M3W12D4 – RemediationMeta

Analisi delle vulnerabilità e azioni di rimedio

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche 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. Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - ScansioneInizio.pdf
2. Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - ScansioneFine.pdf
   Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

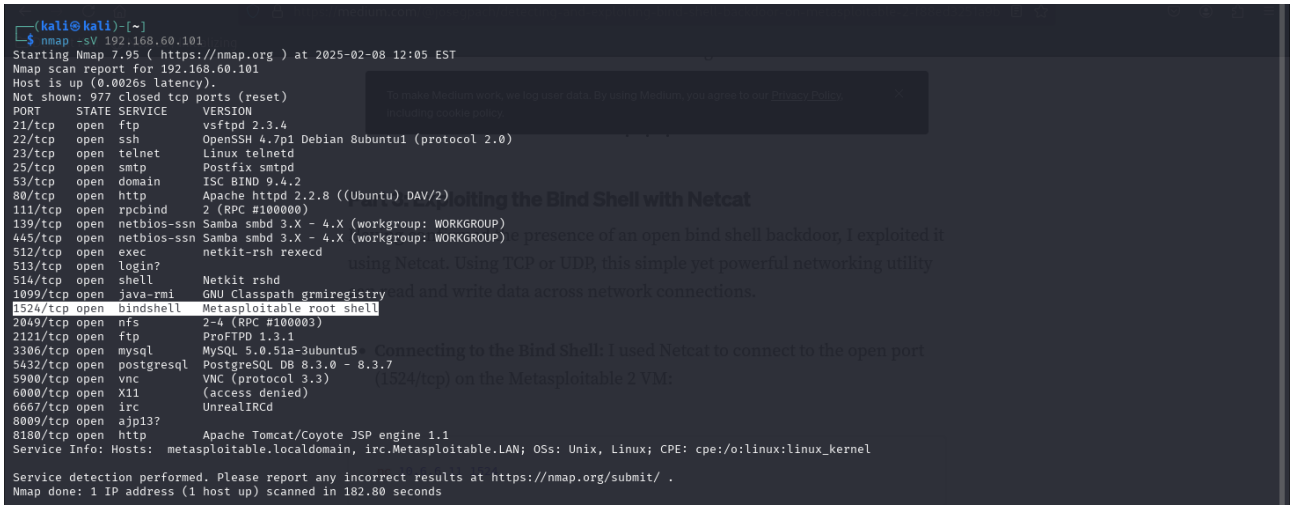
Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

---

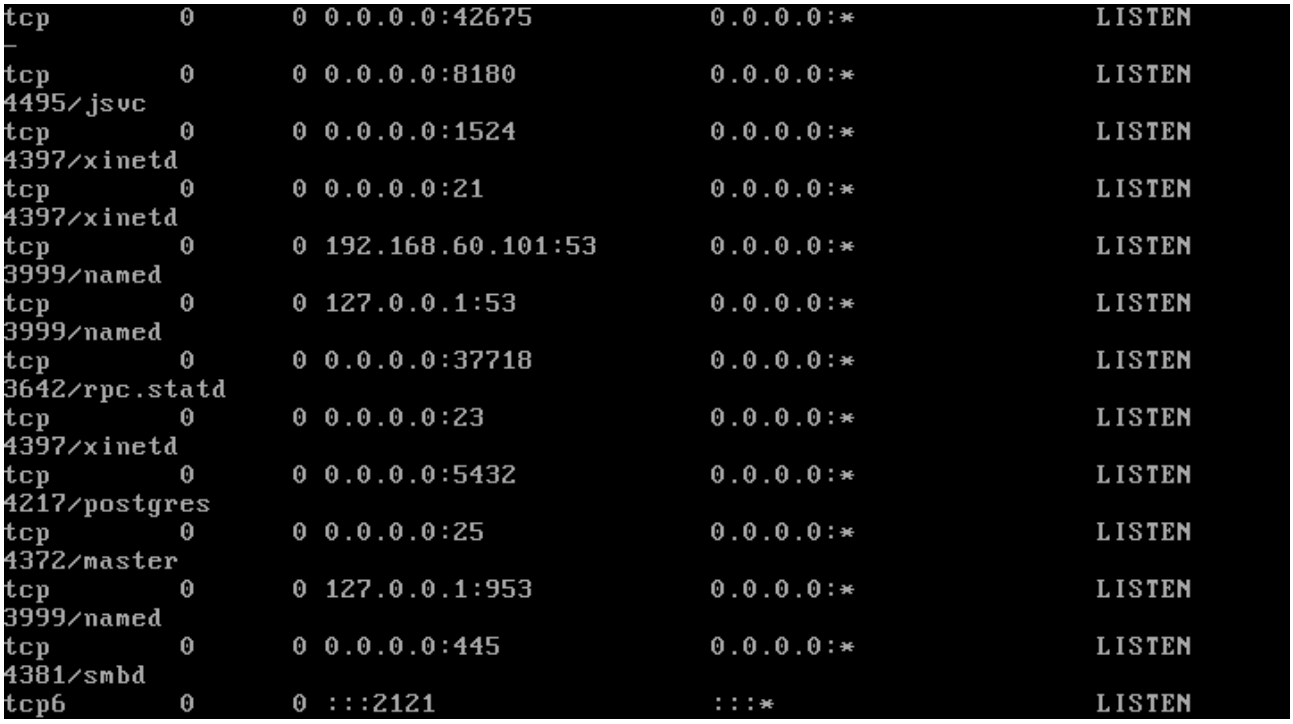
Sistemiamo la prima vulnerabilità, **Bind Shell Backdoor Detection**:

