

Nel esercizio di oggi ci è stato chiesto di effettuare un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni.

In pochi passi la spiegazione...

1. **Accedere a Nessus** e vai alla sezione **Discovery**.
2. Clicca su **Scan Type** e seleziona l'opzione **Custom** per configurare una scansione personalizzata.
3. Successivamente, seleziona **Port Scanning** come tipo di scansione da eseguire.
4. Nella sezione **Port Scan Range**, inserisci l'elenco delle porte che desideri scansionare (ad esempio, 21, 22, 23, 80, 443, ecc.). Puoi specificare un intervallo di porte o singole porte separate da virgola.
5. Dopo aver configurato tutti i parametri, **salva** la scansione.
6. Infine, **avvia** la scansione cliccando sul **Run** per avviare il processo di scansione delle porte.

Una volta che è stato effettuata la scansione cliccare in alto a destra Report ed infine, se si vuole il report semplice cliccare sulla prima opzione altrimenti per maggiori dettagli cliccare la seconda opzione.

Di seguito per comodità ho fatto la prima opzione:

INIZIO REPORT

192.168.64.24



Vulnerabilities						Total: 103
Severity	CVSS V3.0	VPR Score	EPSS Score	Plugin	Name	
CRITICAL	9.8	9.0	0.9741	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection	

PORTA 22 (SSH)

CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
192.168.64.24					5
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	10267	SSH Server Type and Version Information

PORTA 80 (HTTP)

MEDIUM	5.3	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information

PORTA 139 (NetBIOS)

INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
PORTA 25 (SMTP)					

MEDIUM	4.0*	7.3	0.0135	52611	SMTP Service STARTTLS Plaintext Command Injection
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support

PORTA 23 (TELNET)

MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
INFO	N/A	-	-	10281	Telnet Server Detection

PORTA 21 (FTP)

INFO	N/A	-	-	10092	FTP Server Detection
------	-----	---	---	-------	----------------------