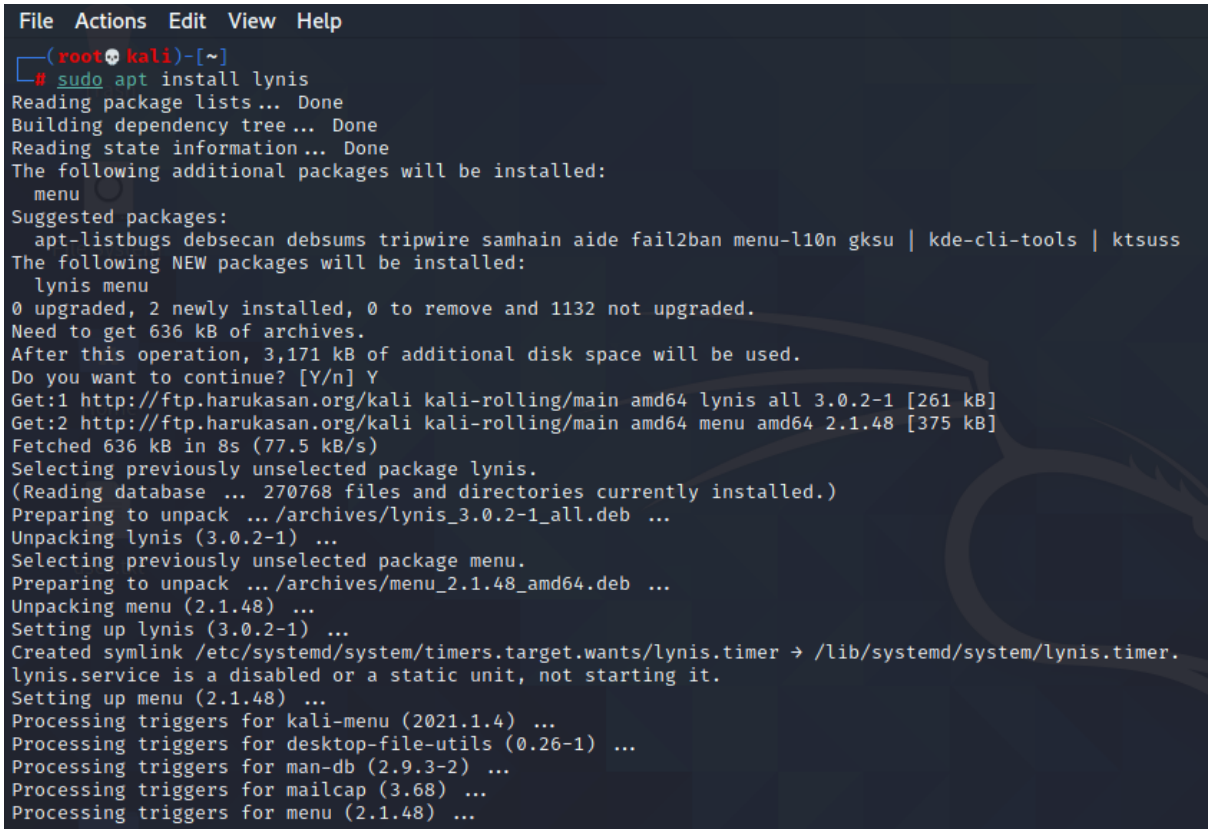
**ARYAMAN MISHRA**

**19BCE1027**

**EXPERIMENT 12-LYNIS AUDIT TOOL**

Installing Lynis on Kali Linux.




Execute Lynis -h for command details

```
    Misc options
    --debug                          : Debug logging to screen
    --no-log                         : Don't create a log file
    --profile <profile>              : Scan the system with the given profile file
    --view-manpage (--man)           : View man page
    --verbose                        : Show more details on screen
    --version (-V)                   : Display version number and quit
    --wait                           : Wait between a set of tests
    --slow-warning <seconds>  : Threshold for slow test warning in seconds (default 10)

    Enterprise options
    --plugindir <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.


┌──(root💀 kali)-[~]
└─#
```

Lynis Audit System command execution:

```
[+] 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 ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                            [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                         [ Not Installed ]
    - apt-listchanges                                      [ Not Installed ]
    - needrestart                                          [ Not Installed ]
    - debsecan                                             [ Not Installed ]
    - debsums                                              [ Not Installed ]
    - fail2ban                                             [ Not Installed ]
]

[+] Boot and services
------------------------------------

  - Service Manager                                        [ systemd ]
  - Checking UEFI boot                                     [ DISABLED ]
  - Checking presence GRUB2                                [ FOUND ]
    - Checking for password protection                     [ NONE ]
  - Check running services (systemctl)                     [ DONE ]
        Result: found 20 running services
  - Check enabled services at boot (systemctl)             [ DONE ]
        Result: found 19 enabled services
  - Check startup files (permissions)                      [ OK ]
  - Running 'systemd-analyze security'
        - ModemManager.service:                            [ MEDIUM ]
        - NetworkManager.service:                          [ EXPOSED ]
        - colord.service:                                  [ EXPOSED ]
        - cron.service:                                    [ UNSAFE ]
        - dbus.service:                                    [ UNSAFE ]
        - dm-event.service:                                [ UNSAFE ]
        - emergency.service:                               [ UNSAFE ]
        - getty@tty1.service:                              [ UNSAFE ]
        - haveged.service:                                 [ OK ]
        - inetutils-inetd.service:                         [ UNSAFE ]
        - libvirtd.service:                                [ UNSAFE ]
        - lightdm.service:                                 [ UNSAFE ]
        - lvm2-lvmpolld.service:                           [ UNSAFE ]
        - lynis.service:                                   [ UNSAFE ]
        - mlocate.service:                                 [ EXPOSED ]
```


- Service Manager [ systemd ]
- Checking UEFI boot [ DISABLED ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ NONE ]
- Check running services (systemctl) [ DONE ]
Result: found 20 running services
- Check enabled services at boot (systemctl) [ DONE ]
Result: found 19 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
- ModemManager.service: [ MEDIUM ]
- NetworkManager.service: [ EXPOSED ]
- colord.service: [ EXPOSED ]
- cron.service: [ UNSAFE ]
- dbus.service: [ UNSAFE ]
- dm-event.service: [ UNSAFE ]
- emergency.service: [ UNSAFE ]
- getty@tty1.service: [ UNSAFE ]
- haveged.service: [ OK ]
- inetutils-inetd.service: [ UNSAFE ]
- libvirtd.service: [ UNSAFE ]
- lightdm.service: [ UNSAFE ]
- lvm2-lvmpolld.service: [ UNSAFE ]
- lynis.service: [ UNSAFE ]
- mlocate.service: [ EXPOSED ]
- plymouth-start.service: [ UNSAFE ]
- polkit.service: [ UNSAFE ]
- rc-local.service: [ UNSAFE ]
- rescue.service: [ UNSAFE ]
- rpc-gssd.service: [ UNSAFE ]
- rpc-svcgssd.service: [ UNSAFE ]
- rsync.service: [ EXPOSED ]
- rsyslog.service: [ UNSAFE ]
- rtkit-daemon.service: [ MEDIUM ]
- smartmontools.service: [ UNSAFE ]
- stunnel4.service: [ UNSAFE ]
- systemd-ask-password-console.service: [ UNSAFE ]
- systemd-ask-password-plymouth.service: [ UNSAFE ]
- systemd-ask-password-wall.service: [ UNSAFE ]
- systemd-fsckd.service: [ UNSAFE ]
- systemd-initctl.service: [ UNSAFE ]
- systemd-journald.service: [ OK ]
- systemd-logind.service: [ OK ]
- systemd-machined.service: [ MEDIUM ]
- systemd-networkd.service: [ OK ]
- systemd-rfkill.service: [ UNSAFE ]
- systemd-udevd.service: [ EXPOSED ]
- udisks2.service: [ UNSAFE ]
- upower.service: [ OK ]
- user@0.service: [ UNSAFE ]
- virtlockd.service: [ UNSAFE ]
- virtlogd.service: [ UNSAFE ]

