

Scansione dei servizi con Nmap - Tecniche di scansione

Si richiede 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.**

Si richiede di effettuare la seguente scansione sul **target Windows 7**:

- **OS fingerprint**

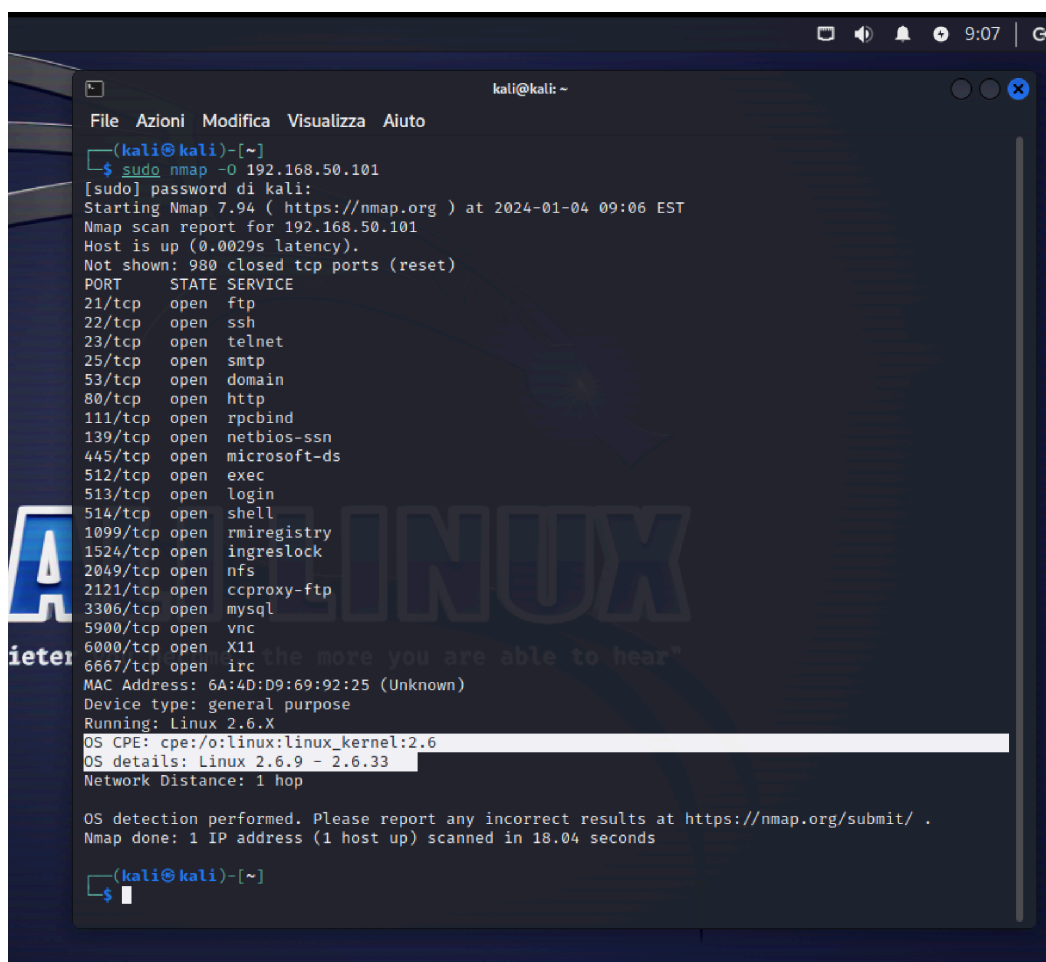
Modifico le impostazioni di rete delle macchine virtuali per fare in modo che **i due target** siano **sulla stessa rete**.

