WIN 10

Report generated by Tenable Nessus™ Fri, 29 Aug 2025 14:25:01 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.2.108

0	0	0	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Aug 29 14:13:14 2025
End time: Fri Aug 29 14:25:01 2025

Host Information

IP: 192.168.2.108
MAC Address: 00:15:5D:1A:01:28

Vulnerabilities

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:15:5D:1A:01:28 : Microsoft Corporation
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:15:5D:1A:01:28
```

84047 - Hyper-V Virtual Machine Detection

Synopsis

The remote host is a Hyper-V virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a Microsoft Hyper-V virtual machine.

See Also

http://www.nessus.org/u?76f71a39

http://www.nessus.org/u?344a6879

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2015/06/09, Modified: 2025/07/14

Plugin Output

tcp/0

```
The remote host is a Hyper-V virtual machine.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508281914
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : WIN 10
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.2.101
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 138.698 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/8/29 14:13 EDT (UTC -04:00)
Scan duration : 696 sec
Scan for malware : no
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.2.101 to 192.168.2.108 :
192.168.2.101

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```