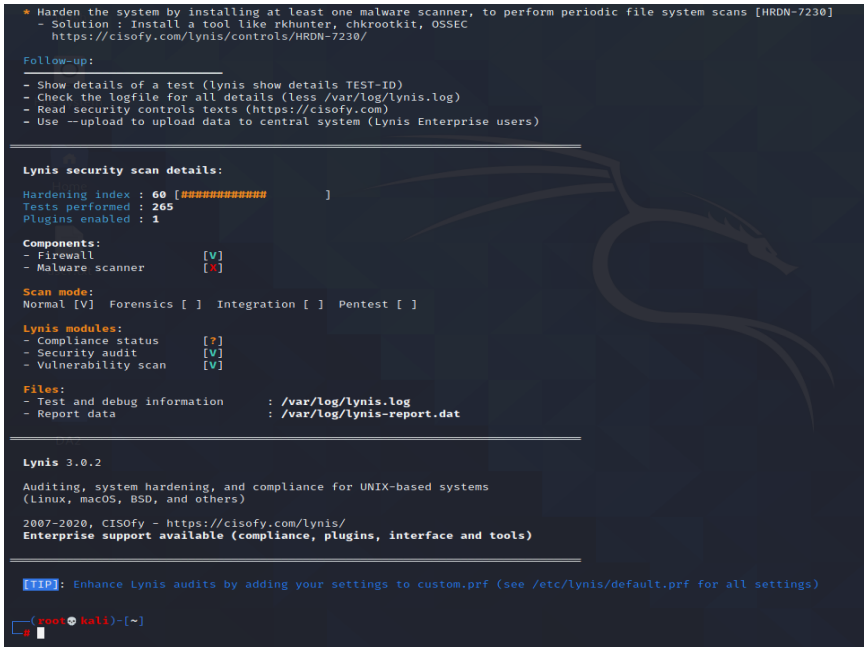
```
[+] Kernel
------------------------------------

  - 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 77 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ NOT FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration
    - configuration in systemd conf files                     [ DEFAULT ]
    - configuration in etc/profile                            [ DEFAULT ]
    - 'hard' configuration in security/limits.conf            [ DEFAULT ]
    - 'soft' configuration in security/limits.conf            [ DEFAULT ]
    - Checking setuid core dumps configuration                [ DISABLED ]
  - Check if reboot is needed                                 [ NO ]

[+] Memory and Processes
------------------------------------

  - Checking /proc/meminfo                                    [ FOUND ]
  - Searching for dead/zombie processes                       [ NOT FOUND ]
  - Searching for IO waiting processes                        [ NOT FOUND ]
  - Search prelink tooling                                    [ NOT FOUND ]

[+] 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 ]
  - Password hashing methods                                  [ OK ]
  - Checking password hashing rounds                          [ DISABLED ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ NOT ENABLED ]
  - Sudoers file(s)                                           [ FOUND ]
    - Permissions for directory: /etc/sudoers.d               [ WARNING ]
    - Permissions for: /etc/sudoers                           [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root         [ OK ]
    - Permissions for: /etc/sudoers.d/README                  [ 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                              [ SUGGESTION ]
  - Accounts without password                                 [ OK ]
```


- Locked accounts [ FOUND ]
- Checking user password aging (minimum) [ DISABLED ]
- User password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]
- Checking Linux single user mode authentication [ OK ]
- 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 11 shells (valid shells: 11).
- 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 ]
- 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 /dev [ HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
- Checking Locate database [ FOUND ]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs 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) [ NOT DISABLED ]

```
[+] NFS
------------------------------------------

  - Query rpc registered programs                              [ DONE ]
  - Query NFS versions                                         [ DONE ]
  - Query NFS protocols                                        [ DONE ]
  - Check running NFS daemon                                   [ NOT FOUND ]

[+] Name services
------------------------------------------

  - Searching DNS domain name                                  [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                          [ NONE ]
    - Presence of configured hostname in /etc/hosts            [ FOUND ]
    - Hostname mapped to localhost                             [ NOT FOUND ]
    - Localhost mapping to IP address                          [ 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 or directory  [ WARNING ]
  - Checking vulnerable packages (apt-get only)                [ DONE ]

  [WARNING]: Test PKGS-7392 had a long execution: 1702.208100 seconds

  - Checking package audit tool                                [ INSTALLED ]
    Found: apt-get
  - Toolkit for automatic upgrades                             [ NOT FOUND ]

[+] Networking
------------------------------------------

  - Checking IPv6 configuration                                [ ENABLED ]
      Configuration method                                     [ AUTO ]
      IPv6 only                                                [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 192.168.29.1                               [ OK ]
        Nameserver: 2405:201:6008:30e3::c0a8:1d01              [ OK ]
    - Minimal of 2 responsive nameservers                      [ OK ]
    - DNSSEC supported (systemd-resolved)                      [ UNKNOWN ]
  - Checking default gateway                                   [ DONE ]
  - Getting listening ports (TCP/UDP)                          [ SKIPPED ]
  - Checking promiscuous interfaces                            [ OK ]
  - Checking waiting connections                               [ OK ]
  - Checking status DHCP client
  - Checking for ARP monitoring software                       [ NOT FOUND ]
  - Uncommon network protocols                                 [ 0 ]

[+] Printers and Spools
------------------------------------------

  - Checking cups daemon                                       [ NOT FOUND ]
```


[+] Printers and Spools
- Checking cups daemon [ NOT 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 [ WARNING ]
- Checking for unused rules [ OK ]
- Checking host based firewall [ ACTIVE ]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [ FOUND (118) ]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [ NOT FOUND ]
mod_reqtimeout/mod_qos [ FOUND ]
ModSecurity: web application firewall [ 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 [ FOUND ]
- Checking PHP disabled functions [ FOUND ]
- Checking expose_php option [ OFF ]
- Checking enable_dl option [ OFF ]
- Checking allow_url_fopen option [ ON ]

```
[+] PHP
------------------------------------------

  - Checking PHP                                [ FOUND ]
    - Checking PHP disabled functions           [ FOUND ]
    - Checking expose_php option                [ OFF ]
    - Checking enable_dl option                 [ OFF ]
    - Checking allow_url_fopen option           [ ON ]
    - Checking allow_url_include option         [ OFF ]
    - Checking listen option                    [ OK ]

[+] 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 remote logging                     [ NOT ENABLED ]
  - Checking log directories (static list)      [ DONE ]
  - Checking open log files                     [ DONE ]
  - Checking deleted files in use               [ FILES FOUND ]

[+] Insecure services
------------------------------------------

  - Installed inetd package                     [ NOT FOUND ]
    - Checking enabled inetd services           [ OK ]
  - Installed xinetd package                    [ OK ]
    - xinetd status
  - Installed rsh client package                [ OK ]
  - Installed rsh server package                [ OK ]
  - Installed telnet client package             [ OK ]
  - Installed telnet server package             [ NOT FOUND ]
  - Checking NIS client installation            [ OK ]
  - Checking NIS server installation            [ OK ]
  - Checking TFTP client installation           [ SUGGESTION ]
  - Checking TFTP server installation           [ SUGGESTION ]

[+] Banners and identification
------------------------------------------

  - /etc/issue                                  [ FOUND ]
    - /etc/issue contents                       [ WEAK ]
  - /etc/issue.net                              [ FOUND ]
    - /etc/issue.net contents                   [ WEAK ]
```




