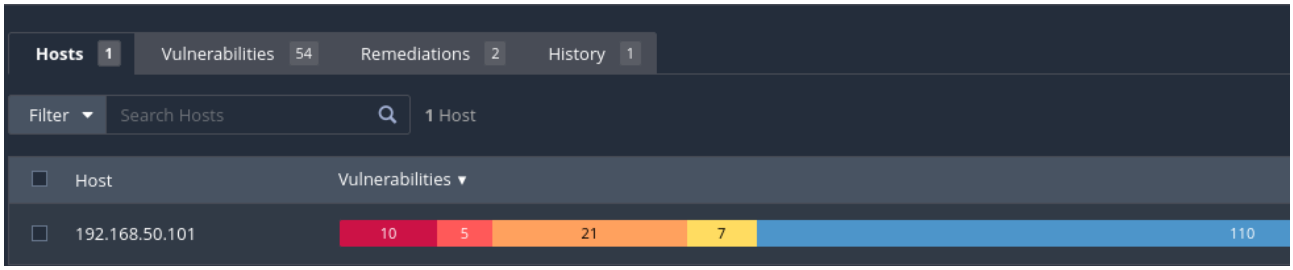
VULNERABILITY ASSSESSMENT

In questo vulnerability assessment sono andato ad analizzare le vulnerabilità presenti nella rete di Metasploitable e a correggere le problematiche più critiche riscontrate.

Lo strumento utilizzato per l'assessment è stato il programma Nessus, un vulnerability scanner molto potente e diffuso che raccoglie informazioni dalla macchina target per poi compararle all'interno di un database con le impronte più aggiornate possibili delle vulnerabilità diffuse per ogni servizio presente nella macchina.

Trattandosi della scansione di un singolo indirizzo IP, il processo non ha richiesto molto tempo ma ha riscontrato comunque una serie di criticità, alcune itenute piuttosto gravi, altre di entità media o lieve.



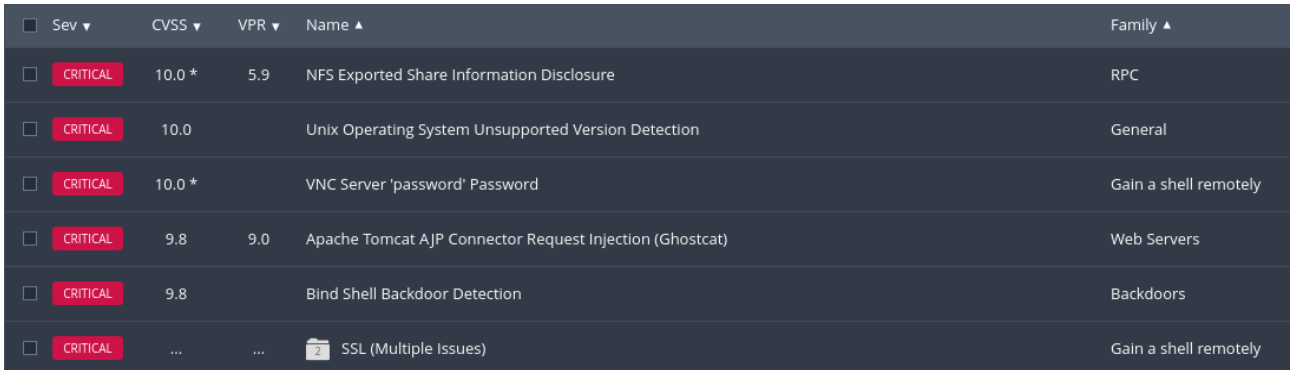
Mi sono focalizzato sulle vulnerabilità critiche, rappresentate in rosso da Nessus, che essendo più gravi sono anche le prime su cui bisognerebbe intervenire con le remediations.

