



Cybersecurity

Project 1 Hardening Summary and Checklist

OS Information

Customer	Baker Street Corporation
Hostname	<u>Baker_Street_Linux_Server</u>
OS Version	<u>20.04.1-Ubuntu</u>
Memory information	<u>MemTotal: 16182796 kB</u> <u>MemFree: 10217780 kB</u> <u>MemAvailable: 14268312 kB</u>
Uptime information	<u>01:08:01 up 25 min, 0 users, load average: 0.27, 0.29, 0.43</u>

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
<ul style="list-style-type: none">•	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 /

		<pre> etc/ufw/applications.d/ etc/ufw/applications.d/samba etc/ufw/applications.d/openssh-server etc/ca-certificates.conf etc/perl/ etc/perl/Net/ etc/perl/Net/Libnet.cfg etc/ethertypes etc/cron.hourly/ etc/cron.hourly/.placeholder etc/dbus-1/ etc/dbus-1/system.d/ etc/dbus-1/session.d/ etc/python3.10/ etc/python3.10/sitecustomize.py boot/ media/ lib32 sbin .dockervenv ar: /: file changed as we read it oot@Baker_Street_Linux_Server:/# </pre>
•	Auditing users and groups	<pre> sudo userdel -r lestrade sudo userdel -r irene sudo userdel -r mary sudo userdel -r gregson getent passwd lestrade irene mary gregson </pre> <pre> sshd:x:107:65534::/run/sshd:/usr/sbin/nologin 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 mrs_hudson:x:1006:1006::/home/mrs_hudson:/bin/bash sysadmin:x:1008:1008::/home/sysadmin:/bin/bash toby:x:1010:1010::/home/toby:/bin/bash adler:x:1011:1011::/home/adler:/bin/bash root@Baker_Street_Linux_Server:/etc# </pre> <pre> sudo usermod --expiredate 1 moriarty sudo usermod --expiredate 1 mrs_hudson </pre> <pre> sudo passwd -S moriarty sudo passwd -S mrs_hudson </pre> <pre> root@Baker_Street_Linux_Server:/etc# sudo passwd -S moriarty sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution moriarty L 02/14/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/etc# sudo passwd -S mrs_hudson sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution mrs_hudson L 12/12/2024 0 99999 7 -1 root@Baker_Street_Linux_Server:/etc# </pre> <pre> sudo passwd -u sherlock sudo passwd -u watson sudo passwd -u mycroft sudo passwd -u toby sudo passwd -u adler </pre> <pre> addgroup research delgroup marketing </pre>

