

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`

`-rw----- 1 root shadow 3428 Oct 17 22:41 /etc/shadow`
 - Command to set permissions (if needed): `was not needed`
2. Permissions on /etc/gshadow should allow only root read and write access.
 - Command to inspect permissions:
`ls -l /etc/gshadow`

`-rw----- 1 root shadow 1173 Oct 17 22:41 /etc/gshadow`
 - Command to set permissions (if needed): `was not needed`
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`

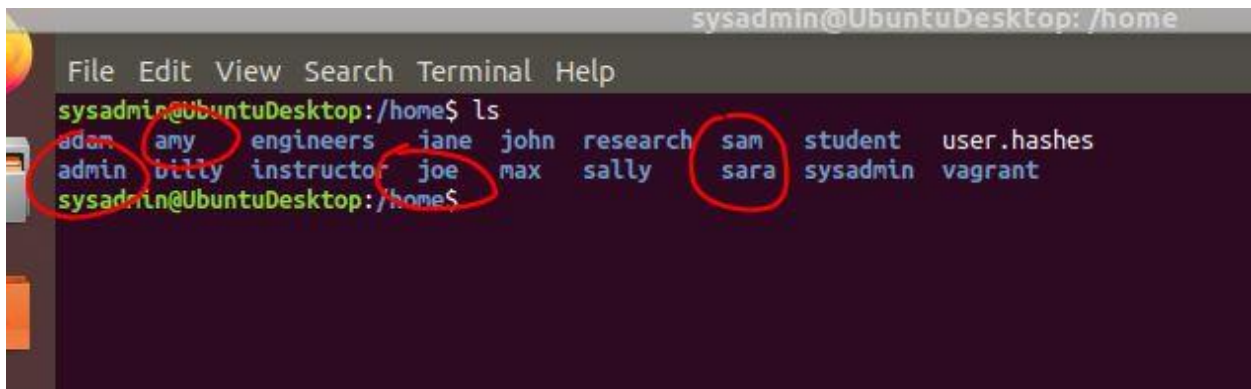
`-rw-r--r-- 1 root root 1422 Oct 17 22:41 /etc/group`
 - Command to set permissions (if needed): `was not needed`
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
 - Command to inspect permissions:
`ls -l /etc/passwd`

`-rw-r--r-- 1 root root 3456 Oct 17 22:41 /etc/passwd`
 - Command to set permissions (if needed): `was not needed`

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):
2. Ensure that only the admin has general sudo access.
 - Command to add admin to the sudo group

`sudo usermod -aG sudo admin`

A terminal window titled 'sysadmin@UbuntuDesktop: /home' showing the output of the 'ls' command. The output lists several files and directories: 'adam', 'amy', 'engineers', 'iane', 'john', 'research', 'sam', 'student', and 'user.hashes' on the first line; 'admin', 'billy', 'instructor', 'joe', 'max', 'sally', 'sara', 'sysadmin', and 'vagrant' on the second line. Red circles are drawn around the words 'adam', 'amy', 'engineers', 'joe', 'max', 'sally', 'sara', and 'sysadmin' in the terminal output.

```
sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/home$ ls
adam amy engineers iane john research sam student user.hashes
admin billy instructor joe max sally sara sysadmin vagrant
sysadmin@UbuntuDesktop:/home$
```

Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.
 - Command to add group:
2. Add users sam, joe, amy, and sara to the managed group.
 - Command to add users to engineers group (include all four users):

`sudo groupadd engineers`

`sudo usermod -aG engineers amy`

`sudo usermod -aG engineers sara`

`sudo usermod -aG engineers sam`

`sudo usermod -aG engineers joe`

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

```
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/home$ ls
adam amy engineers jane john research sam student user.hashes
admin billy instructor joe max sally sara sysadmin vagrant
sysadmin@UbuntuDesktop:/home$ groups sam joe amy sara admin
sam : sam engineers
joe : joe engineers
amy : amy engineers
sara : sara engineers
admin : admin sudo
sysadmin@UbuntuDesktop:/home$
```

- Command to create the shared folder:

`sudo mkdir -p /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/`

```
sysadmin@UbuntuDesktop:/home$ ls -l
total 72
drwxr-xr-x 8 joe adam 4096 May 14 16:29 adam
drwxr-xr-x 8 admin admin 4096 Oct 5 21:16 admin
drwxr-xr-x 8 amy amy 4096 Oct 5 21:15 amy
drwxr-xr-x 8 billy billy 4096 May 14 16:29 billy
drwxr-xr-x 2 root engineers 4096 Oct 5 21:39 engineers
drwxr-xr-x 9 instructor instructor 4096 May 14 16:36 instructor
drwxr-xr-x 8 jane jane 4096 May 14 16:31 jane
drwxr-xr-x 8 joe joe 4096 Oct 5 21:15 joe
drwxr-xr-x 8 john john 4096 May 14 16:29 john
drwxr-xr-x 9 max max 4096 Oct 2 11:35 max
drwxr-xr-x 2 sysadmin sysadmin 4096 Oct 2 13:01 research
drwxr-xr-x 8 sally sally 4096 May 14 16:29 sally
drwxr-xr-x 8 sam sam 4096 Oct 5 21:12 sam
drwxr-xr-x 8 sara sara 4096 Oct 5 21:16 sara
drwxr-xr-x 8 student student 4096 May 14 16:24 student
drwxr-xr-x 21 sysadmin sysadmin 4096 Oct 9 12:36 sysadmin
-rw-r--r-- 1 root root 1581 May 14 16:29 user.hashes
drwxr-xr-x 10 vagrant vagrant 4096 May 14 16:41 vagrant
sysadmin@UbuntuDesktop:/home$
```

