



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

**SCHOOL OF COMPUTER SCIENCE ENGINEERING
AND INFORMATION SYSTEMS**

WINTER SEMESTER 2024-2025

PMCA605L – CYBER SECURITY

DIGITAL ASSIGNMENT – 1

TOOL CHOSEN: LYNIS

SUBMITTED ON: 07 – FEB - 2025

SUBMITTED BY-

AKASH KUMAR BANIK

PROGRAM: MCA

REGISTER No.: 24MCA0242

1. Identify any ONE Cyber Security tool of your choice for providing Security, Analysis, and Audit security for any organization. Expand the tool with a small example or application to understand the functionality of the tool. Write down the step-by-step process to use the tool with its use.

Lynis: A Comprehensive Cybersecurity Tool for Security Auditing and Analysis

Introduction to Lynis

Lynis is a powerful, open-source security auditing tool designed for Unix-based systems, including Kali Linux. It is widely used by system administrators, security professionals, and auditors to assess system security, analyze vulnerabilities, and ensure compliance with security policies. Unlike traditional antivirus programs, Lynis does not focus on detecting malware alone but performs a comprehensive security audit to identify misconfigurations, weak security settings, and potential vulnerabilities that may expose the system to attacks.

Lynis is commonly used for penetration testing, forensic analysis, compliance testing (ISO 27001, PCI-DSS, NIST, and HIPAA), and system hardening. Since Lynis does not require any agents to be installed, it provides a lightweight and efficient method for auditing systems without additional overhead.

Key Features of Lynis

- a) Security Auditing – Lynis performs detailed system audits by analyzing security settings, installed software, and misconfigurations.
- b) System Hardening Recommendations – After scanning the system, Lynis provides actionable recommendations to enhance security.
- c) Compliance Testing – It helps organizations meet compliance requirements for ISO 27001, PCI-DSS, NIST, and HIPAA by detecting violations in security policies.
- d) Malware and Rootkit Detection – Lynis scans the system for potential rootkits, malware, and unauthorized modifications in system files.
- e) Log File Analysis and Forensics – The tool helps identify security incidents by analyzing logs and tracking suspicious activities.

- f) Lightweight and Agentless – Lynis does not require installation of additional software agents, making it efficient for quick system audits.

STEP-BY-STEP GUIDE TO USING LYNIS ON KALI LINUX

Step 1: Installing Lynis

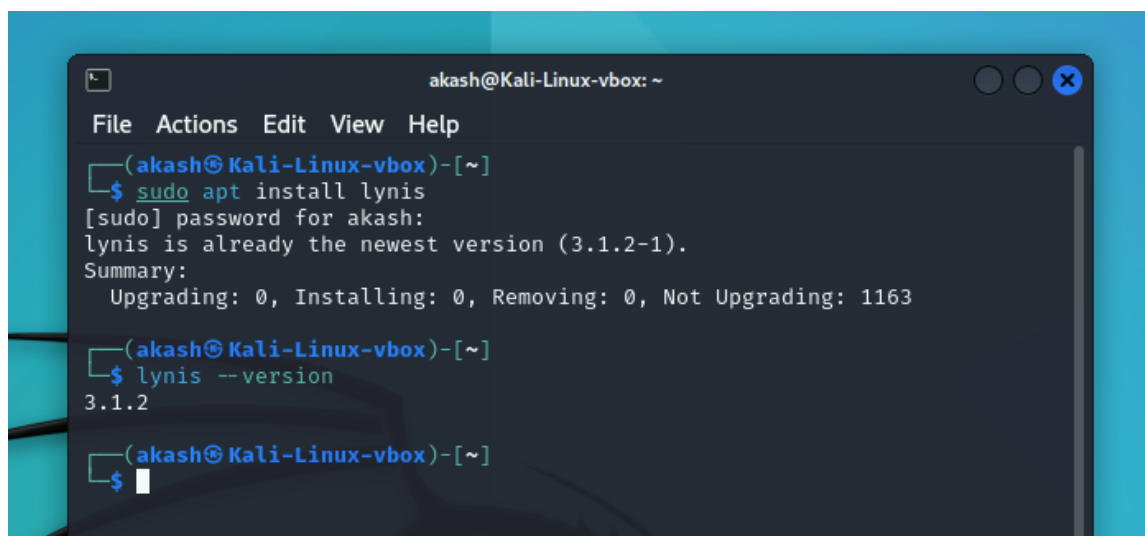
Lynis is pre-installed on Kali Linux, but if it is missing or needs an update, it can be installed using the following command:

```
sudo apt update && sudo apt install lynis
```

