Cybersecurity

10.1 Project 1 Day 1 Activity Guide

Today's focus is on the **BSC's** Linux server's users, groups, files, and directories. You will be completing 5 steps:

- **(1)** Pre-hardening steps: System inventory and backup
- **(2)** Auditing users and groups
- **(3)** Updating and enforcing password policies
- **(4)** Updating and enforcing sudo permissions
- **(5)** Validating and updating permissions on files and directories.

Project 1 - Day 1
Hardening Script

Savannah Carr

*gpt/deepseek were used in the research for this project

```
root@a2e566cabe19:/# hostname
a2e566cabe19
root@a2e566cabe19:/# cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.5 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.5 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
root@a2e566cabe19:/# free -m
               total        used        free      shared  buff/cache   available
Mem:           15548        1045       13179           3        1323       14222
Swap:           4096           0        4096
root@a2e566cabe19:/# uptime
 23:52:37 up 11 min,  0 users,  load average: 0.00, 0.02, 0.00
```

- Collect and document the following information on the summary report.
  - HostName
  - OS version
  - Memory information
  - Uptime information

Hostname is different from the original “baker_street due to having to run docker instance through docker desktop*

Now backup the OS with the following command(note the directories being excluded):

- *sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /*

sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /

```
tar: /: file changed as we read it
root@a2e566cabe19:/#
```

The command creates a compressed archive (`baker_street_backup.tar.gz`) of the entire filesystem (`/`), but it **excludes** certain directories like `/proc`, `/tmp`, `/mnt`, `/sys`, `/dev`, `/run`, and the backup file itself (`/baker_street_backup.tar.gz`). The `-cvpzf` flags ensure that the backup is created in verbose mode, preserving file permissions, and compressed with gzip.

cat /etc/passwd

```
sherlock:x:1000:1000::/home/sherlock:/bin/bash
watson:x:1001:1001::/home/watson:/bin/bash
moriarty:x:1002:1002::/home/moriarty:/bin/bash
mycroft:x:1003:1003::/home/mycroft:/bin/bash
irene:x:1004:1004::/home/irene:/bin/bash
lestrade:x:1005:1005::/home/lestrade:/bin/bash
mrs_hudson:x:1006:1006::/home/mrs_hudson:/bin/bash
mary:x:1007:1007::/home/mary:/bin/bash
sysadmin:x:1008:1008::/home/sysadmin:/bin/bash
gregson:x:1009:1009::/home/gregson:/bin/bash
toby:x:1010:1010::/home/toby:/bin/bash
adler:x:1011:1011::/home/adler:/bin/bash
```

sudo deluser --remove-all-files username
sudo rm -rf /home/username

```
Removing files ...
Removing user `lestrade' ...
Warning: group `lestrade' has no more members.
Done.
Removing files ...
Removing user `irene' ...
Warning: group `irene' has no more members.
Done.
Removing files ...
Removing user `gregson' ...
Warning: group `gregson' has no more members.
Done.
Removing files ...
Removing user `mary' ...
Warning: group `mary' has no more members.
Done.
```

cat /etc/shadow

! = indicates locked accounts

```
sherlock:$y$j9T$btks8gyDy.qXjaumojpYj/$yumzEF9HUN0wMB6YPprnRRtzkFZnVTf1y0srzEpATCB:20122:0:99999:7:::
watson:$y$j9T$0vXpS1aedO4ZX5f7s7THb0$OKOP3zOyAWF8tGGfVe7yvxW6CSkmWbdUVH3nOoTdEX3:20122:0:99999:7:::
moriarty:!$y$j9T$pDNCJKTf3Oyz.frx7BgXr.$u1ZS56iM95E7p6lHqVOVzc.amccWlaMvjGEwvolRXK4:20122:0:99999:7:::
mycroft:$y$j9T$osxOVxUsaiAO6.S.cdArR0$e.g8sgLwmR3MNiaP.bMPqb9t7xx1KYsaUlObSdU0aP6:20122:0:99999:7:::
mrs_hudson:!:20069:0:99999:7:::
mary:!:20069:0:99999:7:::
sysadmin:!:20069:0:99999:7:::
toby:!:20069:0:99999:7:::
adler:!:20069:0:99999:7:::
```

sudo passwd -l username (to lock user)

```
root@a2e566cabe19:/# sudo passwd -l moriarty
passwd: password expiry information changed.
root@a2e566cabe19:/# sudo passwd -l mrs_hudson
passwd: password expiry information changed.
```

sudo passwd -u username (to unlock user)

```
root@a2e566cabe19:/# sudo passwd -u toby
passwd: password expiry information changed.
root@a2e566cabe19:/# sudo passwd -u adler
passwd: password expiry information changed.
```

sudo passwd username

```
root@a2e566cabe19:/# sudo passwd toby
New password:
Retype new password:
passwd: password updated successfully
```

```
root@a2e566cabe19:/# sudo passwd adler
New password:
Retype new password:
passwd: password updated successfully
```

