



# Cybersecurity

## Project 1 Hardening Summary and Checklist

### OS Information

Customer	Baker Street Corporation																					
Hostname	<u>ip-172-22-117-119</u>																					
OS Version	<u>Linux ip-172-22-117-119 6.8.0-1016-aws #17-Ubuntu SMP Mon Sep 2 13:48:07 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux</u>																					
Memory information	<table><tr><td></td><td>total</td><td>used</td><td>free</td><td>shared</td><td>buff/cache</td><td>available</td></tr><tr><td>Mem:</td><td>3.7Gi</td><td>953Mi</td><td>1.3Gi</td><td>27Mi</td><td>1.8Gi</td><td>2.8Gi</td></tr><tr><td>Swap:</td><td>0B</td><td>0B</td><td>0B</td><td></td><td></td><td></td></tr></table>		total	used	free	shared	buff/cache	available	Mem:	3.7Gi	953Mi	1.3Gi	27Mi	1.8Gi	2.8Gi	Swap:	0B	0B	0B			
	total	used	free	shared	buff/cache	available																
Mem:	3.7Gi	953Mi	1.3Gi	27Mi	1.8Gi	2.8Gi																
Swap:	0B	0B	0B																			
Uptime information	<u>23:56:24 up 42 min, 1 user, load average: 0.00, 0.00, 0.00</u>																					

### Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
<input checked="" type="checkbox"/>	OS backup	<pre>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>

		<pre> /etc/mysql/mysql.conf.d/mysqld.cnf /etc/skel/ /etc/skel/.bashrc /etc/skel/.bash_logout /etc/skel/.profile /etc/rc0.d/ /etc/rc0.d/K01uidd /etc/rc0.d/K01open-iscsi /etc/rc0.d/K01unattended-upgrades /etc/rc0.d/K01open-vm-tools /etc/rc0.d/K01nmbd /etc/rc0.d/K01mysql /etc/rc0.d/K01cryptdisks /etc/rc0.d/K01plymouth /etc/rc0.d/K01openbsd-inetd /etc/rc0.d/K01cryptdisks-early /etc/rc0.d/K01smbd /etc/rc0.d/K01irqbalance /etc/rc0.d/K01chrony /etc/rc0.d/K01samba-ad-dc /etc/rc0.d/K01iscsid /etc/vtrgb /etc/subuid </pre> <p>Some of the items that were being backed up during the process</p>
<input checked="" type="checkbox"/>	Auditing users and groups	<pre> sysadmin@ip-172-22-117-119:/home\$ sudo userdel -r irene userdel: irene mail spool (/var/mail/irene) not found sysadmin@ip-172-22-117-119:/home\$ sudo userdel -r mary userdel: mary mail spool (/var/mail/mary) not found sysadmin@ip-172-22-117-119:/home\$ sudo userdel -r gregson userdel: gregson mail spool (/var/mail/gregson) not found sysadmin@ip-172-22-117-119:/home\$ ls adler moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson </pre> <p>Deleted users lestrade,irene,mary,and gregson</p> <pre> sysadmin@ip-172-22-117-119:/home\$ sudo usermod -L moriarty sysadmin@ip-172-22-117-119:/home\$ sudo usermod -L mrs_hudson sysadmin@ip-172-22-117-119:/home\$ ls adler moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson </pre> <p>Locked users moriarty and mrs_hudson as they are on temporary leave</p> <pre> sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U sherlock sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U watson sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U mycroft sysadmin@ip-172-22-117-119:/home\$ sudo usermod -p toby123 toby sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U toby sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U adler usermod: unlocking the user's password would result in a passwordless account. You should set a password with usermod -p to unlock this user's password. sysadmin@ip-172-22-117-119:/home\$ sudo usermod -p adlerpwd adler sysadmin@ip-172-22-117-119:/home\$ sudo usermod -U adler sysadmin@ip-172-22-117-119:/home\$ ls adler moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson </pre> <p>Unlocked users sherlock,watson,mycroft,toby, and adler. Had to create a password for users toby and adler to unlock.</p> <pre> sysadmin@ip-172-22-117-119:/home\$ sudo usermod -g research mycroft </pre> <pre> sysadmin@ip-172-22-117-119:/home\$ groups mycroft mycroft : research marketing </pre> <p>After discovering that mycroft was part of the marketing team using cat /etc/groups, we changed</p>

