Nmap Scan Report - Scanned at Sun Sep 15 08:12:03 2024

Scan Summary

Nmap 7.94SVN was initiated at Sun Sep 15 08:12:03 2024 with these arguments:
nmap -Pn -A -n -v --script=vuln -oA myscan-vuln 192.168.150.135

Verbosity: 1; Debug level 0

Nmap done at Sun Sep 15 08:17:32 2024; 1 IP address (1 host up) scanned in 329.21 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
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-server-header	`Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b`					
	http-trace	`TRACE is enabled`					
	http-dombased-xss	`Couldn't find any DOM based XSS.`					
	http-stored-xss	`Couldn't find any stored XSS vulnerabilities.`					

	http-enum	`/test.php: Test page`
		`/icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'`
		`/manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'`
		`/usage/: Potentially interesting folder`					

	http-csrf	`Couldn't find any CSRF vulnerabilities.`					
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: MYGROUP
443	tcp	open	https	syn-ack	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b		
	sslv2-drown	`ERROR: Script execution failed (use -d to debug)`					
	http-dombased-xss	`Couldn't find any DOM based XSS.`					
	http-aspnet-debug	`ERROR: Script execution failed (use -d to debug)`					
	http-stored-xss	`Couldn't find any stored XSS vulnerabilities.`					
	http-server-header	`Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b`					

	ssl-poodle	`VULNERABLE:`
		`SSL POODLE information leak`
		`  State: VULNERABLE`
		`  IDs:  CVE:CVE-2014-3566  BID:70574`
		`        The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other`
		`        products, uses nondeterministic CBC padding, which makes it easier`
		`        for man-in-the-middle attackers to obtain cleartext data via a`
		`        padding-oracle attack, aka the "POODLE" issue.`
		`  Disclosure date: 2014-10-14`
		`  Check results:`
		`    TLS_RSA_WITH_3DES_EDE_CBC_SHA`
		`  References:`
		`    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566`
		`    https://www.openssl.org/~bodo/ssl-poodle.pdf`
		`    https://www.imperialviolet.org/2014/10/14/poodle.html`
		`    https://www.securityfocus.com/bid/70574`					

	http-csrf	`Couldn't find any CSRF vulnerabilities.`					

ssl-ccs-injection

```
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
  State: VULNERABLE
  Risk factor: High
    OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
    does not properly restrict processing of ChangeCipherSpec messages,
    which allows man-in-the-middle attackers to trigger use of a zero
    length master key in certain OpenSSL-to-OpenSSL communications, and
    consequently hijack sessions or obtain sensitive information, via
    a crafted TLS handshake, aka the "CCS Injection" vulnerability.

  References:
    http://www.cvedetails.com/cve/2014-0224
    http://www.openssl.org/news/secadv_20140605.txt
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
```

ssl-dh-params

```
VULNERABLE:
Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
  State: VULNERABLE
  IDs:  CVE:CVE-2015-4000  BID:74733
    The Transport Layer Security (TLS) protocol contains a flaw that is
    triggered when handling Diffie-Hellman key exchanges defined with
    the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
    to downgrade the security of a TLS session to 512-bit export-grade
    cryptography, which is significantly weaker, allowing the attacker
    to more easily break the encryption and monitor or tamper with
    the encrypted stream.
  Disclosure date: 2015-5-19
  Check results:
    EXPORT-GRADE DH GROUP 1
          Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
          Modulus Type: Safe prime
          Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus
          Modulus Length: 512
          Generator Length: 8
          Public Key Length: 512
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
    https://www.securityfocus.com/bid/74733
    https://weakdh.org

Diffie-Hellman Key Exchange Insufficient Group Strength
  State: VULNERABLE
    Transport Layer Security (TLS) services that use Diffie-Hellman groups
    of insufficient strength, especially those using one of a few commonly
    shared groups, may be susceptible to passive eavesdropping attacks.
  Check results:
    WEAK DH GROUP 1
          Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
          Modulus Type: Safe prime
          Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus
          Modulus Length: 1024
          Generator Length: 8
          Public Key Length: 1024
  References:
    https://weakdh.org
```

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: **33041/udp** (**closed**)
- OS match: **Linux 2.4.9 - 2.4.18 (likely embedded)** (**100%**)

Host Script Output

Script Name	Output
smb-vuln-ms10-054	`false`
samba-vuln-cve-2012-1182	`Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]`
smb-vuln-ms10-061	`Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]`

smb-vuln-cve2009-3103

```
VULNERABLE:
SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
  State: VULNERABLE
  IDs:  CVE:CVE-2009-3103
        Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
        Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
        denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
        PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
        aka "SMBv2 Negotiation Vulnerability."

  Disclosure date: 2009-09-08
  References:
    http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
```

Misc Metrics

Metric	Value
Ping Results	arp-response
System Uptime	2247 seconds (last reboot: Sun Sep 15 07:40:05 2024)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=196 (Good luck!)
IP ID Sequence Generation	All zeros