Controlliamo che la porta sia aperta usando su Kali: nmap -sV 192.168.60.101



Sfruttiamo questa porta aperta per poter entrare su Metasploitable usando Netcat e ci connettiamo alla porta aperta 1524, verifichiamo a che livello siamo di autorizzazione con *whoami* e verifichiamo l'IP con il comando *ip a*.

Ora che abbiamo appurato che un attaccante può attaccare, andiamo su Metasploitable, facciamo sudo su e come amministratore lanciamo questo comando: netstat -tulnp | grep LISTEN



Notiamo che la porta 1524 ha come nome processo xinetd con PID 4397, usiamo allora il comando kill -p 4397 per fermare il processo (il nome del PID esce solo con i permessi di root). Una volta fatto, dobbiamo chiudere la porta del servizio aperto con ufw deny 1524 e se lo vogliamo disinstallare direttamente tutto il servizio possiamo lanciare apt-get remove –purge xinetd -y (dove –-purge ci fa eliminare anche i file di configurazione mentre -y fa rispondere sì a tutte le richieste durante il comando.

```
tcp6       0      0 :::53                   :::*                    LISTEN
3999/named
tcp6       0      0 :::22                   :::*                    LISTEN
4021/sshd
tcp6       0      0 :::5432                 :::*                    LISTEN
4217/postgres
tcp6       0      0 ::1:953                 :::*                    LISTEN
3999/named
root@metasploitable:/home/msfadmin# service --status-all
The program 'service' can be found in the following packages:
 * debian-helper-scripts
 * sysvconfig
Try: apt-get install <selected package>
bash: service: command not found
root@metasploitable:/home/msfadmin# systemctl disable xinetd
bash: systemctl: command not found
root@metasploitable:/home/msfadmin# systemct stop xinetd
bash: systemct: command not found
root@metasploitable:/home/msfadmin# systemctl disable xinetdnetd
xinetd
root@metasploitable:/home/msfadmin# systemctl disable xinetd
bash: systemctl: command not found
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# _
```

Ora ci occupiamo di **VNC Server 'password' Password:**

Abbiamo rimosso quella vecchia col comando rm ~/.vnc/passwd, poi col comando vncpasswd ce ne chiede una nuova e noi abbiamo messo Nuov4.Z

```
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Passwords do not match. Please try again.

Password:
Password too short
root@metasploitable:~# ls -l ~/.vnc/passwd
ls: cannot access /root/.vnc/passwd: No such file or directory
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:~# ls -l ~/.vnc/passwd
-rw------- 1 root root 16 2025-02-10 10:23 /root/.vnc/passwd
root@metasploitable:~# _
```

Ora ci occupiamo di **Apache Tomcat A JP Connector Request Injection (Ghostcat)**

Nel nostro caso, data l'impossibilità di poter scaricare aggionamenti, disattiviamo il connettore AJP: modifichiamo il file server.xml con sudo nano /etc/tomcat5.5/conf/server.xml

e da “<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />” a “<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->”