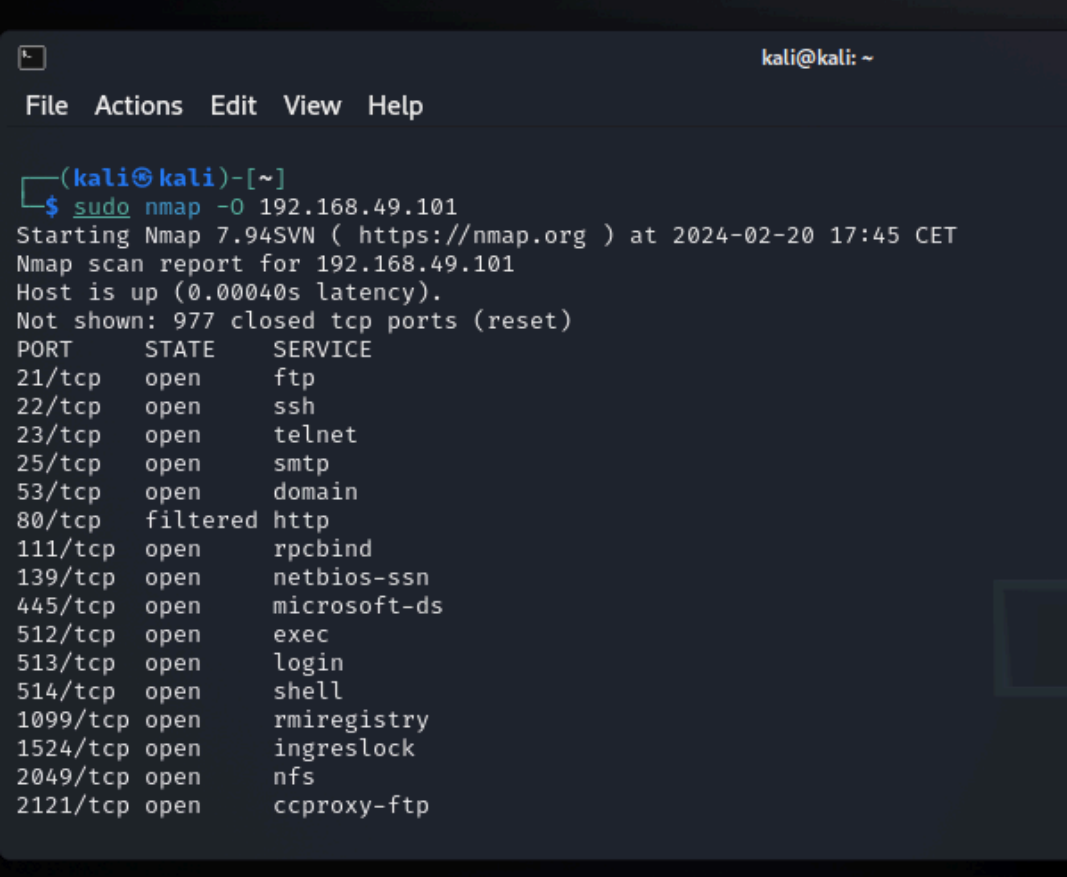


## Esercizio 21-02-24

Nmap («Network Mapper») è uno strumento open-source per la network exploration e l'auditing. È stato progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l'utilizzo verso singoli host. L'output di Nmap è un elenco di obiettivi scansionati, con informazioni supplementari per ognuno a seconda delle opzioni usate.

- **-O Os Fingerprint su Meta**

Una delle più famose caratteristiche di Nmap è la possibilità di identificare da remoto il sistema operativo di un host attraverso il fingerprint dello stack TCP/IP. Nmap invia una serie di pacchetti TCP ed UDP all'host remoto ed esamina ogni bit ricevuto in risposta.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.49.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 17:45 CET  
Nmap scan report for 192.168.49.101  
Host is up (0.00040s latency).  
Not shown: 977 closed tcp ports (reset)  
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    filtered  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
```

```

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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds

(kali@kali)-[~]
$

```

- **-sS SYN Scan su Meta**

Il SYN Scan è l'opzione di default ed è la più usata per buone ragioni. Può essere effettuato velocemente: effettua la scansione su migliaia di porte al secondo su una rete veloce non limitata da firewall restrittivi. Il SYN scan è relativamente nascosto e poco invasivo, poiché non completa mai le connessioni TCP.

Viene chiamato anche "scanning semi-aperto" perché non viene aperta una connessione TCP completa. Viene mandato un pacchetto SYN come se si fosse sul punto di aprire una connessione reale e si attende una risposta. Un SYN/ACK indica che la porta è in ascolto mentre un RST indica che la porta non è in ascolto.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:52 CET
Nmap scan report for 192.168.49.101
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (reset)
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    filtered  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

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds

```

- **-sT TCP connect - su Meta**

La scansione di tipo TCP connect è la scansione TCP di default dove la scansione SYN non è un'opzione viabile. Nmap richiede al sistema operativo sottostante di stabilire una connessione con la macchina di destinazione invocando la chiamata di sistema connect. Questo è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.49.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:56 CET  
Nmap scan report for 192.168.49.101  
Host is up (0.00040s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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    filtered  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  
  
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

- **-sV Version detection su Meta**

-sV esegue una scansione abilitando la feature di «version detection», grazie alla quale oltre al servizio recuperiamo anche la versione e relativi dettagli.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:58 CET
Nmap scan report for 192.168.49.101
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (conn-refused)
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    filtered http
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         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds

```

Eseguiamo lo stesso comando su Win7

- **-O Os fingerprint su Win7**

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -O 192.168.50.102
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:45 CET
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:69:23:32 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 23.82 seconds

(kali@kali)-[~]
$

```

Spesso una macchina potrebbe essere attiva ma non rispondere al ping, ad esempio se c'è una regola firewall che blocca il traffico ICMP.

Per vedere la differenza andiamo a disattivare nel firewall proprio queste regole presenti nel firewall di Win7:

- -O Os fingerprint bypassando il firewall

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nmap -O 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:39 CET  
Nmap scan report for 192.168.50.102  
Host is up (0.00018s latency).  
All 1000 scanned ports on 192.168.50.102 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:69:23:32 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized|VoIP phone|general purpose|phone  
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player  
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_s_8  
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player  
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device  
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 21.98 seconds  
  
(kali@kali)-[~]  
└─$
```

- -O su Win7 e Firewall abbassato

```
(root@kali)-[/home/kali]  
└─# nmap -O 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:20 CET  
Nmap scan report for 192.168.50.102  
Host is up (0.00014s latency).  
Not shown: 991 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
MAC Address: 08:00:27:69:23:32 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 7|2008|8.1  
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1  
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 6.20 seconds  
  
(root@kali)-[/home/kali]
```

## Come possiamo eludere il firewall?

Nella realtà quando eseguiamo uno scan la sorgente da cui lanciamo lo scan che inizia ad inviare le richieste al target. Se il target è protetto da un IPS/IDS questo va a identificare il potenziale attacco proveniente dall'esterno e quindi rigetterà i pacchetti.

Nmap fornisce alcune possibilità:

**Timing template:** un insieme predefinito di opzioni di temporizzazione che possono essere utilizzate per ottimizzare le prestazioni di scansione. L'opzione si attiva con lo switch -T e troviamo sei livelli di timing: da 0 a 5. Questo tipo di scan come possiamo vedere dagli screen richiedono un lasso di tempo maggiore rispetto allo standard.

**Scansioni parallele:** in caso di scansione verso numerosi target, nmap usa l'approccio multi-thread, questo vuol dire che esegue più task su diversi IP in maniera parallela. In

questo caso la scansione diventa più veloce, ma allo stesso tempo identificabile. Per evitare di essere individuati da IPS/IDP potremmo eliminare il parallelismo, così da scansionare un nodo per volta e diminuire il numero di richieste.

**Porta sorgente:** un'altra soluzione è quella di configurare nmap per inviare i pacchetti da una porta nota (80,443) > questo perché gli IPS/IDP in genere non bloccano questi pacchetti. Per eseguire nmap in modo tale da inviare pacchetti da una determinata porta sorgente si utilizza lo switch «--source-port».