

#BYTEREBELS



VAN ZWAM ARJEN

SCANSIONE DEI SERVIZI CON NMAP



NMAP

SCANSIONI SU METASPLOITABLE2

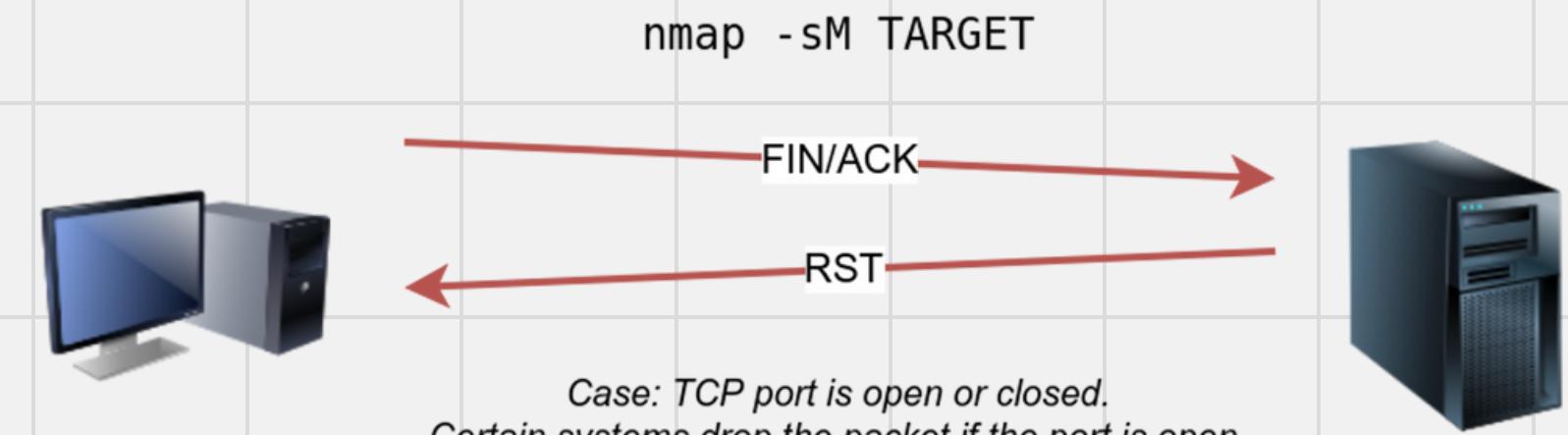


IP STATICO: 192.168.1.222

PAGINA

TIPOLOGIA SCANSIONE

- 3 OS FINGERPRINT
- 4 SYN SCAN
- 5 TCP CONNECT
- 6 VERSION DETECTION





VAN ZWAM ARJEN

OS FINGERPRINT

L'Help di nmap aiuta dicendo:

<<OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively >>

Ho dunque utilizzato la funzione -O nel mio target Meta (192.168.1.222)



L'**OS detection** di Nmap è una funzionalità che consente di identificare il sistema operativo in esecuzione su un host di rete. Questa funzione è utile per diversi scopi, tra cui:

1. Rilevamento delle vulnerabilità
 2. Profilazione del sistema
 3. Pianificazione delle risorse di rete
- Risoluzione dei problemi di rete

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -O 192.168.1.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 08:49 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.222)
Host is up (0.00033s 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    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: 08:00:27:75:1A:B4 (Oracle VirtualBox virtual NIC)
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 2.02 seconds
```



VAN ZWAM ARJEN

SYN SCAN

L'Help di nmap aiuta dicendo:

<< SCAN TECHNIQUES:

-sS/sT/sA/sW/sM:

TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans >>

Ho dunque utilizzato la funzione -sS nel mio
target Meta (192.168.1.222)

In un **SYN scan**, nmap invia una richiesta di connessione TCP SYN all'host di destinazione. Se la porta è aperta, l'host risponderà con un pacchetto di risposta SYN/ACK. Invece di completare la connessione TCP, nmap invia un pacchetto di risposta RST (RESET) per interrompere la connessione. Questo metodo permette a nmap di determinare se una porta è aperta senza stabilire effettivamente una connessione completa.



