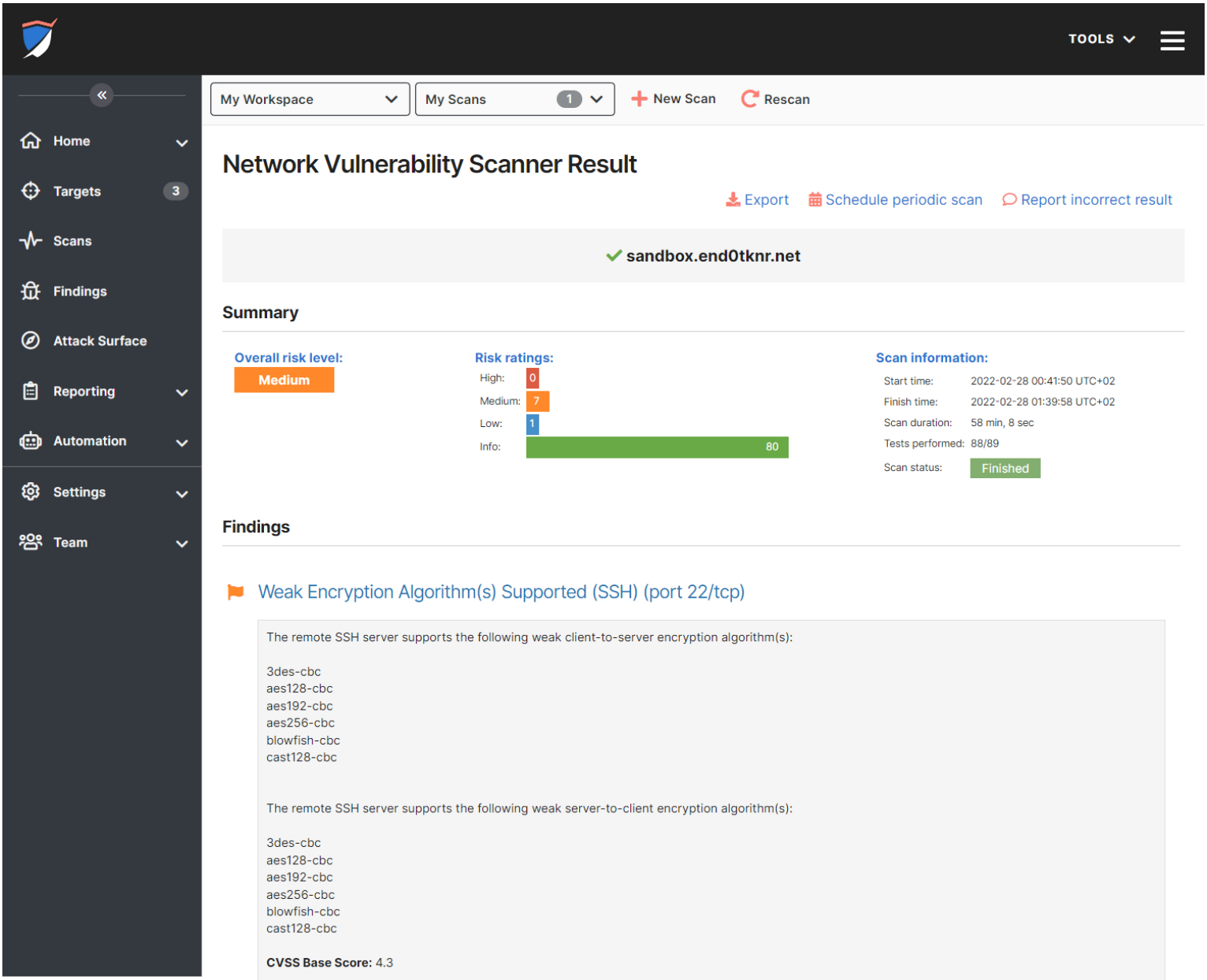
TOOLS
My Workspace
My Scans 1
New Scan
Rescan
Home
Targets 3
Scans
Findings
Attack Surface
Reporting
Automation
Settings
Team
Network Vulnerability Scanner Result
Export
Schedule periodic scan
Report incorrect result
sandbox.end0tknr.net
Summary
Overall risk level:
Medium
Risk ratings:
High: 0
Medium: 7
Low: 1
Info: 80
Scan information:
Start time: 2022-02-28 00:41:50 UTC+02
Finish time: 2022-02-28 01:39:58 UTC+02
Scan duration: 58 min, 8 sec
Tests performed: 88/89
Scan status: Finished
Findings
Weak Encryption Algorithm(s) Supported (SSH) (port 22/tcp)
The remote SSH server supports the following weak client-to-server encryption algorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption algorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
CVSS Base Score: 4.3
CVE: None
Details
Risk description:
The remote SSH server is configured to allow / support weak encryption algorithm(s).
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
Recommendation:
Disable the reported weak encryption algorithm(s).
Read more about this issue:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) (port 22/tcp)
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm | Reason
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1
CVSS Base Score: 4.6
CVE: None

Details

Risk description:
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
- 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime. An attacker can quickly break individual connections.

Recommendation:
Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Read more about this issue:
https://weakdh.org/sysadmin.html
https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html
https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5
https://datatracker.ietf.org/doc/html/rfc6194

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (port 443/tcp)

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

CVSS Base Score: 4.3

CVE: CVE-2011-3389, CVE-2015-0204

Details

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

Recommendation:
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.

Read more about this issue:
https://ssl-config.mozilla.org/
https://bettercrypto.org/
https://datatracker.ietf.org/doc/rfc8996/
https://vnhacker.blogspot.com/2011/09/beast.html
https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (port 443/tcp)

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

CVSS Base Score: 5.0

CVE: CVE-2016-2183, CVE-2016-6329, CVE-2020-12872

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.
These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

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

Read more about this issue:
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

SSL/TLS: Report Weak Cipher Suites (port 443/tcp)

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

CVSS Base Score: 5.0

CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

Details

Risk description:
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

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

Read more about this issue:
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/

HTTP Debugging Methods (TRACE/TRACK) Enabled (port 80/tcp)

The web server has the following HTTP methods enabled: TRACE

CVSS Base Score: 5.8

CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE-2014-7883

Details

Risk description:
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Recommendation:
Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.

Read more about this issue:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trace-verbs/ba-p/784482
https://owasp.org/www-community/attacks/Cross_Site_Tracing

HTTP Debugging Methods (TRACE/TRACK) Enabled (port 443/tcp)

HTTP Debugging Methods (TRACE/TRACK) Enabled (port 443/tcp)

The web server has the following HTTP methods enabled: TRACE

CVSS Base Score: 5.8

CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE-2014-7883

Details

Risk description:
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Recommendation:
Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.

Read more about this issue:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trace-verbs/ba-p/784482
https://owasp.org/www-community/attacks/Cross_Site_Tracing

TCP timestamps

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 503623597
Packet 2: 503624974

CVSS Base Score: 2.6

CVE: None

Details

Risk description:
The remote host implements TCP timestamps and therefore allows to compute the uptime.
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Recommendation:
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

Read more about this issue:
http://www.ietf.org/rfc/rfc1323.txt
http://www.ietf.org/rfc/rfc7323.txt
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Scan coverage information

Port	State	Service	Product	Product Version
22	open	ssh	OpenSSH	7.4
80	open	http	Apache httpd	2.4.52
443	open	https	Apache httpd	2.4.52

Details

Risk description:
This is the list of ports that have been found open on the target hosts. Having unnecessary open ports may expose the target systems to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Not vulnerable to Apache Tomcat - Remote Code Execution (CVE-2017-12617) (port 80)

- Not vulnerable to Apache Server - Arbitrary File Read (CVE-2021-41773) (port 80)
- Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046) (port 80)
- Not vulnerable to Apache Server - Remote Code Execution (CVE-2021-41773) (port 80)
- Not vulnerable to VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 80)
- Not vulnerable to Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 80)
- Not vulnerable to Apache Server Shellshock - Remote Code Execution (CVE-2014-6271) (port 80)
- Not vulnerable to Apache Server - Remote Code Execution (CVE-2021-42013) (port 80)
- Not vulnerable to Node.js Systeminformation - Command Injection (CVE-2021-21315) (port 80)
- Not vulnerable to Apache Struts - Remote Code Execution (CVE-2017-9791) (port 80)
- Not vulnerable to Oracle Weblogic - Path Traversal (CVE-2020-14882) (port 80)
- Not vulnerable to Apache MOD Proxy - Server Side Request Forgery (CVE-2021-40438) (port 80)
- Not vulnerable to Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 80)
- Not vulnerable to Apache Struts 2 - Remote Code Execution (CVE-2018-11776) (port 80)
- Not vulnerable to Apache Struts - Remote Code Execution (CVE-2020-17530) (port 80)
- Not vulnerable to ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539) (port 80)
- Not vulnerable to ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515) (port 80)
- Not vulnerable to Apache OFBiz - Remote Code Execution (CVE-2021-26295) (port 80)
- Not vulnerable to Apache Server - Arbitrary File Read (CVE-2021-42013) (port 80)
- Not vulnerable to Oracle Weblogic - Remote Code Execution (CVE-2018-2894) (port 80)

- Not vulnerable to Apache Struts 2 - Remote Code Execution (CVE-2019-0230) (port 80)
- Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 80)
- Not vulnerable to Apache Tomcat - Remote Code Execution (CVE-2017-12617) (port 443)
- Not vulnerable to Apache Server - Arbitrary File Read (CVE-2021-41773) (port 443)
- Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046) (port 443)
- Not vulnerable to Apache Server - Remote Code Execution (CVE-2021-41773) (port 443)
- Not vulnerable to VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 443)
- Not vulnerable to Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 443)
- Not vulnerable to Apache Server Shellshock - Remote Code Execution (CVE-2014-6271) (port 443)
- Not vulnerable to Apache Server - Remote Code Execution (CVE-2021-42013) (port 443)
- Not vulnerable to Node.js Systeminformation - Command Injection (CVE-2021-21315) (port 443)
- Not vulnerable to Apache Struts - Remote Code Execution (CVE-2017-9791) (port 443)
- Not vulnerable to Oracle Weblogic - Path Traversal (CVE-2020-14882) (port 443)
- Not vulnerable to Apache MOD Proxy - Server Side Request Forgery (CVE-2021-40438) (port 443)
- Not vulnerable to Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 443)
- Not vulnerable to Apache Struts 2 - Remote Code Execution (CVE-2018-11776) (port 443)
- Not vulnerable to Apache Struts - Remote Code Execution (CVE-2020-17530) (port 443)
- Not vulnerable to ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539) (port 443)
- Not vulnerable to ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515) (port 443)

Not vulnerable to Apache OFBiz - Remote Code Execution (CVE-2021-26295) (port 443)

Not vulnerable to Apache Server - Arbitrary File Read (CVE-2021-42013) (port 443)

Not vulnerable to Oracle Weblogic - Remote Code Execution (CVE-2018-2894) (port 443)

Not vulnerable to Apache Struts 2 - Remote Code Execution (CVE-2019-0230) (port 443)

Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 443)

OpenSSH Detection Consolidation

Detected OpenSSH Server

Version: 7.4
Location: 22/tcp
CPE: cpe:/a:openbsd:openssh:7.4

Concluded from version/product identification result:
SSH-2.0-OpenSSH_7.4

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
The script reports a detected OpenSSH including the version number.

Recommendation:

Read more about this issue:
https://www.openssh.com/

Services (port 80/tcp)

A web server is running on this port

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

Services (port 22/tcp)

An ssh server is running on this port

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

Services (port 443/tcp)

A TLScustom server answered on this port

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

Services (port 443/tcp)

A web server is running on this port through SSL

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

SSH Protocol Algorithms Supported (port 22/tcp)

The following options are supported by the remote ssh service:

kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519

encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc

encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc

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

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

compression_algorithms_client_to_server:
none,zlib@openssh.com

compression_algorithms_server_to_client:
none,zlib@openssh.com

CVSS Base Score: 0.0

CVE: None

Details

Risk description:

This script detects which algorithms are supported by the remote SSH Service.

Recommendation:
No recommendation for this issue

SSH Server type and version (port 22/tcp)

Remote SSH server banner: SSH-2.0-OpenSSH_7.4
Remote SSH supported authentication: publickey
Remote SSH text/login banner: (not available)

This is probably:

- OpenSSH

Concluded from remote connection attempt with credentials:

Login: OpenVASVT
Password: OpenVASVT

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
This detects the SSH Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Recommendation:
No recommendation for this issue

SSH Protocol Versions Supported (port 22/tcp)

The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0

SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: af:ce:43:f4:ec:d6:a6:80:81:d5:d4:00:89:68:47:6d
ssh-ed25519: 8d:45:cc:d7:d6:72:02:a0:a1:8b:51:c0:24:ad:12:58
ssh-rsa: 2d:90:95:c5:84:e5:47:34:27:02:8a:23:00:28:10:aa

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service. The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Recommendation:
No recommendation for this issue

SSL/TLS: Version Detection (port 443/tcp)

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

TLSv1.0
TLSv1.1
TLSv1.2

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

OpenSSL Detection Consolidation

Detected OpenSSL

Version: 1.0.2k
Location: 443/tcp
CPE: cpe:/a:openssl:openssl:1.0.2k

Concluded from version/product identification result:
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

Detected OpenSSL

Version: 1.0.2k
Location: 80/tcp
CPE: cpe:/a:openssl:openssl:1.0.2k

Concluded from version/product identification result:
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
Consolidation of OpenSSL detections.

Recommendation:

Read more about this issue:
https://www.openssl.org/

Apache HTTP Server Detection Consolidation

Detected Apache HTTP Server

Version: 2.4.52
Location: 443/tcp
CPE: cpe:/a:apache:http_server:2.4.52

Concluded from version/product identification result:
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

Detected Apache HTTP Server

Version: 2.4.52
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.4.52

Concluded from version/product identification result:
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
Consolidation of Apache HTTP Server detections.

Recommendation:

Read more about this issue:
https://httpd.apache.org

Traceroute

Network route from scanner (172.17.0.2) to target (35.77.196.151):

172.17.0.2
212.111.33.230
109.74.207.20
204.68.252.58
154.54.59.37
154.54.56.130

154.54.72.110
154.54.87.209
154.18.19.162
150.222.3.39
52.93.10.33
52.93.8.111
54.239.43.115
150.222.244.43
150.222.243.157
15.230.160.29
52.95.31.171
52.95.31.158
52.95.31.72
52.93.250.8
15.230.154.143
35.77.196.151

Network distance between scanner and target: 22

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
Collect information about the network route and network distance between the scanner host and the target host.
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.

Recommendation:
No recommendation for this issue

HTTP Server type and version (port 443/tcp)

The remote HTTP Server banner is:

Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

HTTP Server type and version (port 80/tcp)

The remote HTTP Server banner is:

Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing (port 443/tcp)

The remote web server is not enforcing HPKP.

HTTP-Banner:

HTTP/1.1 403 Forbidden
Date: ***replaced***
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips

Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: ***replaced***
ETag: "***replaced***"
Accept-Ranges: bytes
Content-Length: ***replaced***
Content-Type: text/html; charset=UTF-8

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
The remote web server is not enforcing HPKP. Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:
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.

Read more about this issue:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing (port 443/tcp)

The remote web server is not enforcing HSTS.

HTTP-Banner:

HTTP/1.1 403 Forbidden
Date: ***replaced***
Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: ***replaced***
ETag: "***replaced***"
Accept-Ranges: bytes
Content-Length: ***replaced***
Content-Type: text/html; charset=UTF-8

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
The remote web server is not enforcing HSTS.

Recommendation:
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.

Read more about this issue:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: Report Medium Cipher Suites (port 443/tcp)

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendation for this issue

SSL/TLS: Report Non Weak Cipher Suites (port 443/tcp)

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (port 443/tcp)

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_RC4_128_SHA

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:
No recommendation for this issue

SSL/TLS: Report Supported Cipher Suites (port 443/tcp)

'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

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.

'Strong' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA

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.

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service. 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.

Recommendation:
No recommendation for this issue

SSL/TLS: Untrusted Certificate Detection (port 443/tcp)

The remote SSL/TLS server is using the following certificate(s) which failed the verification against the system wide trust store (serial:issuer):

4F295682EAFF9F30:1.2.840.113549.1.9.1=#726F6F744069702D3137322D33312D32322D3135332E61702D6E6F727468656173742D312E636F6D70757465
2E696E7465726E616C,CN=ip-172-31-22-153.ap-northeast-1.compute.internal,OU=ca-490159817457500277,O=Unspecified,C=US (Server certificate)
06CD65C1CAB98075:1.2.840.113549.1.9.1=#726F6F744069702D3137322D33312D32322D3135332E61702D6E6F727468656173742D312E636F6D7075746
52E696E7465726E616C,CN=ip-172-31-22-153.ap-northeast-1.compute.internal,OU=ca-490159817457500277,O=Unspecified,C=US (Certificate in chain)

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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.

Recommendation:
No recommendation for this issue

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection (port 443/tcp)

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.0:HTTP/1.1
TLSv1.1:HTTP/1.1
TLSv1.2:HTTP/1.1

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:

Read more about this issue:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

HTTP Server Banner Enumeration (port 443/tcp)

It was possible to enumerate the following HTTP server banner(s):

Server banner | Enumeration technique

Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips | Valid HTTP 0.9 GET request to '/index.html'

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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).

Recommendation:
No recommendation for this issue

HTTP Security Headers Detection (port 443/tcp)

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/, Note: This is an upcoming header
Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy | https://w3c.github.io/webappsec-feature-policy/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 Permissions Policy
Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#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 help. Note: Most major browsers have dropped / deprecated support for this header 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 supported 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 supported 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 supported 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 supported 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 help.
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 support for this header in 2020.

CVSS Base Score: 0.0

CVE: None

Details

Risk description:

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.

Recommendation:

Read more about this issue:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#div-headers
https://securityheaders.com/

HTTP Security Headers Detection (port 80/tcp)

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/, Note: This is an upcoming header
Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy | https://w3c.github.io/webappsec-feature-policy/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 Permissions Policy
Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#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 supported 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 supported 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 supported 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 supported 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 support for this header in 2020.

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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.

Recommendation:

Read more about this issue:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#div-headers
https://securityheaders.com/

HTTP Server Banner Enumeration (port 80/tcp)

It was possible to enumerate the following HTTP server banner(s):

Server banner | Enumeration technique

Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips | Valid HTTP 0.9 GET request to '/index.html'

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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).

Recommendation:
No recommendation for this issue

OS Detection Consolidation and Reporting

No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify this OS.

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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 portal.

Recommendation:

Read more about this issue:
https://community.greenbone.net/c/vulnerability-tests

Unknown OS and Service Banner Reporting

Unknown banners have been collected which might help to identify the OS running on this host. If these banners containing information about the host OS please report the following information to https://community.greenbone.net/c/vulnerability-tests:

Banner: Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips
Identified from: HTTP Server banner on port 443/tcp

Banner: Server: Apache/2.4.52 () OpenSSL/1.0.2k-fips
Identified from: HTTP Server banner on port 80/tcp

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:

Read more about this issue:
https://community.greenbone.net/c/vulnerability-tests

CGI Scanning Consolidation (port 443/tcp)

The Hostname/IP "sandbox.end0tknr.net" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the 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 NOT able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

https://sandbox.end0tknr.net/
https://sandbox.end0tknr.net/cgi-bin

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

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "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|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://sandbox.end0tknr.net/icons

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:

Read more about this issue:
https://community.greenbone.net/c/vulnerability-tests

CGI Scanning Consolidation (port 80/tcp)

The Hostname/IP "sandbox.end0tknr.net" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the 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 NOT able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

http://sandbox.end0tknr.net/
http://sandbox.end0tknr.net/cgi-bin

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

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "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|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

http://sandbox.end0tknr.net/icons

CVSS Base Score: 0.0

CVE: None

Details

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

Recommendation:

Read more about this issue:
https://community.greenbone.net/c/vulnerability-tests

CPE Inventory

35.77.196.151|cpe:/a:apache:http_server:2.4.52
35.77.196.151|cpe:/a:openbsd:openssh:7.4
35.77.196.151|cpe:/a:openssl:openssl:1.0.2k

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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.

Recommendation:

Read more about this issue:
https://nvd.nist.gov/products/cpe

Hostname Determination Reporting

Hostname determination for IP 35.77.196.151:

Hostname|Source
sandbox.end0tknr.net|Forward-DNS

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
The script reports information on how the hostname of the target was determined.

Recommendation:
No recommendation for this issue

CPE Inventory

35.77.196.151|cpe:/a:apache:http_server:2.4.52
35.77.196.151|cpe:/a:openbsd:openssh:7.4
35.77.196.151|cpe:/a:openssl:openssl:1.0.2k

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
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.

Recommendation:

Read more about this issue:
https://nvd.nist.gov/products/cpe

Hostname Determination Reporting

Hostname determination for IP 35.77.196.151:

Hostname|Source
sandbox.end0tknr.net|Forward-DNS

CVSS Base Score: 0.0

CVE: None

Details

Risk description:
The script reports information on how the hostname of the target was determined.

Recommendation:
No recommendation for this issue

Target hostname resolves to a single IP address

sandbox.end0tknr.net resolves to the following IP address: 35.77.196.151

Details

Risk description:
No risk to display

Recommendation:
No recommendations to show

Scan coverage information

List of tests performed (88/89)

- Checking for open ports...
- Checking for Apache Tomcat - Remote Code Execution (CVE-2017-12617)... (Sniper module)
- Checking for Apache Server - Arbitrary File Read (CVE-2021-41773)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046)... (Sniper module)
- Checking for Apache Server - Remote Code Execution (CVE-2021-41773)... (Sniper module)
- Checking for VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Server Shellshock - Remote Code Execution (CVE-2014-6271)... (Sniper module)
- Checking for Apache Server - Remote Code Execution (CVE-2021-42013)... (Sniper module)
- Checking for Node.js Systeminformation - Command Injection (CVE-2021-21315)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (CVE-2017-9791)... (Sniper module)
- Checking for Oracle Weblogic - Path Traversal (CVE-2020-14882)... (Sniper module)
- Checking for Apache MOD Proxy - Server Side Request Forgery (CVE-2021-40438)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Struts 2 - Remote Code Execution (CVE-2018-11776)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (CVE-2020-17530)... (Sniper module)
- Checking for ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539)... (Sniper module)
- Checking for ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515)... (Sniper module)
- Checking for Apache OFBiz - Remote Code Execution (CVE-2021-26295)... (Sniper module)
- Checking for Apache Server - Arbitrary File Read (CVE-2021-42013)... (Sniper module)
- Checking for Oracle Weblogic - Remote Code Execution (CVE-2018-2894)... (Sniper module)
- Checking for Apache Struts 2 - Remote Code Execution (CVE-2019-0230)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Tomcat - Remote Code Execution (CVE-2017-12617)... (Sniper module)
- Checking for Apache Server - Arbitrary File Read (CVE-2021-41773)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046)... (Sniper module)
- Checking for Apache Server - Remote Code Execution (CVE-2021-41773)... (Sniper module)
- Checking for VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Server Shellshock - Remote Code Execution (CVE-2014-6271)... (Sniper module)
- Checking for Apache Server - Remote Code Execution (CVE-2021-42013)... (Sniper module)
- Checking for Node.js Systeminformation - Command Injection (CVE-2021-21315)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (CVE-2017-9791)... (Sniper module)
- Checking for Oracle Weblogic - Path Traversal (CVE-2020-14882)... (Sniper module)
- Checking for Apache MOD Proxy - Server Side Request Forgery (CVE-2021-40438)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Struts 2 - Remote Code Execution (CVE-2018-11776)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (CVE-2020-17530)... (Sniper module)
- Checking for ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539)... (Sniper module)
- Checking for ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515)... (Sniper module)
- Checking for Apache OFBiz - Remote Code Execution (CVE-2021-26295)... (Sniper module)
- Checking for Apache Server - Arbitrary File Read (CVE-2021-42013)... (Sniper module)
- Checking for Oracle Weblogic - Remote Code Execution (CVE-2018-2894)... (Sniper module)
- Checking for Apache Struts 2 - Remote Code Execution (CVE-2019-0230)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Testing for OpenSSH Detection Consolidation
- Testing for Services
- Testing for Services
- Testing for Services
- Testing for Services
- Testing for SSH Protocol Algorithms Supported
- Testing for SSH Server type and version
- Testing for SSH Protocol Versions Supported
- Testing for SSL/TLS: Version Detection
- Testing for OpenSSL Detection Consolidation
- Testing for Apache HTTP Server Detection Consolidation
- Testing for TCP timestamps
- Testing for Weak Encryption Algorithm(s) Supported (SSH)
- Testing for Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
- Testing for Traceroute
- Testing for HTTP Server type and version
- Testing for HTTP Server type and version
- Testing for SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
- Testing for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
- Testing for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
- Testing for SSL/TLS: Report Medium Cipher Suites

- Testing for SSL/TLS: Report Non Weak Cipher Suites
- Testing for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
- Testing for SSL/TLS: Report Supported Cipher Suites
- Testing for SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
- Testing for SSL/TLS: Report Weak Cipher Suites
- Testing for SSL/TLS: Untrusted Certificate Detection
- Testing for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
- Testing for HTTP Debugging Methods (TRACE/TRACK) Enabled
- Testing for HTTP Debugging Methods (TRACE/TRACK) Enabled
- Testing for HTTP Server Banner Enumeration
- Testing for HTTP Security Headers Detection
- Testing for HTTP Security Headers Detection
- Testing for HTTP Server Banner Enumeration
- Testing for OS Detection Consolidation and Reporting
- Testing for Unknown OS and Service Banner Reporting
- Testing for CGI Scanning Consolidation
- Testing for CGI Scanning Consolidation
- Testing for CPE Inventory
- Testing for Hostname Determination Reporting
- Testing for CPE Inventory
- Testing for Hostname Determination Reporting
- Testing for hostname DNS resolution...

Scan parameters

Target:	sandbox.end0tknr.net
Scan type:	Full
Check alive:	True
Protocol type:	Tcp
Ports to scan:	OpenVAS default