

# Tutorial per Nmap

Dario Pileri

8 agosto 2008

Copyright © 2008 Dario Pileri. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

# Indice

<b>1</b>	<b>Introduzione</b>	<b>4</b>
1.1	Disclaimer . . . . .	4
<b>2</b>	<b>Installazione</b>	<b>5</b>
2.1	Linux . . . . .	5
2.1.1	Installazione da pacchetti precompilati . . . . .	5
2.1.2	Compilazione da sorgente . . . . .	6
2.2	Windows . . . . .	6
2.3	Mac OS X . . . . .	6
<b>3</b>	<b>Teoria</b>	<b>7</b>
3.1	Le porte . . . . .	7
3.2	Infrastruttura client-server . . . . .	7
3.3	TCP e UDP . . . . .	8
3.3.1	TCP . . . . .	8
3.3.2	UDP . . . . .	9
<b>4</b>	<b>Utilizzo di Nmap</b>	<b>11</b>
4.1	Premesse . . . . .	11
4.1.1	Sintassi . . . . .	11
4.1.2	Sintassi dell'obiettivo . . . . .	11
4.1.3	Stati delle porte . . . . .	12
4.1.4	Esecuzione di Nmap . . . . .	12
4.2	Il primo scan: SYN Stealth . . . . .	12
4.3	Service e OS Scan . . . . .	13
4.4	Ping scan . . . . .	14
4.5	Scan speciali . . . . .	15
4.5.1	FIN, Null e Xmas Tree . . . . .	15
4.5.2	UDP Scan . . . . .	16
<b>5</b>	<b>Conclusioni</b>	<b>17</b>
<b>A</b>	<b>Riguardo questo documento</b>	<b>18</b>
<b>GNU Free Documentation License</b>		<b>19</b>
1.	APPLICABILITY AND DEFINITIONS . . . . .	19
2.	VERBATIM COPYING . . . . .	20
3.	COPYING IN QUANTITY . . . . .	21
4.	MODIFICATIONS . . . . .	21

5. COMBINING DOCUMENTS . . . . .	23
6. COLLECTIONS OF DOCUMENTS . . . . .	23
7. AGGREGATION WITH INDEPENDENT WORKS . . . . .	23
8. TRANSLATION . . . . .	24
9. TERMINATION . . . . .	24
10. FUTURE REVISIONS OF THIS LICENSE . . . . .	24
ADDENDUM: How to use this License for your documents . . . . .	24

# Capitolo 1

## Introduzione

Questo tutorial ha come scopo imparare progressivamente l'uso del programma *Nmap*, che può essere considerato una sorta di "coltellino svizzero" per controllare le funzionalità di rete di computer, ma può anche essere usato dagli amministratori di rete per scansionare intere reti, magari per vedere quali PC sono online, oppure per trovare l'indirizzo IP di un determinato computer.

Questo tutorial spiega brevemente le opzioni principali di Nmap, e vuole essere solo un "punto di partenza" per apprendere tutte le potenzialità di Nmap. Sul sito <http://www.insecure.org> è disponibile la documentazione ufficiale, contenente tutte le sue opzioni.

Il sistema operativo principale di riferimento per questo tutorial è Linux, ma tratterò, seppur brevemente, l'installazione e il suo utilizzo anche su sistemi operativi Windows e Mac.

### 1.1 Disclaimer

Prima di iniziare le proprie prove con questo potentissimo programma, raccomando di usarlo *solo* per controllare computer o reti delle quali siete proprietari, oppure dopo aver avuto il consenso del loro amministratore. Molti amministratori considerano questo tipo di controlli un vero e proprio attacco informatico, prendendo provvedimenti adeguati, dato che *ogni* controllo, anche dei più discreti, può essere rilevato.

# Capitolo 2

## Installazione

In questo capitolo vedremo come installare Nmap sui vari sistemi operativi supportati.

### 2.1 Linux

Nmap può essere installato o compilandosi da sé i sorgenti ufficiali del programma, oppure installando un comodo pacchetto precompilato fornito dai gestori della propria distribuzione Linux.

In generale è preferibile, in termini di semplicità e velocità, l'installazione da pacchetti precompilati. Può essere invece una scelta migliore la compilazione da sorgente nel caso la propria distribuzione fornisca una versione vecchia di Nmap, oppure nel caso la propria distribuzione non fornisca addirittura pacchetti precompilati di Nmap.

