Security Testing Report

Pace Massimiliano - efmpas@gmail.com

W11 D1

Sommario:

Scansione :

OS

Fingerprint
SynScan
Tcp connect
Version detection

Descrizione lavoro svolto

Eseguito un set di scansioni Nmap per identificare sistema operativo, porte aperte e versioni dei servizi su Metasploitable. Sono state identificate diverse porte e servizi vulnerabili (FTP, SSH, HTTP, MySQL, ecc.). Di seguito i dettagli tecnici e le raccomandazioni operative per la mitigazione.

Target

Virtual Machine Metasploitable ip 192.168.50.101

Metodologia e comandi utilizzati

OS fingerprint	sudo nmap -O 192.168.50.101
SYN Scan (stealth)	sudo nmap -sS -p- 192.168.50.101
TCP connect scan	sudo nmap -sT -p 1-65535 192.168.50.101
Version detection	sudo nmap -sV -p 21,22,80,3306 192.168.50.101

* in TCP connect abbiamo selezionato un range di porte da 1 a 65535
* in Version detection sono state scelte la porta 21,22,80,3306

Risultati ottenuti

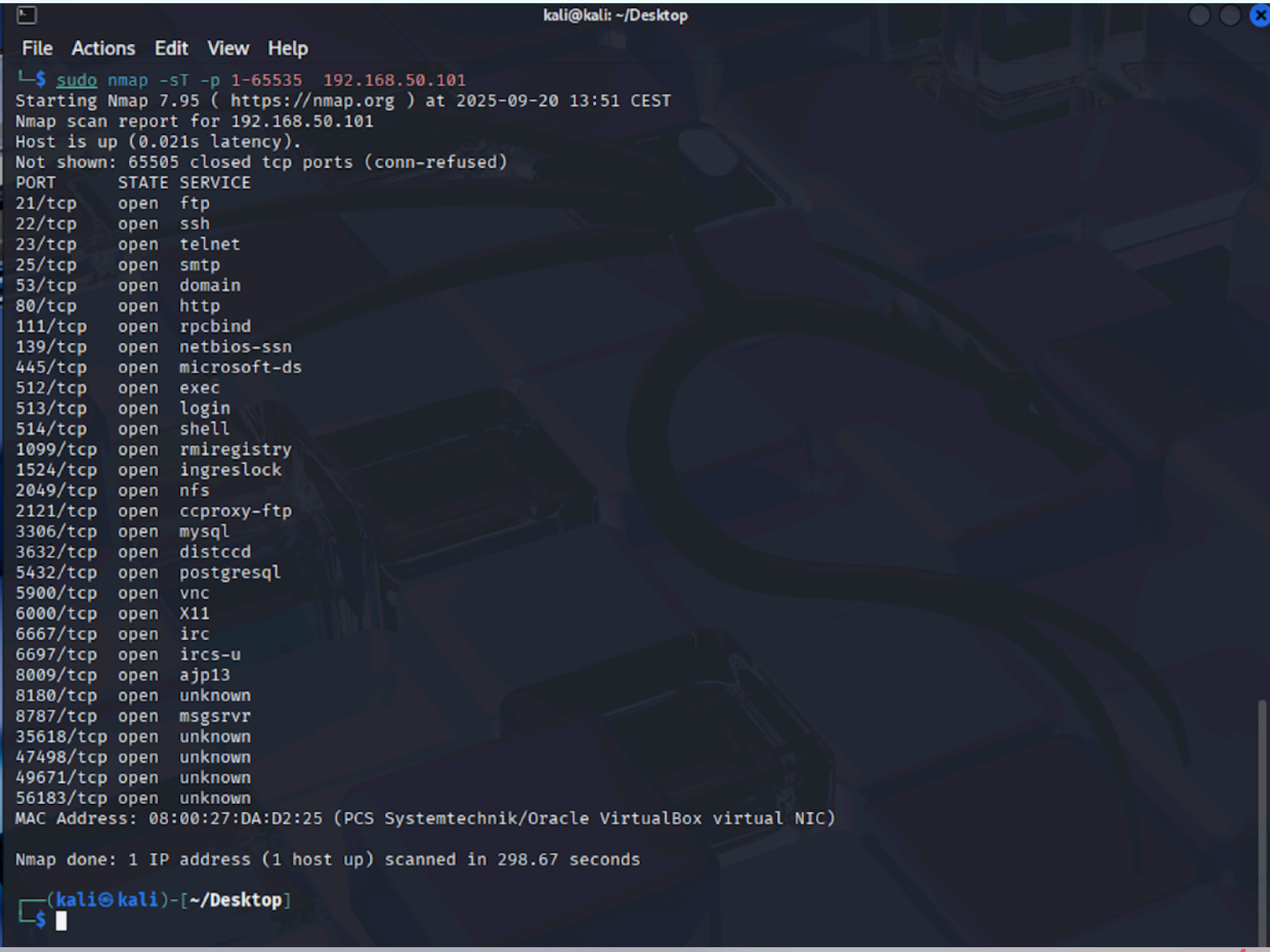
(`sudo nmap -O 192.168.50.101`)

- Comando: scansione standard con rilevamento OS (`-O`).
- Risultati:
  - Tante porte aperte: 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 80 (http), 139 (netbios-ssn), 445 (microsoft-ds), 3306 (mysql), ecc.
  - OS rilevato: **Linux 2.6.x**.
- Tempo di scansione: ~17 secondi.

