



# 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:

```
Is -l /etc/shadow
```

- b. Command to set permissions (if needed):

```
Sudo chown root: root /etc/shadow
```

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

```
Is -l /etc/gshadow
```

- b. Command to set permissions (if needed):

```
Sudo chown root: root /etc/gshadow  
Sudo chmod 644 /etc/gshadow
```

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

- a. Command to inspect permissions:

```
Is -l /etc/group
```

- b. Command to set permissions (if needed):

```
Sudo chown root: root /etc/group for assigning ownership and group to root only  
Sudo chmod 644 /etc/group
```

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

- a. Command to inspect permissions:

```
Is -l /etc/passwd
```

- b. 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 `Admin` with the `useradd` command.

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

```
Sudo adduser sam  
Sudo adduser joe  
Sudo adduser amy  
Sudo adduser sara
```

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

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

```
Sudo usermod -aG sudo admin
```

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

1. Add an `engineer's` 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 the `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:

```
Mkdir /home/engineers
```

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

- a. Command to change ownership of the engineers' shared folder to the `engineers` group:

```
Sudo chown: engineers
```

### Step 4: Lynis Auditing

1. Command to install Lynis:

```
Apt install lynis
```

2. Command to view documentation and instructions:

Man lynis

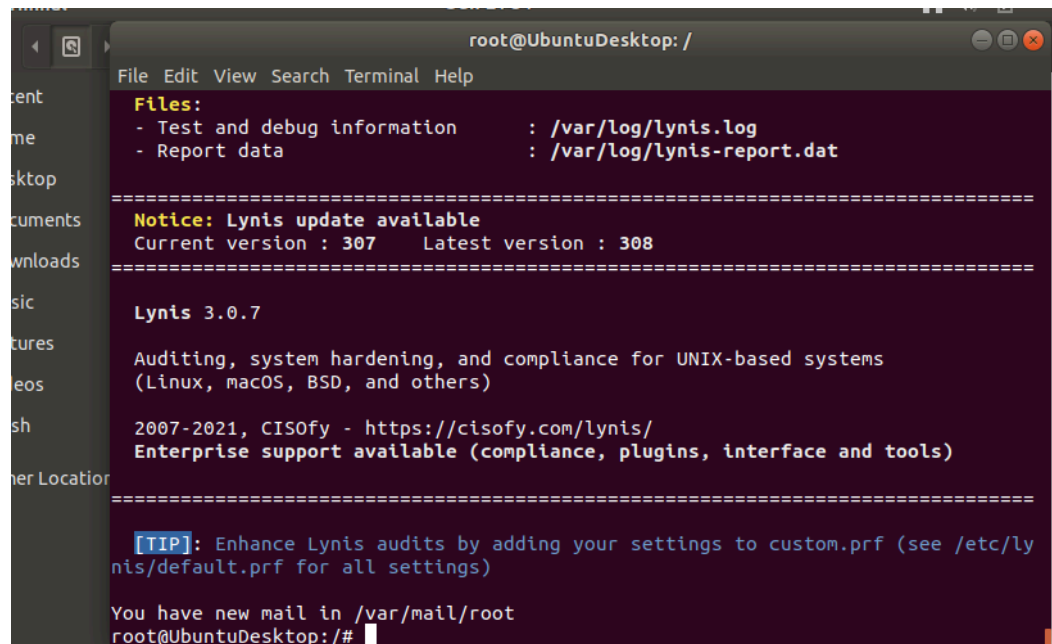
3. Command to run an audit:

Sudo lynis audit system

4. Provide a report from the Lynis output with recommendations for hardening the system. Install compiler(s). Install my antivirus scanner. Install a PAM module for password strength. Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft. Consider hardening the SSH configuration.

- a. Screenshot of report output:

C



```
root@UbuntuDesktop: /  
File Edit View Search Terminal Help  
Files:  
- Test and debug information      : /var/log/lynis.log  
- Report data                    : /var/log/lynis-report.dat  
=====
```

**Notice: Lynis update available**  
Current version : 307 Latest version : 308

=====

**Lynis 3.0.7**  
Auditing, system hardening, and compliance for UNIX-based systems  
(Linux, macOS, BSD, and others)  
2007-2021, CISOfy - <https://cisofy.com/lynis/>  
Enterprise support available (compliance, plugins, interface and tools)

=====

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

You have new mail in /var/mail/root  
root@UbuntuDesktop:/#

## Bonus

1. Command to install chkrootkit:

Apt install chkrootkit -y

2. Command to view documentation and instructions:

Man lynis

3. Command to run expert mode:

(x option) --

4. Provide a report from the chrootkit output with recommendations for hardening the system. The server needs to be patched, and as many layers of security as possible are necessary because the more layers there are, the better. Use reliable backups, like a tested backup that can be done in 3 different places. Take advantage of monitoring tools. Make use of third-party security tools.

a. Screenshot of end of sample output:

```
root@UbuntuDesktop: /
File Edit View Search Terminal Help
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
:
```

```
root@UbuntuDesktop: /
File Edit View Search Terminal Help

/usr/lib/debug/.build-id /usr/lib/python2.7/dist-packages/ansible/galaxy/data/co
ntainer/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/con
tainer/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/containe
r/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/.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
not tested
INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/rev_shell.sh
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/burpsuite_community_linux_v2022_1_1.sh
/tmp/a9xk.sh
```