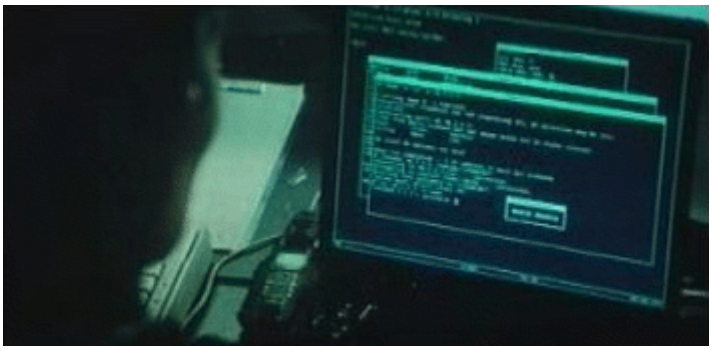
Mengintip Host dengan Tools NMAP

Denny Yerianto
yerianto@yahoo.com
http://www.pemula.com

Pendahuluan

Rangkaian trilogi The Matrix adalah film fiksi ilmiah tentang dunia komputer yang di bintangi aktor Keanu Reeves dimana film ini banyak disukai oleh para penggemar komputer. Jika Anda mencermati film tersebut dengan teliti, Anda akan menemukan adanya sebuah tools hacker sungguhan yang digunakan dalam film tersebut !

Dalam salah satu adegan menjelang akhir film The Matrix: Reloaded, Trinity membobol sistem komputer tenaga listrik darurat menggunakan salah satu tools yang sangat akrab di kalangan hacker: Nmap. Trinity adalah jagoan wanita hacker, yang diperankan Carrie-Ann Moss.



Gambar 1: Adegan pada saat menggunakan Nmap dalam film The Matrix : Reloaded

Penulis skenario ingin mendekatkan film ini sedekat mungkin pada kenyataan. Meskipun versi Nmap yang digunakan dalam film itu agak berbeda dengan versi aslinya, tetapi prinsip membobolnya sama.

Pembuat Nmap, Fyodor, sangat terpukau dengan digunakannya nmap dalam film Hollywood tersebut. Dalam situs Insecure.org, ia menampilkan gambar-gambar adegan saat Trinity menggunakan Nmap *(lihat gambar 1 dan gambar 2)*

Fyodor punya alasan untuk tersanjung, nampaknya Matrix adalah satu-satunya film Hollywood sampai saat ini yang menggunakan metode pembobolan komputer sungguhan. Film-film sebelumnya, seperti *Swordfish* atau *Hackers*, tidak pernah menunjukkan cara sungguhan.

gambar 2: Detail layar Nmap pada monitor di film The Matrix : Reloaded

Cerita di atas mungkin akan memberikan inspirasi bagi Anda untuk mencoba menjadi hacker sungguhan, berani mencoba ? Kami akan tunjukkan beberapa langkah sederhana yang umum dilakukan para hacker. *Namun agar diingat, jangan pernah mencobanya di sistem komputer yang bukan milik Anda sendiri. Tindakan memasuki sistem pihak lain tanpa ijin adalah ilegal dan anda bisa dituntut secara pidana.*

Instalasi Nmap

Nmap yang merupakan singkatan dari Network Mapper merupakan tools para hacker yang digunakan untuk melakukan pemetaan suatu jaringan. Dengan Nmap dapat diketahui, komputer atau host mana yang aktif dan kira-kira dapat di eksploitasi lebih lanjut.

Nmap tersedia di berbagai sistem operasi mulai dari Unix, Linux hingga Windows. Anda dapat mendownload di http://www.nmap.org atau http://www.insecure.org/nmap. Pada tulisan ini kami pergunakan Nmap dengan sistem operasi Windows. Namun demikian kami tidak menggunakan versi grafis melainkan versi text atau *command line*, sehingga instruksi atau c*ommand line* yang sama dapat Anda lakukan pada sistem operasi lainnya seperti Linux, Unix dan keluarganya.

