



Cybersecurity

Project 1 Hardening Summary and Checklist



Auditing users and groups

Deluser lestrade
Deluser irene
Deluser mary
Deluser gregson

```
root@ip-172-22-117-104:/home/sysadmin# deluser lestrade
info: Removing crontab ...
info: Removing user 'lestrade' ...
root@ip-172-22-117-104:/home/sysadmin# deluser irene
info: Removing crontab ...
info: Removing user 'irene' ...
root@ip-172-22-117-104:/home/sysadmin# deluser mary gregson
fatal: The user 'mary' is not a member of group 'gregson'.
root@ip-172-22-117-104:/home/sysadmin# deluser mary
info: Removing crontab ...
info: Removing user 'mary' ...
root@ip-172-22-117-104:/home/sysadmin# deluser gregson
info: Removing crontab ...
info: Removing user 'gregson' ...
root@ip-172-22-117-104:/home/sysadmin#
```

Passwd -l moriarty

Passwd -l mrs_hudson

```
root@ip-172-22-117-104:/home/sysadmin# passwd -l moriarty
passwd: password changed.
root@ip-172-22-117-104:/home/sysadmin# passwd -l ms_hudson
passwd: user 'ms_hudson' does not exist
root@ip-172-22-117-104:/home/sysadmin# passwd -l mrs_hudson
passwd: password changed.
root@ip-172-22-117-104:/home/sysadmin# passwd -l mrs_hudson
```

Passwd -u sherlock

Passwd -u watson

Passwd -u mycroft

Passwd -u toby

Passwd -u adler

```
root@ip-172-22-117-104:/home/sysadmin# passwd -u sherlock
passwd: password changed.
root@ip-172-22-117-104:/home/sysadmin# passwd -u watson
passwd: password changed.
root@ip-172-22-117-104:/home/sysadmin# passwd -u mycroft
passwd: password changed.
root@ip-172-22-117-104:/home/sysadmin# passwd -u toby
passwd: unlocking the password would result in a passwordless account.
You should set a password with usermod -p to unlock the password of this account.
root@ip-172-22-117-104:/home/sysadmin# passwd -u adler
passwd: unlocking the password would result in a passwordless account.
You should set a password with usermod -p to unlock the password of this account.
root@ip-172-22-117-104:/home/sysadmin#
```

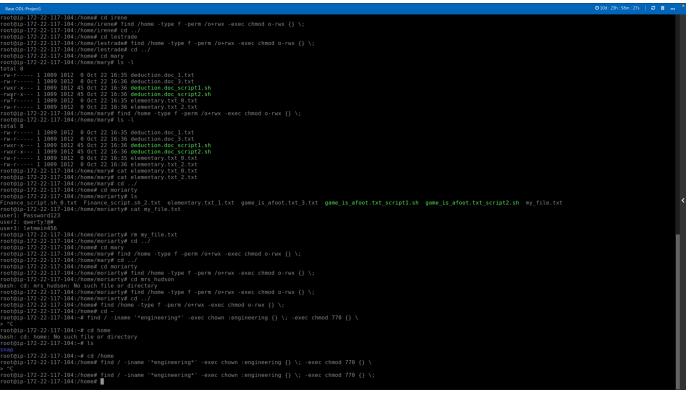
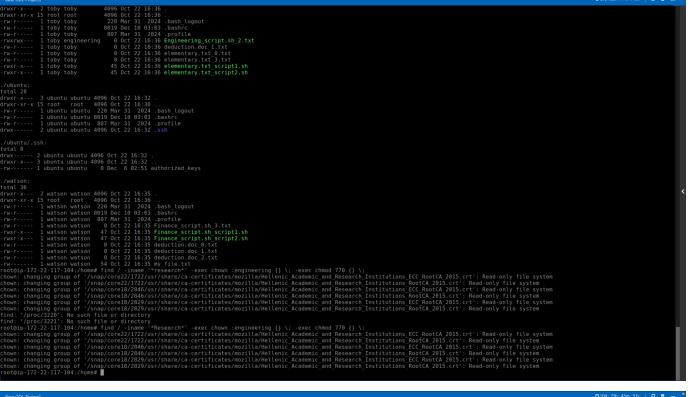
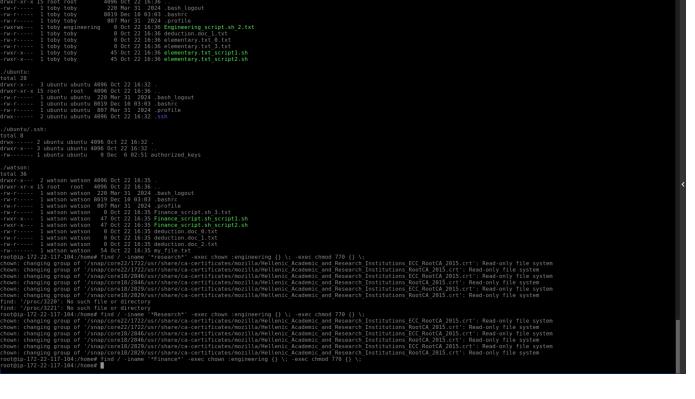
Sudo del user mycroft from marketing