*No users in the marketing group
therefore no users to add to research,
was told to ignore*

groupdel marketing
groupadd research

cat /etc/group

```
engineering:x:1012:sherlock,watson,moriarty
finance:x:1013:mrs_hudson
marketing:x:1014:
```

```
engineering:x:1012:sherlock,watson,moriarty
finance:x:1013:mrs_hudson
research:x:1014:
```

```
 GNU nano 6.2
#
# /etc/pam.d/common-password - password-related modules common to all service
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

cat /etc/pam.d/common-password

Update the password requirements for all users to have:

- Minimum 8 characters
- At least one special character
- Allow 2 retries
- At least one uppercase character

```
# and here are more per-package modules (the "Additional" block)
password requisite pam_pwquality.so minlen=8 retry=2 ocredit=-1 ucredit=-1
# end of pam-auth-update config
```

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

#Allow sherlock full sudo priveleges
sherlock ALL=(ALL) NOPASSWD:ALL

#Allow watson and mycroft to run /var/log/logcleanup.sh with sudo
watson ALL=(ALL) NOPASSWD: /var/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /var/logcleanup.sh

#Allow members of the research group to run /tmp/scripts/research_script.sh with sudo
%research ALL=(ALL:ALL) NOPASSWD: /tmp/scripts/research_script.sh
```

```
root@a2e566cabe19:/# sudo usermod -aG sudo sherlock
root@a2e566cabe19:/# groups sherlock
sherlock : sherlock sudo engineering
```

The only employee who should have **full sudo privileges** is Sherlock. Remove all other full privileged users.
Watson and Mycroft should only have sudo privileges to run a script located here:

- /var/log/logcleanup.sh

All employees who belong to the **research** group should have sudo privileges to run the following script:

- /tmp/scripts/research_script.sh

```
root@a2e566cabe19:/home/watson# ls -lah
total 36K
drwxr-x--- 1 watson watson  4.0K Dec 12 07:45 .
drwxr-xr-x 1 root   root    4.0K Feb  8 18:43 ..
-rw-r----- 1 watson watson   220 Jan  6  2022 .bash_logout
-rw-r----- 1 watson watson  3.7K Jan  6  2022 .bashrc
-rw-r----- 1 watson watson   807 Jan  6  2022 .profile
-rwxrwx--- 1 root   finance    0 Dec 12 07:45 Finance_script.sh_3.txt
-rwxrwx--- 1 root   finance   47 Dec 12 07:45 Finance_script.sh_script1.sh
-rwxrwx--- 1 root   finance   47 Dec 12 07:45 Finance_script.sh_script2.sh
-rw-r----- 1 root   root       0 Dec 12 07:45 deduction.doc_0.txt
-rw-r----- 1 root   root       0 Dec 12 07:45 deduction.doc_1.txt
-rw-r----- 1 root   root       0 Dec 12 07:45 deduction.doc_2.txt
-rw-r----- 1 root   root       0 Dec 12 07:45 my_file.txt
```

Sudo find /home -type f -iname “*engineering*” -exec chgrp engineering {} \; -exec chmod 770 {} \;

Sudo find /home -type f -iname “*research*” -exec chgrp research {} \; -exec chmod 770 {} \;

Sudo find /home -type f -iname “*finance*” -exec chgrp finance {} \; -exec chmod 770 {} \;

Some employees may leave files with hidden passwords. Find those files and remove them as no employee should have their passwords stored on the server

find /home/* -type f \(-iname "*password*" -o -iname "*passwd*" -o -iname "*secret*" \) -exec rm -f {} +

In every user’s home directory, there should be **no files** that have any world permissions to read, write, or execute.