Executing lynis audit system --forensics

```
  - 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 ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                          [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                       [ Not Installed ]
    - apt-listchanges                                    [ Not Installed ]
    - needrestart                                        [ Not Installed ]
    - debsecan                                           [ Not Installed ]
    - debsums                                            [ Not Installed ]
    - fail2ban                                           [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                      [ systemd ]
  - Checking UEFI boot                                   [ DISABLED ]
  - Checking presence GRUB2                              [ FOUND ]
    - Checking for password protection                   [ NONE ]
  - Check running services (systemctl)                   [ DONE ]
        Result: found 20 running services
  - Check enabled services at boot (systemctl)           [ DONE ]
        Result: found 19 enabled services
  - Check startup files (permissions)                    [ OK ]
  - Running 'systemd-analyze security'
      - ModemManager.service:                            [ MEDIUM ]
      - NetworkManager.service:                          [ EXPOSED ]
      - colord.service:                                  [ EXPOSED ]
      - cron.service:                                    [ UNSAFE ]
      - dbus.service:                                    [ UNSAFE ]
      - dm-event.service:                                [ UNSAFE ]
      - emergency.service:                               [ UNSAFE ]
      - getty@tty1.service:                              [ UNSAFE ]
      - haveged.service:                                 [ OK ]
      - inetutils-inetd.service:                         [ UNSAFE ]
      - libvirtd.service:                                [ UNSAFE ]
      - lightdm.service:                                 [ UNSAFE ]
      - lvm2-lvmpolld.service:                           [ UNSAFE ]
```

```
  - lynis.service:                                    [ UNSAFE ]
  - mlocate.service:                                  [ EXPOSED ]
  - plymouth-start.service:                           [ UNSAFE ]
  - polkit.service:                                   [ UNSAFE ]
  - rc-local.service:                                 [ UNSAFE ]
  - rescue.service:                                   [ UNSAFE ]
  - rpc-gssd.service:                                 [ UNSAFE ]
  - rpc-svcgssd.service:                              [ UNSAFE ]
  - rsync.service:                                    [ EXPOSED ]
  - rsyslog.service:                                  [ UNSAFE ]
  - rtkit-daemon.service:                             [ MEDIUM ]
  - smartmontools.service:                            [ UNSAFE ]
  - stunnel4.service:                                 [ UNSAFE ]
  - systemd-ask-password-console.service:             [ UNSAFE ]
  - systemd-ask-password-plymouth.service:            [ UNSAFE ]
  - systemd-ask-password-wall.service:                [ UNSAFE ]
  - systemd-fsckd.service:                            [ UNSAFE ]
  - systemd-initctl.service:                          [ UNSAFE ]
  - systemd-journald.service:                         [ OK ]
  - systemd-logind.service:                           [ OK ]
  - systemd-machined.service:                         [ MEDIUM ]
  - systemd-networkd.service:                         [ OK ]
  - systemd-rfkill.service:                           [ UNSAFE ]
  - systemd-udevd.service:                            [ EXPOSED ]
  - udisks2.service:                                  [ UNSAFE ]
  - upower.service:                                   [ OK ]
  - user@0.service:                                   [ UNSAFE ]
  - virtlockd.service:                                [ UNSAFE ]
  - virtlogd.service:                                 [ UNSAFE ]
  - virtualbox-guest-utils.service:                   [ UNSAFE ]

[+] 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 82 active modules
  - Checking Linux kernel configuration file          [ FOUND ]
  - Checking default I/O kernel scheduler             [ NOT FOUND ]
  - Checking for available kernel update              [ OK ]
  - Checking core dumps configuration
    - configuration in systemd conf files             [ DEFAULT ]
    - configuration in etc/profile                    [ DEFAULT ]
    - 'hard' configuration in security/limits.conf    [ DEFAULT ]
    - 'soft' configuration in security/limits.conf    [ DEFAULT ]
    - Checking setuid core dumps configuration        [ DISABLED ]
  - Check if reboot is needed                         [ NO ]
```

```
[+] Plugins (phase 2)
================================================================================

  -[ Lynis 3.0.2 Results ]-

  Warnings (2):
  ----------------------------
  ! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
      https://cisofy.com/lynis/controls/PKGS-7388/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (51):
  -----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNI
S]
      https://cisofy.com/lynis/controls/LYNIS/

  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
      https://cisofy.com/lynis/controls/DEB-0280/

  * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
      https://cisofy.com/lynis/controls/DEB-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
      https://cisofy.com/lynis/controls/DEB-0811/

  * 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. [DEB-0831]
      https://cisofy.com/lynis/controls/DEB-0831/

  * Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
      https://cisofy.com/lynis/controls/DEB-0870/

  * Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
      https://cisofy.com/lynis/controls/DEB-0875/

  * Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
      https://cisofy.com/lynis/controls/DEB-0880/

  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without
password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/
```

```
  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
      https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/
  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
      https://cisofy.com/lynis/controls/AUTH-9262/
  * When possible set expire dates for all password protected accounts [AUTH-9282]
      https://cisofy.com/lynis/controls/AUTH-9282/

  * Look at the locked accounts and consider removing them [AUTH-9284]
      https://cisofy.com/lynis/controls/AUTH-9284/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/lynis/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * Consider disabling unused kernel modules [FILE-6430]
    - Details  : /etc/modprobe.d/blacklist.conf
    - Solution : Add 'install MODULENAME /bin/true' (without quotes)
      https://cisofy.com/lynis/controls/FILE-6430/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
      https://cisofy.com/lynis/controls/USB-1000/

  * Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
      https://cisofy.com/lynis/controls/STRG-1846/

  * Check DNS configuration for the dns domain name [NAME-4028]
      https://cisofy.com/lynis/controls/NAME-4028/
```

```
  * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configura
tion files, cron jobs and startup scripts. [PKGS-7346]
      https://cisofy.com/lynis/controls/PKGS-7346/

  * Install debsums utility for the verification of packages with known good database. [PKGS-7370]
      https://cisofy.com/lynis/controls/PKGS-7370/

  * Consider using a tool to automatically apply upgrades [PKGS-7420]
      https://cisofy.com/lynis/controls/PKGS-7420/

  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'rds' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
      https://cisofy.com/lynis/controls/HTTP-6640/

  * Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
      https://cisofy.com/lynis/controls/HTTP-6643/

  * Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
      https://cisofy.com/lynis/controls/PHP-2376/

  * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
      https://cisofy.com/lynis/controls/LOGG-2154/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/

  * It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-83
18]
      https://cisofy.com/lynis/controls/INSE-8318/

  * Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [IN
SE-8320]
      https://cisofy.com/lynis/controls/INSE-8320/

  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/lynis/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/lynis/controls/BANN-7130/
```

```
  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/lynis/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/lynis/controls/ACCT-9622/

  * Enable sysstat to collect accounting (disabled) [ACCT-9626]
      https://cisofy.com/lynis/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/lynis/controls/ACCT-9628/

  * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
      https://cisofy.com/lynis/controls/FINT-4350/

  * Determine if automation tools are present for system management [TOOL-5002]
      https://cisofy.com/lynis/controls/TOOL-5002/

  * Consider restricting file permissions [FILE-7524]
    - Details  : See screen output or log file
    - Solution : Use chmod to change file permissions
      https://cisofy.com/lynis/controls/FILE-7524/

  * Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
      https://cisofy.com/lynis/controls/HOME-9304/

  * 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/lynis/controls/KRNL-6000/

  * Harden compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/lynis/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/lynis/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 : 60 [############        ]
  Tests performed : 265
  Plugins enabled : 1
```

```
  Tests performed : 265
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  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

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

  Lynis 3.0.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2020, 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)
```

