



Nmap

network scanning

Network Scanning

- Procedura per identificare gli host attivi su una rete:
 - Per valutare la sicurezza della rete
 - Per vedere tutte le porte aperte
 - Per attaccare un sistema
- La procedura di scansione restituisce informazioni su quali servizi questi host (indirizzi IP attivi nella rete)
 - ping sweeps
 - port scans

nmap

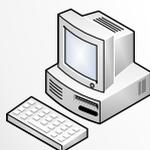
- È fra i più potenti e diffusi software open source per effettuare network scanning.
- Nmap (acronimo di "Network Mapper") è presente sulla rete ormai da anni
- Sono state rilasciate varie versioni, compatibili con molti sistemi operativi. <http://nmap.org/download.html>
- Nmap è uno degli strumenti praticamente indispensabili della "cassetta degli attrezzi" di un network administrator
- Usato per
 - analisi dei sistemi
 - test di penetrazione
 - analisi di sicurezza

• Marcantoni Fausto

• 3

nmap

- Creato per effettuare port scanning: individuare porte aperte e servizi disponibili su un computer target.
- Utilizza la tecnica del fingerprinting: è in grado di ipotizzare quale sistema operativo sia utilizzato dal computer bersaglio.



Host nmap



server target

| PORT | STATE | SERVICE |
|----------|----------|---------------------|
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 53/tcp | open | domain |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 111/tcp | filtered | rpcbind |
| 112/tcp | filtered | ncidas |
| 137/tcp | filtered | netbios-ns |
| 138/tcp | filtered | netbios-dgm |
| 139/tcp | filtered | netbios-ssn |
| 161/tcp | filtered | snmp |
| 162/tcp | filtered | snmptrap |
| 343/tcp | filtered | unknown |
| 443/tcp | open | https |
| 445/tcp | filtered | microsoft-ds |
| 587/tcp | open | submission |
| 993/tcp | open | pop3s |
| 1720/tcp | filtered | ii_sn2/Q.931 |
| 2049/tcp | filtered | nfs |
| 3306/tcp | filtered | mysql |
| 6881/tcp | filtered | bit torrent-tracker |

• Marcantoni Fausto

• 4

nmap

- Utilizza pacchetti IP per ottenere informazioni :
 - gli host presenti/attivi su una rete
 - i servizi che tali host rendono disponibili
 - i sistemi operativi presenti sull'host target
 - la presenza di firewall – ids/ips
 - monitor/diagnostica di host
 - troubleshooting ("eliminazione del problema")
 - altro (virus, ...)

• Marcantoni Fausto

• 5

nmap: lo stato delle porte

- Le porte rilevate possono essere:
 - **Open** – Una applicazione accetta attivamente connessioni TCP o UDP su questa porta.
 - **Closed** – Una porta chiusa è accessibile, ma non vi è alcuna applicazione in ascolto su di essa.
 - **Filtered** – Nmap non può determinare con esattezza se la porta sia aperta o meno in quanto un filtro ne impedisce l'accesso.
 - **Unfiltered** – la porta è accessibile, ma Nmap non può determinarne lo stato.
 - **Open | filtered** – Nmap non è in grado di determinare se una porta è aperta oppure filtrata.
 - **Closed | filtered** – Nmap non è in grado di determinare se una porta è chiusa oppure filtrata.

• Marcantoni Fausto

• 6

nmap: Target Specification

un indirizzo IP
 un nome di host per la scansione
 un gruppo di indirizzi IP
 un'intera rete di host adiacenti notazione CIDR (192.168.3.0/24)

nmap 192.168.3.12

nmap www.cs.unicam.it

nmap 192.168.3.23-37

nmap 192.168.3.0/24

Indirizzi IPv6

nmap [host]

nmap www.cs.unicam.it

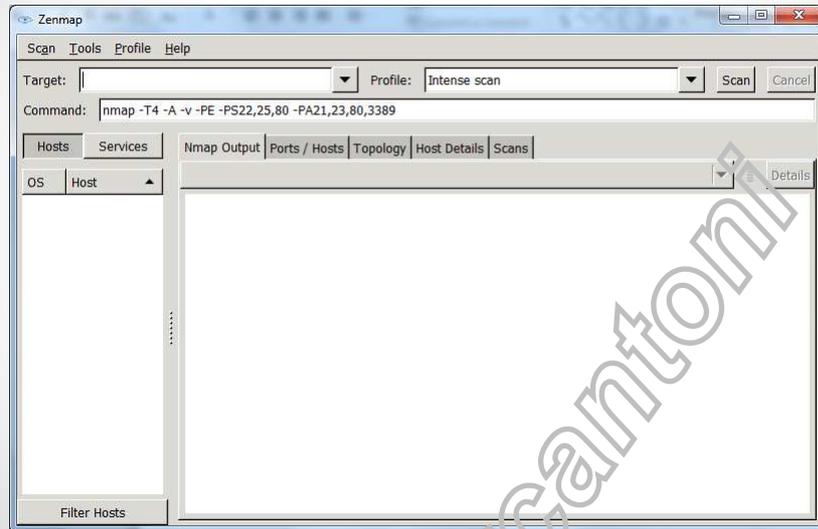
```

C:\Users\fausto>nmap www.cs.unicam.it
Starting Nmap 5.00 ( http://nmap.org ) at 2011-10-27 12:41 ora legale Europa occidentale
Interesting ports on www.cs.unicam.it (193.205.92.31):
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  smb
445/tcp   open  microsoft-ds
10000/tcp open  net-sensor-mgmt
MAC Address: 00:0C:29:AD:A4:63 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.66 seconds
C:\Users\fausto>
  
```

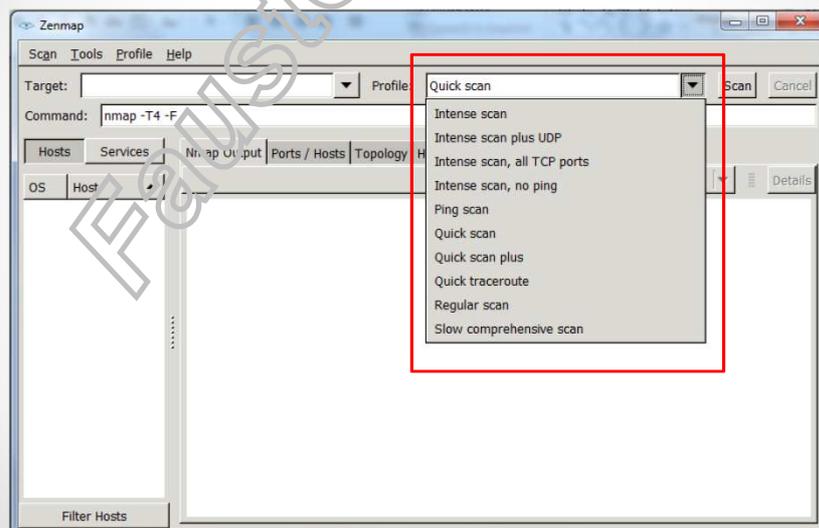
nmap: zenmap

Zenmap: Interfaccia GUI per nmap



nmap: zenmap

Zenmap: profili già definiti



Profile Zenmap

Intense scan

command = `nmap -T4 -A -v`

An intense, comprehensive scan. The `-A` option enables OS detection (`-O`), version detection (`-sV`), script scanning (`-sC`), and traceroute (`--traceroute`). Without root privileges only version detection and script scanning are run. This is considered an intrusive scan.

Intense scan plus UDP

command = `nmap -sS -sU -T4 -A -v`

Does OS detection (`-O`), version detection (`-sV`), script scanning (`-sC`), and traceroute (`--traceroute`) in addition to scanning TCP and UDP ports.

Intense scan, all TCP ports

command = `nmap -p 1-65535 -T4 -A -v`

Scans all TCP ports, then does OS detection (`-O`), version detection (`-sV`), script scanning (`-sC`), and traceroute (`--traceroute`).

Intense scan, no ping

command = `nmap -T4 -A -v -Pn`

Does an intense scan without checking to see if targets are up first. This can be useful when a target seems to ignore the usual host discovery probes.

Ping scan

command = `nmap -sn`

This scan only finds which targets are up and does not port scan them.

Quick scan

command = `nmap -T4 -F`

This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.

Quick scan plus

command = `nmap -sV -T4 -O -F --version-light`

A quick scan plus OS and version detection.

Quick traceroute

command = `nmap -sn --traceroute`

Traces the paths to targets without doing a full port scan on them.

Regular scan

command = `nmap`

A basic port scan with no extra options.

Slow comprehensive scan

command = `nmap -sS -sU -T4 -A -v -PE -PS80,443 -PA3389 -PP -PU40125 -PY --source-port 33 --script all`

This is a comprehensive, slow scan. Every TCP and UDP port is scanned. OS detection (`-O`), version detection (`-sV`), script scanning (`-sC`), and traceroute (`--traceroute`) are all enabled. Many probes are sent for host discovery. This is a highly intrusive scan.

nmap: Regular Scan

Regular Scan

The screenshot shows the Zenmap interface with the following details:

- Target:** 193.205.92.56
- Profile:** Quick scan
- Command:** `nmap -T4 -F 193.205.92.56`
- Hosts:** dida.cs.unicam.it
- OS:** nmap -T4 -F 193.205.92.56
- Output:**

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-07 17:32 ora legale Europa occidentale
Nmap scan report for dida.cs.unicam.it (193.205.92.56)
Host is up (0.000058s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:50:56:A2:78:AF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

Elenco delle opzioni

<http://www.insecure.org/nmap/data/nmap.usage.txt>

```
Usage: nmap [Scan Type(s)] [Options] (target specification)
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0-255.0-255.1-254
  -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
HOST DISCOVERY:
  -sL List Scan - simply list targets to scan
  -sP Ping Scan - go no further than determining if host is online
  -P0 Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery probes to given ports
  -PE/PP/PM ICMP echo, timestamp, and netmask request discovery probes
  -n/R: Never do DNS resolution/Always resolve [default: sometimes resolve]
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[probeport]>: Idlescan
  -sO: IP protocol scan
  -b <ftp relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast - Scan only the ports listed in the nmap-services file
  -r: Scan ports consecutively - don't randomize
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-light: Limit to most likely probes for faster identification
  --version-all: Try every single probe for version detection
  --version-trace: Show detailed version scan activity (for debugging)
OS DETECTION:
  -O: Enable OS detection
```

Ping sweep

- Vengono inviati dei pacchetti **ICMP (Internet Control Message Protocol)**, in particolare dei pacchetti Tipo 8 (**echo request**), conosciuti anche come pacchetti ping che identificano se un host è attivo.
- Ci sono anche altri pacchetti ICMP che possono risultare utili, ad esempio:
 - **Tipo 13 (timestamp request)** – viene richiesto il tempo di sistema di un host target
 - **Tipo 15 (information request)** – è un particolare messaggio creato per supportare alcuni sistemi auto-configuranti (ad esempio diskless workstation) che nel boot devono poter trovare il proprio indirizzo nella rete.
 - **Tipo 17 (subnet address mask request)** – con questo messaggio riusciamo a determinare la subnet mask usata dall'host.

Ping Sweep - Nmap

- Nmap può effettuare ping sweep scans, utilizzando l'opzione `-sP`
- esempio:
- `nmap -sP 193.205.92.0/24` oppure `193.205.92.1-10`

```

C:\Users\fausto>nmap -sP 193.205.92.1-10
Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-07 13:04 ora legale Europa occidentale
Host nameserver.cs.unican.it (193.205.92.1) is up (0.00s latency).
MAC Address: 00:50:56:A2:72:9D (VMware)
Host test.cs.unican.it (193.205.92.2) is up (0.00s latency).
MAC Address: 00:0E:30:39:10:3F (Cisco Systems)
Host 193.205.92.3 is up (0.00s latency).
MAC Address: 00:50:56:A2:3F:41 (VMware)
Host www1.cs.unican.it (193.205.92.5) is up (0.00s latency).
MAC Address: 00:0C:29:0A:42:F9 (VMware)
Host 193.205.92.6 is up (0.00s latency).
MAC Address: 00:25:B3:F2:2F:82 (Hewlett Packard)
Host tele.informatica.unican.it (193.205.92.7) is up (0.00s latency).
MAC Address: 00:0C:29:05:73:DD (VMware)
Host 193.205.92.8 is up (0.00s latency).
MAC Address: 00:17:A4:A7:20:22 (Hewlett Packard)
Host 193.205.92.10 is up (0.00s latency).
MAC Address: 00:40:0C:91:FB:00 (Axis Communications AB)
Nmap done: 10 IP addresses (8 hosts up) scanned in 7.21 seconds
C:\Users\fausto>

```

• Marcantoni Fausto

• 15

Port Scanning

- Il Port Scanning è un processo di connessione a porte TCP e UDP del sistema target al fine di determinare **quali porte siano aperte** e quali servizi siano in stato di esecuzione o in stato di listening su quelle porte
- Un amministratore di sistema deve poter **identificare i servizi offerti dai propri server** ed identificare eventuali debolezze della propria rete e dei propri sistemi, col fine di evitarne lo sfruttamento da parte di utenti indesiderati.

• Marcantoni Fausto

• 16

TCP port scanning

- Esistono diversi tipi di port scanning per controllare se le porte TCP di un sistema sono aperte o chiuse, questi sono classificabili in tre classi:
 - **Standard scanning methods**
 - Vanilla TCP connect() scanning
 - Half-open SYN flag scanning
 - **Stealth TCP scanning methods**
 - Inverse TCP flag scanning
 - ACK flag probe scanning
 - TCP fragmentation scanning
 - **Third-party and spoofed TCP scanning methods**
 - FTP bounce scanning
 - Proxy bounce scanning
 - Sniffer-Based spoofed scanning
 - IP ID header scanning

Standard scanning methods

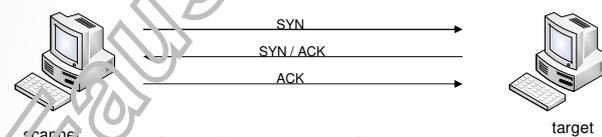
- I metodi definiti nella categoria Standard scanning methods sono delle tecniche **molto semplici** e dirette, usate per identificare le porte e i servizi TCP accessibili in modo accurato.
- Questi sono metodi certi, ma possono essere **facilmente rilevati e loggati**.

Vanilla TCP connect() method

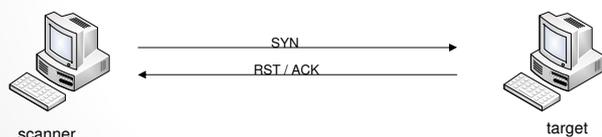
- È il metodo più semplice, conosciuto anche come **TCP connect()** o **Vanilla connect()**
- Viene stabilita **un'intera connessione TCP/IP** con una porta TCP dell'host target
- Data l'affidabilità del protocollo TCP/IP, questo metodo è **molto accurato** per determinare quali servizi sono attivi in un dato host

Vanilla TCP connect() method

pacchetti inviati da questo metodo (**three way handshake**)



Quando una porta è aperta



Quando una porta è chiusa

Vanilla TCP connect() method - Nmap

Nmap può effettuare un TCP connect() portscan, utilizzando l'opzione `-sT`

`nmap -sT 193.205.92.108`

```

C:\>nmap -sT 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 11:52 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.00s latency).
Not shown: 977 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:BB:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 43.06 seconds
C:\>

```

• Marcantoni Fausto

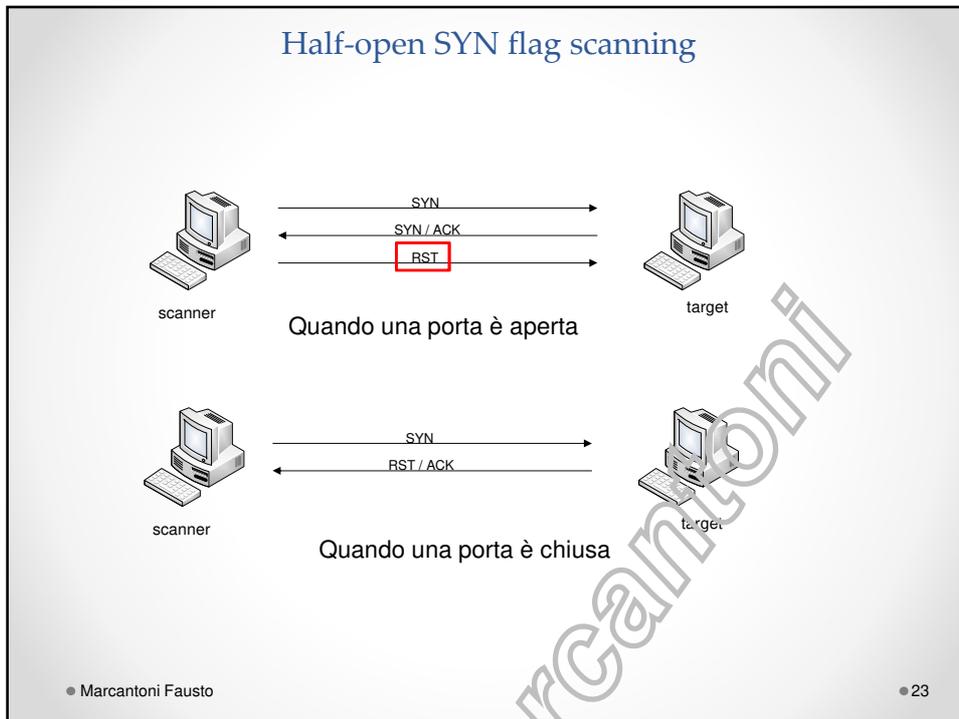
• 21

Half-open SYN flag scanning

- In modo simile al metodo TCP connect(), si **simula un inizio di connessione** come se fosse un three way handshake per sincronizzazione i due host
- Nel caso dell'**half open SYN port scanning**, quando una porta viene rilevata aperta, viene inviato un pacchetto con **flag RST** che resetta la connessione TCP
- Questo fa sì che non ci sia una completa connessione fra i due host, e quindi sia più **difficile rilevare e loggare lo scanning**

• Marcantoni Fausto

• 22



Half-open SYN flag scanning - Nmap

Nmap può effettuare un SYN scan utilizzando l'opzione `-sS`

```

nmap -sS 193.205.92.108
C:\>nmap -sS 193.205.92.108
Starting Nmap 5.0 (https://nmap.org) at 2017-10-27 11:59 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.0002s latency).
Not shown: 655 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
57/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0c:29:8b:ab:1d (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
C:\>
    
```

● Marcantoni Fausto

● 24

Stealth TCP scanning methods

- Questi metodi sfruttano **alcune lacune del protocollo TCP/IP**, provocate inviando pacchetti con configurazioni di bit non standard.
- Queste tecniche non mappano le porte aperte in modo accurato, però **lavorano in modo nascosto** e **difficilmente possono essere rilevati e loggati**.



• Marcantoni Fausto

• 25

Inverse TCP flag scanning

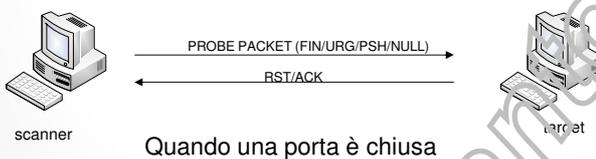
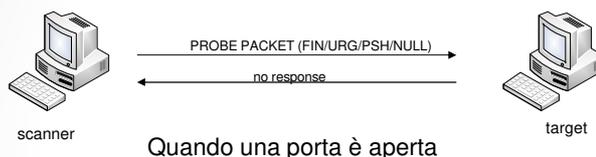
- Questo tipo di scanning viene chiamato **inverse** in quanto rispondono **solo le porte chiuse** di un sistema
- Vengono inviati dei pacchetti "**sonda**" con diversi flag settati, ad esempio:
 - FIN probe, con il FIN TCP flag settato
 - L'XMAS probe con i FIN,URG,PUSH TCP flag settati
 - NULL probe con nessun flag TCP settato

• Marcantoni Fausto

• 26

Inverse TCP flag scanning

Ecco come avvengono le comunicazioni utilizzando questo metodo:



Inverse TCP flag scanning - Nmap

- Nmap può effettuare un TCP flag portscan, utilizzando le opzioni:
 - sF per il FIN probe
 - sX per l'XMAS Tree probe
 - sN per il NULL probe

nmap -sF 193.205.92.108

```

C:\>nmap -sF 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:00 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.0019s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  filtered telnet
25/tcp    open  filtered smtp
53/tcp    open  filtered domain
80/tcp    open  filtered http
111/tcp   open  filtered rpcbind
139/tcp   open  filtered netbios-ssn
445/tcp   open  filtered microsoft-ds
512/tcp   open  filtered exec
513/tcp   open  filtered login
514/tcp   open  filtered shell
1099/tcp  open  filtered rairegistry
1524/tcp  open  filtered ingreslock
2049/tcp  open  filtered nfs
2121/tcp  open  filtered cproxy-ftp
3306/tcp  open  filtered mysql
5432/tcp  open  filtered postgresql
5900/tcp  open  filtered vnc
6000/tcp  open  filtered x11
6667/tcp  open  filtered irc
8009/tcp  open  filtered ajp13
8180/tcp  open  filtered unknown
MAC Address: 00:0c:29:88:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.61 seconds
C:\>

```

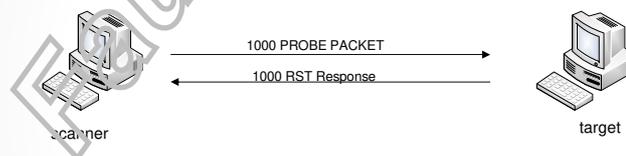
Come vediamo in questo caso **Nmap riesce anche a dirci se la porta in questione è open|filtered** in quanto il sistema, se una porta è aperta non risponde, ma lo stesso avviene se una porta è filtered e quindi inaccessibile