```
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
ports... socket...
[root@kali ~]# nmap -sS 192.168.1.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 08:55 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.222)
Host is up (0.00012s 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    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: 08:00:27:75:1A:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```



VAN ZWAM ARJEN

TCP CONNECT

Come nel SYS SCAN le funzioni sembrano uguali.

Nell'esercizio svolto ho ipotizzato
la funzione **-sT** nel mio **target Meta**
(192.168.1.222)

```
(root@kali)-[/usr/share/nmap/scripts]
# nmap -sT 192.168.1.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 08:59 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.222)
Host is up (0.00059s 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    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: 08:00:27:75:1A:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

TCP connect scan: nmap tenta di stabilire una connessione TCP completa con l'host di destinazione per ogni porta che viene scansionata. Invia un pacchetto di richiesta di connessione TCP e **attende una risposta**. Se la connessione viene stabilita con successo nmap considera la porta come aperta. Al contrario, se la connessione viene rifiutata o non viene ricevuta una risposta nmap considera chiusa la porta.

DIFFERENZE TRA SYS E TCP scan:

Le principali differenze tra SYN scan e TCP connect sono legate al modo in cui vengono gestite le connessioni:

- SYN scan è **più veloce** rispetto a TCP connect perché non stabilisce connessioni complete (come abbiamo visto nella slide precedente, si blocca con RST)
- TCP connect è **meno discreto** rispetto a SYN scan perché stabilisce una connessione completa per ogni porta scansionata, e OLTRETTUTTO può essere più facilmente rilevato dai sistemi di rilevamento delle intrusioni (IDS/IPS)



VAN ZWAM ARJEN

VERSION DETECTION

L'Help di nmap aiuta dicendo:

<< SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info >>

Ho dunque utilizzato la funzione **-sV** nel mio **target Meta** (192.168.1.222)

