Nmap Scan Report - Scanned at Sun Sep 15 07:59:23 2024

Scan Summary

Nmap 7.94SVN was initiated at Sun Sep 15 07:59:23 2024 with these arguments:
nmap -Pn -A -n -v -oA myscan 192.168.150.135

Verbosity: 1; Debug level 0

Nmap done at Sun Sep 15 07:59:43 2024; 1 IP address (1 host up) scanned in 20.15 seconds

192.168.150.135(online)

Address

- 192.168.150.135 (ipv4)
- 08:00:27:BB:47:56 - Oracle VirtualBox virtual NIC (mac)

Ports

The 994 ports scanned but not shown below are in state: **closed**

- 994 ports replied with: **reset**

Port	State		Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	2.9p2	protocol 1.99
		ssh-hostkey	1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1) 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA) 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)				
		sshv1	Server supports SSHv1				
80	tcp	open	http	syn-ack	Apache httpd	1.3.20	(Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
		http-title	Test Page for the Apache Web Server on Red Hat Linux				
		http-server-header	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b				
		http-methods	Supported Methods: GET HEAD OPTIONS TRACE Potentially risky methods: TRACE				
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
		rpcinfo	program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/udp rpcbind 100024 1 32768/tcp status 100024 1 32768/udp status				
139	tcp	open	netbios-ssn	syn-ack	Samba smbd		workgroup: 5MYGROUP
443	tcp	open	https	syn-ack	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b		
		ssl-date	2024-09-15T15:59:42+00:00; +3h59m59s from scanner time.				
		http-server-header	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b				
		http-title	400 Bad Request				
		ssl-cert	Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=-- Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=-- Public Key type: rsa Public Key bits: 1024 Signature Algorithm: md5WithRSAEncryption Not valid before: 2009-09-26T09:32:06 Not valid after: 2010-09-26T09:32:06 MD5: 78ce:5293:4723:e7fe:c28d:74ab:42d7:02f1 SHA-1: 9c42:91c3:bed2:a95b:983d:10ac:f766:ecb9:8766:1d33				
		sslv2	SSLv2 supported ciphers: SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC4_64_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5				
		http-methods	Supported Methods: GET HEAD POST				
32768	tcp	open	status	syn-ack		1	RPC #100024

Remote Operating System Detection

- Used port: **22/tcp** (**open**)

- Used port: **1/tcp** (**closed**)
- Used port: **30022/udp** (**closed**)
- OS match: **Linux 2.4.9 - 2.4.18 (likely embedded)** (**100%**)

Host Script Output

Script Name	Output
| nbstat | ```
NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Names:
  KIOPTRIX<00>          Flags: <unique><active>
  KIOPTRIX<03>          Flags: <unique><active>
  KIOPTRIX<20>          Flags: <unique><active>
  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
  MYGROUP<00>           Flags: <group><active>
  MYGROUP<1d>           Flags: <unique><active>
  MYGROUP<1e>           Flags: <group><active>
``` |
| smb2-time | Protocol negotiation failed (SMB2) |
| clock-skew | 3h59m58s |

Misc Metrics

Metric	Value
Ping Results	arp-response
System Uptime	1179 seconds (last reboot: Sun Sep 15 07:40:04 2024)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=202 (Good luck!)
IP ID Sequence Generation	All zeros