Cyber Security Analyst

PROJECT REPORT

SCANSIONE DEI SERVIZI CON NMAP parte 1

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

Prepared by

Fulvio Zalateu

Security Rookies

Consegna:

Tecniche di scansione con Nmap

Esercizio: Scansione dei servizi - Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable (target e attaccante devono essere su due reti diverse): ● OS fingerprint ● Syn Scan ● TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN? ● Version detection A valle delle scansioni, è prevista la produzione di un report contenente le seguenti info (dove disponibili): ● IP ● Sistema Operativo ● Porte Aperte ● Servizi in ascolto con versione ● Descrizione dei servizi

Configurazione laboratorio virtuale

pfSense come Server DHCP Kali Linux su rete 192.168.1.0/24 Metasploitable2 su rete 192.168.50.0/24

Svolgimento

Per ogni comando in nmap a discrezione si può inserire il flag -v per una modalità più dettagliata.

OS Fingerprinting

Per individuare il sistema operativo con nmap si utilizza il flag -O, richiede privilegi di amministratore. Si possono usare ulteriori opzioni.

nmap -O 192.168.50.100

La scansione, oltre a scansionare il sistema operativo, ha scansionato le porte aperte e riporta che ci sono 2 nodi di distanza tra l'attaccante e il target.

Syn Scan

La Syn Scan è una delle scansioni più comuni e veloci. Può essere eseguita in modalità stealth, invia pacchetti SYN senza stabilire una connessione completa (non completando l'handshake TCP). Utilizza il comando: nmap -sS 192.168.50.100 -sS: esegue una Syn Scan

TCP Connect Scan

La TCP Connect Scan utilizza il sistema operativo per completare il three-way handshake, quindi è meno furtiva della Syn Scan: nmap -sT 192.168.50.100 -sT: esegue una TCP Connect Scan

Version Detection

Per identificare le versioni dei servizi in esecuzione, usa la "version detection": nmap -sV 192.168.50.100 -sV: rileva la versione dei servizi in ascolto

Sono elencati in lista tutti i servizi con porta, nome servizio e versione

Report di scansione Nmap Meta

Informazioni

- IP del Target: 192.168.50.100
- Host: Metasploitable
- Stato Host: Up

Report di scansione Nmap Meta

Porta-Stato-Servizio

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

Dettagli sul Sistema Operativo: • Tipo di Dispositivo: General purpose • Sistema Operativo: Linux 2.6.X • Dettagli OS: Linux 2.6.15 - 2.6.26 (probabilmente embedded), Linux 2.6.29 (Gentoo)

2. TCP Connect Scan (nmap -sT -v)

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql

5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

Differenze rispetto a SYN Scan: • Entrambe le scansioni mostrano porte simili aperte. • Il TCP Connect Scan stabilisce una connessione completa, mentre il SYN Scan non la completa, rendendo il primo più visibile a un IDS.

3. SYN Scan (nmap -sS -v)

Porta-Stato-Servizio

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

4. Version Detection (nmap -sV -v)

Porta Stato Servizio Versione
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X 445/tcp open netbios-ssn Samba smbd 3.X - 4.X 512/tcp open exec netkit-rsh rexecd
513/tcp open login ?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ccproxy-ftp ?
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Conclusioni

Le scansioni hanno rivelato varie porte aperte e servizi in esecuzione su Metasploitable. Utilizzando TCP Connect, SYN e Version Detection ecc. abbiamo potuto osservare un quadro complessivo del sistema.

GRAZIE