Questa guida si riferisce a Nmap versione 4.62.

#### 2.1.1 Installazione da pacchetti precompilati

##### Distribuzioni Debian e derivate

Per Debian e le distribuzioni derivate, che usano i pacchetti nel formato DEB e APT per la gestione degli archivi dei pacchetti, è sufficiente eseguire il comando (come utente *root*):

```
apt-get install nmap
```

##### Distribuzioni che usano RPM

Per le distribuzioni che usano pacchetti RPM (Red Hat e derivate, come Fedora, Mandriva...), Nmap può essere installato o mediante il gestore dei pacchetti della propria distribuzione (*urpmi* su Mandriva, *yum* su Red Hat e Fedora...) oppure mediante i pacchetti RPM forniti direttamente dagli sviluppatori di Nmap.

In questo caso basta eseguire, sempre come utente *root*:

```
rpm -vhU http://nmap.org/dist/nmap-4.68-1.i386.rpm
```

Questo comando serve ad installare la versione 4.68. Nel caso di versioni aggiornate, si mettano i numeri dell'ultima versione.

## Altre distribuzioni

Informazioni sull'installazione da pacchetti precompilati su altre distribuzioni sono disponibili sul sito ufficiale di Nmap, <http://nmap.org>.

### 2.1.2 Compilazione da sorgente

Per compilare ed installare Nmap da codice sorgente, si seguano queste istruzioni:

1. Si scarichi dal sito <http://nmap.org/download.html> l'ultima versione dei sorgenti di Nmap. Il file scaricato dovrebbe chiamarsi **nmap-VERSION.tar.bz2**, sostituendo a *VERSION* la versione di Nmap scaricata.
2. Si decomprima il contenuto compresso, o usando un archiviatore grafico (Ark, File Roller, Xarchiver), oppure a riga di comando:  
`tar xvjf nmap-VERSION.tar.bz2`
3. Si entri nella cartella contenente i files decompressi:  
`cd nmap-VERSION`
4. Si configuri il pacchetto:  
`./configure`  
Questo comando controlla che Nmap sia compilabile nel proprio sistema. Per ottenere ciò è necessario avere installato il compilatore GCC e GNU Make.
5. Si compili  
`make`
6. Si diventi utente *root* e si installi:  
`su` oppure `sudo -s`  
`make install`

## 2.2 Windows

Nmap nelle versioni consumer di Windows (Windows XP e Windows Vista) ha delle grosse limitazioni di performance e di possibilità di scansione, a causa del mancato supporto a caratteristiche avanzate di rete (*raw socket*) e a limitazioni al numero di connessioni. Per questi motivi ne sconsiglio l'uso su queste piattaforme. Le versioni server di Windows (Windows Server 2003 e Windows Server 2008) non sono affette da queste limitazioni.

Per installare Nmap su Windows è disponibile sul sito <http://nmap.org/download.html> un comodo installer, che si preoccuperà di tutti i passi dell'installazione.

## 2.3 Mac OS X

Sul sito di Nmap è disponibile un installer, in formato *DMG*, del programma, per Mac OS X versione 10.4 (Tiger) o successive.

# Capitolo 3

## Teoria

Per comprendere il funzionamento di Nmap, è necessario conoscere almeno una base di teoria delle reti informatiche. In questo documento tratterò assai brevemente questo argomento, spiegando il minimo indispensabile per capire il funzionamento di Nmap. Per chi fosse interessato, in internet sono presenti ottime guide sull'argomento, come *Appunti di informatica libera* di Daniele Giacomini (<http://na.mirror.garr.it/mirrors/appuntilinux/HTML/a2.htm>).

### 3.1 Le porte

Tecnicamente, Nmap è un *port scanner*, ovvero un software che va a controllare lo stato delle porte di un host (qualunque apparecchio connesso ad una rete) remoto.

Le porte (in inglese *port*, non *door*) possiamo chiamarle delle "vie d'accesso" per collegarsi ad un computer remoto, ed è possibile paragonarle alle porte nella vita reale. Immaginiamo il nostro computer come ad una casa, con tante porte. Quando volete comunicare con l'esterno, la vostra comunicazione passerà per una porta specifica, in quanto non è possibile mantenere due comunicazioni contemporaneamente per la medesima porta.

