Scan Report

December 9, 2018

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 "rz.lab - internal network assessment". The scan started at Sun Dec 9 15:22:26 2018 UTC and ended at Sun Dec 9 16:10:43 2018 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
10.100.10.1 router.rz.lab	1	4	0	23	0
10.100.10.2 acs.rz.lab	0	3	0	24	0
10.100.10.3 utility.rz.lab	0	3	1	37	0
10.100.10.4 dc.rz.lab	0	3	0	39	0
10.100.10.11 docker-manager.rz.lab	0	3	1	29	0
10.100.10.12 docker-worker.rz.lab	0	3	1	28	0
Total: 6	1	19	3	180	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.

This report contains all 203 results selected by the filtering described above. Before filtering there were 203 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.100.10.1 - router.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.2 - acs.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.3 - utility.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.4 - dc.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.11 - docker-manager.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant
10.100.10.12 - docker-worker.rz.lab	SSH	Success	Protocol SSH, Port 22, User vagrant

2 Results per Host

2.1 10.100.10.1

Host scan start	Sun Dec 9 15:22:43 2018 UTC
Host scan end	Sun Dec 9 16:00:13 2018 UTC

Service (Port)	Threat Level
53/tcp	High
22/tcp	Medium
general/tcp	Medium
53/tcp	Medium
22/tcp	Log
general/CPE-T	Log
general/icmp	Log
general/tcp	Log
53/tcp	Log
general/HOST-T	Log

2.1.1 High 53/tcp

High (CVSS: 7.8)
NVT: ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability

Product detection result
`cpe:/a:isc:bind:9.11.3.1ubuntu1.3`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to a denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.11.3.1ubuntu1.3`
`Fixed version: 9.11.4-P1`

Impact
Successful exploitation will allow remote attackers to cause a denial of service (assertion failure).

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.13-P1 or 9.10.8-P1 or 9.11.4-P1 or 9.12.2-P1 or 9.11.3-S3 or later. For updates refer to Reference links.

Affected Software/OS
ISC BIND versions 9.7.0 through 9.8.8, 9.9.0 through 9.9.13, 9.10.0 through 9.10.8, 9.11.0 through 9.11.4, 9.12.0 through 9.12.2 and 9.13.0 through 9.13.2.

Vulnerability Insight
The flaw exists due to a defect in the feature 'deny-answer-aliases' which leads to assertion failure in 'name.c'.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ISC BIND 'deny-answer-aliases' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.813750
Version used: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2018-5740
Other:
URL:https://kb.isc.org/article/AA-01639/0
URL:https://kb.isc.org/article/AA-01646/81/BIND-9.11.3-S3-Release-Notes.html
URL:https://kb.isc.org/article/AA-01645/81/BIND-9.12.2-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01644/81/BIND-9.11.4-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01643/81/BIND-9.10.8-P1-Release-Notes.html
URL:https://kb.isc.org/article/AA-01642/81/BIND-9.9.13-P1-Release-Notes.html
URL:https://www.isc.org

[return to 10.100.10.1]

2.1.2 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15919`
`Other:`
`URL:http://www.openssh.com`
`URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`URL:https://seclists.org/oss-sec/2018/q3/180`

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15473
Other:
URL:http://www.openssh.com
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

[return to 10.100.10.1]

2.1.3 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 12690 $`

References
```
CVE: CVE-2009-2624
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 10.100.10.1]

2.1.4 Medium 53/tcp

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability

. . . continues on next page . . .

... continued from previous page ...

Product detection result
cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND is prone to a remote denial-of-service vulnerability because the application fails to properly handle specially crafted dynamic update requests.

Vulnerability Detection Result
It seems that OpenVAS was able to crash the remote Bind.
Please check its status right now.

Impact
Successfully exploiting this issue allows remote attackers to crash affected DNS servers, denying further service to legitimate users.

Solution
Solution type: VendorFix
The vendor released an advisory and fixes to address this issue. Please see the references for more information.

Affected Software/OS
Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 are vulnerable.

Vulnerability Detection Method
Details: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100251
Version used: $Revision: 4436 $

Product Detection Result
Product: cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2009-0696
BID:35848
Other:
URL:http://www.securityfocus.com/bid/35848
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514292
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=538975
URL:http://www.isc.org/products/BIND/
URL:https://www.isc.org/node/474
URL:http://www.kb.cert.org/vuls/id/725188

[return to 10.100.10.1]

2.1.5 Log 22/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
`This port was detected as being open by a port scanner but is now closed.`
`This service might have been crashed by a port scanner or by a plugin`

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `$Revision: 5348 $`

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
```
It was possible to login using the provided SSH credentials. Hence authenticated
↪ checks are enabled.
```

Log Method
Details: `SSH Authorization Check`
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: `$Revision: 10873 $`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
```

... continues on next page ...

... continued from previous page ...

```
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@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 9609 $

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: f0:32:b8:97:a8:41:86:e9:a5:62:f0:c0:20:b4:fa:32
ssh-ed25519: 94:8d:6f:a4:34:4a:23:26:f5:fa:1f:6b:27:d9:a5:d8
ssh-rsa: a5:66:fa:54:40:6c:d2:2f:b5:0e:fd:e0:85:7f:28:f8
```

Log Method
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 10929 $

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

Vulnerability Detection Result
```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 10902 $`

[return to 10.100.10.1]

2.1.6 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
```
10.100.10.1|cpe:/a:gnu:bash:4.4.19
10.100.10.1|cpe:/a:gnu:gzip:1.2.4
10.100.10.1|cpe:/a:gnu:gzip:1.6
10.100.10.1|cpe:/a:isc:bind:9.11.3.1ubuntu1.3
10.100.10.1|cpe:/a:isc:dhcp:4.3.5
10.100.10.1|cpe:/a:openbsd:openssh:7.6p1
10.100.10.1|cpe:/a:openssl:openssl:1.1.0g
10.100.10.1|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
10.100.10.1|cpe:/a:vmware:open-vm-tools:10.3.0.5330
10.100.10.1|cpe:/o:canonical:ubuntu_linux:18.04:-:lts
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 12413 $`

[return to 10.100.10.1]

2.1.7 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

Log (CVSS: 0.0)
NVT: Record route

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
`Here is the route recorded between 10.100.10.105 and 10.100.10.1 :`
`10.100.10.1.`
`10.100.10.1.`

Log Method

... continues on next page ...

... continued from previous page ...

Details: Record route
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: $Revision: 10411 $

[return to 10.100.10.1]

2.1.8 Log general/tcp

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result
```
Detected GNU bash
Version:  4.4.19
Location: /bin/bash
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: GNU Bash Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: $Revision: 12551 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
```

... continues on next page ...

