S5/L5
Progetto settimanale

Ci è stato chiesto di Effettuare una scansione completa sul target Metasploitable.

Scegliere da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

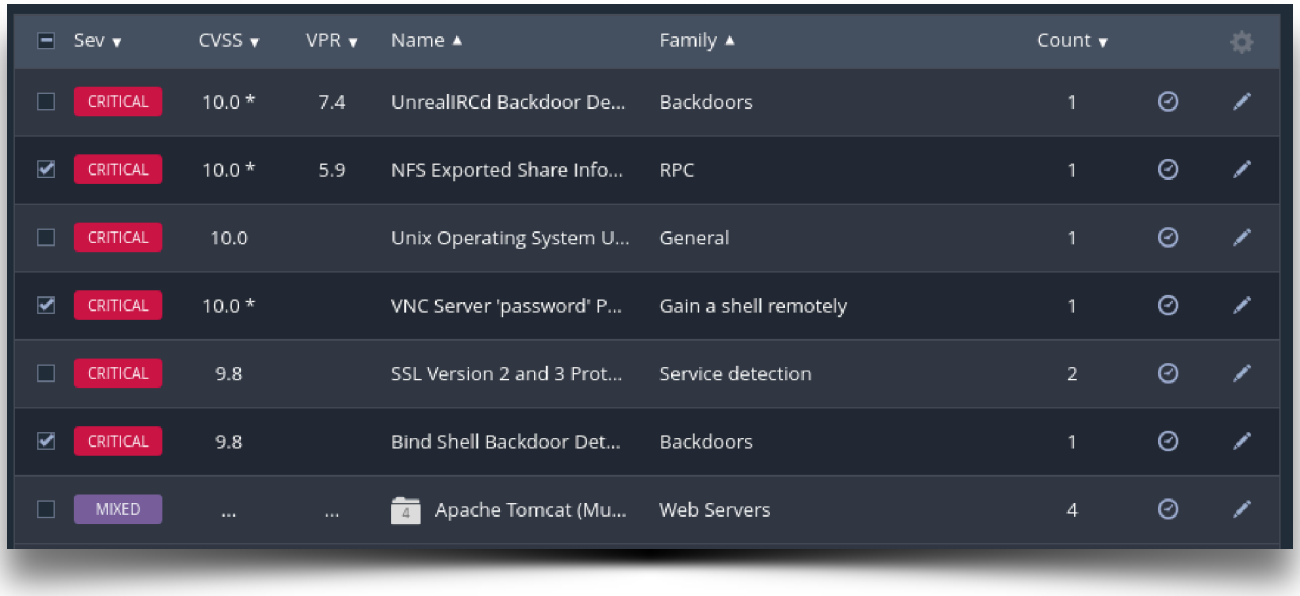
N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Da una prima scansione possiamo notare le diverse vulnerabilità rilevate

Dai risultati ottenuti sono state scelte 3 vulnerabilità

- NFS Exported Share Information Disclosure
- VNC Server 'password' Password
- Bind Shell Backdoor Detection