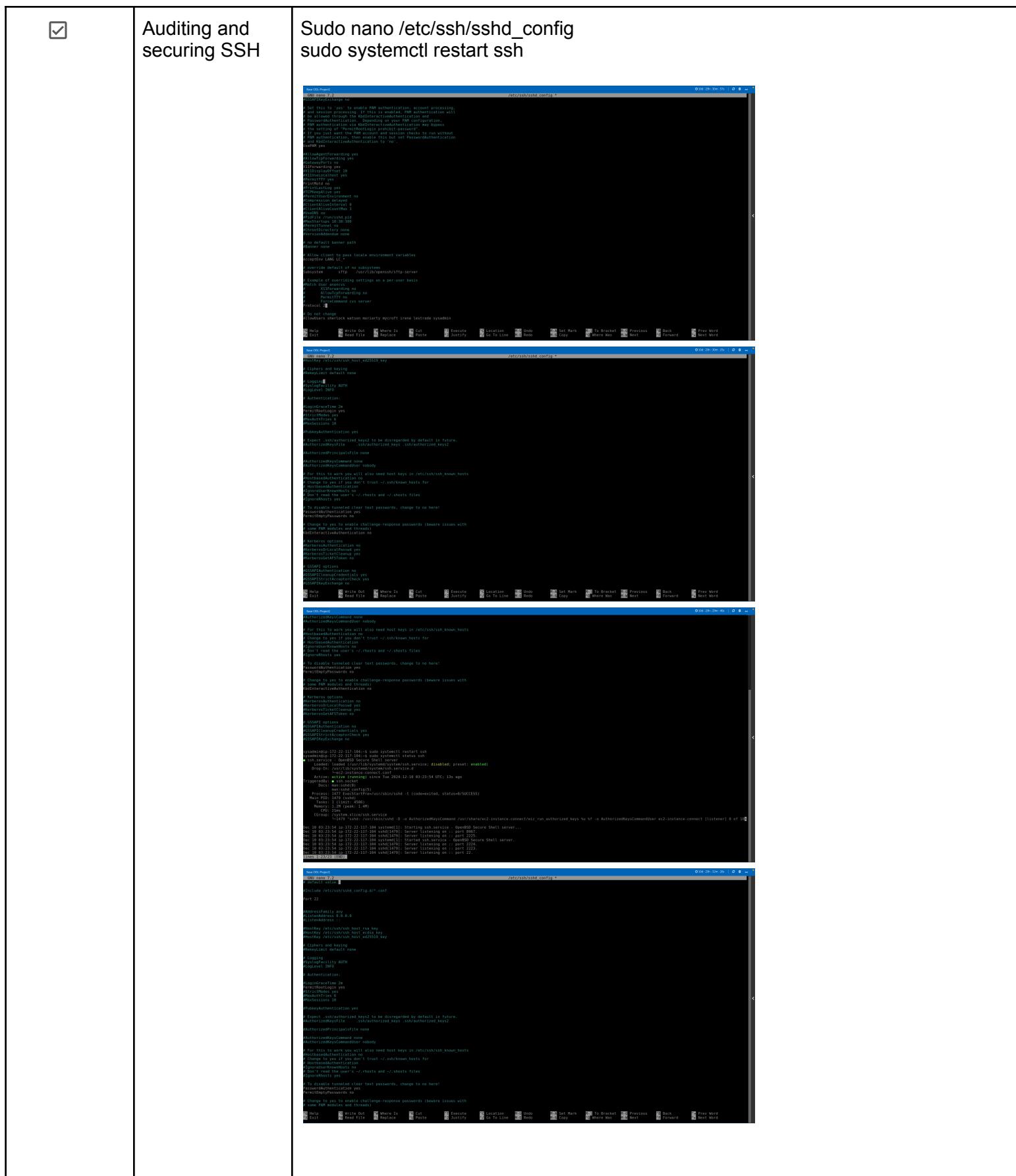
```
sysadmin@ip-172-22-117-104:~$ sudo delgroup mycroft marketing
info: Removing user 'mycroft' from group 'marketing' ...
sysadmin@ip-172-22-117-104:~$
```

