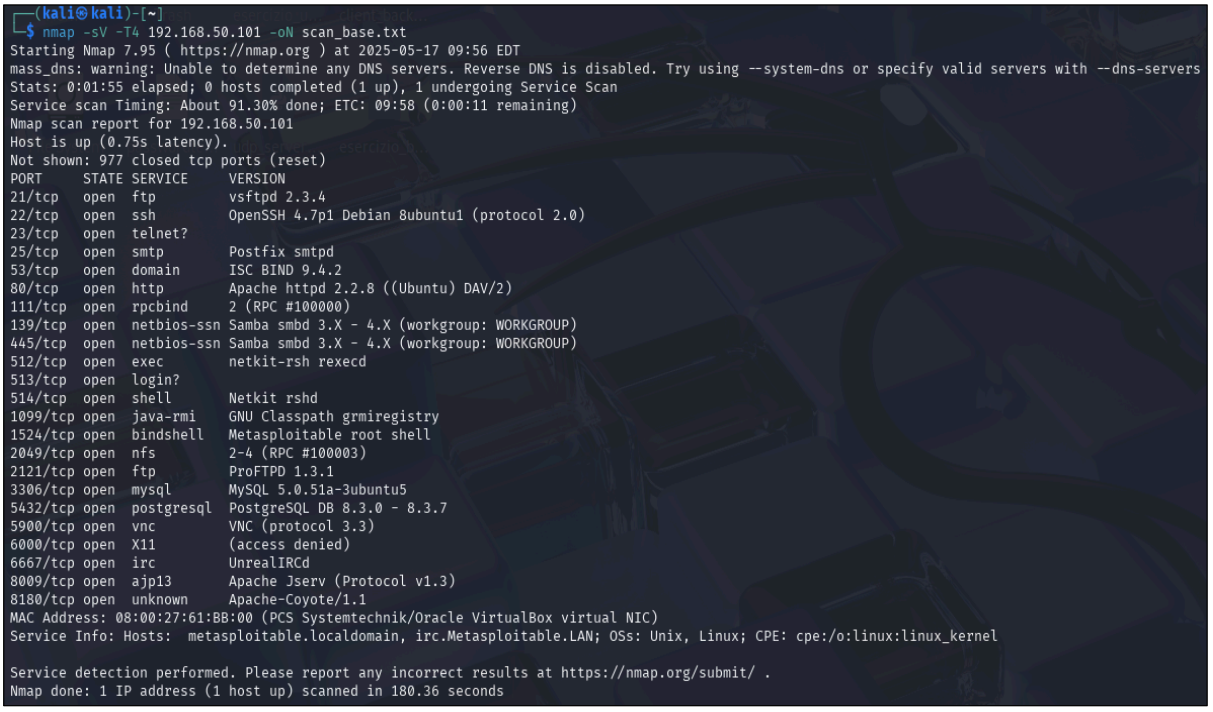
# M3 - Progetto Finale - Scansione Iniziale

## Premessa

La presente analisi di vulnerabilità è stata condotta utilizzando la suite di strumenti integrata in Kali Linux, nello specifico lo scanner di rete Nmap e i suoi script NSE (Nmap Scripting Engine). A causa di limitazioni hardware che impattavano significativamente sulle prestazioni del sistema in uso, non è stato possibile impiegare tool di vulnerability assessment più complessi come OpenVas o Nessus. Le vulnerabilità riscontrate e documentate nel presente report sono state analizzate con l'obiettivo di identificare potenziali debolezze nella sicurezza del sistema target Metasploitable.