... continued from previous page ...

```
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method
Details: `ISC DHCP Client Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result
```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method
Details: `OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 11279 $`

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

Summary

. . . continues on next page . . .

... continued from previous page ...

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

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.108014 (DNS Server OS Identification)
Concluded from DNS server banner on port 53/tcp: 9.11.3-1ubuntu1.3-Ubuntu
```

Log Method

Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 12700 $

References

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary

Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
```

... continues on next page ...

... continued from previous page ...

```
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
```

Log Method
Details: Ruby Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary
This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                                                  Value/Content
----------------------------------
↪                                                  -------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find)  : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪                                                  : 1
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                  : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                  : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                  : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)              : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                  : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                  : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                  : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                  : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                               : FALSE
Login successful (login/SSH/success)
↪                                                  : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                  : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
```

... continues on next page ...

... continued from previous page ...

```
↪                                                    : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                    : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)               : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                    : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                    : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                    : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                    : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                    : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                    : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                    : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                    : vagrant
locate: Command available (ssh/locate/available)
↪                                                    : TRUE
```

Log Method
Details: SSH Authenticated Scan Info Consolidation
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: $Revision: 9954 $

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result

```
Here is the route from 10.100.10.105 to 10.100.10.1:
10.100.10.105
10.100.10.1
```

Solution
Block unwanted packets from escaping your network.

Log Method

... continues on next page ...

. . . continued from previous page . . .

Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
```
VMware Open Virtual Machine Tools  version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host
```

Log Method
Details: VMware Open Virtual Machine Tools Version Detection
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: $Revision: 11015 $

[return to 10.100.10.1]

2.1.9 Log 53/tcp

Log (CVSS: 0.0)
NVT: Determine which version of BIND name daemon is running

Summary
BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.

Vulnerability Detection Result
```
Detected Bind
Version:  9.11.3.1ubuntu1.3
Location: 53/tcp
CPE:      cpe:/a:isc:bind:9.11.3.1ubuntu1.3
Concluded from version/product identification result:
9.11.3-1ubuntu1.3-Ubuntu
```

Solution
Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

Log Method
Details: `Determine which version of BIND name daemon is running`
OID:1.3.6.1.4.1.25623.1.0.10028
Version used: `$Revision: 10945 $`

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

Summary
A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result
```
The remote DNS server banner is:
9.11.3-1ubuntu1.3-Ubuntu
```

Log Method
Details: `DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `$Revision: 8140 $`

[return to 10.100.10.1]

2.1.10 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
```
traceroute:10.100.10.105,10.100.10.1
TCP ports:22,53
UDP ports:
```

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 10.100.10.1]

2.2 10.100.10.2

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 15:56:45 2018 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Medium
22/tcp	Log
general/HOST-T	Log
general/tcp	Log
general/icmp	Log
general/CPE-T	Log

2.2.1 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15919
Other:
  URL:http://www.openssh.com
   URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
```
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

[return to 10.100.10.2]

2.2.2 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 12690 $`

References
`CVE: CVE-2009-2624`
`BID:37888`
`Other:`
`URL:http://secunia.com/advisories/38132`
`URL:http://www.vupen.com/english/advisories/2010/0185`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711`
`URL:http://www.gzip.org/index-f.html#sources`
`URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338`
`↪1dba5032f4dfc1744cf2`

[return to 10.100.10.2]

2.2.3 Log 22/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
`This port was detected as being open by a port scanner but is now closed.`
`This service might have been crashed by a port scanner or by a plugin`

Log Method
Details: `Check open ports`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `$Revision: 5348 $`

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 10922 $

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
```
It was possible to login using the provided SSH credentials. Hence authenticated
↪ checks are enabled.
```

Log Method
Details: SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: $Revision: 10873 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-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@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
```

... continues on next page ...

... continued from previous page ...

```
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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
```

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `$Revision: 9609 $`

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: 65:99:a2:6f:47:cf:0a:5b:01:e1:05:e5:11:07:fc:9d
ssh-ed25519: d0:b7:f3:81:49:87:5b:ea:77:8e:53:a9:58:be:3e:f5
ssh-rsa: b9:a1:13:89:9e:76:4d:c2:0d:e8:88:a1:42:41:63:09
```

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 10929 $`

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

Vulnerability Detection Result

```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
```

... continues on next page ...

... continued from previous page ...

```
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 10902 $`

[return to 10.100.10.2]

2.2.4 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result

```
traceroute:10.100.10.105,10.100.10.2
TCP ports:22
UDP ports:
```

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 10.100.10.2]

2.2.5 Log general/tcp

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detects the installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Detected GNU GCC
Version:  7
Location: /usr/bin/gcc
CPE:      cpe:/a:gnu:gcc:7
Concluded from version/product identification result:
gcc-7
```

Log Method
Details: GCC Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: $Revision: 10901 $

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result

```
Detected GNU bash
Version:  4.4.19
Location: /bin/bash
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: GNU Bash Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: $Revision: 12551 $

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary
This script finds the GNU Binutils installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result

```
Detected GNU Binutils
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
```

... continues on next page ...

... continued from previous page ...

```
Concluded from version/product identification result:
2.30
```

Log Method
Details: GNU Binutils Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: $Revision: 10906 $

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary
This script finds the GNU Assembler installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result

```
Detected GNU assembler
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method
Details: GNU_Assembler Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
```

... continues on next page ...

... continued from previous page ...

```
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method
Details: `ISC DHCP Client Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result
```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method
Details: `OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 11279 $`

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

Summary

. . . continues on next page . . .

... continued from previous page ...

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

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 12700 $`

References

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary

Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: Ruby Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary
This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                                                  Value/Content
---------------------------------
↪                                                  -------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find)  : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪                                                  : None
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                  : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                  : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                  : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)              : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                  : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                  : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                  : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                  : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                               : FALSE
Login successful (login/SSH/success)
↪                                                  : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                  : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                  : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                  : Not applicable for target
```

... continues on next page ...