Ogni computer ha 65 535 porte ( $2^{16} - 1$ ) che usano il protocollo *TCP* e altre 65 535 che usano il protocollo *UDP* (di questi protocolli tratterò successivamente), e sono chiamate con il loro numero (per es. «La porta 80»).

### 3.2 Infrastruttura client-server

In una rete, vi possono essere diversi tipi di trasferimento di dati, con scopi diversi, e ad ogni scopo è associato un *potocollo*, ovvero un insieme di norme molto strette che regolano nei minimi dettagli una comunicazione. Per esempio via internet possiamo visitare siti Web (e in questo caso usiamo il protocollo *HTTP*), oppure possiamo inviare e-mail (usando il protocollo *SMTP*): vediamo quindi che l'invio di e-mail e la navigazione Web sono tipi di comunicazione diversi, con scopi diversi, che quindi usano protocolli diversi.

In qualunque tipo di comunicazione (detta anche connessione), che è sempre tra due *host* (un qualunque apparecchio [computer o quant'altro] connesso ad una rete è detto *host*), un host svolge il ruolo di *client*, ed l'altro svolge il ruolo di *server*. Il *client* è quell'host che contatta il server e richiede un determinato servizio, e il *server* è appunto quell'host che sta in ascolto in attesa di richieste di client, e fornisce il servizio richiesto. Tornando all'esempio precedente, nel caso si voglia visitare un sito Web, il

Tabella 3.1: Porte e servizi più comuni

Porta	Servizio	Descrizione
22 TCP	SSH	Controllo remoto
25 TCP	SMTP	Invio di e-mail
80 TCP	HTTP	Navigazione Web
110 TCP	POP3	Ricezione di e-mail
445 TCP	SMB	Condivisione cartelle di Windows

client si collega al server richiedendo una determinata pagina Web; il server la fornisce, e il client la visualizza.

Questo tipo di comunicazione utilizza, come già detto, le porte. Il client, mediante una sua porta, si collega ad una porta del server, che a differenza di quella del client, è *aperta*, ovvero vi è in ascolto un programma server che risponde alle richieste di connessione a quella porta.

Un'altra differenza tra la porta client e la porta server è che la porta client è una porta detta *non privilegiata*, ovvero di numero superiore a 1024, scelta casualmente e usata solo per la durata della connessione, nonché non permette ad altri client di collegarsi ad essa (ovviamente, in quanto per collegarsi ad una porta è necessario che vi sia in ascolto un programma server). Invece la porta server è detta *privilegiata*, di numero inferiore a 1024, ed è generalmente fissa in base al protocollo. Questo perché in questo modo il client sa a che porta collegarsi per richiedere un determinato servizio.

Lo IANA (Internet Assigned Numbers Authority) gestisce gli assegnamenti porte-servizi. La lista aggiornata con le porte associate ai relativi servizi si può trovare all'indirizzo nel sito <http://www.iana.org/assignments/port-numbers>. Nella tabella 3.1 sono rappresentate le porte più comuni ed i servizi ad esse associati.

Una volta spiegato ciò, il funzionamento di Nmap è ora chiaro. Nmap controlla uno o più host, dicendoci quali porte sono aperte. Questo è il suo funzionamento "basilare", in quanto Nmap offre molte altre possibilità, come la rilevazione esatta dei programmi server in ascolto sulle porte aperte, o la rilevazione del sistema operativo dell'host.

### 3.3 TCP e UDP

Prima ho detto che esistono due protocolli che possono essere usati nella gestione delle porte: *TCP* e *UDP*. Questi due protocolli agiscono *sotto* i protocolli associati ai servizi (HTTP, SMTP...), quindi non sono confrontabili con essi, ma vengono usati dai servizi, e per i servizi viene scelto TCP o UDP in base alle necessità.

Prima di procedere, è necessario introdurre un altro concetto importante. I dati, su internet, non sono inviati come un flusso continuo, ma in realtà sono divisi in *pacchetti*, ovvero parti contenenti questi dati. I servizi (HTTP, SMTP...) operano ad un livello di astrazione alto, tale che non gestiscono "pacchetti" di dati, ma gestiscono flussi di dati. I pacchetti vengono invece gestiti proprio da TCP e UDP, rendendoli trasparenti ai servizi.

