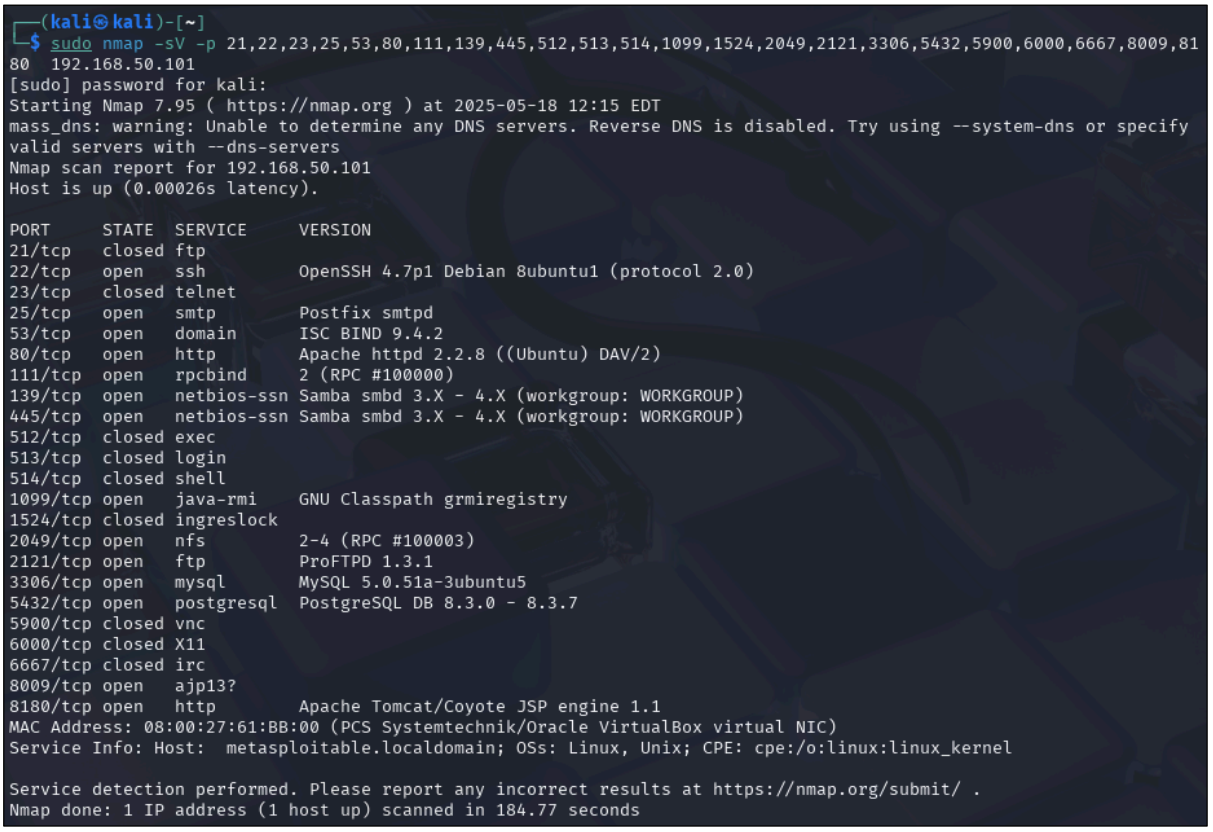
M3 - Progetto Finale - Scansione Finale

Il presente report documenta i risultati della scansione di sicurezza finale condotta sull'host 192.168.50.101 dopo l'implementazione delle azioni di remediation descritte nel report precedente. L'obiettivo di questa scansione è di valutare l'efficacia delle misure di mitigazione intraprese e di fornire un quadro aggiornato dello stato di sicurezza del sistema Metasploitable. I risultati di questa scansione saranno confrontati con quelli ottenuti durante la scansione iniziale per evidenziare i miglioramenti nella postura di sicurezza.

Riepilogo delle Porte Aperte e Chiuse

La scansione iniziale sull'host 192.168.50.101 aveva rilevato un totale di 23 porte TCP aperte. Dopo l'implementazione delle azioni di remediation mirate, la scansione finale del 18/05/2025 ha rilevato un cambiamento significativo nello stato delle porte.

Un totale di 11 porte precedentemente aperte risultano ora chiuse. Questo include le porte 21 (ftp), 512 (exec), 5900 (vnc) e 6667 (irc), che erano state oggetto specifico delle nostre attività di mitigazione. Di conseguenza, il numero di porte TCP aperte sull'host 192.168.50.101 nella scansione finale è diminuito a 12. Questo indica un miglioramento nella superficie di attacco del sistema, con un numero inferiore di servizi esposti sulla rete.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,81
80  192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 12:15 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).