Executing Lynis Audit system –pentest command:

```
┌──(root💀kali)-[/]
└─# lynis audit system --pentest

[ Lynis 3.0.2 ]

################################################################################
  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.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################

[+] Initializing program
------------------------------------

  - Detecting OS ...                                          [ DONE ]
  - Checking profiles ...                                     [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.2
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  kali-rolling
  Kernel version:            5.10.0
  Hardware platform:         x86_64
  Hostname:                  kali
  ---------------------------------------------------
  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 ...                                 [ NO UPDATE ]

[+] 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 ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                          [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                       [ Not Installed ]
    - apt-listchanges                                    [ Not Installed ]
    - needrestart                                        [ Not Installed ]
    - debsecan                                           [ Not Installed ]
    - debsums                                            [ Not Installed ]
    - fail2ban                                           [ Not Installed ]

[+] Boot and services
------------------------------------
  - Service Manager                                      [ systemd ]
  - Checking UEFI boot                                   [ DISABLED ]
  - Checking presence GRUB2                              [ FOUND ]
    - Checking for password protection                   [ NONE ]
  - Check running services (systemctl)                   [ DONE ]
        Result: found 20 running services
  - Check enabled services at boot (systemctl)           [ DONE ]
        Result: found 19 enabled services
  - Check startup files (permissions)                    [ OK ]
  - Running 'systemd-analyze security'
        - ModemManager.service:                          [ MEDIUM ]
        - NetworkManager.service:                        [ EXPOSED ]
        - colord.service:                                [ EXPOSED ]
        - cron.service:                                  [ UNSAFE ]
        - dbus.service:                                  [ UNSAFE ]
        - dm-event.service:                              [ UNSAFE ]
        - emergency.service:                             [ UNSAFE ]
        - getty@tty1.service:                            [ UNSAFE ]
        - haveged.service:                               [ OK ]
        - inetutils-inetd.service:                       [ UNSAFE ]
        - libvirtd.service:                              [ UNSAFE ]
        - lightdm.service:                               [ UNSAFE ]
        - lvm2-lvmpolld.service:                         [ UNSAFE ]
        - lynis.service:                                 [ UNSAFE ]
        - mlocate.service:                               [ EXPOSED ]
```

```
  - plymouth-start.service:                                   [ UNSAFE ]
  - polkit.service:                                           [ UNSAFE ]
  - rc-local.service:                                         [ UNSAFE ]
  - rescue.service:                                           [ UNSAFE ]
  - rpc-gssd.service:                                         [ UNSAFE ]
  - rpc-svcgssd.service:                                      [ UNSAFE ]
  - rsync.service:                                            [ EXPOSED ]
  - rsyslog.service:                                          [ UNSAFE ]
  - rtkit-daemon.service:                                     [ MEDIUM ]
  - smartmontools.service:                                    [ UNSAFE ]
  - stunnel4.service:                                         [ UNSAFE ]
  - systemd-ask-password-console.service:                     [ UNSAFE ]
  - systemd-ask-password-plymouth.service:                    [ UNSAFE ]
  - systemd-ask-password-wall.service:                        [ UNSAFE ]
  - systemd-fsckd.service:                                    [ UNSAFE ]
  - systemd-initctl.service:                                  [ UNSAFE ]
  - systemd-journald.service:                                 [ OK ]
  - systemd-logind.service:                                   [ OK ]
  - systemd-machined.service:                                 [ MEDIUM ]
  - systemd-networkd.service:                                 [ OK ]
  - systemd-rfkill.service:                                   [ UNSAFE ]
  - systemd-udevd.service:                                    [ EXPOSED ]
  - udisks2.service:                                          [ UNSAFE ]
  - upower.service:                                           [ OK ]
  - user@0.service:                                           [ UNSAFE ]
  - virtlockd.service:                                        [ UNSAFE ]
  - virtlogd.service:                                         [ UNSAFE ]
  - virtualbox-guest-utils.service:                           [ UNSAFE ]

[+] 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 82 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ NOT FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration
    - configuration in systemd conf files                     [ DEFAULT ]
    - configuration in etc/profile                            [ DEFAULT ]
    - 'hard' configuration in security/limits.conf            [ DEFAULT ]
    - 'soft' configuration in security/limits.conf            [ DEFAULT ]
  - Checking setuid core dumps configuration                  [ DISABLED ]
  - Check if reboot is needed                                 [ NO ]

[+] Memory and Processes
------------------------------------
```

```
[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                [ FOUND ]
  - Searching for dead/zombie processes                   [ NOT FOUND ]
  - Searching for IO waiting processes                    [ NOT FOUND ]
  - Search prelink tooling                                [ NOT FOUND ]

[+] 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 ]
  - Password hashing methods                              [ OK ]
  - Checking password hashing rounds                      [ DISABLED ]
  - Query system users (non daemons)                      [ DONE ]
  - NIS+ authentication support                           [ NOT ENABLED ]
  - NIS authentication support                            [ NOT ENABLED ]
  - Sudoers file(s)                                       [ FOUND ]
    - Permissions for directory: /etc/sudoers.d           [ WARNING ]
    - Permissions for: /etc/sudoers                       [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root     [ OK ]
    - Permissions for: /etc/sudoers.d/README              [ 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                          [ SUGGESTION ]
  - Accounts without password                             [ OK ]
  - Locked accounts                                       [ FOUND ]
  - Checking user password aging (minimum)                [ DISABLED ]
  - User password aging (maximum)                         [ DISABLED ]
  - Checking expired passwords                            [ OK ]
  - Checking Linux single user mode authentication        [ OK ]
  - 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 11 shells (valid shells: 11).
    - 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
```


[+] File systems
- Checking mount points
- Checking /home mount point [ SUGGESTION ]
- Checking /tmp mount point [ SUGGESTION ]
- Checking /var mount point [ SUGGESTION ]
- 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 /dev [ HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
- Checking Locate database [ FOUND ]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs 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) [ NOT DISABLED ]
[+] NFS
- Query rpc registered programs [ DONE ]
- Query NFS versions [ DONE ]
- Query NFS protocols [ DONE ]
- Check running NFS daemon [ NOT FOUND ]
[+] Name services
- Searching DNS domain name [ UNKNOWN ]
- Checking /etc/hosts
- Duplicate entries in hosts file [ NONE ]
- Presence of configured hostname in /etc/hosts [ FOUND ]
- Hostname mapped to localhost [ NOT FOUND ]
- Localhost mapping to IP address [ OK ]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [ FOUND ]


[+] 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 or directory [ WARNING ]
- Checking vulnerable packages (apt-get only) [ DONE ]
[WARNING]: Test PKGS-7392 had a long execution: 11.672215 seconds
- Checking package audit tool [ INSTALLED ]
Found: apt-get
- Toolkit for automatic upgrades [ NOT FOUND ]
[+] Networking
- Checking IPv6 configuration [ ENABLED ]
Configuration method [ AUTO ]
IPv6 only [ NO ]
- Checking configured nameservers
- Testing nameservers
Nameserver: 192.168.29.1 [ OK ]
Nameserver: 2405:201:6008:30e3::c0a8:1d01 [ OK ]
- Minimal of 2 responsive nameservers [ OK ]
- DNSSEC supported (systemd-resolved) [ UNKNOWN ]
- Checking default gateway [ DONE ]
- Getting listening ports (TCP/UDP) [ SKIPPED ]
- Checking promiscuous interfaces [ OK ]
- Checking waiting connections [ OK ]
- Checking status DHCP client
- Checking for ARP monitoring software [ NOT FOUND ]
- Uncommon network protocols [ 0 ]
[+] Printers and Spools
- Checking cups daemon [ NOT 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 [ WARNING ]
- Checking for unused rules [ OK ]
- Checking host based firewall [ ACTIVE ]


