ESERCIZIO S5L2

Prendo l'ip della meta lanciando il comando nmap –sn 192.168.50.0/24 cosi verifica quali host sulla mia rete sono attivi e trovo l'indirizzo della meta che è 192.168.50.11

Lancio il comando nmap –sT per verificare quali porte sono connesse e completano l'handshake e come output mi dice che 997 porte hanno rifiuato ineve porte come http, telnet, ssh sono risultate aperte

Ho lanciato anche il comando nmap –sS per fare una scansione syn che non completa l'handshake e mi permette di essere furtivo. L'output ' molto simile ma ci sono differenze nella velocità. Il sS è più veloce.

Ho lanciato il comando nmpa –sV per vedere quale applicazione ha risposto alla porta aperta: 21/tcp open ftp vsftpd 2.3.4 (un esempio dell'output)

Ho lanciato il comando nmap –O –sV per vedere il sistema operativo e anche la sua versione e questo è stato l'output generato

└─$ sudo nmap -O -sV 192.168.50.11

Starting Nmap 7.95 (https://nmap.org) at 2026-01-08 16:50 EST

Nmap scan report for 192.168.50.11

Host is up (0.0048s 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 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: 08:00:27:81:57:1D (PCS Systemtechnik/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

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 14.42 seconds