- Find any of them and update to remove the world permissions.

find /home -type f -perm /o=rwx -exec chmod o-rwx {} +

```
root@a2e566cabe19:/home/adler# ls -lah
total 36K
drwxr-x--- 1 adler adler       4.0K Dec 12 07:45 .
drwxr-xr-x 1 root  root        4.0K Feb  8 18:43 ..
-rw-r----- 1 adler adler        220 Jan  6  2022 .bash_logout
-rw-r----- 1 adler adler       3.7K Jan  6  2022 .bashrc
-rw-r----- 1 adler adler        807 Jan  6  2022 .profile
-rwxrwx--- 1 root  engineering    0 Dec 12 07:45 Engineering_script.sh_0.txt
-rwxrwx--- 1 root  engineering    0 Dec 12 07:45 Engineering_script.sh_3.txt
-rwxrwx--- 1 root  engineering   46 Dec 12 07:45 Engineering_script.sh_script1.sh
-rwxrwx--- 1 root  engineering   46 Dec 12 07:45 Engineering_script.sh_script2.sh
-rw-r----- 1 root  root           0 Dec 12 07:45 deduction.doc_2.txt
-rw-r----- 1 root  root           0 Dec 12 07:45 game_is_afoot.txt_1.txt
root@a2e566cabe19:/home/moriarty# ls -lah
total 36K
drwxr-x--- 1 moriarty moriarty 4.0K Dec 12 07:45 .
drwxr-xr-x 1 root     root     4.0K Feb  8 18:43 ..
-rw-r----- 1 moriarty moriarty  220 Jan  6  2022 .bash_logout
-rw-r----- 1 moriarty moriarty 3.7K Jan  6  2022 .bashrc
-rw-r----- 1 moriarty moriarty  807 Jan  6  2022 .profile
-rwxrwx--- 1 root     finance     0 Dec 12 07:45 Finance_script.sh_0.txt
-rwxrwx--- 1 root     finance     0 Dec 12 07:45 Finance_script.sh_2.txt
-rw-r----- 1 root     root        0 Dec 12 07:45 elementary.txt_1.txt
-rw-r----- 1 root     root        0 Dec 12 07:45 game_is_afoot.txt_3.txt
-rwxr-x--- 1 root     root       49 Dec 12 07:45 game_is_afoot.txt_script1.sh
-rwxr-x--- 1 root     root       49 Dec 12 07:45 game_is_afoot.txt_script2.sh
-rw-r----- 1 root     root        0 Dec 12 07:45 my_file.txt
```

In every user's home directory, there should be **no files** that have any world permissions to read, write, or execute.

- Find any of them and update to remove the world permissions.

Find the following files and make the associated updates:

(**Hint:** Search with the case-insensitive option.)

- **Engineering scripts (scripts with the word 'engineering' in the filename):** Only members of the engineering group can view, edit, or execute.
- **Research scripts:** Only members of the research group can view, edit, or execute.
- **Finance scripts:** Only members of the finance group can view, edit, or execute.

