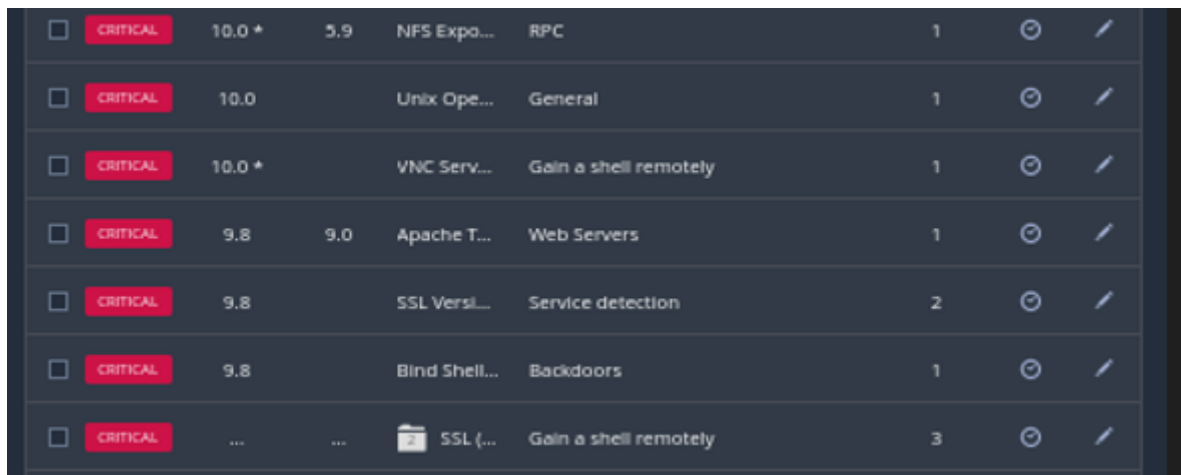


Progetto S5/L5

Per questo nuovo esame pratico ho effettuato una scansione iniziale per identificare le vulnerabilità presenti sulla macchina Metasploitable. Questo processo è fondamentale per valutare la sicurezza del sistema e identificare eventuali punti deboli che potrebbero essere sfruttati da un'attaccante.



<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Expo...	RPC	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Ope...	General	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Serv...	Gain a shell remotely	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache T...	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Versi...	Service detection	2	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell...	Backdoors	1	🔄	✎
<input type="checkbox"/>	CRITICAL	2 SSL (...)	Gain a shell remotely	3	🔄	✎

Con la prima scansione ho rilevato diverse vulnerabilità e mi sono concentrato sulle 7 più critiche.

Per procedere con la risoluzione ho avviato un processo di ricerca, consultando vari siti dove hanno spiegato nel dettaglio la criticità in questione ed i passaggi per estinguerla.

1) La prima criticità su cui ho lavorato è la NFS exported share information discisure

Dove tramite comando `sudo nano /etc/hosts.deny` sono andato a configurare il file così da limitare l'accesso "ALL: ALL"

2) La seconda criticità risolta è la Apache Tomcat AJP (Ghostcat) qui vi era una debolezza nel connettore ajp e si è quindi dovuti andare a lavorare sulla configurazione del file `server.xml` così da poterlo disabilitare e rimuovere la vulnerabilità

3) La terza ed ultima criticità risolta è la Bind shell backdoor detection, dove tramite scan è stata rivelata una backdoor sulla porta 1524 ed era quindi possibile connettersi alla macchina Metasploitable con il comando `nc`. Con il comando `kill -9` sono andato "killare" il processo in ascolto sulla porta 1524 e con il comando `sudo nano /etc/inetd.conf` ho eliminato la stringa "Shell stream".

Successivamente con iptables ho creato una regola che va a bloccare il traffico verso quella porta `iptables -A INPUT -p TCP --dport 1524 -j DROP`.

Dopo aver apportato le modifiche descritte ho effettuato una seconda scansione per verificare che le criticità rilevate in precedenza fosse state risolte con successo.

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		⚙
<input type="checkbox"/> CRITICAL	10.0 *	5.1	Debi...	Gain a shell remotely	2	🕒	✎
<input type="checkbox"/> CRITICAL	10.0		Unix ...	General	1	🕒	✎
<input type="checkbox"/> CRITICAL	10.0 *		VNC ...	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/> CRITICAL	9.8		SSL V...	Service detection	2	🕒	✎
<input type="checkbox"/> HIGH	7.5	5.9	Sam...	General	1	🕒	✎
<input type="checkbox"/> MIXED	16	SSL (General	29	🕒	✎
<input type="checkbox"/> MIXED			16	SSL (General	29	🕒	✎

Come mostra lo screen dopo il lavoro svolto è possibile constatare che le criticità rimaste sono 4, purtroppo non è stato per me possibile estinguerle del tutto.

In conclusione è fondamentale risolvere le criticità rilevate da uno scanner di vulnerabilità per garantire la sicurezza e l'integrità del sistema. Questo processo permette di identificare e mitigare potenziali punti deboli che potrebbero essere sfruttati da attaccanti per compromettere o danneggiare il sistema, accedere a dati sensibili o interrompere i servizi. Risolvere le vulnerabilità riduce significativamente il rischio di incidenti di sicurezza, protegge la reputazione dell'organizzazione e assicura la continuità operativa. Inoltre, aiuta a mantenere conformità con le normative di sicurezza e a promuovere una cultura di sicurezza informatica proattiva all'interno dell'organizzazione.