أساسيات أمن الشبكات

جون إ. كانافان

بوسطون – لندن

ترجمة شعيب التجاني مدني

مدير مشاريع نظم معلومات

إهداء

أبنائي شيماء ولمياء ويزن وكمال الدين

حفظهم الله

نبذة عن الكاتب

بدأ جون إ. كانافان حياته المهنية في مجال تكنولوجيا المعلومات منذ أكثر من 17 عاما خلت بالعمل لدى شركة تايم شير المحدودة، وهي شركة خدمات الحاسوب والبرمجيات التي انتجت شبكة Tymnet X.25، ويعمل حالياً نائب الرئيس لنظم المعلومات والتكنولوجيا في شركة شيفرون FCU وأستاذ مساعد في جامعة جولدن جيت حيث يدرس برنامج إدارة الاتصالات. وهو حاصل على بكالوريوس في نظم المعلومات ودرجة الماجستير في إدارة الاتصالات.ويعيش حالياً مع زوجته وابنته في سان فرانسيسكو.

مقدمة الكتاب

عن هذا الكتاب

لقد قررت أن أكتب هذا الكتاب لعدة أسباب. أولا، تتويج لثمانية عشرة عاما من الخبرة المهنية في مجال تكنولوجيا المعلومات (IT) ورغبتي في تعلم المزيد عن هذه المادة، كما أنه أيضا نتيجة لبحث أجريته أثناء أكمال دراستي العليا. معظم قبل كل شيء، قبل كل شيء وفوق ذلكً إن هذا الكتاب نتيجة لالقاء محاضرات في أمن الشبكات. لعدد من سنوات قمت بتدريس محاضرات تطويرية بعنوان "أساسيات أمن الشبكات".

معظم طلابي من المهنيين العاملين في مجال تكنولوجيا المعلومات أو الاتصالات و الذين يحضرون للمحاضرات فيما بعد مواعيد عملهم الرسمية. بعضهم ينخرط في الجانب التقني للعمليات، في حين أن البعض الآخر ينخرط في جانب الأعمال والتسويق.

عندما بدأت في التدريس بحثت عن نص يتناول المواضيع ذات الصلة بطلابي والتي يمكن تطبيقها في مجال عملهم اليومي. بما أن المحاضرات كانت تمهيدية ، أردت أن يغطي الكتاب أساسيات أمن الشبكة.

تتوفر العديد من الكتب الجيدة التي تغطي أمن الحاسوب أو الشبكة. الا أن معظمها تركز على نظام تشغيل معين. بينما أردت كتاب لتوفير معلومات عملية يمكن لطلابي تطبيقها في وظائفهم، بدلا من كتاب واحد يركز فقط على الأمن لنظامي تشغيل يونكس أو النوافذ أن تي.

ونتيجة لذلك، بدأت كتابة هذا الكتاب. عند الكتابة حاولت تغطية المبادئ و المفاهيم الأساسية التي يمكن تطبيقها على جميع أنظمة التشغيل، كما حاولت بقدر الإمكان تقديم أمثلة مفيدة للتطبيق العملي لتلك المبادئ والمفاهيم.

أمن الشبكات والحاسوب أمر بالغ الأهمية للصحة المالية في كل منشأة. إذا كنت لديك شك في هذه العبارة ما عليك سوى قراءة الصحف المحلية. في كل يوم يتم تسجيل حوادث تتعلق بأمن الشبكات. وذكر تقرير صدر مؤخرا أنه في عام 2000 أن القرصنة والفيروسات ستكلف الشركات حوالي 1600000000000 تريليون دولار في جميع أنحاء العالم. يعتبر هذا المبلغ من المال مذهل و له تأثير مباشر على مقدرة الشركات على عوائد استثماراتها أو على اصولها. ويزداد الرقم بصورة مزهلة بالاخذ في الحسبان حقيقة أن الشركات والجامعات ما زالت لا تعامل قضية أمن الحاسوب من ضمن نشاطاتها الأساسية. وبشكل عام، الشركات لاتنفق المال على الحاسوب وأمن الشبكات الا عندما تكون هناك حاجة ملحة لذلك. وحقيقة أن الطلاب يتخرجون من معظم الجامعات او برامج الحاسوب التدريبية من دون أعطائهم ولو درس واحد في أمن الشبكات، الحاسوب أو أمن المعلومات مما يدل على عدم اكتمال وعي معظم الجامعات على أهمية أمن المعلومات.

القطاع المستهدف

هذا الكتاب ليس دليل لقراصنة الحاسوب ، ولا هو معد لخبراء أمن الحاسوب . أنا لا أدعي بأني خبير في أمن الحاسوب. ثم مرة أخرى، أنا لا أعتقد في الذين يدعون التميز على أنهم خبراء على النحو الذي يفعلون. هذا الكتاب أعد لأولئك الذين في بداية رحلتهم الاستكشافية في مجال الحاسوب وأمن الشبكات . إنها نقطة الانطلاق التي منها يتمكن الفرد على بناء أساست المعرفة.

هذا الكتاب والذي يركز على الأمن من منظور الإدارة، يتناول المبادئ والأساليب في سياق علمي حقيقي. تشمل بعض الموضوعات التي تم تناولها إستعراض لأمن الشركات، وضع سياسات الأمن ؛ تحليل المخاطر؛ التهديدات المحتملة ، نقاط الضعف، والتدابير المضادة. التجارة الإلكترونية ، التشفير والأصفار.

المحتويات

الفصل الأول: يستعرض أهمية أمن الشبكات ويعرض بعض المعلومات الأساسية ذات الصلة وكذلك لمحة تاريخية. أيضا بعض المصطلحات الأساسية التي سوف يتم استخدامها في الكتاب لتعريف الشبكة، والمعلومات، وأمن الحاسوب.

الفصل الثاني: يركز على التهديدات ونقاط الضعف، وأنواع مختلفة من الهجمات. أيضا يحدد مصادر مفيدة للمعلومات عن الشبكات وقرصنة الحواسيب.

الفصل الثالث: يناقش التشفير وتطبيقه بصورة عملية. بالإضافة إلى ذلك، يبين بالتفصيل مختلف أنواع الأصفار وتطبيقها، كما أنه يقدم التوقيعات الرقمية، الشهادات الرقمية ، ومفهوم تركيبة المفتاح العام.

الفصل الرابع: لمحة عامة عن برنامج أمان كيربيروس، والتقنية الأساسية التي يستخدمها نظام كيربيروس لتوفير أمن الشبكات. كما أنه يقارن بين برنامج كيربيروس ونظام تركيبة المفتاح العام.

الفصل الخامس: يقدم بروتوكول طبقة مآخذ التوصيل الآمنة (SSL)، ويوضح كيف يستخدم متصفحي ميكروسوفت للشبكات ونت اسكاب نظام تشفير الاصفار الذي تم شرحه في الفصل الثالث.

الفصل السادس: يناقش القضايا الأمنية المرتبطة بإرسال وإستقبال والمصادقة على البريد الالكتروني وحفظه، علاوة على ذلك يستعرض الفصل السادس بروتوكولات البريد الإلكتروني الأمنة المتعددة والتطبيقات المختلفة لتشفير للبريد الإلكتروني كما يناقش مفهوم البريد الإلكتروني كسلاح.

الفصل السابع: يغطى المبادئ التوجيهية الأمنية العامة لنظم التشغيل ويقدم المفاهيم الشائعة أو التي يمكن تطبيقها على معظم أنظمة التشغيل متضمنة المبادئ التوجيهية لكلمة السر وضوابط الدخول للشبكات. بالإضافة إلى ذلك، يستعرض بعض التقنيات المستخدمة لكسر كلمات السر وطرق مواجهة هذه التقنيات. كما يستعرض الفصل السابع القضايا المرتبطة بأجهزة المودم ويقدم بعض الأدوات المفيدة التي يمكن استخدامها لجعل النظام أكثر أمنا.

الفصل الثامن: يغطي المبادئ التوجيهية الأمنية العامة للشبكات المحلية ويقدم مفاهيم سياسة إدارة الشبكات، وأنظمة اكتشاف القرصنة، وتجزئة حركة مرور المعلومات في الشبكات المحلية، وقضايا الأمن المرتبطة باستخدام بروتوكول المضيف الديناميكي (DHCP).

الفصل التاسع: يقدم القضايا الأمنية المرتبطة بالوسائل المادية التي يمكن اسستخدامها لتركيب الشبكات المحلية، كما يناقش القضايا الأمنية التي يجب أن تأخذ في الاعتبار عند تركيب الكوابل واختيار دوائر الشبكات واسعة النطاق و الوسائل ، والبروتوكولات. بالإضافة إلى ذلك، يصف الفصل التاسع نظم الشبكات التالية "frame relay" ، "Xdsl" ، الشبكات المحلية اللاسلكية "LAN"، والشبكات واسعة النطاق "WAN" وأنواع مختلفة من الدوائر.

الفصل العاشر: يناقش المسائل الأمنية بالمتعلقة بأجهزة توجيه بيانات الشبكة ويقدم نظام تشغيل سيسكو الخاص بالإنترنت. كما يناقش بروتوكول إدارة الشبكة البسيطة (SNMP) وبعض المخاطر المترتبة على استخدام هذا البروتوكول.

الفصل الحادي عشر: يشرح طريقة عمل الشبكات الخاصة الافتراضية (VPNs) والاعتبارات التي يجب مراعاتها قبل تنفيذ الشبكات الخاصة الإفتراضية VPN. أيضاً يتناول الفصل الحادي عشر مختلف البروتوكولات قيد الاستخدام وقدم مثالا لتنفيذ الشبكات الخاصة الافتراضية VPN منخفضة التكلفة.

الفصل الثاني عشر: يتناول مفهوم جدار الحماية النارية ويشرح كيف يعمل. بالإضافة إلى ذلك يناقش إيجابيات وسلبيات جدران الحماية النارية ويستعرض أنواع مختلفة من جدران الحماية النارية وكيفية تنفيذها. كما يناقش ايضاً بعض جدران الحماية النارية المجانية والشخصية المتاحة للتحميل.

الفصل الثالث عشر: يتناول مزايا وعيوب أنظمة التحقق من الهوية (Biometrics) وأنظمة المصادقة. بالإضافة إلى ذلك يناقش تقنيات أنظمة التحقق من الهوية المختلفة (Biometerics) والمسائل التي يجب دراستها قبل نشر نظام التحقق من الهوية.

الفصل الرابع عشر: يقدم مناقشة مفصلة لتطوير وتنسيق و المحتوى، التنفيذ، وإنفاذ سياسات وإجراءات أمن الشبكات في الشركة. أيضا يقدم بعض التوصيات العامة للسياسات والإجراءات.

الفصل الخامس عشر: يركز دور التدقيق والمراقبة على الشبكات والنظم في النهج متعدد الطبقات (multitiered) لأمن الشبكات. كما يناقش بالإضافة إلى ذلك طرق التدقيق التقليدية وأدوات التدقيق الآلي والتطور في مجال أنظمة كشف التسلل.

الفصل السادس عشر: يناقش ضرورة وضع الشركات الخطط المناسبة للرد على كارثة أو حادث يتعلقان بأمن الحاسوب. وبالإضافة إلى ذلك، يشرح التخطيط للتعافي من الكوارث ويعرض حالة دراسة. أيضا يتناول التخطيط للاستجابة لطوارئ الحواسيب ويوفر بعض المبادئ التوجيهية العامة. كما يزود بقائمة مصادر معلومات عن التخطيط للاستجابة.

الفصل السابع عشر: يحدد المخاطر المرتبطة بكعكات (Cookie) المتصفحات وملفات تسريع التصفح المؤقتة بالإضافة إلى ذلك يناقش مخاطر وظيفة الإكمال التلقائي المرتبطة بمتصفح ميكروسوفت "Internet explorer".

الفصل 1: مفاهيم الأمن الأساسية

نظرة عامة

يبدو أنه كل يومين تطالعنا الصحف بأخبار عن شبكة حاسوب تعرضت للخطر من قبل قراصنة. في الواقع، منذ وقت ليس ببعيد وقعت وزارة الدفاع الأمريكية ضحية لهجوم قراصنة ناجح؛ تمكن من خلاله القراصنة على اختراق أجهزة حاسوب الوزارة لمدة اسبوعين كاملين قبل اكتشافهم. لحسن الحظ كانت الأجهزة تحتوي فقط على معلومات غير سيرية تتعلق باللموظفين والرواتب، وبناءاً عليه لم يتعرض الأمن القومي للتهديد

وفي الآونة الأخيرة، تم استهداف موقع ياهو (Yahoo)، وامازون دوت كوم (Amazon.com) وإي باي (Ebay) ، وبعض المواقع المشهورة الأخرى في الشبكة العالمية لما يبدو أنه هجوم منسق يعرف ب "الحرمان من الخدمة" ، حيث تعرضت هذه المواقع خلال فترة ثلاثة أو أربعة أيام للزحمة من قصف الكتروني كاذب متزامن من عدة مواقع الكترونية توقفت على اثره هذه المواقع لساعات مرات متكررة. هذه الهجمات توضح مدى خطورة تهديد القراصنة الخارجي على الشركات والمؤسسات.

في نفس الوقت، كل منشأة تستخدم أجهزة حاسوب تواجه القرصنة من أفراد داخل المنشأة. الموظفين الحاليين أو الموظفين السابقين ذوي النوايا السيئة الذين يرغبون في الحصول على معلومات مثل رواتب الموظفين أو الاطلاع علىملفات الموظفين الآخرين. هم أيضا يمثلون تهديدا لحواسيب شبكات المؤسسات.

في الأونة الأخيرة تدور في عالم الحواسيب قصة موظف يعمل مبرمج لدى احدى الشركات شن هجوم الحرمان من الخدمة ضد شركته التي تقدم خدمات تداول الأسهم عبر الانترنت. على ما يبدو، كان هذا مبرمج في مفاوضات مع الشركة لزيادة راتبه.

لقد احبط من طريقة المفاوضات، فقرر أن يثبت للشركة امكانية تعرضها لخطر القرصنة فقام بشن هجوم على أنظمتها من الإنترنت. وبما أنه كان على دراية دقيقة بأنظمة وبرمجيات الشركة مكنته تلك المعرفة الداخلية للشركة ضربها بطريقة أدت الى إغلاقها. في الحقيقة أدى الهجوم الى تعطيل خدمات تداول الأسهم في الشركة لمدة ثلاثة أيام. في نهاية المطاف تمت الاستعانة بجهاز الخدمة السرية الأمريكي وتم تتبع الهجوم الذي قادهم إلى الموظف، وتم ألقاء القبض عليه.

على كل مؤسسة مراقبة أنظمتها من الاقتحام عن طريق الاشخاص غير المصرح لهم وغيرها من الهجمات. يجب أن يكون هذا النشاط جزءا من الروتين اليومي لوحدة تكنولوجيا المعلومات في كل منشأة، حيث أنه ضروري لحماية أصول الشركة من المعلومات.

الطريقة الأكثر وثوقا لضمان سلامة أجهزة حواسيب الشركة هي عدم وضعها على الشبكة والاحتفاظ بها وراء أبواب مغلقة. لسؤ الحظ، هذا ليس حلا عمليا. حيث أنه اليوم تصبح أجهزة الحاسوب أكثر فائدة إذا تم ربطهما معا في شبكة ليتم تبادل المعلومات وتقاسم الموارد، وعلى الشركات التي تضع أجهزة الحواسيب الخاصة بها في شبكة اتخاذ بعض الاحتياطات البسيطة للحد من مخاطر الوصول غير المصرح به.

كل عام الشركات والحكومات، والمنظمات الأخرى تصرف مليارات الدولارات كنفقات متعلقة بأمن الشبكات. كما أن معدل نفقات هذه الجهات يبدو في زيادة مستمرة. ومع ذلك، عندما تحتاج الشركات لإيجاد المجالات التي يمكن خفض الإنفاق عليها من بنود الميزانية ثبت تاريخيا أنها تلجأ للخفض أولا من موازنات التخطيط وأمن الملعومات.

لماذا يعتبر أمن الحاسوب والشبكات مهما؟

ربما يبدو سخيفا أن نطرح هذا السؤال. "لماذا يعتبر أمن الحاسوب و الشبكات مهما؟"

أنه لمن المهم بالنسبة للمنشآت تقدير لماذا يريدون تحقيق أمنً للحواسيب ، وتحديد الكيفية التي سيتم بها تحقيق ذلك. بل هو أيضا أداة مفيدة للاستخدام عند السعي للحصول على إذن الإدارة التنفيذية لتأمين النفقات المتصلة بالأمن. يعتبر أمن الحواسيب والشبكات مهم للأسباب التالية:

• لحماية أصول الشركة: واحد من الأهداف الأساسية لأمن الحاسوب والشبكات هو حماية أصول الشركة. باستخدام عبارة "الأصول"، أنا لا أعني الأجهزة والبرامج التي تشكل الحواسيب والشبكة في الشركة. الأصول هي المعلومات التي يتم حفظها في أجهزة حواسيب الشركة وشبكاتها. تعتبر المعلومات أصول حيوية للشركات وهي ما يهتم به امن الحواسيب والشبكات. وفوق كل هذا حماية وسلامة، وتوافر المعلومات في الوقت المناسب. يمكن تعريف المعلومات بانها البيانات التي يتم تنظيمها والوصول إليها بطريقة متسقة وذات معنى.