#### 3.3.1 TCP

TCP (Transmission Control Protocol) è il protocollo per la gestione delle porte più usato, perché gestisce automaticamente le connessioni, controlla e rimedia a perdite di dati, controllandone l'integrità e ri assemblandone i pacchetti nell'ordine corretto.

In questa parte ci occuperemo principalmente della gestione delle connessioni. Vediamo come funziona una connessione tra due host usando TCP:

Tabella 3.2: Flag dei pacchetti TCP

Pacchetto	Traduzione	Descrizione
URG	Urgent	Identifica dati urgenti
ACK	Acknowledgment	Connessione effettuata
PSH	Push	Chiede di inoltrare i dati anziché bufferizzarli
RST	Reset	Termina brutalmente una connessione
SYN	Synchronize	Usato per instaurare una connessione
FIN	Finish	Usato per terminare una connessione

**Instaurazione della connessione** Nella prima fase possiamo dire che i due servizi si "conoscono", e, scambiandosi dei pacchetti particolari (di cui poi parlerò), instaurano una connessione tra i due servizi.

**Scambio dati** Una volta instaurata la connessione, mediante questa connessione vengono scambiati i dati necessari.

**Termine della connessione** Sempre mediante pacchetti particolari, la connessione viene chiusa.

La connessione è una pura astrazione logica per gestire al meglio le comunicazioni. Possiamo vederla come una connessione fisica tra due PC usando un cavo. Collegando i cavi e abilitandoli nei sistemi operativi noi andiamo ad instaurare la connessione. Fatto tutto, si scambiano i dati mediante questo cavo, e alla fine il cavo viene scollegato (termine della connessione).

### Tipi di pacchetti TCP

Ogni pacchetto TCP può avere dei *flag*, ovvero dei valori impostati nel pacchetto. I possibili flag dei pacchetti TCP sono contenuti nella tabella 3.2. Ogni pacchetto ha impostato uno o più di questi flag, e in base ad essi TCP gestisce le connessioni.

### Handshake

Per instaurare una nuova connessione, avviene un cosiddetto *handshake* tra il client ed il server. Un handshake è uno scambio di specifici pacchetti che segue un rigido protocollo.

Nel nostro caso l'handshake è svolto in questa maniera:

1. Il client, che inizia la connessione, invia un pacchetto TCP al server con impostato solo il flag *SYN*.
2. Il server risponde al client con un pacchetto TCP con i flag *SYN* e *ACK*.
3. Il client risponde con un pacchetto con impostato solo il flag *ACK*.

Terminata questa "procedura" la connessione è instaurata ed è possibile iniziare il trasferimento di dati.

Questo handshake è molto importante perché Nmap lo userà per determinare le porte aperte.

### 3.3.2 UDP

UDP (User Datagram Protocol) è invece un protocollo del tutto privo delle caratteristiche di TCP, e quindi lascia al servizio la gestione delle connessioni (semmai fosse necessaria) e la gestione degli errori (ricomposizione dei pacchetti, ritrasmissione dei

pacchetti persi e così via). In cambio però offre un overhead minimo, ovvero consuma molte meno risorse di sistema e quindi la trasmissione è più veloce.

Per questi motivi UDP è poco utilizzato, ed è usato principalmente dai protocolli DNS e DHCP, oppure da VPN e giochi.

## Capitolo 4

# Utilizzo di Nmap

Terminata la parte teorica, possiamo ora iniziare ad utilizzare questo programma. Nonostante esista una GUI (interfaccia grafica) ufficiale di Nmap, *Zenmap*, questa guida tratterà esclusivamente il suo utilizzo a riga di comando. Tuttavia, conoscendo bene il suo utilizzo a riga di comando, l'uso di *Zenmap* risulterà estremamente semplice da apprendere.

### 4.1 Premesse

#### 4.1.1 Sintassi

La sintassi di Nmap a riga di comando (presa dalla pagina man) è `nmap [Tipo di scan] [Opzioni] {Obiettivo/i}`

#### 4.1.2 Sintassi dell'obiettivo

Al posto di `{Obiettivo/i}` va messo l'effettivo obiettivo dello scan. L'obiettivo può essere specificato nei seguenti modi:

**Singolo host** È possibile specificare un singolo host come obiettivo, scrivendone l'indirizzo IP (ad es. *192.168.0.1*), oppure scrivendone il nome di dominio (ad es. *scanme.nmap.org*).