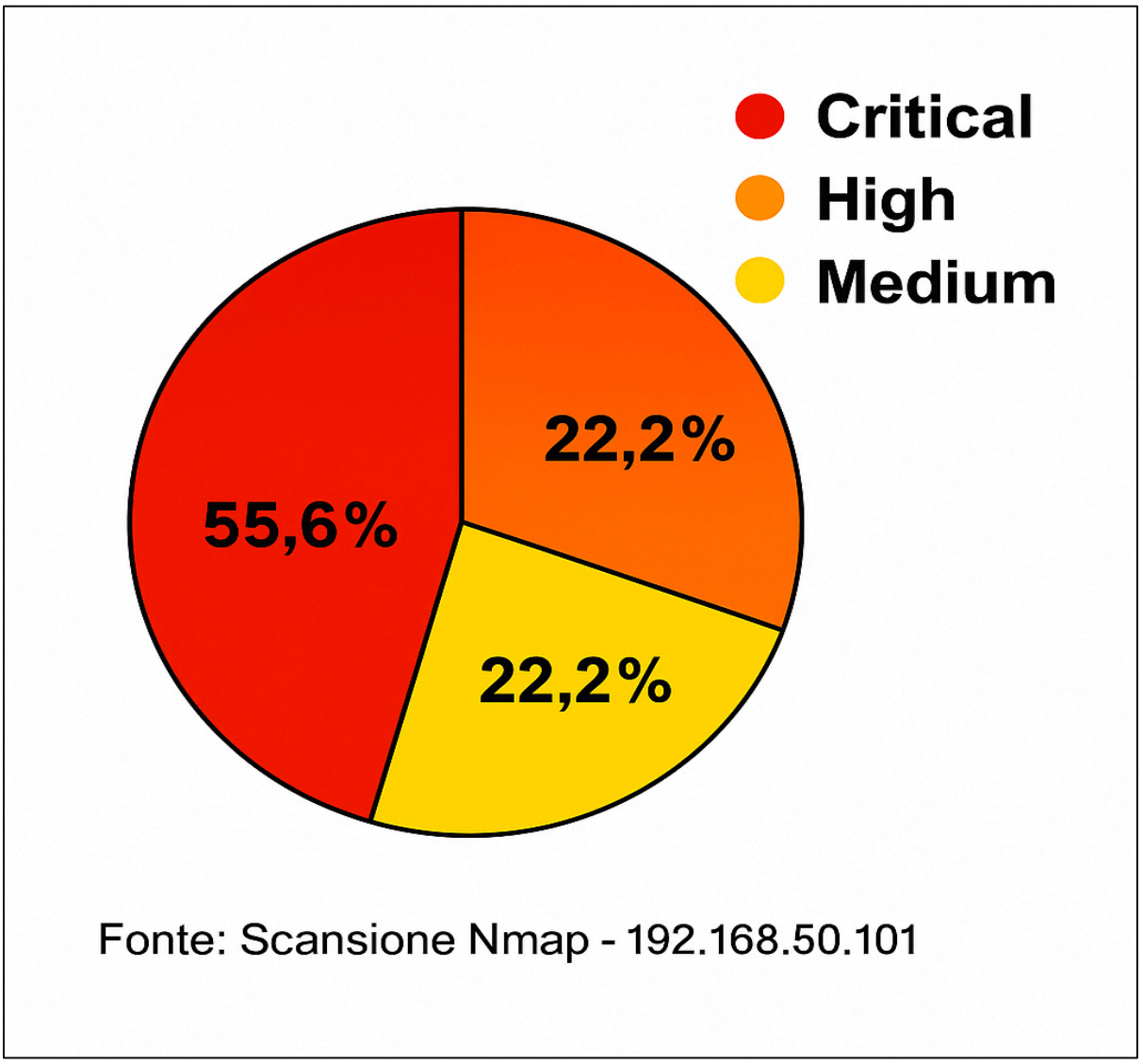
## Scansione

La scansione iniziale, eseguita tramite Nmap, ha permesso di identificare i servizi di rete attivi sull'host target 192.168.50.101. Un totale di 977 porte TCP risultano chiuse (state: reset), mentre diverse porte appaiono aperte, indicando servizi potenzialmente vulnerabili.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.50.101 -oN scan_base.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 09:56 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
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 09:58 (0:00:11 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.75s 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?
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  unknown     Apache-Coyote/1.1
MAC Address: 08:00:27:61:BB:00 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, 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 180.36 seconds
```




Il grafico a torta illustra la distribuzione delle vulnerabilità rilevate in base al loro livello di severità. La porzione più ampia (55.6%) è rappresentata dalle vulnerabilità classificate come Critiche, evidenziando una significativa presenza di debolezze che potrebbero consentire a un attaccante di compromettere gravemente il sistema. Le vulnerabilità di severità Alta e Media costituiscono ciascuna il 22.2% del totale, indicando ulteriori aree di rischio che necessitano di attenzione e mitigazione.