[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [ FOUND (118) ]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [ NOT FOUND ]
mod_reqtimeout/mod_qos [ FOUND ]
ModSecurity: web application firewall [ 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 [ FOUND ]
- Checking PHP disabled functions [ FOUND ]
- Checking expose_php option [ OFF ]
- Checking enable_dl option [ OFF ]
- Checking allow_url_fopen option [ ON ]
- Checking allow_url_include option [ OFF ]
- Checking listen option [ OK ]
[+] Squid Support
- Checking running Squid daemon [ 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 remote logging [ NOT ENABLED ]
- Checking log directories (static list) [ DONE ]
- Checking open log files [ DONE ]
- Checking deleted files in use [ FILES FOUND ]
[+] Insecure services
- Installed inetd package [ NOT FOUND ]
- Checking enabled inetd services [ OK ]
- Installed xinetd package [ OK ]
- xinetd status
- Installed rsh client package [ OK ]
- Installed rsh server package [ OK ]
- Installed telnet client package [ OK ]
- Installed telnet server package [ NOT FOUND ]
- Checking NIS client installation [ OK ]
- Checking NIS server installation [ OK ]
- Checking TFTP client installation [ SUGGESTION ]
- Checking TFTP server installation [ SUGGESTION ]
[+] Banners and identification
- /etc/issue [ FOUND ]
- /etc/issue contents [ WEAK ]
- /etc/issue.net [ FOUND ]
- /etc/issue.net contents [ WEAK ]
[+] Scheduled tasks
- Checking crontab and cronjob files [ DONE ]
[+] Accounting
- Checking accounting information [ NOT FOUND ]
- Checking sysstat accounting data [ DISABLED ]
- Checking auditd [ NOT FOUND ]


[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/132] [ NONE ]
[WARNING]: Test CRYP-7902 had a long execution: 19.277655 seconds
- Found 0 encrypted and 1 unencrypted swap devices in use. [ OK ]
- Kernel entropy is sufficient [ YES ]
- HW RNG & rngd [ NO ]
- SW prng [ YES ]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [ FOUND ]
- Checking AppArmor status [ DISABLED ]
- Checking presence SELinux [ NOT FOUND ]
- Checking presence TOMOYO Linux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ NONE ]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [ DISABLED ]
- dm-verity (status) [ DISABLED ]
- 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
File: /boot/grub/grub.cfg [ OK ]
File: /etc/crontab [ SUGGESTION ]
File: /etc/group [ OK ]

```
    File: /etc/crontab                                          [ SUGGESTION ]
    File: /etc/group                                            [ OK ]
    File: /etc/group-                                           [ OK ]
    File: /etc/hosts.allow                                      [ OK ]
    File: /etc/hosts.deny                                       [ OK ]
    File: /etc/issue                                            [ OK ]
    File: /etc/issue.net                                        [ OK ]
    File: /etc/motd                                             [ OK ]
    File: /etc/passwd                                           [ OK ]
    File: /etc/passwd-                                          [ OK ]
    File: /etc/ssh/sshd_config                                  [ SUGGESTION ]
    Directory: /root/.ssh                                       [ OK ]
    Directory: /etc/cron.d                                      [ SUGGESTION ]
    Directory: /etc/cron.daily                                  [ SUGGESTION ]
    Directory: /etc/cron.hourly                                 [ SUGGESTION ]
    Directory: /etc/cron.weekly                                 [ SUGGESTION ]
    Directory: /etc/cron.monthly                                [ SUGGESTION ]

[+] Home directories
------------------------------------

  - Permissions of home directories                             [ WARNING ]
  - Ownership of home directories                               [ OK ]
  - Checking shell history files                                [ OK ]

[+] Kernel Hardening
------------------------------------

  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                           [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                               [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                           [ OK ]
    - fs.protected_regular (exp: 2)                             [ OK ]
    - fs.protected_symlinks (exp: 1)                            [ OK ]
    - fs.suid_dumpable (exp: 0)                                 [ OK ]
    - kernel.core_uses_pid (exp: 1)                             [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                              [ OK ]
    - kernel.dmesg_restrict (exp: 1)                            [ OK ]
    - kernel.kptr_restrict (exp: 2)                             [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                          [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                       [ OK ]
    - kernel.randomize_va_space (exp: 2)                        [ OK ]
    - kernel.sysrq (exp: 0)                                     [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)                 [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                     [ DIFFERENT ]
    - net.core.bpf_jit_harden (exp: 2)                          [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)               [ DIFFERENT ]
    - 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)                     [ OK ]
    - 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 3.0.2 Results ]-

  Warnings (2):
  ----------------------------
  ! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
    https://cisofy.com/lynis/controls/PKGS-7388/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
    https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (51):
  ----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
    https://cisofy.com/lynis/controls/DEB-0280/

  * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
    https://cisofy.com/lynis/controls/DEB-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
    https://cisofy.com/lynis/controls/DEB-0811/

  * 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. [DEB-0831]
    https://cisofy.com/lynis/controls/DEB-0831/

  * Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
    https://cisofy.com/lynis/controls/DEB-0870/

  * Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
    https://cisofy.com/lynis/controls/DEB-0875/

  * Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
    https://cisofy.com/lynis/controls/DEB-0880/

  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    https://cisofy.com/lynis/controls/BOOT-5122/

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
    https://cisofy.com/lynis/controls/KRNL-5820/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
    https://cisofy.com/lynis/controls/AUTH-9230/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
    https://cisofy.com/lynis/controls/AUTH-9262/

  * When possible set expire dates for all password protected accounts [AUTH-9282]
    https://cisofy.com/lynis/controls/AUTH-9282/

  * Look at the locked accounts and consider removing them [AUTH-9284]
    https://cisofy.com/lynis/controls/AUTH-9284/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/lynis/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/
```

```
* Consider disabling unused kernel modules [FILE-6430]
  - Details  : /etc/modprobe.d/blacklist.conf
  - Solution : Add 'install MODULENAME /bin/true' (without quotes)
    https://cisofy.com/lynis/controls/FILE-6430/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
    https://cisofy.com/lynis/controls/USB-1000/

* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
    https://cisofy.com/lynis/controls/STRG-1846/

* Check DNS configuration for the dns domain name [NAME-4028]
    https://cisofy.com/lynis/controls/NAME-4028/

* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
    https://cisofy.com/lynis/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
    https://cisofy.com/lynis/controls/PKGS-7370/

* Consider using a tool to automatically apply upgrades [PKGS-7420]
    https://cisofy.com/lynis/controls/PKGS-7420/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
    https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
    https://cisofy.com/lynis/controls/HTTP-6643/

* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
    https://cisofy.com/lynis/controls/PHP-2376/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
    https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]
    https://cisofy.com/lynis/controls/LOGG-2190/

* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]
    https://cisofy.com/lynis/controls/INSE-8318/

* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]
    https://cisofy.com/lynis/controls/INSE-8320/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
    https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
    https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
    https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]
    https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
    https://cisofy.com/lynis/controls/ACCT-9628/

* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
    https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]
    https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]
  - Details  : See screen output or log file
  - Solution : Use chmod to change file permissions
    https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
    https://cisofy.com/lynis/controls/HOME-9304/

* 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/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
    https://cisofy.com/lynis/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/lynis/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)
```

```
* Harden compilers like restricting access to root user only [HRDN-7222]
    https://cisofy.com/lynis/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/lynis/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 : 60 [############        ]
Tests performed : 265
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [ ]  Forensics [ ]  Integration [ ]  Pentest [V] (running privileged)

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

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

Lynis 3.0.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2020, 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)
```

```
[+] Memory and Processes
------------------------------------

  - Checking /proc/meminfo                                  [ FOUND ]
  - Searching for dead/zombie processes                     [ NOT FOUND ]
  - Searching for IO waiting processes                      [ NOT FOUND ]
  - Search prelink tooling                                  [ NOT FOUND ]

[+] 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 ]
  - Password hashing methods                                [ OK ]
  - Checking password hashing rounds                        [ DISABLED ]
  - Query system users (non daemons)                        [ DONE ]
  - NIS+ authentication support                             [ NOT ENABLED ]
  - NIS authentication support                              [ NOT ENABLED ]
  - Sudoers file(s)                                         [ FOUND ]
    - Permissions for directory: /etc/sudoers.d             [ WARNING ]
    - Permissions for: /etc/sudoers                         [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root       [ OK ]
    - Permissions for: /etc/sudoers.d/README                [ 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                            [ SUGGESTION ]
  - Accounts without password                               [ OK ]
  - Locked accounts                                         [ FOUND ]
  - Checking user password aging (minimum)                  [ DISABLED ]
  - User password aging (maximum)                           [ DISABLED ]
  - Checking expired passwords                              [ OK ]
  - Checking Linux single user mode authentication          [ OK ]
  - 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 11 shells (valid shells: 11).
    - 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 ]
  - 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 /dev                                     [ HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
  - Checking Locate database                                  [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs 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)           [ NOT DISABLED ]

[+] NFS
------------------------------------
  - Query rpc registered programs                             [ DONE ]
  - Query NFS versions                                        [ DONE ]
  - Query NFS protocols                                       [ DONE ]
  - Check running NFS daemon                                  [ NOT FOUND ]
[+] Name services
------------------------------------
  - Searching DNS domain name                                 [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                         [ NONE ]
    - Presence of configured hostname in /etc/hosts           [ FOUND ]
    - Hostname mapped to localhost                            [ NOT FOUND ]
    - Localhost mapping to IP address                         [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                          [ FOUND ]
    - Querying package manager
```

```
[+] 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 or directory  [ WARNING ]
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 38820 (apt-get)
E: Unable to lock directory /var/lib/apt/lists/
  - Checking vulnerable packages (apt-get only)     [ DONE ]
  - Checking package audit tool                     [ INSTALLED ]
    Found: apt-get
  - Toolkit for automatic upgrades                  [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                     [ ENABLED ]
      Configuration method                          [ AUTO ]
      IPv6 only                                     [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 192.168.29.1                    [ OK ]
        Nameserver: 2405:201:6008:30e3::c0a8:1d01   [ OK ]
    - Minimal of 2 responsive nameservers           [ OK ]
    - DNSSEC supported (systemd-resolved)           [ UNKNOWN ]
  - Checking default gateway                        [ DONE ]
  - Getting listening ports (TCP/UDP)               [ SKIPPED ]
  - Checking promiscuous interfaces                 [ OK ]
  - Checking waiting connections                    [ OK ]
  - Checking status DHCP client
  - Checking for ARP monitoring software            [ NOT FOUND ]
  - Uncommon network protocols                      [ 0 ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                            [ NOT 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                    [ WARNING ]
    - Checking for unused rules                     [ OK ]
  - Checking host based firewall                    [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache (binary /usr/sbin/apache2)      [ FOUND ]
      Info: Configuration file found (/etc/apache2/apache2.conf)
```


