

# Hosts\_srv\_wks2\_physio

Sat, 08 Mar 2025 12:49:09 FLE Standard Time

## TABLE OF CONTENTS

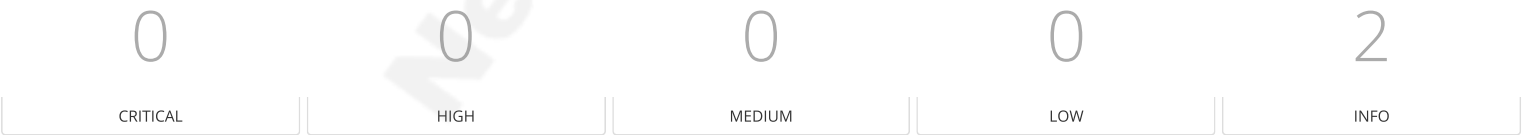
### Vulnerabilities by Host

- 192.168.100.1
- 192.168.100.2
- 192.168.100.11
- 192.168.100.100

## Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

### 192.168.100.1



### Scan Information

Start time:	Sat Mar 8 12:46:49 2025
End time:	Sat Mar 8 12:48:53 2025

### Host Information

IP:	192.168.100.1
-----	---------------

### Vulnerabilities

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- Whether the display of superseded patches is enabled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: 2024/12/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.8.3  
Nessus build : 20010  
Plugin feed version : 202503070251  
Scanner edition used : Nessus Home  
Scanner OS : WINDOWS  
Scanner distribution : win-x86-64  
Scan type : Normal  
Scan name : Hosts\_srv\_wks2\_physio  
Scan policy used : Host Discovery  
Scanner IP : 192.168.100.11

WARNING : No port scanner was enabled during the scan. This may lead to incomplete results.

Port range : default  
Ping RTT : 1.878 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 : no  
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Display superseded patches : yes (supersedence plugin did not launch)  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 : 2025/3/8 12:47 FLE Standard Time (UTC +02:00)  
Scan duration : 97 sec  
Scan for malware : no

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

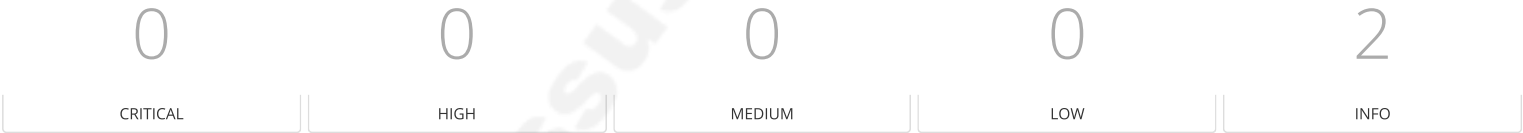
Published: 1999/06/24, Modified: 2025/02/25

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 00:50:56:c0:00:08
```

192.168.100.2



Scan Information

Start time: Sat Mar 8 12:46:49 2025  
End time: Sat Mar 8 12:48:32 2025

Host Information

IP: 192.168.100.2  
MAC Address: 00:50:56:E2:FF:C6

Vulnerabilities

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: 2024/12/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.8.3  
Nessus build : 20010  
Plugin feed version : 202503070251  
Scanner edition used : Nessus Home  
Scanner OS : WINDOWS  
Scanner distribution : win-x86-64  
Scan type : Normal  
Scan name : Hosts\_srv\_wks2\_physio  
Scan policy used : Host Discovery  
Scanner IP : 192.168.100.11

WARNING : No port scanner was enabled during the scan. This may lead to incomplete results.

Port range : default  
Ping RTT : 656.993 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 : no  
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 : 2025/3/8 12:47 FLE Standard Time (UTC +02:00)  
Scan duration : 75 sec  
Scan for malware : no

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2025/02/25

Plugin Output

tcp/0

The remote host is up  
The host replied to an ARP who-is query.  
Hardware address : 00:50:56:e2:ff:c6

192.168.100.11



Scan Information

Start time: Sat Mar 8 12:46:49 2025  
End time: Sat Mar 8 12:47:42 2025

Host Information

DNS Name: Server01.amidom.local  
IP: 192.168.100.11

Vulnerabilities

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: 2024/12/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.8.3  
Nessus build : 20010  
Plugin feed version : 202503070251  
Scanner edition used : Nessus Home  
Scanner OS : WINDOWS  
Scanner distribution : win-x86-64  
Scan type : Normal  
Scan name : Hosts\_srv\_wks2\_physio  
Scan policy used : Host Discovery  
Scanner IP : 192.168.100.11  
Ping RTT : Unavailable  
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 : no  
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 : 2025/3/8 12:47 FLE Standard Time (UTC +02:00)  
Scan duration : 18 sec  
Scan for malware : no

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

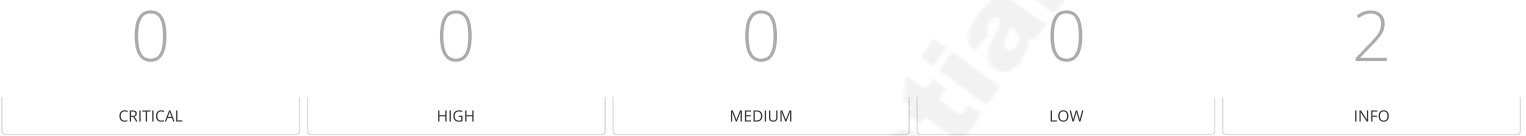
Published: 1999/06/24, Modified: 2025/02/25

Plugin Output

tcp/0

The remote host is up  
The host is the local scanner.

192.168.100.100



Scan Information

Start time: Sat Mar 8 12:47:20 2025  
End time: Sat Mar 8 12:49:09 2025

Host Information

IP: 192.168.100.100  
MAC Address: 00:0C:29:CF:4C:24

Vulnerabilities

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: 2024/12/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.8.3  
Nessus build : 20010  
Plugin feed version : 202503070251  
Scanner edition used : Nessus Home  
Scanner OS : WINDOWS  
Scanner distribution : win-x86-64  
Scan type : Normal  
Scan name : Hosts\_srv\_wks2\_physio  
Scan policy used : Host Discovery  
Scanner IP : 192.168.100.11

WARNING : No port scanner was enabled during the scan. This may lead to incomplete results.

Port range : default  
Ping RTT : 52.008 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 : no  
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 : 2025/3/8 12:47 FLE Standard Time (UTC +02:00)  
Scan duration : 102 sec  
Scan for malware : no

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2025/02/25

Plugin Output

tcp/0

The remote host is up  
The host replied to an ARP who-is query.  
Hardware address : 00:0c:29:cf:4c:24