Some employees may leave files with hidden passwords. Find those files and remove them as no employee should have their passwords stored on the server.

```
root@a2e566cabe19:/home/mrs_hudson# ls -lah
total 36K
drwxr-x--- 1 mrs_hudson mrs_hudson  4.0K Dec 12 07:45 .
drwxr-xr-x 1 root       root        4.0K Feb  8 18:43 ..
-rw-r----- 1 mrs_hudson mrs_hudson   220 Jan  6  2022 .bash_logout
-rw-r----- 1 mrs_hudson mrs_hudson  3.7K Jan  6  2022 .bashrc
-rw-r----- 1 mrs_hudson mrs_hudson   807 Jan  6  2022 .profile
-rwxrwx--- 1 root       engineering    0 Dec 12 07:45 Engineering_script.sh_1.txt
-rw-r----- 1 root       root           0 Dec 12 07:45 deduction.doc_0.txt
-rw-r----- 1 root       root           0 Dec 12 07:45 deduction.doc_2.txt
-rw-r----- 1 root       root           0 Dec 12 07:45 elementary.txt_3.txt
-rwxr-x--- 1 root       root          51 Dec 12 07:45 elementary.txt_script1.sh
-rwxr-x--- 1 root       root          51 Dec 12 07:45 elementary.txt_script2.sh
root@a2e566cabe19:/home/mycroft# ls -lah
total 36K
drwxr-x--- 1 mycroft mycroft     4.0K Dec 12 07:45 .
drwxr-xr-x 1 root    root        4.0K Feb  8 18:43 ..
-rw-r----- 1 mycroft mycroft      220 Jan  6  2022 .bash_logout
-rw-r----- 1 mycroft mycroft     3.7K Jan  6  2022 .bashrc
-rw-r----- 1 mycroft mycroft      807 Jan  6  2022 .profile
-rwxrwx--- 1 root    engineering    0 Dec 12 07:45 Engineering_script.sh_0.txt
-rwxrwx--- 1 root    finance        0 Dec 12 07:45 Finance_script.sh_3.txt
-rwxrwx--- 1 root    finance       48 Dec 12 07:45 Finance_script.sh_script1.sh
-rwxrwx--- 1 root    finance       48 Dec 12 07:45 Finance_script.sh_script2.sh
-rw-r----- 1 root    root           0 Dec 12 07:45 deduction.doc_1.txt
-rw-r----- 1 root    root           0 Dec 12 07:45 deduction.doc_2.txt
```

```
root@a2e566cabe19:/home/sherlock# ls -lah
total 36K
drwxr-x--- 1 sherlock sherlock 4.0K Feb  4 02:32 .
drwxr-xr-x 1 root     root     4.0K Feb  8 18:43 ..
-rw-r----- 1 sherlock sherlock  220 Jan  6  2022 .bash_logout
-rw-r----- 1 sherlock sherlock 3.7K Jan  6  2022 .bashrc
-rw-r----- 1 sherlock sherlock  807 Jan  6  2022 .profile
-rw-r----- 1 sherlock sherlock    0 Feb  4 02:32 .sudo_as_admin_successful
-rw-r----- 1 root     root        0 Dec 12 07:45 deduction.doc_3.txt
-rwxr-x--- 1 root     root       49 Dec 12 07:45 deduction.doc_script1.sh
-rwxr-x--- 1 root     root       49 Dec 12 07:45 deduction.doc_script2.sh
-rw-r----- 1 root     root        0 Dec 12 07:45 elementary.txt_0.txt
-rw-r----- 1 root     root        0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r----- 1 root     root        0 Dec 12 07:45 game_is_afoot.txt_2.txt
-rw-r----- 1 root     root        0 Dec 12 07:45 my_file.txt
```

```
root@a2e566cabe19:/home/toby# ls -lah
total 36K
drwxr-x--- 1 toby toby        4.0K Dec 12 07:45 .
drwxr-xr-x 1 root root        4.0K Feb  8 18:43 ..
-rw-r----- 1 toby toby         220 Jan  6  2022 .bash_logout
-rw-r----- 1 toby toby        3.7K Jan  6  2022 .bashrc
-rw-r----- 1 toby toby         807 Jan  6  2022 .profile
-rwxrwx--- 1 root engineering    0 Dec 12 07:45 Engineering_script.sh_2.txt
-rw-r----- 1 root root           0 Dec 12 07:45 deduction.doc_1.txt
-rw-r----- 1 root root           0 Dec 12 07:45 elementary.txt_0.txt
-rw-r----- 1 root root           0 Dec 12 07:45 elementary.txt_3.txt
-rwxr-x--- 1 root root          45 Dec 12 07:45 elementary.txt_script1.sh
-rwxr-x--- 1 root root          45 Dec 12 07:45 elementary.txt_script2.sh
```

Cybersecurity

10.2 Project 1 Day 2 Activity Guide

Today's focus is on BSC's Linux server's SSH settings, system packages, services, and logging configurations:

- **(1)** Auditing and securing SSH
- **(2)** Reviewing and updating system packages
- **(3)** Disabling unnecessary services
- **(4)** Enabling and configuring logging

Project 1 - Day 2
Hardening Script

Complete the following:

1. Configure SSH to **not** allow the ability to:
    a. SSH with empty passwords
    b. SSH with the root user
    c. SSH with any other ports besides 22
2. Enable SSH protocol 2.
3. Restart the SSH service to set your updates
    a. Use the following command: `*service ssh restart*`
4. Be sure to note on your checklist what you have completed.
    a. Don't forget to add in your screenshots!

nano /etc/ssh/sshd_config

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords yes
```

```
Port 22
Protocol 2
```



```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
```

```
root@a2e566cabe19:/# apt update -y
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
24 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
root@a2e566cabe19:/# apt list --installed > package_list.txt