**Reti** In questo caso bisogna specificare la rete da controllare, nella forma `[Indirizzo IP]/[Subnet mask]`. La subnet mask deve essere nella forma decimale, per esempio se si ha una subnet mask di *255.255.255.0* la subnet mask decimale è *24*, perché nella forma binaria di *255.255.255.0* i primi 24 bit sono impostati

Tabella 4.1: Subnet mask più comuni

Subnet mask	Numero indirizzi	Decimale
255.255.255.255	1	32
255.255.255.0	256	24
255.255.0.0	65 536	16
255.240.0.0	1 048 576	12
255.0.0.0	16 777 216	8

ad 1 mentre gli altri a 0. Nella tabella 4.1 sono visualizzate le subnet mask più comuni e il loro equivalente decimale.

### 4.1.3 Stati delle porte

Terminato un port scan, Nmap può classificare le porte dell'host (o degli hosts) con un massimo di cinque possibilità:

**Open** La porta è aperta: c'è un programma server in ascolto

**Closed** La porta è chiusa: non c'è nessun programma in ascolto

**Filtered** Nmap non è riuscito a determinare lo stato della porta, in quanto qualcosa (come un firewall) ha bloccato i pacchetti

**UNfiltered** Non è presente un filtro di pacchetti, ma Nmap non è riuscito a determinare se la porta è aperta o chiusa

**Open—filtered** La porta può essere o aperta oppure è presente un filtro che ha bloccato i pacchetti

### 4.1.4 Esecuzione di Nmap

Nmap, usando tecniche avanzate di rete, deve essere eseguito con i privilegi di root. Per diventare root su Linux bisogna eseguire il comando `su` oppure `sudo -s`.

## 4.2 Il primo scan: SYN Stealth

Iniziamo ad eseguire questo comando:

```
nmap -sS -T4 scanme.nmap.org
```

Dovremo ottenere un output del tipo:

```
Starting Nmap 4.62 ( http://nmap.org ) at 2008-07-07 11:50 CEST
```

```
Interesting ports on scanme.nmap.org (64.134.134.52):
```

```
Not shown: 1709 filtered ports
```

```
PORT STATE SERVICE
```

```
22/tcp open  ssh
```

```
25/tcp closed smtp
```

```
53/tcp open  domain
```

```
70/tcp closed gopher
```

```
80/tcp open  http
```

```
113/tcp closed auth
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.299 seconds
```

Analizziamo bene il tutto. Nella riga di comando, ho detto di analizzare l'host *scanme.nmap.org*, che è un host di proprietà degli sviluppatori di Nmap, creato apposta per fare le proprie prove di scansione. Poi ho dato l'opzione *-T4*, che non fa altro che rendere più veloce lo scan, e con l'opzione *-sS* ho detto di fare uno scan *SYN Stealth*.

Uno scan SYN Stealth usa appunto l'handshake spiegato prima per determinare lo stato delle porte. Nmap invia ad ogni porta un pacchetto TCP con il flag SYN. Se la porta invia un pacchetto SYN/ACK allora la porta è aperta. Se invece si riceve un pacchetto RST, allora la porta è chiusa, in quanto le specifiche dicono di rispondere con un pacchetto RST a richieste di connessione alle porte chiuse (questo invio è operato dallo stack TCP/IP del sistema operativo). Nel caso non si riceva alcuna risposta, allora la porta è detta filtered (filtrata).

Lo scan SYN Stealth è chiamato semi-aperto, in quanto non apre totalmente una connessione. In questo modo va a sostituire lo scan *TCP connect()* (*-sT*), che invece si connetteva proprio alla porta, facendo una connessione completa. Rispetto allo scan

TCP connect(), lo scan SYN Stealth è più veloce, ed è più difficile da rilevare in quanto non viene aperta una connessione.

Analizzando i risultati, vediamo che ha trovato alcune porte aperte e chiuse, segnalate nella tabella. Per esempio, la porta 22 TCP è aperta, ed è presente il servizio ssh, mentre la porta 25 TCP è chiusa, ed appartiene al servizio smtp. Le altre porte, non presenti in tabella, sono filtrate, come si evince dalla scritta *Not shown: 1709 filtered ports*.

