

**Traccia: Tecniche di scansione con Nmap** Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

Ecco una relazione tecnica sulle differenze tra i comandi Nmap specificati e i risultati che producono in output:

### 1. **nmap -O ip target --osscan-target:**

- Questo comando esegue un'analisi di rilevamento del sistema operativo (OS) del target specificato.
- Utilizza i pacchetti inviati al target per analizzare le caratteristiche e le risposte del sistema operativo.
- Fornisce informazioni sull'OS del target, come il nome, la versione, e talvolta altre caratteristiche specifiche del sistema operativo.
- Questo comando richiede privilegi di amministratore per eseguire l'analisi del sistema operativo con precisione.
- L'output includerà una valutazione dell'OS più probabile del target, basata sulle risposte ricevute durante l'analisi.

```
(root@Team1-BuildWeek-Epicode)-[/home/kali]
# nmap -O 192.168.50.101 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:46 EDT
Nmap scan report for meta.epi (192.168.50.101)
Host is up (0.00020s 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: 08:00:27:68:CF:D4 (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 1.60 seconds
```

### 2. **nmap -sV iptarget:**

- Questo comando esegue una scansione dei servizi sul target specificato per determinare le versioni dei servizi in esecuzione.
- Interroga le porte aperte sul target e tenta di determinare i servizi e le relative versioni.
- L'output fornirà un elenco dei servizi e delle versioni trovate sul target.
- È utile per comprendere quali versioni dei servizi sono in esecuzione sul target, consentendo di identificare possibili vulnerabilità o versioni non aggiornate.

```

root@Team1-BuildWeek-Epicode: /home/kali
File Actions Edit View Help

(root@Team1-BuildWeek-Epicode)-[/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:45 EDT
Nmap scan report for meta.epi (192.168.50.101)
Host is up (0.000042s 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         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
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: 08:00:27:68:CF:D4 (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 http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.52 seconds

(root@Team1-BuildWeek-Epicode)-[/home/kali]
# 

```

### 3. nmap -sT ip target:

- Questo comando esegue una scansione TCP completa del target specificato.
- Utilizza una connessione TCP completa per determinare lo stato delle porte sul target, come aperto, chiuso o filtrato.
- Richiede l'invio di un pacchetto di connessione TCP completo per ogni porta da analizzare, rendendolo più lento rispetto ad altre modalità di scansione come `-sS`.
- L'output fornirà lo stato delle porte TCP sul target, insieme ad altre informazioni pertinenti come il servizio associato a ciascuna porta, se disponibile.

```
(root@Team1-BuildWeek-Epicode)-[/home/kali]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:47 EDT
Nmap scan report for meta.epi (192.168.50.101)
Host is up (0.00039s 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: 08:00:27:68:CF:D4 (Oracle VirtualBox virtual NIC)

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

