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: ls -l /etc/shadow
    - Command to set permissions (if needed): 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 chmod 600 /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: ls -l /etc/group
    - Command to set permissions (if needed): sudo chmod 644 /etc/group
4. Permissions on `/etc/passwd` a allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions: ls -l /etc/passwd
    - Command to set permissions (if needed): sudo chmod 644 /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):
        1. sudo useradd sam
        2. sudo useradd joe
        3. sudo useradd amy
        4. sudo useradd sara
        5. sudo useradd admin
2. Ensure that only the `admin` has general sudo access.
    - Command to add `admin` to the `sudo` group:
        1. sudo usermod -G sudo admin

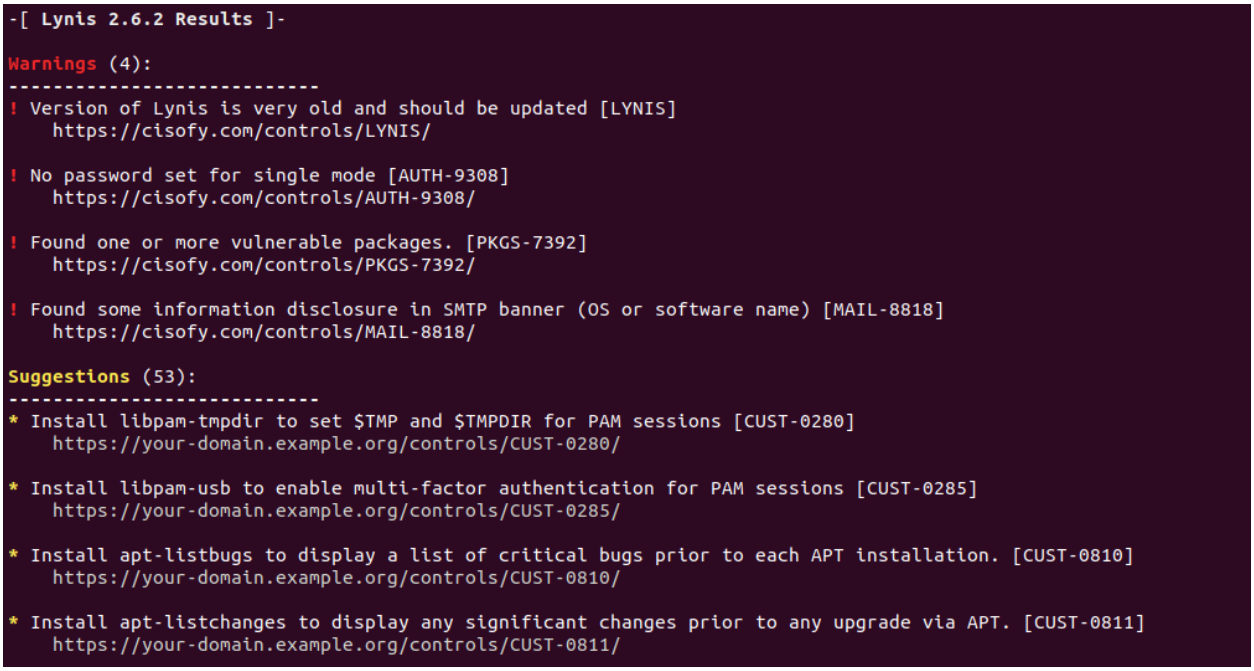
Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.
    - Command to add group:
        1. sudo addgroup engineers
2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
    - Command to add users to `engineers` group (include all four users):
        1. sudo usermod -G engineers sam
        2. sudo usermod -G engineers joe
        3. sudo usermod -G engineers amy
        4. sudo usermod -G 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 chown :engineers /home/engineers

Step 4: Lynis Auditing

1. Command to install Lynis: sudo apt install Lynis
2. Command to see documentation and instructions: man lynis
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:



```
  * 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-5
122]
      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/

* Check 9 files in /tmp which are older than 90 days [FILE-6354]
    https://cisofy.com/controls/FILE-6354/

* 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 (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron
jobs and startup 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)

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

Lynis security scan details:

Hardening index : 57 [###########         ]
Tests performed : 240
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [V]

Lynis Modules:
- Compliance Status      [?]
```

```
 - Security Audit            [V]
 - Vulnerability Scan        [V]
 Help
 Files:
 - Test and debug information      : /var/log/lynis.log
 - Report data                     : /var/log/lynis-report.dat

================================================================================
 Notice: Lynis update available
 Current version : 262    Latest version : 306
================================================================================

 Lynis 2.6.2

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

 2007-2018, 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@UbuntuDesktop:/etc$
```

Bonus

1. Command to install chkrootkit: sudo apt install chkrootkit
2. Command to see documentation and instructions: man chkrootkit
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:

It appears that nothing needs to be done to harden the system based on the data generated by running sudo chkrootkit -x.

```
! root        13611 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        14049 pts/0  ./chkutmp
! root        14051 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        14050 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        13610 pts/0  sudo chkrootkit -x
! sysadmin     3928 pts/0  bash
chkutmp: nothing deleted
not tested
```