TECNICHE BASE DI SCANNING

Questa sezione copre le basi della scansione di rete con Nmap. Prima di cominciare è importante capire i concetti seguenti:

- firewall, router, server proxy e altri apparati di sicurezza possono compromettere il risultato della scansione di Nmap. Le informazioni di scansioni remote, quindi che non sono nella nostra rete, possono risultare sbagliate.
- Alcune opzioni richiedono privilegi elevati. Su sistemi Unix e Linux potrebbe esserti richiesto di loggarti come root oppure usare il comando sudo.

Ci sono altri importanti avvertimenti che bisogna prendere in considerazione:

- scansionare reti di cui non si ha il permesso di procedere potrebbe metterti nei guai con il tuo service provider, la polizia, e verosimilmente anche con apparati statali. Non scansionare l'FBI o i Servizi segreti almeno che tu non voglia avere guai ;)
- scansionare aggressivamente alcuni sistemi potrebbe causare il loro crash, rischiando downtime e perdita di dati. Scansiona sistemi critici con cautela!

Cominciamo a scansionare!

Scansionare un singolo target

Lanciare Nmap senza opzioni nella riga di comando, produrrà una scansione base del target, questo può essere specificato sia come indirizzo IP sia come nome host (che Nmap tenterà di risolvere).

Sintassi : nmap [target]

```
$ nmap 192.168.10.1
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 19:38
CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT   STATE   SERVICE
20/tcp closed  ftp-data
21/tcp closed  ftp
80/tcp open    http
Nmap done: 1 IP address (1 host up) scanned in 7.21 seconds
```

Il risultato della scansione ci mostra lo stato delle porte rilevate sul target specificato. La tabella seguente descrive i campi dell'output mostrati dallo scan.

PORT	STATE	SERVICE
Port number/protocol	*Stato della porta*	*Servizio della porta*

Lo scan di default di Nmap controlla le 1000 porte TCP/IP usate più comuni. Le porte che rispondono ad una richiesta sono classificate in uno dei sei stati: aperta, chiusa, filtrata, non filtrata, aperta|filtrata, chiusa|filtrata.

Scansionare target multipli
Nmap può essere utilizzato per scansionare più host allo stesso tempo. Il modo più semplice è quello di specificare gli indirizzi IP o i loro nomi nella riga di comando, separati da uno spazio.

Sintassi : nmap [target1 target2 target3 etc]

```
$ nmap 192.168.10.1 192.168.10.100 192.168.10.101
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 20:30
CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
80/tcp open   http
Interesting ports on 192.168.10.100:
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
Nmap done: 3 IP addresses (2 hosts up) scanned in 6.23
seconds
```

L'esempio sopra indicato dimostra come scansionare tre host allo stesso tempo. Dato che tutti e tre i target sono nella stessa sotto-rete si può utilizzare una scorciatoia **Nmap 192.168.10.1,100,101** per raggiungere lo stesso risultato.

Scansionare un range di IP
Un range di IP può essere utilizzato per specificare un intervallo di più target come dimostrato in questo esempio:

Sintassi: nmap [range di indirizzi IP]

```
$ nmap 192.168.10.1-100
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 20:40
CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
80/tcp open   http
Interesting ports on 192.168.10.100:
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Nmap done: 100 IP addresses (2 hosts up) scanned in 25.84
seconds
```

In questo esempio abbiamo istruito nmap a scansionare un range di IP dal 192.168.10.1 al 192.168.10.100 . Puoi anche usare range per scansionare più reti/sotto reti. Per esempio digitando **nmap 192.168.1-100.*** scansionerà la classe C di IP da 192.168.1.* a 192.168.100.* .
L'asterisco è un carattere "wildcard" che rappresenta tutti gli intervalli validi 0-255

Scansionare l'intera sotto-rete
Nmap può essere utilizzato per scansionare l'intera sotto-rete utilizzando la notazione CIDR (classless inter-domain routing).

Sintassi: nmap [network/CIDR]

```
$ nmap 192.168.10.1/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 20:43
CDT
Interesting ports on 192.168.10.1:
Not shown: 996 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
23/tcp closed telnet
80/tcp open   http
Interesting ports on 192.168.10.100:
Not shown: 995 closed ports
PORT    STATE  SERVICE
22/tcp  open   ssh
111/tcp  open  rpcbind
```

```
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.78
second
```

L'esempio riporta come istruire nmap per scansionare l'intera rete 192.168.10.0 utilizzando la notazione CIDR. Questa notazione consiste nell'indirizzo di rete e la maschera (in bit binari) separati dalla slash.

Scansionare una lista di target
Se avete un ampio numero di sistemi da scansionare, si possono inserire gli indirizzi o i nomi in un file di testo e usare quel testo come input nella linea di comando per Nmap.

```
$ cat list.txt
192.168.10.1
192.168.10.100
192.168.10.101
```

il file list.txt contiene una lista di host che devono essere scansionati. Ogni indirizzo della lista deve essere separato da uno spazio, tab o newline. L'opzione -iL indica ad Nmap di estrarre i target dal file *list.txt.*

Sintassi: nmap -iL [list.txt]

```
$ nmap -iL list.txt
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 19:44
CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
80/tcp open   http
Interesting ports on 192.168.10.100:
Not shown: 995 closed ports
PORT   STATE  SERVICE
22/tcp open   ssh
...
```

il risultato verrà mostrato per ogni host presente nel file.

Scansionare target casuali
L'opzione -iR può essere usate per scansionare un host casuale (random). Nmap genererà casualmente l'indirizzo del target secondo il numero specificato e lo scansionerà.

Sintassi: nmap -iR [numero di target]

```
# nmap -iR 3
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07 23:40
CDT
...
Nmap done: 3 IP addresses (2 hosts up) scanned in 36.91
seconds
```

eseguire **nmap –iR 3** impartisce ad Nmap di generare casualmente 3 indirizzi IP da scansionare. Non ci sono buone ragioni per fare una scansione casuale, almeno che non si lavori in un progetto di ricerca (o si sia veramente annoiato). In più, se si fanno molte scansioni aggressive casuali si potrebbe finire nei guai con il proprio service provider.

Escludere target dallo scan
L'opzione utilizzata è **––exclude**

sintassi: nmap [target] --exclude [target(s)]

```
$ nmap 192.168.10.0/24 --exclude 192.168.10.100
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 20:39
CDT
Interesting ports on 192.168.10.1:
Not shown: 996 filtered ports
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
23/tcp closed telnet
80/tcp open   http
...
```

L'opzione –**exclude** è utile quando si vogliono escludere certi host da un largo numero di target. Nell'esempio l'host 192.168.10.100 è escluso dell'intervallo di indirizzi che sono stati scansionati. L'opzione –exclude accetta singoli hosts, range, o interi blocchi di rete (usando la notazione CIDR) come mostrato nell'esempio:

```
$ nmap 192.168.10.0/24 --exclude 192.168.10.100-105
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 20:39
CDT
...
```

Abbiamo inoltre la possibilità di escludere hosts fornendo ad nmap una lista contenuta in un file. L'opzione da utilizzare in questo caso è **--excludefile**

```
$ cat list.txt
192.168.10.1
192.168.10.12
192.168.10.44
```

sintassi: nmap [targets] --excludefile [list.txt]

```
$ nmap 192.168.10.0/24 --excludefile list.txt
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 20:49
CDT
Interesting ports on 192.168.10.100:
Not shown: 995 closed ports
PORT     STATE  SERVICE
22/tcp   open   ssh
111/tcp  open   rpcbind
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2049/tcp open   nfs
Nmap done: 253 IP addresses (1 host up) scanned in 33.10
second
```

nell'esempio sopra riportato i target presenti in list.txt vengono escludi dallo scan.

Scansioni aggressive

Con l'opzione **-A** Nmap effettuerà una scansione aggressiva.

Sintassi: nmap -A [target]

```
# nmap -A 10.10.1.51
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-10 09:39
CDT
Interesting ports on 10.10.1.51:
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Linksys WAP54G wireless-G router http
config
|_ html-title: 401 Unauthorized
|
http-auth: HTTP Service requires authentication
|_
Auth type: Basic, realm = Linksys WAP54G
MAC Address: 00:12:17:AA:66:28 (Cisco-Linksys)
Device type: general purpose
Running: Linux 2.4.X
```

```
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop
Service Info: Device: WAP
OS and Service detection performed. Please report any
incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds
```

La scansione aggressiva seleziona alcune delle opzioni più comuni di Nmap ed è utilizzata come semplice alternativa all'inserimento di lunghe stringhe di argomenti nella linea di comando. Il parametro **-A** è sinonimo di importanti opzioni avanzate (come **-O -sC --traceroute**) anche se sono accessibili individualmente e verranno trattate dopo.

DISCOVERY OPTIONS

Discovery options overview

Prima di scansionare un target, Nmap proverà ad inviare un ICMP echo request per verificare che l'host sia *"alive"*. Questo può salvare del tempo quando si scansionano più host, se gli host non sono online non si perderà del tempo inutilmente. Dato che le ICMP request sono spesso bloccate dal firewall, Nmap tenterà di connettersi anche alle porte 80 e 443, visto che spesso queste porte sono aperte. Le opzioni *"discovery"* di default non sono utili quando si scansionano sistemi messi in sicurezza. La sezione seguente descrive metodi alternativi che ci permettono di comprendere meglio quali host sono disponibili in rete.

Feature	Opzione
Non pingare	**-PN**
Only ping scan	**-sP**
TCP SYN ping	**-PS**
TCP ACK ping	**-PA**
UDP ping	**-PU**
SCTP INIT ping	**-PY**
ICMP Echo ping	**-PE**
ICMP Timestamp ping	**-PP**
ICMP Address mask ping	**-PM**
IP protocol ping	**-PO**
ARP ping	**-PR**
Traceroute	**--traceroute**
Force reverse DNS resolution	**-R**
Disable reverse DNS resolution	**-n**
Alternative DNS lookup	**--system-dns**
Manually specify DNS server	**--dns-servers**
Crea una lista di host	**-sL**

Non pingare (don't ping)
Di default, prima che Nmap cominci a scansionare le porte aperte di un sistema effettuerà un ping per verificare che questo sia online. Questa feature ci salva del tempo in quanto se non risponde non si procede o si passa al target successivo.

```
$ nmap 10.10.5.11
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 08:43
CDT
Note: Host seems down. If it is really up, but blocking our
ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
```

in questo esempio vediamo che Nmap non ha effettuato la scansione in quanto l'host non ha risposto al suo ping. Specificando l'opzione **-PN** abbiamo impostato Nmap a non effettuare il controllo di default ma di fare una scansione completa delle porte. Questo è utile quando un target è protetto da un firewall che blocca il ping.

