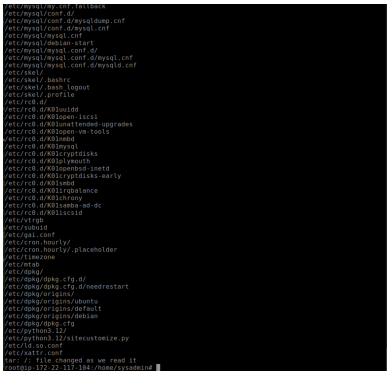
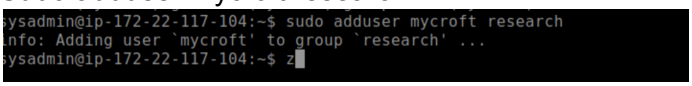
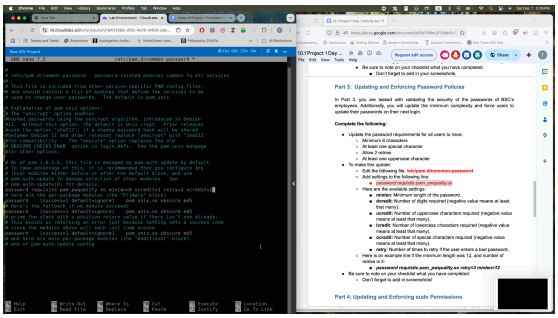
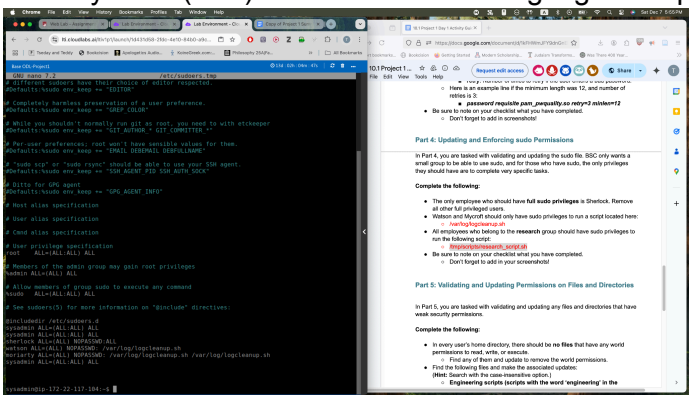
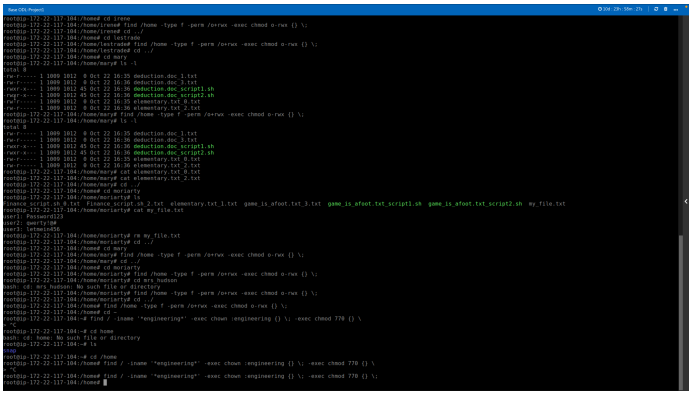
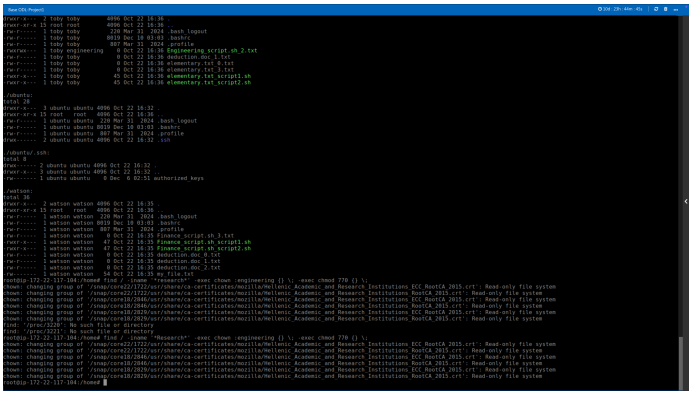
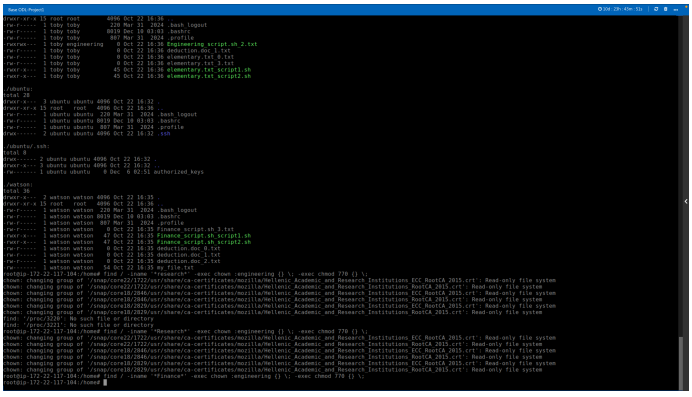
Cybersecurity