Info: No virtual hosts found
* Loadable modules [ FOUND (118) ]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [ NOT FOUND ]
mod_reqtimeout/mod_qos [ FOUND ]
ModSecurity: web application firewall [ 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 [ FOUND ]
- Checking PHP disabled functions [ FOUND ]
- Checking expose_php option [ OFF ]
- Checking enable_dl option [ OFF ]
- Checking allow_url_fopen option [ ON ]
- Checking allow_url_include option [ OFF ]
- Checking listen option [ OK ]
[+] 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 remote logging [ NOT ENABLED ]
- Checking log directories (static list) [ DONE ]
- Checking open log files [ DONE ]

```
  - Checking log directories (static list)                    [ DONE ]
  - Checking open log files                                   [ DONE ]
  - Checking deleted files in use                             [ FILES FOUND ]

[+] Insecure services
------------------------------------

  - Installed inetd package                                   [ NOT FOUND ]
    - Checking enabled inetd services                         [ OK ]
  - Installed xinetd package                                  [ OK ]
    - xinetd status
  - Installed rsh client package                              [ OK ]
  - Installed rsh server package                              [ OK ]
  - Installed telnet client package                           [ OK ]
  - Installed telnet server package                           [ NOT FOUND ]
  - Checking NIS client installation                          [ OK ]
  - Checking NIS server installation                          [ OK ]
  - Checking TFTP client installation                         [ SUGGESTION ]
  - Checking TFTP server installation                         [ SUGGESTION ]

[+] Banners and identification
------------------------------------

  - /etc/issue                                                [ FOUND ]
    - /etc/issue contents                                     [ WEAK ]
  - /etc/issue.net                                            [ FOUND ]
    - /etc/issue.net contents                                 [ WEAK ]

[+] Scheduled tasks
------------------------------------

  - Checking crontab and cronjob files                        [ DONE ]

[+] Accounting
------------------------------------

  - Checking accounting information                           [ NOT FOUND ]
  - Checking sysstat accounting data                          [ DISABLED ]
  - Checking auditd                                           [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------

  - Checking for expired SSL certificates [0/132]             [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 19.769443 seconds

  - Found 0 encrypted and 1 unencrypted swap devices in use.  [ OK ]
  - Kernel entropy is sufficient                              [ YES ]
  - HW RNG & rngd                                             [ NO ]
  - SW prng                                                   [ YES ]

[+] Virtualization
------------------------------------
```