Sintassi: nmap -PN [target]

```
$ nmap -PN 10.10.5.11
Starting Nmap 5.00 (http://nmap.org) at 2009-08-13 08:43 CDT
Interesting ports on 10.10.5.11:
Not shown: 999 filtered ports
PORT      STATE   SERVICE
3389/tcp  open    ms-term-serv
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
```

Specificando l'opzione **-PN** sullo stesso target, Nmap è in grado di produrre una lista delle porte aperte su un sistema non pingabile.

Ping only scan
L'opzione **-sP** è usata per effettuare un semplice ping verso i/gli 'host specificato/i.

Sintassi: nmap -sP [target]

```
$ nmap -sP 192.168.10.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 20:54
CDT
Host 192.168.10.1 is up (0.0026s latency).
Host 192.168.10.100 is up (0.00020s latency).
Host 192.168.10.101 is up (0.00026s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.18
second
```

Questa opzione è utile quando si vuole ricercare velocemente all'interno della rete quali host sono online senza attualmente scansionare le porte aperte. Nell'esempio sopra riportato, tutti i 254 indirizzi della sotto-rete 192.168.10.0 sono stati pingati e viene mostrato il risultato degli host *"alive"* .
Quando si scansionano reti locali, si può eseguire Nmap con i privilegi di root in modo da aggiungere funzionalità al ping. Quando eseguito, l'opzione **-sP** effettuerà anche un ARP ping ritornando il MAC address dei sistemi rilevati.

Sintassi: nmap -sP [target]

```
# nmap -sP 192.168.10.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 21:00
CDT
Host 192.168.10.1 is up (0.0037s latency).
MAC Address: 00:16:B6:BE:6D:1D (Cisco-Linksys)
...
```

TCP SYN ping
L'opzione **-PS** eseguirà un ping TCP SYN.

Sintassi: nmap -PS [port1,port2,etc] [target]

```
# nmap -PS scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:31
CDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 995 filtered ports
PORT      STATE   SERVICE
53/tcp    open    domain
70/tcp    closed  gopher
80/tcp    open    http
113/tcp   closed  auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 27.41 seconds
```

Il ping TCP SYN invia un pacchetto SYN al target e si mette in ascolto per la risposta. Questa alternativa di *"discovery"* è utile per quei sistemi che sono configurati per bloccare il ping ICMP standard.
La porta di default per l'opzione **-PS** è l'80, ma si possono specificare altre porte con questa sintassi: **nmap -PS 22,25,80,443,etc**.

TCP ACK ping
L'opzione **-PA** eseguirà un ping TCP ACK sul target specificato.

Sintassi: nmap -PA [port1,port2,etc] [target]

```
# nmap -PA 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:31
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

Anche questa alternativa di *"discovery"* è utile per quei sistemi che sono configurati per bloccare il ping ICMP standard.
La porta di default per l'opzione **-PA** è l'80, ma si possono specificare altre porte con questa sintassi: **nmap -PA 22,25,80,443,etc**.

UDP ping
L'opzione **-PU** eseguirà un ping alle porte UDP nel sistema target.

Sintassi: nmap -PU [port1,port1,etc] [target]

```
# nmap -PU 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:30
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 0.81 second
```

Questo metodo invia pacchetti UDP e sollecita il target ad una risposta.
La maggior parte dei firewall bloccherà questo tipo di connessione, ma alcuni possono essere mal configurati e filtrare solamente le connessioni TCP.
La porta di default per l'opzione **-PU** è 40125. Altre porte possono essere specificate usando la sintassi seguente: **nmap -PU22,25,80,443,etc.**

SCTP INIT ping
Il parametro **-PY** effettuerà il ping SCTP INIT.

Sintassi: nmap -PY [port1,port1,etc] [target]

```
# nmap -PY 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:28
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT      STATE   SERVICE
80/tcp    open    http
443/tcp   open    https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

Questo metodo localizza gli host usando lo "*Stream Control Transmission Protocol*" (SCTP) che solitamente è utilizzato dai sistemi con telefonia basata su IP. La porta di default per l'opzione **-PY** è l'80. Altre porte possono essere specificate con la seguente sintassi: **nmap -PY22,25,80,443,etc.**

ICMP Echo Ping
L'opzione **-PE** esegue un ICMP (*Internet Control Message Protocol*) echo ping sul target specificato.

Sintassi: nmap -PE [target]

```
# nmap -PE 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:26
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT     STATE   SERVICE
80/tcp   open    http
443/tcp  open    https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

L'opzione **-PE** invia un ICMP ping standard verso il sistema target per vedere se risponde. Questo tipo di *"discovery"* lavora meglio nelle reti locali dove i pacchetti ICMP possono essere trasmessi con poche restrizioni. Alcuni internet host, comunque, sono configurati per non rispondere al ping ICMP per questioni di sicurezza. L'opzione **-PE** viene eseguita automaticamente se nessuna altra opzione di ping viene specificata.

ICMP Timestamp Ping
L'opzione **-PP** esegue un ICMP timestamp ping.

Sintassi: nmap -PP [target]

```
# nmap -PP 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:27
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

Mentre la maggior parte dei sistemi con firewall sono configurati per non rispondere o bloccare l'ICMP echo request, quelli mal configurati potrebbero ancora rispondere all'ICMP timestamp request. Questo rende **-PP** utile per sollecitare risposte dai sistemi dietro un firewall.

ICMP Address Mask Ping
L'opzione **-PM** eseguirà un ICMP Address Mask Ping .

Sintassi: nmap -PM [target]

```
# nmap -PM 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:26
CDT
Interesting ports on home (192.168.1.254):
Not shown: 998 closed ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp open   https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

Questa ICMP query non convenzionale (simile alla opzione **-PP**) esegue un ping verso l'host utilizzando un registro ICMP alternativo. Questo tipo di ping a volte riesce a *strisciare* dietro ad un firewall configurato in modo da bloccare le normali echo request.

IP Protocol Ping
L'opzione **–PO** esegue un ping con il protocollo IP.

Sintassi: nmap -PO[protocol1,protocol2,etc] [target]

```
# nmap -PO 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-17 09:38
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT         STATE     SERVICE
21/tcp       open      ftp
22/tcp       open      ssh
25/tcp       open      smtp
80/tcp       open      http
111/tcp      open      rpcbind
2049/tcp     open      nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

un ping con il protocollo IP invia pacchetti al target con il protocollo specificato. Se nessun protocollo viene specificato vengono usati quelli di default 1 (ICMP), 2 (IGMP), 3 (IP-in-IP). Per utilizzare un proprio set di protocolli, questa è la sintassi: **nmap –PO 1,2,4,etc.** La lista completa dei numeri dei Protocolli Internet può essere trovata qui *www.iana.org/assignments/protocol-numbers/*

ARP ping
L'opzione **–PR** viene utilizzata per eseguire un ping ARP (*Address Resolution Protocol -protocollo di risoluzione degli indirizzi-*).

Sintassi: nmap -PR [target]

```
# nmap -PR 192.168.1.254
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:16
CDT
Interesting ports on 192.168.1.254:
Not shown: 998 closed ports
PORT     STATE   SERVICE
80/tcp   open    http
443/tcp  open    https
MAC Address: 00:25:3C:5F:5A:89 (2Wire)
Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

L'opzione -PR viene eseguita automaticamente quando si scansionano reti locali. Questo tipo di "discovery" è molto più veloce rispetto agli altri metodi descritti in

questa guida. Ha in più anche il beneficio di essere molto accurata perchè gli host nella LAN non bloccano le richieste ARP. Le scansioni ARP non possono essere eseguite su target che non risiedono nella nostra rete locale.

Traceroute
Il parametro –Traceroute può essere utilizzato per tracciare il percorso verso l'host specificato.

Sintassi: nmap --traceroute [target]

```
# nmap --traceroute scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-16 13:01
CDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 996 filtered ports
PORT      STATE     SERVICE
53/tcp    open      domain
70/tcp    closed    gopher
80/tcp    open      http
113/tcp   closed    auth
TRACEROUTE (using port 113/tcp)
HOP   RTT  ADDRESS
1  0.91    home (192.168.1.254)
2  24.40   99-60-32-2.lightspeed.wchtks.sbcglobal.net(99.60.32.2)
3  23.12   76.196.172.4
4  22.69   151.164.94.52
5  32.79   ex3-p12-0.eqdltx.sbcglobal.net (69.220.8.53)
6   32.74  asn2828-XO.eqdltx.sbcglobal.net (151.164.249.134)
...
13  74.90  p65-46-255-94.z255-46-65.customer.algx.net (65.46.255.94)
14  75.01  scanme.nmap.org (64.13.134.52)
Nmap done: 1 IP address (1 host up) scanned in 33.72 seconds
```

Le informazioni mostrate sono simili ai comandi Unix/Linux traceroute e tracepath, con in più il vantaggio della superiore funzionalità di Nmap.

Force Reverse DNS Resolution
Il parametro **–R** istruisce Nmap a risolvere sempre gli indirizzi dei target.

Sintassi: nmap -R [target]

```
# nmap -R 64.13.134.52
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 17:22
Central
Daylight Time
```

```
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT        STATE    SERVICE
25/tcp      closed   smtp
53/tcp      open     domain
70/tcp      closed   gopher
80/tcp      open     http
110/tcp     closed   pop3
113/tcp     closed   auth
31337/tcp   closed   Elite
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
```

Di default, Nmap cercherà di fare il DNS reverse solo degli host che sono online. L'opzione **–R** è utile quando si è in fase di ricognizione e abbiamo blocchi di indirizzi, Nmap cercherà di risolvere gli indirizzi IP di ogni target. Le informazioni del reverse DNS possono rivelarsi molto interessanti anche se gli host sono off-line oppure stanno bloccando le investigazioni di Nmap. L'opzione **–R** può ridurre drasticamente la performance dello scan.

Disable Reverse DNS Resolution

L'opzione **–n** viene usata per disabilitare il reverse DNS lookup.

Sintassi: nmap -n [target]

