EPICODE PROGETTO W12D4

Report: Analisi delle vulnerabilità e azioni di rimedio

Data di esecuzione: Da Domenica a Lunedì
Ambiente:

- [ ] **Scanner:** Kali Linux con Nessus
- [ ] **Target:** Metasploitable (clone isolato per evitare modifiche sull'originale)
- [ ] **Virtualizzazione:** Entrambe le macchine virtuali su VirtualBox

Introduzione

Il presente report ha l'obiettivo di documentare l'analisi delle vulnerabilità riscontrate sull'ambiente di test costituito da una macchina **Kali Linux** (strumento di scansione con **Nessus**) e una macchina target **Metasploitable**, clonata e isolata. Lo scopo è evidenziare le debolezze del sistema e proporre azioni di rimedio per mitigarle.

Scansione delle vulnerabilità:

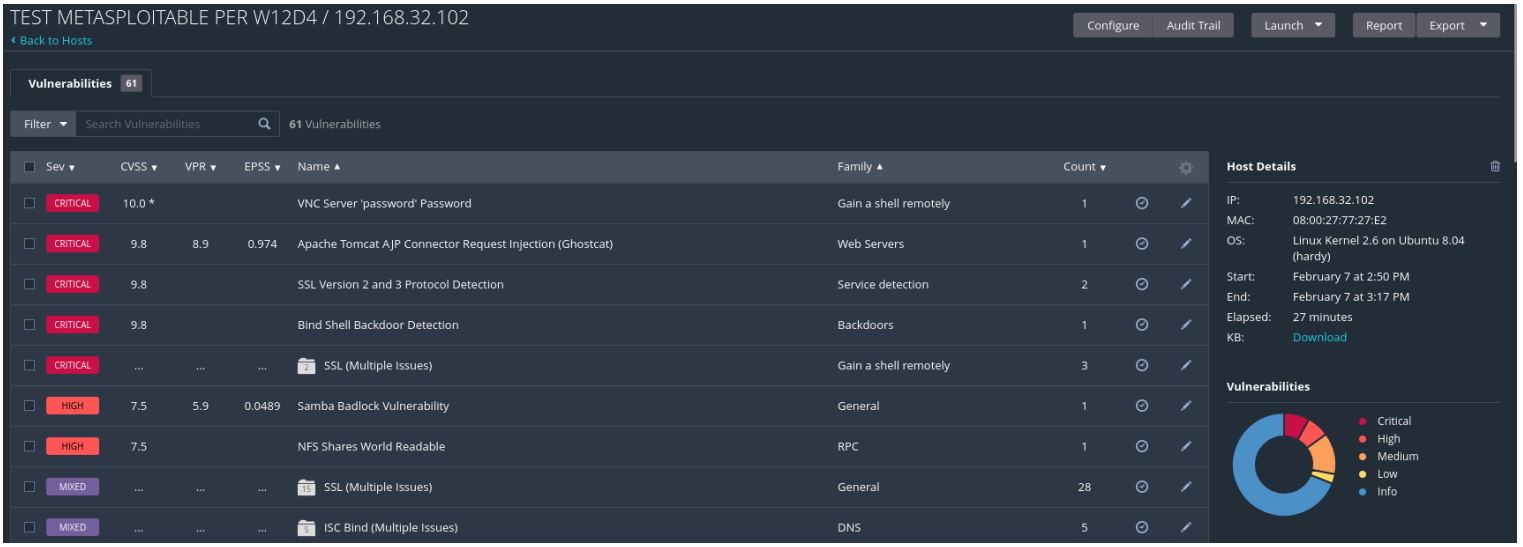
- [ ] Avvio di una scansione "basic" su tutte le porte del target utilizzando Nessus.
- [ ] Raccolta dei dati e generazione dei report di vulnerabilità.

Analisi dei risultati:

- [ ] Revisione dei report generati da Nessus per individuare le principali vulnerabilità.
- [ ] Documentazione delle vulnerabilità rilevate e delle possibili azioni di rimedio.

Risultati della Scansione Nessus

Di seguito sono riportate le evidenze e i report estratti da Nessus.



Risolveremo alcune delle vulnerabilità presenti nello screen.

1. Remediation Bind Shell Backdoor Detection

Questo tipo di backdoor permette a un attaccante di connettersi direttamente alla porta vulnerabile ed eseguire comandi sul sistema compromesso senza alcuna restrizione. La presenza di una bind shell aperta rappresenta una seria minaccia alla sicurezza del sistema, un attaccante che scopre questa vulnerabilità può ottenere il pieno controllo del sistema remoto, eseguendo comandi arbitrari come utente root.

Porta e Servizio Rilevati:

- ☐ **Porta:** 1524/tcp
- ☐ **Servizio:** wild_shell
- ☐ **Indirizzo IP:** 192.168.32.102

Soluzione:

- ☐ Implementare misure di sicurezza come firewall, monitoraggio delle porte aperte e aggiornamenti regolari del software per prevenire future compromissioni.