Target: META

- ❖ **IP:** 192.168.50.101
- ❖ **Sistema Operativo:** distribuzione Linux che utilizza il kernel compreso tra le versioni 2.6.9 e 2.6.33
- ❖ **Porte Aperte:** 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5900, 6000, 6667

OS fingerprint

Ho identificato il tipo e la versione del sistema operativo con il comando “sudo nmap -O 192.168.50.101”:



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
(kali@kali)~  
$ sudo nmap -O 192.168.50.101  
[sudo] password di kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 09:06 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.0029s latency).  
Not shown: 980 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  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
MAC Address: 6A:4D:D9:69:92:25 (Unknown)  
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 18.04 seconds  
  
(kali@kali)~  
$
```

OS Fingerprinting (Rilevamento del Sistema Operativo): Questo comando serve per rilevare il sistema operativo in esecuzione su un host di rete analizzando le risposte alle richieste inviate. Si basa su pattern di risposta specifici per i diversi sistemi operativi. Tuttavia, può essere impreciso a causa della possibilità di alterare o nascondere deliberatamente le informazioni di risposta.

Era possibile aggiungere questo script alla scansione di base dell'OS (-O) “—script smb-os-discovery” per ottenere informazioni più dettagliate sul sistema operativo dell'host tramite il protocollo SMB.

Syn Scan

La scansione Syn delle porte invia pacchetti SYN alle varie porte dell'host di destinazione. Se la porta è aperta, l'host risponderà con un pacchetto SYN-ACK; se è chiusa, l'host risponderà con un pacchetto RST.

Ho utilizzato il comando “sudo nmap -sS 192.168.50.101”:

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 09:08 EST
Nmap scan report for 192.168.50.101
Host is up (0.00073s latency).
Not shown: 980 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
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
MAC Address: 6A:4D:D9:69:92:25 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

TCP connect

La scansione TCP tenta di stabilire una connessione TCP completa con tutte le porte sull'host di destinazione.

Ho utilizzato il comando “sudo nmap -sT 192.168.50.101”

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 09:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 980 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
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
MAC Address: 6A:4D:D9:69:92:25 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 16.66 seconds
```

Differenze tra i risultati della scansioni TCP connect e SYN?

Nei risultati delle scansioni non ci sono differenze ma hanno comunque caratteristiche diverse:

TCP Connect	SYN Scan
Esegue una connessione TCP completa , che è più affidabile e preciso ma potenzialmente più lenta.	Invia pacchetti SYN per determinare lo stato delle porte senza stabilire una connessione completa (solo il primo step della connessione TCP). È più veloce, ma può non essere accurato al 100%
È più facilmente rilevabile	È meno invasiva e più discreta, ad esempio se non si volesse lasciare tracce
È utile per ottenere informazioni dettagliate sullo stato delle porte	Potrebbe non riuscire a identificare correttamente lo stato delle porte speciali o filtrate

Se il "Three-Way-Handshake" non va a buon fine, la connessione non è stabilita e non si completa il processo di handshake.

Si ferma al SYN-ACK: interrompe la comunicazione inviando un pacchetto RST(reset) per "chiudere" la potenziale connessione.

Version detection

Version Detection (Rilevamento della Versione) serve per identificare la versione dei servizi in ascolto sulle porte aperte. Analizza le risposte dei servizi per determinare la versione esatta del software in esecuzione su tali porte, aiutando a individuare potenziali vulnerabilità o versioni datate di software.

Ho usato il comando “`sudo nmap -sV 192.168.50.101`” per ottenere i **servizi in ascolto con versione**:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 09:10 EST
Nmap scan report for 192.168.50.101
Host is up (0.00065s latency).
Not shown: 980 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
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
MAC Address: 6A:4D:D9:69:92:25 (Unknown)
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 53.59 seconds
```

Target: WINDOWS

- ❖ IP: 192.168.50.102
- ❖ Sistema Operativo: Windows
- ❖ Porte Aperte: 135, 139, 445, 5357, 49152-49156

OS fingerprint

```
(kali㉿kali)-[~]  
$ sudo nmap -O 192.168.50.102  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 09:13 EST  
Nmap scan report for 192.168.50.102  
Host is up (0.0035s latency).  
All 1000 scanned ports on 192.168.50.102 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 0A:AE:3F:E0:66:7B (Unknown)  
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_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 38.93 seconds
```

Quesito extra: 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?

Si possono modificare nel Pannello di controllo di Windows:

- Apertura TCP/UDP nelle regole firewall in entrata
- Apertura TCP/UDP nelle regole firewall in uscita
- Aggiungere ICMPv4

ICMPv4 svolge un ruolo cruciale nel garantire la corretta comunicazione e il funzionamento delle reti IP, fornendo meccanismi di segnalazione e diagnostica per individuare e risolvere problemi di rete.