Per prima cosa allego il report di Nessus al collegamento ipertestuale sotto.

https://github.com/MarcoBortolotti987/S5-L5-Vulnerability-Assessment

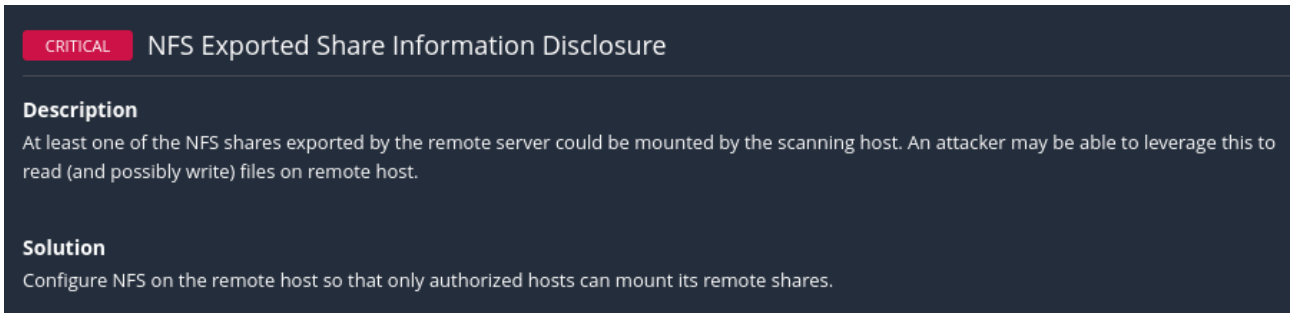
Il report evidenzia non solo su quale servizio è stata individuata la criticità, ma anche il livello di rischio che pone (tramite due operatori di score) e il plugin usato.
Si tratta di un repot completo nel senso che ripota tutte le vulnerabilità, tuttavia è un report basico, non dettagliato; Nessus offre quattro tipi di report, via via più dettagliati.

Vado ora a vedere quali sono le principali criticità riscontrate.

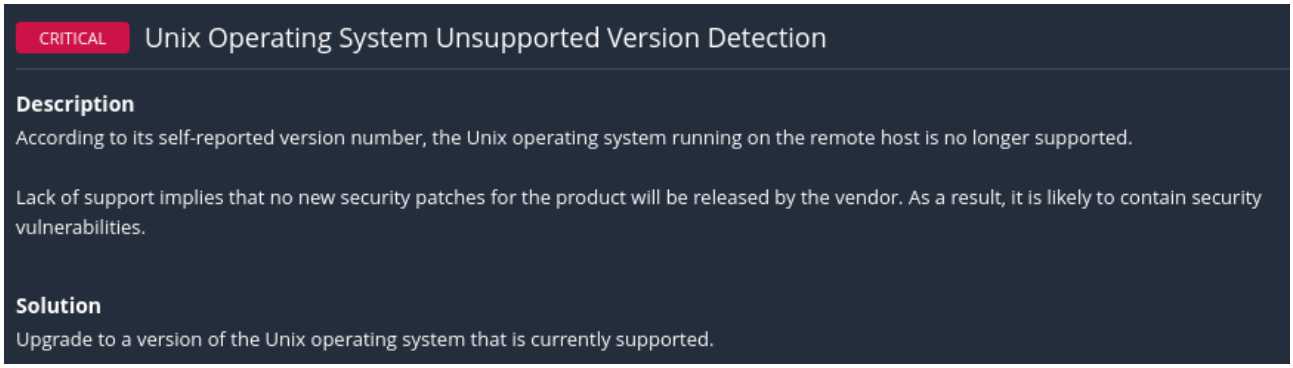


Nessus riporta sei vulnerabilità critiche, di cui cinque con punteggi molto alti, di 10 o 9,8.
Se clicchiamo su ogni criticità possiamo accedere ai maggiori dettagli su ciascuna, in particolare una descrizione della vulnerabilità e una possibile soluzione della stessa.