		<pre> root@Baker_Street_Linux_Server:/etc# sudo groupadd research sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution root@Baker_Street_Linux_Server:/etc# addgroup research addgroup: The group 'research' already exists. root@Baker_Street_Linux_Server:/etc# rmgroup marketing bash: rmgroup: command not found root@Baker_Street_Linux_Server:/etc# delgroup marketing Removing group 'marketing' ... Done. root@Baker_Street_Linux_Server:/etc# </pre>
•	Updating and enforcing password policies	<pre> # end of pam-auth-update config #New password requisites 2/13/25 As password requisite pam_pwquality.so retry=2 minlen=8 ucredit=-1 ocredit=-1 </pre>
•	Updating and enforcing sudo permissions	<pre> @includedir /etc/sudoers.d sherlock ALL=(ALL:ALL) ALL watson ALL=(ALL) /var/log/logcleanup.sh mycroft ALL=(ALL) /var/log/logcleanup.sh %research All=(ALL) /tmp/scripts/research_scripts.sh </pre>
•	Validating and updating permissions on files and directories	<pre> root@Baker_Street_Linux_Server/# chown :research /tmp/scripts/research_script.sh root@Baker_Street_Linux_Server/# chmod 770 /tmp/scripts/research_script.sh root@Baker_Street_Linux_Server/# find / -type f -iname "finance" 2>/dev/null /home/moriarty/finance_script.sh.2.txt /home/mycroft/finance_script.sh.0.txt /home/mycroft/finance_script.sh.3.txt /home/mycroft/finance_script.sh_script2.sh /home/mycroft/finance_script.sh_script1.sh /home/watson/finance_script.sh_script2.sh /home/watson/finance_script.sh_script1.sh root@Baker_Street_Linux_Server/# chown :research /home/mycroft/finance_script.sh_script2.sh /home/mycroft/finance_script.sh_script1.sh /home/watson/finance_script.sh_script2.sh /home/watson/finance_script.sh_script1.sh root@Baker_Street_Linux_Server/# chmod 770 /home/mycroft/finance_script.sh_script2.sh /home/mycroft/finance_script.sh_script1.sh /home/watson/finance_script.sh_script2.sh /home/watson/finance_script.sh_script1.sh root@Baker_Street_Linux_Server/# </pre> <pre> root@Baker_Street_Linux_Server:/home/adler# ls -l Engineering_script.sh_script1.sh Engineering_script.sh_script2.sh deduction.doc.3.txt game_is_afout.txt -rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh.3.txt -rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh.0.txt -rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh.3.txt -rwxr-x--- 1 root root 46 Dec 12 07:45 Engineering_script.sh_script1.sh -rwxr-x--- 1 root root 46 Dec 12 07:45 Engineering_script.sh_script2.sh -rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc.2.txt -rw-r--r-- 1 root root 0 Dec 12 07:45 game_is_afout.txt.1.txt root@Baker_Street_Linux_Server:/home/adler# </pre> <pre> root@Baker_Street_Linux_Server/# find /home -type f -iname "password" -o -iname "cred" -o -iname "secret" -o -iname ".bak" -o -iname ".old" -o -iname ".txt" 2>/dev/null /home/adler/Engineering_script.sh.0.txt /home/adler/Engineering_script.sh.3.txt /home/adler/deduction.doc.2.txt /home/adler/game_is_afout.txt.1.txt /home/adler/hacking_files.txt /home/herlock/deduction.doc.3.txt /home/herlock/game_is_afout.txt.1.txt /home/herlock/elementary.txt.0.txt /home/herlock/game_is_afout.txt.1.txt /home/moriarty/finance_script.sh.2.txt /home/moriarty/hacking_files.txt /home/moriarty/elementary.txt.1.txt /home/moriarty/game_is_afout.txt.1.txt /home/moriarty/finance_script.sh.0.txt /home/mycroft/finance_script.sh.3.txt /home/mycroft/Engineering_script.sh.0.txt /home/mycroft/deduction.doc.1.txt /home/mycroft/deduction.doc.2.txt /home/toby/elementary.txt.1.txt /home/toby/Engineering_script.sh.2.txt /home/toby/deduction.doc.1.txt /home/watson/finance_script.sh.1.txt /home/watson/hacking_files.txt /home/watson/deduction.doc.1.txt /home/watson/deduction.doc.2.txt /home/watson/deduction.doc.0.txt /home/mr_hudson/elementary.txt.1.txt /home/mr_hudson/Engineering_script.sh.1.txt /home/mr_hudson/deduction.doc.0.txt root@Baker_Street_Linux_Server/# find /home -type f -iname "password" -o -iname "cred" -o -iname "secret" -o -iname ".bak" -o -iname ".old" -o -iname ".txt" 2>/dev/null root@Baker_Street_Linux_Server/# find /home -type f -iname "password" -o -iname "cred" -o -iname "secret" -o -iname ".bak" -o -iname ".old" -o -iname ".txt" 2>/dev/null root@Baker_Street_Linux_Server/# find /home -type f -iname "password" -o -iname "cred" -o -iname "secret" -o -iname ".bak" -o -iname ".old" -o -iname ".txt" 2>/dev/null root@Baker_Street_Linux_Server/# </pre>

<ul style="list-style-type: none"> • 	Optional: Updating password hashing configuration	
<ul style="list-style-type: none"> • 	Auditing and securing SSH	<pre> 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 no #StrictModes yes #MaxAuthTries 6 #MaxSessions 10 #PubkeyAuthentication yes #IgnoreRhosts yes # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes PermitEmptyPasswords no # Change to yes to enable challenge-response passwords (beware issues with # the PAM libshells module if you are using a challenge-response password) # #X11Forwarding no # #AllowTcpForwarding no # #PermitTTY no # #ForceCommand cvs server #Port 2222 #Port 2223 #Port 2224 #Port 2225 Protocol 2 AllowUsers sherlock watson moriarty mycroft irene lestrade </pre> <pre> File Edit View Search Terminal Help root@Baker_Street_Linux_Server:/# service ssh restart * Restarting OpenBSD Secure Shell server sshd root@Baker_Street_Linux_Server:/# </pre>