```
(root@Team1-BuildWeek-Epicode)-[/home/kali]
#
```

#### 4. **nmap -sS ip target:**

- Questo comando esegue una scansione TCP SYN del target specificato.
- Utilizza pacchetti SYN per determinare lo stato delle porte sul target.
- Poiché non stabilisce una connessione completa, è più veloce rispetto a una scansione TCP completa (-sT), ma può essere meno affidabile in determinate situazioni.
- L'output fornirà lo stato delle porte TCP sul target, utilizzando la tecnica di scansione SYN.

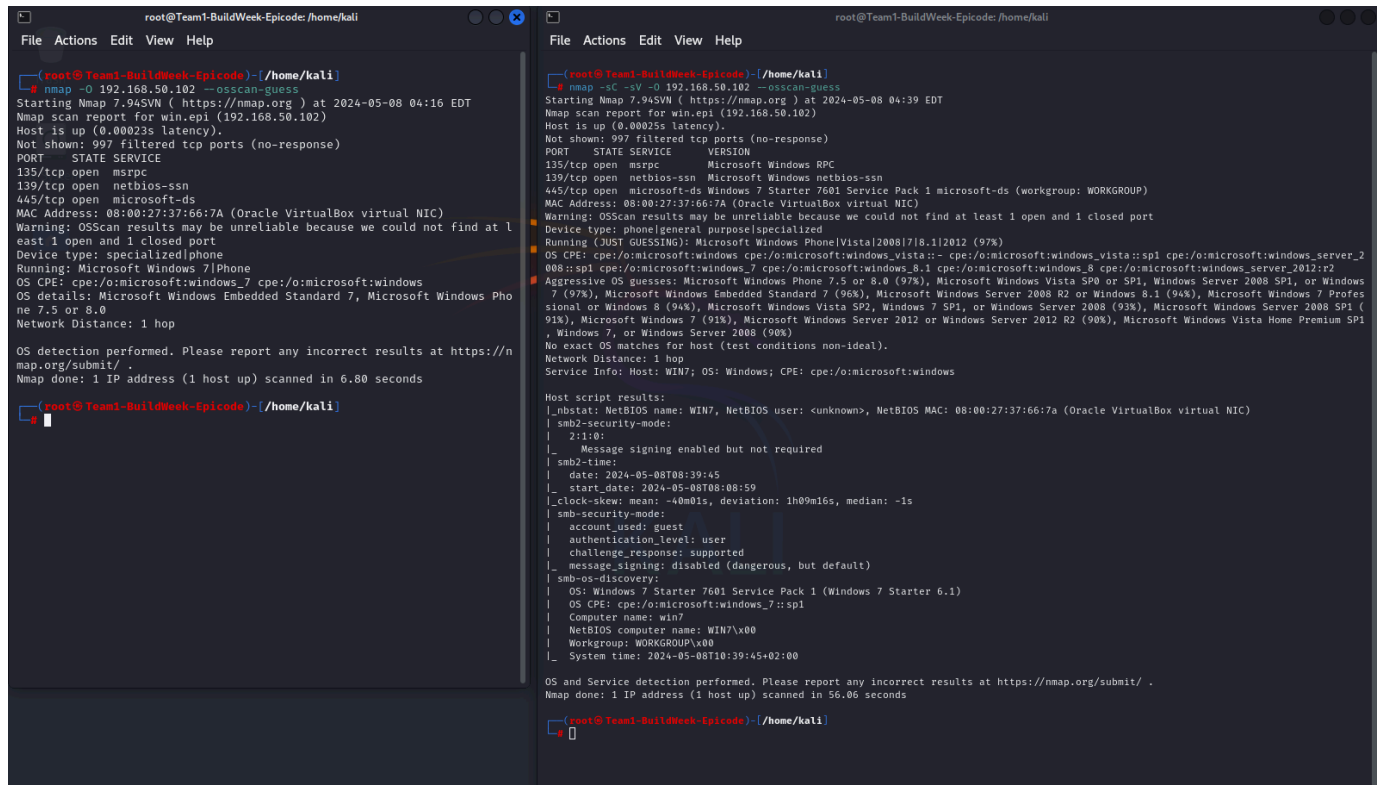
```
(root@Team1-BuildWeek-Epicode)-[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:47 EDT
Nmap scan report for meta.epi (192.168.50.101)
Host is up (0.00010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
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: 08:00:27:68:CF:D4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

In sintesi, mentre tutti questi comandi Nmap sono utilizzati per eseguire varie forme di scansione e rilevamento sui target specificati, ciascuno ha un approccio unico e fornisce informazioni diverse. La scelta del comando dipenderà dall'obiettivo specifico dell'analisi e dalle condizioni della rete.

E la seguente sul target Windows 7: • OS fingerprint.