... continued from previous page ...

```
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)        : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                             : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                             : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                             : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                             : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                             : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                             : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                             : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                             : vagrant
locate: Command available (ssh/locate/available)
↪                                             : TRUE
```

Log Method
Details: SSH Authenticated Scan Info Consolidation
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: $Revision: 9954 $

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result

```
Here is the route from 10.100.10.105 to 10.100.10.2:
10.100.10.105
10.100.10.2
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
`VMware Open Virtual Machine Tools version 10.3.0.5330 build 8931395 running at ↪location /usr/bin/vmtoolsd was detected on the host`

Log Method
Details: `VMware Open Virtual Machine Tools Version Detection`
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: `$Revision: 11015 $`

[return to 10.100.10.2]

2.2.6 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

Log (CVSS: 0.0)
NVT: Record route

. . . continues on next page . . .

... continued from previous page ...

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
```
Here is the route recorded between 10.100.10.105 and 10.100.10.2 :
10.100.10.2.
10.100.10.2.
```

Log Method
Details: `Record route`
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: `$Revision: 10411 $`

[return to 10.100.10.2]

2.2.7 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
```
10.100.10.2|cpe:/a:gnu:bash:4.4.19
10.100.10.2|cpe:/a:gnu:binutils:2.30
10.100.10.2|cpe:/a:gnu:gcc:7
10.100.10.2|cpe:/a:gnu:gzip:1.2.4
10.100.10.2|cpe:/a:gnu:gzip:1.6
10.100.10.2|cpe:/a:isc:dhcp:4.3.5
10.100.10.2|cpe:/a:openbsd:openssh:7.6p1
10.100.10.2|cpe:/a:openssl:openssl:1.1.0g
10.100.10.2|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
10.100.10.2|cpe:/a:vmware:open-vm-tools:10.3.0.5330
10.100.10.2|cpe:/o:canonical:ubuntu_linux:18.04:-:lts
```

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 12413 $`

[return to 10.100.10.2]

2.3 10.100.10.3

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:10:40 2018 UTC

Service (Port)	Threat Level
general/tcp	Medium
22/tcp	Medium
general/tcp	Low
general/tcp	Log
22/tcp	Log
5601/tcp	Log
9200/tcp	Log
9600/tcp	Log
5000/tcp	Log
general/CPE-T	Log
general/icmp	Log
general/HOST-T	Log
9300/tcp	Log

2.3.1 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

References
CVE: CVE-2009-2624
BID:37888
Other:
URL:http://secunia.com/advisories/38132
URL:http://www.vupen.com/english/advisories/2010/0185
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
URL:http://www.gzip.org/index-f.html#sources
URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2

[return to 10.100.10.3]

2.3.2 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15919`
`Other:`
`URL:http://www.openssh.com`
`URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`URL:https://seclists.org/oss-sec/2018/q3/180`

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15473`
`Other:`
`URL:http://www.openssh.com`
`URL:https://0day.city/cve-2018-15473.html`
`URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a`
`↪7d1e0`

[return to 10.100.10.3]

2.3.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1240493766
Packet 2: 1240494778

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

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

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.
Details: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 10411 $

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

Note

```
vagrant@utility:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE                                                  CO
↪MMAND                  CREATED             STATUS              PORTS
```

... continues on next page ...

... continued from previous page ...

```
↪      NAMES
b0a03ad874e7        docker.elastic.co/logstash/logstash-oss:6.5.0             "/
↪usr/local/bin/dock..."   3 days ago          Up 3 days           5044/tcp, 9600/
↪tcp   elk_logstash.1.zsdd592xd2tz8z94j5y5blf2w
514bf68d6ad3        docker.elastic.co/elasticsearch/elasticsearch-oss:6.5.0   "/
↪usr/local/bin/dock..."   3 days ago          Up 3 days           9200/tcp, 9300/
↪tcp   elk_elasticsearch.1.jbtbx5yenu3bu1j3bkwncbymq
ec510d73f649        docker.elastic.co/kibana/kibana-oss:6.5.0                 "/
↪usr/local/bin/kiba..."   3 days ago          Up 3 days           5601/tcp
↪      elk_kibana.1.tpo6edfno68tk3lkycac6ipax
tcp_timestamps Status for guest containers:
b0a03ad874e7: net.ipv4.tcp_timestamps = 1
514bf68d6ad3: net.ipv4.tcp_timestamps = 1
ec510d73f649: net.ipv4.tcp_timestamps = 1
Container host confirmed to have mitigated this vulnerability detection result.
elasticsearch container image confirmed to be implementing RFC 1323
kibana container image confirmed to be implementing RFC 1323
logstash container image confirmed to be implementing RFC 1323
```

Last modified: Sun Dec 9 16:17:04 2018 UTC

[return to 10.100.10.3]

2.3.4 Log general/tcp

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detects the installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result

```
Detected GNU GCC
Version:  7
Location: /usr/bin/gcc
CPE:      cpe:/a:gnu:gcc:7
Concluded from version/product identification result:
gcc-7
```

Log Method
Details: `GCC Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: `$Revision: 10901 $`

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result
```
Detected GNU bash
Version:  4.4.19
Location: /bin/bash
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: `GNU Bash Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: `$Revision: 12551 $`

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary
This script finds the GNU Binutils installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result
```
Detected GNU Binutils
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method
Details: `GNU Binutils Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: `$Revision: 10906 $`

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary
This script finds the GNU Assembler installed version on Linux.

. . . continues on next page . . .

... continued from previous page ...

The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result

```
Detected GNU assembler
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method

Details: GNU_Assembler Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary

Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method

Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

... continues on next page ...

... continued from previous page ...

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method

... continues on next page ...

. . . continued from previous page . . .

Details: ISC DHCP Client Version Detection
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result

```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method
Details: OpenSSL Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: $Revision: 11279 $

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

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

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
```

. . . continues on next page . . .

... continued from previous page ...

```
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 12700 $`

References

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary
Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
```

Log Method
Details: `Ruby Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary
This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                                                    Value/Content
```

... continues on next page ...

... continued from previous page ...

```
----------------------------------
↪                                                 -------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find)  : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪                                                 : 25
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                 : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                 : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                 : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)                 : no
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                 : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                 : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                 : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                 : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                              : FALSE
Login successful (login/SSH/success)
↪                                                 : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                 : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                 : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                 : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)            : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                 : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                 : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                 : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                 : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                 : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                 : Not applicable for target
Solaris version (ssh/login/solosversion)
```

... continues on next page ...

... continued from previous page ...

```
↪                                                    : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                    : vagrant
locate: Command available (ssh/locate/available)
↪                                                    : TRUE
```

Log Method
Details: SSH Authenticated Scan Info Consolidation
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: $Revision: 9954 $

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result

```
Here is the route from 10.100.10.105 to 10.100.10.3:
10.100.10.105
10.100.10.3
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result

```
VMware Open Virtual Machine Tools  version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host
```

Log Method

... continues on next page ...

... continued from previous page ...

Details: `VMware Open Virtual Machine Tools Version Detection`
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: `$Revision: 11015 $`

[return to 10.100.10.3]

2.3.5 Log 22/tcp

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

An ssh server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 10922 $

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
It was possible to login using the provided SSH credentials. Hence authenticated checks are enabled.