```
# nmap -n 64.13.134.52
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 17:23
Central Daylight Time
Interesting ports on 64.13.134.52:
Not shown: 993 filtered ports
PORT      STATE    SERVICE
25/tcp    closed   smtp
53/tcp    open     domain
70/tcp    closed   gopher
80/tcp    open     http
110/tcp   closed   pop3
113/tcp   closed   auth
31337/tcp closed   Elite
Nmap done: 1 IP address (1 host up) scanned in 8.48 seconds
```

Il reverse DNS rallenta drammaticamente lo scan di Nmap, usando l'opzione **–n** si riduce il tempo di scansione, specialmente quando si deve scansionare un largo numero di host. Questa opzione è utile quando non ci interessano le informazioni del DNS dei sistemi target e si preferisce una scansione che produca un rapido risultato.

Metodo alternativo di DNS lookup
L'opzione –**system-dns** istruisce Nmap ad usare la risoluzione dei DNS del sistema host piuttosto che del proprio metodo interno.

Sintassi: nmap --system-dns [target]

```
$ nmap --system-dns scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-09 21:47
CDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 972 closed ports, 26 filtered ports
PORT     STATE   SERVICE
53/tcp   open    domain
80/tcp   open    http
Nmap done: 1 IP address (1 host up) scanned in 19.86 second
```

Questa opzione è usata raramente in quanto è più lenta del metodo di default. Comunque può essere utile quando si fa del *"troubleshooting"* per problemi di DNS. Questo metodo è usato per le scansioni di IPV6 in quanto Nmap non ha ancora completamente integrato un sistema di risoluzione IPV6 interno.

Specificare manualmente un server DNS
L'opzione –**dns-servers** è usata per aggiungere manualmente un server DNS a cui vengono inoltrate le richieste in fase di scan.

Sintassi: nmap --dns-servers [server1,server2,etc] [target]

```
$ nmap --dns-servers 208.67.222.222,208.67.220.220
scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-09 22:40
CDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 998 closed ports
PORT    STATE  SERVICE
53/tcp  open   domain
80/tcp  open   http
Nmap done: 1 IP address (1 host up) scanned in 32.07 seconds
```

Il comportamento di default di Nmap è quello di utilizzare i server DNS che sono configurati sul nostro sistema. L'opzione **–dns-servers** ci consente di specificare manualmente uno o più server alternativi per quei sistemi che non hanno un DNS configurato oppure quando si vuole evitare che il nostro server logghi il nostro lookup scan. Questa opzione non è attualmente disponibile per le scansioni di IPV6.

Creare una lista di Host
L'opzione **–sL** mostrerà una lista di indirizzi ed eseguirà un DNS lookup degli IP specificati.

Sintassi: nmap -sL [target]

```
$ nmap -sL 10.10.1.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-14 13:56
CDT
Host 10.10.1.0 not scanned
Host router.nmapcookbook.com (10.10.1.1) not scanned
Host server.nmapcookbook.com (10.10.1.2) not scanned
Host 10.10.1.3 not scanned
Host 10.10.1.4 not scanned
Host mylaptop.nmapcookbook.com (10.10.1.5) not scanned
Host 10.10.1.6 not scanned
Host 10.10.1.7 not scanned
Host 10.10.1.8 not scanned
Host mydesktop.nmapcookbook.com (10.10.1.9) not scanned
Host mydesktop2.nmapcookbook.com (10.10.1.10) not scanned
Host 10.10.1.11 not scanned
Host 10.10.1.16 not scanned
Host 10.10.1.17 not scanned
...
```

L'esempio ci mostra il risultato dei nomi DNS per i sistemi specificati. Questa scansione è utile per identificare gli indirizzi IP e il loro nome DNS senza inviare a loro alcun pacchetto. Alcuni nomi DNS possono rivelare interessanti informazioni sugli indirizzi IP incluso il loro utilizzo o la loro locazione.

OPZIONI DI SCANNING AVANZATE

Advanced Scanning Functions Overview

Nmap supporta un certo numero di scansioni selezionabili dall'utente. Di default Nmap effettuerà uno scan TCP base sui sistemi target. In certe situazioni può essere necessario compiere scansioni TCP (o anche UDP) molto più complesse in modo da scovare servizi non comuni o per evadere firewall. Queste scansioni avanzate verranno trattate in questa sessione.

Sommario

Feature	Opzioni
TCP SYN scan	**-sS**
TCP connected scan	**-sT**
UDP scan	**-sU**
TCP NULL scan	**-sN**
TCP FIN scan	**-sF**
Xmas scan	**-sX**
TCP ACK scan	**-sA**
Custom TCP scan	**--scanflags**
IP protocol scan	**-sO**
Send raw Ethernet packets	**--send-eth**
Send IP Packets	**--send-ip**

Alcune delle scansioni presenti in questa sessione necessitano di privilegi di root, quindi è necessario l'utilizzo di sudo o di loggarsi come root per poterle eseguire.

TCP SYN Scan
L'opzione da utilzzare per TCP SYN Scan è -**sS.**

Sintassi: nmap -sS [target]

```
# nmap -sS 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-25 11:01
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT         STATE   SERVICE
21/tcp       open    ftp
22/tcp       open    ssh
25/tcp       open    smtp
80/tcp       open    http
111/tcp      open    rpcbind
2049/tcp     open    nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```

Il TCP SYN scan è l'opzione di default per gli utenti con privilegi elevati (utenti root in unix/linux o gli amministratori in Winz). Il TCP SYN scan tenta di identificare le 1000 porte TCP più comuni inviando pacchetti SYN al target e attendendo la risposta. Questo tipo di scan viene anche chiamato *"stealthy"* (invisibile, nascosto) in quanto non apre completamente la connessione con l'host remoto. Questo previene di essere identificati e loggati come sistemi connessi. L'operazione non è comunque garantita, ormai sistemi e firewall avanzati sono in grado di scovare scansioni TCP SYN.

TCP Connect Scan
L'opzione **–sT** è utilizzata per la TCP Connect Scan .

Sintassi: nmap -sT [target]

```
$ nmap -sT 10.10.1.1
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-31 13:06
CDT
Interesting ports on 10.10.1.1:
Not shown: 998 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

Questa scansione è usata di default per gli utenti non privilegiati. E' usata anche quando si scansionano target IPV6. La TCP Connect scan è una semplice indagine

che consiste nel connettersi direttamente all'host remoto, senza l'utilizzo di alcuna precauzione "stealthy". Di norma è sempre meglio utilizzare Nmap con privilegi di root in modo che si utilizzi la TCP SYN scan, che ci permette di avere risultati più accurati e più velocemente.

UDP Scan
Per scansionare le porte UDP (User Datagram Protocol) si utilizza la flag **-sU**.

Sintassi: nmap -sU [target]

```
# nmap -sU 10.10.1.41
Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-06 21:20
CDT
Interesting ports on 10.10.1.41:
Not shown: 984 closed ports
PORT     STATE             SERVICE
7/udp    open              echo
9/udp    open|filtered     discard
13/udp   open              daytime
19/udp   open               chargen
37/udp   open               time
69/udp   open|filtered     tftp
111/udp  open|filtered     rpcbind
137/udp  open|filtered     netbios-ns
138/udp  open|filtered     netbios-dgm
177/udp  open|filtered     xdmcp
514/udp  open|filtered     syslog
518/udp  open|filtered     ntalk
1028/udp open|filtered     ms-lsa
1030/udp open|filtered     iad1
2049/udp open|filtered     nfs
MAC Address: 00:60:B0:59:B6:14 (Hewlett-Packard CO.)
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

Questo esempio ci mostra il risultato di una scansione delle porte UDP. Mentre il TCP è il protocollo comunemente usato, alcuni servizi (come DNS, DHCP, SNMP) utilizzano ancora l'UDP. Quando dobbiamo condurre un audit sulla rete è sempre una buona idea controllare sia i servizi TCP che UDP in modo da ottenere una più completa comprensione del host/network target.

TCP NULL Scan
L'opzione -sN opera una TCP NULL Scan .

Sintassi: nmap -sN [target]

```
# nmap -sN 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-01 13:19
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE             SERVICE
21/tcp   open|filtered     ftp
22/tcp   open|filtered     ssh
25/tcp   open|filtered     smtp
80/tcp   open|filtered     http
111/tcp  open|filtered     rpcbind
2049/tcp open|filtered     nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Questa scansione viene eseguita da Nmap inviando pacchetti con la flag TCP impostata a 0 nell'header. Inviare un pacchetto NULL ad un target è un metodo valido per raggirare il firewall e generare una risposta. Purtroppo non tutti i sistemi risponderanno a questa richiesta.

TCP FIN Scan
L'opzione da utilizzare è la **–sF.**

Sintassi: nmap -sF [target]

```
# nmap -sF 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-01 13:21
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE             SERVICE
21/tcp   open|filtered     ftp
22/tcp   open|filtered     ssh
25/tcp   open|filtered     smtp
80/tcp   open|filtered     http
111/tcp  open|filtered     rpcbind
2049/tcp open|filtered     nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Nella scansione TCP FIN nmap setta il bit TCP FIN come attivo nel tentativo di

sollecitare una risposta TCP ACK dal sistema target. Questo è un altro metodo per l'invio di pacchetti che il target non si aspetterebbe nello sforzo di produrre un risultato sul target protetto da firewall, anche in questo caso non tutti i sistemi potrebbero rispondere alla richiesta.

Xmas Scan
Opzione **–sX.**

Sintassi: nmap -sX [target]

```
# nmap -sX 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-01 13:34
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
25/tcp   open|filtered smtp
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
2049/tcp open|filtered nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

Con questa scansione Nmap invierà pacchetti con le flag URG, FIN e PSH attive, questo ha l'effetto di *"illuminare i pacchetti come alberi di natale"* e può essere usato per ottenere risposte da un sistema protetto da firewall. Non tutti i sistemi potrebbero rispondere a questa richiesta.

Custom TCP Scan
L'opzione –**scanflags** è usata per effettuare una scansione TCP personalizzata.
Sintassi: nmap --scanflags [flag(s)] [target]

```
# nmap --scanflags SYNURG 10.10.1.127
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-12 14:53
CST
Interesting ports on 10.10.1.127:
Not shown: 996 filtered ports
PORT     STATE    SERVICE
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
3389/tcp closed   ms-term-serv
5900/tcp open     vnc
MAC Address: 00:14:22:59:3D:DE (Dell)
Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

L'opzione –**scanflags** concede all'utente di definire la propria flag TCP da inserire nell'header. Può essere utilizzata ogni combinazione di flag listate nella tabella che segue, per esempio nmap –scanflags FINACK (senza spazzi) attiverà sia la flag tcp FIN sia la flag tcp ACK.

