arghas@3FWT763:~/Desktop$ dmitry

Command 'dmitry' not found, but can be installed with:

sudo apt install dmitry

arghas@3FWT763:~/Desktop$ sudo apt install dmitry

[sudo] password for arghas:

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages were automatically installed and are no longer required:

chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi gyp javascript-common

libc-ares2 libfwupdplugin1 libjs-inherits libjs-is-typedarray libjs-psl

libjs-typedarray-to-buffer libnvidia-cfg1-470 libnvidia-common-470

libnvidia-decode-470 libnvidia-encode-470 libnvidia-extra-470

libnvidia-fbc1-470 libnvidia-gl-470 libnvidia-ifr1-470 libssl-dev libuv1-dev

libva-wayland2 libx11-xcb1:i386 libxmlb1 libxnvctrl0 node-abbrev node-ajv

node-ansi node-ansi-align node-ansi-regex node-ansi-styles node-ansistyles

node-aproba node-archy node-are-we-there-yet node-asap node-asn1

node-assert-plus node-asynckit node-aws-sign2 node-aws4 node-balanced-match

node-bcrypt-pbkdf node-bl node-bluebird node-boxen node-brace-expansion

node-builtins node-cacache node-call-limit node-camelcase node-caseless

node-chalk node-chownr node-ci-info node-cli-boxes node-cliui node-clone

node-co node-color-convert node-color-name node-colors node-columnify

node-combined-stream node-concat-map node-concat-stream node-config-chain

node-configstore node-console-control-strings node-copy-concurrently

node-core-util-is node-cross-spawn node-crypto-random-string node-cyclist

node-dashdash node-debug node-decamelize node-decompress-response

node-deep-extend node-defaults node-define-properties node-delayed-stream

node-delegates node-detect-indent node-detect-newline node-dot-prop

node-duplexer3 node-duplexify node-ecc-jsbn node-editor node-encoding

node-end-of-stream node-err-code node-errno node-es6-promise

node-escape-string-regexp node-execa node-extend node-extsprintf

node-fast-deep-equal node-find-up node-flush-write-stream node-forever-agent

node-form-data node-from2 node-fs-vacuum node-fs-write-stream-atomic

node-fs.realpath node-function-bind node-gauge node-genfun

node-get-caller-file node-get-stream node-getpass node-glob node-got

node-graceful-fs node-har-schema node-har-validator node-has-flag

node-has-symbol-support-x node-has-to-string-tag-x node-has-unicode

node-hosted-git-info node-http-signature node-iconv-lite node-iferr

node-import-lazy node-imurmurhash node-inflight node-inherits node-ini

node-invert-kv node-ip node-ip-regex node-is-npm node-is-obj node-is-object

node-is-path-inside node-is-plain-obj node-is-retry-allowed node-is-stream

node-is-typedarray node-isarray node-isexe node-isstream node-isurl

node-jsbn node-json-parse-better-errors node-json-schema

node-json-schema-traverse node-json-stable-stringify

node-json-stringify-safe node-jsonify node-jsonparse node-jsonstream

node-jsprim node-latest-version node-lazy-property node-lcid node-libnpx

node-locate-path node-lockfile node-lodash node-lodash-packages

node-lowercase-keys node-lru-cache node-make-dir node-mem node-mime

node-mime-types node-mimic-fn node-mimic-response node-minimatch

node-minimist node-mississippi node-mkdirp node-move-concurrently node-ms

node-mute-stream node-nopt node-normalize-package-data node-npm-bundled

node-npm-package-arg node-npm-run-path node-npmlog node-number-is-nan

node-oauth-sign node-object-assign node-once node-opener node-os-locale

node-os-tmpdir node-osenv node-p-cancelable node-p-finally node-p-is-promise

node-p-limit node-p-locate node-p-timeout node-package-json

node-parallel-transform node-path-exists node-path-is-absolute

node-path-is-inside node-performance-now node-pify node-prepend-http

node-process-nextick-args node-promise-inflight node-promise-retry

node-promzard node-proto-list node-prr node-pseudomap node-psl node-pump

node-pumpify node-punycode node-qs node-qw node-rc node-read

node-read-package-json node-readable-stream node-registry-auth-token

node-registry-url node-request node-require-directory

node-require-main-filename node-resolve node-resolve-from node-retry

node-rimraf node-run-queue node-safe-buffer node-semver node-semver-diff

node-set-blocking node-sha node-shebang-command node-shebang-regex

node-signal-exit node-slash node-slide node-sorted-object node-spdx-correct

node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids

node-sshpk node-ssri node-stream-each node-stream-iterate node-stream-shift

node-strict-uri-encode node-string-decoder node-string-width node-strip-ansi

node-strip-eof node-strip-json-comments node-supports-color node-tar

node-term-size node-text-table node-through node-through2 node-timed-out

node-tough-cookie node-tunnel-agent node-tweetnacl node-typedarray

node-typedarray-to-buffer node-uid-number node-unique-filename

node-unique-string node-unpipe node-uri-js node-url-parse-lax

node-url-to-options node-util-deprecate node-uuid

node-validate-npm-package-license node-validate-npm-package-name node-verror

node-wcwidth.js node-which node-which-module node-wide-align

node-widest-line node-wrap-ansi node-wrappy node-write-file-atomic

node-xdg-basedir node-xtend node-y18n node-yallist node-yargs

node-yargs-parser nvidia-compute-utils-470 nvidia-prime nvidia-settings

nvidia-utils-470 python-pkg-resources screen-resolution-extra

xserver-xorg-video-nvidia-470

Use 'sudo apt autoremove' to remove them.

The following NEW packages will be installed:

dmitry

0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.

Need to get 19.8 kB of archives.

After this operation, 55.3 kB of additional disk space will be used.

Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 dmitry amd64 1.3a-1build1 [19.8 kB]

Fetched 19.8 kB in 1s (15.0 kB/s)

Selecting previously unselected package dmitry.

(Reading database ... 209613 files and directories currently installed.)

