| Cybersecurity |
| --- |
| Module 4 Challenge Submission File |

## **Linux Systems Administration**

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

### **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:

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

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

| sudo chown root:root /etc/shadow  sudo chmod 600 /etc/shadow |
| --- |

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

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

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

| sudo chown root:root /etc/gshadow  sudo chmod 600 /etc/gshadow |
| --- |

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

| sudo ls -l /etc/group |
| --- |

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

| sudo chown root:root /etc/group  sudo chmod 644 /etc/group |
| --- |

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

| sudo ls -l /etc/passwd |
| --- |

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

| sudo chown root:root /etc/passwd  sudo chmod 644 /etc/passwd |
| --- |

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

1. Add user accounts for sam, joe, amy, sara, and admin1 with the useradd command.
   1. Command to add each user account (include all five users):

| sudo adduser sam  sudo adduser joe  sudo adduser amy  sudo adduser sara  sudo adduser admin1 |
| --- |

1. Ensure that only the admin1 has general sudo access.
   1. Command to add admin1 to the sudo group:

| sudo usermod -aG sudo admin1 |
| --- |

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

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

| sudo addgroup 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 -aG engineers sam  sudo usermod -aG engineers joe  sudo usermod -aG engineers amy  sudo usermod -aG engineers sara |
| --- |

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

| cd /home/engineers  …  sudo mkdir SharedFolder |
| --- |

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 chown root:engineers /home/engineers/SharedFolder/ |
| --- |

### Step 4: Lynis Auditing

1. Command to install Lynis:

| sudo apt install lynis or sudo apt -y install lynis |
| --- |

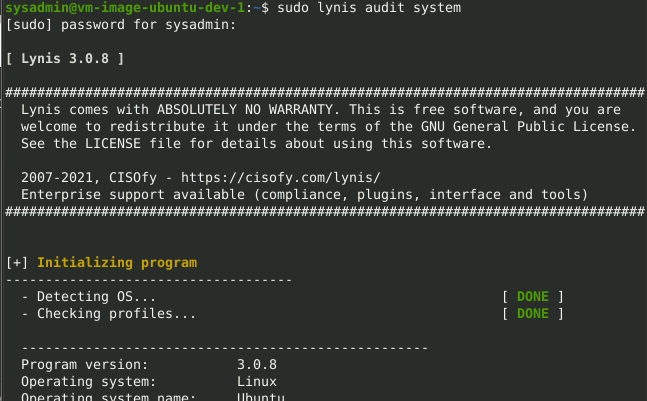
1. Command to view documentation and instructions:

| sudo lynis --help or sudo man lynis |
| --- |

1. Command to run an audit:

| sudo lynis audit system |
| --- |

1. Provide a report from the Lynis output with recommendations for hardening the system.
   1. Screenshot of report output: [**FILE HERE**](https://drive.google.com/file/d/1husDQyC_4HnWPIZvvpN5ON4AgHE1zmG-/view?usp=drive_link)



| Downloads/SystemAuditData.txt Details  Activity    [1;37m[ Lynis 3.0.8 ] [0m  ################################################################################  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)  ################################################################################  [+] [1;33mInitializing program [0m  ------------------------------------  [2C- Detecting OS... [41C [ [1;32mDONE [0m ]  [2C- Checking profiles... [37C [ [1;32mDONE [0m ]  ---------------------------------------------------  Program version: 3.0.8  Operating system: Linux  Operating system name: Ubuntu  Operating system version: 20.04  Kernel version: 5.15.0  Hardware platform: x86\_64  Hostname: vm-image-ubuntu-dev-1  ---------------------------------------------------  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  ---------------------------------------------------  [2C- Program update status... [32C [ [1;32mNO UPDATE [0m ]  [+] [1;33mSystem tools [0m  ------------------------------------  [2C- Scanning available tools... [30C  [2C- Checking system binaries... [30C  [+] [1;35mPlugins (phase 1) [0m  ------------------------------------  [0CNote: plugins have more extensive tests and may take several minutes to complete [0C  [0C [0C  [2C- Plugins enabled [42C [ [1;37mNONE [0m ]  [+] [1;33mBoot and services [0m  ------------------------------------  [2C- Service Manager [42C [ [1;32msystemd [0m ]  [2C- Checking UEFI boot [39C [ [1;32mENABLED [0m ]  [2C- Checking Secure Boot [37C [ [1;33mDISABLED [0m ]  [2C- Checking presence GRUB2 [34C [ [1;32mFOUND [0m ]  [4C- Checking for password protection [23C [ [1;31mNONE [0m ]  [2C- Check running services (systemctl) [23C [ [1;32mDONE [0m ]  [8CResult: found 48 running services [20C  [2C- Check enabled services at boot (systemctl) [15C [ [1;32mDONE [0m ]  [8CResult: found 106 enabled services [19C  [2C- Check startup files (permissions) [24C [ [1;32mOK [0m ]  [2C- Running 'systemd-analyze security' [23C  [8C- ModemManager.service: [30C [ [1;37mMEDIUM [0m ]  [8C- NetworkManager.service: [28C [ [1;33mEXPOSED [0m ]  [8C- accounts-daemon.service: [27C [ [1;31mUNSAFE [0m ]  [8C- acpid.service: [37C [ [1;31mUNSAFE [0m ]  [8C- alsa-state.service: [32C [ [1;31mUNSAFE [0m ]  [8C- anacron.service: [35C [ [1;31mUNSAFE [0m ]  [8C- apache2.service: [35C [ [1;31mUNSAFE [0m ]  [8C- apport.service: [36C [ [1;31mUNSAFE [0m ]  [8C- atd.service: [39C [ [1;31mUNSAFE [0m ]  [8C- avahi-daemon.service: [30C [ [1;31mUNSAFE [0m ]  [8C- blueman-mechanism.service: [25C [ [1;31mUNSAFE [0m ]  [8C- chrony.service: [36C [ [1;33mEXPOSED [0m ]  [8C- cloud-init-hotplugd.service: [23C [ [1;31mUNSAFE [0m ]  [8C- colord.service: [36C [ [1;33mEXPOSED [0m ]  [8C- containerd.service: [32C [ [1;31mUNSAFE [0m ]  [8C- cron.service: [38C [ [1;31mUNSAFE [0m ]  [8C- cups-browsed.service: [30C [ [1;31mUNSAFE [0m ]  [8C- cups.service: [38C [ [1;31mUNSAFE [0m ]  [8C- dbus.service: [38C [ [1;31mUNSAFE [0m ]  [8C- dm-event.service: [34C [ [1;31mUNSAFE [0m ]  [8C- dmesg.service: [37C [ [1;31mUNSAFE [0m ]  [8C- docker.service: [36C [ [1;31mUNSAFE [0m ]  [8C- emergency.service: [33C [ [1;31mUNSAFE [0m ]  [8C- gdm.service: [39C [ [1;31mUNSAFE [0m ]  [8C- getty@tty1.service: [32C [ [1;31mUNSAFE [0m ]  [8C- hddtemp.service: [35C [ [1;31mUNSAFE [0m ]  [8C- hv-fcopy-daemon.service: [27C [ [1;31mUNSAFE [0m ]  [8C- hv-kvp-daemon.service: [29C [ [1;31mUNSAFE [0m ]  [8C- hv-vss-daemon.service: [29C [ [1;31mUNSAFE [0m ]  [8C- irqbalance.service: [32C [ [1;37mMEDIUM [0m ]  [8C- iscsid.service: [36C [ [1;31mUNSAFE [0m ]  [8C- kerneloops.service: [32C [ [1;31mUNSAFE [0m ]  [8C- lvm2-lvmpolld.service: [29C [ [1;31mUNSAFE [0m ]  [8C- lxd-agent.service: [33C [ [1;31mUNSAFE [0m ]  [8C- multipathd.service: [32C [ [1;31mUNSAFE [0m ]  [8C- nessusd.service: [35C [ [1;31mUNSAFE [0m ]  [8C- networkd-dispatcher.service: [23C [ [1;31mUNSAFE [0m ]  [8C- nginx.service: [37C [ [1;31mUNSAFE [0m ]  [8C- nmbd.service: [38C [ [1;31mUNSAFE [0m ]  [8C- ondemand.service: [34C [ [1;31mUNSAFE [0m ]  [8C- open-vm-tools.service: [29C [ [1;31mUNSAFE [0m ]  [8C- plymouth-start.service: [28C [ [1;31mUNSAFE [0m ]  [8C- polkit.service: [36C [ [1;31mUNSAFE [0m ]  [8C- postfix@-.service: [33C [ [1;31mUNSAFE [0m ]  [8C- rc-local.service: [34C [ [1;31mUNSAFE [0m ]  [8C- rescue.service: [36C [ [1;31mUNSAFE [0m ]  [8C- resolvconf.service: [32C [ [1;31mUNSAFE [0m ]  [8C- rsync.service: [37C [ [1;31mUNSAFE [0m ]  [8C- rsyslog.service: [35C [ [1;31mUNSAFE [0m ]  [8C- rtkit-daemon.service: [30C [ [1;37mMEDIUM [0m ]  [8C- serial-getty@ttyS0.service: [24C [ [1;31mUNSAFE [0m ]  [8C- smbd.service: [38C [ [1;31mUNSAFE [0m ]  [8C- snap.lxd.daemon.service: [27C [ [1;31mUNSAFE [0m ]  [8C- snapd.aa-prompt-listener.service: [18C [ [1;31mUNSAFE [0m ]  [8C- snapd.service: [37C [ [1;31mUNSAFE [0m ]  [8C- ssh.service: [39C [ [1;31mUNSAFE [0m ]  [8C- switcheroo-control.service: [24C [ [1;33mEXPOSED [0m ]  [8C- systemd-ask-password-console.service: [14C [ [1;31mUNSAFE [0m ]  [8C- systemd-ask-password-plymouth.service: [13C [ [1;31mUNSAFE [0m ]  [8C- systemd-ask-password-wall.service: [17C [ [1;31mUNSAFE [0m ]  [8C- systemd-fsckd.service: [29C [ [1;31mUNSAFE [0m ]  [8C- systemd-initctl.service: [27C [ [1;31mUNSAFE [0m ]  [8C- systemd-journald.service: [26C [ [1;32mPROTECTED [0m ]  [8C- systemd-logind.service: [28C [ [1;32mPROTECTED [0m ]  [8C- systemd-networkd.service: [26C [ [1;32mPROTECTED [0m ]  [8C- systemd-resolved.service: [26C [ [1;32mPROTECTED [0m ]  [8C- systemd-rfkill.service: [28C [ [1;31mUNSAFE [0m ]  [8C- systemd-udevd.service: [29C [ [1;33mEXPOSED [0m ]  [8C- ubuntu-advantage.service: [26C [ [1;31mUNSAFE [0m ]  [8C- udisks2.service: [35C [ [1;31mUNSAFE [0m ]  [8C- unattended-upgrades.service: [23C [ [1;31mUNSAFE [0m ]  [8C- upower.service: [36C [ [1;32mPROTECTED [0m ]  [8C- user@1002.service: [33C [ [1;31mUNSAFE [0m ]  [8C- user@129.service: [34C [ [1;31mUNSAFE [0m ]  [8C- uuidd.service: [37C [ [1;32mPROTECTED [0m ]  [8C- vgauth.service: [36C [ [1;31mUNSAFE [0m ]  [8C- vncserver2@:1.service: [29C [ [1;31mUNSAFE [0m ]  [8C- vncserver@:1.service: [30C [ [1;31mUNSAFE [0m ]  [8C- walinuxagent.service: [30C [ [1;31mUNSAFE [0m ]  [8C- whoopsie.service: [34C [ [1;31mUNSAFE [0m ]  [8C- wpa\_supplicant.service: [28C [ [1;31mUNSAFE [0m ]  [8C- xrdp-sesman.service: [31C [ [1;31mUNSAFE [0m ]  [8C- xrdp.service: [38C [ [1;31mUNSAFE [0m ]  [+] [1;33mKernel [0m  ------------------------------------  [2C- Checking default run level [31C [ [1;32mRUNLEVEL 5 [0m ]  [2C- Checking CPU support (NX/PAE) [28C  [4CCPU support: PAE and/or NoeXecute supported [14C [ [1;32mFOUND [0m ]  [2C- Checking kernel version and release [22C [ [1;32mDONE [0m ]  [2C- Checking kernel type [37C [ [1;32mDONE [0m ]  [2C- Checking loaded kernel modules [27C [ [1;32mDONE [0m ]  [6CFound 92 active modules [32C  [2C- Checking Linux kernel configuration file [17C [ [1;32mFOUND [0m ]  [2C- Checking default I/O kernel scheduler [20C [ [1;37mNOT FOUND [0m ]  [2C- Checking for available kernel update [21C [ [1;32mOK [0m ]  [2C- Checking core dumps configuration [24C  [4C- configuration in systemd conf files [20C [ [1;37mDEFAULT [0m ]  [4C- configuration in /etc/profile [26C [ [1;37mDEFAULT [0m ]  [4C- 'hard' configuration in /etc/security/limits.conf [6C [ [1;37mDEFAULT [0m ]  [4C- 'soft' configuration in /etc/security/limits.conf [6C [ [1;37mDEFAULT [0m ]  [4C- Checking setuid core dumps configuration [15C [ [1;37mPROTECTED [0m ]  [2C- Check if reboot is needed [32C [ [1;31mYES [0m ]  [+] [1;33mMemory and Processes [0m  ------------------------------------  [2C- Checking /proc/meminfo [35C [ [1;32mFOUND [0m ]  [2C- Searching for dead/zombie processes [22C [ [1;32mNOT FOUND [0m ]  [2C- Searching for IO waiting processes [23C [ [1;32mNOT FOUND [0m ]  [2C- Search prelink tooling [35C [ [1;32mNOT FOUND [0m ]  [+] [1;33mUsers, Groups and Authentication [0m  ------------------------------------  [2C- Administrator accounts [35C [ [1;32mOK [0m ]  [2C- Unique UIDs [46C [ [1;32mOK [0m ]  [2C- Consistency of group files (grpck) [23C [ [1;32mOK [0m ]  [2C- Unique group IDs [41C [ [1;32mOK [0m ]  [2C- Unique group names [39C [ [1;32mOK [0m ]  [2C- Password file consistency [32C [ [1;33mSUGGESTION [0m ]  [2C- Password hashing methods [33C [ [1;33mSUGGESTION [0m ]  [2C- Checking password hashing rounds [25C [ [1;33mDISABLED [0m ]  [2C- Query system users (non daemons) [25C [ [1;32mDONE [0m ]  [2C- NIS+ authentication support [30C [ [1;37mNOT ENABLED [0m ]  [2C- NIS authentication support [31C [ [1;37mNOT ENABLED [0m ]  [2C- Sudoers file(s) [42C [ [1;32mFOUND [0m ]  [4C- Permissions for directory: /etc/sudoers.d [14C [ [1;32mOK [0m ]  [4C- Permissions for: /etc/sudoers [26C [ [1;32mOK [0m ]  [4C- Permissions for: /etc/sudoers.d/README [17C [ [1;32mOK [0m ]  [4C- Permissions for: /etc/sudoers.d/90-cloud-init-users [4C [ [1;32mOK [0m ]  [2C- PAM password strength tools [30C [ [1;33mSUGGESTION [0m ]  [2C- PAM configuration files (pam.conf) [23C [ [1;32mFOUND [0m ]  [2C- PAM configuration files (pam.d) [26C [ [1;32mFOUND [0m ]  [2C- PAM modules [46C [ [1;32mFOUND [0m ]  [2C- LDAP module in PAM [39C [ [1;37mNOT FOUND [0m ]  [2C- Accounts without expire date [29C [ [1;33mSUGGESTION [0m ]  [2C- Accounts without password [32C [ [1;32mOK [0m ]  [2C- Locked accounts [42C [ [1;31mFOUND [0m ]  [2C- Checking user password aging (minimum) [19C [ [1;33mDISABLED [0m ]  [2C- User password aging (maximum) [28C [ [1;33mDISABLED [0m ]  [2C- Checking expired passwords [31C [ [1;32mOK [0m ]  [2C- Checking Linux single user mode authentication [11C [ [1;32mOK [0m ]  [2C- Determining default umask [32C  [4C- umask (/etc/profile) [35C [ [1;33mNOT FOUND [0m ]  [4C- umask (/etc/login.defs) [32C [ [1;33mSUGGESTION [0m ]  [2C- LDAP authentication support [30C [ [1;37mNOT ENABLED [0m ]  [2C- Logging failed login attempts [28C [ [1;32mENABLED [0m ]  [+] [1;33mShells [0m  ------------------------------------  [2C- Checking shells from /etc/shells [25C  [4CResult: found 9 shells (valid shells: 9). [16C  [4C- Session timeout settings/tools [25C [ [1;33mNONE [0m ]  [2C- Checking default umask values [28C  [4C- Checking default umask in /etc/bash.bashrc [13C [ [1;33mNONE [0m ]  [4C- Checking default umask in /etc/profile [17C [ [1;33mNONE [0m ]  [+] [1;33mFile systems [0m  ------------------------------------  [2C- Checking mount points [36C  [4C- Checking /home mount point [29C [ [1;33mSUGGESTION [0m ]  [4C- Checking /tmp mount point [30C [ [1;33mSUGGESTION [0m ]  [4C- Checking /var mount point [30C [ [1;33mSUGGESTION [0m ]  [2C- Query swap partitions (fstab) [28C [ [1;33mNONE [0m ]  [2C- Testing swap partitions [34C [ [1;32mOK [0m ]  [2C- Testing /proc mount (hidepid) [28C [ [1;33mSUGGESTION [0m ]  [2C- Checking for old files in /tmp [27C [ [1;32mOK [0m ]  [2C- Checking /tmp sticky bit [33C [ [1;32mOK [0m ]  [2C- Checking /var/tmp sticky bit [29C [ [1;32mOK [0m ]  [2C- ACL support root file system [29C [ [1;32mENABLED [0m ]  [2C- Mount options of / [39C [ [1;33mNON DEFAULT [0m ]  [2C- Mount options of /dev [36C [ [1;33mNON DEFAULT [0m ]  [2C- Mount options of /dev/shm [32C [ [1;33mPARTIALLY HARDENED [0m ]  [2C- Mount options of /run [36C [ [1;32mHARDENED [0m ]  [2C- Total without nodev:8 noexec:28 nosuid:19 ro or noexec (W^X): 16 of total 58 [0C  [2C- Checking Locate database [33C [ [1;32mFOUND [0m ]  [2C- Disable kernel support of some filesystems [15C  [+] [1;33mUSB Devices [0m  ------------------------------------  [2C- Checking usb-storage driver (modprobe config) [12C [ [1;37mNOT DISABLED [0m ]  [2C- Checking USB devices authorization [23C [ [1;32mDISABLED [0m ]  [2C- Checking USBGuard [40C [ [1;37mNOT FOUND [0m ]  [+] [1;33mStorage [0m  ------------------------------------  [2C- Checking firewire ohci driver (modprobe config) [10C [ [1;32mDISABLED [0m ]  [+] [1;33mNFS [0m  ------------------------------------  [2C- Check running NFS daemon [33C [ [1;37mNOT FOUND [0m ]  [+] [1;33mName services [0m  ------------------------------------  [2C- Checking search domains [34C [ [1;32mFOUND [0m ]  [2C- Searching DNS domain name [32C [ [1;33mUNKNOWN [0m ]  [2C- Checking /etc/hosts [38C  [4C- Duplicate entries in hosts file [24C [ [1;32mNONE [0m ]  [4C- Presence of configured hostname in /etc/hosts [10C [ [1;32mFOUND [0m ]  [4C- Hostname mapped to localhost [27C [ [1;32mNOT FOUND [0m ]  [4C- Localhost mapping to IP address [24C [ [1;32mOK [0m ]  [+] [1;33mPorts and packages [0m  ------------------------------------  [2C- Searching package managers [31C  [4C- Searching dpkg package manager [25C [ [1;32mFOUND [0m ]  [6C- Querying package manager [29C  [4C- Query unpurged packages [32C [ [1;33mFOUND [0m ]  [2C- Checking security repository in sources.list file [8C [ [1;32mOK [0m ]  [2C- Checking APT package database [28C [ [1;32mOK [0m ]  [2C- Checking vulnerable packages [29C [ [1;31mWARNING [0m ]  [30;43m[WARNING] [0m: Test PKGS-7392 had a long execution: 14.280291 seconds [0m  [2C- Checking upgradeable packages [28C [ [1;37mSKIPPED [0m ]  [2C- Checking package audit tool [30C [ [1;32mINSTALLED [0m ]  [4CFound: apt-get [43C  [2C- Toolkit for automatic upgrades (unattended-upgrade) [6C [ [1;32mFOUND [0m ]  [+] [1;33mNetworking [0m  ------------------------------------  [2C- Checking IPv6 configuration [30C [ [1;37mENABLED [0m ]  [6CConfiguration method [35C [ [1;37mAUTO [0m ]  [6CIPv6 only [46C [ [1;37mNO [0m ]  [2C- Checking configured nameservers [26C  [4C- Testing nameservers [36C  [8CNameserver: 8.8.8.8 [34C [ [1;32mOK [0m ]  [8CNameserver: 127.0.0.53 [31C [ [1;32mOK [0m ]  [4C- DNSSEC supported (systemd-resolved) [20C [ [1;33mNO [0m ]  [2C- Checking default gateway [33C [ [1;32mDONE [0m ]  [2C- Getting listening ports (TCP/UDP) [24C [ [1;32mDONE [0m ]  [2C- Checking promiscuous interfaces [26C [ [1;32mOK [0m ]  [2C- Checking waiting connections [29C [ [1;32mOK [0m ]  [2C- Checking status DHCP client [30C  [2C- Checking for ARP monitoring software [21C [ [1;33mNOT FOUND [0m ]  [2C- Uncommon network protocols [31C [ [1;33m0 [0m ]  [+] [1;33mPrinters and Spools [0m  ------------------------------------  [2C- Checking cups daemon [37C [ [1;32mRUNNING [0m ]  [2C- Checking CUPS configuration file [25C [ [1;32mOK [0m ]  [4C- File permissions [39C [ [1;31mWARNING [0m ]  [2C- Checking CUPS addresses/sockets [26C [ [1;32mFOUND [0m ]  [2C- Checking lp daemon [39C [ [1;37mNOT RUNNING [0m ]  [+] [1;33mSoftware: e-mail and messaging [0m  ------------------------------------  [2C- Postfix status [43C [ [1;32mRUNNING [0m ]  [4C- Postfix configuration [34C [ [1;32mFOUND [0m ]  [6C- Postfix banner [39C [ [1;31mWARNING [0m ]  [+] [1;33mSoftware: firewalls [0m  ------------------------------------  [2C- Checking iptables kernel module [26C [ [1;32mFOUND [0m ]  [4C- Checking iptables policies of chains [19C [ [1;32mFOUND [0m ]  [4C- Checking for empty ruleset [29C [ [1;32mOK [0m ]  [4C- Checking for unused rules [30C [ [1;33mFOUND [0m ]  [2C- Checking host based firewall [29C [ [1;32mACTIVE [0m ]  [+] [1;33mSoftware: webserver [0m  ------------------------------------  [2C- Checking Apache (binary /usr/sbin/apache2) [15C [ [1;32mFOUND [0m ]  [6CInfo: Configuration file found (/etc/apache2/apache2.conf) [0C  [6CInfo: No virtual hosts found [27C  [4C\* Loadable modules [39C [ [1;32mFOUND (118) [0m ]  [8C- Found 118 loadable modules [25C  [10Cmod\_evasive: anti-DoS/brute force [18C [ [1;37mNOT FOUND [0m ]  [10Cmod\_reqtimeout/mod\_qos [29C [ [1;32mFOUND [0m ]  [10CModSecurity: web application firewall [14C [ [1;37mNOT FOUND [0m ]  [2C- Checking nginx [43C [ [1;37mNOT FOUND [0m ]  [+] [1;33mSSH Support [0m  ------------------------------------  [2C- Checking running SSH daemon [30C [ [1;32mFOUND [0m ]  [4C- Searching SSH configuration [28C [ [1;32mFOUND [0m ]  [4C- OpenSSH option: AllowTcpForwarding [21C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: ClientAliveCountMax [20C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: ClientAliveInterval [20C [ [1;32mOK [0m ]  [4C- OpenSSH option: Compression [28C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: FingerprintHash [24C [ [1;32mOK [0m ]  [4C- OpenSSH option: GatewayPorts [27C [ [1;32mOK [0m ]  [4C- OpenSSH option: IgnoreRhosts [27C [ [1;32mOK [0m ]  [4C- OpenSSH option: LoginGraceTime [25C [ [1;32mOK [0m ]  [4C- OpenSSH option: LogLevel [31C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: MaxAuthTries [27C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: MaxSessions [28C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: PermitRootLogin [24C [ [1;32mOK [0m ]  [4C- OpenSSH option: PermitUserEnvironment [18C [ [1;32mOK [0m ]  [4C- OpenSSH option: PermitTunnel [27C [ [1;32mOK [0m ]  [4C- OpenSSH option: Port [35C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: PrintLastLog [27C [ [1;32mOK [0m ]  [4C- OpenSSH option: StrictModes [28C [ [1;32mOK [0m ]  [4C- OpenSSH option: TCPKeepAlive [27C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: UseDNS [33C [ [1;32mOK [0m ]  [4C- OpenSSH option: X11Forwarding [26C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: AllowAgentForwarding [19C [ [1;33mSUGGESTION [0m ]  [4C- OpenSSH option: AllowUsers [29C [ [1;37mNOT FOUND [0m ]  [4C- OpenSSH option: AllowGroups [28C [ [1;37mNOT FOUND [0m ]  [+] [1;33mSNMP Support [0m  ------------------------------------  [2C- Checking running SNMP daemon [29C [ [1;37mNOT FOUND [0m ]  [+] [1;33mDatabases [0m  ------------------------------------  [4CNo database engines found [32C  [+] [1;33mLDAP Services [0m  ------------------------------------  [2C- Checking OpenLDAP instance [31C [ [1;37mNOT FOUND [0m ]  [+] [1;33mPHP [0m  ------------------------------------  [2C- Checking PHP [45C [ [1;37mNOT FOUND [0m ]  [+] [1;33mSquid Support [0m  ------------------------------------  [2C- Checking running Squid daemon [28C [ [1;37mNOT FOUND [0m ]  [+] [1;33mLogging and files [0m  ------------------------------------  [2C- Checking for a running log daemon [24C [ [1;32mOK [0m ]  [4C- Checking Syslog-NG status [30C [ [1;37mNOT FOUND [0m ]  [4C- Checking systemd journal status [24C [ [1;32mFOUND [0m ]  [4C- Checking Metalog status [32C [ [1;37mNOT FOUND [0m ]  [4C- Checking RSyslog status [32C [ [1;32mFOUND [0m ]  [4C- Checking RFC 3195 daemon status [24C [ [1;37mNOT FOUND [0m ]  [4C- Checking minilogd instances [28C [ [1;37mNOT FOUND [0m ]  [2C- Checking logrotate presence [30C [ [1;32mOK [0m ]  [2C- Checking remote logging [34C [ [1;33mNOT ENABLED [0m ]  [2C- Checking log directories (static list) [19C [ [1;32mDONE [0m ]  [2C- Checking open log files [34C [ [1;32mDONE [0m ]  [2C- Checking deleted files in use [28C [ [1;33mFILES FOUND [0m ]  [+] [1;33mInsecure services [0m  ------------------------------------  [2C- Installed inetd package [34C [ [1;32mNOT FOUND [0m ]  [2C- Installed xinetd package [33C [ [1;33mFOUND [0m ]  [4C- xinetd status [42C  [6C- Enabled xinetd.d services [28C [ [1;32mNOT FOUND [0m ]  [2C- Installed rsh client package [29C [ [1;32mOK [0m ]  [2C- Installed rsh server package [29C [ [1;32mOK [0m ]  [2C- Installed telnet client package [26C [ [1;32mOK [0m ]  [2C- Installed telnet server package [26C [ [1;32mNOT FOUND [0m ]  [2C- Checking NIS client installation [25C [ [1;32mOK [0m ]  [2C- Checking NIS server installation [25C [ [1;32mOK [0m ]  [2C- Checking TFTP client installation [24C [ [1;32mOK [0m ]  [2C- Checking TFTP server installation [24C [ [1;32mOK [0m ]  [+] [1;33mBanners and identification [0m  ------------------------------------  [2C- /etc/issue [47C [ [1;32mFOUND [0m ]  [4C- /etc/issue contents [36C [ [1;33mWEAK [0m ]  [2C- /etc/issue.net [43C [ [1;32mFOUND [0m ]  [4C- /etc/issue.net contents [32C [ [1;33mWEAK [0m ]  [+] [1;33mScheduled tasks [0m  ------------------------------------  [2C- Checking crontab and cronjob files [23C [ [1;32mDONE [0m ]  [2C- Checking atd status [38C [ [1;32mRUNNING [0m ]  [4C- Checking at users [38C [ [1;32mDONE [0m ]  [4C- Checking at jobs [39C [ [1;32mNONE [0m ]  [+] [1;33mAccounting [0m  ------------------------------------  [2C- Checking accounting information [26C [ [1;33mNOT FOUND [0m ]  [2C- Checking sysstat accounting data [25C [ [1;33mNOT FOUND [0m ]  [2C- Checking auditd [42C [ [1;37mNOT FOUND [0m ]  [+] [1;33mTime and Synchronization [0m  ------------------------------------  [2C- NTP daemon found: chronyd [32C [ [1;32mFOUND [0m ]  [2C- Checking for a running NTP daemon or client [14C [ [1;32mOK [0m ]  [+] [1;33mCryptography [0m  ------------------------------------  [2C- Checking for expired SSL certificates [0/142] [12C [ [1;32mNONE [0m ]  [30;43m[WARNING] [0m: Test CRYP-7902 had a long execution: 28.460405 seconds [0m  [2C- Found 0 encrypted and 0 unencrypted swap devices in use. [1C [ [1;37mOK [0m ]  [2C- Kernel entropy is sufficient [29C [ [1;32mYES [0m ]  [2C- HW RNG & rngd [44C [ [1;33mNO [0m ]  [2C- SW prng [50C [ [1;33mNO [0m ]  [2C- MOR variable not found [35C [ [1;37mWEAK [0m ]  [+] [1;33mVirtualization [0m  ------------------------------------  [+] [1;33mContainers [0m  ------------------------------------  [4C- Docker [49C  [6C- Docker daemon [40C [ [1;32mRUNNING [0m ]  [8C- Docker info output (warnings) [22C [ [1;32mNONE [0m ]  [6C- Containers [43C  [8C- Total containers [35C [ [1;37m0 [0m ]  [4C- File permissions [39C [ [1;32mOK [0m ]  [+] [1;33mSecurity frameworks [0m  ------------------------------------  [2C- Checking presence AppArmor [31C [ [1;32mFOUND [0m ]  [4C- Checking AppArmor status [31C [ [1;32mENABLED [0m ]  [8CFound 2598 unconfined processes [22C  [2C- Checking presence SELinux [32C [ [1;37mNOT FOUND [0m ]  [2C- Checking presence TOMOYO Linux [27C [ [1;37mNOT FOUND [0m ]  [2C- Checking presence grsecurity [29C [ [1;37mNOT FOUND [0m ]  [2C- Checking for implemented MAC framework [19C [ [1;32mOK [0m ]  [+] [1;33mSoftware: file integrity [0m  ------------------------------------  [2C- Checking file integrity tools [28C  [4C- Tripwire [47C [ [1;32mFOUND [0m ]  [2C- dm-integrity (status) [36C [ [1;37mDISABLED [0m ]  [2C- dm-verity (status) [39C [ [1;37mDISABLED [0m ]  [2C- Checking presence integrity tool [25C [ [1;32mFOUND [0m ]  [+] [1;33mSoftware: System tooling [0m  ------------------------------------  [2C- Checking automation tooling [30C  [2C- Automation tooling [39C [ [1;33mNOT FOUND [0m ]  [2C- Checking for IDS/IPS tooling [29C [ [1;33mNONE [0m ]  [+] [1;33mSoftware: Malware [0m  ------------------------------------  [2C- Checking chkrootkit [38C [ [1;32mFOUND [0m ]  [2C- Malware software components [30C [ [1;32mFOUND [0m ]  [4C- Active agent [43C [ [1;37mNOT FOUND [0m ]  [4C- Rootkit scanner [40C [ [1;32mFOUND [0m ]  [+] [1;33mFile Permissions [0m  ------------------------------------  [2C- Starting file permissions check [26C  [4CFile: /boot/grub/grub.cfg [32C [ [1;32mOK [0m ]  [4CFile: /etc/at.deny [39C [ [1;33mSUGGESTION [0m ]  [4CFile: /etc/crontab [39C [ [1;33mSUGGESTION [0m ]  [4CFile: /etc/group [41C [ [1;32mOK [0m ]  [4CFile: /etc/group- [40C [ [1;32mOK [0m ]  [4CFile: /etc/hosts.allow [35C [ [1;32mOK [0m ]  [4CFile: /etc/hosts.deny [36C [ [1;32mOK [0m ]  [4CFile: /etc/issue [41C [ [1;32mOK [0m ]  [4CFile: /etc/issue.net [37C [ [1;32mOK [0m ]  [4CFile: /etc/passwd [40C [ [1;32mOK [0m ]  [4CFile: /etc/passwd- [39C [ [1;32mOK [0m ]  [4CFile: /etc/ssh/sshd\_config [31C [ [1;33mSUGGESTION [0m ]  [4CDirectory: /root/.ssh [36C [ [1;32mOK [0m ]  [4CDirectory: /etc/cron.d [35C [ [1;33mSUGGESTION [0m ]  [4CDirectory: /etc/cron.daily [31C [ [1;33mSUGGESTION [0m ]  [4CDirectory: /etc/cron.hourly [30C [ [1;33mSUGGESTION [0m ]  [4CDirectory: /etc/cron.weekly [30C [ [1;33mSUGGESTION [0m ]  [4CDirectory: /etc/cron.monthly [29C [ [1;33mSUGGESTION [0m ]  [+] [1;33mHome directories [0m  ------------------------------------  [2C- Permissions of home directories [26C [ [1;31mWARNING [0m ]  [2C- Ownership of home directories [28C [ [1;32mOK [0m ]  [2C- Checking shell history files [29C [ [1;32mOK [0m ]  [+] [1;33mKernel Hardening [0m  ------------------------------------  [2C- Comparing sysctl key pairs with scan profile [13C  [4C- dev.tty.ldisc\_autoload (exp: 0) [24C [ [1;31mDIFFERENT [0m ]  [4C- fs.protected\_fifos (exp: 2) [28C [ [1;31mDIFFERENT [0m ]  [4C- fs.protected\_hardlinks (exp: 1) [24C [ [1;32mOK [0m ]  [4C- fs.protected\_regular (exp: 2) [26C [ [1;32mOK [0m ]  [4C- fs.protected\_symlinks (exp: 1) [25C [ [1;32mOK [0m ]  [4C- fs.suid\_dumpable (exp: 0) [30C [ [1;31mDIFFERENT [0m ]  [4C- kernel.core\_uses\_pid (exp: 1) [26C [ [1;31mDIFFERENT [0m ]  [4C- kernel.ctrl-alt-del (exp: 0) [27C [ [1;32mOK [0m ]  [4C- kernel.dmesg\_restrict (exp: 1) [25C [ [1;32mOK [0m ]  [4C- kernel.kptr\_restrict (exp: 2) [26C [ [1;31mDIFFERENT [0m ]  [4C- kernel.modules\_disabled (exp: 1) [23C [ [1;31mDIFFERENT [0m ]  [4C- kernel.perf\_event\_paranoid (exp: 3) [20C [ [1;31mDIFFERENT [0m ]  [4C- kernel.randomize\_va\_space (exp: 2) [21C [ [1;32mOK [0m ]  [4C- kernel.sysrq (exp: 0) [34C [ [1;31mDIFFERENT [0m ]  [4C- kernel.unprivileged\_bpf\_disabled (exp: 1) [14C [ [1;31mDIFFERENT [0m ]  [4C- kernel.yama.ptrace\_scope (exp: 1 2 3) [18C [ [1;32mOK [0m ]  [4C- net.core.bpf\_jit\_harden (exp: 2) [23C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.all.accept\_redirects (exp: 0) [12C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.all.accept\_source\_route (exp: 0) [9C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.all.bootp\_relay (exp: 0) [17C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.all.forwarding (exp: 0) [18C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.all.log\_martians (exp: 1) [16C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.all.mc\_forwarding (exp: 0) [15C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.all.proxy\_arp (exp: 0) [19C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.all.rp\_filter (exp: 1) [19C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.all.send\_redirects (exp: 0) [14C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.default.accept\_redirects (exp: 0) [8C [ [1;32mOK [0m ]  [4C- net.ipv4.conf.default.accept\_source\_route (exp: 0) [5C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.conf.default.log\_martians (exp: 1) [12C [ [1;31mDIFFERENT [0m ]  [4C- net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) [10C [ [1;32mOK [0m ]  [4C- net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1) [4C [ [1;32mOK [0m ]  [4C- net.ipv4.tcp\_syncookies (exp: 1) [23C [ [1;32mOK [0m ]  [4C- net.ipv4.tcp\_timestamps (exp: 0 1) [21C [ [1;32mOK [0m ]  [4C- net.ipv6.conf.all.accept\_redirects (exp: 0) [12C [ [1;32mOK [0m ]  [4C- net.ipv6.conf.all.accept\_source\_route (exp: 0) [9C [ [1;32mOK [0m ]  [4C- net.ipv6.conf.default.accept\_redirects (exp: 0) [8C [ [1;32mOK [0m ]  [4C- net.ipv6.conf.default.accept\_source\_route (exp: 0) [5C [ [1;32mOK [0m ]  [+] [1;33mHardening [0m  ------------------------------------  [4C- Installed compiler(s) [34C [ [1;31mFOUND [0m ]  [4C- Installed malware scanner [30C [ [1;32mFOUND [0m ]  [4C- Non-native binary formats [30C [ [1;31mFOUND [0m ]  [+] [1;33mCustom tests [0m  ------------------------------------  [2C- Running custom tests... [33C [ [1;37mNONE [0m ]  [+] [1;35mPlugins (phase 2) [0m  ------------------------------------  ================================================================================  -[ [1;37mLynis 3.0.8 Results [0m ]-  [1;31mWarnings [0m (3):  [1;37m---------------------------- [0m  [1;31m! [0m Reboot of system is most likely needed [KRNL-5830]  - Solution : reboot  https://cisofy.com/lynis/controls/KRNL-5830/  [1;31m! [0m Found one or more vulnerable packages. [PKGS-7392]  https://cisofy.com/lynis/controls/PKGS-7392/  [1;31m! [0m Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]  https://cisofy.com/lynis/controls/MAIL-8818/  [1;33mSuggestions [0m (55):  [1;37m---------------------------- [0m  [1;33m\* [0m This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]  [0;37mhttps://cisofy.com/lynis/controls/LYNIS/ [0m  [1;33m\* [0m Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]  [0;37mhttps://cisofy.com/lynis/controls/BOOT-5122/ [0m  [1;33m\* [0m Consider hardening system services [BOOT-5264]  - Details : [0;36mRun '/usr/bin/systemd-analyze security SERVICE' for each service [0m  [0;37mhttps://cisofy.com/lynis/controls/BOOT-5264/ [0m  [1;33m\* [0m If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]  [0;37mhttps://cisofy.com/lynis/controls/KRNL-5820/ [0m  [1;33m\* [0m Run pwck manually and correct any errors in the password file [AUTH-9228]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9228/ [0m  [1;33m\* [0m Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9229/ [0m  [1;33m\* [0m Configure password hashing rounds in /etc/login.defs [AUTH-9230]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9230/ [0m  [1;33m\* [0m Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9262/ [0m  [1;33m\* [0m When possible set expire dates for all password protected accounts [AUTH-9282]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9282/ [0m  [1;33m\* [0m Look at the locked accounts and consider removing them [AUTH-9284]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9284/ [0m  [1;33m\* [0m Configure minimum password age in /etc/login.defs [AUTH-9286]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/ [0m  [1;33m\* [0m Configure maximum password age in /etc/login.defs [AUTH-9286]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/ [0m  [1;33m\* [0m Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  [0;37mhttps://cisofy.com/lynis/controls/AUTH-9328/ [0m  [1;33m\* [0m To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]  [0;37mhttps://cisofy.com/lynis/controls/FILE-6310/ [0m  [1;33m\* [0m To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]  [0;37mhttps://cisofy.com/lynis/controls/FILE-6310/ [0m  [1;33m\* [0m To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]  [0;37mhttps://cisofy.com/lynis/controls/FILE-6310/ [0m  [1;33m\* [0m Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]  [0;37mhttps://cisofy.com/lynis/controls/USB-1000/ [0m  [1;33m\* [0m Check DNS configuration for the dns domain name [NAME-4028]  [0;37mhttps://cisofy.com/lynis/controls/NAME-4028/ [0m  [1;33m\* [0m Purge old/removed packages (6 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]  [0;37mhttps://cisofy.com/lynis/controls/PKGS-7346/ [0m  [1;33m\* [0m Install debsums utility for the verification of packages with known good database. [PKGS-7370]  [0;37mhttps://cisofy.com/lynis/controls/PKGS-7370/ [0m  [1;33m\* [0m Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]  [0;37mhttps://cisofy.com/lynis/controls/PKGS-7392/ [0m  [1;33m\* [0m Install package apt-show-versions for patch management purposes [PKGS-7394]  [0;37mhttps://cisofy.com/lynis/controls/PKGS-7394/ [0m  [1;33m\* [0m Determine if protocol 'dccp' is really needed on this system [NETW-3200]  [0;37mhttps://cisofy.com/lynis/controls/NETW-3200/ [0m  [1;33m\* [0m Determine if protocol 'sctp' is really needed on this system [NETW-3200]  [0;37mhttps://cisofy.com/lynis/controls/NETW-3200/ [0m  [1;33m\* [0m Determine if protocol 'rds' is really needed on this system [NETW-3200]  [0;37mhttps://cisofy.com/lynis/controls/NETW-3200/ [0m  [1;33m\* [0m Determine if protocol 'tipc' is really needed on this system [NETW-3200]  [0;37mhttps://cisofy.com/lynis/controls/NETW-3200/ [0m  [1;33m\* [0m Access to CUPS configuration could be more strict. [PRNT-2307]  [0;37mhttps://cisofy.com/lynis/controls/PRNT-2307/ [0m  [1;33m\* [0m 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]  [0;37mhttps://cisofy.com/lynis/controls/MAIL-8818/ [0m  [1;33m\* [0m Disable the 'VRFY' command [MAIL-8820:disable\_vrfy\_command]  - Details : [0;36mdisable\_vrfy\_command=no [0m  - Solution : run postconf -e disable\_vrfy\_command=yes to change the value  [0;37mhttps://cisofy.com/lynis/controls/MAIL-8820/ [0m  [1;33m\* [0m Check iptables rules to see which rules are currently not used [FIRE-4513]  [0;37mhttps://cisofy.com/lynis/controls/FIRE-4513/ [0m  [1;33m\* [0m Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]  [0;37mhttps://cisofy.com/lynis/controls/HTTP-6640/ [0m  [1;33m\* [0m Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]  [0;37mhttps://cisofy.com/lynis/controls/HTTP-6643/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mAllowTcpForwarding (set YES to NO) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mClientAliveCountMax (set 3 to 2) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mCompression (set YES to NO) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mLogLevel (set INFO to VERBOSE) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mMaxAuthTries (set 6 to 3) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mMaxSessions (set 10 to 2) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mPort (set 22 to ) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mTCPKeepAlive (set YES to NO) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mX11Forwarding (set YES to NO) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Consider hardening SSH configuration [SSH-7408]  - Details : [0;36mAllowAgentForwarding (set YES to NO) [0m  [0;37mhttps://cisofy.com/lynis/controls/SSH-7408/ [0m  [1;33m\* [0m Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]  [0;37mhttps://cisofy.com/lynis/controls/LOGG-2154/ [0m  [1;33m\* [0m Check what deleted files are still in use and why. [LOGG-2190]  [0;37mhttps://cisofy.com/lynis/controls/LOGG-2190/ [0m  [1;33m\* [0m If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]  [0;37mhttps://cisofy.com/lynis/controls/INSE-8100/ [0m  [1;33m\* [0m Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]  [0;37mhttps://cisofy.com/lynis/controls/BANN-7126/ [0m  [1;33m\* [0m Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]  [0;37mhttps://cisofy.com/lynis/controls/BANN-7130/ [0m  [1;33m\* [0m Enable process accounting [ACCT-9622]  [0;37mhttps://cisofy.com/lynis/controls/ACCT-9622/ [0m  [1;33m\* [0m Enable sysstat to collect accounting (no results) [ACCT-9626]  [0;37mhttps://cisofy.com/lynis/controls/ACCT-9626/ [0m  [1;33m\* [0m Enable auditd to collect audit information [ACCT-9628]  [0;37mhttps://cisofy.com/lynis/controls/ACCT-9628/ [0m  [1;33m\* [0m Determine if automation tools are present for system management [TOOL-5002]  [0;37mhttps://cisofy.com/lynis/controls/TOOL-5002/ [0m  [1;33m\* [0m Consider restricting file permissions [FILE-7524]  - Details : [0;36mSee screen output or log file [0m  - Solution : Use chmod to change file permissions  [0;37mhttps://cisofy.com/lynis/controls/FILE-7524/ [0m  [1;33m\* [0m Double check the permissions of home directories as some might be not strict enough. [HOME-9304]  [0;37mhttps://cisofy.com/lynis/controls/HOME-9304/ [0m  [1;33m\* [0m 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>)  [0;37mhttps://cisofy.com/lynis/controls/KRNL-6000/ [0m  [1;33m\* [0m Harden compilers like restricting access to root user only [HRDN-7222]  [0;37mhttps://cisofy.com/lynis/controls/HRDN-7222/ [0m  [0;36mFollow-up [0m:  [1;37m---------------------------- [0m  [1;37m- [0m Show details of a test (lynis show details TEST-ID)  [1;37m- [0m Check the logfile for all details (less /var/log/lynis.log)  [1;37m- [0m Read security controls texts (https://cisofy.com)  [1;37m- [0m Use --upload to upload data to central system (Lynis Enterprise users)  ================================================================================  [1;37mLynis security scan details [0m:  [0;36mHardening index [0m : [1;37m67 [0m [ [1;33m############# [0m ]  [0;36mTests performed [0m : [1;37m267 [0m  [0;36mPlugins enabled [0m : [1;37m0 [0m  [1;37mComponents [0m:  - Firewall [ [1;32mV [0m]  - Malware scanner [ [1;32mV [0m]  [1;33mScan mode [0m:  Normal [V] Forensics [ ] Integration [ ] Pentest [ ]  [1;33mLynis modules [0m:  - Compliance status [ [1;33m? [0m]  - Security audit [ [1;32mV [0m]  - Vulnerability scan [ [1;32mV [0m]  [1;33mFiles [0m:  - Test and debug information : [1;37m/var/log/lynis.log [0m  - Report data : [1;37m/var/log/lynis-report.dat [0m  ================================================================================  [1;37mLynis [0m 3.0.8  Auditing, system hardening, and compliance for UNIX-based systems  (Linux, macOS, BSD, and others)  2007-2021, CISOfy - https://cisofy.com/lynis/  [1;37mEnterprise support available (compliance, plugins, interface and tools) [0m  ================================================================================  [0;44m[TIP] [0m: [0;94mEnhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings) [0m |
| --- |

### 

### Optional Additional Challengev

1. Command to install chkrootkit:

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

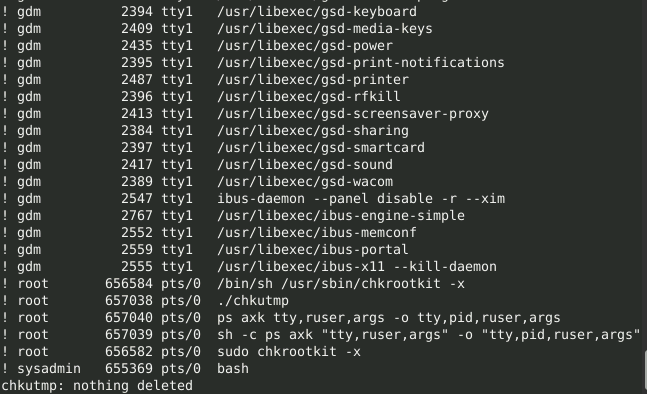
1. Command to view documentation and instructions:

| sudo chkrootkit --help or sudo man chrootkit |
| --- |

1. Command to run expert mode:

| sudo chkrootkit -x |
| --- |

1. Provide a report from the chrootkit output with recommendations for hardening the system.
   1. Screenshot of end of sample output: [**FILE HERE**](https://drive.google.com/file/d/1_knb3K9BWL8u1nJ-74L1qAOrWLeCzJcX/view?usp=drive_link)sudo chkrootkit -e system



| sudo chkrootkit -x |
| --- |
| Tail -250 Downloads/chkrootkit\_report.txt  —---------------------------------------------------------  EXE 656546: /opt/google/chrome/chrome  CWD 656547: /proc/640667/fdinfo  EXE 656547: /opt/google/chrome/chrome  CWD 656548: /proc/640667/fdinfo  EXE 656548: /opt/google/chrome/chrome  CWD 656549: /proc/640667/fdinfo  EXE 656549: /opt/google/chrome/chrome  CWD 656550: /proc/640667/fdinfo  EXE 656550: /opt/google/chrome/chrome  CWD 656551: /proc/640667/fdinfo  EXE 656551: /opt/google/chrome/chrome  CWD 656553: /proc/640667/fdinfo  EXE 656553: /opt/google/chrome/chrome  CWD 656554: /proc/640667/fdinfo  EXE 656554: /opt/google/chrome/chrome  CWD 656555: /proc/640667/fdinfo  EXE 656555: /opt/google/chrome/chrome  CWD 656556: /proc/640667/fdinfo  EXE 656556: /opt/google/chrome/chrome  CWD 656557: /proc/640667/fdinfo  EXE 656557: /opt/google/chrome/chrome  CWD 656558: /proc/640667/fdinfo  EXE 656558: /opt/google/chrome/chrome  CWD 656559: /proc/640667/fdinfo  EXE 656559: /opt/google/chrome/chrome  CWD 656560: /proc/640667/fdinfo  EXE 656560: /opt/google/chrome/chrome  CWD 656561: /proc/640667/fdinfo  EXE 656561: /opt/google/chrome/chrome  CWD 656562: /proc/640667/fdinfo  EXE 656562: /opt/google/chrome/chrome  CWD 656563: /proc/640667/fdinfo  EXE 656563: /opt/google/chrome/chrome  CWD 656564: /proc/640667/fdinfo  EXE 656564: /opt/google/chrome/chrome  CWD 656565: /proc/640667/fdinfo  EXE 656565: /opt/google/chrome/chrome  CWD 656566: /proc/640667/fdinfo  EXE 656566: /opt/google/chrome/chrome  CWD 656568: /proc/640667/fdinfo  EXE 656568: /opt/google/chrome/chrome  CWD 656571: /proc/640667/fdinfo  EXE 656571: /opt/google/chrome/chrome  CWD 656572: /proc/640667/fdinfo  EXE 656572: /opt/google/chrome/chrome  CWD 656573: /proc/640667/fdinfo  EXE 656573: /opt/google/chrome/chrome  CWD 656574: /proc/640667/fdinfo  EXE 656574: /opt/google/chrome/chrome  CWD 656575: /proc/640667/fdinfo  EXE 656575: /opt/google/chrome/chrome  CWD 656576: /proc/640667/fdinfo  EXE 656576: /opt/google/chrome/chrome  CWD 656577: /proc/640667/fdinfo  EXE 656577: /opt/google/chrome/chrome  CWD 656578: /proc/640667/fdinfo  EXE 656578: /opt/google/chrome/chrome  CWD 656579: /proc/640667/fdinfo  EXE 656579: /opt/google/chrome/chrome  CWD 656580: /proc/640667/fdinfo  EXE 656580: /opt/google/chrome/chrome  CWD 656581: /proc/640667/fdinfo  EXE 656581: /opt/google/chrome/chrome  CWD 656583: /home/sysadmin  EXE 656583: /opt/google/chrome/chrome  CWD 656884: /home/sysadmin  EXE 656884: /opt/google/chrome/chrome  PID 656998(/proc/656998): not in readdir output  PID 656998: not in ps output  CWD 656998: /proc/640667/fdinfo  EXE 656998: /opt/google/chrome/chrome  PID 656999(/proc/656999): not in readdir output  PID 656999: not in ps output  CWD 656999: /proc/640667/fdinfo  EXE 656999: /opt/google/chrome/chrome  PID 657000(/proc/657000): not in readdir output  PID 657000: not in ps output  CWD 657000: /proc/640667/fdinfo  EXE 657000: /opt/google/chrome/chrome  PID 657001(/proc/657001): not in readdir output  PID 657001: not in ps output  CWD 657001: /proc/640667/fdinfo  EXE 657001: /opt/google/chrome/chrome  PID 657002(/proc/657002): not in readdir output  PID 657002: not in ps output  CWD 657002: /proc/640667/fdinfo  EXE 657002: /opt/google/chrome/chrome  PID 657003(/proc/657003): not in readdir output  PID 657003: not in ps output  CWD 657003: /proc/640667/fdinfo  EXE 657003: /opt/google/chrome/chrome  You have 6 process hidden for readdir command  You have 6 process hidden for ps command  not found  ###  ### Output of: ./ifpromisc  ###  lo: not promisc and no packet sniffer sockets  eth0: PACKET SNIFFER(/usr/lib/systemd/systemd-networkd[704])  docker0: not promisc and no packet sniffer sockets  not infected  ###  ### Output of: ./chkwtmp -f /var/log/wtmp  ###  not infected  not infected  ###  ### Output of: ./chklastlog -f //var/log/wtmp -l //var/log/lastlog  ###  The tty of the following user process(es) were not found  in /var/run/utmp !  ! RUID PID TTY CMD  ! gdm 2084 tty1 /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.AVCN51 -listen 4 -listen 5 -displayfd 6 -listen 7  ! gdm 2073 tty1 /usr/libexec/at-spi-bus-launcher  ! gdm 2379 tty1 /usr/libexec/at-spi2-registryd --use-gnome-session  ! gdm 1406 tty1 dbus-daemon --nofork --print-address 4 --session  ! gdm 2078 tty1 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3  ! gdm 1403 tty1 dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart  ! gdm 1525 tty1 /usr/libexec/dconf-service  ! gdm 1326 tty1 /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart  ! gdm 2377 tty1 /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications  ! gdm 1407 tty1 /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart  ! gdm 1556 tty1 /usr/bin/gnome-shell  ! gdm 2424 tty1 /usr/libexec/gsd-a11y-settings  ! gdm 2391 tty1 /usr/libexec/gsd-color  ! gdm 2406 tty1 /usr/libexec/gsd-datetime  ! gdm 2433 tty1 /usr/libexec/gsd-housekeeping  ! gdm 2394 tty1 /usr/libexec/gsd-keyboard  ! gdm 2409 tty1 /usr/libexec/gsd-media-keys  ! gdm 2435 tty1 /usr/libexec/gsd-power  ! gdm 2395 tty1 /usr/libexec/gsd-print-notifications  ! gdm 2487 tty1 /usr/libexec/gsd-printer  ! gdm 2396 tty1 /usr/libexec/gsd-rfkill  ! gdm 2413 tty1 /usr/libexec/gsd-screensaver-proxy  ! gdm 2384 tty1 /usr/libexec/gsd-sharing  ! gdm 2397 tty1 /usr/libexec/gsd-smartcard  ! gdm 2417 tty1 /usr/libexec/gsd-sound  ! gdm 2389 tty1 /usr/libexec/gsd-wacom  ! gdm 2547 tty1 ibus-daemon --panel disable -r --xim  ! gdm 2767 tty1 /usr/libexec/ibus-engine-simple  ! gdm 2552 tty1 /usr/libexec/ibus-memconf  ! gdm 2559 tty1 /usr/libexec/ibus-portal  ! gdm 2555 tty1 /usr/libexec/ibus-x11 --kill-daemon  ! root 656584 pts/0 /bin/sh /usr/sbin/chkrootkit -x  ! root 657038 pts/0 ./chkutmp  ! root 657040 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args  ! root 657039 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"  ! root 656582 pts/0 sudo chkrootkit -x  ! sysadmin 655369 pts/0 bash  chkutmp: nothing deleted  not tested |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.