S5.L3

Obiettivo: Esercizio Traccia Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Risultato Atteso: Al termine dell'esercizio, lo studente dovrebbe essere in grado di: ● Configurare e avviare scansioni di vulnerabilità con Nessus. ● Analizzare i report di vulnerabilità e comprendere le informazioni fornite.

Introduzione

Questo report descrive il risultato di una scansione delle vulnerabilità effettuata utilizzando Nessus sulla macchina virtuale Metasploitable con indirizzo IP 192.168.50.101/24

Svolgimento:

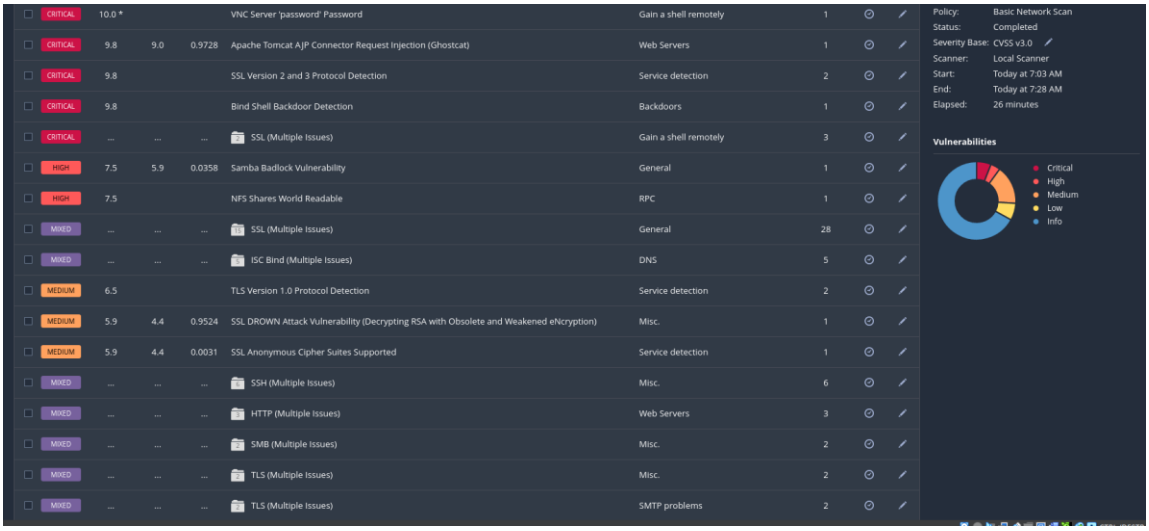
Configurazione della Scansione

- **Target**: Macchina Metasploitable (IP: 192.168.50.101)
- **Tipo di scansione**: Basic Network Scan
- **Porte**: Solo porte comuni

La scansione ha identificato un totale di 99 vulnerabilità, di cui:

- **6** vulnerabilità critiche
- **4** vulnerabilità ad alto rischio
- **16** vulnerabilità di rischio medio
- **7** vulnerabilità a basso rischio
- **66** informazioni di livello in formativo

Analizzeremo in maniera più approfondita le prime 5 vulnerabilità.



CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1		
CRITICAL	9.8	9.0	0.9728	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	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1		
HIGH	7.5			NFS Shares World Readable	RPC	1		
MIXED	...	...	...	SSL (Multiple Issues)	General	28		
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5		
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2		
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1		
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1		
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	6		
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	3		
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2		
MIXED	...	...	...	TLS (Multiple Issues)	Misc.	2		
MIXED	...	...	...	TLS (Multiple Issues)	SMTP problems	2		

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:03 AM
End: Today at 7:28 AM
Elapsed: 26 minutes

Vulnerabilities

192.168.50.101

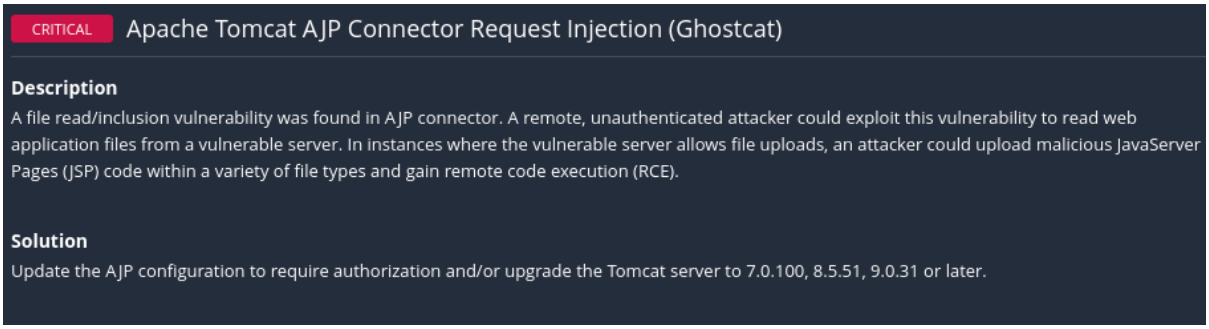
6	4	16	7	66
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 99