		<p>the user to the research team</p> <pre>sysadmin@ip-172-22-117-119:/home\$ sudo deluser mycroft marketing info: Removing user 'mycroft' from group 'marketing' ... sysadmin@ip-172-22-117-119:/home\$ groups mycroft mycroft : research</pre> <p>We then remove mycroft from the marketing group as it does not exist anymore</p> <pre>sysadmin@ip-172-22-117-119:/home\$ sudo delgroup marketing info: Removing group 'marketing' ... sysadmin@ip-172-22-117-119:/home\$ cat /etc/group   grep marketing sysadmin@ip-172-22-117-119:/home\$</pre> <p>As there is no more marketing group, we delete it and then check to see if it is there, and it no longer exists.</p>
<input checked="" type="checkbox"/>	Updating and enforcing password policies	<pre># here are the per-package modules (the "Primary" block) password      requisite pam_pwquality.so retry=2 minlen=8 ucredit=-1 ocredit=-1</pre> <p>Nanoed into the file and added the updates to the password: minlen=8,retry=2,ucredit=-1,ocredit=-1. The negative values are because it required at least one uppercase letter and special character.</p> <p>Had to add libpam-pwquality to the library as it was not present originally when nanoing into the file.</p>
<input checked="" type="checkbox"/>	Updating and enforcing sudo permissions	<pre>@includedir /etc/sudoers.d sysadmin ALL=(ALL:ALL) ALL sysadmin ALL=(ALL:ALL) ALL sherlock ALL=(ALL:ALL) ALL watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh research ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh #moriarty ALL=(ALL) NOPASSWD:ALL sysadmin ALL=(ALL:ALL) ALL</pre> <p>In the sudoers file, changed sudo permissions to allow only sherlock all sudo permissions, watson and mycroft sudo permission to /var/loglogcleanup.sh, and research group sudo permission to run the script /tmp/script/research_script.sh.</p>

<input checked="" type="checkbox"/>	<p>Validating and updating permissions on files and directories</p>	<pre> sysadmin@ip-172-22-117-60:/home\$ sudo find /home -perm /o-rwx -exec chmod o-rwx {} \; sysadmin@ip-172-22-117-60:/home\$ sudo find /home -perm /o-rwx sysadmin@ip-172-22-117-60:/home\$ </pre> <p>After finding the world permission files, we changed them so none were world permission files, and confirming that none were there.</p> <pre> sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "engineering" /home/mrs.hudson/Engineering_script.sh.1.txt /home/toby/Engineering_script.sh.2.txt /home/mycroft/Engineering_script.sh.0.txt /home/adler/Engineering_script.sh_script2.sh /home/adler/Engineering_script.sh.3.txt /home/adler/Engineering_script.sh_script1.sh /home/adler/Engineering_script.sh.0.txt sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "engineering" -exec chgrp engineering {} \; -exec chmod 770 {} \; sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "engineering" /home/mrs.hudson/Engineering_script.sh.1.txt /home/toby/Engineering_script.sh.2.txt /home/mycroft/Engineering_script.sh.0.txt /home/adler/Engineering_script.sh_script2.sh /home/adler/Engineering_script.sh.3.txt /home/adler/Engineering_script.sh_script1.sh /home/adler/Engineering_script.sh.0.txt </pre> <p>Next was to find the scripts with engineering in it. After finding them, changed it to wear only the owner and engineering group could read, write and execute.</p> <pre> sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "finance" /home/watson/Finance_script.sh_script2.sh /home/watson/Finance_script.sh_script1.sh /home/watson/Finance_script.sh.3.txt /home/moriarty/Finance_script.sh.2.txt /home/moriarty/Finance_script.sh.0.txt /home/mycroft/Finance_script.sh_script2.sh /home/mycroft/Finance_script.sh_script1.sh /home/mycroft/Finance_script.sh.3.txt sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "finance" -exec chgrp finance {} \; -exec chmod 770 {} \; sysadmin@ip-172-22-117-60:/home\$ sudo find /home -iname "finance" /home/watson/Finance_script.sh_script2.sh /home/watson/Finance_script.sh_script1.sh /home/watson/Finance_script.sh.3.txt /home/moriarty/Finance_script.sh.2.txt /home/moriarty/Finance_script.sh.0.txt /home/mycroft/Finance_script.sh_script2.sh /home/mycroft/Finance_script.sh_script1.sh /home/mycroft/Finance_script.sh.3.txt </pre> <p>Then did the same thing for finance and changed all the scripts to be read, written, and executed by the owner and finance group.</p> <p>Tried for research, but found no research.sh files in the home directory.</p> <pre> sysadmin@ip-172-22-117-60:~\$ sudo grep -iRL 'password' /home /home/sherlock/my_file.txt /home/watson/my_file.txt /home/moriarty/my_file.txt sysadmin@ip-172-22-117-60:~\$ sudo rm /home/sherlock/my_file.txt sysadmin@ip-172-22-117-60:~\$ sudo rm /home/watson/my_file.txt sysadmin@ip-172-22-117-60:~\$ sudo rm /home/moriarty/my_file.txt </pre> <p>Then we were tasked with finding any files that employees may have left a password in. With the find, we found sherlock, watson, and mycroft had files where the word password was used, so we deleted those files from the system.</p>
	<p>Optional: Updating password hashing configuration</p>	



## Auditing and securing SSH

```
#Include /etc/ssh/sshd_config.d/*.conf
Port 22
#Port 2223
#Port 2224
#Port 2225
#Port 8967

#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
```

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

We were asked to ensure that SSH was not allowed to have the ability to have empty passwords, root users, and to have any ports besides 22. I changed the yes to no for empty passwords and root users, and then commented out all the ports and left Port 22 uncommented.

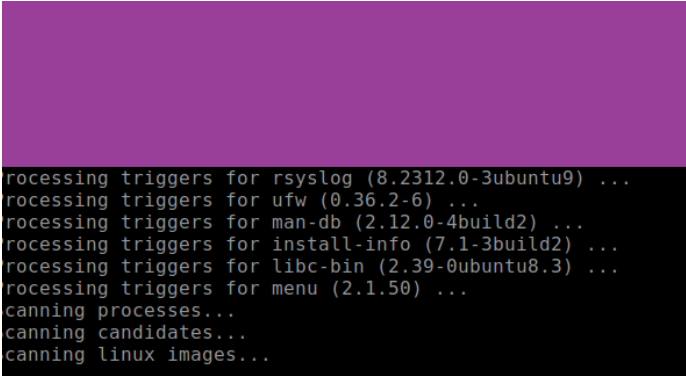
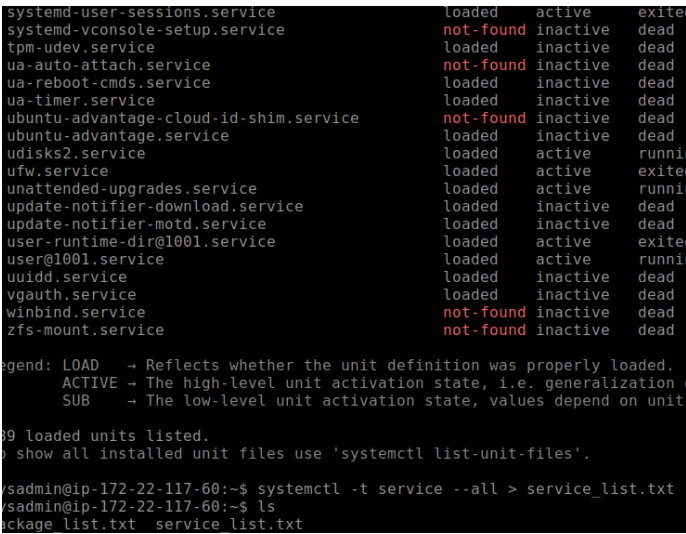
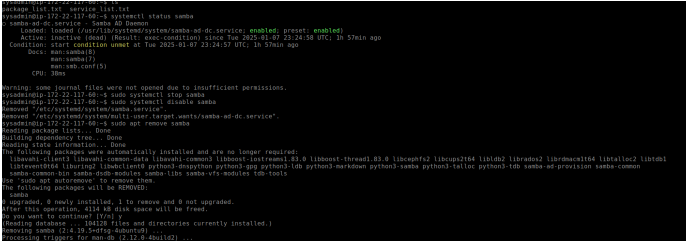
```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
Protocol 2
```

We were then asked to enable Protocol 2, so I changed Protocol 1 to Protocol 2.

```
sysadmin@ip-172-22-117-60:/home$ service ssh restart
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Authenticating as: Ubuntu (ubuntu)
Password:
==== AUTHENTICATION COMPLETE ====
sysadmin@ip-172-22-117-60:/home$
```

I then updated the SSH service with the new updates using the given command **service ssh restart**.