Riassumendo, lo scan SYN Stealth è lo scan di default di Nmap. È veloce, relativamente discreto, e ci dice chiaro e tondo quali porte sono aperte e quali sono chiuse. Prima di analizzare gli altri tipi di scan, più esotici, vediamo le opzioni principali di Nmap che aggiungono utili informazioni ad uno scan "puro" SYN Stealth.

### 4.3 Service e OS Scan

Proviamo ad eseguire questo comando: `nmap -T4 -A -sS scanme.nmap.org`.

L'output sarà del tipo:

```
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT STATE SERVICE VERSION
22/tcp open  ssh OpenSSH 4.3 (protocol 2.0)
25/tcp closed smtp
53/tcp open  domain ISC BIND 9.3.4
70/tcp closed gopher
80/tcp open  http Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp closed auth
Device type: general purpose|specialized|media device|storage-misc|WAP|VoIP
gateway
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (96%), Infoblox NIOS 4.X (93%),
Dream Multimedia Linux 2.6.X (92%), Iomega Linux 2.6.X (92%), FON Linux 2.4.X|2.6.X
(91%), Linksys Linux 2.6.X (90%), Netgear Linux 2.6.X (90%), Tandberg Linux
2.6.X (90%)
Aggressive OS guesses: Linux 2.6.20-1 (Fedora Core 5) (96%), Linux 2.6.9 -
2.6.15 (95%), Infoblox NIOS 4.1r5 (93%), Linux 2.6.9 - 2.6.19 (92%), Linux
2.6.17 - 2.6.21 (92%), Linux 2.6.23 (92%), Linux 2.6.8 (92%), Linux 2.6.9 -
2.6.15 (x86) (92%), Linux 2.6.9 - 2.6.20 (92%), Linux 2.6.9 - 2.6.23 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime: 5.898 days (since Wed Jul 2 14:49:14 2008)

TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 1.69 xx.xx.xx.xx
2 8.46 xx.xx.xx.xx
3 8.13 xx.xx.xx.xx
4 8.62 xx.xx.xx.xx
5 9.78 ae0-17.mil19.ip.tiscali.net (213.200.68.21)
6 183.70 so-0-0-0.sjc11.ip.tiscali.net (213.200.80.89)
7 188.74 213.200.80.134
8 188.22 64.125.30.174
9 190.84 so-4-2-0.mpr3.pao1.us.above.net (64.125.28.142)
10 408.35 metro0.sv.svcolo.com (208.185.168.173)
11 189.66 scanme.nmap.org (64.13.134.52)
```

A prima vista, vediamo che stavolta Nmap ci ha fornito molte più informazioni rispetto al precedente SYN Stealth. In questo caso, infatti, Nmap ha dapprima operato un normale scan SYN Stealth, ma ha anche operato un OS Scan (scansione del sistema operativo), andato a indovinare il sistema operativo in uso (usa Fedora Linux), un Version Scan e Script Scan, che ci hanno fornito ulteriori dettagli dei servizi attivi (vediamo che sulla porta 22 TCP c'è OpenSSH 4.3 che usa il protocollo SSH 2.0, o che sulla porta 80 TCP c'è il server Web Apache 2.2.2), in più è stato fatto un traceroute, ovvero è stato tracciato il percorso che fanno i dati per raggiungere l'obiettivo.

Tutte queste opzioni sono attivate dall'opzione `-A`. Per informazioni dettagliate sull'opzione `-A`, e sulle opzioni che attiva, rimando alla pagina `man` di Nmap (`man nmap`) che spiega molto esaurientemente tutte le opzioni di Nmap.

## 4.4 Ping scan

Passiamo alla funzione più apprezzata dagli amministratori di rete: il ping scan. Questo non controlla le porte di un host, ma si limita a dirci se l'host è attivo o meno. Possiamo vederlo come un sistema automatizzato per "pingare" host remoti, ma è ben più potente del comando ping per i seguenti motivi:

- Nmap permette di controllare automaticamente e molto velocemente intere reti, rendendo semplice e veloce l'individuazione degli host connessi ad una rete.
- Nmap non invia pacchetti ICMP Echo-Request (come viene fatto dall'utility *ping*), in quanto ormai moltissimi firewall li bloccano, ma usa un metodo più intelligente: nelle LAN usa quello che viene chiamato *ARP Ping*, che permette di individuare se un host è connesso o meno bypassando qualunque firewall installato sull'host, altrimenti nelle reti alle quali non siamo direttamente connessi effettua un ping alla porta 80 TCP. Comunque, il modo usato da Nmap per i ping scan può essere ampiamente personalizzato.

