Scan Report

June 22, 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 "tria$_t$ask''.$Thescanstartedat Mon Jun 22 10 : 16 : 15 2020 UTC and ended at Mon Jun 22 11 : 00 : 49 2020 UTC. The report first summarises the results found. Then, for each host,$

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
127.0.0.1 localhost	0	3	0	30	0
Total: 1	0	3	0	30	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 33 results selected by the filtering described above. Before filtering there were 33 results.

2 Results per Host

2.1 127.0.0.1

Host scan start	Mon Jun 22 10:16:40 2020 UTC
Host scan end	Mon Jun 22 11:00:49 2020 UTC

Service (Port)	Threat Level
631/tcp	Medium
4000/tcp	Medium
631/tcp	Log
general/CPE-T	Log
general/tcp	Log
4000/tcp	Log

2.1.1 Medium 631/tcp

. . . continues on next page . . .

... continued from previous page ...

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              L=Unknown,ST=Unknown,OU=Unknown,O=ubuntu,CN=ubuntu,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 11524 $`

References
```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

[return to 127.0.0.1]

2.1.2 Medium 4000/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

... continues on next page ...

... continued from previous page ...

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

[return to 127.0.0.1]

2.1.3 Log 631/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.

... continues on next page ...

... continued from previous page ...

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.
A possible recursion was detected during CGI scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
https://localhost:631/admin (dbus://)
https://localhost:631/admin-bak (dbus://)
https://localhost:631/admin-console (dbus://)
https://localhost:631/admin-old (dbus://)
https://localhost:631/admin/ (dbus://)
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_
```

... continues on next page ...

... continued from previous page ...

```
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
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 [fe62178435a913922e6964572bfb18bb] CHANGESETTING
↪S [Change Settings] KERBEROS [] OP [config-server] REMOTE_ADMIN [] )
https://localhost:631/admin/ (notify_subscription_id [49] ADVANCEDSETTINGS [YES]
↪ org.cups.sid [fe62178435a913922e6964572bfb18bb] 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] QUERY [] TOPIC [Getti
↪ng+Started] )
https://localhost:631/help/accounting.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/api-admin.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-filter.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-ppd.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-raster.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/cgi.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YE
↪S] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/cupspm.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/encryption.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/glossary.html (QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/kerberos.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/license.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Getting+Started] )
```

... continues on next page ...

... continued from previous page ...

https://localhost:631/help/man-backend.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cancel.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-classes.conf.html (SEARCH [Search] CLEAR [Clear]
↪PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-client.conf.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cups-config.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cups-files.conf.html (SEARCH [Search] CLEAR [Clea
↪r] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cups-lpd.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cups-snmp.conf.html (TOPIC [Man+Pages])
https://localhost:631/help/man-cups-snmp.html (SEARCH [Search] CLEAR [Clear] PRI
↪NTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cups.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupsaccept.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupsaddsmb.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupsctl.html (TOPIC [Man+Pages])
https://localhost:631/help/man-cupsd-helper.html (SEARCH [Search] CLEAR [Clear]
↪PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cupsd-logs.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-cupsd.conf.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man Pages] QUERY [])
https://localhost:631/help/man-cupsd.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupsenable.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupsfilter.html (TOPIC [Man+Pages])
https://localhost:631/help/man-cupstestdsc.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-cupstestppd.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-filter.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ipptool.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-ipptoolfile.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-lp.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Man+Pages])

... continues on next page ...

... continued from previous page ...

https://localhost:631/help/man-lpadmin.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-lpc.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-lpinfo.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-lpmove.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-lpoptions.html (SEARCH [Search] CLEAR [Clear] PRI
↪NTABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-lpq.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-lpr.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-lprm.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-lpstat.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-mime.convs.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-mime.types.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-notifier.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ppdc.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ppdcfile.html (TOPIC [Man+Pages])
https://localhost:631/help/man-ppdhtml.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ppdi.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ppdmerge.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-ppdpo.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] TOPIC [Man+Pages] QUERY [])
https://localhost:631/help/man-printers.conf.html (SEARCH [Search] CLEAR [Clear]
↪ PRINTABLE [YES] QUERY [] TOPIC [Man+Pages])
https://localhost:631/help/man-subscriptions.conf.html (SEARCH [Search] CLEAR [C
↪lear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY [])
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])

... continues on next page ...

