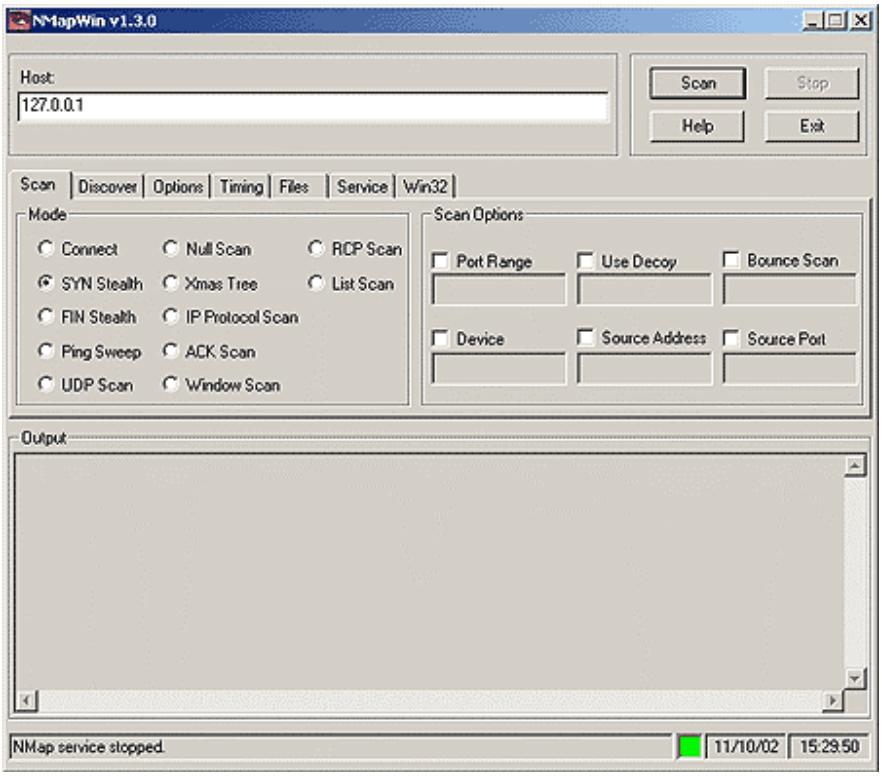
Nmap Scanner

این نرم‌افزار مجموعه ابزارهای footprinting مثل پورت اسکن، آی‌پی اسکن، تشخیص سیستم‌عامل کامپیوتر مورد نظر (OS detection) و ... را گرد هم آورده است. شکل ظاهری برنامه را در زیر می‌بینید:



بررسی ظاهر برنامه

شکل ظاهری برنامه چهار قسمت دارد:

۱- Network Section :
بالاترین قسمت پنجره برنامه است که محلی برای ورود ip یا ip ها دارد به نام Host. بعد از وارد کردن ip و تنظیم کردن پارامترها، دکمه Scan را کلیک می‌کنیم تا کار اسکن شروع شود.
اگر قرار باشد بیش از یک ip وارد شود، این کار را می‌توان به صورت‌های مختلف انجام داد. مثلا: *.*.*.192.130 یعنی تمام ip هایی که با 192.130 شروع می‌شوند ولی دو عدد بعدی هرچیزی می‌تواند باشد. و نوشتن به صورت 192.130.120.12-15 یعنی عدد آخری می‌تواند از ۱۲ تا ۱۵ باشد.

۲- Option Folder :
این قسمت در واقع محل تنظیمات است و به کمک آن مشخص می‌کنیم که از برنامه می‌خواهیم که چه‌کاری انجام دهد که مفصلا در موردش صحبت خواهم کرد. در این قسمت، برگه‌هایی با نامهای Option , Scan , Discover , ... وجود دارد.

۳- Log Output :
محل ظاهر شدن نتایج است. در حالتی که اسکن شروع نشده باشد، خالی است.