Una volta spiegate le potenzialità del ping scan, proviamo a farne uno. Io adesso sto scansionando la mia LAN, quindi sostituite all'indirizzo della mia LAN l'indirizzo della vostra.

```
Il comando è nmap -T4 -sP 192.168.0.0/24, e il risultato è:  
Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-09 12:25 CEST  
Host rfc-1918 (192.168.0.1) appears to be up.  
MAC Address: 00:xx:xx:xx:xx:xx (D-Link)  
Host rfc-1918 (192.168.0.100) appears to be up.  
Host rfc-1918 (192.168.0.101) appears to be up.  
MAC Address: 00:xx:xx:xx:xx:xx (Siemens AG)  
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.800 seconds
```

Osserviamo che Nmap ha elencato gli host attivi all'interno della LAN, indicandone indirizzo, reverse-DNS (chiede ai server DNS se hanno un nome di dominio quegli host), e indirizzo MAC, indicando il nome del produttore, se noto. Siccome ho scansionato una LAN a cui sono collegato direttamente, Nmap ha effettuato un *ARP Ping*, trovando gli host attivi anche quelli protetti da un firewall.

Nel caso si controllino hosts non connessi alla propria LAN, Nmap provvede a scansionare la porta 80 TCP (HTTP) e ad inviare un pacchetto ICMP Echo-Request (usato dall'utility *ping*). Nel caso il gateway che fornisce l'accesso ad internet sia un *transparent proxy*, ovvero che intercetta automaticamente le richieste verso la porta 80 e le mandi ad un server proxy, allora un Ping scan restituirà ogni host da controllare come attivo, in quanto il proxy risponderà sempre ad ogni richiesta! In questo caso è utile l'opzione `-PE`, che obbliga Nmap ad usare solo i pacchetti ICMP Echo-Request per trovare gli host attivi.

Prima di effettuare un qualunque scan, Nmap prima fa sempre un Ping scan agli obiettivi per assicurarsi che siano attivi, e in caso contrario sospende lo scan. Nel caso si sia sicuri che un host è attivo, ma impedisce ogni tentativo di Ping scan, allora si può usare l'opzione `-PN` per impedire il Ping scan iniziale.

## 4.5 Scan speciali

In questa sezione vediamo dei tipi di scan speciali, che usano caratteristiche di rete avanzate per scopi specifici.

### 4.5.1 FIN, Null e Xmas Tree

Questi scan funzionano tutti più o meno allo stesso modo. Viene inviato un pacchetto TCP "impossibile", ovvero un pacchetto FIN (FIN scan), un pacchetto con nessun flag attivato (Null scan) e un pacchetto con i flag FIN, PSH e URG, "accendendo il pacchetto come un albero di Natale" (dalla pagina man di Nmap).

A cosa serve inviare questi pacchetti "impossibili"? Viene sfruttato un particolare nelle specifiche TCP, dove viene prescritto l'invio di un pacchetto RST nel caso venga inviato un pacchetto senza i flag SYN, RST e ACK verso una porta chiusa. Nel caso la porta sia aperta, o filtrata, non si riceverà nulla in risposta.

Che vantaggi si hanno? Bé, il primo vantaggio è che inviando pacchetti "impossibili" è più complicato il rilevamento del port scan, innanzitutto. Il secondo vantaggio è che nel caso il PC da scansionare sia protetto da un firewall *stateless*, lo scan eviterà del tutto il firewall! Purtroppo adesso i firewall sono quasi tutti *stateful*<sup>1</sup>, quindi questo sistema eviterà solo i firewall vecchi.

