Att installera och använda nmap

nmap är ett verktyg främst för att scanna det egna lokala nätverket efter öppna portar. Förutom information om vilka portar som är öppna kan information fås om vilket operativsystem som används på datorerna.

Ladda ner och installera nmap

Steg 1: Börja med att ladda ner filen nmap-2_12-1_i386.rpm från http://www.linuxkurser.nu – downloads .

Om du kör någon Microsoft-produkt ladda ner filen till en temporär katalog, för att därefter kopiera filen till en diskett.

I Linux får du sedan montera disketten, för att därefter kopiera ner filen till lämplig katalog. Är du osäker hur du gör för att montera, titta i dokumentet Att montera enheter.

Steg 2: Installera filen eller paketet med kommandot rpm –i nmap-2_12-1_i386.rpm .

```
[root@ /root]# rpm –i nmap-2_12-1_i386.rpm
<ENTER>
```

Använda nmap

Bästa sättet att lära sig hur nmap fungerar är att experimentera med programmet. Nedan följer lite exempel på vad man kan göra. Läs annars manualen, den finns på samma ställe som du hämtade programmet.

Scanna värd efter öppna portar

nmap -F ip.adress – scannar aktuell värd efter öppna portar. (Alt. Nmap –sS ip.adress)

Steg 1: Skriv in följande kommando vid prompten: nmap –F ip.adress, tryck därefter på Enter.

```
[root@ /root]# nmap –F 192.168.10.6
<ENTER>
```

Ger följande resultat:

```
Starting nmap V. 2.12 by Fyodor
(fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.10.6):
Port    State       Protocol  Service
21      open        tcp        ftp
```

```
25      open        tcp        smtp
42      open        tcp        nameserver
53      open        tcp        domain
80      open        tcp        http
81      open        tcp        hosts2-ns
135     open        tcp        loc-srv
139     open        tcp        netbios-ssn
443     open        tcp        https
465     open        tcp        smtps
1080    open        tcp        socks

Nmap run completed -- 1 IP address (1 host
up) scanned in 76 seconds
```

Scanna flera värdar efter öppna portar

nmap -F ip.adress-range – scannar aktuella värdar efter öppna portar.

Steg 1: Skriv in följande kommando vid prompten: nmap –F ip.adress-range tryck därefter på Enter.

```
[root@ /root]# nmap –F 192.168.10.0:255
<ENTER>
```

Ger följande resultat:

```
Starting nmap V. 2.12 by Fyodor
(fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.10.6):
Port    State       Protocol  Service
21      open        tcp        ftp
25      open        tcp        smtp
42      open        tcp        nameserver
53      open        tcp        domain
80      open        tcp        http
81      open        tcp        hosts2-ns
135     open        tcp        loc-srv
139     open        tcp        netbios-ssn
443     open        tcp        https
465     open        tcp        smtps
1080    open        tcp        socks

Interesting ports on  (192.168.10.7):
Port    State       Protocol  Service
139     open        tcp        netbios-ssn

Interesting ports on  (192.168.10.160):
Port    State       Protocol  Service
21      open        tcp        ftp
25      open        tcp        smtp
```

```
42      open        tcp         nameserver
53      open        tcp         domain
80      open        tcp         http
81      open        tcp         hosts2-ns
135     open        tcp         loc-srv
443     open        tcp         https
465     open        tcp         smtps
1080    open        tcp         socks

Nmap run completed -- 256 IP addresses (3
hosts up) scanned in 245 seconds
```

