Relazione sulle Tecniche di Scansione con Nmap

Obiettivo:

Effettuare scansioni su Metasploitable e Windows 7 per raccogliere informazioni su sistema operativo, porte aperte e servizi in ascolto con le rispettive versioni.

Target:

- **Metasploitable: 192.168.50.101**
- **Windows 7: 192.168.50.102**

Scansioni Effettuate su Metasploitable (192.168.50.101)

1. **OS Fingerprint**
   - Comando: sudo nmap -O 192.168.50.101
   - Risultato: Linux, molte porte aperte tra cui ftp, ssh, telnet, smtp, http, mysql.
2. **SYN Scan**
   - Comando: sudo nmap -sS 192.168.50.101
   - Risultato: Stesse porte aperte della TCP Connect Scan, metodo più stealth.
3. **TCP Connect Scan**
   - Comando: sudo nmap -sT 192.168.50.101
   - Risultato: Stesse porte aperte della SYN Scan, metodo più visibile nei log.
4. **Version Detection**
   - Comando: sudo nmap -sV 192.168.50.101
   - Risultato: Dettagliate versioni dei servizi, ad esempio vsftpd 2.3.4, OpenSSH 4.7p1.

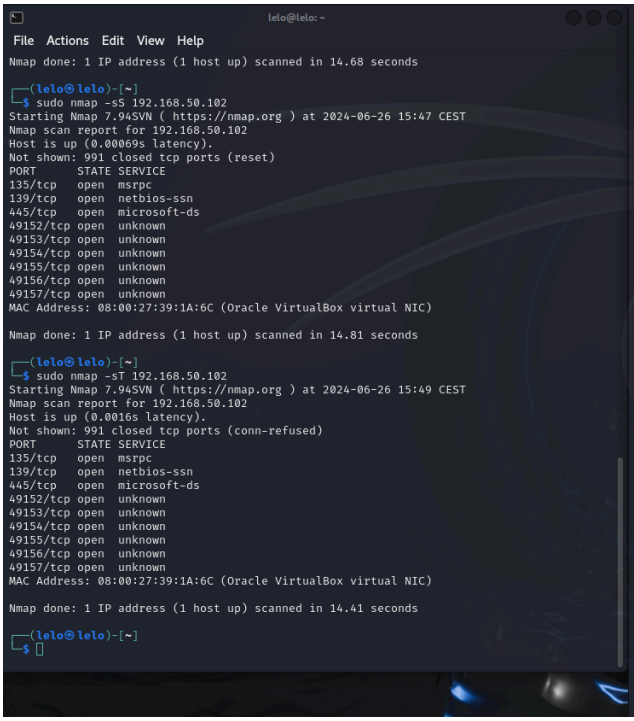
Scansioni Effettuate su Windows 7 (192.168.50.102)

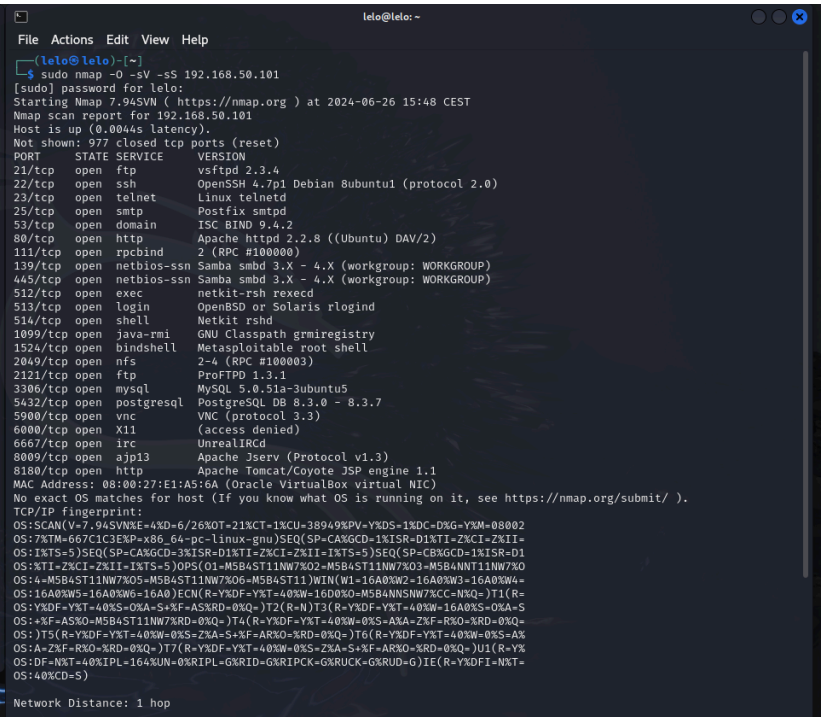
1. OS Fingerprint
   - Comando: sudo nmap -O 192.168.50.102
   - Risultato: Microsoft Windows 7 SP0 - SP1