Risultati ottenuti

(sudo nmap -sT –p 1-65535 192.168.50.101)

- Comando: scansione di **tutte le 65535 porte TCP**.
- Risultati:
  - Conferma le stesse porte aperte già viste prima.
  - Mostra che le altre sono “conn-refused”.
- Tempo di scansione: ~298 secondi (più lungo perché ha controllato ogni porta).

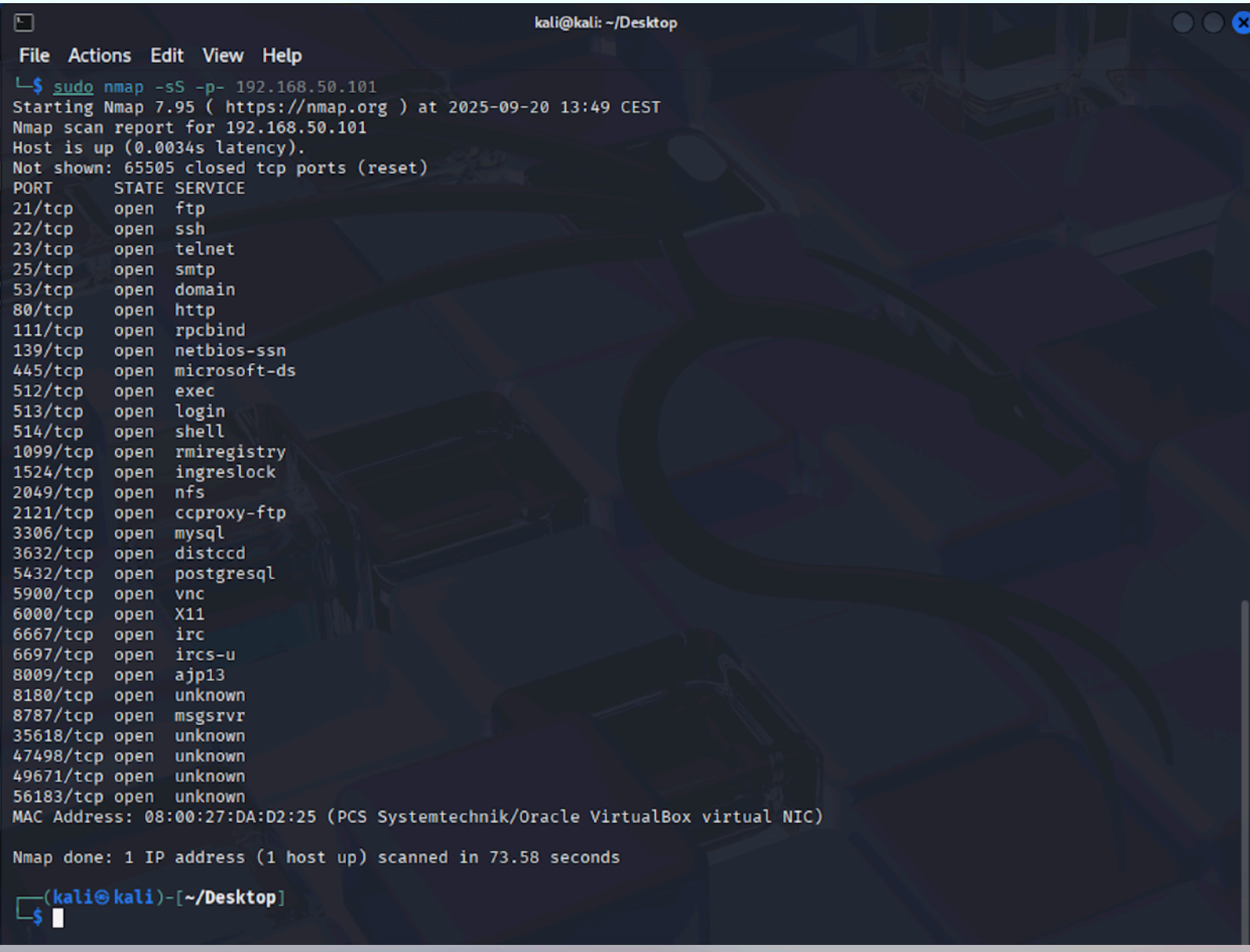


Risultati ottenuti

`sudo nmap -sS -p- 192.168.50.101` (SYN scan / half-open scan su tutte le porte o su un range).