Preparing to unpack .../dmitry\_1.3a-1build1\_amd64.deb ...

Unpacking dmitry (1.3a-1build1) ...

Setting up dmitry (1.3a-1build1) ...

Processing triggers for man-db (2.9.1-1) ...

arghas@3FWT763:~/Desktop$ dmitry -h

Deepmagic Information Gathering Tool

"There be some deep magic going on"

dmitry: invalid option -- 'h'

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host

-o Save output to %host.txt or to file specified by -o file

-i Perform a whois lookup on the IP address of a host

-w Perform a whois lookup on the domain name of a host

-n Retrieve Netcraft.com information on a host

-s Perform a search for possible subdomains

-e Perform a search for possible email addresses

-p Perform a TCP port scan on a host

\* -f Perform a TCP port scan on a host showing output reporting filtered ports

\* -b Read in the banner received from the scanned port

\* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )

\*Requires the -p flagged to be passed

arghas@3FWT763:~/Desktop$ dmitry -s www.vulweb.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for www.vulweb.com

Continuing with limited modules

HostIP:

HostName:www.vulweb.com

Gathered Subdomain information for vulweb.com

---------------------------------

Searching Google.com:80...

Searching Altavista.com:80...

Found 0 possible subdomain(s) for host vulweb.com, Searched 0 pages containing 0 results

All scans completed, exiting

arghas@3FWT763:~/Desktop$ dmitry -s www.ZemosoLabs.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:65.0.79.182

HostName:www.ZemosoLabs.com

Gathered Subdomain information for ZemosoLabs.com

---------------------------------

Searching Google.com:80...

Searching Altavista.com:80...

Found 0 possible subdomain(s) for host ZemosoLabs.com, Searched 0 pages containing 0 results

All scans completed, exiting

arghas@3FWT763:~/Desktop$ dmitry -s www.zemosolabs.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:65.0.79.182

HostName:www.zemosolabs.com

Gathered Subdomain information for zemosolabs.com

---------------------------------

Searching Google.com:80...

HostName:www.zemosolabs.com

HostIP:65.0.79.182

HostName:eng.zemosolabs.com

HostIP:162.159.153.4

Searching Altavista.com:80...

Found 2 possible subdomain(s) for host zemosolabs.com, Searched 0 pages containing 0 results

All scans completed, exiting

arghas@3FWT763:~/Desktop$ lynis

Command 'lynis' not found, but can be installed with:

sudo apt install lynis

arghas@3FWT763:~/Desktop$ sudo apt install lynis

[sudo] password for arghas:

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages were automatically installed and are no longer required:

chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi gyp javascript-common

libc-ares2 libfwupdplugin1 libjs-inherits libjs-is-typedarray libjs-psl

libjs-typedarray-to-buffer libnvidia-cfg1-470 libnvidia-common-470

libnvidia-decode-470 libnvidia-encode-470 libnvidia-extra-470

libnvidia-fbc1-470 libnvidia-gl-470 libnvidia-ifr1-470 libssl-dev libuv1-dev

libva-wayland2 libx11-xcb1:i386 libxmlb1 libxnvctrl0 node-abbrev node-ajv

node-ansi node-ansi-align node-ansi-regex node-ansi-styles node-ansistyles

node-aproba node-archy node-are-we-there-yet node-asap node-asn1

node-assert-plus node-asynckit node-aws-sign2 node-aws4 node-balanced-match

node-bcrypt-pbkdf node-bl node-bluebird node-boxen node-brace-expansion

node-builtins node-cacache node-call-limit node-camelcase node-caseless

node-chalk node-chownr node-ci-info node-cli-boxes node-cliui node-clone

node-co node-color-convert node-color-name node-colors node-columnify

node-combined-stream node-concat-map node-concat-stream node-config-chain

node-configstore node-console-control-strings node-copy-concurrently

node-core-util-is node-cross-spawn node-crypto-random-string node-cyclist

node-dashdash node-debug node-decamelize node-decompress-response

node-deep-extend node-defaults node-define-properties node-delayed-stream

node-delegates node-detect-indent node-detect-newline node-dot-prop

node-duplexer3 node-duplexify node-ecc-jsbn node-editor node-encoding

node-end-of-stream node-err-code node-errno node-es6-promise

node-escape-string-regexp node-execa node-extend node-extsprintf

node-fast-deep-equal node-find-up node-flush-write-stream node-forever-agent

node-form-data node-from2 node-fs-vacuum node-fs-write-stream-atomic

node-fs.realpath node-function-bind node-gauge node-genfun

node-get-caller-file node-get-stream node-getpass node-glob node-got

node-graceful-fs node-har-schema node-har-validator node-has-flag

node-has-symbol-support-x node-has-to-string-tag-x node-has-unicode

node-hosted-git-info node-http-signature node-iconv-lite node-iferr

node-import-lazy node-imurmurhash node-inflight node-inherits node-ini

node-invert-kv node-ip node-ip-regex node-is-npm node-is-obj node-is-object

node-is-path-inside node-is-plain-obj node-is-retry-allowed node-is-stream

node-is-typedarray node-isarray node-isexe node-isstream node-isurl

node-jsbn node-json-parse-better-errors node-json-schema

node-json-schema-traverse node-json-stable-stringify

node-json-stringify-safe node-jsonify node-jsonparse node-jsonstream

node-jsprim node-latest-version node-lazy-property node-lcid node-libnpx

node-locate-path node-lockfile node-lodash node-lodash-packages

node-lowercase-keys node-lru-cache node-make-dir node-mem node-mime

node-mime-types node-mimic-fn node-mimic-response node-minimatch

node-minimist node-mississippi node-mkdirp node-move-concurrently node-ms

node-mute-stream node-nopt node-normalize-package-data node-npm-bundled

node-npm-package-arg node-npm-run-path node-npmlog node-number-is-nan

node-oauth-sign node-object-assign node-once node-opener node-os-locale

node-os-tmpdir node-osenv node-p-cancelable node-p-finally node-p-is-promise

node-p-limit node-p-locate node-p-timeout node-package-json

node-parallel-transform node-path-exists node-path-is-absolute

node-path-is-inside node-performance-now node-pify node-prepend-http

node-process-nextick-args node-promise-inflight node-promise-retry

node-promzard node-proto-list node-prr node-pseudomap node-psl node-pump

node-pumpify node-punycode node-qs node-qw node-rc node-read

node-read-package-json node-readable-stream node-registry-auth-token

node-registry-url node-request node-require-directory

node-require-main-filename node-resolve node-resolve-from node-retry

node-rimraf node-run-queue node-safe-buffer node-semver node-semver-diff

node-set-blocking node-sha node-shebang-command node-shebang-regex

node-signal-exit node-slash node-slide node-sorted-object node-spdx-correct

node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids

node-sshpk node-ssri node-stream-each node-stream-iterate node-stream-shift

node-strict-uri-encode node-string-decoder node-string-width node-strip-ansi

node-strip-eof node-strip-json-comments node-supports-color node-tar

node-term-size node-text-table node-through node-through2 node-timed-out

node-tough-cookie node-tunnel-agent node-tweetnacl node-typedarray

node-typedarray-to-buffer node-uid-number node-unique-filename

node-unique-string node-unpipe node-uri-js node-url-parse-lax

node-url-to-options node-util-deprecate node-uuid

node-validate-npm-package-license node-validate-npm-package-name node-verror

node-wcwidth.js node-which node-which-module node-wide-align

node-widest-line node-wrap-ansi node-wrappy node-write-file-atomic

node-xdg-basedir node-xtend node-y18n node-yallist node-yargs

node-yargs-parser nvidia-compute-utils-470 nvidia-prime nvidia-settings

nvidia-utils-470 python-pkg-resources screen-resolution-extra

xserver-xorg-video-nvidia-470

Use 'sudo apt autoremove' to remove them.

The following additional packages will be installed:

menu

Suggested packages:

apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu

| kde-runtime | ktsuss

The following NEW packages will be installed:

lynis menu

0 upgraded, 2 newly installed, 0 to remove and 4 not upgraded.

Need to get 537 kB of archives.

After this operation, 2,899 kB of additional disk space will be used.

Do you want to continue? [Y/n] Y

Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lynis all 2.6.2-1 [183 kB]

Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 menu amd64 2.1.47ubuntu4 [354 kB]

Fetched 537 kB in 2s (234 kB/s)

Selecting previously unselected package lynis.

(Reading database ... 209620 files and directories currently installed.)

Preparing to unpack .../archives/lynis\_2.6.2-1\_all.deb ...

Unpacking lynis (2.6.2-1) ...

Selecting previously unselected package menu.

Preparing to unpack .../menu\_2.1.47ubuntu4\_amd64.deb ...

Unpacking menu (2.1.47ubuntu4) ...

Setting up lynis (2.6.2-1) ...

Setting up menu (2.1.47ubuntu4) ...

Processing triggers for mime-support (3.64ubuntu1) ...

Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...

Processing triggers for man-db (2.9.1-1) ...

Processing triggers for install-info (6.7.0.dfsg.2-5) ...

Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...

Processing triggers for menu (2.1.47ubuntu4) ...

arghas@3FWT763:~/Desktop$ lynis show version

/usr/sbin/lynis: 204: .: Can't open /usr/share/lynis/include/consts

arghas@3FWT763:~/Desktop$ lynis show

/usr/sbin/lynis: 204: .: Can't open /usr/share/lynis/include/consts

arghas@3FWT763:~/Desktop$ cd ..

arghas@3FWT763:~$ lynis show

/usr/sbin/lynis: 204: .: Can't open /usr/share/lynis/include/consts

arghas@3FWT763:~$ lynis

/usr/sbin/lynis: 204: .: Can't open /usr/share/lynis/include/consts

arghas@3FWT763:~$ sudo apt install lynis

Reading package lists... Done

Building dependency tree

Reading state information... Done

lynis is already the newest version (2.6.2-1).

The following packages were automatically installed and are no longer required:

chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi gyp javascript-common

libc-ares2 libfwupdplugin1 libjs-inherits libjs-is-typedarray libjs-psl

libjs-typedarray-to-buffer libnvidia-cfg1-470 libnvidia-common-470

libnvidia-decode-470 libnvidia-encode-470 libnvidia-extra-470

libnvidia-fbc1-470 libnvidia-gl-470 libnvidia-ifr1-470 libssl-dev libuv1-dev

libva-wayland2 libx11-xcb1:i386 libxmlb1 libxnvctrl0 node-abbrev node-ajv

node-ansi node-ansi-align node-ansi-regex node-ansi-styles node-ansistyles

node-aproba node-archy node-are-we-there-yet node-asap node-asn1

node-assert-plus node-asynckit node-aws-sign2 node-aws4 node-balanced-match

node-bcrypt-pbkdf node-bl node-bluebird node-boxen node-brace-expansion

node-builtins node-cacache node-call-limit node-camelcase node-caseless

node-chalk node-chownr node-ci-info node-cli-boxes node-cliui node-clone

node-co node-color-convert node-color-name node-colors node-columnify

node-combined-stream node-concat-map node-concat-stream node-config-chain

node-configstore node-console-control-strings node-copy-concurrently

node-core-util-is node-cross-spawn node-crypto-random-string node-cyclist

node-dashdash node-debug node-decamelize node-decompress-response

node-deep-extend node-defaults node-define-properties node-delayed-stream

node-delegates node-detect-indent node-detect-newline node-dot-prop

node-duplexer3 node-duplexify node-ecc-jsbn node-editor node-encoding

node-end-of-stream node-err-code node-errno node-es6-promise

node-escape-string-regexp node-execa node-extend node-extsprintf

node-fast-deep-equal node-find-up node-flush-write-stream node-forever-agent

node-form-data node-from2 node-fs-vacuum node-fs-write-stream-atomic

node-fs.realpath node-function-bind node-gauge node-genfun

node-get-caller-file node-get-stream node-getpass node-glob node-got

node-graceful-fs node-har-schema node-har-validator node-has-flag

node-has-symbol-support-x node-has-to-string-tag-x node-has-unicode

node-hosted-git-info node-http-signature node-iconv-lite node-iferr

node-import-lazy node-imurmurhash node-inflight node-inherits node-ini

node-invert-kv node-ip node-ip-regex node-is-npm node-is-obj node-is-object

node-is-path-inside node-is-plain-obj node-is-retry-allowed node-is-stream

node-is-typedarray node-isarray node-isexe node-isstream node-isurl

node-jsbn node-json-parse-better-errors node-json-schema

node-json-schema-traverse node-json-stable-stringify

node-json-stringify-safe node-jsonify node-jsonparse node-jsonstream

node-jsprim node-latest-version node-lazy-property node-lcid node-libnpx

node-locate-path node-lockfile node-lodash node-lodash-packages

node-lowercase-keys node-lru-cache node-make-dir node-mem node-mime

node-mime-types node-mimic-fn node-mimic-response node-minimatch

node-minimist node-mississippi node-mkdirp node-move-concurrently node-ms

node-mute-stream node-nopt node-normalize-package-data node-npm-bundled

node-npm-package-arg node-npm-run-path node-npmlog node-number-is-nan

node-oauth-sign node-object-assign node-once node-opener node-os-locale

node-os-tmpdir node-osenv node-p-cancelable node-p-finally node-p-is-promise

node-p-limit node-p-locate node-p-timeout node-package-json

node-parallel-transform node-path-exists node-path-is-absolute

node-path-is-inside node-performance-now node-pify node-prepend-http

node-process-nextick-args node-promise-inflight node-promise-retry

node-promzard node-proto-list node-prr node-pseudomap node-psl node-pump

node-pumpify node-punycode node-qs node-qw node-rc node-read

node-read-package-json node-readable-stream node-registry-auth-token

node-registry-url node-request node-require-directory

node-require-main-filename node-resolve node-resolve-from node-retry

node-rimraf node-run-queue node-safe-buffer node-semver node-semver-diff

node-set-blocking node-sha node-shebang-command node-shebang-regex

node-signal-exit node-slash node-slide node-sorted-object node-spdx-correct

node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids

node-sshpk node-ssri node-stream-each node-stream-iterate node-stream-shift

node-strict-uri-encode node-string-decoder node-string-width node-strip-ansi

node-strip-eof node-strip-json-comments node-supports-color node-tar

node-term-size node-text-table node-through node-through2 node-timed-out

node-tough-cookie node-tunnel-agent node-tweetnacl node-typedarray

node-typedarray-to-buffer node-uid-number node-unique-filename

node-unique-string node-unpipe node-uri-js node-url-parse-lax

node-url-to-options node-util-deprecate node-uuid

node-validate-npm-package-license node-validate-npm-package-name node-verror

node-wcwidth.js node-which node-which-module node-wide-align

node-widest-line node-wrap-ansi node-wrappy node-write-file-atomic

node-xdg-basedir node-xtend node-y18n node-yallist node-yargs

node-yargs-parser nvidia-compute-utils-470 nvidia-prime nvidia-settings

nvidia-utils-470 python-pkg-resources screen-resolution-extra

xserver-xorg-video-nvidia-470

Use 'sudo apt autoremove' to remove them.

0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.

arghas@3FWT763:~$ lynis

/usr/sbin/lynis: 204: .: Can't open /usr/share/lynis/include/consts

arghas@3FWT763:~$ sudo lynis

[ Lynis 2.6.2 ]

################################################################################

Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are

welcome to redistribute it under the terms of the GNU General Public License.

See the LICENSE file for details about using this software.

2007-2018, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

################################################################################

[+] Initializing program

------------------------------------

Usage: lynis command [options]

Command:

audit

audit system : Perform local security scan

audit system remote <host> : Remote security scan

audit dockerfile <file> : Analyze Dockerfile

show

show : Show all commands

show version : Show Lynis version

show help : Show help

update

update info : Show update details

Options:

--no-log : Don't create a log file

--pentest : Non-privileged scan (useful for pentest)

--profile <profile> : Scan the system with the given profile file

--quick (-Q) : Quick mode, don't wait for user input

Layout options

--no-colors : Don't use colors in output

--quiet (-q) : No output

--reverse-colors : Optimize color display for light backgrounds

Misc options

--debug : Debug logging to screen

--view-manpage (--man) : View man page

--verbose : Show more details on screen

--version (-V) : Display version number and quit

Enterprise options

--plugin-dir "<path>" : Define path of available plugins

--upload : Upload data to central node

More options available. Run '/usr/sbin/lynis show options', or use the man page.

No command provided. Exiting..

arghas@3FWT763:~$ sudo lynis show version

2.6.2

arghas@3FWT763:~$ sudo lynis audit system

[ Lynis 2.6.2 ]

################################################################################

Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are

welcome to redistribute it under the terms of the GNU General Public License.

See the LICENSE file for details about using this software.

2007-2018, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

################################################################################

[+] Initializing program

------------------------------------

- Detecting OS... [ DONE ]

- Checking profiles... [ DONE ]

---------------------------------------------------

Program version: 2.6.2

Operating system: Linux

Operating system name: Ubuntu Linux

Operating system version: 20.04

Kernel version: 5.15.0

Hardware platform: x86\_64

Hostname: 3FWT763

---------------------------------------------------

Profiles: /etc/lynis/default.prf

Log file: /var/log/lynis.log

Report file: /var/log/lynis-report.dat

Report version: 1.0

Plugin directory: /etc/lynis/plugins

---------------------------------------------------

Auditor: [Not Specified]

Language: en

Test category: all

Test group: all

---------------------------------------------------

- Program update status... [ WARNING ]

===============================================================================

Lynis update available

===============================================================================

Current version is more than 4 months old

Current version : 262 Latest version : 308

Please update to the latest version.

New releases include additional features, bug fixes, tests, and baselines.

