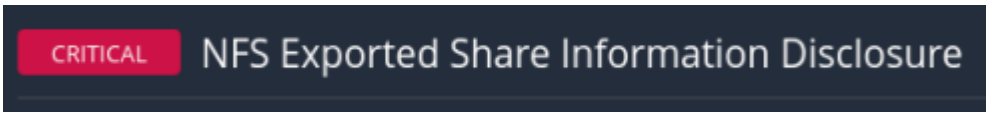
1.



NFS Exported Share Information Disclosure

Descrizione e risoluzione:

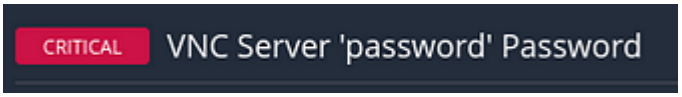
Questa vulnerabilità critica riscontrata dalla scansione verso l'host target specifica che è possibile accedere alle condivisioni NFS (Network File System) dell'host senza nessun tipo di restrizione. Questo significa che un attaccante sulla stessa rete potrebbe essere in grado di accedere e leggere i file system esportati dal server NFS senza nessuna autorizzazione. Data la scansione effettuata con Nessus, confermata dall'ausilio di nmap, si nota la porta *111* aperta con servizio *rcpbind* attivo. Si procede dunque alla configurazione dalla macchina Metasploitable del firewall *iptables* per il filtraggio dei pacchetti in entrata sulla porta 111 con protocollo TCP. Questo permetterà agli utenti non autorizzati di non accedervi e mitigare la vulnerabilità riscontrata.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp --dport 111 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 111 -j DROP
```

Scansionando nuovamente con nmap, possiamo confermare che la porta 111/tcp è stata correttamente filtrata e questo permetterà di proteggere il sistema dalla vulnerabilità in questione.

```
111/tcp  filtered rpcbind
```

2.

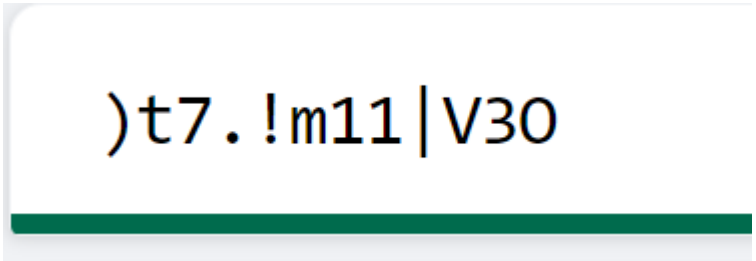


VNC Server ‘password’ password

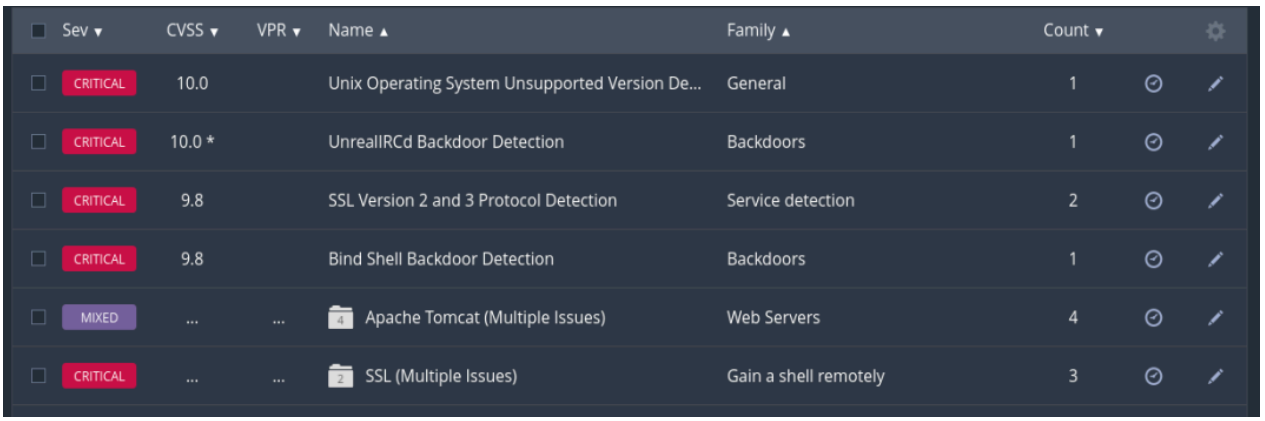
Descrizione e soluzione:

Questa vulnerabilità critica riscontrata dalla scansione verso l’host target specifica che il Server VNC in esecuzione usufruisce di una password molto debole, pertanto si raccomanda fortemente di cambiarla con una complessa.
Il metodo più veloce ma efficace consiste appunto nella sostituzione di una password difficilmente intuibile.
Si procede nella sostituzione da Metasploitabile con il comando *vncpasswd.*

Mi avvalgo di un tool specializzato nella generazione randomica di password complesse e genero la password.

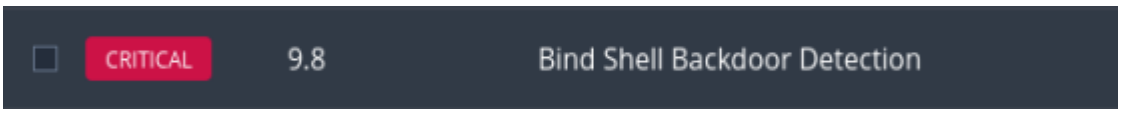


Inserisco e verifico la password generata e rieseguo la scansione. Come si può notare, la vulnerabilità non è più riscontrata tra quelle critiche presenti.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version De...	General	1
CRITICAL	10.0 *		UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3

3.



Bind Shell Backdoor Detection

Descrizione e soluzione:

Una gravissima vulnerabilità è stata inoltre riscontrata dalla scansione su Nessus, ovvero risulta che una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta e inviando direttamente i comandi. Andiamo ad identificare la porta sulla quale è in ascolto la shell non autorizzata e il servizio responsabile.

Port	Hosts
1524 / tcp / wild_shell	192.168.1.32

verifico su nmap:

Il servizio *ingreslock* in questo contesto sta a significare che è presente una backdoor sulla porta 1524. Le backdoor infatti vengono spesso utilizzate per ottenere accesso ad un sistema bypassando le normali procedure di autenticazione e sicurezza. Essendo Metasploitable un sistema sviluppato appositamente per essere vulnerabile, si potrebbero riscontrare ancora problemi in fase di analisi successive anche dopo la reinstallazione, motivo per cui decido di procedere diversamente per eliminare la backdoor. Tramite il comando *sudo lsof -i :1524* possiamo vedere un elenco delle connessioni attive sulla porta 1524.

