Report – M3W12D5 – Scansione Iniziale

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:
Il primo passaggio è quindi l'esecuzione di una scansione completa del target, assicurandoci di aver selezionato le impostazioni corrette come la scansione di tutte le porte e non soltanto quelle note e la scansione delle web vulnerabilities.
Dopo circa un'ora il risultato della scansione è il seguente:

192.168.1.187

68	9	26	8	136
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 4 12:21:56 2024
End time:	Mon Mar 4 13:14:12 2024

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.1.187
MAC Address:	08:00:27:0E:75:83
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Di seguito la lista delle vulnerabilità critiche rilevate:

CRITICAL	10.0	10.0	156232	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)
CRITICAL	10.0	10.0	156132	Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP)
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	-	171340	Apache Tomcat SEoL (<= 5.5.x)
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*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Vulnerabilities Total: 138

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	6.7	184080	PyTorch TorchServe SSRF (CVE-2023-43654)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	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)