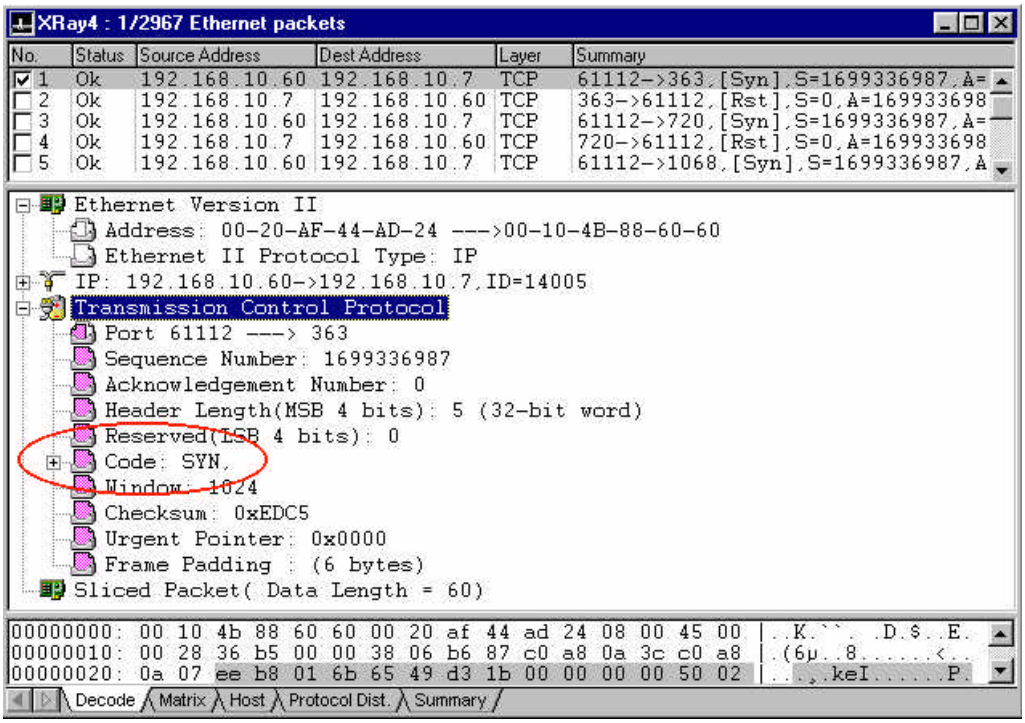
Vad är det som egentligen händer?

Programmet kan använda sig av tre olika typer av portscanning: TCP connect() och scan (-sT) är två typer som vi inte skall använda pga dessa varianter loggas.

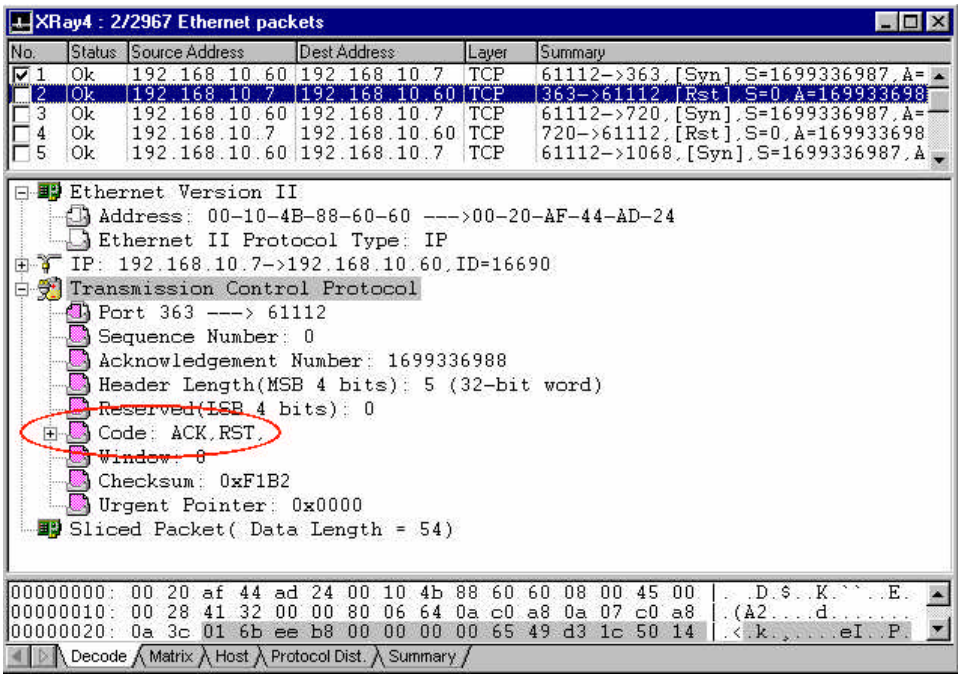
Tredje alternativet är SYN scan, arbetshästen vad det gäller portscanning. Ett annat namn för typen är ”half-open” scan, detta för att den helt enkelt först skickar ett SYN-paket, tittar efter ett svar som kan komma som ett SYN/ACK (öppen) eller RST (stängd). Programmet bryr sig sen inte om att skicka ett ACK som är det normala vid en TCP/IP-handskakning, utan bryter förbindelsen.

Hur ser det ut i protokollanalysatorn?

Som jag skrev, skickar nmap först ett SYN-paket till värd, i detta fallet 192.168.10.7 .



192.168.10.7 svarar med att skicka ett ACK/RST-paket.



Programmet hoppar vidare till nästa, där den gör om samma sak, skickar först ett SYN-paket, för att sedan lyssna efter SYN/ACK eller ACK/RST-paket.

Denna typ av scanning är svårare att upptäcka – TCP-wrappers eller någonting annat utanför kernel kan inte upptäcka det – paket filters som ipfwadm eller en brandvägg kan dock upptäcka aktiviteten. Om en dator använder sig av filtrering kommer NMAP:s syn scan att upptäcka detta och rapportera porten som är filtrerad.

