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.
    a. Command to inspect permissions:

```
ls -l /etc/shadow
```

    b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/shadow
```

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

```
ls -l /etc/gshadow
```

    b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/gshadow
```

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.

    a. Command to inspect permissions:

```
ls -l /etc/group
```

    b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/group
```

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

    a. Command to inspect permissions:

```
ls -l /etc/passwd
```

    b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/passwd
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin` with the `useradd` command.

    a. Command to add each user account (include all five users):

```
sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin
```

2. Ensure that only the `admin` has general sudo access.

    a. Command to add `admin` to the sudo group:

```
sudo usermod -G sudo admin
```

Step 3: Create User Group and Collaborative Folder

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

```
sudo addgroup engineers
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
    a. 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
```

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

```
sudo mkdir /home/engineers
```

4. Change ownership on the new engineers' shared folder to the `engineers` group.
    a. Command to change ownership of engineers' shared folder to `engineers` group:

```
sudo chown :engineers /home/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt install lynis
```

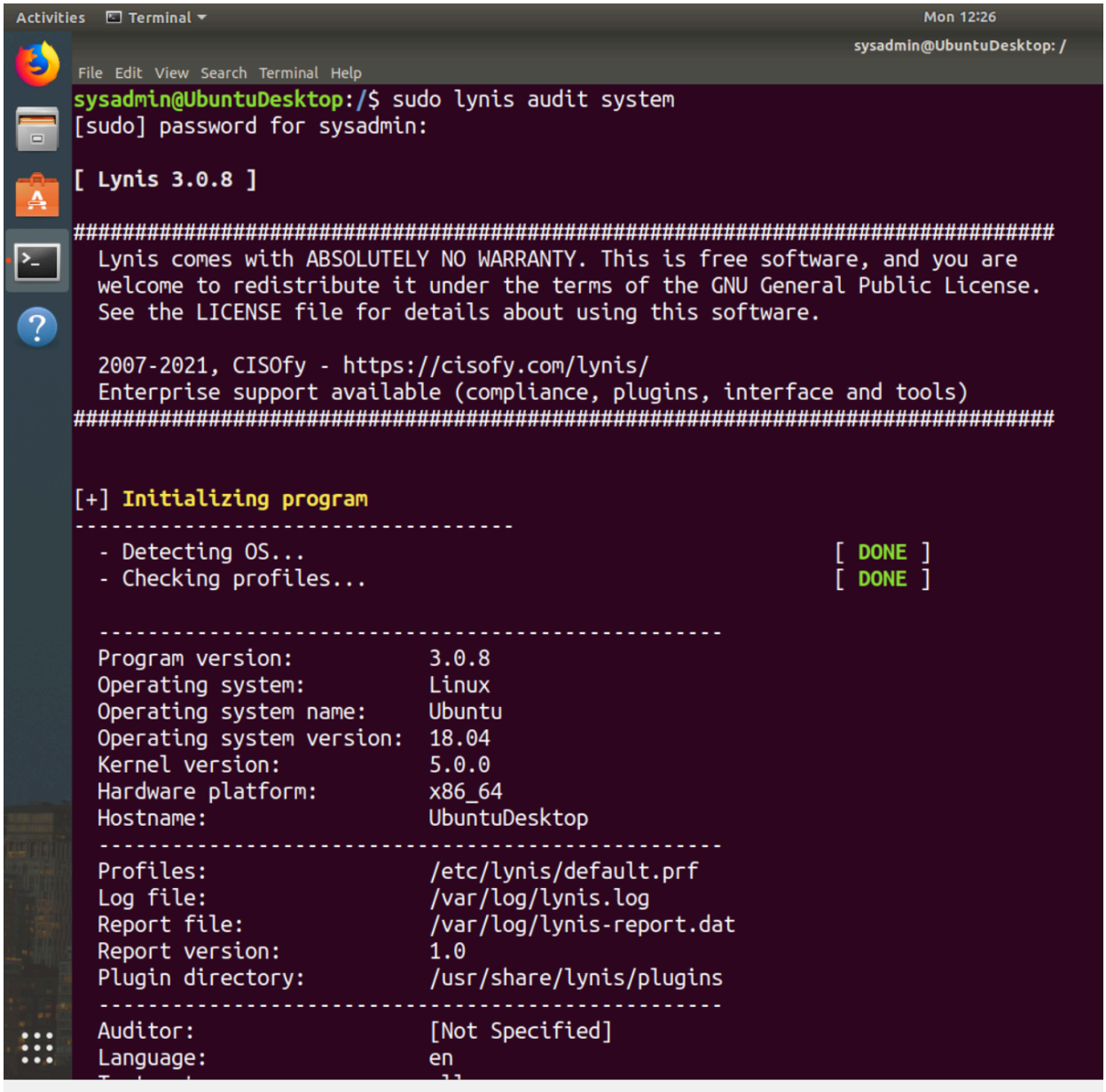
2. Command to view documentation and instructions:

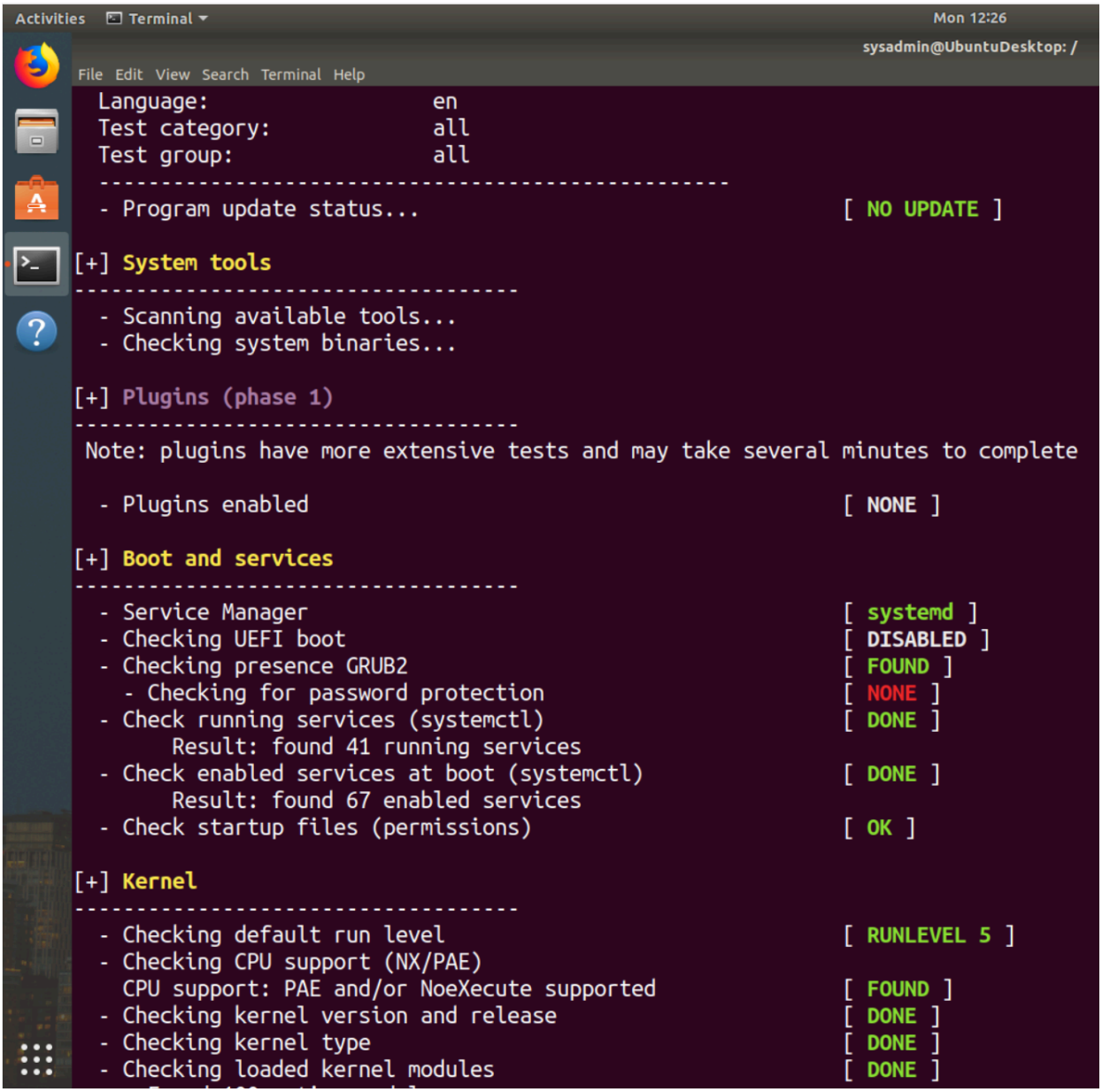
```
man lynis
```

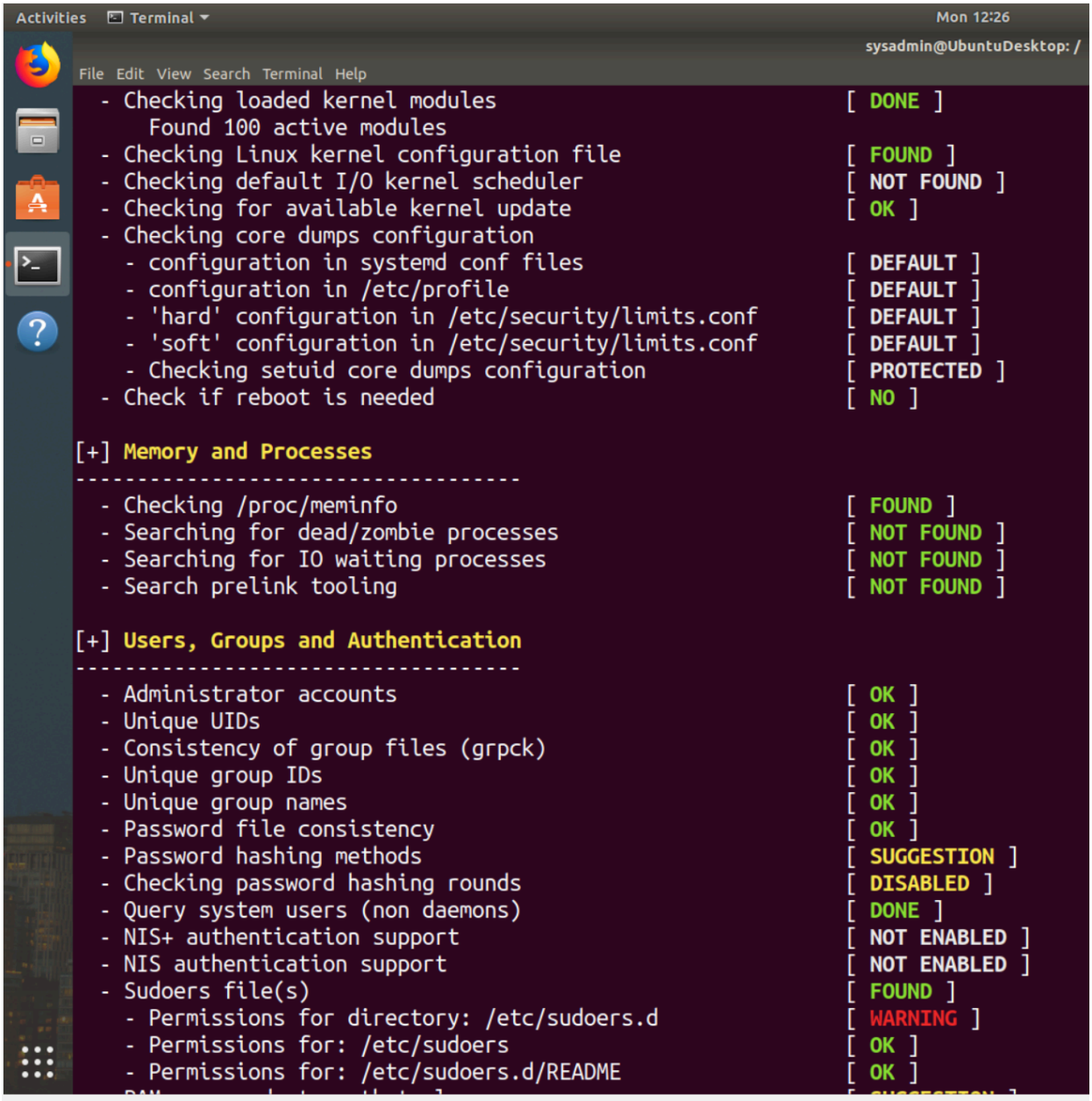
3. Command to run an audit:

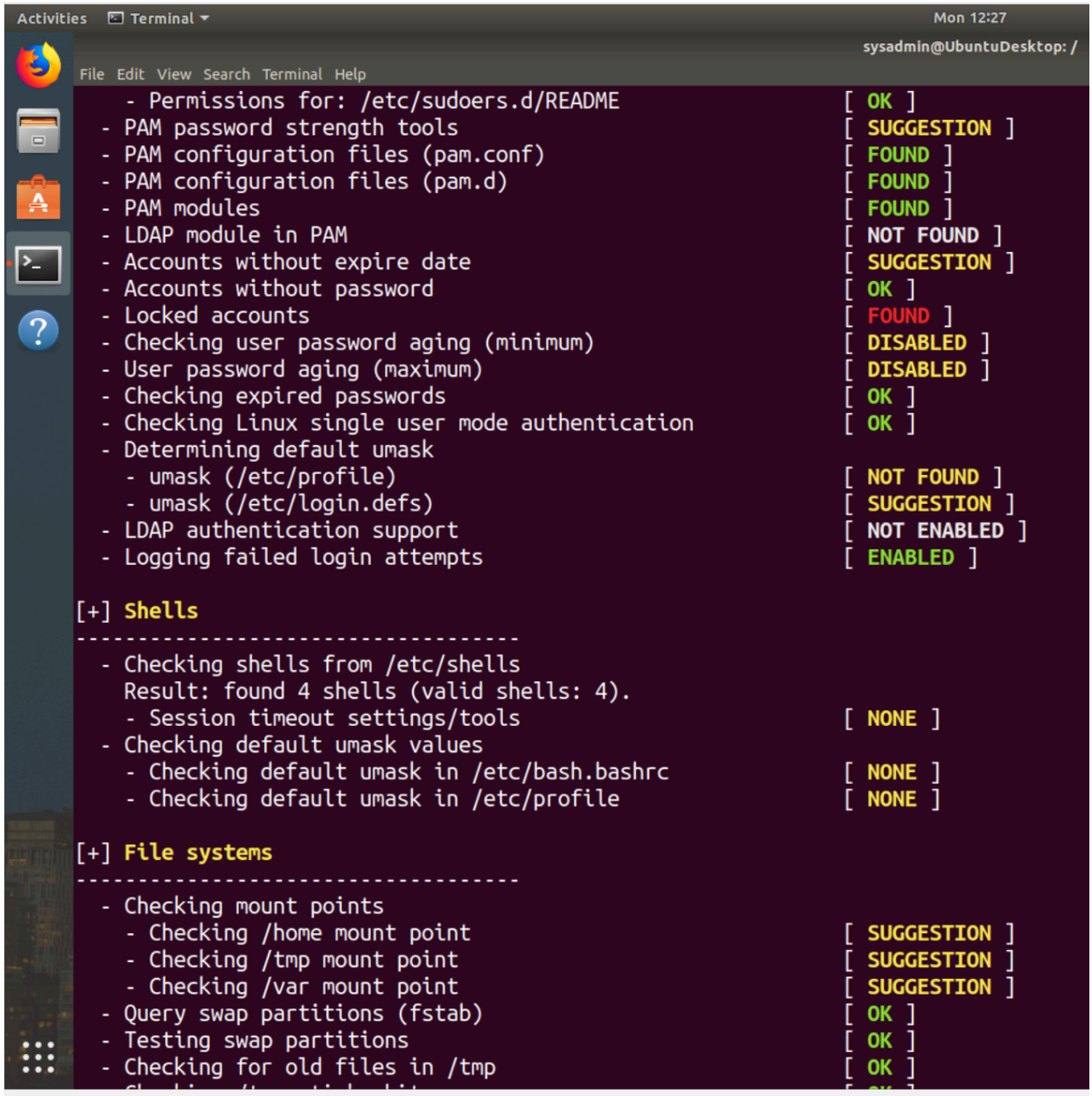
```
sudo lynis audit system
```

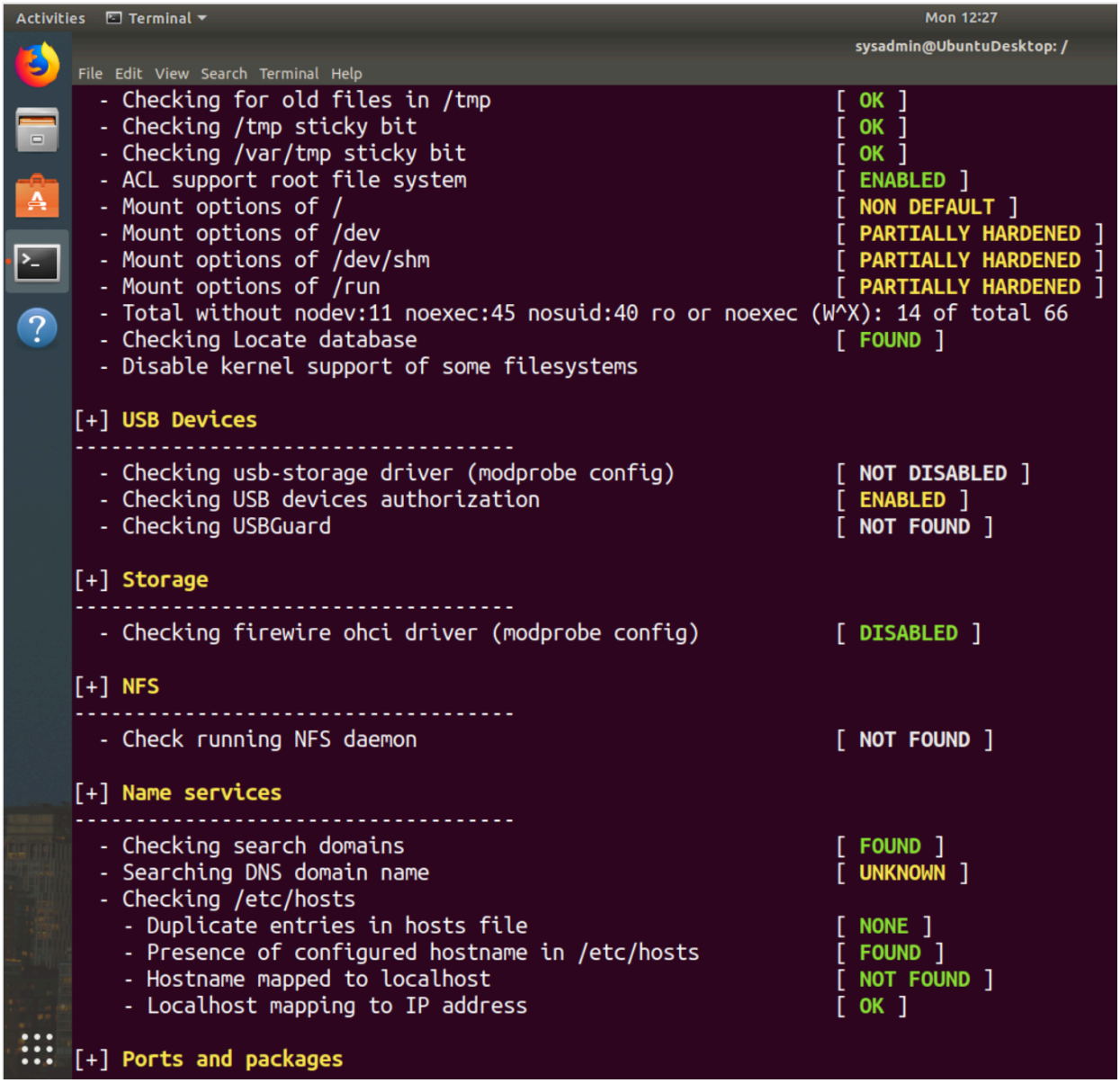
4. Provide a report from the Lynis output with recommendations for hardening the system.
    a. Screenshot of report output:


Activities
Terminal
Mon 12:26
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/$ sudo lynis audit system
[sudo] password for sysadmin:
[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: 18.04
Kernel version: 5.0.0
Hardware platform: x86_64
Hostname: UbuntuDesktop
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

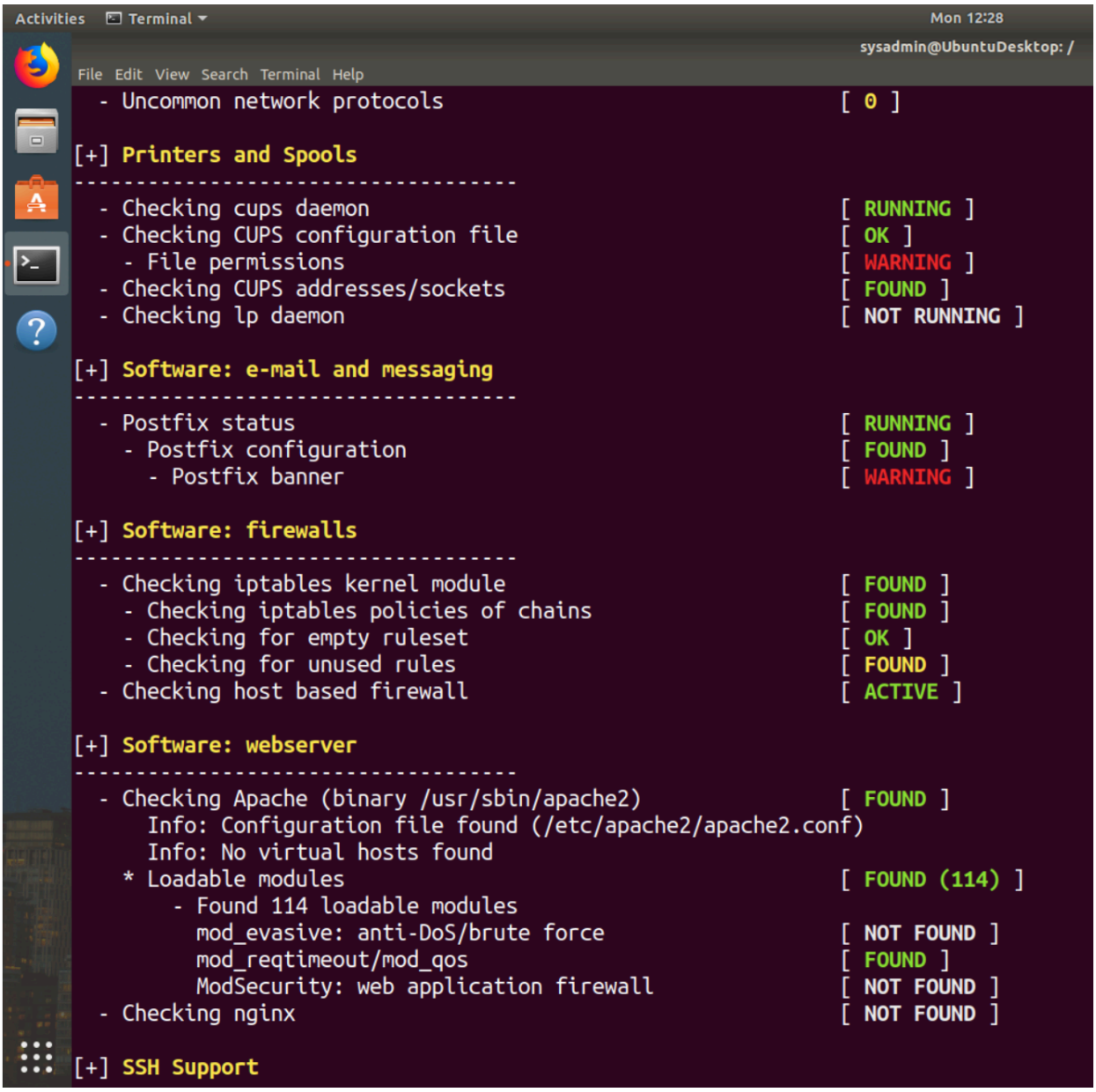

Activities
Terminal
Mon 12:26
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
Language: en
Test category: all
Test group: all
- Program update status... [NO UPDATE]
[+] System tools
- Scanning available tools...
