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 shadow
```

    b. Command to set permissions (if needed):

```
chmod 704 gshadow
```

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

    a. Command to inspect permissions:

```
ls -l gshadow
```

    b. Command to set permissions (if needed):

```
chmod 704 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 group
```

   b. Command to set permissions (if needed):

```
chmod 704 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 passwd
```

   b. Command to set permissions (if needed):

```
chmod 704 gshadow
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin1` with the `useradd` command.

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

```
Sudo useradd sam
Sudo useradd sara
Sudo useradd joe
Sudo useradd amy
Sudo useradd admin1
```

2. Ensure that only the `admin1` has general sudo access.

   a. 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.

    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 sara
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy


sudo usermod -aG manage joe
```

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

    a. Command to create the shared folder:

```
sudo mkdir/home/engineers
or
cd /home
Sudo mkdir 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 -R root:engineers engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
apt-get install lynis
```

2. Command to view documentation and instructions:

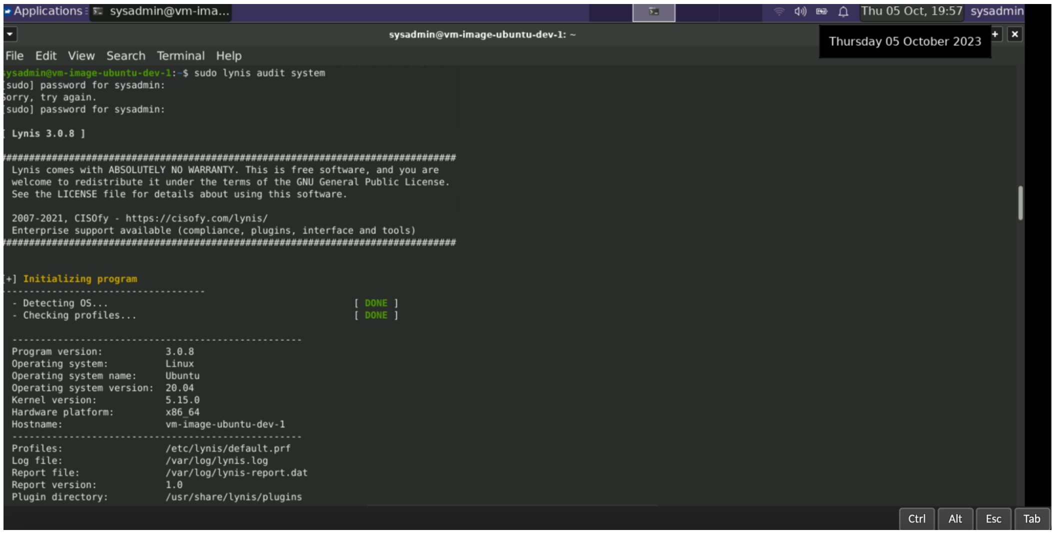
```
man lynis
```

3. Command to run an audit:

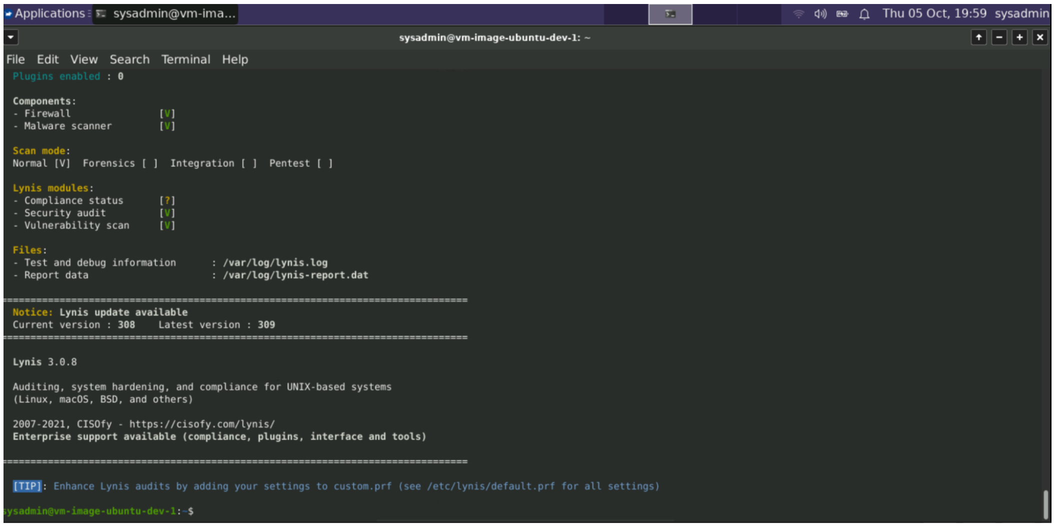
```
sudo lynis audit system
```

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

    a. Screenshot of report output:


Applications
sysadmin@vm-ima...
Thu 05 Oct, 19:57 sysadmin
sysadmin@vm-image-ubuntu-dev-1: ~
Thursday 05 October 2023
File Edit View Search Terminal Help
Ctrl Alt Esc Tab

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo lynis audit system
[sudo] password for sysadmin:
Sorry, try again.
[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:  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
```


