



Cybersecurity

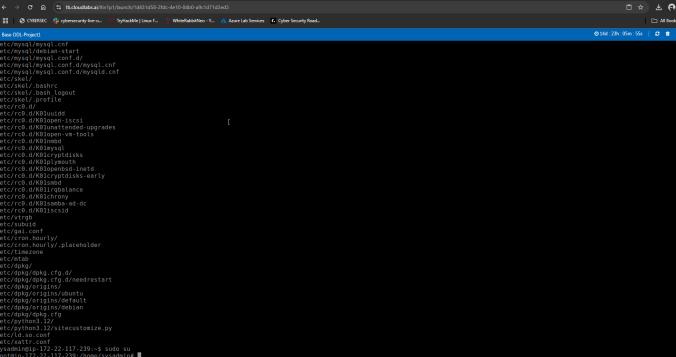
Project 1 Hardening Summary and Checklist

OS Information

Customer	Baker Street Corporation
Hostname	Command used: hostname Output: ip-172-22-117-239
OS Version	Command used: lsb_release -a Output: <pre>root@ip-172-22-117-239:/home# lsb_release -a No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 24.04.1 LTS Release: 24.04 Codename: noble root@ip-172-22-117-239:/home#</pre>
Memory information	Command used: free -h Output: <pre>root@ip-172-22-117-239:/home/sysadmin# free -h total used free shared buff/cache available Mem: 3.7Gi 835Mi 2.7Gi 5.8Mi 423Mi 2.9Gi Swap: 0B 0B 0B</pre>
Uptime information	Command used: uptime Output: <pre>root@ip-172-22-117-239:/home/sysadmin# uptime 01:00:48 up 10 min, 2 users, load average: 0.01, 0.04, 0.03</pre>

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
-----------	----------	--

<input checked="" type="checkbox"/>	OS backup	<p>Command used: 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 /</p> <p>Output:</p>  <pre> root@baker-street:~# 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 / root@baker-street:~# </pre> <p>#sidenote: I ran the code posted in the guide but when i clicked out of the vm, the whole thing refreshed and took me out of root. I had done so before, but the second to last line in the screenshot is me switching back to root.</p>
<input checked="" type="checkbox"/>	Auditing users and groups	<p>(deleting irene) Command used: sudo deluser --remove-all-files irene</p> <p>Output:</p>  <pre> root@baker-street:~# sudo deluser --remove-all-files irene root@baker-street:~# </pre> <p>(deleting mary) Command used: sudo deluser --remove-all-files mary</p> <p>Output:</p> <pre> root@baker-street:~# sudo deluser --remove-all-files mary info: Looking for files to backup/remove ... </pre> <p>(deleting gregson) Command used: sudo deluser --remove-all-files gregson</p> <p>Output:</p>

```
root@ip-172-22-117-239:/home/sysadmin# sudo deluser --remove-all-files gregson
info: Looking for files to backup/remove ...
info: Not backing up/removing '/bin', it matches ^/bin$.
info: Not backing up/removing '/lib', it matches ^/lib$.
info: Not backing up/removing '/lib64', it matches ^/lib$.
info: Not backing up/removing '/sbin', it matches ^/sbin$.
info: Not backing up/removing '/media', it matches ^/media$.
info: Not backing up/removing '/lib usr-ismerged', it matches ^/lib$.
info: Not backing up/removing '/boot', it matches ^/boot$.
info: Not backing up/removing '/srv', it matches ^/srv$.
info: Not backing up/removing '/usr', it matches ^/usr$.
info: Not backing up/removing '/run', it matches ^/run$.
info: Not backing up/removing '/sys', it is a mount point.
warn: Cannot handle special file /snap/core18/2846/dev/null
warn: Cannot handle special file /snap/core18/2846/dev/random
warn: Cannot handle special file /snap/core18/2846/dev/urandom
warn: Cannot handle special file /snap/core18/2846/dev/zero
```