		 <pre> File Edit View Search Terminal Help GNU nano 6.2 /etc/logrotate.conf # see "man logrotate" for details # global options do not affect preceding include directives # rotate log files weekly weekly # use the adm group by default, since this is the owning group # of /var/log/syslog. 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. rotating pattern: /var/log/mysql.log /var/log/mysql/*log after 1 days (7 rotations) empty log files are rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 3714) considering log /var/log/mysql.log log /var/log/mysql.log does not exist -- skipping creating new state considering log /var/log/mysql/error.log Creating new state Now: 2025-02-20 02:10 Last rotated at 2025-02-20 02:00 log does not need rotating (log has already been rotated) not running postrotate script, since no logs were rotated switching euid from 0 to 0 and egid from 4 to 0 (pid 3714) rotating pattern: /var/log/syslog /var/log/mail.info /var/log/mail.warn /var/log/mail.err /var/log/mail.log /var/log/dmccm.log /var/log/kern.log /var/log/auth.log /var/log/user.log /var/log/lpr.log /var/log/cron.log /var/log/debug /var/log/messages weekly (4 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 3714) considering log /var/log/syslog log /var/log/syslog does not exist -- skipping </pre>
<ul style="list-style-type: none"> • 	Scripts created	<h3>Hardening_script1.sh</h3> <pre> 1 #!/bin/bash 2 3 # Variable for the report output file, choose an output file name 4 REPORT_FILE="system_report.txt" 5 6 # Output the hostname 7 echo "Gathering hostname..." 8 # Placeholder for command to get the hostname 9 echo "Hostname: \$(hostname)" >> \$REPORT_FILE 10 printf "\n" >> \$REPORT_FILE 11 12 13 # Output the OS version 14 echo "Gathering OS version..." 15 # Placeholder for command to get the OS version 16 # (Using /etc/os-release for basic OS info) 17 echo "OS Version: \$(grep "PRETTY_NAME=" /etc/os-release cut -d= -f2 tr -d '"')" >> \$REPORT_FILE 18 printf "\n" >> \$REPORT_FILE 19 20 21 # Output memory information 22 echo "Gathering memory information..." 23 # Placeholder for command to get memory info 24 echo "Memory Information: \$(free -h)" >> \$REPORT_FILE 25 printf "\n" >> \$REPORT_FILE 26 27 28 # Output uptime information 29 echo "Gathering uptime information..." 30 # Placeholder for command to get uptime info 31 echo "Uptime Information: \$(uptime -p)" >> \$REPORT_FILE 32 printf "\n" >> \$REPORT_FILE 33 34 35 # Backup the OS 36 echo "Backing up the OS..." 37 # Placeholder for command to back up the OS 38 # This example compresses the /etc, /var, and /home directories into /backup. 39 tar -czf /backup/os_backup_\$(date +%F).tar.gz /etc /var /home 2>/dev/null 40 41 echo "OS backup completed." >> \$REPORT_FILE 42 printf "\n" >> \$REPORT_FILE 43 44 45 # Output the sudoers file to the report 46 echo "Gathering sudoers file..." 47 # Placeholder for command to output sudoers file 48 echo "Sudoers file: \$(sudo cat /etc/sudoers)" >> \$REPORT_FILE 49 printf "\n" >> \$REPORT_FILE 50 </pre>

```

51
52 # Script to check for files with world permissions and update them
53 echo "Checking for files with world permissions..."
54
55 # Placeholder for command to remove all world permissions, starting at the /home directory
56 find /home -type f -perm -o-rwx -exec chmod o-rwx {} +
57
58 echo "World permissions have been removed from any files found." >> $REPORT_FILE
59 printf "\n" >> $REPORT_FILE
60
61
62 # Find specific files and update their permissions
63 echo "Updating permissions for specific scripts..."
64
65 # Engineering scripts - Only members of the engineering group
66 echo "Updating permissions for Engineering scripts."
67 # Placeholder for command to update permissions
68 find / -type f -iname '*engineering*' -exec chown :engineering {} + -exec chmod 770 {} +
69 echo "Permissions updated for Engineering scripts." >> $REPORT_FILE
70 printf "\n" >> $REPORT_FILE
71 |
72
73 # Research scripts - Only members of the research group
74 echo "Updating permissions for Research scripts..."
75 # Placeholder for command to update permissions
76 find / -type f -iname '*research*' -exec chown :research {} + -exec chmod 770 {} +
77 echo "Permissions updated for Research scripts" >> $REPORT_FILE
78 printf "\n" >> $REPORT_FILE
79
80
81 # Finance scripts - Only members of the finance group
82 echo "Updating permissions for Finance scripts"
83 # Placeholder for command to update permissions
84 find / -type f -iname '*finance*' -exec chown :finance {} + -exec chmod 770 {} +
85 echo "Permissions updated for Finance scripts." >> $REPORT_FILE
86 printf "\n" >> $REPORT_FILE
87
88
89 echo "Script execution completed. Check $REPORT_FILE for details."
90
91