**Quesito extra (al completamento dei quesiti sopra): 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?**



```
root@Team1-BuildWeek-Epicode: /home/kali
File Actions Edit View Help

root@Team1-BuildWeek-Epicode: /home/kali
# nmap -O 192.168.50.102 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:16 EDT
Nmap scan report for win.epi (192.168.50.102)
Host is up (0.00023s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:37:66:7A (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|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 6.80 seconds

root@Team1-BuildWeek-Epicode: /home/kali
File Actions Edit View Help

root@Team1-BuildWeek-Epicode: /home/kali
# nmap -sC -sV -O 192.168.50.102 --osscan-guess
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:39 EDT
Nmap scan report for win.epi (192.168.50.102)
Host is up (0.00025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Starter 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:37:66:7A (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: phone|general purpose|specialized
Running (JUST GUESSED): Microsoft Windows Phone|Vista|2008|7|8.1|2012 (97%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (97%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (97%), Microsoft Windows Embedded Standard 7 (96%), Microsoft Windows Server 2008 R2 or Windows 8.1 (94%), Microsoft Windows 7 Professional or Windows 8 (94%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft Windows Server 2008 SP1 (91%), Microsoft Windows 7 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (90%), Microsoft Windows Vista Home Premium SP1, Windows 7, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:37:66:7A (Oracle VirtualBox virtual NIC)
|_ smb-security-mode:
|   21:0:
|_   Message signing enabled but not required
|_ smb2-time:
|   date: 2024-05-08T08:39:45
|_   start_date: 2024-05-08T08:08:59
|_ clock-skew: mean: -40m01s, deviation: 1h09m16s, median: -1s
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|   OS: Windows 7 Starter 7601 Service Pack 1 (Windows 7 Starter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2024-05-08T10:39:45+02:00

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.06 seconds

root@Team1-BuildWeek-Epicode: /home/kali
#
```

**Se durante la scansione su una macchina Windows 7 si ottiene un risultato inaspettato o incompleto, potrebbero esserci diverse ragioni:**

**Firewall:** Il firewall integrato di Windows 7 potrebbe bloccare o filtrare le richieste di scansione inviate da Nmap, limitando la capacità di Nmap di determinare lo stato delle porte o identificare i servizi in esecuzione.

**Risposta alle Scansioni:** Windows 7 potrebbe non rispondere correttamente alle richieste di scansione inviate da Nmap. Questo potrebbe essere dovuto a configurazioni di rete specifiche, politiche di sicurezza o altre ragioni.

**Servizi non in Esecuzione:** Se non ci sono servizi o porte aperte sulla macchina Windows 7, Nmap potrebbe non trovare nulla durante la scansione.

Per continuare le scansioni su una macchina Windows 7, potremmo considerare le

**seguenti soluzioni:**

**Escludere il Firewall:** Temporaneamente disattivare il firewall di Windows 7 durante la scansione per vedere se ciò influisce sui risultati. Tuttavia, dobbiamo fare attenzione a mantenere la sicurezza della rete durante questa operazione.

**Configurare il Firewall:** Aggiungere regole al firewall di Windows 7 per consentire le comunicazioni in ingresso da Nmap, in modo da garantire che le scansioni siano consentite e che le risposte non vengano bloccate.

**Utilizzare Opzioni di Scansione Specifiche:** Utilizzare opzioni di scansione specifiche di Nmap che potrebbero essere più adatte per bypassare le difese della rete o le politiche di sicurezza di Windows 7. Ad esempio, potresti provare a utilizzare la scansione SYN stealth (`-sS`) o la scansione UDP (`-sU`).

**Esaminare le Impostazioni di Sicurezza:** Verificare le impostazioni di sicurezza della macchina Windows 7 per assicurarti che non ci siano configurazioni che potrebbero interferire con le scansioni di Nmap. Questo potrebbe includere controlli dell'account utente (UAC), impostazioni del firewall, politiche di gruppo e altro ancora.

**Aggiornamenti e Patch:** Assicurarci che il sistema Windows 7 sia aggiornato con gli ultimi aggiornamenti di sicurezza e patch, poiché questo potrebbe influenzare il comportamento del sistema durante le scansioni.

**Monitoraggio e Logging:** Monitorare attentamente il traffico di rete e i log di sistema durante le scansioni per individuare eventuali anomalie o segni di attività sospetta. Questo può aiutare a identificare eventuali problemi e a prendere provvedimenti correttivi.