Once installed, the user can verify the installation by checking the version of Lynis:

```
lynis --version
```

If the installation is successful, the terminal will display the installed version of Lynis.

A screenshot of a terminal window titled 'akash@Kali-Linux-vbox: ~'. The terminal shows the following commands and output:

```
File Actions Edit View Help
(akash@Kali-Linux-vbox)-[~]
$ sudo apt install lynis
[sudo] password for akash:
lynis is already the newest version (3.1.2-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1163
(akash@Kali-Linux-vbox)-[~]
$ lynis --version
3.1.2
(akash@Kali-Linux-vbox)-[~]
$
```

Step 2: Performing a Full System Security Audit

To conduct a comprehensive security audit, the following command is used:

```
sudo lynis audit system
```

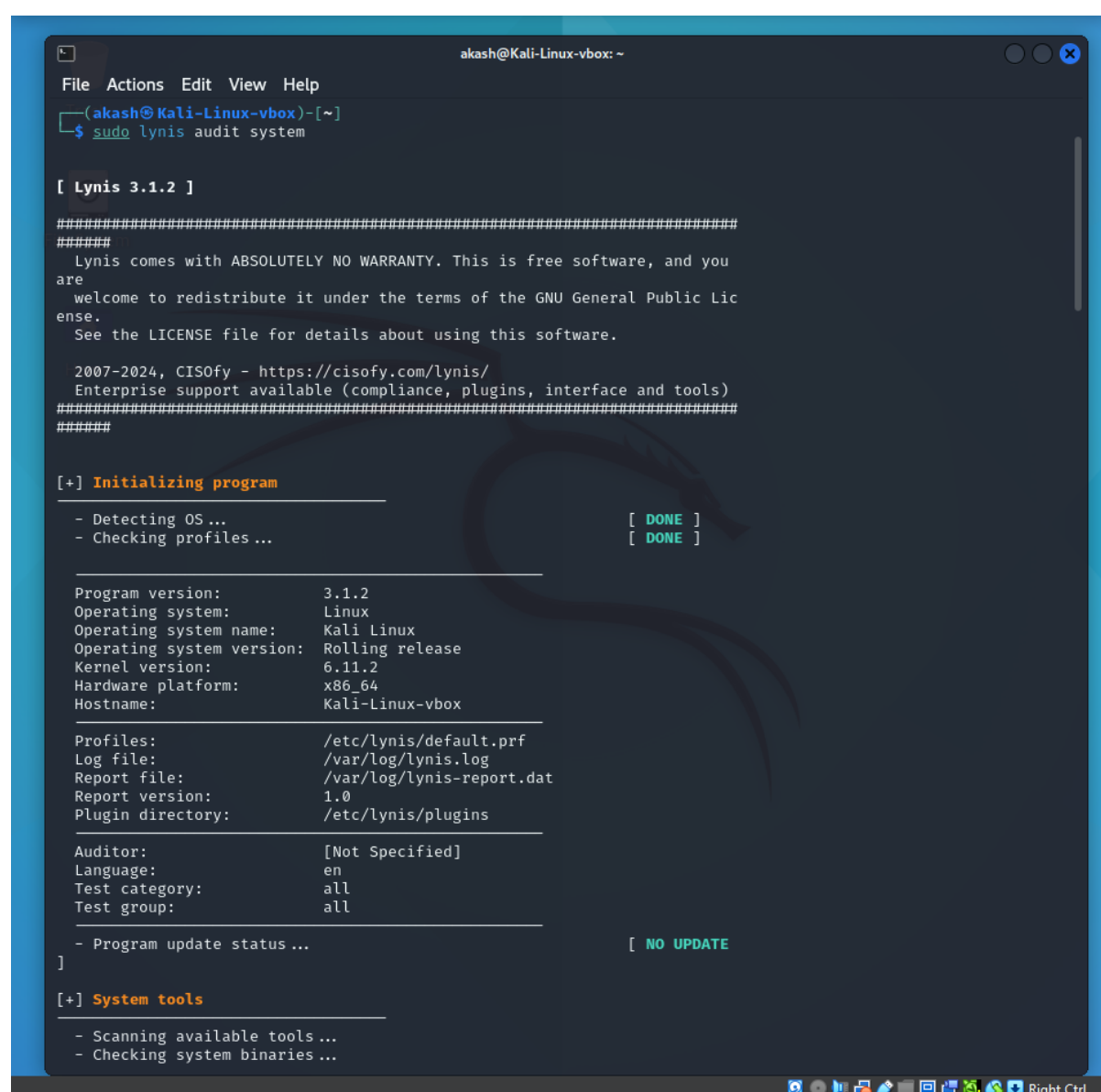
What Happens During the Scan?