```

```

root@Baker_Street_Linux_Server:~# sudo ./hardening_script1.sh
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Gathering hostname...
Gathering OS version...
Gathering memory information...
Gathering uptime information...
Backing up the OS... I
Gathering sudoers file...
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Checking for files with world permissions...
Updating permissions for specific scripts...
Updating permissions for Engineering scripts...
Updating permissions for Research scripts...
Updating permissions for Finance scripts
Script execution completed. Check system_report.txt for details.
root@Baker_Street_Linux_Server:~# cat system_report.txt
Hostname: Baker_Street_Linux_Server

OS Version: Ubuntu 22.04.5 LTS

Memory Information:
Mem:          15Gi      1.0Gi      12Gi      287Mi      1.9Gi      13Gi
Swap:         0B           0B           0B

Uptime Information: up 54 minutes

OS backup completed.

Sudoers file: #
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults      use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent

```

		<pre># Ditto for GPG agent #Defaults:%sudo env_keep += "GPG_AGENT_INFO" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification robt ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # 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 sherlock ALL=(ALL:ALL) ALL watson ALL=(ALL) /var/log/logcleanup.sh mycroft ALL=(ALL) /var/log/logcleanup.sh %research All=(ALL) /tmp/scripts/research_scripts.sh World permissions have been removed from any files found. Permissions updated for Engineering scripts. Permissions updated for Research scripts Permissions updated for Finance scripts. root@Baker_Street_Linux_Server:~#</pre>
		hardening_script2.sh


```

1 #!/bin/bash
2
3 # Variable for the report output file, choose a NEW output file name
4 REPORT_FILE="system_security_report.txt"
5
6 # Output the sshd configuration file
7 echo "Gathering details from sshd configuration file"
8 echo "sshd configuration file:" >> $REPORT_FILE
9 cat /etc/ssh/sshd_config >> $REPORT_FILE
10 printf "\n" >> $REPORT_FILE
11
12 # Update packages and services
13 echo "Updating packages and services"
14
15 # Update package list
16 apt update -y
17
18 # Upgrade installed packages
19 apt upgrade -y
20
21 echo "Packages have been updated and upgraded" >> $REPORT_FILE
22 printf "\n" >> $REPORT_FILE
23
24 # List all installed packages
25 echo "Installed Packages:" >> $REPORT_FILE
26 apt list --installed >> $REPORT_FILE
27 printf "\n" >> $REPORT_FILE
28
29 echo "Printing out logging configuration data"
30
31 # Display journald.conf file
32 echo "journald.conf file data:" >> $REPORT_FILE
33 cat /etc/systemd/journald.conf >> $REPORT_FILE
34 printf "\n" >> $REPORT_FILE
35
36 # Display logrotate.conf file
37 echo "logrotate.conf file data:" >> $REPORT_FILE
38 cat /etc/logrotate.conf >> $REPORT_FILE
39 printf "\n" >> $REPORT_FILE
40
41 echo "Script execution completed. Check $REPORT_FILE for details."