Groupdel marketing

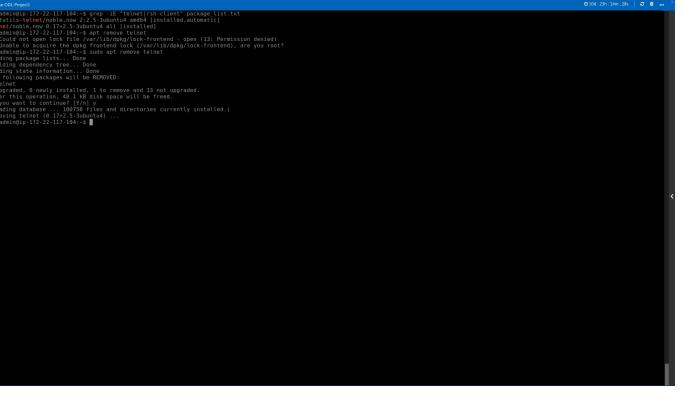
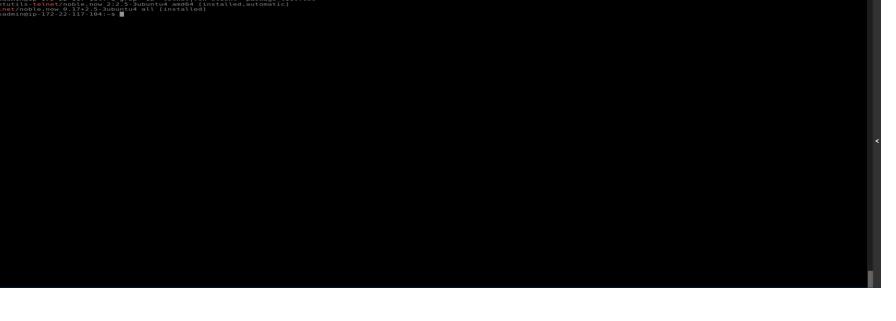
```
sysadmin@ip-172-22-117-104:~$ groupdel marketing
groupdel: Permission denied.
groupdel: cannot lock /etc/group; try again later.
sysadmin@ip-172-22-117-104:~$ sudo groupdel marketing
sysadmin@ip-172-22-117-104:~$
```

