Report di scansione sul target Metasploitable

Ip attaccante: 192.168.50.100 (Kali – rete intnet)

Ip attaccato: 192.168.60.101 (Metasploitable – rete meta)

Sistema operativo del target individuato da nmap -O: Linux 2.6.15 – 2.6.26 (likely embedded)

Tabelle riassuntive su porte aperte riscontrate e i servizi in ascolto con la relativa versione

Porta	Proto	Stato	Servizio
21	tcp	open	ftp
22	tcp	open	ssh
23	tcp	open	telnet
25	tcp	open	smtp
53	tcp	open	domain
80	tcp	filtered	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

Porta	Servizio	Versione
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
23	telnet	Linux telnetd
25	smtp	Postfix smtpd
53	domain	ISC BIND 9.4.2
111	rpcbind	2 (RPC #100000)
139	netbios-ssn	Samba smbd 3.X - 4.X
445	netbios-ssn	Samba smbd 3.X - 4.X
512	exec	netkit-rsh rexecd
513	login	(unknown)
514	shell	Netkit rshd
1099	java-rmi	GNU Classpath grmiregistry
1524	bindshell	Metasploitable root shell
2049	nfs	2-4 (RPC #100003)
2121	ccproxy-ftp	(unknown)
3306	mysql	MySQL 5.0.51a-3ubuntu5
5432	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	vnc	VNC (protocol 3.3)
6000	X11	(access denied)
6667	irc	UnrealIRCd
8009	ajp13	Apache Jserv (Protocol v1.3)
8180	http	Apache Tomcat/Coyote JSP engine

Breve descrizione dei servizi trovati:

FTP (vsftpd 2.3.4): File Transfer Protocol, viene utilizzato per trasferire file tra computer su una rete, noto per sicurezza e velocità.

SSH (OpenSSH 4.7p1 Debian 8ubuntu1): Secure Shell, è un protocollo crittografico utilizzato per operazioni di rete sicure. Questa particolare versione di OpenSSH permette connessioni remote sicure, trasferimenti di file e l'esecuzione di comandi remoti.

Telnet (Linux telnetd): è un protocollo di rete che permette agli utenti di comunicare con un dispositivo remoto tramite una connessione testuale.

SMTP (Postfix smtpd): Il Simple Mail Transfer Protocol (SMTP) è utilizzato per inviare e ricevere e-mail. Postfix è un MTA (Mail Transfer Agent) che gestisce il trasferimento e la consegna delle e-mail.

Domain (ISC BIND 9.4.2): BIND è il software più utilizzato per i server DNS, responsabile della traduzione di nomi di dominio leggibili dall'uomo in indirizzi IP. ISC BIND 9.4.2 è una versione stabile e ampiamente implementata in molti sistemi.

RPCBind (2): detto anche Remote Procedure Call, permette l'esecuzione di codice in un'altra macchina remota.

NetBIOS-SSN (Samba smbd 3.X - 4.X): Samba è una suite di programmi che permette l'interoperabilità tra i sistemi Unix/Linux e Windows. Il servizio NetBIOS-SSN consente la condivisione di file e stampanti su reti Microsoft.

Exec (netkit-rsh rexecd): questo servizio permette l'esecuzione remota di comandi su un altro computer. Il servizio rexecd di netkit-rsh è utilizzato principalmente per scopi amministrativi e di scripting automatizzato.

Login (unknown): questo servizio consente l'accesso remoto a un sistema, simile a telnet.

Shell (Netkit rshd): un altro servizio per l'accesso remoto, rshd permette di eseguire comandi shell su un computer remoto senza richiedere una sessione interattiva completa.

Java-RMI (GNU Classpath grmiregistry): Remote Method Invocation, è una tecnologia Java che consente l'invocazione di metodi su oggetti remoti. GNU Classpath grmiregistry fornisce un registro per la gestione di tali oggetti remoti.

Bindshell (Metasploitable root shell): questo è un servizio ‘pericoloso’ che apre una shell di root sul sistema target, spesso utilizzato da aggressori per ottenere il controllo completo di un sistema compromesso.

NFS (2-4): Network File System consente di condividere file tra sistemi su una rete, facilitando la collaborazione e la gestione dei dati distribuiti.

CCProxy-FTP (unknown): questo è un server proxy per FTP, e consente di instradare le connessioni FTP attraverso il proxy per migliorare la sicurezza o la gestione della rete.

MySQL (5.0.51a-3ubuntu5): è un popolare sistema di gestione di database relazionali. È utilizzato per gestire database web e applicativi grazie alla sua efficienza e capacità di gestione di grandi quantità di dati.

PostgreSQL (8.3.0 - 8.3.7): è un avanzato sistema di gestione di database relazionali noto per la sua robustezza e la conformità agli standard SQL. Supporta funzionalità avanzate come le transazioni ACID e le estensioni procedurali.

VNC (protocol 3.3): Virtual Network Computing è un sistema di condivisione del desktop che consente di controllare un computer remoto come se si fosse seduti davanti ad esso. È utilizzato per il supporto remoto e la gestione dei sistemi.

X11: X11 è un sistema di finestre per interfacce grafiche sui sistemi Unix. Consente di eseguire applicazioni grafiche su macchine remote e visualizzarle localmente.

IRC (UnrealIRCd): Internet Relay Chat è un protocollo per la comunicazione in tempo reale. Risulta essere un'implementazione del server IRC nota per le sue estese funzionalità e la configurabilità.

AJP13 (Apache Jserv Protocol v1.3): è un protocollo binario che permette la comunicazione tra un server web Apache e il container di servlet Apache Tomcat, migliorando l'efficienza e la gestione delle richieste.

HTTP (Apache Tomcat/Coyote JSP engine): Apache Tomcat è un server web e container di servlet che esegue applicazioni web basate su Java. Il Coyote JSP engine gestisce le richieste JSP (JavaServer Pages), consentendo la generazione dinamica di contenuti web.

Differenze tra scansione TCP connect e SYN

Syn Scan (-sS)

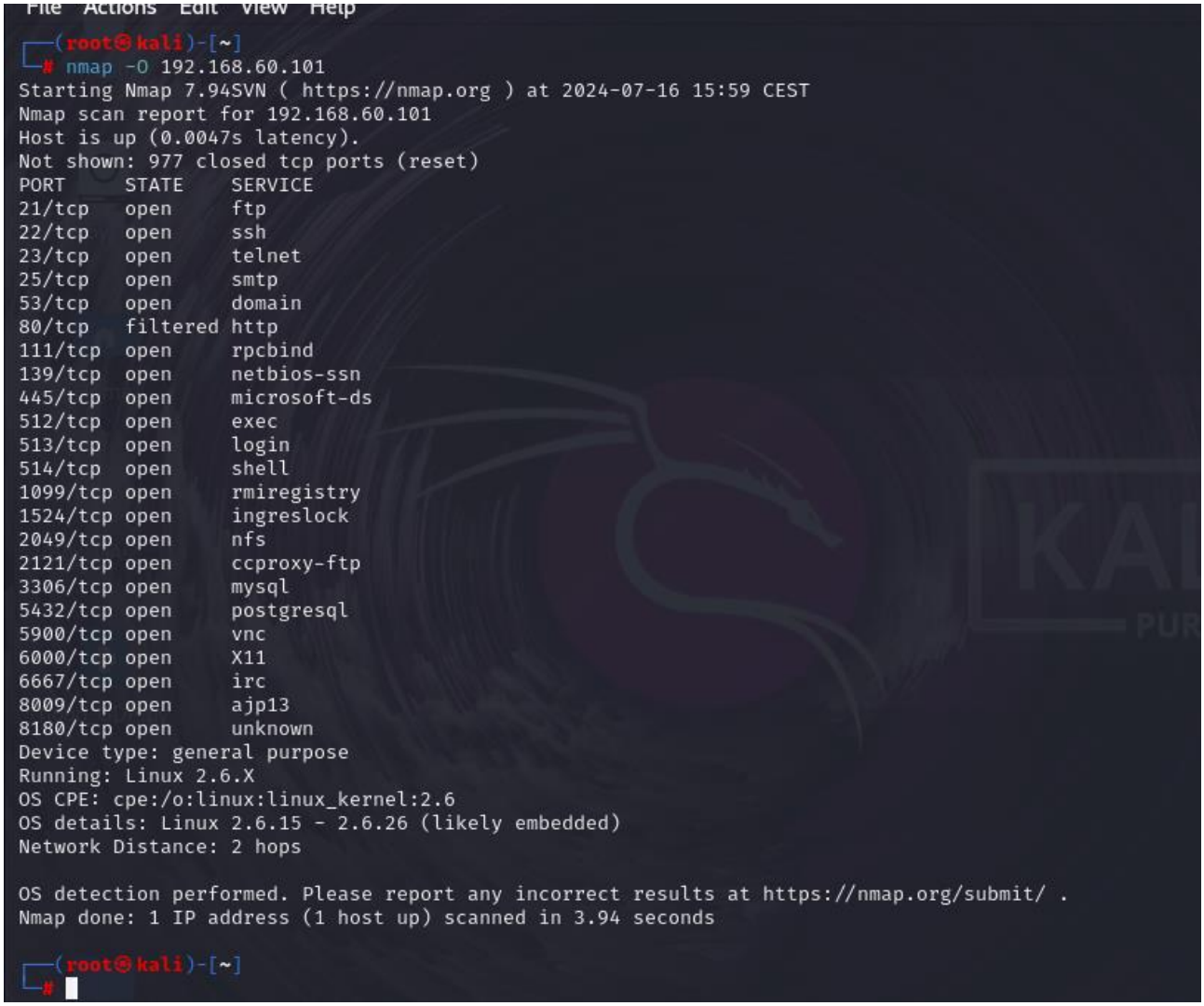
Il Syn Scan è una tecnica che invia pacchetti SYN alle porte del target e attende le risposte. Se la porta risponde con un SYN-ACK, significa che è aperta, mentre una risposta RST indica che è chiusa. Questo metodo è meno rilevabile dai sistemi di rilevamento delle intrusioni (IDS) perché non completa l'handshake TCP. Nei risultati del Syn Scan, le porte 21, 22, 23, 25, 53, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009 e 8180 sono risultate aperte, mentre la porta 80 è risultata filtrata.

TCP Connect Scan (-sT)

Il TCP Connect Scan, invece, completa l'handshake TCP per ogni porta, effettuando una connessione completa. Questo metodo funziona su qualsiasi sistema e non richiede privilegi di root, ma è più rilevabile dai sistemi IDS perché effettua una connessione completa. Nei risultati del TCP Connect Scan, le stesse porte 21, 22, 23,

25, 53, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009 e 8180 sono risultate aperte, e anche qui la porta 80 è risultata filtrata.

Entrambe le scansioni rilevano le stesse porte aperte e filtrate, ma il Syn Scan offre il vantaggio di essere meno rilevabile, mentre il TCP Connect Scan è più universale e non richiede privilegi speciali.



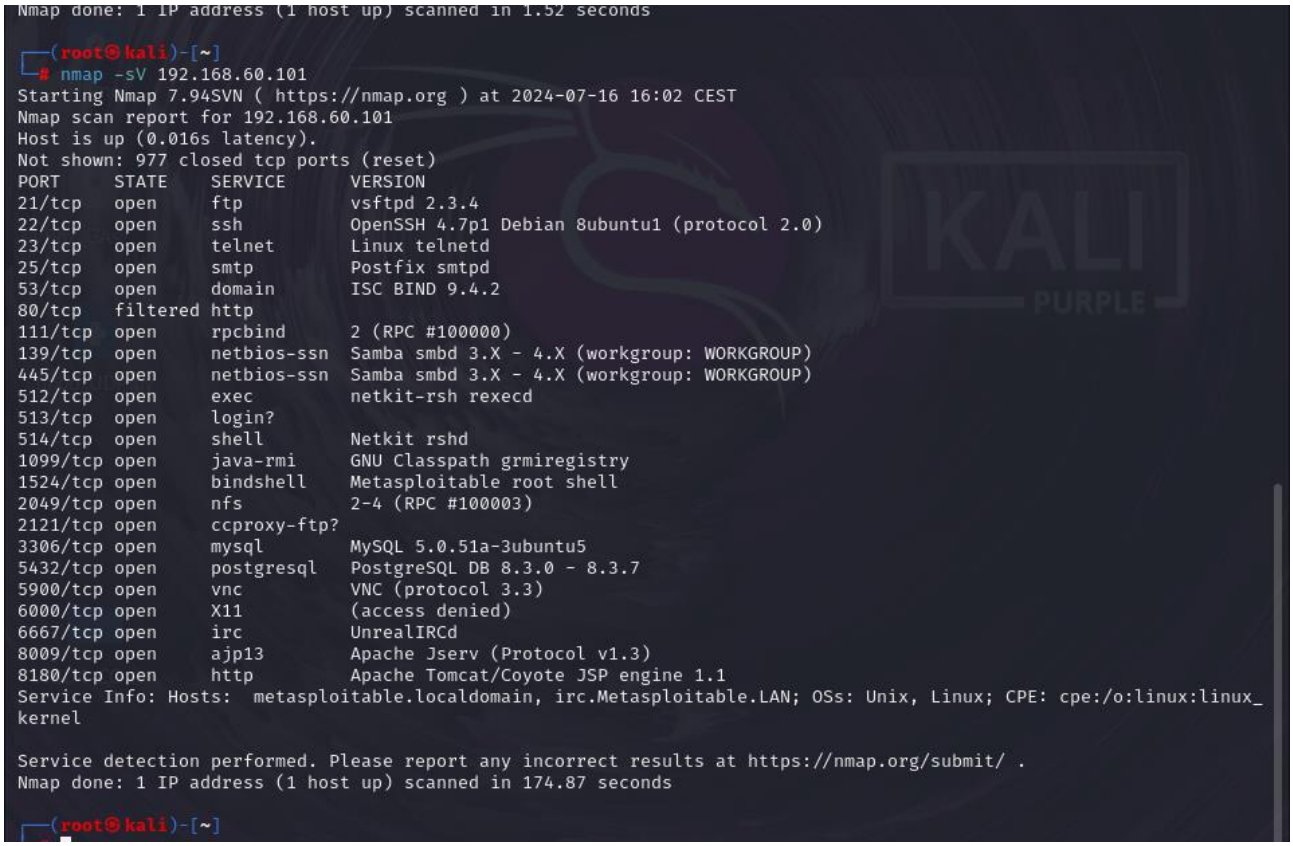
```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 16:01 CEST
Nmap scan report for 192.168.60.101
Host is up (0.022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 16:00 CEST
Nmap scan report for 192.168.60.101
Host is up (0.017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```


Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.60.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-16 16:02 CEST
Nmap scan report for 192.168.60.101
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp filtered http
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.87 seconds
┌──(root㉿kali)-[~]