- Checking system binaries...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
- Plugins enabled [NONE]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 41 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 67 enabled services
- Check startup files (permissions) [OK]
[+] 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]

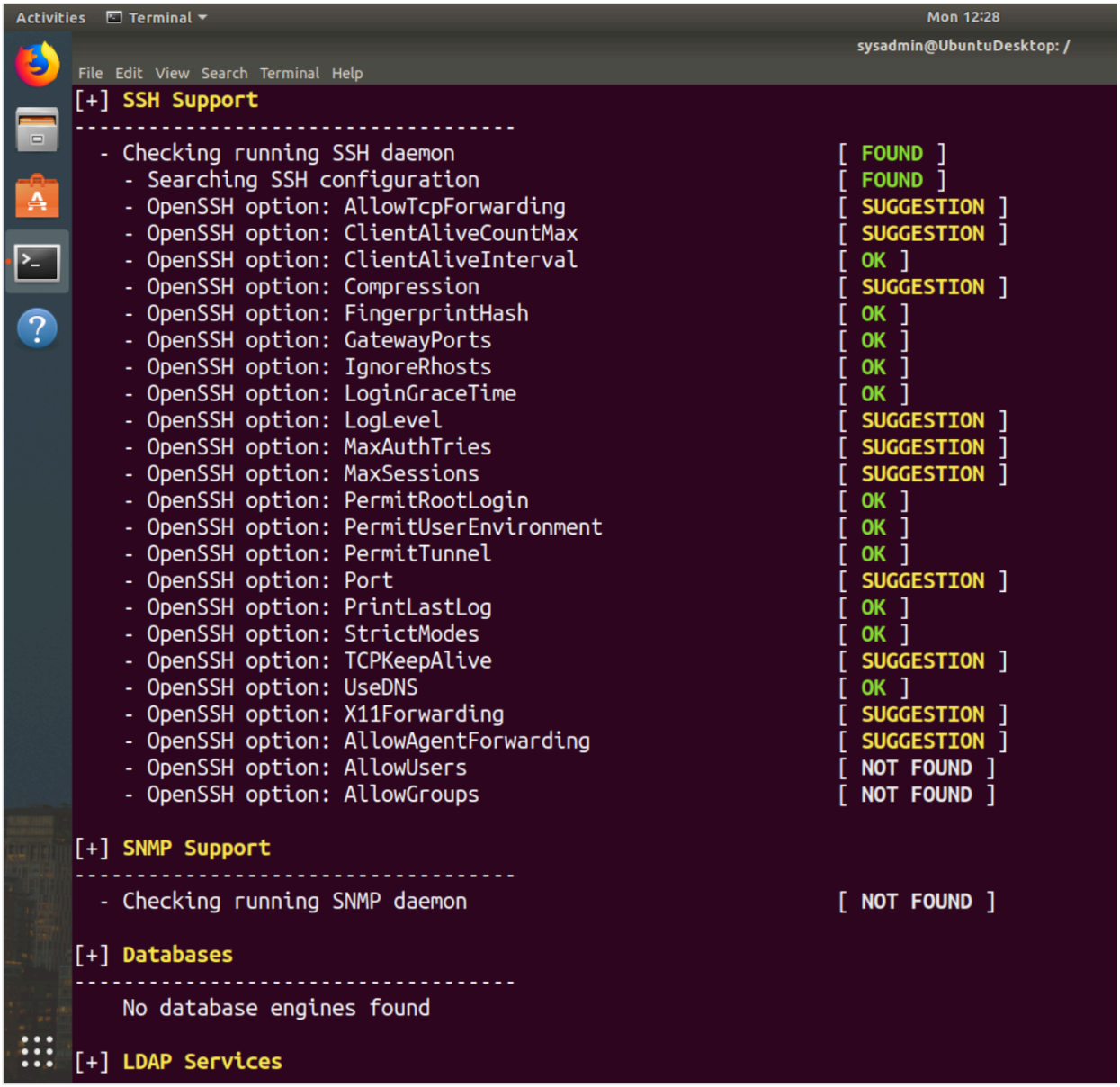

Activities
Terminal
Mon 12:26
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Checking loaded kernel modules [DONE]
Found 100 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- 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 [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 [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 [WARNING]
- Permissions for: /etc/sudoers [OK]
- Permissions for: /etc/sudoers.d/README [OK]

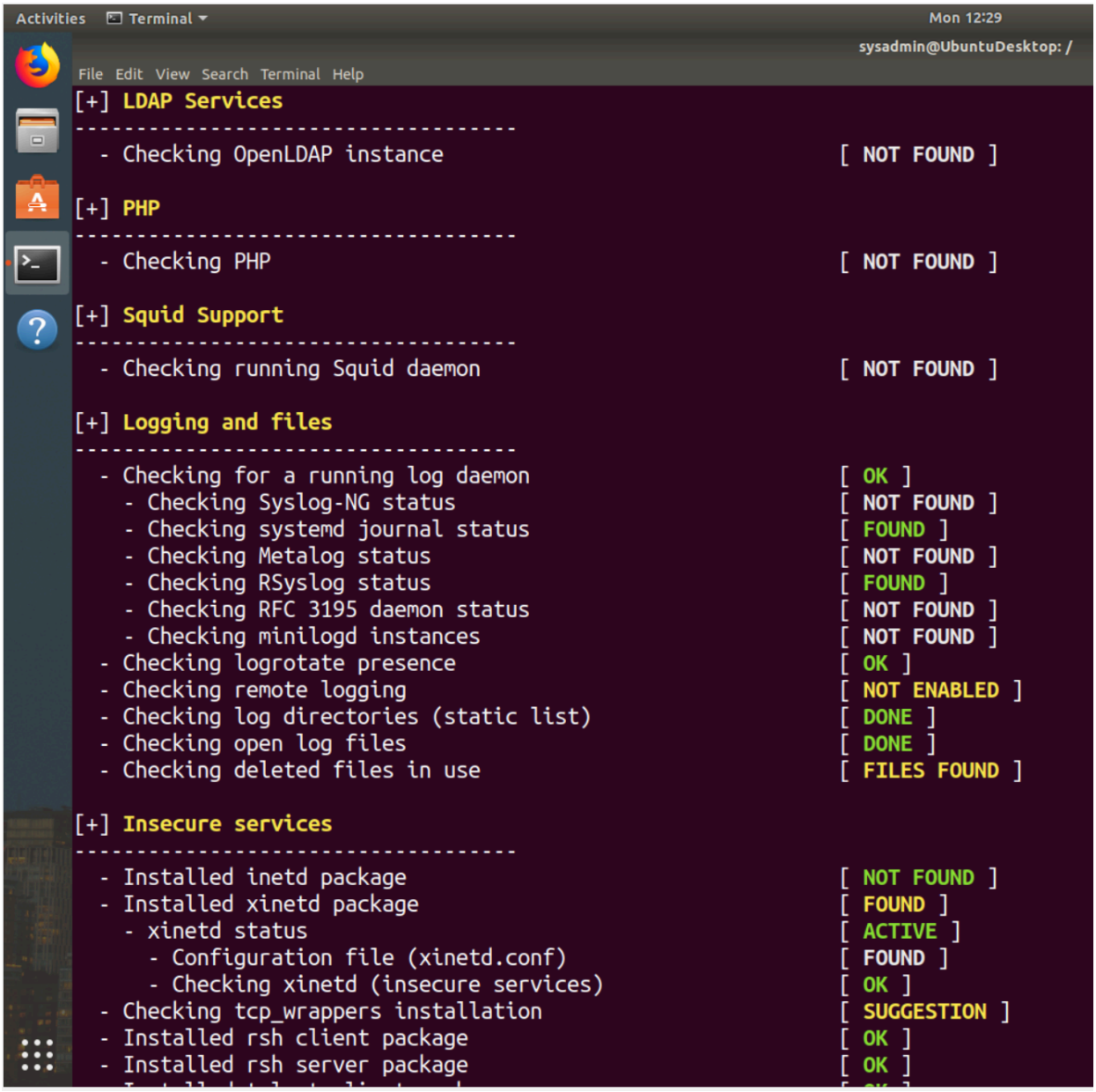

Activities
Terminal
Mon 12:27
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Permissions for: /etc/sudoers.d/README [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [SUGGESTION]
- Accounts without password [OK]
- Locked accounts [FOUND]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 4 shells (valid shells: 4).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Checking for old files in /tmp [OK]

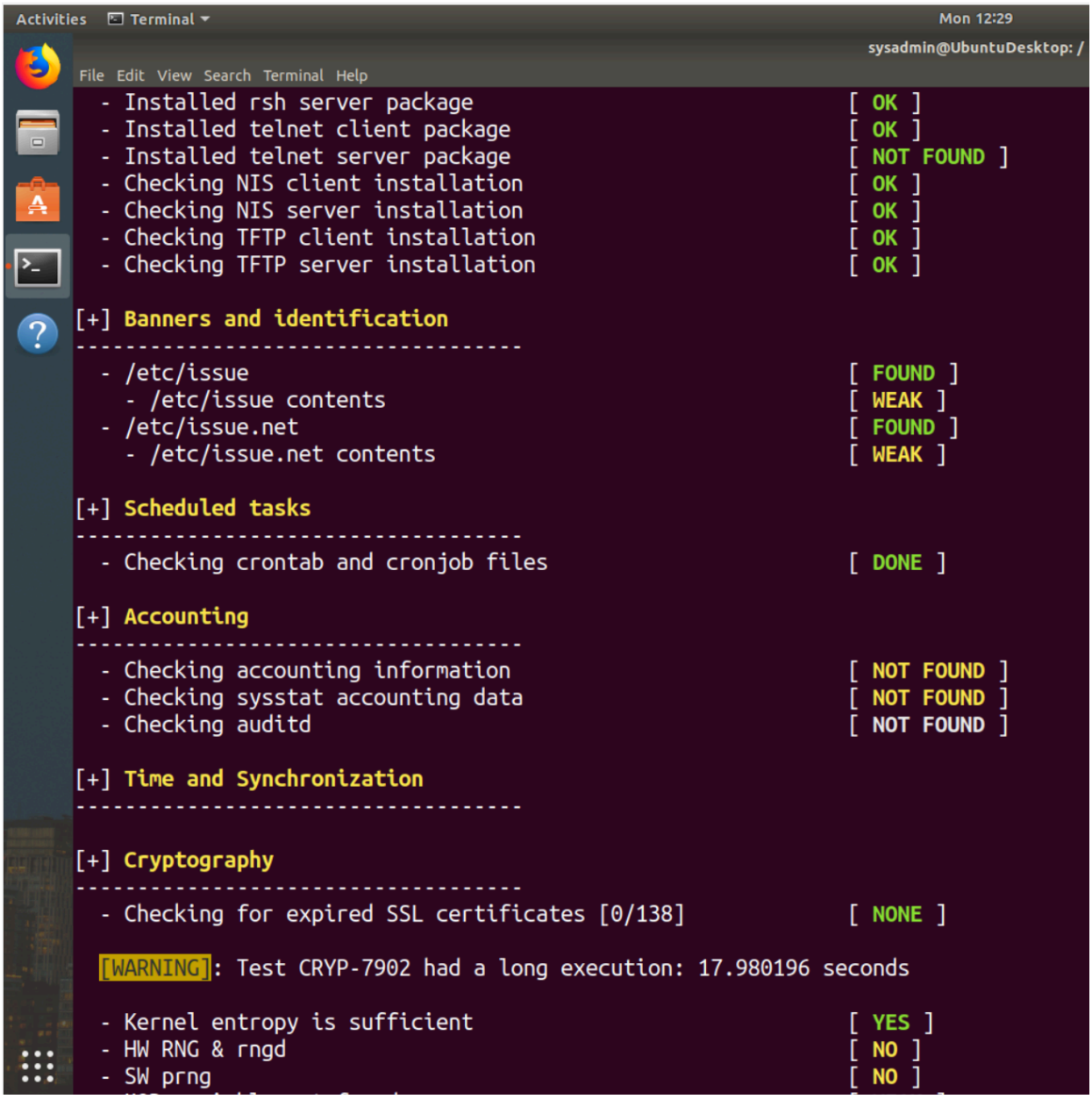

Activities
Terminal
Mon 12:27
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Mount options of /dev [PARTIALLY HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED]
- Mount options of /run [PARTIALLY HARDENED]
- Total without nodev:11 noexec:45 nosuid:40 ro or noexec (W^X): 14 of total 66
- 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) [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 [FOUND]
- Hostname mapped to localhost [NOT FOUND]
- Localhost mapping to IP address [OK]
[+] Ports and packages

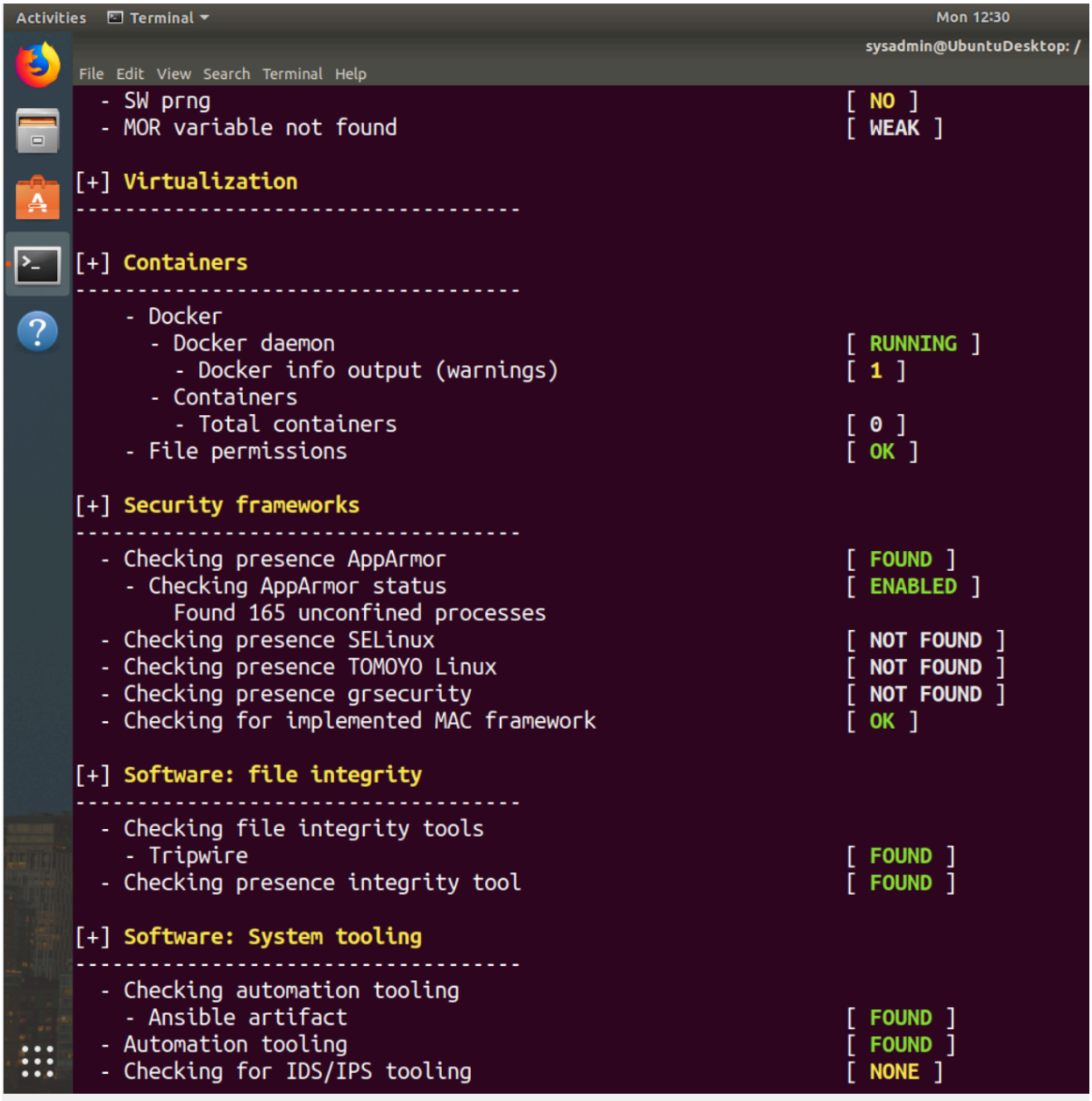

Activities
Terminal
Mon 12:28