```
(root㉿kali)-[/usr/share/nmap/scripts]
# nmap -sV 192.168.1.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:04 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.222)
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
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        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
MAC Address: 08:00:27:75:1A:B4 (Oracle VirtualBox virtual NIC)
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 63.62 seconds
```

La funzione **-sV** su nmap viene utilizzata per eseguire la scansione di **TUTTI** i servizi su un host di rete. Questa opzione consente di identificare le **versioni** dei servizi che sono in **esecuzione** solo sulle porte aperte.

Le richieste possono variare a seconda del servizio.

-sV può essere utile per diversi scopi:

1. Identificazione dei servizi
2. Rilevamento delle vulnerabilità
3. Profilazione dei servizi

L'opzione "**-sV**" può richiedere più tempo rispetto a una scansione standard e potrebbe essere più **intrusiva** nei confronti dei servizi.

SCANSIONI SU WINDOWS 7

IP STATICO: 192.168.1.11

PAGINA

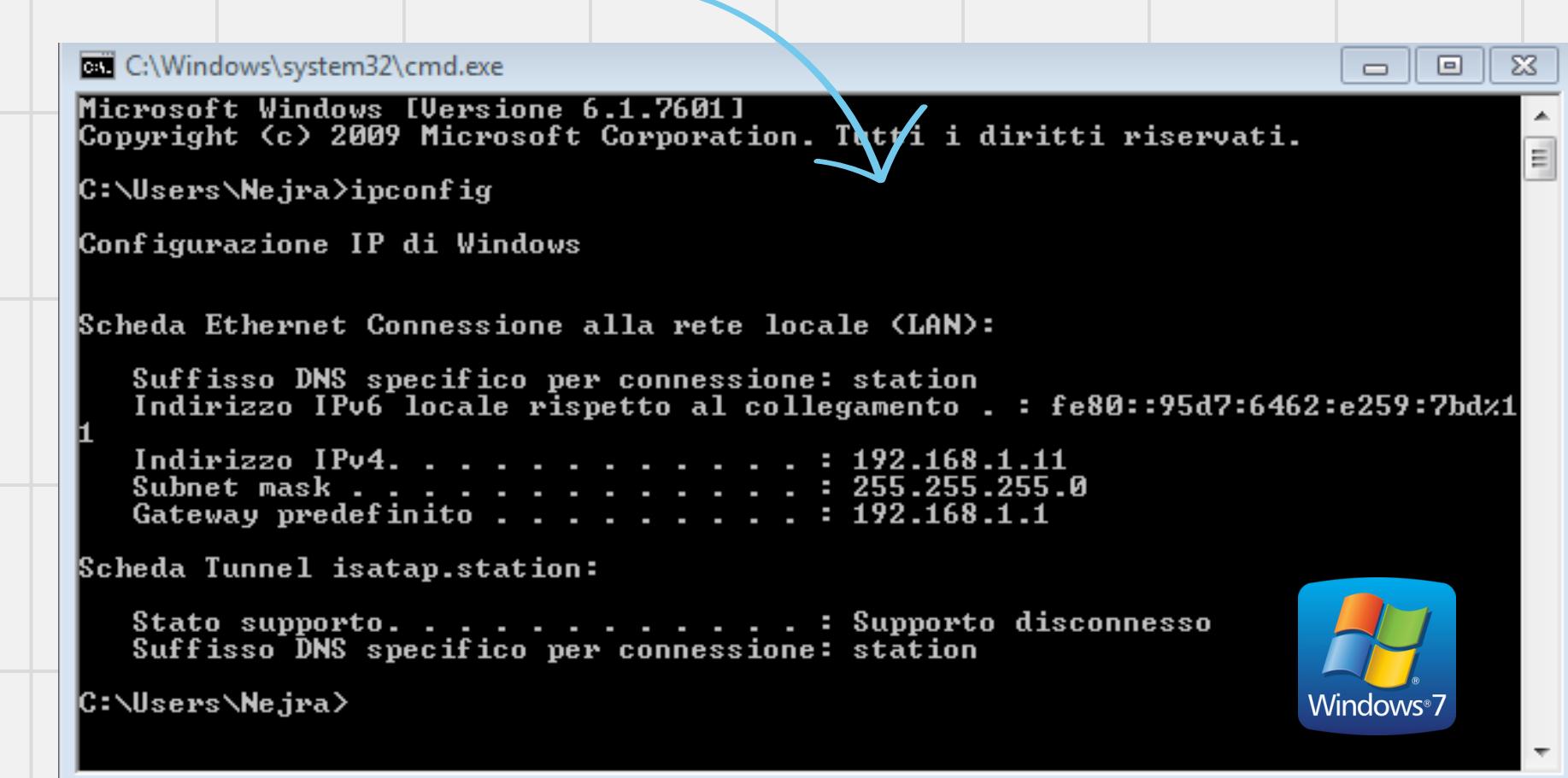
TIPOLOGIA SCANSIONE

8

OS FINGERPRINT

9

INFO OTTENUTE



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Nejra>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):
  Suffisso DNS specifico per connessione: station
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::95d7:6462:e259:7bd%1
  1  Indirizzo IPv4. . . . . : 192.168.1.11
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.station:
  Stato supporto. . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione: station

C:\Users\Nejra>
```





VAN ZWAM ARJEN

OS FINGERPRINT

Lo stesso Help di nmap utilizzato precedentemente aiuta dicendo:

<<OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to

promising targets

--osscan-guess: Guess OS more aggressively >>

Ho dunque utilizzato la funzione -O nel mio target Win7(192.168.1.11)