Download the latest version:

Packages (DEB/RPM) - https://packages.cisofy.com

Website (TAR) - https://cisofy.com/downloads/

GitHub (source) - https://github.com/CISOfy/lynis

===============================================================================

[+] System Tools

------------------------------------

- Scanning available tools...

- Checking system binaries...

[+] Plugins (phase 1)

------------------------------------

Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: debian

[

[+] Debian Tests

------------------------------------

- Checking for system binaries that are required by Debian Tests...

- Checking /bin... [ FOUND ]

- Checking /sbin... [ FOUND ]

- Checking /usr/bin... [ FOUND ]

- Checking /usr/sbin... [ FOUND ]

- Checking /usr/local/bin... [ FOUND ]

- Checking /usr/local/sbin... [ FOUND ]

- Authentication:

- PAM (Pluggable Authentication Modules):

- libpam-tmpdir [ Not Installed ]

- libpam-usb [ Not Installed ]

- File System Checks:

- DM-Crypt, Cryptsetup & Cryptmount:

- Checking / on /dev/mapper/sda3\_crypt [ ENCRYPTED (Type: LUKS2) ]

- Checking /snap/brave/244 on /var/lib/snapd/snaps/brave\_244.snap [ NOT ENCRYPTED ]

- Checking /snap/bare/5 on /var/lib/snapd/snaps/bare\_5.snap [ NOT ENCRYPTED ]

- Checking /snap/core18/2785 on /var/lib/snapd/snaps/core18\_2785.snap [ NOT ENCRYPTED ]

- Checking /snap/brave/246 on /var/lib/snapd/snaps/brave\_246.snap [ NOT ENCRYPTED ]

- Checking /snap/core20/1950 on /var/lib/snapd/snaps/core20\_1950.snap [ NOT ENCRYPTED ]

- Checking /snap/chromium/2497 on /var/lib/snapd/snaps/chromium\_2497.snap [ NOT ENCRYPTED ]

- Checking /snap/core18/2751 on /var/lib/snapd/snaps/core18\_2751.snap [ NOT ENCRYPTED ]

- Checking /snap/core22/766 on /var/lib/snapd/snaps/core22\_766.snap [ NOT ENCRYPTED ]

- Checking /snap/chromium/2529 on /var/lib/snapd/snaps/chromium\_2529.snap [ NOT ENCRYPTED ]

- Checking /snap/vlc/3078 on /var/lib/snapd/snaps/vlc\_3078.snap [ NOT ENCRYPTED ]

- Checking /snap/intellij-idea-community/434 on /var/lib/snapd/snaps/intellij-idea-community\_434.snap [ NOT ENCRYPTED ]

- Checking /snap/gnome-42-2204/105 on /var/lib/snapd/snaps/gnome-42-2204\_105.snap [ NOT ENCRYPTED ]

- Checking /snap/gnome-3-38-2004/140 on /var/lib/snapd/snaps/gnome-3-38-2004\_140.snap [ NOT ENCRYPTED ]

- Checking /snap/core22/750 on /var/lib/snapd/snaps/core22\_750.snap [ NOT ENCRYPTED ]

- Checking /snap/cups/950 on /var/lib/snapd/snaps/cups\_950.snap [ NOT ENCRYPTED ]

- Checking /snap/gtk-common-themes/1535 on /var/lib/snapd/snaps/gtk-common-themes\_1535.snap [ NOT ENCRYPTED ]

- Checking /snap/cups/962 on /var/lib/snapd/snaps/cups\_962.snap [ NOT ENCRYPTED ]

- Checking /snap/snapd/19457 on /var/lib/snapd/snaps/snapd\_19457.snap [ NOT ENCRYPTED ]

- Checking /snap/snap-store/638 on /var/lib/snapd/snaps/snap-store\_638.snap [ NOT ENCRYPTED ]

- Checking /snap/discord/151 on /var/lib/snapd/snaps/discord\_151.snap [ NOT ENCRYPTED ]

- Checking /snap/gnome-3-38-2004/137 on /var/lib/snapd/snaps/gnome-3-38-2004\_137.snap [ NOT ENCRYPTED ]

- Checking /snap/snapd/19361 on /var/lib/snapd/snaps/snapd\_19361.snap [ NOT ENCRYPTED ]

- Checking /snap/discord/153 on /var/lib/snapd/snaps/discord\_153.snap [ NOT ENCRYPTED ]

- Checking /snap/gnome-42-2204/111 on /var/lib/snapd/snaps/gnome-42-2204\_111.snap [ NOT ENCRYPTED ]

- Checking /snap/intellij-idea-community/442 on /var/lib/snapd/snaps/intellij-idea-community\_442.snap [ NOT ENCRYPTED ]

- Checking /snap/snap-store/959 on /var/lib/snapd/snaps/snap-store\_959.snap [ NOT ENCRYPTED ]

- Checking /snap/gtk-common-themes/1519 on /var/lib/snapd/snaps/gtk-common-themes\_1519.snap [ NOT ENCRYPTED ]

- Checking /boot on /dev/sda2 [ NOT ENCRYPTED ]

- Checking /boot/efi on /dev/sda1 [ NOT ENCRYPTED ]

- Checking /run/user/1001/doc on /dev/fuse [ NOT ENCRYPTED ]

- Checking /snap/core20/1974 on /var/lib/snapd/snaps/core20\_1974.snap [ NOT ENCRYPTED ]

- Software:

- apt-listbugs [ Not Installed ]

- apt-listchanges [ Not Installed ]

- checkrestart [ Not Installed ]

- needrestart [ Not Installed ]

- debsecan [ Not Installed ]

- debsums [ Not Installed ]

- fail2ban [ Not Installed ]

]

[+] Boot and services

------------------------------------

- Service Manager [ SysV Init ]

- Checking UEFI boot [ ENABLED ]

- Checking Secure Boot [ DISABLED ]

- Checking presence GRUB2 [ FOUND ]

- Checking for password protection [ WARNING ]

- Check running services (systemctl) [ DONE ]