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
[WARNING]: Test PKGS-7345 had a long execution: 16.892538 seconds
- Query unpurged packages [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: 44.327248 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 [RUNNING]
- Checking for ARP monitoring software [NOT FOUND]
- Uncommon network protocols [0]

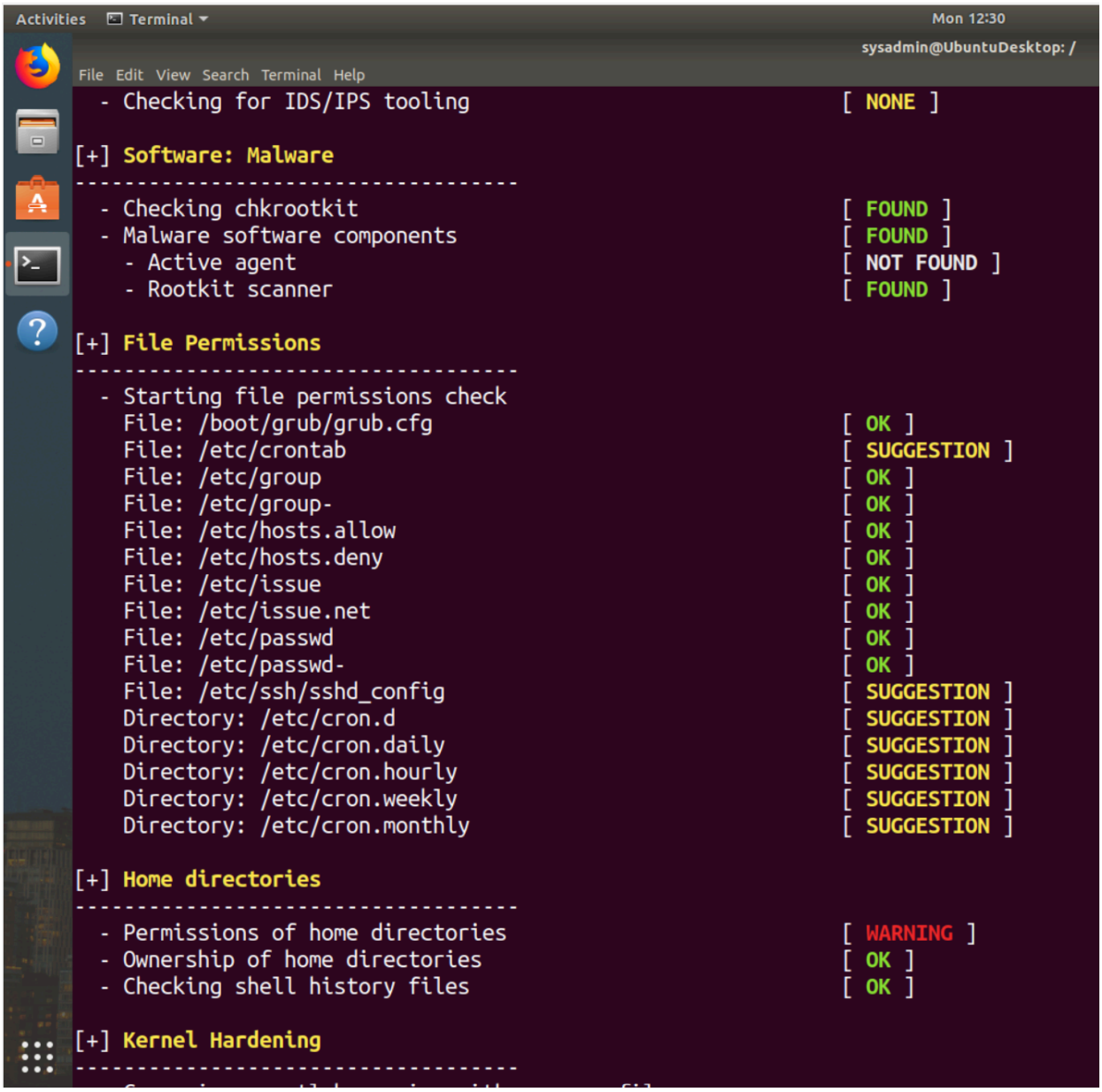

Activities
Terminal
Mon 12:28
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Uncommon network protocols [0]
[+] Printers and Spools
- Checking cups daemon [RUNNING]
- Checking CUPS configuration file [OK]
- File permissions [WARNING]
- Checking CUPS addresses/sockets [FOUND]
- Checking 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 (114)]
- Found 114 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

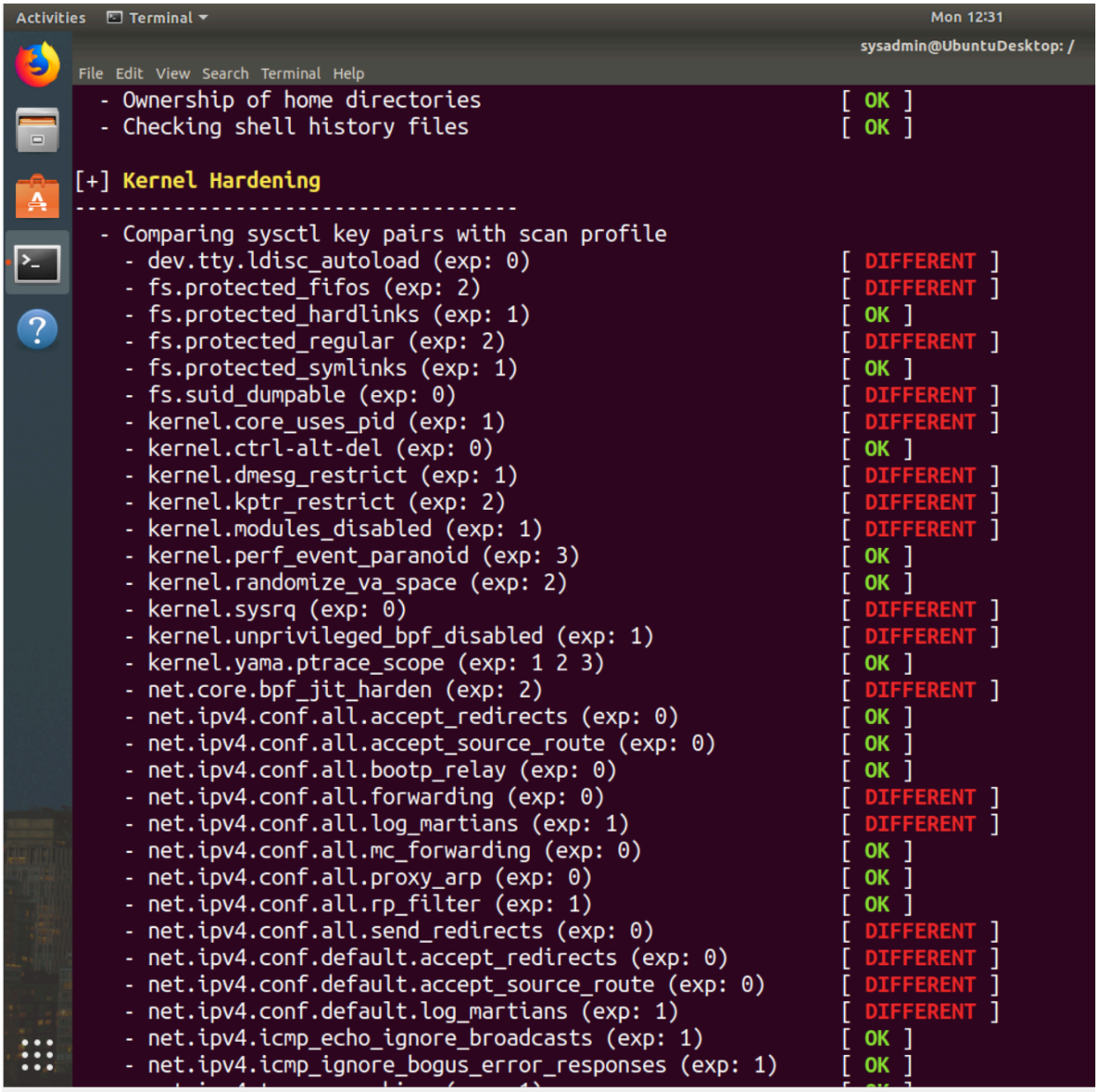

Activities
Terminal
Mon 12:28
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
[+] SSH Support
- Checking running SSH daemon [FOUND]
- Searching SSH configuration [FOUND]
- OpenSSH option: AllowTcpForwarding [SUGGESTION]
- OpenSSH option: ClientAliveCountMax [SUGGESTION]
- OpenSSH option: 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

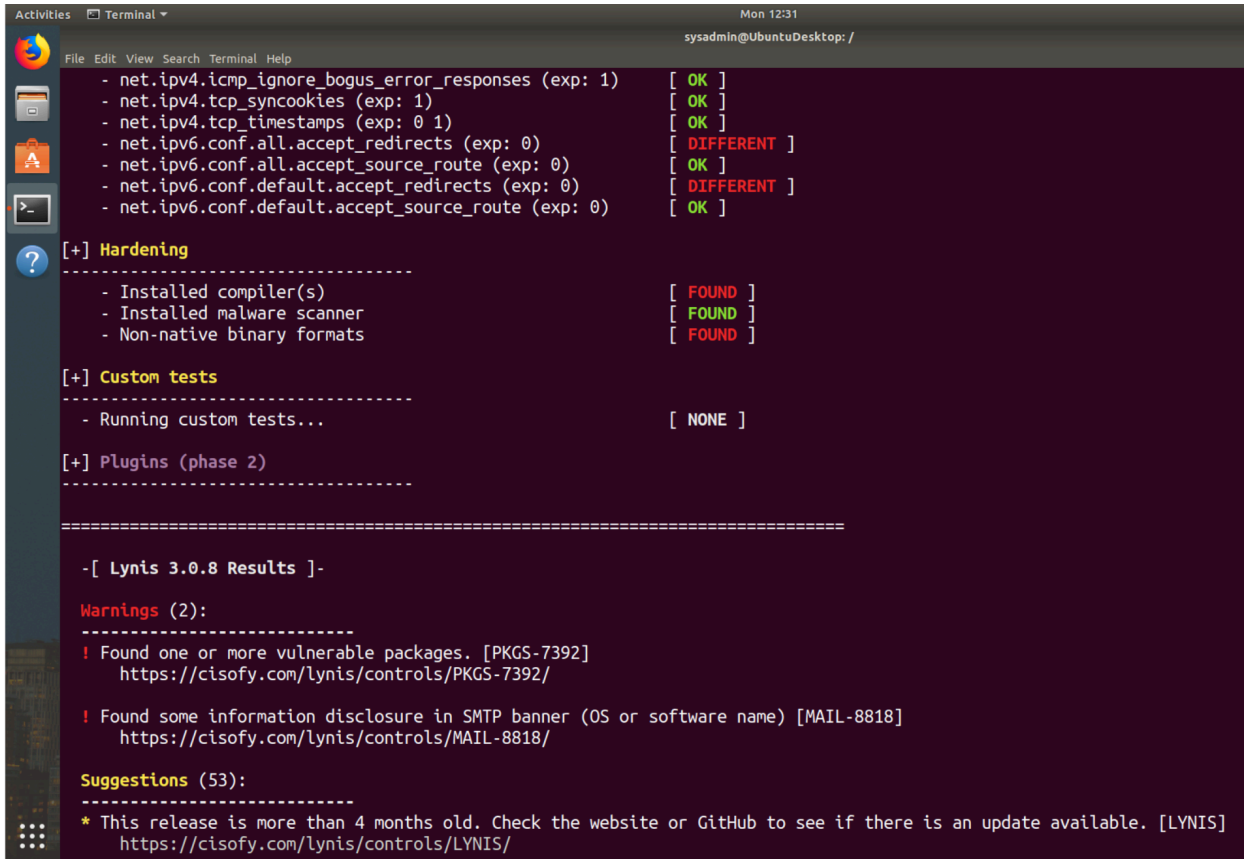

Activities
Terminal
Mon 12:29
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [NOT FOUND]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [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 [ACTIVE]
- Configuration file (xinetd.conf) [FOUND]
- Checking xinetd (insecure services) [OK]
- Checking tcp_wrappers installation [SUGGESTION]
- Installed rsh client package [OK]
- Installed rsh server package [OK]

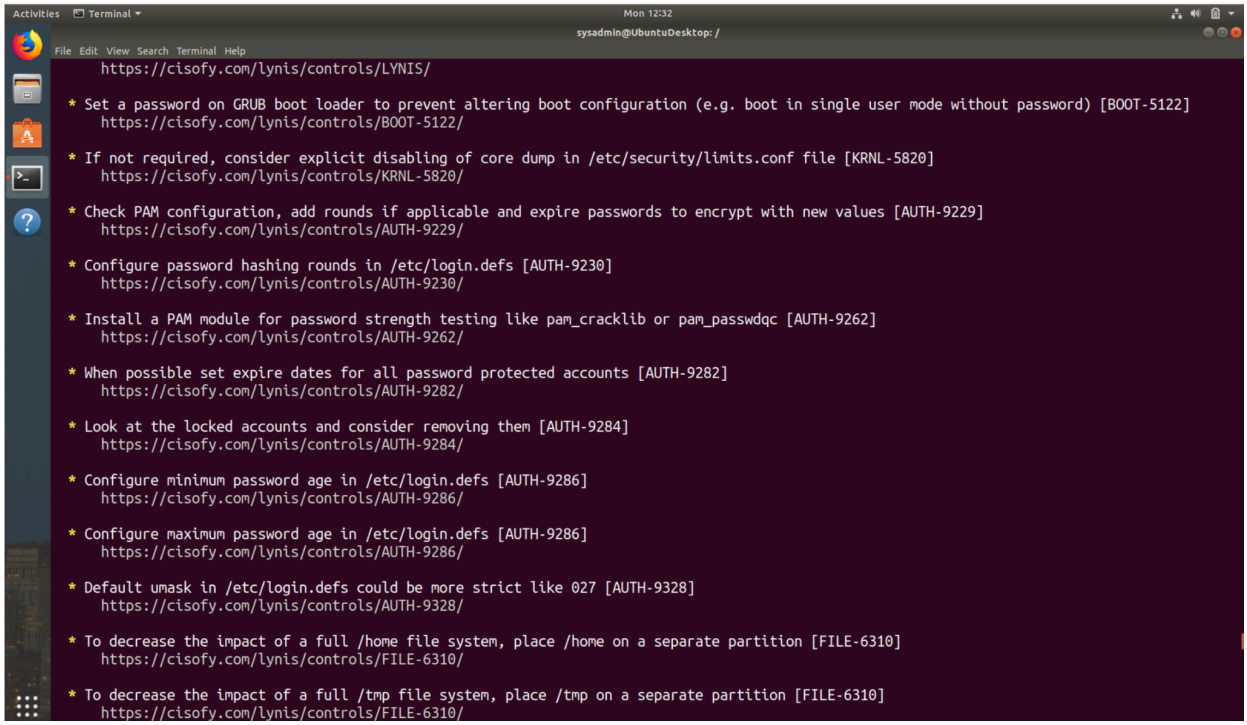

Activities
Terminal
Mon 12:29
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking 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]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [NOT FOUND]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/138] [NONE]