PORT     STATE  SERVICE     VERSION
21/tcp   closed ftp
22/tcp   open   ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   closed telnet
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  closed exec
513/tcp  closed login
514/tcp  closed shell
1099/tcp open   java-rmi    GNU Classpath grmiregistry
1524/tcp closed ingreslock
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 closed vnc
6000/tcp closed X11
6667/tcp closed irc
8009/tcp open   ajp13?
8180/tcp open   http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:61:BB:00 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Linux, Unix; 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 184.77 seconds
```

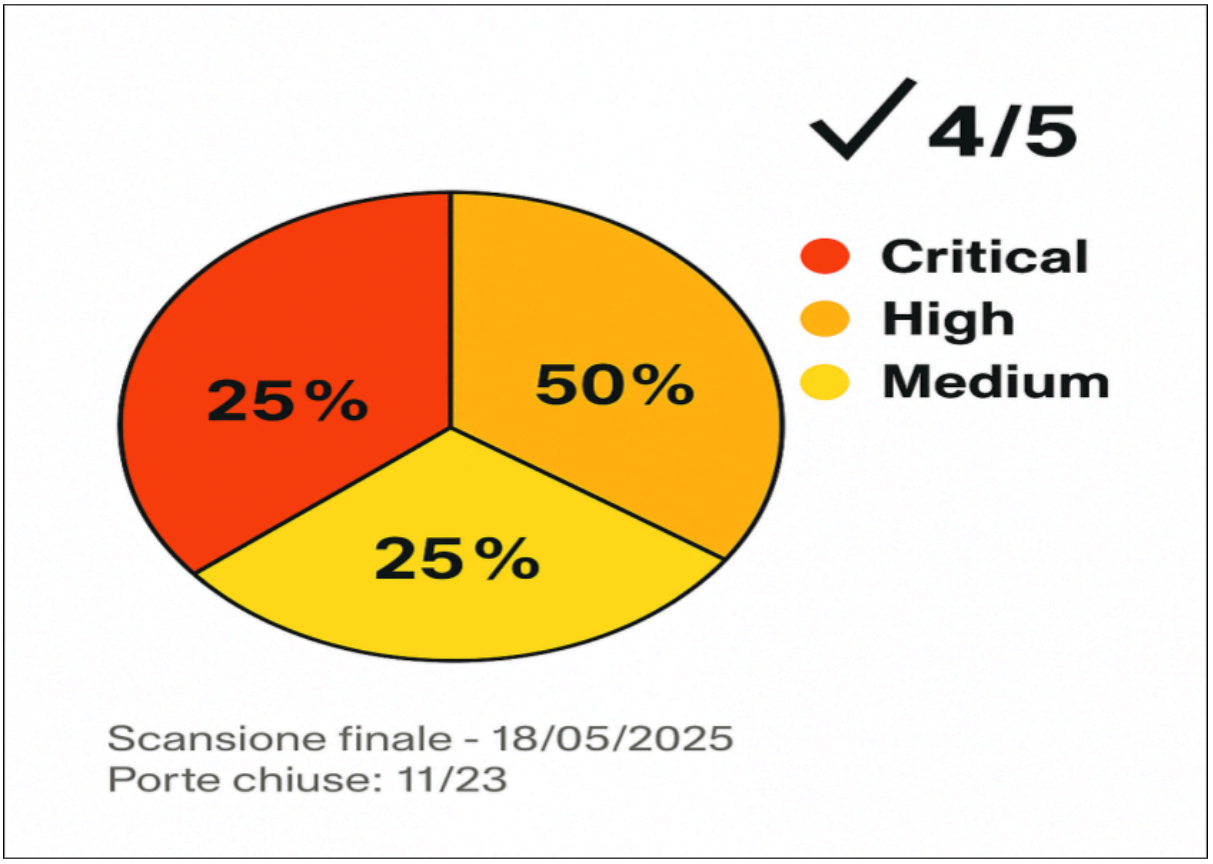
Confronto con la Scansione Iniziale

Confrontando i risultati della scansione finale con quelli della scansione iniziale, è evidente un miglioramento nella superficie di attacco del sistema. Il numero di porte TCP aperte è diminuito da 23 a 12, rappresentando una riduzione di 11 servizi potenzialmente vulnerabili esposti sulla rete.

In particolare, le porte associate alle vulnerabilità mirate durante la fase di remediation risultano ora chiuse o gestite diversamente:

- Porta 512/tcp (exec): Da open a closed;
- Porta 5900/tcp (vnc): Da open a closed.
- Porta 6667/tcp (irc): Da open a closed.
- Porta 2049/tcp (nfs): Sebbene la porta rimanga aperta, la configurazione del servizio NFS è stata modificata per limitare l'accesso, come descritto nel report di remediation.

Tuttavia, la scansione finale rivela che rimangono aperte diverse porte con servizi potenzialmente vulnerabili, come SSH (porta 22), Telnet (porta 23), SMTP (porta 25), DNS (porta 53), HTTP (porta 80), Samba (porte 139 e 445), Java RMI (porta 1099), la bind shell (porta 1524), FTP (porta 21 e 2121), MySQL (porta 3306) e PostgreSQL (porta 5432).



Conclusioni della Scansione Finale

La scansione finale del sistema Metasploitable (192.168.50.101) evidenzia un miglioramento nella postura di sicurezza rispetto alla scansione iniziale, con una riduzione significativa del numero di porte aperte (da 23 a 12) grazie alle azioni di remediation intraprese su rexecd, VNC, UnrealIRCd e la configurazione di NFS.

Tuttavia, l'analisi delle porte ancora aperte e il riepilogo delle vulnerabilità rimanenti per gravità indicano che il sistema rimane vulnerabile. La presenza di vulnerabilità critiche e alte, associate a servizi obsoleti e potenzialmente mal configurati come SSH, Telnet, DNS (BIND), HTTP (Apache), Samba, Java RMI, la bind shell e database (MySQL, PostgreSQL), rappresenta ancora un rischio considerevole per la sicurezza del sistema.

Sebbene la fase di remediation mirata abbia avuto successo nell'affrontare le specifiche vulnerabilità selezionate, è fondamentale riconoscere che Metasploitable è intrinsecamente progettato per essere vulnerabile e presenta molteplici altre debolezze.

Pertanto, si raccomanda di considerare questo sistema come un ambiente di test e apprendimento isolato e di non esporlo a reti di produzione senza ulteriori e approfondite misure di hardening e mitigazione.