RISULTATI SCANSIONI CON NMAP

METASPLOITABLE

OS FINGERPRINT

OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33

SYN SCAN

Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 14:15 CET
Nmap scan report for 192.168.50.101
Host is up (0.00095s 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 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
MAC Address: 08:00:27:1F:1E:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

TCP CONNECT SCAN

Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 14:17 CET
Nmap scan report for 192.168.50.101

Host is up (0.00045s 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 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
MAC Address: 08:00:27:1F:1E:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

DIFFERENZE TRA TCP CONNECT SCAN E SYN SCAN

Scannando la macchina Metasploitable con i due tipi di scan a livello di terminale non si notano grandi differenze, entrambi danno come risultati le porte aperte e i vari servizi associati.
A livello teorico però le principali differenze tra i due tipi di scan sono che il TCP Connect è una scansione più accurata che fa un completo three-way-handshake ed è quindi un po' più lenta e meno stealth.
Mentre il Syn Scan è più veloce e più stealth, ma a differenza del TCP Connect scan richiede i privilegi di root.

VERSION DETECTION

Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 14:19 CET
Nmap scan report for 192.168.50.101
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (conn-refused)

```
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   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 (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  ftp         ProFTPD 1.3.1
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 25.38 seconds
```

WINDOWS XP

OS FINGERPRINT

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 14:23 CET
Nmap scan report for 192.168.50.102
Host is up (0.00055s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2
(97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or
Windows XP SP0 - SP1 (95%), Microsoft Windows Server 2003 SP1 or SP2 (95%),
```

Microsoft Windows 2000 SP4 or Windows XP SP1a (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP SP3 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows 2000 Server SP3 or SP4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.73 seconds

REPORT FINALE

IP:

1. **METASPLOITABLE:** 192.168.50.101
2. **WINDOWS XP:** 192.168.50.102

SISTEMA OPERATIVO:

1. **METASPLOITABLE:** OS CPE: cpe:/o:linux:linux_kernel:2.6
   OS details: Linux 2.6.9 - 2.6.33
2. **WINDOWS:** Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP SP3 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows 2000 Server SP3 or SP4 (92%)

PORTE APERTE E SERVIZI CON VERSIONE:

1. **METASPLOITABLE:**

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	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 (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	ftp	ProFTPD 1.3.1
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

2. WINDOWS XP:

PORT	STATE	SERVICE	VERSION
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds

DIFFERENZE TRA SWITCH -g E -f

L'opzione `-g` di Nmap permette di specificare una porta sorgente personalizzata per i pacchetti inviati durante la scansione.

Normalmente, Nmap sceglie una porta casuale superiore a 1024 come porta sorgente. Tuttavia, con `-g`, possiamo impostare una porta fissa.

Funzionamento:

Nmap invierà i pacchetti SYN usando la porta scelta come porta sorgente.

L'opzione `-f` suddivide i pacchetti TCP in più frammenti di piccole dimensioni.

Questo rende più difficile per firewall e IDS analizzare e rilevare la scansione.