Step 1: Ensure Permissions on Sensitive Files

The /etc/ directory is where system configuration files exist. Start by navigating to this directory with cd /etc/.

Inspect the file permissions of each of the files below. This should have already been completed in the activity, but let's double check! If they do not match the descriptions, please update the permissions.

1. Permissions on /etc/shadow should allow only root read and write access.

```
sysadmin@UbuntuDesktop:/etc$ la shadow
shadow
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 2893 Jun 28 07:05 shadow
sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 shadow
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 2893 Jun 28 07:05 shadow
```

2. Permissions on /etc/gshadow should allow only root read and write access.

```
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1068 Jun 28 06:44 gshadow
sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 gshadow
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1068 Jun 28 06:44 gshadow
```

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

```
sysadmin@UbuntuDesktop:/etc$ ls -l groups
ls: cannot access 'groups': No such file or directory
sysadmin@UbuntuDesktop:/etc$ ls -l group
-rw-r--r-- 1 root root 1292 Jun 28 06:44 group
sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 group
sysadmin@UbuntuDesktop:/etc$ ls -l group
```

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

```
sysadmin@UbuntuDesktop:/etc$ ls -l passwd
-rw-r--r-- 1 root root 3214 Jun 28 07:05 passwd
sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 passwd
sysadmin@UbuntuDesktop:/etc$ ls -l passwd
-rw-r--r-- 1 root root 3214 Jun 28 07:05 passwd
```

- **Hints:**

- Run the following command to view the file permissions: ls -l <file>
- If permissions need to be changed or modified, use the chmod command.

Step 2: Create User Accounts

This step asks you to set up various users. These commands do not require you to be working from a specific directory.

1. Add user accounts for sam, joe, amy, sara, and admin.
    - **Hint:** In order for users to be added to the system, you need to run the command with sudo.
    - ```
      sysadmin@UbuntuDesktop:/etc$ sudo adduser sam
      Adding user `sam' ...
      Adding new group `sam' (1014) ...
      Adding new user `sam' (1012) with group `sam' ...
      Creating home directory `/home/sam' ...
      Copying files from `/etc/skel' ...
      Enter new UNIX password:
      Retype new UNIX password:
      passwd: password updated successfully
      Changing the user information for sam
      Enter the new value, or press ENTER for the default
              Full Name []: Sam
              Room Number []: 01
              Work Phone []:
              Home Phone []:
              Other []:
      Is the information correct? [Y/n] y
      ```
      ```

```
sysadmin@UbuntuDesktop:/etc$ sudo adduser joe
Adding user `joe' ...
Adding new group `joe' (1015) ...
Adding new user `joe' (1013) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
        Full Name []: Joe
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

```
sysadmin@UbuntuDesktop:/etc$ sudo adduser amy
Adding user `amy' ...
Adding new group `amy' (1016) ...
Adding new user `amy' (1014) with group `amy' ...
Creating home directory `/home/amy' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for amy
Enter the new value, or press ENTER for the default
        Full Name []: Amy
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

- ```
  sysadmin@UbuntuDesktop:/etc$ sudo adduser sara
  Adding user `sara' ...
  Adding new group `sara' (1017) ...
  Adding new user `sara' (1015) with group `sara' ...
  Creating home directory `/home/sara' ...
  Copying files from `/etc/skel' ...
  Enter new UNIX password:
  Retype new UNIX password:
  passwd: password updated successfully
  Changing the user information for sara
  Enter the new value, or press ENTER for the default
          Full Name []: Sara
          Room Number []:
          Work Phone []:
          Home Phone []:
          Other []:
  Is the information correct? [Y/n] y
  ```
- ```
  sysadmin@UbuntuDesktop:/etc$ sudo adduser admin
  Adding user `admin' ...
  Adding new group `admin' (1018) ...
  Adding new user `admin' (1016) with group `admin' ...
  Creating home directory `/home/admin' ...
  Copying files from `/etc/skel' ...
  Enter new UNIX password:
  Retype new UNIX password:
  passwd: password updated successfully
  Changing the user information for admin
  Enter the new value, or press ENTER for the default
          Full Name []: admin
          Room Number []:
          Work Phone []:
          Home Phone []:
          Other []:
  Is the information correct? [Y/n] y
  ```

2. We want to make sure that only the admin user has general sudo group access. This requires a command that will allow user modifications.

```
sysadmin@UbuntuDesktop:/etc$ groups admin
admin : admin
sysadmin@UbuntuDesktop:/etc$ tail /etc/group
postdrop:x:128:
dovecot:x:130:
dovenull:x:131:
rdma:x:132:
jane:x:1013:
sam:x:1014:
joe:x:1015:
amy:x:1016:
sara:x:1017:
admin:x:1018:
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG sudo admin
sysadmin@UbuntuDesktop:/etc$ tail /etc/group
postdrop:x:128:
dovecot:x:130:
dovenull:x:131:
rdma:x:132:
jane:x:1013:
sam:x:1014:
joe:x:1015:
amy:x:1016:
sara:x:1017:
admin:x:1018:
sysadmin@UbuntuDesktop:/etc$ groups admin
admin : admin sudo
```

Step 3: Create User Group and Collaborative Folder

Now we want to execute the commands to fully set up a group on our system.

This requires us to create a group, add users to it, create a shared group folder, set the group folder owners for these shared folders.

1. Add the group engineers to the system.

```
sysadmin@UbuntuDesktop:/etc$ sudo addgroup engineers
Adding group `engineers' (GID 1019) ...
Done.
sysadmin@UbuntuDesktop:/etc$ less /etc/group
```

2. Add users sam, joe, amy, and sara to the managed group. This will be similar to how you added admin to the sudo group in the previous exercise.

```
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG managed sam
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG managed joe
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG managed amy
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG managed sara
sysadmin@UbuntuDesktop:/etc$ groups sam joe amy sara
sam : sam managed
joe : joe managed
amy : amy managed
sara : sara managed
```

3. Create a shared folder for this group: /home/engineers.

```
sysadmin@UbuntuDesktop:/etc$ sudo mkdir /home/engineers
sysadmin@UbuntuDesktop:/etc$ ls -l /home/engineers
```

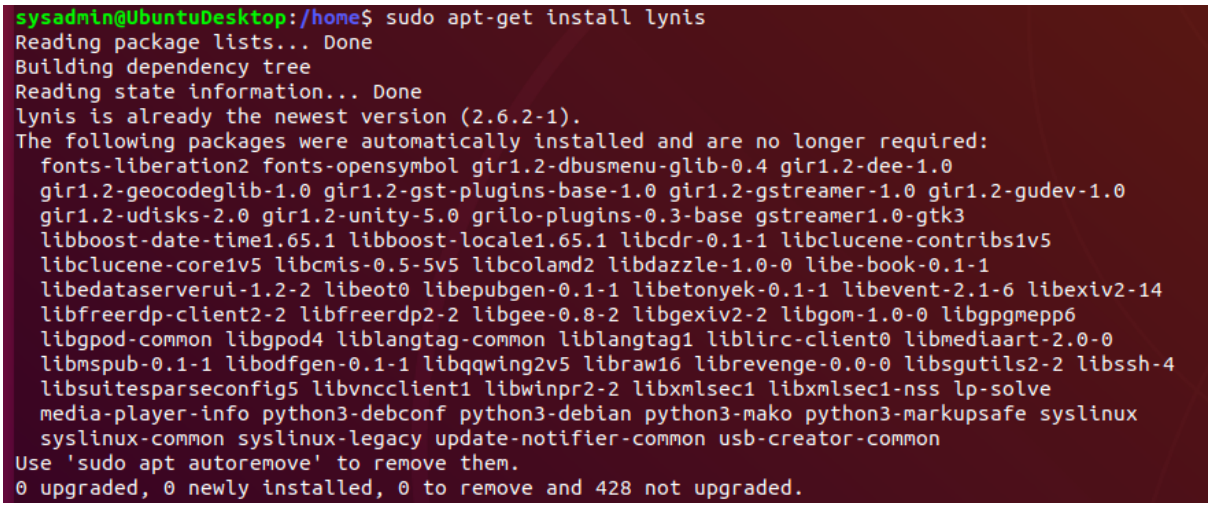
4. Change ownership on the new engineers' shared folder to the engineers group.

```
sysadmin@UbuntuDesktop:/home$ sudo chown :engineers engineers
sysadmin@UbuntuDesktop:/home$ ls -l
total 76
drwxr-xr-x  8 adam       adam       4096 May 14 16:29 adam
drwxr-xr-x  8 admin      admin      4096 Jul  2 18:48 admin
drwxr-xr-x  8 amy        amy        4096 Jul  2 18:47 amy
drwxr-xr-x  8 billy      billy      4096 May 14 16:29 billy
drwxr-xr-x  2 root       engineers  4096 Jul  2 19:04 engineers
drwxr-xr-x  8 http       http       4096 May 14 16:29 http
drwxr-xr-x  9 instructor instructor 4096 May 14 16:36 instructor
drwxr-xr-x  8 jack       jack       4096 May 14 16:29 jack
drwxr-xr-x  8 jane       jane       4096 May 14 16:31 jane
drwxr-xr-x  8 joe        joe        4096 Jul  2 18:46 joe
drwxr-xr-x  8 john       john       4096 May 14 16:29 john
drwxr-xr-x  9 max        max        4096 Jun 25 22:57 max
drwxr-xr-x  9 sally      sally      4096 Jun 25 22:40 sally
drwxr-xr-x  8 sam        sam        4096 Jul  2 18:36 sam
drwxr-xr-x  8 sara       sara       4096 Jul  2 18:48 sara
drwxr-xr-x  8 student    student    4096 May 14 16:24 student
drwxr-xr-x 22 sysadmin   sysadmin   4096 Jun 28 17:18 sysadmin
-rw-r--r--  1 root       root       1581 May 14 16:29 user.hashes
drwxr-xr-x 19 vagrant    vagrant    4096 Jun 16 06:30 vagrant
```