```

```

2
root@baker-street:~# sudo ./hardening_script2.sh
sudo: unable to resolve host baker-street: Temporary failure in name resolution
Gathering details from sshd configuration file
Updating packages and services
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2618 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2939 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1230 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1252 kB]
Fetched 8609 kB in 12s (724 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  libgnutls30 libpython3.10-minimal libpython3.10-stdlib libssl3 openssl python3.10 python3.10-minimal
Upgraded: 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 9496 kB of archives.
After this operation, 1424 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libssl3 amd64 3.0.2-0ubuntu1.19 [1095 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3.10-stdlib amd64 3.10.12-1-22.04.9 [508 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpython3.10-stdlib amd64 3.10.12-1-22.04.9 [1850 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3.10-minimal amd64 3.10.12-1-22.04.9 [2263 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpython3.10-minimal amd64 3.10.12-1-22.04.9 [115 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgnutls30 amd64 3.7.3-0ubuntu1.6 [969 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssl amd64 3.0.2-0ubuntu1.19 [1186 kB]
Fetched 9496 kB in 10s (924 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
(Reading database ... 14120 files and directories currently installed.)
Preparing to unpack .../libssl3:amd64 (3.0.2-0ubuntu1.19) over (3.0.2-0ubuntu1.18) ...
Unpacking libssl3:amd64 (3.0.2-0ubuntu1.19) over (3.0.2-0ubuntu1.18) ...
Setting up libssl3:amd64 (3.0.2-0ubuntu1.19) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
Unpacking libssl3:amd64 (3.0.2-0ubuntu1.19) over (3.0.2-0ubuntu1.18) ...
Setting up libssl3:amd64 (3.0.2-0ubuntu1.19) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
(Reading database ... 14120 files and directories currently installed.)
Preparing to unpack .../python3.10 3.10.12-1-22.04.9 amd64.deb ...
Unpacking python3.10 (3.10.12-1-22.04.9) over (3.10.12-1-22.04.8) ...
Preparing to unpack .../libpython3.10-stdlib 3.10.12-1-22.04.9 amd64.deb ...
Unpacking libpython3.10-stdlib:amd64 (3.10.12-1-22.04.9) over (3.10.12-1-22.04.8) ...
Preparing to unpack .../python3.10-minimal 3.10.12-1-22.04.9 amd64.deb ...
Unpacking python3.10-minimal (3.10.12-1-22.04.9) over (3.10.12-1-22.04.8) ...
Preparing to unpack .../libpython3.10-minimal 3.10.12-1-22.04.9 amd64.deb ...
Unpacking libpython3.10-minimal:amd64 (3.10.12-1-22.04.9) over (3.10.12-1-22.04.8) ...
Preparing to unpack .../libpython3.10 3.10.12-1-22.04.9 amd64.deb ...
Unpacking libpython3.10:amd64 (3.10.12-1-22.04.9) over (3.10.12-1-22.04.8) ...
Setting up libpython3.10:amd64 (3.10.12-1-22.04.9) ...
(Reading database ... 14120 files and directories currently installed.)
Preparing to unpack .../openssl 3.0.2-0ubuntu1.19 amd64.deb ...
Unpacking openssl (3.0.2-0ubuntu1.19) over (3.0.2-0ubuntu1.18) ...
Setting up libpython3.10-minimal:amd64 (3.10.12-1-22.04.9) ...
Setting up python3.10-minimal (3.10.12-1-22.04.9) ...
Setting up python3.10 (3.10.12-1-22.04.9) ...
Setting up python3.10 (3.10.12-1-22.04.9) ...
Processing triggers for libc-bin (2.35-0ubuntu1.9) ...

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

Printing out logging configuration data
Script execution completed. Check system_security_report.txt for details.