```
msfadmin@metasploitable:~$ sudo lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4360 root   12u  IPv4  12494       TCP *:ingreslock (LISTEN)
msfadmin@metasploitable:~$
```

```
NAME
*:ingreslock (LISTEN)
```

Qui, tra le varie opzioni, possiamo identificare il PID (Process ID) che gestisce la connessione. La risoluzione può consistere nel killare il PID e verificare se la vulnerabilità sia stata mitigata.

```
msfadmin@metasploitable:~$ sudo kill 4360
msfadmin@metasploitable:~$ sudo lsof -i :1524
msfadmin@metasploitable:~$
```

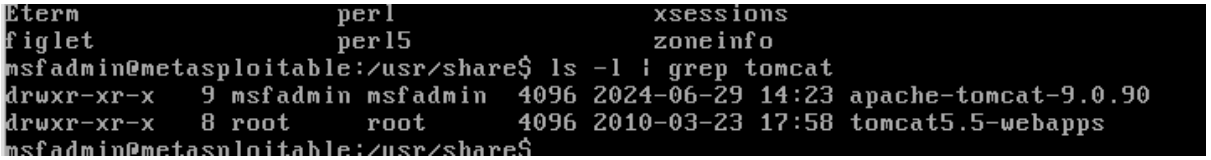
4.

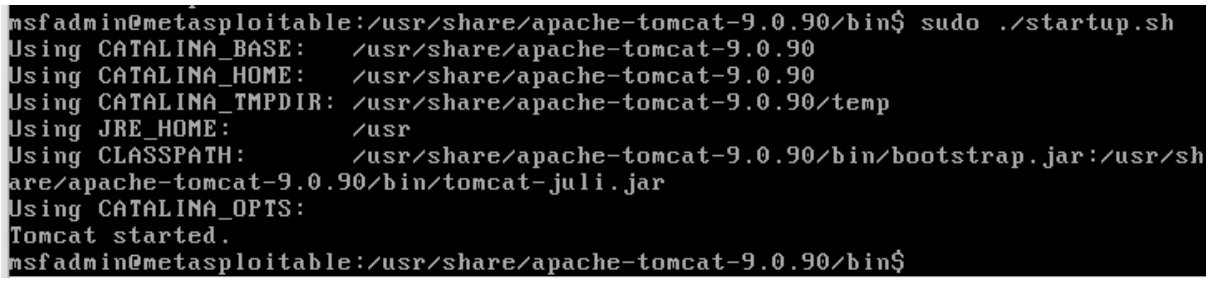
CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione e soluzione:

L'Apache Tomcat AJP Connector Request Injection, nota come "Ghostcat," è una vulnerabilità che consente agli attaccanti di leggere o scrivere file su server vulnerabili tramite il protocollo AJP (Apache JServ Protocol). Questo exploit può essere sfruttato per ottenere accesso non autorizzato ai dati sensibili o per eseguire codice arbitrario, mettendo a rischio la sicurezza delle applicazioni web ospitate su Tomcat. La vulnerabilità colpisce le versioni di Tomcat precedenti alla 9.0.31, ed è stata mitigata attraverso aggiornamenti e configurazioni di sicurezza appropriate. Questo è il motivo per cui una delle soluzioni potrebbe essere scaricare e aggiornare Tomcat nella versione 9.0.90.





Verifichiamo che la vulnerabilità sia stata mitigata.