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

root@a2e566cabe19:/# cat package_list.txt
Listing...
adduser/jammy,now 3.118ubuntu5 all [installed]
apt/jammy-updates,now 2.4.13 amd64 [installed]
attr/jammy,now 1:2.5.1-1build1 amd64 [installed,automatic]
base-files/jammy-updates,now 12ubuntu4.7 amd64 [installed]
base-passwd/jammy,now 3.5.52build1 amd64 [installed]
bash/jammy-updates,jammy-security,now 5.1-6ubuntu1.1 amd64 [installed]
bsdutils/jammy-updates,jammy-security,now 1:2.37.2-4ubuntu3.4 amd64 [installed]
ca-certificates/jammy-updates,jammy-security,now 20240203~22.04.1 all [installed,automatic]
coreutils/jammy-updates,now 8.32-4.1ubuntu1.2 amd64 [installed]
```

Identify if any of the following packages are on the list as having these could introduce a security issue:

a. telnet
b. rsh-client

If they are on the list, remove those packages.

a. Research and note why these could have security issues.

```
root@a2e566cabe19:/# dpkg -l | grep -E 'telnet|rsh-client'
ii  rsh-client                  0.17-22                    amd64        client programs for remote shell connections
ii  telnet                      0.17-44build1              amd64        basic telnet client
```

```
root@a2e566cabe19:/# apt-get remove --purge telnet rsh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  rsh-client* telnet*
0 upgraded, 0 newly installed, 2 to remove and 24 not upgraded.
After this operation, 263 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 16312 files and directories currently installed.)
Removing rsh-client (0.17-22) ...
update-alternatives: using /usr/bin/scp to provide /usr/bin/rcp (rcp) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rcp.1.gz because associated file /usr/share/man/man1/scp.1.gz (of link group rcp) doesn't exist
update-alternatives: using /usr/bin/ssh to provide /usr/bin/rsh (rsh) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rsh.1.gz because associated file /usr/share/man/man1/ssh.1.gz (of link group rsh) doesn't exist
update-alternatives: using /usr/bin/slogin to provide /usr/bin/rlogin (rlogin) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rlogin.1.gz because associated file /usr/share/man/man1/slogin.1.gz (of link group rlogin) doesn't exist
Removing telnet (0.17-44build1) ...
(Reading database ... 16292 files and directories currently installed.)
Purging configuration files for telnet (0.17-44build1) ...
```

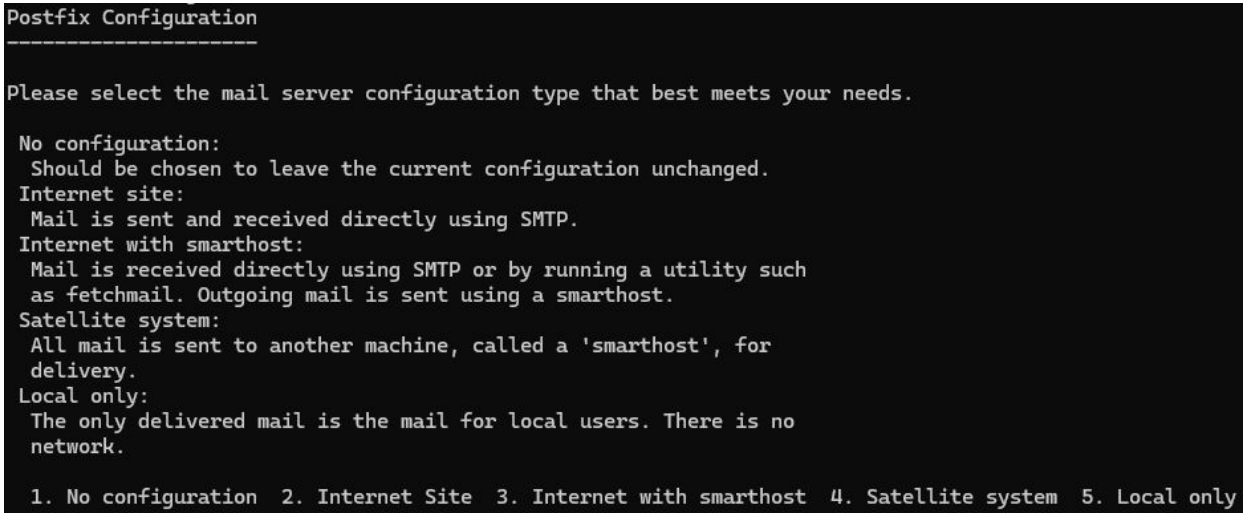
```
root@a2e566cabe19:/# apt autoremove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 24 not upgraded.
```

Add the following packages:

a. ufw
b. lynis
c. tripwire

Once the packages have been installed, research and document the hardening features these packages can provide.

