

Week 4 Homework Submission File: Linux Systems Administration

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

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 shadow`
 - Command to set permissions (if needed): `sudo chmod 600 shadow`
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
 - Command to inspect permissions: `ls -l gshadow`
 - Command to set permissions (if needed): `sudo chmod 600 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 group`
 - Command to set permissions (if needed): `sudo chmod 644 group`
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 passwd`
 - Command to set permissions (if needed): `sudo chmod 644 passwd`

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.

Frank Lin - Unit 4 Homework - Linux Systems Administration

- Command to add each user account (include all five users): `sudo adduser sam`

`sudo adduser joe` `sudo adduser amy` `sudo adduser sara` `sudo adduser admin`

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

`sudo -lU admin`

- Command to add `admin` to the `sudo` group: `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: `sudo addgroup engineers`

`sudo usermod -G engineers sam`

`sudo usermod -G engineers joe`

`sudo usermod -G engineers amy`

`sudo usermod -G engineers sara`

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

- Command to add users to `engineers` group (include all four users)

*add option “a” to append user to the group vs change them to only the “engineers” group without changing their current one(s)

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

- 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 -R engineers /home/engineers` or `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` or `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: *See additional pages at the end...

Bonus

1. Command to install chkrootkit: `sudo apt install chkrootkit`

2. Command to see documentation and instructions: `man chkrootkit` or

`sudo chkrootkit --help`

3. Command to run expert mode:

`sudo chkrootkit -x [test ...]`

Frank Lin - Unit 4 Homework - Linux Systems Adminstration

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

- Screenshot of end of sample output:

```
sysadmin@ubuntuucb:~$ sudo chkrootkit -x | tail
/usr/sbin/chkrootkit: 608: /usr/sbin/chkrootkit: exportmode_output: not found
/usr/sbin/chkrootkit: 609: /usr/sbin/chkrootkit: exportmode_output: not found
! root      27427 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root      26989 pts/0  sudo chkrootkit -x
! sysadmin   3238 pts/0  bash
! sysadmin   8222 pts/0  bash
! sysadmin   7690 pts/0  su admin
! sysadmin   26990 pts/0  tail
! sysadmin   5381 pts/1  bash
! sysadmin   6049 pts/2  bash
chkutmp: nothing deleted
not tested
sysadmin@ubuntuucb:~$
```

*Alternatively, rkhunter could also be used for checking for rootkits

```
sudo rkhunter --check
```

```
sysadmin@ubuntuucb:~$ sudo rkhunter --check
[sudo] password for sysadmin:
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
  Checking for prerequisites [ OK ]
    /usr/sbin/adduser [ OK ]
    /usr/sbin/chroot [ OK ]

System checks summary
=====
File properties checks...
  Files checked: 152
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 500
  Possible rootkits: 10

Applications checks...
  All checks skipped

The system checks took: 3 minutes and 12 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

sysadmin@ubuntuucb:~$
```

Lynis Output Screenshots:

```
sysadmin@ubuntuucb: ~
=====
-[ Lynis 2.6.2 Results ]-
=====
Warnings (5):
-----
! Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/
!
! Multiple users with UID 0 found in passwd file [AUTH-9204]
  https://cisofy.com/controls/AUTH-9204/
!
! Multiple accounts found with same UID [AUTH-9208]
  https://cisofy.com/controls/AUTH-9208/
!
! No password set for single mode [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/
!
! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
  https://cisofy.com/controls/MAIL-8818/
!

Suggestions (52):
-----
* 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://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/
```

```
sysadmin@ubuntu: ~
File Edit View Search Terminal Help
https://ciscofy.com/controls/DEB-0000/
* 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/
* Install a PAM module for password strength testing like pam_cracklib or pam_passewdqc [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)
* 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/
* Add the IP name and FQDN to /etc/hosts for proper name resolving [NAME-4404]
  https://ciscofy.com/controls/NAME-4404/
* Purge old/removed packages (7 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/
* 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 config file (/etc/postfix/main.cf) [MAIL-0019]
```

```
sysadmin@ubuntuucb: ~
File Edit View Search Terminal Help

* 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/
```

```
sysadmin@ubuntuubc: ~
File Edit View Search Terminal Help
* 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 : 60 [#####
] Tests performed : 241 Plugins enabled : 1

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

```
sysadmin@ubuntuuucb: ~
File Edit View Search Terminal Help
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 [KRLN-6000]
  - Solution : Change sysctl value or disable test (skip-test=KRLN-6000:<sysctl-key>)
    https://cisofy.com/controls/KRLN-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 : 60 [#####
] Tests performed : 241 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, 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@ubuntuuucb:~$
```