tenable Nessus

Report generated by Tenable Nessus™

Solstice

Tue, 17 Feb 2026 18:02:00 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.108

0	1	2	1	60
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Feb 17 17:45:11 2026
End time:	Tue Feb 17 18:02:00 2026

Host Information

Netbios Name:	SOLSTICE
IP:	192.168.0.108
MAC Address:	08:00:27:E4:C5:1C
OS:	Linux Kernel 2.6

Vulnerabilities

207864 - CUPS cups-browsed Remote Unauthenticated Printer Registration (CVE-2024-47176) -

Synopsis

The remote web server is a CUPS server and responds to untrusted requests.

Description

The cups-browsed server running on the remote host trusts any well formatted packet received and responds to a potentially attacker controlled URL. A remote, unauthenticated attacker can exploit this vulnerability to solicit information and, combined with other CVEs, achieve RCE.

See Also

http://www.nessus.org/u?ebf4de66

http://www.nessus.org/u?03d62753

Solution

Upgrade to the latest available version or apply the recommended security patch per the vendor advisory.

Risk Factor

High

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

4.9 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:F/RL:OF/RC:C)

References

CVE	CVE-2024-47176

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/09/27, Modified: 2025/07/14

Plugin Output

tcp/631

```
Nessus was able to exploit the vulnerability by sending a CUPS Browsing Protocol packet to the remote host.

The host then responded on the out of band port with:

POST /printers/it3oZN HTTP/1.1
Content-Length: 184
Content-Type: application/ipp
Date: Tue, 17 Feb 2026 17:48:49 GMT
Host: 192.168.0.111:39189
User-Agent: CUPS/2.2.10 (Linux 4.19.0-8-amd64; x86_64) IPP/2.0
Expect: 100-continue

.
```

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

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) -

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
  Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
  Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
  Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
  Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
  Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
  Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
  Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
  Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
  Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
  Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
  Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
  Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```

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 difference between the local and remote clocks is 1 second.
```

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/www

```
URL : http://192.168.0.108/
Version : 2.4.99
Source : Server: Apache/2.4.38 (Debian)
backported : 1
os : ConvertedDebian
```

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH 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/22/ssh

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

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/www

```
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

```
The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.38 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:openbsd:openssh:7.9 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:7.9p1 -> OpenBSD OpenSSH
cpe:/a:samba:samba:4.9.5 -> Samba Samba
cpe:/a:squid-cache:squid:4.6 -> squid-cache.org Squid
```

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 : 65
```

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:E4:C5:1C : 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:E4:C5:1C
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
  The remote FTP banner is :

  220 pyftpdlib 1.5.6 ready.
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/2121/ftp

```
  The remote FTP banner is :

  220 pyftpdlib 1.5.6 ready.
```

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/www

```
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/www

```
The remote web server type is :

Apache/2.4.38 (Debian)
```

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/3128/http_proxy

```
The remote web server type is :

squid/4.6
```

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/www

```
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, 17 Feb 2026 17:47:01 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Thu, 25 Jun 2020 14:45:19 GMT
ETag: "128-5a8e9a431c517"
Accept-Ranges: bytes
Content-Length: 296
```

```
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<head>
Currently configuring the database, try later.
<style type ="text/css" >
.footer{
position: fixed;
text-align: center;
bottom: 0px;
width: 100%;
}
</style>
</head>
<body>
<div class="footer">Proudly powered by phpIPAM 1.4</div>
</body>
```

