Scan Report

January 21, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "test5$_1$579541506$_t$ask". The scan started at an
48 : 482020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please

Contents

1 Result Overview **2**

2 Results per Host **2**

2.1 10.10.60.55 2

2.1.1 Log general/CPE-T 2

2.1.2 Log 7070/tcp 3

2.1.3 Log 5000/tcp 6

2.1.4 Log general/tcp 9

2.2 127.0.0.1 11

2.2.1 High 9390/tcp 11

2.2.2 Log general/CPE-T 12

2.2.3 Log 9390/tcp 13

2.2.4 Log general/tcp 17

2.2.5 Log 7070/tcp 19

2.2.6 Log 631/tcp 21

2.2.7 Log 80/tcp 31

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.10.60.55 csirtadmin-virtualbox	0	0	0	14	0
127.0.0.1 localhost	1	0	0	34	0
Total: 2	1	0	0	48	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 49 results selected by the filtering described above. Before filtering there were 49 results.

2 Results per Host

2.1 10.10.60.55

Host scan start	Mon Jan 20 20:30:05 2020 UTC
Host scan end	Mon Jan 20 20:32:02 2020 UTC

Service (Port)	Threat Level
general/CPE-T	Log
7070/tcp	Log
5000/tcp	Log
general/tcp	Log

2.1.1 Log general/CPE-T

. . . continues on next page . . .

. . . continued from previous page . . .

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
`10.10.60.55|cpe:/a:python:python:3.8.0`
`10.10.60.55|cpe:/o:linux:linux_kernel:2.6.32`

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2019-10-24T11:29:24+0000`

References
`Other:`
`URL:https://nvd.nist.gov/products/cpe`

[return to 10.10.60.55]

2.1.2 Log 7070/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary
The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result
`The remote service does not support perfect forward secrecy cipher suites.`

Log Method
Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: $Revision: 4743 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `$Revision: 11108 $`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result
```
Nmap service detection (unknown) result for this port: ssl|realserver
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 7070 10.10.60.55' and submit a possible collected f
↪ingerprint to the nmap database.
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References
```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 10.10.60.55]

2.1.3 Log 5000/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "csirtadmin-virtualbox" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.0.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://csirtadmin-virtualbox:5000/
```

... continues on next page ...

... continued from previous page ...

While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result
Missing Headers

Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2019-11-08T10:10:55+0000

References
Other:
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
URL:https://securityheaders.io/

Log (CVSS: 0.0)
NVT: HTTP Server type and version

... continues on next page ...

... continued from previous page ...

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
`The remote web server type is :`
`Werkzeug/0.16.0 Python/3.8.0`

Solution
- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2019-12-17T11:41:26+0000`

Log (CVSS: 0.0)
NVT: Python Version Detection (Remote)

Summary
Detects the installed version of Python.
The script detects the version of Python on the remote host and sets the KB entries.

Vulnerability Detection Result
```
Detected Python
Version:       3.8.0
Location:      5000/tcp
CPE:           cpe:/a:python:python:3.8.0
Concluded from version/product identification result:
Server: Werkzeug/0.16.0 Python/3.8.0
```

Log Method
Details: `Python Version Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.107020
Version used: `$Revision: 10908 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A web server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

[return to 10.10.60.55]

2.1.4 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS:           Linux 2.6.32
CPE:          cpe:/o:linux:linux_kernel:2.6.32
Found by NVT: 1.3.6.1.4.1.25623.1.0.108021 (Nmap OS Identification (NASL wrapper
↪))
Concluded from Nmap TCP/IP fingerprinting:
OS details: Linux 2.6.32
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-12-17T06:24:59+0000

References

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 10.10.60.55 to 10.10.60.55:
10.10.60.55
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: 2019-09-09T06:03:58+0000

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://community.greenbone.net/c/vulnera
↪bility-tests:
Banner: Server: Werkzeug/0.16.0 Python/3.8.0
Identified from: HTTP Server banner on port 5000/tcp
```

Log Method

... continues on next page ...

... continued from previous page ...

Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: $Revision: 12934 $

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

[return to 10.10.60.55]

2.2 127.0.0.1

Host scan start Mon Jan 20 20:30:05 2020 UTC
Host scan end Mon Jan 20 20:48:48 2020 UTC

Service (Port)	Threat Level
9390/tcp	High
general/CPE-T	Log
9390/tcp	Log
general/tcp	Log
7070/tcp	Log
631/tcp	Log
80/tcp	Log

2.2.1 High 9390/tcp

High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials

Product detection result
cpe:/a:openvas:openvas_manager:7.0
Detected by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.
↪1.25623.1.0.103825)

Summary
The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result
It was possible to login using the following credentials (username:password:role
↪):
admin:admin:Admin

... continues on next page ...

... continued from previous page ...

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Solution type: Workaround
Change the password of the mentioned account(s).

Vulnerability Insight
It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

Vulnerability Detection Method
Try to login with default credentials via the OMP/GMP protocol.
Details: `OpenVAS / Greenbone Vulnerability Manager Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.108554
Version used: `2019-09-06T14:17:49+0000`

Product Detection Result
Product: `cpe:/a:openvas:openvas_manager:7.0`
Method: `OpenVAS / Greenbone Vulnerability Manager Detection`
OID: 1.3.6.1.4.1.25623.1.0.103825)

[return to 127.0.0.1]

2.2.2 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
`127.0.0.1|cpe:/a:apple:cups:2.2.10`
`127.0.0.1|cpe:/a:openvas:openvas_manager:7.0`
`127.0.0.1|cpe:/o:linux:kernel`

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002

... continues on next page ...

... continued from previous page ...

Version used: 2019-10-24T11:29:24+0000

References

```
Other:
  URL:https://nvd.nist.gov/products/cpe
```

[return to 127.0.0.1]

2.2.3 Log 9390/tcp

Log (CVSS: 0.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Detection

Summary

The script sends a connection request to the server and attempts to determine if it is a OpenVAS Manager (openvasmd) or Greebone Vulnerability Manager (gmvd).

Vulnerability Detection Result

```
Detected OpenVAS Manager
Version:       7.0
Location:      9390/tcp
CPE:           cpe:/a:openvas:openvas_manager:7.0
Concluded from version/product identification result:
OMP protocol version request '<GET_VERSION/>', response: <version>7.0</version>
```

Log Method

Details: OpenVAS / Greenbone Vulnerability Manager Detection
OID:1.3.6.1.4.1.25623.1.0.103825
Version used: 2019-08-05T07:09:20+0000

Log (CVSS: 0.0)
NVT: Service Detection with '<xml/>' Request

Summary

This plugin performs service detection.
This plugin is a complement of find_service.nasl. It sends a '<xml/>' request to the remaining unknown services and tries to identify them.

Vulnerability Detection Result

```
A OpenVAS / Greenbone Vulnerability Manager supporting the OMP/GMP protocol seem
↪s to be running on this port.
```

Log Method

Details: Service Detection with '<xml/>' Request
OID:1.3.6.1.4.1.25623.1.0.108198

... continues on next page ...

... continued from previous page ...

Version used: 2019-08-05T07:09:20+0000

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A TLScustom server answered on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=csirtadmin-VirtualBox
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for csir
↪tadmin-VirtualBox
serial ....: 1C09DF55B688961C9CEF2F7E9B17F8A87778BE4F
valid from : 2019-12-22 22:03:10 UTC
valid until: 2021-12-21 22:03:10 UTC
fingerprint (SHA-1): 0442451D30AFC7366F7CBF84C4BB86A08966E70B
fingerprint (SHA-256): 3189884906E05F7861BEF2EBCBA19F362666CEBB22427C53C86305B85
↪1265AE2
```

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary
The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result
`The remote service does not support perfect forward secrecy cipher suites.`

Log Method
Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: `SSL/TLS: Report Medium Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 4743 $`

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Log Method
Details: `SSL/TLS: Report Non Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 11108 $

[return to 127.0.0.1]

2.2.4 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:           Linux/Unix
CPE:          cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 631/tcp: <title>Home - CUPS 2.2.
↪10</title>
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
```

... continues on next page ...