Result: found 43 running services

- Check enabled services at boot (systemctl) [ DONE ]

Result: found 79 enabled services

- Check startup files (permissions) [ OK ]

- Checking sulogin in rescue.service [ NOT FOUND ]

[+] Kernel

------------------------------------

- Checking default run level [ RUNLEVEL 5 ]

- Checking CPU support (NX/PAE)

CPU support: PAE and/or NoeXecute supported [ FOUND ]

- Checking kernel version and release [ DONE ]

- Checking kernel type [ DONE ]

- Checking loaded kernel modules [ DONE ]

Found 206 active modules

- Checking Linux kernel configuration file [ FOUND ]

- Checking default I/O kernel scheduler [ NOT FOUND ]

- Checking for available kernel update [ UNKNOWN ]

- Checking core dumps configuration [ DISABLED ]

- Checking setuid core dumps configuration [ PROTECTED ]

- Check if reboot is needed [ NO ]

[+] Memory and Processes

------------------------------------

- Checking /proc/meminfo [ FOUND ]

- Searching for dead/zombie processes [ OK ]

- Searching for IO waiting processes [ OK ]

[+] Users, Groups and Authentication

------------------------------------

- Administrator accounts [ OK ]

- Unique UIDs [ OK ]

- Consistency of group files (grpck) [ OK ]

- Unique group IDs [ OK ]

- Unique group names [ OK ]

- Password file consistency [ OK ]

- Query system users (non daemons) [ DONE ]

- NIS+ authentication support [ NOT ENABLED ]

- NIS authentication support [ NOT ENABLED ]

- sudoers file [ FOUND ]

- Check sudoers file permissions [ OK ]

- PAM password strength tools [ SUGGESTION ]

- PAM configuration files (pam.conf) [ FOUND ]

- PAM configuration files (pam.d) [ FOUND ]

- PAM modules [ FOUND ]

- LDAP module in PAM [ NOT FOUND ]

- Accounts without expire date [ OK ]

- Accounts without password [ OK ]

- Checking user password aging (minimum) [ DISABLED ]

- User password aging (maximum) [ DISABLED ]

- Checking expired passwords [ OK ]

- Checking Linux single user mode authentication [ WARNING ]

- Determining default umask

- umask (/etc/profile) [ NOT FOUND ]

- umask (/etc/login.defs) [ SUGGESTION ]

- LDAP authentication support [ NOT ENABLED ]

- Logging failed login attempts [ ENABLED ]

[+] Shells

------------------------------------

- Checking shells from /etc/shells

Result: found 7 shells (valid shells: 7).

- Session timeout settings/tools [ NONE ]

- Checking default umask values

- Checking default umask in /etc/bash.bashrc [ NONE ]

- Checking default umask in /etc/profile [ NONE ]

[+] File systems

------------------------------------

- Checking mount points

- Checking /home mount point [ SUGGESTION ]

- Checking /tmp mount point [ SUGGESTION ]

- Checking /var mount point [ SUGGESTION ]

- Checking LVM volume groups [ FOUND ]

- Checking LVM volumes [ FOUND ]

- Query swap partitions (fstab) [ OK ]

- Testing swap partitions [ OK ]

- Testing /proc mount (hidepid) [ SUGGESTION ]

- Checking for old files in /tmp [ OK ]

- Checking /tmp sticky bit [ OK ]

- Checking /var/tmp sticky bit [ OK ]

- ACL support root file system [ ENABLED ]

- Mount options of / [ NON DEFAULT ]

- Mount options of /boot [ NON DEFAULT ]

- Disable kernel support of some filesystems

- Discovered kernel modules: cramfs freevxfs hfs hfsplus jffs2 udf

[+] USB Devices

------------------------------------

- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]

- Checking USB devices authorization [ ENABLED ]

- Checking USBGuard [ NOT FOUND ]

[+] Storage

------------------------------------

- Checking firewire ohci driver (modprobe config) [ DISABLED ]

[+] NFS

------------------------------------

- Check running NFS daemon [ NOT FOUND ]

[+] Name services

------------------------------------

- Checking /etc/resolv.conf options [ FOUND ]

- Searching DNS domain name [ UNKNOWN ]

- Checking /etc/hosts

- Checking /etc/hosts (duplicates) [ OK ]

- Checking /etc/hosts (hostname) [ SUGGESTION ]

- Checking /etc/hosts (localhost) [ OK ]

- Checking /etc/hosts (localhost to IP) [ OK ]

[+] Ports and packages

------------------------------------

- Searching package managers

- Searching dpkg package manager [ FOUND ]

- Querying package manager

- Query unpurged packages [ FOUND ]

- Checking security repository in sources.list file [ OK ]

- Checking APT package database [ OK ]

- Checking vulnerable packages [ OK ]

- Checking upgradeable packages [ FOUND ]

- Checking package audit tool [ INSTALLED ]

Found: apt-check

[+] Networking

------------------------------------

- Checking IPv6 configuration [ ENABLED ]

Configuration method [ AUTO ]

IPv6 only [ NO ]

- Checking configured nameservers

- Testing nameservers

Nameserver: 127.0.0.53 [ OK ]

- Minimal of 2 responsive nameservers [ WARNING ]

- Checking default gateway [ DONE ]

- Getting listening ports (TCP/UDP) [ DONE ]

\* Found 16 ports

- Checking promiscuous interfaces [ OK ]

- Checking waiting connections [ OK ]

- Checking status DHCP client [ NOT ACTIVE ]

- Checking for ARP monitoring software [ NOT FOUND ]

[+] Printers and Spools

------------------------------------

- Checking cups daemon [ RUNNING ]

- Checking CUPS configuration file [ OK ]

- File permissions [ OK ]

- Checking CUPS addresses/sockets [ FOUND ]

- Checking lp daemon [ NOT RUNNING ]

[+] Software: e-mail and messaging

------------------------------------

[+] Software: firewalls

------------------------------------

- Checking iptables kernel module [ FOUND ]

- Checking iptables policies of chains [ FOUND ]

- Checking for empty ruleset [ OK ]