I comandi per attivare questi tipi di scan sono i seguenti:

**FIN Scan** `-sF`

**Null Scan** `-sN`

**Xmas Tree Scan** `-sX`

Vediamo per esempio uno scan FIN:

```
nmap -T4 -sF scanme.nmap.org
```

```
Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-29 18:28 CEST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1712 open|filtered ports
PORT STATE SERVICE
25/tcp closed smtp
70/tcp closed gopher
113/tcp closed auth
```

```
Nmap done: 1 IP address (1 host up) scanned in 27.405 seconds
```

Osserviamo che questo scan non è stato in grado di distinguere le porte aperte da quelle filtrate, quindi ci ha segnalato solamente le porte chiuse, avendo ricevuto in risposta un pacchetto RST.

---

<sup>1</sup>Si definisce un firewall (inteso come filtro di pacchetti) *stateless* quando si limita a controllare ogni singolo pacchetto senza analizzarne il contesto, mentre un firewall è definito *stateful* quando tiene traccia di tutte le connessioni effettuate, analizzando ciascun pacchetto nel proprio contesto e attribuendolo a connessioni.

## 4.5.2 UDP Scan

Fin'ora ho trattato della scansione delle porte TCP. In questa parte parliamo dell'UDP Scan, che controlla le porte UDP. Il problema è che questo scan è lento e molto meno efficace dello scan TCP, per il fatto che non esiste un metodo standard per UDP di instaurare connessioni, in quanto dipende esclusivamente dall'applicazione in ascolto.

Nmap quindi invia un pacchetto UDP vuoto ad ogni porta. Nel caso si ottenga in risposta un pacchetto ICMP port-unreachable, allora la porta è chiusa. Con altre risposte di errore ICMP, allora la porta è filtrata. Se si ottiene risposta la porta è aperta. Nel caso non si ottenga alcuna risposta dopo numerose ritrasmissioni, allora la porta viene marcata come open—filtered.

Questo è un metodo estremamente empirico, e per questo non è molto accurato. Per questo, si consiglia di abbinarlo ad un version scan (-A) per determinare con precisione i servizi attivi o meno.

Vediamo uno scan UDP:

```
nmap -T4 -sV -sU localhost
```

```
Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-29 18:41 CEST
```

```
Interesting ports on localhost (127.0.0.1):
```

```
Not shown: 1482 closed ports
```

```
PORT STATE SERVICE VERSION
```

```
68/udp open|filtered dhcpc
```

```
111/udp open rpcbind
```

```
123/udp open ntp?
```

```
631/udp open|filtered unknown
```

```
946/udp open|filtered unknown
```

```
5353/udp open|filtered zeroconf
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/
```

```
.
```

```
Nmap done: 1 IP address (1 host up) scanned in 56.430 seconds
```

Vediamo che ha trovato alcune porte aperte o filtrate, e per alcune ha trovato il servizio in esecuzione. Osserviamo che uno scan UDP è meno accurato di uno scan alle porte TCP.

## Capitolo 5

# Conclusioni

In questo tutorial ho spiegato le più diffuse opzioni di Nmap, ma ovviamente non era nel suo scopo l'analisi di tutte le opzioni. Come già detto nell'introduzione, la documentazione completa si può trovare sul sito <http://www.insecure.org>, comprendente tutte le opzioni e funzionalità.

Ora, per "stimolare la curiosità" dei lettori, vediamo alcune delle più sofisticate funzionalità:

**ACK Scan** Questo scan invia pacchetti ACK alle porte, e serve per mappare in maniera veloce ed invisibile le regole di un firewall

**Decoys** In questo modo lo scan non apparirà proveniente dal vostro indirizzo IP, ma fornirete altri indirizzi IP "falsi" per rendere difficoltosa la vostra identificazione

**FTP Bounce** In questo modo sfrutterete un server FTP pubblico per fare un port scan al posto vostro!

## Appendice A

# Riguardo questo documento

Questo documento l'ho scritto nel mio tempo libero in base alla mia esperienza, e quindi è normale che sia dotato di errori e/o imprecisioni. In quanto questo documento è stato rilasciato con licenza GNU Free Documentation License, siete liberi di modificarlo e redistribuirlo nei termini della suddetta licenza. Assieme al documento in formato PDF sono disponibili i sorgenti in formato  $\text{\LaTeX}$  per poter modificare il documento nel formato originale di composizione.

# GNU Free Documentation License

Version 1.2, November 2002  
Copyright © 2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in

part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties; any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and

that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

### 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

### 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add

another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

## 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

## ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with . . . Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.