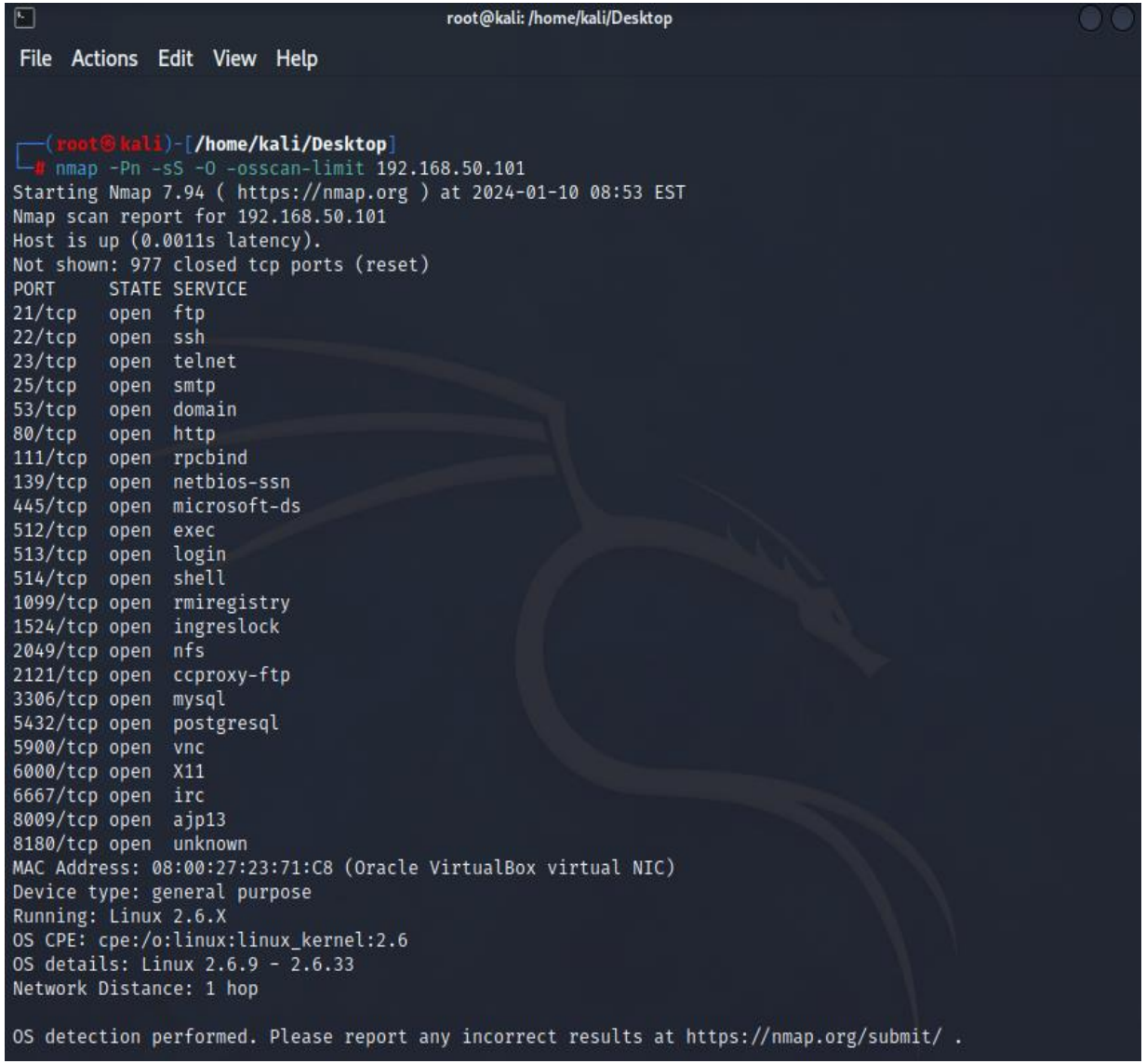
S5 L3

Davide Andreozzi

Tecniche di Scansione con Nmap



Scansione OS Fingerprint + SYN Scan METASPLOITABLE

Comando eseguito:
«nmap –Pn –sS –O –osscan-limit 192.168.50.101»

