EPICODE

ESERCIZIO W11D1

SCANSIONE DEI SERVIZI CON NMAP PT.1

Mungiovì Fabio

TASK

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
- 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

ESECUZIONE

Effettuiamo la scansione delle porte della macchina virtuale Metasploitable 2, con i seguenti comandi:

OS fingerprint `nmap -O 192.168.51.101`

Questo comando effettua una scansione per determinare il sistema operativo in uso sul target. Utilizza tecniche di fingerprinting per identificare il kernel e la versione del sistema operativo.

Syn Scan `nmap -sS 192.168.51.101`

La SYN Scan è una delle scansioni più comuni e veloci. Invia un pacchetto SYN (richiesta di connessione) e analizza la risposta per determinare se la porta è aperta, chiusa o filtrata. Non stabilisce una connessione completa, rendendola meno rilevabile.

TCP Scan `nmap -sT 192.168.51.101`

Questo comando stabilisce una connessione completa (3-way handshake) con il target per rilevare le porte aperte. È più lento e facilmente rilevabile rispetto alla SYN Scan, ma non richiede privilegi amministrativi.

Version Detection `nmap -sV 192.168.51.101`

La scansione di rilevamento versione identifica i servizi in ascolto e tenta di determinare la versione specifica del software in uso. Questo aiuta a individuare eventuali vulnerabilità note associate a quei servizi.

RISULTATI

IP: 192.168.51.101

Sistema Operativo: Linux 2.6.X

Network Distance: 2 hops

Porte Aperte: 23 porte rilevate

ANALISI PORTE APERTE RILEVATE

Porta	Stato	Servizio	Versione	Descrizione
21/tcp	Aperta	FTP	vsftpd 2.3.4	Servizio per il trasferimento di file. Versione vulnerabile.
22/tcp	Aperta	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Accesso remoto sicuro. Versione obsoleta e vulnerabile.
23/tcp	Aperta	Telnet	Linux telnetd	Protocollo di accesso remoto non sicuro.
25/tcp	Aperta	SMTP	Postfix smtpd	Servizio per l'invio di email.
53/tcp	Aperta	DNS	ISC BIND 9.4.2	Server DNS per la risoluzione di nomi di dominio.
80/tcp	Aperta	HTTP	Apache httpd 2.2.8 (Ubuntu DAV/2)	Server web.

Porta	Stato	Servizio	Versione	Descrizione
111/tcp	Aperta	RPC	RPC #100000	Servizio RPC per NFS.
139/tcp	Aperta	NetBIOS-SSN	Samba smbd 3.X - 4.X	Condivisione file su rete Windows.
445/tcp	Aperta	Microsoft-DS	Samba smbd 3.X - 4.X	Condivisione file su rete Windows.
512/tcp	Aperta	Exec	Netkit-rsh rexecd	Servizio remoto per l'esecuzione di comandi.
513/tcp	Aperta	Login	Netkit-rshd	Servizio remoto per l'accesso al sistema.
514/tcp	Aperta	Shell	-	Servizio remoto per la shell.
1099/tcp	Aperta	RMI Registry	GNU Classpath grmiregistry	Registro per Java Remote Method Invocation (RMI).
1524/tcp	Aperta	IngresLock	Metasploitable root shell	Accesso alla shell root vulnerabile.
2049/tcp	Aperta	NFS	RPC #100003	Network File System per la condivisione di file.
2121/tcp	Aperta	CCPROXY-FTP	-	Servizio FTP proxy.
3306/tcp	Aperta	MySQL	MySQL 5.0.51a-3ubuntu5	Database relazionale.
5432/tcp	Aperta	PostgreSQL	PostgreSQL DB 8.3.0 - 8.3.7	Database relazionale.
5900/tcp	Aperta	VNC	VNC (protocol 3.3)	Accesso remoto al desktop.
6000/tcp	Aperta	X11	-	Server grafico X11.
6667/tcp	Aperta	IRC	UnrealIRCd	Server chat IRC.
8009/tcp	Aperta	AJP13	Apache Jserv (Protocol v1.3)	Protocollo AJP per Apache Tomcat.
8180/tcp	Aperta	HTTP	Apache Tomcat/Coyote JSP engine 1.1	Server JSP per applicazioni web.