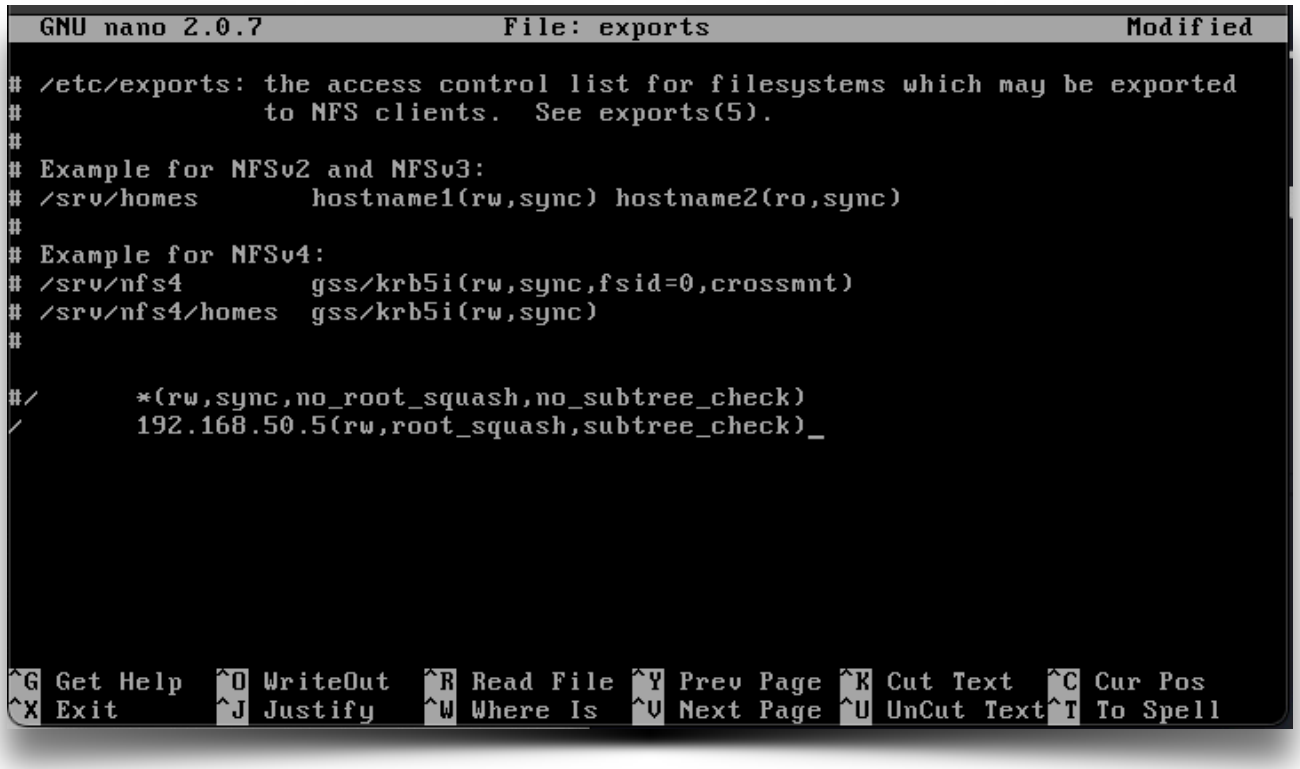
Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor De...	Backdoors	1
CRITICAL	10.0 *	5.9	NFS Exported Share Info...	RPC	1
CRITICAL	10.0		Unix Operating System U...	General	1
CRITICAL	10.0 *		VNC Server 'password' P...	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Prot...	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Det...	Backdoors	1
MIXED	...	...	4 Apache Tomcat (Mu...	Web Servers	4

1. NFS Exported Share Information Disclosure

“NFS Exported Share Information Disclosure” si riferisce a una potenziale vulnerabilità di sicurezza associata all’esposizione non autorizzata di informazioni sensibili attraverso l’implementazione di NFS (Network File System) in una configurazione non sicura.
Quando si parla di “NFS exported share information disclosure”, potrebbe indicare che le condivisioni NFS sono configurate in modo improprio, consentendo a un potenziale aggressore di ottenere informazioni sensibili sulle condivisioni NFS esistenti, permettendogli la manipolazione delle stesse.
Per mitigare questa potenziale minaccia, è importante configurare correttamente le condivisioni NFS, limitare l’accesso solo a utenti autorizzati e applicare corrette pratiche di sicurezza per proteggere le informazioni sensibili.

Il servizio era originariamente configurato per accettare tutte le connessioni da tutte le macchine assegnando i permessi di root con condivisione completa di tutto l’hard disk.

Entrando nel file export con il comando **sudo nano /etc/exports** abbiamo autorizzato solo un indirizzo IP (in questo caso l’indirizzo IP di pfSense).



Successivamente abbiamo utilizzato il comando **sudo exportfs -ra** per restartare il NFS,

2. VNC Server 'password' Password

Un VNC (Virtual Network Computing) è un software utilizzato per controllare un pc/ server da remoto.

Con la scansione effettuata con Nessus è stato appurato che il server VNC è protetto con una password debole, identificando la password come “Password”. Un utente malintenzionato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema in modo non autorizzato.

Usando il comando **sudo vncpasswd** sulla macchina metasploitable, è stata cambiata la password di default.

3. Bind Shell Backdoor Detection

La rilevazione di una “Bind Shell Backdoor” si riferisce all’identificazione di un punto di accesso non autorizzato (backdoor) creato attraverso l’installazione di un servizio “bind shell”. Un “bind shell” consente a un potenziale aggressore di collegarsi al sistema compromesso tramite una connessione di rete, offrendo così l’accesso al terminale del sistema.

La vulnerabilità rilevata sulla porta 1524 è stata risolta con una regola Firewall configurandolo in modo appropriato.

È stato usato il comando **sudo iptables -L --line-numbers** per visualizzare le regole firewall

Successivamente e stato usato il comando **sudo iptables -A INPUT -p tcp --dport 1524 -j DROP** per impostare la regola, e in fine in comando **sudo iptables -nL | grep 1524** per vedere la sola regola impostata

```
root@metasploitable:~/.vnc# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  anywhere             anywhere            tcp dpt:ingres
lock

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@metasploitable:~/.vnc# iptables -nL | grep 1524
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:1524
root@metasploitable:~/.vnc# _
```

Per verificare che le vulnerabilità siano state risolte in modo corretto abbiamo effettuato un'ulteriore scansione con Nessus.
Come possiamo non sono più presenti.