Step 4: Lynis Auditing

The final step on your administrator's list involves running an audit against the system in order to harden it. You'll use the system and security auditing tool Lynis to do so.

1. Install the Lynis package to your system if it is not already installed.



2. Check the Lynis documentation for instructions on how to run a system audit.

3. Run a Lynis system audit with sudo.

```
sysadmin@UbuntuDesktop:/home$ sudo lynis audit system

[ Lynis 2.6.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


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

  ---------------------------------------------------
  Program version:           2.6.2
  Operating system:          Linux
  Operating system name:     Ubuntu Linux
  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:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ WARNING ]

      ===============================================================================
        Lynis update available
      ===============================================================================

        Current version is more than 4 months old

        Current version : 262   Latest version : 305
```

4. Provide a report from the Lynis output on what more could be done to harden the system.

```
  -[ Lynis 2.6.2 Results ]-

  Warnings (4):
  ----------------------------
  ! Version of Lynis is very old and should be updated [LYNIS]
      https://cisofy.com/controls/LYNIS/

  ! No password set for single mode [AUTH-9308]
      https://cisofy.com/controls/AUTH-9308/

  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/controls/PKGS-7392/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
      https://cisofy.com/controls/MAIL-8818/

  Suggestions (52):
  ----------------------------
  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
      https://your-domain.example.org/controls/CUST-0280/

  * Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
      https://your-domain.example.org/controls/CUST-0285/

  * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
      https://your-domain.example.org/controls/CUST-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
      https://your-domain.example.org/controls/CUST-0811/

  * Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libr
aries and need restarting. [CUST-0830]
      https://your-domain.example.org/controls/CUST-0830/

  * Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons a
re using old versions of libraries and need restarting. [CUST-0831]
      https://your-domain.example.org/controls/CUST-0831/

  * Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
      https://your-domain.example.org/controls/CUST-0870/

  * Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
      https://your-domain.example.org/controls/CUST-0875/

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

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

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

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

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

  * Set password for single user mode to minimize physical access attack surface [AUTH-9308]
      https://cisofy.com/controls/AUTH-9308/

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

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

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

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

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
      https://cisofy.com/controls/STRG-1840/

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

  * Purge old/removed packages (2 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and star
tup scripts. [PKGS-7346]
      https://cisofy.com/controls/PKGS-7346/

  * Install debsums utility for the verification of packages with known good database. [PKGS-7370]
      https://cisofy.com/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/controls/PKGS-7392/

  * Install package apt-show-versions for patch management purposes [PKGS-7394]
      https://cisofy.com/controls/PKGS-7394/

  * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
      https://cisofy.com/controls/NETW-3032/

  * Access to CUPS configuration could be more strict. [PRNT-2307]
      https://cisofy.com/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/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/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
      https://cisofy.com/controls/FIRE-4513/

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

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

  * Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]
      https://cisofy.com/controls/HTTP-6710/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (3 --> 2)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (YES --> (DELAYED|NO))
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (INFO --> VERBOSE)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (6 --> 2)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (10 --> 2)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (WITHOUT-PASSWORD --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (22 --> )
      https://cisofy.com/controls/SSH-7408/
```

```
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

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

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

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

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

  * Enable sysstat to collect accounting (no results) [ACCT-9626]
      https://cisofy.com/controls/ACCT-9626/

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

  * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
      https://cisofy.com/controls/CONT-8104/

  * 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/controls/KRNL-6000/

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

================================================================================
```

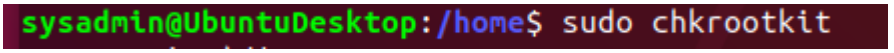
Bonus

Despite claims from enthusiasts, Linux is *not* immune to malware. You will need to install and run the application chkrootkit, to search for any potential rootkits installed on the system.

