Scan Report

March 6, 2025

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 "cred ". The scan started at Thu Mar 6 02:34:39 2025 UTC and ended at Thu Mar 6 06:19:05 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.2.1 mynetwork.home	0	6	1	62	0
Total: 1	0	6	1	62	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 69 results selected by the filtering described above. Before filtering there were 86 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.2.1 - mynetwork.home	SSH	Failure	Protocol SSH, Port 22, User harlin : Login failure
192.168.2.1 - mynetwork.home	SMB	Success	Protocol SMB, Port 445, User harlin

2 Results per Host

2.1 192.168.2.1

Host scan start Thu Mar 6 02:52:44 2025 UTC
Host scan end Thu Mar 6 06:18:56 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium
9443/tcp	Medium
80/tcp	Medium
general/icmp	Low

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
22/tcp	Log
9000/tcp	Log
445/tcp	Log
443/tcp	Log
general/CPE-T	Log
53/tcp	Log
10080/tcp	Log
9443/tcp	Log
80/tcp	Log
general/tcp	Log

2.1.1 Medium 443/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2012-6708`
`url: https://bugs.jquery.com/ticket/11290`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K18/1131`
`dfn-cert: DFN-CERT-2023-1197`
`dfn-cert: DFN-CERT-2020-0590`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

References
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2024-09-30T08:38:05Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 192.168.2.1]

2.1.2 Medium 9443/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 98%

Vulnerability Detection Result
`The service is only providing the deprecated TLSv1.0 protocol and supports one o`
`↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S`
`↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.`

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`

... continues on next page ...

... continued from previous page ...

```
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=*,L=SanDiego,ST=California,OU=TwonkyServer,O=PacketVide
↪o,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.

... continues on next page ...

... continued from previous page ...

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: `2021-10-15T11:13:32Z`

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

[return to 192.168.2.1]

2.1.3 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2012-6708`
`url: https://bugs.jquery.com/ticket/11290`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K18/1131`
`dfn-cert: DFN-CERT-2023-1197`
`dfn-cert: DFN-CERT-2020-0590`

[return to 192.168.2.1]

2.1.4 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2025-01-21T05:37:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.2.1]

2.1.5 Log 22/tcp

Log (CVSS: 0.0)
NVT: SSH Login Failed For Authenticated Checks

Summary
It was NOT possible to login using the provided SSH credentials. Hence authenticated checks are NOT enabled.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was not possible to login using the provided SSH credentials. Hence authentic
↪ated checks are not enabled.
If the SSH credentials are correct the login might have failed because of the fo
↪llowing reasons:
- The password of the provided SSH credentials has expired and the user is requi
```

... continues on next page ...

... continued from previous page ...

↪red to change it before a login is possible again.

Solution:
Recheck the SSH credentials for authenticated checks or evaluate the script output for the required algorithms on the remote SSH server or the scanner.

Log Method
Details: SSH Login Failed For Authenticated Checks
OID:1.3.6.1.4.1.25623.1.0.105936
Version used: 2022-09-22T10:44:54Z

References
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html#requiremen
↪ts-on-target-systems-with-linux-unix

Log (CVSS: 0.0)
NVT: SSH Authorization Check

Summary
This script tries to login with provided credentials.
If the login was successful, it marks this port as available for any authenticated tests.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
It was not possible to login using the provided SSH credentials. Hence authentic
↪ated checks are not enabled.

Solution:

Log Method
Details: SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: 2023-07-28T16:09:07Z

[return to 192.168.2.1]

2.1.6 Log 9000/tcp

Log (CVSS: 0.0)
NVT: UPnP Detection (TCP)

Summary

... continues on next page ...

... continued from previous page ...

TCP based detection of the UPnP protocol.
The script sends a HTTP request to URLs for the root description XML, either based on previously detected location or a list of known possible locations.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote Host exposes an UPnP root device XML on port 9000/tcp.
The XML can be found at the location:
  http://mynetwork.home:9000/rss/Starter_desc.xml
```

Solution:

Log Method
Details: UPnP Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.170204
Version used: 2024-09-06T15:39:29Z

References
url: https://openconnectivity.org/foundation/faq/upnp-faq/

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                                                                 | Enu
↪meration technique
------------------------------------------------------------------------------
↪-------------------------------------------------------------
Server: Linux/2.x.x, UPnP/1.0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1 | Inv
↪alid HTTP 00.5 GET request (non-existent HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2025-01-31T15:39:24Z

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
```

... continues on next page ...

... continued from previous page ...

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, Note: Most major browsers have dropped / deprecated support for this header in 2020.