۴- Status bar :
پایین‌ترین بخش پنجره برنامه است و دو بخش مهم دارد:

قسمت سمت چپ نشان می‌دهد که اگر بخواهیم در nmap همین کار رو انجام بدیم، چه سویچ‌هایی را باید بکار بریم (دقت کنید که nmap برخلاف NMapWin گرافیکی نیست). هر تغییری که در قسمت Option Folder اعمال کنیم، در این قسمت تغییری را مشاهده می‌کنیم و توصیه می‌کنم که حتما به این قسمت توجه ویژه‌ای داشته باشید.
اما در سمت راست آن، یک مربع کوچک مشاهده می‌شود که می‌تواند به رنگ‌های سبز یا قرمز باشد. سبز یعنی اینکه برنامه آماده برای اجرای دستورات شماست و قرمز یعنی در حال انجام دستورات وارد شده است و فعلا دستور جدید نمی‌پذیرد.

شروع کار با NMapWin

فرض کنید که می‌خواهم سایت far30.com رو می‌خواهم مورد بررسی قرار دهم. برای اینکار ابتدا ip رو بدست آورده (63.148.227.65) و در قسمت Host تایپ می‌کنیم. حالا فعلا بدون اعمال تغییری در قسمت Option Folder ، دکمه Scan رو کلیک می‌کنیم. اسکن شروع می‌شود و بعد از چند دقیقه، نتایج زیر در قسمت Log Output ظاهر می‌شود:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (63.148.227.65):
(The 1583 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
31/tcp     open        msg-auth
53/tcp     open        domain
80/tcp     open        http
110/tcp    open        pop-3
135/tcp    open        loc-srv
143/tcp    open        imap2
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
1026/tcp   open        LSA-or-nterm
1050/tcp   open        java-or-OTGfileshare
1433/tcp   open        ms-sql-s
3372/tcp   open        msdtc
3389/tcp   open        ms-term-serv
6666/tcp   open        irc-serv
7007/tcp   open        afs3-bos
Remote operating system guess: Windows 2000/XP/ME
Nmap .... -- 1 IP address (1 host up) scanned in 156 seconds
```

در همین‌جا سه نوع اطلاعات قابل دسترسی است:
۱- لیست پورت‌های باز روی کامپیوتر سرور و کاربرد آن پورت‌ها
۲- تشخیص سیستم عامل که Windows 2000/XP/ME حدس زده شده است (سطر ماقبل آخر)
۳- و سطر آخر می‌گوید که این ip روشن (up) است.

بررسی برگه Scan از قسمت Option Folder

این برگه خود ۲ بخش دارد:

بخش : Mode
در درس‌های قبلی گفتم که اسکنینگ انواع مختلفی داره، و اینجا جایی است که نوع اسکنینگ رو مشخص می‌کنیم:
- Connect : اسکن از نوع scan TCP connect است که قبلا در درس هفتم درباره‌اش بحث کرده‌ام.
- SYN Stealth : در درس هفتم درباره این هم گفته‌ام. - پیش‌فرض هم همین است
- , FIN Stealth Null Scan , Xmas tree : برای سرورهای غیر از ویندوز کار می‌کنند.
- UDP Scan : برای اسکن کردن پورت‌های udp است.
- Ping Sweep : برای عمل ip scanning است که بدانیم که از بین یک سری ip کدام‌ها فعال هستند.
- List Scan : همان Ping Sweep است ولی به طوری که ip مان لو نرود.
