



STEPES-TR

Report generated by Nessus™

Fri, 04 Dec 2020 09:04:08 EST

TABLE OF CONTENTS

Vulnerabilities by Host

• 35.199.110.191.....	4
• 54.196.179.100.....	35

Nessus Essentials

Vulnerabilities by Host

35.199.110.191



Scan Information

Start time: Fri Dec 4 08:38:31 2020

End time: Fri Dec 4 08:46:41 2020

Host Information

DNS Name: 191.110.199.35.bc.googleusercontent.com

IP: 35.199.110.191

OS: Linux Kernel 4.15 on Ubuntu 18.04 (bionic)

Vulnerabilities

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: 2020/11/17

Plugin Output

tcp/0

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

```
cpe:/o:canonical:ubuntu_linux:18.04 -> Canonical Ubuntu Linux 18.04
```

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

```
cpe:/a:openbsd:openssh:7.6
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 95
```

11919 - HMAP Web Server Fingerprinting

Synopsis

HMAP fingerprints the remote HTTP server.

Description

Nessus was able to identify the remote web server type by sending several valid and invalid HTTP requests. In some cases, its version can also be approximated, as well as some options.

See Also

<http://www.nessus.org/u?05d4ce87>

<http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf>

<http://projects.webappsec.org/w/page/13246925/Fingerprinting>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/11/11, Modified: 2020/06/12

Plugin Output

tcp/9000/www

```
Nessus was not able to exactly identify this server. It might be :
```

```
Microsoft-IIS/5 (OWA on Exchange 5.5)
```

```
The fingerprint differs from the known signatures on 3 point(s).
```

```
If you know what this server is and if you are using an up to date version  
of this script, please send this signature to www-signatures@nessus.org :
```

```
400:400:200:400:400:400:400:400:400:400:400:404:404:404:404:404:200:404:: [R]  
Including these headers :
```

```
X-Content-Type-Options: nosniff  
X-Xss-Protection: 1; mode=block
```

```
Try to provide as much information as you can - software & operating  
system release, sub-version, patch numbers, and specific configuration  
options, if any.
```


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_\(OTG-CONFIG-006\)](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: 2019/03/19

Plugin Output

tcp/9000/www

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY
OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
35.199.110.191 resolves as 191.110.199.35.bc.googleusercontent.com.
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/9000/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Accept-Ranges: bytes

Cache-Control: max-age=31536000

Content-Length: 23167

Content-Type: text/html; charset=utf-8

Last-Modified: Mon, 31 Aug 2020 09:04:27 GMT

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Date: Fri, 04 Dec 2020 13:43:14 GMT

Connection: close

Response Body :

<!DOCTYPE html

><html lang="en" ng-app="portainer">

<head>

<meta charset="utf-8" />

<title>Portainer</title>

<meta name="description" content="" />

<meta name="author" content="Portainer.io" />

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

None

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

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

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

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.
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

<http://www.nessus.org/u?55aa8f57>

<http://www.nessus.org/u?07cc2a06>

<https://content-security-policy.com/>

<https://www.w3.org/TR/CSP2/>

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2018/11/15

Plugin Output

tcp/9000/www

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy:

- <http://191.110.199.35.bc.googleusercontent.com:9000/>

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

<https://en.wikipedia.org/wiki/Clickjacking>

<http://www.nessus.org/u?399b1f56>

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2017/05/16

Plugin Output

tcp/9000/www

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- <http://191.110.199.35.bc.googleusercontent.com:9000/>

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: 2020/09/14

Plugin Output

tcp/22/ssh

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

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: 2020/09/14

Plugin Output

tcp/9000/www

```
Port 9000/tcp was found to be open
```

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.
- 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: 2020/08/27

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 8.12.1  
Plugin feed version : 202012041017  
Scanner edition used : Nessus Home  
Scan type : Normal  
Scan policy used : Advanced Scan  
Scanner IP : 192.168.0.32  
Port scanner(s) : nessus_syn_scanner  
Port range : default  
Thorough tests : no  
Experimental tests : no
```

```
Paranoia level : 1
Report verbosity : 1
Safe checks : no
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : some_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : never
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/12/4 8:38 EST
Scan duration : 467 sec
```

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: 2020/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
Confidence level : 95
Method : SSH
```

```
The remote host is running Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
```

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may have been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.
- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2020/09/22

Plugin Output

tcp/0

Port 22 was detected as being open but is now unresponsive

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: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :
```

```
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 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 encryption_algorithms_server_to_client :

```
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_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 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 compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib@openssh.com
```

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: 2020/02/18

Plugin Output

tcp/22/ssh

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

```
- 2.0
```

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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
SSH supported authentication : publickey,password
```

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: 2020/11/19

Plugin Output

tcp/22/ssh

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

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: 2020/11/19

Plugin Output

tcp/9000/www

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

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: 2019/03/06

Plugin Output

tcp/0

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: 2020/10/15

Plugin Output

tcp/0

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


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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.32 to 35.199.110.191 :
192.168.0.32
192.168.0.1
?
152.255.151.102
152.255.175.248
?
72.14.220.222
216.239.58.231
172.253.50.72
216.239.49.80
35.199.110.191

Hop Count: 10
```