• للحصول على ميزة تنافسية: تطبيق وتطوير سياسات أمن معلومات فعال يعطي المنشأة ميزة تنافسية على المنشآت المنافسة لها. لأمن الشبكات أهمية خاصة في ساحة خدمات الإنترنت المالية والتجارة الإلكترونية. ويمكن أن تعني الفرق بين الخدمة واسعة القبول واستجابة العملاء دون المتوسط. على سبيل المثال، كم من الناس تتوقع أن يستخدم نظام الخدمات المصرفية عبر الإنترنت لبنك ما لو يعلمون أن النظام قد اخترق بنجاح في الماضي؟ بالتأكيد قليلا. بل سوف يذهبون إلى استخدام الخدمات المصرفية عبر الإنترنت لمؤسسات مالية أخرى منافسة.

• للتوافق مع المتطلبات التنظيمية والمسؤوليات الائتمانية: الموظفون المعنيين في كل شركة تقع عليهم مسؤولية ضمان سلامة وصحة

المنشأة. جزء من هذه المسؤولية تشمل ضمان ديمومة عمل المنشأة. وبناءاً عليه فان المنشآت التي تعتمد على أجهزة الحاسوب في استمرار عملها يجب أن تضع سياسات وإجراءات معالجة تهتم بمتطلبات أمن المعلومات. هذه السياسات والإجراءات ليست ضرورية فقط لحماية أصول الشركة ولكن أيضا لحماية المنشأة من المسؤولية. لتحقيق الربح أيضاً يجب على المنشآت حماية استثمارات المساهمين وتعظيم العائد. بالإضافة إلى ذلك إن العديد من المنشأت تخضع للتنظيم الحكومي، والذي غالبا ما ينص على متطلبات السلامة والأمن للمنشأة. مثلا، معظم المؤسسات المالية تخضع للتنظيم الاتحادي، وعدم الامتثال للمبادئ التوجيهية الاتحادية يؤدي إلى مصادرة المؤسسة المالية من قبل الجهة التنظيمية الاتحادية. في بعض الحالات، موظفي الشركات الذين لم ينجزوا مهامهم التنظيمية والائتمانية يخضعون للمسائلة الشخصية من قبل المؤسسات المالية التي يعملون بها عن أي خسائر تتكبدها الشركة.

• للحفاظ على وظيفتك: وأخيرا، لتأمين موقف الفرد الوظيفي داخل المنشأة ولضمان آفاق المستقبل الوظيفي، من المهم أن يضع الشخص نفسه في مكان يهتم بوضع تدابير تحمي الأصول التنظيمية. ينبغي أن يكون الأمن جزء من كل شبكة حاسب أو مهام مديرالأنظمة. عدم أداء المهام الوظيفية بشكل كاف يؤدي إلى إنهاء الخدمة.

لا ينبغي أن يكون إنهاء الخدمة نتيجة تلقائية لفشل في نظام أمن المعلومات، ولكن إذا ثبت بعد التحري الدقيق بعد الحادثة، وتم تحديد أن الفشل كان نتيجة لعدم وجود سياسات وإجراءات مناسبة أو عدم الامتثال للإجراءات القائمة، فإنه يتحتم على الإدارة التدخل وإجراء بعض التغييرات.

هناك شيء واحد يجب وضعه في الاعتبار هو أمن الشبكات يكلف المال: إنه يكلف المال للتوظيف و يكلف المال لتدريب الموظفين، وابقائهم في المنشأة؛ يكلف المال لشراء الأجهزة والبرمجيات لتأمين شبكات المنشآة. و لدفع زيادة النفقات العامة وتدني أداء الشبكة والنظام الذي ينتج عن استخدام جدران الحماية النارية والمرشحات، وأنظمة كشف التسلل . ونتيجة لكل لذلك فأن أمن الشبكات ليس رخيصا. ومع ذلك فانه أرخص من التكاليف الناتجة عن أختراق شبكة المؤسسة.

خلفية

بينما أنا دائما قلق من الإحصاءات المستخدمة من قبل المنظمات المختلفة لقياس أو تحديد حوادث أمن المعلومات، إنه من المفيد أن نستعرض بعض الأرقام التي ذكرت مؤخرا. في عام 1999، أجري مسح (دراسة استقصائية) مشترك بين الجمعية الأمريكية للأمن الصناعي و شركة برايس ووتر هاوس كوبرز-(ASIS / PWC) أن 1000 شركة فقدت *أكثر من* 45 بليون دولار نتيجة لسرقة "معلومات خاصة". وقد حصل المسح المشترك على 97 رد صحيح.

وأيضا للفائدة أفاد المسح بما يلي:

- قال خمسة وأربعون في المئة من المستطلعين بأنهم قد تعرضوا لخسارة مالية نتيجة لفقدان المعلومات، والسرقة، أو الاختلاس.
- ذكرت الشركات التي استجابت للبحث أن متوسط حوادث أمن المعلومات 2.45 بتكلفة تقديرية 000,500 دولار لكل حادث.
- زاد عدد حوادث أمن المعلومات المبلغ عنهاشهرياً في السبعة شهراً الاخيرة.

وكذلك أظهر المسح السنوي المشترك بين مكتب التحقيقات الأمريكية ومعهد أمن الحاسوب (FBI (CSI، بعض الأرقام الجديرة بالملاحظة. حصل المسح المشترك بين FBI / CSI على 512 رد من أفراد يعملون في أمن الحاسوب. تقريبا في جميع المجالات، فقد ارتفعت الأرقام للأنواع مختلفة من الحوادث:

- ذكر ثلاثون في المئة من المستطلعين اختراق أمني من مصدر خارجي.
- ذكر خمسة وخمسون في المئة من المستطلعين تدخلا غير مصرح به من قبل مصدرداخل المنشأة.
- من بين هؤلاء المستجيبون الذين حلت بهم خسائر أرتفع متوسط الخسائر الناتج من سرقة المعلومات خاصة من 1677000 دولار في عام 1998 إلى 1847652 دولار في عام 1999.
- ارتفع متوسط الخسائرة الناجمة عن الاحتيال المالي من 388،000 دولار في عام 1998 إلى أكثر من 1400000 دولار في عام 1999.
- تم تقدير إجمالي الخسائر المالية بسبب الجرائم ذات الصلة بالحاسوب للمستطلعين ال 521 إلى أكثر من 120 مليون دولار.

ومن المثير للاهتمام أن نلاحظ أن معظم الجرائم المتعلقة بالحاسوب لم يبلغ عنها. إذا أخذت الأرقام التي ذكرت في هذه الاستطلاعات وحاوت الاستنتاج بالتعميم على جميع المنشآت،فان العدد المحتمل لحوادث أمن المعلمات والخسائر المالية المرتبطة بها قد تربك العقل. بعض التقديرات تزعم أن أن ما يصل إلى 90٪ من الجرائم ذات الصلة بالحاسوب لم يتم الإبلاغ عنها للسلطات القانونية ولا للمحاكم. ربما قد تعرض الشركات نفسها للدعاوى قضائية، السخرية، وفقدان ثقة العملاء عن طريق الاعتراف بالخسائر المالية ذات الصلة بالحاسوب.

لقد أطلعت على تقديرات من مصادر مختلفة عن الخسائر المالية السنوية ذات الصلة بالجرائم المتعلقة بالحاسوب تتراوح بين 5 مليار و 45 مليار دولار. يبدو واضحا أن التكلفة السنوية المرتبطة بجرائم الحاسوب كبيرة وأنها في تزايد كل عام.

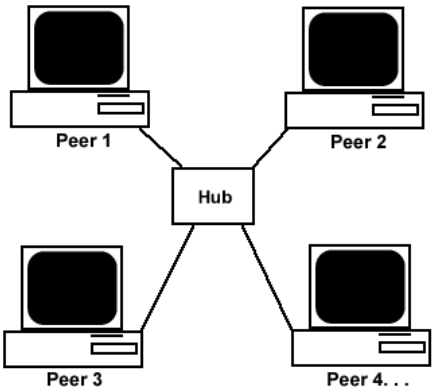
لمحة تاريخية

الحاجة إلى أمن الشبكات متطلب جديد نسبيا. قبل ثمانينيات الفرن الماضي أكثر الحواسيب لم يكن مرتبطا بشبكة. ولم يكن ذلك بسبب عدم وجود رغبة لربط الأجهزة ؛ بل كان نتيجة لعدم وجود التقنية. وكانت معظم الأنظمة كبيرة أو أنظمة متوسطة يتحكم بها و تدار مركزيا. يتواصل المستخدمون مع أجهزة الحاسوب المركزية من خلال شاشات فرعية وكانت تلك الشاشات ذات قدرات محدودة. تتطلب الشاشات اتصال فعلي على منفذ مخصص. في كثير من الأحيان تستخدم منافذ الاتصالات التسلسلية التي تستخدم بروتوكول (RS-232). و عادة ما يتطلب منفذ واحد لكل شاشة واحدة. شركة أي بي أم للمعدات الرقمية، وبعض الشركات الأخرى المصنعة للحواسيب طورت بعض الاختلافات على هذه العمارة من خلال استخدام خادمات الشبكات الطرفية، ولكن المفهوم الأساسي كان هو نفسه. لم يكن هناك شيء يعادل ما لدينا اليوم من تكنلوجيا حيث مئات أو الآلاف من الاتصالات يمكن أن تتصل بالنظام من خلال دائرة شبكة الكترونية واحدة.

في الثمانينيات، مزيج تطوير أجهزة الحاسوب الشخصية (PC) ووضع معايير قياسية لبروتوكول الشبكات، وانخفاض تكلفة عتاد الأجهزة وتطوير تطبيقات برمجية جديدة جعل الشبكات ممارسة أكثر قبولا بكثير. ونتيجة لذلك شهدت الشبكات المحلية والشبكات الواسعة النطاق والحواسيب الموزعة نموا هائلا خلال تلك الفترة.

عند بداية تطوير الشبكات المحلية كانت آمنة نسبياً، آمنة لأنهاكانت اساساً معزولة ولم تكن مرتبطة بالشبكات الواسعة النطاق لذلك طبيعتها المستقلة أدت الى المحافظة على موارد الشبكة.

في الواقع الشبكات الواسعة النطاق سبقت الشبكات المحلية وكان متواجدة منذ فترة، لكنها عادة كان يتم التحكم فيها مركزيا ويمكن الوصول إليها من قبل عدد قليل من الأفراد في معظم المنشآت. الشبكات الواسعة النطاق تستخدام الدوائر المباشرة أو المملوكة الخاصة أو المؤجرة وكانت آمنة نسبيا لأن الوصول إلى الدوائر محدود النطاق. ولتوصيل موقعين (النقطتين أ و ب) عادة يتطلب دائرة توصيل من نوع نقطة الى نقطة (أ – ب). إذا أردت ربط موقع ثالث (نقطة ج) الى الموقعين السابقين (أ و ب) فإن ذلك يتطلب دائرتين اضافيتين حيث يصير الاتصال (أ – ب ، أ – ج و ب – ج). الشكل 1.1 ويوضح هذا المفهوم.



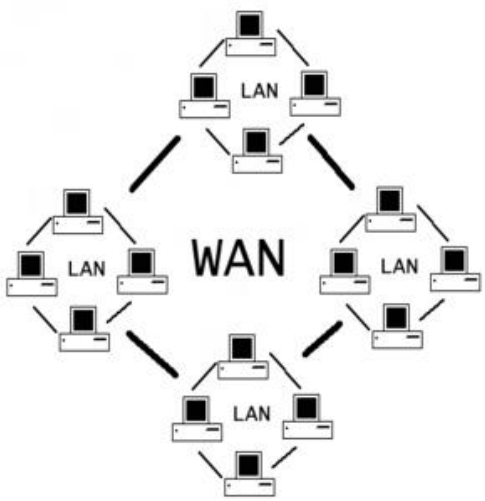
الشكل 1.1: شبكات النطاق الواسع نوع نقطة إلى نقطة.

تطوير بروتوكولات حزم البيانات مثل X.25 وبرتوكول التحكم بالإرسال / بروتوكول الإنترنت تي سي بي / أي بي (TCP / IP) ادي الى تخفيض تكلفة تركيب الشبكات واسعة النطاق، مما جعلها أكثر جاذبية للمستخدمين. هذه البروتوكولات سمحت للعديد من الأنظمة المشاركة في استخدام الدوائر. كثير الأشخاص أو المنشآت يمكنهم أن الإتصال عن طريق الشبكة المشتركة. وبناءاً عليه لم يعد من الضروري استخدام نظام ربط الأنظمة نوع نقطة إلى نقطة. بدأت نقاط الضعف تظهر مع تطويرهذه البيئة من الأجهزة الموزعة التي

تستخدم نظم مشاركة الحواسيب، واستخدام نظام الحزم المعتمدة على بروتوكولات مثل تي سي بي / أي بي TCP / IP ومفهوم النظم الموثوق بها.

الأنظمة في شبكة الاتصال "تثق" في بعضها البعض. وقد يصبح الموقف سيئ في كثير من الأحيان نتيجة لربط شبكات محلية آمنة نسبيا إلى شبكات واسعة النطاق غير أمنة . ويوضح الشكل 1.2 مفهوم شبكة تبادل الحزم.

مبدئيا شبكة اتصالات المنشأة تدخل في سحابة شبكة تبادل الحزم وتكون هناك منشأت أخرى تشترك في استخدام نفس السحابة،وبناءاً عليه تختلط حزم بيانات المنشآة مع حزم بيانات المنشآت الأخرى.



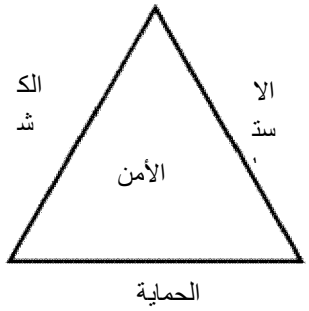
الشكل 1.2: شبكة واسعة النطاق تستخدم نظام حزم البيانات

في بيئة التوزع هذه يكون التركيز على توفير سهولة الوصول والربط بين الشبكات. أمن الشبكة كان يعامل كأمر ثانوي، هذا إذا وضع في الحسبان من الأساس. ونتيجة لذلك فإن العديد من الأنظمة تكون مفتوحة و معرضة بشكل كبير لتهديدات لم تكن موجودة في السابق.

الإنترنت هي النظام الأكبر والأكثر شهرة في استخدام هذا النوع من الشبكات. تستخدم الإنترنت برتكول تي سي بي / أي بي (TCP / IP) الذي يهدف في المقام الأول لربط أجهزة الحاسوب بطريقة سهلة فعالة بغض النظر عن نظم التشغيل الخاصة بها. الأمن لم يكن جزءا من التصميم المبكر لبرتكول تي سي بي/ أي بي (TCP / IP)، وكانذلك سبباً للعديد من الهجمات على نطاق واسع التي تم فيها استغلال نقاط الضعف في تصميم البرتكول. وكان أحد الأحداث المعروفة دودة الإنترنت التي تسببت في جثو الإنترنت على ركبتيها في عام 1986. واليوم يعتبر الأمن أكثر أهمية من سهولة الوصول.

مثلث الأمن

إن أضلاع مثلث الأمن الثلاثة هي الوقاية والكشف والرد على ذلك، تمثل أساس أمن الشبكات. وينبغي أن يكون مثلث الأمن الأساس لجميع السياسات الأمنية والتدابير التي تطورها المنشأة وتقوم بتطبيقا . انظر الشكل 1.3



الشكل 1.3: مثلث الأمن.

الحماية

إن أساس "قاعدة" مثلث الأمن هو الوقاية. لتوفير مستوى معين من الأمن من الضروري اتخاذ تدابير لمنع استغلال نقاط الضعف. وذلك بعمل خطط أمن الشبكات، ينبغي على المنشأت التركيز على التدابير الوقائية أكثر من الكشف والاستجابة ، إنه أسهل وأكثر كفاءة و أقل تكلفة لمنع خرق أمني من الاكتشاف أو الرد. تذكر أنه من المستحيل وضع خطة أمنية من شأنها أن تمنع جميع نقاط الضعف من الاستغلال، لكنه ينبغي للشركات أن تتخذ تدابير أمن وقائية قوية تكفي لتثبيط المجرمين المحتملين ، مما يجعلهم يتجهون الى أهداف أخري سهلة .

الكشف

حالما تم اعداد التدابير الوقائية يجب وضع الإجراءات حيز التنفيذ حالا وذلك من أجل الكشف عن المشاكل المحتملة أو الخروقات الأمنية، في حال فشلت التدابير الوقائية. كما سوف نبين في فصل لاحق، من المهم جدا أن يتم الكشف عن المشاكل على الفور. كلما تم الكشف عن مشكلة بسرعة فإنه من الأسهل لتصحيح والإصلاح.