```

```
root@Baker_Street_Linux_Server:~# cat system_security_report.txt
sshd configuration file:

# This is the sshd server system-wide configuration file. See
# sshd_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/*.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 no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
,
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

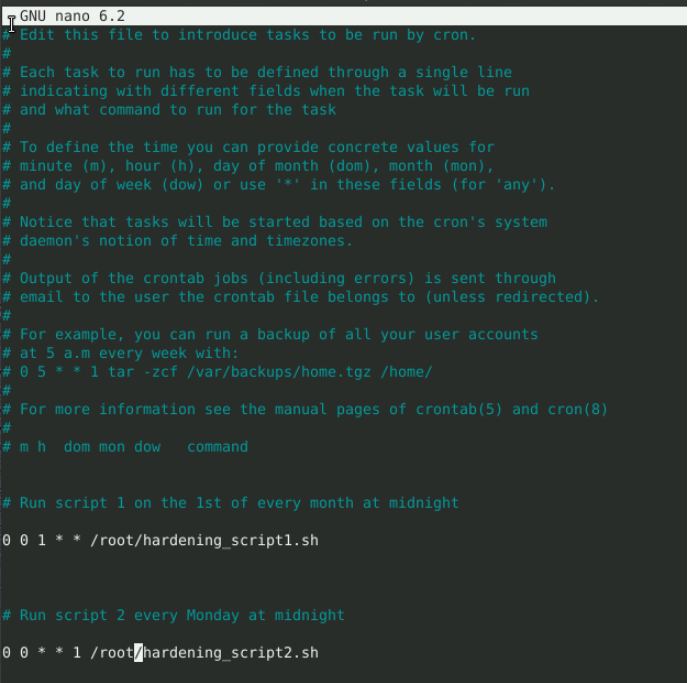
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords no

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

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
```

<ul style="list-style-type: none"> • 	<p>Scripts scheduled with cron</p>	 <pre>GNU nano 6.2 # 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 # 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 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 * * 1 tar -zcf /var/backups/home.tgz /home/ # # For more information see the manual pages of crontab(5) and cron(8) # # m h dom mon dow command # # Run script 1 on the 1st of every month at midnight 0 0 1 * * /root/hardening_script1.sh # # Run script 2 every Monday at midnight 0 0 * * 1 /root/hardening_script2.sh</pre>
---	------------------------------------	---

Summary of Security Findings

During the hardening process, several security risks were identified and mitigated to enhance the security posture of the system. Below is a summary of the key security concerns addressed:

1. Security Risks Identified

- Unrestricted SSH Access:

- Root login was enabled, allowing direct access to the system.
- Empty passwords were permitted, increasing the risk of unauthorized access.

- Unnecessary Services Running:

- MySQL and Samba were installed but not required, posing a potential attack vector.

- Insecure File Permissions:

- Some files in /home/ had world-readable and executable permissions (rwx for others), making them accessible to unauthorized users.

- Lack of Log Management:

- System logs were set to rotate weekly, allowing logs to grow excessively large or retain too much historical data.

- Outdated System Packages:

- The system was not regularly updated, leaving it vulnerable to security flaws and exploits.

2. Security Hardening Implemented

- SSH Hardening

- Root login disabled (PermitRootLogin no).

- Empty passwords disabled (PermitEmptyPasswords no).
- SSH access restricted to port 22 and Protocol 2 only.
- Firewall configured to allow only SSH access (ufw allow ssh).

- Service Removal
 - Unnecessary services disabled and removed:
 - MySQL (unless needed for database operations).
 - Samba (not required for file sharing in this system).
 - Removed dependencies and unused packages to reduce the attack surface.

- Log Rotation Improvements
 - Changed log rotation from weekly to daily.
 - Configured logs to retain data for 7 days only to prevent excessive log storage.
 - Captured system logs and SSH logs for auditing purposes.

- File Permission Fixes
 - World (others) permissions removed from sensitive files in /home/ to prevent unauthorized access.
 - Restricted access to specific department scripts:
 - Engineering scripts → Only the engineering group can read, write, and execute.
 - Research scripts → Restricted to the research group.
 - Finance scripts → Restricted to the finance group.

- Automated Security Maintenance
 - Scheduled system hardening scripts using cron:
 - Script 1 runs on the 1st of each month to maintain system security.
 - Script 2 runs every Monday to ensure logs, SSH settings, and updates remain in place.

- 3. Additional Security Recommendations
 - Implement Multi-Factor Authentication (MFA) for SSH
 - Add an extra security layer by requiring MFA before accessing the system.

 - Enforce Stronger Password Policies
 - Require minimum 12-character passwords with uppercase, lowercase, numbers, and special characters.
 - Implement password expiration policies to force users to change passwords periodically.

 - Enable Automatic Security Updates
 - Configure unattended-upgrades to apply security updates automatically:


```
sudo apt install unattended-upgrades -y
```

```
sudo dpkg-reconfigure --priority=low unattended-upgrades
```

 - Encrypt System Backups
 - Ensure that OS backups are encrypted and stored securely.

