Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
   - Command to inspect permissions:
     - **sudo ls -l /etc/shadow**
   - Command to set permissions (if needed):
     - **sudo chown root /etc/shadow**
     - **sudo chmod 600 /etc/shadow**

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
   - Command to inspect permissions:
     - **ls -l /etc/gshadow**
   - Command to set permissions (if needed):
     - **sudo chown root /etc/gshadow**
     - **sudo chmod 600 /etc/gshadow**
     - **sudo chgrp root /etc/gshadow**

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.
   - Command to inspect permissions:
     - **sudo ls -l /etc/group**
   - Command to set permissions (if needed):
     - **sudo chown root /etc/group**
     - **sudo chmod 644 /etc/group**

    - **sudo chgrp root /etc/group**

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions:
        - **sudo ls -l /etc/passwd**
    - Command to set permissions (if needed):
    - **sudo chown root /etc/passwd**
    - **sudo chmod 644 /etc/passwd**
    - **sudo chgrp root /etc/passwd**

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.
    - Command to add each user account (include all five users):
    - **sudo adduser --disabled-password --gecos "" sam**
    - **sudo adduser --disabled-password --gecos "" joe**
    - **sudo adduser --disabled-password --gecos "" amy**
    - **sudo adduser --disabled-password --gecos "" sara**
    - **sudo adduser --disabled-password --gecos "" admin**

2. Ensure that only the `admin` has general sudo access.
    - Command to add `admin` to the `sudo` group:
        - **sudo usermod -aG sudo admin**

Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.
   - Command to add group:
     - **sudo addgroup --system engineers**

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
   - 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`.
   - Command to create the shared folder:
     - **sudo mkdir /home/engineers**

4. Change ownership on the new engineers' shared folder to the `engineers` group.
   - Command to change ownership of engineer's shared folder to engineer group:
   - **sudo chgrp engineers /home/engineers**

Step 4: Lynis Auditing

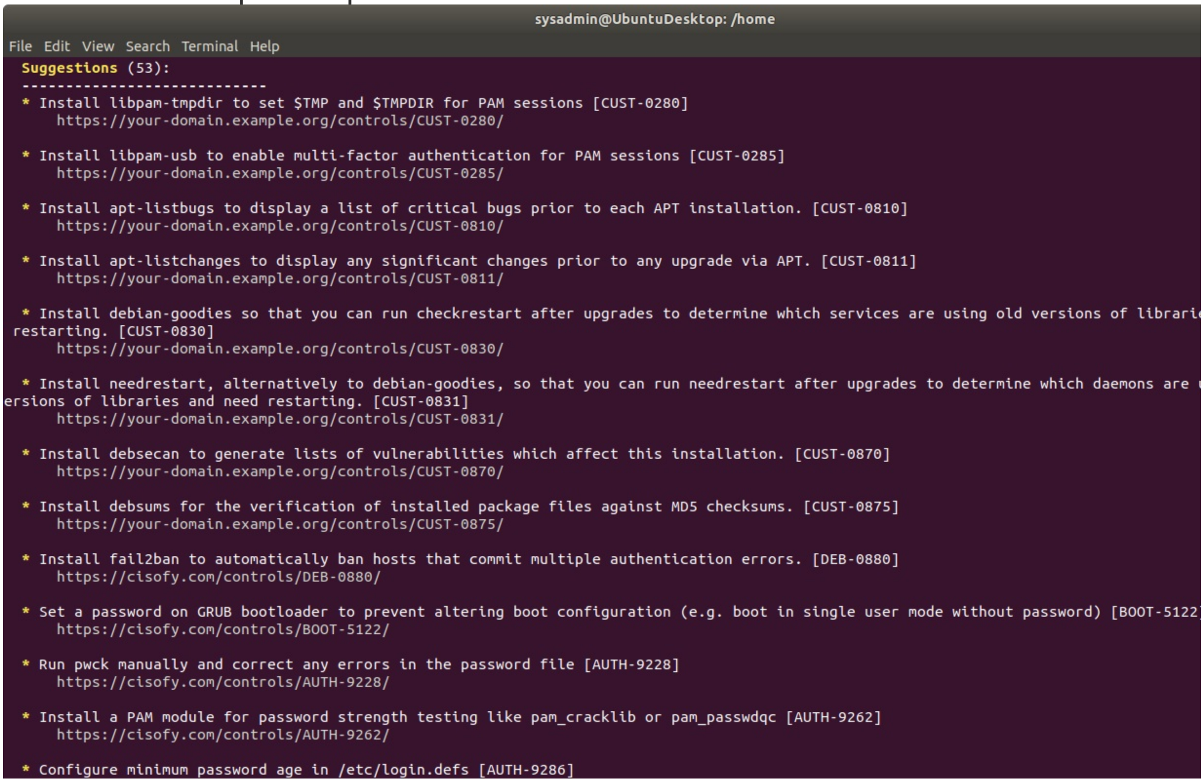
1. Command to install Lynis:
   sudo apt-get install lynis

2. Command to see documentation and instructions:
   sudo lynis --help

3. Command to run an audit:
   sudo lynis audit system

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

   - Screenshot of report output:


sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help

```
  Suggestions (53):
  ----------------------------
  * 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 librari
 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 are 
ersions 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/

  * Run pwck manually and correct any errors in the password file [AUTH-9228]
      https://cisofy.com/controls/AUTH-9228/

  * 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]
```

Bonus

1. Command to install chkrootkit:

   sudo apt install chkrootkit

2. Command to see documentation and instructions:

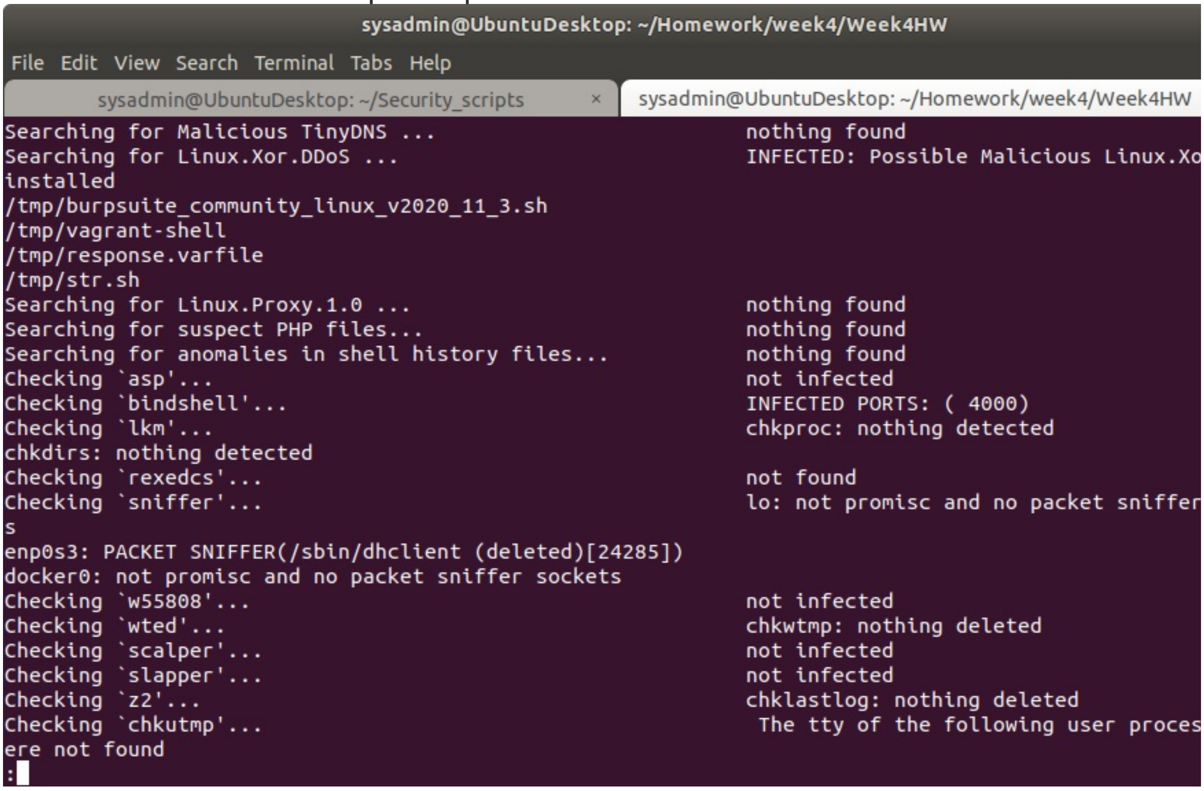
   sudo chkrootkit --help

3. Command to run expert mode:

   sudo chkrootkit -x

4. Provide a report from the chrootkit output on what can be done to harden the system.

- Screenshot of end of sample output:



sysadmin@UbuntuDesktop: ~/Homework/week4/Week4HW
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~/Security_scripts
sysadmin@UbuntuDesktop: ~/Homework/week4/Week4HW

```
Searching for Malicious TinyDNS ...                         nothing found
Searching for Linux.Xor.DDoS ...                            INFECTED: Possible Malicious Linux.Xo
installed
/tmp/burpsuite_community_linux_v2020_11_3.sh
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/str.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'...                                     INFECTED PORTS: ( 4000)
Checking `lkm'...                                           chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer
s
enp0s3: PACKET SNIFFER(/sbin/dhclient (deleted)[24285])
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 proces
ere not found
:
```

-