Nmap Scan Report - Scanned at Thu Jan 16 10:54:28 2025

Nmap Scan Report - Scanned at Thu Jan 16 10:54:28 2025

- Scan Summary
- | metasploitable (192.168.50.102)

Scan Summary

Nmap 7.95 was initiated at Thu Jan 16 10:54:28 2025 with these arguments: */usr/lib/nmap/nmap --privileged -oX syn_scan.xml -sS -r 192.168.50.102*

Verbosity: 0; Debug level 0

Nmap done at Thu Jan 16 10:54:29 2025; 1 IP address (1 host up) scanned in 0.27 seconds

---

192.168.50.102 / metasploitable(online)

Address

- 192.168.50.102 (ipv4)
- 00:0C:29:F9:38:81 - VMware (mac)

Hostnames

- metasploitable (PTR)

Ports

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

- 977 ports replied with: **reset**

Table 1:

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			

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response

Go to top
Toggle Closed Ports
Toggle Filtered Ports