ACK flag probe scanning

- Un altro metodo consiste nell'inviare dei pacchetti ACK ed analizzare il pacchetto RST ottenuto in risposta.
- Ci sono due parametri principali da osservare:
 - il time-to-live (ttl)
 - il parametro WINDOW (win)
- Questo sistema è molto difficile da rilevare, ma per funzionare sfrutta un bug nell'implementazione dello standard TCP/IP che non è più presente nei sistemi più aggiornati

ACK flag probe scanning

Vengono spediti moltissimi pacchetti ACK verso porte TCP diverse

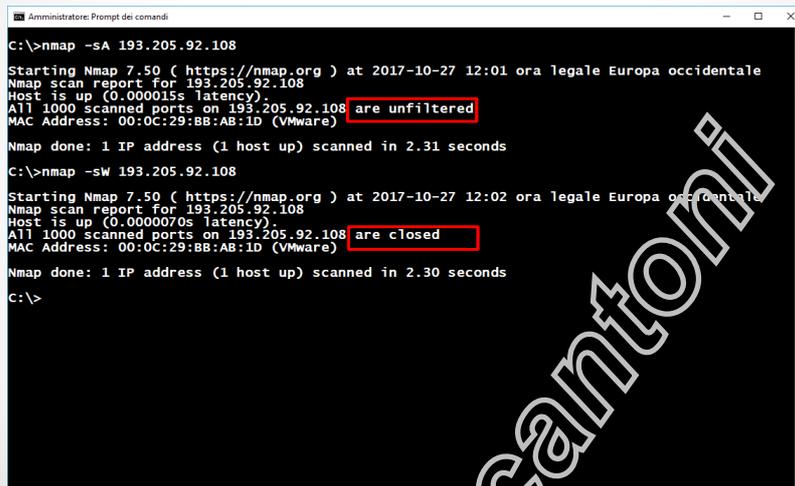


Questo scan fa affidamento a un dettaglio implementativo di una minoranza di sistemi presenti in internet, segue che questo non è sempre affidabile

ACK flag probe scanning

Nmap può effettuare un ACK flag probe scanning, usando le opzioni:

- sA per analizzare il parametro ttl
- sW per analizzare il parametro win



```

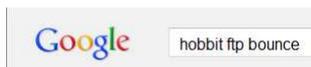
C:\>nmap -sA 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:01 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.000015s latency).
All 1000 scanned ports on 193.205.92.108 are unfiltered
MAC Address: 00:0C:29:BB:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
C:\>nmap -sW 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:02 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.0000070s latency).
All 1000 scanned ports on 193.205.92.108 are closed
MAC Address: 00:0C:29:BB:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
C:\>
  
```

FTP bounce attack

- Una "caratteristica" interessante del protocollo ftp (RFC 959) è il supporto per le connessioni ftp "proxy". In altre parole, io dovrei essere in grado di connettermi da mioftp.com al server FTP di target.com e richiedere che tale server mandi un file OVUNQUE su internet!
- Ora questo poteva andare bene nel 1985 quando la RFC fu scritta.
- Come Hobbit scrisse nel 1995, questo punto debole nel protocollo "può essere usato per postare mail e news virtualmente irrintracciabili, riempire i dischi, provare a scavalcare i firewall, e generalmente è fastidioso e difficile da rintracciare allo stesso tempo."



<https://nmap.org/hobbit.ftpbounce.txt>

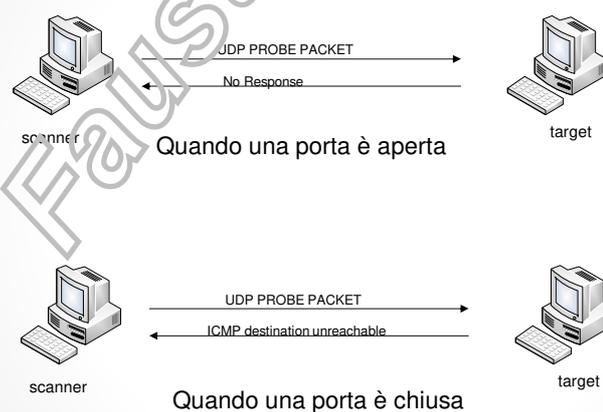
UDP port scanning

- Il protocollo **UDP (user datagram protocol)**, consente di stabilire quali porte possono essere aperte in un host, in soli due modi:
 - Inviando **pacchetti UDP probe** a tutte le porte UDP di un host (65535), e aspettando i messaggi "ICMP destination port unreachable"
 - Oppure **usando degli specifici client per servizi UDP** e controllando se ci sono delle risposte da degli host (che in caso positivo possiedono il servizio)
- La maggior parte dei firewall però consente di **filtrare i messaggi ICMP**, da e per gli host protetti, questo rende difficile capire quali servizi UDP sono accessibili, attraverso un semplice UDP port scanning

• Marcantoni Fausto

• 33

UDP port scanning



• Marcantoni Fausto

• 34

UDP port scanning - Nmap -

- Nmap può effettuare l'UDP port scanning, utilizzando l'opzione -sU

nmap -sU 193.205.92.108

```

Amministratore: Prompt dei comandi
C:\>nmap -sU 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 11:53 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.000088s latency).
Not shown: 946 closed ports, 50 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 00:0C:29:BB:AB:1D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1033.00 seconds
C:\>

```

● Marcantoni Fausto

● 35

UDP port scanning - Nmap -

- Nmap può effettuare l'UDP port scanning, con una porta specifica o con un gruppo di porte utilizzando l'opzione -sU

nmap -sU -p 2002 193.205.92.108

```

Amministratore: Prompt dei comandi
C:\>nmap -sU -p 2002 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:03 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.005147s latency).
PORT      STATE SERVICE
2002/udp  open  liveris-globe
MAC Address: 00:0C:29:BB:AB:1D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
C:\>

```

● Marcantoni Fausto

● 36

Fingerprinting

- Ogni sistema operativo possiede una propria interpretazione degli standard del protocollo IP
- Analizzando le risposte ottenute, inviando alcuni pacchetti TCP ed UDP ad un host remoto, si può determinare il sistema operativo presente
- Nmap ad esempio compara i risultati ottenuti con il suo database, contenente oltre 1500 SO, e ne visualizza i dettagli se trova riscontri

• Marcantoni Fausto

• 37

Fingerprinting - Nmap -

- Nmap effettua il fingerprinting utilizzando l'opzione `-O`

nmap -O 193.205.92.108

```

Administrator: Prompt dei comandi
c:\>nmap -O 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:04 ora legale Europea occidentale
Nmap scan report for 193.205.92.108
Host is up (0.013s latency)
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  smb
445/tcp   open  microsoft-ds
512/tcp   open  xtcp
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  nfs-registry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  http
8180/tcp  open  unknown
MAC Address: 00:0C:29:BB:AB:1D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
c:\>

```

• Marcantoni Fausto

• 38

Service e Version Detection

- Si possono sfruttare i messaggi ricevuti in risposta da porte aperte in un host target, oltre che per la determinazione del SO, anche per altre funzionalità avanzate
- Nmap, ad esempio, è in grado di analizzare i messaggi ottenuti da una porta di un host e confrontarli con un suo database interno con oltre 2200 servizi

Service e Version Detection

- Questa funzionalità diventa di fondamentale importanza per un amministratore di sistema.
- Infatti conoscendo queste informazioni, e confrontandole con opportuni database, si può determinare a quali bugs è vulnerabile il server.
- Purtroppo lo stesso procedimento può essere effettuato da utenti malintenzionati che possono sfruttare tali bugs per controllare servizi e dati dell'host target.

Service e Version Detection

- nmap può utilizzare l'opzione -sV per "Version Detection"

nmap -sV 193.205.92.108

```

C:\>nmap -sV 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:06 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.00043s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  rmiregistry   GNU Classpath grmiregistry
1524/tcp  open  shell         Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8095/tcp  open  ajp13        Apache Jserv (protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port:514-TCP:V=7.50O=700-10/27X=1665-1665-oc-windows-windows
SF:(NULL,45,"x01couldn't\x20get\x20address\x20for\x20your\x20host\x20on
SF:(fausto.administrazione.unicam)\n")%r(GetRequest,45,"x01couldn't\x20
SF:get\x20address\x20for\x20your\x20host\x20(mfausto.administrazione.19
SF:(cam)\n");
MAC Address: 00:0C:29:8B:AB:1D (Vmware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OS: Unix
Linux; CPE: o:/linux/linux_kernel
  
```

• Marcantoni Fausto

• 41

Service e Version Detection

- nmap può utilizzare le opzioni -A per abilitare contemporaneamente sia "OS Detection" che "Version Detection"

nmap -A 193.205.92.108

```

C:\>nmap -A 193.205.92.108
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:09 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.00006s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE        VERSION
15/tcp    open  ftp            vsftpd 2.3.4
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN.
|_ssl-cert: subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
|_ssl-cert: there is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2017-10-27T10:12:06+00:00; -17s from scanner time.
sslv2:
SSLv2 supported
cipher:
SSL2_RC2_128_CBC_WITH_MD5
SSL2_RC4_128_WITH_MD5
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
53/tcp    open  domain        ISC BIND 9.4.2
dns-nsid:
bind.version: 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind       2 (RPC #100000)
rpcinfo:
program version port/proto service
100000 2 111/tcp rpcbind
  
```

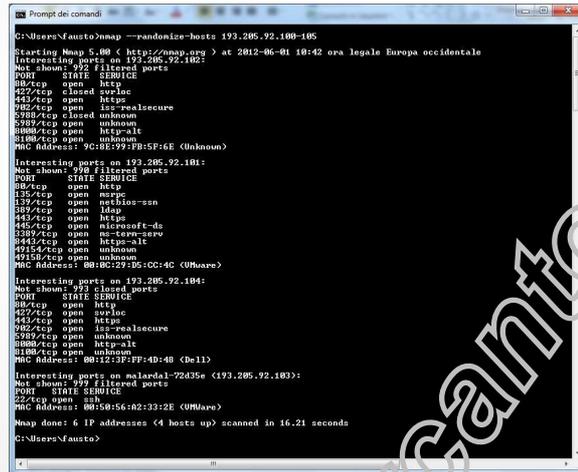
• Marcantoni Fausto

• 42

nmap - Random Order

nmap può randomizzare lo scan degli host

```
nmap --randomize-hosts 193.205.92.0/24
nmap --randomize-hosts 193.205.92.100-200
```



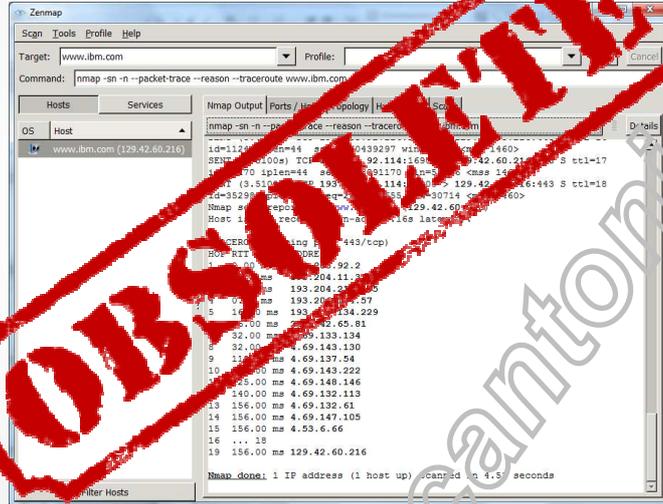
nmap - traceroute

tracert www.ibm.com



nmap - traceroute

```
nmap -sP --traceroute --reason -n --packet-trace www.ibm.com
```