<input checked="" type="checkbox"/>	Reviewing and updating system packages	<pre>Setting up cloud-init (24.4.0ubuntu1-24.04.2) ... Setting up open-iscsi (2.1.9-3ubuntu5.2) ... Installing new version of config file /etc/iscsi/iscsid.conf ... Setting up software-properties-common (0.99.49.1) ... Setting up python3-boto3 (1.34.46+repack-lubuntu1) ... Setting up libgssapi-krb5-2:amd64 (1.20.1-6ubuntu2.2) ... Setting up update-manager-core (1:24.04.9) ... Setting up initramfs-tools-core (0.142ubuntu25.4) ... Setting up initramfs-tools (0.142ubuntu25.4) ... update-initramfs: deferring update (trigger activated) Setting up python3-s3transfer (0.10.1-lubuntu2) ... Setting up python3-boto3 (1.34.46+dfsg-lubuntu1) ... Setting up apport-core-dump-handler (2.28.1-0ubuntu3.3) ... Setting up apport (2.28.1-0ubuntu3.3) ... apport-autoreport.service is a disabled or a static unit not run Processing triggers for dbus (1.14.10-4ubuntu4.1) ... Processing triggers for libc-bin (2.39-0ubuntu8.3) ... Processing triggers for rsyslog (8.2312.0-3ubuntu9) ... Processing triggers for man-db (2.12.0-4build2) ... Processing triggers for initramfs-tools (0.142ubuntu25.4) ... update-initramfs: Generating /boot/initrd.img-6.8.0-1021-aws Scanning processes... Scanning candidates... Scanning linux images...  Running kernel seems to be up-to-date.</pre> <p>After running apt update, we can see how the package manager is making sure it has all the latest packages.</p> <pre>sysadmin@ip-172-22-117-60:~\$ sudo apt upgrade -y Reading package lists... Done Building dependency tree... Done Reading state information... Done Calculating upgrade... Done 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.</pre> <p>It shows now that if we run apt upgrade -y, we see that all packages are updated and installed.</p> <pre>sysadmin@ip-172-22-117-60:~\$ apt list --installed &gt; package_list.txt WARNING: apt does not have a stable CLI interface. Use with caution in scripts.  sysadmin@ip-172-22-117-60:~\$ ls package_list.txt</pre> <p>I created a text file called package_list.txt that lists all the installed packages.</p> <pre>sysadmin@ip-172-22-117-60:~\$ sudo apt remove telnet -y Reading package lists... Done Building dependency tree... Done Reading state information... Done The following packages will be REMOVED:   telnet 0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded. After this operation, 48.1 kB disk space will be freed. (Reading database ... 103593 files and directories currently installed.) Removing telnet (0.17+2.5-3ubuntu4) ...</pre> <p>The telnet package was installed so I removed it. Telnet can lead to security issues as they leave passwords and data in plain text unencrypted, which leaves that vulnerable to hackers attacking.</p> <pre>sysadmin@ip-172-22-117-60:~\$ sudo apt autoremove -y Reading package lists... Done Building dependency tree... Done Reading state information... Done 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.</pre> <p>Then I tried to remove any dependencies that may have been present, but there were none to be removed.</p>
-------------------------------------	--	--

		<div></div> <p>We were then tasked with installing,ufw,lynis, and tripwire. The image shows it being installed. At one point I was asked to create a sitekey and localkey for the configuration.UFW creates an easy interface for configuring common firewall cases. Lynis can perform an extensive health scan of your systems to check for security risks and creates a report of that. Tripwire can monitor for unauthorized file and directory manipulation on local systems.</p>
<input checked="" type="checkbox"/>	Disabling unnecessary services	<div></div> <p>After listing out all the services, I added them to the text file service_list.txt.</p> <div></div> <p>This shows me stopping, disabling, and removing the service samba. This is one of the two services</p>

