



# 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):

```
sudo chown root:root /etc/shadow (for assigning ownership)  
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 gshadow
```

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

```
sudo chown root:root /etc/gshadow (for assigning ownership)  
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 group
```

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

```
sudo chown root:root /etc/passwd (for assigning ownership)
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 chown root:root /etc/passwd (for assigning ownership)
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.

- a. 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
```

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 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 engineers' shared folder to `engineers` group:

```
sudo chown :engineers engineers
```

### Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt install lynis
```

2. Command to view documentation and instructions:

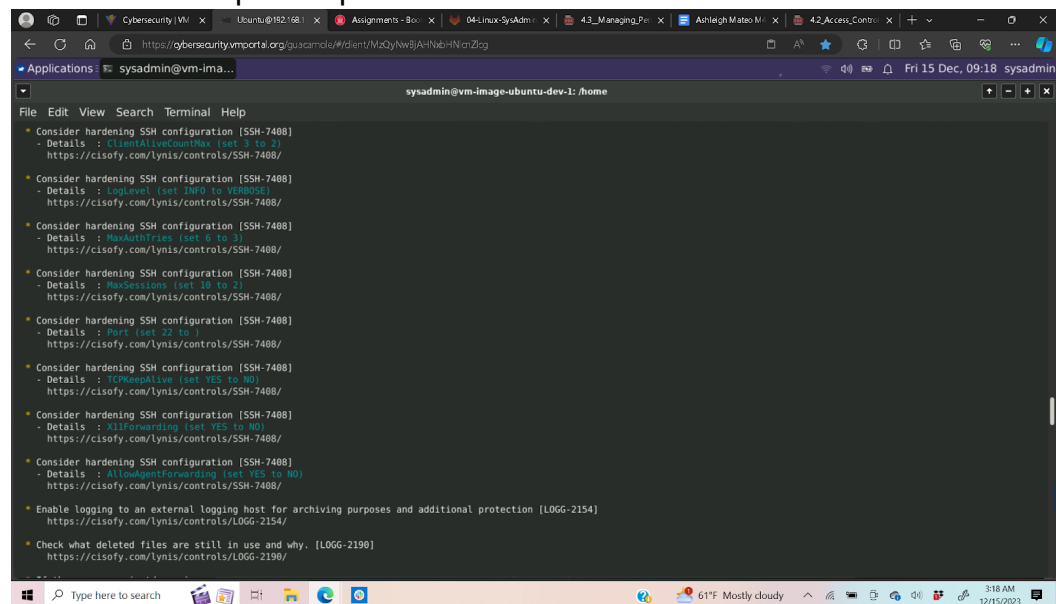
Man lynis

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:



## Optional Additional Challenge

1. Command to install chkrootkit:

```
Sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

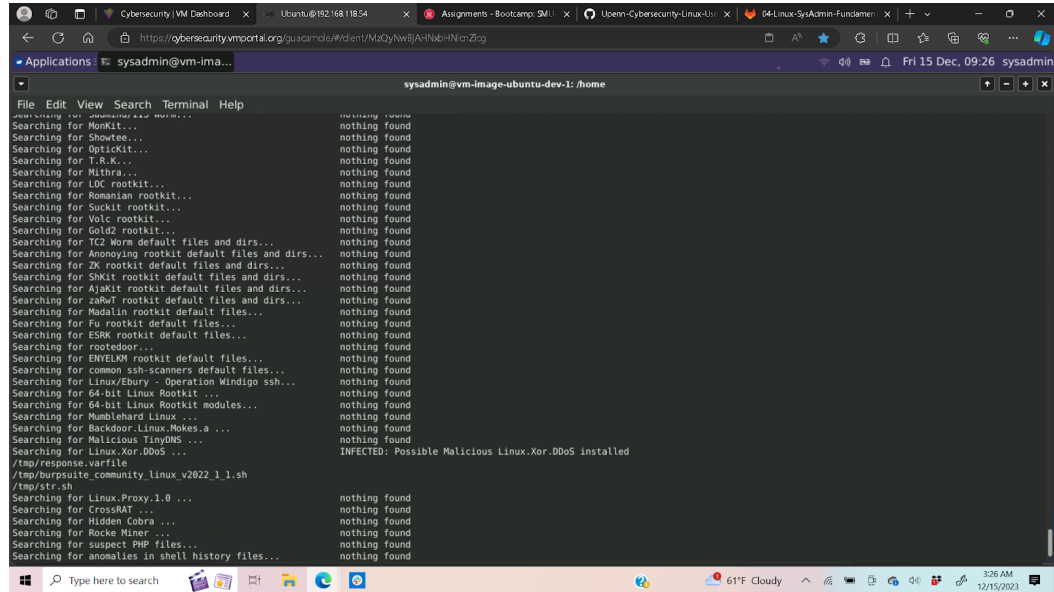
Man chkrootkit

3. Command to run expert mode:

Sudo chkrootkit

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

- a. Screenshot of end of sample output:



```
File Edit View Search Terminal Help
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OptiKit... 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 TIC Worm default files and dirs... nothing found
Searching for Annoying 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 zaRw 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 ESXi rootkit default files... nothing found
Searching for rootedoor... nothing found
Searching for ENYELM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for Linux/Ebury - Operation Windigo ssh... nothing found
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/response.varfile
/tmp/burpsuite_community_linux_v2022.1.1.sh
/tmp/str.sh
Searching for Linux.Proxy.1.0 ... nothing found
Searching for CrossRAT ... nothing found
Searching for Hidden Cobra ... nothing found
Searching for Rocke Miner ... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
```