

Benchmark M3

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

Report di Vulnerability Assessment

Redatto da: Pandolfi Luciano

Data: 22/11/2024

Obiettivo del Report: Identificare le vulnerabilità di sicurezza di un SO, valutarne i rischi e proporre soluzioni.

[Repository BenchmarkM3 W12D4](#)

[Guida alla comprensione del contenuto della repository:](#)

1. **Scan_Meta_Inizio:** Fornisce una linea di base delle vulnerabilità presenti prima di qualsiasi intervento di remediation.
2. **Remediation_Meta:** Evidenzia i passaggi intrapresi per risolvere ciascuna vulnerabilità critica.
3. **Scansione_Meta_Fine:** Verifica che le vulnerabilità critiche identificate nella scansione iniziale siano state risolte con successo.

Questa repository contiene la documentazione e i file relativi ad una serie di valutazioni delle vulnerabilità effettuate utilizzando il tool “Nessus”.

La documentazione è la seguente:

1. **SCAN_META_INIZIO.pdf**: Report della scansione delle vulnerabilità iniziale.
2. **REMEDIATION_META.pdf**: Descrizione dettagliata dei passaggi di remediation intrapresi per risolvere le vulnerabilità identificate.
3. **SCAN_META_FINE.pdf**: Report della scansione delle vulnerabilità finale che mostra i risultati dopo la remediation.

Dettagli dell'Ambiente:

- **ATTANCANTE**: Kali Linux
 - **Indirizzo IP**: 192.168.1.100
- **TARGET**: Metasploitable2
 - **Indirizzo IP**: 192.168.2.50

Vulnerabilità Critiche Risolte:

La scansione iniziale ha identificato vulnerabilità critiche sulla macchina target, che sono state successivamente risolte. Queste vulnerabilità e i relativi passaggi di remediation sono di seguito riportati ed esaminati:

1. **Password del Server VNC 'password'**

a. **Descrizione del Problema:**

La Password del server VNC (Virtual Network Computing) predefinita è debole, consente agli eventuali attaccanti di accedere facilmente al server remoto.

b. **Passaggi di Remediation:**

- Cambiare la password predefinita('password') con una complessa e sicura(Luc123!"£), utilizzando '**sudo vncpasswd**' entrando al server tramite Kali Linux con il comando '**sudo vncviewer 192.168.2.50**';
- Verifica della connessione al server VNC e screen che evidenziano il cambio della nuova password inserita, testata con l'accesso al server.

- **Screen:**

```
(kali㉿kali)-[~]  
$ sudo vncviewer 192.168.2.50  
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  
^CCleanupSignalHandler called  
  
(kali㉿kali)-[~]  
$ sudo vncviewer 192.168.2.50  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:  
Authentication failure
```

```
root@metasploitable: /  
root@metasploitable:/# sudo vncpasswd  
Using password file /root/.vnc/passwd  
Password:  
Verify:  
Would you like to enter a view-only password (y/n)? y  
Password:  
Warning: password truncated to the length of 8.  
Verify:  
root@metasploitable:/# sudo vncpasswd  
Using password file /root/.vnc/passwd  
Password:  
Verify:  
Would you like to enter a view-only password (y/n)? y  
Password:  
Verify:  
root@metasploitable:/# █
```

2. Iniezione di Richieste del Connettore AJP di Apache Tomcat (Ghostcat)

a. Descrizione del Problema:

Questa vulnerabilità (Ghostcat) permette l'iniezione di richieste tramite il connettore AJP di Apache Tomcat e consente agli attaccanti di leggere il

contenuto dei file web applicativi, in alcune casistiche anche di eseguirli.

b. Passaggi di Remediation:

