Cyber Security Analyst

PROJECT REPORT

SCANSIONE CON NESSUS

Prepared by

Fulvio Zalateu

In risposta all'esercizio su: (vedi consegna nella pag. seguente)

Security Rookies

Traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l’advanced e poi configurarlo) A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all’interno dei report e/o con contenuto da Web. Gli obiettivi dell’esercizio sono: Fare pratica con lo strumento, con la configurazione e l’avvio delle scansioni Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester

Consegna:

• Report PDF per «tecnico» Report tecnico è inteso come "quasi completo" che va ad indicare sia le porte che la vulnerabilità che la risoluzione, in modo da poter intervenire. • Suggerimento: fare traduzione in italiano della descrizione e/o remediation

Configurazione del laboratorio virtuale

pfSense come Server DHCP Kali Linux su rete 192.168.1.0/24 Tutte le altre macchine su rete 192.168.50.0/24

Svolgimento

L’interfaccia di Nessus è semplice da utilizzare. Per eseguire una scansione, seguiamo questi passaggi:

1. Vai alla sezione Scans e clicca su New Scan.
2. Scegli la tipologia di scansione desiderata. Per questo esercizio, seleziona la scansione delle porte comuni:
   - Discovery > Port scan (common ports).
3. Inserisci il nome della scansione (es. "Scansione rete Metasploitable") e il target. In questo caso, utilizza l’intervallo di rete dove si trova Metasploitable2:
   - Rete target: 192.168.50.0/24
   - IP di Metasploitable2: 192.168.50.103

4. Una volta configurata la scansione, clicca su Save per salvare le impostazioni, e poi su Launch per avviarla.
Anche se scansionare l'intera rete (192.168.50.0/24) può richiedere più tempo rispetto alla scansione di una singola macchina (192.168.50.103), il vantaggio è che otterremo una panoramica completa di tutte le macchine presenti sulla rete.
Questo processo ci permette di individuare non solo le vulnerabilità su Metasploitable2, ma anche di vedere quali altri dispositivi sono attivi e vulnerabili sulla rete.

Report

192.168.50.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	1	27

Vulnerabilities Total: 31

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.8	-	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	-	106375	nginx HTTP Server Detection
INFO	N/A	-	-	106952	pfSense Detection
INFO	N/A	-	-	106198	pfSense Web Interface Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

GRAZIE