- Checking for unused rules [ FOUND ]

- Checking host based firewall [ ACTIVE ]

[+] Software: webserver

------------------------------------

- Checking Apache [ NOT FOUND ]

- Checking nginx [ NOT FOUND ]

[+] SSH Support

------------------------------------

- Checking running SSH daemon [ NOT FOUND ]

[+] SNMP Support

------------------------------------

- Checking running SNMP daemon [ NOT FOUND ]

[+] Databases

------------------------------------

No database engines found

[+] LDAP Services

------------------------------------

- Checking OpenLDAP instance [ NOT FOUND ]

[+] PHP

------------------------------------

- Checking PHP [ NOT FOUND ]

[+] Squid Support

------------------------------------

- Checking running Squid daemon [ NOT FOUND ]

[+] Logging and files

------------------------------------

- Checking for a running log daemon [ OK ]

- Checking Syslog-NG status [ NOT FOUND ]

- Checking systemd journal status [ FOUND ]

- Checking Metalog status [ NOT FOUND ]

- Checking RSyslog status [ FOUND ]

- Checking RFC 3195 daemon status [ NOT FOUND ]

- Checking minilogd instances [ NOT FOUND ]

- Checking logrotate presence [ OK ]

- Checking log directories (static list) [ DONE ]

- Checking open log files [ DONE ]

- Checking deleted files in use [ FILES FOUND ]

[+] Insecure services

------------------------------------

- Checking inetd status [ NOT ACTIVE ]

[+] Banners and identification

------------------------------------

- /etc/issue [ FOUND ]

- /etc/issue contents [ WEAK ]

- /etc/issue.net [ FOUND ]

- /etc/issue.net contents [ WEAK ]

[+] Scheduled tasks

------------------------------------

- Checking crontab/cronjob [ DONE ]

[+] Accounting

------------------------------------

- Checking accounting information [ NOT FOUND ]

- Checking sysstat accounting data [ NOT FOUND ]

- Checking auditd [ NOT FOUND ]

[+] Time and Synchronization

------------------------------------

- NTP daemon found: systemd (timesyncd) [ FOUND ]

- Checking for a running NTP daemon or client [ OK ]

[+] Cryptography

------------------------------------

- Checking for expired SSL certificates [0/4] [ NONE ]

[+] Virtualization

------------------------------------

[+] Containers

------------------------------------

- Docker

- Docker daemon [ RUNNING ]

- Docker info output (warnings) [ NONE ]

- Containers

- Total containers [ UNKNOWN ]

- File permissions [ OK ]

[+] Security frameworks

------------------------------------

- Checking presence AppArmor [ FOUND ]

- Checking AppArmor status [ ENABLED ]

- Checking presence SELinux [ NOT FOUND ]

- Checking presence grsecurity [ NOT FOUND ]

- Checking for implemented MAC framework [ OK ]

[+] Software: file integrity

------------------------------------

- Checking file integrity tools

- Checking presence integrity tool [ NOT FOUND ]

[+] Software: System tooling

------------------------------------

- Checking automation tooling

- Automation tooling [ NOT FOUND ]

- Checking for IDS/IPS tooling [ NONE ]

[+] Software: Malware

------------------------------------

[+] File Permissions

------------------------------------

- Starting file permissions check

[+] Home directories

------------------------------------

- Checking shell history files [ OK ]

[+] Kernel Hardening

------------------------------------

- Comparing sysctl key pairs with scan profile

- fs.protected\_hardlinks (exp: 1) [ OK ]

- fs.protected\_symlinks (exp: 1) [ OK ]

- fs.suid\_dumpable (exp: 0) [ DIFFERENT ]

- kernel.core\_uses\_pid (exp: 1) [ DIFFERENT ]

- kernel.ctrl-alt-del (exp: 0) [ OK ]

- kernel.dmesg\_restrict (exp: 1) [ DIFFERENT ]

- kernel.kptr\_restrict (exp: 2) [ DIFFERENT ]

- kernel.randomize\_va\_space (exp: 2) [ OK ]

- kernel.sysrq (exp: 0) [ DIFFERENT ]

- kernel.yama.ptrace\_scope (exp: 1 2 3) [ OK ]

- net.ipv4.conf.all.accept\_redirects (exp: 0) [ OK ]

- net.ipv4.conf.all.accept\_source\_route (exp: 0) [ OK ]

- net.ipv4.conf.all.bootp\_relay (exp: 0) [ OK ]

- net.ipv4.conf.all.forwarding (exp: 0) [ DIFFERENT ]

- net.ipv4.conf.all.log\_martians (exp: 1) [ DIFFERENT ]

- net.ipv4.conf.all.mc\_forwarding (exp: 0) [ OK ]

- net.ipv4.conf.all.proxy\_arp (exp: 0) [ OK ]

- net.ipv4.conf.all.rp\_filter (exp: 1) [ DIFFERENT ]

- net.ipv4.conf.all.send\_redirects (exp: 0) [ DIFFERENT ]

- net.ipv4.conf.default.accept\_redirects (exp: 0) [ DIFFERENT ]

- net.ipv4.conf.default.accept\_source\_route (exp: 0) [ DIFFERENT ]

- net.ipv4.conf.default.log\_martians (exp: 1) [ DIFFERENT ]

- net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) [ OK ]

- net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1) [ OK ]

- net.ipv4.tcp\_syncookies (exp: 1) [ OK ]

- net.ipv4.tcp\_timestamps (exp: 0 1) [ OK ]

- net.ipv6.conf.all.accept\_redirects (exp: 0) [ DIFFERENT ]

- net.ipv6.conf.all.accept\_source\_route (exp: 0) [ OK ]

- net.ipv6.conf.default.accept\_redirects (exp: 0) [ DIFFERENT ]

- net.ipv6.conf.default.accept\_source\_route (exp: 0) [ OK ]

[+] Hardening

------------------------------------

- Installed compiler(s) [ FOUND ]

- Installed malware scanner [ NOT FOUND ]

