|  |  |  |
| --- | --- | --- |
|  |  | **X** |

[**راههای نفوذ به شبکه**](http://black-hack.blogfa.com/post-86.aspx)

شما در اينجا با كليه مراحل نفوذ به يك شبكه اشنا ميشويد.   
  
خوب همان طور كه ميدانيد اولين مرحله نفوذ به يك شبكه, شناسايي شبكه مورد نظر ميباشد. شما صحنه يك جنگ را تصور كنيد چطور ميتوان بدون اگاهي از موقعيت جغرافياي , ميزان قدرت دشمن- تعداد نفرات و تجهيزات و...... همين طور كور كورانه به سمت دشمن حمله كرد . مشخص است اين حمله موفق نميباشد . حمله به شبكه هم به مانند صحنه جنگ ميباشد.   
  
گام اول : شناسايي مقدماتي شبكه.   
  
شناسايي مقدماتي شبكه هدف بدون نياز به ابزار .!   
  
اين روش مبتني بر اصول روان شناختي ميباشد. و نياز به ابزار يا تخصص فني ندارد. ( بستگي به زبون بازي و مخ زني شما دارد ). شايد اين روش به نظر شما مسخره باشد ولي يكي از بهترين راههاي شناسايي ميباشد.   
  
براي مثال فرض كنيد. نفوذگر در يك مهماني خانوادگي يكي از كارمندان شبكه شركت ميكند. در اين مهماني ميشنود كه در شبكه از سرويس دهنده قديمي BIND به عنوان سيستم DNS استفاده ميشود و سيستم عامل ان سرويس سولاريس است .شبكه با همين جملات خانه خراب و ويران ميشود   
  
  
  
شناسايي شبكه به روش روان شناختي و تعاملات اجتماعي.!!   
  
  
  
روش ديگر براي شناسايي مقدماتي شبكه , تماسهاي مكرري است كه گاه و بي گاه با گروهاي پشتيباني فني بر قرارميشود. وظيفه شبانه روزي اين گروه رسيدگي به مشكلات احتمالي كاربران بي اطلاع است. (( پس در زمان صحبت با اين گروه اين مورد را رعايت كنيد : با لحن ابلهان صحبت كنيد تا طرف مقابل شك نكند.‌))   
  
حالا فرض كنيد در زمان اوج مشكلات و مشغلۀ كاري , يك نفر با گروه پشتيباني تماس ميگيرد و ادعا ميكند از ديشب تا به الان نتوانسته با كلمه عبور 123456 وارد شبكه بشود. و از اين موضوع ناراحت است و ميخواهد از عملكرد شبكه شكايت كند. گروه پشتيباني فني كلمه كاربري USER ID او را ميگيرد و بعد از بررسي با ملاطفت به او پاسخ ميدهد كه او رمز عبور خود را فراموش كرده و كلمه عبورش abcdef ميباشد .   
  
  
  
فردي عصباني با گروه پشتيباني فني تماس ميگيرد و با حالت طلب كارانه ميگوييد كه نتوانسته از سرويس TELNET براي بر قراري ارتباط با شبكه استفاده كند. انها هم مهربانانه پاسخ ميدهند كه بواسطه ديوار اتشي تمام پورت ها به غير از پورتهاي 80,25,20,21.53 مسدود هستند.   
  
  
  
كسي با گروه پشتيباني فني تماس ميگيرد و همه انها را متهم به سوادي ميكند كه چرا توپولوژي شبكه و نوع مسريابي شبكه را نميدانند , همچنين بلد نيستن قواعد ديوار اتشي را به درستي تنظيم كنند. گروه پشتيباني با دلتنگي پاسخ ميدهد كه : اولا ديوار اتشي وجود ندارد كه بخواهند قواعد ان را تنظيم كنند ثانيا بهترين مسرياب Cisce با فلان مدل را تهيه كردند و استفاده ميكنند و ثالثا توپولوژي شبكه با بهترين سوئيچهاي 3Com شكل گرفته شده و سپس گوشي را به زمين ميكوبند. در حالي كه طرف مقابل قلم به دست لبخند ميزند.   
  
  
  
جستجو در وب به دنبال اطلاعات و اخبار در مورد شبكه هدف.!   
  
  
  
در حملات را دور نمي توان متكي به شناسايي روان شناختي يا دسترسي فيزيكي به شبكه بود.وقتي يك نام حوزه Domain Name ثبت ميشود, شركت يا گروه يا فرد ثبت كنند مجبور ميباشد اطلاعات لازم در مورد خود و شبكه خود به ثبت كنند ادرس Registrer ارائه دهد. اين اطلاعات عمومي و در دسترس همگان خواهد بود همينطور وقتي يك كلاس ادرس IP ثبت ميشود سازمان ثبت كنند بطور ضمني اطلاعاتي از ماهيت شبكه را و چگونگي اداره ان را فاش ميكند.به طور كلي يك نفوذگر در وب به دنبال اطلاعات زير از شبكه هدف ميگردد.   
  
  
  
  
  
  
  
#- ادرسهاي حوزه ثبت شده براي شبكه Domain Name   
  
#- ادرسهاي IP ثبت شده براي شبكه .   
  
#-ادرسهاي پست الكترونيكي و شماره تلفن و ادرس و UIN يا همان ID در Yahoo Messenger .   
  