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/3128/http_proxy

```
Response Code : HTTP/1.1 400 Bad Request

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

Server: squid/4.6
Mime-Version: 1.0
Date: Tue, 17 Feb 2026 17:47:01 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3505
X-Squid-Error: ERR_INVALID_URL 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from localhost
X-Cache-Lookup: NONE from localhost:3128
Via: 1.1 localhost (squid/4.6)
Connection: close

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2018 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
/*
* Copyright (C) 1996-2019 The Squid Software Foundation and contributors
*
* Squid software is distributed under GPLv2+ license and includes
* contributions from numerous individuals and organizations.
* Please see the COPYING and CONTRIBUTORS files for details.
*/
```

```
/*
Stylesheet for Squid Error pages
Adapted from design by Free CSS Templates
http://www.freecsstemplates.org
Released for free under a Creative Commons Attribution 2.5 License
*/

/* Page basics */
* {
font-family: verdana, sans-serif;
}

html body {
margin: 0;
padding: 0;
background: #efefef;
font-size: 12px;
color: #1e1e1e;
}

/* Page displayed title area */
#titles {
margin-left: 15px;
padding: 10px;
padding-left: 100px;
background: url('/squid-internal-static/icons/SN.png') no-repeat left;
}

/* initial title */
#titles h1 {
color: #000000;
}
#titles h2 {
color: #000000;
}

/* special event: FTP success page titles */
#titles ftpsuccess {
background-color:#00ff00;
width:100%;
}

/* Page displayed body content area */
#content {
padding: 10px;
background: #ffffff;
}

/* General text */
p {
}

/* error brief description */
#error p {
}

/* some data which may have caused the problem */
#data {
}

/* the error message received from the system or other software */
#sysmsg {
}

pre {
}

/* special event: FTP / Gopher directory listing */
#dirmsg {
font-family: courier, monospace;
color: black;
font-size: 10pt;
}
#dirlisting {
margin-left: 2%;
margin-right: 2%;
}
#dirlisting tr.entry td.icon,td.filename,td.size,td.date {
border-bottom: groove;
}
#dirlisting td.size {
width: 50px;
text-align: right;
padding-right: 5px;
}

/* horizontal lines */
hr {
margin: 0;
}

/* page displayed footer area */
#footer {
font-size: 9px;
padding-left: 10px;
}


body
```

```
:lang(fa) { direction: rtl; font-size: 100%; font-family: Tahoma, Roya, sans-serif; float: right; }
:lang(he) { direction: rtl; }
--></style>
</head><body id=ERR_INVALID_URL>
<div id="titles">
<h1>ERROR</h1>
<h2>The requested URL could not be retrieved</h2>
</div>
<hr>

<div id="content">
<p>The following error was encountered while trying to retrieve the URL: <a href="/">/</a></p>

<blockquote id="error">
<p><b>Invalid URL</b></p>
</blockquote>

<p>Some aspect of the requested URL is incorrect.</p>

<p>Some possible problems are:</p>
<ul>
<li><p>Missing or incorrect access protocol (should be <q>http://</q> or similar)</p></li>
<li><p>Missing hostname</p></li>
<li><p>Illegal double-escape in the URL-Path</p></li>
<li><p>Illegal character in hostname; underscores are not allowed.</p></li>
</ul>

<p>Your cache administrator is <a href="mailto:webmaster?subject=CacheErrorInfo%20-
%20ERR_INVALID_URL&amp;body=CacheHost%3A%20localhost%0D%0AErrPage%3A%20ERR_INVALID_URL%0D%0AErr%3A%20%5Bnone%5D%0D%0ATimeStamp%3A%20
Tue,%2017%20Feb%202026%2017%3A47%3A01%20GMT%0D%0A%0D%0AClientIP%3A%20192.168.0.111%0D%0A%0D%0AHTTP%20Request%3A%0D%0A%0D%0A%0D%0A">w
ebmaster</a>.</p>
<br>
</div>

<hr>
<div id="footer">
<p>Generated Tue, 17 Feb 2026 17:47:01 GMT by localhost (squid/4.6)</p>
<!-- ERR_INVALID_URL -->
</div>
</body></html>
```

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-1-5-21-1049045055-609373089-4176931349

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 4.9.5-Debian
The remote SMB Domain Name is : SOLSTICE
```

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 : \\SOLSTICE\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 : \\SOLSTICE\IPC$
Local path : C:\tmp
Comment : IPC Service (Samba 4.9.5-Debian)
[*] 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$
- 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
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2121/ftp

```
  Port 2121/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/3128/http_proxy

```
  Port 3128/tcp was found to be open
```

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 : Solstice
Scan policy used : Advanced Scan
Scanner IP : 192.168.0.111
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 323.683 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 : 2026/2/17 17:45 UTC
Scan duration : 998 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 : 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

Following fingerprints could not be used to determine OS :
SSH:!:SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
HTTP:!:Server: Apache/2.4.38 (Debian)

SMTP:!:220 solstice ESMTP Exim 4.92 Tue, 17 Feb 2026 12:45:16 -0500
```

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 : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:!:SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SinFP:
P1:B10113:F0x12:W64240:O0204ffff:M1460:
P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191303_7_p=139
HTTP:!:Server: Apache/2.4.38 (Debian)

SMTP:!:220 solstice ESMTP Exim 4.92 Tue, 17 Feb 2026 12:45:16 -0500


The remote host is running Linux Kernel 2.6
```

117886 - OS Security Patch Assessment Not Available -

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

- Plugin : no_local_checks_credentials.nasl
Plugin ID : 110723
Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
Message :
Credentials were not provided for detected SSH service.
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.9p1
Banner : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

```
. You need to take the following action :

[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.
```

10263 - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 solstice ESMTP Exim 4.92 Tue, 17 Feb 2026 12:45:16 -0500
```

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```

Nessus negotiated the following encryption algorithm(s) with the server :

Client to Server: aes256-ctr
Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for kex_algorithms :

curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
```

```
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH supported authentication : publickey,password
```

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 4.9.5-Debian
```

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.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/25/smtp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2121/ftp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/3128/http_proxy

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

tcp/3128/http_proxy

```
An HTTP proxy is running on this port.
```

49692 - Squid Proxy Version Detection -

Synopsis

It was possible to obtain the version number of the remote Squid proxy server.

Description

The remote host is running the Squid proxy server, an open source proxy server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/09/28, Modified: 2024/06/17

Plugin Output

tcp/3128/http_proxy

```
URL : http://192.168.0.108:3128/
Version : 4.6
Source : Server: squid/4.6
```

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

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

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 192.168.0.111 to 192.168.0.108 :
192.168.0.111
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 :

SOLSTICE = Computer name
SOLSTICE = Messenger Service
SOLSTICE = 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 : solstice.local.

- Advertised services :
o Service name : SOLSTICE._smb._tcp.local.
Port number : 445
o Service name : SOLSTICE._device-info._tcp.local.
Port number : 0
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

Suggested Remediations