Step 4: Lynis Auditing

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

```
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 libraries 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 are 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://ciscofy.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://ciscofy.com/controls/BOOT-5122/

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

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
  https://ciscofy.com/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
  https://ciscofy.com/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
  https://ciscofy.com/controls/AUTH-9286/

* Set password for single user mode to minimize physical access attack surface [AUTH-9308]
  https://ciscofy.com/controls/AUTH-9308/
```

```
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
  https://ciscofy.com/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]
  https://ciscofy.com/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]
  https://ciscofy.com/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]
  https://ciscofy.com/controls/FILE-6310/

* Check 6 files in /tmp which are older than 90 days [FILE-6354]
  https://ciscofy.com/controls/FILE-6354/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
  https://ciscofy.com/controls/STRG-1840/

* Check DNS configuration for the dns domain name [NAME-4028]
  https://ciscofy.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://ciscofy.com/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
  https://ciscofy.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://ciscofy.com/controls/PKGS-7392/

* Install package apt-show-versions for patch management purposes [PKGS-7394]
  https://ciscofy.com/controls/PKGS-7394/

* Consider running ARP monitoring software (arpwatch, arpon) [NETW-3032]
  https://ciscofy.com/controls/NETW-3032/

* Access to CUPS configuration could be more strict. [PRNT-2307]
  https://ciscofy.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://ciscofy.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://ciscofy.com/controls/MAIL-8820/
```

```

* Check iptables rules to see which rules are currently not used [FIRE-4513]
  https://cisoфы.com/controls/FIRE-4513/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
  https://cisoфы.com/controls/HTTP-6640/

* Install Apache mod_security to guard webserver against web application attacks [HTTP-6643]
  https://cisoфы.com/controls/HTTP-6643/

* Consider hardening SSH configuration [SSH-7408]
  - Details : AllowTcpForwarding (YES --> NO)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : ClientAliveCountMax (3 --> 2)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : Compression (YES --> (DELAYED)NO))
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : LogLevel (INFO --> VERBOSE)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : MaxAuthTries (6 --> 2)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : MaxSessions (10 --> 2)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : PermitRootLogin (WITHOUT-PASSWORD --> NO)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : Port (22 --> )
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : TCPKeepAlive (YES --> NO)
    https://cisoфы.com/controls/SSH-7408/

```

```

* Consider hardening SSH configuration [SSH-7408]
  - Details : X11Forwarding (YES --> NO)
    https://cisoфы.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : AllowAgentForwarding (YES --> NO)
    https://cisoфы.com/controls/SSH-7408/

* Check what deleted files are still in use and why. [LOGG-2190]
  https://cisoфы.com/controls/LOGG-2190/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
  https://cisoфы.com/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
  https://cisoфы.com/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
  https://cisoфы.com/controls/ACCT-9622/

* Enable sysstat to collect accounting (no results) [ACCT-9626]
  https://cisoфы.com/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
  https://cisoфы.com/controls/ACCT-9628/

* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
  https://cisoфы.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://cisoфы.com/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
  https://cisoфы.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://cisoфы.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

```

```

Lynis security scan details:

Hardening Index : 56 [#####          ]
Tests performed : 232
Plugins enabled : 1

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

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 : 262 Latest version : 306
=====

Lynis 2.6.2

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

2007-2018, CISOфы - https://cisoфы.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)

```

Bonus

1. Command to install chkrootkit: `sudo apt-get install chkrootkit -y`
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: /home
File Edit View Search Terminal Help
! gdm          2044 tty1   ibus-daemon --xim --panel disable
! gdm          2047 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2218 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2051 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     8451 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthorit
y -background none -noreset -keeptty -verbose 3
! sysadmin     8449 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=
ubuntu gnome-session --session=ubuntu
! sysadmin     8472 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     8646 tty2   /usr/bin/gnome-shell
! sysadmin     9104 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     8807 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     8809 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     8801 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     8814 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     8889 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     8815 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     8822 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     8828 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     8767 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     8768 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     8772 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     8858 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     8773 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     8776 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     8778 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     8785 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     8789 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     8791 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     8794 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     8680 tty2   ibus-daemon --xim --panel disable
! sysadmin     8684 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     8976 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     8686 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     8887 tty2   nautilus-desktop
! root         18149 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root         18582 pts/0  ./chkutmp
! root         18584 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root         18583 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         18148 pts/0  sudo chkrootkit -x
! sysadmin     9183 pts/0  bash
chkutmp: nothing deleted
not tested

```