نكته : UIN همان شماره جهاني هويت افراد در محيط چت ICQ ميباشد.   
  
#-نوع سرويسهاي كه شبكه هدف عرضه ميكند.   
  
  
  
استفاده از موتورهاي جستجو در ايترنت .!!   
  
  
  
Excite موتورهاي هستن كه گاهي اوقات اطلاعات بسيار مهمي در اختيار نفوذگر قرار ميدهد. براي مثال ميتوان با تايپ   
  
( ادرس هدف Link: ) تمام سرويسهاي كه به اين ادرس لينك داده اند را بدست اوريد.   
  
مثال: من از اسمه خودم براي مثال استفاده ميكنم.   
  
خوب توي قسمت جستجوي سايت Altavista اين جمله را تايپ ميكنيم .   
  
Link:akabr.com   
  
پاسخ موتور :   
  
[http://www.iranbooter.com](http://www.iranbooter.com/)   
  
[http://www.ashiyane.com](http://www.ashiyane.com/)   
  
[http://www.chatmasters.com](http://www.chatmasters.com/)   
  
[http://www.netninja.com](http://www.netninja.com/)   
  
[http://www.merelin.com](http://www.merelin.com/)   
  
و ..............   
  
خوب شما با ورود به اين سايتها ميتوانيد اطلاعاتي در مورد شبكه هدف بدست بياوريد.!!!!!   
  
استفاده از Usenet .!!   
  
  
  
يكي ديگر از روشهاي كسب اطلاعات در مورد شبكه هدف كه بهترين و موثرترين راه است استفاده از بانك اطلاعاتي   
  
Whois ميباشد. در اين بانك كليه اطلاعات لازم براي يك نفوذگر وجود دارد .   
  
وقتي شما ميخواهيد يك ادرس حوزه باپسوندهاي .com , ,.net , .org را در اينترنت ثبت كنيد بايد به يكي از سايتهاي ثبت دهنده نام مراجعه كنيد و پس از پرداخت وجه مربوط نام حوزه را تعيين كنيد.در اينجا با طي يكسري از مراحل كه تشريح آن از حوصله بحث ما خارج است شما بايد يكسري اطلاعات را به شركت كي ميخواهيد ادرس خود را به وسيلۀ ان ثبت كنيد بدهد. كه اين اطلاعات به صورت مستقيم در بانك اطلاعاتي whois ذخيره ميشود   
  
اين همان اطلاعات مورد نياز يك نفوذگر ميباشد..   
  
[Http://www.internic.net/alpha.html](http://www.internic.net/alpha.html)   
  
[Http://www.allwhois.com/home.html](http://www.allwhois.com/home.html) ( از .ac متعلق به ايرلند تا .yu متعلق به يوگسلاوي )   
  
براي جستجو اطلاعات در مورد موسسات نظامي امريكا با پسوند .mil ميتوانيد به ادرس زير مراجعه كنيد.   
  
[http://whois.nic.mil](http://whois.nic.mil/)   
  
و در مورد دانشگاه هاي تحقيقاتي امريكا ميتوانيد از ادرس زير استفاده كنيد.   
  
<http://www.networksolution.com/>   
  
. در مورد ادرسهاي متعلق به ادرات دولتي امريكا نيز ميتوانيد به ادرس زير مراجعه كنيد.   
  
[http://whois.nic.gov](http://whois.nic.gov/)   
  
بعد از طي مراحل گفته شده بانك اطلاعاتي مشخصات زير رادر اختيار شما قرار ميدهد.   
  
☻نامها: نفوذگر از اسامي معرفي شده توسط مديريت سايت ميتواند براي شناسايهاي روانشناختي خود استفاده كند.   
  
☻شمارهاي تلفن: از شماره تلفن براي شناسايي خطوط متصل به مودم و سازماندهي حمله بر عليه مودمها استفاده ميشود.   
  
☻ادرسهاي پست الترونيكي يا همان ايميل: نفوذگر از ادرسهاي پست الكترونيكي به دو نكته مهم پي خواهد برد.   
  
الف): قالبهاي تمام ادرسهاي پست الكترونيكي كاربران ان مشخص ميشود.   
  
ب): ادرس پست الكترونيكي مسئولين ذيربط به دست مي ايد.   
  
Name Server: اين مشخصه بسيار مفيد نفوذگر را براي بدست اوردن اطلاعات بيشتر در مورد ماشينهاي سرويس دهندۀ DNS متعلق به ان شركت هدايت ميكند.؟   
  
استفاده از سايت ARIN جهت تحقيق در مورد ادرس IP   
  
سايت ARIN ( American Registry for Internet ) سرويسي مشابه Whois در اختيار كاربران قرار ميدهد دراين سايت ميتوانيد بفهميد كه مثلا يك ادرس IP متعلق به چه شركتي يا سازماني ميباشد . ARIN   
  
تمام ادرسهاي اختصاص داده شده به يك شركت يا موسسه خاص را به كاربران ارائه ميدهد. البته بايد اشاره كنم كه اين سايت فقط ادرسهاي كه در محدوده جغرافيايي زير باشد را ارئه ميدهد.   
  
  
  
  
  
#-منطقه امريكا (شمالي و جنوبي )   
  
#- منطقه Caribbean   
  
#- منطقه صحرايي افريقا.   
  