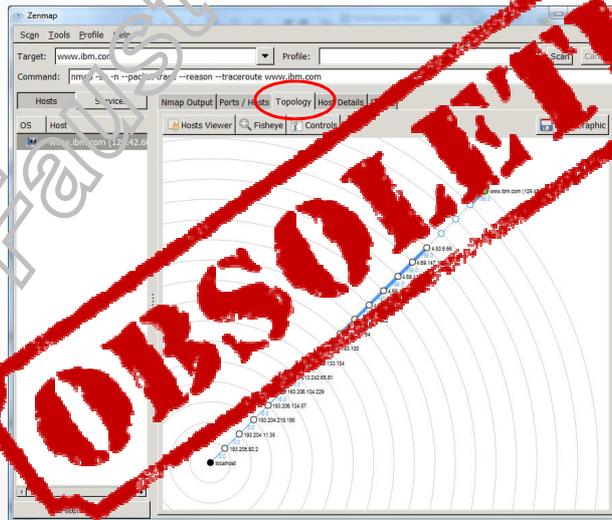


● Marcantoni Fausto

● 45

nmap - traceroute

```
nmap -sP --traceroute --reason -n --packet-trace www.ibm.com
```



● Marcantoni Fausto

● 46

nmap - traceroute

nmap -sP --traceroute --reason -n --packet-trace www.ibm.com

```

root@pentest:~# nmap -sP --traceroute --reason -n --packet-trace www.ibm.com
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-19 09:40 CET
SENT (0.28035) ICMP [193.205.92.99 > 23.1.74.26 Echo request (type=8/code=0) id=54920 seq=0] IP [ttl=59 id=54451 ipLen=28 ]
SENT (0.28045) TCP [193.205.92.99:53261 > 23.1.74.26:80 A ttl=38 id=5931 ipLen=44 seq=4150089185 win=1824 <mss 1460>
SENT (0.28055) TCP [193.205.92.99:53261 > 23.1.74.26:80 A ttl=51 id=5813 ipLen=40 seq=0 win=1824
SENT (0.28065) ICMP [193.205.92.99 > 23.1.74.26 Timestamp request (type=13/code=0) id=49965 seq=0 orig=0 recv=0 trans=0] IP [ttl=47 id=38902 ipLen=40 ]
RcvD (0.28095) TCP [23.1.74.26:80 > 193.205.92.99:53261 RA ttl=254 id=54826 ipLen=40 seq=4150089185 win=1824
SENT (0.28835) TCP [193.205.92.99:61584 > 23.1.74.26:80 A ttl=10 id=38889 ipLen=40 seq=4081214763 win=21712
SENT (0.28845) TCP [193.205.92.99:61585 > 23.1.74.26:80 A ttl=9 id=36249 ipLen=40 seq=920528368 win=17104
SENT (0.28855) TCP [193.205.92.99:61586 > 23.1.74.26:80 A ttl=8 id=17641 ipLen=40 seq=609687590 win=29749
SENT (0.28865) TCP [193.205.92.99:61587 > 23.1.74.26:80 A ttl=7 id=33161 ipLen=40 seq=2641256326 win=50111
SENT (0.28875) TCP [193.205.92.99:61588 > 23.1.74.26:80 A ttl=6 id=53894 ipLen=40 seq=3121807236 win=64099
SENT (0.28885) TCP [193.205.92.99:61589 > 23.1.74.26:80 A ttl=5 id=58918 ipLen=40 seq=495142860 win=9420
SENT (0.28895) TCP [193.205.92.99:61590 > 23.1.74.26:80 A ttl=4 id=51535 ipLen=40 seq=1326898320 win=54301
SENT (0.28905) TCP [193.205.92.99:61591 > 23.1.74.26:80 A ttl=3 id=35037 ipLen=40 seq=1368105806 win=64540
SENT (0.28915) TCP [193.205.92.99:61592 > 23.1.74.26:80 A ttl=2 id=58767 ipLen=40 seq=178937881 win=57859
SENT (0.28915) TCP [193.205.92.99:61593 > 23.1.74.26:80 A ttl=1 id=24133 ipLen=40 seq=2766992586 win=6059
RcvD (0.28865) TCP [23.1.74.26:80 > 193.205.92.99:61584 RA ttl=254 id=41485 ipLen=40 seq=885924960 win=21712
RcvD (0.28875) TCP [23.1.74.26:80 > 193.205.92.99:61585 RA ttl=254 id=49398 ipLen=40 seq=3445877334 win=17184
RcvD (0.28895) TCP [23.1.74.26:80 > 193.205.92.99:61587 RA ttl=254 id=33619 ipLen=40 seq=616124656 win=50111
RcvD (0.28895) TCP [23.1.74.26:80 > 193.205.92.99:61586 RA ttl=254 id=52828 ipLen=40 seq=71692901 win=29749
RcvD (0.28905) TCP [23.1.74.26:80 > 193.205.92.99:61588 RA ttl=254 id=35730 ipLen=40 seq=933830085 win=64099
RcvD (0.28915) TCP [23.1.74.26:80 > 193.205.92.99:61589 RA ttl=254 id=57684 ipLen=40 seq=3897875125 win=9420
RcvD (0.28915) TCP [23.1.74.26:80 > 193.205.92.99:61590 RA ttl=254 id=62091 ipLen=40 seq=3597012536 win=54301
RcvD (0.28925) TCP [23.1.74.26:80 > 193.205.92.99:61591 RA ttl=254 id=35649 ipLen=40 seq=3315646858 win=64540
RcvD (0.28955) TCP [23.1.74.26:80 > 193.205.92.99:61592 RA ttl=254 id=58525 ipLen=40 seq=3939971650 win=57859
RcvD (0.28955) ICMP [193.205.92.99 > 193.205.92.99 TTL=0 during transit (type=1/code=0) ] IP [ttl=255 id=23397 ipLen=60 ]
Nmap scan report for www.ibm.com (23.1.74.26)
Host is up, received reset ttl 254 (0.80040s latency).
Other addresses for www.ibm.com (not scanned): 2a02:26f0:4:19a::b3a 2a02:26f0:4:183::b3a

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.40 ms 193.205.92.2
2 0.48 ms 23.1.74.26

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@pentest:~#

```

● Marcantoni Fausto

● 47

nmap - fragmentation

nmap può frammentare i pacchetti per evitare un firewall

nmap -f 193.205.92.108

```

Administrator: Prompt dei comandi
C:\>nmap -f 193.205.92.108
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.
This may or may not work.

Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-27 12:17 ora Legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.00047s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  xec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  sftp
8180/tcp  open  unknown
MAC Address: 00:0C:29:BB:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
C:\>

```

● Marcantoni Fausto

● 48

nmap - fragmentation

The screenshot shows a list of network packets. Packet 8 is highlighted with a red box. Its details pane shows it is an Internet Protocol Version 4 (IP) packet with a length of 20 bytes. The data field is highlighted with another red box and labeled 'Data (8 bytes)'. The data content is shown as hexadecimal and ASCII: 'df7006bb8341877'.

Frammentazione

Frammenti da 8 byte

● Marcantoni Fausto ● 49

nmap - traceroute "2" LA VENDETTA

nmap -sn -f --traceroute www.libero.it

The screenshot shows the Zenmap interface. The command field contains 'nmap -sn -f --traceroute www.libero.it'. The output window shows the following results:

```

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-02 10:33 ora
legale Europa occidentale
Martianna Packet: Fragmentation selected on a host other than
Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.
Nmap scan report for www.libero.it (151.1.67.216)
Host is up (0.677s latency).
Other addresses for www.libero.it (not scanned): 151.1.67.221
151.1.67.227 151.1.67.215
rDNS record for 151.1.67.216: vhp-d6.rmce.libero.it

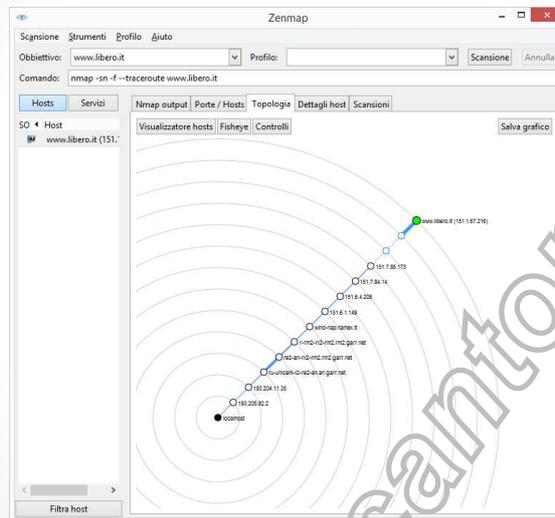
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.00 ms 193.205.92.2
2 0.00 ms 193.204.11.35
3 15.00 ms ru-unicam-12-rn2-an.an.garr.net (193.204.218.185)
4 175.00 ms re2-an-rn2-rn2.rm2.garr.net (90.147.81.9)
5 62.00 ms r-rn2-rx2-rn2.rm2.garr.net (90.147.80.57)
6 19.00 ms wind-nsp.namex.it (193.201.28.11)
7 19.00 ms 151.6.1.149
8 19.00 ms 151.6.4.205
9 23.00 ms 151.7.84.14
10 23.00 ms 151.7.85.173
11 ... 12
13 258.00 ms vhp-d6.rmce.libero.it (151.1.67.216)

Nmap done: 1 IP address (1 host up) scanned in 12.61 seconds
    
```

● Marcantoni Fausto ● 50

nmap – traceroute - "2" LA VENDETTA

```
nmap -sn -f --traceroute www.libero.it
```



● Marcantoni Fausto

● 51

nmap – decoy address

nmap può inviare i pacchetti con un indirizzo «esca» per evitare un firewall

```
nmap -D 193.205.92.253 193.205.92.108
```

```
nmap -D [decoy] [target]
```

```
nmap -D RND:10 [target] (Generates a random number of decoys)
```

```
nmap -D decoy1,decoy2,decoy3 etc. (Manually specify the IP addresses of the decoys)
```

```

c:\>nmap -D 193.205.92.253 193.205.92.108
Starting Nmap 7.50 (http://nmap.org) at 2017-10-27 12:27 ora legale Europa occidentale
Nmap scan report for 193.205.92.108
Host is up (0.0039s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:BB:AB:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
c:\>

```

● Marcantoni Fausto

● 52

nmap - decoy address

decoy address

Frame 1: 60 bytes captured on interface (60 bytes captured) (480 bits)

Ethernet II, Src: Quantico_37:66:be (00:25:9e:57:66:be), Dst: Intel_b0:17:91 (00:04:23:b0:17:91)

Internet Protocol Version 4, Src: 193.205.92.253 (193.205.92.253), Dst: 193.205.92.145 (193.205.2.145)

Transmission Control Protocol, Src Port: 62560 (62560), Dst Port: http-alt (8080), Seq: 0, Len: 0

● Marcantoni Fausto

● 53

nmap - decoy address

L'opzione `-D` è usata per mascherare uno scan di porte usando uno o più IP "esca", questo fa sembrare all'host remoto che gli hosts specificati come esche stiano facendo anche loro una scansione della rete di destinazione.

nmap -D [decoy] [target]

Sintassi: `nmap -D [decoy1, decoy2, decoy3, etc] RND:Number [IP destinazione]`

nmap -D 192.168.1.33 192.168.1.31 192.168.1.32 **192.138.1.34**

In questo esempio l'indirizzo ip in grassetto è l'indirizzo IP del bersaglio remoto

Inoltre, durante l'esecuzione di una scansione con esca, Nmap manderà ulteriori pacchetti dal numero specificato di indirizzo esca.