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	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*	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*	-	-	61708	VNC Server 'password' Password
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	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9722	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9524	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)

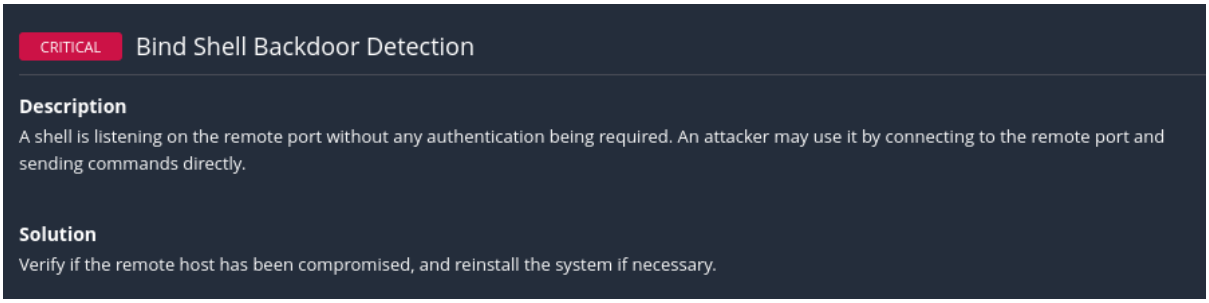
1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Severità**: Critica
- **Descrizione**: Questa vulnerabilità permette a un attaccante di inviare richieste dannose tramite il connettore AJP di Apache Tomcat, il che può consentire l'accesso a file sensibili o persino l'esecuzione di codice remoto.
- **Impatto**: Possibilità di accesso non autorizzato e potenziale compromissione del server.
- **Rimedi**: Aggiornare Apache Tomcat all'ultima versione



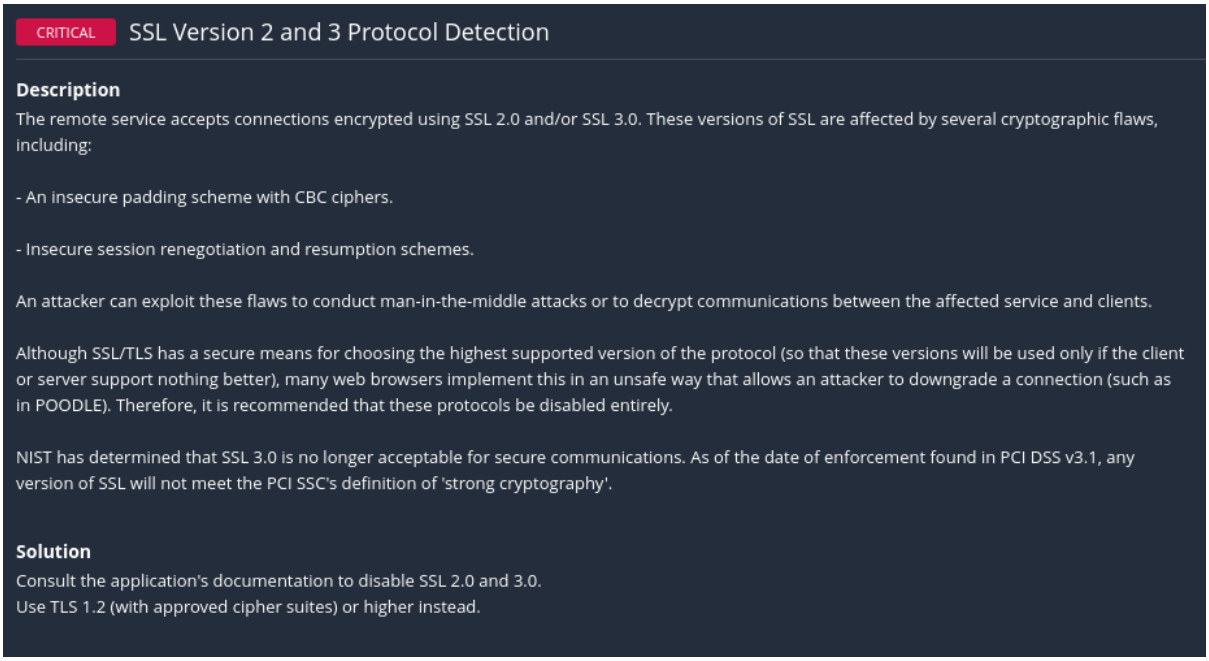
2. Bind Shell Backdoor Detection

- **Severità**: Critica
- **Descrizione**: La presenza di una "bind shell" suggerisce un potenziale accesso remoto malevolo sul sistema. Questa vulnerabilità può consentire a un attaccante di ottenere un accesso persistente alla macchina compromessa.
- **Impatto**: Accesso continuo e non autorizzato alla macchina.
- **Rimedi**: Disabilitare i servizi non necessari come Telnet, analizzare il sistema per processi sospetti e reinstallare il sistema.



