W11D2

SCANSIONE SERVIZI NMAP SU METASPLOITABLE

La traccia

Traccia: Tecniche di scansione con Nmap

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

La traccia

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

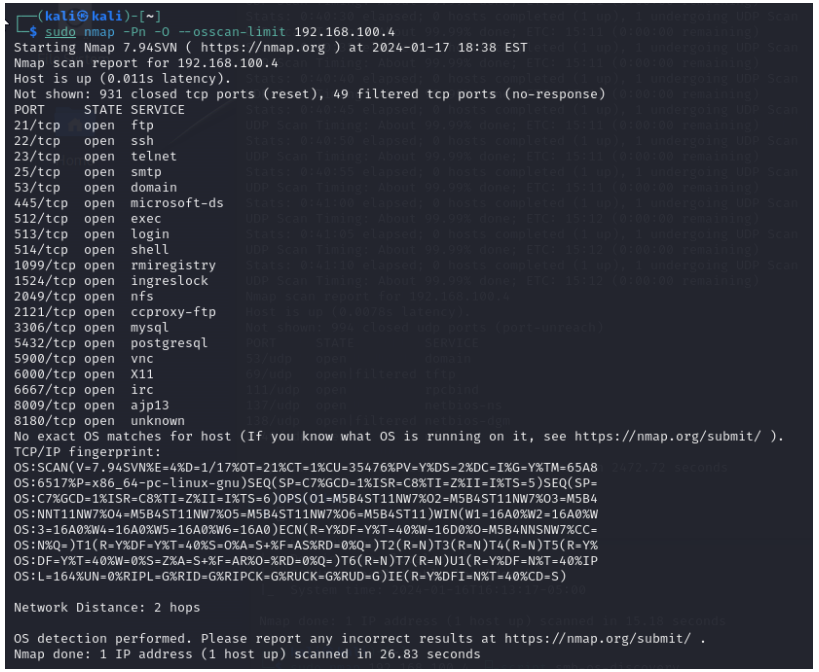
- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

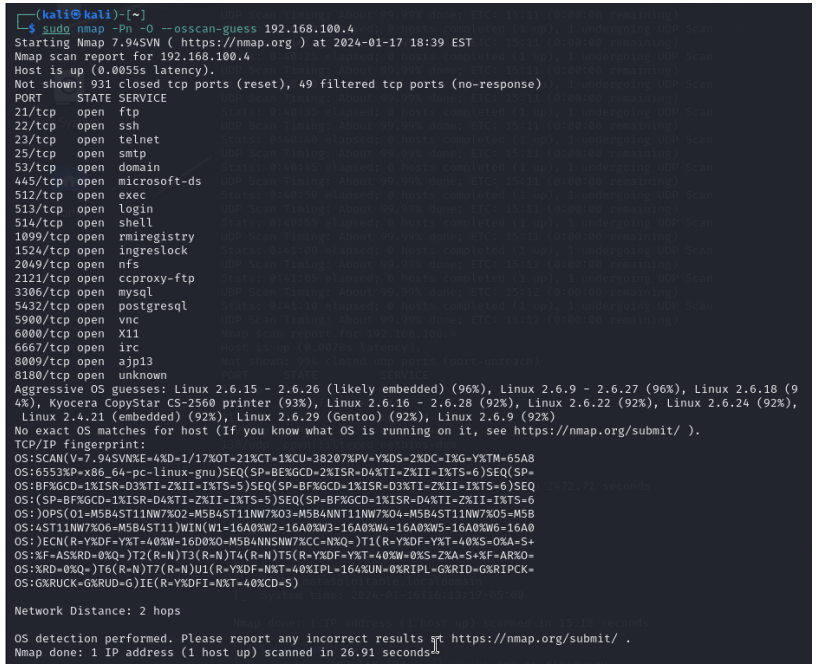
https://www.poftut.com/nmap-output/

nmap -oN report1 IP

Os Fingerprint

Per sapere il sistema operativo del target senza utilizzare il ping abbiamo usato il comando in figura. La differenza tra il primo e il secondo è che col primo non abbiamo avuto risultati, col secondo invece anche se più aggressivo e meno accurato nmap ci da dei possibili risultati.





SYN e TCP Scan and version detection

Si può evincere dalle scansioni che non vi sono differenze in quanto dal TCP Scan, solitamente più invasivo, risultano gli stessi servizi attivi elencati nonostante dovrebbero esserne di più.
In questo caso invece no. Avendo attivato l'opzione dei servizi(-sV) possiamo anche vedere le versioni dei servizi scansionati.