[WARNING]: Test CRYP-7902 had a long execution: 17.980196 seconds
- Kernel entropy is sufficient [YES]
- HW RNG & rngd [NO]
- SW prng [NO]

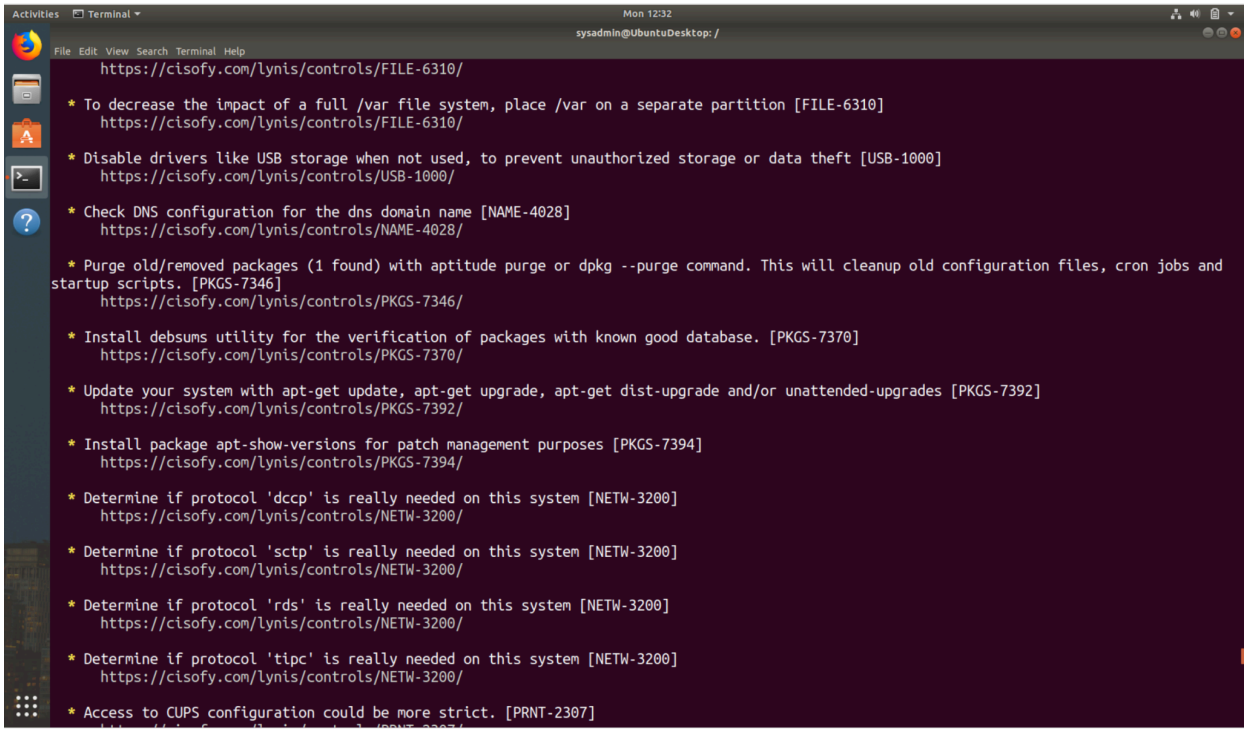

Activities
Terminal
Mon 12:30
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- SW prng [NO]
- MOR variable not found [WEAK]
[+] Virtualization
[+] Containers
- Docker
- Docker daemon [RUNNING]
- Docker info output (warnings) [1]
- Containers
- Total containers [0]
- File permissions [OK]
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [ENABLED]
Found 165 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]
- Checking presence integrity tool [FOUND]
[+] Software: System tooling
- Checking automation tooling
- Ansible artifact [FOUND]
- Automation tooling [FOUND]
- Checking for IDS/IPS tooling [NONE]

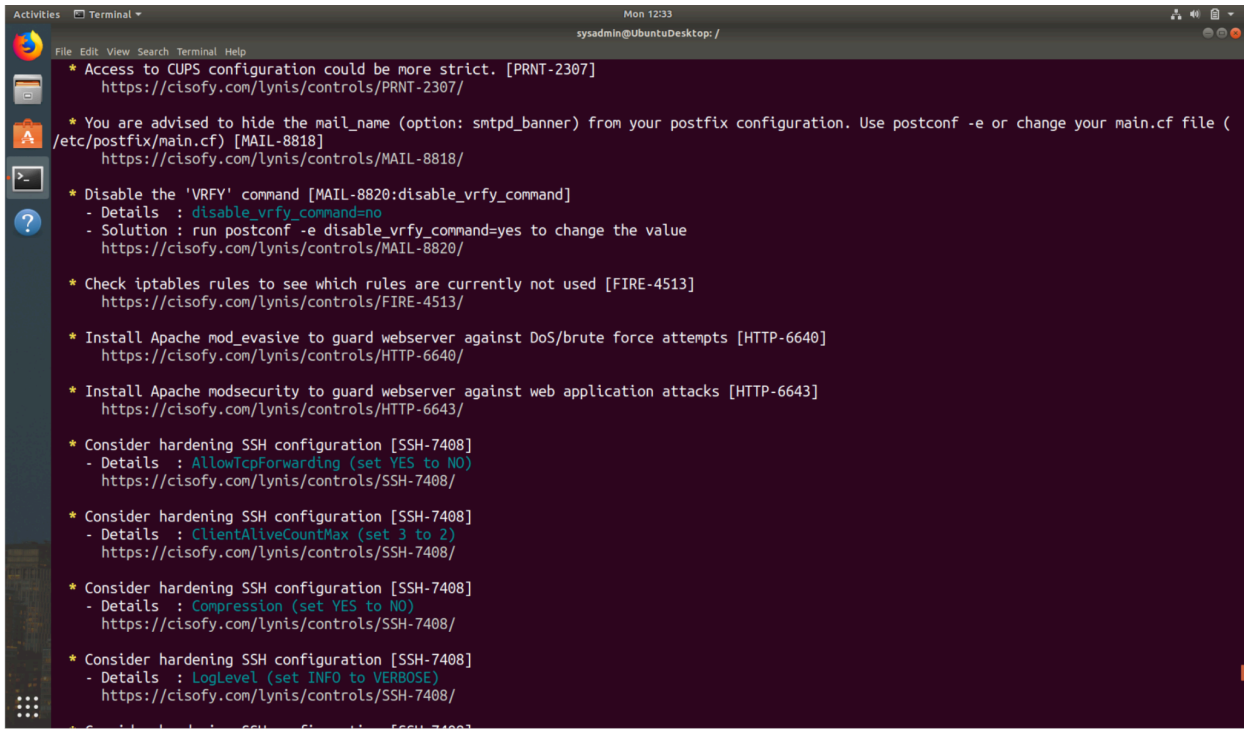

Activities
Terminal
Mon 12:30
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Checking for IDS/IPS tooling [NONE]
[+] Software: Malware
- Checking chkrootkit [FOUND]
- Malware software components [FOUND]
- Active agent [NOT FOUND]
- Rootkit scanner [FOUND]
[+] File Permissions
- Starting file permissions check
File: /boot/grub/grub.cfg [OK]
File: /etc/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: /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

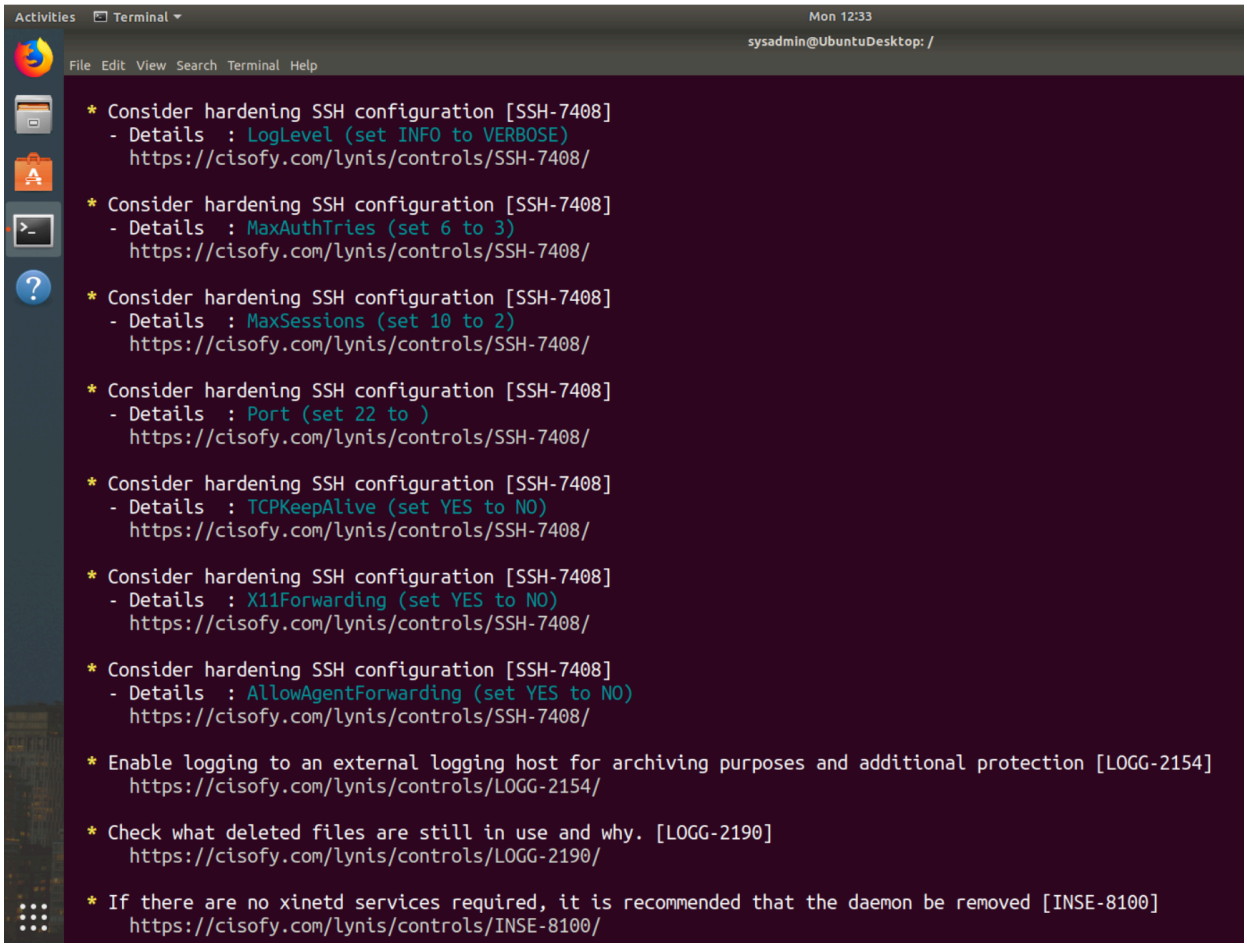

Activities
Terminal
Mon 12:31
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- Ownership of home directories [OK]
- Checking shell history files [OK]
[+] Kernel Hardening
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFFERENT]
- fs.protected_fifos (exp: 2) [DIFFERENT]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [DIFFERENT]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFFERENT]