Att ta sig förbi brandvägg

SYN-scan kan kombineras med flaggan (-f), detta för att få en sk ”small fragment scan”. Detta splittrar paketet till två små fragment som ibland kan ta sig förbi och genom en brandvägg utan att det blir upptäckt.

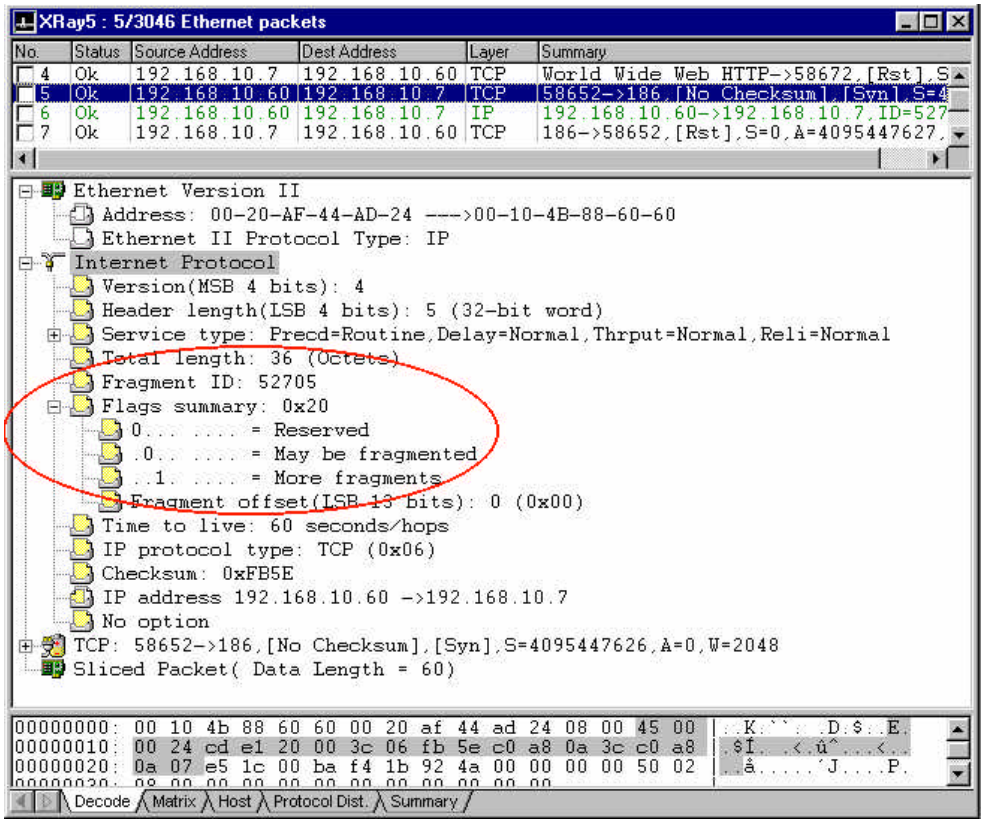
```
[root@ /root]# nmap –Ss –f 192.168.10.6
<ENTER>

Ger följande resultat:

Starting nmap V. 2.12 by Fyodor
(fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.10.7):
Port    State       Protocol  Service
139     open        tcp        netbios-ssn

Nmap run completed -- 1 IP address (1 host
up) scanned in 78 seconds
```

Hur ser det ut i protokollanalysatorn:



Andra lämpliga varianter

Scanna efter portar samt se vilket operativsystem

nmap -O ip.adress – scannar aktuella värdar efter öppna portar och rapporterar op.system.

Steg 1: Skriv in följande kommando vid prompten: nmap –F ip.adress-range tryck därefter på Enter.

```
[root@ /root]# nmap -O 192.168.10.6  <ENTER>
```

Ger följande resultat:

```
Starting nmap V. 2.12 by Fyodor
fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.10.6):
Port    State       Protocol  Service
21      open        tcp        ftp
25      open        tcp        smtp
42      open        tcp        nameserver
53      open        tcp        domain
80      open        tcp        http
```

```
81      open        tcp        hosts2-ns
135     open        tcp        loc-srv
139     open        tcp        netbios-ssn
443     open        tcp        https
465     open        tcp        smtps
1080    open        tcp        socks

TCP Sequence Prediction: Class=trivial time
dependency
       Difficulty=2 (Trivial joke)
Remote operating system guess: Windows NT4 /
Win95 / Win98

Nmap run completed -- 1 IP address (1 host
up) scanned in 79 seconds
```