البته منابع ديگري هم موجود ميباشد كه اسيا و اروپا را پوشش ميدهند ولي اين مورد نيز جزء موارد حساس ميباشد.   
  
براي يافتن ادرسهاي IP اختصاص داده شده در اروپا بايد به سايت RIPENCC در ادرس زير مراجعه كنيد.   
  
<http://ripe.net/>   
  
مشخصات ادرسهاي IP اختصاص داده شده در اسيا و در سايت APNIC با ادرس زير در دسترس ميباشد.   
  
<http://www.apnic.net/>   
  
ҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖ   
  
كسب اطلاعات از سرويس دهندۀ DNS در راستاي حمله.   
  
نكته: در اينجا شما بايد مقداري با ساختار بانك اطلاعاتي سرويس دهندهاي نام اشنا باشيد. كه توضيح اين مطلب از حوصلهاين مقاله خارج است.   
  
در قسمت قبلي اموختيد كه سيستم DNS حاوي اطلاعات بسيار مفيدي است كه متاسفانه گاهي در خدمت نفوذگر قرار ميگيرد. بطور معمول نفوذگر براي شناسايي مقدماتي شبكۀ هدف بوسيله DNS مراحل زير را دنبال ميكند.   
  
√ او ابتدا نياز دارد تا حداقل يك سرويس دهندۀ DNS را در شبكه هدف پيدا كند . پيدا كردن سرويس دهندۀ DNS از يك شبكه( بگونهاي كه تشريح شد ) بسادگي و از طريق سرويس Whois در اينترنت امكان پذير است .   
  
مثال:   
  
حالا سرويس دهنده هاي DNS از شبكۀ Security.com با ادرسهاي IP زير معرفي شده اند.   
  
● 216.57.130.1 ( سرويس دهندۀ DNS اصلي )   
  
● 216.57.120.2 ( سرويس دهندۀ ثانويه ) و سرويس دهندۀ سوم و چهارم   
  
سرويس دهندۀ اوليه و سرويس دهندۀ ثانويه تفاوتي ندارند. سرويس دهندۀ بعنوان پشتيبان سرويس دهندۀ اوليه , قابليت اعتماد شبكه را بالا ميبرد و در مواقعي كه سرويس دهندۀ اصلي مختل ميشود سرويس دهندۀ دوم در اختيار كاربران اينترنت قرار ميگيرد. ( قابل توجه هكرهاي اماتور , متوسط و حتي سطح بالاتر به اين نكته اي كه در بالا ذكر شد خيلي توجه كنيد.)   
  
براي استخراج اطلاعات لازم از سرويس دهندۀ DNS نفوذگر بايد از ابزارهاي خاص استفاده كند يكي از ابزارهايعمومي و ساده در سيستم عامل ويندوز و يونيكس برنامۀ nslookup است كه در خط فرمان اجرا ميشود . نفوذگر به راحتي درخط فرمان nslookup را تايپ كرد و سپس Enter را فشار ميدهد و پس از اجراي اين برنامه ميتواند با سرويس دهندۀ DNS ارتباط بر قرار كند.   
  
در مرحله بعدي نفوذگر سعي ميكند تا از طريق nslookup اقدام به "در يافت كل اطلاعات يك Zone نمايد. برين معني كه تمام ركوردهاي موجود در ارتباط با يك تام حوزه منتقل شود . nslookup از DNS متلعق به يك شركت يا موسسه تقاضا ميكند تا تمام ركودهائي را كه در خصوص يك نام حوزه در بانك اطلاعاتي ذخيره شده است. برايش ارسال نمايد .   
  
بدين منظور پس از اجراي nslookup با يد از طريق فرمان SERVER نام سويس دهندۀ مورد نظر تعيين شود.   
  
براي انتقال ركورهاي موجود در خصوص يك نام حوزه را تقاضا كند. بايد از فرمان زير استفاده كنيد.   
  
Set type = any   
  
سپس براي انكه انتقال ركوردهاي موجود موجود در DNS هدف شروع شود بايد از فرمان زير استفاده كنيد.   
  
] نام حوزۀ مورد نظر [ ls -d   
  
  
  
$ nslookup   
  
Default server: Merelin.attacker.com   
  
Address: 10.200.100.45   
  
  
  
Server 10.1.1.34   
  
  
  
Default Server : ns.Aramis.com   
  
Adress: 10.1.1.34   
  
  
  
Set type=any   
  
Ls -d Aramis.com   
  
System 1 D IN A 10.1.1.36   
  
1 D IN HINFO "Solaris 2.6 mailServer"   
  
1 D IN MX 10 mail   
  
Web 1 D IN A 10.1.1.49   
  
1 D IN HINFO "NT$WWW"   
  
  
  
  
  
ntftp 1 D IN A 10.1.1.50   
  
ws 1 D IN A 10.1.1.20   
  
1 D IN "TXT" "Administrator Workstatoin"   
  
  
  
( در متن بالا من خروجي ها را خلاصه كردم تا خوناتر باشد. )   
  
حال اگر به دقت به ركوردهاي نمايش داده شود را بررسي كنيد اطلاعات مهمي در ان خواهيد ديد. اين اطلاعات براي نفوذگر بسيار با ارزش است:   
  
Syetem 1 : ركورد اول تا سوم از خروجي مشخص كنندۀ انست كه ماشيني با ادرس 10.1.1.36 سرويس دهندۀ پست الكترونيكي وسيستم عامل ان سولاريس ورژن 2.6 است.   
  
Web: ركورد چهارم وپنجم از خروجي مشخص كنندۀ انست كه ماشيني با ادرس 10.1.1.49 نقش سرويس دهندۀ وب را بازي ميكندو سيستم عامل ان Windows NT 4.0 است.   
  
Ntftp:ركورد ششم از خروجي نشان ميدهد كه سرويس دهندۀ FTP بر روي ماشيني با ادرس 10.1.1.50 نصب شده و احتملا سيستم عامل   
  
ان Windows NT ميباشد .( ntftp→NT FTP)   
  
Ws: دو ركورد اخر ازخروجي نشان ميدهد كه ماشين با ادرس 10.1.1.20 متعلق به شبكه است .   
  
خوب حالا با nslookup اشنا شديد . البته من براي اين بعدا ( حرف و حديث پيش نيايد‌ ) يك برنامه بسيار قوي و جالب را براي اين كار به شما معرفي ميكنم.   
  
Adig: اين برنامه در ادرس زير عرضه ميشود.   
  
<http://nscan.hypermart.net/index.cgi?index=dns>   
  
در اينجا لازم من چند برنامه براي شناسايي شبكه به شما دوستان عزيز معرفي كنم. .   
  
ابزار Samspade   
  
اين نرم افزار ابزاري ساده براي شناسايي شبكه ميباشد. اين نرم افزار توسط Steve Atkins نوشته شده و در ادرس زير در دسترس عموم قرار دارد.   
  
[http://www.samspade.org.ssw](http://www.samspade.org.ssw/)   
  
Cyber Kit: اين نرم افزار هم براي شناسايي شبكه ميباشد. كه از ادرس زير قابل دسترس است.   
  
[http://www.cyber](http://www.cyber/) kit.net/index.html/   
  
iNet Tools: اين نيز يك نرم افزار براي شناسايي شبكه تحت ويندوز و مكينتاش است كه در ادرس زير در دسترس عموم قرار دارد.   
  
<http://www.wildpackets.com/products/inettools>   
√ در جستجوي مودمهاي شبكه   
  
نفوذگر در اولين اقدام خود براي يافتن رخنۀ نفوذ , به سراغ مودمهاي شبكه ميرود. اين ابزار مفيد و ساده گاهي نقش يك خائن را براي شبكه ايفا ميكند. و نفوذگر را از يك در پنهان به دورن شبكه هدايت ميكند.   
  
● در اين مرحله نفوذگر با در اختيار داشتن فهرستي از شماره هاي تلفن كه در مرحلۀ ( شناسايي مقدماتي شبكه ) گرد اوري كرده . براي پيدا كردن مودمهاي اسيب پذير شروع به پويش ميكند .!   
  
پويش مودمها با هدف يافتن يك راه نفوذ طبق مكانيزم زير انجام ميشود.   
  
● نفوذگر مجموعه اي از شماره هاي تلفن را كه احتمال ميدهد متعلق به شبكه هدف حمله است, مشخص مي نمايد . در اينجا نفوذگر مجبور است اين شماره ها را در يك فايل ذخيره كند . يا يك محدود از شماره ها را تععيين نمايد .( مثلا شمارهاي 9876000 تا 9876999   
  
معادل هزار شماره تلفن ).   
  
● سپس براي پويش اين خطوط تلفن از يك ابزار خودكار استفاده ميكند. تا در روال پي در پي با اين شماره هاي تلفن تماس برقرار شودو به محض تشخيص يك سيگنال حامل ( Carrier ) متعلق به مودم , شماره تلفن مربوط در جائي ذخيره شود .   
  
● پس از يافتن شمارهاي تلفني كه به مودم متصل است . نفوذگر از طريق يك ابزار نرم افزاري روي اين مودم ها متمرگز ميشود.   
  
تا:   
  
◘ نوع مودم و پروتكل ارتباطي ان را تشخيص بدهد .   
  
◘ سرويس دهندۀ آن مودم را شناسايي كند.   
  
◘ كلمه عبور براي وصل ارتباط ان مودم را بدست بياورد.   
  
◙ نفوذگر در صورت پيدا كردن مودم ازاد و متصلي كه بتوان از طريق ان به يكي از ماشينهاي شبكه متصل شد. مراحل بعدي حمله را طرح ريزي ميكند.   
  
معمولا براي سرويس دهي با مودم از راه دور از نرم افزارهاي مشهوري مثل :   
  
■ Symantec's pcAnyWhere   
  
■ Laplink   
  
■ ControlIT   
  
كه هر كدام در صورت پيكر بندي نادرست نقش ستون پنجم را براي شبكه بازي ميكنند. من در اينجا يكسري از بهترين ابزارهاي حمله به شبكه را به شما معرفي ميكنم.   
  
  
  
◙ THC-Scan 2.0   
  
در سال 1998 توسط Van Hauser نوشته شده است كه شايد بتوان ادعا كرد قدرتمند ترين ابزار براي حمله به مودم ميباشد.   
  
اين نرم افزار در ادرس زير در دسترس عموم ميباشد.   
  
<http://thc.inferno.tusculum.edu/>   
  
البته بايد توجه داشته باشيد كه اين برنامه خروجي گرافيكي ندارد و در خط فرمان اجرا ميشود.   
  
.   
  
  
  
√ حملات پس از پيدا شدن مودمهاي فعال .!   
  
در اين جا دو حالت براي نفوذگر پيش مي ايد:   
  
حالت اول: ارتباط با مودم بدون درخواست كلمه عبور برقرار ميشود.   
  
حالت دوم: براي برقراري ارتباط با مودم كلمه بور درخواست ميشود. در اين زمان نيز دو حالت براي شما پيش مي ايد . حالت اول اين است كه به صورت دستي شروع به وارد كردن كلمه هاي عبور احتمالي كنيد يا از طريق ابزار خودكار كه من حالت دوم را به شما عزيزان پيشنهاد ميكنم.   
  
◙ THC Login Hacker   
  
  
  
اين يك ابزار جهت ورود به سيستمهاي است كه از كاربر كلمه عبور ميخواهد. اين ابزار را ميتونيد از ادرس زير دانلود كنيد.   
  
<http://thc.inferno.tusculum.edu/>   
  
نكته: به هر حال كشف كلمه عبور چه بصورت دستي و چه بصورت خودكار وقتگير ميباشد. ولي تنها سرمايه يك نفوذگر حرفه اي براي نفوذ به يك سيستم "زمان" است.   
  
  
  
√نقشه برداري از شبكه .!   
  
نقشه برداري از شبكه براي پي ريزي يك حمله شامل مراحل زير خواهد بود.   
  
● مشخص كردن ماشين هاي فعال: براي نقشه برداري از شبكه بايد تمام ماشينهاي شبكه Ping شوند.فرض كنيد در مرحلۀ شناسايي مقدماتي نفوذگر ادرس IP يك شبكه را 195.145.11.0 تشخيص داده باشد اين ادرس كلاس C است و در چنين شبكه اي حداكثر 254 ماشين قابل تعريف هستند. لذا بايد تمام اين ادرسها از 192.145.11.1 تا 192.145.11.245 با ارسال بسته هاي Ping از لحاظ اماده بودن مورد ازمايش قرار بگيرد.   
  
چون در اينجا كليه مخاطبان ما اماتور هستند و با در نظر گرفتن عدم اگاهي و تسلط مخاطبان ,در زمينه پروتكل TCP/IP من و دوست عزيزم LORD.ARAMIS تصميم گرفتيم كه براي راحتي كاربران و درك بهتر مطالب اين مقاله بيشتر با ابزارها, نحوۀ حمله را تشريح كنيم.   
  
● Cheops : نرم افزاري براي نقشه براداري از شبكه.   
  
اين نرم افزار را ميتوانيد از ادرس زير دانلود كنيد.   
  
<http://www.marko.net/cheops/>   
  
اين نرم افزار توپولوژي شبكه را طبق روالي كه گفته شد از طريق ارسال بسته هاي Ping و فرمان Traceroute و پردازش هوشمندانۀ نتايج اين فرامين استخراج ميكند. اين نرم افزار خروجي گرافيكي و بسيار زيبا و قابل فهمي را براي اماتورها ارئه ميدهد.   
  
  
  
√تعيين پورتهاي باز بر روي يك ماشين.!   
  
دراين مرحله نفوذگر ماشينهاي فعال شبكه را و همچنين توپولوژي تقريبي انرا ميشناسد. حال او ميخواهد بداند هر ماشين چه وظيفه اي را برعهد دارد و چه خدماتي به ارئه ميدهد. و در ضمن هر كدام از سرويس ها به چه نحو در اختيار كاربران قرار ميگيرند.   
  
باز در اينجا ما به مشكل عدم درك مفاهيم TCP/IP بر ميخوريم البته من سعي ميكنم يك مقدار از اين مفاهيم را براي اشنايي شما با عمل تعيين پورتهاي باز بر روي يك ماشين توضيح بدم.   
  
در پروتكل TCP/IP هر ماشين ميتواند حداكثر 65535 پورت TCP و به همين تعداد پورت UDP باز داشته باشد. كه البته بر روي يك ماشين فقط تعداد بسيار محدودي از انها باز و فعال ميباشند . يعني مجموع پروسه هاي در حال اجرا فقط به تعداد محدودي از اين پورتها گوش ميدند. به تناسب سرويسي كه ارئه ميكند.   
  
هر پورت باز بر روي ماشين يك در ورودي پنهان ماشين محسوب ميشود. بعنوان مثال اگر يك برنامه Web Server را اجرا كرده باشيد به پورت 80 گوش ميدهد.و بسته هاي TCP با شماره پورت 80 را ميپذيرد. اگر شما يك سرويس دهندۀ DNS داشته باشيد پورت UDP 53 باز است . و همچنين با نصب و اجراي سرويس دهند. پست الكترونيكي پورت 25 TCP باز و فعال خواهد بود.   
  
سرويس دهنده هاي مشهور و استاندارد جهاني داراي پورتهاي مشخص و معيني هستند.   
  
  
  
◙ Super Scan For Windows NT/98/2000/XP   
  
  
  
اين نرم افزار يكي از قدرتمندترين نرم افزارهاي پويش پورت ( Port Scanner ) ميباشد كه در ادرس زير در دسترس عموم قرار دارد.   
  
<http://members.home.com/rikeir/software.html/>   
  
  
  
◙ Nmap   
  
  
  
اين نرم افزار نيز يكي از بهترين نرم افزارهاي پويش پورت ميباشد كه داراي مكانيزيم هاي مختلف براي پويش پورت ميباشد.   
  
اين نرم افزار را ميتوانيد از ادرس زير دانلود كنيد.   
  
<http://www.inseure.org/Nmap>   
  
مكانيزم هاي زيادي براي پويش پورت وجود دارد. كه توضيح نحوۀ عمل كرد اين مكانيزيم ها از حوصلۀ اين مقاله خارج ميباشد.   
  
نكته بسيار مهم: يك نفوذگر حرفه اي براي رد گم كردن تعدادي ادرس IP جعلي انتخاب كرده و هنكامي كه يك بسته را با ادرس حقيقي خودش ارسال مي نمايد چند بستۀ بي مصرف را با ادرس IP جعلي نيز به همراه ان مي فرستد. فرض مثال از هر 6 بسته 5 بسته جعلي ميباشد. لذا اگر بازرسان امنيتي بخواهند با بررسي فايل هاي ثبت شده ( Log Files ) به هويت نفوذگر پي ببرند . با مجموعه اي از   
  
ادرسهاي IP مواجه ميشوند. كه مشخص نيست كداميك از انها نفوذگر است.و كدام بي گناه.!   
  
  
  
√تعيين سيستم عامل ماشين هدف.   
  
  
  
من در اينجا باز با استفاده از ابزار توضيح ميدهم. ابزارهاي پويش مثل Nmap يك بانك اطلاعاتي از عملكرد سيستم عامل هاي مختلف دارند كه در مواجهه با اتفاقات غير معمول از ان استفاده ميكنند. براي پي بردن به سيستم عامل ماشين هدف . بسته هاي نا متعارف زير به سمت   
  
ماشين هدف ارسال ميشود.   
  
● بستۀ SYN به سمت يك پورت باز ماشين.   
  
● بستۀ NULL به سمت يك پورت باز (( بستة NULL بسته اي بدون Code Bits است از اين براي حملات DDOS استفاده ميكنند‌)   
  
● بستۀ PSH-URG-FIN به سمت يك پورت باز ماشين.   
  
●بستۀ UDP به شمت يك پورت بستۀ ماشين.   
  
● بستۀ ACK به سمت يك پورت بسته ماشين.   
  
ҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖҖ   
  
  
  
FireWalk بر عليه FireWall   
  
.   
  
يكي از ابزارهاي بسيار قدرتمند و زيركانه كه مي تواند در خدمت نفوذگر قرار بگيرد . نرم افزار FireWalk ميباشد كه بر ضد ديوار اتشي بكار ميرود. اين نرم افزار اين نرم افزار توسط 2 نفر از خبرگان هك بنامهاي ديويد گلداسميت و ميخائل شفمن نوشته شده است .   
  
FireWalk سعي ميكند تا متوجه شود چه پورتهاي از طريق ديوار اتشي باز مانده است.! فراموش نكنيد كه اگر پويشگري مثل Nmap پورتي را بر روي يك ماشين بسته اعلام كرد . نمي توانيد يقعين داشته باشيد كه اين پورت واقعا بسته ميباشد. شايد كه ديوار اتشي مانع از شناسايي ان شده باشد.   
  
نكته: البته بايد دقت داشته باشيد كه FireWalk تحت لينوكس ميباشد.   
  
شما اين نرم افزار را ميتوانيد از ادرس زير دانلود كنيد.   
  
  
  
<http://www.packetfactory.net/projects/Firewalk-final.html>   
  
  
  
نكته: در اينجا شما بايد توجه داشته باشيد كه نرم افزار Firewalk در موارد پراكسي ( proxy ) نتيجه موثري نخواهد داشت .   
  
◘ يك ارتباط TCP بين پراكسي و ماشين مبداء برقرار ميشود .   
  
◘ يك ارتباط TCP بين پراكسي و ماشين مقصد ايجاد ميشود.   
  
◘ دادها ابتدا از مبداء تحويل گرفته ميشوند و سپس براي مقصد ارسال ميگردد. ( دادهاي ارسالي از مبداء بطور كامل تحويل لايۀ كاربرد ( Application ) در پراكسي شده و پس از بررسي هاي لازم از طريق ارتباط TCP بين پراكسي و هدف , تحويل داده خواهد شد. ) بدين ترتيب هيچ ارتباط مستقيم و انتها به انتها بين ماشين مبداء و مقصد ايجاد نخواهد شده.   
  
  
  
√ ابزارهاي جستجوي نقاط اسيب پذير.!   
  
اين ابزارها با پروسۀ اجرا شده روي ماشين هدف ارتباط برقرار ميكند و با ارسال دادههاي نامتعارف به ان پروسه , نقاط ضعف انرا در مواجهه با اين دادها بديت مي اورد . نفوذگر نيز از همين حربه براي ضربه زدن به ماشين هدف استفاده ميكند. چون اين فرايند. بطور خودكار و ازطريق برنامه نجام ميشود لذا هزاران هزار حالت مختلف را بررسي كرد و در صورت وقت كافي نقاط ضعف پروسه هاي ماشين هدف را استخراج ميكند.   
  
نكته: به اشكالات بنيادي سيستم عامل ها و نرم افزارها, باگ (Bug) گفته ميشود .   
  
من در اينجا چند برنامه را براي پويش و جستجوي نقاط اسيب پذير به شما عزيزان معرفي ميكنم.   
  
نكته: بهترين ابزار پويش در اين زمينه ابزار Nessus ميباشد كه بصورت رايگان عرضه ميشود خصوصيات اين نرم افزار رايگان در نسخه هاي تجاري اين نرم افزار ها نيز يافت نمي شود.   
  
اين نرم افزار در ادرس زير در دسترس عموم قرار داد.   
  
  
  
<http://www.nessus.org/>   
  
  
  
در اينجا نيز لينك دانلود چند نرم افزار را به شما عزيزان معرفي ميكنم.   
  
  
  
<http://www-are.com/sara/>   
  
<http://www.wwdsi.com/saint/>   
  
<http://razor.bindview.com/tools/>   
  
  
  
نكته: عزيزان توجه داشته باشند كه كليه Plug-in هاي ساخته شده براي برنامه Nessus را نيز از دارس داده شده دانلود كنند. من سعي ميكنم در ضميمه اين مقاله Plug-in هاي اين نرم افزار را براي شما عزيزان توضيح بدهم.   
  
  
  
√ حمله به IDS بر اساس قطعات كوچك و قطهات هم پوشان IP   
  
فرض كنيد يك بستۀ IP محتوي يك بستۀ TCP ( در فليد Payload) باشد. چون بخش اول Payload از هر بستۀ IP ميتواند قطعه قطعه شود , لذا بطور عمدي قطعۀ اول به قدري كوچك در نظر گرفته ميشود كه فقط دو بايت اول بستۀ TCP را شامل شود و بنابراين در بايت دوم از بستۀ TCP شمارۀ پورت مقصد ( Destination Port ) را در بر ميگيرد در بستۀ دوم ارسال ميشود. معمولا سيستمهاي IDS براي تشخيص حمله به سرايند بستۀ TCP احتياج دارند. تا مثلا تلاش براي بر قراري ارتباط با پورت 23 مربوط به TelNet را كشف نمايد. چون بستۀ اول سرايند كامل بستۀ TCP و شماره پورت مقصد را ندارد معمولا IDS انرا معمولي در نظر گرفته و از ان ميگذرد .   
  
بدين صورت نفوذگر IDS را دور ميزند.   
  
√ FragRouter : ابزاري براي فرار از چنگ سيستم IDS   
  
ابزار FragRouter كه توسط گروه Dug Song طراحي شده , انواع حملات به سيستم IDS را بر اساس تكنيك قطعه قطعه سازي   
  
بسته هاي IP , پياده سازي كرده است.   
  
عزيزان ميتوانيد اين ابزار را از لينك زير دانلود كنيد.   
  
  
  
<http://www.anzen.com/research/nidsbench/>   
  
  
  
√ Whisker براي فريب IDS   
  
  
  
قابل توجه هكرهاي اماتور اين بخش را به دقت مطالعه كنند. اين بخش يكي از مهمترين و حساس ترين بخشهاي اين مقاله ميباشد.من به دليل حساسيت اين بخش سعي كردم كليه جزئيات و نكات اين بخش را براي شما عزيزان تشريح كنم اميدوارم استفاده لازم راببريد.   
  
  
  
☻مكانيزيمهاي Whisker براي فريب دادن IDS .   
  
  
  
Whisker ده روش متنوع و قدرتمند براي گول زدن IDS بكار ميگيرد كه من اين روشها را يك به يك براي شما عزيزان معرفي خواهم كرد.   
  
نكته: در تمام اين روشها تقاضا , ارسال يك فرمان HTTP به سرويس دهندۀ وب براي فعل و انفعال با برنامۀ CGI تلقي ميشود.   
  
  
  
☻URL Encoding : قسمت ادرس در URL ارسالي با كدهاي معمولي ASCll ارسال نميشود.بلكه ابتدا هر كاركتر با معادل يوني كد آن ( يعني با قالب %xx تعريف شده در MINE ) جايگزين و سپس ارسال ميشود . برخي از سيستمهاي IDS قادر نيستند چنينقالبي را تشخيص دهند و لذا تقاضاي خطرناك كشف نخواهد شد.   
  
  
  
☻/./ Directory Insertion : URL ارسالي شامل كاركترهاي /./ است كه در برخي از سرويس دهنده هاي وب به اين شكل تعبيرو تفسير ميشود كه "لطفا به شاخۀ جاري تغيير مسير بدهيد.!" تغيير مسير به شاخۀ جاري هيچ خاصيت يا ضرري ندارد . بلكه فقط شكل ظاهري URL را به گونه اي تغيير ميدهد تا به الگوي حمله شباهت نداشته باشد.   
  
مثال: GET /./cgi-bin/./broken.cgi http/1.0   
  
  
  
☻Premature URL Endig: در URL ارسالي اطلاعاتي در خصوص اسكريپ مورد نظر قرار داده نميشود . در عوض اين اطلاعات در بخش سراينده HTTP جا سازي ميشوند به مثال زير دقت كنيد.   
  
GET /HTTP/1.0\r\Nheader:../../cgi-bin/broken.cgi/HTTP/1.0   
  
كساني كه با پروتكل HTTP اشنا هستند صحت اين URL و اعتبار تقاضاي GET را تاييد ميكنند.   
  