		<p>we were asked to check for and remove from the system. The other service was mysql which looked similar to this when doing the process of stopping, disabling, and removing the services.</p>
<input checked="" type="checkbox"/>	Enabling and configuring logging	<pre>[Journal] Storage=persistent #Compress=yes #Seal=yes #SplitMode=uid #SyncIntervalSec=5m #RateLimitIntervalSec=30s #RateLimitBurst=10000 SystemMaxUse=300M #SystemKeepFree= #SystemMaxFileSize= #SystemMaxFiles=100 #RuntimeMaxUse= #RuntimeKeepFree= #RuntimeMaxFileSize= #RuntimeMaxFiles=100 #MaxRetentionSec= #MaxFileSec=1month #ForwardToSyslog=no #ForwardToKMsg=no #ForwardToConsole=no #ForwardToWall=yes #TTYPath=/dev/console #MaxLevelStore=debug</pre> <p>I moved to the /etc/systemd/ directory and nanoed into the journald.conf file. In it, I changed storage=persistent, and SystemMaxUse=300M as was required.</p> <pre># rotate log files daily daily  # use the adm group by default, since this is the owning group # of /var/log/. su root adm  # keep 7 days worth of backlogs rotate 7</pre> <p>We were then tasked to help prevent logs from taking up too much space. I changed the rotation of logs from weekly to daily and then changed the rotate of 4 weeks worth of logs to 7 days worth of logs.</p> <p>All the changes were saved.</p>



<div data-bbox="253 212 285 243"><input checked="" type="checkbox"/></div>	<div data-bbox="505 212 699 243">Scripts created</div>	<div data-bbox="802 212 1479 926"><pre>#!/bin/bash  # Variable for the report output file, choose an output file name REPORT_FILE="hardening_script_1.txt"  # Output the hostname echo "Gathering hostname..."  # Placeholder for command to get the hostname echo "Hostname: \$(hostname)" &gt;&gt; \$REPORT_FILE printf "\n" &gt;&gt; \$REPORT_FILE  # Output the OS version echo "Gathering OS version..."  # Placeholder for command to get the OS version echo "OS Version: \$(uname -a)" &gt;&gt; \$REPORT_FILE printf "\n" &gt;&gt; \$REPORT_FILE  # Output memory information echo "Gathering memory information..."  # Placeholder for command to get memory info echo "Memory Information: \$(free -h)" &gt;&gt; \$REPORT_FILE printf "\n" &gt;&gt; \$REPORT_FILE</pre></div> <div data-bbox="802 936 1479 999">Here is a little chunk out of hardening_script1.sh as I nanoed in and began scripting.</div> <div data-bbox="802 1010 1479 1356"><pre>/etc/dpkg/ /etc/dpkg/dpkg.cfg.d/ /etc/dpkg/dpkg.cfg.d/needrestart /etc/dpkg/origins/ /etc/dpkg/origins/ubuntu /etc/dpkg/origins/default /etc/dpkg/origins/debian /etc/dpkg/dpkg.cfg /etc/python3.12/ /etc/python3.12/sitecustomize.py /etc/ld.so.conf /etc/xattr.conf Gathering sudoers file... 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 hardening script 1.txt for details.</pre></div> <div data-bbox="802 1367 1479 1430">After fixing errors and running the script a couple times, we see that the script ran as written.</div> <div data-bbox="802 1440 1479 1808"><pre># See sudoers(5) for more information on "@include" directives:  @includedir /etc/sudoers.d sysadmin ALL=(ALL:ALL) ALL sysadmin ALL=(ALL:ALL) ALL sherlock ALL=(ALL:ALL) ALL watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh research ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh #moriarty ALL=(ALL) NOPASSWD:ALL sysadmin ALL=(ALL:ALL) ALL  World permissions have been removed from any files found.  Permissions updated for Engineering scripts. Permissions updated for Research scripts Permissions updated for Finance scripts.</pre></div> <div data-bbox="802 1818 1479 1881">As we cat the report file, the permissions have been updated and the list of users with sudo access is</div>
--	--	--

there. At the top it lists the hostname, os version, memory information and uptime information.

```
echo "Installed Packages:$(sudo 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: $(sudo cat /etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Placeholder for command to display logrotate data

echo "logrotate.conf file data:$(sudo cat /etc/logrotate.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Script execution completed. Check $REPORT_FILE for details."
```