- (locking temporary leave staff)

Command used:

```
sudo usermod -L moriarty
sudo usermod -L mrs_hudson
```

output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -L moriarty
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -L mrs_hudson
```

- (unlocking employed users)

Command used:

```
sudo passwd -d adler (bypasses "no password"
error when using sudo usermod -U adler)
```

```
sudo usermod -U adler
```

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo passwd -d adler
passwd: password changed.
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -U adler
```

Command used: sudo passwd -d toby (bypasses "no password" error)

```
sudo usermod -U toby
```

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo passwd -d toby
passwd: password changed.
root@ip-172-22-117-239:/home/sysadmin# openssl passwd -l "new_password"
sudo usermod -U toby
```

(please ignore the openssl command)

- (creating and moving group users from marketing to research group)

(creating research group) Command used: sudo addgroup research

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo addgroup research
info: Selecting GID from range 1000 to 59999 ...
info: Adding group 'research' (GID 1009) ...
```

		<p>(checking users) Command used: groups <username></p> <p>then</p> <p>(moving moriarty) Command used: sudo usermod -G research moriarty</p> <p>Output:</p> <pre>root@ip-172-22-117-239:/home/sysadmin# groups sherlock sherlock : sherlock engineering root@ip-172-22-117-239:/home/sysadmin# groups watson watson : watson engineering root@ip-172-22-117-239:/home/sysadmin# groups mycroft mycroft : mycroft marketing root@ip-172-22-117-239:/home/sysadmin# groups moriarty moriarty : moriarty engineering root@ip-172-22-117-239:/home/sysadmin# groups mrs_hudson mrs_hudson : mrs_hudson finance root@ip-172-22-117-239:/home/sysadmin# groups mary groups: 'mary': no such user root@ip-172-22-117-239:/home/sysadmin# groups toby toby : toby root@ip-172-22-117-239:/home/sysadmin# groups adler adler : adler root@ip-172-22-117-239:/home/sysadmin# sudo usermod -G research moriarty</pre> <p>(deleting marketing group) Command used: sudo delgroup marketing</p> <p>Output:</p> <pre>root@ip-172-22-117-239:/home/sysadmin# sudo usermod -G research moriarty root@ip-172-22-117-239:/home/sysadmin# sudo delgroup marketing info: Removing group 'marketing' ...</pre>
<input checked="" type="checkbox"/>	Updating and enforcing password policies	<p>Command used: apt-get install libpam-pwquality</p> <p>Output:</p>  <p>(bottom of install, way too long to screenshot full install)</p> <p>(Common password file prior to editing password requisites):</p> <pre>/etc/pam.d/common-passwd: password-related modules common to all services # This file contains a list of modules that are loaded for all services in the # system. It is used by the pam_start(3) function in libpam.0. It is also used # by the pam_sm_setcred(3) module, introduced in version # 1.1. With this module, it is possible to have a password module that will be shared # between several services. This is useful for example if you want to have a # common module for both root and regular users. See the man-page for # common(1) for more information. # # As of pam 1.0.6, this file is managed by pam-passwd-update by default. # If you want to manage it yourself, you must use the 'use_pam' option and # pass the 'modules' parameter to the 'pam_start' function. # # Note: the default 'pam_unix' module, the 'primary' module, is set to 'strict=1 credit=1 retry=3' # and 'use_pam' is set to 'no'. This means that pam_unix will always fail if # the password is incorrect, even if the user has already # tried several times. This is a security bug that needs to be fixed. See the # pam_unix(1) man-page for more information.</pre> <p>(new password policies) command used: minlen=8 dcredit=-1 ucredit=-1 lcredit=0 ocredit=-1 retry=2</p> <p>Output:</p>

