

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`

```
(kali@kali) [~]
$ nmap -sV 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 12:05 EST
Nmap scan report for 192.168.60.101
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnetd      Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath gcrmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.80 seconds
```

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`.

```
kali@kali: ~  
File Actions Edit View Help  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp open rpcbind 2 (RPC #100000)  
139/tcp open smb Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open smb Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp open exec netkit-rsh rshd  
513/tcp open login? netkit-rsh rexecd  
514/tcp open shell Netkit rshd  
1099/tcp open java-rmi GNU Classpath gcrimetry  
1524/tcp open bindshell Metasploitable root shell  
2049/tcp open nfs 2-4 (RPC #100003)  
2121/tcp open ftp ProFTPD 1.3.1  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp open vnc VNC (protocol 3.3)  
6000/tcp open X11 (access denied)  
6667/tcp open irc UnrealIRCd  
8009/tcp open ajp13? Apache Tomcat/Coyote JSP engine 1.1  
8180/tcp open http Metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service Info: Hosts: Metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 182.80 seconds  
(kali@kali)-[~]  
$ nc 192.168.60.101 1524  
root@metasploitable:/# whoami  
root  
root@metasploitable:/# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 1636 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:f1:dd:02 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.60.101/24 brd 192.168.60.255 scope global eth0  
        inet6 fe80::a0:27:f1:dd:02/64 scope link  
            valid_lft forever preferred_lft forever  
root@metasploitable:/#
```

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`

```
tcp        0      0 0.0.0.0:42675        0.0.0.0:*            LISTEN  
tcp        0      0 0.0.0.0:8180         0.0.0.0:*            LISTEN  
4495/jsvc  0      0 0.0.0.0:1524        0.0.0.0:*            LISTEN  
4397/xinetd 0      0 0.0.0.0:21         0.0.0.0:*            LISTEN  
tcp        0      0 0.0.0.0:21          0.0.0.0:*            LISTEN  
4397/xinetd 0      0 192.168.60.101:53  0.0.0.0:*            LISTEN  
3999/named 0      0 127.0.0.1:53       0.0.0.0:*            LISTEN  
3999/named 0      0 0.0.0.0:37718      0.0.0.0:*            LISTEN  
3642/rpc.statd 0      0 0.0.0.0:23        0.0.0.0:*            LISTEN  
4397/xinetd 0      0 0.0.0.0:5432       0.0.0.0:*            LISTEN  
4217/postgres 0      0 0.0.0.0:25        0.0.0.0:*            LISTEN  
4372/master 0      0 127.0.0.1:953     0.0.0.0:*            LISTEN  
3999/named 0      0 0.0.0.0:445       0.0.0.0:*            LISTEN  
4381/smbd  0      0 :::2121            :::*                LISTEN  
tcp6       0      0 :::2121            :::*                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 aggiornamenti, 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" /> -->”
