Rapporto di Rilevamento Rete / Vulnerabilità

Data: 29/04/2025

Operatore: Francesco Prisco

Dettagli del Target: Metasploitable

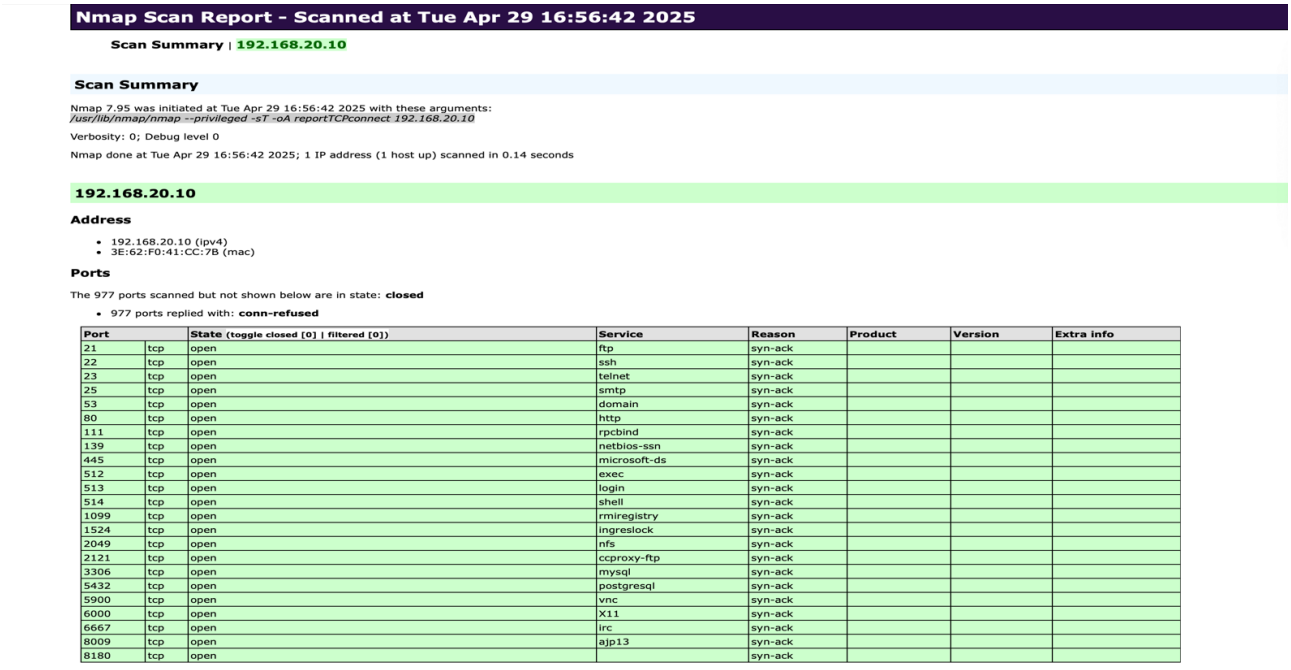
- **Indirizzo IP:** 192.168.20.10

Porte Aperte & Servizi Rilevati

Per scoprire le porte aperte e i servizi di questa macchina, ho usato i seguenti comandi:

- nmap -sT 192.168.20.10 (TCP Connect Scan)
- nmap -sS 192.168.20.10 (Syn Scan)

Entrambi mostrano le porte aperte e i servizi, ma con una differenza, il tcp connect scan completa il three-way handshake, mentre il syn no, infatti da come vediamo nelle immagini allegate qui sotto, il Syn Scan ha una risposta più veloce rispetto al TCP connect scan.



Nmap Scan Report - Scanned at Tue Apr 29 16:56:42 2025

Scan Summary | 192.168.20.10

Scan Summary

Nmap 7.95 was initiated at Tue Apr 29 16:56:42 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -sT -oA reportTCPconnect 192.168.20.10

Verbosity: 0; Debug level 0

Nmap done at Tue Apr 29 16:56:42 2025; 1 IP address (1 host up) scanned in 0.14 seconds

192.168.20.10

Address

- 192.168.20.10 (ipv4)
- 3E:62:F0:41:CC:7B (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **conn-refused**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack			
22	tcp	open	ssh	syn-ack			
23	tcp	open	telnet	syn-ack			
25	tcp	open	smtp	syn-ack			
53	tcp	open	domain	syn-ack			
80	tcp	open	http	syn-ack			
111	tcp	open	rpcbind	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
512	tcp	open	exec	syn-ack			
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack			
1099	tcp	open	rmiregistry	syn-ack			
1524	tcp	open	ingreslock	syn-ack			
2049	tcp	open	nfs	syn-ack			
2121	tcp	open	ccproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack			
5432	tcp	open	postgresql	syn-ack			
5900	tcp	open	vnc	syn-ack			
6000	tcp	open	X11	syn-ack			
6667	tcp	open	irc	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8180	tcp	open		syn-ack			

TCP Connect Scan

Nmap Scan Report - Scanned at Tue Apr 29 16:56:16 2025

Scan Summary | **192.168.20.10**

Scan Summary

Nmap 7.95 was initiated at Tue Apr 29 16:56:16 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -sS -oA reportSynScan 192.168.20.10

Verbosity: 0; Debug level 0

Nmap done at Tue Apr 29 16:56:16 2025; 1 IP address (1 host up) scanned in 0.18 seconds

192.168.20.10

Address

- 192.168.20.10 (ipv4)
- 3E:62:F0:41:CC:7B (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack			
22	tcp	open	ssh	syn-ack			
23	tcp	open	telnet	syn-ack			
25	tcp	open	smtp	syn-ack			
53	tcp	open	domain	syn-ack			
80	tcp	open	http	syn-ack			
111	tcp	open	rpcbind	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
512	tcp	open	exec	syn-ack			
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack			
1099	tcp	open	rmiregistry	syn-ack			
1524	tcp	open	ingreslock	syn-ack			
2049	tcp	open	nfs	syn-ack			
2121	tcp	open	ccproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack			
5432	tcp	open	postgresql	syn-ack			
5900	tcp	open	vnc	syn-ack			
6000	tcp	open	X11	syn-ack			
6667	tcp	open	irc	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8180	tcp	open		syn-ack			

Syn Scan

Rilevazione sistema operativo & versioni dei servizi aperti

Per scoprire il target che sistema operativo usa e che versione dei servizi ha sulle porte aperte ho usato i seguenti comandi:

- nmap -O 192.168.20.10 (OS fingerprint)
- nmap -sV 192.168.20.10 (Version Detection)

essendo che questi due possono essere comparati insieme, ho usato una sola istruzione:

- nmap -sV -O 192.168.20.10

192.168.20.10

Address

- 192.168.20.10 (ipv4)
- 3E:62:F0:41:CC:7B (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack	Netkit rshd		
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **36204/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

OS fingerprint e Version Detection

OS match: Linux 2.6.9 - 2.6.33 (100%)

Dettagli del Target: Windows 10

- **Indirizzo IP:** 192.168.20.12

Rilevazione sistema operativo

Per scoprire il target che sistema operativo ho usato il seguente comando:

- Nmap -O 192.168.20.12 (OS fingerprint)

192.168.20.12

Address

- 192.168.20.12 (ipv4)
- 76:81:41:C0:F0:5F (mac)

Ports

The 981 ports scanned but not shown below are in state: **closed**

- 981 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
7	tcp	open	echo	syn-ack			
9	tcp	open	discard	syn-ack			
13	tcp	open	daytime	syn-ack			
17	tcp	open	qotd	syn-ack			
19	tcp	open	chargen	syn-ack			
80	tcp	open	http	syn-ack			
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
1801	tcp	open	msmq	syn-ack			
2103	tcp	open	zephyr-clt	syn-ack			
2105	tcp	open	eklogin	syn-ack			
2107	tcp	open	msmq-mgmt	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
5357	tcp	open	wsdapi	syn-ack			
5432	tcp	open	postgresql	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8080	tcp	open	http-proxy	syn-ack			
8443	tcp	open	https-alt	syn-ack			

Remote Operating System Detection

- Used port: **7/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **43630/udp** (**closed**)
- OS match: **Microsoft Windows 10 1507 - 1607** (**100%**)

OS fingerprint

OS match: Microsoft Windows 10 1507 - 1607 (100%)