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

<http://www.nessus.org/u?5496c8d9>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/9000/www

The following sitemap was created from crawling linkable content on the target host :

- <http://191.110.199.35.bc.googleusercontent.com:9000/>
- <http://191.110.199.35.bc.googleusercontent.com:9000/07745d55b001c85826eedd479285cdabb.svg>
- <http://191.110.199.35.bc.googleusercontent.com:9000/5ba13dcb526292ae707310a54e103cd1.png>
- <http://191.110.199.35.bc.googleusercontent.com:9000/dc4d092847be46242d8c013d1bc7c494.png>
- <http://191.110.199.35.bc.googleusercontent.com:9000/f9508a64a1beb81be174e194573f7450.png>
- <http://191.110.199.35.bc.googleusercontent.com:9000/main.df5487ae7f62fcda715d.css>
- <http://191.110.199.35.bc.googleusercontent.com:9000/vendor.1.css>

Attached is a copy of the sitemap file.

54.196.179.100

0

CRITICAL

0

HIGH

1

MEDIUM

0

LOW

38

INFO

Scan Information

Start time: Fri Dec 4 08:38:31 2020

End time: Fri Dec 4 09:04:07 2020

Host Information

DNS Name: ec2-54-196-179-100.compute-1.amazonaws.com

IP: 54.196.179.100

OS: Linux Kernel 4.15 on Ubuntu 18.04 (bionic)

Vulnerabilities

81777 - MongoDB Service Without Authentication Detection

Synopsis

The remote host is running a database system that does not have authentication enabled.

Description

MongoDB, a document-oriented database system, is listening on the remote port, and it is configured to allow connections without any authentication. A remote attacker can therefore connect to the database system in order to create, read, update, and delete documents, collections, and databases.

See Also

<https://www.mongodb.com/>

Solution

Enable authentication or restrict access to the MongoDB service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2015/03/12, Modified: 2019/01/17

Plugin Output

tcp/27017/mongodb

```
Nessus was able to run the following database query on the remote MongoDB
service without authenticating since authentication is not enabled:
```

```
local.startup_log.findOne();
```

```
This produced a response document with the following truncated
contents: (limited to 10 lines)
```

```
----- snip -----
----- snip -----
```

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-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL      : http://ec2-54-196-179-100.compute-1.amazonaws.com/
Version  : 2.4.99
backported : 1
os       : ConvertedUbuntu
```

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: 2020/11/17

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:18.04 -> Canonical Ubuntu Linux 18.04

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.29 -> Apache Software Foundation Apache HTTP Server 2.4.29

cpe:/a:apache:http_server:2.4.99

cpe:/a:mongodb:mongodb:3.6.21

cpe:/a:mysql:mysql:5.7.32-0ubuntu0.18.04.1

cpe:/a:openbsd:openssh:7.6

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 95
```


Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80/www

```
2 external URLs were gathered on this web server :  
URL... - Seen on...  
  
http://httpd.apache.org/docs/2.4/mod/mod_userdir.html - /  
https://bugs.launchpad.net/ubuntu/+source/apache2 - /
```

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_\(OTG-CONFIG-006\)](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: 2019/03/19

Plugin Output

tcp/80/www

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/icons

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/icons

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_\(OTG-CONFIG-006\)](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: 2019/03/19

Plugin Output

tcp/8000/www

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY
OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods 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/2.4.29 (Ubuntu)
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
54.196.179.100 resolves as ec2-54-196-179-100.compute-1.amazonaws.com.
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : yes
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Date: Fri, 04 Dec 2020 13:52:01 GMT
```

```
    Server: Apache/2.4.29 (Ubuntu)
```

```
    Last-Modified: Sun, 11 Oct 2020 03:11:08 GMT
```

```
    ETag: "2aa6-5b15c887ca914"
```

```
    Accept-Ranges: bytes
```

```
    Content-Length: 10918
```

```
    Vary: Accept-Encoding
```

```
    Keep-Alive: timeout=5, max=100
```

```
    Connection: Keep-Alive
```

```
    Content-Type: text/html
```

```
Response Body :
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
  <!--
```

```
    Modified from the Debian original for Ubuntu
```



```
Last updated: 2016-11-16
See: https://launchpad.net/bugs/1288690
-->
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Ubuntu Default Page: It works</title>
  <style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}

body, html {
  padding: 3px 3px 3px 3px;

  background-color: #D8DBE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

div.main_page {
  position: relative;
  display: table;

  width: 800px;

  margin-bottom: 3px;
  margin-left: auto;
  margin-right: auto;
  padding: 0px 0px 0px 0px;

  border-width: 2px;
  border-color: #212738;
  border-style: solid;

  background-color: #FFFFFF;

  text-align: center;
}

div.page_header {
  height: 99px;
  width: 100%;

  background-color: #F5F6F7;
}

div.page_header span {
  margin: 15px 0px 0px 50px;

  font-size: 180%;
  font-weight: bold;
}

div.page_header img {
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;
```

```
    text-align: left;
}

div.table_of_contents_item {
    clear: left;

    width: 100%;

    margin: 4px 0px 0px 0px;

    backgroun [...]
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/8000/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