  
  
☻Long URL: قسمت ادرس در URL ارسالي شامل نام بسيار طولاني يك شاخه است كه وجود ندارد. در انتهاي نام كاركتر /../   
  
قرار ميگيرد. بدين ترتيب در سويس دهندۀ وب از نام شاخه چشم پوشي ميشود. برخي از سيستمهاي IDS فقط بخش اول ادرس   
  
URL را بررسي مكنند. و لذا يك تقاضاي خطرناك كشف نخواهد شد.   
  
مثال:   
  
GET /thisissaunchofjunktomaketheURLlonger/../cgi-bin/broken.cgi HTTP/1.0   
  
  
  
☻Fake Parameter: URL ارسالي شمامل پرامترهاي است كه هيچ خاصيت يا ضرري ندارد. فقط شكل URL را بگونه اي   
  
تغيير ميدهد تا به الگوي حمله شبيه نباشد. و IDS انرا مجاز بداند.   
  
مثال   
  
GET /index.html?param=/../cgi-bin/broken.cgi HTTP/1.0   
  
  
  
☻TAB Separation: بخشهاي مختلف URL ارسالي بجاي انكه با كاراكتر "فاصله" (SPACE) جدا شده باشند با كاراكتر <tab>   
  
جدا ميشوند. در اين حالت شكل URL بگونهاي تغيير ميكند. تا به الگوي حمله شباهت نداشته باشد و IDS انرا مجاز بداند. ( برخي از   
  
سيستمهاي IDS به اين نحو گمراه ميشوند. و به تقاضا اجازۀ اجرا ميدهند. و برخي ديگر ان را حذف ميكنند.)   
  
مثال   
  
GET<tab>/cgi-bin/broken.cgi<tab>HTTP/1.0   
  
  
  
☻Case Senitvity: برخي از سيستهاي ,IDS انتظار URL را با حروف كوچك دارند و ليكن در تعدادي از سرويس دهندهاي وب ( مثل IIS در ويندوز ) ارسال URL با حروف بزرگو كوچك فرقي نمكندو قابل اجراست. بدين ترتيب سيستم IDS فريب ميخورد و تقاضايارسالي را اجرا ميشود.   
  
مثال :   
  
GET/CGI-BIN/broken.cgi HTTP/1.0   
  
  
  
☻Windows Delimiter: در سيستم عامل ويندوز استفاده از علامت \ به جاي / ( جدا كنندۀ شاخه) مجاز شمرده ميشود در حاليكه برخي از سيستم هاي IDS به ان حساسيت ندارند لذا در مورد شكل URL گمراه ميشوند.   
  
مثال:   
  
GET/cgi-bin\broken.cgi HTTP/1.0   
  
  
  
☻NULL Method: بسياري از سيستهاي IDS براي تحليل رشتۀ URL از توابع رشته اي استفاده ميكنند . حال اگر در بين رشتۀ URL   
  
كاراكتر00 % (NULL Character) وجود داشته باشد توابع رشته اي انرا بعنوان خاتمه رشته تلقي ميكنند. و بدين نحو IDS گمراه ميشود. در حالي كه URL اعتبار خود را از دست نخواخد داد.   
  
مثال:   
  
GET%00 /cgi-bin/broken.cgi HTTP/1.0   
  
  
  
به گونه اي كه خدمت شما عزيزان توضيح دادام . Whisker از روشهاي ساده و قدرتمندي براي مخفي ماندن بهره ميگيرد.   
  
اين نرم افزار در ادرس زير در اختيار عموم قرار گرفته است.   
  
نكته: اين برنامه مبتني بر Perl ميباشد. و روي تمام محيط هاي كه زبان Perlرا پشتيباني ميكنند قابل اجرا ميباشد.   
  
<http://wiretrip.net/rfp/>   
  
  
  
√Exploit Code   
  
  
  
كدهايي كه با ارسال انها به يك پروسۀ سرويس دهنده. انرا مختل كرده و درهم ميشكند و كنترل انرا در اختيار نفوذگر قرار ميدهد. اصطلاحا   
  
Exploit Code ميگويند. برنامه اي مستقلي كه اين كدها را ارسال ميكنند. برنامهاي Exploit ناميده ميشود.   
  
  
  
√ چگونگي استفاده از اكسپوليت .   
  
  
  
كدهاي اكسپلويت براي بكار گيري نيازبه كامپايل شدن دارند. در اينجا شما بايد مقداري با برنامه نويسي اشنا باشيد..بعد از كامپايل كردن اكسپوليت يك خط فرمان يا يك پوشه به نام( read me) به شما داده ميشود. كه دستوراتي را كه ميتوان از ان استفاده كرد را توضيح داده..براي اجراي اكسپلويت شما بايد مسير اكسپوليت كامپايل شده را درcommand سيستم مشخص كنيد و با استفاده از دستورات خود اكسپلويت و آي پي هدف به سايت مورد نظر وصل بشويد.   
  
√نحوه كامپايل كردن اكسپوليت.   
  
اكسپلويت هم مثل همه برنامه اي ديگر با يكي از زبانهاي برنامه نويسي نوشته شده . پس بايد با همان برنامه اي كه نوشته شده كامپايل شود   
  
مانند:Perl-C++-Borland C- و......   
  
.