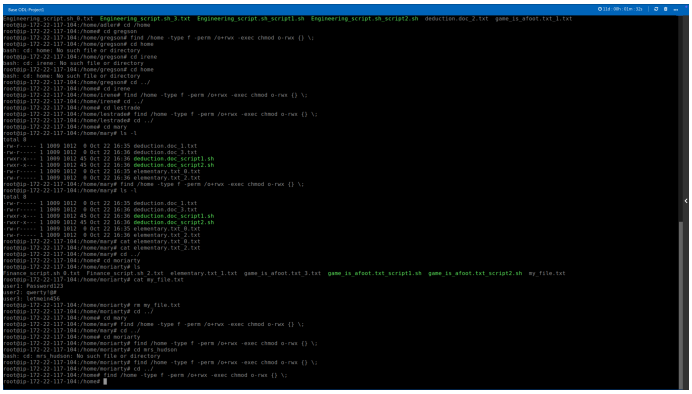
Project 1 Hardening Summary and Checklist

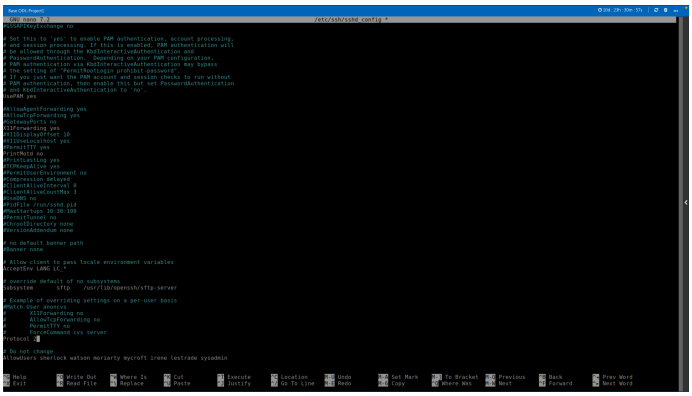
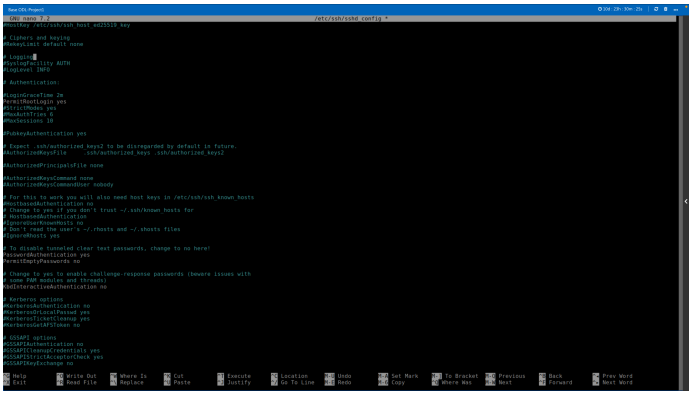
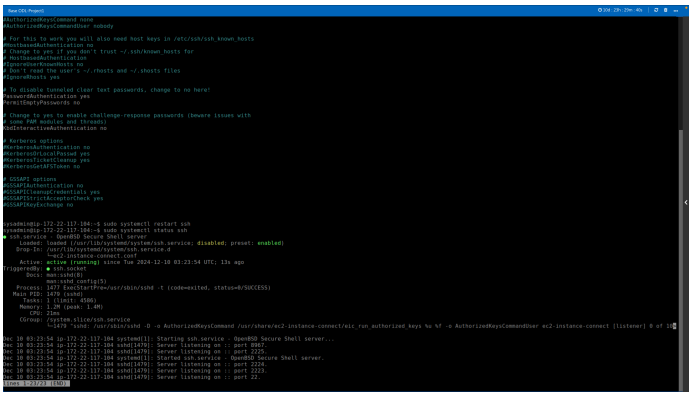
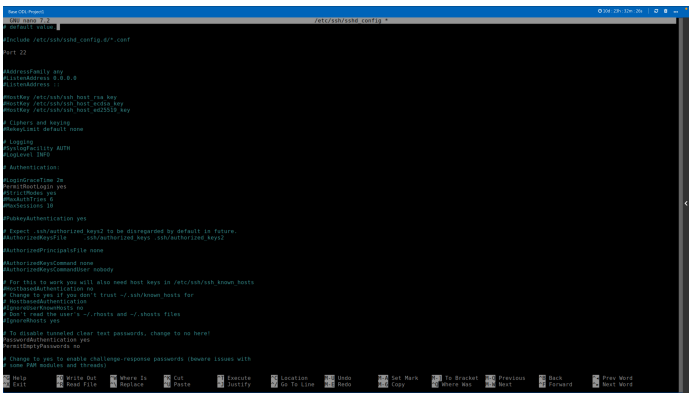
Completed	Activity	Script(s) used / Tasks completed / Screenshots
☑	OS backup	 sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /

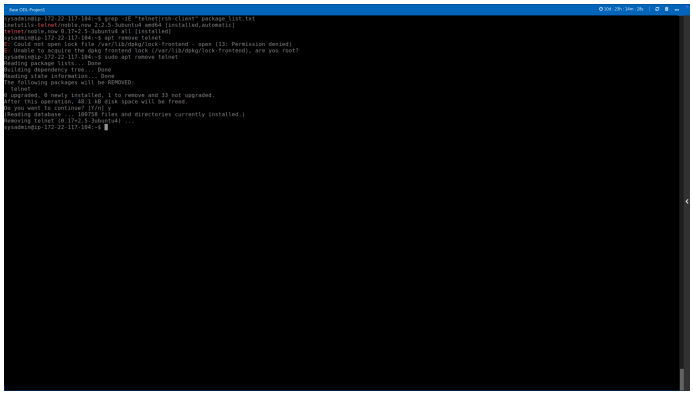
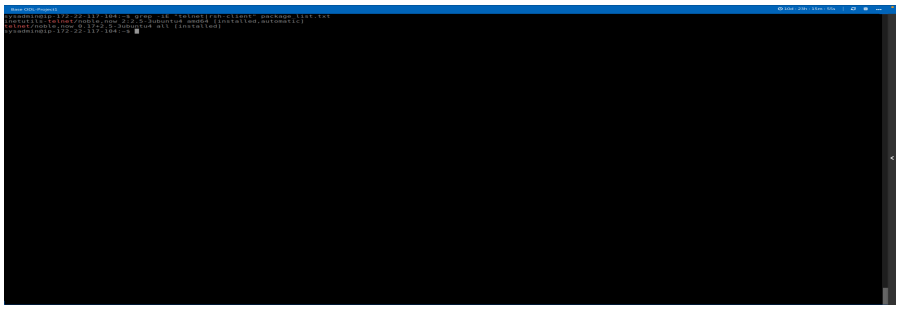
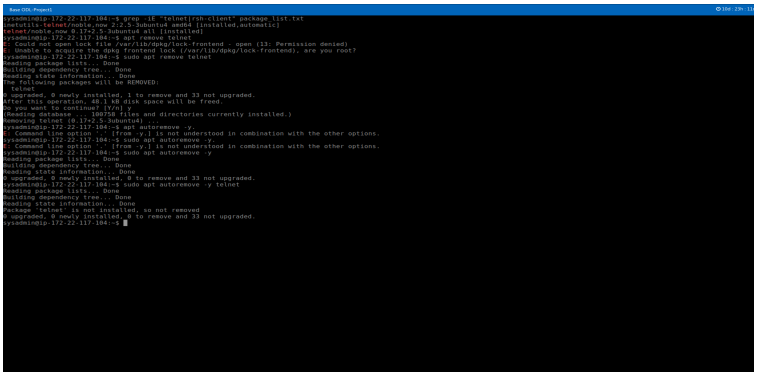
☑	Auditing users and groups	Deluser lestrade Deluser irene Deluser mary Deluser gregson ``` root@ip-172-22-117-104:/home/sysadmin# deluser lestrade info: Removing crontab ... info: Removing user `lestrade' ... root@ip-172-22-117-104:/home/sysadmin# deluser   irene info: Removing crontab ... info: Removing 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:~$ ```

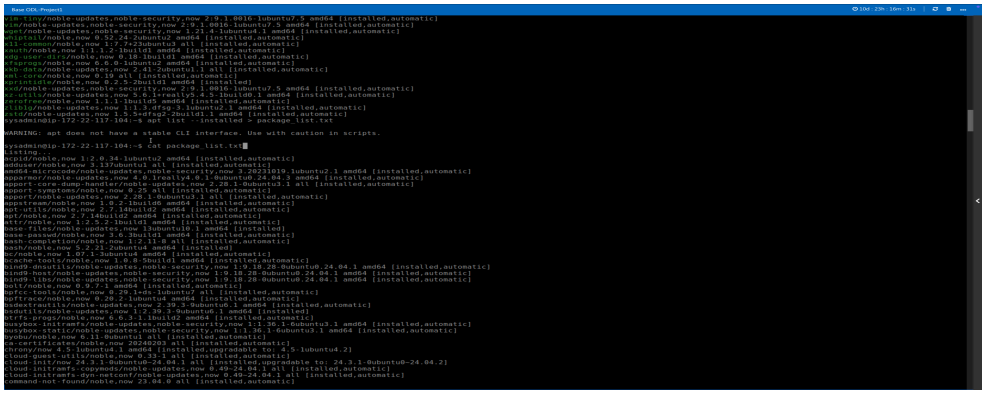
		Sudo adduser mycroft research 
☐	Updating and enforcing password policies	Sudo nano /etc/pam.d/common-password password requisite pam_pwquality.so minlen=8 ocredit=1 retry=2 ucredit=1 
☑	Updating and enforcing sudo permissions	Visudo sudoers Watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh /var/log/logcleanup/sh Moriarty ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh var/log/logcleanup.sh 