Effetto/interpretazione corretta:

- È una scansione **stealth** (SYN) che invia SYN e valuta le risposte (SYN/ACK = open, RST = closed).
- Fornisce un elenco di porte **aperte** più velocemente e con meno possibilità di completare connessioni TCP complete rispetto a `-sT`.
- Può comunque essere registrata da IDS/Firewall (non è invisibile), ma tende a risultare meno rumorosa sui log delle applicazioni rispetto a scansioni full connect.
- Tempo di scansione (nello screenshot) ~73s — compatibile con scansione SYN su molte porte.

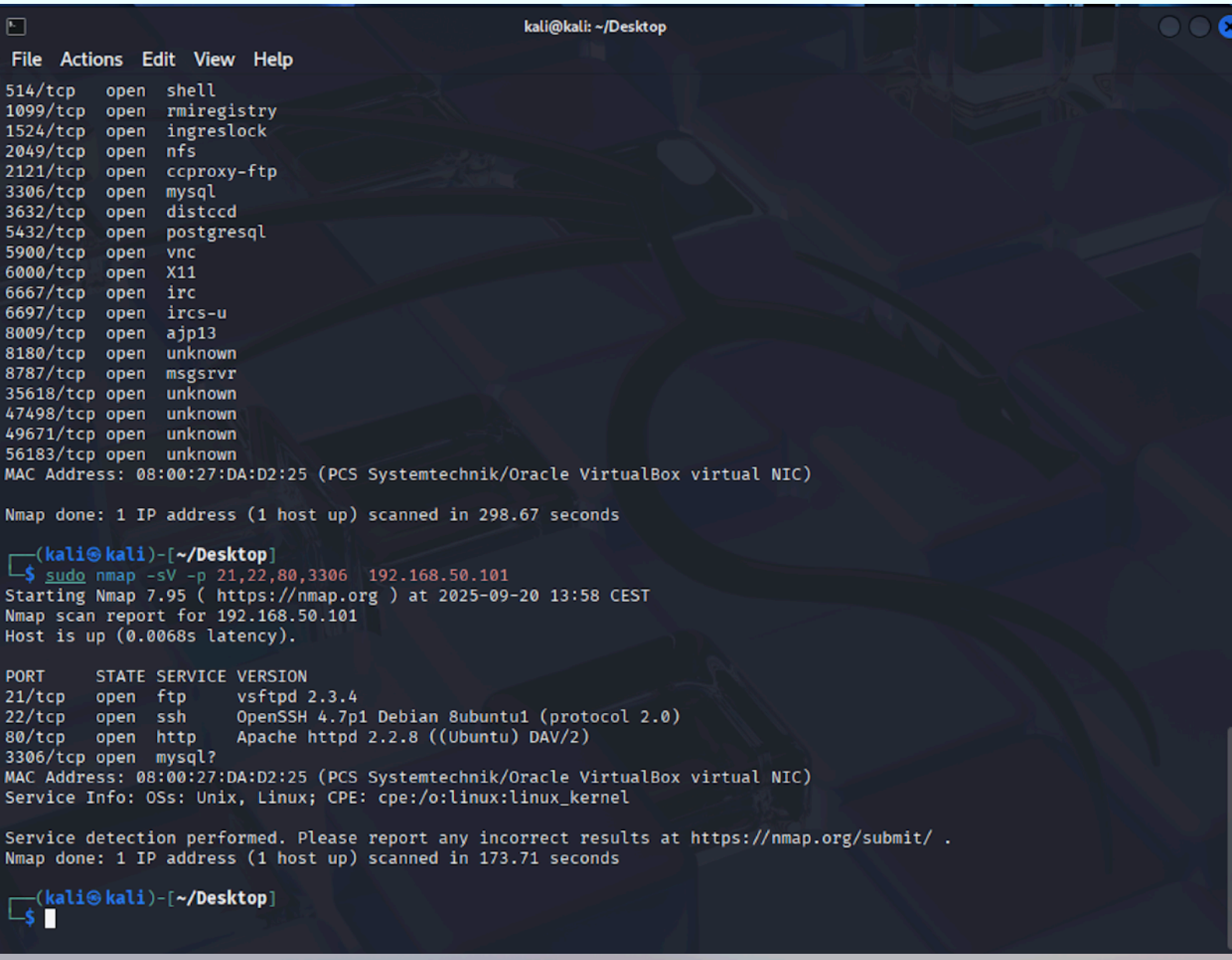


Risultati ottenuti

`sudo nmap -sV -p 21,22,80,3306 192.168.50.101`
(scansione mirata con detection delle versioni del servizio, `-sV`, sulle porte specificate).

output mostra banner/versioni dettagliate (`vsftpd 2.3.4`, `OpenSSH 4.7p1`, `Apache 2.2.8`, `MySQL 5.0.51a`) — tipico risultato di `-sV`.