Flag	Utilizzo
SYN	Sincronizza
ACK	Acknowledgment
PSH	Push
URG	Urgente
RST	Reset
FIN	Fine

TCP ACK Scan
Opzione da utilizzare **–sA.**

Sintassi: nmap -sA [target]

```
# nmap -sA 10.10.1.70
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-18 10:33
CST
Interesting ports on 10.10.1.70:
Not shown: 994 filtered ports
PORT          STATE         SERVICE
139/tcp       unfiltered    netbios-ssn
445/tcp       unfiltered    microsoft-ds
2967/tcp      unfiltered    symantec-av
5900/tcp      unfiltered    vnc
19283/tcp     unfiltered    unknown
19315/tcp     unfiltered    unknown
MAC Address: 00:0C:F1:A6:1F:16 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 5.33 seconds
```

L'opzione **–sA** può essere usata per stabilire se un sistema è protetto da un firewall. Quando si compie uno scan TCP ACK, Nmap interrogherà il target in attesa di una risposta RST. Se non riceve nessuna risposta il sistema è considerato *"filtrato"* o *"filtered"*. Se viene ricevuto il pacchetto RST, allora viene etichettato come *"non filtrato"* o *"unfiltered"*. Nell'esempio precedente 994 porte sono etichettate come *"filtered"* il che significa probabilmente che il sistema è protetto da un firewall. Le 6 porte *"unfiltered"* hanno una configurazione nel firewall che le

consentono di essere abilitate come aperte o chiuse. L'opzione **–sA** non ci indica se le porte *"unfiltered"* sono aperte oppure chiuse, l'unico scopo di questa opzione è quello di determinare se il sistema le sta filtrando oppure no.

IP Protocol Scan

Opzione **–sO .**

Sintassi: nmap -sO [target]

```
# nmap -sO 10.10.1.41
Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-06 21:32
CDT
Interesting protocols on 10.10.1.41:
Not shown: 253 open|filtered protocols
PROTOCOL STATE    SERVICE
1        open     icmp
6        open     tcp
17       open     udp
MAC Address: 00:60:B0:59:B6:14 (Hewlett-Packard CO.)
Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
```

L' IP protocol scan ci mostra quali protocolli IP sono supportati sul sistema target. I protocolli più comuni che si riscontrano nelle reti moderne sono ICMP, TCP e UDP come viene anche mostrato nell'esempio. Usando l'opzione -**sO** si può determinare velocemente che tipo di scansione si deve effettuare sul target basandosi sui protocolli supportati. Una lista completa dei protocolli IP può essere trovata sul sito della IANA all'indirizzo *www.iana.org/assignments/protocol-numbers/*.

Send Raw Ethernet Packets

L'opzione **–send–eth** viene usata per inviare pacchetti ethernet puri mentre si scansiona un sistema.

Sintassi: nmap --send-eth [target]

```
$ nmap --send-eth 10.10.1.51
Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-01 14:19
CDT
Interesting ports on 10.10.1.51:
Not shown: 997 closed ports
PORT      STATE   SERVICE
80/tcp    open    http
443/tcp   open    https
49152/tcp open    unknown
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Abilitando questa opzione consentiamo ad Nmap di bypassare l'IP layer nel nostro sistema e di inviare direttamente pacchetti ethernet puri nel data link layer. Questa può essere usata per superare problemi nello stack IP del nostro sistema. L'argomento **–sent–eth** è automaticamente selezionato da Nmap quando necessario, quindi è raro che si debba usare come argomento nella linea di comando.

Send IP Packets
L'opzione **–send–ip** si usa per inviare pacchetti IP mentre si sta scansionando.

Sintassi: nmap --send-ip [target]

```
$ nmap --send-ip 10.10.1.51
Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-01 14:15
CDT
Interesting ports on 10.10.1.51:
Not shown: 997 closed ports
PORT      STATE   SERVICE
80/tcp    open    http
443/tcp   open    https
49152/tcp open    unknown
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Abilitando questa opzione si forza Nmap ad utilizzare lo stack IP del sistema locale invece che generare pacchetti ethernet puri. L'argomento **–sent–ip** è automaticamente selezionato da Nmap quando necessario, quindi è raro che si debba usare come argomento nella linea di comando.

OPZIONI DI PORT SCANNING

Port Scanning Options Overview

In totale ci sono 131070 porte TCP/IP (65,535 TCP and 65,535 UDP). Di default Nmap ne scansiona solo 1000, quelle maggiormente utilizzate, questo viene fatto per risparmiare tempo. Capita a volte che si voglia scansionare fuori dall'intervallo standard alla ricerca di servizi insoliti oppure porte che sono state "forwardate" in posizioni differenti dalla standard. La lista completa delle porte TCP/IP possono essere trovate sul sito della IANA all'indirizzo *www.iana.org/assignments/protocol-numbers/*.

Sommario:

Feature	Opzione
Scansione rapida	**-F**
Scansione Porta specifica	**-p [porta]**
Scansione Porta dal nome	**-p [nome]**
Scansione Porta dal protocollo	**-p U: [porta], T: [porta]**
Scansione tutte le porte	**-p "*"**
Scansione porte principali	**--top-ports [porta]**
Scansione sequenziale delle porte	**-r**

Scansione rapida (fast scan)
Con l'opzione **-F** si scansionano le 100 porte comuni più usate.

Sintassi: nmap -F [target]

```
$ nmap -F 10.10.1.44
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 10:13
CDT
Interesting ports on 10.10.1.44:
Not shown: 91 closed ports
PORT     STATE    SERVICE
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
3389/tcp open     ms-term-serv
8000/tcp open     http-alt
10000/tcp open snet-sensor-mgmt
Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
```

Nmap normalmente scansionerebbe le 1000 porte più usate. Con l'opzione **-F** si riduce il numero a 100. Questa ha il solo scopo di ridurre il tempo di scansione senza tralasciare le porte maggiormente usate.

Scansione di una porta specifica
L'opzione per specificare una porta è **-p.**

Sintassi: nmap -p [port] [target]

```
$ nmap -p 80 10.10.1.44
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 10:10
CDT
Interesting ports on 10.10.1.44:
PORT     STATE    SERVICE
80/tcp   open     http
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

L'esempio dimostra come scansionare solo la porta 80. Possiamo estendere la scansione a più porte semplicemente separandole con una virgola.

Sintassi: nmap -p [porta1,porta2,etc|range porte] [target]

```
$ nmap -p 25,53,80-200 10.10.1.44
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 10:10
CDT
Interesting ports on 10.10.1.44:
Not shown: 118 closed ports
PORT     STATE    SERVICE
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

In questo esempio l'opzione **-p** viene usata per scansionare le porte 25, 53 e dall'80 al 200.

Scansionare le porte dal nome
L'opzione è ancora **-p**.

Sintassi: nmap -p [nome porta] [target]

```
$ nmap -p smtp,http 10.10.1.44
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-17 10:37
CDT
Interesting ports on 10.10.1.44:
PORT     STATE    SERVICE
25/tcp   open     smtp
80/tcp   open     http
8008/tcp closed   http
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

L'esempio ci mostra come ricercare le porte aperte SMTP e HTTP specificandone il nome usando l'opzione **-p.** I nomi devono coincidere con i servizi specificati nel file nmap-service. Questo file solitamente si trova in ***/usr/local/share/nmap/*** nei sitemi unix/linux o in ***C:\Program Files\Nmap*** in Windows . Quando si specifica un nome possiamo ricorrere all'utilizzo della wildcards. Per esempio eseguendo **nmap -p "http*" 10.10.1.44** verranno scansionate tutte le porte che iniziano con http (incluso http e https). Il nome con la wildcards deve essere racchiuso in "" (virgolette) in modo che non venga interpretata come una wildcard della shell.

Scansione delle porte dal protocollo
Ancora l'opzione **-p** seguita da **T**: o **O:** ci consente di specificare porte e protocolli.

Sintassi: nmap -p U: [UDP porta],T:[TCP porta] [target]

```
# nmap -sU -sT -p U:53,T:25 10.10.1.44
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-18 12:52
CDT
Interesting ports on 10.10.1.44:
PORT     STATE    SERVICE
25/tcp   open     smtp
53/udp   open     domain
MAC Address: 00:14:22:0F:3C:0E (Dell)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Usando la sintassi **-p U:53,T:25** Nmap eseguirà una scansione sulla porta 53 UDP e sulla 25 TCP. Di default Nmap esegue scansioni solo sulle porte TCP. In modo da eseguire scansioni sia sulle UDP che sulle TCP dobbiamo abilitare altri tipi di scansione come **-sU** e **-sT**.

Scansionare tutte le porte
Per poter scansionare tutte le 65.535 porte TCP/IP si utilizza ancora l'opzione **-p** seguita dalla wildcard **"*".**

Sintassi: nmap -p "*" [target]

```
# nmap -p "*" 10.10.1.41
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-16 14:07
Central
Standard Time
Interesting ports on 10.10.1.41:
Not shown: 4204 closed ports
PORT     STATE    SERVICE
7/tcp    open     echo
9/tcp    open     discard
13/tcp   open     daytime
19/tcp   open     chargen
21/tcp   open     ftp
23/tcp   open     telnet
25/tcp   open     smtp
37/tcp   open     time
111/tcp  open     rpcbind
113/tcp  open     auth
139/tcp  open     netbios-ssn
512/tcp  open     exec
```

```
513/tcp  open     login
514/tcp  open     shell
515/tcp  open     printer
543/tcp  open     klogin
...
```

La wildcards deve essere racchiusa in "" (virgolette) in modo che non venga interpretata come una wildcard della shell.