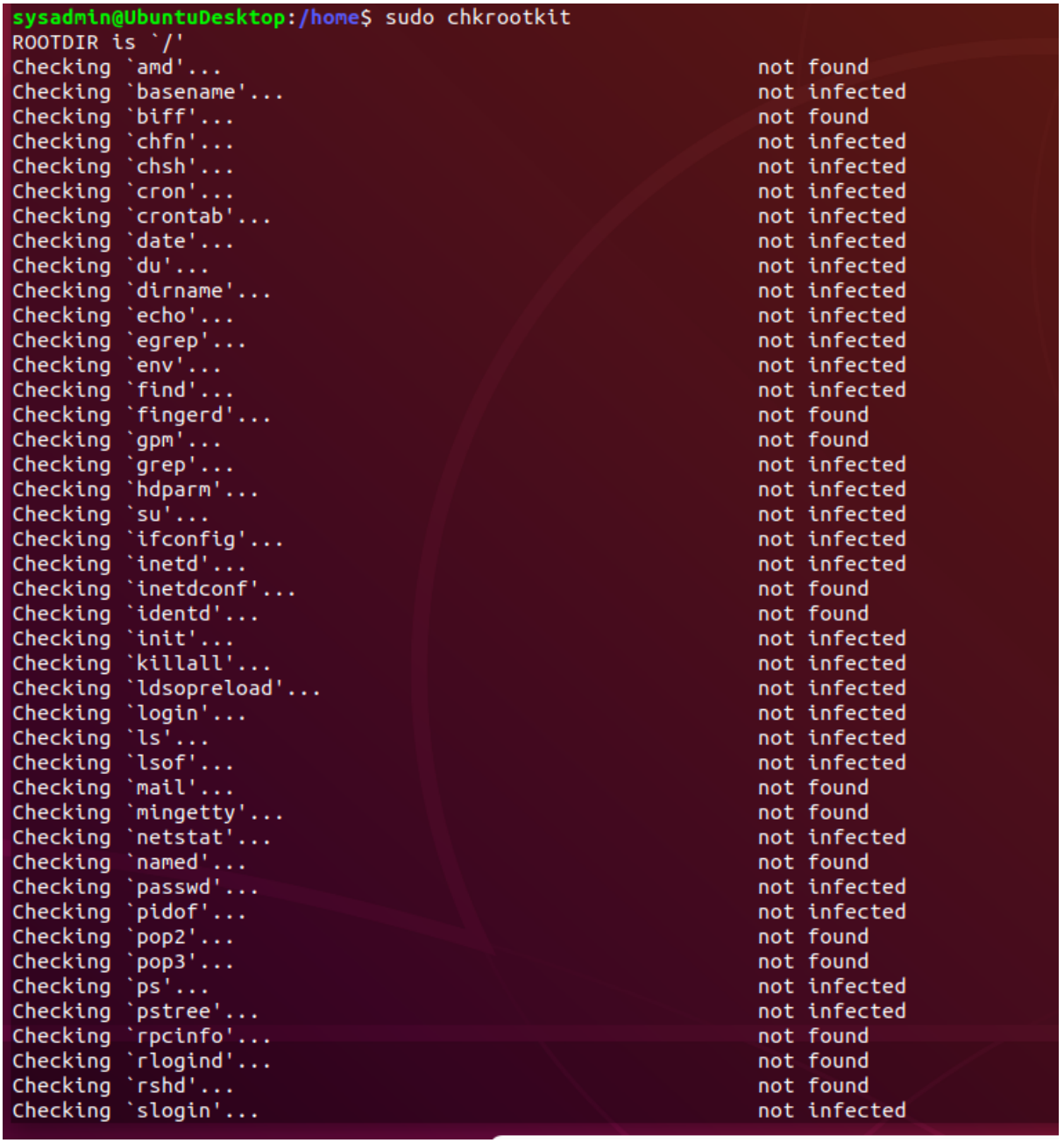
1. Install the chkrootkit package to your system if it is not already installed.

```
sysadmin@UbuntuDesktop:/home$ sudo apt-get install chkrootkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
chkrootkit is already the newest version (0.52-1ubuntu0.1).
The following packages were automatically installed and are no longer required:
  fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0
  gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0
  gir1.2-udisks-2.0 gir1.2-unity-5.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
  libboost-date-time1.65.1 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5
  libclucene-core1v5 libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1
  libedataserverui-1.2-2 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14
  libfreerdp-client2-2 libfreerdp2-2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6
  libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 libmediaart-2.0-0
  libmspub-0.1-1 libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4
  libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxmlsec1 libxmlsec1-nss lp-solve
  media-player-info python3-debconf python3-debian python3-mako python3-markupsafe syslinux
  syslinux-common syslinux-legacy update-notifier-common usb-creator-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 433 not upgraded.
```

2. Check the chkrootkit documentation for instructions on how to run a scan to find system root kits.



3. Run chkrootkit (with sudo) in expert mode to verify the system does not have a root kit installed.



4. Provide a report from chkrootkit output on what more could be done to harden the system.