Instalasi Nmap versi windows sangat mudah, yang Anda harus lakukan adalah sebagai berikut:

1. Install Winpcap versi 2.1-beta atau versi yang lebih baru dari http://winpcap.polito.it/, yaitu `WinPcap_3_0.exe` *(versi ketika tulisan ini dibuat)*
2. Reboot
3. Download file program Nmap dari www.nmap.org , yaitu `nmap-3.45-win32.zip` *(versi ketika tulisan ini dibuat)*
4. Unzip file tersebut menggunakan Winzip atau utility dekompresi lainnya. Hasil unzip akan diletakkan di dalam sebuah direktori menggunakan format `nmap-Version,` untuk file zip di atas direktorinya adalah `nmap-3.45` dengan isi sebagai berikut:

```
C:\nmap-3.45> dir

 Volume in drive C is PEMULA
 Volume Serial Number is 2508-15F7
 Directory of C:\nmap-3.45

.              <DIR>        25/09/03 12:06p .
..             <DIR>        25/09/03 12:06p ..
NMAP-O~1           450.903  15/09/03  2:21p nmap-os-fingerprints
NMAP-P~1             8.124  15/09/03  2:21p nmap-protocols
NMAP-RPC            15.985  15/09/03  2:21p nmap-rpc
NMAP-S~1            59.816  15/09/03  2:21p nmap-service-probes
NMAP-S~2           106.088  15/09/03  2:21p nmap-services
NMAP     EXE       336.896  15/09/03  2:21p nmap.exe
NMAP_P~1 REG           372  15/09/03  2:21p nmap_performance.reg
README~1             5.773  15/09/03  2:21p README-WIN32
         8 file(s)        983.957 bytes
         2 dir(s)       3.793.70 MB free

C:\nmap-3.45>
```

Memulai Nmap

Sebelum memulai, sebaiknya Anda perlu mengetahui fasilitas apa yang tersedia dari Nmap. Untuk itu Anda dapat memulai dengan melihat option yang tersedia. Untuk mengetahui option yang tersedia dari Nmap, cukup memanggil Helpnya sebagai berikut:

```
C:\>nmap -h
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)
* -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
C:\
```

Mendeteksi Host yang Aktif

Cara yang paling sederhana untuk mengetahui apakah sebuah komputer atau host aktif atau tidak aktif adalah dengan menggunakan perintah ping sebagai berikut:

```
C:\>ping server1

Pinging server1 [128.1.10.25] with 32 bytes of data:

Reply from 128.1.10.25: bytes=32 time<10ms TTL=128
Reply from 128.1.10.25: bytes=32 time<10ms TTL=128
Reply from 128.1.10.25: bytes=32 time<10ms TTL=128
Reply from 128.1.10.25: bytes=32 time<10ms TTL=128

Ping statistics for 128.1.10.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Hasil reply di atas menunjukkan bahwa host server1 sedang aktif alias tidak mati. Jika hostnya sedang tidak aktif alias mati hasilnya adalah sebagai berikut:

```
C:\>ping 192.168.1.95

Pinging 192.168.1.95 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.95:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Nah yang menjadi masalah adalah bagaimana jika Anda (hacker) ingin mencari tahu apakah ada host yang aktif dalam sebuah network perusahaan tertentu yang terhubung ke internet. Jika network perusahaan tersebut merupakan network kelas C maka jumlah host maksimalnya adalah 256 host. Jadi jika harus menggunakan perintah `ping` satu per satu, berapa kali Anda harus mengetikkan perintah ping tersebut ? Wah, tentu saja membutuhkan waktu yang lama.

Nmap memberikan solusi yang cepat. Misalnya Anda ingin memeriksa apakah ada host yang aktif pada network kelas C dengan nomor IP 192.168.1.1 s/d 192.168.1.10 Maka Anda dapat memeriksa dengan perintah sebagai berikut:

```
C:\> nmap -sP 192.168.1.91-100

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-26 15:40
SE Asia
Standard Time
Host UNYIL (192.168.1.91) appears to be up.
Host USRO (192.168.1.92) appears to be up.
Host UCRIT (192.168.1.93) appears to be up.
Host ABLEH (192.168.1.94) appears to be up.
Host OGAH (192.168.1.96) appears to be up.
Host MELAN (192.168.1.97) appears to be up.
Host PAK_RADEN (192.168.1.98) appears to be up.
```

```
Host ADMINISTRASI (192.168.1.100) appears to be up.
Nmap run completed -- 10 IP addresses (8 hosts up) scanned in 9.880
seconds

C:\>
```

Perhatikan hasil Nmap di atas bahwa dari 10 host yang discan ternyata hanya ditemukan 8 host yang aktif, IP 192.168.1.95 dan IP 192.168.1.99 tidak ditemukan atau tidak aktif atau mungkin memang tidak ada.

Option `–sP` merupakan salah satu type scanning dari Nmap berbasis ICMP, dimana umumnya dipergunakan untuk melakukan `ping` terhadap sejumlah IP sekaligus. Harap diperhatikan bahwa –sP bersifat case sensitive. Jika anda menggunakan –sp maka perintah tersebut tidak dikenal.