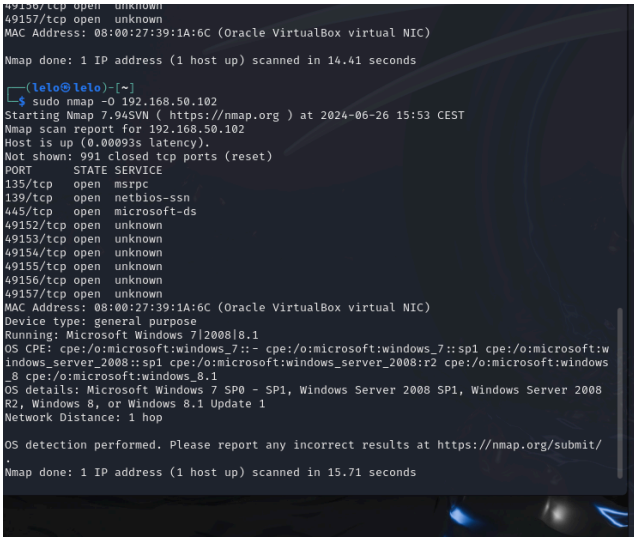
Quesito Extra

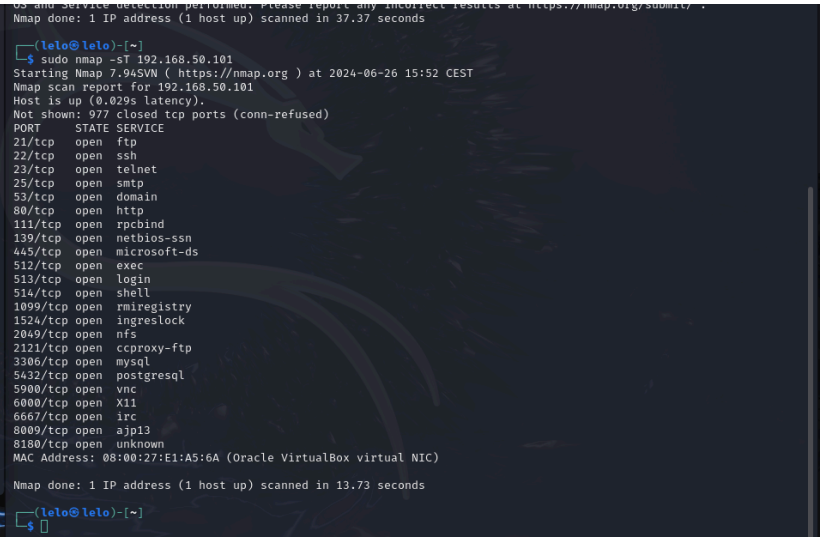
Analisi dei Risultati della Scansione su Windows 7

- **Ragione per i Risultati Ottenuti**: Le porte risultano filtrate, probabilmente a causa del firewall attivo.
- **Soluzione Proposta**: Usare il comando “sudo nmap -T1-2 per avere una ricerca più dedicata e minuziosa, così da poter aggirare il firewall attivo su windows (non c’è lo screen poichè richiedeva molto tempo la scansione). Si potrebbe anche disattivare direttamente il firewall, ma avrebbe poco senso l’esercizio (negli screen c’è la prova con il firewall disattivato).


lelo@lelo: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
┌──(lelo㉿lelo)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 15:47 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00069s 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: 08:00:27:39:1A:6C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
┌──(lelo㉿lelo)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 15:49 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0016s latency).
Not shown: 991 closed tcp ports (conn-refused)
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: 08:00:27:39:1A:6C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
┌──(lelo㉿lelo)-[~]
└─$


lelo@lelo: ~
File Actions Edit View Help
┌──(lelo㉿lelo)-[~]
└─$ sudo nmap -O -sV -sS 192.168.50.101
[sudo] password for lelo:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 15:48 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0044s 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 OpenBSD or Solaris rlogind
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:E1:A5:6A (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/26%OT=21%CT=1%CU=38949%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=667C1C3E%P=x86_64-pc-linux-gnu)SEQ(SP=CA%GCD=1%ISR=D1%TI=Z%CI=Z%II=
OS:I%TS=5)SEQ(SP=CA%GCD=3%ISR=D1%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=CB%GCD=1%ISR=D1
OS:%TI=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O
OS:4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=
OS:16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=
OS:Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S
OS:+%F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF=N%T=
OS:40%CD=S)
Network Distance: 1 hop


49157/tcp open unknown
MAC Address: 08:00:27:39:1A:6C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
┌──(lelo㉿lelo)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 15:53 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00093s 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: 08:00:27:39:1A:6C (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 15.71 seconds


Nmap done: 1 IP address (1 host up) scanned in 37.37 seconds
┌──(lelo㉿lelo)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 15:52 CEST
Nmap scan report for 192.168.50.101
Host is up (0.029s 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:E1:A5:6A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.73 seconds
┌──(lelo㉿lelo)-[~]
└─$