الاستجابة

تحتاج المنشآت لوضع خطة تحدد الرد المناسب على الإختراق الأمني. وينبغي أن تكون الخطة مكتوبة وتحديد الشخص المسؤول عن كل اجراءا والردود ومستويات التصعيد المختلفة.

قبل البدء في مناقشة جدية عن أمن الحواسيب وأمن الشبكات، نحن بحاجة لتحديد ما تنطوي عليه الخطة.أولاً : أمن الشبكات ليس مشكلة تقنية؛ بل هو مشكلة متعلقة بالعمل والأشخصاص. التقنية هي الجزء السهل من الأمر. الجزء الصعب هو وضع خطة أمنية تناسب مهام المنشأة العملية و حمل الموظفين على الألتزام بالخطة.

وبعد ذلك، يتعين على الشركات الإجابة على بعض الأسئلة الأساسية، بما في ذلك ما يلي.

- كيف يمكن تعريف أمن الشبكات؟
- كيف تعرف المستوى الأمني المناسب؟

للإجابة على هذه الأسئلة، من الضروري تحديد ما تريد تحاول حمايته.

أمن المعلومات

قبل كل شي أمن الشبكات يهتم بأمن أصول الشركة من معلومات. كثيرا ما نغفل عن حقيقة أن المعلومات وقدرتنا على الوصول إلىها هو ما نحاول حمايته وليس أجهزة الحاسوب والشبكات. لدي تعريف بسيط لأمن المعلومات:

أمن المعلومات = السرية + الصحة + توفر المعلومة + عمليات الوصول اليها

لذا لا يمكن أن يكون هناك أمن معلومات بدون السرية؛ هذا يضمن أن المستخدمين الغير مصرح لهم لايمكنهم اعتراض المعلومات أو نسخها، أو تكرارها. في نفس الوقت التكامل ضروري بحيث يكون للمنشآت ما يكفي من الثقة في دقة المعلومات للعمل عليها. علاوة على ذلك يتطلب أمن المعلومات أن تكون المنشأة قادرة على استرجاع البيانات؛ تعتبر تدابير أمن المعلومات لا قيمة لها إذا لم تتمكن المنشأة من الوصول إلى المعلومات الحيوية التي تحتاجها للعمل في الوقت المناسب. وأخيرا تعتبر المعلومات غير آمنة بدون وجود صلاحيات تحدد المستخدم النهائي الذي يسمح له بالوصول اليها.

من بين العديد من عناصر أمن المعلومات يجب التأكد من الأمن المادي الكافي وتوظيف الأشخاص المؤهلين وتطوير السياسات والإجراءات والالتزام بها، وتعزيز ومراقبة الشبكات والأنظمة. وتطوير تطبيقات برمجية آمنة. من المهم أن نتذكر أن أمن المعلومات ليس فقط عن حماية الأصول من المتسللين الخارجيين. في معظم الأحيان تأتي التهديدات من داخل المنشأة: "لقد وجدنا العدو، أنه نحن ".

أمن المعلومات أيضا يختص بالإجراءات والسياسات التي تحمي المعلومات من الحوادث، وعدم الكفاءة، والكوارث الطبيعية. هذه السياسات والإجراءات يجب أن تعالج ما يلي:

- النسخ الاحتياطي، وضوابط التكوين، وضوابط الوسائط.
- التعافي من الكوارث وتخطيط للطوارئ.
- سلامة البيانات.

ومن المهم أيضا أن نتذكر أن أمن الشبكات ليستمطلقاً . الأمني نسبي. يجب التفكير في أمن الشبكات كطيف ينطلق من غير مأمون جدا لغاية أمن جداً . مستوى الأمن لنظام أو شبكة يعتمد على موقعها على طول هذا الطيف بالنسبة للأنظمة الأخرى. فهو إما أكثر أمنا أو أقل أمانا من الأنظمة الأخرى بالنسبة إلى تلك النقطة. وليس هناك شيء اسمه شبكة آمنة تماما أونظام آمن تماماً .

أمن الشبكة هو الفعل المتوازن الذي يتطلب نشر "الدفاعات المناسبة." يجب أن تكون الدفاعات التي يتم نشرها أو تنفيذها متناسبة مع التهديد. تحدد المنشأت ما هو مناسب بعدة طرق، وصفت على النحو التالي:

- تحقيق التوازن بين تكلفة الأمن مقابل قيمة الأصول التي يحمون.
- موازنة المحتمل مقابل الممكن؛
- موازنة احتياجات الأعمال مقابل الاحتياجات الأمنية.

يجب على المنشآت تحديد مقدار التكلفة التي سوف تترتب على اختراق كل النظام أو الشبكة، أو بعبارة أخرى، كم سيكلف بالدولار فقدان المعلومات أو الوصول للنظام أو سرقة المعلومات. عن طريق قياس قيمة نقدية للتكلفة التي سوف تترتب على اختراق النظام أو الشبكة ، يمكن للمنشأت تحديد الحد الأعلى الذي هم على ستعداد لدفعه لحماية أنظمتهم. بالنسبة للعديد من المنشأت هذه العملية ليست ضرورية ، لأن الأنظمة هي شريان الحياة بالنسبة للمنشآة. بدونها لا وجود للشركة.

تحتاج المنشأت أيضا إلى تحقيق التوازن بين تكلفة الأمن مقابل تكلفة المهددات الأمنية. عموما، حيث أن الاستثمار في الأمن في زيادة، ينبغي أن تتناقص الخسائر المتوقعة. كما يجب على شركات ألا تستثمر في الأمن أكثر من قيمة الأصول التي يراد حمايتها. وهنا مكمن استخدام تحليل فوائد التكاليف المالية.

وعلاوة على ذلك، يجب على المنشآت أ، توازن التهديدات المتوقعة مقابل التهديدات المحتملة: إذ أنه من المستحيل الدفاع ضد كل نوع ممكن من الهجوم، من الضروري تحديد ما هي أنواع التهديدات أو الاعتداءات التي لديها احتمال حدوث أكبر ومن ثم تحمي المنشأة ضدها. على سبيل المثال، فمن الممكن أن تخضع المنشأة لمراقبة فان إيك (VAN ECK) [1] أو التعرض للهجوم عن طريق تردد الراديو عالي الطاقة (2] (HERF] ، لكن الاحتمال ضعيف.

من المهم أيضا تحقيق التوازن بين احتياجات العمل والحاجة إلى الأمن، وتقييم تأثيرالتشغيل لتنفيذ التدابير الأمنية. التدابير والإجراءات الأمنية التي تتعارض مع عملية المنشأة تعتبر عديمة الفائدة. هذه الأنواع من التدابير عادة ما يتم تجاهلها أو الالتفاف حولها من قبل موظفي الشركة، لذلك فإنهم يميلون إلى خلق الثغرات الأمنية بدلا عن اغلاقها. بقدر الامكان، ينبغي أن تكمل التدابير الأمنية للاحتياجات التشغيلية والتجارية للمنشأة.

[1] مراقبة فان إيك (VAN ECK) هو رصد لنشاط جهاز حاسوب أو غيره من المعدات الإلكترونية عن طريق الكشف عن مستويات منخفضة من الانبعاثات الكهرومغناطيسية من الجهاز. وقد تم اطلاق هذا الاسم بعد أن نشر الدكتور ويم فان إيك الذي عن هذا الموضوع في عام 1985.

[2] سلاح تردد الراديو عالي الطاقة (HERF) هو جهاز يمكن أن يعطل التشغيل العادي للمعدات الرقمية مثل أجهزة الحاسوب والمعدات الملاحية من خلال توجيه انبعاثات تردد الراديو عالية الطاقة (HERF) عليه.

تقييم المخاطر

فكرة تقييم المخاطر أمر بالغ الأهمية لتطوير الدفاعات المناسبة. لإجراء تحليل المخاطر، تحتاج المنشأت لفهم التهديدات ونقاط الضعف المحتملة. الخطر هو احتمال أنه سيتم استغلال نقطة ضعف. فيما يلي قائمة الخطوات الأساسية لتقييم المخاطر :

1. تحديد وترتيب أولويات الأصول؛
2. تحديد نقاط الضعف.
3. تحديد التهديدات واحتمالات وقوعها؛
4. تحديد التدابير المضادة؛
5. عمل تحليل التكاليف والفوائد.
6. تطوير السياسات والإجراءات الأمنية.

لتحديد وترتيب أولويات أصول المعلومات ووضع تحليل التكاليف والفوائد، من المفيد طرح بعض الأسئلة البسيطة مثل التالية.

- ماذا هو الشيء الذي تريد حمايته؟
- لماذا تريد حمايته؟
- ما هي قيمته؟
- ما هي التهديدات؟

- ما هي المخاطر؟
- ما هي الآثار المترتبة عند حدوثها؟
- ما هي السيناريوهات المختلفة؟
- كم ستكلف خسارة المعلومات أو نظام؟

تحديد أولويات الأصول والنظم عن طريق تعيين قيمة نقدية لها. القيمة النقدية يمكن أن تكون تكلفة الاستبدال، تكلفة فقدان الأصول أو تكلفة تملك الأصل، مثل المعلومات السرية التي حصل عليها منافس. من الضروري أيضا تضمين تكاليف غير مرئية "أكثر غموضا"، مثل فقدان ثقة العملاء. إبعاد أمكانية حدوث التهديدات المحتملة. تحديد ما هي التهديدات على الأرجح، ووضع تدابير حماية من تلك التهديدات.

نماذج الأمن

هناك ثلاثة أساليب أساسية مستخدمة لتطوير أمن الشبكات. وعادة ما تستخدم الشركات مزيج من الأساليب الثلاثة لتحقيق الأمن. الثلاثة أساليب هي الأمن من خلال الغموض، ونموذج الدفاع المحيط، ونموذج الدفاع في العمق.

الأمن عن طريق الغموض

الأمن عن طريق الغموض يعتمد على التخفي للحماية. المفهوم الكامن وراء هذا النموذج هو أنه إذا كان لا أحد يعرف وجود شبكة أو نظام في المنشأة، فانها لن تكون عرضة للهجوم. الأمل الأساسي هو أن تخبأ الشبكة أو على الأقل لا يتم الإعلان عن وجودها فإن ذلك يؤدي الغرض كنظام أمن. المشكلة في هذا الأسلوب هو أنه لن يعمل على المدى الطويل، حال ما تم اكتشفاف الشبكة، سوف تكون الشبكة معرضة للخطر تماما.

دفاع المحيط

نموذج دفاع المحيط مشابه لقلعة يحيط بها خندق. عند استخدام هذا النموذج من أمن الشبكات فان المنشأت تقوي أو تعزز محيط الأنظمة وأجهزة التوجيه الحدودية، أو تخفي المنشأة شبكتها خلف جدار حماية نارية ليعزل شبكتها الأمنة عن الشبكات الغير موثوق بها. هذا النموذج لا يفعل الكثير لتأمين الأنظمة الأخرى في الشبكة. الافتراض هو أن أسلوب دفاع المحيط كافي لوقف أي دخلاء من الخارج وبناءاً عليه تكون الأنظمة الداخلية آمنة.

هناك العديد من العيوب في هذا المفهوم: أولا، هذا النموذج لا يفعل شيئا لحماية الأنظمة الداخلية من الهجوم من الداخل. كما ناقشنا سابقا، فإن غالبية الهجمات على شبكة الشركة يتم شنها من شخص داخل المنشأة.ثانياً، تقريبا دائما ما يفشل دفاع المحيط في نهاية المطاف. وحالما حدث ذلك، فإن الأنظمة الداخلية تكون مفتوحة على مصراعيها للهجوم.

الدفاع في العمق

الأسلوب الأكثر قوة يمكن استخدامه هو نموذج الدفاع في العمق. أسلوب الدفاع في العمق يقاتل من أجل الأمن من خلال تقوية ومراقبة كل نظام على حدة. كل نظام هو جزيرة تدافع عن نفسها. كما أن هناك تدابير إضافية تتخذ على أسلوب الدفاع محيط، ولكن أمن الشبكة الداخلية لا يبقي منفصلا عن أنظمة الدفاع في المحيط. هذا الأسلوب أكثر صعوبة في التحقيق ويتطلب من جميع النظم ومسؤولي الشبكة القيام بدورهم في العملية. مع ذلك في ظل هذا النموذج من غير المرجح أن يتم المساس بالشبكة الداخلية في حال أن أحد مسؤولي النظام ارتكب خطأ ، على سبيل المثال وضع جهاز مودم غير آمن في النظام، عند استخدام أسلوب الدفاع في العمق فإن النظام الذي تم تركيب المودم فيه قد يكون عرضة للاختراق بينما تكون الأنظمة الأخرى في الشبكة قادرة على الدفاع عن نفسها. كما ينبغي أيضا على الأنظمة الأخرى أن تكون قادرة على الكشف عن أي محاولة اختراق من أي نظام مخترق في الشبكة. أيضا هذا الاسلوب يوفر حماية أكثر ضد العمليات الداخلية.أنشطة المخترق الداخلي تكون سهلة الكشف نسبياً .

مصطلحات الأساسية

التهديدات

التهديد أي شيء يمكن أن يعطل عمل أو وظائف أو سلامة أو توافر الشبكة أو النظام للاستخدام. هناك أنواع مختلفة من التهديدات، هناك تهديدات حوادث الطبيعية مثل الفيضانات والزلازل، والعواصف. وهناك أيضا التهديدات غير المتعمدة التي تنتج عن الحوادث والاخطاء الناتجة عن الاهمال. وأخيرا، هناك التهديدات المتعمدة و التي تكون نتيجة لسوء النية. أي نوع من أنواع التهديد يمكن أن تكونمميتاً للشبكة.

نقاط الضعف (الثغرات)

الثغرة هي نقطة ضعف تكون في تصميم أو تهيئة أو تنفيذ الشبكة أو النظام الشيء الذي يجعلها عرضة للتهديد. معظم نقاط الضعف عادة ما يمكن ارجاعها الى واحد من ثلاثة مصادر:

1. **ضعف التصميم**: الأجهزة والبرامج التي تحتوي على عيوب في التصميم والتي يمكن استغلالها.مبدئياً عندما يتم انشاء الأنظمة تحتوي على ثغرات أمنية. مثال على ذلك هذا النوع من الضعف، تغرة ارسال البريد في النسخ الأولي لنظام يونكس. عيوب ارسال البريد مكنت القراصنة من الحصول على ميزة الدخول الى النظام "الأصلي" في نظام تشغيل يونكس. تم استغلال هذه العيوب في مناسبات عديدة.

2. **سوء التنفيذ:** الأنظمة التي تم تكوينها بشكل غير صحيح تكون عرضة للهجوم. هذا النوع من الضعف عادة ما يكون ناتجاً عن قلة الخبرة، عدم الحصول على تدريب كاف، أو تنفيذ العمل بصورة غير متقنة. مثال على هذا النوع من الضعف أن لا يحتوى النظام على امتيازات تقيد الوصول للملفات التنفيذية الحساسة، وبالتالي السماح للمستخدمين غير المصرح لهم بتعديل هذه الملفات.

3. **سوء الإدارة**: الإجراءات غير الكافية وعدم كفاية التأكد والموازنة. الإجراءات الأمنية لا يمكن أن تعمل في فراغ. يجب أن تكون موثقة ومراجعة. حتى الأشياء البسيط مثل النسخ الاحتياطي اليومي للنظام يجب أن يتم التحقق منه. وهناك حاجة أيضا لفصل المهام لبعض الوظائف وازدواج لآخرى. بهذه الطريقة، يمكن للمنشأة أن تضمن تقيد الموظفين بالإجراءات ، وأنه لا يوجد شخص واحد لديه السيطرة الكاملة على النظام.

في حين أن هناك ثلاثة مصادر فقط لنقاط الضعف، فإنها يمكن أن تعبر عن نفسها بطرق كثيرة.

نقاط الضعف المادية

القاعدة الأولى لأمن كانافان (Canavan) هي لحماية مكونات الأنظمة والشبكات. هل أنظمتك ومعدات الاتصالات والوسائط توجد في مكان آمن؟ أجهزة الاستضافة المركزية وخودم الشبكات يجب أن توضع في غرف مؤمنة يدخلها فقط الموظفين المصرح لهم. وينبغي أيضا أن تبقى أجهزة التوجيه ومعدات الاتصالات في مواقع آمنة مقيدة الوصول. إضافة إلى ذلك الوسائط المهمة القابلة للحركة ، مثل وسائط النسخ الاحتياطي يجب أن تخزن في المنطقة أمنة يستطيع الموظفين المخولين فقط الوصول اليها.