Pada umumnya server-server web publik yang baik selalu berada dibelakang firewall, sehingga biasanya proses ping dapat diblokir apabila melewati router atau firewall tersebut, akibatnya Anda tidak dapat mendeteksi apakah server web tersebut aktif atau tidak. Untuk itu diperlukan teknik lainnya untuk memastikan apakah server web tersebut dalam kondisi hidup atau tidak. Perhatikan contoh hasil `ping` pada server web yang berada di belakang firewall berikut ini:

```
C:\>ping webserver

Pinging webserver [128.1.7.13] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 128.1.7.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Nmap dapat dipergunakan untuk menyiasati masalah diatas yaitu dengan melakukan scanning terhadap port yang terbuka dari host target. Jika host yang menjadi target pemeriksaan adalah server web, maka umumnya akan membuka port 80 http. Dengan memanfaatkan port 80, maka Anda dapat mendeteksi apakah host target tersebut dalam keadaan hidup atau mati.

```
C:\> nmap -sP -PT80 128.1.7.13

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-26 16:42
SE Asia
Standard Time
Host webserver (128.1.7.13) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 3.890 seconds

C:\>
```

Option `–PT80` menunjukkan port yang akan dimanfaatkan adalah port 80. Default dari Nmap adalah port 80, jadi sebenarnya Anda dapat mencantumkan –PT saja untuk menunjukkan proses scanning melalui port 80.

Selanjutnya Anda dapat pula menguji coba untuk port umum lainnya. Misalnya jika host yang menjadi target Anda adalah mail maka Anda dapat menguji dengan port 25 (SMTP) atau port 110 (POP3), demikian seterusnya.

Port Scanning

Port scanning adalah proses koneksi ke port-port TCP atau UDP pada host yang menjadi target untuk menentukan service apa yang sedang berjalan (Listening). Dengan mengidentifikasi port-port yang listening ini Anda dapat menentukan jenis aplikasi dan sistem operasi apa yang dipergunakan pada host tersebut. Service yang dalam status listening ini memungkinkan orang yang tidak berhak menerobos ke dalam host tersebut.

Untuk mengetahui port apa saja yang listening dari sebuah host dapat menggunakan cara sebagai berikut:

```
C:\> nmap -sS 128.1.71.103

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (128.1.71.103):
(The 1589 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
17/tcp     open        qotd
19/tcp     open        chargen
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1026/tcp   open        LSA-or-nterm
1031/tcp   open        iad2

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

C:\>
```

Option `–sS` merupakan salah satu type scanning dari Nmap yaitu TCP SYN scan yang dipergunakan untuk mendeteksi port apa saja yang terbuka. Teknik ini sering disebut Half Open scan karena dalam melakukan evaluasi terhadap port tidak membuka hubungan komunikasi TCP/IP secara penuh. Artinya secara teknis komputer yang Anda pergunakan untuk mendeteksi port tersebut akan mengirimkan paket SYN ke host target. Jika SYN|ACK paket dikirim balik, berarti port tersebut tertutup. Setelah memperoleh paket balasan, komputer Anda akan menjawab dengan paket RST untuk me-reset hubungan yang hampir terjadi tersebut (itu sebabnya disebut half Open). Teknik ini hampir tidak terdeteksi oleh host target yang tidak secara maksimal mencatat aktifitas portnya. Istilah kerennya –sS adalah stealth scan atau scan yang tidak terdeteksi.

Untuk melakukan scan port tertentu dapat menggunakan option `–p` sebagai berikut:

```
C:\>nmap -sS -p 21,23,25,53,80,110 adminristek

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-30 14:50 SE
Asia
Standard Time
Interesting ports on adminristek (128.1.9.81):
PORT    STATE  SERVICE
21/tcp  open   ftp
23/tcp  open   telnet
25/tcp  open   smtp
53/tcp  closed domain
80/tcp  open   http
110/tcp closed pop-3

