Cyber Security Analyst

PROJECT REPORT

SCANSIONE DEI SERVIZI CON NMAP parte 2

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

Prepared by

Fulvio Zalateu

Security Rookies

Consegna:

Si richiede allo studente di effettuare le scansioni dell’esercizio precedente con Nmap sul target Windows 7. Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report..

Configurazione laboratorio virtuale :

pfSense come Server DHCP Kali Linux su rete 192.168.1.0/24 Windows 7 su rete 192.168.50.0/24

Svolgimento

1. OS Fingerprinting (nmap -O)

sudo nmap -o 192.168.50.101

2. TCP Connect Scan (nmap -sT)

sudo nmap -sT 192.168.50.101

3. SYN Scan (nmap -sS)

sudo nmap -sS 192.168.50.101

4. Version Detection (nmap -sV)

sudo nmap -sV 192.168.50.101

Report di Scansione Nmap su Windows 7

Indirizzo IP: 192.168.50.101 Stato dell'host: Attivo (latenza: 0.0044s) Nome host: CORSO-PC Sistema Operativo: Microsoft Windows Embedded Standard 7 / Windows Phone 7.5 o 8.0 CPE: cpe:/o:microsoft, cpe:/o:microsoft Common Platform Enumeration, ed è uno standard utilizzato per identificare in modo univoco sistemi operativi, applicazioni e hardware

Porte Aperte e Servizi

Porta - Stato - Servizio - Versione/Descrizione

135/tcp Aperta msrpc Microsoft Windows RPC

139/tcp Aperta netbios-ssn Microsoft Windows netbios-ssn

445/tcp Aperta microsoft-ds Microsoft Windows 7 - 10, SMB (Workgroup: WORKGROUP)

5357/tcp Aperta http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

49152/tcp Aperta msrpc Microsoft Windows RPC

49153/tcp Aperta msrpc Microsoft Windows RPC

49154/tcp Aperta msrpc Microsoft Windows RPC

49155/tcp Aperta msrpc Microsoft Windows RPC

49156/tcp Aperta msrpc Microsoft Windows RPC

Rilevazione del Sistema Operativo

- Il sistema sembra essere Microsoft Windows Embedded Standard 7 o Windows Phone 7.5/8.0.
- L'identificazione del sistema operativo potrebbe non essere precisa a causa del numero insufficiente di porte aperte o chiuse, rendendo difficile una rilevazione affidabile.

GRAZIE