```
sudo apt-get install ufw lynis tripwire -y
```



UFW

- Simplified firewall management.
- Can be configured to deny all incoming connections by default and allow only explicitly permitted traffic.

Lynis

- Security auditing.
- Performs comprehensive vulnerability scans
- Checks for compliance standards.
- Detail reporting and continuous monitoring.

Tripwire

- File integrity monitoring.
- Regular integrity checks.
- Email alerts when a change is detected.

1. Run the command to list out all services. Output this into a file called service_list.txt.

```
root@a2e566cabe19:/# systemctl list-unit-files --type=service > service_list.txt
root@a2e566cabe19:/# cat service_list.txt
UNIT FILE                              STATE    VENDOR PRESET
apt-daily-upgrade.service              static   -
apt-daily.service                      static   -
autovt@.service                        alias    -
console-getty.service                  disabled disabled
container-getty@.service               static   -
cron.service                           enabled  enabled
cryptdisks-early.service               masked   enabled
cryptdisks.service                     masked   enabled
```

2. Identify if any of the following services are running:
   a. mysql
   b. samba
3. If any of the above services are running,
   a. Stop them
   b. Disable them
   c. Remove them
4. For Step 2&3, use the `service` command, as systemctl is not installed.

```
root@a2e566cabe19:/# service mysql status
 * MySQL is stopped.
root@a2e566cabe19:/# service smbd status
 * smbd is running
```

```
root@a2e566cabe19:/# service mysql stop
 * Stopping MySQL database server mysqld
root@a2e566cabe19:/# sudo service smbd stop
 * Stopping SMB/CIFS daemon smbd
```

```
root@a2e566cabe19:/# service mysql stop
 * Stopping MySQL database server mysqld
```

```
smbd.service                                    enabled
```

Update-rc.d smbd

```
smbd.service                                    disabled
```

Apt-get remove –purge samba -y

```
The following packages will be REMOVED:
  samba*
```

```
root@a2e566cabe19:/# service smbd status
smbd: unrecognized service
```

```
mysql.service                                   enabled
```

Update-rc.d mysql disable

```
mysql.service                                   disabled
```

apt-get remove --purge mysql-server mysql-client mysql-common -y

```
The following packages will be REMOVED:
  mysql-client-8.0* mysql-common* mysql-server* mysql-server-8.0*
```

```
root@a2e566cabe19:/# service mysql status
mysql: unrecognized service
```

Access the *journald.conf* file located */etc/systemd/*.
Use nano to edit the following settings in the file. Be sure to uncomment the lines!

a. Set "**storage=persistent**"
   i. This setting will save the logs locally on the machine.
b. Set "**systemMaxUse=300M**"
   i. This setting configures the maximum disk space the logs can utilize.

```
Storage=persistent
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5
#RateLimitInterval
#RateLimitBurst=10
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize
#SystemMaxFiles=10
RuntimeMaxUse=300M
```

To prevent logs from taking up too much space, you will need to configure log rotation.
(Use the following guide to assist: https://linux.die.net/man/8/logrotate)

a. Edit the file: /etc/logrotate.conf with the following settings:
   i. Change the log rotation from weekly to daily.
   ii. Rotate out the logs after 7 days.

```
# rotate log files daily
daily

# use the adm group by default,
# of /var/log/syslog.
su root adm

# keep 7 days worth of backlogs
rotate 7
```

Complete the following:

- Using cron, schedule script 1 to run Once a month on the first of the month
- Using cron, schedule script 2 to run Once a week every Monday

Crontab -e

```
0 0 1 * * /hardening_script1.sh
0 0 * * 1 /Hardening_script2.sh
```

Project Summary

- Users/employees who were terminated still had access/accounts on the server
  - Incorrect sudo privileges assigned
  - Incorrect world rwx permissions assigned
  - User passwords stored in home directories
  - ssh running on multiple open ports when it required only port 22

- Telnet was removed as it makes the server vulnerable by transmitting all data, including usernames and passwords in plaintext
  - rsh also removed as it does not encrypt data