- È una scansione **di versione** che interroga le porte selezionate per ottenere banner e fingerprinting di servizi.
- Non è una semplice scansione di porte: fornisce informazioni utili per ricerca di CVE/PoC.
- Tempo di scansione più breve rispetto a `-p-` ma più informativo su quelle porte.



Report di scansione Nmap — 192.168.50.101

Autore: Pace Massimiliano
Data scansione: 2025-09-20
Host target: 192.168.50.101
MAC: 08:00:27:DA:D2:25 (Oracle VirtualBox virtual NIC)
OS stimato: Linux 2.6.x (risultato Nmap `-O`)
Note ambiente: Kali Linux in VirtualBox (scanner). L'host target e' una macchina vulnerabile/di laboratorio

Sintesi

È stata eseguita una serie di scansioni Nmap (scansione OS, ping/host discovery, scansione porte singole e scansione 1–65535). L'host risponde ed espone numerosi servizi TCP (sia su porte conosciute sia su alte porte non identificate). Alcuni servizi espongono versioni datate note per vulnerabilità. Il livello di rischio complessivo è **Alto** se l'host è raggiungibile da rete non fidata, dato il numero e la natura dei servizi attivi (Telnet, FTP vulnerabile, MySQL vecchio, Apache datato, servizi RPC/SMB).

Evidenze chiave

- Banner e versioni ottenute: vsftpd 2.3.4, OpenSSH 4.7p1, Apache 2.2.8, MySQL 5.0.51a. Versioni vecchie con CVE noti.
- OS fingerprint: Linux 2.6.x (compatibile con host vulnerabile).
- MAC address VirtualBox: indica ambiente virtuale.
- Scansione a tutta porta (~1–65535) conferma numerose porte aperte e molte risposte "conn-refused" o "reset" per porte chiuse.
- Scansione mirata di porte specifiche ha prodotto informazioni di versione utili per enumerazione vulnerabilità.

Porte e servizi identificati

- 21/tcp — ftp — **vsftpd 2.3.4**
- 22/tcp — ssh — **OpenSSH 4.7p1 Debian**
- 23/tcp — telnet
- 25/tcp — smtp
- 53/tcp — domain (DNS)
- 80/tcp — http — **Apache httpd 2.2.8** (Ubuntu/DAV/2)
- 111/tcp — rpcbind
- 139/tcp — netbios-ssn
- 445/tcp — microsoft-ds (SMB)
- 512/tcp — exec
- 513/tcp — login
- 514/tcp — shell
- 1099/tcp — rmiregistry
- 1524/tcp — ingreslock (porta associata a backdoor in Metasploitable)
- 2049/tcp — nfs
- 2121/tcp — ccproxy-ftp
- 3306/tcp — mysql — **MySQL** (version mostrata in uno screenshot: 5.0.51a)
- 3632/tcp — distccd
- 5432/tcp — postgresql
- 5900/tcp — vnc
- 6000/tcp — X11
- 6667/tcp — irc
- 8009/tcp — ajp13
- 8180/tcp — (unknown / web app)
- 8787/tcp — msgsrv r
- Porte alte: 35618, 47498, 49671, 56183 (unknown/open)

Valutazione rischio / Priorità

Attribuisco priorità **alta** a questi elementi:

1. **Telnet (23/tcp)** — traffico in chiaro: rischio compromissione credenziali.
2. **FTP (vsftpd 2.3.4)** — versione vulnerabile (nota per exploit in passato, es. backdoor).
3. **Apache 2.2.8** — versione datata, potenziali vulnerabilità di directory traversal, RCE tramite moduli datati.
4. **MySQL 5.0.x** — versioni vecchie con potenziali escalation/SQL injection facilità.
5. **SMB (139/445)** — esposizione di servizi di file sharing: possibile divulgazione di info sensibili.
6. **RPC/exec/login/shell (512–514)** — servizi obsoleti per login remoto, pericolosi.
7. **Altri servizi (NFS, distccd, vnc, ajp, msgsrvr)** — aumentano superficie d'attacco e possibilità di exploit.

Raccomandazioni immediate

Azioni immediate

- Isolare la macchina dalla rete (mettere in subnet di laboratorio o disconnettere).
- Disabilitare servizi non necessari: Telnet, FTP, rsh/executables remoti (512/513/514), rmiregistry, ccproxy, distccd, vnc se non richiesto.
- Configurare firewall (host-based + network) per limitare accesso alle porte critiche (solo IP amministrativi).
- Cambiare tutte le password/credenziali locali se credenziali deboli possibili.
- Abilitare logging e monitoraggio (fail2ban/IDS).