Report di Remediation delle Vulnerabilità su Metasploitable

Vulnerabilità 1:

Bind Shell Backdoor Detection (Porta 1524)

Il servizio ***inetd*** su Metasploitable esponeva una shell backdoor sulla porta 1524 tramite la configurazione del servizio ingreslock.

Ho utilizzato il comando: ***sudo lsof -i :1524***, è ho trovato che la porta 1524 era associata al servizio ***inetd***.

Ho aperto il seguente file: ***/etc/inetd.conf*** e ho commentato la seguente riga:

#ingreslock stream tcp nowait root /bin/bash bash -i.

Successivamente, ho riavviato il servizio inted.

La vulnerabilità è stata risolta disabilitando permanentemente il servizio ingreslock. La porta 1524 non è più accessibile e non è più in ascolto.

Vulnerabilità 2:

Apache Tomcat AJP Connector Request Injection (Ghostcat) (Porta 8009)

Il server Tomcat su Metasploitable esponeva il connettore AJP sulla porta 8009, che volendo poteva essere sfruttato da un malintenzionato per eseguire richieste non autorizzate e/o accedere a file riservati e/o eseguire codice remoto.

Ho aperto il file ***/etc/tomcat5.5/server.xml***.

Ho commentato la seguente riga di configurazione del connettore AJP:

<!-- <Connector port="8009" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" /> -->.

Poi ho riavviato il servizio di Tomcat.

Infine, ho controllato con il comando: ***netstat -tuln*** che la porta 8009 non fosse più in ascolto.

Per prassi finale, ho effettuato una scansione tramite Linux verso Meta con Nmap per confermare che la porta fosse chiusa:

sudo nmap -p 8009 192.168.32.101.

La vulnerabilità è stata risolta in modo definitivo. La porta 8009 non è più accessibile e il connettore AJP è stato disabilitato.

Conclusione:

Le vulnerabilità **Bind Shell Backdoor Detection** e **Apache Tomcat AJP Connector** sono state mitigate con successo.

Entrambe non sono più presenti nella scansione finale di Nessus. Il sistema è ora più sicuro rispetto ai rischi inizialmente individuati nel report iniziale.