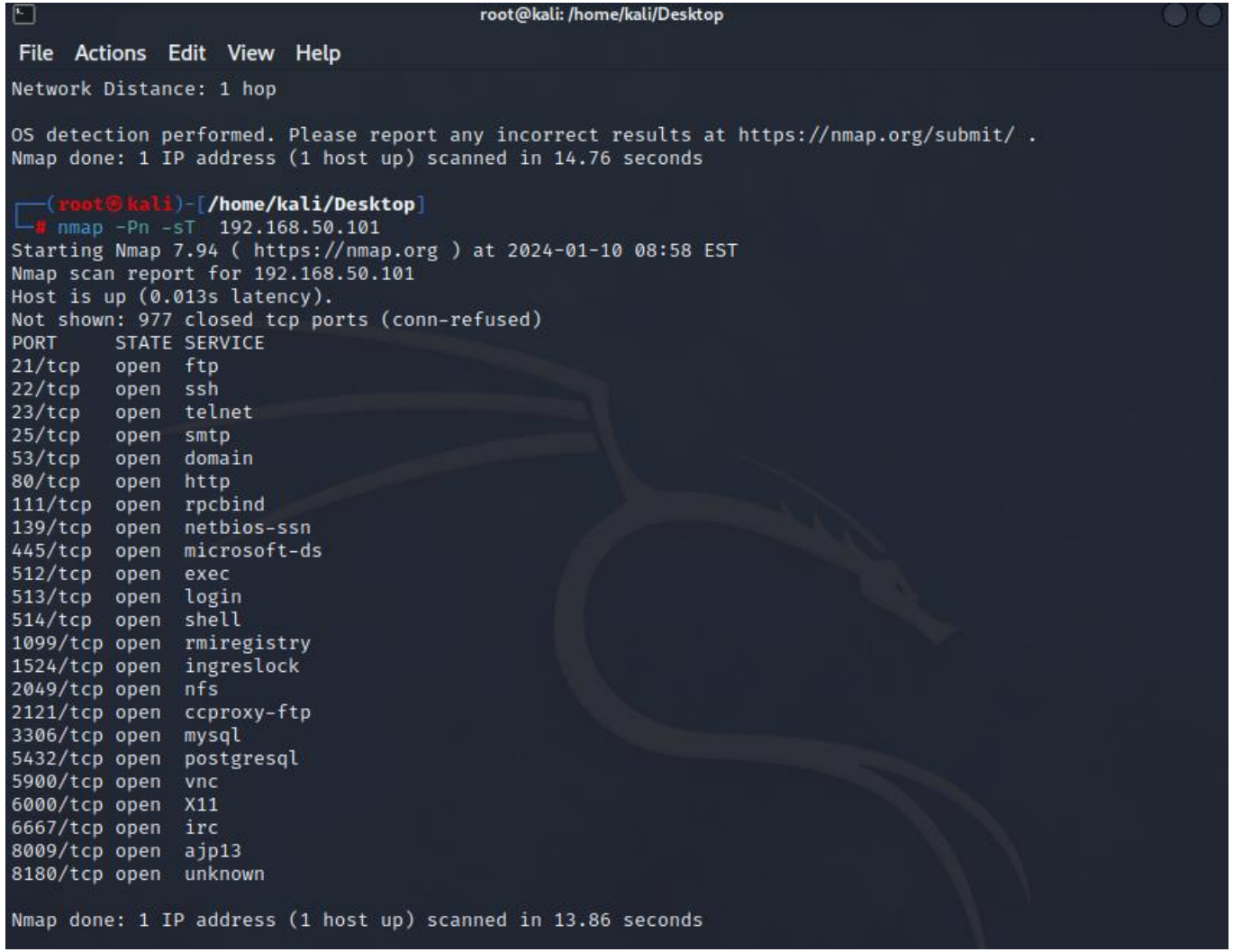
Da questo comando abbiamo eseguito l'identificazione del sistema operativo e una SYN Scan in contemporanea.

Come output riceviamo il numero delle porte chiuse che sono 977 e il pacchetto di risposta «reset». Questa tecnica è più silenziosa della scansione tcp completa proprio perché non andiamo a stabilirla completamente.

Riceveremo anche i dettagli dell'os che in questo caso essendo la macchina target metasploitable avremo come dicitura Linux in OS details.

Ovviamente, abbiamo la lista delle porte aperte e i relativi servizi

Tecniche di Scansione con Nmap



Scansione TCP Completa METASPLOITABLE

Comando eseguito:
«nmap –Pn –sT 192.168.50.101»

Da questo comando abbiamo eseguito una scansione completa, in quanto andremo a completare tutti i passaggi di una connessione TCP

Questo tipo di scansione è più lenta della scansione SYN ("-sS") perché richiede l'intero processo di connessione TCP e quindi può essere più facilmente rilevabile dagli strumenti di monitoraggio della rete. Si può notare rispetto alla precedente slide che la risposta per le porte chiuse è diversa (conn-refused) ovvero la connessione è stata rifiutata.

Tecniche di Scansione con Nmap

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn -sV -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:18 EST
Nmap scan report for 192.168.50.101
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li
nux: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 24.71 seconds
```

Scansione TCP Completa + Versione METASPLOITABLE

Comando eseguito:
«nmap –Pn –sV –sT 192.168.50.101»

Rispetto alla precedente scansione abbiamo aggiunto –sV che ci va ad indicare la versione dei servizi installati.

Utile per andare a cercare eventuali exploit.

OS Fingerprint (Windows 7)

In basso:

Eseguito il comando per rivelare l'OS Fingerprint ma essendo attivo Windows Defender non riusciamo a scansionare il target

A destra:

Disabilitando il FW (Windows Defender) possiamo notare come riusciamo ad eseguire correttamente lo scan e ricevere l'informazioni sulla macchina target e le relative porte aperte, servizi correlati e versioni

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn -sV -sT -O --osscan-limit 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:20 EST
Nmap scan report for 192.168.50.102
Host is up (0.00093s 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:A0:8B:D9 (Oracle VirtualBox virtual NIC)

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 35.68 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn -sV -sT -O --osscan-limit 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:23 EST
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.50.102
Host is up (0.00072s latency).
Not shown: 991 closed tcp ports (conn-refused)
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:A0:8B:D9 (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_ser
::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Window
Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

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 74.90 seconds
```