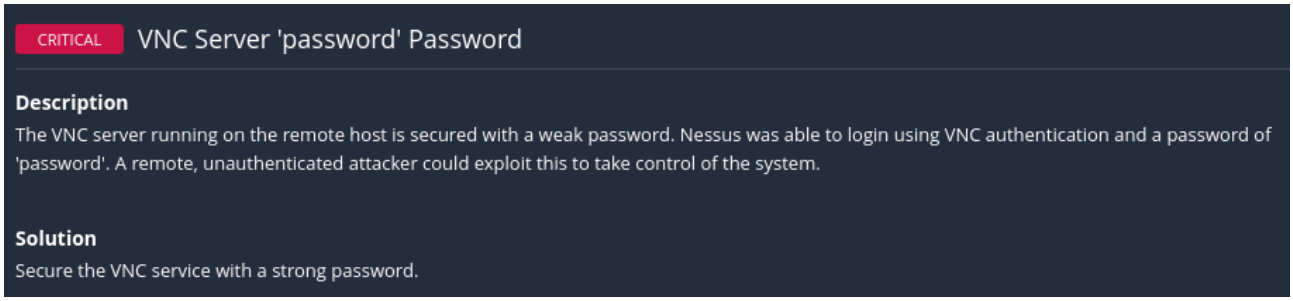
La prima vulnerabilità riscontrata riguarda l'NFS Share, un protocollo che gestisce lo stoccaggio e il recupero di dati da pate di dispositivi di storage su rete (in pratica un fyle system di rete).
Almeno uno degli NFS può essere attaccato e i file in esso contenuti letti o persino riscritti.
La soluzione che viene proposta è di mettere al sicuro gli NFS configurando una regola che permetta solo a determinati host di accedervi (potrebbe essere fatto tramite una regola di firewall).



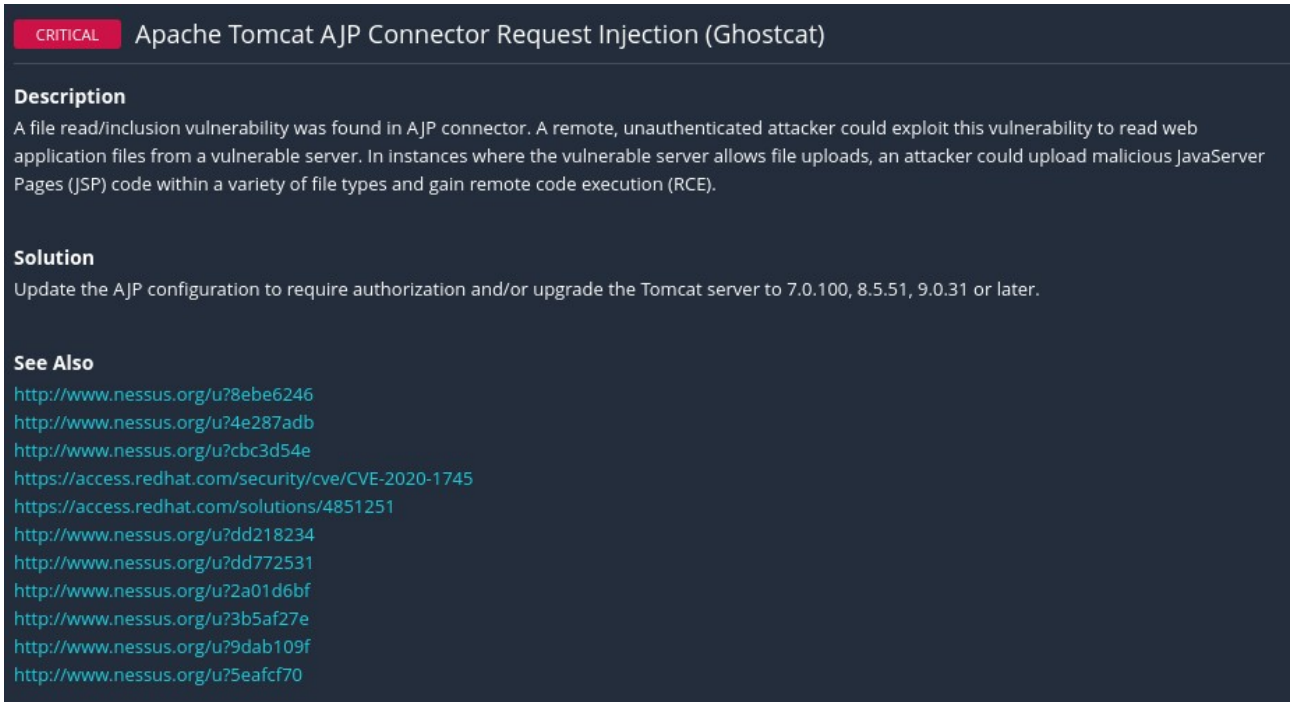
La seconda vulnerabilità riguarda l'intero sistema operativo, che è obsoleto e andrebbe quindi completamente aggiornato ad una nuova versione. Non potendo farlo su Metasploitable, lascio aperta questa vulnerabilità (in una situazione reale bisognerebbe aggiornare il sistema operativo al più presto).