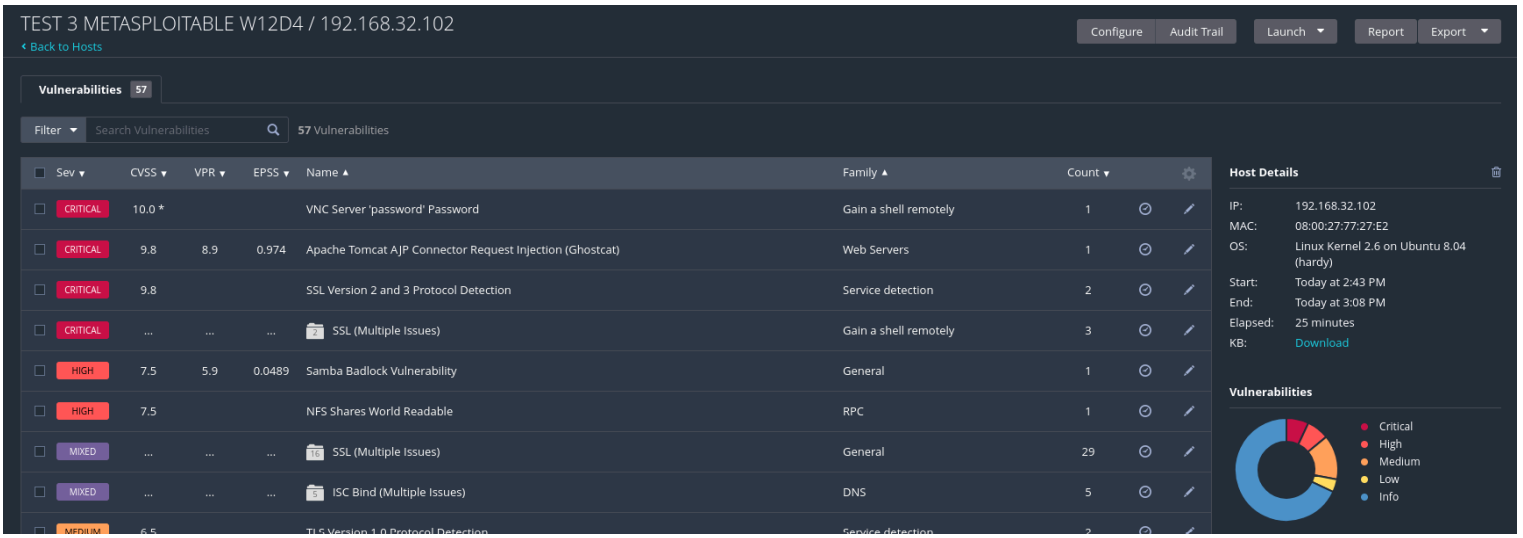
Il sistema è volutamente vulnerabile e progettato per restare in quello stato, ciò che andrò a fare è semplicemente la “chiusura temporanea” della porta in questione. Terminare il processo chiuderà la porta solo fino al prossimo riavvio del sistema o finché un altro servizio non la riaprirà.

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524            0.0.0.0:*
4496/xinetd
msfadmin@metasploitable:~$ sudo kill -9 4496
msfadmin@metasploitable:~$
```

Attraverso il comando: **`sudo netstat -tulnp | grep 1524`** identifichiamo il processo in ascolto sulla porta 1524 e restituirà il PID del processo per la successiva chiusura con **`sudo kill -9 4496`** (PID). Per finire, ricontrollo i processi, per assicurarmi che siano stati effettivamente terminati.

```
msfadmin@metasploitable:~$ sudo kill -9 4496
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ _
```

Non sono presenti processi attivi, eseguiamo una nuova scansione con Nessus:



La vulnerabilità critica è stata risolta, ma temporaneamente.

Risoluzione permanente:

- ☐ Disabilitare il servizio che apre la porta.
- ☐ Rimuovere eventuali script di avvio che riattivano la bind shell.
- ☐ Applicare regole firewall permanenti (ad esempio con **iptables** o **ufw**).

2. Remediation VNC Server 'password' Password

Questa vulnerabilità si verifica quando un server VNC (Virtual Network Computing) è configurato con una password predefinita debole o facilmente indovinabile, come "password".

Passaggi per la risoluzione:

Verificare se il server VNC è attivo, controllo dei processi in esecuzione con comando: **`ps aux | grep Xtightvnc.`**

```
msfadmin@metasploitable:~$ ps aux | grep Xtightvnc
root      4602  0.0  2.3  13928 12008 ?        S    14:00   0:00 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
msfadmin  4703  0.0  0.1   3004   748 tty1     R+   14:05   0:00 grep Xtightvnc
msfadmin@metasploitable:~$ sudo kill -9 4602
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ps aux | grep Xtightvnc
msfadmin  4722  0.0  0.1   3004   752 tty1     R+   14:09   0:00 grep Xtightvnc
msfadmin@metasploitable:~$
```

Arrestare il servizio VNC

Dopo aver identificato il processo VNC, è possibile terminarlo con il comando: **`sudo kill -9 4602 (PID).`**

Dopo aver eseguito il comando, verifica che il processo non sia più attivo: **`ps aux | grep Xtightvnc.`**

Cambiare la password

Per modificare la password VNC, usa il comando: **`vncpasswd`**

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

VNC permette solo password di massimo 8 caratteri.

Dopo aver cambiato la password, riavvio il server VNC con il comando: **`vncserver :1`**