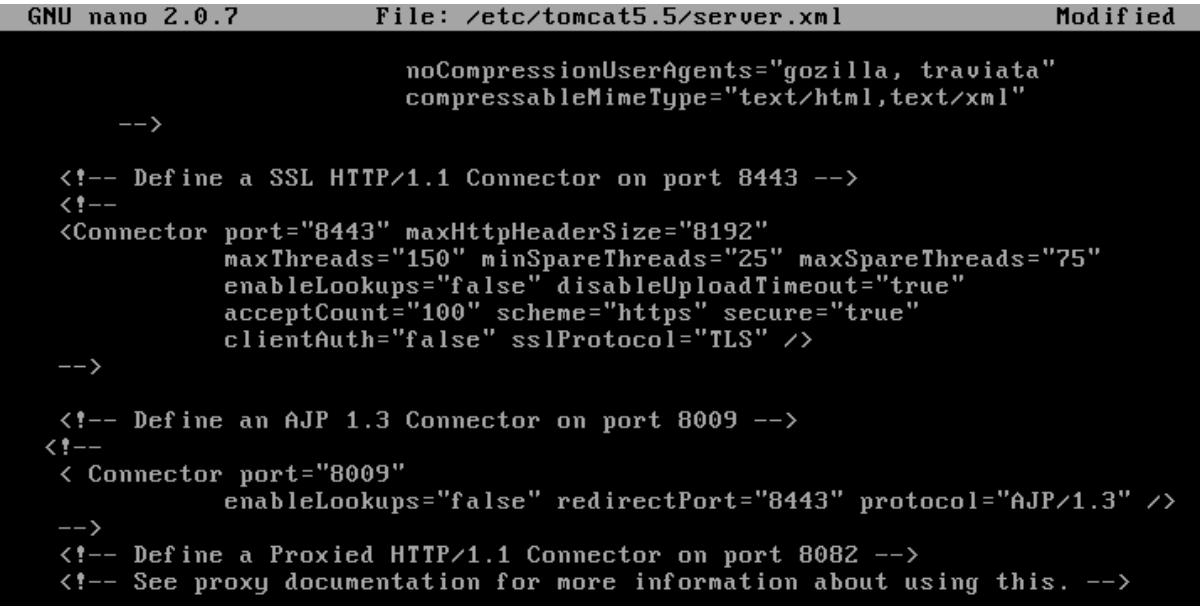
- Disabilitazione del connettore AJP nel file server.xml (accedendo al file tramite il comando `'sudo nano /etc/tomcat5.5/server.xml'`), andando in seguito a commentare la riga `<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />` ;

- Metodo di commento riga:

```
<!--  
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />  
--> ;
```

- In conclusione riavviare il servizio con le modifiche apportate al file `'server.xml'` con il comando `'sudo /etc/init.d/tomcat5.5 restart'`.

- Screen:



```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml      Modified  
  
noCompressionUserAgents="gozilla, traviata"  
compressableMimeType="text/html,text/xml"  
  
-->  
  
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->  
<!--  
<Connector port="8443" maxHttpHeaderSize="8192"  
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"  
    enableLookups="false" disableUploadTimeout="true"  
    acceptCount="100" scheme="https" secure="true"  
    clientAuth="false" sslProtocol="TLS" />  
-->  
  
<!-- 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. -->
```

3. Rilevazione del Protocollo SSL Versione 2 e 3 (porta 25 e 5432)

a. Descrizione del Problema:

- Le versioni 2 e 3 del protocollo SSL(Secure Sockets Layer) sono obsolete e insicure mettendo a rischio la sicurezza delle comunicazioni.

b. Passaggi di Remediation:

- Configurazione delle regole del firewall per bloccare, in modo temporaneo, l'accesso alle porte associate(porta 25 e porta 5432) a questo protocollo tramite iptables con i comandi:

'sudo iptables -A INPUT -p tcp --dport 25 -j REJECT'
'sudo iptables -A INPUT -p tcp --dport 5432 -j REJECT'

- Screen:

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 25 -j REJECT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j REJECT
```

- Inoltre attivando questa configurazione andiamo a filtrare la comunicazione in modo tale che altre vulnerabilità collegate alle porte 25 e 5432 vengano bonificate. (es. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)).
- Se si volessero salvare queste regole applicate dal firewall(iptables) dopo il riavvio della macchina, si potrebbe creare e modificare un file eseguibile nel percorso di destinazione.(es. sudo iptables-save > /etc/iptables/file_eseguibile)

4. Rilevazione della Backdoor Bind Shell (porta 1524)

a. Descrizione del Problema:

- Presenza di una backdoor bind shell che permette agli attaccanti di ottenere l'accesso remoto ad un SO tramite una shell di comando.
Questa vulnerabilità consente il controllo totale del sistema per questo è molto pericolosa.

b. Passaggi di Remediation:

- Identificazione e terminazione del processo associato(4533) alla porta 1524 con i comandi:
'sudo netstat -tulnp | grep 1524' (Identificazione Processo);
'sudo ls -l /proc/4533/exe'(Identificazione del file eseguibile del Processo);
- successiva rimozione del file eseguibile (percorso file: **'/usr/sbin/xinetd'**)ed accertamento che la backdoor non possa riavviarsi, con i comandi:
'sudo kill -9 4431' (Termina il processo)
'sudo rm /usr/sbin/xinetd' (Eliminazione del file eseguibile)

- Screen:

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4533/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4533/exe
lrwxrwxrwx 1 root root 0 2024-11-23 10:57 /proc/4533/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo kill -9 4533
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
msfadmin@metasploitable:~$ sudo rm /usr/sbin/xinetd
```

5. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (porta 22)

a. Descrizione del Problema:

Questa vulnerabilità determina una debolezza nel generatore di numeri casuali che compromette le chiavi crittografiche, comprese chiavi SSH e certificati, rendendole prevedibili e vulnerabili ad attacchi di brute force.