Scansione porte principali (Scan Top Ports)
Opzione: **--top-ports.**

Sintassi: nmap --top-ports [number] [target]

```
# nmap --top-ports 10 10.10.1.41
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-15 13:46
CST
Interesting ports on 10.10.1.41:
PORT     STATE    SERVICE
21/tcp   open         ftp
22/tcp   closed   ssh
23/tcp   open     telnet
25/tcp   open     smtp
80/tcp   closed   http
110/tcp  closed   pop3
139/tcp  open     netbios-ssn
443/tcp  closed   https
445/tcp  closed   microsoft-ds
3389/tcp closed   ms-term-serv
MAC Address: 00:60:B0:59:B6:14 (Hewlett-packard CO.)
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Di default, Nmap scansiona le 1000 porte più usate comunemente, l'opzione -F le riduce a 100 mentre con l'opzione **–top-ports** possiamo specificare qualsiasi numero delle porte più "importanti". In questo esempio vediamo come Nmap viene impostato per scansionare le 10 porte più importanti, comunque possiamo usare qualsiasi numero. Per esempio nmap **--top-ports 500** scansionerà le 500 porte più importanti oppure nmap **--top-ports 5000** scansionerà le 5000 porte più importanti.

Port scan sequenziale
L'opzione da utilizzare è **–r.**

Sintassi: nmap -r [target]

```
$ nmap -r 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 13:02
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
2049/tcp open     nfs
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

L'algoritmo usato da Nmap per generare casualmente le porte da scansionare consente di evadere il firewall o i sistemi di prevenzione delle intrusioni. Il parametro **–r** sovrascrive questa funzionalità e istruisce Nmap di ricercare in ordine numerico le porte aperte. In combinazione con l'opzione **–v** verrà mostrato in tempo reale la scoperta sequenziale delle porte aperte.

RILEVAMENTO DEI SISTEMI OPERATIVI E DEI SERVIZI

Version Detection Overview

Una delle più famose e utili abilità di Nmap è quella si saper determinare il sistema operativo e i servizi presenti sul target remoto. Questa funzione analizza le risposte del sistema scansionato riuscendo così a determinare sia il sistema operativo sia i servizi installati sull'host target. Il processo di identificazione del sistema operativo e della versione dei servizi viene chiamato TCP/IP fingerprinting (*impronta digitale)*. Questa però non è una scienza esatta, gli sviluppatori di Nmap hanno molta cura per questa "feature" cercando di renderla sempre più precisa e accurata. Come altre opzioni di Nmap anche il fingerprinting può essere controllato dall'utente usando array di argomenti che verranno trattati in questa sessione.

Sommario

Feature	Opzione
Determinare il sistema operativo	**-O**
Ipotizzare l' OS	**--osscan-guess**
Determinare la versione del servizio	**-sV**
RPC Scan	**--version-trace**
Troubleshooting Version Scans	**-sR**

Determinare il sistema operativo
Opzione da utilizzare **–O**.

Sintassi: nmap -O [target]

```
# nmap -O 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-11 13:09
Central
Daylight Time
...
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.28
Network Distance: 1 hop
...
```

Come dimostrato in questo esempio Nmap (in molti casi) è in grado di identificare il sistema operativo dei target remoti. Questa operazione consiste nell'analizzare le risposte del target e confrontarle con delle caratteriste note, in questo modo viene identificato il sistema operativo del target remoto. In modo che l'identificazione del sistema operativo funzioni bene ci devono essere almeno una porta aperta e una porta chiusa sul sistema target. Quando si scansionano target multipli l'opzione **–osscan-limit** può essere combinata con l'opzione **–O** in modo che Nmap non scansioni il SO di host che non rientrano in questi criteri. Anche l'opzione **–v** può essere combinata con **–O** per avere più informazioni.

SottoporreTCP/IP Fingerprints
Se Nmap non è in grado di determinare il SO del target, ci proporrà il fingerprinting da aggiungere al DataBase presente a questo indirizzo: www.nmap.org/submit/ .
L'esempio seguente dimosta l'output di Nmap in questo scenario:

```
# nmap -O 10.10.1.11
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-16 14:16
Central
Standard Time
...
No exact OS matches for host (If you know what OS is running
on it,
see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.00%D=12/16%OT=3001%CT=1%CU=32781%PV=Y%DS=1%G=Y
%M=00204A%TM=4B29                    OS:4048%P=i686-pc-windows-
windows)SEQ(CI=III=ITS=U)OPS(O1=M400%O2=%O3=%O4       OS:=%O5=
%O6=)OPS(O1=M400%O2=M400%O3=%O4=%O5=%O6=)OPS(O1=
```

```
%O2=M400%O3=M400%O4   OS:=%O5=%O6=)OPS(O1=%O2=%O3=M400%O4=%O5=
%O6=)OPS(O1=M400%O2=%O3=M400%O4=%O5        OS:=%O6=)WIN(W1=7FF
%W2=0%W3=0%W4=0%W5=0%W6=0)WIN(W1=7FF%W2=7FF%W3=0%W4=0%W5
OS:=0%W6=0)WIN(W1=0%W2=7FF
%W3=7FFW4=0%W5=0%W6=0)WIN(W1=0%W2=0%W3=7FF%W4=0%
OS:W5=0%W6=0)WIN(W1=7FF%W2=0%W3=7FF%W4=0%W5=0%W6=0)ECN(R=Y
%DF=Y%T=40%W=0%O=   OS:%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=O%A=O      OS:%F=AS%RD=0%Q=)T1(R=Y
%DF=Y%T=40%S=Z%A=S+%F=AR%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=  OS:0%S=Z
%A=S+%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
%RD=0%Q=                OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=             OS:S+%F=AR%O=
%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y
%DF        OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=Y
%T=40%IPL=38%UN=0%RIPL=G              OS:%RID=G%RIPCK=G%RUCK=G
%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)
...
```

Sottoponendo il fingerprinting generato e identificato correttamente il SO del target si può migliorare l'accuratezza dell'identificazione dei SO nei prossimi rilasci di Nmap.

Ipotizzare un sistema operativo sconosciuto

Se Nmap non è in grado di determinare il SO con accurata certezza, possiamo forzare di ipotizzare quale sia utilizzando l'opzione **–osscan-guess.**

Sintassi: nmap -O --osscan-guess [target]

```
# nmap -O --osscan-guess 10.10.1.11
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-17 13:25
CDT
Interesting ports on 10.10.1.11:
Not shown: 999 closed ports
PORT     STATE    SERVICE
3001/tcp open     nessus
MAC Address: 00:20:4A:69:FD:94 (Pronet Gmbh)
Aggressive OS guesses: Enerdis Enerium 200 energy monitoring
device or Mitsubishi XD1000 projector (96%), Lantronix UDS200
external serial device server (96%), Lantronix Xport-03
embedded serial device server (firmware 6.1.0.3) (95%), Larus
54580 NTP server (95%), Lantronix Evolution OS (93%),
Lantronix UDS1100 external serial device server (92%),
Lantronix XPort embedded Ethernet device server (90%),
Stonewater Control Systems environmental monitoring appliance
(88%), FreeBSD 6.3-PRERELEASE (88%), Crestron MC2E, MP2E,
PRO2, or QM-RMC control and automation system (2-Series)
```

```
(87%)
...
```

In questo esempio viene mostrato una lista di possibili SO del target. Ogni possibilità è listata con una percentuale di confidenza. L'opzione **—fuzzy** è un sinonimo che può essere usato come scorciatoia più semplice da ricordare.

Determinare la versione di un servizio
Per determinare la versione di un servizio si usa l'opzione **-sV.**

Sintassi: nmap -sV [target]

```
# nmap -sV 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-11 12:49
Central Daylight Time
Interesting ports on 10.10.1.48:
Not shown: 996 closed ports
PORT STATE  SERVICE    VERSION
21/tcp open ftp        vsftpd 2.0.6
22/tcp open ssh        OpenSSH 4.7p1 Debian (protocol 2.0)
25/tcp open smtp       Postfix smtpd
80/tcp open http       Apache httpd 2.2.8 ((Ubuntu))
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Service Info: Host: 10.10.1.48; OSs: Unix, Linux

Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.33 seconds
```

L'opzione **-sV** tenterà di identificare il produttore e la versione del software di ogni porta aperta scovata. Il risultato mostra il produttore e la versione dei servizi che Nmap è stato in grado di identificare. L'identificazione delle versioni viene evitata di proposito per alcune porte considerate "problematiche" (9100-9107). Questo può essere evitato combinando l'opzione **-sV** con l'opzione **—allports** istruendo Nmap a non escludere nessuna porta.

Troubleshooting Version Scans
--version-trace è un'opzione che può essere abilitata per mostrare i dettagli della scansione attiva.

Sintassi: nmap -sV --version-trace [target]

```
$ nmap -sV --version-trace 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 13:16
CDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0,
SCTP:0)
-------------- Timing report --------------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-------------------------------------------
NSE: Loaded 3 scripts for scanning.
Overall sending rates: 319.95 packets / s.
Increased max_successful_tryno for 10.10.1.48 to 1 (packet
drop)
Overall sending rates: 756.69 packets / s.
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:21
(IOD #1) EID 8
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:22
(IOD #2) EID 16
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:25
(IOD #3) EID 24
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:80
(IOD #4) EID 32
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:111
(IOD #5) EID 40
NSOCK (1.6000s) TCP connection requested to 10.10.1.48:2049
(IOD #6) EID 48
NSOCK (1.6000s) nsock_loop() started (no timeout). 6 events
pending
NSOCK (1.6010s) Callback: CONNECT SUCCESS for EID 8
[10.10.1.48:21]
...
```

L'opzione **–version-trace** può essere utilie per debuggare problemi o per guadagnare informazioni aggiuntive sul sistema target. Per maggiori informazioni sul troubleshooting e debugging guardare la sezione 10.

Scansione RPC
Per effettuare una scansione RPC (Remote Procedure Call) sul nostro target utilizzare l'opzione **–sR.**

Sintassi: nmap -sR [target]

```
$ nmap -sR 10.10.1.176
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 14:22
Central Daylight Time
Interesting ports on 10.10.1.176:
Not shown: 995 closed ports
PORT     STATE    SERVICE                VERSION
22/tcp   open     ssh
111/tcp  open     rpcbind (rpcbind V2)   2 (rpc #100000)
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
2049/tcp open     nfs (nfs V2-4)         2-4 (rpc #100003)
MAC Address: 00:16:EA:F0:92:50 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
```

L'output della scansione con -sR ci mostra le informazioni a proposito del servizio RPC in esecuzione sul sistema target. RPC è comunemente associato ai sistemi unix/linux specialmente per il servizio NFS (Network File System) . In questo esempio NFS versione 2 del servizio RPC è stata scovata sulle porte 111 e 2049.

OPZIONI DI TIMING

Timing Options Overview

Alcune opzioni di Nmap possono essere configurate anche sotto un profilo che riguarda il tempo. Queste opzioni di timing posso essere usate per velocizzare o rallentare la scansione in accordo con le nostre necessità. Quando si scansionano un largo numero di host in una rete veloce possiamo desiderare di aumentare il numero di operazioni parallele per avere risultati più veloci. In alternativa quando si scansionano reti poco veloci o attraverso internet, possiamo aver bisogno di rallentare la scansione in modo da avere risultati migliori o per evadere gli IDS. Questa sessione tratta delle opzioni disponibili per il timing.