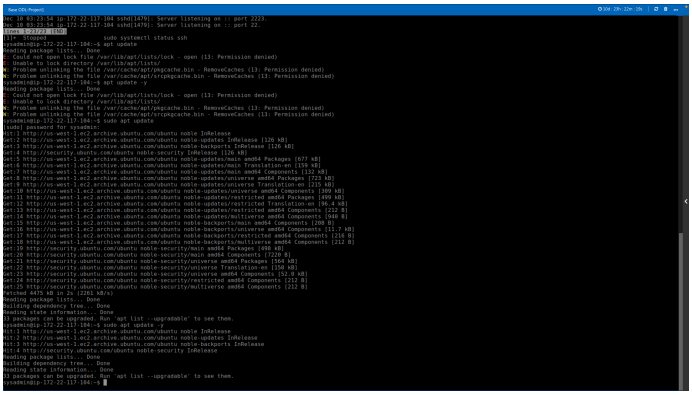
☑	Validating and updating permissions on files and directories	sudo find / -iname '*research*' -exec chown :research {} \; -exec chmod 770 {} \; sudo find / -iname '*engineering*' -exec chown :engineering {} \; -exec chmod 770 {} \; sudo find / -iname '*finance*' -exec chown :finance {} \; -exec chmod 770 {} \;   

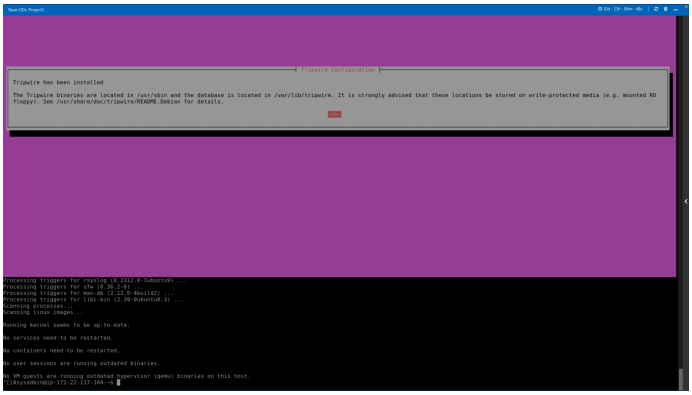
		 Find /hom e -type f -perm /o+rwx -exec chmod o+rwx {} \;

☑	Auditing and securing SSH	Sudo nano /etc/ssh/sshd_config sudo systemctl restart ssh    

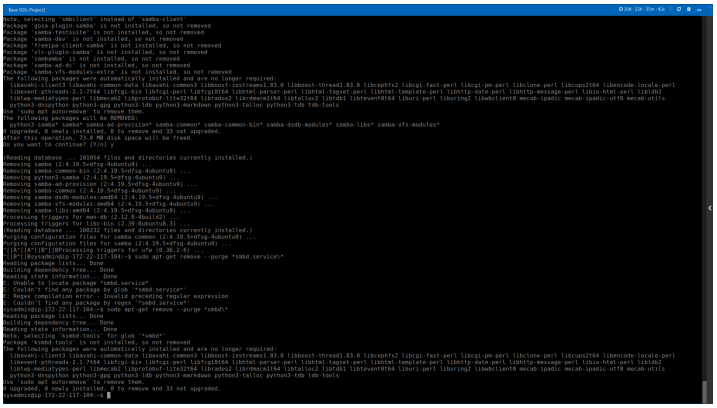
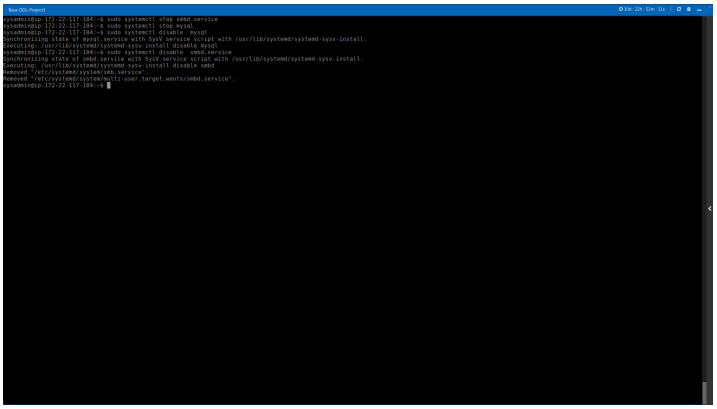
☑	Reviewing and updating system packages	Sudo apt remove telnet    Sudo apt update Sudo apt list --installed Sudo apt auto remove