Here is a chunk of the second hardening script. In this example, we see the scripts for listing the installed packages, and showing the data from journald.conf and logrotate.conf.

```
Get:1 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-host amd64 1:9.18.30-0ubuntu0.24.04.1 [60.4 kB]
Get:2 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-dnswriter amd64 1:9.18.30-0ubuntu0.24.04.1 [155 kB]
Get:3 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-dnswriter amd64 1:9.18.30-0ubuntu0.24.04.1 [1251 kB]
Fetched 1450 kB in 6s (43.1 MB/s)
(Reading database ... 104015 files and directories currently installed.)
Preparing to unpack .../bind9-host_1:9.18.30-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9-host (1:9.18.30-0ubuntu0.24.04.1) over (1:9.18.28-0ubuntu0.24.04.1) ...
Preparing to unpack .../bind9-dnswriter_1:9.18.30-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9-dnswriter (1:9.18.30-0ubuntu0.24.04.1) over (1:9.18.28-0ubuntu0.24.04.1) ...
Preparing to unpack .../bind9-dnswriter_1:9.18.30-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9-dnswriter (1:9.18.30-0ubuntu0.24.04.1) over (1:9.18.28-0ubuntu0.24.04.1) ...
Setting up bind9-host (1:9.18.30-0ubuntu0.24.04.1) ...
Setting up bind9-dnswriter (1:9.18.30-0ubuntu0.24.04.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu0.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

"Printing out logging configuration data"
Script execution completed. Check hardening script2 report.txt for details.
```

After running the script, it was completed so I can go look at the report file.

		<pre> sshd configuration file: # This is the ssh client system-wide configuration file. See # ssh_config(5) for more information. This file provides defaults for # users, and the values can be changed in per-user configuration files # or on the command line.  # Configuration data is parsed as follows: # 1. command line options # 2. user-specific file # 3. system-wide file # Any configuration value is only changed the first time it is set. # Thus, host-specific definitions should be at the beginning of the # configuration file, and defaults at the end.  # Site-wide defaults for some commonly used options. For a comprehensive # list of available options, their meanings and defaults, please see the # ssh_config(5) man page.  Include /etc/ssh/ssh_config.d/*.conf  Host * # ForwardAgent no # ForwardX11 no # ForwardX11Trusted yes # PasswordAuthentication yes # HostbasedAuthentication no # GSSAPIAuthentication no # GSSAPIDelegateCredentials no # GSSAPIKeyExchange no # GSSAPITrustDNS no # BatchMode no # CheckHostIP no # AddressFamily any # ConnectTimeout 0 # StrictHostKeyChecking ask # IdentityFile ~/.ssh/id_rsa # IdentityFile ~/.ssh/id_dsa # IdentityFile ~/.ssh/id_ecdsa # IdentityFile ~/.ssh/id_ed25519 # Port 22 </pre> <p>When opening hardening_script2_report.txt, I immediately see the sshd configuration file. Scrolling through it using the more command, I saw the list of installed packages as well as the data contents of the journald.conf and logrotate.conf files as well.</p>
<input checked="" type="checkbox"/>	Scripts scheduled with cron	<pre> # For example, you can run a backup of all your user accounts I # at 5 a.m every week with: # 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/  #Run hardeing script 1 once a month on the first of the month 0 0 1 * * /home/sysadmin/hardening_script1.sh  #Run hardening script 2 once a week every Monday 0 0 * * 1 /home/sysadmin/hardening_script2.sh </pre> <p>The cron jobs for the hardening scripts were asked for script 1 on the first day of every month and for script 2 once a week every monday. So I used a cron job calculator to get the correct format for each specific job.</p>

		<pre>sysadmin@ip-172-22-117-60:~\$ sudo crontab -l # 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/  #Run hardeing script 1 once a month on the first of the month 0 0 1 * * /home/sysadmin/hardening_script1.sh  #Run hardening script 2 once a week every Monday 0 0 * * 1 /home/sysadmin/hardening_script2.sh</pre> <p>The cron jobs are now listed when asking the system for the list of cron jobs.</p>
--	--	--

The only concern I had was the telnet package being installed on the system. Telnet being installed can lead to security issues as they leave passwords and data in plain text unencrypted, which leaves that vulnerable to hackers attacking. I removed this when looking for it so that this would not be a problem for the system and its users.