- kernel.core_uses_pid (exp: 1) [DIFFERENT]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [DIFFERENT]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.modules_disabled (exp: 1) [DIFFERENT]
- kernel.perf_event_paranoid (exp: 3) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFFERENT]
- kernel.yama.ptrace_scope (exp: 1 2 3) [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) [OK]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]

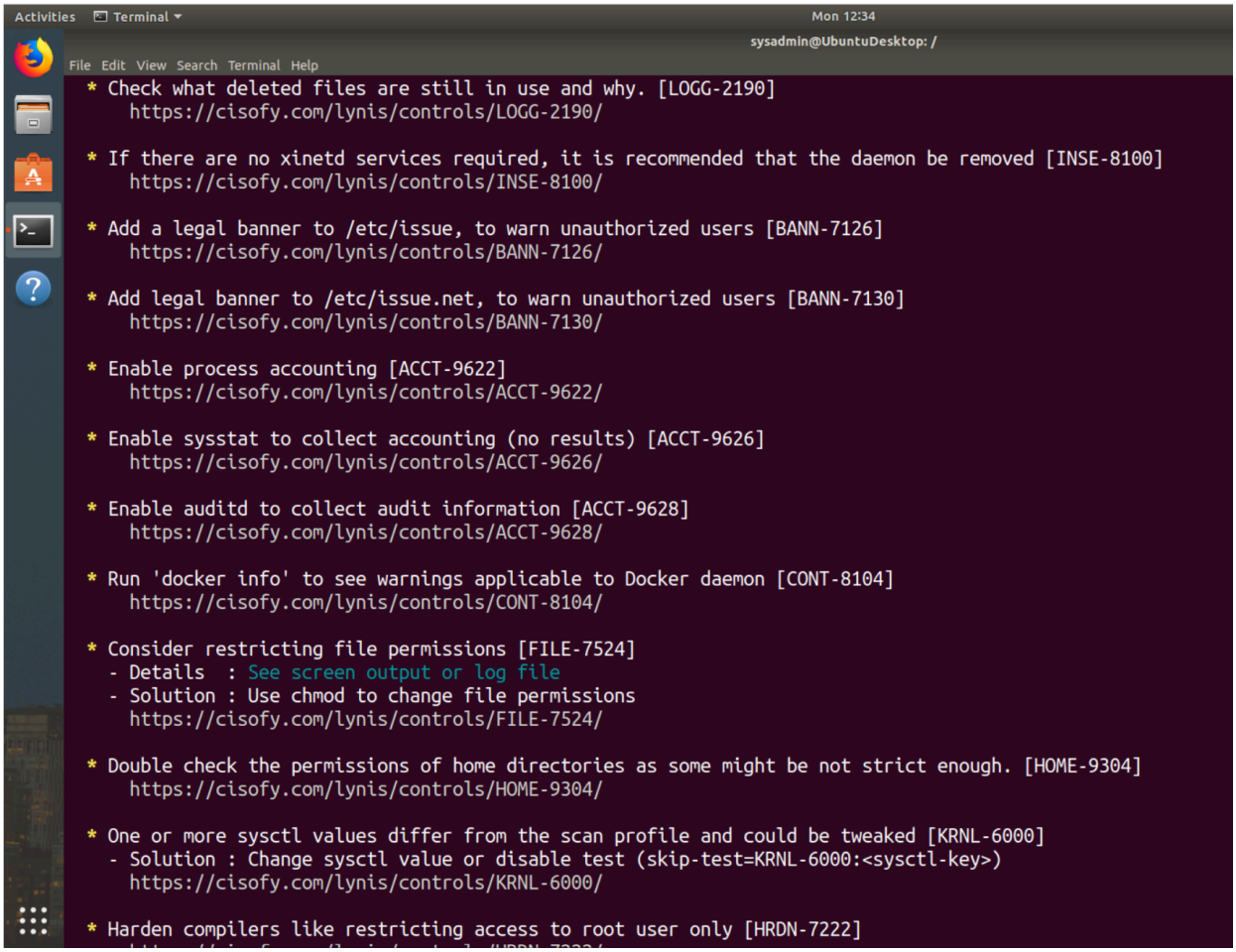

Activities
Terminal
Mon 12:31
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Hardening
- Installed compiler(s) [FOUND]
- Installed malware scanner [FOUND]
- Non-native binary formats [FOUND]
[+] Custom tests
- Running custom tests... [NONE]
[+] Plugins (phase 2)
-[Lynis 3.0.8 Results]-
Warnings (2):
! 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 (53):
* 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/

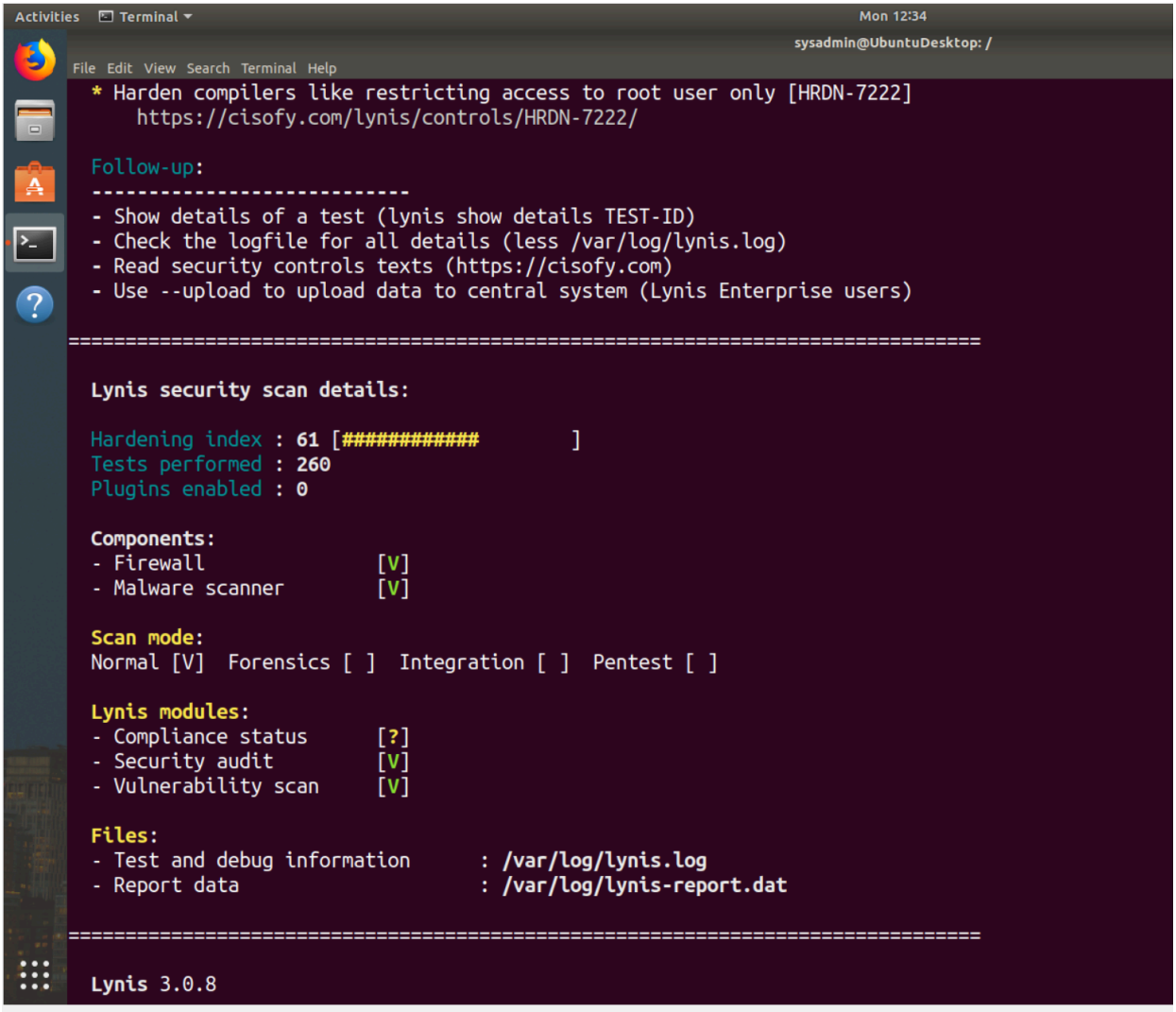

Activities
Terminal
Mon 12:32
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
https://cisofy.com/lynis/controls/LYNIS/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/lynis/controls/BOOT-5122/
* 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/

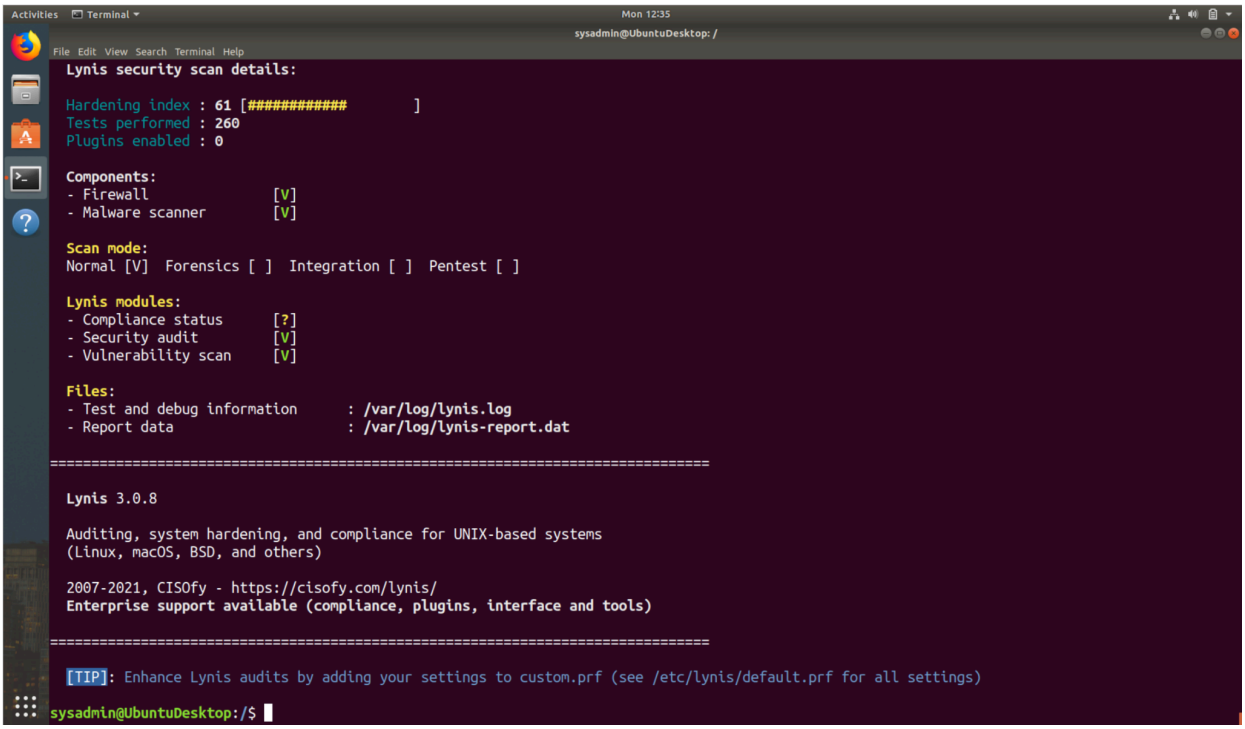

Activities
Terminal
Mon 12:32
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
https://cisofy.com/lynis/controls/FILE-6310/
* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/
* Disable drivers like 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/
* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
https://cisofy.com/lynis/controls/PKGS-7346/
* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
https://cisofy.com/lynis/controls/PKGS-7370/
* 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]


Activities
Terminal
Mon 12:33
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
* 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/


Activities
Terminal
Mon 12:33
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