		<p>Sudo adduser mycroft research</p> <pre>sysadmin@ip-172-22-117-104:~\$ sudo adduser mycroft research info: Adding user 'mycroft' to group 'research' ... sysadmin@ip-172-22-117-104:~\$ z</pre>
<input type="checkbox"/>	Updating and enforcing password policies	<p>Sudo nano /etc/pam.d/common-password</p> <p>password requisite pam_pwquality.so minlen=8 ocredit=1 retry=2 uccredit=1</p>
<input checked="" type="checkbox"/>	Updating and enforcing sudo permissions	<p>Visudo sudoers</p> <p>Watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh /var/log/logcleanup/sh</p> <p>Moriarty ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh var/log/logcleanup.sh</p>

<input checked="" type="checkbox"/>	<p>Validating and updating permissions on files and directories</p>	<pre>sudo find / -iname "*research*" -exec chown :research {} \; -exec chmod 770 {} \; sudo find / -iname "*engineering*" -exec chown :engineering {} \; -exec chmod 770 {} \; } sudo find / -iname "*finance*" -exec chown :finance {} \; -exec chmod 770 {} \;</pre>   
-------------------------------------	---	--



--	--	--

<input checked="" type="checkbox"/>	<p>Reviewing and updating system packages</p>	<h3>Sudo apt remove telnet</h3>   
<p>Sudo apt update Sudo apt list --installed Sudo apt auto remove</p>		

```
Processing Triggers for mysql@ (8.0.23-0-Debian9) ...
Processing Triggers for vte@ (8.0.23-0-Debian9) ...
Processing Triggers for monit@ (2.27-0-Debian9) ...
Cleaning triggers...
Cleaning trigger images...

Running kernel seems to be up-to-date.

No services need to be restarted.
No container(s) need to be restarted.
No user sessions are running outdated binaries.

[KEYMAP] panic! Aborted due to corrupted supervisor (QEMU) binaries on this host.
```

When telnet is used over an unencrypted channel (like the Internet), things like usernames and passwords are transferred in clear text. This allows an attacker to eavesdrop on connections and discover confidential information.