Sommario

Feature	Opzione
Timing Templates	**-T[0-5]**
Settaggio pacchetto TTL	**--ttl**
Operazioni parallele minimo	**--min-parallelism**
Operazioni parallele massime	**--max-parallelism**
Grandezza min gruppo host	**--min-hostgroup**
Grandezza max gruppo host	**--max-hostgroup**
Max RTT timeout	**--max-rtt-timeout**
Timeout RTT iniziale	**--initial-rtt-timeout**
Tentativi max	**--max-retries**
Host timeout	**--host-timeout**
Ritardo min scansione	**--scan-delay**
Ritardo max scansione	**--max-scan-delay**
Rate min pacchetti	**--min-rate**
Rate max pacchetti	**--max-rate**
Defeat Reset Rate Limits	**--defeat-rst-ratelimit**

Parametri di timing
Nmap accetta i parametri di timing in millisecondi. Ma si possono anche specificare i parametri in secondi, minuti, ore semplicemente aggiungendo un qualificatore dopo il parametro di timing. Questa tabella mostra esempi di sintassi.

Parametri	Definizione	Esempio	significato
Nessuno	Millisecondi	500	500 millisecondi
s	Secondi	300s	300 secondi
m	Minuti	5m	5 minuti
h	Ore	1h	1 ora

Esempio: --host-timeout è l'opzione utilizzata per specificare il timing. Per impostare la scansione a 5 minuti possiamo utilizzare una delle seguenti forme:

nmap --host-timeout 300000 10.10.5.11

nmap --host-timeout 300s 10.10.5.11

nmap --host-timeout 5m 10.10.5.11

300000ms = 300s = 5m ognuno di quei comandi produrrà lo stesso risultato.

Timing Templates
Il parametro **-T** è usato per specificare il template (modello).

Sintassi: nmap -T [0-5] [target]

```
$ nmap -T4 10.10.1.1
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-12 16:59
CDT
Interesting ports on 10.10.1.1:
Not shown: 998 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

I timing templates sono delle utili scorciatoie per le varie opzioni di timing. Ci sono 6 template numerati da 0 a 5 che possono essere usate per velocizzare la scansione (per risultati più veloci) o per rallentare (per evadere i firewall). Questa tabella descrivere i vari template.

Template	Nome	Note
-T0	paranoid	Estremamente lento
-T1	sneaky	Utile per evadere gli IDS
-T2	polite	Poche interferenze con il target
-T3	normal	Default template
-T4	aggressive	Risultati veloci nella rete locale
-T5	insane	Velocissimo e aggressivo

Numero minimo di operazioni parallele
Questa opzione **—min-parallelism** è usata per specificare il minor numero di operazioni parallele che devono essere eseguite per ogni scansione.

Sintassi: nmap --min-parallelism [number] [target]

```
# nmap --min-parallelism 100 10.10.1.70
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-17 09:02
CST
Interesting ports on 10.10.1.70:
Not shown: 994 filtered ports
PORT          STATE    SERVICE
139/tcp       open     netbios-ssn
445/tcp       open     microsoft-ds
2967/tcp      closed   symantec-av
5900/tcp      open     vnc
19283/tcp     closed   unknown
19315/tcp     closed   unknown
MAC Address: 00:0C:F1:A6:1F:16 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 3.43 seconds
```

Nmap aggiusta automaticamente l'opzione di scansioni parallele basandosi sulle condizioni della rete. In rari casi si deve procedere ad aggiustare questo valore. L'esempio riportato istruisce Nmap ad effettuare almeno 100 scansioni parallele. Il settaggio manuale di questa opzione aumenta la performance della scansione, valori troppo alti possono ritornare risultati poco accurati.

Numero massimo di operazioni parallele
L'opzione **–max-parallelism** è usata per controllare il numero massimo di operazioni parallele che vengono effettuate.

Sintassi: nmap --max-parallelism [number] [target]

```
# nmap --max-parallelism 1 10.10.1.70
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-17 09:03
CST
Interesting ports on 10.10.1.70:
Not shown: 994 filtered ports
PORT          STATE    SERVICE
139/tcp       open     netbios-ssn
445/tcp       open     microsoft-ds
2967/tcp      closed   symantec-av
5900/tcp      open     vnc
19283/tcp     closed   unknown
19315/tcp     closed   unknown
MAC Address: 00:0C:F1:A6:1F:16 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 213.76 seconds
```

L'esempio restringe le operazioni di Nmap ad 1 alla volta. Questa scansione sarà considerevolmente lenta, ma sarà meno invasiva in quanto non ci sarà un flood di pacchetti verso il sistema target.

Grandezza min gruppo host
L'opzione –**min-hostgroup** viene usata per specificare il minimo numero di target che nmap dovrebbe scansionare in parallelo.

Sintassi: nmap --min-hostgroup [number] [targets]

```
# nmap --min-hostgroup 30 10.10.1.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-10 10:17
CST
Interesting ports on 10.10.1.1:
Not shown: 998 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
MAC Address: 00:06:B1:12:0D:14 (Sonicwall)
Interesting ports on 10.10.1.2:
Not shown: 998 closed ports
PORT     STATE    SERVICE
23/tcp   open     telnet
80/tcp   open     http
MAC Address: 00:19:B9:A6:ED:D9 (Dell)
...
```

Nmap compie scansioni in parallelo in modo da risparmiare tempo quando deve scansionare target multipli come range o subnet. Di default Nmap aggiusta automaticamente il numero di host del gruppo basandosi sul tipo di scansione da effettuare e sulle condizioni della rete.

Grandezza max gruppo host
L'opzione –**max-hostgroup** è usata per specificare il numero massimo di target che Nmap dovrebbe scansionare in parallelo.

Sintassi: nmap --max-hostgroup [number] [targets]

```
# nmap --max-hostgroup 10 10.10.1.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-10 10:18
CST
Interesting ports on 10.10.1.1:
Not shown: 998 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
MAC Address: 00:06:B1:12:0D:14 (Sonicwall)
Interesting ports on 10.10.1.2:
Not shown: 998 closed ports
PORT     STATE    SERVICE
23/tcp   open     telnet
80/tcp   open     http
MAC Address: 00:19:B9:A6:ED:D9 (Dell)
...
```

A differenza del –**min-hostgroup,** l'opzione **–max-hostgroup** controlla il numero massimo di host appartenenti ad un gruppo. Questa opzione è utile se si vuole ridurre il carico di rete o per impedire qualsiasi "red flag" (allarmi) da parte dei sistemi di sicurezza presenti nella rete.

Ritardo min scansione

L'opzione **--scan-delay** specifica ad Nmap di fare una pausa tra una richiesta e l'altra.

Sintassi: nmap --scan-delay [time] [target]

```
# nmap --scan-delay 5s scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-04 13:29
CST
Interesting ports on 64.13.134.52:
Not shown: 993 filtered ports
PORT      STATE   SERVICE
25/tcp    closed  smtp
53/tcp    open    domain
70/tcp    closed  gopher
80/tcp    open    http
110/tcp   closed  pop3
113/tcp   closed  auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 229.28 seconds
```

Alcuni sistemi utilizzano un "rate limit" che potrebbe intralciare la scansione di Nmap. Nmap aggiusta automaticamente il ritardo di scansione in quei sistemi dove viene rilevata la presenza del "rate limit". In alcuni casi può essere utile specificare manualmente il ritardo soprattutto se siamo a conoscenza che IDS o "rate limit" sono in uso sul sistema target. Nell'esempio è stato impostato un ritardo di 5 secondi tra una richesta e l'altra.

Ritardo max scansione

--max-scan-delay si usa per specificare l'ammontare massimo di tempo che Nmap dovrebbe attendere tra una richiesta e l'altra.

Sintassi: nmap --max-scan-delay [time] [target]

```
# nmap --max-scan-delay 300 scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-09 15:35
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT     STATE    SERVICE
25/tcp   closed   smtp
53/tcp   open     domain
70/tcp   closed   gopher
80/tcp   open     http
110/tcp  closed   pop3
113/tcp  closed   auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
```

Nmap aggiusta automaticamente il ritardo in base alle condizioni della rete e/o quando siamo in presenza di host con "rate limit". Il –**max-scan-delay** può utilizzato per impostare un limite di ritardo più alto tra una richiesta e l'altra. Questo può però stressare la rete

Rate min pacchetti
L'opzione –**min-rate** è usata per specificare il numero minimo di pacchetti per secondo che Nmap dovrebbe inviare.

Sintassi: nmap --min-rate [numero] [target]

```
# nmap --min-rate 30 scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-10 14:13
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT      STATE    SERVICE
25/tcp    closed   smtp
53/tcp    open     domain
70/tcp    closed   gopher
80/tcp    open     http
110/tcp   closed   pop3
113/tcp   closed   auth
31337/tcp closed   Elite
Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
```

Nmap, normalmente, è in grado di aggiustare la quantità di pacchetti da inviare durante la scansione basandosi sulle condizioni della rete. Ci sono casi in cui si voglia specificare un minimo anche se generalmente non è consigliato. In questo esempio **–min-rate 30** indica ad Nmap di inviare almeno 30 pacchetti al secondo. Nmap userà questo numero come valore minimo, quindi se le condizioni di rete lo permettono potrebbe scansionare anche più velocemente, è quindi solo un valore indicativo. Impostare un valore di **–min-rate** troppo alto potrebbe ridurre l'accuratezza della scansione.

Rate max pacchetti
L'opzione –**max-rate** è usata per specificare il numero massimo di pacchetti per secondo che Nmap dovrebbe inviare.

Sintassi: nmap --max-rate [numero] [target]

```
# nmap --max-rate 30 scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-10 14:14
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT     STATE    SERVICE
25/tcp   closed   smtp
53/tcp   open     domain
70/tcp   closed   gopher
80/tcp   open     http
110/tcp  closed   pop3
113/tcp  closed   auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 68.51 seconds
```

In questo esempio, specificando **--max-rate 30** consentiamo ad Nmap di inviare non più di 30 pacchetti per secondo. Questo può decisamente rallentare la scansione ma può essere utile per aggirare gli IDS o il "rate limiting" impostato sul sistema target.

Defeat Reset Rate Limits
L'opzione –**defeat-rst-ratelimit** è usata per *"sconfiggere"* quei target che applicano il *"rate limiting"* anche sui pacchetti RST (reset).

Sintassi: nmap --defeat-rst-ratelimit [target]