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Linux/2.x.x, UPnP/1.0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary

... continues on next page ...

... continued from previous page ...

The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "mynetwork.home" 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.
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; Greenbone OS 22.04.27)" was used to ac
↪cess the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://mynetwork.home:9000/
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
```

Solution:

Log Method

Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References

`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0) NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result `A web server is running on this port`
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). 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.
Log Method Details: `Services` OID:1.3.6.1.4.1.25623.1.0.10330 Version used: `2023-06-14T05:05:19Z`

[return to 192.168.2.1]

2.1.7 Log 445/tcp

Log (CVSS: 0.0) NVT: SMB Remote Version Detection
Summary Detection of Server Message Block(SMB). This script sends SMB Negotiation request and try to get the version from the response.
Quality of Detection (QoD): 80%
Vulnerability Detection Result `SMBv1, SMBv2 and SMBv3 are enabled on remote target`
Solution:
Log Method Details: `SMB Remote Version Detection` OID:1.3.6.1.4.1.25623.1.0.807830 Version used: `2023-07-26T05:05:09Z`

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

Summary
It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `2023-07-28T16:09:07Z`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following shares were found
IPC$
```

Solution:

Log Method
Details: `Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `2023-01-31T10:08:41Z`

Log (CVSS: 0.0)
NVT: SMBv1 Enabled - Active Check

Summary
The host has enabled SMBv1 for the SMB Server.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`SMBv1 is enabled for the SMB Server`

Solution:

Log Method
Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:
- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).
Details: `SMBv1 Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.140151
Version used: `2024-01-09T05:06:46Z`

References
`url: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices`
`url: https://support.microsoft.com/en-us/kb/2696547`
`url: https://support.microsoft.com/en-us/kb/204279`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A CIFS server is running on this port`

Solution:

Log Method
Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: SMB log in

... continues on next page ...

... continued from previous page ...

Summary
This script attempts to logon into the remote host using login/password credentials.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
`It was possible to log into the remote host using the SMB protocol.`

Solution:

Log Method
Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `2023-11-28T05:05:32Z`

[return to 192.168.2.1]

2.1.8 Log 443/tcp

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)              | 645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)            | D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC
↪429A692B8E7B1497FA
issued by                        | CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 00C4BBECECC04303A2
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN)  | None
valid from                       | 2015-10-02 09:55:43 UTC
valid until                      | 2115-09-08 09:55:43 UTC
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

Solution:

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
```

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2023-07-07T05:05:26Z`

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The certificate of the remote service is self signed.
Certificate details:

fingerprint (SHA-1)	645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)	D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC ↪429A692B8E7B1497FA
issued by	CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm	RSA
public key size (bits)	2048
serial	00C4BBECECC04303A2
signature algorithm	sha256WithRSAEncryption
subject	CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN)	None
valid from	2015-10-02 09:55:43 UTC
valid until	2115-09-08 09:55:43 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "mynetwork.home".
Certificate details:

fingerprint (SHA-1)	645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)	D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC ↪429A692B8E7B1497FA
issued by	CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm	RSA
public key size (bits)	2048
serial	00C4BBECECC04303A2
signature algorithm	sha256WithRSAEncryption
subject	CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN)	None
valid from	2015-10-02 09:55:43 UTC
valid until	2115-09-08 09:55:43 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate Too Long Valid

. . . continues on next page . . .

... continued from previous page ...

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate expiration date is too far in the future.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service is valid for more than 15 years from now a
↪nd will expire on 2115-09-08 09:55:43.
Certificate details:

fingerprint (SHA-1)	645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)	D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC ↪429A692B8E7B1497FA
issued by	CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm	RSA
public key size (bits)	2048
serial	00C4BBECECC04303A2
signature algorithm	sha256WithRSAEncryption
subject	CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN)	None
valid from	2015-10-02 09:55:43 UTC
valid until	2115-09-08 09:55:43 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any do not have a reasonable expiration date.

Log Method
Details: SSL/TLS: Certificate Too Long Valid
OID:1.3.6.1.4.1.25623.1.0.103958
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

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

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 200 OK
Content-Language: en
Content-Type: text/html
Accept-Ranges: bytes
ETag: "***replaced***"
Last-Modified: ***replaced***
Content-Length: ***replaced***
Connection: close
Date: ***replaced***
Server: HTTP Server
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

References
```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
```

... continues on next page ...

... continued from previous page ...

url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

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

Summary
The remote web server is not enforcing HTTP Public Key Pinning (HPKP).
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Content-Language: en
Content-Type: text/html
Accept-Ranges: bytes
ETag: "***replaced***"
Last-Modified: ***replaced***
Content-Length: ***replaced***
Connection: close
Date: ***replaced***
Server: HTTP Server

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-

... continues on next page ...

... continued from previous page ...

```
↪for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
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. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
```

... continues on next page ...

... continued from previous page ...

```
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
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-Frame-Options                 | https://owasp.org/www-project-secure-headers
↪/#x-frame-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, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

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

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

... continues on next page ...

... continued from previous page ...

This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

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

Quality of Detection (QoD): 98%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

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: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
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.
'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

... continues on next page ...

... continued from previous page ...

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
```

... continues on next page ...

... continued from previous page ...

↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.3 | Disabled (The TLSv1.3 protocol generally doesn't support rene
↪gotiation so this is always reported as 'Disabled')

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
00C4BBECECC04303A2:CN=self-signedkey,O=Sagemcom Ca,C=FR (Server certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

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

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: HTTP Server
```

Solution:

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner       | Enumeration technique
--------------------------------------------------------------------------------
↪------
Server: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

Log Method

Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

... continues on next page ...

... continued from previous page ...

Summary
The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "mynetwork.home" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
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; Greenbone OS 22.04.27)" was used to ac
↪cess the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://mynetwork.home/
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 directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
https://mynetwork.home/gui/js
https://mynetwork.home/js/thirdParty
```

... continues on next page ...

... continued from previous page ...

```
https://mynetwork.home/js/thirdParty/noUiSlider
https://mynetwork.home/js/thirdParty/pikaday
https://mynetwork.home/js/thirdParty/pikaday/css
https://mynetwork.home/js/thirdParty/pikaday/plugins
https://mynetwork.home/layout/css/desktop
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
https://mynetwork.home/common-bundle.js (_v [7.2.4] )
https://mynetwork.home/gui/js/gui-api.js (_v [7.2.4] )
https://mynetwork.home/gui/js/gui-core.js (_v [7.2.4] )
https://mynetwork.home/gui/js/jquery-utils.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/IPSubnetCalculator.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/attrchange.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/circle-progress.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/cssua.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/dust-full-0.3.0.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/dust-helpers-1.1.1.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/jquery.csv-0.71.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/jquery.nouislider.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/jquery.sortElements.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/md5.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/modernizr.custom.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/noUiSlider/wNumb.min.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/pikaday/moment.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/pikaday/pikaday.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/pikaday/plugins/pikaday.jquery.js (_v [7.2.
↪4] )
https://mynetwork.home/js/thirdParty/raphael.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/typeahead.js (_v [7.2.4] )
https://mynetwork.home/js/thirdParty/yepnope.1.5.4-min.js (_v [7.2.4] )
https://mynetwork.home/layout/css/desktop/desktop.css (_v [7.2.4] )
https://mynetwork.home/main-bundle.js (_v [7.2.4] )
https://mynetwork.home/system-csp-production.js (_v [7.2.4] )
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
TLSv1.3

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: SSL/TLS: Version Detection
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: 2024-09-27T05:05:23Z

[return to 192.168.2.1]

2.1.9 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.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.0
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.2
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.3
192.168.2.1|cpe:/a:jquery:jquery:1.8.3
192.168.2.1|cpe:/o:linux:kernel:2.x.x

Solution:

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: 2022-07-27T10:11:28Z

References
url: https://nvd.nist.gov/products/cpe

[return to 192.168.2.1]

2.1.10 Log 53/tcp

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary
TCP based detection of a DNS server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote DNS server banner is:
UNKNOWN

Solution:

Log Method
Details: DNS Server Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: 2021-11-30T08:05:58Z

[return to 192.168.2.1]

2.1.11 Log 10080/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host returns a 30x (e.g. 301) error code when a non-existent file is request ↪ed. Some HTTP-related checks have been disabled.`

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.

. . . continues on next page . . .

... continued from previous page ...

The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2023-07-07T05:05:26Z`

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
```

... continues on next page ...

... continued from previous page ...

```
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-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, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `2021-07-14T06:19:43Z`

References
`url: https://owasp.org/www-project-secure-headers/`
`url: https://owasp.org/www-project-secure-headers/#div-headers`
`url: https://securityheaders.com/`

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: HTTP Server
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner       | Enumeration technique
--------------------------------------------------------------------------------
↪------
Server: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called '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)

... continues on next page ...

... continued from previous page ...

- 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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "mynetwork.home" 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; Greenbone OS 22.04.27)" was used to ac
↪cess the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://mynetwork.home:10080/
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
```

Solution:

Log Method

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

[return to 192.168.2.1]

2.1.12 Log 9443/tcp

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

Summary
This VT consolidates and reports the information collected by the following VTs:
- 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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
An unknown service is running on this port. If you know this service, please rep
↪ort the following information to https://forum.greenbone.net/c/vulnerability-t
↪ests/7:
Method: get_httpHex
0x00:  15 03 01 00 02 02 28 15 03 01 00 02 02 00          ......(.......
Nmap service detection (unknown) result for this port: ssl|tungsten-https
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 9443 192.168.2.1' and submit a possible collected f
↪ingerprint to the nmap database.
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

The remote service does not support perfect forward secrecy cipher suites.

Solution:

Log Method
Details: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: 2024-09-27T05:05:23Z

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol.
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.

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary

... continues on next page ...

... continued from previous page ...

Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
-------------------------------------------------------------------------------
↪--
SSLv3            | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.0          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.1          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.2          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.3          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
```

Solution:

Log Method

Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References

url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary

Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.0

Solution:

... continues on next page ...

. . . continued from previous page . . .

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

[return to 192.168.2.1]

2.1.13 Log 80/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
```

Solution:

Vulnerability Insight

This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method

Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2023-07-07T05:05:26Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP

Summary

This script checks if the remote HTTP server is sending a HPKP, HSTS and/or Expect-CT header via plain HTTP.
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP server is sending HPKP, HSTS and/or Expect-CT headers via plain
↪HTTP.
HSTS-Header:
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Workaround
Configure the remote host to only send HPKP, HSTS and Expect-CT headers via HTTPS. Sending those headers via plain HTTP doesn't comply with the referenced RFCs.

Log Method
Details: SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP
OID:1.3.6.1.4.1.25623.1.0.108248
Version used: 2023-07-25T05:05:58Z

References
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
url: https://owasp.org/www-project-secure-headers/#expect-ct
url: https://tools.ietf.org/html/rfc6797
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: http://httpwg.org/http-extensions/expect-ct.html#http-request-type

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Header Name	Header Value
X-Content-Type-Options	nosniff
X-Frame-Options	DENY
X-XSS-Protection	1; mode=block

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers

... continues on next page ...

... continued from previous page ...

```
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: HTTP Server
```

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner       | Enumeration technique
--------------------------------------------------------------------------------
↪------
Server: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The Hostname/IP "mynetwork.home" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
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; Greenbone OS 22.04.27)" was used to ac
↪cess the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://mynetwork.home/
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 directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
```

... continues on next page ...

... continued from previous page ...

```
http://mynetwork.home/gui/js
http://mynetwork.home/js/thirdParty
http://mynetwork.home/js/thirdParty/noUiSlider
http://mynetwork.home/js/thirdParty/pikaday
http://mynetwork.home/js/thirdParty/pikaday/css
http://mynetwork.home/js/thirdParty/pikaday/plugins
http://mynetwork.home/layout/css/desktop
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
http://mynetwork.home/common-bundle.js (_v [7.2.4] )
http://mynetwork.home/gui/js/gui-api.js (_v [7.2.4] )
http://mynetwork.home/gui/js/gui-core.js (_v [7.2.4] )
http://mynetwork.home/gui/js/jquery-utils.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/IPSubnetCalculator.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/attrchange.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/circle-progress.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/cssua.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/dust-full-0.3.0.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/dust-helpers-1.1.1.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.csv-0.71.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.nouislider.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.sortElements.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/md5.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/modernizr.custom.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/wNumb.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/moment.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/pikaday.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/plugins/pikaday.jquery.js (_v [7.2.4
↪] )
http://mynetwork.home/js/thirdParty/raphael.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/typeahead.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/yepnope.1.5.4-min.js (_v [7.2.4] )
http://mynetwork.home/layout/css/desktop/desktop.css (_v [7.2.4] )
http://mynetwork.home/main-bundle.js (_v [7.2.4] )
http://mynetwork.home/system-csp-production.js (_v [7.2.4] )
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

[return to 192.168.2.1]

2.1.14 Log general/tcp

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
self-signedkey

Solution:

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

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

Summary
This VT consolidates and reports the information collected by the following VTs:
- 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 forum.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

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://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: UNKNOWN
Identified from: DNS server banner on port 53/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 10080/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 443/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 80/tcp
```

Solution:

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

References

`url: https://forum.greenbone.net/c/vulnerability-tests/7`

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

Summary

This script consolidates the OS information detected by several VTs 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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Best matching OS:
OS:           Linux 2.x.x
Version:      2.x.x
CPE:          cpe:/o:linux:kernel:2.x.x
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 9000/tcp: Server: Linux/2.x.x, UPnP/1.
```

... continues on next page ...

... continued from previous page ...