- ACK Scan : معمولا برای تشخیص فایروال‌ها کاربرد دارد.
- Window Scan : همان ACK Scan است ولی کامل‌تر
- RCP Scan : جزو کامل‌ترین حالت‌های اسکنینگ است با اطلاعات فراوان.

بخش : Scan Options
این قسمت شش گزینه دارد که فقط یکی‌شان به درد می‌خوره:
- Port Range : مشخص می‌کند که چه پورت‌هایی باید اسکن شود: اگر خالی بماند، یعنی همه پورت‌ها ، اگر یک عدد نوشته شود یعنی فقط آن پورت و اگر به‌صورت n-m نوشته شود (که n و m عدد هستند) یعنی از پورت n تا پورت m اسکن شود.

بررسی برگه Discover از قسمت Option Folder

این برگه دارای چهار گزینه است:

- TCP Ping : برای بررسی فعال بودن کامپیوتر مورد نظر می‌تواند به‌کار رود.
- ICMP Ping : پینگ فقط از نوع ICMP باشد.
- TCP+ICMP : برای بررسی فایروال‌ها مناسب است (پیش‌فرض)
- Don"t Ping : پینگ نکند.

بررسی برگه Options از قسمت Option Folder

این برگه خود ۲ بخش دارد:

بخش : Options

- Fragmentation : اگر بخواهیم در اسکنینگ‌هایی از نوع Null, Xmas, FIN, SYN تا حدودی تغییرات اعمال کنیم تا حداقل خطر را برای ما داشته باشند، می‌توان این گزینه را انتخاب کرد. ولی باید توجه داشت که گاهی با انتخاب این گزینه اسکنینگ موفقیت آمیز نخواهد بود.
- Get Idented Info : اگر بخواهیم اسکنینگ از نوع connect صورت دهیم، با انتخاب این گزینه گاه اطلاعات ذی‌قیمتی برای ما به ارمغان می‌آورد.
- Resolve All : در حالت پیش‌فرض، این نرم‌افزار روی ip هایی که up هستند، عمل Reverse Whois را انجام می‌دهد (یعنی از روی ip، به دنبال اسم DNS مربوطه می‌گردد). اگر Resolve All را انتخاب کرده باشیم، روی همه ip ها، چه up و چه down عمل Reverse Whois انجام خواهد شد.
- Don"t Resolve : هرگز Whois Reverse نخواهد کرد.
- OS Detection : از جمله مهم‌ترین گزینه‌های این نرم‌افزار است که اگر انتخاب‌شده باشد، برنامه سعی می‌کند که سیستم‌عامل کامپیوتر مقابل را حدس بزند.
- Random Host : به صورت تصادفی ip هایی را تست می‌کند، و هرگز هم به پایان نمی‌رسد.

بخش : Debug

- Debug : اگر مارک شده باشد، نتایج دیباگ مرحله به مرحله در خروجی نشان داده می‌شود.
- Verbose : اگر انتخاب‌شده باشد، پیشرفت کار را نشان می‌دهد.
- Very Verbose : پیشرفت کار را با نهایت جزئیات نشان می‌دهد.

بررسی برگه Timing از قسمت Option Folder
این برگه خود ۲ بخش دارد:

بخش : Throttle

در این بخش هرچه گزینه‌های بالاتر را انتخاب کنید، کار کندتر و دقیق‌تر است و احتمال detection (لو رفتن) شما کمتر است و هرچه پایین تر برعکس. به نظر می‌رسد، Normal بهترین انتخاب باشد.

بخش : Timeouts

- Host Timeout : حداکثر زمانی را مشخص می‌کند که برای یک ip می‌تواند صرف شود.
- Max RTT : حداکثر زمانی را مشخص می‌کند که برای یک probe می‌تواند صرف شود. پیش‌فرض، 9000 است (یعنی ۹ ثانیه)
- Min RTT : برای هر probe حداقل به این اندازه صبر می‌کند.