Nmap run completed -- 1 IP address (1 host up) scanned in 1.590 seconds

C:\>
```

Perhatikan bahwa terdapat port 53 yang sedang tidak terbuka alias close.

Lebih Jauh tentang Jenis Port Scanning pada Nmap

Setiap pengelola sistem memiliki strategi pengamanan yang berbeda-beda. Untuk itu cara-cara yang telah dijelaskan di atas mungkin tidak selalu dapat diterapkan. Nmap sendiri memberikan beberapa teknik port scanning untuk menghadapi "medan" tempur yang berbeda-beda. Untuk itu terkadang dibutuhkan latihan dan kreatifitas yang tinggi bagi Anda yang ingin menembus sistem pertahanan lawan tanpa diketahui pemiliknya *(Oops, kami tidak menyarankan apalagi memprovokasi Anda lho).*

Diatas telah diperkenalkan beberapa option dari Nmap yang merupakan teknik scan. Berikut ini teknik scan lanjutan yang dapat Anda manfaatkan sesuai dengan medan tempur yang ada:

a. TCP connect scan -sT
Jenis scan ini terhubung ke port host target dan menyelesaikan three-way handshake (SYN, SYN/ACK dan ACK) Scan ini mudah terdeteksi oleh pengelola host target.

b. TCP SYN Scan -sS
Teknik ini dikenal sebagai *half-opening scanning* karena suatu koneksi penuh tidak sampai terbentuk. Suatu paket SYN dikirimkan ke port host target. Bila SYN/ACK diterima dari port host target, maka Anda dapat mengambil kesimpulan bahwa port tersebut dalam status listening. Jika RST/ACK Anda terima, biasanya menunjukkan bahwa port tersebut tidak listening. Suatu RST/ACK akan dikirim oleh mesin yang melakukan scanning sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat siluman dibandingkan dengan TCP koneksi penuh dan tidak akan tercatat pada log host target.

c. TCP FIN scan –sF
Teknik ini mengirimkan suatu paket FIN ke port host target. Berdasarkan RFC 793, host target akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis Unix.

d. TCP Xmas tree scan -sX
Teknik ini mengirimkan suatu paket FIN, URG dan PUSH ke port host target. Berdasarkan RFC 793, host target akan mengembalikan suatu RST untuk semua port yang tertutup.

e. TCP Null scan -sN
Teknik ini membuat off semua flag. Berdasarkan RFC 793, host target akan mengirim balik suatu RST untuk semua port yang tertutup.

f. TCP ACK scan -sA
Teknik ini digunakan untuk memetakan set aturan firewall. Hal ini sangat membantu Anda dalam menentukan apakah firewall yang dipergunakan adalah *simple packet filter* yang membolehkan hanya koneksi penuh saja (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.

g. TCP Windows scan -sW
Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem-sistem tertentu seperti pada AIX dan Free BSD sehubungan dengan anomali dari ukuran windows TCPnya.

h. TCP RPC Scan -sR
Teknik ini spesifik hanya pada sistem Unix dan digunakan untuk mendeteksi dan mengidentifikasi port RPC dan program serta nomor versi yang berhubungan dengannya

i. UDP Scan -sU
Teknik ini mengirimkan suatu paket UDP ke port host target. Bila port host target memberikan response pesan berupa "ICMP port unreachable" artinya port ini tertutup. Sebaliknya bila tidak menerima pesan tersebut, Anda dapat menyimpulkan bahwa port tersebut terbuka. Karena UDP dikenal sebagai

connectionless protocol, maka akurasi teknik ini sangat bergantung pada banyak hal sehubungan dengan penggunaan jaringan dan sistem reources lainnya.

Apapun teknik port scan yang akan Anda pergunakan, Anda perlu berhati-hati dalam menggunakan terhadap host target. Tindakan Anda melakukan port scanning ke host target yang bukan wewenang Anda dapat saja menimbulkan reaksi yang mungkin tidak Anda duga sebelumnya dari pengelola host target seperti serangan balik, pemblokiran terhadap acount oleh ISP dan sebagainya. Jadi sebaiknya Anda menguji coba pada sistem Anda sendiri.

Mendeteksi Sistem Operasi

Cara klasik mendeteksi sistem operasi host tertentu sebenarnya dapat dilakukan dengan cara menggunakan telnet sebagai berikut:

```
#telnet hpux.u-aizu.ac.jp

Trying 163.143.103.12 ...
Connected to hpux.u-aizu.ac.jp.
Escape character is '^]'.

HP-UX hpux B.10.01 A 9000/715 (ttyp2)

login:
```

Pengelola sistem komputer yang pengalaman tentu saja tidak akan memberikan banner sistem operasi dengan begitu saja dan biasanya fasilitas banner tersebut mereka memodifikasi atau dihilangkan. Jika hal tersebut terjadi, Anda dapat mencoba dengan cara lain misalnya melalui service yang terbuka semisal FTP sebagai berikut:

```
# telnet ftp.netscape.com 21
Trying 207.200.74.26 ...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

Namun demikian, semua yang default sekali lagi biasanya diubah oleh pengelola sistem komputer. Untuk itu maka umumnya para hacker langsung memanfaatkan Nmap !

Untuk mendeteksi sistem operasi dari host target, sebenarnya Anda dapat menganalisa dari hasil port scanning di atas. Apabila Anda menemukan port 139 dan 135 terbuka, maka besar kemungkinan bahwa host target adalah Windows NT. Windows NT umumnya *listen* pada port 135 dan 139. Berbeda dengan listen pada windows 95/98 yang hanya *listen* pada port 139. Aktifnya beberapa port di sistem Unix juga dapat mencirikan jenis sistem operasi tersebut.

Penggunaan option –O diperuntukan untuk mendeteksi jenis sistem operasi, sebagai berikut:

```
C:\> nmap -O ristbook

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on ristbook (128.1.71.103):
(The 1589 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
17/tcp     open        qotd
19/tcp     open        chargen
80/tcp     open        http
```

```
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1026/tcp   open        LSA-or-nterm
1031/tcp   open        iad2
Remote operating system guess: Windows Millennium Edition (Me), Win 2000,
or Win
XP

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

C:\>
```

Berikut ini contoh untuk hasil pada sistem operasi Linux:

```
C:\> nmap -O adminristek

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-26 18:01
SE Asia
Standard Time
Interesting ports on adminristek (128.1.9.81):
(The 1646 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
98/tcp   open  linuxconf
113/tcp  open  auth
139/tcp  open  netbios-ssn
513/tcp  open  login
514/tcp  open  shell
1984/tcp open  bigbrother
Device type: general purpose
Running: Linux 2.1.X|2.2.X
OS details: Linux 2.1.19 - 2.2.25, Linux 2.2.19 on a DEC Alpha

Nmap run completed -- 1 IP address (1 host up) scanned in 12.020 seconds

C:\>
```

Berikut ini contoh untuk hasil pada sebuah Cisco 1750:

```
C:\> nmap -sS -O 128.1.8.5

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-30 15:18
SE Asia
Standard Time
Interesting ports on 128.1.8.5:
(The 1655 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
23/tcp open  telnet
79/tcp open  finger
Device type: router|switch
Running: Cisco IOS 11.X
OS details: Cisco switch/router with IOS 11.1(7)-11.2(8.10), Cisco
Router/Switch
 with IOS 11.2

Nmap run completed -- 1 IP address (1 host up) scanned in 30.160 seconds

C:\>
```

Jika host target hanya membuka port 80 (http), maka kita dapat mensiasati dengan port scanning melalui port tersebut sebagai berikut:

```
C:\>nmap -PT80 -O webserver

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-09-26 18:55
SE Asia
Standard Time
Interesting ports on webserver (128.1.7.13):
(The 1647 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
1433/tcp open  ms-sql-s
1503/tcp open  imtc-mcs
1720/tcp open  H.323/Q.931
3372/tcp open  msdtc
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000
Professional
 or Advanced Server, or Windows XP

Nmap run completed -- 1 IP address (1 host up) scanned in 7.520 seconds

C:\>
```

Penutup

Nmap hanyalah salah satu dari sekian banyak tools hacker yang biasanya dimanfaatkan untuk mengintip host target, karena Nmap sangat fleksibel dalam menghadapi medan dari host target yang mungkin berbeda-beda tingkat pengamanannya. Penguasaan teknik scan dipadu dengan kelengkapan fitur scan pada Nmap menjadi ancaman serius bagi para pengelola sistem komputer.

Bagi pengelola sistem komputer, segala upaya mengintip dari pihak lain yang tidak berwenang perlu diwaspadai.

Referensi

- Fyodor, *"Remote OS Detection via TCP/IP Stack Finger Printing"*, www.insecure.org. , 1999
- Fyodor, *"The art of port scanning"*, www.insecure.org, 1997
- Man Pages, *Nmap versi 3.45.*
- Stuart McClure, Joel Scambray, George Kurtz *"Hacking Exposed: Network Security Secrets and Solutions"*, McGraw-Hill Professional Publishing, 2003.

Biografi Penulis

Denny Yerianto. Lahir di Jakarta 20 Januari 1969. Alumni Ilmu Komputer Universitas Indonesia tahun 1992. Pernah bekerja di sebuah lembaga pasar modal dan saat ini bekerja di Lembaga Perbankan Nasional. Disela-sela kesibukan membangun dan mengelola infrastruktur & security IT di lembaga-lembaga tersebut, masih sempat meng-“oprek” dan menulis untuk beberapa majalah dan situs di internet.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui :
mail: yerianto@yahoo.com
URL: http://www.pemula.com