tenable Nessus

Report generated by Tenable Nessus™

Photographer1

Tue, 10 Feb 2026 14:08:38 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.108

0	1	1	1	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Feb 10 14:06:18 2026
End time:	Tue Feb 10 14:08:38 2026

Host Information

Netbios Name:	PHOTOGRAPHER
IP:	192.168.0.108
MAC Address:	08:00:27:55:50:C4
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial), Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)

Vulnerabilities

42411 - Microsoft Windows SMB Shares Unprivileged Access -

Synopsis

It is possible to access a network share.

Description

The remote host has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, right click on each share, go to the 'Sharing' tab, and click on 'Permissions'.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	8026
CVE	CVE-1999-0519
CVE	CVE-1999-0520

Plugin Information

Published: 2009/11/06, Modified: 2025/02/26

Plugin Output

tcp/445/cifs

```
The following shares can be accessed using a NULL session :

- sambashare - (readable)
+ Content of this share :
..
mailsent.txt
wordpress.bkp.zip
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

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.

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

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.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

It is possible to determine the exact time set on the remote host.

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).

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

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

18261 - Apache Banner Linux Distribution Disclosure -

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

Plugin Output

tcp/0

```
The Linux distribution detected was :
- Ubuntu 16.04 (xenial)
- Ubuntu 16.10 (yakkety)
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80

```
URL : http://192.168.0.108/
Version : 2.4.99
Source : Server: Apache/2.4.18 (Ubuntu)
backported : 1
os : ConvertedUbuntu
```

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.18 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:jquery:jquery:1.11.3 -> jQuery
cpe:/a:samba:samba:4.3.11 -> Samba Samba
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 85
```

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 :

08:00:27:55:50:C4 : PCS Systemtechnik GmbH
```

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:
- 08:00:27:55:50:C4
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.4.18 (Ubuntu)
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Tue, 10 Feb 2026 14:07:31 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 21 Jul 2020 09:32:32 GMT
ETag: "164f-5aaf04d7cd1a0"
Accept-Ranges: bytes
Content-Length: 5711
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE HTML>
<!--
Photographer by v1n1v131r4
-->
<html>
<head>
<title>Photographer by v1n1v131r4</title>
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<link rel="stylesheet" href="assets/css/main.css" />
</head>
<body>

<!-- Header -->
<header id="header" class="alt">
<div class="logo"><a href="index.html">Photographer <span>by v1n1v131r4</span></a></div>
<a href="#menu">Menu</a>
</header>

<!-- Nav -->
<nav id="menu">
<ul class="links">
<li><a href="index.html">Home</a></li>
<li><a href="generic.html">Generic</a></li>
<li><a href="elements.html">Elements</a></li>
</ul>
</nav>

<!-- Banner -->
<section class="banner full">
<article>
<img src="images/slide01.jpg" alt="" />
<div class="inner">
<header>
<p>A prep OSCP machine by <a href="https://templated.co">v1n1v131r4</a></p>
<h2>Photographer</h2>
</header>
</div>
</article>
<article>
<img src="images/slide02.jpg" alt="" />
<div class="inner">
<header>
<p>Lorem ipsum dolor sit amet nullam feugiat</p>
<h2>Magna etiam</h2>
</header>
</div>
```

```
</article>
<article>
<img src="images/slide03.jpg" alt="" />
<div class="inner">
<header>
<p>Sed cursus aliuam veroeros lorem ipsum nullam</p>
<h2>Tempus dolor</h2>
</header>
</div>
</article>
<article>
<img src="images/slide04.jpg" alt="" />
<div class="inner">
<header>
<p>Adipiscing lorem ipsum feugiat sed phasellus consequat</p>
<h2>Etiam feugiat</h2>
</header>
</div>
</article>
<article>
<img src="images/slide05.jpg" alt="" />
<div class="inner">
<header>
<p>Ipsum dolor sed magna veroeros lorem ipsum</p>
<h2>Lorem adipiscing</h2>
</header>
</div>
</article>
</section>

<!-- One -->
<section id="one" class="wrapper style2">
<div class="inner">
<div class="grid-style">

<div>
<div class="box">
<div class="image fit">
<img src="images/pic02.jpg" alt="" />
</div>
<div class="content">
<header class="align-center">
<p>maecenas sapien feugiat ex purus</p>
<h2>Lorem ipsum dolor</h2>
</header>
<p> Cras aliquet urna ut sapien tincidunt, quis malesuada elit facilisis. Vestibulum sit amet tortor velit. Nam elementum nibh a
libero pharetra elementum. Maecenas feugiat ex purus, quis volutpat lacus placerat malesuada.</p>
<footer class="align-center">
<a href="#" class="button alt">Learn More</a>
</footer>
</div>
</div>
</div>

<div>
<div class="box">
<div class="image fit">
<img src="images/pic03.jpg" alt="" />
</div>
<div class="content">
<header class="align-center">
<p>mattis elementum sapien pretium tellus</p>
<h2>Vestibulum sit amet</h2>
</header>
<p> Cras aliquet urna ut sapien tincidunt, quis malesuada elit facilisis. Vestibulum sit amet tortor velit. Nam elementum nibh a
libero pharetra elementum. Maecenas feugiat ex purus, quis volutpat lacus placerat malesuada.</p>
<footer class="align-center">
<a href="#" class="button alt">Learn More</a>
</footer>
</div>
</div>
</div>