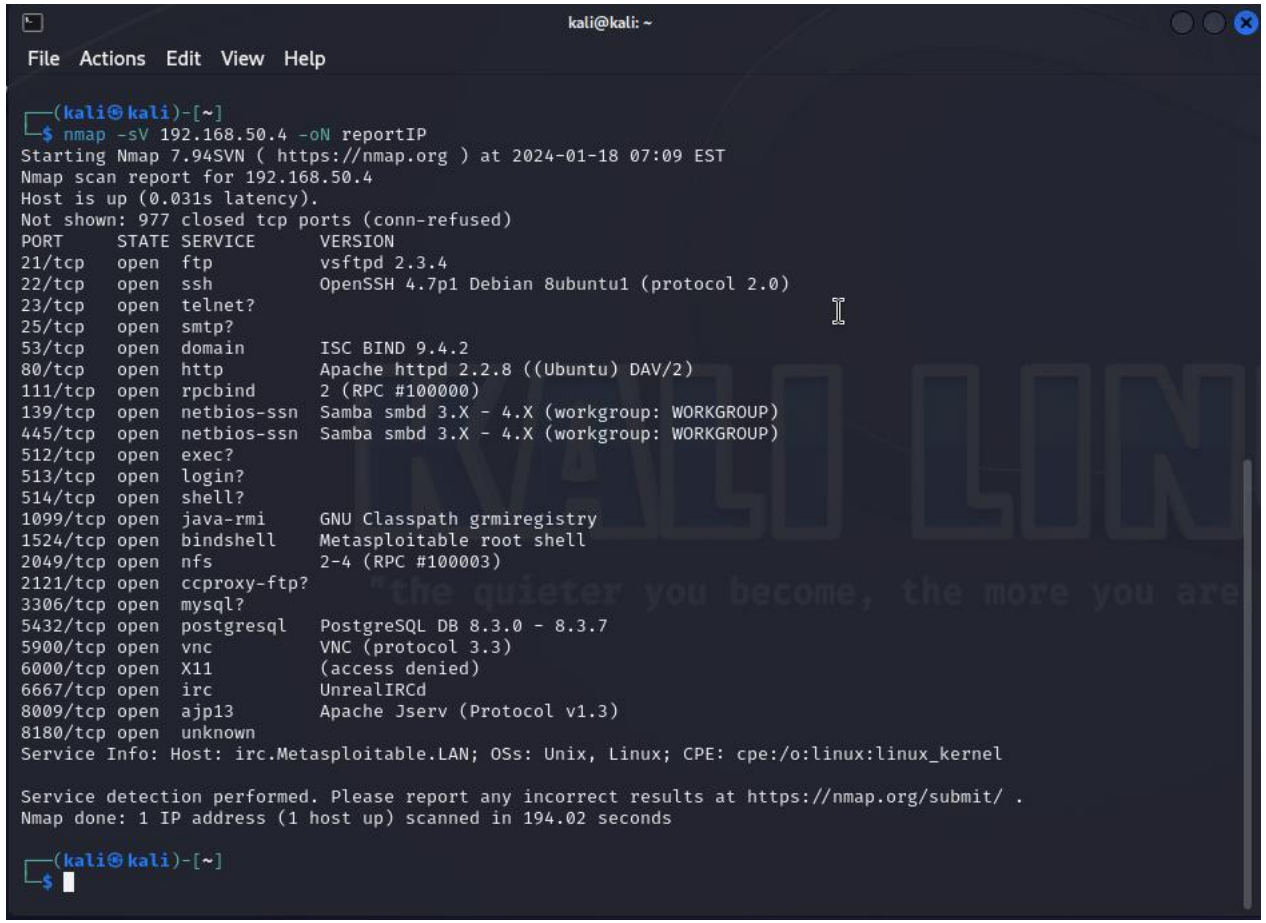
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:48 EST
Nmap scan report for 192.168.100.4
Host is up (0.019s latency).
Not shown: 931 closed tcp ports (reset), 49 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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  unknown
Service Info: Host: 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 195.16 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sT 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:54 EST
Nmap scan report for 192.168.100.4
Host is up (0.018s latency).
Not shown: 931 closed tcp ports (conn-refused), 49 filtered tcp ports (no-response)
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?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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  unknown
Service Info: Host: 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 194.93 seconds
```

Scansione di meta su stessa rete di Kali



In questo caso la scansione dei servizi viene innanzitutto salvata in un file.
Facendo un confronto tra la scansione attuale e quella della stessa macchina ma su rete diversa notiamo che i servizi rilevati sono di più servizi nell'attuale scansione in quanto non stando sulla stessa rete il traffico non viene filtrato dal firewall (per esempio il firewall filtrava di pfsense filtrava il traffico sulla porta 80)