- Initial RTT : این گزینه خصوصا در ip هایی که فایروال دارند، مفید است.
- Parallelism : اگر در مورد acw_spscan دقت کرده باشید، این برنامه هر بار فقط یک پورت را پروب می‌کند و نه بیشتر (به همین خاطر است که اول اسم آن simple دارد). ولی محصولات واقعی باید همزمان تعدادی پورت را تست کنند. در این قسمت می‌توان حداکثر تعداد پورت‌هایی که می‌تواند همزمان پروب شوند را مشخص می‌کنیم.
- Scan Delay : بین هر اسکن، حداقل به این میزان صبر می‌کند.

بررسی برگه Files از قسمت Option Folder

این برگه خود ۲ بخش دارد:

بخش : Input

برای اینکه روند کارها را سریع‌تر کنیم، می‌توان از این بخش استفاده کرد. در این حالت ورودی از یک فایل خوانده می‌شود.

بخش : Output

این قسمت برای آن است که نتایج را در یک فایل ذخیره کنیم. این فایل می‌تواند به‌صورت Normal (متنی معمولی)، Grep (که الان دیگه به‌کار نمیره)، XML و یا All (هر سه مورد) باشد.

بررسی برگه Service از قسمت Option Folder

فرض کنید می‌خواهید اول هر هفته فلان ip رو تست کنید و کارهایی از این‌دست... این برگه برای همین‌جور کارهاست (میشه گفت یک نوع اتوماسیون)

- بررسی برگه Win32 از قسمت Option Folder

این برگه دو بخش دارد به نام‌های , Commands Options که فقط Options رو بررسی می‌کنم:

- No Pcap : وقتی که NMapWin را نصب می‌کنیم، Pcap هم نصب می‌شود (که فقط روی سیستم‌های ویندوز ۲۰۰۰ و xp می‌تواند نصب شود) و کارها را برعهده می‌گیرد. اگر بخواهیم که از آن استفاده نشود و به‌جای آن از Raw Socket استفاده شود، این گزینه را مارک می‌کنیم.
- No IP HLP Api مثل بالایی فقط اینکه بین ارسال هر پکت، ۱۵ ثانیه منتظر می‌ماند.
- Sockets No Raw : با انتخاب آن Raw Socket به‌کار نمی‌رود.

- Force Raw Socket : باعث می‌شود که فقط Raw Socket به‌کار رود.
- Win Trace : برای سیستم‌های Win32 کمی اطلاعات بیشتری به‌دست می‌دهد.

استفاده از NMapWin برای تعیین نوع سیستم عامل

اگر مهم‌ترین کاربردهای nmap را بخواهیم بدانیم، یکی port scanning و دیگری OS detection (تشخیص سیستم‌عامل مقابل) است که ویژگی دوم به قدری مهم است که گاه nmap را با همین ویژگی می‌شناسند. برای اینکه نوع سیستم‌عامل را تعیین کنیم، باید در برگه Options از NMapWin، گزینه OS detection انتخاب شده باشد.
حالا چند مثال را بررسی می‌کنیم (شما خودتان این ip ها و ip های دیگر را تست و تمرین کنید) :

194.225.184.15
server SP2 Windows 2000 Remote operating system guess:

195.219.176.5
Linux Kernel 2.4.0 - 2.5.20 Remote operating system guess:

206.104.238.208
2.2.20 Linux 2.1.19 - operating system guess: Remote

217.66.199.6
a6)12.2-12.1.5 Cisco router running IOS Remote operating system guess:)

63.148.227.65
Windows 2000/XP/ME Remote operating system guess:

194.225.184.2
