FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

ScanTest

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 2 | Vulnerabilities 20 | History 1

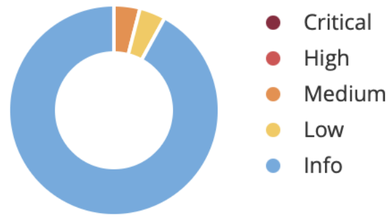
Filter | Search Hosts | 2 Hosts

Host	Vulnerabilities
192.168.1.28	1 30
192.168.1.43	1 10

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 3:56 PM
End:	Today at 4:06 PM
Elapsed:	10 minutes

Vulnerabilities



FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

New Scan / Basic Network Scan

Back to Scan Templates

Plugins are done compiling.

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

Settings | Credentials | Plugins

BASIC
- General
- Schedule
- Notifications

DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Name — REQUIRED

Description

Folder — My Scans

Targets — 192.168.1.28, 192.168.1.43

Upload Targets — Add File

Save | Cancel

Tenable News

OpenAI ChatGPT "Command Memories" Injection via Se...

Read More

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

My Scans

This folder is empty. Create a new scan.

Plugins are done compiling.

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: 192.168.1.28, 192.168.1.43

Close | Submit

Tenable News

OpenAI SearchGPT Results Tampering with Prompt Inj...

Read More

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

ScanTest / Plugin #57608

Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 17

MEDIUM **SMB Signing not required**

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.1.28

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 5.3

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.7

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/user]
└──╼ #sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 19:53 UTC
Nmap scan report for Docsis-Gateway (192.168.1.1)
Host is up (0.014s latency).
MAC Address: 94:4E:5B:64:6A:83 (Ubee Interactive, Limited)
Nmap scan report for 192.168.1.15
Host is up (0.050s latency).
MAC Address: 18:60:24:05:28:2F (Hewlett Packard)
Nmap scan report for 192.168.1.28
Host is up (0.065s latency).
MAC Address: 64:80:99:B9:04:1A (Intel Corporate)
Nmap scan report for Chris-s-S24 (192.168.1.43)
Host is up (0.11s latency).
MAC Address: C6:98:12:11:1A:AE (Unknown)
Nmap scan report for DAEDMAC01 (192.168.1.60)
Host is up (0.086s latency).
MAC Address: 70:AE:D5:40:A7:64 (Apple)
Nmap scan report for 192.168.1.65
Host is up (0.045s latency).
MAC Address: 7A:1E:41:4F:2D:DA (Unknown)
Nmap scan report for 192.168.1.77
Host is up (0.0012s latency).
```

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

ScanTest / 192.168.1.28

Back to Hosts

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 17

Filter | Search Vulnerabilities | 17 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not ...	Misc.	1
INFO	...	...	...	SMB (Multi...	Windows	6
INFO				DCE Services En...	Windows	8
INFO				Nessus SYN sca...	Port scanners	3
INFO				Common Platfor...	General	1
INFO				Device Type	General	1
INFO				Ethernet Card M...	Misc.	1
INFO				Ethernet MAC A...	General	1
INFO				Link-Local Multic...	Service detection	1
INFO				mDNS Detection...	Service detection	1

Host: 192.168.1.28

Host Details

IP:	192.168.1.28
MAC:	64:80:99:B9:04:1A
OS:	Microsoft Windows 10 Enterprise Microsoft Windows Server 2019 LTSC Microsoft Windows Server 2019
Start:	Today at 3:56 PM
End:	Today at 4:06 PM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities

Tenable News

OpenAI ChatGPT "Command Memories" Injection via Se...

Read More

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
└─# #ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.164  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2600:480a:3393:6900:f629:83d4:567b:a700  prefixlen 64  scopeid 0x0
<global>
        inet6 fe80::dd10:9e64:5bff:7dd9  prefixlen 64  scopeid 0x20<link>
        inet6 2600:480a:3393:6900::9e29  prefixlen 128  scopeid 0x0<global>
        ether de:df:d4:0a:5b:d9  txqueuelen 1000  (Ethernet)
        RX packets 569  bytes 64096 (62.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 925  bytes 66892 (65.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌─[root@parrot]─[/home/user]
└─# #sudo nmap -sn 192.168.1.0/24
```

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

ScanTest / Plugin #10114

Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 11

LOW **ICMP Timestamp Request Remote Date Disclosure**

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Output

```
The remote clock is synchronized with the local clock.
```

To see debug logs, please visit individual host

Port ▲	Hosts
0 / icmp	192.168.1.43

Plugin Details

Severity:	Low
ID:	10114
Version:	1.56
Type:	remote
Family:	General
Published:	August 1, 1999
Modified:	October 7, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 1.4
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 2.2
Exploit Prediction Scoring System (EPSS): 0.0037

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

My Scans

This folder is empty. Create a new scan.

Plugins are done compiling.

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Close | Submit

Tenable News

OpenAI SearchGPT Results Tampering with Prompt Inj...

Read More

tenable Nessus Essentials | Scans | Settings | craigsw86

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

My Scans

Import | New Folder | New Scan

This folder is empty. Create a new scan.

Tenable News

OpenAI SearchGPT Results Tampering with Prompt Inj...

Read More

« Back to Hosts

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

Vulnerabilities 11

Filter | Search Vulnerabilities | 11 Vulnerabilities

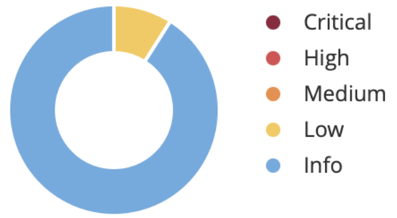
Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1 *	2.2	0.0037	ICMP Timestam...	General	1
INFO				Common Platfor...	General	1
INFO				Device Type	General	1
INFO				Ethernet MAC A...	General	1
INFO				Nessus Scan Inf...	Settings	1
INFO				Nessus SYN sca...	Port scanners	1
INFO				OS Fingerprints ...	General	1
INFO				OS Identification	General	1
INFO				TCP/IP Timesta...	General	1
INFO				Traceroute Infor...	General	1
INFO				Unknown Servic...	Service detection	1

Host: 192.168.1.43

Host Details

IP:	192.168.1.43
MAC:	C6:98:12:11:1A:AE
OS:	Linux Kernel 4.9
Start:	Today at 3:56 PM
End:	Today at 3:58 PM
Elapsed:	2 minutes
KB:	Download

Vulnerabilities



Tenable News

Progress WhatsUp Gold Unauthenticated Wireless MAC...

Read More