

Nmap Scan Report - Scanned at Tue Oct 15 17:14:47 2024

Scan Summary

Nmap 7.94SVN was initiated at Tue Oct 15 17:14:47 2024 with these arguments:
nmap -Pn -v -A --open -oA metaport 192.168.0.105

Verbosity: 1; Debug level 0

Nmap done at Tue Oct 15 17:16:50 2024; 1 IP address (1 host up) scanned in 126.37 seconds

192.168.0.105(online)

Address

- 192.168.0.105 (ipv4)
- 08:00:27:5A:48:AA - Oracle VirtualBox virtual NIC (mac)

Ports

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

- 977 ports replied with: **reset**

Port	State	Service	Reason	Product	Version
21	tcp	open	ftp	syn-ack	vsftpd
22	tcp	open	ssh	syn-ack	OpenSSH
	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	telnet	syn-ack	Linux telnetd
25	tcp	open	smtp	syn-ack	Postfix smtpd
	sslv2	SSLv2 supported ciphers: SSL2_DES_64_CBC_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5			
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/co Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/co Public Key type: rsa Public Key bits: 1024 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45 MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828 SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6			
	ssl-date	2024-10-15T21:17:06+00:00; +16s from scanner time.			
	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN			
53	tcp	open	domain	syn-ack	ISC BIND
	dns-nsid	bind.version: 9.4.2			
80	tcp	open	http	syn-ack	Apache httpd
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2			
	http-title	Metasploitable2 - Linux			
	http-methods	Supported Methods: GET HEAD POST OPTIONS			
111	tcp	open	rpcbind	syn-ack	2
139	tcp	open	netbios-ssn	syn-ack	Samba smbd
445	tcp	open	netbios-ssn	syn-ack	Samba smbd
512	tcp	open	exec	syn-ack	
513	tcp	open	login	syn-ack	OpenBSD or Solaris rlogind
514	tcp	open	shell	syn-ack	
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	
2121	tcp	open	ftp	syn-ack	ProFTPD
3306	tcp	open	mysql	syn-ack	MySQL
	mysql-info	Protocol: 10 Version: 5.0.51a-3ubuntu5 Thread ID: 9 Capabilities flags: 43564 Some Capabilities: SupportsCompression, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions Status: Autocommit Salt: _60,-;"4"M<'K&wKP.5_			
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB
	ssl-date	2024-10-15T21:17:05+00:00; +16s from scanner time.			
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/co Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/co Public Key type: rsa Public Key bits: 1024 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45			

MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6

5900	tcp	open	vnc	syn-ack	VNC	
	vnc-info	Protocol version: 3.3 Security types: VNC Authentication (2)				
6000	tcp	open	X11	syn-ack		
6667	tcp	open	irc	syn-ack	UnrealIRCd	
8009	tcp	open	ajp13	syn-ack	Apache Jserv	
	ajp-methods	Failed to get a valid response for the OPTION request				
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1
	http-methods	Supported Methods: POST OPTIONS				
	http-server-header	Apache-Coyote/1.1				
	http-title	Apache Tomcat/5.5				

Remote Operating System Detection

- Used port: **21/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **36375/udp (closed)**
- OS match: **Linux 2.6.9 - 2.6.33 (100%)**

Host Script Output

Script Name	Output
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown) Names: METASPLOITABLE<00> Flags: <unique><active> METASPLOITABLE<03> Flags: <unique><active> METASPLOITABLE<20> Flags: <unique><active> \\x01\\x02_MSBROWSE__\\x02<01> Flags: <group><active> WORKGROUP<00> Flags: <group><active> WORKGROUP<1d> Flags: <unique><active> WORKGROUP<1e> Flags: <group><active>
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
smb2-time	Protocol negotiation failed (SMB2)
clock-skew	mean: 15s, deviation: 0s, median: 15s

Misc Metrics

Metric	Value
Ping Results	arp-response
System Uptime	1483 seconds (last reboot: Tue Oct 15 16:52:07 2024)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=204 (Good luck!)
IP ID Sequence Generation	All zeros