		<pre>#Updated password policies password requisite pam_pwquality.so minlen=8 dcredit=-1 ucredit=0 ocredit=-1 retry=2</pre>
<input checked="" type="checkbox"/>	Updating and enforcing sudo permissions	<ul style="list-style-type: none"> (giving sherlock full sudo privileges) <p>Command used: sudo visudo (opens sudoers file) sherlock ALL=(ALL) NOPASSWD:ALL</p> <ul style="list-style-type: none"> (giving sudo privileges to mycroft and watson to run logcleanup.sh) <p>Command used: mycroft ALL=(ALL) /var/log/logcleanup.sh watson ALL=(ALL) /var/log/logcleanup.sh</p> <p>(giving research group privileges to run research_script.sh)</p> <p>Command used: %research ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh</p> <p>Output (for all the above):</p> <pre>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 DEBUGNAME" # "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 Defaults: sudo env_keep += "\$GPG_AGENT_INFO" # Host alias specification # User alias specification # Cmd alias specification # User privilege specification # 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 #sysadmin ALL=(ALL:ALL) ALL #sysadmin ALL=(ALL:ALL) ALL #sherlock ALL=(ALL) NOPASSWD:ALL #graham ALL=(ALL:ALL) ALL #Sudo Privileges to run logcleanup.sh #mycroft ALL=(ALL) /var/log/logcleanup.sh #watson ALL=(ALL) /var/log/logcleanup.sh #Sudo Group privileges for research script.sh %research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh</pre>
<input checked="" type="checkbox"/>	Validating and updating permissions on files and directories	<ul style="list-style-type: none"> (removing world permissions from user's home directories) <p>Command used: chmod o-x <filename>, chmod o-r <filename>, chmod o-w <filename></p> <p>(sherlock) Output:</p> <pre>root@ip-172-31-22-117:~# chmod o-w deduction.doc_script1.sh total 12 -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 deduction.doc_3.txt -rwxr--x-- 1 sherlock sherlock 49 Oct 22 16:13 DEDUCTION_DOC_SCRIPT1.sh -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 game_is_afoot.txt_3.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file1.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file2.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file3.txt root@ip-172-31-22-117:~# ls -l total 12 -rwxr--x-- 1 sherlock sherlock 49 Oct 22 16:13 deduction.doc_script1.sh -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 deduction.doc_3.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 DEDUCTION_DOC_SCRIPT1.sh -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 game_is_afoot.txt_3.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file1.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file2.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file3.txt root@ip-172-31-22-117:~# ls -l total 12 -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 deduction.doc_3.txt -rwxr--x-- 1 sherlock sherlock 49 Oct 22 16:13 DEDUCTION_DOC_SCRIPT1.sh -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 game_is_afoot.txt_3.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file1.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file2.txt -rwxr--x-- 1 sherlock sherlock 0 Oct 22 16:13 my_file3.txt</pre>

(watson) Output:

```
root@ip-172-22-117-239:~/home# cd Watson
total 12
-rwxr--r-- 1 Watson Watson 0 Oct 22 16:35 Finance script.sh 3.txt
-rwxr--r-- 1 Watson Watson 47 Oct 22 16:35 Finance script.sh script1.sh
-rwxr--r-- 1 Watson Watson 47 Oct 22 16:35 Finance script.sh script2.sh
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_0.txt
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_2.txt
-rw-r--r-- 1 Watson Watson 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:~/home/Watson# chmod o-r Finance script.sh 3.txt
root@ip-172-22-117-239:~/home/Watson# chmod o-rx Finance script.sh
Finance script.sh 3.txt
root@ip-172-22-117-239:~/home/Watson# chmod o-rx Finance script.sh script1.sh
root@ip-172-22-117-239:~/home/Watson# chmod o-rx Finance script.sh script2.sh
root@ip-172-22-117-239:~/home/Watson# chmod o-rx deduction.doc_0.txt
root@ip-172-22-117-239:~/home/Watson# chmod o-r deduction.doc_1.txt
root@ip-172-22-117-239:~/home/Watson# chmod o-r deduction.doc_2.txt
root@ip-172-22-117-239:~/home/Watson# total 12
total 12
-rwxr--r-- 1 Watson Watson 0 Oct 22 16:35 Finance script.sh 3.txt
-rwxr--r-- 1 Watson Watson 47 Oct 22 16:35 Finance script.sh script1.sh
-rwxr--r-- 1 Watson Watson 47 Oct 22 16:35 Finance script.sh script2.sh
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_0.txt
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 Watson Watson 0 Oct 22 16:35 deduction.doc_2.txt
-rw-r--r-- 1 Watson Watson 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:~/home/Watson#
```

