SCANSIONE META

Questo rapporto descrive le vulnerabilità rilevate su una macchina virtuale Metasploitable2 e le misure adottate per mitigarle. L'attenzione è rivolta a tre specifiche vulnerabilità critiche e di alta gravità che sono state risolte efficacemente: l'analisi è supportata dall'utilizzo del software Tenable Nessus Essentials, che ha effettuato scansioni di sicurezza prima e dopo le modifiche.

PRIMA SCANSIONE

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:37 AM
End:	Today at 7:06 AM
Elapsed:	28 minutes

Vulnerabilities

1: VNC Server 'password' Password (CVSS 10.0)

Famiglia: Guadagnare una shell da remoto

Impatto: La configurazione del server VNC con una password debole o predefinita esponeva il sistema a un accesso remoto non autorizzato, aumentando il rischio di attacchi malevoli e la possibile compromissione del sistema.

2: Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVSS 9.8)

Famiglia: Server Web

Impatto: Una vulnerabilità critica nel connettore AJP di Apache Tomcat permetteva l'iniezione di richieste malevole, potenzialmente conducendo all'esecuzione di codice arbitrario da parte di un attaccante remoto.

3: Bind Shell Backdoor Detection (CVSS 9.8)

Famiglia: Backdoors

Impatto: Rilevamento di una backdoor che consente l'esecuzione remota di comandi, fornendo agli attaccanti un controllo potenzialmente illimitato sulla macchina compromessa.

RIPARAZIONE PRIMA VULNERABILITA’

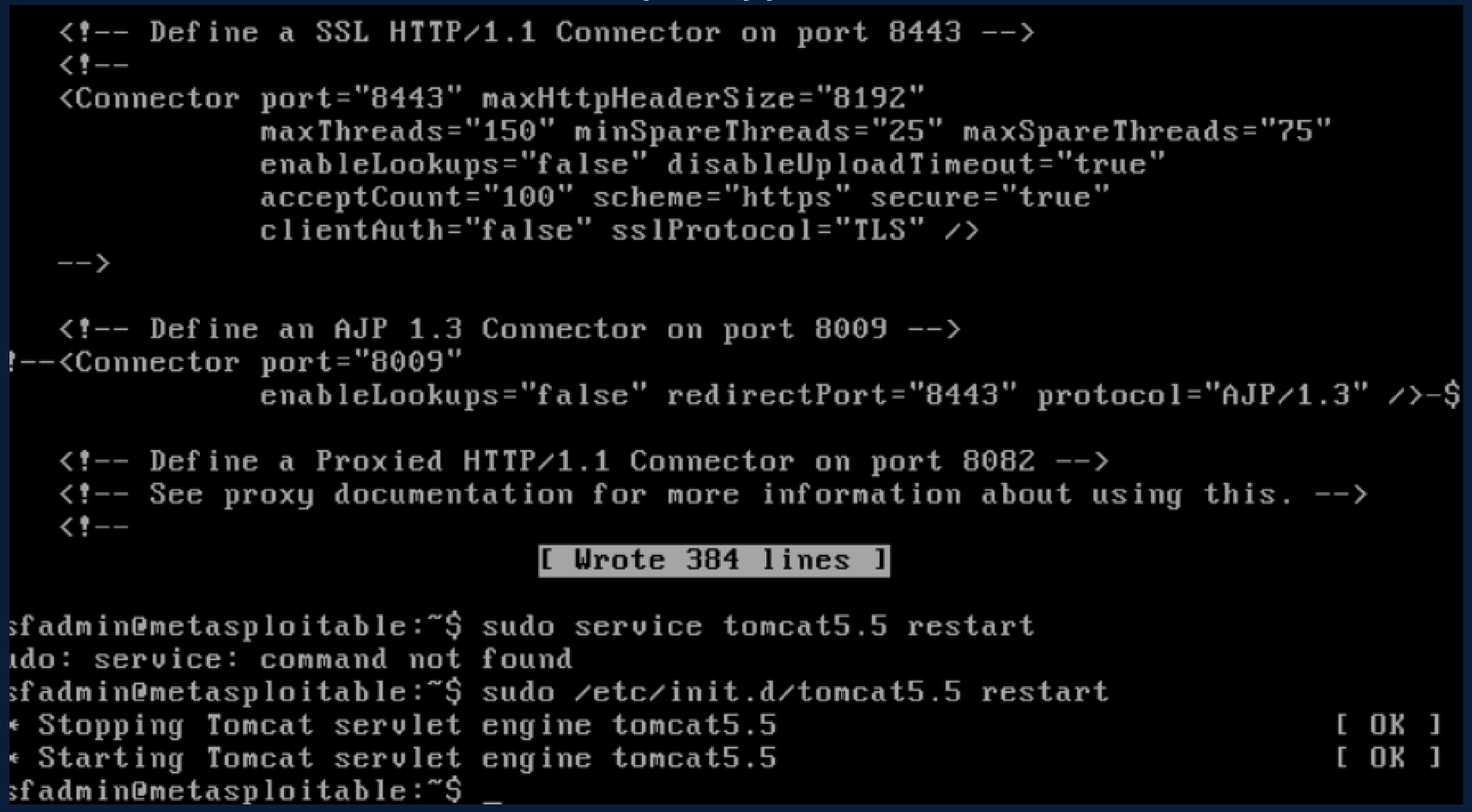
Cambio Password VNC (vncpasswd):
Ho migliorato la sicurezza del server VNC cambiando la password con una più robusta e aggiungendo una password "solo visualizzazione". Queste misure hanno significativamente ridotto il rischio di accesso remoto non autorizzato.

```
root@metasploitable:/home/msfadmin# 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:/home/msfadmin# _
```

RIPARAZIONE SECONDA VULNERABILITA’

Configurazione di Tomcat:

Ho modificato la configurazione del connettore AJP per mitigare vulnerabilità come l'iniezione di richieste. Questo include la disabilitazione del connettore AJP o la sua configurazione in modo sicuro, seguito da un riavvio del servizio Tomcat per applicare le modifiche.



RIPARAZIONE TERZA VULNERABILITA’

Per affrontare la presenza di una backdoor di tipo bind shell, ho seguito un processo di mitigazione metodico.
Inizialmente, ho compreso che una backdoor bind shell è un tipo di malware configurato per ascoltare attivamente su una specifica porta TCP, consentendo agli attaccanti di connettersi in remoto alla macchina compromessa e eseguire comandi arbitrari, simile a un accesso fisico al computer.
Per eliminare questa minaccia, ho intrapreso i seguenti passaggi:
Identificazione del processo sospetto: Utilizzando il comando netstat, ho individuato il PID (Process ID) associato alla porta sospetta che la backdoor utilizzava per ascoltare.
Esame dei dettagli del processo: Successivamente, ho esaminato i dettagli del processo per confermare la sua natura malevola e determinare se era effettivamente parte della backdoor.
Terminazione del processo: Una volta confermata la natura malevola del processo, ho terminato il processo utilizzando il comando kill per interrompere l’attività della backdoor.
Prevenzione della riattivazione: Per prevenire la riattivazione della backdoor al riavvio del sistema, ho ricercato i file di configurazione o gli script di avvio automatico che potrebbero essere stati utilizzati per avviare la backdoor e li ho eliminati.
Questo approccio ha aiutato a mitigare efficacemente la minaccia della backdoor bind shell, riducendo il rischio di accesso non autorizzato e proteggendo la sicurezza del sistema.

SECONDA SCANSIONE

Questo screenshot mostra la scansione di Metasploitable dopo le azioni di riparazione, evidenziando correttamente la rimozione delle vulnerabilità riscontrate.