Lynis begins analyzing system files, configurations, and installed software.

It runs hundreds of security tests, including checks for firewall status, SSH security, user authentication methods, system integrity, and log file analysis.

A detailed audit report is displayed in the terminal, highlighting warnings and security suggestions.

The results are stored in a log file (**/var/log/lynis.log**) for later review.



```
akash@Kali-Linux-vbox: ~  
File Actions Edit View Help  
(akash@Kali-Linux-vbox)-[~]  
$ sudo lynis audit system  
  
[ Lynis 3.1.2 ]  
#####  
#####  
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 Lic  
ense.  
See the LICENSE file for details about using this software.  
  
2007-2024, CISOfy - https://cisofy.com/lynis/  
Enterprise support available (compliance, plugins, interface and tools)  
#####  
#####  
[+] Initializing program  
-----  
- Detecting OS ... [ DONE ]  
- Checking profiles ... [ DONE ]  
-----  
Program version: 3.1.2  
Operating system: Linux  
Operating system name: Kali Linux  
Operating system version: Rolling release  
Kernel version: 6.11.2  
Hardware platform: x86_64  
Hostname: Kali-Linux-vbox  
-----  
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 ...
```

Step 3: Understanding the Audit Results

Once the audit is complete, Lynis provides a security report with warnings and recommendations. Each finding is assigned a status, such as:

- [OK] – No issues detected.
- [WARNING] – A potential security risk that should be reviewed.
- [SUGGESTION] – Recommended improvement for better security.

AUDIT REPORT OUTPUT:

```

File  Actions  Edit  View  Help

[+] 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 18 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 18 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
  - ModemManager.service: [ MEDIUM ]
  - NetworkManager.service: [ EXPOSED ]
  - accounts-daemon.service: [ MEDIUM ]
  - colord.service: [ PROTECTED ]
  - cron.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - emergency.service: [ UNSAFE ]
  - getty@tty1.service: [ UNSAFE ]
  - haveged.service: [ PROTECTED ]
  - lightdm.service: [ UNSAFE ]
  - lynis.service: [ UNSAFE ]
  - pcscd.service: [ UNSAFE ]
  - plymouth-start.service: [ UNSAFE ]
  - polkit.service: [ PROTECTED ]
  - rc-local.service: [ UNSAFE ]
  - rescue.service: [ UNSAFE ]
  - rpc-gssd.service: [ UNSAFE ]
  - rpc-statd-notify.service: [ UNSAFE ]
  - rpc-svcgssd.service: [ UNSAFE ]
  - rtkit-daemon.service: [ MEDIUM ]
  - smartmontools.service: [ UNSAFE ]
  - ssh.service: [ UNSAFE ]
  - systemd-ask-password-console.service: [ UNSAFE ]
  - systemd-ask-password-plymouth.service: [ UNSAFE ]
  - systemd-ask-password-wall.service: [ UNSAFE ]
  - systemd-bsod.service: [ UNSAFE ]
  - systemd-hostnamed.service: [ PROTECTED ]
  - systemd-initctl.service: [ UNSAFE ]
  - systemd-journald.service: [ PROTECTED ]
  - systemd-logind.service: [ PROTECTED ]
  - systemd-networkd.service: [ PROTECTED ]
  - systemd-rfkill.service: [ UNSAFE ]

```

```

File Actions Edit View Help
[+] Kernel
- Checking default runlevel [ runlevel 5 ]
- Checking CPU support (NX/PAE) [ FOUND ]
  CPU support: PAE and/or NoeXecute supported [ DONE ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules
  Found 90 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 /etc/security/limits.conf [ ENABLED ]
  - 'soft' configuration in /etc/security/limits.conf [ DISABLED ]
- 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/ospd-openvas [ OK ]
  - Permissions for: /etc/sudoers.d/README [ OK ]
  - Permissions for: /etc/sudoers.d/kali-grant-root [ OK ]
- PAM password strength tools [ SUGGESTION ]

```

```

File Actions Edit View Help
[+] Kerberos
- Check for Kerberos KDC and principals [ NOT FOUND ]

[+] Shells
- Checking shells from /etc/shells
  Result: found 14 shells (valid shells: 14).
- Session timeout settings/tools [ NONE ]
- Checking default umask values [ NONE ]
- 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 [ OK ]
  - 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 [ PARTIALLY HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Mount options of /tmp [ PARTIALLY HARDENED ]
- Total without nodev:5 noexec:9 nosuid:3 ro or noexec (W^X): 9 of total 31
- JBD driver loaded and in use [ OK ]
- Checking locate database [ FOUND ]
- Disable kernel support of some filesystems

[+] 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 ]

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
[+] 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 RPM package manager [ FOUND ]
- Querying RPM package manager
- Searching dpkg package manager [ FOUND ]
- Querying package manager

[WARNING]: Test PKGS-7345 had a long execution: 22.628994 seconds
- Query unpurged packages [ NONE ]
- Checking APT package database [ OK ]
- Checking vulnerable packages (apt-get only) [ DONE ]

[WARNING]: Test PKGS-7392 had a long execution: 89.789997 seconds
- Checking upgradeable packages [ SKIPPED ]
- 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: 10.0.2.3 [ OK ]
- Minimal of 2 responsive nameservers [ WARNING ]
- Checking default gateway [ DONE ]
- Getting listening ports (TCP/UDP) [ SKIPPED ]
- Checking promiscuous interfaces [ OK ]
- Checking waiting connections [ OK ]
- Checking status DHCP client [ NOT ACTIVE ]
- Checking for ARP monitoring software [ NOT FOUND ]
- Uncommon network protocols [ 0 ]

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
[+] 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 ]

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
[+] 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 [ NOT FOUND ]
- Checking RFC 3195 daemon status [ NOT FOUND ]
- Checking minilogd instances [ NOT FOUND ]
- Checking wazuh-agent daemon status [ 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 ]
- Installed xinetd package [ OK ]
- xinetd status [ NOT ACTIVE ]
- Installed rsh client package [ SUGGESTION ]
- 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 ]

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
[+] 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 [ FOUND ]
- dm-integrity (status) [ DISABLED ]
- dm-verity (status) [ DISABLED ]
- Checking presence integrity tool [ NOT FOUND ]

[+] Software: System tooling
- Checking automation tooling [ FOUND ]
- Automation tooling [ NOT FOUND ]
- Checking for IDS/IPS tooling [ NONE ]

[+] Software: Malware
- Malware software components [ NOT FOUND ]

```



```
akash@Kali-Linux-vbox: ~  
File Actions Edit View Help  
[+] Hardening  
- Installed compiler(s) [ FOUND ]  
- Installed malware scanner [ NOT FOUND ]  
- Non-native binary formats [ FOUND ]  
[+] Custom tests  
- Running custom tests... [ NONE ]  
[+] Plugins (phase 2)  
  
-[ Lynis 3.1.2 Results ]-  
  
Warnings (2):  
! Couldn't find 2 responsive nameservers [NETW-2705]  
  https://cisofy.com/lynis/controls/NETW-2705/  
! iptables module(s) loaded, but no rules active [FIRE-4512]  
  https://cisofy.com/lynis/controls/FIRE-4512/
```

```
Suggestions (50):  
* 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 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/
```

```
akash@Kali-Linux-vbox: ~  
File Actions Edit View Help  
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 : 273
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 3.1.2

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

2007-2024, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

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

(akash@Kali-Linux-vbox)-[~]
```

INTERPRETING THE RESULTS

Boot and Services

- systemd is used as the service manager.
- UEFI boot is disabled, reducing security benefits.
- GRUB2 lacks password protection, making it vulnerable.
- 18 services are running at boot; some (cron.service, dbus.service, lightdm.service, ssh.service) are marked UNSAFE.
- Protected services include polkit.service and systemd-timesyncd.service.

Kernel Security

- Kernel is up to date, but 90 active modules should be reviewed.
- Setuid core dumps are disabled.

- Some kernel parameters (kernel.kptr_restrict, net.ipv4.conf.all.accept_redirects) need adjustment for security.

Memory and Processes

- No zombie or IO waiting processes.
- Prelink tooling is absent but not critical.

Ports and Packages

- RPM and dpkg are functional; no unpurged packages.
- APT database is OK, but vulnerability checks are slow.
- Automatic updates are disabled.

Networking

- IPv6 is enabled.
- Only one nameserver detected; two recommended.
- Default gateway and DHCP settings are correct.
- No promiscuous mode detected.

Security Framework

- AppArmor is disabled.
- No SELinux, grsecurity, or MAC frameworks found.

File Integrity and Permissions

- dm-integrity and dm-verity are disabled.
- Files like /etc/crontab and /etc/ssh/sshd_config need permission adjustments.
- Home directory permissions are misconfigured.

Malware and IDS/IPS

- No malware detection or IDS/IPS tools installed.

Kernel Hardening

- Some sysctl settings (kernel.kptr_restrict, net.core.bpf_jit_harden) need adjustments.
- Others (fs.protected_hardlinks, kernel.randomize_va_space) are properly configured.

Based on these results, the system administrator can apply security fixes to improve system security.

Recommendations:

- Enable UEFI boot and GRUB2 password protection.
- Secure unsafe services (cron, ssh, lightdm).
- Adjust kernel parameters for better security.
- Enable AppArmor and consider additional security frameworks.
- Install malware detection and IDS/IPS tools.
- Use at least two nameservers.
- Fix file permissions for sensitive system files and home directories.

Implementing these changes will enhance security.

Step 4: Running a Specific Security Check

Instead of performing a full audit, Lynis allows users to run specific security checks. For example, if the analyst wants to check only for malware and rootkits, the following command is used:

```
sudo lynis audit system --tests-from-group malware
```

This command focuses only on malware-related tests, reducing scan time while providing targeted insights.

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
(akash@Kali-Linux-vbox)-[~]
$ sudo lynis audit system --tests-from-group malware

[ Lynis 3.1.2 ]

#####
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.

2007-2024, CISOFY - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

Program version: 3.1.2
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.11.2
Hardware platform: x86_64
Hostname: Kali-Linux-vbox

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: malware

- Program update status... [ NO UPDATE ]

[+] System tools
- Scanning available tools...
- Checking system binaries...

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
[+] 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):
[WARNING]: Test DEB-0001 had a long execution: 36.845704 seconds
- libpam-tmpdir [ Not Installed ]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Software:
- apt-listbugs [ Not Installed ]
- apt-listchanges [ Not Installed ]
- needrestart [ Not Installed ]
- fail2ban [ Not Installed ]
]
[+] Software: Malware
- Malware software components [ NOT FOUND ]
[+] Custom tests
- Running custom tests... [ NONE ]
[+] Plugins (phase 2)

-[ Lynis 3.1.2 Results ]-
Great, no warnings
Suggestions (6):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update availab
e. [LYNIS]

```

```

akash@Kali-Linux-vbox: ~
File Actions Edit View Help
Suggestions (6):
* 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 fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
  https://cisofy.com/lynis/controls/DEB-0880/

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 : 1 [#]
Tests performed : 16
Plugins enabled : 1

Components:
- Firewall [X]
- 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

```

```

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

Lynis 3.1.2

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

2007-2024, 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)

(akash@Kali-Linux-vbox)-[~]
$

```

Summary of Scan Results:

- Malware software components: NOT FOUND (No detected malware)
- Warnings: None (which is a good sign!)
- Suggestions (6):
 - Lynis version is outdated (Consider updating)
 - Install libpam-tmpdir (Helps set secure temp directories)
 - Install apt-listbugs (Shows critical bugs before installing packages)
 - Install apt-listchanges (Displays significant package changes before upgrades)
 - Install needrestart (Checks which services need restarting after updates)
 - Install fail2ban (Protects against brute-force attacks)

Step 5: Exporting and Reviewing the Audit Report

After performing a security audit with Lynis, it is crucial to save and analyze the findings for further investigation and future security improvements. The Lynis report contains valuable insights about system vulnerabilities, recommended security enhancements, and compliance status.

To save the audit results for further analysis, the analyst can export the report using:

```
sudo lynis show report > lynis-security-report.txt
```

This generates a text file (lynis-security-report.txt) containing all audit findings, allowing system administrators to track security improvements over time.

OR,

We can also use the following command:

```
# Copy the Lynis report to a more accessible location  
sudo cp /var/log/lynis-report.dat ~/lynis-security-report.txt  
  
# Change file ownership to the current user for easy access  
sudo chown $USER:$USER ~/lynis-security-report.txt
```

Why This Approach?

Direct redirection (> issue fix):

- Running `sudo lynis show report > lynis-security-report.txt` may not work as expected because lynis show report displays the report interactively and does not output text in a structured format.
- Instead, copying the Lynis report file (`/var/log/lynis-report.dat`) ensures that all results are preserved.

Making the file accessible:

- By default, Lynis logs are stored in `/var/log/`, a directory that requires root permissions to access.
- Copying the file to the user's home directory (`~/`) and changing ownership (`chown`) allows a non-root user to read and analyze it without using `sudo` repeatedly.

Viewing the Report

Once the report is saved, we can review it using various methods:

- View the report in the terminal:

```
cat ~/lynis-security-report.txt
```

- Open it in a text editor (nano, vim, or less):

```
nano ~/lynis-security-report.txt # Edit in nano
```

```
vim ~/lynis-security-report.txt # View in Vim
```

```
less ~/lynis-security-report.txt # Paginated view
```

Analyzing the Report

After reviewing the report, system administrators can:

- Identify security gaps (e.g., outdated software, weak configurations).
- Follow Lynis recommendations to improve hardening scores.
- Track security enhancements over time by comparing previous audit reports.
- Export results for compliance reporting in security audits.

Conclusion

By following the step-by-step guide above, users can leverage Lynis to conduct comprehensive security audits, identify risks, and implement recommended security measures to strengthen their Linux systems. Regular audits with Lynis ensure that the system remains secure, hardened, and compliant with industry best practices.