Passaggi di Remediation:

- Identificare la versione di OpenSSL con il comando:

‘sudo openssl version -a’

- Aggiornamento dei pacchetti OpenSSL con i seguenti comandi:

‘sudo apt-get update’

‘sudo apt-get upgrade’ (può generare errori durante l’aggiornamento)

- Eliminare le chiavi(key) d’interesse con il comando:

‘sudo rm /etc/ssh/ssh_host_*’

- Generare nuovamente le chiavi SSH con il comando:

‘sudo dpkg-reconfigure openssh-server’

- Infine riavviare i servizi con il comando:

‘sudo /etc/init.d/ssh restart’

- Screen:

```
msfadmin@metasploitable:~$ cd /etc/ssh
msfadmin@metasploitable:/etc/ssh$ ls
moduli      sshd_config      ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_rsa_key
msfadmin@metasploitable:/etc/ssh$ sudo rm ssh_host_*
msfadmin@metasploitable:/etc/ssh$ ls
moduli  ssh_config  sshd_config
msfadmin@metasploitable:/etc/ssh$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd [ OK ]

msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_*
msfadmin@metasploitable:~$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
```

```
msfadmin@metasploitable:/etc/ssh$ sudo /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
```

6. UnrealIRCd Backdoor Detection (porta 6667)

a. Descrizione del Problema:

Questa vulnerabilità riguarda una backdoor nascosta nella versione 3.2.8.1 di UnrealIRCd, consente ad un attaccante di poter sfruttare un comando IRC modificato appositamente per ottenere l'accesso remoto al server ed eseguire comandi direttamente nel sistema Target.

b. Passaggi di Remediation:

- Non essendo riuscito ad aggiornare il server IRC, ho inizialmente identificato il processo root relativo alla porta in esame con il comando:

'ps aux | grep ircd' (processo associato 4612 - percorso processo /usr/bin/unrelircd)

- Terminare il processo con il comando:

'sudo kill -9 4612'

- Infine ho inserito con il firewall UFW una regola che bloccasse(deny) tutte le richieste di connessione sulla porta 6667 con il comando:

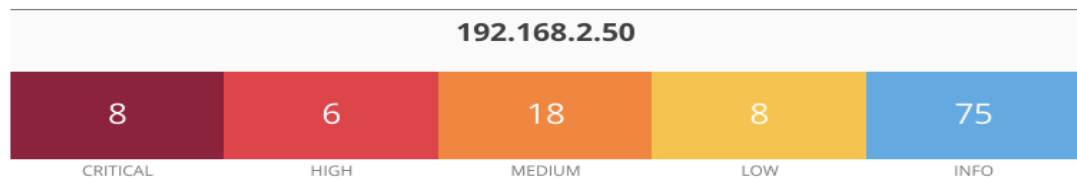
'sudo ufw deny 667'

- Screen:

```
msfadmin@metasploitable:~$ ps aux | grep ircd
root      4612  0.0  0.1  8540  2524 ?        S   11:28   0:00 /usr/bin/unrelircd
ircd
msfadmin  6645  0.0  0.0   3004   752 tty1      R+  11:38   0:00 grep ircd
msfadmin@metasploitable:~$ sudo kill -9 4612

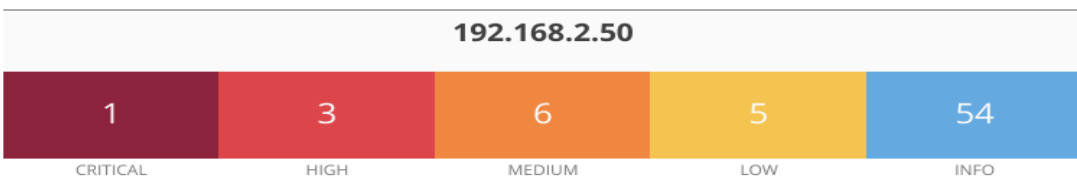
msfadmin@metasploitable:~$ ps aux | grep ircd
msfadmin  7586  0.0  0.0   3004   764 tty1      R+  11:59   0:00 grep ircd
msfadmin@metasploitable:~$ sudo ufw deny 6667
Rules updated
```

IN QUESTA SEZIONE INSERISCO LE SCANSIONI EFFETTUATE PRIMA E POST REMEDIATION:



Vulnerabilities Total: 115

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9737	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6661	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password



Vulnerabilities Total: 69

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	4.4	0.9717	136808	ISC BIND Denial of Service
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
LOW	3.7	3.4	0.6115	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled