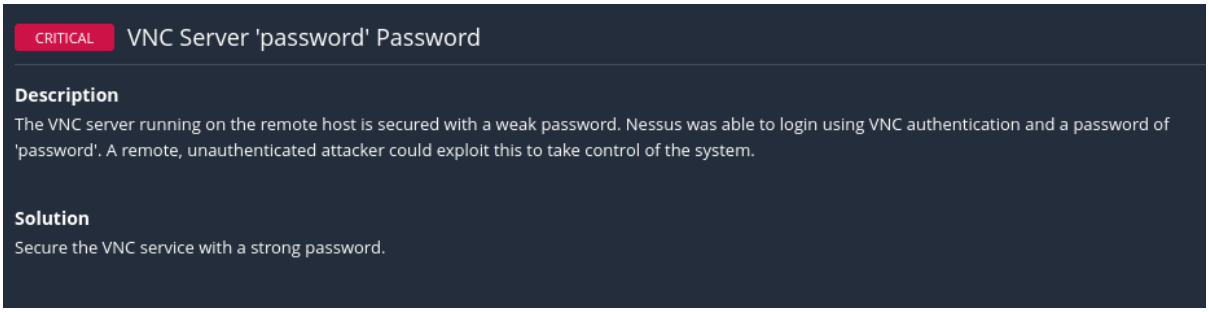
3. SSL Version 2 and 3 Protocol Detection

- **Severità**: Critica
- **Descrizione**: L'utilizzo dei protocolli SSL v2 e v3 è considerato insicuro e obsoleto, essendo vulnerabile a vari attacchi. La loro presenza espone il sistema a potenziali attacchi di tipo Man-in-the-Middle.
- **Impatto**: Rischio di decrittazione del traffico cifrato da parte di un attaccante.
- **Rimedi**: Disabilitare i protocolli SSL v2 e v3, e configurare solo TLS v1.2



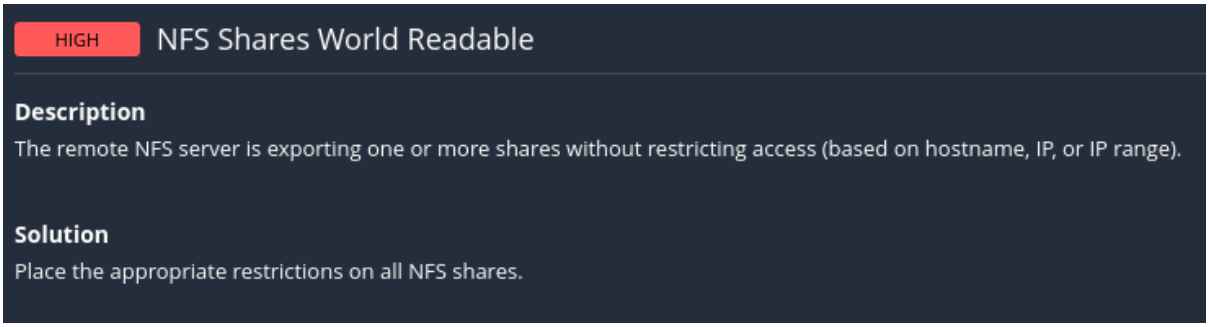
4. VNC Server ‘password’ Password

- **Severità**: Critica
- **Descrizione**: Questa vulnerabilità indica che l'accesso al server VNC è protetto da una password debole o di default, facilmente compromettibile.
- **Impatto**: Possibilità di accesso completo e non autorizzato alla sessione desktop del server.
- **Rimedi**: Sostituire la password con una più sicura e complessa



5. NFS Shares World Readable

- **Severità**: Alta
- **Descrizione**: Le condivisioni NFS configurate come leggibili da chiunque espongono potenzialmente file sensibili a tutti gli utenti della rete.
- **Impatto**: Rischio di divulgazione di informazioni riservate o sensibili.
- **Rimedi**: Limitare i permessi di lettura sulle condivisioni NFS e configurare l'accesso solo per utenti autorizzati.



Conclusione

La scansione ha evidenziato numerose vulnerabilità critiche e ad alto rischio, indicando la necessità di:

1. **Aggiornamenti di sicurezza**: Applicare patch e aggiornamenti di sicurezza.
2. **Password sicure**: Rimuovere le password di default, e sostituirle con password più forti.
3. **Restrizioni sull'accesso**: Limitare l'accesso ai servizi critici
4. **Rimozione di servizi non necessari**: Disabilitare servizi obsoleti e potenzialmente pericolosi come Telnet, se non necessari.

.