Log Method
Details: SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: $Revision: 10873 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-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@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:

... continues on next page ...

... continued from previous page ...

```
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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
```

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `$Revision: 9609 $`

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: 48:b5:1a:94:51:20:c0:6a:e6:e7:1f:a4:1e:eb:50:a9
ssh-ed25519: 82:c8:42:10:33:d4:ac:6f:7c:ae:e8:f8:24:82:a9:7b
ssh-rsa: 70:09:92:aa:a2:0f:8e:f2:e4:99:59:db:5f:75:ba:fb
```

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 10929 $`

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.

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result

```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method

Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 10902 $`

[return to 10.100.10.3]

2.3.6 Log 5601/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

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

Vulnerability Detection Result

```
The Hostname/IP "utility.rz.lab" 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.
```

... continues on next page ...

... continued from previous page ...

```
The User-Agent "Mozilla/5.0 [en] (X11, U; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://utility.rz.lab:5601/
http://utility.rz.lab:5601/core
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

Log (CVSS: 0.0)
NVT: Elasticsearch Kibana/X-Pack Version Detection

Summary
Detection of installed version of Elasticsearch Kibana and X-Pack.
This script sends HTTP GET request and try to ensure the presence of Elasticsearch Kibana and X-Pack from the response.

Vulnerability Detection Result

```
Detected Elasticsearch Kibana
Version:  6.5.0
Location: /
CPE:      cpe:/a:elasticsearch:kibana:6.5.0
Concluded from version/product identification result:
version&quot;:&quot;6.5.0
```

Log Method
Details: Elasticsearch Kibana/X-Pack Version Detection
OID:1.3.6.1.4.1.25623.1.0.808087
Version used: $Revision: 10890 $

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 host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

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

Log Method

Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

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

Log (CVSS: 0.0)
NVT: Services

Summary

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

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

[return to 10.100.10.3]

2.3.7 Log 9200/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

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

Vulnerability Detection Result
```
The Hostname/IP "utility.rz.lab" 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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://utility.rz.lab:9200/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 11638 $`

Log (CVSS: 0.0)
NVT: Elasticsearch and Logstash Detection

Summary
Check for the version of Elasticsearch.

. . . continues on next page . . .

... continued from previous page ...

The script sends a connection request to the server and attempts to extract the version number from the reply. Once a Elasticsearch service was detected it is assumed that Logstash is installed in the same version (ELK Stack).

Vulnerability Detection Result

```
Detected Elasticsearch
Version:  6.5.0
Location: /
CPE:      cpe:/a:elasticsearch:elasticsearch:6.5.0
Concluded from version/product identification result:
number" : "6.5.0",
Extra information:
Collected information (truncated) from http://utility.rz.lab:9200/_cat/indices?v
↪ :
health status index                       uuid                   pri rep docs.co
↪unt docs.deleted store.size pri.store.size
yellow open   metricbeat-6.5.1-2018.12.08 2BP-YJcoQvawxJJaKg2Aiw   1   1     965
↪220            0    469.2mb        469.2mb
yellow open   filebeat-6.5.1-2018.12.05   X8HK-ZG8QDGjQAQXaLCZbg   5   1
↪  0            0      1.2kb          1.2kb
yellow open   logstash-2018.12.09         L1wSgT8nQwWhe-r3V6j0Xg   5   1
↪525            0    473.2kb        473.2kb
yellow open   metricbeat-6.5.1-2018.12.07 TBBUnfd8R7uy6rsaObbIAw   1   1     954
↪143            0    457.4mb        457.4mb
yellow open   filebeat-6.5.1-2018.12.06   hbxkLtuTTj-0hFF8GY8orw   5   1     172
↪797            0     33.9mb         33.9mb
yellow open   metricbeat-6.5.1-2018.12.09 8eg6D79ET3SoNftPL5uZaw   1   1     623
↪548            0    336.4mb        336.4mb
yellow open   filebeat-6.5.1-2018.12.09   w1JI8WUgScalj76K1RjIBw   5   1     141
↪642            0     28.1mb         28.1mb
yellow open   fil
Detected Logstash
Version:  6.5.0
Location: /
CPE:      cpe:/a:elasticsearch:logstash:6.5.0
Concluded from version/product identification result:
Existence of Elasticsearch service, the actual version of the Logstash service m
↪ight differ.
```

Log Method

Details: Elasticsearch and Logstash Detection
OID:1.3.6.1.4.1.25623.1.0.105031
Version used: $Revision: 10400 $

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result

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

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: $Revision: 10899 $

References

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

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 10922 $

[return to 10.100.10.3]

2.3.8 Log 9600/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

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

Vulnerability Detection Result
```
The Hostname/IP "utility.rz.lab" 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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://utility.rz.lab:9600/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 11638 $`

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 host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Header Name                Header Value
-----------                ------------
X-Content-Type-Options  : nosniff
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: $Revision: 10899 $

References

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

Log (CVSS: 0.0)
NVT: Services

Summary

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

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method

Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 10922 $

[return to 10.100.10.3]

2.3.9 Log 5000/tcp

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for VTUN
```

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

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

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

Vulnerability Detection Result
```
Nmap service detection result for this port: upnp
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 5000 10.100.10.3' and submit a possible collected f
↪ingerprint to the nmap database.
```

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 11748 $`

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

[return to 10.100.10.3]

2.3.10 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
Vulnerability Detection Result 10.100.10.3|cpe:/a:elasticsearch:elasticsearch:6.5.0 10.100.10.3|cpe:/a:elasticsearch:kibana:6.5.0 10.100.10.3|cpe:/a:elasticsearch:logstash:6.5.0 10.100.10.3|cpe:/a:gnu:bash:4.4.19 10.100.10.3|cpe:/a:gnu:binutils:2.30 10.100.10.3|cpe:/a:gnu:gcc:7 10.100.10.3|cpe:/a:gnu:gzip:1.2.4 10.100.10.3|cpe:/a:gnu:gzip:1.6 10.100.10.3|cpe:/a:isc:dhcp:4.3.5 10.100.10.3|cpe:/a:openbsd:openssh:7.6p1 10.100.10.3|cpe:/a:openssl:openssl:1.1.0g 10.100.10.3|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57 10.100.10.3|cpe:/a:vmware:open-vm-tools:10.3.0.5330 10.100.10.3|cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: $Revision: 12413 $

[return to 10.100.10.3]

2.3.11 Log general/icmp

Log (CVSS: 0.0) NVT: ICMP Timestamp Detection
Summary The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details: ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 10411 $

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

Log (CVSS: 0.0)
NVT: Record route

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
Here is the route recorded between 10.100.10.105 and 10.100.10.3 :
10.100.10.3.
10.100.10.3.

