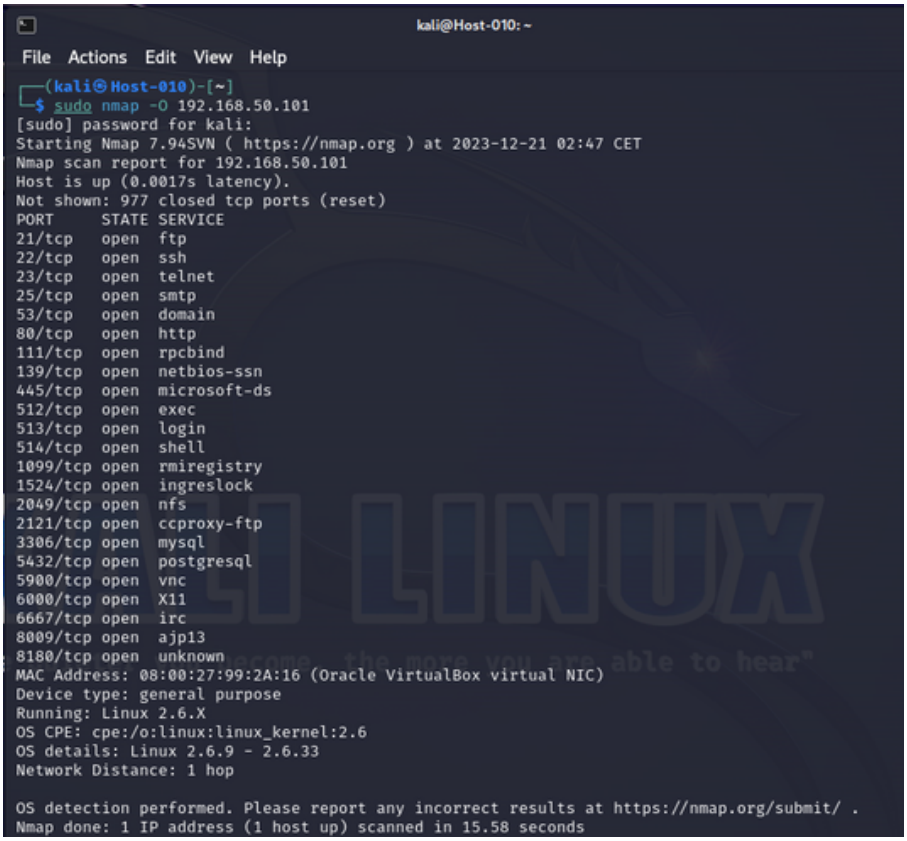
Tecniche di scansione con Nmap

Traccia: 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.
E le seguenti sul target Windows 7:
OS fingerprint .
A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):
IP
Sistema Operativo
Porte Aperte
Servizi in ascolto con versione
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?

Target: Metasploitable (IP 192.168.50.101)

OS fingerprint:

- Comando: sudo nmap -O 192.168.50.101
- Descrizione: questo comando effettua l'individuazione del sistema operativo



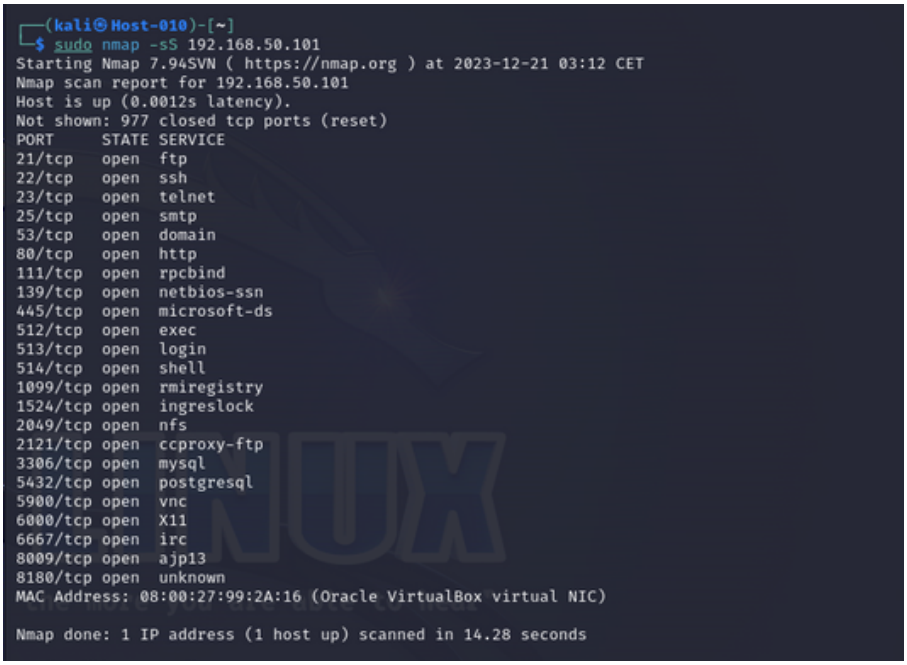
Porte Aperte:

- 21/tcp: FTP (File Transfer Protocol)
- 22/tcp: SSH (Secure Shell)
- 23/tcp: Telnet (non sicuro)
- 25/tcp: SMTP (Simple Mail Transfer Protocol)
- 53/tcp: DNS (Domain Name Service)
- 80/tcp: HTTP (Hypertext Transfer Protocol)
- 111/tcp: RPCbind
- 139/tcp e 445/tcp: NetBIOS e Microsoft DS, utilizzati per la condivisione di file e stampanti in Windows
- 512/tcp, 513/tcp, 514/tcp: Servizi Unix rlogin/rsh
- 1099/tcp: RMI (Java Remote Method Invocation) Registry
- 1524/tcp: Ingreslock, potenzialmente vulnerabile
- 2049/tcp: NFS (Network File System)
- 2121/tcp: CCProxy FTP
- 3306/tcp: MySQL Database
- 5432/tcp: PostgreSQL Database
- 5900/tcp: VNC (Virtual Network Computing)
- 6000/tcp: X11 (sistema di finestre usato con Unix)
- 6667/tcp: IRC (Internet Relay Chat)
- 8009/tcp e 8180/tcp: Sembra essere legato a server Apache Tomcat o servizi simili.

Sistema Operativo: Esegue Linux, con un kernel versione tra 2.6.9 e 2.6.33.

SYN SCAN:

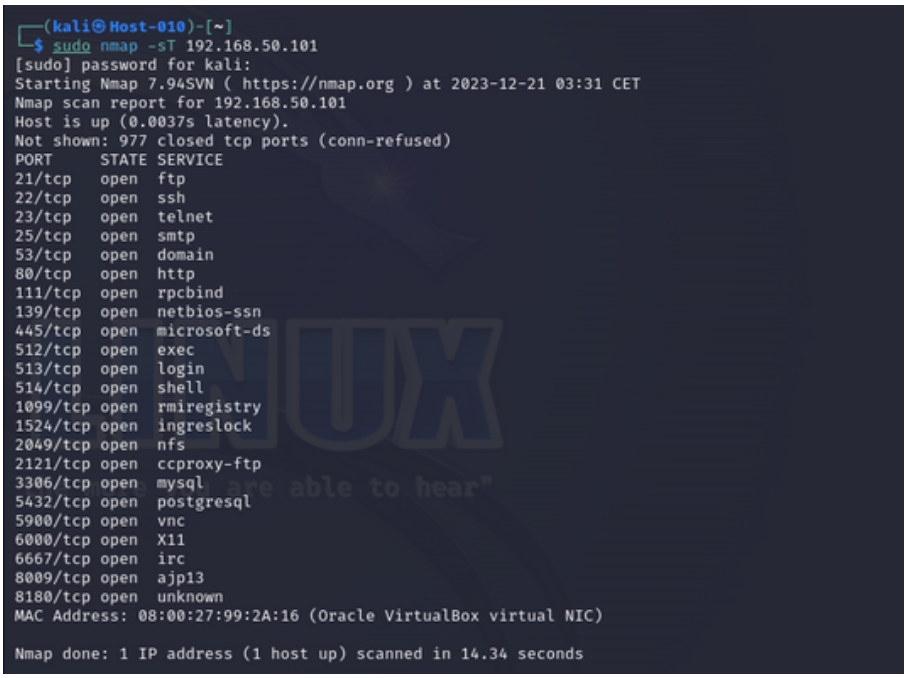
- Comando: sudo nmap -sS 192.168.50.101
- Descrizione: una scansione SYN invia pacchetti TCP SYN per iniziare una connessione, ma non completa il "3-way handshake".



Risultato della scansione SYN:
La scansione SYN, "half-open scanning", è meno intrusiva e meno rilevabile rispetto ad una scansione completa TCP Connect. I risultati sono coerenti con la scansione precedente, suggerendo che le porte aperte sono effettivamente in ascolto e accessibili.

TCP CONNECT:

- Comando: sudo nmap -sT 192.168.50.101
- Descrizione: la scansione TCP Connect completa il "3-way handshake" TCP.



Risultati ottenuti dalla scansione TCP Connect:
La scansione TCP Connect ha confermato ulteriormente i risultati ottenuti nelle precedenti scansioni (SYN e OS Fingerprinting). Diversamente dalla scansione SYN la scansione TCP Connect completa il processo di handshake TCP per ogni porta, rendendola più visibile nei log rispetto alla scansione SYN.

PRIMO QUESITO "Confronto con la Scansione SYN":

- Il fatto che i risultati della scansione TCP Connect siano in linea con quelli della scansione SYN indica che non ci sono filtri o firewall che stanno bloccando le richieste di handshake completo, che è ciò che fa la differenza tra le due scansioni.
- La scansione TCP Connect è più facile da rilevare rispetto alla scansione SYN perché completa il processo di handshake TCP. Questo tipo di scansione può essere registrato più facilmente dai sistemi di rilevamento intrusioni.
- La conferma che le stesse porte sono aperte in entrambe le scansioni SYN e TCP Connect fornisce una maggiore sicurezza che questi servizi sono attivamente in ascolto e non sono falsi positivi dovuti a filtraggi di pacchetti.

Version Detection:

- Comando: sudo nmap -sV 192.168.50.101
- Descrizione: identifica le versioni dei servizi in ascolto sulle porte aperte

```
┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 03:51 CET
Nmap scan report for 192.168.50.101
Host is up (0.0014s 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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:99:2A:16 (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 140.22 seconds
```

Risultati ottenuti dalla Version Detection:
La scansione per la Version Detection è particolarmente utile per identificare versioni specifiche dei software che potrebbero essere vulnerabili.
Molte delle versioni dei servizi rilevati sono note per essere vulnerabili.
In particolare il servizio bindshell sulla 1524/tcp indica una backdoor aperta per l'accesso root al sistema.
Servizi obsoleti o configurazioni non sicure, come indicato dalle versioni dei servizi e dai protocolli, suggeriscono che questa macchina è altamente vulnerabile e potrebbe essere facilmente compromessa.
Tali risultati non dovrebbero sorprenderci dato che Metasploitable è una macchina virtuale creata appositamente per essere vulnerabile.

Target: WINDOWS 7 (IP 192.168.50.102)

OS Fingerprinting:

- Comando: sudo nmap -O 192.168.50.102
- Descrizione: il comando identifica il sistema operativo.

```
┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 04:06 CET
Nmap scan report for 192.168.50.102
Host is up (0.0018s 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:AC:8B:2D (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embe
dded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:window
s_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded S
tandard 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 dev
ice
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 35.30 seconds
```

Risultati ottenuti:
L'avviso mostrato indica che i risultati del rilevamento del sistema operativo potrebbero non essere affidabili a causa della mancanza di porte aperte e chiuse trovate. Questo è un aspetto importante da considerare nell'interpretazione dei risultati.
Sistemi Operativi Potenziali:

- 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 o 8.0
- Microsoft Windows XP SP3, Windows 7 o Windows Server 2012
- Palmmicro AR1688 VoIP module
- VMware Player virtual NAT device

Quesito EXTRA
Per ottenere un risultato più preciso è possibile:

- disabilitare temporaneamente il firewall su Windows
- creare una regola del firewall di Windows per consentire il traffico dalla mia macchina Kali
- usare opzioni di scansione aggressive: come -T4 o -A che possono a volte superare alcune forme di filtraggio, ma più invasive e facilmente rilevabili
- specificare le porte: posso chiedere ad esempio a Nmap di scansionare quelle porte che so essere aperte o chiuse utilizzando l'opzione -p. Ad esempio: sudo nmap -p 80,443 -O 192.168.50.102.

Aggiungo una regola del firewall di Windows e lancio il comando:
sudo nmap -O 192.168.50.102
La scansione indica che il sistema operativo in esecuzione sulla macchina target è probabilmente una versione di Microsoft Windows 7, Windows Server 2008, Windows 8 o Windows 8.1.

```
┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 04:31 CET
Nmap scan report for 192.168.50.102
Host is up (0.00089s 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:AC:8B:2D (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 16.21 seconds

┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 04:33 CET
Nmap scan report for 192.168.50.102
Host is up (0.0022s latency).
Not shown: 991 closed tcp ports (reset)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:AC:8B:2D (Oracle VirtualBox virtual NIC)
Service Info: Host: MARIA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.84 seconds
```

Lancio successivamente il comando:
sudo nmap -sV 192.168.50.102 per ottenere informazioni dettagliate sulle porte aperte, sui servizi attivi e le loro versioni. Nella prossima pagina vediamo nel dettaglio Porte e Servizi.

.

Porte e Servizi:

- 135/tcp: Microsoft Windows RPC (Remote Procedure Call), un servizio che permette ai programmi di eseguire codice su macchine remote.
- 139/tcp: NetBIOS Session Service (SSN), usato per la condivisione di file e stampanti in reti Windows.
- 445/tcp: Microsoft Directory Services, usato per la condivisione di file e stampanti e per altre funzioni di rete in Windows.
- 49152/tcp - 49157/tcp: Queste porte sono tipicamente utilizzate da Microsoft Windows per servizi RPC dinamici. Sono assegnate dinamicamente quando un servizio che utilizza RPC viene avviato e possono variare ad ogni riavvio del servizio o del sistema.