```
# nmap --defeat-rst-ratelimit scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-10 15:14
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT      STATE   SERVICE
25/tcp    closed  smtp
53/tcp    open    domain
70/tcp    closed  gopher
80/tcp    open    http
110/tcp   closed  pop3
113/tcp   closed  auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 7.71 seconds
```

Questa opzione risulta utile quando si vuole velocizzare le scansione verso target che implementano *"rate limit"* sui pacchetti RST. Questo comunque può portare a risultati inaccurati, per questo motivo è usata raramente, e nella maggior parte dei casi Nmap riconosce il "rate limit" e aggiusta di conseguenza il valore adatto alla situazione.

TECNICHE DI EVASIONE DEI FIREWALL

Firewall Evasion Techniques Overview

Firewall e IPS sono in grado di disturbare Nmap e evitare che si riesca ad avere un'accurata immagine dei sistemi che stanno proteggendo. Nmap include una serie di feature destinate all'evasione di queste difese.

Sommario

Feature	opzione
Fragment Packets	**-f**
Specify a Specific MTU	**--mtu**
Use a Decoy	**-D**
Idle Zombie Scan	**-sl**
Manually Specify a Source Port	**--source-port**
Append Random Data	**--data-lenght**
Randomize Target Scan Order	**--randomize-hosts**
Spoof MAC Address	**--spoof-mac**
Send Bad Checksums	**--badsum**

Pacchetti frammentati
L'opzione **–f** è usata per frammentare le richieste in pacchetti da 8 byte.

Sintassi: nmap -f [target]

```
# nmap -f 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-11 10:10
CST
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
2049/tcp open     nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

L'opzione **–f** è usata per inviare piccoli pacchetti da 8 byte. Questa opzione non è particolarmente utile nelle situazioni normali, comunque può essere utile quando si cerca di aggirare vecchi firewall o mal configurati. Certi sistemi operativi possono richiedere l'utilizzo di –**send–eth** combinata all'opzione **–f** per trasmettere i pacchetti frammentati in modo corretto.

Specificare manualmente l'MTU
L'opzione **–mtu** serve a specificare il valore dell'MTU (Maximum Transmission Unit).

Sintassi: nmap --mtu [numero] [target]

```
# nmap --mtu 16 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-11 10:11
CST
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
2049/tcp open     nfs
MAC Address: 00:0C:29:D5:38:F4 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

L'opzione **–mtu** è simile all'opzione **-f,** e concede di specificare manualmente l'MTU da utilizzare durante la scansione. Questo crea pacchetti frammentati che potrebbero confondere i firewall. In questo esempio **--mtu 16** istruice Nmap ad utilizzare pacchetti da 16-byte per la scansione. L'MTU deve essere un multiplo di 8 (8, 16, 24, 32, etc). Anche in questo caso potrebbe essere necessario combinare l'opzione –**send-eth** per trasmettere correttamente i pacchetti frammentati.

Usare un decoy (esca)
L'opzione da usare è **-D** e serve per aggiungere 1 o più decoys.

Sintassi: nmap -D [decoy1,decoy2,etc|RND:numero] [target]

```
# nmap -D RND:10 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-02 16:41
CST
...
```

Quando si compie questo tipo di scansione Nmap *"spooferà"* pacchetti aggiuntivi da tutti gli indirizzi specificati. In questo modo appare effettivamente che il target venga scansionato da più sistemi contemporaneamente, rendendo difficile l'individuazione e il tracciamento della reale sorgente dello scan. In questo esempio abbiamo impostato Nmap a generare 10 indirizzi random. Si possono specificare manualmente gli indirizzi usando questa sintassi: **nmap -D decoy1,decoy2,decoy3,etc.**

Usando troppi decoy possiamo congestionare la rete, riducendo l'efficacia della scansione. In oltre, certi internet providers possono filtrare il traffico spoofato rendendo poco utile l'utilizzo delle esche.

Idle Zombie Scan
L'opzione da usare è **-sI**

Sintassi: nmap -sI [zombie host] [target]

```
# nmap -sI 10.10.1.41 10.10.1.252
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-14 18:35
CST
Idle scan using zombie 10.10.1.41 (10.10.1.41:443); Class:
Incremental
Interesting ports on 10.10.1.252:
Not shown: 997 closed|filtered ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
```

```
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
MAC Address: 00:25:64:D7:FF:59 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 8.29 seconds
```

L'idle zombie scan è l'unica tecnica di scanning che ci permette di exploitare un sistema inattivo ed utilizzarlo per compiere la scansione al nostro posto.
In questo esempio 10.10.1.41 è lo zombie e 10.10.1.252 è il target. Per che funzioni correttamente il sistema zombie deve essere realmente inattivo al momento della scansione. Con questa scansione non viene inviato nessuno pacchetto dal nostro sistema verso il target, ciò nonostante un ping iniziale verrà inviato al target almeno che non si combini con l'opzione **–PN.**
Maggiori informazioni sull'*idle zombie scan* possono essere trovate sul sito di Nmap *www.nmap.org/book/idlescan.html*.

Specificare manualmente la porta sorgente
--source-port è l'opzione per specificare manualmente il numero della porta che effettuerà la richiesta.

Sintassi: nmap --source-port [port] [target]

```
# nmap --source-port 53 scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-16 16:41
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT     STATE    SERVICE
25/tcp   closed   smtp
53/tcp   open     domain
70/tcp   closed   gopher
80/tcp   open     http
110/tcp  closed   pop3
113/tcp  closed   auth
31337/tcp closed  Elite
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
```

Ogni segmento TCP contiene informazioni sulla porta sorgente oltre che sulla porta di destinazione. Di default Nmap randomizza la scelta della sorgente tra quelle disponibili, con questa opzione forziamo nmap ad utilizzare una specifica porta come sorgente di tutti i pacchetti. Questa tecnica può essere utilizzata per sfruttare delle vulnerabilità nei firewall che non sono stati configurati correttamente e che accettano ciecamente traffico in entrata che proviene da porte considerate "legittime". La porta 20 (ftp), 53(dns) e 67 (dhcp) sono porte che possono essere usate per questo tipo di scansione. La scorciatoia per questo

opzione è **-g.**

Aggiungere dati casuali
--data-lenght aggiunge ai pacchetti dei dati casualmente.

Sintassi: nmap --data-length [numero] [target]

```
# nmap --data-length 25 10.10.1.252
Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-14 18:41
CST
Interesting ports on 10.10.1.252:
Not shown: 995 filtered ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
5800/tcp open     vnc-http
5900/tcp open     vnc
MAC Address: 00:25:64:D7:FF:59 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds
```

Nmap trasmette pacchetti che sono generalmente di una specifica dimensione. I produttori di Firewall ne sono a conoscenza e controllano pacchetti di dimensioni ipoteticamente appartenenti ad nmap. L'opzione –data-leght aggiunge una certa quantità di dati a questi pacchetti in modo da aggirare questo controllo. In questo esempio sono stati aggiunti 25 bytes a tutti i pacchetti inviati al target.

Ordine di scansione casuale
--randomize-hosts specifica un ordine casuale della scansione.

Sintassi: nmap --randomize-hosts [targets]

```
$ nmap --randomize-hosts 10.10.1.100-254
Interesting ports on 10.10.1.109:
Not shown: 996 filtered ports
PORT     STATE    SERVICE
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
5800/tcp open     vnc-http
5900/tcp open     vnc
MAC Address: 00:1C:23:49:75:0C (Dell)
Interesting ports on 10.10.1.100:
Not shown: 996 filtered ports
```

```
PORT     STATE    SERVICE
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
5800/tcp open     vnc-http
5900/tcp open     vnc
MAC Address: 00:21:9B:3F:AC:EC (Dell)
Interesting ports on 10.10.1.107:
Not shown: 997 closed ports

PORT     STATE    SERVICE
22/tcp   open     ssh
139/tcp  open     netbios-ssn
...
```

Questa opzione ci aiuta a non essere intercettati da firewall o IDS quando svolgiamo scansioni multiple.

Mac address spooffato
L'opzione **–spoof-mac** falsifica l'indirizzo MAC (Media Access Control) di un device.

Sintassi: nmap --spoof-mac [vendor|MAC|0] [target]

```
# nmap -sT -PN --spoof-mac 0 192.168.1.1
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-15 19:48
CST
Spoofing MAC address 00:01:02:25:56:AE (3com)
Interesting ports on 192.168.1.1:
Not shown: 995 filtered ports
PORT     STATE    SERVICE
20/tcp   closed   ftp-data
21/tcp   closed   ftp
23/tcp   closed   telnet
80/tcp   open     http
2869/tcp open     unknown
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

In questo esempio nmap viene istruito a generare casualmente un MAC address. Questo rende la nostra scansione attivamente complicata da tracciare. L'opzione **–spoof-mac** può essere controllata da questi parametri:

Argomento	Funzione
0 (zero)	Generazione casuale
MAC add. specifico	MAC specifico
vendor	Genera MAC Apple, Dell, 3Com, etc

Invio di checksum errati
--badsum invia pacchetti con checksum errati all'host specificato.