    Date: Fri, 04 Dec 2020 13:52:02 GMT
    Content-Length: 9
    Content-Type: text/plain; charset=utf-8
    Connection: close

Response Body :
```

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

None

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

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

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

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.
```

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

<http://www.nessus.org/u?55aa8f57>

<http://www.nessus.org/u?07cc2a06>

<https://content-security-policy.com/>

<https://www.w3.org/TR/CSP2/>

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2018/11/15

Plugin Output

tcp/80/www

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy:

- <http://ec2-54-196-179-100.compute-1.amazonaws.com/>

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

<https://en.wikipedia.org/wiki/Clickjacking>

<http://www.nessus.org/u?399b1f56>

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2017/05/16

Plugin Output

tcp/80/www

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- <http://ec2-54-196-179-100.compute-1.amazonaws.com/>

Synopsis

The remote host is running a database system.

Description

A document-oriented database system is listening on the remote port.

See Also

<https://www.mongodb.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/10, Modified: 2019/11/22

Plugin Output

tcp/27017/mongodb

```
Version      : 3.6.21
Git version  : 1cd2db51dce4b16f4bc97a75056269df0dc0bddb
Databases    : config - system.sessions,_id_
               READ_ME_TO_RECOVER_YOUR_DATA - README,_id_
               admin - system.version,_id_
```


Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2020/09/22

Plugin Output

tcp/3306/mysql

```
Version : 5.7.32-0ubuntu0.18.04.1
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

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: 2020/09/14

Plugin Output

tcp/22/ssh

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

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: 2020/09/14

Plugin Output

tcp/80/www

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

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: 2020/09/14

Plugin Output

tcp/1883

```
Port 1883/tcp was found to be open
```

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: 2020/09/14

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

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: 2020/09/14

Plugin Output

tcp/8000/www

```
Port 8000/tcp was found to be open
```

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: 2020/09/14

Plugin Output

tcp/9000

```
Port 9000/tcp was found to be open
```

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: 2020/09/14

Plugin Output

tcp/27017/mongodb

```
Port 27017/tcp was found to be open
```


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: 2020/09/14

Plugin Output

tcp/32768

```
Port 32768/tcp was found to be open
```

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.
- 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: 2020/08/27

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 8.12.1  
Plugin feed version : 202012041017  
Scanner edition used : Nessus Home  
Scan type : Normal  
Scan policy used : Advanced Scan  
Scanner IP : 192.168.0.32  
Port scanner(s) : nessus_syn_scanner  
Port range : default  
Thorough tests : no  
Experimental tests : no
```

```
Paranoia level : 1
Report verbosity : 1
Safe checks : no
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : some_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : never
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2020/12/4 8:38 EST
Scan duration : 1531 sec
```

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: 2020/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
Confidence level : 95
Method : SSH
```

```
The remote host is running Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
```

Synopsis

Record route

Description

It is possible to obtain the traceroute to the remote host by sending packets with the 'Record Route' option set. It is a complement to traceroute.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2004/06/09, Modified: 2019/03/06

Plugin Output

icmp/0

```
Here is the route recorded between 192.168.0.32 and 54.196.179.100 :  
179.225.232.211  
152.255.151.105  
200.204.31.8  
152.255.150.50  
84.16.7.219  
94.142.100.207  
213.140.43.207  
176.52.252.10  
54.240.228.44
```

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: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :
```

```
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 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 encryption_algorithms_server_to_client :

```
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_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 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 compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib@openssh.com
```

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: 2020/02/18

Plugin Output

tcp/22/ssh

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

```
- 2.0
```


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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
SSH supported authentication : publickey
```

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: 2020/11/19

Plugin Output

tcp/22/ssh

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

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: 2020/11/19

Plugin Output

tcp/80/www

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

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: 2020/11/19

Plugin Output

tcp/8000/www

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

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: 2020/10/15

Plugin Output

tcp/0

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

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.32 to 54.196.179.100 :
192.168.0.32
192.168.0.1
?
152.255.151.102
187.100.186.96
84.16.7.218
94.142.98.155
213.140.43.206
216.184.113.139
52.93.236.47
52.93.37.44
?

Hop Count: 11
```

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

<http://www.nessus.org/u?5496c8d9>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

The following sitemap was created from crawling linkable content on the target host :

- <http://ec2-54-196-179-100.compute-1.amazonaws.com/>

Attached is a copy of the sitemap file.

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

<http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location>

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
The following directories were discovered:  
/icons
```

```
While this is not, in and of itself, a bug, you should manually inspect  
these directories to ensure that they are in compliance with company  
security standards
```