Applications
sysadmin@vm-ima...
Thu 05 Oct, 19:59 sysadmin
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help

```
  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

================================================================================
  Notice: Lynis update available
  Current version : 308    Latest version : 309
================================================================================

  Lynis 3.0.8

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

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

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

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

sysadmin@vm-image-ubuntu-dev-1:~$
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
sudo chkrootkit
```

2. Command to view documentation and instructions:

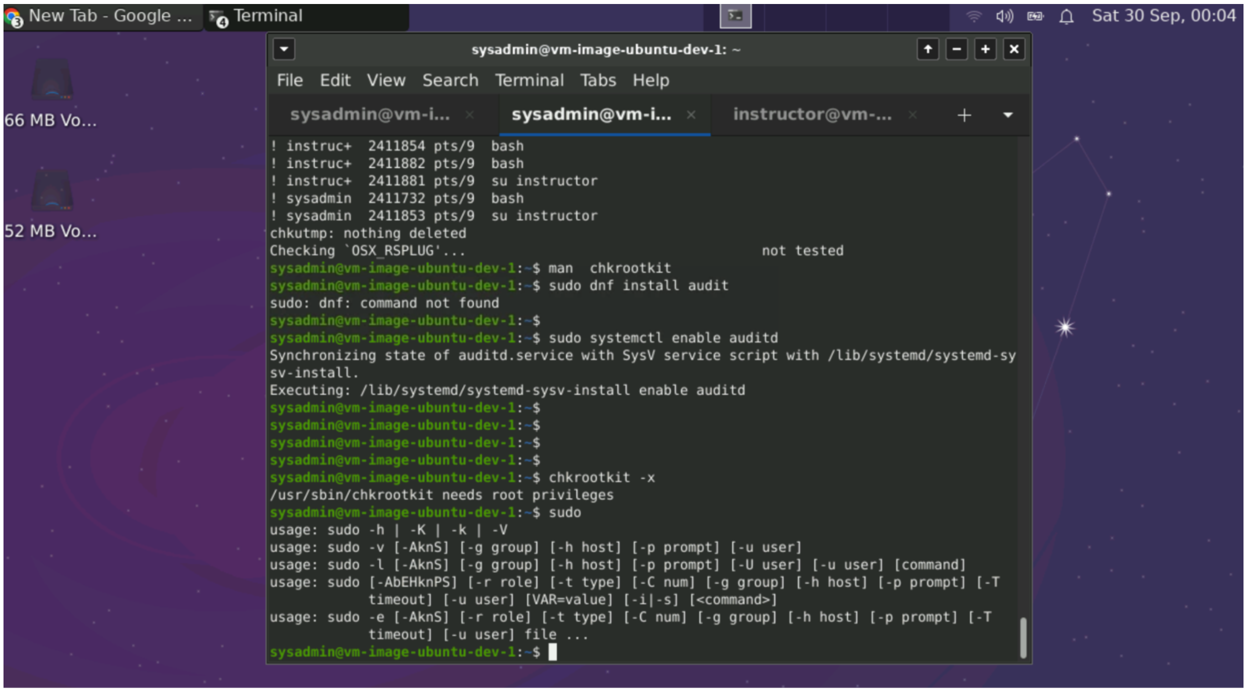
```
man chkrootkit
```

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:



```
! instruc+  2411854 pts/9  bash
! instruc+  2411882 pts/9  bash
! instruc+  2411881 pts/9  su instructor
! sysadmin  2411732 pts/9  bash
! sysadmin  2411853 pts/9  su instructor
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                    not tested
sysadmin@vm-image-ubuntu-dev-1:~$ man  chkrootkit
sysadmin@vm-image-ubuntu-dev-1:~$ sudo dnf install audit
sudo: dnf: command not found
sysadmin@vm-image-ubuntu-dev-1:~$
sysadmin@vm-image-ubuntu-dev-1:~$ sudo systemctl enable auditd
Synchronizing state of auditd.service with SysV service script with /lib/systemd/systemd-sy
sv-install.
Executing: /lib/systemd/systemd-sysv-install enable auditd
sysadmin@vm-image-ubuntu-dev-1:~$
sysadmin@vm-image-ubuntu-dev-1:~$
sysadmin@vm-image-ubuntu-dev-1:~$
sysadmin@vm-image-ubuntu-dev-1:~$
sysadmin@vm-image-ubuntu-dev-1:~$ chkrootkit -x
/usr/sbin/chkrootkit needs root privileges
sysadmin@vm-image-ubuntu-dev-1:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T
            timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T
            timeout] [-u user] file ...
sysadmin@vm-image-ubuntu-dev-1:~$
```