... continued from previous page ...

```
OS:           Linux/Unix
CPE:          cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 631/tcp: Server: CUPS/2.2 IPP/2.1
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-12-17T06:24:59+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result

```
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
csirtadmin-VirtualBox
csirtadmin-virtualbox
```

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: $Revision: 13774 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 127.0.0.1 to 127.0.0.1:
127.0.0.1
```

... continues on next page ...

... continued from previous page ...

Solution
Block unwanted packets from escaping your network.

Log Method
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2019-09-09T06:03:58+0000`

[return to 127.0.0.1]

2.2.5 Log 7070/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary
The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result
`The remote service does not support perfect forward secrecy cipher suites.`

Log Method
Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: $Revision: 4743 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `$Revision: 11108 $`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Nmap service detection (unknown) result for this port: ssl|realserver
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 7070 127.0.0.1' and submit a possible collected fin
↪gerprint to the nmap database.
```

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 127.0.0.1]

2.2.6 Log 631/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "localhost" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
https://localhost:631/
https://localhost:631/admin
https://localhost:631/admin-bak
https://localhost:631/admin-console
https://localhost:631/admin-old
https://localhost:631/admin.back
https://localhost:631/admin_
https://localhost:631/adminer
https://localhost:631/administration
https://localhost:631/administrator
https://localhost:631/adminuser
https://localhost:631/adminweb
https://localhost:631/classes
https://localhost:631/es
https://localhost:631/help
https://localhost:631/helpdesk
https://localhost:631/printers
```

... continues on next page ...

... continued from previous page ...

```
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://localhost:631/admin (USER_CANCEL_ANY [] SHARE_PRINTERS [] DEBUG_LOGGING
↪[] REMOTE_ANY [] org.cups.sid [028405d1834086ded2f32b86aa88dfac] CHANGESETTING
↪S [Change Settings] KERBEROS [] OP [config-server] REMOTE_ADMIN [] )
https://localhost:631/admin/ (ADVANCEDSETTINGS [YES] org.cups.sid [028405d183408
↪6ded2f32b86aa88dfac] OP [add-printer] )
https://localhost:631/admin/log/access_log ()
https://localhost:631/admin/log/error_log ()
https://localhost:631/admin/log/page_log ()
https://localhost:631/classes/ (CLEAR [Clear] QUERY [] )
https://localhost:631/help/ (SEARCH [Search] CLEAR [Clear] TOPIC [Getting+Starte
↪d] QUERY [] )
https://localhost:631/help/accounting.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/cgi.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/encryption.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/glossary.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/kerberos.html (TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/license.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/network.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/options.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/overview.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] QUERY [] TOPIC [Getting Started] )
https://localhost:631/help/policies.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/security.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/sharing.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/translation.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/jobs (which_jobs [completed] )
https://localhost:631/jobs/ (CLEAR [Clear] QUERY [] )
https://localhost:631/printers/ (CLEAR [Clear] QUERY [] )
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: CUPS Version Detection

Summary
Detects the installed version of Common Unix Printing System (CUPS)
This script sends an HTTP GET request and tries to get the version from the response.

Vulnerability Detection Result
```
Detected CUPS
Version:       2.2.10
Location:      /
CPE:           cpe:/a:apple:cups:2.2.10
Concluded from version/product identification result:
<title>Home - CUPS 2.2.10</title>
```

Log Method
Details: CUPS Version Detection
OID:1.3.6.1.4.1.25623.1.0.900348
Version used: 2019-12-17T11:41:26+0000

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result
```
Header Name                Header Value
-----------                ------------
Content-Security-Policy  : frame-ancestors 'none'
X-Frame-Options          : DENY
Missing Headers
---------------
Referrer-Policy
X-Content-Type-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2019-11-08T10:10:55+0000

References
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
URL:https://securityheaders.io/

Log (CVSS: 0.0)
NVT: robot(s).txt exists on the Web Server

Summary
Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Vulnerability Detection Result

```
The file 'robots.txt' contains the following:
#
# This file tells search engines not to index your CUPS server.
#
User-agent: *
Disallow: /
```

Solution
Solution type: Mitigation
Review the content of the robots file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

Vulnerability Insight
Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.
Any entries listed in this file are not even hidden anymore.