Sintassi: nmap --badsum [target]

```
# nmap --badsum 10.10.1.41
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-24 16:19
CDT
All 1000 scanned ports on 10.10.1.41 are filtered
MAC Address: 00:60:B0:59:B6:14 (Hewlett-packard CO.)
Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

Il protocollo TCP/IP utilizza il checksum per assicurare che i dati inviati siano integri. Creando pacchetti con un checksum errato si può, in rari casi, produrre una risposta da sistemi mal configurati. In questo esempio non abbiamo ricevuto una risposta in quanto il sistema target è stato configurato correttamente, questo è un tipico risultato quando si usa questa opzione. Solo un sistema configurato male potrebbe rispondere a pacchetti con un checksum errato. Non di meno è un ottimo strumento quando si testa la sicurezza della rete oppure si tenta di evadere un firewall.

TROUBLESHOOTING E DEBUGGING

I problemi tecnici sono una parte intrinseca dell'utilizzo dei computer. Nmap non fa purtroppo eccezione.
Di tanto in tanto una scansione non produrrà l'output che ti aspettavi: è possibile ricevere un errore o potresti non ricevere proprio alcun output. Nmap offre diverse opzioni per l'analisi e il debug di una scansione, che può aiutare a identificare perché questo accade. La sezione seguente descrive come risolvere questi problemi e il debug in dettaglio.

Funzione	Opzione
Trovare Aiuto	**-h**
Visualizzare la versione di Nmap	**-V**
Output dettagliato	**-v**
Debug	**-d**
Visualizzare lo stato delle porte	**--reason**
Visualizzare solo le porte aperte	**--open**
Visualizzare i pacchetti scambiati	**--packet-trace**
Visualizzare la configurazione di rete	**--iflist**
Specificare l'interfaccia di rete	**-e**

Trovare aiuto
Eseguendo il comando **nmap -h** si avrà una lista di tutte le opzioni disponibili
Sintassi : nmap -h

```
$ nmap -h
Nmap 5.00 ( http://nmap.org )
Usage: nmap [Scan Type(s)] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-
255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
...
```

Per altri dettagli o informazioni è utile e consigliabile leggere il manuale di Nmap.
Lo si può fare utilizzando il comando:

```
$ man nmap
```

Il manuale di tutti i programmi in linux si trova sempre dando il comando nmap prima del nome del programma. Gli utenti Windows possono trovare il manuale alla pagina www.nmap.org/book/man.html. Si può anche trovare aiuto scrivendo alla mailing list di Nmap all'indirizzo www.seclists.org.

Visualizzare la Versione di Nmap

l'opzione **–V** è utilizzata per visualizzare la versione installata di Nmap:

```
$ nmap -V
Nmap version 5.00 ( http://nmap.org )
```

Quando si cerca la risoluzione dei problemi di Nmap ci si dovrebbe sempre assicurare di avere installato la versione più avanzata. Programmi open source come Nmap sono sviluppati ad un ritmo rapido e i bug sono tipicamente risolti non appena vengono scoperti. Confronta la versione installata rispetto alla versione più recente disponibile sul sito di Nmap **www.nmap.org** per assicurarti di avere installato la versione più aggiornata. Questo farà sì che si possa avere accesso alle funzionalità più recenti, e i bug sino ad oggi rilevati saranno stati sicuramente fixati.

Output Dettagliato

L'opzione -v è utilizzata per abilitare la visualizzazione dei dettagli.

Sintassi: nmap -v [target]

```
$ nmap -v scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-12 15:06
CDT
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 15:06
Scanning 64.13.134.52 [2 ports]
Completed Ping Scan at 15:06, 1.87s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:06
Completed Parallel DNS resolution of 1 host. at 15:06, 0.16s
elapsed
Initiating Connect Scan at 15:06
Scanning scanme.nmap.org (64.13.134.52) [1000 ports]
Discovered open port 53/tcp on 64.13.134.52
Discovered open port 80/tcp on 64.13.134.52
Completed Connect Scan at 15:06, 7.00s elapsed (1000 total
ports)
Host scanme.nmap.org (64.13.134.52) is up (0.087s latency).
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 998 filtered ports
```

```
PORT STATE SERVICE
/tcp open domain
/tcp open http
Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.41 seconds
```

L'opzione dettagliata è utile se serve risolvere problemi di connessione, oppure semplicemente per capire cosa accade dietro le scene quando si effettua una scansione. è possibile lanciare il comando **-v** due volte, **-vv** o **-v -v** per avere ancora più dettagli.

Debug
L'opzione **-d** abilita la funzionalità di debug.

Sintassi: nmap -d [target]

```
$ nmap -d scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-12 15:26
CDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0,
SCTP:0)
--------------- Timing report ---------------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 15:26
Scanning 64.13.134.52 [2 ports]
Completed Ping Scan at 15:26, 2.83s elapsed (1 total hosts)
Overall sending rates: 1.06 packets / s.
mass_rdns: Using DNS server 10.10.1.44
mass_rdns: Using DNS server 10.10.1.45
Initiating Parallel DNS resolution of 1 host. at 15:26
mass_rdns: 0.00s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR:
1]
Completed Parallel DNS resolution of 1 host. at 15:26, 0.00s
elapsed
...
```

L'output di debug fornisce informazioni aggiuntive che possono essere utilizzate per tenere traccia degli errori o per risolvere dei problemi. L'output predefinito **-d** fornisce una discreta quantità di informazioni di debug. È inoltre possibile

specificare un livello di debug di 1-9 per essere usato con l'opzione **-d**, questo parametro serve per aumentare o diminuire la quantità di output. Ad esempio: **-d1** fornisce l'importo più basso di informazioni di debug e **-d9** il più alto.

Visualizzare lo stato delle porte
Il parametro **--reason** visualizza perchè una porta è considerata in un determinato stato.

Sintassi: nmap --reason [target]

```
$ nmap --reason scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-12 15:43
CDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
Reason: 993 no-responses
PORT     STATE    SERVICE  REASON
25/tcp   closed   smtp     conn-refused
53/tcp   open     domain   syn-ack
70/tcp   closed   gopher   conn-refused
80/tcp   open     http     syn-ack
110/tcp  closed   pop3     conn-refused
113/tcp  closed   auth     conn-refused
31337/tcp closed  Elite    conn-refused
Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

Notare l'aggiunta del campo **reason** nella scansione precedente. Un informazione in questo settore può essere utile quando si cerca di determinare perché le porte di un bersaglio sono in uno stato particolare. Le porte che rispondono con syn-ack sono considerate aperte. Porte che rispondono con **conn-refused** o **reset** sono in genere chiuse. Porte che non rispondono affatto sono generalmente filtrate (da un firewall).

Visualizzare solo le porte aperte
Il parametro **--open** comanda a Nmap di visualizzare solo le porte aperte.

sintassi: nmap --open [target]

```
$ nmap --open scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-18 12:47
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports, 5 closed ports
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
Nmap done: 1 IP address (1 host up) scanned in 8.26 second
```

Il parametro **--open** rimuove le porte chiuse filtrandole dai risultati della scansione. Questa opzione è utile quando si desidera riordinare i risultati della scansione in modo che solo le porte aperte vengano visualizzate. Qua sotto confrontiamo la stessa scansione precedente senza applicare il parametro **--open**:

```
$ nmap scanme.insecure.org
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-18 12:49
CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT     STATE    SERVICE
25/tcp   closed   smtp
53/tcp   open     domain
70/tcp   closed   gopher
80/tcp   open     http
110/tcp  closed   pop3
113/tcp  closed   auth
...
```

Tracciamento dei pacchetti
il parametro **--packet-trace** chiede a Nmap di visualizzare un riepilogo di tutti i pacchetti inviati e ricevuti

Sintassi: nmap --packet-trace [target]

```
$ nmap --packet-trace 10.10.1.1
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 17:14 CDT
CONN (0.1600s) TCP localhost > 10.10.1.1:80 => Operation now in progress
CONN (0.1600s) TCP localhost > 10.10.1.1:443 => Operation now in progress
NSOCK (0.1610s) UDP connection requested to 10.10.1.45:53 (IOD #1) EID 8
NSOCK (0.1610s) Read request from IOD #1 [10.10.1.45:53] (timeout: -1ms) EID
18
NSOCK (0.1610s) UDP connection requested to 10.10.1.44:53 (IOD #2) EID 24
NSOCK (0.1610s) Read request from IOD #2 [10.10.1.44:53] (timeout: -1ms) EID
```

```
34
NSOCK (0.1610s) Write request for 40 bytes to IOD #1 EID 43 [10.10.1.45:53]:
V!..........1.1.10.10.in-addr.arpa.....
NSOCK (0.1610s) nsock_loop() started (timeout=500ms). 5 events pending
NSOCK (0.1610s) Callback: CONNECT SUCCESS for EID 8 [10.10.1.45:53]
NSOCK (0.1610s) Callback: CONNECT SUCCESS for EID 24 [10.10.1.44:53]
NSOCK (0.1610s) Callback: WRITE SUCCESS for EID 43 [10.10.1.45:53]
...
```

Il parametro **--packet-trace** è un altro strumento utile per la risoluzione dei problemi di connettività. L'esempio precedente mostra informazioni dettagliate su ogni pacchetto inviato e ricevuto dal sistema di destinazione.

Visualizzare la configurazione di rete

L'opzione **--iflist** viene utilizzata per visualizzare le interfacce di rete e il router configurati sul sistema locale

```
$ nmap --iflist
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 17:03
CDT
************************INTERFACES**************************
DEV       (SHORT)        IP/MASK        TYPE      UP MAC
lo        (lo)           127.0.0.1/8    loopback  up
eth0      (eth0)         10.10.1.107/24 ethernet  up 00:21:70:AC:F7:E7
wlan0     (wlan0)        10.10.1.176/24 ethernet  up 00:16:EA:F0:92:50


**************************ROUTES****************************
DST/MASK      DEV       GATEWAY

10.10.1.0/0     eth0
10.10.1.0/0     wlan0
169.254.0.0/0   wlan0
0.0.0.0/0       eth0      10.10.1.1
```

L'esempio precedente visualizza la rete e le informazioni di routing del sistema locale. Questa opzione può essere utile per identificare rapidamente le informazioni di rete o per risolvere problemi di connettività.
Ulteriori comandi che sono utili per la risoluzione dei problemi di configurazione di rete sono **ifconfig** (Unix / Linux) e **ipconfig** (Windows). Sistemi basati su Windows e Unix includono anche il comando **netstat** che può fornire ulteriori informazioni di rete.

Specificare quale interfaccia di rete utilizzare
L'opzione **-e** serve per indicare quale interfaccia di rete dovrà essere usata.

Sintassi: nmap -e [interface] [target]

```
$ nmap -e eth0 10.10.1.48
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-25 08:30
CDT
Interesting ports on 10.10.1.48:
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
2049/tcp open     nfs
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Molti sistemi hanno più interfacce di rete. La maggior parte dei moderni computer portatili, per esempio, ha sia una normale presa Ethernet che una scheda wireless. Se si vuol esser certi che Nmap utilizzi l'interfaccia di rete è possibile utilizzare **-e** per specificarlo sulla riga di comando. In questo esempio **-e** serve per forzare Nmap ad eseguire la scansione tramite l'interfaccia eth0.

Questo documento è stato redatto dalla under_r00t crew per puro spirito di condivisione. Grazie a tutti!

Puoi trovare questo e altro materiale sul nostro blog:
https://under12oot.noblogs.org/

Per qualsiasi informazione, segnalazione o se vuoi solo contattarci, lo puoi fare a questo indirizzo:
under_root@hacari.org

happy hacking!