وكجزء من هذه العملية، تحتاج المنشأت إلى الأخذ في الاعتبار البيئة المادية والطبيعية التي تعمل فيها. ينبغي أن تنظر في احتمال حدوث الزلازل والحرائق و الفيضانات و "أقدار الله سبحانه وتعالى" الأخرى وتخطط وفقا لذلك. التخطيط السليم للمرافق المادية يمكن أن يخفف كثيرا من آثار الكوارث الطبيعية. على سبيل المثال، المنشأت في المناطق المعرضة للزلازل في حاجة إلى تثبيت معداتهم في هيكل المبنى بحيث لا تسقط من الجدران أو من النوافذ أثناء وقوع زلزال قوي. المنشأت الواقعة في مناطق الفيضانات يجب لا تضع غرف أجهزة الحاسوب الخاصة بها في اقبية المباني. انه حقا لا شيء أكثر من الحس السليم.

الأجهزة والبرمجيات

عيوب التصميم في الأجهزة أو البرامج تجعل الأنظمة عرضة للهجوم أو تؤثر على توافر النظم. على سبيل المثال، خلل ارسال رسائل البريد الالكتروني في الإصدارات الأولي لنظام تشغيل يونكس مكنت القراصنة من الحصول على امتيازات الوصول إلى النظم.

نقاط الضعف الوسائط

الأقراص والأشرطة الوسائط الأخرى يمكن أن تتعرض للسرقة، الفقدان، أو العطب. يمكن نسخ المعلومات واخذها من مرافق المؤسسة دون الكشف عنها. وفقا لذلك، تحتاج الشركات إلى ضمان سلامة جميع الوسائط التي تحتوي على معلومات حيوية.

نقاط ضعف بث الإشارة - اعتراض المعلومات

الإشارة المرسلة من المعدات الكهربائية يمكن اعتراضها عن بعد ومراقبتها باستخدام أجهزة متطورة في عملية يشار إليها أحيانا برصد فان إيك (VAN ECK). المنشأت تحتاج أيضا إلى أن تكون قلقة بشأن اعتراض معظم أشكال الاتصال.

الاتصال هو تبادل المعلومات عبر وسيط. على هذا النحو، فهو بطبيعته عرضة للاعتراض والرصد والسرقة والتغيير، والانقطاع. كل واسطة تستخدم لنقل المعلومات يمكن "استغلالها". متحسس الشبكات أو متحسس حزم الاتصالات هي أدوات القراصنة المشتركة التي يمكن أن تقرأ حركة مرور البيانات عندما تمر عبر شبكة، أيضاً الثغرات ربما تسبب ضررا أكثر مما ينفع القراصنة عندما يتعلق الأمر بعرقلة الاتصالات.

نقاط الضعف البشرية

الأهمال البشري، اللامبالاة، الكسل، الجشع، والغضب تمثل أكبر تهديدات للشبكات والنظم وتسبب الكثير من الضرر عن بقية العوامل الاخري مجتمعة.

علاوة على ذلك فان نقاط الضعف البشرية والمخاطر المرتبطة بها هي أصعب التهديدات التي يمكن التصدي لها.

من المهم أن نضع في اعتبارنا أن كل شبكة أو نظام تم تصميمه أو تهيئته أو تم تطويره مؤخرا لديه نقاط ضعف. لا يوجد شيء يسمى شبكة آمنة تماما أونظام آمن تماماً . ذلك شيء لا وجود له!

التدابير المضادة

التدابير المضادة هي التقنيات أو الأساليب المستخدمة للدفاع ضد الهجمات و سد أو قفل نقاط الضعف في الشبكات أو الأنظمة.

مصطلحات أساسية إضافية

قبل الشروع في مناقشة جدية لأمن الشبكة، من الضروري أولا تعريف بعض المصطلحات الأساسية المتعلقة بأمن الشبكة. هذه المسطلحات هي الأساس لأي مناقشة لأمن الشبكات وهي العناصر المستخدمة لقياس أمن الشبكة. ليتم اعتبارها متقدمة بما فيه الكفاية على طول الطيف الأمني، يجب أن يعالج النظام بشكل كاف تحديد الهوية، والمصادقة، التحكم في الدخول أو الإذونات، التوافر والسرية والسلامة والمسئوليات، وعدم الإنكار. سيتم شروح كل منها في الأقسام التالية.

تحديد الهوية

تحديد الهوية ببساطة هو عملية تحديد الذات إلى كيان آخر أو تحديد هوية الفرد أو الكيان الذين تتواصل معهما.

المصادقة

تخدم المصادقة كدليل على أنك الشخص الذي تدعيه أو ما تدعي أن تكون. المصادقة أمر بالغ الأهمية إذا أريد أن يكون هناك ثقة بين طرفين. المصادقة مطلوبة عند الاتصال بواسطة شبكة أو تسجيل الدخول إلى الشبكة. عند الاتصال بواسطة شبكة يجب أن تسأل نفسك سؤالين: 1) مع من أنا اتواصل؟ و2) لماذا اصدق أن هذا الشخص أو الكيان هو أو هي أو من يدعي أن يكون هو الشخص الحقيقي؟ إذا لم يكن لديك إجابة جيدة للسؤال رقم 2، هناك احتمالات أن تكون أخطأت في الإجابة على السؤال رقم 1.

عند تسجيل الدخول إلى شبكة، تستخدم ثلاثة سناريوهات أساسية للمصادقة. في كثير من الأحيان تستخدم الشبكات استخدام مزيج من أكثر من واحد من هذه السيناريوهات، من السناريوهات شيء تعرفه، شيء لديك، وشيء كنته ، سيتم شرح هذه السناريوهات على النحو التالي:

شيء تعرفه: السيناريو الأكثر استخداما هو "شيء تعرفه " وعادة ما يكون شيئا تعلم أنه يصادق هويتك مثل كلمة سر، أو رمز، أو تسلسل. يقوم الأمن على فرضية إذا كنت تعرف كلمة المرور السرية أو رمز المرور فانه يجب أن تكون أنت الشخص الذي تدعيهوبناءاً عليه يؤذن لك باستخدام لشبكة. على الرغم من أن هذا السيناريو يستخدم على نطاق واسع الا أنه غير أمن تماماً . فمن السهل الالتفاف عليه أو اختراقه.

• **شيء لديك**: "شيء ما لديك" يتطلب مفتاح، شارة، أو بطاقة رمزية، بعض الأدوات أو شيء الذي يتيح لك الاستخدام. ويعتمد الأمن على مفهوم أن الأفراد أو الكيانات المصرح لها فقط يمكنهم استخدام جهاز معين. يعيب هذا السيناريو أن "الشيء" يمكن أن يضيع أو يسرق.

• **شيء يتعلق بك**: "شيء يتعلق بشخصك" المصادقة تعتمد على السمات المادية أو السلوكية. ويشار إلى هذا النوع بالمصادقة الحيوية (Biometric) . وفقا لنظام البيومترك يمكن مصادقة الهوية بناء على بصمات الأصابع، أو صوت الشخص، أو مسح قزحية العين. حتى

نقرات المفاتيح (مرافقة بسمة مادية أو سلوكية تقريبا) يمكن استخدامها. هذه النظم إذا صمم بشكل صحيح التحايل عليه أو اختراقه يكون صعباً للغاية. الحيلة هي العثور على نظام واحد يعمل بشكل صحيح.

التحكم في الوصول (الترخيص)

وهذا يشير إلى المقدرة على التحكم في مستوى استخدام الأفراد أو الكيانات لشبكة أو نظام، وكم المعلومات التي يمكنهم الحصول عليها. مستواك في التصريح يحدد في الاساس ما الذي يسمح لك أن تفعله بمجرد المصادقة لك والسمح لك باستخدام الشبكة، أوالنظام، أو بعض الموارد الأخرى مثل البيانات أو المعلومات. التحكم في الوصول تحديد مستوى إذن استخدام نظام أو شبكة، أو معلومات (على سبيل المثال مصنفة، سرية، أو سرية للغاية).

توفر النظام

هذا يشير إلى ما إذا كانت الشبكة أونظام أوالأجهزة أوالبرمجيات موثوق بها ويمكن استعادتها بسرعة وبشكل كامل في حال حدوث انقطاع في الخدمة. من الناحية المثالية ينبغي أن تكون هذه العناصر عرضة لهجمات الحرمان من الخدمة.

السرية

وهذا أيضا يمكن أن يطلق عليه الخصوصية أو السرية، ويشير إلى حماية المعلومات من الكشف غير المصرح به. وعادة ما يتحقق إما عن طريق تقييد الوصول إلى المعلومات أو عن طريق تشفير المعلومات بحيث تصبح غير مفيدة للأفراد أو الكيانات الغير مصرح لها بالاطلاع عليها.

سلامة المعلومات

يمكن التفكير في هذا على أنه دقة المعلومات. ويشار إلى هذا على أنه القدرة على حماية المعلومات والبيانات، أو الإرسال من التعديلات غير مصرح بها أوغير المتحكم فيها أو الاعتراضية. مصطلح السلامة أيضا يمكن أن يستخدم في إشارة إلى سير عمل الشبكة، النظام أو البرنامج التطبيقي.

عندما يستخدم المصطلح في الإشارة إلى المعلومات أو البيانات هناك عدة متطلبات للسلامة. أولا، يجب أن تكون البيانات متسقة مع المتطلبات الداخلية. على سبيل المثال، العمليات الحسابية يجب أن تكون دقيقة. جميع الأرقام في عمود الودائع في حساب الشركة المصرفي يجب أن تساوي إجمالي المبالغ المحفوظة لهذه العمود من الودائع. ثانيا، أيضاً يجب أن تكون البيانات متسقة مع المتطلبات الخارجية. فمجموع المبالغ الذي يمثل الودائع يجب أن يتطابق مع ما أودعفعلياً في الحساب المصرفي. كما يجب أن تكون البيانات متاحة في الوقت المناسب وكاملة. إذا كانت البيانات تعطي مؤشر متأخر يومٌ أو أسبوعٌ، فإن سلامتها يكون موضع تساؤل. وبالمثل إن لم يتم تسجيل جميع البيانات فإن سلامتها أمر مشكوك فيه.

تتحقق من سلامة البيانات عن طريق منع التغييرات غير المصرح بها أو غير الملائمة في البيانات، وضمان الاتساق داخلياً وخارجيا، والتأكد من أن سمات البيانات الأخرى (مثل التوقيت واكتمالها) تتسق مع المتطلبات.

يمكن استخدام السلامة في إشارة إلى حسن سير عمل الشبكة أو النظام أو البرامج التطبيقية. على سبيل المثال، عند استخدام مصطلح السلامة في إشارة إلى نظام فهذا يعني أن النظام يعمل وفقا للتصميم، والمواصفات، والتوقعات حتى في ظل الظروف الحرجة مثل هجوم أو كارثة. تبقى سلامة النظام عالية حتى في ظل الضغوط.

المساءلة

وهذا يشير إلى القدرة على تتبع أو تدقيق النشاط الذي يقوم به فرد أو كيان في الشبكة أو النظام. هل يقوم النظام بعمل سجل الكتروني يحتوي على الأعمال التي أنجزت والملفات التي تم استخدامها، والمعلومات التي جرت عليها عمليات تغيير؟

عدم الإنكار (التثبت)

القدرة على منع الأفراد أو الكيانات من إناكر أن المعلومات، أو البيانات أو الملفات تم ارسالها أو استلامها أو تم استخدام هذه المعلومات أو الملفات أو تغييرها، عندما يكونوا في الواقع قد قاموا بذلك. هذه الإمكانية ذات أهمية عالية للتجارة الإلكترونية. وبدونها يمكن الفرد أو الكيان أن ينكر أنه أو انها مسؤول عن صفقة مالية وبالتالي أنه، هي، أو هو ليس مسؤول ماليا عن ذلك.

المفاهيم والمصطلحات التي تم استعراضها في هذا الفصل سوف تظهر في فصول لاحقة، وقد يجد القراء من المفيد الرجوع إليها. سنبحث كيف نفذت هذه المفاهيم من التطبيقات في الواقع. والتطورات الأخيرة مثل مفتاح التشفير العام والتوقيع الرقمي وأهميتها لتحقيق السرية، السلامة، والتصديق، وعدم الانكار "الإثبات"، وإلى درجة ما التوافر. ونحن نمضي قدما سنرى كيف تم استخدام التشفير التطبيقي لمعالجة العديد من هذه المفاهيم. وسوف نتعرض أيضاً لمحدودية التكنولوجيا في توفير الأمن.

الفصل 2: التهديدات ونقاط الضعف، والهجمات

قبل أن نبدأ مناقشتنا للتهديدات، ونقاط الضعف، والهجمات، من المهم مراجعة أساسيات برتوكول تي سي بي / أي بي (TCP / IP) و نموزج أو أس أي (OSI) ذي السبعة طبقات. هذا الاستعراض مهم لأن الكثير الهجمات التي تحدث اليوم تستغل بعض نقاط الضعف الكامنة في تصميم في بروتوكولات تي سي بي / أي بي (TCP / IP) . في الواقع الهجمات تستخدام وظائف تي سي بي / أي بي (TCP/IP) لاختراق البروتوكول.

بروتوكولات

البروتوكولات ليست أكثر من مجموعة من القواعد أو المعايير الرسمية التي تستخدم كأساس للاتصالات. تم تصميم البروتوكولات لتسهيل الاتصالات. سوف نستخدم ضابط البروتوكول في سفارة كمثال لتوضيح كيفية عمل البروتوكولات. وظيفة ضابط البروتوكول هو ضمان التواصل السليم بين السفارة والبلد المضيف. وظيفة بروتوكول الشبكة مشابه لذلك غير أنها تعمل لضمان الاتصالات بين أجهزة الشبكة. قبل أن تقوم أجهزة بعملية تبادل البيانات، من الضروري للأجهزة الاتفاق على القواعد (بروتوكول) التي ستحكم فترة الاتصال.

نموذج أو أس أي (OSI) المرجعي

نموذج أو أس أي (OSI) المرجعي هو نموذج ذي سبعة طبقات تم تطويره من قبل الهيئة الدولية للمواصفات والمقاييس (ISO) في عام 1978. نموذج أو أس أي هو إطار للمعايير الدولية التي يمكن استخدامها لتنفيذ بنية شبكة حاسوب متجانسة. يقسم نموذج أو أس أي إلى سبع طبقات. الشكل 2.1 يوضح طبقات نموذج أو أس أي (OSI). كل طبقة تستخدم الطبقة التي تحتها مباشرة وتقدم خدمة للطبقة التي أعلاها. في بعض التطبيقات قد تكون هي نفسها مكونة من طبقات فرعية.

7- طبقة البرامج (التطبيقات)	
6- طبقة التقديم	
5- طبقة الجلسة	
4- طبقة النقل	
3- طبقة الشبكة	
4- طبقة ربط البيانات	
5- الطبقة المادية	

الشكل :2.1 نموذج أو أس أي (OSI)

الطبقة المادية تقوم بالارتباط الفعلي وتختص بإشارة الجهد، ومعدل البت، ومدتها. تهتم طبقة وصلة البيانات بتأمين انتقال البيانات بطريقة يعتمد عليها خلال رابط مادي. وبعبارة أخرى، توصيل الإشارة من احد أطراف السلك إلى الطرف الآخر. وتتولى التحكم في التدفق وتصحيح الخطأ. طبقة الشبكة تتولي توجيه البيانات وتضمن أن البيانات قد وجهت إلى الوجهة الصحيحة. توفر طبقة النقل التحكم من البداية وإلى نهاية وتبني الحزم التي يتم وضعها البيانات فيها لاجل نقلها عبر الدائرة المنطقية. طبقة الجلسة تقوم بتهيئة جلسة الاتصال مع وصلة شبكة أخرى. وهي تتولى عملية الاتصال الأولية وتفاوض بشأن تدفق المعلومات وإنهاء الاتصالات بين الشبكتين. طبقة العرض تتولى تحويل البيانات من طبقة الجلسة، حيث تقدمها لطبقة التطبيقات في هيئة مفهومة. طبقة التطبيقات هي واجهة المستخدم النهائية. وتشمل واجهات مثل المتصفحات، والمحطات الافتراضية، وبرامج اف تي بي (FTP).

مجموعة بروتوكول تي سي بي / أي بي **TCP / IP**

تي سي أي بي (TCP / IP) هي مجموعة من البروتوكولات يمكن استخدامها لربط الأنواع المختلفة لأجهزة الحاسوب وأجهزة الشبكات. أكبر شبكة لبرتكول تي سي بي/ أي بي (TCP / IP) هي الإنترنت. وقد تم تطوير الإنترنت من قبل وزارة الدفاع الامريكية تحت رعاية وكالة مشروع أبحاث الدفاع المتقدمة (DARPA) عندما واجهت علماء وزارة الدفاع مشكلة ربط آلاف أجهزة الحاسوب التي تعمل بأنظمة تشغيل مختلفة. وكالة مشروع أبحاث الدفاع المتقدمة (DARPA) هو منشأة صغيرة داخل البنتاغون، ولكن تأثيرها على التكنولوجيا عامة وفي اتصالات البيانات على وجه الخصوص ضخما. لجميع الأغراض العملية برامج وتمويل وكالة مشروع بحوث الدفاع المتقدمة أوجدت الإنترنت. يمكنك التفكير في مجموعة تي سي بي/ أي بي (TCP / IP) كشريان الحياة بالنسبة للإنترنت. وقد تم تبني مجموعة بروتكول تي سي بي/ أي بي (TCP / IP) على نطاق واسع، لأنه معيار بروتوكول مفتوح يمكن تنفيذه على أي منصة بغض النظر عن

الشركة المصنعة. بالإضافة إلى ذلك فهو مستقل عن أي أجهزة شبكة مادية. يمكن تنفيذ تي سي بي/ أي بي (TCP / IP) على إيثرنت، X.25، ونظام توكن رينج (Token ring) من ضمن المنصات الاخرى.

ورغم أن هناك تفسيرات مختلفة حول كيفية وصف برتكول تي سي بي / أي بي (TCP / IP) ضمن نموذج يحتوي على طبقات، عموما يوصف على أنه يتألف من أقل من السبعة طبقات المستخدمة في نموذج OSI. مجموعة بروتوكولات تي سي بي / أي بي (TCP / IP) عادة يتبع بنية ذات أربع طبقات.

جزء برتكول تي سي بي / أي بي (TCP / IP) أي بي (IP) هو طبقة الشبكة التي تعمل بدون إتصال. ويطلق عليه أحيانا البروتوكول غير الموثوق به، يعني هذا أن أي بي (IP) لا يقوم بتأسيس اتصال قبل نقل مخططات البيانات وأنه لا يحتوي على مكتشاف للأخطاء ولا رمز للاسترداد. مخطط البيانات هو هيئة حزمة البيانات التي يحددها ال أي بي (IP) . يعمل ال أي بي (IP) خلال الشبكة وطبقات وصلة البيانات من نموذج OSI ويعتمد على بروتوكول تي يس بي (TCP) لضمان أن البيانات تصل الى وجهتها بشكل صحيح.

لب الجزء أي بي (IP) من بروتوكول تي سي بي / أي بي (TCP / IP) هو مفهوم يسمى عنوان إنترنت. وهذا عبارة عن عدد من 32 بت يمنح لكل طرف في الشبكة. تتم كتابة عناوين أي بي (IP) على النظام العددي العشري علي هيئة أو نسق منقط، يتسق مع النظام العددي الثنائي المكون من 32 بت. يتم تعيين كل ثمانية أعدد بين 0 و 255. مثال على عنوان IP على النظام العشري المنقط هو 12.31.80.1 ، يترجم عنوان أي بي (IP) هذا الى رقم ثنائي في هيئة 32 بت كالتالي:

00000001 01010000 00011111 00001100

وينقسم عنوان ال أي بي (IP) إلى قسمين، معرف الشبكة ومعرف الجهاز المضيف، ولكن هيئة هذه الأجزاء تعتمد على فئة العنوان. هناك ثلاث فئات رئيسية لعنوان الأي بي: الفئة أ (A)، الفئة ب (B) والفئة ج (C). تختلف هيئتها في عدد البتات المخصصة لمعرف الشبكة ومعرف الجهاز المضيف ويمكن تمييزها عن طريق البتات الثلاثة الأولى من العنوان المكون من 32 بت..

الجزء تي يس بي (TCP) من بروتكول تي يس بي / أي بي (TCP / IP) يبدأ العمل حالما يتم تسليم حزمة البيانات إلى عنوان إنترنت صحيح. على النقيض من الجزء أي بي (IP) البروتوكول الذي يعمل بدون اتصال فإن ال تي سي بي (TCP) يعمل على أساس الاتصال. فهو يقوم لعمل اتصال منطقي كامل بين طرفي التواصل أو الأجهزة. يعمل تي سي بي (TCP) في طبقة النقل من نموذج أو أس أي (OSI)، ويقوم بتوفر دارة إفتراضية بين تطبيقات المستخدم النهائي، مع نقل البيانات بطريقة موثوق بها، الشيء الذ يفتقر اليه نموذج مخطط البيانات أي بي (IP).

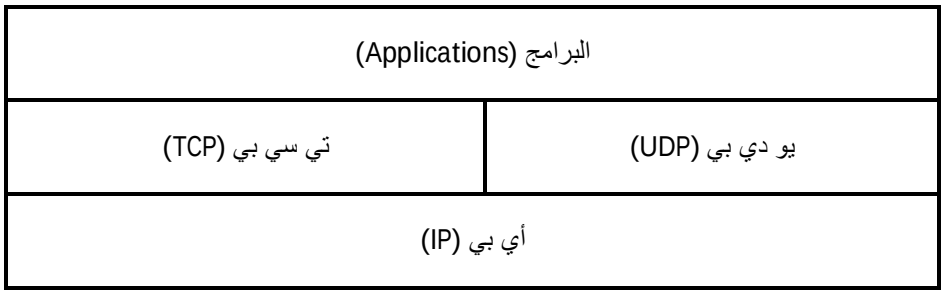
حزم البرامج التي تتبع معيار تي سي بي (TCP) التي توجد في كل جهاز تأسس اتصال مع بعضها البعض، وتقوم بإدارة تبادل الاتصالات. يوفر تي سي بي (TCP) التحكم في التدفق، اكتشاف الخطأ، وتسلسل البيانات؛ يبحث عن الاستجابات؛ ويتخذ الإجراء اللازم ليحل كتل البيانات المفقودة.

يتم تأسيس الاتصال الكامل من خلال تبادل معلومات التحكم. يسمى تبادل المعلومات هذا المصافحة الثلاثية. هذه المصافحة ضرورية لتأسيس اتصال منطقي والسماح ببدء نقل البيانات.

في أبسط أشكالها، فإن الجهاز المضيف أ يرسل إلى الجهاز المضيف ب رقم تسلسل متزامن في شكل مجموعة بت. هذا يخبر الجهاز المضيف ب أن الجهاز المضيف أ يرغب في تأسيس اتصال معه ويبلغه أيضاً ببداية الرقم التسلسلي للمضيف أ. الجهاز المضيف ب يرسل إلى للجهاز المضيف أ إفادة بالعلم ويؤكد الرقم التسلسلي . الجهاز المضيف أ يؤكد استلام إفادة المضيف ب ويبدأ نقل البيانات. لاحقً ، في هذا الفصل سوف أشرح كيف يمكن أستغلال طريقة المصافحة الثلاثية لتعطيل تشغيل نظام.

بروتوكول تي سي بي / أي بي (TCP / IP) آخر مهم هو بروتوكول مخطط بيانات المستخدم يو دي بي (UDP). مثل بروتوكول تي سي بي (TCP) يعمل برتوكول يو دي بي (UDP) في طبقة النقل. والفرق الرئيسي بين تي سي بي (TCP) و يو دي بي (UDP) هو أن يو دي بي (UDP) بروتوكول مخطط بيانات يعمل بدون تأسيس اتصال. يو دي بي (UDP) يتيح للتطبيقات الوصول المباشر إلى مخطط

البيانات وهي خدمة شبيهة بالتي يتيحها أي بي (IP). هذا يسمح للتطبيقات بتبادل البيانات باستخدام الحد الأدنى من البروتوكول. الشكل 2.2 يوضح العلاقة بين أي بي (IP) و تي سي بي/يو دي بي (TCP / UDP) والتطبيقات التي تعتمد على هذا البروتوكولات.



الشكل 2.2: نموذج تي سي بي / أي بي (TCP / IP).

بروتوكول يو دي بي (UDP) هو الأنسب للتطبيقات التي تنقل كميات صغيرة من البيانات، حيث قد تكون عملية إنشاء وصلات وضمان تسليم البيانات أكبر من عملية إعادة إرسال البيانات. حالة أخرى يكون فيها يو دي بي (UDP) مناسبا أيضاً هي عندما تكون للتطبيق منهجية خاصة للتحقق من الخطأ وضمان التسليم.

الفصل الثاني

التهديدات ونقاط الضعف، والهجمات

مقدمة

الآن بعد أن استعرضنا بعض أساسيات تي سي بي / أي بي (TCP / IP) يمكننا المضي قدما في مناقشتنا للتهديدات ونقاط الضعف والهجمات. من المهم أن نفهم الفرق بين التهديد، نقاط الضعف، أو هجوم في سياق أمن الشبكة.

التهديدات

التهديد أي شيء يمكن أن يعطل العمل، الوظائف، سلامة المعلومات، أو توافر الشبكة أو النظام. و يمكن لهذا أن يأخذ أي شكل ويمكن أن يكون فعل متعمد ، عرضي، أو ببساطة فعل الطبيعة.

نقاط الضعف (الثغرات)

الثغرة (نقطة الضعف) هو الضعف المتأصل في التصميم أوالتكوين أوالتنفيذ، أو إدارة الشبكة أو النظام الذي يجعلهما عرضة للتهديد. نقاط الضعف هو كل ما يجعل الشبكات عرضة لفقدان المعلومات والتوقف. كل شبكة وكل نظام به نقاط ضعف من نوعا ما.

الهجمات

الهجوم هو تقنية معينة تستخدم لاستغلال الثغرات. على سبيل المثال، يمكن أن يكون التهديدا الحرمان من الخدمة. على سبيل المثال لثغرة في تصميم نظام التشغيل، الهجوم يمكن أن يكون من نوع "الاتصال القاتل". هناك فئتين عامتين من الهجمات، السلبية والنشطة. الهجمات السلبية من الصعب جدا اكتشافها، لأنه لا يوجد نشاط واضح تمكن مراقبتة أو الكشف عنه. من أمثلة الهجمات السلبية تحسس حزمة البيانات أو تحليل البيانات عبر شبكة. لقد صممت هذه الأنواع من الهجمات لمراقبة حركة المرور البيانات في الشبكة وتسجيلها. وعادة ما تستخدم لجمع المعلومات التي يمكن استخدامها في وقت لاحق في هجمات نشطة.

الهجمات النشطة، كما يوحي الاسم، تستخدم عمليات أكثر وضوحاً في الشبكة أو النظام. نتيجة لذلك فإنه من السهل اكتشافها، ولكن في الوقت نفسه أنها يمكن أن تكون أكثر تدميرا للشبكة. ومن أمثلة هذا النوع من الهجوم أن يكون هجوم الحرمان من الخدمة أو نشاط التحقق من الأنظمة والشبكات.

الشبكات والأنظمة تواجه العديد من أنواع التهديدات. فهناك الفيروسات، والديدان، وأحصنة طروادة، فخ الأبواب، الاحتيال، والتنكر، الاعادة، كسر كلمة المرور ، الهندسة الاجتماعية، المسح ، الترصد، اتصال الحرب، و هجمات الحرمان من الخدمة ، والهجمات الأخرى على البروتوكول. ويبدو أنه يتم تطوير أنواع جديدة من التهديدات كل شهر. يتم في الأقسام التالية مراجعة أنواع التهديدات العامة التي تواجه مسؤولي الشبكة كل يوم، بما في ذلك وصف محدد لعدد قليل من الهجمات المعروفة على نطاق واسع.

الفيروسات

وفقا لاقتصاديات الحاسوبالألكترونية (http://www.computereconomics.com)، مجموعة متخصصة في تحليل وأبحاث الحاسوب، أكثر من 12 مليار دولار أنفقت على مستوى العالم في عام 1999 نتيجة لفيروسات الحاسوب. الفيروس برنامج طفيلي لا يمكن أن يعمل بشكل مستقل، هو برنامج أو جزء من تعليمات برمجية تتمتع بخاصية الانتشار الذاتي. ويطلق عليه فيروس، لأنه مثل نظيره البيولوجي، يحتاج الى مضيف لكي يعمل. في حالة فيروس الحاسوب المضيف هو بعض البرامج الأخرى التي يثبت الفيروس نفسه فيها. عادة ما ينتشر فيروس عن طريق تنفيذ برنامج مصاب أو عن طريق إرسال ملف مصاب إلى شخص آخر، وعادة ما يكون في شكل مرفق بريد الإلكتروني.

هناك العديد من برامج مكافحة الفيروسات المتاحة في السوق. أكثرها فعال ضد الفيروسات المعروفة. لسوء الحظ مع ذلك إنها غير قادرة على التعرف والتكيف مع الفيروسات الجديدة.

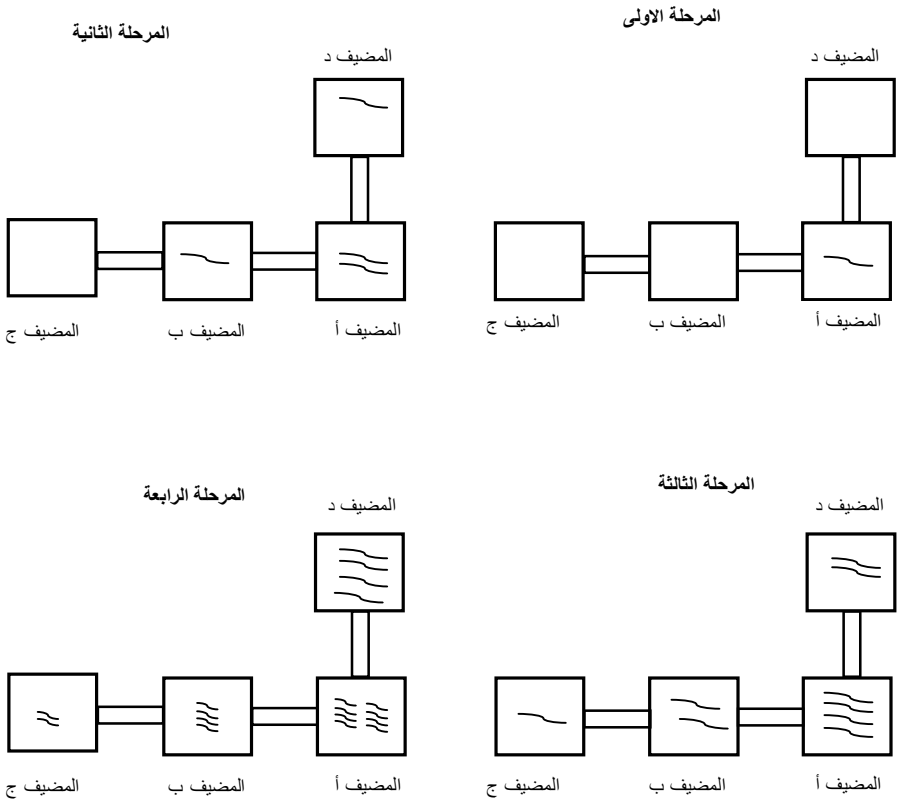
وبصفة عامة، برامج مكافحة الفيروسات تعتمد على التعرف على توقيع الفيروسات المعروفة. ترجع إلى قاعدة بيانات من تواقيع الفيروسات المعروفة التي تستخدمها لمقارنتها مع نتائج البحث عن الفيروسات، يتم الكشف عن فيروس عندما يتم العثور على تطابق في قاعدة البيانات. إذا لم يتم تحديث قاعدة البيانات بانتظام فإن برنامج مكافحة الفيروساتيصبح منتهي الصلاحية سريعاً . كما هو متوقع، عادة ما يكون هناك بعض الوقت الضائع بين ظهور فيروس جديد وتحديث الشركات لقاعدة بيانات الفيروسات الخاصة ببرامجها. دائما، دائما هناك شخص ما مشكوك في كونه واحد من أوائل ضحايا فيروس صدر حديثا.

الدودة

الدودة هو برنامج قائم بذاته ومستقل وعادة ما يكون مصمم لينتشر أو يفرخ نفسه على الأنظمة المصابة والسعي إلى أنظمة أخرى عبر الشبكات المتاحة. الفرق الرئيسي بين الفيروس والدودة هو أن الفيروس برنامج غير مستقل.

عموماً ، هنالك سلالات جديدة من حشرات الحاسوب التي تم فيها طمس الفرق بين الفيروسات والديدان. مثال على هذا الهجين الجديد فيروس ميليسا. في عام 1999 هاجم فيروس مليسيا العديد من مستخدمي منتجات ميكروسوفت. وقد انتشر في البدء كمرفق، ولكن الفيروس واصل الانتشار كعملية نشطة بدأها الفيروس بنفسه. ولم يكن فيروس سلبي مر على مستخدمين مطمئنين.

واحدة من الديدان الأولى وربما الأكثر شهرة دودة الإنترنت التي صممت و أطلقت بواسطة روبرت موريس. في عام 1986، كتب موريس برنامج دودة وأطلقه في الانترنت. كانت عمليات الدودة حميدة نسبيا، ولكنها لا زال لها تأثير مدمر على الإنترنت. وقد تم تصميم الدودة لتعيد نسخ نفسها وتصيب الأنظمة الأخرى. حالما أطلق البرنامج يقوم بتفريخ أو اجراء عملية أخرى. وببساطة العملية الأخرى هي عمل وتشغيل نسخة أخرى من البرنامج. ثم يقوم البرنامج بالبحث عن أنظمة أخرى متصلة بالنظام المصاب وينشر نفسه على الأنظمة الأخرى في الشبكة. وينمو عدد العمليات الجارية هندسيا (عدد الديدان) . يوضح الشكل 2.3 كيف تنمو دودة الإنترنت و تنتشر: عملية واحدة تتوالد لتصبح عمليتين. عمليتين تتوالد لتصبح أربع عمليات. أربع عمليات تتوالد لتصبح ثمانية. لن يستغرق وقتا طويلا جدا للعمليات المتوالدة حتى تستهلك كل وحدة المعالجة المركزية وموارد الذاكرة ثم يتعطل النظام. وبالإضافة إلى ذلك، في كل مرة تتوالد العمليات مرة اخري، فإن العمليات (الدودة) تبحث عن وصلة خارج الشبكة. وقد تم تصميم الدودة لتنتشر، تبحث عن أنظمة أخرى لتصيبها، ثم تكرر العملية.



الشكل 2.3: دودة الإنترنت.

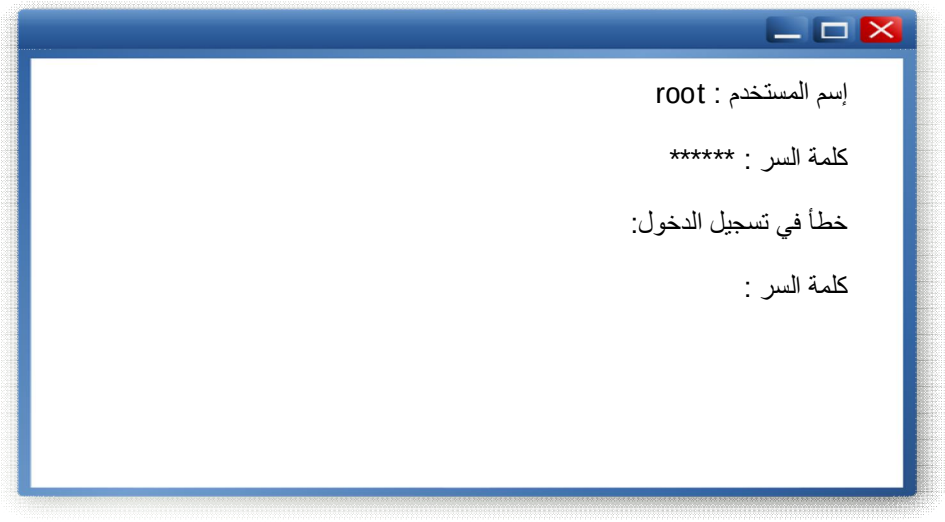
وقف العمليات من التكاثر كان مسألة بسيطة وهي إعادة تشغيل النظام. ومع ذلك، وجد مسؤولي النظام يمكنهم جعل اجهزتهم تعمل بصورة طبيعية عن طريق إعادة تشغيلها ، ألا أنها تصاب بالعدوي مرة اخري من قبل جهاز أخر مصاب في الإنترنت. ولوقف الدودة من إصابة الأنظمة على الشبكة كان لا بد من اغلاق جميع الأجهزة في الوقت نفسه أو فصلها عن الشبكة . وقدرت تكلفة تنظيف دودة الإنترنت بعشرات الملايين من الدولارات. اعتقل موريس وقدم للمحاكمة، وتمت ادانته على الأعمال التخريبية التي قام بها.

أحصنة طروادة

حصان طروادة برنامج أو جزء شفرة برنامج يخفي داخل البرنامج وينفذ وظيفته في تخفي. هذا النوع من التهديد حصل على اسمه من الأساطير اليونانية وقصة حصار طروادة. تحكي القصة كيف غزى أوديسيوس ورجاله طروادة عن طريق الإختفاء داخل حصان خشبي عملاق. يخفي برنامج حصان طروادة نفسه داخل برنامج آخر أو يتخفي في هيئة برنامج شرعي. ويتم ذلك عن طريق تعديل البرنامج الحالي أو ببساطة عن طريق استبدال البرنامج القائم بواحد أخر جديد. يعمل حصان طروادة بنفس الطريقة التي يعمل بها البرنامج الحالي المشروع، ولكن عادة ما يؤدي الوظائف الأخرىأيضاً ، مثل تسجيل المعلومات الحساسة أو نصب فخ.

مثال لذلك برنامج سرقة كلمة السر. برنامج سرقة كلمة السر هو برنامج صمم ليظهر كأنه واجهة المستخدم الطبيعية لادخال كملة السر التي تظهر للمستخدم عند بدء النظام .

مثال لذلك في الشاشة المبينة أدناه في الشكل 2.4، أدخل المستخدم إسم المستخدم جون وكلمة المرور الصحيحة. ومع ذلك النظام أخبر المستخدم أن معلومات الدخول غير صحيحة. عندما حاول المستخدم مرة أخرى اشتغلت كلمة السر واستطاع هو/هي تسجيل الدخول للنظام .



الشكل 2.4: تسجيل الدخول عن طريق حصان طروادة.

حقيقة في هذا المثال حصان طروادة مصمم لسرقة كلمات السر سيطر على العمليات. تم استبدال برنامج الدخول التنفيذي (Login.exe) ببرنامج حصان طروادة. يبدو مثل شاشة تسجيل الدخول الأساسية، ولكن ما حدث في الواقع هو أن شاشة تسجيل الدخول الأولي كانت حصان طروادة وعندما تم إدخال اسم المستخدم وكلمة المرور تم تسجيل المعلومات وتخزينها، ثم عرض برنامج حصان طروادة على رسالة "معلومات الدخول غير صحيحة" ثم وجه بعدها المستخدم إلى برنامج تسجيل الدخول الحقيقي، حتى يمكنه تسجيل الدخول فعليا إلى النظام. ببساطة يفترض المستخدم انه او انها أخطأت في كتابة كلمة السر المرة الأولى ولا يعلمأبداً أن اسم المستخدم وكلمة المرور خاصتها او خاصته للتو قد سرقت.

فخ الأبواب

فخ الباب أو الباب الخلفي هو وسيلة غير موثقة تمكن من الدخول إلى النظام وضعت في النظام من قبل مصممه / مصممته. ويمكن أيضا أن يكون برنامج تم تعديله ليسمح لشخص ما بالحصول على ميزة الدخول إلى نظام أو عملية.

هناك العديد من القصص عن الباعة يستخدمون فخ الأبواب للأستفادة منها في النزاعات مع العملاء. أحد الأمثلة على ذلك قصة الاستشاري الذي تم التعاقد معه لتصميم نظام لشركة، صمم الأستشاري فخ باب في النظام . عندما حصل نزاع بين الاستشاري و الشركة حول الدفع، استخدام الاستشاري فخ الباب للدخول إلى النظام وتعطيله. اضطرت الشركة للدفع للاستشاري من أجل تشغيل النظام مرة أخرى.

قنابل المنطق

القنبلة المنطقية هي برنامج أو جزء من برنامج صمم حسب نوايا سيئة. ويشار إليه بقنبلة المنطق لأنه يتم تشغيل البرنامج عند حدوث بعض الظروف المنطقية. تقريباً هذا النوع من الهجوم يرتكب دائما من الداخل من شخص حاصل على ميزة الدخول إلى الشبكة. الجاني يمكن أن يكون مبرمجا أو بائع يزود بالبرمجيات.

مثال على ذلك، مرة سمعت قصة عن مبرمج في شركة كبيرة يقوم بهندسة هذا النوع من الهجوم. على ما يبدو، أن المبرمج قد واجه بعض المتاعب في الشركة التي كان يعمل وكان تحت الفترة التجريبية. خوفا من انه قد يسرح من الخدمة و بوضع دافع الانتقام في باله، أضاف بريمج إلى برنامج آخر. تمت إضافة بريمج إلى برنامج ينفذ مرة واحدة في الشهر، وكان يهدف إلى تحليل قاعدة بيانات الموارد البشرية للشركة للتأكد ما إذا كان قد تم تسجيل موعد إنهاء خدمة في سجله الوظيفي. إذا وجد البريمج أن تاريخ إنهاء خدمة قد تم تسجيله، بناءاً على تصميمه يقوم بالقضاء على النظام بأكمله عن طريق حذف كافة الملفات على الأقراص. استمر البرنامج في العمل كل الشهر وطالما أن تاريخ انها الخدمة لم يعبأ في سجل هذا المبرمج فإن شيئا لن يحدث. وبعبارة أخرى، إذا لم يتم انها خدمته فإن البرنامج لن يسبب أي ضرر.

بما لا يدع مجالاً للشك إن هذا الموظف المتميز تم الإستغناء عن خدماته، و في المرة القادمة قنبلة المنطق التي صممها اشتغلت ووجدت تاريخ إنهاء الخدمة في سجل الموظف محدث وقضت على النظام. هذا مثال يوضح كيف انه من السهولة لموظف حاصل على ميزة استخدام النظام يمكنه القيام بهذا النوع الهجوم.

مسح المنافذ

مثل لص يترصد هدفا يخطط لكسره (سرقته) غالبا ما يترصد القرصان حالة نظام ما لجمع معلومات يمكن أن يستخدمها لاحقا في مهاجمة النظام. احدى الأدوات التي غالباً ما يستخدمها القراصنة لهذا النوع من الاستطلاع هو ماسح المنافذ. برنامج ماسح المنافذ هو برنامج يتصنت على منافذ ذات أرقام معروفة للكشف عن الخدمات تعملحالياً في النظام والتي يمكن استغلالها لاقتحام النظام.

هناك العديد من برامج مسح المنافذ متاحة على شبكة الإنترنت في مواقع مختلفة، والحصول عليها يسير. ويمكن للمنشأت مراقبة ملفات سجل النظام من أجل كشف مسح المنافذ كمؤشر تمهيد لهجوم. معظم برمجيات كشف التسلل تعمل على مراقبة مسح المنافذ. إذا اكتشفت أن منافذ النظام الخاص بك تم مسحها يمكنك تتبع المسح إلى نقطة نشأته وربما اتخاذ بعض الإجراءات الاستباقية. ومع ذلك، بعض برامج مسح المنافذ تأخذ نهجاً أكثر في التخفي للمسح لذلك من الصعب جدا كشفها. على سبيل المثال، بعض البرامج تستخدم مسح (تزامن) SYN، التي توظف حزمة SYN لإنشاء اتصال نصف مفتوحة حتي لا يحصل تسجيل لنشاط المسح. سيتم شرح حزم SYN والوصلات نصف مفتوحة لاحقا في هذا الفصل بالتفصيل.

الانتحال (التحايل)

الانتحال او التحايل يغطي أنواع واسعة من التهديدات. وبصورة عامة، الانتحال يستلزم تزوير هوية فرد أو التنكر في هيئة فرد أو كيان آخر من اجل الدخول في نظام أو الشبكة للحصول على معلومات من أجل بعض الأهداف غير المصرح بها. هناك العديد من أنواع الانتحال المختلفة، وذلك ضمن أشياء أخرى كثيرة، خداع عنوان الانترنت (IP)، إختطاف جلسة الاتصال، محاكاة خدمة اسم النطاق (DNS) ، محاكاة تسلسل الأرقام، وهجمات الاعادة.

محاكاة عنوان الانترنت (IP)

لكل جهاز في شبكة ال تي سي بي/ أي بي (TCP / IP) عنوان انترنت فريد من نوعه (IP). عنوان الانترنت (IP) هو عنوان فريد من نوعه للتعرف على الجهاز، ولا يمكن أن يكون لجهازين في الشبكة نفس العنوان (IP). يتم تنسيق عناوين الانترنت (IP) علي هيئة أربعة أرقام عشرية مفصولة بنقاط (على سبيل المثال، 147.34.28.103).

انتحال عنوان الانترنت (IP) يستفيد من الأنظمة والشبكات التي تعتمد على عنوان الانترنت (IP) لربط الأنظمة أو الأجهزة في المصادقة. على سبيل المثال، أجهزة التوجيه الخاصة بتصفية الحزم تستخدم أحيانا لحماية الشبكة الداخلية من الشبكات الخارجية الغير موثوق بها. هذه الموجهات تسمح فقط لعناوين انترنت (IP) محددة لتمر من الشبكة الخارجية إلى الشبكة الداخلية. إذا استطاع القراصان تحديد عنوان انترنت (IP) مسموح له بالعبور من خلال جهاز التوجيه، فانه يقدرعلى انتحال عنوان انترنت الشبكة الخارجية للوصول إلى الشبكة الداخلية. في الواقع استطاع الهاكر من تقمص شخصية شخص آخر.

انتحال الأرقام التسلسلية (تحايل)

الشبكات تي سي بي/أي بي (TCP / IP) تستخدم أرقام متسلسلة. الأرقام المتسلسلة جزء من كل عملية نقل ويتم تبادلها مع كل معاملة. ويستند رقم التسلسل على الساعة الداخلية لكل كمبيوتر، يمكن التنبوء بالعدد لأنه يقوم على مجموعة من الخوارزمية.

من خلال رصد اتصال الشبكة، يمكن للقراصان تسجيل الأرقام التسلسلية المتبادلة وتوقع المجموعة التالية من الأرقام المتسلسلة. مع هذه المعلومات، يمكن للقراصان من ادخال نفسه أو نفسها في اتصال الشبكة و على نحو فعال يمكنه التحكم بالشبكة أو إدراج معلومات خاطئة.

خير وسيلة للدفاع ضد انتحال أرقام التسلسل بالتحايل هو تشفير الاتصال. تشفير الاتصال يمنع أي شخص قد يكون مراقب للشبكة من التعرف على تسلسل الأرقام أو أية معلومات مفيدة أخرى.

قرصنة جلسة الاتصال

خطف جلسة الاتصال مشابه لانتحال على أرقام التسلسل. في هذه العملية، يستولي القرصان على جلسة اتصال، عادة ما تكون بين مستخدم وخادم ملفات . وغالباً ما يتم هذا عن طريق الوصول إلى جهاز توجيه أو بعض أجهزة الشبكة الآخر التي تعمل كبوابة بين المستخدم الشرعي وخادم ملفات عن طريق احتيال عنوان الانترنت (IP). بما أن قرصنة الجلسة عادة ما يتطلب من القرصان الحصول على امتياز الدخول إلى جهاز في الشبكة، أفضل وسيلة دفاع يمكن اتخاذها هي تأمين جميع الأجهزة في الشبكة بشكل جيد.

DNS

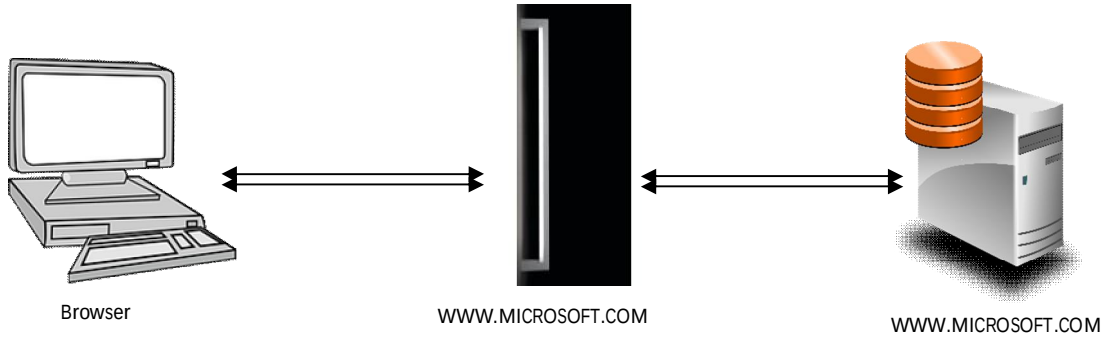
خدمة اسم النطاق (DNS) هي خدمة اسم هرمية تستخدم مع مضيفي برتكول تي سي بي/أي بي (TCP / IP) ويتم توزيعها وتكرارها على الخوادم عبر الإنترنت. ويستخدام في شبكة الإنترنت وعلى الشبكات الداخلية (Intranet) لترجمة عناوين الانترنت (IP) إلى أسماء مضيفين. يمكن استخدام أسماء المضيف في عناوين المواقع (URL) . يمكن التفكير في اسم النطاق (DNS) كجدول بحث يسمح للمستخدمين بتحديد أجهزة الحاسوب النائية بواسطة أسماء المضيفين بدلا عن عناوين الانترنت (IP) . ميزة اسم النطاق (DNS) هي أنه ليس من الضروري أن تكون لديك معرفة بعناوين الانترنت (IP) لجميع مواقع الإنترنت للوصول اليها. يمكن تهيئة اسم النطاق (DNS) لاستخدام سلسلة من أسماء الخوادم ، استنادا إلى النطاقات في الاسم المنشود، حتى يتم العثور على اسم مطابق. برنامج خادم اسم النطاق

(DNS) الشائع الاستخدام في شبكة الإنترنت هو (BIND DNS) و يخضع لعدة عمليات احتيال، اثنين شائعة الاستخدام من هذه العمليات الرجل في منتصف (MIM) و تسميم اسم النطاق (DNS). إعادة التحويل هجوم آخر أقل شيوعا، يعتمد على التلاعب في سجل اسم النطاق لتسجيل نفسه من أجل إعادة توجيه وصلة الانترنت URL.