(moriarty) Output:

```
ootelp-172-22-117-239:/home/moriarty# chmod o+r Finance_script.sh 0.txt
root@ip-172-22-117-239:/home/moriarty# chmod o+r Finance_script.sh 2.txt
root@ip-172-22-117-239:/home/moriarty# chmod o+r elementary.txt 1.txt
root@ip-172-22-117-239:/home/moriarty# chmod o+r game_is_afoot.txt 3.txt
root@ip-172-22-117-239:/home/moriarty# chmod o+r game_is_afoot.txt script1.sh
root@ip-172-22-117-239:/home/moriarty# chmod o+r game_is_afoot.txt script2.sh
root@ip-172-22-117-239:/home/moriarty# la -l
total 28
-rw-r--r-- 1 moriarty moriarty 220 Mar 31 2024 bash_logout
-rw-r--r-- 1 moriarty moriarty 8163 Dec 3 22:12 bashrc
-rw-r--r-- 1 moriarty moriarty 807 Mar 31 2024 .profile
-rw-r--r-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_0.txt
-rw-r--r-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_2.txt
-rwxr-x--- 1 moriarty moriarty 0 Oct 22 16:35 game_is_afoot.txt_1.sh
-rwxr-x--- 1 moriarty moriarty 0 Oct 22 16:35 game_is_afoot.txt_3.sh
-rwxr-x--- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt script1.sh
-rwxr-x--- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt script2.sh
-rw-r--r-- 1 moriarty moriarty 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/moriarty# ls -l
total 12
-rw-r--r-- 1 moriarty moriarty 0 Oct 09 22 16:35 Finance_script.sh_0.txt
-rw-r--r-- 1 moriarty moriarty 0 Oct 09 22 16:35 Finance_script.sh_2.txt
-rwxr-x--- 1 moriarty moriarty 0 Oct 09 22 16:35 game_is_afoot.txt_1.sh
-rwxr-x--- 1 moriarty moriarty 0 Oct 09 22 16:35 game_is_afoot.txt_3.sh
-rwxr-x--- 1 moriarty moriarty 49 Oct 09 22 16:35 game_is_afoot.txt script1.sh
-rwxr-x--- 1 moriarty moriarty 49 Oct 09 22 16:35 game_is_afoot.txt script2.sh
-rw-r--r-- 1 moriarty moriarty 54 Oct 09 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/moriarty#
```

(mycroft) Output:

```
root@ip-172-22-117-230:~/home/mycroft# ls -l
total 8
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Engineering_script.sh 0.txt
-rw-r--r-- 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh 3.txt
-rwxr--r-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh script1.sh
-rwxr--r-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh script2.sh
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc 2.txt
root@ip-172-22-117-230:~/home/mycroft# chmod o-r Engineering_script.sh 0.txt
root@ip-172-22-117-230:~/home/mycroft# chmod o-r Finance_script.sh script1.s
root@ip-172-22-117-230:~/home/mycroft# chmod o-r Finance_script.sh script2.s
root@ip-172-22-117-230:~/home/mycroft# chmod o-r deduction.doc 1.txt
root@ip-172-22-117-230:~/home/mycroft# chmod o-r deduction.doc 2.txt
root@ip-172-22-117-230:~/home/mycroft# ls
total 8
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Engineering_script.sh 0.txt
-rw-r--r-- 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh 1.sh
-rwxr--r-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh script1.sh
-rwxr--r-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh script2.sh
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc 1.txt
```