<input checked="" type="checkbox"/>	<p>Scripts created</p>	<pre> Sudo nano hardening_script1.sh Sudo nano hardening_script2.sh Sudo chmod -x hardening_script1.sh Sudo chmod -x hardening_script2.sh Sudo ./hardening_script1.sh Sudo ./hardening_script2.sh [Base-ODS-Project1] \$ /bin/bash # Placeholder for command to get the hostname echo "Hostname: \$(hostname)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Output the OS version echo "Gathering OS version..." echo "OS Version: ?" echo "OS Version: ?" # Placeholder for command to report output file, choose an output file name REPORT_FILE="hardening_script1.sh" # Output the hostname echo "Gathering hostname..." echo "Gathering hostname..." echo "Hostname: \$(hostname)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Output the OS version echo "Gathering OS version..." echo "OS Version: ?" # Placeholder for command to get the 05 version echo "OS Version: \$(cat /etc/os-release)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Gathering memory information..." # Placeholder for command to get memory info echo "Memory Information: \$(free -h)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Output uptime information... echo "Gathering uptime information..." echo "Uptime Information: \$(uptime)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Backup the OS" # Placeholder for command to back up the OS sudo tar -czvf /baker_street/backup.tar.gz --exclude=/baker_street/backup.tar.gz --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run / echo "OS backup complete" # Placeholder for command to output sudoers file # Placeholder for command to check file permissions and update them echo "Checking for files with world permissions...find /home -type f -perm /o+rwx -exec chmod o-rwx {} \;" echo "World permissions have been removed from any files found." >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Placeholder for command to update permissions... echo "Updating permissions for specific scripts..." # Engineering scripts - Only members of the engineering group find / -name "Engineering" -exec chown engineering {} \; -exec chmod 770 {} \; echo "Permissions update for engineering scripts" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Placeholder for command to update permissions... echo "Updating permissions for Research scripts..." # Research scripts - Only members of the research group find / -name "Research" -exec chown research {} \; -exec chmod 770 {} \; echo "Permissions updated for Research scripts" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Placeholder for command to update permissions... echo "Updating permissions for Finance scripts..." # Finance scripts - Only members of the finance group find / -name "Finance" -exec chown finance {} \; -exec chmod 770 {} \; echo "Permissions updated for Finance scripts." >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Script execution completed. Check \$REPORT_FILE for details." # Placeholder for command to update permissions... apt update -y # Placeholder for command to upgrade packages # Place Upgrade Packages Command Here echo "Packages have been updated and upgraded" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Placeholder for command to list all installed packages apt list --installed >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Printing out logging configuration data" # Placeholder for command to display logging data echo "journald.conf file data: \$(cat /etc/system/journal.conf)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "logrotate.conf file data: \$(cat /etc/system/logrotate.conf)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "sshd configuration file: \$(cat /etc/ssh/sshd_config)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Script execution completed. Check \$REPORT_FILE for details." # This is the sshd server system-wide configuration file. See # ssd_config(5) for more information # This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games # The strategy used for options in the default sshd_config shipped with # OpenSSH is to specify options with their default value where # # possible, but leave them commented. Uncommented options override the # # default value. #Include /etc/ssh/sshd_config.d/* Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress :: #HostKey /etc/ssh/ssh_host_rsa_key #HostKey /etc/ssh/ssh_host_ecdsa_key #HostKey /etc/ssh/ssh_host_ed25519_key # Ciphers and keying #RekeyLimit default none # Logging #SyslogFacility AUTH #LogLevel INFO # Authentication: #LoginGraceTime 2m PermitRootLogin yes [hardening script2.sh] \$ /bin/bash # Placeholder for command to report output file, choose a NEW output file name REPORT_FILE="hardening_script2.sh" # Output the sshd configuration file echo "Gathering details from sshd configuration file" echo "Gathering details from sshd configuration file" echo "sshd configuration file:\$(cat /etc/ssh/sshd_config)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Update packages and service apt update -y # Placeholder for command to update packages apt update -y # Placeholder for command to upgrade packages # Place Upgrade Packages Command Here echo "Packages have been updated and upgraded" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Placeholder for command to list all installed packages apt list --installed >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Printing out logging configuration data" # Placeholder for command to display logging data echo "journald.conf file data: \$(cat /etc/system/journal.conf)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "logrotate.conf file data: \$(cat /etc/system/logrotate.conf)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "sshd configuration file: \$(cat /etc/ssh/sshd_config)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE echo "Script execution completed. Check \$REPORT_FILE for details." # This is the sshd server system-wide configuration file. See # ssd_config(5) for more information # This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games # The strategy used for options in the default sshd_config shipped with # OpenSSH is to specify options with their default value where # # possible, but leave them commented. Uncommented options override the # # default value. #Include /etc/ssh/sshd_config.d/* Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress :: #HostKey /etc/ssh/ssh_host_rsa_key #HostKey /etc/ssh/ssh_host_ecdsa_key #HostKey /etc/ssh/ssh_host_ed25519_key # Ciphers and keying #RekeyLimit default none # Logging #SyslogFacility AUTH #LogLevel INFO # Authentication: #LoginGraceTime 2m PermitRootLogin yes </pre>
-------------------------------------	------------------------	--

```

Box COD Project
/usr/local/share/gml/dtd/
/usr/local/share/gml/misc/
/usr/local/share/gml/declaration/
/usr/local/include/
/usr/local/sbin/
/usr/local/bin/
/usr/local/etc/
/usr/lib/x86_64-linux-gnu/libc.so.6
/usr/share/nord
/usr/share/grub/grub-fxpayload-lists/blacklist/