رجل في المنتصف (MIM)

في هجوم الرجل في المنتصف (MIM) يضع القرصان نفسه أو نفسها بين برنامج عميل وخادم على شبكة. وبذلك يمكن للقرصان اعتراض المعلومات التي تم إدخالها من قبل العميل، مثل أرقام بطاقات الائتمان وكلمات السر ومعلومات الحسابات. عند تنفيذ مخطط واحد من هذه فإن القرصان يضع نفسه أو نفسها بين متصفح وخادم انترنت. وعادة ما يتم هجوم رجل في المنتصف (MIM) والذي يسمى أحيانا بالتحايل على الانترنت من خلال اسم نطاق (DNS) أو بالتحايل على الارتباط التشعبي.

هنالك عدة طرق يمكن للقرصان أن يشن هجوم رجل في الوسط (MIM) من خلالها . أحدى هذه الطريق تسجيل عنوان انترنت (URL) مشابهة جدا لعنوان انترنت (URL) موجودة . على سبيل المثال يمكن أن يسجل القرصان عنوان انترنت (URL) مثل www.microsoft.com. عندما يقوم شخص ما يرغب في استخدام موقع ميكروسوفت في الشبكة العنكبوتية ويطبع بالخطأ www.microsoft.com فسوف يتم تحويله إلى موقع على شبكة الإنترنت تم تصميمه بواسطة قرصان ليبدو وكأنه موقع ميكروسوفت في الشبكة العنكبوتية. يوضح الشكل 2.5 كيف تعمل هذه العملية.



الشكل 2.5: هجوم رجل في المنتصف (MIM).

لمتصفحي الانترنت يبدو كل شيء طبيعياً ، فيتفاعلون مع الموقع المزيف تماما كما يفعلون مع الموقع الحقيقي. عندما يدخل الشخص المتصفح بعض المعلومات والخيارات قد يقوم موقع القرصان بتمرير هذه المعلومات للموقع الحقيقي ويعيد الشخص المتصفح للموقع الحقيقي وتظهر له الشاشات الحقيقية للموقع .

تسميم إسم النطاق (DNS)

طريقة أخرى يمكن استخدامها لإطلاق هذا النوع من الهجوم هي استغلال خادم اسم النطاقات (DNS) . احدي الطرق للقيام بذلك يطلق عليها تسميم DNS اسم النطاق. تسميم اسم النطاق (DNS) يستغل ثغرة أمنية في الإصدارات الأولى مما يعرف ب بيركلي إنترنت نيم دامون (BIND). وهو برنامج اسم النطاق الأكثر انتشاراً في الشبكة العنكبوتية ، وقد طور لاستخدام نظام يونكس (BSD UNIX). تقوم شبكة خوادم BIND للانترنت بترجمة عناوين الانترنت (IP) الأساسية (الأم) إلى أسماء شائعة الاستخدام مثل www.ggu.edu لجامعة جولدن جيت. قبل الإصدار 8.1 من BIND، كان من الممكن أن يتم تسميم مدخلات جدول خادم النطاقات (DNS) بمعلومات خاطئة.

ويمكن أن تشمل هذه المعلومات عنوان انترنت (IP) كاذبة تدخل في جدول الخادم. النتيجة عندما يستخدم شخص ما ذلك الخادم (DNS) للوصول الى عنوان انترنت (URL) يتم توجيهه إلى عنوان انترنت (IP) غير صحيح.

بالتحايل على اسم خادم نطاق (DNS) يمكن أن يصنع القرصان عنوان انترنت (URL) مشروع لموقعه في شبكة الإنترنت. قد يقوم متصف شبكة الانترنت بكتابة www.amazon.com ويتوقع أن يدخل إلى موقع Amazon.com لشراء كتاب. في نظام الانترنت يشار الى العنوان www.amazon.com ب xxx.xxx.xxx.xxx، ولكن القرصان قد قام بالتحايل على خادم النطاقات (DNS) لكي يشير الى الموقع الخاص به أو بها. ونتيجة لذلك يتم توجيه متصفح الانترنت إلى موقع القرصان وليس لموقع Amazon.com.

إعادة التوجيه (Redirects)

تحت طريقة أخرى لهجوم اسم النطاق (DNS)، يقوم القراصنة بخرق وصلة على صفحة شخص آخر أو إنشاء صفحة خاصة بهم مع وصلات كاذبة. في كلتا الحالتين يشير الرابط على أنه موقع شرعي، لكن في واقع الأمر الرابط يجلب متصفح الانترنت إلى موقع تم تصميمه ويتم التحكم فيه بواسطة قرصان و يبدو مثل الموقع الذي يتوقعه الشخص المتصفح.

إذا فشلت كل المحاولات الأخرى، يمكن للقرصان محاولة التلاعب في نظام تسجيل اسم النطاق الذي تم تصميمه بواسطة InterNIC. في عام 1999 على الأقل في ثلاث مناسبات، تمكن القراصنة من نقل أسماء النطاقات أو إعادة توجيه متصفحي الإنترنت إلى مواقع أخرى بدلا عن تلك التي كانوا يحاولون الوصول اليها. في حالة واحدة تم تغيير طريقة دخول لاسم النطاق (DNS) الخاص بشركة حلول الشبكة (Netwrok solutions)، بحيث عندما يدخل المستخدمين في موقع شركة حلول الشبكة تتم إعادة توجيههم إلى موقع آخر.

في ثلاث حالات أخرى على الأقل تمكن القراصنة من نقل ملكية أسماء النطاقات إلى أسماء نطاقات أخرى. حالما ما تم نقل الملكية الملكية وقاعدة البيانات (NSI) ، أي شخص حاول الوصول إلى تلك النطاقات يتم توجيهه إلى مواقع جديدة. في حالة واحدة تم نقل ملكية نطاق موقع excite.com إلى موقع صغير وجد نفسه غمر بملايين من الزيارات التي يتلقاها موقع excite.com بشكل طبيعي. وفي حالات أخرى تم تغيير ملكية نطاق موقع كو كلوكس كلان (Ku Klux Klan) وموقع آخر الى مواقع تختص بالشذوذ الجنسي والكراهية الدينية. وتم نقل ملكية الموقع كو كلوكس كلان إلى موقع مخصص لمحاربة التعصب. ومن المفارقات، تم نقل إسم نطاق الموقع المختص بالشذوذ الجنسي والكراهية الدينية الى موقع ينادي للتسامح ونبذ التعصب (godlovesfags.com). علماً بأنه لا أحد من أفراد المواقع التي أعيد توجيه نطاقها والتلاعب به تورط في هذه العلميات.

عندما استخدام هجوم رجل في الوسط (MIM) في الواقع يمكن أن يمرر موقع القرصان الكاذب أو المزور طلبات العميل الى الموقع الحقيقي، ويظهر للعميل الصفحات المطلوبة من الموقع الحقيقي. في حين أن القرصان يرصد ويسجيل جميع العمليات بين العميل والملقم.

ليس هناك إجراء مضاد فعال لهجوم رجل في الوسط (MIM). يمكن لهذا الهجوم أن يكون ناجحا حتى في ظل استخدام نظام تشفير، مثل (SSL). فإنه فقط يتطلب من القرصان الحصول على شهادة رقمية صالحة لتحميلها على الجهاز الخادم الخاص به أو بها ، بحيث يمكن تفعيل نظام تشفير (SSL) . يحتاج مستخدمي شبكة الانترنت أن يكونوا حذرين حول أين يتصفحون يجب أن يتأكدوا من الروابط التي يزورونها والتنقل فقط في روابط من موقع آمنة وموثوق بها.

يلاحظ أن هناك أساليب أخرى لتنفيذ هجوم إعادة التوجيه أو هجوم رجل في الوسط (MIM). على سبيل المثال، أنظمة التشغيل بعينها مثل برامج مايكروسوفت: النوافذ 95 و 98 و 2000 و سن سولاريس (Sun Solaris) لها نقاط ضعف متأصلة في تصميم بروتوكول رسائل التحكم في الإنترنت (ICMP) و برتكول اكتشاف الموجه (IRDF)؛ بروتوكول رسائل التحكم في الإنترنت (ICMP)هو جزء من حزمة برتوكول تي سي بي/أي بي (TCP / IP). يمكن للقراصنة استغلال هذه الثغرة الأمنية بتحويل مسار حركة البيانات الصادرة أو التعديل عليهما حسب اختيارهم. نقطة ضعف رئيسية في الهجوم باستغلال هذه هي أن المهاجم يجب أن يكون في نفس الشبكة التي يستخدمها النظام المستهدف.

إعادة الهجوم

ينفذ القراصان أعادة الهجوم عن طريق اعتراض وتخزين معلومات مرسلة بصورة شرعية بين نظامين ويقوم بإعادة بثها في وقة لاحق. نظريا، يمكن لهذا الهجوم أن يكونناجحاً حتي في حالة الإرسال المشفر. أفضل دفاع ضد هذا الهجوم هو استخدام مفاتيح الجلسة ، والتحقق من الطابع الزمني على كل المراسلات، وتوظف رسالة تعتمد على الزمن المستغرق . سوف يتم نقاش هذا بمزيد من التفاصيل في الفصلين الثالث والرابع.

كسر كلمة السر

أحياناً يطلق على هجوم كسر كلمة السر الهجوم القائم على قاموس. برامج كسر كلمة السر هي برامج تقوم بفك شفرة ملف كلمات السر. برامج كسر كلمة السر متوفرة لمعظم نظم الشبكات ونظم تشغيل الحاسوب. وهي قادرة على فك تشفير ملفات كلمات المرور عن طريق استخدام نفس الخوارزمية المستخدمة لإنشاء كلمة المرور المشفرة. وبصورة عامة تسختدم قاموس من الكلمات أو العبارات المعروفة، والتي تم تشفيرها أيضا بخوارزمية كلمة المرور. يقوم برنامج كسركلمة السر بمقارنة كل سجل في ملف كلمة المرور مقابل كل سجل في القاموس لإيجاد كلمة مطابقة. و عندما يتم التطابق يكون قد تم العثور على كلمة سر.

يمكن العثور على شفرة المصدر لبرامج كسر كلمة السر لمعظم الحواسيب وأنظمة تشغيل الشبكات (NOSS) بسهولة على شبكة الإنترنت في مواقع مثل http://www.L0pht.com. بعض من البرامج المتاحة على الشبكة تشمل Brute، CrackerJack، John The Ripper و New Hak، . يتناول الفصل السادس كلمات السر وكسر كلمات السر بالتفصيل.

الهندسة الاجتماعية

الهندسة الاجتماعية، والتي تشير إلى الأساليب غير التقنية التي يستخدمها القراصنة من أجل الوصول إلى النظم، يمكن أن تكون فعالة بشكل مثير للدهشة. الهندسة الاجتماعية عادة ما تشير إلى عملية إقناع شخص للكشف عن معلومات (مثل كلمة السر) التي تمكن القرصان من الوصول إلى نظام أو شبكة.

في مثال لسيناريو حقيقي، يتحصل القرصان علي دليل الهاتف الخاص بالشركة ومن ثم يتصل بموظف من غير المتشككين، مدعيا أنه يتصل من إدارة نظم معلومات الشركة. وربما يقوم القرصان باستخدام اسم شخص ما من إدارة نظم المعلومات، وقد يقول ان هناك مشكلة ويطلب من الموظف ادخال سلسلة طويلة من الأوامر الغامضة للتحقق من المشكلة. يدخل الموظف الأوامر، التي لا يبدو أنها تعمل، في حين أن موظف نظم الملعومات المتصل يدعي التواصل على نحو متزايد مع الموظف. الموظف المستهدف يشعر بالضغط عليه نتيجة لفشله / فشلها على ما يبدو في إدخال الأوامر بشكل صحيح، وأخيرا يقول موظف ادارة نظم المعلومات المزيف شيء من هذا القبيل "فقط أعطني كلمة السر الخاصة بك حتى أستطيع التحقق من ذلك بنفسي ونتمكن من حل هذه المشكلة. "وبالتالي يكشف الموظف كلمة السر الخاصة بها أو به للقرصانمعتقداً أن القرصان موظف إدارة نظم في المعلومات الشركة. وبهذه البساطة الأن حصل القرصان على اسم مستخدم وكلمة مرور وإمكانية الوصول إلى نظام الشركة.إنه حقاً مدهش كم مرة سمعتبأن هذا الأسلوب كان ناجحاً .

من المهم أن يكون لكل منشأة سياسة بخصوص الكشف عن كلمات السر. عموما يجب أن تنص السياسة بأنه غير مسموح بكشف كلمات السر لأي أي شخص بما في ذلك موظفي إدارة نظم المعلومات. وينبغي إبلاغ هذه السياسة لجميع موظفي الشركة.

طريقة أخرى تستخدم عادة من قبل القراصنة تعرف بالغوص في القمامة. الغوص في القمامة لا يقع رسميا تحت فئة الهندسة الاجتماعية، لكنه بالتأكيد تقنية غير متقدمة. يعرف الغوص في القمامة بعملية جمع المعلومات عن طريق البحث في القمامة. مطبوعات الحاسوب ذات قيمة مميزة لهجوم الغوص القمامة. يبحث القراصنة على معلومات مثل أسماء حسابات النظام، وشفرة المصدر (وخاصة إذا كانت تحتوي على كلمات سر ضمنية)، أو أرقام حسابات العملاء (للمؤسسات المالية). من المهم أن يكون لدي المنشأة ضوابط مناسبة للتخلص من السجلات والملفات الورقية. يجب تدوين الضوابط في سياسة رسمية.

التحسس

تحسس شبكة الحاسوب أو تحسس حزم البيانات هي عملية رصد الشبكة في محاولة لجمع المعلومات التي قد تكون مفيدة للهجوم. مع الأدوات المناسبة يمكن للقراصان مراقبة حزم بيانات الشبكة للحصول على كلمات السر أو عناوين الانترنت (IP). العديد من البائعين يصنعون الأجهزة والبرمجيات لأغراض مشروعة والتي يمكن أن يساء استخدامها من قبل القراصنة. الحقيقة الوحدية المريحة عن هذه المنتجات هو أن القراصنة لا يستطيعون تحمل نفقات شرائها، ومع ذلك يمكنهم سرقتها. وهناك أيضا بعض الأدوات البرمجية والبرامج العامة متاحة للتنزيل من مواقع القراصنة مثل tcpmon، TCPDUMP، أو gobbler. برنامج Sniffer Pro مثال للمنتجات المتوفرة بصورة تجارية.

يشكل تحسس كلمات السر تهديدا خاصاً للمستخدمين الذين يقومون بتسجيل الدخول إلى أنظمة يونكس عبر شبكhت اتصال. وعادة ما يتم استخدام التلنت (Telnet) أو آر لوق ان (rLogin) عند تسجيل الدخول إلى أنظمة يونكس عبر شبكة حاسوب. تلنت و أر لوقن لا تشفر كلمات السر. ونتيجة لذلك، عندما يدخل المستخدم كلمة السر الخاصة به / بها ، تنتقل في الشبكة بصورة مقروءة، بمعني أن أي شخص مراقب للشبكة يمكنه قراءتها. على النقيض من ذلك، على حد سواء نظام نوفل و نظام النوافذ أن تي يشفران كلمات المرور لارسالها في الشبكة.

هناك العديد من الأدوات المتوفرة للحد من مخاطر تحسس الشبكة. في الفصول 7 و 8 و 11 تتم مناقشة بعض منها، بما في ذلك الصدفة المحمية (SSH) والشبكات الخاصة الإفتراضية (VPN). ومع ذلك، يمكن الحصول على معلومات مفيدة من شبكة حاسوب تم تشفيرها بصورة تمامة. في بعض الأحيان تحليل بسيط لحركة البيانات يمكن من الحصول على معلومات مفيدة. وبالتمكن من التعرف على الأنظمة الأكثر نشاطاً يمكن أن تكون ذات قيمة كبيرة. استخدام محولات الشبكة بدلا من المحاور التقليدية يعتبر طريقة أخرى للحد من خطر رصد الشبكة. الفصل الثامن يناقش هذا الموضوع بمزيد من التفاصيل.

وهناك أيضا أدوات متاحة ترمي إلى الكشف عن راصدي حزم البيانات غير المصرح لهم في الشبكة. مثال لبرنامج واحد مضاد لترصد الشبكات متوفر من شركة L0pht للصناعات الثقيلة على موقعها في الانترنت http://www.10pht.com. بالتحديد هذه المنتجات تكشف خصائص بطاقة واجهة الشبكة (NIC) التي تم تهيئة بشكل مختلط، والتي يمكن أن تستغل في رصد حزم بيانات الشبكة. ومع ذلك، فإن هذه النظم ببساطة يمكن تخطيها عن طريق قطع سلك الإرسال على كابل بطاقة واجهة الشبكة (NIC). وبهذه الطريق لا تستطيع بطاقة واجهة الشبكة (NIC) إرسال الحزم على الشبكة.وبناءاً عليه فإن برامج الكشف عن رصد الشبكة لا تكون قادرة على كشف بطاقة واجهة شبكة (NIC) تم تهيئتها في وضع مشكوك فيه.

تشويه المواقع

لست حقاً متأكدا من أن هذا يستحق أن يصنف في حد ذاته. ومع ذلك، فإنه يحدث كثيراً ، لذلك جدير بالذكر. كل أسبوع يتم تشويه مواقع بعض الشركات من قبل قراصنة الحاسوب الذين ينشرون بعض رسائل الاحتجاج على شيء ما أو غيره. عادة يتم هجوم تشويه المواقع على شبكة الإنترنت من خلال استغلال بعض التهيئات الخاطئة أو نقاط ضعف معروفة تعيب برنامج خادم الشبكة الإنترنت، أو من عن طريق استغلال بعض الضعف القائم على بروتوكول آخر في نظام تشغيل خادم الشبكة.

أفضل وسيلة دفاع تتخذها المنشأة ضد تشويه موقعها هو الحصول على آخر إصدارات برنامج خادم شبكة الانترنت والنسخ المحدثة من نظام تشغيل الخادم. أيضا ينبغي للمنشأة أن تكفل التدريب السليم لمدير النظام لديها بحيث يكون قادرا على تثبيت وصيانة البرامج. وقد اتخذت بعض المنشأت المزيد من الأساليب الإبداعية لضمان سلامة مواقعها على الانترنت عن طريق نشر خوادم شبكات ثانوية تسمي كاش سرفرس "Cash servers" تقوم بتحديث خوادم الإنترنت. تقوم خوادم الكاش سرفرس بعكس موقع معين يحدث ملقم الشبكة بصورة دورية من نسخة النظام الأصلية. إذا تم تشويه الموقع من قبل القراصنة، يقوم خادم الكاش بإعادة النسخة الأصلية بنسخها فوق التعديلها التي فعلها القراصنة وذلك عن طريق تكنلوجيا الدفع "Push".

اتصال الحرب

اتصال الحرب طريقة القوة الغاشمة في العثور على باب خلفي في شبكة المنشأة. هذا النوع من الهجوم فعال ضد الدفاع من المحيط. معظم المنشأت لديها أرقام هاتف ضمن نطاق محدد وتبدأ بنفس البادئة. على سبيل المثال، دعونا نفترض شركة افتراضية تدعى شبكة أكمي. كل هواتف الشركة تبدأ بالأرقام 895. هناك 4000 تحويلة؛ والتحويلة الاولى هي 1000. نطاق هواتف أكمي يبدأ بالرقم 595-1000 وينتهي في 595-5000. اتصال الحرب عادة ما يستخدم نظام الاتصال الآلي (برنامج) ليتصل على كل هاتففي المنشأة بحثاً عن تحويلة تستخدم جهاز مودم.

يسجل البرنامج رقم الهاتف كلما وجد جهاز مودم. لاحقا بعدما يتصل البرنامج على كل تحويلات الشركة، يوم القراصان بمراجعة سجل الاتصالات على أجهزة المودم ومن ثم يقوم بمحاولة اقتحام النظام المتصل بجهاز مودم من أجل الدخول في الشبكة .

هذا الأسلوب دائما ينجح مع المؤسسات الكبيرة. عند التعامل مع شركة فيها عدة آلاف من أرقام الهاتف، يكون الاحتمال الى جانب القرصان بأن بعض منها متصل بأجهزة مودم. لقد عملت لشركة كبيرة استأجرت واحدة من الشركات الاستشارية الكبرى لاختبار أمن الشبكات في الشركة وقد فشلة شركة الاستشارات اختراق جدار الحماية للشركة. ومع ذلك اجرت اتصل حرب تكمنت من خلاله تحديد عدد من أرقام الهواتف المتصلة بأجهزة مودم . أحد أجهزة المودم كان موصلا بجهاز حاسوب شخصي به برنامج بي سي أني وير (PC Anywhere) معد لاستقبال اتصال شخص ما على المكتب من المنزل. وقد تمكنت الشركة الدخول إلى الشبكة من خلال استغلال خلل في نسخة برنامج (PcAnywhere) الاولي يسمح للمستخدم تجاوز كلمة السر. وفي مرة واحدة تمكن الاستشاري من أختراق جميع الأجهزة في الشبكة من غير أن يكتشف أي شخص نشاط غير مشروع. وكان الاستثناء الوحيد المجموعة التي أعمل فيها حيث أكتشفنا نشاط على الأنظمة غير معروق وبالتحري عن مصدر النشاط تم ابلاغنا بأنه اختبار لنظام أمن المعلومات في الشركة.

يمكن الحصول علي شفرة المصدر لبرامج اتصال الحرب بسهولة في العديد من مواقع القراصنة. بعض من البرامج المتاحة هي ToneLoc، PhoneTap، و Blue Deep. إذا كنت مبرمجا، كنت قد تكون مهتما في الاطلاع على الشفرة ، ولكي لا أنصح باستخدام هذه البرامج. توخي الحذر ضروري هنا، يجب أن تكون حذرا عند تحميل برامج من شبكة الانترنت، ولكن عند تنزيل من مواقع القراصنة عليك أن تكون أكثر حذراً . ولكي تفهم لماذا الحذر ببساطة اقرأ القسم الخاص بأحصنة طروادة.

الحرمان من الخدمة

الحرمان من الخدمة مصمم من أجل تعطيل أو جعل النظام أو الشبكة غير قادر على العمل. والهدف من هذا هجوم الحرمان من الخدمة ليس الدخول في الشبكة أو الحصول على معلومات، ولكن لجعل الشبكة أو نظام غير متاح للاستخدام من قبل المستخدمين الآخرين. وسمي بهجوم الحرمان من الخدمة، لأن النتيجة النهائية هي أن يعطل المستخدمين الشرعيين من الوصول إلى خدمات الشبكة. غالباً ما تستخدم مثل هذه الهجمات للانتقام أو لمعاقبة بعض فرد أو كيان نتيجة للظلم. على عكس القرصنة الحقيقية هجوم الحرمان من الخدمة يتطلب قدرا كبيرا من خبرة والمهارة، أو الذكاءليكون ناجحاً ونتيجة لذلك، عادة ما يتم إطلاقه من قبل المبرمجين الشباب المتمردين الذين يتوهم أحدهم نفيه بأنه قرصان مخضرم.

هناك العديد من أنواع هجوم الحرمان من الخدمة، الأقسام الحالية التالية تتناول أربعة أمثلة: بينغ القاتل "، ارقام التسلسل المتزامنة" (SYN) الإغراق، البريد الالكتروني غير المرغوب، والتركيب او التجزئة. هذه أمثلة فقط وليست بالضرورة أن تكون الأشكار الأكثر استخداما من هجمات الحرمان من الخدمة.

الإتصال القاتل (Ping of death)

هجوم الاتصال القاتل، مع الاسم الميلودرامي، هو مثال على كم هو بسيط شن هجوم الحرمان من الخدمة حالما تم اكتشاف ثغرة أمنية. أولئك يكتشوف الثغرات يستحقون جائزة بينما لا يحتاج استغلال الثغرة الى مهارة كبيرة أو ذكاءاً خاصاً .

لكي نفهم بصورة افضل كيف يتم هجوم الاتصال القاتل نحن بحاجة إلى أن نلقي النظر مرة أخرى على بعض الأساسيات برتوكول تي سي بي / أي بي (TCP / IP). يستغل هجوم الاتصال القاتل وجود خلل في نظام (ICMP) في العديد من البرامج التي تطورها الشركات بائعة البرامج . (ICMP) هو جزء من أي بي (IP) في برتكول تي سي بي / أي بي (TCP / IP) ، ويعمل في طبقة الإنترنت مستخدما مخطط بيانات أي بي (IP) لتسليم الرسائل. بينغ تعليمة من تعليمات تي سي بي / أي يي (TCP / IP) ببساطة ترسل بيانات عنوان (IP) الى عنوان IP انترنت معين أو عنوان صفحة مضيف لمعرفة ما إذا كان هناك رد من عنوان الأي بي أو المضيف. هذا وكثيرا ما يستخدم لتحديد ما إذا كان المضيف على الشبكة أو على قيد الحياة. ضيغة امر الاتصال (ping) كالتالي :

- Ping 145.34.35.56
- Ping www.acme.net

العديد من أنظمة التشغيل معرضة لخطر التعرض لحزم ICMP أكبر من المعتاد. ونتيجة لذلك، تحديد حزمة كبيرة في أمر ping يمكن أن يحدث تجاوز الحد المطلوب من البيانات في بعض النظم الداخلية والذي يمكن أن يؤدي إلى تعطل النظام. إن صيغة الأمر تختلف تبعا لنظام التشغيل الذي تستخدمه. وفيما يلي مثالين، واحدة للويندوز وغيرها لصن سولاريس.

نظام تشغيل النوافذ :

- Ping-16557-s 1 hostname

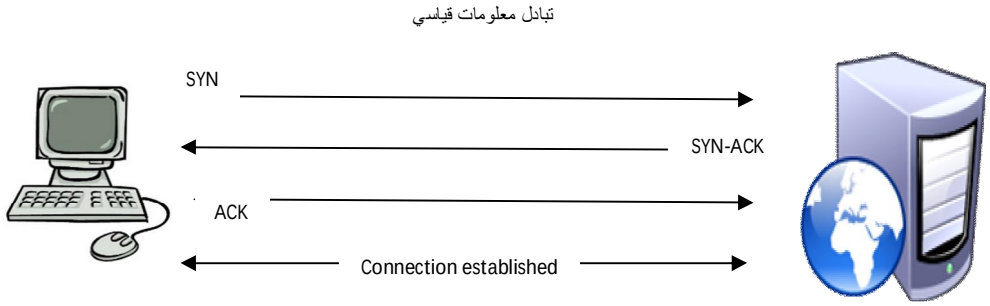
نظام تشغيل سن سولاريس

- Ping –s hostname 65527

وعادة ما يتطلب اصدار مجموعة كبيرة من امر بينغ لتعطيل نظام. علاوة على ذلك، من تجربتي الشخصية وجدت انه من المرجح أن تعطل النظام الذي يقوم بإطلاق الهجوم منه كما تعطل النظام الذي تستهدفه. ومع ذلك، فإن نهج الاتصال القاتل لايزال يشكل هجوم فعال للحرمان من الخدمة. حالما يتم اكتشاف نقطة الضعف، يقوم معظم المنتجين بارسال ترقيات لنظام التشغيل للقضاء على هذه المشكلة.

هجوم اغراق التزامن (SYN)

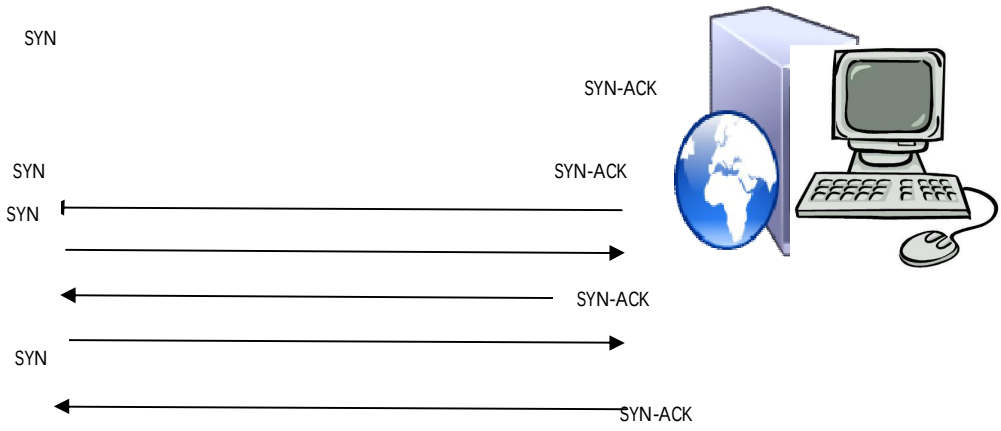
إغراق التزامن SYN هو نوع من هجوم الحرمان من الخدمة التي يستغل نظام المصافحة الثلاثي الذي يستخدمه نظام تي سي بي / أي بي (TCP / IP) لتأسيس اتصال. في الواقع يقوم هجوم اغراق التزامن (SYN) بتعطيل النظام المستهدف من خلال خلق العديد من الاتصالات نصف المفتوحة. يوضح الشكل 2.6 نموذج طبق الأصل لكيفية تأسيس اتصال TCP / IP.



الشكل 2.6: مصافحة عادية TCP / IP.

في الشكل 2.6، ينقل العميل إلى الملقم المتزامن (SYN) مجموعة بت. هذا يخبر الخادم أن العميل يرغب في تأسيس اتصال ويسأله عن بداية رقم التسلسل الذي سوف يخصص للعميل. يرد الملقم إلى العميل بالعلم (SYN-ACK) ويؤكد له بدية رقم التسلسل. يرد العميل باستلام رسالة الملقم بالعلم ويبدأ نقل البيانات.

مع هجوم اغرق التزامن (SYN) يخلق القرصان العديد من الاتصالات نصف المفتوحة عن طريق الشروع في اتصالات مع الملقم ب عدد SYN من البيانات. ومع ذلك، فإن العنوان المرسل المقترن مع SYN يكون عنوانا غير صالحا. يرسل الملقم رسالة بالعلم SYN-ACK إلى عنوان ليس له وجود ولا يقوم بالرد عليه. باستخدام البرامج المتاحة، يرسل القرصان العديد من الحزم SYN مع عناوين كاذبة إلى الملقم. يقوم الملقم بالرد لكل SYN بالعلم ثم يبقى منتظراً للرد النهائي من الجهاز العميل ويكون الاتصال نصف مفتوحا. ويوضح الشكل 2.7 كيف يعمل اغراق SYN.



الشكل 2.7: تبادل بيانات اغراق التزامن SYN.

نتيجة هذا النوع من الهجوم يمكن أن تكون أن النظام الذي يتعرض للهجوم يكون غير قادراً على استقبال طلبات الاتصال الواردة من الأجهزة المرتبطة شرعيا بالجهاز فلا يستطيع المستخدمون من الدخول الى النظام. لكل نظام تشغيل له حدود لعدد الاتصالات التي يمكن استقبالها. بالإضافة إلى ذلك، إن هجوم اغراق SYN قد يستنفد ذاكرة النظام ممايؤدي تلقائياً إلى انهيار النظام. والنتيجة النهائية هي أن النظام غير متوفر أو متعطل

احدى الإجراءات المضادة لهذا النوع من الهجوم هو وضع ضوابط مؤقت للتزامن SYN ذي الصلة لمدد زمنية قليلة لكي يغلق نظام يغلق الاتصالات نصف مفتوحة بعد فترة قصيرة نسبيا من الزمن. مع ضبط توقيت منخفضة، سيقوم الملقم بإغلاق اتصالات المفتوحة حتى أثناء فتح هجوم SYN للمزيد من الاتصالات.

البريد المؤذي(SPAM)

SPAM هي البريد الإلكتروني غير المرغوب فيه. أي شخص لديه حساب بريد اللكتروني يتلقى رسائل غير مرغوب فيها. وعادة ما يأخذ شكل محاولة تسويق من بعض الشركات التي تحاول بيع شيء نحن لا نريده أو لسنا في حاجة اليه. لمعظمنا انه مجرد مصدر ازعاج، ولكن إلى الملقم فإنه يمكن أن تستخدم كهجوم حرمان من الخدمة. وذلك بإغراق النظام المستهدف بالآلاف من رسائل البريد الإلكتروني ، رسائل البريد يمكن أن تسبب ازدحام في نطاق حزم البيانات المتاحة للشبكة، وتزيد الحمل على حدات المعالجة المركزية ، وتؤدي الى نمو سجلات العمليات فتصبح كبيرة جدا مما يؤدي الى استهلاك كافة مساحة القرص الصلب المتاحة في النظام. و في نهاية المطاف فإنه يتسبب في انهيار او تعطل النظام.

البريد المؤذي يمكن استخدامه كوسيلة لشن هجوم غير مباشر على طرف ثالث. رسائل البريد المؤذي يمكن أن تحتوي على عنوان المرسل مزور، والذي قد يكون العنوان الشرعي لبعض الأشخاص الأبرياء المطمئنين. ونتيجة لذلك فان الشخص البريء الذي استخدم عنوانه، قد يكون عرضة لهجوم بريد مؤوي من قبل جميع الأفراد المستهدفين في رسالة البريد المؤذي الأصلية.

تصفية البريد الإلكتروني يمكن أن تحد من ورود الكثير من رسائل البريد الإلكتروني غير المرغوب فيها. لسوء الحظ فإنه في كثير من الأحيان يتم تصفية البريد الإلكتروني الشرعي أيضا.