(mrs hudson) Output:

```
root@ip-172-22-117-239:/home# cd mrs_hudson
/home/mrs_hudson$ ls -l
total 8
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 Engineering_script.sh 1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 deduction.doc 2.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 deduction.doc 3.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 elementary.txt 3.txt
-rwxr-xr-x 1 mrs_hudson mrs_hudson 21 Oct 22 16:35 elementary.txt_script1.sh
-rwxr-xr-x 1 mrs_hudson mrs_hudson 21 Oct 22 16:35 elementary.txt_script2.sh
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r Engineering_script.sh 1.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r deduction.doc 2.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r deduction.doc 3.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r elementary.txt 3.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r elementary.txt_script1.sh
root@ip-172-22-117-239:/home/mrs_hudson# chmod +r elementary.txt_script2.sh
root@ip-172-22-117-239:/home/mrs_hudson$ ls -l
total 8
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 Engineering_script.sh 1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 deduction.doc 2.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 deduction.doc 3.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 0 Oct 22 16:35 elementary.txt 3.txt
-rwxr-xr-x 1 mrs_hudson mrs_hudson 21 Oct 22 16:35 elementary.txt_script1.sh
-rwxr-xr-x 1 mrs_hudson mrs_hudson 21 Oct 22 16:35 elementary.txt_script2.sh
```

(toby) Output:

```
[root@ip-172-22-117-239 ~]# /home/toby cd toby
[root@ip-172-22-117-239 ~]# /home/toby ls -l
total 8
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 Engineering.script.sh_2.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 deduction.doc_1.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 elementary.txt_0.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 elementary.txt_3.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 elementary.txt_script1.sh
-rw-r--r-- 1 toby toby 45 Oct 22 16:36 elementary.txt_script2.sh
[root@ip-172-22-117-239 ~]# chmod o-r Engineering.script.sh_2.txt
[root@ip-172-22-117-239 ~]# chmod o-r deduction.doc_1.txt
[root@ip-172-22-117-239 ~]# chmod o-r elementary.txt_0.txt
[root@ip-172-22-117-239 ~]# chmod o-r elementary.txt_3.txt
[root@ip-172-22-117-239 ~]# chmod o-rx elementary.txt_script1.sh
[root@ip-172-22-117-239 ~]# chmod o-rx elementary.txt_script2.sh
[root@ip-172-22-117-239 ~]# /home/toby ls -l
total 8
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 Engineering.Script.sh_2.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 deduction.doc_1.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 elementary.txt_0.txt
-rw-r--r-- 1 toby toby 0 Oct 22 16:36 elementary.txt_3.txt
-rw-r--r-- 1 toby toby 45 Oct 22 16:36 elementary.txt_script1.sh
-rw-r--r-- 1 toby toby 45 Oct 22 16:36 elementary.txt_script2.sh
[root@ip-172-22-117-239 ~]# /home/toby/
```

(adler) Output:

```
root@ip-172-22-117-239:/home/adler# cd adler
root@ip-172-22-117-239:/home/adler# ls -l
total 8
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_3.txt
-rw-r--r-- 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script1.sh
-rwxr-xr-x 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 deduction.doc_2.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 game_is_afroot.txt_1.txt
root@ip-172-22-117-239:/home/adler# chmod o+r Engineering_script.sh_0.txt
root@ip-172-22-117-239:/home/adler# chmod o+rx Engineering_script.sh_script1.sh
root@ip-172-22-117-239:/home/adler# chmod o+r Engineering_script.sh_script2.sh
root@ip-172-22-117-239:/home/adler# chmod o+r deduction.doc_2.txt
root@ip-172-22-117-239:/home/adler# chmod o+r game_is_afroot.txt_1.txt
root@ip-172-22-117-239:/home/adler# ls -l
total 8
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_3.txt
-rw-r--r-- 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script1.sh
-rwxr-xr-x 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 deduction.doc_2.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 game_is_afroot.txt_1.txt
root@ip-172-22-117-239:/home/adler#
```