Log Method
Details: Record route
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: $Revision: 10411 $

[return to 10.100.10.3]

2.3.12 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
traceroute:10.100.10.105,10.100.10.3
TCP ports:5601,9300,9200,5000,9600,22
UDP ports:

Log Method
Details: Host Summary

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.810003
Version used: $Revision: 8287 $

[return to 10.100.10.3]

2.3.13 Log 9300/tcp

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

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

Vulnerability Detection Result

```
An unknown service is running on this port. If you know this service, please rep
↪ort the following information to https://community.greenbone.net/c/vulnerabili
↪ty-tests:
Method: get_http
0x00:  54 68 69 73 20 69 73 20 6E 6F 74 20 61 6E 20 48    This is not an H
0x10:  54 54 50 20 70 6F 72 74                            TTP port
Nmap service detection result for this port: vrace
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 9300 10.100.10.3' and submit a possible collected f
↪ingerprint to the nmap database.
```

Log Method
Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: $Revision: 11748 $

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

[return to 10.100.10.3]

2.4 10.100.10.4

Host scan start	Sun Dec 9 15:22:43 2018 UTC
Host scan end	Sun Dec 9 16:02:51 2018 UTC

Service (Port)	Threat Level
general/tcp	Medium
22/tcp	Medium
general/HOST-T	Log
general/tcp	Log
general/icmp	Log
389/tcp	Log
general/CPE-T	Log
636/tcp	Log
22/tcp	Log

2.4.1 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 12690 $`

References
`CVE: CVE-2009-2624`
`BID:37888`
`Other:`

... continues on next page ...

... continued from previous page ...

```
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 10.100.10.4]

2.4.2 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: $Revision: 12308 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

[return to 10.100.10.4]

2.4.3 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
```
traceroute:10.100.10.105,10.100.10.4
TCP ports:636,22,389
UDP ports:
```

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 10.100.10.4]

2.4.4 Log general/tcp

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detects the installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result
```
Detected GNU GCC
Version:  7
Location: /usr/bin/gcc
CPE:      cpe:/a:gnu:gcc:7
Concluded from version/product identification result:
gcc-7
```

Log Method
Details: `GCC Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: `$Revision: 10901 $`

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result
```
Detected GNU bash
Version:  4.4.19
Location: /bin/bash
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: `GNU Bash Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: `$Revision: 12551 $`

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary
This script finds the GNU Binutils installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result
```
Detected GNU Binutils
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method
Details: `GNU Binutils Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: `$Revision: 10906 $`

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary
This script finds the GNU Assembler installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result
```
Detected GNU assembler
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method
Details: `GNU_Assembler Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.

. . . continues on next page . . .

... continued from previous page ...

The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method

Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary

Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
```

... continues on next page ...

... continued from previous page ...

```
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method
Details: ISC DHCP Client Version Detection
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result
```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: OpenSSL Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: $Revision: 11279 $

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

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

Vulnerability Detection Result
```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 12700 $

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary

... continues on next page ...

... continued from previous page ...

Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
```

Log Method

Details: `Ruby Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary

This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                                                  Value/Content
---------------------------------
↪                                                  -------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find)  : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪                                                  : None
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                  : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                  : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                  : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)              : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                  : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                  : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                  : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                  : FALSE
```

... continues on next page ...

... continued from previous page ...

```
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                                : FALSE
Login successful (login/SSH/success)
↪                                                   : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                   : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                   : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                   : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)              : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                   : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                   : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                   : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                   : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                   : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                   : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                   : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                   : vagrant
locate: Command available (ssh/locate/available)
↪                                                   : TRUE
```

Log Method
Details: SSH Authenticated Scan Info Consolidation
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: $Revision: 9954 $

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result
Here is the route from 10.100.10.105 to 10.100.10.4:

... continues on next page ...

... continued from previous page ...

10.100.10.105
10.100.10.4

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
VMware Open Virtual Machine Tools version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host

Log Method
Details: VMware Open Virtual Machine Tools Version Detection
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: $Revision: 11015 $

[return to 10.100.10.4]

2.4.5 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method

... continues on next page ...

... continued from previous page ...

Details: ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 10411 $

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

Log (CVSS: 0.0)
NVT: Record route

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
Here is the route recorded between 10.100.10.105 and 10.100.10.4 :
10.100.10.4.
10.100.10.4.

Log Method
Details: Record route
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: $Revision: 10411 $

[return to 10.100.10.4]

2.4.6 Log 389/tcp

Log (CVSS: 0.0)
NVT: LDAP Detection

Summary
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.

Vulnerability Detection Result
The LDAP Server supports LDAPv3.

Log Method
Details: LDAP Detection
OID:1.3.6.1.4.1.25623.1.0.100082
Version used: $Revision: 8145 $

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

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

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: CN=*.rz.lab
subject alternative names (SAN):
*.rz.lab
issued by .: CN=*.rz.lab
serial ....: 00CEB7
valid from : 2018-12-05 16:27:20 UTC
valid until: 2028-12-02 16:27:20 UTC
fingerprint (SHA-1): B72701DDB6A9FF379424F543F40A7C5019A118A1
fingerprint (SHA-256): 07AE0C79FDF503E38A066E17CAF8A06868EDC0FC53D4BAADEA73D7944
↪1967650
```

Log Method
Details: `SSL/TLS: Certificate - Self-Signed Certificate Detection`
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: `$Revision: 8981 $`

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

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

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

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: CN=*.rz.lab
subject alternative names (SAN):
*.rz.lab
issued by .: CN=*.rz.lab
serial ....: 00CEB7
valid from : 2018-12-05 16:27:20 UTC
valid until: 2028-12-02 16:27:20 UTC
fingerprint (SHA-1): B72701DDB6A9FF379424F543F40A7C5019A118A1
```

... continues on next page ...

... continued from previous page ...

fingerprint (SHA-256): 07AE0C79FDF503E38A066E17CAF8A06868EDC0FC53D4BAADEA73D7944
↪1967650

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 11908 $

Log (CVSS: 0.0)
NVT: SSL/TLS: LDAP 'Start TLS OID' Detection

Summary
Checks if the remote LDAP server supports SSL/TLS with the 'Start TLS' OID.

Vulnerability Detection Result
The remote LDAP server supports SSL/TLS with the 'Start TLS' OID.

Log Method
Details: SSL/TLS: LDAP 'Start TLS OID' Detection
OID:1.3.6.1.4.1.25623.1.0.105016
Version used: $Revision: 11915 $

References
Other:
URL:https://tools.ietf.org/html/rfc2830

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

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

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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 TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

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_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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

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

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

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

Summary

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
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
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

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

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

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

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: $Revision: 4771 $

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

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

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_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
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
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_CAMELLIA_128_CBC_SHA256
```

... continues on next page ...

... continued from previous page ...

```
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

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

[return to 10.100.10.4]

2.4.7 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
10.100.10.4|cpe:/a:gnu:bash:4.4.19
10.100.10.4|cpe:/a:gnu:binutils:2.30
10.100.10.4|cpe:/a:gnu:gcc:7
10.100.10.4|cpe:/a:gnu:gzip:1.2.4
10.100.10.4|cpe:/a:gnu:gzip:1.6
10.100.10.4|cpe:/a:isc:dhcp:4.3.5
```

... continues on next page ...

... continued from previous page ...

10.100.10.4|cpe:/a:openbsd:openssh:7.6p1
10.100.10.4|cpe:/a:openssl:openssl:1.1.0g
10.100.10.4|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
10.100.10.4|cpe:/a:vmware:open-vm-tools:10.3.0.5330
10.100.10.4|cpe:/o:canonical:ubuntu_linux:18.04:-:lts

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 12413 $

[return to 10.100.10.4]

2.4.8 Log 636/tcp

Log (CVSS: 0.0)
NVT: LDAP Detection

Summary
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.

Vulnerability Detection Result
The LDAP Server supports LDAPv3.

Log Method
Details: LDAP Detection
OID:1.3.6.1.4.1.25623.1.0.100082
Version used: $Revision: 8145 $

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
A TLScustom server answered on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 10922 $

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

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

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: CN=*.rz.lab
subject alternative names (SAN):
*.rz.lab
issued by .: CN=*.rz.lab
serial ....: 00CEB7
valid from : 2018-12-05 16:27:20 UTC
valid until: 2028-12-02 16:27:20 UTC
fingerprint (SHA-1): B72701DDB6A9FF379424F543F40A7C5019A118A1
fingerprint (SHA-256): 07AE0C79FDF503E38A066E17CAF8A06868EDC0FC53D4BAADEA73D7944
↪1967650
```

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 8981 $

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

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

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

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: CN=*.rz.lab
subject alternative names (SAN):
*.rz.lab
issued by .: CN=*.rz.lab
```

... continues on next page ...

... continued from previous page ...

```
serial ....: 00CEB7
valid from : 2018-12-05 16:27:20 UTC
valid until: 2028-12-02 16:27:20 UTC
fingerprint (SHA-1): B72701DDB6A9FF379424F543F40A7C5019A118A1
fingerprint (SHA-256): 07AE0C79FDF503E38A066E17CAF8A06868EDC0FC53D4BAADEA73D7944
↪1967650
```

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 11908 $

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

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

Vulnerability Detection Result

```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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 TLSv1.1 protocol:
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_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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
```

... continues on next page ...

... continued from previous page ...

TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

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

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

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

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

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
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

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
```

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

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

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

Vulnerability Detection Result
`Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv`

... continues on next page ...

... continued from previous page ...

```
↪ice via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
```

Log Method
Details: `SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: `$Revision: 4771 $`

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

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

Vulnerability Detection Result

```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_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
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_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
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
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_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_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_CCM
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_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

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

[return to 10.100.10.4]

2.4.9 Log 22/tcp

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
```
It was possible to login using the provided SSH credentials. Hence authenticated
↪ checks are enabled.
```

Log Method
Details: `SSH Authorization Check`
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: `$Revision: 10873 $`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
```

... continues on next page ...

... continued from previous page ...

```
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 9609 $

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: ac:02:ed:3c:15:00:6e:23:f0:08:30:7c:98:0f:fe:27
ssh-ed25519: 12:80:3a:d6:80:dd:cc:4a:32:69:7d:84:1c:16:ad:71
ssh-rsa: 2b:31:99:45:5e:b7:b8:c2:3d:0b:f2:2a:6b:b8:c8:dc
```

Log Method
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 10929 $

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

Vulnerability Detection Result
`Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1`
`Remote SSH supported authentication: publickey`
`Remote SSH banner: (not available)`
`CPE: cpe:/a:openbsd:openssh:7.6p1`
`Concluded from remote connection attempt with credentials:`
`Login: VulnScan`
`Password: VulnScan`

Log Method Details: `SSH Server type and version` OID:1.3.6.1.4.1.25623.1.0.10267 Version used: `$Revision: 10902 $`

[return to 10.100.10.4]

2.5 10.100.10.11

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:05:53 2018 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Medium
general/tcp	Low
8080/tcp	Log
80/tcp	Log
general/HOST-T	Log
22/tcp	Log
general/icmp	Log
general/tcp	Log
general/CPE-T	Log

2.5.1 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15919`

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: $Revision: 12116 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15473
Other:
URL:http://www.openssh.com
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

[return to 10.100.10.11]

2.5.2 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: $Revision: 12690 $

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2009-2624
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 10.100.10.11]

2.5.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4152699885
Packet 2: 4152700938
```

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The remote host implements TCP timestamps, as defined by RFC1323.

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.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 10411 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

Note

```
vagrant@docker-manager:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE               COMMAND                  CREATED
↪     STATUS              PORTS               NAMES
618c683b4e9c        traefik:1.7.5       "/traefik --debug=tr..."   2 days ago
↪     Up 2 days           80/tcp              lbr_traefik.lr51y1kymw9ojw8pheyi2
↪b168.xb97dmsh4wmklhjl74ropby1y
tcp_timestamps Status for guest containers:
618c683b4e9c: OCI runtime exec failed: exec failed: container_linux.go:348: star
↪ting container process caused "exec: \"sysctl\": executable file not found in
↪$PATH": unknown
Container host confirmed to have mitigated this vulnerability detection result.
traefik container image assumed to be implementing RFC 1323.
sysctl binary was not available on traefik container image to verify mitigation
↪status.
```

Last modified: Sun Dec 9 16:19:19 2018 UTC

[return to 10.100.10.11]

2.5.4 Log 8080/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:

... continues on next page ...

... continued from previous page ...

- 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 these are wrong please report to https://community.greenbone.net/c/vulnerability-tests.

Vulnerability Detection Result

```
The Hostname/IP "docker-manager.rz.lab" 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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://docker-manager.rz.lab:8080/
http://docker-manager.rz.lab:8080/dashboard
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 CGI scanning because of the "Regex
↪pattern to exclude directories from CGI scanning" setting of the NVT "Global v
↪ariable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):
http://docker-manager.rz.lab:8080/dashboard/assets/images
```

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

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 host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

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

Log Method

Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

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

Log (CVSS: 0.0)
NVT: Services

Summary

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

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

[return to 10.100.10.11]

2.5.5 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

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

Vulnerability Detection Result
```
The Hostname/IP "docker-manager.rz.lab" 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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://docker-manager.rz.lab/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

Log (CVSS: 0.0)
NVT: Services

Summary

. . . continues on next page . . .

... continued from previous page ...

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

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

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

[return to 10.100.10.11]

2.5.6 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
`traceroute:10.100.10.105,10.100.10.11`
`TCP ports:80,8080,22`
`UDP ports:`

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 10.100.10.11]

2.5.7 Log 22/tcp

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
`It was possible to login using the provided SSH credentials. Hence authenticated`

... continues on next page ...

... continued from previous page ...

```
↪ checks are enabled.
```

Log Method
Details: SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: $Revision: 10873 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-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@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 9609 $

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: 5d:ea:e7:b6:b4:8c:78:a7:f4:e0:b0:21:48:ee:d6:cc
ssh-ed25519: a6:19:4b:64:b9:34:de:56:fa:ab:33:64:78:cb:5f:b2
ssh-rsa: 68:8c:f6:b6:a0:dd:50:75:f9:0b:ee:f9:3c:de:50:ce
```

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 10929 $`

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

Vulnerability Detection Result
```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 10902 $`

[return to 10.100.10.11]

2.5.8 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

Log (CVSS: 0.0)
NVT: Record route

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
```
Here is the route recorded between 10.100.10.105 and 10.100.10.11 :
10.100.10.11.
10.100.10.11.
```

Log Method
Details: `Record route`
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: `$Revision: 10411 $`

[return to 10.100.10.11]

2.5.9 Log general/tcp

Log (CVSS: 0.0)
NVT: Docker Service Detection (LSC)

. . . continues on next page . . .

... continued from previous page ...

Summary
This script performs ssh based detection of Docker

Vulnerability Detection Result
```
Detected Docker
Version:  18.09.0
Location: ssh
CPE:      cpe:/a:docker:docker:18.09.0
Concluded from version/product identification result:
Server Version: 18.09.0
```

Log Method
Details: `Docker Service Detection (LSC)`
OID:1.3.6.1.4.1.25623.1.0.140119
Version used: `$Revision: 11885 $`

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detects the installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result
```
Detected GNU GCC
Version:  7
Location: /usr/bin/gcc
CPE:      cpe:/a:gnu:gcc:7
Concluded from version/product identification result:
gcc-7
```

Log Method
Details: `GCC Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: `$Revision: 10901 $`

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Detected GNU bash
Version:  4.4.19
Location: /bin/bash
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method

Details: `GNU Bash Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: `$Revision: 12551 $`

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary

This script finds the GNU Binutils installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result

```
Detected GNU Binutils
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method

Details: `GNU Binutils Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: `$Revision: 10906 $`

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary

This script finds the GNU Assembler installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result

```
Detected GNU assembler
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
```

... continues on next page ...

... continued from previous page ...

```
Concluded from version/product identification result:
2.30
```

Log Method
Details: GNU_Assembler Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
```

... continues on next page ...

... continued from previous page ...

```
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method
Details: ISC DHCP Client Version Detection
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result
```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method
Details: `OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 11279 $`

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

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

Vulnerability Detection Result
```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 12700 $

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary
Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]

Log Method
Details: Ruby Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary
This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result
Description (Knowledge base entry)
↪ Value/Content

↪ ---
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find) : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪ : None

... continues on next page ...

... continued from previous page ...

```
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                    : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                    : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                    : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)                    : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                    : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                    : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                    : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                    : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                                 : FALSE
Login successful (login/SSH/success)
↪                                                    : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                    : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                    : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                    : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)               : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                    : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                    : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                    : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                    : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                    : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                    : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                    : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                    : vagrant
locate: Command available (ssh/locate/available)
↪                                                    : TRUE
```

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: `SSH Authenticated Scan Info Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: `$Revision: 9954 $`

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result
```
Here is the route from 10.100.10.105 to 10.100.10.11:
10.100.10.105
10.100.10.11
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
```
VMware Open Virtual Machine Tools  version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host
```

Log Method
Details: `VMware Open Virtual Machine Tools Version Detection`
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: `$Revision: 11015 $`

[return to 10.100.10.11]

2.5.10 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
Vulnerability Detection Result 10.100.10.11|cpe:/a:docker:docker:18.09.0 10.100.10.11|cpe:/a:gnu:bash:4.4.19 10.100.10.11|cpe:/a:gnu:binutils:2.30 10.100.10.11|cpe:/a:gnu:gcc:7 10.100.10.11|cpe:/a:gnu:gzip:1.2.4 10.100.10.11|cpe:/a:gnu:gzip:1.6 10.100.10.11|cpe:/a:isc:dhcp:4.3.5 10.100.10.11|cpe:/a:openbsd:openssh:7.6p1 10.100.10.11|cpe:/a:openssl:openssl:1.1.0g 10.100.10.11|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57 10.100.10.11|cpe:/a:vmware:open-vm-tools:10.3.0.5330 10.100.10.11|cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: $Revision: 12413 $

[return to 10.100.10.11]

2.6 10.100.10.12

Host scan start Sun Dec 9 15:22:43 2018 UTC
Host scan end Sun Dec 9 16:05:53 2018 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Medium
general/tcp	Low
8080/tcp	Log
general/icmp	Log
22/tcp	Log
general/tcp	Log
general/CPE-T	Log
80/tcp	Log
general/HOST-T	Log

2.6.1 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: $Revision: 12116 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15473
Other:
URL:http://www.openssh.com
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

[return to 10.100.10.12]

2.6.2 Medium general/tcp

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800453

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 12690 $

References

```
CVE: CVE-2009-2624
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 10.100.10.12]

2.6.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1249564279
Packet 2: 1249565289
```

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

... continues on next page ...

... continued from previous page ...