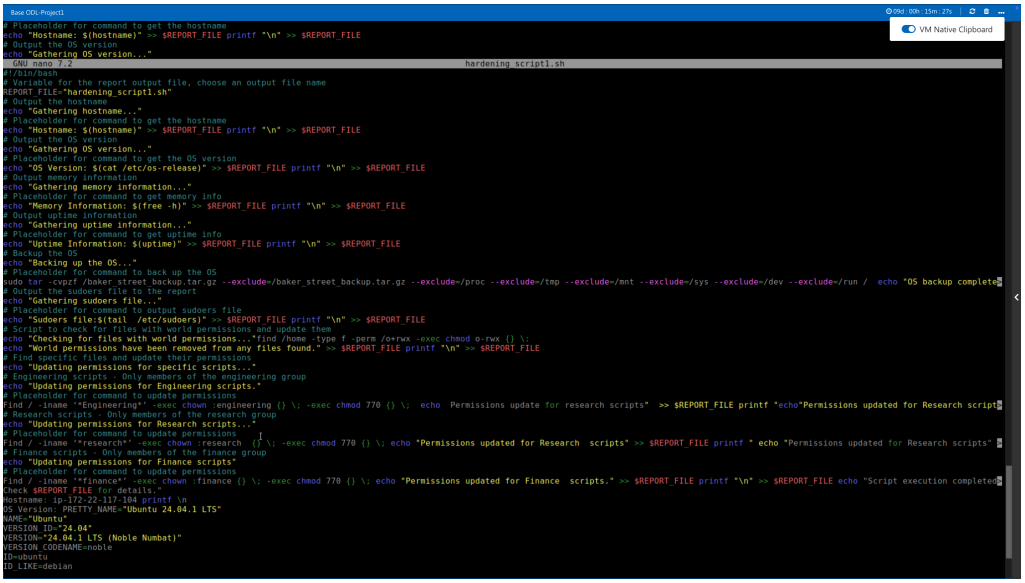
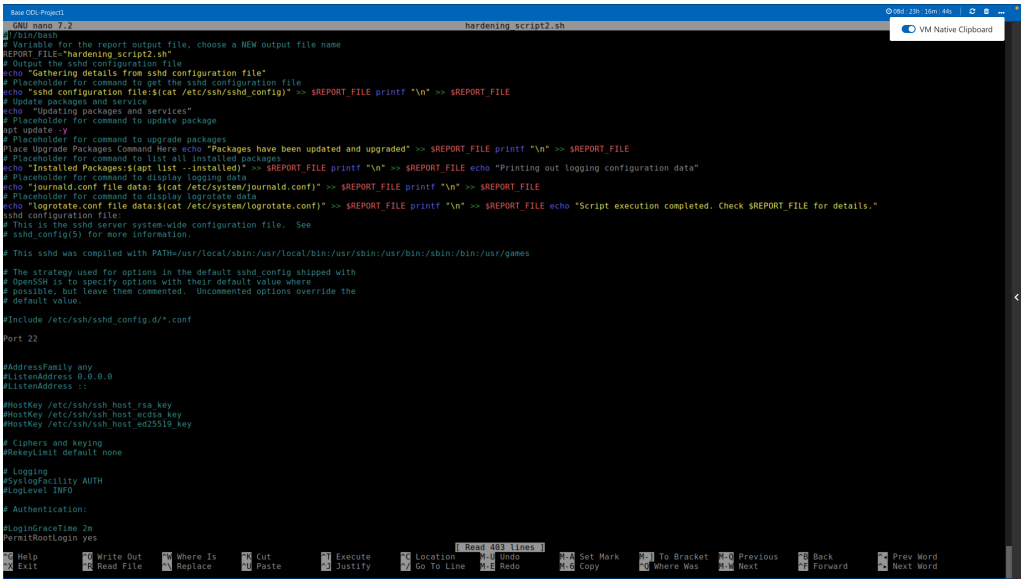






When telnet is used over an unencrypted channel (like the Internet), things like usernames and passwords are transferred in clear text. This allows an attacker to eavesdrop on connections and discover confidential information.

		
☑	Disabling unnecessary services	Sudo systemctl disable smbd.service Sudo systemctl disable mysql 

☑	Scripts created	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 ODL-Project1