```
msfadmin@metasploitable:~$ vncserver :1
xauth:  creating new authority file /home/msfadmin/.Xauthority

New 'X' desktop is metasploitable:1

Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log
```

3. Remediation Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVE-2020-1938)

La vulnerabilità in questione interessa **Apache Tomcat**, che a causa di una configurazione insicura del **connettore AJP (Apache JServ Protocol)**, permette ad un attaccante remoto non autenticato di **leggere file arbitrari** dal server Tomcat.

Passaggi per la risoluzione:

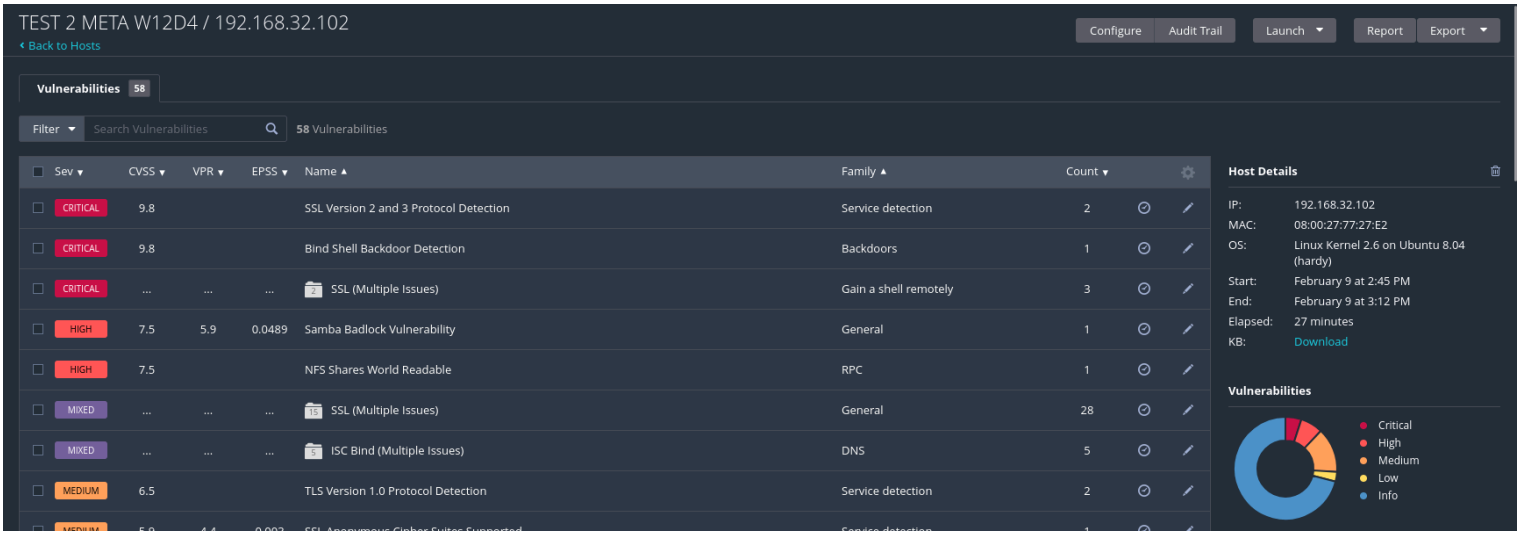
- ☐ Disabilitare completamente il connettore AJP

Il connettore AJP si trova nel file di configurazione di Tomcat: **`sudo nano /etc/tomcat*/server.xml`**
Ho cercato la sezione: **`<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />,`** ed ho eliminato la riga (se questa riga è presente e attiva, significa che il connettore AJP è abilitato e il server è vulnerabile).

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
           enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" acceptCount="100" connectionTimeout="20000"
           proxyPort="80" disableUploadTimeout="true" />
-->
```

Dopo la modifica ho riavviato Tomcat con il comando: **`sudo /etc/init.d/tomcat restart.`**



NB: Queste due vulnerabilità sono state risolte una dopo l'altra, in quanto mancanza di tempo per eseguire ulteriori scanner con Nessus, quindi mostrerò un solo scanning finale per entrambe le remediation.

NB: Per mancanza di tempo, la prima vulnerabilità e le ultime due, sono state risolte con 2 cloni di metasploitable, in quanto il primo clone è stato reso inutilizzabile. (Infatti nell'ultimo screen è ancora presente il Bind Shell)

NB: le ricerche per le risoluzioni ed i comandi sono state effettuate da internet, report nessus e chat gpt.