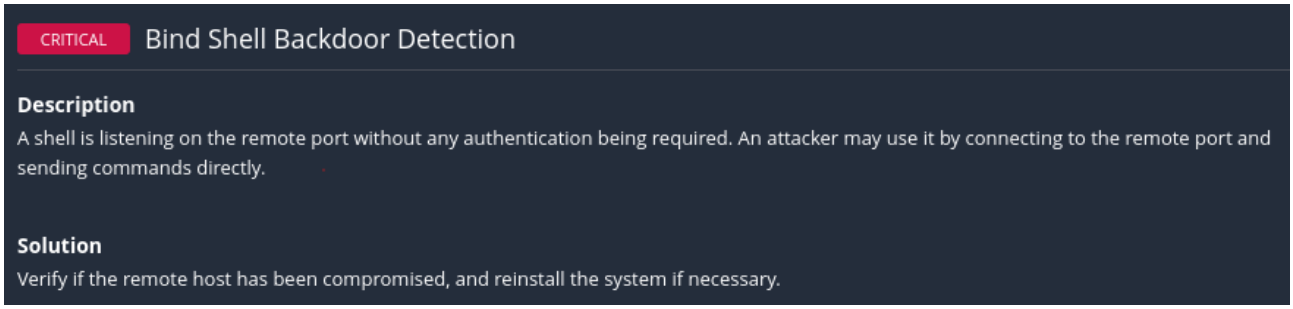
La terza vulnerabilità si riscontra comunemente e riguarda la debolezza di una password usata a protezione di un server VNC, rendendolo un facile target per un eventuale malintenzionato.
La soluzione migliore è cambiare sostituire la password esistente con una più forte (normalmente vengono suggeriti almeno 8 caratteri, che siano un misto di lettere minuscole, maiuscole, numeri e caratteri speciali).



La quarta vulnerabilità riguarda il server Apache e il suo protocollo AJP, in cui un attaccante potrebbe inserirsi e leggere file contenuti nel server o persino caricare un file malevolo. La soluzione proposta da Nessus è aggiornare il server oppure la configurazione di AJP in modo che richieda un'autorizzazione.



L'ultima vulnerabilità riguarda una bind shell backdoor, cioè una porta d'ascolto in input non autorizzata.



REMEDIATION

Per prima cosa ho cambiato la password d'accesso al server VNC con una più sicura.
Per farlo ho fatto l'accesso come root da Metasploitable e ho usato il comando «vncpasswd» per settare la nuova password, quindi i comandi «vncserver -kill» e «vncserver» per per forzare la chiusura del server stesso e poi riavviarlo.
A questo punto ho controllato da Kali che le nuove credenziali funzionassero, tramite il comando «vncviewer».

```
root@metasploitable:/etc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/etc#
```