* 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/


Activities
Terminal
Mon 12:34
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
* 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/
* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
https://cisofy.com/lynis/controls/CONT-8104/
* 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]


Activities
Terminal
Mon 12:34
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
* 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 : 61 [############]
Tests performed : 260
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



Bonus

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

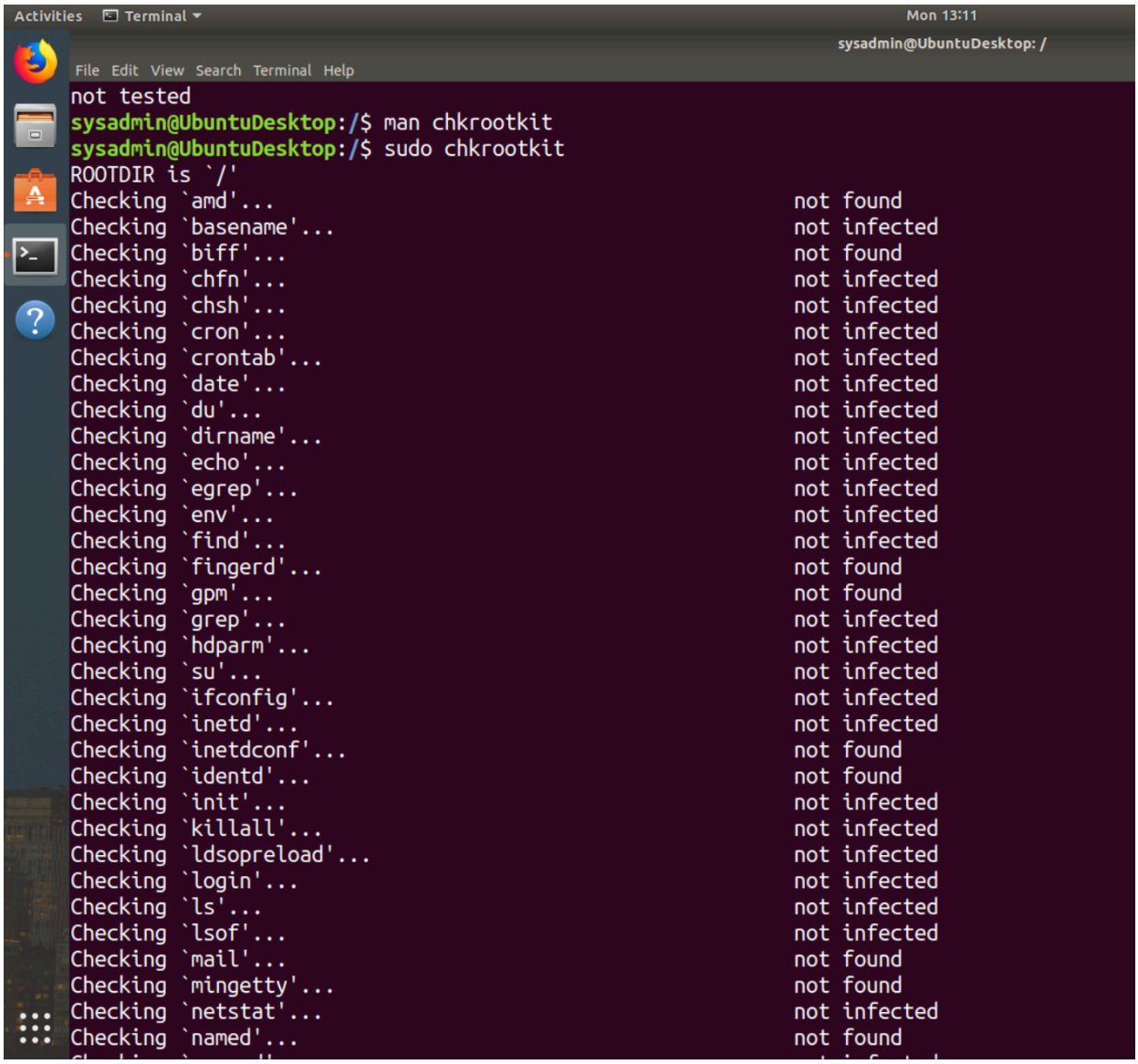
2. Command to view documentation and instructions:

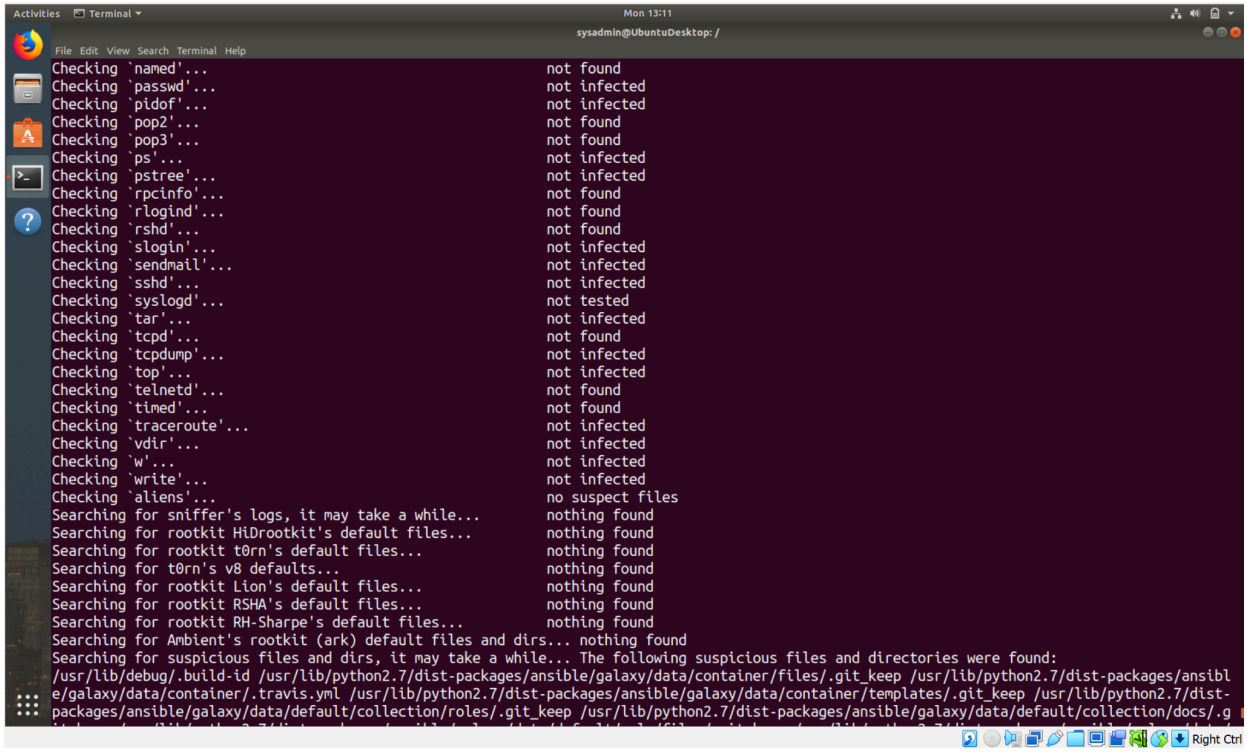
```
man chkrootkit
```

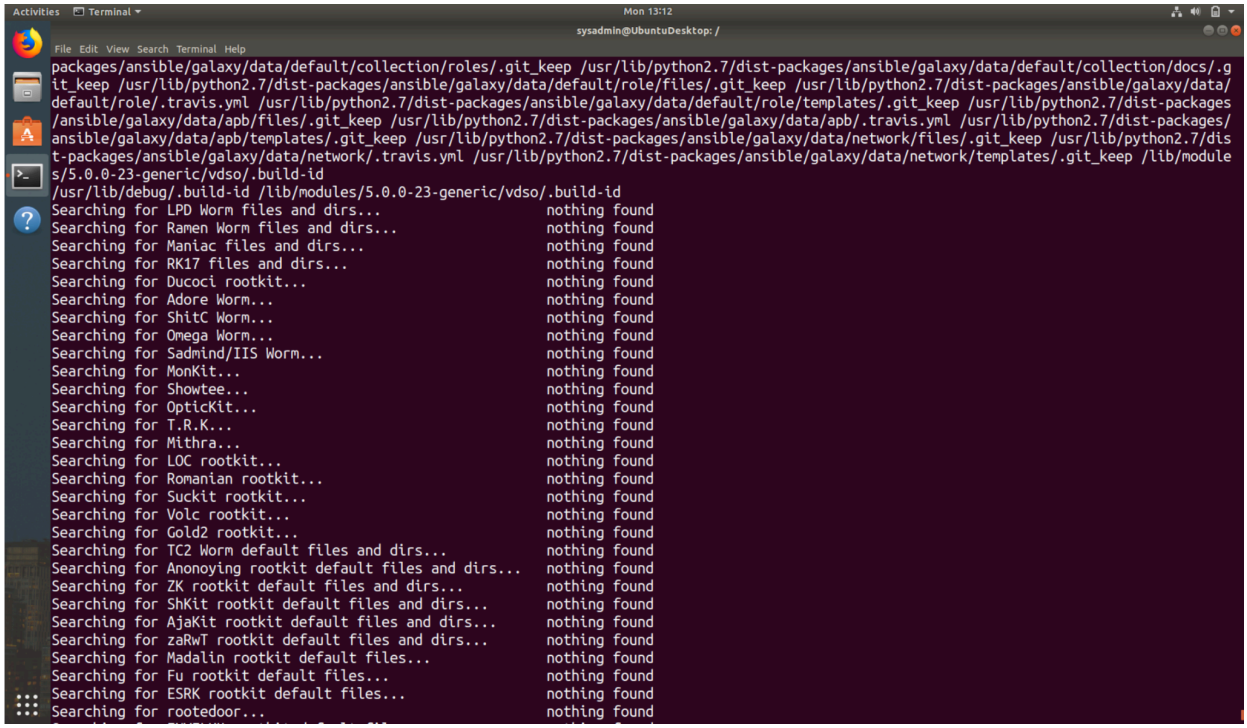
3. Command to run expert mode:

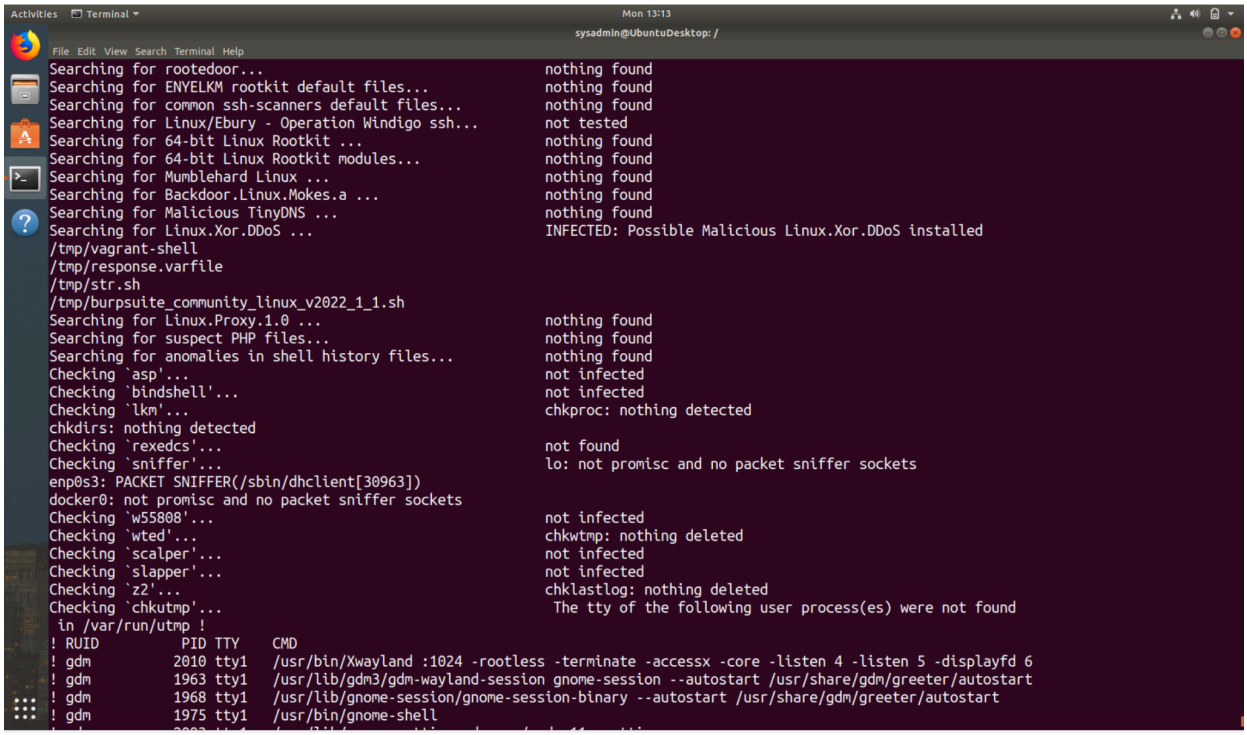
```
sudo chkrootkit -x
```

4. Provide a report from the chrootkit output with recommendations for hardening the system.
    a. Screenshot of end of sample output:


Activities
Terminal
Mon 13:11
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
not tested
sysadmin@UbuntuDesktop:/$ man chkrootkit
sysadmin@UbuntuDesktop:/$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not infected
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not found
Checking `mingetty'... not found
Checking `netstat'... not infected
Checking `named'... not found


Activities
Terminal
Mon 13:11
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not found
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not tested
Checking `tar'... not infected
Checking `tcpd'... not found
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not found
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for rootkit HiDrootkit's default files... nothing found