Questo fa sembrare effettivamente che l'obiettivo sia sottoposto a scansione da più sistemi contemporaneamente.

Utilizzando le esche l'ip sorgente si "**mescola nella folla**" cosa che lo rende più difficile da rintracciare.

● Marcantoni Fausto

● 54

nmap - Idle Zombie Scan

Questa tecnica consente di utilizzare un altro host della rete che è inattivo. Il principale vantaggio di questo metodo è che i file di log del firewall registra l'indirizzo IP dello Zombie e non il nostro IP. Tuttavia per avere un risultato ottimale **bisogna trovare padroni di casa che sono inattivi sulla rete.**

```
nmap -sI 193.205.92.69 193.205.92.145
nmap -sI [zombie host] [target]
```

```
Prompt dei comandi
C:\Users\fausto>nmap -sI 193.205.92.69 193.205.92.145
WARNING: Many people use -PN w/IdleScan to prevent pings from their true IP. On the other hand, timing i
p, more reliable scans.
Starting Nmap 7.00 (http://nmap.org) at 2018-06-01 11:35 ora legale Europa occidentale
Idle scan using zombie 193.205.92.69 (193.205.92.69:443); Class: Incremental
Interesting ports on 193.205.92.145:
Not shown: 997 closed/filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
902/tcp   open  iss-realsecure
MAC Address: 00:04:23:B0:17:91 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 17.11 seconds
C:\Users\fausto>
```

● Marcantoni Fausto

● 55

nmap - Idle Zombie Scan

bisogna trovare padroni di casa che sono inattivi sulla rete

Internet si basa sull'unione di due protocolli fondamentali: TCP e IP, quando host A si collega ad host B, invierà un pacchetto TCP contenente un flag SYN attivo all'interno del quale vi sarà presente un numero K compreso tra 0 e 2³²-1. Tale numero viene chiamato Identification Sequence Number (da ora ISN). Host B, ricevuto il pacchetto TCP da host A, risponderà a sua volta con un altro pacchetto contenente flag SYN e ACK con ISN J proprio e ISN K+1 (ovvero l'ISN di host A aumentato di 1). Al ricevimento del pacchetto SYN+ACK, host A provvederà all'invio di un terzo pacchetto contenente esclusivamente flag ACK con i due numeri (K e J) aumentati di 1. Dopo questi tre banali passaggi la connessione TCP/IP è stabilita; a questo punto vi domanderete cosa mai potrà aver a che fare il funzionamento del protocollo TCP/IP con l'ultima "apparizione" dell'argomento di nmap. La risposta è semplice: Kevin Mitnick (famoso hacker americano) dimostrò che i numeri ISN potevano essere facilmente prevedibili per il fatto che venivano generati in sequenza fissa, vediamo come. Prendiamo in considerazione tre host: host A (attaccante), host B (Zombie) ed host C (Target). Prima di tutto invieremo un pacchetto SYN+ACK dall'host attaccante (A) all'host zombie (B); per quanto abbiamo detto prima ciò non dovrebbe essere consentito in quanto la comunicazione TCP viene inizialmente iniziata con il solo flag SYN, ciò nonostante host B risponde alla richiesta con un pacchetto contenente il flag RST che a sua volta include il numero, esemplificativo, ISN 1000. Fatto questo siamo a conoscenza dell'ISN di B e sappiamo anche che lo stesso verrà incrementato linearmente: inviamo da A un pacchetto "alterato" a C contenente l'ip di B facendo ricadere quasi sulla responsabilità al medesimo; abbiamo in questa circostanza introdotto il concetto di spoofing. Nel caso in cui la porta H di C è aperta questi invierà un pacchetto a B (impersonificazione di A) contenente un pacchetto SYN+ACK ma, non avendo B legittimo richiedo alcunché, questi chiuderà la connessione con un RST, incrementando logicamente l'ISN di 1: 1001. Dopo aver fatto questo l'attaccante invierà un pacchetto SYN+ACK a B che, come in precedenza, chiuderà la comunicazione con un RST ed incrementerà l'ISN di 2: 1002 facendo denotare lo stato open della porta H. Se invece la porta H di C è chiusa questi invierà un pacchetto a B (impersonificazione di A) con flag RST e, pertanto, l'ISN di B non cambierà. Quando A invierà un nuovo pacchetto SYN+ACK a B ed in risposta troverà un RST, constaterà che l'ISN sarà aumentato solo di 1 facendo notare lo stato closed di H. Nmap è in grado di fare tutto ciò ed è proprio qui che entra in gioco l'opzione -I dello stesso (dove I sta, guarda caso, per idle scan). Tramite il TCP Sequence Prediction, nmap segnala il "grado di difficoltà" al fine di "intrapolare" un host zombie.

<http://openskill.info/infobox.php?ID=1274>

● Marcantoni Fausto

● 56

nmap – Idle Zombie Scan

bisogna trovare padroni di casa che sono inattivi sulla rete

```
[*] Auxiliary module running as background job 1.
[*] 90.147.42.12's IPID sequence class: Randomized
[*] 90.147.42.2's IPID sequence class: Randomized
[*] 90.147.42.39's IPID sequence class: Unknown
[*] 90.147.42.30's IPID sequence class: All zeros
[*] 90.147.42.31's IPID sequence class: Unknown
[*] 90.147.42.36's IPID sequence class: All zeros
[*] 90.147.42.32's IPID sequence class: Incremental!
[*] 90.147.42.35's IPID sequence class: Unknown
[*] 90.147.42.41's IPID sequence class: All zeros
[*] 90.147.42.40's IPID sequence class: Incremental!
[*] 90.147.42.45's IPID sequence class: Unknown
[*] 90.147.42.43's IPID sequence class: Unknown
msf auxiliary(scanner/ip/ipidseq) >
```



nmap – MAC Address Spoofing

Un altro metodo per bypassare le restrizioni del firewall, è lo spoofing dell'indirizzo MAC del proprio host.

```
nmap --spooof-mac 00:01:02:25:56:AE 193.205.92.145
```

Specify MAC address from a Vendor → -spooof-mac Dell/Apple/3Com

Generate a random MAC address → -spooof-mac 0

Specify your own MAC address → -spooof-mac 00:01:02:25:56:AE

**A ME (NON) FUNZIONA ...
anzi funziona male ...
e poi ...**

nmap – Append Random Data

Molti firewall ispezionano i pacchetti, cercando in loro dimensioni e contenuti, al fine di identificare un potenziale scan.

Per evitare questo tipo di rilevazione è possibile utilizzare il comando `--data-length` aggiungendo altri dati e di inviare pacchetti di dimensione diversa da quella default.

```
nmap --data-length 30 193.205.92.145
```

```
Prompt dei comandi
C:\Users\Fausto>nmap --data-length 30 193.205.92.145
Starting Nmap 5.00 ( http://nmap.org ) at 2012-06-01 11:27 ora legale Europa occidentale
Interesting ports on 193.205.92.145:
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
902/tcp   open  iss-realsecure
MAC Address: 00:04:23:B0:17:91 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
C:\Users\Fausto>
```

● Marcantoni Fausto

● 61

nmap - output

I Formati di Output di Nmap

```
nmap -oN scan.txt 193.205.92.108
```

```
--append-output (Accoda anziché sovrascrivere i file di output)
```

```
Prompt dei comandi
C:\Users\Fausto>type scan.txt
# Nmap 5.00 scan.txt started Wed May 09 12:03:34 2012 as: nmap -oN scan.txt 193.205.92.56
Interesting ports on 193.205.92.56 (193.205.92.56):
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:50:56:A2:78:AF (VMWare)

# Nmap done at Wed May 09 12:03:42 2012 -- 1 IP address (1 host up) scanned in 7.92 seconds
C:\Users\Fausto>
```

● Marcantoni Fausto

● 62

nmap - output

I Formati di Output di Nmap

`nmap -oX scan.xml 193.205.92.108`

`--append-output` (Accoda anziché sovrascrivere i file di output)

```

C:\Users\fausto>type scan.xml
<?xml version="1.0" ?>
<?xml-stylesheet href="file:///C:/Program Files (x86)/Unit/Nmap/nmap.xsl" type="text/xsl" ?>
<!-- Nmap 5.80 scan initiated Wed May 09 12:05:31 2012 as: nmap -oX scan.xml 193.205.92.108 --append-output --
Kmaprun scanner="nmap" args="nmap -oX scan.xml 193.205.92.56" start="1336557931" real st
"1.03">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1 3-4 6-7 9 11-14 16-17 19-21 23-24 26-27 29-30 32-33 35-36 38-39 41-42 44-45 47-48 50-51 53-54 56-57 59-60 62-63 65-66 68-69 71-72 74-75 77-78 80-81 83-84 86-87 89-90 92-93 95-96 98-99 101-102 104-105 107-108 110-111 113-114 116-117 119-120 122-123 125-126 128-129 131-132 134-135 137-138 140-141 143-144 146-147 149-150 152-153 155-156 158-159 161-162 164-165 167-168 170-171 173-174 176-177 179-180 182-183 185-186 188-189 191-192 194-195 197-198 200-201 203-204 206-207 209-210 212-213 215-216 218-219 221-222 224-225 227-228 230-231 233-234 236-237 239-240 242-243 245-246 248-249 251-252 254-255 257-258 260-261 263-264 266-267 269-270 272-273 275-276 278-279 281-282 284-285 287-288 290-291 293-294 296-297 299-300 302-303 305-306 308-309 311-312 314-315 317-318 320-321 323-324 326-327 329-330 332-333 335-336 338-339 341-342 344-345 347-348 350-351 353-354 356-357 359-360 362-363 365-366 368-369 371-372 374-375 377-378 380-381 383-384 386-387 389-390 392-393 395-396 398-399 401-402 404-405 407-408 410-411 413-414 416-417 419-420 422-423 425-426 428-429 431-432 434-435 437-438 440-441 443-444 446-447 449-450 452-453 455-456 458-459 461-462 464-465 467-468 470-471 473-474 476-477 479-480 482-483 485-486 488-489 491-492 494-495 497-498 500-501 503-504 506-507 509-510 512-513 515-516 518-519 521-522 524-525 527-528 530-531 533-534 536-537 539-540 542-543 545-546 548-549 551-552 554-555 557-558 560-561 563-564 566-567 569-570 572-573 575-576 578-579 581-582 584-585 587-588 590-591 593-594 596-597 599-600 602-603 605-606 608-609 611-612 614-615 617-618 620-621 623-624 626-627 629-630 632-633 635-636 638-639 641-642 644-645 647-648 650-651 653-654 656-657 659-660 662-663 665-666 668-669 671-672 674-675 677-678 680-681 683-684 686-687 689-690 692-693 695-696 698-699 701-702 704-705 707-708 710-711 713-714 716-717 719-720 722-723 725-726 728-729 731-732 734-735 737-738 740-741 743-744 746-747 749-750 752-753 755-756 758-759 761-762 764-765 767-768 770-771 773-774 776-777 779-780 782-783 785-786 788-789 791-792 794-795 797-798 800-801 803-804 806-807 809-810 812-813 815-816 818-819 821-822 824-825 827-828 830-831 833-834 836-837 839-840 842-843 845-846 848-849 851-852 854-855 857-858 860-861 863-864 866-867 869-870 872-873 875-876 878-879 881-882 884-885 887-888 890-891 893-894 896-897 899-900 902-903 904-905 907-908 910-911 913-914 916-917 919-920 922-923 925-926 928-929 931-932 934-935 937-938 940-941 943-944 946-947 949-950 952-953 955-956 958-959 961-962 964-965 967-968 970-971 973-974 976-977 979-980 982-983 985-986 988-989 991-992 994-995 997-998 1000--
156,13722,13782-13783,14080,14230,14441-14442,15000,15002-15004,15008,15742,16000-16001,1
    
```

nmap - output

I Formati di Output di Nmap

`nmap -oX scan.xml 193.205.92.108`

```

C:\Users\fausto>type scan.xml
<?xml version="1.0" ?>
<?xml-stylesheet href="file:///C:/Program Files (x86)/Unit/Nmap/nmap.xsl" type="text/xsl" ?>
<!-- Nmap 5.80 scan initiated Wed May 09 12:05:31 2012 as: nmap -oX scan.xml 193.205.92.108 --append-output --
Kmaprun scanner="nmap" args="nmap -oX scan.xml 193.205.92.56" start="1336557931" real st
"1.03">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1 3-4 6-7 9 11-14 16-17 19-21 23-24 26-27 29-30 32-33 35-36 38-39 41-42 44-45 47-48 50-51 53-54 56-57 59-60 62-63 65-66 68-69 71-72 74-75 77-78 80-81 83-84 86-87 89-90 92-93 95-96 98-99 101-102 104-105 107-108 110-111 113-114 116-117 119-120 122-123 125-126 128-129 131-132 134-135 137-138 140-141 143-144 146-147 149-150 152-153 155-156 158-159 161-162 164-165 167-168 170-171 173-174 176-177 179-180 182-183 185-186 188-189 191-192 194-195 197-198 200-201 203-204 206-207 209-210 212-213 215-216 218-219 221-222 224-225 227-228 230-231 233-234 236-237 239-240 242-243 245-246 248-249 251-252 254-255 257-258 260-261 263-264 266-267 269-270 272-273 275-276 278-279 281-282 284-285 287-288 290-291 293-294 296-297 299-300 302-303 305-306 308-309 311-312 314-315 317-318 320-321 323-324 326-327 329-330 332-333 335-336 338-339 341-342 344-345 347-348 350-351 353-354 356-357 359-360 362-363 365-366 368-369 371-372 374-375 377-378 380-381 383-384 386-387 389-390 392-393 395-396 398-399 401-402 404-405 407-408 410-411 413-414 416-417 419-420 422-423 425-426 428-429 431-432 434-435 437-438 440-441 443-444 446-447 449-450 452-453 455-456 458-459 461-462 464-465 467-468 470-471 473-474 476-477 479-780 782-783 785-786 788-789 791-792 794-795 797-798 800-801 803-804 806-807 809-810 812-813 815-816 818-819 821-822 824-825 827-828 830-831 833-834 836-837 839-840 842-843 845-846 848-849 851-852 854-855 857-858 860-861 863-864 866-867 869-870 872-873 875-876 878-879 881-882 884-885 887-888 890-891 893-894 896-897 899-900 902-903 904-905 907-908 910-911 913-914 916-917 919-920 922-923 925-926 928-929 931-932 934-935 937-938 940-941 943-944 946-947 949-950 952-953 955-956 958-959 961-962 964-965 967-968 970-971 973-974 976-977 979-980 982-983 985-986 988-989 991-992 994-995 997-998 1000--
156,13722,13782-13783,14080,14230,14441-14442,15000,15002-15004,15008,15742,16000-16001,1
    
```

nmap - verbosità

Livello di verbosità

```
nmap -v 193.295.92.108
```

```
Prompt dei comandi
C:\Users\fausto>nmap -v 193.295.92.56

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-09 12:12 ora legale Europa occidentale
NSE: Loaded 0 scripts for scanning.
Initiating ARP Ping Scan at 12:13
Scanning 193.295.92.56 [1 port]
Completed ARP Ping Scan at 12:13, 0.80s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:13
Completed Parallel DNS resolution of 1 host. at 12:13, 5.52s elapsed
Initiating SYN Stealth Scan at 12:13
Scanning dida.cs.unican.it (193.295.92.56) [1000 ports]
Discovered open port 22/tcp on 193.295.92.56
Discovered open port 443/tcp on 193.295.92.56
Discovered open port 80/tcp on 193.295.92.56
Discovered open port 3306/tcp on 193.295.92.56
Discovered open port 10000/tcp on 193.295.92.56
Completed SYN Stealth Scan at 12:13, 0.11s elapsed (1000 total ports)
Host dida.cs.unican.it (193.295.92.56) is up (0.00s latency).
Interesting ports on dida.cs.unican.it (193.295.92.56):
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:50:56:A2:78:AF (VMWare)

Read data files from: C:\Program Files (x86)\Ulti\Nmap
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
Raw packets sent: 1001 (44.042KB) | Rcvd: 1001 (40.653KB)

C:\Users\fausto>
```

● Marcantoni Fausto

● 65

nmap - debug

Livello di debugging

```
nmap -d[0-9] 193.295.92.108
```

```
Prompt dei comandi
C:\Users\fausto>nmap -d 193.295.92.56
WinPcap present (kernel) linked to: WinPcap version 4.1.2 (packet.dll version 4.1.0.2001)

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-09 12:15 ora legale Europa occidentale
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)

-----
Host options:
host_timeout: 1s, max: 1000000
rtt_timeout: 1s, min: 1000, max: 10000
max_scan_delay: 1s, min: 0, max: 10000
packet_size: 1440, min: 0, max: 0
max_retry: 5, host_timeout: 0
max_rate: 0, max-rate: 0
-----

NSE: Loaded 0 scripts for scanning.
Initiating ARP Ping Scan at 12:15
Scanning 193.295.92.56 [1 port]
Packet capture filter (device eth14): arp and ether dst host 00:26:9E:57:66:BE
Completed ARP Ping Scan at 12:15, 0.70s elapsed (1 total hosts)
Overall sending rates: 1.20 packets / s, 53.85 bytes / s.
mass_dns: Using DNS server 193.295.92.70
mass_dns: Using DNS server 193.295.92.1
mass_dns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 12:15
mass_dns: 5.52s 0/1 [H: 3, OK: 0, NX: 0, DR: 0, SF: 0, TR: 3]
Completed Parallel DNS resolution of 1 host. at 12:15, 5.52s elapsed
DNS resolution of 1 IPs took 5.52s. Mode: Async [H: 3, OK: 1, NX: 0, DR: 0, SF: 0, TR: 3]
Initiating SYN Stealth Scan at 12:15
Scanning dida.cs.unican.it (193.295.92.56) [1000 ports]
Packet capture filter (device eth14): dst host 193.295.92.114 and (icmp or ((tcp or udp o
Discovered open port 80/tcp on 193.295.92.56
Discovered open port 443/tcp on 193.295.92.56
Discovered open port 22/tcp on 193.295.92.56
Discovered open port 3306/tcp on 193.295.92.56
```

● Marcantoni Fausto

● 66

Nmap Scripting Engine

Con nmap vengono forniti anche una serie di script ufficiali elaborati all'interno del progetto.

Introdotta relativamente di recente, il **Nmap Script Engine** è un versatile motore di scripting per estendere le capacità di Nmap senza forzare gli sviluppatori ad approcciare un compito impegnativo quale la modifica dei sorgenti C del programma.

NSE è un motore per script in linguaggio **LUA** e permette agli utenti di automatizzare una serie di procedure e test verso gli host target.



<http://www.lua.org/>

Nmap Scripting Engine

Aggiornare gli script (ma serve ????)

bisogna essere amministratori, ma non è così semplice

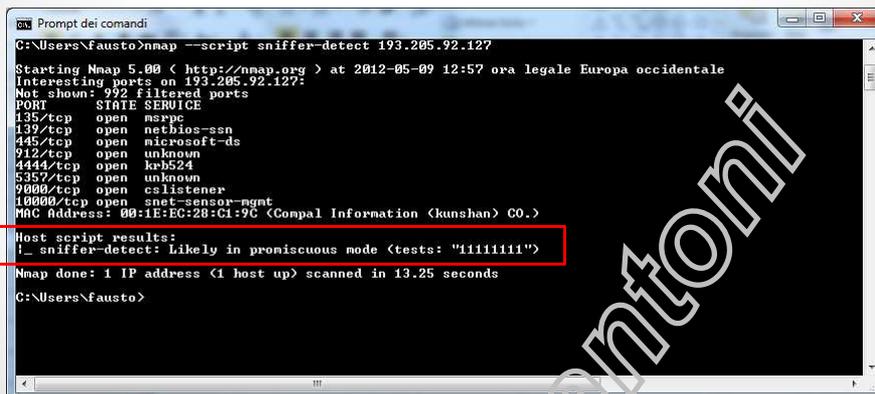
```

C:\Windows\system32\nmap --script-updatedb
Starting nmap 5.10 < http://nmap.org > at 2012-05-09 12:22 ora legale Europa occidentale
NSE: Updating file database.
NSE: script database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.98 seconds
C:\Windows\system32>
  
```

Nmap Scripting Engine

Verificare la presenza di un computer della LAN in "promiscuous mode"

```
nmap -sV --script sniffer-detect 193.205.92.108
```



```

C:\Users\Fausto>nmap --script sniffer-detect 193.205.92.127
Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-09 12:57 ora legale Europa occidentale
Interesting ports on 193.205.92.127:
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  nmapc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
912/tcp   open  unknown
4444/tcp   open  hls24
5357/tcp   open  unknown
9000/tcp   open  cslistener
10000/tcp  open  snet-sensor-rgmt
MAC Address: 00:1E:EC:20:C1:9C (Compal Information (Kunshan) CO.)

Host script results:
|_ sniffer-detect: Likely in promiscuous mode (tests: "1111111")
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
C:\Users\Fausto>

```

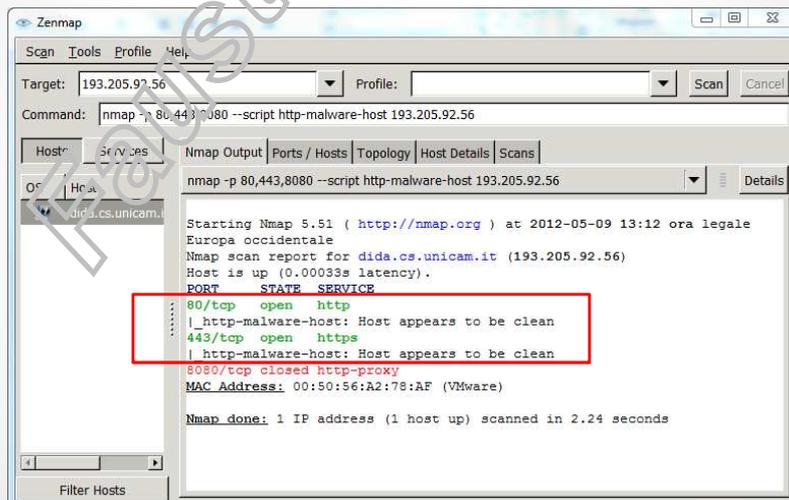
● Marcantoni Fausto

● 69

Nmap Scripting Engine

Verificare la presenza di un malware su un web serve

```
nmap -p80,443,8080 --script=http-malware-host 193.205.92.108
```



```

Zenmap
Scan Tools Profile Help
Target: 193.205.92.56 Profile: Scan Cancel
Command: nmap -p 80,443,8080 --script http-malware-host 193.205.92.56
Hosts: Services Nmap Output Ports / Hosts Topology Host Details Scans
OS: Hosts
did.cs.unicam.it
Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-09 13:12 ora legale
Europa occidentale
Nmap scan report for dida.cs.unicam.it (193.205.92.56)
Host is up (0.00033s latency).
PORT      STATE SERVICE
80/tcp    open  http
|_ http-malware-host: Host appears to be clean
443/tcp    open  https
|_ http-malware-host: Host appears to be clean
8080/tcp   closed http-proxy
MAC Address: 00:50:56:A2:78:AF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
Filter Hosts

```

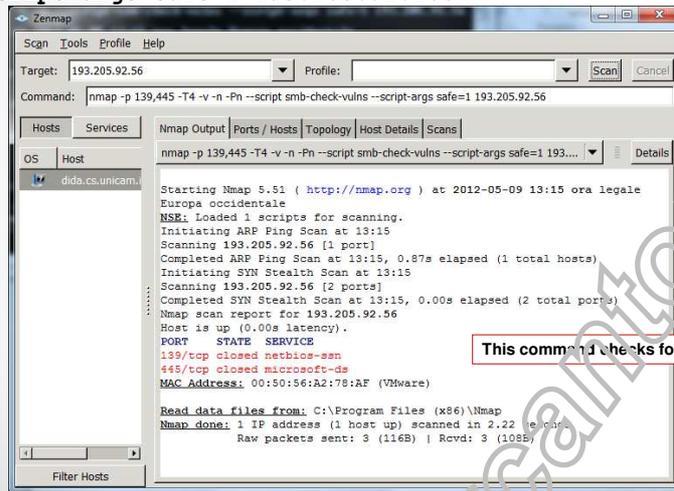
● Marcantoni Fausto

● 70

Nmap Scripting Engine

Verificare la presenza di Conficker tra i computer inseriti nella LAN.

nmap -PN -T4 -p139,445 -v -n --script=smb-check-vulns --script-args safe=1 193.205.92.108



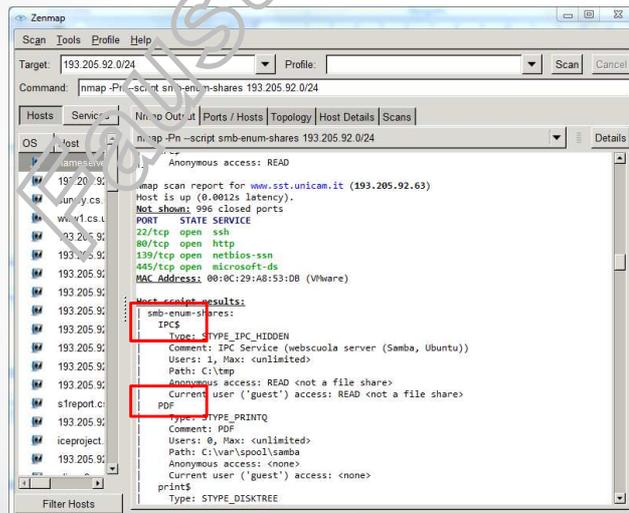
-n DNS resolve
-v verbose

This command checks for the MS08-067 vulnerability

Nmap Scripting Engine

Enumerare le risorse condivise in un sistema Windows o Samba file server.

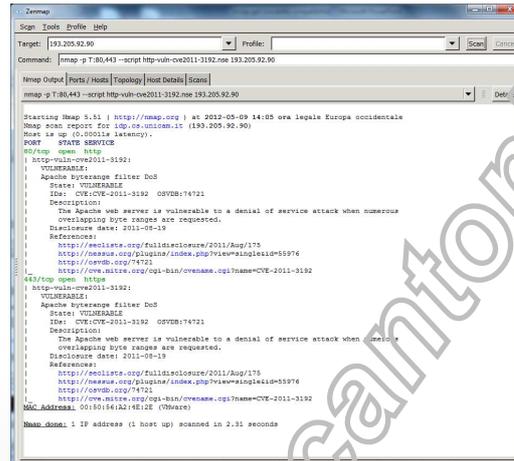
nmap -Pn --script=smb-enum-shares 193.205.92.0/24



Nmap Scripting Engine

Verificare la vulnerabilità di apache cve2011-3192

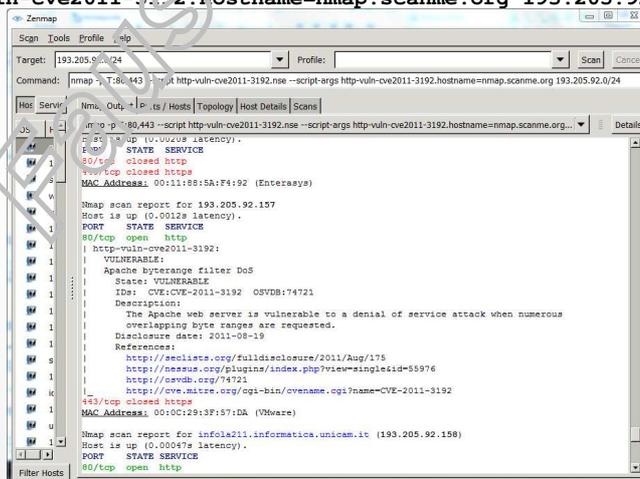
`nmap -p T:80,443 --script http-vuln-cve2011-3192.nse 193.205.92.108`



Nmap Scripting Engine

Verifica la vulnerabilità di apache cve2011-3192 (tutta una network)

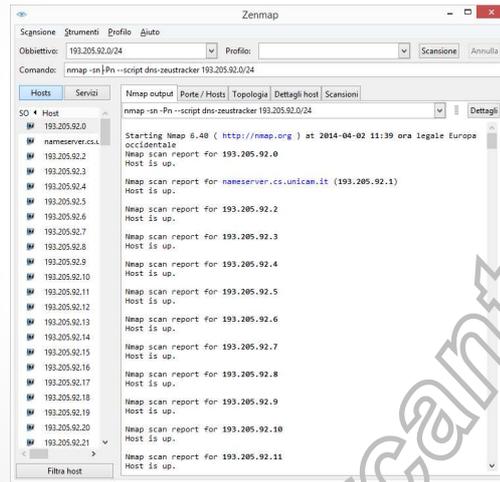
`nmap -p T:80,443 --script http-vuln-cve2011-3192.nse --script-args http-vuln-cve2011-3192.hostname=nmap.scanme.org 193.205.92.0/24`



Nmap Scripting Engine

Checks if the target IP range is part of a Zeus botnet (tutta una network)

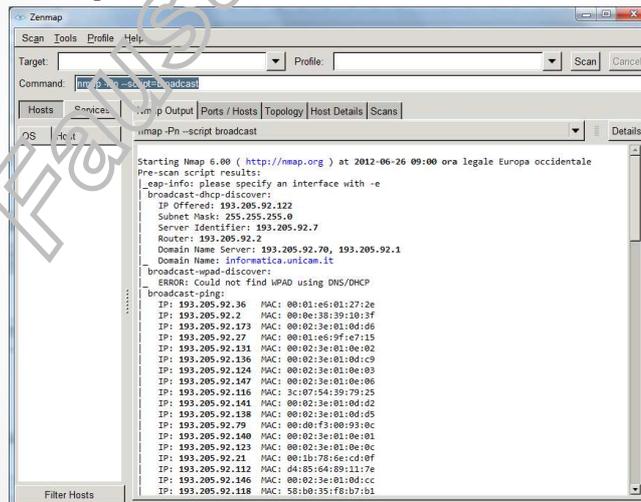
`nmap -sn -PN --script=dns-zeustracker 193.205.92.0/24 [-oX scan.xml]`



Nmap Scripting Engine

These scripts find hosts and services that advertise themselves to the network broadcast address

`nmap -Pn --script=broadcast`



NSE Documentation

<http://nmap.org/nsedoc/index.html>

| NSEDoc | |
|-------------------------------------|--|
| Index | |
| NSE Documentation | |
| Categories | |
| auth | |
| broadcast | |
| brute | |
| default | |
| discovery | |
| dos | |
| exploit | |
| external | |
| fuzzer | |
| intrusive | |
| malware | |
| safe | |
| version | |
| vuln | |
| Scripts (show 370) | |
| Libraries (show 96) | |

| Scripts | |
|----------------------------------|---|
| acarsd-info | Retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (Aircraft Communication Addressing and Reporting System) data in real time. The information retrieved by this script includes the daemon version, API version, administrator e-mail address and listening frequency. |
| address-info | Shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available. |
| atp-brute | Performs password guessing against Apple Filing Protocol (AFP). |
| atp-is | Attempts to get useful information about files from AFP volumes. The output is intended to resemble the output of <code>ls</code> . |
| atp-path-vuln | Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533. |
| atp-serverinfo | Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for example Macmini1 of MacBookPro). |
| atp-showmount | Shows AFP shares and ACLs. |
| ajp-auth | Retrieves the authentication scheme and realm of an AJP service that requires authentication. |
| ajp-headers | Performs a HEAD or GET request against either the root directory or any optional directory and returns the server response headers. |
| ajp-methods | Finds out what options are supported by the AJP server by sending an OPTIONS request and lists potentially risky methods. |
| amqp-info | Gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server. |
| asn-query | Maps IP addresses to autonomous system (AS) numbers. |
| auth-owners | Attempts to find the owner of an open TCP port by querying an auth daemon which must also be open on the target system. The auth service, also known as ident, normally runs on port 113. |
| auth-spoof | Checks for an ident (auth) server which is spoofing its replies. |
| backoffice-brute | Performs brute force password auditing against the BackOffice service. The <code>backoffice-brute-ports</code> script argument is mandatory (it specifies ports to run the script against). |
| backoffice-info | Connects to a BackOffice service and gathers information about the host and the BackOffice service itself. |
| banner | A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds. |
| bitcoin-getaddr | Queries a Bitcoin server for a list of known Bitcoin nodes. |
| bitcoin-info | Extracts version and node information from a Bitcoin server. |

● Marcantoni Fausto ● 77

ncat

Ncat is a general-purpose command-line tool for

- Reading
- Writing
- Redirecting
- Encrypting data across a network



Swiss Army knife

<http://nmap.org/ncat/guide/index.html>

● Marcantoni Fausto ● 78

ncat

connect to a network service

```
ncat dida.cs.unicam.it 80
ncat -C dida.cs.unicam.it 80
```

The -C option turns on CRLF replacement

GET / HTTP/1.0

```
C:\Program Files (x86)\Nmap>ncat dida.cs.unicam.it 80
GET / HTTP/1.0

HTTP/1.1 403 Forbidden
Date: Thu, 03 Nov 2011 09:16:40 GMT
Server: Apache/2.2.3 (Gentoo)
Accept-Ranges: bytes
Content-Length: 5043
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<head>
  <title>Apache HTTP Server Test Page powered by OpenSSL</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <style type="text/css">
    body {

```

● Marcantoni Fausto
● 79

ncat

using Ncat as a web browser

```
ncat -l localhost 8080 < hello.http
"c:\Program Files (x86)\Nmap">ncat -l localhost 8080 < c:\hello.http
```

```
C:\Users\Fausto.mfausto>cd c:\
Data corrente: 02/04/2016
Immettere la nuova data (es. mm-aa)
C:\Users\Fausto.mfausto>ncat -l localhost 8080 < hello.http
GET / HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: deflate
Connection: keep-alive

C:\Users\Fausto.mfausto>
```

Creare un file: hello.http

```
HTTP/1.0 200 OK

<html>
<body>
  <h1>Hello, world!</h1>
</body>
</html>
```

A ME (NON) FUNZIONA ... anzi funziona male Anzi funziona

● Marcantoni Fausto
● 80

ncat

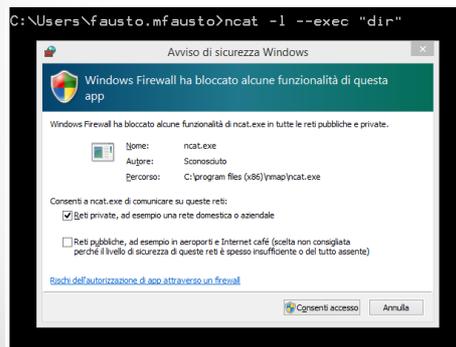
execute an external command

ncat -l --exec

Default port: 31337

ncat -l --sh-exec

The --sh-exec option (-c) works the same as --exec, except that it executes the command by passing it to /bin/sh -c on Unix or cmd.exe /C on Windows.



● Marcantoni Fausto

● 81

ncat

execute an external command

ncat -l --exec: "/bin/echo HELLO"

Default port: 31337

```
C:\Program Files (x86)\Nmap>ncat 193.205.92.139
HELLO
C:\Program Files (x86)\Nmap>
```

● Marcantoni Fausto

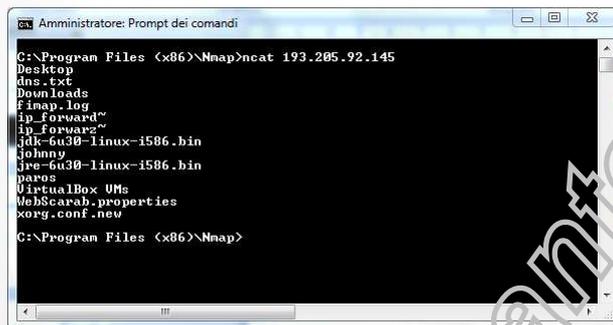
● 82

ncat

execute an external command

ncat -l --exec "/bin/ls"

Default port: 31337



```

C:\Program Files (x86)\Nmap>ncat 193.205.92.145
Desktop
Dns.txt
Downloads
Fimap.log
Ip_forward~
Ip_forward~
jdk-bu30-linux-1586.bin
Johnny
jre-bu30-linux-1586.bin
Nmap
VirtualBox VMs
WebScarab.properties
xorg.conf.new
C:\Program Files (x86)\Nmap>

```

ncat

execute an external command

ncat -l --exec "cmd.exe"

```
C:\Program Files (x86)\Nmap>ncat -l --exec "cmd.exe"
```

```

studente@student-virtual-machine:~$ ncat 193.205.92.109
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Program Files (x86)\Nmap>

```

ncat

execute an external command

ncat -l --exec "cmd.exe"

```
C:\Program Files (x86)\Nmap>dir/w
dir/w
Il volume nell'unit  C non ha etichetta.
Numero di serie del volume: 28E5-29FD

Directory di C:\Program Files (x86)\Nmap

[.]                [..]                3rd-party-licenses.txt
ca-bundle.crt      CHANGELOG            COPYING
COPYING_HIGWIDGETS hello.http           icon1.ico
libeay32.dll       [licenses]          ncat.exe
ndiff.exe          NDIFF_README        nmap-mac-prefiles
nmap-os-db         nmap-payloads       nmap-protocols
nmap-rpc           nmap-service-probes nmap-services
nmap.exe           nmap.xsl            nmap_performance_reg
nping.exe          [nseelib]           nse_main.lua
[py2exe]           python26.dll         python27.dll
README-WIN32       [scripts]           [share]
ssleay32.dll       tutto_cs.txt         Uninstall.exe
zenmap.exe         ZENMAP_README

                31 File      14.310.980 byte
                7 Directory 262.013.968.384 byte disponibili

C:\Program Files (x86)\Nmap>
```

●85

ncat

execute an external command

ncat -l --sh-exec "/bin/sh"

```
studente@student@virtual-machine:~$ ncat -l --sh-exec "/bin/sh"
```

```
C:\Program Files (x86)\Nmap>ncat 193.205.92.139
comando -> ls
Documenti
examples.desktop
Immagini
Modelli
Musica
Pubblici
Scaricati
Scrivania
Video
risultato ->
```

● Marcantoni Fausto

●86

ncat

proxying

```
ncat -l 3128 --proxy-type http
ncat -vvv -l 3128 --proxy-type http
```

Ncat can act as a proxy server itself in listen mode.
The only proxy type supported is http.

```
studente@student-virtual-machine:~$ ncat -l 3128 --proxy-type http -v
Ncat: Version 5.21 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:3128
```



Opzioni Internet

Server proxy

Utilizza un server proxy per le connessioni LAN. Queste impostazioni non verranno applicate alle connessioni remote o VPN.

Indirizzo: 193.205.92.139 Porta: 3128 Avanzate

Ignora server proxy per indirizzi locali

● Marcantoni Fausto ● 87

ncat

Ncat simply moves bits from one place to another

```
ncat -l ncat [host]
```

```
studente@student-virtual-machine:~$ ncat -l
ciao
saluti
```

```
C:\Program Files (x86)\Nmap>ncat 193.205.92.139
ciao
saluti
```

● Marcantoni Fausto ● 88

ncat

two users can communicate with each other

```

ncat -l --chat
studente@studente-virtual-machine:~$ ncat -l --chat -v
Ncat: Version 5.21 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:31337

ncat [host]
C:\Program Files (x86)\Nmap>ncat 193.205.92.109
<announce> 193.205.92.109 is connected as <user3>.
<announce> already connected: 193.205.92.109 as <user4>.

ncat [host]
C:\Program Files (x86)\Nmap>ncat 193.205.92.109
<announce> 193.205.92.109 is connected as <user4>.
<announce> already connected: nobody.
<announce> 193.205.92.109 is connected as <user5>.
<announce> already connected: 193.205.92.109 as <user4>.

studente@studente-virtual-machine:~$ ncat -l --chat -v
Ncat: Version 5.21 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:31337
Ncat: Connection from 193.205.92.109 on file descriptor 4.
Ncat: Connection from 193.205.92.109 on file descriptor 5.

```

● Marcantoni Fausto

● 89

ncat

two users can transfer files between them

receiver listens

```
ncat -l > outputfile
ncat --send-only host2 < inputfile
```

sender listens

```
ncat -l --send-only < inputfile
ncat host1 > outputfile
```

● Marcantoni Fausto

● 90

nping

Nping is an open-source tool for

- network packet generation,
- response analysis
- response time measurement

Nping allows users

- to generate network packets of a wide range of protocols

<http://nmap.org/book/nping-man.html>

nping

execute an external command

```
nping -c 1 --tcp -p 80 www.google.it
```

```
C:\Program Files (x86)\Nmap>nping -c 1 --tcp -p 80 www.google.it
Starting Nping 0.5.1 [11:52:00] http://nmap.org/nping > at 2011-11-03 11:52 ora solare Europa occidentale
SENT (0.3820s) ICMP 209.85.149.99:29422 > 193.205.92.109:80 S ttl=64 id=52676 iplen=40 seq=3584724084 win=1480
RCVD (0.6570s) ICMP 209.85.149.99:80 > 193.205.92.109:29422 SA ttl=53 id=8156 iplen=44 seq=2326878128 win=5720 <mss 1
RCVD (0.9670s) ICMP 209.85.149.99:80 > 193.205.92.109:29422 SA ttl=53 id=8157 iplen=44 seq=2326878128 win=5720 <mss 1
RCVD (1.5650s) ICMP 209.85.149.99:80 > 193.205.92.109:29422 SA ttl=53 id=8158 iplen=44 seq=2326878128 win=5720 <mss 1
Max rtt: 930.000ms | Min rtt: 22.000ms | Avg rtt: 420.000ms
Raw packets sent: 1 (40B) | Recv: 3 (138B) | Lost: 0 (0.00%)
Tx time: 0.25300s | Rx bytes/s: 213.44 | Tx pkts/s: 3.95
Rx time: 1.25300s | Rx bytes/s: 110.14 | Rx pkts/s: 2.39
Nping done: 1 IP address pinged in 1.64 seconds
```

riferimenti

- www.insecure.org
- www.nmap-tutorial.com
- nmap.org/man/it/index.html
- nmap.org/book/nse.html
- nmap.org/nsedoc/index.html

- Manuali on line:
- http://resources.infosecinstitute.com/nmap_cheat-sheet/
- <http://blog.hackersonlineclub.com/2014/01/nmap-network-mapping-cheat-sheet.html>

Fausto Marcantoni