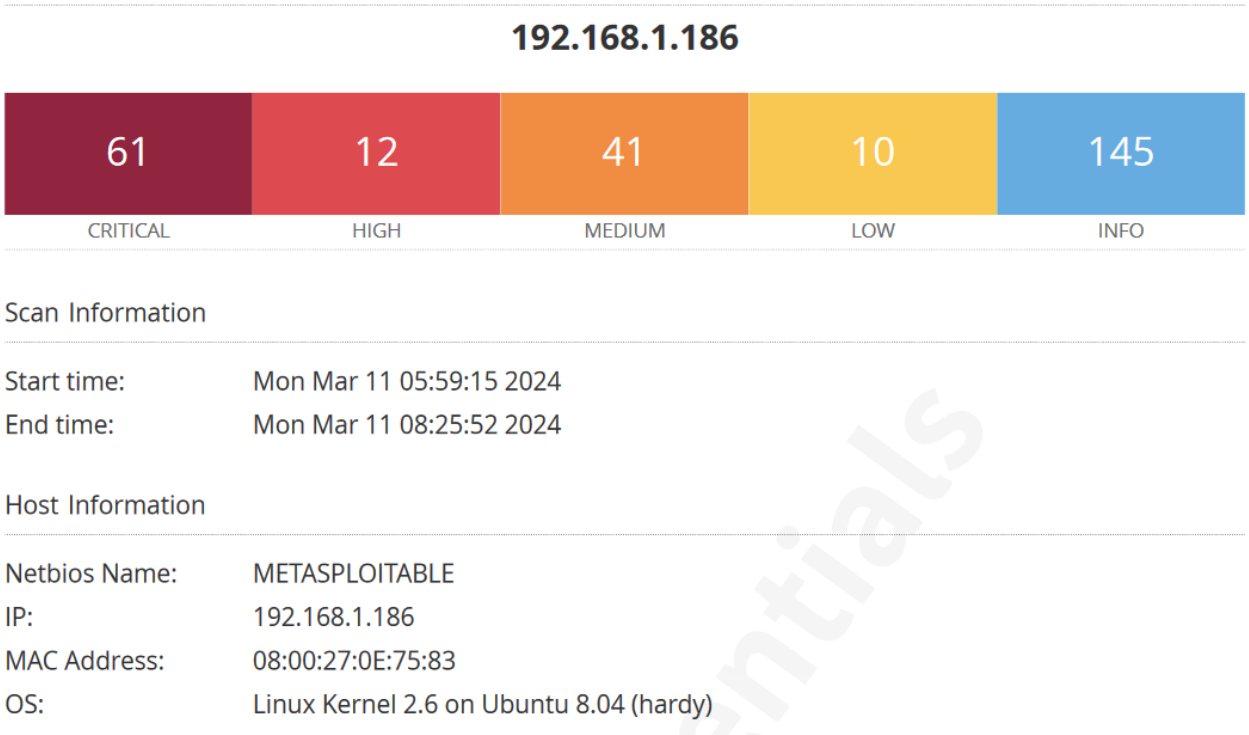
Report – M3W12D5 – Scansione Finale

Introduzione:
Obbiettivo di questa esercitazione è individuare tramite l'utilizzo del tool Nessus le vulnerabilità della macchina Metasploitable2, tra le critiche sceglierne un certo numero e implementare delle azioni di rimedio, infine effettuare una seconda scansione per verificarne l'efficacia.

Scansione Finale:
In questa fase dell'esercitazione verrà analizzata una seconda scansione della macchina Metasploitable2 effettuata con Nessus dopo aver eseguito le azioni di rimedio per valutare se sono state efficaci.
Nel caso che la vulnerabilità sia ancora presente si cercerà di speculare il motivo e di proporre una ulteriore azione di remediation.

Di seguito screenshot del riepilogo e della lista delle vulnerabilità critiche:

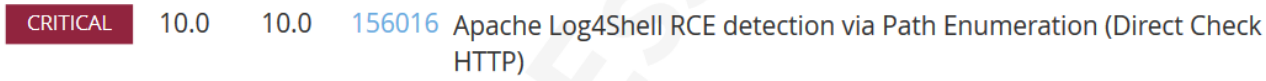


Vulnerabilities Total: 165

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	6.7	184080	PyTorch TorchServe SSRF (CVE-2023-43654)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	9.7	159375	Spring Cloud Function SPEL Expression Injection (direct check)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	9.0	8.1	156164	Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution
CRITICAL	10.0	10.0	156016	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
CRITICAL	10.0	10.0	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
CRITICAL	10.0	10.0	156257	Apache Log4Shell RCE detection via callback correlation (Direct Check DNS)
CRITICAL	10.0	10.0	156115	Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)
CRITICAL	10.0	10.0	156014	Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
CRITICAL	10.0	10.0	156669	Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC)
CRITICAL	10.0	10.0	156197	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)
CRITICAL	10.0	10.0	156559	Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND)
CRITICAL	10.0	10.0	156232	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)
CRITICAL	10.0	10.0	156166	Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)
CRITICAL	10.0	10.0	156162	Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection

Analisi: si nota subito che il numero delle vulnerabilità critiche si è ridotto, da 68 a 61 (anche se quello delle vulnerabilità elevate è aumentato da 9 a 12), quindi è ragionevole pensare che le azioni di remediation siano state corrette.
Rivediamole una ad una:

1.



Risultato: non essendo stati in grado di eseguire l'aggiornamento delle librerie Log4j compromesse, la vulnerabilità rimane presente sulla macchina.
Fortunatamente è ragionevole pensare che questa vulnerabilità possa essere risolta facilmente in un ambiente diverso da quello compromesso di Metasploitable2.

2.

Risultato: questa vulnerabilità non è più presente nella lista.
Quindi le azioni di remediation, e cioè la corretta configurazione del servizio di sharing remoto, sono state efficaci.

3.

Risultato: anche questa vulnerabilità è stata risolta e non è più comparsa nella scansione di Nessus grazie all'aggiornamento di una password molto debole e della corretta configurazione di iptables.

4.

Risultato: commentando la riga del file di configurazione che consentiva l'accesso alla shell non protetta è stata risolta anche questa vulnerabilità del sistema.

5.

Risultato: sfortunatamente questa vulnerabilità risulta essere ancora presente sulla macchina.
La configurazione di apache per disattivare i protocolli di codifica vulnerabili non è stata sufficiente, anche in questo caso l'utilizzo Metasploitable non consente l'installazione di protocolli più recenti, cosa che sarebbe sufficiente a risolvere la vulnerabilità.

Conclusione: delle 5 vulnerabilità critiche scelte, 3 sono state risolte correttamente e le rimanenti due possono essere considerate facilmente risolvibili in un ambiente di lavoro normale dove l'aggiornamento della macchina è possibile.