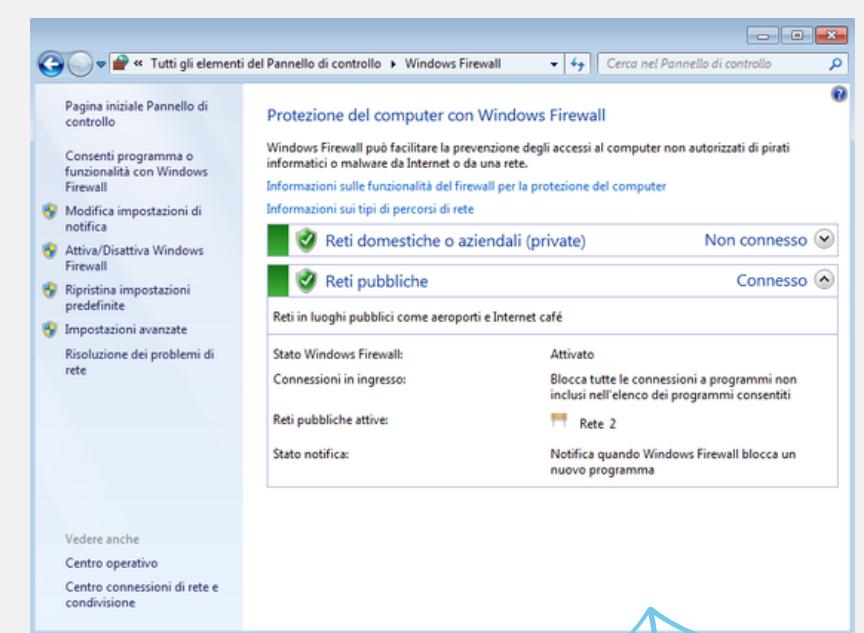


L'OS detection su Windows7 ha evidenziato differenze rispetto alle informazioni relative a Metasploitable2

```
(root㉿kali)-[~/usr/share/nmap/scripts]
# nmap -O 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 10:14 EDT      Firewall Win7 ON
Nmap scan report for Windows7.station (192.168.1.11)
Host is up (0.00042s latency).
All 1000 scanned ports on Windows7.station (192.168.1.11) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:ED:91:8C (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 27.85 seconds

(root㉿kali)-[~/usr/share/nmap/scripts]
#
```





VAN ZWAM ARJEN



QUALE POTREBBE ESSERE UNA VALIDA RAGIONE PER SPIEGARE IL RISULTATO OTTENUTO DALLA SCANSIONE SULLA MACCHINA WINDOWS 7? CHE TIPO DI SOLUZIONE POTRESTE PROPORRE PER CONTINUARE LE SCANSIONI?

Ovviamente non ci sono grossi risultati perché i **Firewall** di Windows 7 sono **ABILITATI**.

The screenshot shows the Windows Firewall control panel. On the left, there's a sidebar with links like 'Pagina iniziale Pannello di controllo', 'Consenti programma o funzionalità con Windows Firewall', 'Modifica impostazioni di notifica', 'Attiva/Disattiva Windows Firewall', 'Ripristina impostazioni predefinite', 'Impostazioni avanzate', 'Risoluzione dei problemi di rete', 'Vedere anche', 'Centro operativo', and 'Centro connessioni di rete e condivisione'. The main area displays 'Protezione del computer con Windows Firewall' with sections for 'Reti domestiche o aziendali (private)' (Non connesso) and 'Reti pubbliche' (Connesso). Below these are sections for 'Reti in luoghi pubblici come aeroporti e Internet café', 'Stato Windows Firewall', 'Connessioni in ingresso', and 'Reti pubbliche attive'. A terminal window at the bottom shows the command `# nmap -O 192.168.1.11` being run, followed by the output of an Nmap scan.

PRIMA

The screenshot shows the Windows Firewall control panel after changes have been made. The 'Reti pubbliche' section now shows a red warning icon and the status 'Non sono attualmente in uso le impostazioni consigliate di Windows Firewall per la protezione del computer'. The terminal window shows the same Nmap command and output as the previous screenshot, but the results are different, indicating that the firewall is active and blocking the scan.

DOPPO