```
↪0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1
Setting key "Host/runs_unixoide" based on this information
```

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2025-01-31T15:39:24Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
It was possible to route a TCP packet through the target host and received an an
↪swer which means IP forwarding is enabled.
```

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205
Version used: `2021-12-03T08:27:06Z`

References
`cve: CVE-1999-0511`

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Network route from scanner (192.168.2.108) to target (192.168.2.1):
192.168.2.108
192.168.2.1
Network distance between scanner and target: 2
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2022-10-17T11:13:19Z`

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Hostname determination for IP 192.168.2.1:
Hostname|Source
mynetwork.home|Reverse-DNS
```

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2022-07-27T10:11:28Z`

Log (CVSS: 0.0)
NVT: jQuery Detection Consolidation

Summary
Consolidation of jQuery detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected jQuery
Version:       1.8.3
Location:      /js/thirdParty/jquery-1.8.3.min.js
CPE:           cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="/js/thirdParty/jquery-1.8.3.min.js
Concluded from version/product identification location:
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
Detected jQuery
Version:       1.8.3
Location:      /js/thirdParty/jquery-1.8.3.min.js
CPE:           cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="/js/thirdParty/jquery-1.8.3.min.js
Concluded from version/product identification location:
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

Solution:

Log Method
Details: `jQuery Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.150658
Version used: `2023-07-14T05:06:08Z`

References
`url: https://jquery.com/`

Log (CVSS: 0.0)
NVT: Authenticated Scan / LSC Info Consolidation (Windows SMB Login)

Summary
Consolidation and reporting of various technical information about authenticated scans / local security checks (LSC) via SMB for Windows targets.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                : Value/Content
------------------------------------------------------------------------------
↪------------------------------
Access to the registry possible (SMB/registry_access)
↪                : TRUE
Access via WMI possible (WMI/access_successful)
↪                : FALSE
Architecture of the OS (SMB/Windows/Arch)
↪                : Empty/None
Build number of the OS (SMB/WindowsBuild)
↪                : Empty/None
Disable file search via WMI on Windows (win/lsc/disable_wmi_search)
↪                : FALSE
Disable the usage of win_cmd_exec for remote commands on Windows (win/lsc/disabl
↪e_win_cmd_exec) : FALSE
Domain used for authenticated scans (kb_smb_domain())
↪                : Empty/None
Enable Detection of Portable Apps on Windows (win/lsc/search_portable_apps)
↪                : FALSE
Extended SMB support available via openvas-smb module (Tools/Present/smb)
↪                : TRUE
Extended WMI support available via openvas-smb module (Tools/Present/wmi)
↪                : TRUE
Login via SMB failed (login/SMB/failed)
↪                : FALSE
Login via SMB successful (login/SMB/success)
↪                : TRUE
Missing access permissions to the registry (SMB/registry_access_missing_permissi
↪ons)            : FALSE
Name of the most recent service pack installed (SMB/CSDVersion)
↪                : Empty/None
Never send SMB credentials in clear text (SMB/dont_send_in_cleartext)
↪                : TRUE
Only use NTLMv2 (SMB/dont_send_ntlmv1)
↪                : FALSE
Path to the OS SystemRoot (smb_get_systemroot())
↪                : Empty/None
Path to the OS SystemRoot for 32bit (smb_get_system32root())
↪                : Empty/None
Port configured for authenticated scans (kb_smb_transport())
↪                : 445/tcp
Port used for the successful login via SMB
↪                : 445/tcp
Product name of the OS (SMB/WindowsName)
```

... continues on next page ...

... continued from previous page ...

```
↪                : Empty/None
SMB name used for authenticated scans (kb_smb_name())
↪                : 192.168.2.1
User used for authenticated scans (kb_smb_login())
↪                : harlin
Version number of the OS (SMB/WindowsVersion)
↪                : Empty/None
Version string of the OS (SMB/WindowsVersionString)
↪                : FALSE
Workgroup of the SMB server (SMB/workgroup)
↪                : Empty/None
```

Solution:

Log Method
Details: Authenticated Scan / LSC Info Consolidation (Windows SMB Login)
OID:1.3.6.1.4.1.25623.1.0.108442
Version used: 2023-08-03T05:05:16Z

References
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html#requiremen
↪ts-on-target-systems-with-microsoft-windows

[return to 192.168.2.1]