[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [ FOUND ]
- Checking AppArmor status [ DISABLED ]
- Checking presence SELinux [ NOT FOUND ]
- Checking presence TOMOYO Linux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ NONE ]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [ DISABLED ]
- dm-verity (status) [ DISABLED ]
- 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
File: /boot/grub/grub.cfg [ OK ]
File: /etc/crontab [ SUGGESTION ]
File: /etc/group [ OK ]
File: /etc/group- [ OK ]
File: /etc/hosts.allow [ OK ]
File: /etc/hosts.deny [ OK ]
File: /etc/issue [ OK ]
File: /etc/issue.net [ OK ]
File: /etc/motd [ OK ]
File: /etc/passwd [ OK ]
File: /etc/passwd- [ OK ]
File: /etc/ssh/sshd_config [ SUGGESTION ]
Directory: /root/.ssh [ OK ]
Directory: /etc/cron.d [ SUGGESTION ]
Directory: /etc/cron.daily [ SUGGESTION ]
Directory: /etc/cron.hourly [ SUGGESTION ]
Directory: /etc/cron.weekly [ SUGGESTION ]

```
[+] Home directories
------------------------------------

  - Permissions of home directories                         [ WARNING ]
  - Ownership of home directories                           [ OK ]
  - Checking shell history files                            [ OK ]

[+] Kernel Hardening
------------------------------------

  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                       [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                           [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                       [ OK ]
    - fs.protected_regular (exp: 2)                         [ OK ]
    - fs.protected_symlinks (exp: 1)                        [ OK ]
    - fs.suid_dumpable (exp: 0)                             [ OK ]
    - kernel.core_uses_pid (exp: 1)                         [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                          [ OK ]
    - kernel.dmesg_restrict (exp: 1)                        [ OK ]
    - kernel.kptr_restrict (exp: 2)                         [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                      [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                   [ OK ]
    - kernel.randomize_va_space (exp: 2)                    [ OK ]
    - kernel.sysrq (exp: 0)                                 [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)             [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                 [ DIFFERENT ]
    - net.core.bpf_jit_harden (exp: 2)                      [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)           [ DIFFERENT ]
    - 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)                 [ OK ]
    - 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 ]
```

```
* Enable sysstat to collect accounting (disabled) [ACCT-9626]
    https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
    https://cisofy.com/lynis/controls/ACCT-9628/

* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
    https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]
    https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]
  - Details  : See screen output or log file
  - Solution : Use chmod to change file permissions
    https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
    https://cisofy.com/lynis/controls/HOME-9304/

* 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/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
    https://cisofy.com/lynis/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/lynis/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 : 60 [############        ]
Tests performed : 265
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]
```

```
[+] Scheduled tasks
------------------------------------------------------------
  - Checking crontab and cronjob files                        [ DONE ]

[+] Accounting
------------------------------------------------------------
  - Checking accounting information                           [ NOT FOUND ]
  - Checking sysstat accounting data                          [ DISABLED ]
  - Checking auditd                                           [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------------------------------

[+] Cryptography
------------------------------------------------------------
  - Checking for expired SSL certificates [0/132]             [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 20.065627 seconds

  - Found 0 encrypted and 1 unencrypted swap devices in use.  [ OK ]
  - Kernel entropy is sufficient                              [ YES ]
  - HW RNG & rngd                                             [ NO ]
  - SW prng                                                   [ YES ]

[+] Virtualization
------------------------------------------------------------

[+] Containers
------------------------------------------------------------

[+] Security frameworks
------------------------------------------------------------
  - Checking presence AppArmor                                [ FOUND ]
    - Checking AppArmor status                                [ DISABLED ]
  - Checking presence SELinux                                 [ NOT FOUND ]
  - Checking presence TOMOYO Linux                            [ NOT FOUND ]
  - Checking presence grsecurity                              [ NOT FOUND ]
  - Checking for implemented MAC framework                    [ NONE ]

[+] Software: file integrity
------------------------------------------------------------
  - Checking file integrity tools
  - dm-integrity (status)                                     [ DISABLED ]
  - dm-verity (status)                                        [ DISABLED ]
  - 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
    File: /boot/grub/grub.cfg                                [ OK ]
    File: /etc/crontab                                       [ SUGGESTION ]
    File: /etc/group                                         [ OK ]
    File: /etc/group-                                        [ OK ]
    File: /etc/hosts.allow                                   [ OK ]
    File: /etc/hosts.deny                                    [ OK ]
    File: /etc/issue                                         [ OK ]
    File: /etc/issue.net                                     [ OK ]
    File: /etc/motd                                          [ OK ]
    File: /etc/passwd                                        [ OK ]
    File: /etc/passwd-                                       [ OK ]
    File: /etc/ssh/sshd_config                               [ SUGGESTION ]
    Directory: /root/.ssh                                    [ OK ]
    Directory: /etc/cron.d                                   [ SUGGESTION ]
    Directory: /etc/cron.daily                               [ SUGGESTION ]
    Directory: /etc/cron.hourly                              [ SUGGESTION ]
    Directory: /etc/cron.weekly                              [ SUGGESTION ]
    Directory: /etc/cron.monthly                             [ SUGGESTION ]

[+] Home directories
------------------------------------

  - Permissions of home directories                          [ WARNING ]
  - Ownership of home directories                            [ OK ]
  - Checking shell history files                             [ OK ]

[+] Kernel Hardening
------------------------------------

  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                        [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                            [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                        [ OK ]
    - fs.protected_regular (exp: 2)                          [ OK ]
    - fs.protected_symlinks (exp: 1)                         [ OK ]
    - fs.suid_dumpable (exp: 0)                              [ OK ]
    - kernel.core_uses_pid (exp: 1)                          [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                           [ OK ]
    - kernel.dmesg_restrict (exp: 1)                         [ OK ]
    - kernel.kptr_restrict (exp: 2)                          [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                       [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                    [ OK ]
    - kernel.randomize_va_space (exp: 2)                     [ OK ]
    - kernel.sysrq (exp: 0)                                  [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)              [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                  [ DIFFERENT ]
    - net.core.bpf_jit_harden (exp: 2)                       [ DIFFERENT ]
```

```
    - 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)                   [ OK ]
    - 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 3.0.2 Results ]-

  Warnings (2):
  ----------------------------
  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (51):
  ----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
      https://cisofy.com/lynis/controls/LYNIS/

  * Consider using a tool to automatically apply upgrades [PKGS-7420]
      https://cisofy.com/lynis/controls/PKGS-7420/

  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
```

```
Suggestions (51):

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

* Consider using a tool to automatically apply upgrades [PKGS-7420]
    https://cisofy.com/lynis/controls/PKGS-7420/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
    https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
    https://cisofy.com/lynis/controls/HTTP-6643/

* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
    https://cisofy.com/lynis/controls/PHP-2376/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
    https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]
    https://cisofy.com/lynis/controls/LOGG-2190/

* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]
    https://cisofy.com/lynis/controls/INSE-8318/

* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]
    https://cisofy.com/lynis/controls/INSE-8320/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
    https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
    https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
    https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]
```

Remotely trying to access contents of phone on same network:

```
┌──(root💀kali)-[~]
└─# lynis audit system remote 192.168.29.142

How to perform a remote scan:
═══════════════════════════════
Target  : 192.168.29.142
Command : ./lynis audit system

* Step 1: Create tarball
  mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis

* Step 2: Copy tarball to target 192.168.29.142
  scp -q ./files/lynis-remote.tar.gz 192.168.29.142:~/tmp-lynis-remote.tgz

* Step 3: Execute audit command
  ssh 192.168.29.142 "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system"

* Step 4: Clean up directory
  ssh 192.168.29.142 "rm -rf ~/tmp-lynis"

* Step 5: Retrieve log and report
  scp -q 192.168.29.142:/tmp/lynis.log ./files/192.168.29.142-lynis.log
  scp -q 192.168.29.142:/tmp/lynis-report.dat ./files/192.168.29.142-lynis-report.dat

* Step 6: Clean up tmp files (when using non-privileged account)
  ssh 192.168.29.142 "rm /tmp/lynis.log /tmp/lynis-report.dat"
```

```
┌──(root💀kali)-[~]
└─# sudo apt install apt-listbugs
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
apt-listbugs is already the newest version (0.1.35).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.

┌──(root💀kali)-[~]
└─# sudo apt install needrestart
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
needrestart is already the newest version (3.5-5).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.

┌──(root💀kali)-[~]
└─# sudo apt install apt-listchanges
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
apt-listchanges is already the newest version (3.24).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.
```

Executing suggestions:

```
┌──(root💀kali)-[/lynis]
└─# sudo apt-get install -y libpam-tmpdir
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  libpam-tmpdir
0 upgraded, 1 newly installed, 0 to remove and 1162 not upgraded.
Need to get 11.9 kB of archives.
After this operation, 54.3 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libpam-tmpdir amd64 0.09+b2 [11.9 kB]
Fetched 11.9 kB in 2s (5,106 B/s)
Selecting previously unselected package libpam-tmpdir.
(Reading database ... 271070 files and directories currently installed.)
Preparing to unpack .../libpam-tmpdir_0.09+b2_amd64.deb ...
Unpacking libpam-tmpdir (0.09+b2) ...
Setting up libpam-tmpdir (0.09+b2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install fail2ban
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  python3-systemd
Suggested packages:
  mailx monit
The following NEW packages will be installed:
  fail2ban python3-systemd
0 upgraded, 2 newly installed, 0 to remove and 1160 not upgraded.
Need to get 487 kB of archives.
After this operation, 2,337 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 fail2ban all 0.11.2-2 [451 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-systemd amd64 234-3+b4 [36.4 kB]
Fetched 487 kB in 15s (31.6 kB/s)
Retrieving bug reports ... Done
Parsing Found/Fixed information ... Done
serious bugs of fail2ban (→ 0.11.2-2) <Forwarded>
 b1 - #991449 - fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
Summary:
 fail2ban(1 bug)
Are you sure you want to install/upgrade the above packages? [Y/n/?/...] Y
Selecting previously unselected package fail2ban.
(Reading database ... 273242 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-2_all.deb ...
Unpacking fail2ban (0.11.2-2) ...
Selecting previously unselected package python3-systemd.
Preparing to unpack .../python3-systemd_234-3+b4_amd64.deb ...
Unpacking python3-systemd (234-3+b4) ...
Setting up fail2ban (0.11.2-2) ...
update-rc.d: We have no instructions for the fail2ban init script.
update-rc.d: It looks like a network service, we disable it.
fail2ban.service is a disabled or a static unit, not starting it.
Setting up python3-systemd (234-3+b4) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install debsecan
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  bsd-mailx exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libidn12 liblockfile1 libunbound8
Suggested packages:
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl
The following NEW packages will be installed:
  bsd-mailx debsecan exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libidn12 liblockfile1 libunbound8
0 upgraded, 9 newly installed, 0 to remove and 1160 not upgraded.
Need to get 3,327 kB of archives.
After this operation, 6,648 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-config all 4.95-2 [335 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-base amd64 4.95-2 [1,187 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libunbound8 amd64 1.13.1-1 [504 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libgnutls-dane0 amd64 3.7.2-2 [404 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 libidn12 amd64 1.38-3 [83.3 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-daemon-light amd64 4.95-2 [674 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 liblockfile1 amd64 1.17-1+b1 [17.0 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-2 [88.6 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 debsecan all 0.4.20.1 [33.2 kB]
Fetched 3,327 kB in 1min 14s (45.2 kB/s)
Retrieving bug reports ... Done
Parsing Found/Fixed information ... Done
Preconfiguring packages ...
Selecting previously unselected package exim4-config.
(Reading database ... 273712 files and directories currently installed.)
Preparing to unpack .../0-exim4-config_4.95-2_all.deb ...
Unpacking exim4-config (4.95-2) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../1-exim4-base_4.95-2_amd64.deb ...
Unpacking exim4-base (4.95-2) ...
Selecting previously unselected package libunbound8:amd64.
Preparing to unpack .../2-libunbound8_1.13.1-1_amd64.deb ...
Unpacking libunbound8:amd64 (1.13.1-1) ...
Selecting previously unselected package libgnutls-dane0:amd64.
Preparing to unpack .../3-libgnutls-dane0_3.7.2-2_amd64.deb ...
Unpacking libgnutls-dane0:amd64 (3.7.2-2) ...
Selecting previously unselected package libidn12:amd64.
Preparing to unpack .../4-libidn12_1.38-3_amd64.deb ...
Unpacking libidn12:amd64 (1.38-3) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../5-exim4-daemon-light_4.95-2_amd64.deb ...
Unpacking exim4-daemon-light (4.95-2) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack .../6-liblockfile1_1.17-1+b1_amd64.deb ...
Unpacking liblockfile1:amd64 (1.17-1+b1) ...
Selecting previously unselected package bsd-mailx.
```

```
Unpacking exim4-config (4.95-2) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../1-exim4-base_4.95-2_amd64.deb ...
Unpacking exim4-base (4.95-2) ...
Selecting previously unselected package libunbound8:amd64.
Preparing to unpack .../2-libunbound8_1.13.1-1_amd64.deb ...
Unpacking libunbound8:amd64 (1.13.1-1) ...
Selecting previously unselected package libgnutls-dane0:amd64.
Preparing to unpack .../3-libgnutls-dane0_3.7.2-2_amd64.deb ...
Unpacking libgnutls-dane0:amd64 (3.7.2-2) ...
Selecting previously unselected package libidn12:amd64.
Preparing to unpack .../4-libidn12_1.38-3_amd64.deb ...
Unpacking libidn12:amd64 (1.38-3) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../5-exim4-daemon-light_4.95-2_amd64.deb ...
Unpacking exim4-daemon-light (4.95-2) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack .../6-liblockfile1_1.17-1+b1_amd64.deb ...
Unpacking liblockfile1:amd64 (1.17-1+b1) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack .../7-bsd-mailx_8.1.2-0.20180807cvs-2_amd64.deb ...
Unpacking bsd-mailx (8.1.2-0.20180807cvs-2) ...
Selecting previously unselected package debsecan.
Preparing to unpack .../8-debsecan_0.4.20.1_all.deb ...
Unpacking debsecan (0.4.20.1) ...
Setting up libunbound8:amd64 (1.13.1-1) ...
Setting up libidn12:amd64 (1.38-3) ...
Setting up debsecan (0.4.20.1) ...
Setting up exim4-config (4.95-2) ...
Adding system-user for exim (v4)
Setting up liblockfile1:amd64 (1.17-1+b1) ...
Setting up libgnutls-dane0:amd64 (3.7.2-2) ...
Setting up exim4-base (4.95-2) ...
exim: DB upgrade, deleting hints-db
update-rc.d: As per Kali policy, exim4 init script is left disabled.
Created symlink /etc/systemd/system/timers.target.wants/exim4-base.timer → /lib/systemd/system/exim4-base.timer.
exim4-base.service is a disabled or a static unit not running, not starting it.
Setting up exim4-daemon-light (4.95-2) ...
Setting up bsd-mailx (8.1.2-0.20180807cvs-2) ...
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Processing triggers for libc-bin (2.31-9) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install debsums
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libfile-fnmatch-perl
The following NEW packages will be installed:
  debsums libfile-fnmatch-perl
0 upgraded, 2 newly installed, 0 to remove and 1160 not upgraded.
Need to get 55.7 kB of archives.
After this operation, 155 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libfile-fnmatch-perl amd64 0.02-2+b8 [10.4 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 debsums all 3.0.2 [45.3 kB]
Fetched 55.7 kB in 3s (18.4 kB/s)
Retrieving bug reports... Done
Parsing Found/Fixed information... Done
Selecting previously unselected package libfile-fnmatch-perl.
(Reading database ... 273948 files and directories currently installed.)
Preparing to unpack .../libfile-fnmatch-perl_0.02-2+b8_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-2+b8) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Setting up libfile-fnmatch-perl (0.02-2+b8) ...
Setting up debsums (3.0.2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

After installing all dependancies and installations,we will see this difference along with normal execution of all above executed commands: