## **Linux Systems Administration**

### **Step 1: Ensure/Double Check Permissions on Sensitive Files**

1. Permissions on /etc/shadow should allow only root read and write access.
   1. Command to inspect permissions:

|  |
| --- |
| ls -l /etc/shadow |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chown root:root /etc/gshadow |

1. Permissions on /etc/gshadow should allow only root read and write access.
   1. Command to inspect permissions:

|  |
| --- |
| ls -l /etc/gshadow |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chown root:root /etc/passwd |

1. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
   1. Command to inspect permissions:

|  |
| --- |
| ls -l group |

* 1. Command to set permissions (if needed):

|  |
| --- |
| chmod *+rwx* group (or -rwx) |

1. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   1. Command to inspect permissions:

|  |
| --- |
| ls -l passwd |

* 1. Command to set permissions (if needed):

|  |
| --- |
| chmod *+rwx* passwd (or -rwx) |

### **Step 2: Create User Accounts**

1. Add user accounts for sam, joe, amy, sara, and admin with the useradd command.
   1. Command to add each user account (include all five users):

|  |
| --- |
| 1. Change to root by using sudo su 2. Useradd Sam 3. Useradd Joe 4. Useradd Amy 5. Useradd Sara 6. Useradd Admin 7. Check using cat /etc/passwd |

1. Ensure that only the admin has general sudo access.
   1. Command to add admin to the sudo group:

|  |
| --- |
| 1. Make sure you are still in root 2. sudo usermod -aG sudo admin |

### **Step 3: Create User Group and Collaborative Folder**

1. Add an engineers group to the system.
   1. Command to add group:

|  |
| --- |
| sudo groupadd engineers |

1. Add users sam, joe, amy, and sara to the managed group.
   1. Command to add users to engineers group (include all four users):

|  |
| --- |
| sudo usermod -a -G engineers sam |

1. Create a shared folder for this group at /home/engineers.
   1. Command to create the shared folder:

|  |
| --- |
| sudo mkdir -p /home/engineers |

1. Change ownership on the new engineers’ shared folder to the engineers group.
   1. Command to change ownership of engineers’ shared folder to engineers group:

|  |
| --- |
| sudo chgrp -R engineers /home/engineers |

### **Step 4: Lynis Auditing**

1. Command to install Lynis:

|  |
| --- |
| apt-cache policy lynis |

1. Command to view documentation and instructions:

|  |
| --- |
| lynis man |

1. Command to run an audit:

|  |
| --- |
| sudo lynis audit system |

1. Provide a report from the Lynis output with recommendations for hardening the system.

[ Lynis 3.0.8 ]

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

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.

2007-2021, CISOfy - https://cisofy.com/lynis/

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

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

[+] Initializing program

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

- Detecting OS... [ DONE ]

- Checking profiles... [ DONE ]

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

Program version: 3.0.8

Operating system: Linux

Operating system name: Ubuntu

Operating system version: 20.04

Kernel version: 5.13.0

Hardware platform: x86\_64

Hostname: image-ubuntu-adhoc-vm-student33

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

Profiles: /etc/lynis/default.prf

Log file: /var/log/lynis.log

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

Report version: 1.0

Plugin directory: /usr/share/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

- Plugins enabled [ NONE ]

[+] Boot and services

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

- Service Manager [ systemd ]

- Checking UEFI boot [ ENABLED ]

- Checking Secure Boot [ DISABLED ]

- Checking presence GRUB2 [ FOUND ]

- Checking for password protection [ NONE ]

- Check running services (systemctl) [ DONE ]

Result: found 47 running services

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

Result: found 107 enabled services

- Check startup files (permissions) [ OK ]

- Running 'systemd-analyze security'

- ModemManager.service: [ MEDIUM ]

- NetworkManager.service: [ EXPOSED ]

- accounts-daemon.service: [ UNSAFE ]

- acpid.service: [ UNSAFE ]

- alsa-state.service: [ UNSAFE ]

- anacron.service: [ UNSAFE ]

- apache2.service: [ UNSAFE ]

- apport.service: [ UNSAFE ]

- atd.service: [ UNSAFE ]

- avahi-daemon.service: [ UNSAFE ]

- blueman-mechanism.service: [ UNSAFE ]

- chrony.service: [ EXPOSED ]

- cloud-init-hotplugd.service: [ UNSAFE ]

- colord.service: [ EXPOSED ]

- containerd.service: [ UNSAFE ]

- cron.service: [ UNSAFE ]

- cups-browsed.service: [ UNSAFE ]

- cups.service: [ UNSAFE ]

- dbus.service: [ UNSAFE ]

- dm-event.service: [ UNSAFE ]

- dmesg.service: [ UNSAFE ]

- docker.service: [ UNSAFE ]

- dovecot.service: [ EXPOSED ]

- emergency.service: [ UNSAFE ]

- firewalld.service: [ UNSAFE ]

- gdm.service: [ UNSAFE ]

- getty@tty1.service: [ UNSAFE ]

- hddtemp.service: [ UNSAFE ]

- hv-fcopy-daemon.service: [ UNSAFE ]

- hv-kvp-daemon.service: [ UNSAFE ]

- hv-vss-daemon.service: [ UNSAFE ]

- irqbalance.service: [ MEDIUM ]

- iscsid.service: [ UNSAFE ]

- kerneloops.service: [ UNSAFE ]

- lvm2-lvmpolld.service: [ UNSAFE ]

- lxd-agent.service: [ UNSAFE ]

- multipathd.service: [ UNSAFE ]

- nessusd.service: [ UNSAFE ]

- networkd-dispatcher.service: [ UNSAFE ]

- nginx.service: [ UNSAFE ]

- nmbd.service: [ UNSAFE ]

- ondemand.service: [ UNSAFE ]

- open-vm-tools.service: [ UNSAFE ]

- plymouth-start.service: [ UNSAFE ]

- polkit.service: [ UNSAFE ]

- postfix@-.service: [ UNSAFE ]

- rc-local.service: [ UNSAFE ]

- rescue.service: [ UNSAFE ]

- resolvconf.service: [ UNSAFE ]

- restore\_firewall.service: [ UNSAFE ]

- rsync.service: [ UNSAFE ]

- rsyslog.service: [ UNSAFE ]

- rtkit-daemon.service: [ MEDIUM ]

- serial-getty@ttyS0.service: [ UNSAFE ]

- smbd.service: [ UNSAFE ]

- snap.lxd.daemon.service: [ UNSAFE ]

- snapd.aa-prompt-listener.service: [ UNSAFE ]

- snapd.service: [ UNSAFE ]

- ssh.service: [ UNSAFE ]

- switcheroo-control.service: [ EXPOSED ]

- 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: [ PROTECTED ]

- systemd-logind.service: [ PROTECTED ]

- systemd-networkd.service: [ PROTECTED ]

- systemd-resolved.service: [ PROTECTED ]

- systemd-rfkill.service: [ UNSAFE ]

- systemd-udevd.service: [ EXPOSED ]

- udisks2.service: [ UNSAFE ]

- unattended-upgrades.service: [ UNSAFE ]

- upower.service: [ PROTECTED ]

- user@1002.service: [ UNSAFE ]

- user@128.service: [ UNSAFE ]

- uuidd.service: [ PROTECTED ]

- vgauth.service: [ UNSAFE ]

- vsftpd.service: [ UNSAFE ]

- walinuxagent.service: [ UNSAFE ]

- whoopsie.service: [ UNSAFE ]

- wpa\_supplicant.service: [ UNSAFE ]

- xinetd.service: [ UNSAFE ]

- xrdp-sesman.service: [ UNSAFE ]

- xrdp.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 98 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 [ DEFAULT ]

- 'soft' configuration in /etc/security/limits.conf [ DEFAULT ]

- Checking setuid core dumps configuration [ PROTECTED ]

- Check if reboot is needed [ YES ]

[+] 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 [ SUGGESTION ]

- 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 [ OK ]

- Permissions for: /etc/sudoers [ WARNING ]

- Permissions for: /etc/sudoers.d/README [ OK ]

- Permissions for: /etc/sudoers.d/90-cloud-init-users [ 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 9 shells (valid shells: 9).

- 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) [ NONE ]

- 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 [ NON DEFAULT ]

- Mount options of /dev/shm [ PARTIALLY HARDENED ]

- Mount options of /run [ HARDENED ]

- Total without nodev:7 noexec:26 nosuid:19 ro or noexec (W^X): 13 of total 55

- Checking Locate database [ FOUND ]

- Disable kernel support of some filesystems

[+] USB Devices

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

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

- Checking USB devices authorization [ DISABLED ]

- Checking USBGuard [ NOT FOUND ]

[+] Storage

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

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

[+] NFS

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

- Check running NFS daemon [ NOT FOUND ]

[+] Name services

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

- Checking search domains [ FOUND ]

- Searching DNS domain name [ UNKNOWN ]

- Checking /etc/hosts

- Duplicate entries in hosts file [ NONE ]

- Presence of configured hostname in /etc/hosts [ NOT 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 [ OK ]

- Checking APT package database [ OK ]

- Checking vulnerable packages [ WARNING ]

[WARNING]: Test PKGS-7392 had a long execution: 22.041293 seconds

- Checking upgradeable packages [ SKIPPED ]

- Checking package audit tool [ INSTALLED ]

Found: apt-get

- Toolkit for automatic upgrades (unattended-upgrade) [ FOUND ]

[+] Networking

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

- Checking IPv6 configuration [ ENABLED ]

Configuration method [ AUTO ]

IPv6 only [ NO ]

- Checking configured nameservers

- Testing nameservers

Nameserver: 8.8.8.8 [ OK ]

Nameserver: 127.0.0.53 [ OK ]

- DNSSEC supported (systemd-resolved) [ NO ]

- Checking default gateway [ DONE ]

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

- 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 [ RUNNING ]

- Checking CUPS configuration file [ OK ]

- File permissions [ WARNING ]

- Checking CUPS addresses/sockets [ FOUND ]

- Checking lp daemon [ NOT RUNNING ]

[+] Software: e-mail and messaging

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

- Postfix status [ RUNNING ]

- Postfix configuration [ FOUND ]

- Postfix banner [ WARNING ]

[+] Software: firewalls

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

- Checking iptables kernel module [ FOUND ]

- Checking iptables policies of chains [ FOUND ]

- Checking for empty ruleset [ OK ]

- Checking for unused rules [ FOUND ]

- Checking host based firewall [ ACTIVE ]

[+] Software: webserver

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

- Checking Apache (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 [ FOUND ]

- Searching SSH configuration [ FOUND ]

- OpenSSH option: AllowTcpForwarding [ SUGGESTION ]

- OpenSSH option: ClientAliveCountMax [ SUGGESTION ]

- OpenSSH option: ClientAliveInterval [ OK ]

- OpenSSH option: Compression [ SUGGESTION ]

- OpenSSH option: FingerprintHash [ OK ]

- OpenSSH option: GatewayPorts [ OK ]

- OpenSSH option: IgnoreRhosts [ OK ]

- OpenSSH option: LoginGraceTime [ OK ]

- OpenSSH option: LogLevel [ SUGGESTION ]

- OpenSSH option: MaxAuthTries [ SUGGESTION ]

- OpenSSH option: MaxSessions [ SUGGESTION ]

- OpenSSH option: PermitRootLogin [ OK ]

- OpenSSH option: PermitUserEnvironment [ OK ]

- OpenSSH option: PermitTunnel [ OK ]

- OpenSSH option: Port [ SUGGESTION ]

- OpenSSH option: PrintLastLog [ OK ]

- OpenSSH option: StrictModes [ OK ]

- OpenSSH option: TCPKeepAlive [ SUGGESTION ]

- OpenSSH option: UseDNS [ OK ]

- OpenSSH option: X11Forwarding [ SUGGESTION ]

- OpenSSH option: AllowAgentForwarding [ SUGGESTION ]

- OpenSSH option: AllowUsers [ NOT FOUND ]

- OpenSSH option: AllowGroups [ NOT FOUND ]

[+] SNMP Support

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

- Checking running SNMP daemon [ NOT FOUND ]

[+] Databases

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

No database engines found

[+] LDAP Services

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

- Checking OpenLDAP instance [ NOT FOUND ]

[+] PHP

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

- Checking PHP [ NOT FOUND ]

[+] Squid Support

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

- Checking running Squid daemon [ NOT FOUND ]

[+] Logging and files

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

- Checking for a running log daemon [ OK ]

- Checking Syslog-NG status [ NOT FOUND ]

- Checking systemd journal status [ FOUND ]

- Checking Metalog status [ NOT FOUND ]

- Checking RSyslog status [ FOUND ]

- Checking RFC 3195 daemon status [ NOT FOUND ]

- Checking minilogd instances [ NOT FOUND ]

- Checking logrotate presence [ OK ]

- Checking 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 [ FOUND ]

- xinetd status

- Enabled xinetd.d services [ NOT FOUND ]

- 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 [ OK ]

- Checking TFTP server installation [ OK ]

[+] 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 ]

- Checking atd status [ RUNNING ]

- Checking at users [ DONE ]

- Checking at jobs [ NONE ]

[+] Accounting

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

- Checking accounting information [ NOT FOUND ]

- Checking sysstat accounting data [ NOT FOUND ]

- Checking auditd [ NOT FOUND ]

[+] Time and Synchronization

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

- NTP daemon found: chronyd [ FOUND ]

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

[+] Cryptography

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

- Checking for expired SSL certificates [0/129] [ NONE ]

[WARNING]: Test CRYP-7902 had a long execution: 19.482465 seconds

- Found 0 encrypted and 0 unencrypted swap devices in use. [ OK ]

- Kernel entropy is sufficient [ YES ]

- HW RNG & rngd [ NO ]

- SW prng [ NO ]

- MOR variable not found [ WEAK ]

[+] Virtualization

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

[+] Containers

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

- Docker

- Docker daemon [ RUNNING ]

- Docker info output (warnings) [ NONE ]

[WARNING]: Test CONT-8104 had a long execution: 14.321128 seconds

- Containers

- Total containers [ 0 ]

- File permissions [ OK ]

[+] Security frameworks

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

- Checking presence AppArmor [ FOUND ]

- Checking AppArmor status [ ENABLED ]

Found 2975 unconfined processes

- Checking presence SELinux [ NOT FOUND ]

- Checking presence TOMOYO Linux [ NOT FOUND ]

- Checking presence grsecurity [ NOT FOUND ]

- Checking for implemented MAC framework [ OK ]

[+] Software: file integrity

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

- Checking file integrity tools

- Tripwire [ FOUND ]

- dm-integrity (status) [ DISABLED ]

- dm-verity (status) [ DISABLED ]

- Checking presence integrity tool [ FOUND ]

[+] Software: System tooling

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

- Checking automation tooling

- Ansible artifact [ FOUND ]

- Automation tooling [ FOUND ]

- Checking for IDS/IPS tooling [ NONE ]

[+] Software: Malware

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

- Checking chkrootkit [ FOUND ]

- Malware software components [ FOUND ]

- Active agent [ NOT FOUND ]

- Rootkit scanner [ FOUND ]

[+] File Permissions

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

- Starting file permissions check

File: /boot/grub/grub.cfg [ OK ]

File: /etc/at.deny [ SUGGESTION ]

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/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) [ DIFFERENT ]

- 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) [ DIFFERENT ]

- 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) [ OK ]

- net.core.bpf\_jit\_harden (exp: 2) [ DIFFERENT ]

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

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

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

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

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

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

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

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

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

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

- 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) [ OK ]

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

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

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

[+] Hardening

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

- Installed compiler(s) [ FOUND ]

- Installed malware scanner [ FOUND ]

- Non-native binary formats [ FOUND ]

[+] Custom tests

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

- Running custom tests... [ NONE ]

[+] Plugins (phase 2)

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

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

-[ Lynis 3.0.8 Results ]-

Warnings (3):

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

! Reboot of system is most likely needed [KRNL-5830]

- Solution : reboot

https://cisofy.com/lynis/controls/KRNL-5830/

! Found one or more vulnerable packages. [PKGS-7392]

https://cisofy.com/lynis/controls/PKGS-7392/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]

https://cisofy.com/lynis/controls/MAIL-8818/

Suggestions (54):

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

\* 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/

\* 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/

\* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]

https://cisofy.com/lynis/controls/AUTH-9229/

\* 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/

\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

https://cisofy.com/lynis/controls/USB-1000/

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

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

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

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

\* Purge old/removed packages (4 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/

\* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]

https://cisofy.com/lynis/controls/PKGS-7392/

\* Install package apt-show-versions for patch management purposes [PKGS-7394]

https://cisofy.com/lynis/controls/PKGS-7394/

\* 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/

\* Access to CUPS configuration could be more strict. [PRNT-2307]

https://cisofy.com/lynis/controls/PRNT-2307/

\* You are advised to hide the mail\_name (option: smtpd\_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]

https://cisofy.com/lynis/controls/MAIL-8818/

\* Disable the 'VRFY' command [MAIL-8820:disable\_vrfy\_command]

- Details : disable\_vrfy\_command=no

- Solution : run postconf -e disable\_vrfy\_command=yes to change the value

https://cisofy.com/lynis/controls/MAIL-8820/

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

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

\* 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/

\* Consider hardening SSH configuration [SSH-7408]

- Details : AllowTcpForwarding (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : ClientAliveCountMax (set 3 to 2)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : Compression (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : LogLevel (set INFO to VERBOSE)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxAuthTries (set 6 to 3)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxSessions (set 10 to 2)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : Port (set 22 to )

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : TCPKeepAlive (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : X11Forwarding (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : AllowAgentForwarding (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

\* 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/

\* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]

https://cisofy.com/lynis/controls/INSE-8100/

\* 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 (no results) [ACCT-9626]

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

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

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

\* 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/

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 : 63 [############ ]

Tests performed : 267

Plugins enabled : 0

Components:

- Firewall [V]

- Malware scanner [V]

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 3.0.8

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

(Linux, macOS, BSD, and others)

2007-2021, 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)

You have new mail in /var/mail/root

root@image-ubuntu-adhoc-vm-student33:/etc#

### **Bonus**

1. Command to install chkrootkit:

|  |
| --- |
| apt install chkrootkit -y |

1. Command to view documentation and instructions:

|  |
| --- |
| sudo man chkrootkit |

1. Command to run expert mode:

|  |
| --- |
| chkrootkit -x |

1. Provide a report from the chrootkit output with recommendations for hardening the system.

It has issues copying so here is a screenshot. It did run!

