Nmap Scan Report - Scanned at Thu Jan 16 11:04:23 2025

- Scan Summary
- | metasploitable (192.168.50.102)

Scan Summary

Nmap 7.95 was initiated at Thu Jan 16 11:04:23 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -oX scan.xml -A -r 192.168.50.102

Verbosity: 0; Debug level 0

Nmap done at Thu Jan 16 11:06:32 2025; 1 IP address (1 host up) scanned in 128.44 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**

Port		State [[(toggle closed [0]]{. small}]{.n oprint }[[| fi ltered [0])] {.smal l}]{.n oprint }	S ervice	Reason	P roduct	V ersion	Extra info
21	tcp	open	ftp	s yn-ack	v sftpd	2.3.4	

ftp-syst	STAT: FTP se rver status: Connected to 192.168.50.101 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection i s plai n text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable En d of status

	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
	ssh-hostkey	1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)					
23	tcp	open	t elnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		

	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN					
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
	dns-nsid	bind.version: 9.4.2					
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
	http-title	Metasploitable2 - Linux					
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					

111	tcp	open	rpcbind	syn-ack		2	RPC #100000

rp
cinfo

pr
ogram
versio
n p
ort/pr
oto s
ervice
10
0000 2
111/t
cp r
pcbind
10
0000 2
111/u
dp r
pcbind
1000
03 2,
3,4 20
49/tcp
nfs
1000
03 2,
3,4 20
49/udp
nfs
1
00005
1,2,3
38107/
tcp
mountd
1
00005
1,2,3
49853/
udp
mountd
100
021 1
,3,4 57
306/tc
p nl
ock-
mgr
100
021 1
,3,4 60
067/ud
p nl
ock-
mgr
1
00024

139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.0.20-Debian	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	

mysql-info	Protocol: 10 V**ersion** 5.0.51a-3ubuntu5 Thread ID: 361 Capabilities flags: 43564 Some Capabilities: ConnectWithDatabase, SupportsTransactions, SwitchToSSLAfterHandshake, Support41Auth, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression **Status** Autocommit Salt:

5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45				

	ssl-date	2025-01-16T16:08:03+00:00; +1m38s from scanner time.					
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
	vnc-info	Protocol version: 3.3 Security types: VNC Authentication (2)					
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
	ajp-methods	Failed to get a valid response for the OPTION request					

8180	tcp	open	http	syn-ack	Apache T omcat/Coyote JSP engine	1.1
	http-title	Apache Tomcat/5.5				
	http-favicon	Apache T omcat				

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **31244/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

Host Script Output

Script Name	Output
smb2-time	Protocol negotiation failed (SMB2)
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: , NetBIOS MAC: (unknown)
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain Syste m time: 2025-01-16T11:06:41-05:00
clock-skew	mean: 1h41m38s, deviation: 2h53m13s, median: 1m38s

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
System Uptime	59681 seconds (last reboot: Wed Jan 15 18:31:51 2025)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=201 (Good luck!)
IP ID Sequence Generation	All zeros

Go to top
Toggle Closed Ports
Toggle Filtered Ports