[+] Custom Tests

------------------------------------

- Running custom tests... [ NONE ]

[+] Plugins (phase 2)

------------------------------------

================================================================================

-[ Lynis 2.6.2 Results ]-

Warnings (3):

----------------------------

! Version of Lynis is very old and should be updated [LYNIS]

https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]

https://cisofy.com/controls/AUTH-9308/

! Couldn't find 2 responsive nameservers [NETW-2705]

https://cisofy.com/controls/NETW-2705/

Suggestions (41):

----------------------------

\* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]

https://your-domain.example.org/controls/CUST-0280/

\* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]

https://your-domain.example.org/controls/CUST-0285/

\* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]

https://your-domain.example.org/controls/CUST-0810/

\* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]

https://your-domain.example.org/controls/CUST-0811/

\* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]

https://your-domain.example.org/controls/CUST-0830/

\* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]

https://your-domain.example.org/controls/CUST-0831/

\* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]

https://your-domain.example.org/controls/CUST-0870/

\* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]

https://your-domain.example.org/controls/CUST-0875/

\* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

https://cisofy.com/controls/DEB-0880/

\* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

https://cisofy.com/controls/BOOT-5122/

\* Protect rescue.service by using sulogin [BOOT-5260]

https://cisofy.com/controls/BOOT-5260/

\* Determine why /vmlinuz is missing on this Debian/Ubuntu system. [KRNL-5788]

- Details : /vmlinuz

https://cisofy.com/controls/KRNL-5788/

\* Check the output of apt-cache policy manually to determine why output is empty [KRNL-5788]

https://cisofy.com/controls/KRNL-5788/

\* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]

https://cisofy.com/controls/AUTH-9262/

\* Configure minimum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/controls/AUTH-9286/

\* Configure maximum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/controls/AUTH-9286/

\* Set password for single user mode to minimize physical access attack surface [AUTH-9308]

https://cisofy.com/controls/AUTH-9308/

\* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

https://cisofy.com/controls/AUTH-9328/

\* To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]

https://cisofy.com/controls/STRG-1840/

\* Check DNS configuration for the dns domain name [NAME-4028]

https://cisofy.com/controls/NAME-4028/

\* Add the IP name and FQDN to /etc/hosts for proper name resolving [NAME-4404]

https://cisofy.com/controls/NAME-4404/

\* Purge old/removed packages (35 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]

https://cisofy.com/controls/PKGS-7346/

\* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

https://cisofy.com/controls/PKGS-7370/

\* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]

https://cisofy.com/controls/NETW-2705/

\* Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]

https://cisofy.com/controls/NETW-3032/

\* Check iptables rules to see which rules are currently not used [FIRE-4513]

https://cisofy.com/controls/FIRE-4513/

\* Check what deleted files are still in use and why. [LOGG-2190]

https://cisofy.com/controls/LOGG-2190/

\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

https://cisofy.com/controls/BANN-7126/

\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

https://cisofy.com/controls/BANN-7130/

\* Enable process accounting [ACCT-9622]

https://cisofy.com/controls/ACCT-9622/

\* Enable sysstat to collect accounting (no results) [ACCT-9626]

https://cisofy.com/controls/ACCT-9626/

\* Enable auditd to collect audit information [ACCT-9628]

https://cisofy.com/controls/ACCT-9628/

\* Test output of both 'docker ps -a' and 'docker info', to determine why they report a different amount of containers [CONT-8106]

https://cisofy.com/controls/CONT-8106/

\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

https://cisofy.com/controls/FINT-4350/

\* Determine if automation tools are present for system management [TOOL-5002]

https://cisofy.com/controls/TOOL-5002/

\* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]

- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

https://cisofy.com/controls/KRNL-6000/

\* Harden compilers like restricting access to root user only [HRDN-7222]

https://cisofy.com/controls/HRDN-7222/

\* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]

- Solution : Install a tool like rkhunter, chkrootkit, OSSEC

https://cisofy.com/controls/HRDN-7230/

Follow-up:

----------------------------

- Show details of a test (lynis show details TEST-ID)

- Check the logfile for all details (less /var/log/lynis.log)

- Read security controls texts (https://cisofy.com)

- Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

Lynis security scan details:

Hardening index : 53 [########## ]

Tests performed : 227

Plugins enabled : 1

Components:

- Firewall [V]

- Malware scanner [X]

Lynis Modules:

- Compliance Status [?]

- Security Audit [V]

- Vulnerability Scan [V]

Files:

- Test and debug information : /var/log/lynis.log

- Report data : /var/log/lynis-report.dat

================================================================================

Notice: Lynis update available

Current version : 262 Latest version : 308

================================================================================

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems

(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

================================================================================

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

arghas@3FWT763:~$ dmitry -s www.vulnweb.com

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:44.228.249.3

HostName:www.vulnweb.com

Gathered Subdomain information for vulnweb.com

---------------------------------

Searching Google.com:80...

HostName:www.vulnweb.com

HostIP:44.228.249.3

HostName:testhtml5.vulnweb.com

HostIP:44.228.249.3

HostName:testphp.vulnweb.com

HostIP:44.228.249.3

HostName:testasp.vulnweb.com

HostIP:44.238.29.244

HostName:testaspnet.vulnweb.com

HostIP:44.238.29.244

HostName:rest.vulnweb.com

HostIP:35.81.188.86

HostName:252Ftestasp.vulnweb.com

HostIP:44.228.249.3

HostName:scan-report-testphp.vulnweb.com

HostIP:44.228.249.3

HostName:stphp.vulnweb.com

HostIP:44.228.249.3

HostName:www.whois.vulnweb.com

HostIP:44.228.249.3

HostName:antivirus1.vulnweb.com

HostIP:44.228.249.3

HostName:autoconfig.demo.vulnweb.com

HostIP:44.228.249.3

HostName:hp.vulnweb.com

HostIP:44.228.249.3

Searching Altavista.com:80...

Found 13 possible subdomain(s) for host vulnweb.com, Searched 0 pages containing 0 results

All scans completed, exiting