/usr/share/grub/grub-fxpayload-lists/blacklist/10_vmmfare
/usr/share/grub/grub-fxpayload-lists/blacklist/11_header
/usr/share/grub/grub-fxpayload-lists/blacklist/11_virtualbox
/usr/share/grub/grub-fxpayload-lists/blacklist/20_radeon_hd6800
/usr/share/grub/grub-fxpayload-lists/blacklist/21_nvidia
/usr/share/systemd/tmp.mount
/usr/share/systemd/language-fallback-map
/usr/share/glib2.0/abdu慈-model-map
/usr/share/glib2.0/
/usr/share/glib2.0/static/
/usr/share/glib2.0/static/glib-favicon.png
/usr/share/glib2.0/static/glib-logo.png
/usr/share/glib2.0/static/glib2.js
/usr/share/glib2.0/static/glib-web.css
/usr/share/glib2.0/index.cgi
/usr/share/glib2.0/glib.cgi
/usr/share/doc-base/man-db.man.db
/usr/share/doc-base/python3.python-policy
/usr/share/doc-base/texiski.pdfish
/usr/share/doc-base/findutils
/usr/share/doc-base/bc.bc
/usr/share/doc-base/systat.systat-faq
/usr/share/doc-base/base-passwd.users-and-groups
/usr/share/doc-base/libpng16-16f64.libpng16
/usr/share/doc-base/nano-faq
/usr/share/doc-base/timedate
/usr/share/doc-base/shared-font-formats
/usr/share/doc-base/shared-time.info.shared-mime-info
/usr/share/distro-info
/usr/share/distro-info/ubuntu.csv
/usr/share/distro-info/debian.csv
/usr/share/ieee-data/man.csv
/usr/share/ieee-data/uil36.txt
/usr/share/ieee-data/lab.txt
/usr/share/ieee-data/uil.txt
/usr/share/ieee-data/lab.csv
/usr/share/ieee-data/uil36_update
/usr/share/ieee-data/uil36.csv
/usr/share/ieee-data/uil.csv

Box COD Project
#include /etc/ssh/sshd_config.d/*.conf
Port 22

AddressFamily any
ListenAddress 0.0.0.0
ListenAddress ::

HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

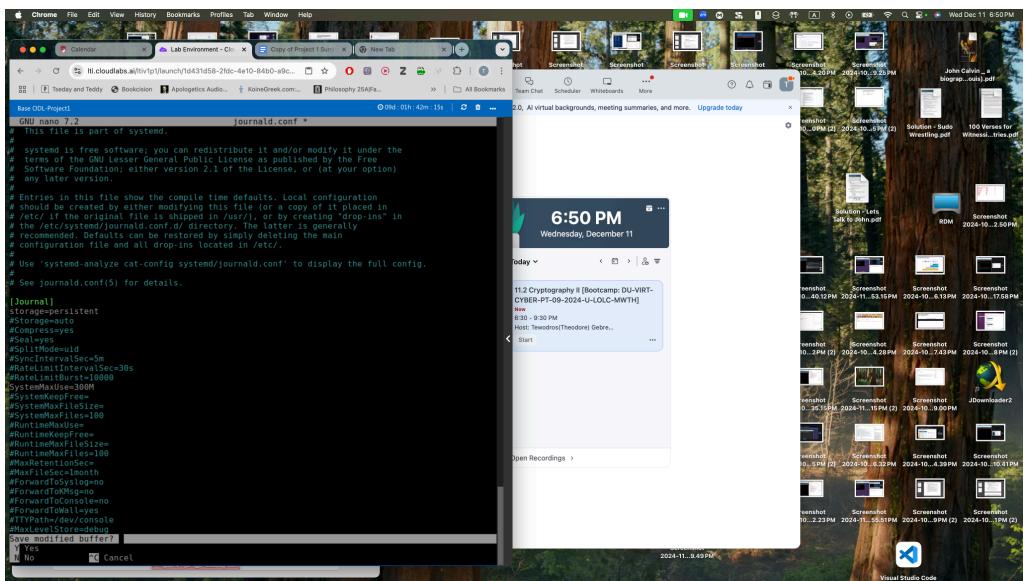
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes

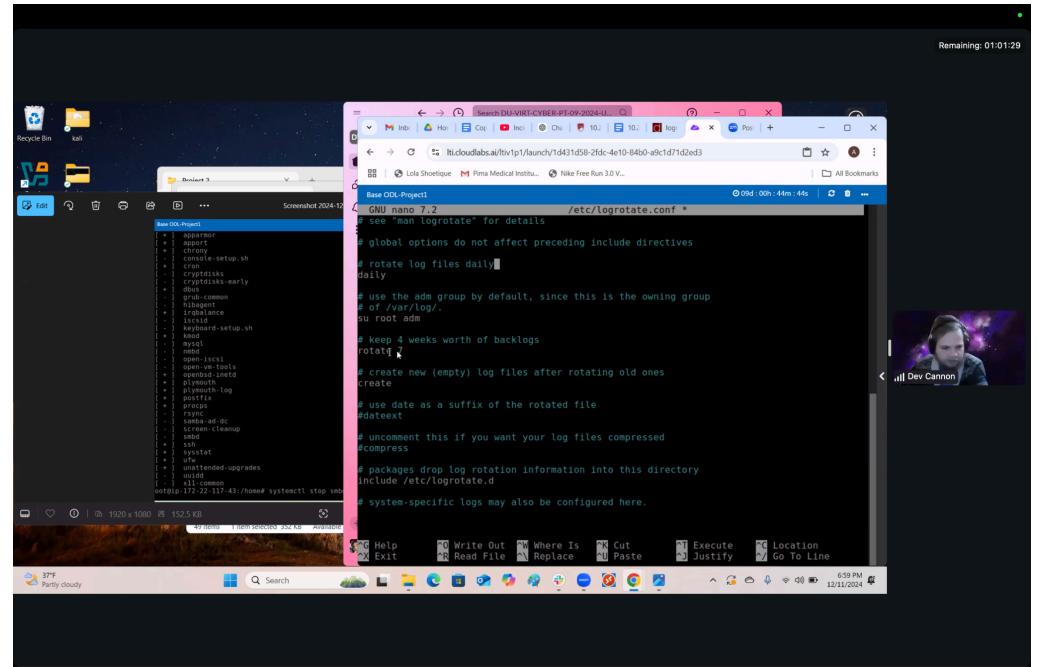
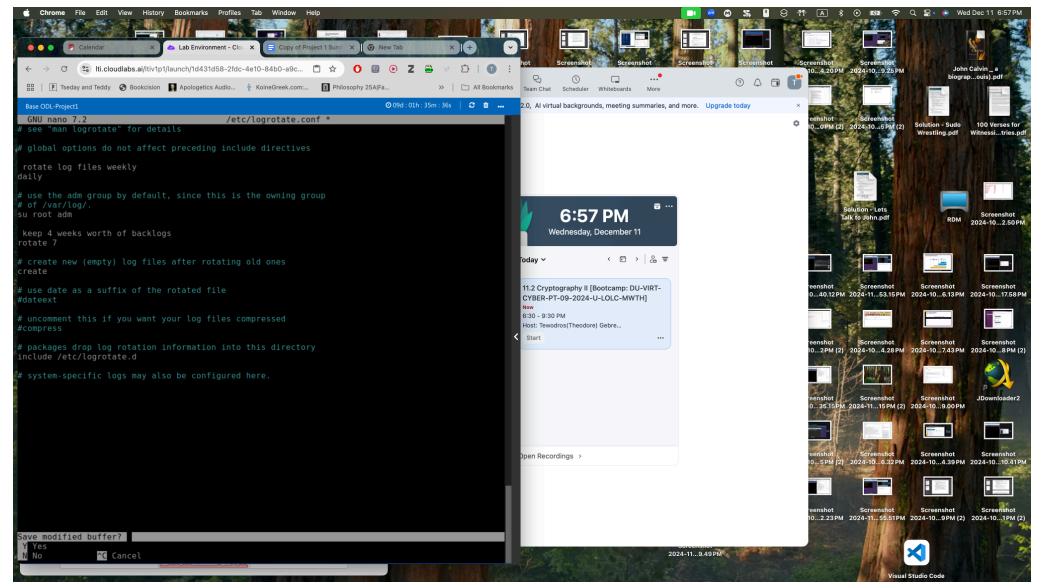
sysadmin@172-22-117-104:~$ sudo ./hardening_script2.sh
Gathering details from ssh configuration file
Reading package lists... done
Hit:1 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [706 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [164 kB]
Get:7 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Get:8 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [729 kB]
Get:9 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [151 kB]
Get:10 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [310 kB]
Get:11 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [537 kB]
Get:12 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [93 kB]
Get:13 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 kB]
Get:14 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [940 kB]
Get:15 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [117 kB]
Get:16 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.7 kB]
Get:17 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:18 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Packages [212 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [591 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [102 kB]
Get:21 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [564 kB]
Get:22 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:23 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [93.1 kB]
Get:24 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [93.1 kB]
Get:25 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:26 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [206 B]
Get:27 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [206 B]
Fetched 5111 kB in 2378 kB/s

```

Enabling and configuring logging

Sudo nano /etc/systemd/journal.conf
Sudo nano /etc/logrotate.conf





	<pre>Base CDI:Project1 GNU nano 2.2 # See "man logrotate" for details # global options do not affect preceding include directives # rotate log files weekly daily # use the adm group by default, since this is the owning group # of /var/log/. su root adm # keep 4 weeks worth of backlog rotate 7 # create new (empty) log files after rotating old ones create # use date as a suffix of the rotated file dateext # uncomment this if you want your log files compressed #compress # packages drop log rotation information into this directory include /etc/logrotate.d # system-specific logs may also be configured here.</pre>
<input type="checkbox"/>	<h2>Scripts scheduled with cron</h2> <p>crontab -e</p> <pre>Base CDI:Project1 GNU nano 7.2 # Edit this file to introduce tasks to be run by cron. # Each task to run has to be defined through a single line # indicating with different fields when the task will be run # and what command to run for the task. # To define the time you can provide concrete values for # hour (or min), day of month (dom), month (mon), # and day of week (dow) or use '*' in these fields (for 'any'). # Notice that tasks will be started based on the cron's system # daemon's notion of time and timezones. # Output of the crontab jobs (including errors) is sent through # email to the user the crontab file belongs to (unless redirected). # For example, you can run a backup of all your user accounts # at 5 a.m. every week with: # 0 5 * * * tar -zcf /var/backups/home.tgz /home/ # For more information see the manual pages of crontab(5) and cron(8) # h dom mon dow command 0 0 1 * * root@home/sysadmin/hardening_script1.sh * * * * 1 root@home/sysadmin/hardening_script2.sh</pre>

```

Box COD Project
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of TIME and TIMEZONES.
#
# Output of the cron jobs (including errors) is sent through
# email to the user the cronfile belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# every星期一 23:00:
# 0 23 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# h m dom mon dow   command
# 0 23 * * 1 root    /root/kyadmin/hardening_script1.sh
# * * * * 1 root    /root/kyadmin/hardening_script_2.sh

```

crontab: installing new crontab
kyadmin@ip-172-22-117-104:~\$

Hostname	<u>IP-172-22-117-104</u>
Uptime information	<u>1313.61 2525.10</u>
OS Version	<u>Ubuntu 24.04.1 LTS</u>
Memory information	<u>3836</u>
Customer	Baker Street Corporation