If you know what OS is running on it, see) for host No exact OS matches
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
در این مورد می‌بینید که nmap موفق به تعیین نوع سیستم‌عامل نشده است. ممکن است دلیلش این باشد که ip در آن لحظه up نبوده است.

نکته‌ای که باید در نظر داشت این است که گاه باید از یک سری اطلاعات فنی هم استفاده کرد تا به جواب قطعی رسید :
- مثلا ip ماقبل آخر که نتیجه آن به صورت Windows 2000/XP/ME ظاهر شده است، متعلق به sazin.com است که چون یک سایت است و باید در یک سرور باشد و هیچ سروری نمی‌تواند ME یا XP باشد، پس سیستم‌عامل آن Win 2000 خواهد بود.
- یا یک حالت دیگر موردی است که ببینید صفحات یک وب سایت با asp یا asp.net درست شده است (مثلا اسم صفحه به صورت zzzzzz.asp یا zzzzzz.aspx باشد، که نمونه آن سایت far30.com است که اسم همین صفحه default.asp است). در این حالت سرور آن حتما سروری از محصولات مایکروسافت است مثل Win NT و یا Win 2000 و نمی‌تواند Linux یا Unix یا Sun Solaris و... باشد.

چگونه از nmap استفاده کنیم؟

قبلا با نرم‌افزار NMapWin آشنا شدید که نسخه گرافیکی nmap برای ویندوز بود. nmap در واقع نرم‌افزار اصلی است که هم برای یونیکس (لینوکس) و هم برای ویندوز نسخه‌هایی را دارد. nmap برخلاف NMapWin، حالت خط فرمانی (command prompt) دارد. در این قسمت می‌خواهیم با nmap مخصوص ویندوز آشنا شویم. برای داونلود این نرم‌افزار اینجا را کلیک کنید. (اگر قبلا NMapWin را نصب نکرده‌اید، باید از یک نسخه دیگر از nmap که اصطلاحا nmap installer نام دارد، استفاده کنید. این نسخه nmap را می‌توانید از اینجا داونلود کنید.)
همان‌طور که می‌دانید، در نرم‌افزارهای خط فرمانی، باید از پارامترها استفاده کنیم. با توجه به اینکه پارامترهای nmap بسیار زیاد و یادگیری آنها مشکل است، ما برای پیدا کردن پارامترهای درست برای یک عمل خاص (که معمولا scanning ip یا port scanning است) از NMapWin استفاده می‌کنیم. به این ترتیب

که در NMapWin تنظیمات را انجام می‌دهیم و بعد در پایین پنجره آن مشاهده می‌کنید که در قسمت CMD: لیست پارامترها را به دست می‌آوریم. این مراحل را با دو مثال شرح می‌دهم:

۱- می‌خواهیم برای پورت‌های ۱ تا ۲۰۰ در کامپیوتری که ip آن 63.148.227.65 است، یک پورت اسکنینگ انجام دهیم. برای این‌کار در NMapWin، برگه Scan را درحالت SYN Stealth تنظیم می‌کنیم و Port Range را می‌نویسیم: 1-200 و بعد برگه Discover باید در حالت TCP+ICMP باشد و اگر بخواهیم نوع سیستم‌عامل را هم مشخص کنیم، در برگه Options، گزینه OS detection را در حالت انتخاب شده قرار می‌دهیم. ip را هم در بالای پنجره، 63.148.227.65 می‌نویسیم. حالا آماده اسکن هستیم ولی ما می‌خواهیم این کار را با nmap انجام دهیم، پس فقط باید قسمت CMD را از پایین پنجره ببینید، ملاحظه می‌کنید که نوشته شده:

```
CMD: -sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

با حذف کلمه CMD: به عبارت زیر می‌رسیم:

```
-sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

اینها پارامترهایی است که باید در nmap استفاده کنید. به این صورت که می‌نویسید:

```
nmap -sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

و بعد از اجرای دستور و صبر کردن برای چند دقیقه، نتایج را می‌بینیم.
بعد از مدتی که با nmap کار کنید، این پارامترها را می‌آموزید و دیگه نیازی به NMapWin نخواهید داشت.
مثلا همین O- یعنی OS detection، و p 1-200 یعنی پورت‌های ۱ تا ۲۰۰ می‌باشد. بعدها خودتان می‌بینید که کار کردن با nmap بسیار دلچسب‌تر از NMapWin است.

- می‌خواهیم یک ip scanning انجام دهیم برای 195.219.176.0 تا 195.219.176.10 . برای اینکار در NMapWin، در برگه Mode، گزینه Ping Sweep را انتخاب می‌کنیم. در برگه Discovery، گزینه ICMP Ping را انتخاب کرده و در برگه Options، گزینه detection OS را در حالت انتخاب نشده قرار می‌دهیم. برای نوشتن ip ملاحظه می‌فرمایید که 195.219.176 در هر دو مشترک است، پس می‌نویسیم: 195.219.176.0-10 .حالا می‌بینیم که پارامترها به صورت زیر است:

```
-sP -PI -T 3 195.219.176.0-10
```

پس ما می‌نویسیم:

```
nmap -sP -PI -T 3 195.219.176.0-10
```

سیستم عامل هدف را چگونه تشخیص دهیم ؟

يكي از راههايي كه برنامه هاي مانند nmap و ... براي تشخيص نوع سيستم عامل استفاده مي كنند استفاده از فيلد هاي بسته هاي دريافتي مي باشد. يكي از اين فيلد ها كه بسيار استفاده مي شود TTL مي باشد. (TTL فيلد بسيار مهمي در بسته هاي TCP/IP مي باشد)
مثلا هنگامي كه يك سيستم معمولي را ping مي كنيد به شما يك زمان TTL مي دهد. مثلا به دستور زير را مشاهده كنيد :

xxx.xxx.xxx.xxx ping<C:\

ms TTL=128 1>xxx.xxx.xxx.xxx: bytes=32 time Reply from
ms TTL=1281>xxx.xxx.xxx.xxx: bytes=32 time Reply from
ms TTL=1281>xxx.xxx.xxx.xxx: bytes=32 time Reply from
ms TTL=1281>xxx.xxx.xxx.xxx: bytes=32 time Reply from

:127.0.0.1 Ping statistics for
Received = 4, Lost = 0 (0% loss), Packets: Sent = 4,
times in milli-seconds: Approximate round trip
ms,Average = 6 ms12= Minimum =5ms, Maximum

TTL=128 نشان مي دهد كه سيستم عامل هدف ، ويندوز مي باشد. به ليستي كه در زير آمده است توجه كنيد. همانطور كه مشاهده مي كنيد توسط فيلد هاي مشخصي مي توان به سيستم عامل و حتي دقيق تر به نسخه آن پي برد.

```
DF          WINDOW     TTL          PLATFORM     VERSION            OS
TOS
--   --          -------     ---     --- --------   ---------         ------
-
0   n             8192      30     Pyramid/NILE      95-1.1         DC-OSx
0   y         9000-5000     32            Intel       x/NT9        Windows
0   y             8760      54      5.2.2-5.1.2       OnTap         NetApp
0   n         2150-2100     59                    HP_Printer    HPJetDirect
0   y  16100-006016000      60           IBM/RS       x.4.3           AIX
0   n  16100-006016000      60           IBM/RS       x.4.2           AIX
0   y            65535      60             7507        11.2         Cisco
16   y            33580      60            Alpha         4.0    DigitalUnix
16   y            61320      60              SGI        X6.x           IRI
0   n            32756      60         IBM/S390         2.6         OS390
0   n            65534      60   Pyramid/RM1000        5.43       Reliant
16   y            17520      64            Intel         x.3       FreeBSD
0   n         5840-5804     64           J3113A      G.07.x     JetDirect
0   y            32120      64            Intel       x.2.2         Linux
16   n            17520      64            Intel         x.2       OpenBSD
0   y             8192      64          AS/400        R4.4        OS/400
0   n            24820      64          Compaq          R5           SCO
0   y            24820      64      Intel/Sparc           8       Solaris
0   n            32768      64          STRATUS         3.3     FTX(UNIX)
0   n            32768      64        Mainframe           x        Unisys
0   y       32768-32000     128            Intel        4.11       Netware
0   y         9000-5000     128            Intel       x/NT9       Windows
0   y       18000-17000     128            Intel        2000       Windows
n         5000-3800     255             2514        12.0         Cisco
192
0   y             8760     255      Intel/Sparc         x.2       Solaris
```

حتما مي دانيد كه مشخص شدن نوع سيستم عامل چه كمكي به يك هكر مي كند ؟ ولي زياد هم نمي شود به اين روش اعتماد كرد چون بسياري از سيستم عامل ها را مي تواند طوري تنظيم كرد كه فيلد هاي فوق را به صورت دروغين تغيير دهند.