</div>
</div>
</section>

<!-- Two -->
<section id="two" class="wrapper style3">
<div class="inner">
<header class="align-center">
<p>Nam vel ante sit amet libero scelerisque facilisis eleifend vitae urna</p>
<h2>Morbi maximus justo</h2>
</header>
</div>
</section>

<!-- Three -->
<section id="three" class="wrapper style2">
<div class="inner">
<header class="align-center">
<p class="special">Nam vel ante sit amet libero scelerisque facilisis eleifend vitae urna</p>
<h2>Morbi maximus justo</h2>
</header>
<div class="gallery">
<div>
<div class="image fit">
<a href="#"><img src="images/pic01.jpg" alt="" /></a>
</div>
```

```
</div>
<div>
<div class="image fit">
<a href="#"><img src="images/pic02.jpg" alt="" /></a>
</div>
</div>
<div>
<div class="image fit">
<a href="#"><img src="images/pic03.jpg" alt="" /></a>
</div>
</div>
<div>
<div class="image fit">
<a href="#"><img src="images/pic04.jpg" alt="" /></a>
</div>
</div>
</div>
</div>
</section>


<!-- Footer -->
<footer id="footer">
<div class="container">
<ul class="icons">
<li><a href="#" class="icon fa-twitter"><span class="label">Twitter</span></a></li>
<li><a href="#" class="icon fa-facebook"><span class="label">Facebook</span></a></li>
<li><a href="#" class="icon fa-instagram"><span class="label">Instagram</span></a></li>
<li><a href="#" class="icon fa-envelope-o"><span class="label">Email</span></a></li>
</ul>
</div>
<div class="copyright">
&copy; Untitled. All rights reserved.
</div>
</footer>

<!-- Scripts -->
<script src="assets/js/jquery.min.js"></script>
<script src="assets/js/jquery.scrollex.min.js"></script>
<script src="assets/js/skel.min.js"></script>
<script src="assets/js/util.js"></script>
<script src="assets/js/main.js"></script>

</body>
</html>
```

106658 - JQuery Detection -

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80

```
URL : http://192.168.0.108/assets/js/jquery.min.js
Version : 1.11.3
```

17651 - Microsoft Windows SMB : Obtains the Password Policy -

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration -

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-3693138109-3993630114-3057792995

The value of 'RestrictAnonymous' setting is : unknown
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu
The remote SMB Domain Name is : PHOTOGRAPHER
```

11011 - Microsoft Windows SMB Service Detection -

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection -

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

60119 - Microsoft Windows SMB Share Permissions Enumeration -

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx
https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

Plugin Output

tcp/445/cifs

```
Share path : \\PHOTOGRAPHER\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
FILE_GENERIC_READ: YES
FILE_GENERIC_WRITE: YES
FILE_GENERIC_EXECUTE: YES

Share path : \\PHOTOGRAPHER\sambashare
Local path : C:\home\agi\share
Comment : Samba on Ubuntu
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
FILE_GENERIC_READ: YES
FILE_GENERIC_WRITE: YES
FILE_GENERIC_EXECUTE: YES

Share path : \\PHOTOGRAPHER\IPC$
Local path : C:\tmp
Comment : IPC Service (photographer server (Samba, Ubuntu))
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
FILE_GENERIC_READ: YES
FILE_GENERIC_WRITE: YES
FILE_GENERIC_EXECUTE: YES
```

10395 - Microsoft Windows SMB Shares Enumeration -

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host :

- print$
- sambashare
- IPC$
```

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
SMBv1
SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_ _introduced in windows version_
2.0.2 Windows 2008
2.1 Windows 7
2.2.2 Windows 8 Beta
```

```
2.2.4 Windows 8 Beta
3.0 Windows 8
3.0.2 Windows 8.1
3.1 Windows 10
3.1.1 Windows 10
```

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 : 202508200628
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Photographer1
Scan policy used : Advanced Scan
Scanner IP : 192.168.0.112
Port scanner(s) : nessus_syn_scanner
Port range : 65535
Ping RTT : 121.239 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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
```

```
Scan Start Date : 2026/2/10 14:06 UTC
Scan duration : 136 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected -

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 18.04 Linux Kernel 4.15
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Ubuntu 16.x
Confidence level : 85
Method : HTTP
Type : general-purpose
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W64240:O0204ffff:M1460:
P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191303_7_p=139
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Ubuntu 16.x
Confidence level : 85
Method : HTTP


The remote host is running Ubuntu 16.x
```

25240 - Samba Server Detection -

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

https://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

tcp/445/cifs

104887 - Samba Version -

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 4.3.11-Ubuntu
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Synopsis

The remote host supports the SMBv1 protocol.

Description

The remote host (Windows and/or Samba server) supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, most security and compliance agencies recommend that users disable SMBv1 per SMB best practices.

See Also

http://www.nessus.org/u?59bfc3ef
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2025/08/13

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

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 192.168.0.112 to 192.168.0.108 :
192.168.0.112
192.168.0.108

Hop Count: 1
```

135860 - WMI Not Available -

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2025/07/21

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure -

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 7 NetBIOS names have been gathered :

PHOTOGRAPHER = Computer name
PHOTOGRAPHER = Messenger Service
PHOTOGRAPHER = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Workgroup / Domain name
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

66717 - mDNS Detection (Local Network) -

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

- mDNS hostname : photographer.local.
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations