OPENVAS NETWORK VULNERABILITY SCAN

ATTACKER'S NARRATIVE

An attacker targeting scanme.nmap.org could exploit multiple SSH vulnerabilities to compromise the system. The server supports weak SSH configurations including vulnerable host key algorithms (ssh-dss), weak key exchange algorithms (diffie-hellman-group1-sha1), weak encryption algorithms (3des-cbc, arcfour), and weak MAC algorithms (hmac-md5). These vulnerabilities could be chained together to perform man-in-the-middle attacks, decrypt communications, or potentially gain unauthorized access to the system. The server is running OpenSSH 6.6.1p1 on Ubuntu 14.04, which is outdated and likely contains additional security vulnerabilities.

The TCP timestamps feature is also enabled, allowing attackers to determine system uptime and potentially time their attacks accordingly. Additionally, the web server (Apache 2.4.7) lacks important security headers such as Content-Security-Policy, X-Content-Type-Options, and X-Frame-Options, which could expose the web application to various attacks including cross-site scripting and clickjacking.

To remediate these issues, administrators should disable weak SSH algorithms by updating the SSH configuration to only allow secure algorithms for host keys, key exchange, encryption, and MAC. The system should be updated to a current version of Ubuntu and OpenSSH. TCP timestamps should be disabled by adding 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. For the web server, implement recommended security headers and update Apache to the latest version. Regular security scans should be conducted to identify and address new vulnerabilities as they emerge.

Scan Report

April 5, 2026

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 "Full Fast Alive Scan of Recurring Test". The scan started at Sun Apr 5 20:57:00 2026 UTC and ended at Sun Apr 5 21:33:31 2026 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
45.33.32.156 scanme.nmap.org	0	3	2	19	0
2600:3c01::f03c:91ff:fe18:bb2f scanme.nmap.org	0	0	0	2	0
Total: 2	0	3	2	21	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 "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 26 results selected by the filtering described above. Before filtering there were 85 results.

2 Results per Host

2.1 45.33.32.156

Host scan start	Sun Apr 5 20:57:11 2026 UTC
Host scan end	Sun Apr 5 21:33:25 2026 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Low
22/tcp	Low
80/tcp	Log
general/tcp	Log
31337/tcp	Log
22/tcp	Log
9929/tcp	Log
general/CPE-T	Log
123/udp	Log

2.1.1 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
---
ssh-dss | Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: Weak Host Key Algorithm(s) (SSH)
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
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
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

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.

Vulnerability Insight

- 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.

Vulnerability Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1

. . . continues on next page . . .

... continued from previous page ...

- using RSA 1024-bit modulus key
Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

... continues on next page ...

... continued from previous page ...

The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- 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.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: Weak Encryption Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563

... continues on next page ...

... continued from previous page ...

url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[return to 45.33.32.156]

2.1.2 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3236407442
Packet 2: 3236408550

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

... continues on next page ...

... continued from previous page ...

Details: TCP Timestamps Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2023-12-15T16:10:08Z

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 45.33.32.156]

2.1.3 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
hmac-md5
hmac-md5-96

... continues on next page ...

... continued from previous page ...

```
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 45.33.32.156]

2.1.4 Log 80/tcp

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.

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "scanme.nmap.org" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 23.35.3)" was used to acces
↪s 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://scanme.nmap.org/
http://scanme.nmap.org/search
http://scanme.nmap.org/shared
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?/)"
http://scanme.nmap.org/icons
http://scanme.nmap.org/images
http://scanme.nmap.org/shared/css
http://scanme.nmap.org/shared/images
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://scanme.nmap.org/search/ (q [] )
The following cgi scripts were excluded from web application scanning because of
```

... continues on next page ...

... continued from previous page ...

↪ 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://scanme.nmap.org/shared/css/nst-foot.css (v [2])
http://scanme.nmap.org/shared/css/nst.css (v [2])

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: 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: Apache/2.4.7 (Ubuntu)

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 Security Headers Detection

Summary

... continues on next page ...

... continued from previous page ...

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
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
```

... continues on next page ...

... continued from previous page ...

```
↪/#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 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: Apache/2.4.7 (Ubuntu) | 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: 2022-06-28T10:11:01Z

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 45.33.32.156]

2.1.5 Log general/tcp

Log (CVSS: 0.0)

NVT: OpenSSH Detection Consolidation

Summary
Consolidation of OpenSSH detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected OpenSSH Server
Version:       6.6.1p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:6.6.1p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2022-03-28T10:48:38Z`

References
`url: https://www.openssh.com/`

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 45.33.32.156:
Hostname|Source
scanme.nmap.org|Forward-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: Traceroute

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

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Network route from scanner (172.31.2.154) to target (45.33.32.156):
172.31.2.154
240.3.180.14
240.64.220.129
151.148.14.42
151.148.14.43
23.209.165.97
23.32.62.79
23.207.232.37
23.203.158.53
45.33.32.156
Network distance between scanner and target: 10
```

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: Apache HTTP Server Detection Consolidation

Summary

Consolidation of Apache HTTP Server detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Apache HTTP Server
Version:       2.4.7
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.7
Concluded from version/product identification result:
Server: Apache/2.4.7 (Ubuntu)
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Apache HTTP Server Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: `2024-03-08T15:37:10Z`

References
`url: https://httpd.apache.org`

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:           Ubuntu 14.04
Version:      14.04
CPE:          cpe:/o:canonical:ubuntu_linux:14.04
Found by VT:  1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH
↪ Banner))
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu
↪2.13
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
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 80/tcp: Server: Apache/2.4.7 (Ubuntu)
```

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2024-10-11T15:39:44Z

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

[return to 45.33.32.156]

2.1.6 Log 31337/tcp

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

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: 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)

... continues on next page ...

... continued from previous page ...

- 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

```
Nmap service detection (wrapped) result for this port: tcpwrapped
```

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
```

[return to 45.33.32.156]

2.1.7 Log 22/tcp

Log (CVSS: 0.0)

NVT: SSH Server type and version

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVASVT
Password: OpenVASVT
```

... continues on next page ...

... continued from previous page ...

Solution:

Vulnerability Insight
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2024-08-02T05:05:39Z`

Log (CVSS: 0.0)

NVT: SSH Protocol Algorithms Supported

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following options are supported by the remote SSH service:
kex_algorithms:
curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nis
↪tp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,
↪diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,ae
↪s256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfis
↪h-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,ae
↪s256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfis
↪h-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server:
hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-
↪128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.co
↪m,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@
↪openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-s
↪ha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,h
↪mac-md5-96
mac_algorithms_server_to_client:
```

... continues on next page ...

... continued from previous page ...

```
hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-
↪128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.co
↪m,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@
↪openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-s
↪ha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,h
↪mac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Solution:

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2024-06-17T08:31:37Z`

Log (CVSS: 0.0)

NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57
ssh-ed25519: 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56
ssh-rsa: 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2
```

Solution:

Log Method
The following versions are tried: 1.33, 1.5, 1.99 and 2.0.
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `2024-06-17T08:31:37Z`

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`An ssh 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 45.33.32.156]

2.1.8 Log 9929/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`An nping-echo server seems to be running on this port.`

Solution:

Vulnerability Insight
. . . continues on next page . . .

... continued from previous page ...

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2024-09-27T05:05:23Z`

[return to 45.33.32.156]

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`45.33.32.156|cpe:/a:apache:http_server:2.4.7`
`45.33.32.156|cpe:/a:ietf:secure_shell_protocol:2.0`
`45.33.32.156|cpe:/a:openbsd:openssh:6.6.1p1`
`45.33.32.156|cpe:/o:canonical:ubuntu_linux:14.04`

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 45.33.32.156]

2.1.10 Log 123/udp

Log (CVSS: 0.0) NVT: Network Time Protocol (NTP) / NTPd / NTPsec Detection (UDP)
Summary UTP based detection of services supporting the Network Time Protocol (NTP). In addition to the protocol itself the existence of the ntpd (NTPd) / NTPsec daemon is detected as well.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Quickfix: Restrict default access to ignore all info packets.
Vulnerability Insight It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings.
Log Method Details: `Network Time Protocol (NTP) / NTPd / NTPsec Detection (UDP)` OID:1.3.6.1.4.1.25623.1.0.10884 Version used: `2024-02-20T14:37:13Z`

References
`url: https://www.eecis.udel.edu/~mills/ntp/html/ntpd.html`
`url: https://www.ntp.org/`
`url: https://www.ntpsec.org/`

[return to 45.33.32.156]

2.2 2600:3c01::f03c:91ff:fe18:bb2f

Host scan start	Sun Apr 5 20:57:11 2026 UTC
Host scan end	Sun Apr 5 20:57:23 2026 UTC

Service (Port)	Threat Level
general/tcp	Log

2.2.1 Log general/tcp

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
```
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.
```

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2024-10-11T15:39:44Z`

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

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 2600:3c01::f03c:91ff:fe18:bb2f:
Hostname|Source
scanme.nmap.org|Forward-DNS
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

[return to 2600:3c01::f03c:91ff:fe18:bb2f]