## Dettagli delle Vulnerabilità Rilevate

La seguente tabella riassume le porte TCP aperte rilevate durante la scansione sull'host target 192.168.50.101 e le vulnerabilità associate identificate.

| Porta | Protocollo | Stato | Servizio Rilevato | Vulnerabilità Potenziale |
|---|---|---|---|---|
| 21 | tcp | open | ftp | Backdoor nota in vsftpd 2.3.4 |
| 22 | tcp | open | ssh | Versione obsoleta |
| 23 | tcp | open | telnet | Autenticazione in chiaro, possibile brute-force |
| 25 | tcp | open | smtp | Configurazioni errate possono permettere spam |
| 53 | tcp | open | dns | Vulnerabilità come cache poisoning o DoS |
| 80 | tcp | open | http | Versioni vecchie con vulnerabilità |
| 111 | tcp | open | rcp | Possibile enumerazione dei servizi RCP o exploit |
| 139 | tcp | open | samba | Vulnerabilità come Samba Cry o brute-force |
| 445 | tcp | open | smb | Possibile sfruttamento di protocolli SMB vulnerabili |
| 512-514 | tcp | open | remote shell | Autenticazione debole, trasmissione dati in chiaro |
| 1099 | tcp | open | java rmi | Vulnerabile a deserializzazione malevola |

| | | | | |
|---|---|---|---|---|
| 1524 | tcp | open | meta root shell | Backdoor con accesso root senza autenticazione |
| 2049 | tcp | open | nfs | Accesso non autorizzato a share se malconfigurato |
| 2121 | tcp | open | ftp | Vulnerabile a exploit |
| 3306 | tcp | open | mysql | Versioni obsolete |
| 5432 | tcp | open | postgresql | Vulnerabilità come CVE-2007-3280 o brute-force |
| 5900 | tcp | open | vnc | Autenticazione debole o sessioni esposte |
| 6000 | tcp | open | x11 | Accesso non autorizzato a sessioni grafiche |
| 6667 | tcp | open | irc | Backdoor o exploit per comandi remoti |
| 8009 | tcp | open | ajp | Vulnerabile a Ghostcat per lettura file arbitrari |
| 8180 | tcp | open | http | Possibili exploit per Tomcat |

## Conclusioni

Il sistema analizzato presenta numerose vulnerabilità critiche, molte delle quali legate a servizi obsoleti, configurazioni non sicure e backdoor note. Questi problemi espongono la macchina a rischi significativi, tra cui:

1. Accesso non autorizzato
    - Diverse porte (21/tcp FTP, 1524/tcp bindshell) consentono l'accesso remoto senza autenticazione robusta o addirittura con backdoor preinstallate;
    - Servizi come Telnet (23/tcp) e rexecd (512/tcp) trasmettono dati in chiaro, facilitando attacchi di intercettazione (sniffing) e brute-force.

2. Esecuzione di codice remoto ed escalation dei privilegi
    - Versioni vulnerabili di vsftpd, Proftpd e Samba possono essere sfruttate per ottenere l'accesso root;
    - Servizi RPC e Java RMI (1099/tcp) sono esposti a deserializzazione malevola, permettendo l'esecuzione di comandi arbitrari.

3. Esposizione di dati sensibili
    - NFS (2049/tcp) e SMB (445/tcp) potrebbero consentire l'accesso non autorizzato a file condivisi;
    - Database come MySQL (3306/tcp) e PostgreSQL (5432/tcp) sono spesso obiettivi di attacchi SQL injection o credential sniffing.

4. Servizi non necessari
    - Molti servizi (IRC, X11, VNC) non sono essenziali per l'operatività del sistema, ma aumentano il rischio di exploit.

Le vulnerabilità rilevate sono altamente sfruttabili in contesti reali, specialmente se il sistema è esposto a internet. Senza interventi immediati, il rischio di compromissione è elevatissimo.