... continued from previous page ...

```
https://localhost:631/help/postscript-driver.html (SEARCH [Search] CLEAR [Clear]
↪ PRINTABLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/ppd-compiler.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/raster-driver.html (SEARCH [Search] CLEAR [Clear] PRI
↪NTABLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/security.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/sharing.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Getting+Started] )
https://localhost:631/help/translation.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] 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:       2.2.7
Location:      /
CPE:           cpe:/a:apple:cups:2.2.7
Concluded from version/product identification result:
<title>Home - CUPS 2.2.7</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                   | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪---
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection
```

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2020-03-18T09:31:42+0000

References

```
Other:
  URL:https://owasp.org/www-project-secure-headers/
   URL:https://owasp.org/www-project-secure-headers/#div-headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner            | Enumeration technique
-------------------------------------------------------------------
Server: CUPS/2.2 IPP/2.1 | Valid HTTP 1.0 GET request to '/index.htm'
```

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2020-02-25T12:12:27+0000

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

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: CUPS/2.2 IPP/2.1
```

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-02-06T14:44:42+0000

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.
#
```

. . . continues on next page . . .

... continued from previous page ...

```
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`

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`

... 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: 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=ubuntu,CN=ubuntu,C=US
subject alternative names (SAN):
None
issued by .: L=Unknown,ST=Unknown,OU=Unknown,O=ubuntu,CN=ubuntu,C=US
serial ....: 5E8356D0
valid from : 2020-03-31 14:42:24 UTC
valid until: 2030-03-29 14:42:24 UTC
fingerprint (SHA-1): 3EE954A83C8CA6FB00D7F74BFABB354EC16FDC58
fingerprint (SHA-256): 59D720C2ACAFAA8C0CE7BE9035A4DF569DF96BBBA37DC69E507E514EA
↪E570BBB
```

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
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: 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: 2020-03-18T09:31:42+0000

References
```
Other:
  URL:https://owasp.org/www-project-secure-headers/
   URL:https://owasp.org/www-project-secure-headers/#public-key-pinning-extensio
↪n-for-http-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
```

... continues on next page ...

... continued from previous page ...

```
X-Frame-Options: DENY
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: 2020-02-28T07:44:42+0000

References

```
Other:
  URL:https://owasp.org/www-project-secure-headers/
   URL:https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transp
↪ort_Security_Cheat_Sheet.html
   URL:https://owasp.org/www-project-secure-headers/#http-strict-transport-secur
↪ity-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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'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_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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'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_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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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]

2.1.4 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

... continues on next page ...

... continued from previous page ...

127.0.0.1|cpe:/a:apple:cups:2.2.7
127.0.0.1|cpe:/a:greenbone:greenbone_security_assistant:7.0.3
127.0.0.1|cpe:/o:linux:kernel

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 127.0.0.1]

2.1.5 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 banner on port 631/tcp: Server: CUPS/2.2 IPP/2.1
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
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.
↪7</title>
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2020-03-30T08:21:10+0000

... continues on next page ...

. . . continued from previous page . . .

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:
ubuntu

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

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: 2020-03-21T13:23:23+0000

[return to 127.0.0.1]

2.1.6 Log 4000/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:4000/
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: Greenbone Security Assistant (GSA) Detection

Summary
The script sends a connection request to the server and attempts to determine if it is a GSA from the reply.

Vulnerability Detection Result
```
Detected Greenbone Security Assistant
Version:       7.0.3
Location:      /
CPE:           cpe:/a:greenbone:greenbone_security_assistant:7.0.3
Concluded from version/product identification result:
<span class="version">Version 7.0.3</span>
```

Log Method
Details: Greenbone Security Assistant (GSA) Detection
OID:1.3.6.1.4.1.25623.1.0.103841
Version used: 2019-11-12T09:49:27+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 | default-src 'self' 'unsafe-inline'; img-src 'self' blo
↪b
X-Frame-Options         | SAMEORIGIN
Missing Headers                   | More Information
------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪---
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
```
... continues on next page ...

... continued from previous page ...

```
↪/#referrer-policy
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection
```

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2020-03-18T09:31:42+0000

References
Other:
URL:https://owasp.org/www-project-secure-headers/
URL:https://owasp.org/www-project-secure-headers/#div-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 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: 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 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: 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/1.1 303 See Other
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Expires: ***replaced***
Location: https://localhost:4000/login/login.html
Date: ***replaced***
```

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: 2020-03-18T09:31:42+0000

References
```
Other:
  URL:https://owasp.org/www-project-secure-headers/
   URL:https://owasp.org/www-project-secure-headers/#public-key-pinning-extensio
↪n-for-http-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/1.1 303 See Other
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Expires: ***replaced***
Location: https://localhost:4000/login/login.html
Date: ***replaced***
```

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: 2020-02-28T07:44:42+0000

References
```
Other:
  URL:https://owasp.org/www-project-secure-headers/
   URL:https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transp
↪ort_Security_Cheat_Sheet.html
   URL:https://owasp.org/www-project-secure-headers/#http-strict-transport-secur
↪ity-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.

. . . continues on next page . . .

... continued from previous page ...

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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'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_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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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

... continues on next page ...

... continued from previous page ...

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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'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_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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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.

... continues on next page ...

... continued from previous page ...

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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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_3DES_EDE_CBC_SHA
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
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_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]

This file was automatically generated.