Searching for rootkit t0rn's default files... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for rootkit Lion's default files... nothing found
Searching for rootkit RSHA's default files... nothing found
Searching for rootkit RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following suspicious files and directories were found:
/usr/lib/debug/.build-id /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/roles/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.g
Right Ctrl


Activities
Terminal
Mon 13:12
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
packages/ansible/galaxy/data/default/collection/roles/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/templates/.git_keep /lib/modules/5.0.0-23-generic/vdso/.build-id
/usr/lib/debug/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found


Activities
Terminal
Mon 13:13
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
Searching for rootedoor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for Linux/Ebury - Operation Windigo ssh... not tested
Searching for 64-bit Linux Rootkit ... nothing found
Searching for 64-bit Linux Rootkit modules... nothing found
Searching for Mumblehard Linux ... nothing found
Searching for Backdoor.Linux.Mokes.a ... nothing found
Searching for Malicious TinyDNS ... nothing found
Searching for Linux.Xor.DDoS ... INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/str.sh
/tmp/burpsuite_community_linux_v2022_1_1.sh
Searching for Linux.Proxy.1.0 ... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[30963])
docker0: not promisc and no packet sniffer sockets
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'... The tty of the following user process(es) were not found
in /var/run/utmp !
! RUID PID TTY CMD
! gdm 2010 tty1 /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm 1963 tty1 /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm 1968 tty1 /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm 1975 tty1 /usr/bin/gnome-shell