إختبار الإختراق على الشبكة المحلية المحولة

Brian Wilson الكاتب
CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA
Slimjim100@gmail.com
anti-hacker.info
www.ethicalhacker.net
Translated by medfox2010@hotmail.com ترجمت
medfox2010@gmail.com

سوف أتناول في هذه المقالة وجود الثغرات المعروفة في الشبكات المحلية ، وآمل بذلك أن أفتح عينيك على بعض الأدوات و التقنيات التي تستطيع الحصول عليها بالمجان كي تستخدمها في إجراء إختبار لشبكتك . فلنبدأ مع بعض الأسس المتواجدة في معظم الشبكات الصغيرة و المتوسطة ، وقصد تقييم الشبكة و جمع معلومات عنها ، نحتاج في البداية إلى النظر إلى عدة أمور كي نعرف العقبات التي ربما تعترضنا أثناء الإختبار ، لذلك إتخذ من هذه الأسئلة الأساسية أساس لك لجمع المعلومات.

أين توجد المحولات switches ؟
هل تستطيع الوصول إلى المعدات ؟
ماهي نوعية المحولات و المحاور hubs الموجودة على الشبكة ؟
هل السويتشات مطيعة وهل لها واجهة على شبكة الأنترنت ؟
ماهو شكل أو التصميم الفيزيائي الطوبولوجي للشبكة ؟
هل للسويتشات خصائص أمنية (نظام تحري التطفل IDS) وهل هناك إستخدام للشبكة المحلية الإفتراضية (VLAN) ؟

عندما تكون لدينا المعلومات الأساسية حول تصميم الشبكة والمعدات المستخدمة فيها ، نحن بحاجة للبحث في النشرات الأمنية للباعة لنرى إذا كان هناك أي إستغلال للثغرات من أجل القيام بإختبارها ، و إذا كانت الشبكة لاسلكية هناك تقنيات أخرى تستخدم لإيجاد الثغرات . أيضا يجب علينا أن نأخذ بعين الإعتبار الوسيلة المستخدمة لنقل البيانات على الشبكة (CAT5 ، الألياف الصناعية ، أو لاسلكيا) ، وعندما تعرفها تستطيع أن تجد أفضل طريقة للتتبع .تجد أدناه بعض الأفكار بشأن التتبع و الأدوات المستخدمة لذلك .

إيثرنت (CAT3 , CAT5 , CAT6) :

تتبع إيثرنت يتم عادة بإستخدام بروتوكول التنصت مثل Ethereal . كي تتنصت على شبكة محلية إيثرنت تحتاج إلى الوصول إلى الشبكة من خلال منفذ سويتش المرتبطين الآخرين بالشبكة .

الألياف (Gig-e أوFDDI) :

لتتبع شبكة تستخدم الألياف تحتاج إلى فاصل بصري مثل netoptics ، وتحتاج بعد ذلك الوصول إلى خطوط الألياف، وبعد تركيبك للفاصل عليها يمكنك تشغيل Ethereal أو أي متنصت آخر للشبكة .

لاسلكي (802.11 A , B , & G) :

لتتبع الشبكة اللاسلكية تحتاج في البداية أن تعرف أي نوع من الإشارة مستخدم بالشبكة . معظم الشبكات تستخدم 802.11 B أو G ، ولكن هناك أيضا من يستخدم 802.11 A ، كي تعرف أي نوع مستخدم يمكنك تشغيل بعض البرامج مثل Network Stumbler ، يمكنك هذا البرنامج من معرفة نقاط الإرتباط ومعلومات عنها مثل : القناة ، الإشارة ، و التشفير

المستخدم . عندما تعرف ما إذا كانت نقطة الإرتباط مفتوحة أو مشفرة يمكنك أن تضع خطة للوصول للشبكة ، إذا كانت الشبكة اللاسلكية مشفرة سوف يكون لزاما عليك البحث عن أدوات لكسر التشفير ، للتشفير من نوع WEP تستطيع إستخدام أدوات مثل AirCrack ، و فور إرتباطك بالشبكة تستطيع إستعمال المتنصت على الشبكة مثل Ethereal للحصول على حزم البيانات .

تنصت / تتبع الشبكة

كما أشرت في السابق ، يعتبر Ethereal أداة تنصت جيدة جدا(ومجانية) للشبكة ، ولكن هناك أدوات بروتوكول تنصت أخرى على الأنترنت منها ماهو مجاني والبعض الآخر يتطلب دفع رسوم . الفكرة وراء التنصت هي أنك تسنطيع مشاهدة كل الحزم الرقمية بالشبكة والحصول عليها وإعادة بنائها للحصول على كلمات السر وكلمات السر المشفرة وبيانات البريد الإلكتروني للموقع ، و معلومات عن قاعدة البيانات ومعلومات حساسة عديدة أخرى . إذا كانت الشبكة تستخدم المحول سوف تواجهك بعض العقبات أثناء عملية التنصت لأنك لن ترى سوى بيانات مارة وبيانات موجهة لIP الخاص بك ، ولمواجهة هذه المشكلة عليك التنصت على المنفذ الرئيسي ، منفذ المرآة ، أو قم بعملية التحايل على بيانات الشبكة لتتجاوز المنفذ الخاص بك ، ويعتبر برنامج Cain & Able أداة جيدة للتحايل والتنصت ، وبه أيضا تستطيع التنصت على مكالمات VoIP و العديد من كلمات السر الأخرى .

مسح المنافذ

عملية مسح المنافذ هي طريقة لإختبار أدوات الشبكة لمعرفة منافذ الإتصال التي قد تكون مفتوحة ، ويمكن القيام بذلك من LAN , WAN , MAN أو على الأنترنت . وتعتبر أدوات مسح المنافذ من أهم الأدوات التي يستخدمها المختبرون قصد معرفة ماهو مفتوح وكذلك معرفة أفضل للأدوات والخدمات المشغلة على الشبكة . على سبيل المثال إذا مسحت منافذ IP معين و رأيت أن المنفذ 25 مفتوح ، إذن هناك إمكانية أن تكون خدمة البريد تعمل ، والخطوة التالية لإختبار هذا المنفذ هي أن تقوم ب "تلنتtelnet" على المنفذ و تأكد من الرد إذا كان "بانرbanner" ، إذا كان الجهاز هو خادم البريد سوف يتم الرد عليكم ب service banner ، سوف يقدم خادم تبادل مايكروسوفت Microsoft Exchange Server تقريرا عن بروتوكول نقل البريد الإلكتروني SMTP ونسخة التبادل الحالية على الخادم . بعض المنافذ المهمة الأخرى هي :
(23 Telnet, 21 FTP, 23 SSH, 80 HTTP, 443 HTTPS, and 3389 Terminal servers (RDP)
بعض البرامج الجيدة لمسح المنافذ هي : SuperScan (من foundstone) ، Nmap (من insecure.org) ، و X-Scan (من xfocuse.com) ، هناك المئات من هذه البرامج والعديد منها مختص في مسح بعض الخدمات أو إستغلال الثغرات . إن كنت ترغب في الحصول على معلومات إضافية حول عملية مسح المنافذ ، إبحث في محرك البحث Google وسوف تنشغل لأشهر من كثرة ماستحصل عليه من معلومات .

إستعادة كلمة السر

يمكن إستعادة كلمة السر عن بعد ويمكن أيضا إستعادتها مباشرة بإستخدام برنامج مخصص لذلك . في الحاسوب الذي يشتغل بنظام ويندوز يمكنك تشغيل البرامج عن بعد مثل PWDump ، و إذا أمكنك الإرتباط بالحاسوب تستطيع تشغيل العديد من الأقراص الذاتية الإقلاع للحصول على كلمات السر وتغييرها . من بين الطرق الأخرى المستخدمة لإستعادة كلمة السر تلك التي تتطلب تشغيل Hash أو أدوات إستعادة ملفات Sam من حسابات مستخدمي الحاسوب ، بعدها تستطيع كسر كلمات السر المشفرة الموجودة بملف Sam لتحصل على كلمة السر الحقيقية .

كسر كلمة السر

يتم كسر كلمة السر بأخذ القيمة المشفرة Hash و إستخدام تقنية ما للكسر أو إعادة هندستها ، ومن بين هذه الطرق deanery ، القوة الضاربة bruteforce ، أو هجمات تحليل الشفرات على ال Hash ، وهناك أيضا العديد من البرامج على الأنترنت التي تستخدم قاموس كلمات السر التي كسر تشفيرها و هجمات القوة الضاربة ، ولكن أسرع طريقة هي بإستخدام جداول قوس قزح Rainbow Tables . هناك بعض المواقع على الشبكة التي تستخدم طريقة Rainbow لكسر التشفير، و برنامج rcrack.exe هو مجاني للتحميل مع قنهي المصدري source code من موقع antsight.com/zsl/rainbowcrack ، والموقع الأكثر شعبية على الأنترنت هو plain-text.info يسمح بكسر تشفير كلمتين مشفرتين مجانا في الساعة الواحدة . طريقة Rainbow جعلت مهمة خبراء الإختراق تصبح أكثر سهولة ، حيث أن الطرق القديمة مثل طريقة Bruteforce قد تتطلب أشهر لكسر كلمة السر، و قاموس الهجمات dictionary attacks لاتؤدي إلى أية نتيجة إلى إذا كانت كلمة السر من النوع المألوف .

لقد ناقشنا حتى الآن ، كيفية تحليل شبكة ما و تجهيزها لإختبار الإختراق ، وتناولنا أيضا طرق التتبع/التنصت على البيانات على الشبكة . يمكن أن يكون ماناقشناه سابقا عبارة عن دورة أولية جيدة ، كي تعرف من أين تبدأ لإنجاز إختبار للإختراق ، وكل اللأدوات المذكورة في هذه المقالة تجدها و بالمجان على الأنترنت . إذا إحتجت لأي مساعدة في هذا الموضوع فقط إبحث على الأنترنت فهناك إرشادات عديدة تغطي مجالات متخصصة حول إختبار الإختراق ، وتذكر أن الفكرة وراء إختبار الإختراق هي ان تتعلم و تأمن شبكتك .