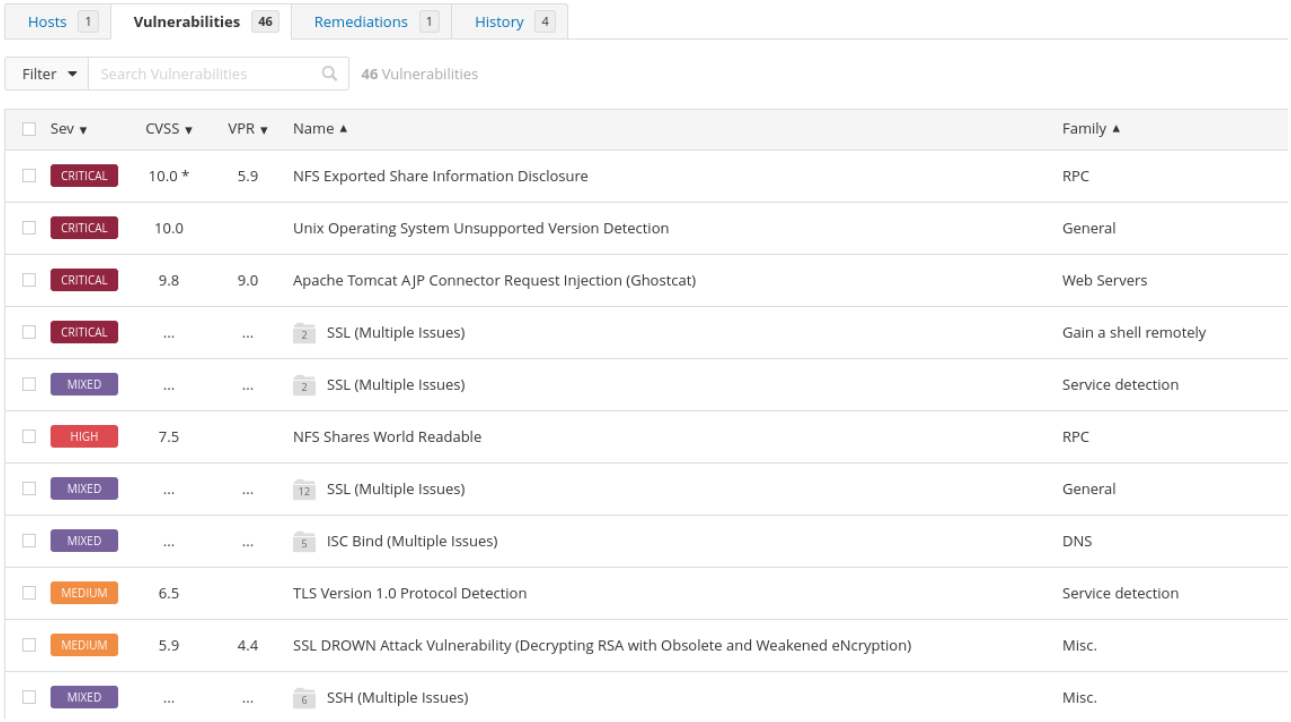
```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.50.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Per risolvere il problema della backdoor ho abilitato il firewall su Meta con il comando «sudo ufw enable» e ho imposto la regola deny ai pacchetti in entrata dalla porta 1524, quella interessata dalla bind shell backdoor.

```
root@metasploitable:/etc# ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere
```

Dopo queste azioni sono riuscito a ridurre le vulnerabilità critiche, come si può vedere dalla nuova scansione.

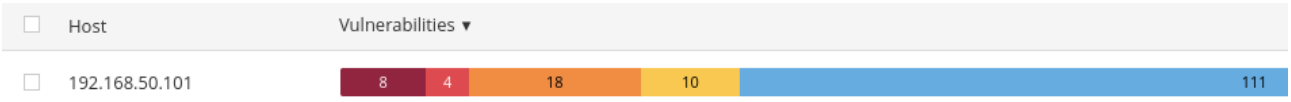


Hosts 1 | Vulnerabilities 46 | Remediations 1 | History 4

Filter | Search Vulnerabilities | 46 Vulnerabilities

Sev	CVSS	VPR	Name	Family
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers
CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely
MIXED	...	...	2 SSL (Multiple Issues)	Service detection
HIGH	7.5		NFS Shares World Readable	RPC
MIXED	...	...	12 SSL (Multiple Issues)	General
MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.
MIXED	...	...	6 SSH (Multiple Issues)	Misc.

Le vulnerabilità totali sono scese da 54 a 46 e quelle critiche da 10 a 8.



Host	Vulnerabilities
192.168.50.101	8 4 18 10 111

Questo significa che la risoluzione di alcune vulnerabilità critiche ha impattato anche su vulnerabilità di entità minore.

Anche il report della seconda scansione si può trovare al link:

https://github.com/MarcoBortolotti987/S5-L5-Vulnerability-Assessment