Log Method
Details: `robot(s).txt exists on the Web Server`
OID:1.3.6.1.4.1.25623.1.0.10302
Version used: `2019-11-22T13:51:04+0000`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A TLScustom server answered on this port`

... continues on next page ...

... continued from previous page ...

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port through SSL

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary
The SSL/TLS certificate on this port is self-signed.

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: L=Unknown,ST=Unknown,OU=Unknown,O=csirtadmin-virtualbox,CN=csirtadm
↪in-virtualbox,C=US
subject alternative names (SAN):
None
issued by .: L=Unknown,ST=Unknown,OU=Unknown,O=csirtadmin-virtualbox,CN=csirtadm
↪in-virtualbox,C=US
serial ....: 5E247ECB
valid from : 2020-01-19 16:07:39 UTC
valid until: 2030-01-16 16:07:39 UTC
fingerprint (SHA-1): F02D45182C9DC7CDB3F0DA53C794C090C965B121
fingerprint (SHA-256): 9C1FB73C73BF37FB44C52C3D00A26B9CA3A0FD13991C88E9F79CC74CD
↪DB6C888
```

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 8981 $

References
Other:
URL:http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=csirtadmin-VirtualBox
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for csir
↪tadmin-VirtualBox
serial ....: 1C09DF55B688961C9CEF2F7E9B17F8A87778BE4F
valid from : 2019-12-22 22:03:10 UTC
valid until: 2021-12-21 22:03:10 UTC
fingerprint (SHA-1): 0442451D30AFC7366F7CBF84C4BB86A08966E70B
fingerprint (SHA-256): 3189884906E05F7861BEF2EBCBA19F362666CEBB22427C53C86305B85
↪1265AE2
```

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HPKP.

Vulnerability Detection Result
```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Connection: close
```

... continues on next page ...

... continued from previous page ...

```
Content-Language: en
Content-Length: ***replaced***
Content-Type: text/html; charset=utf-8
Date: ***replaced***
Last-Modified: ***replaced***
Accept-Encoding: gzip, deflate, identity
Server: CUPS/2.2 IPP/2.1
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none'
```

Solution
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: $Revision: 7391 $

References
Other:
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hpkp
URL:https://tools.ietf.org/html/rfc7469
URL:https://securityheaders.io/

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HSTS.

Vulnerability Detection Result
The remote web server is not enforcing HSTS.
HTTP-Banner:

```
HTTP/1.1 200 OK
Connection: close
Content-Language: en
Content-Length: ***replaced***
Content-Type: text/html; charset=utf-8
Date: ***replaced***
Last-Modified: ***replaced***
Accept-Encoding: gzip, deflate, identity
Server: CUPS/2.2 IPP/2.1
X-Frame-Options: DENY
```

... continues on next page ...

... continued from previous page ...

```
Content-Security-Policy: frame-ancestors 'none'
```

Solution
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: $Revision: 7391 $

References
```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Shee
↪t
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hsts
   URL:https://tools.ietf.org/html/rfc6797
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary
The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result
```
The remote service does not support perfect forward secrecy cipher suites.
```

Log Method
Details: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: `SSL/TLS: Report Medium Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 4743 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Log Method
Details: `SSL/TLS: Report Non Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 11108 $

[return to 127.0.0.1]

2.2.7 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "localhost" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://localhost/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Header Name                Header Value
-----------                ------------
Content-Security-Policy  : default-src 'self' 'unsafe-inline'; img-src 'self' bl
↪ob:; frame-ancestors 'self'
X-Frame-Options          : SAMEORIGIN
Missing Headers
---------------
Referrer-Policy
X-Content-Type-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2019-11-08T10:10:55+0000

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port

Log Method
Details: Services

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2019-07-08T14:12:44+0000

[return to 127.0.0.1]