08d : 23h : 45m : 22s

VM Native Clipboard

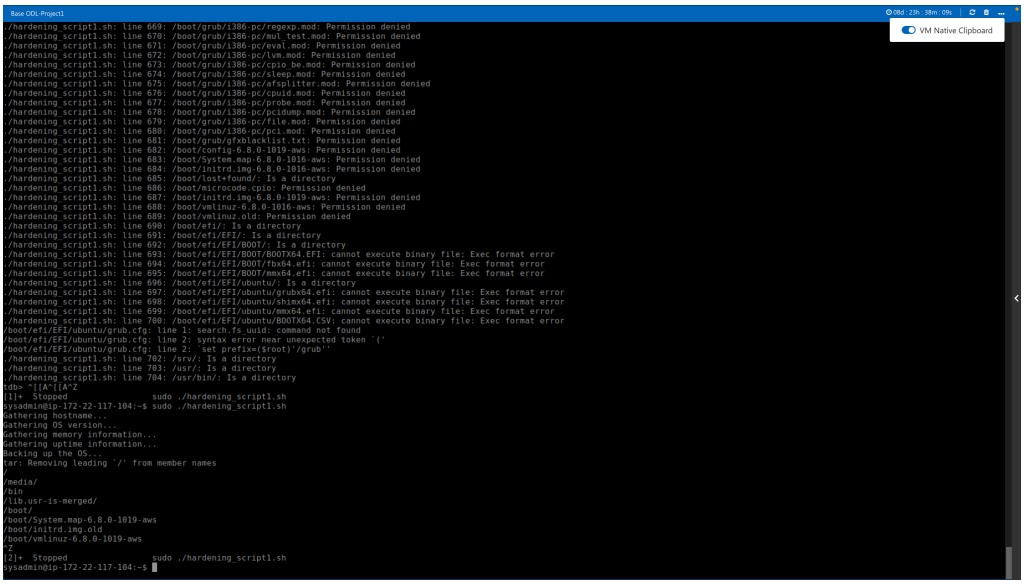
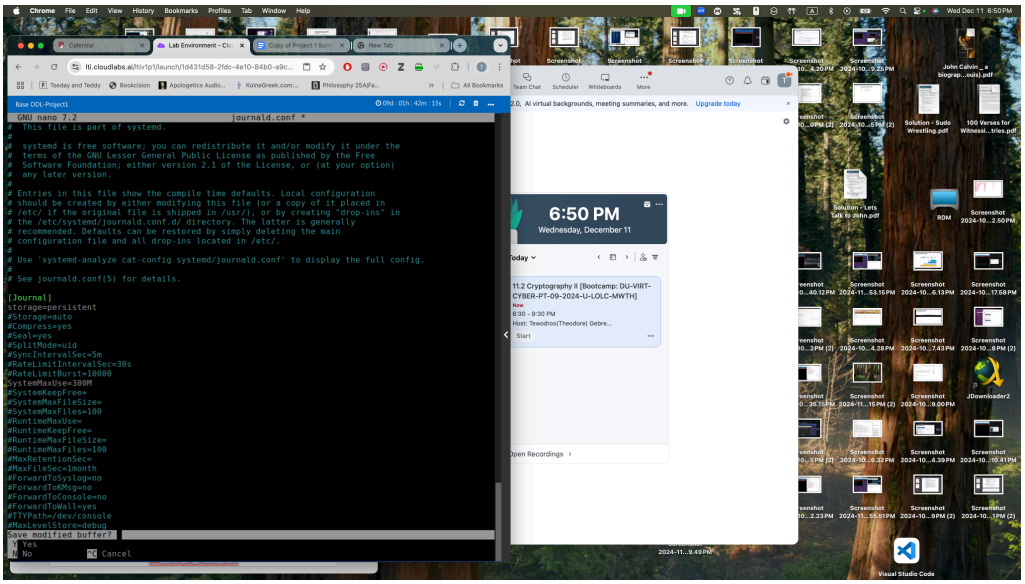
```
/usr/local/share/sgml/dtd/
/usr/local/share/sgml/misc/
/usr/local/share/sgml/declaration/
/usr/local/include/
/usr/local/sbin/
/usr/local/src/
/usr/local/etc/
/usr/lib64/
/usr/lib64/ld-linux-x86-64.so.2
/usr/share/
/usr/share/motd
/usr/share/grub-gfxpayload-lists/
/usr/share/grub-gfxpayload-lists/blacklist/
/usr/share/grub-gfxpayload-lists/blacklist/10_vmware
/usr/share/grub-gfxpayload-lists/blacklist/00_header
/usr/share/grub-gfxpayload-lists/blacklist/11_virtualbox
/usr/share/grub-gfxpayload-lists/blacklist/20_radeon_hd6800
/usr/share/systemd/
/usr/share/systemd/tmp.mount
/usr/share/systemd/language-fallback-map
/usr/share/systemd/kbd-model-map
/usr/share/gitweb/
/usr/share/gitweb/static/
/usr/share/gitweb/static/git-favicon.png
/usr/share/gitweb/static/git-logo.png
/usr/share/gitweb/static/gitweb.js
/usr/share/gitweb/static/gitweb.css
/usr/share/gitweb/index.cgi
/usr/share/gitweb/gitweb.cgi
/usr/share/doc-base/
/usr/share/doc-base/man-db.man-db
/usr/share/doc-base/python3.python-policy
/usr/share/doc-base/gdisk.gdisk
/usr/share/doc-base/findutils.findutils
/usr/share/doc-base/bc.bc
/usr/share/doc-base/menu.menu
/usr/share/doc-base/sysstat.sysstat-faq
/usr/share/doc-base/base-passwd.users-and-groups
/usr/share/doc-base/nano.nano
/usr/share/doc-base/libpng16-16t64.libpng16
/usr/share/doc-base/nano.nano-faq
/usr/share/doc-base/time.time
/usr/share/doc-base/kbd.kbd-font-formats
/usr/share/doc-base/shared-mime-info.shared-mime-info
/usr/share/distro-info/
/usr/share/distro-info/ubuntu.csv
/usr/share/distro-info/debian.csv
/usr/share/ieee-data/
/usr/share/ieee-data/mam.csv
/usr/share/ieee-data/oui36.txt
/usr/share/ieee-data/iab.txt
/usr/share/ieee-data/mam.txt
/usr/share/ieee-data/oui.txt
/usr/share/ieee-data/iab.csv
/usr/share/ieee-data/.lastupdate
/usr/share/ieee-data/oui36.csv
/usr/share/ieee-data/oui.csv
```

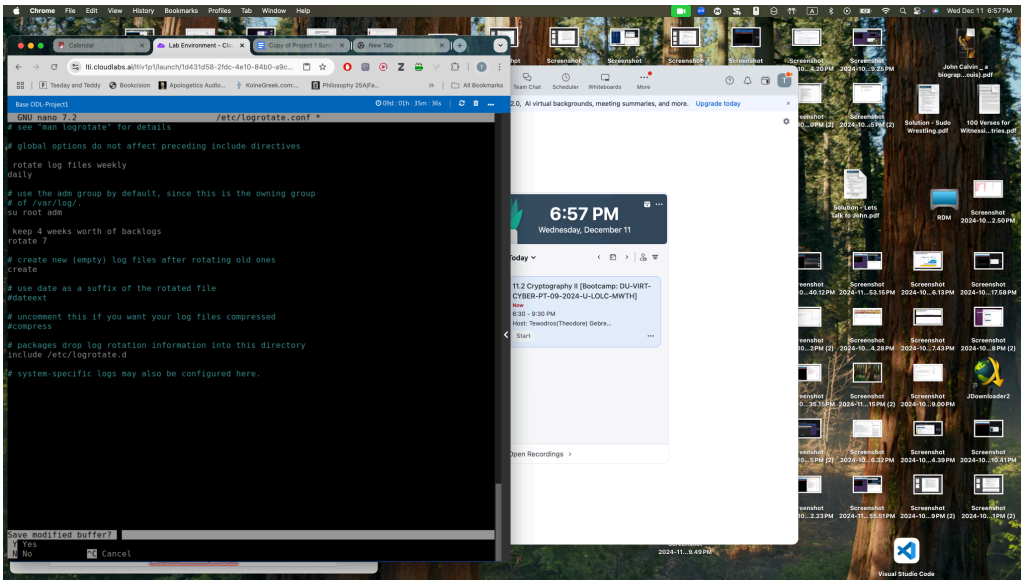
Base ODL-Project1

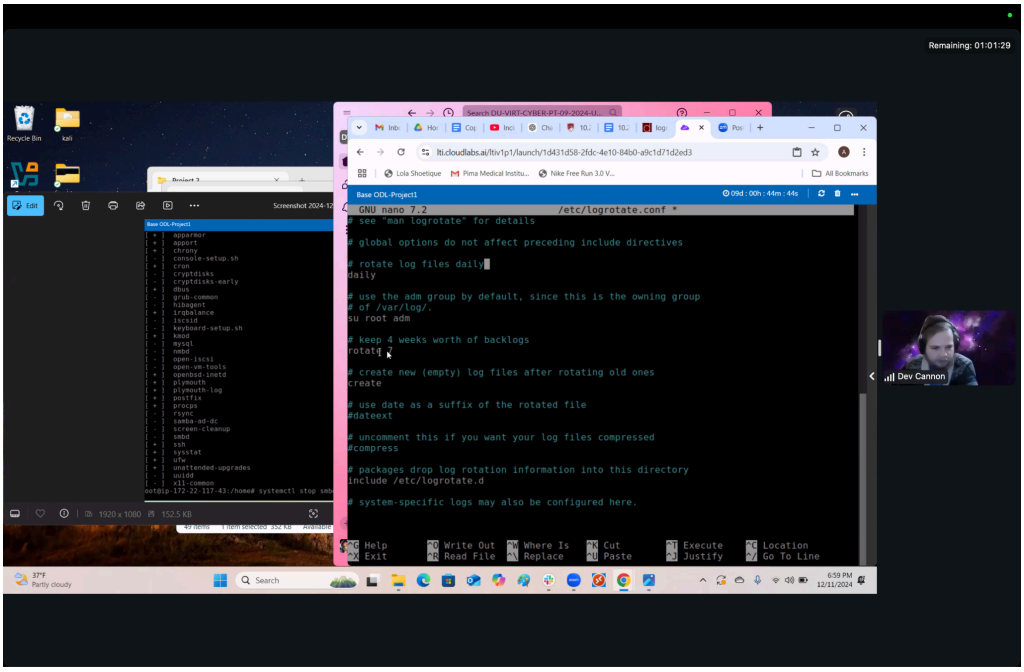
08d : 23h : 15m : 48s

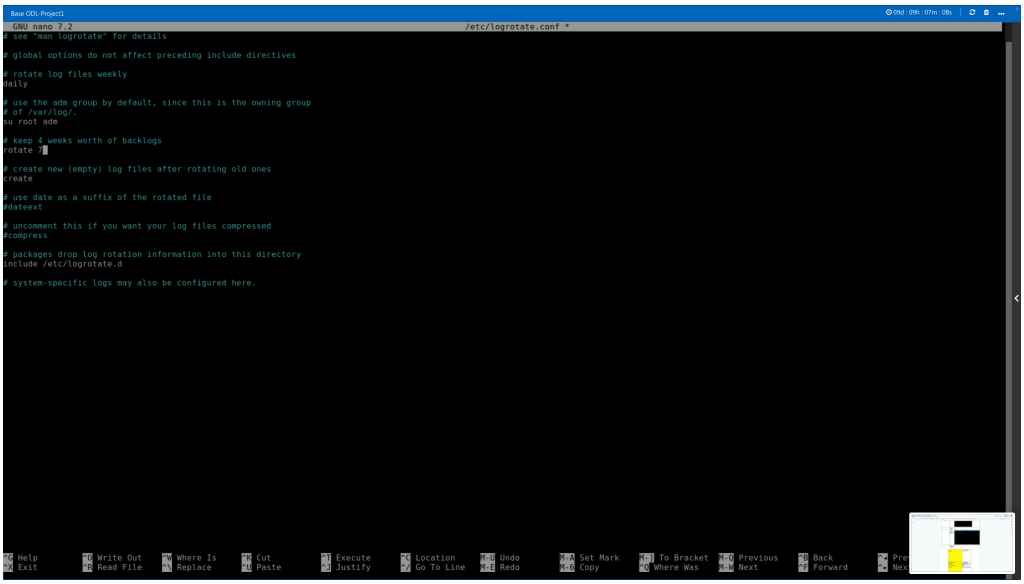
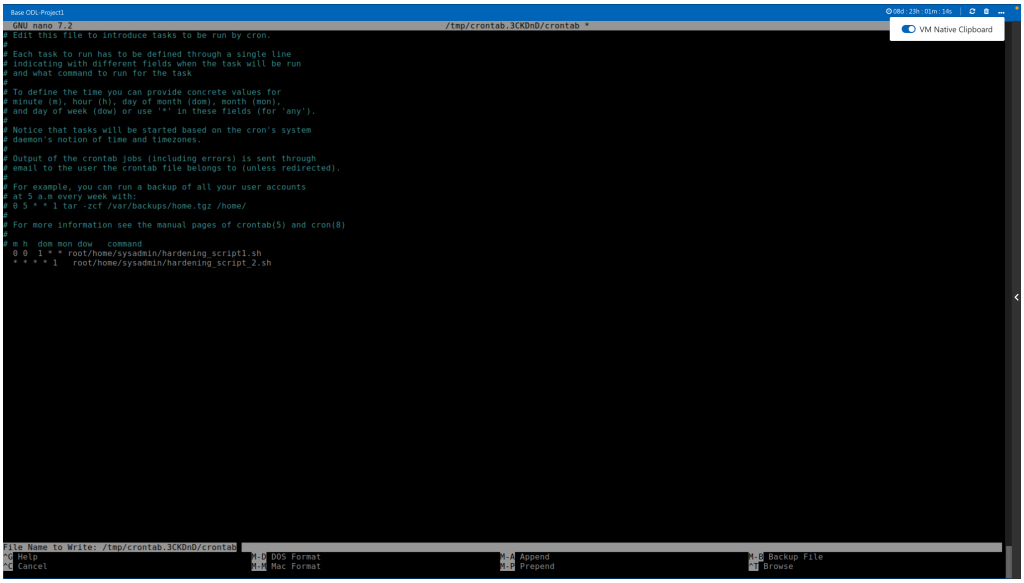
VM Native Clipboard

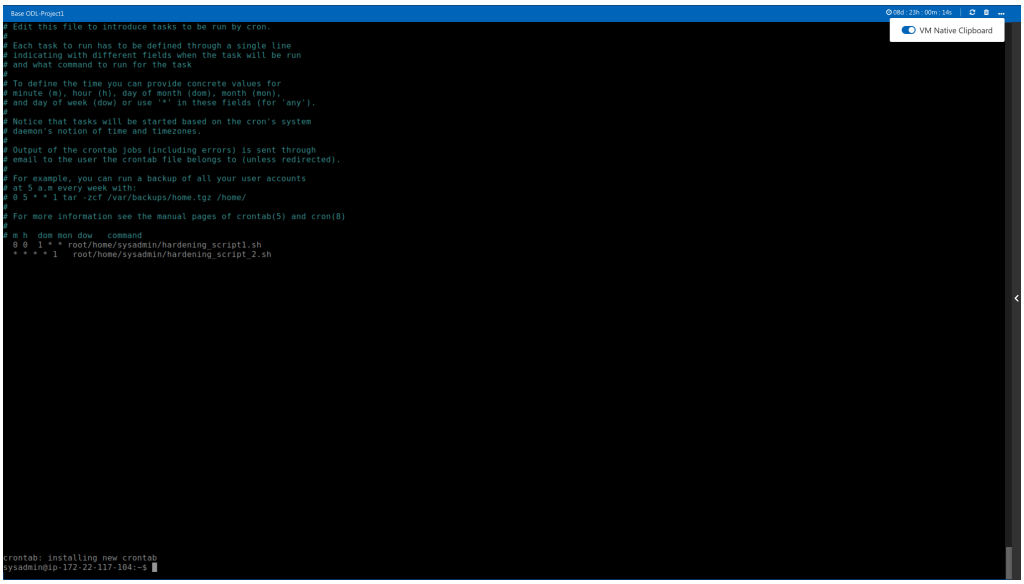
```
#Include /etc/ssh/sshd_config.d/*.conf

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


sysadmin@ip-172-22-117-104:~$ sudo ./hardening_script2.sh
Gathering details from sshd configuration file
"Updating packages and services"
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://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/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 Translation-en [217 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 Translation-en [104 kB]
Get:13 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:14 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:15 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
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/multiverse amd64 Components [212 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [501 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [102 kB]
Get:21 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7192 B]
Get:22 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [564 kB]
Get:23 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:24 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [482 kB]
Get:25 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [93.1 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:27 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Fetched 5111 kB in 2s (2378 kB/s)
```

		
	Enabling and configuring logging	Sudo nano /etc/systemd/journal.conf Sudo nano /etc/logrotate.conf 


GNU nano 7.2 /etc/logrotate.conf *
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 backlogs
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.
Save modified buffer?
Y Yes
N No
^C Cancel
6:57 PM
Wednesday, December 11


Remaining: 01:01:29
GNU nano 7.2 /etc/logrotate.conf *
see "man logrotate" for details
global options do not affect preceding include directives
rotate log files daily
daily
use the adm group by default, since this is the owning group
of /var/log/.
su root adm
keep 4 weeks worth of backlogs
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.
Dev Cannon

		
☐	Scripts scheduled with cron	crontab -e 

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