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

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.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 10411 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

Note

```
vagrant@docker-worker:~$ sudo ./verify_tcp_timestamps_mitigation.sh
tcp_timestamps Status for Container Host:
net.ipv4.tcp_timestamps = 0
/usr/bin/docker
CONTAINER ID        IMAGE               COMMAND                  CREATED
↪     STATUS              PORTS                 NAMES
960cb9d24d3f        wordpress:latest    "docker-entrypoint.s..."   35 hours ago
↪     Up 35 hours         80/tcp                blog_wordpress.1.don6vicmultaxt
↪3t4pquj7hdt
76d977508cff        mysql:5.7           "docker-entrypoint.s..."   2 days ago
↪     Up 2 days           3306/tcp, 33060/tcp   blog_db.1.y83cylgdl7jrwjz5hzdvl
↪uxxo
tcp_timestamps Status for guest containers:
960cb9d24d3f: net.ipv4.tcp_timestamps = 1
76d977508cff: OCI runtime exec failed: exec failed: container_linux.go:348: star
↪ting container process caused "exec: \"sysctl\": executable file not found in
↪$PATH": unknown
Container host confirmed to have mitigated this vulnerability detection result.
wordpress container image confirmed to be implementing RFC 1323.
mysql container image assumed to be implementing RFC 1323.
sysctl binary was not available on the mysql container image to verify mitigatio
↪n status.
```

Last modified: Sun Dec 9 16:18:32 2018 UTC

[return to 10.100.10.12]

2.6.4 Log 8080/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

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

Vulnerability Detection Result

```
The Hostname/IP "docker-worker.rz.lab" 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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://docker-worker.rz.lab:8080/
http://docker-worker.rz.lab:8080/dashboard
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 CGI scanning because of the "Regex
↪pattern to exclude directories from CGI scanning" setting of the NVT "Global v
↪ariable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):
http://docker-worker.rz.lab:8080/dashboard/assets/images
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

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

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

Vulnerability Detection Result
```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

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

Log (CVSS: 0.0)
NVT: Services

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

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

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

[return to 10.100.10.12]

2.6.5 Log general/icmp

Log (CVSS: 0.0) NVT: ICMP Timestamp Detection
Summary The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Log Method Details: `ICMP Timestamp Detection` OID:1.3.6.1.4.1.25623.1.0.103190 Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

Log (CVSS: 0.0) NVT: Record route
Summary This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
`Here is the route recorded between 10.100.10.105 and 10.100.10.12 :`
`10.100.10.12.`
`10.100.10.12.`

Log Method Details: `Record route` OID:1.3.6.1.4.1.25623.1.0.12264 Version used: `$Revision: 10411 $`

[return to 10.100.10.12]

2.6.6 Log 22/tcp

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary
This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

. . . continues on next page . . .

... continued from previous page ...

Log (CVSS: 0.0)
NVT: SSH Authorization Check

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

Vulnerability Detection Result
```
It was possible to login using the provided SSH credentials. Hence authenticated
↪ checks are enabled.
```

Log Method
Details: `SSH Authorization Check`
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: `$Revision: 10873 $`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-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@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-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,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
```

... continues on next page ...

... continued from previous page ...

```
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 9609 $

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.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: d2:00:bb:2e:f9:ec:99:21:6c:d4:ba:48:4b:0f:cb:77
ssh-ed25519: b8:d5:62:ba:5d:1e:ad:60:14:e2:fd:f0:9b:45:e8:ee
ssh-rsa: a3:5a:ee:9c:5c:8f:01:c3:7d:46:9e:23:c2:d2:9f:3f
```

Log Method
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 10929 $

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

Vulnerability Detection Result

```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
```

... continues on next page ...

... continued from previous page ...

Login: VulnScan
Password: VulnScan

Log Method
Details: SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: $Revision: 10902 $

[return to 10.100.10.12]

2.6.7 Log general/tcp

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detects the installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result
Detected GNU GCC
Version: 7
Location: /usr/bin/gcc
CPE: cpe:/a:gnu:gcc:7
Concluded from version/product identification result:
gcc-7

Log Method
Details: GCC Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: $Revision: 10901 $

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result
Detected GNU bash
Version: 4.4.19
Location: /bin/bash

... continues on next page ...

... continued from previous page ...

```
CPE:      cpe:/a:gnu:bash:4.4.19
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: `GNU Bash Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: `$Revision: 12551 $`

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary
This script finds the GNU Binutils installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result

```
Detected GNU Binutils
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method
Details: `GNU Binutils Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: `$Revision: 10906 $`

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary
This script finds the GNU Assembler installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result

```
Detected GNU assembler
Version:  2.30
Location: /
CPE:      cpe:/a:gnu:binutils:2.30
Concluded from version/product identification result:
2.30
```

Log Method

... continues on next page ...

... continued from previous page ...

Details: GNU_Assembler Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
```

... continues on next page ...

... continued from previous page ...

```
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5

Log Method
Details: ISC DHCP Client Version Detection
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.

... continues on next page ...

... continued from previous page ...

The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result

```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method

Details: `OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 11279 $`

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

Summary

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

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 12700 $

References

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

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary

Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
```

Log Method

Details: Ruby Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary

This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result

```
Description (Knowledge base entry)
↪                                                Value/Content
---------------------------------
↪                                                -------------
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find)  : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪                                               : None
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                               : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                               : FALSE
```

... continues on next page ...

... continued from previous page ...

```
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)                : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                             : FALSE
Login successful (login/SSH/success)
↪                                                : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)           : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                : vagrant
locate: Command available (ssh/locate/available)
↪                                                : TRUE
```

Log Method

Details: SSH Authenticated Scan Info Consolidation
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: $Revision: 9954 $

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result
```
Here is the route from 10.100.10.105 to 10.100.10.12:
10.100.10.105
10.100.10.12
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
```
VMware Open Virtual Machine Tools  version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host
```

Log Method
Details: `VMware Open Virtual Machine Tools Version Detection`
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: `$Revision: 11015 $`

[return to 10.100.10.12]

2.6.8 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
. . . continues on next page . . .

... continued from previous page ...

This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
10.100.10.12|cpe:/a:gnu:bash:4.4.19
10.100.10.12|cpe:/a:gnu:binutils:2.30
10.100.10.12|cpe:/a:gnu:gcc:7
10.100.10.12|cpe:/a:gnu:gzip:1.2.4
10.100.10.12|cpe:/a:gnu:gzip:1.6
10.100.10.12|cpe:/a:isc:dhcp:4.3.5
10.100.10.12|cpe:/a:openbsd:openssh:7.6p1
10.100.10.12|cpe:/a:openssl:openssl:1.1.0g
10.100.10.12|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
10.100.10.12|cpe:/a:vmware:open-vm-tools:10.3.0.5330
10.100.10.12|cpe:/o:canonical:ubuntu_linux:18.04:-:lts
```

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 12413 $`

[return to 10.100.10.12]

2.6.9 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

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

Vulnerability Detection Result

```
The Hostname/IP "docker-worker.rz.lab" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
```

... continues on next page ...

... continued from previous page ...

```
↪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; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://docker-worker.rz.lab/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
A web server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 10922 $

[return to 10.100.10.12]

2.6.10 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

... continues on next page ...

... continued from previous page ...

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
`traceroute:10.100.10.105,10.100.10.12`
`TCP ports:80,8080,22`
`UDP ports:`

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 10.100.10.12]