrypted? Close the document again.
25. Maximize the VeraCrypt window and then click Dismount to stop your container. A container will also be unmounted when you log off.