- (managing group scripts)

(engineering scripts) Command used:
chown sherlock:engineering <script_name>

Output:

```
root@ip-172-22-117-239:/home/adler# chown sherlock:engineering Engineering_script.sh_0.txt
chown: cannot change file permissions for 'Engineering_script.sh_0.txt': No such file or directory
root@ip-172-22-117-239:/home/adler# chown sherlock:engineering Engineering_script.sh_3.txt
chown: cannot change file permissions for 'Engineering_script.sh_3.txt': No such file or directory
root@ip-172-22-117-239:/home/adler# chown sherlock:engineering Engineering_script.sh_script1.sh
chown: cannot change file permissions for 'Engineering_script.sh_script1.sh': No such file or directory
root@ip-172-22-117-239:/home/adler# chown sherlock:engineering Engineering_script.sh_script2.sh
chown: cannot change file permissions for 'Engineering_script.sh_script2.sh': No such file or directory
root@ip-172-22-117-239:/home/adler# ls -l
total 8
-rw-r--r-- 1 sherlock engineering 0 Oct 22 16:36 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_3.txt
-rwxr-xr-x 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script1.sh
-rw-r--r-- 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 deduction.doc_2.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 game_is_afroot.txt_1.txt
root@ip-172-22-117-239:/home/adler# chown sherlock:engineering Engineering_script.sh_script1.sh
root@ip-172-22-117-239:/home/adler# ls -l
total 8
-rw-r--r-- 1 sherlock engineering 0 Oct 22 16:36 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh_3.txt
-rwxr-xr-x 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script1.sh
-rw-r--r-- 1 adler adler 46 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 deduction.doc_2.txt
-rw-r--r-- 1 adler adler 0 Oct 22 16:36 game_is_afroot.txt_1.txt
root@ip-172-22-117-239:/home/adler# cd ..
```

(research scripts) Command used: no research group scripts

(finance scripts) Command used: chown mrs_hudson:finance <script_name>

```
root@ip-172-22-117-239:/home/mycroft# ls -l
total 8
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Engineering_script.sh_0.txt
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-xr-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script1.sh
-rw-r--r-- 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc_2.txt
root@ip-172-22-117-239:/home/mycroft# chown mrs_hudson:finance Finance_script.sh_script1.sh
root@ip-172-22-117-239:/home/mycroft# chown mrs_hudson:finance Finance_script.sh_script2.sh
root@ip-172-22-117-239:/home/mycroft# ls -l
total 8
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Engineering_script.sh_0.txt
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-xr-x 1 mrs_hudson finance 48 Oct 22 16:35 Finance_script.sh_script1.sh
-rw-r--r-- 1 mrs_hudson finance 48 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 mycroft mycroft 0 Oct 22 16:35 deduction.doc_2.txt
root@ip-172-22-117-239:/home/mycroft#
```

- (Removing hidden files from sherlock, moriarty, watson)

Command used: cd <user>, ls -la (displays all files including hidden files), rm <filename>
(sherlock) Output:

	<pre>root@ip-172-22-117-239:/home# cd sherlock root@ip-172-22-117-239:/home/sherlock# ls -la total 40 drwxr-x--- 2 sherlock sherlock 4096 Oct 22 16:35 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 sherlock sherlock 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 sherlock sherlock 14859 Dec 5 03:04 .bashrc -rw-r--r-- 1 sherlock sherlock 807 Mar 31 2024 .profile -rw-rw-x-- 1 sherlock sherlock 0 Oct 22 16:35 deduction.doc_3.txt -rw-r--x-- 1 sherlock sherlock 49 Oct 22 16:35 deduction.doc_script1.sh -rw-r-x--- 1 sherlock sherlock 49 Oct 22 16:35 deduction.doc_script2.sh -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 elementary.txt_0.txt -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 game_is_afoot.txt_1.txt -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 game_is_afoot.txt_2.txt root@ip-172-22-117-239:/home/sherlock# cat my_file.txt user1: Password123 user2: qwertyst0f user3: letmein456 root@ip-172-22-117-239:/home/sherlock# rm my_file.txt root@ip-172-22-117-239:/home/sherlock# ls -la total 40 drwxr-x--- 2 sherlock sherlock 4096 Dec 5 03:07 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 sherlock sherlock 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 sherlock sherlock 14859 Dec 5 03:04 .bashrc -rw-r--r-- 1 sherlock sherlock 807 Mar 31 2024 .profile -rw-rw-x-- 1 sherlock sherlock 0 Oct 22 16:35 deduction.doc_3.txt -rw-r--x-- 1 sherlock sherlock 49 Oct 22 16:35 deduction.doc_script1.sh -rw-r-x--- 1 sherlock sherlock 49 Oct 22 16:35 deduction.doc_script2.sh -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 elementary.txt_0.txt -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 game_is_afoot.txt_1.txt -rw-r----- 1 sherlock sherlock 0 Oct 22 16:35 game_is_afoot.txt_2.txt root@ip-172-22-117-239:/home/sherlock#</pre>	
	<p>(watson) Output:</p> <pre>root@ip-172-22-117-239:/home# cd watson root@ip-172-22-117-239:/home/watson# ls -la total 44 drwxr-x--- 2 watson watson 4096 Oct 22 16:35 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 watson watson 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 watson watson 14859 Dec 5 03:04 .bashrc -rw-r--r-- 1 watson watson 807 Mar 31 2024 .profile -rw-rw-x-- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_3.txt -rw-r--x-- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_script1.sh -rw-r-x--- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_script2.sh -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_0.txt -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_1.txt -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_2.txt -rw-r----- 1 watson watson 54 Oct 22 16:35 my_file.txt root@ip-172-22-117-239:/home/watson# cat my_file.txt user1: Password123 user2: qwertyst0f user3: letmein456 root@ip-172-22-117-239:/home/watson# rm my_file.txt root@ip-172-22-117-239:/home/watson# ls -la total 40 drwxr-x--- 2 watson watson 4096 Dec 5 03:09 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 watson watson 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 watson watson 14931 Dec 5 03:09 .bashrc -rw-r--r-- 1 watson watson 807 Mar 31 2024 .profile -rw-rw-x-- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_3.txt -rw-r--x-- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_script1.sh -rw-r-x--- 1 mrs_hudson finance 47 Oct 22 16:35 Finance_script.sh_script2.sh -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_0.txt -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_1.txt -rw-r----- 1 watson watson 0 Oct 22 16:35 deduction.doc_2.txt -rw-r----- 1 watson watson 54 Oct 22 16:35 my_file.txt root@ip-172-22-117-239:/home/watson#</pre>	
	<p>(moriarty) Output:</p> <pre>root@ip-172-22-117-239:/home/moriarty# ls -la total 44 drwxr-x--- 2 moriarty moriarty 4096 Dec 5 02:58 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 moriarty moriarty 4096 Dec 5 02:58 . -rw-r--r-- 1 moriarty moriarty 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 moriarty moriarty 14715 Dec 5 02:54 .bashrc -rw-r--r-- 1 moriarty moriarty 807 Mar 31 2024 .profile -rw-rw-x-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_0.txt -rw-r--x-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_2.txt -rw-r-x--- 1 moriarty moriarty 0 Oct 22 16:35 elementary.txt_1.txt -rw-r----- 1 moriarty moriarty 0 Oct 22 16:35 game_is_afoot.txt_0.txt -rw-r----- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script1.sh -rw-r----- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script2.sh root@ip-172-22-117-239:/home/moriarty# cat my_file.txt user1: Password123 user2: qwertyst0f user3: letmein456 root@ip-172-22-117-239:/home/moriarty# rm my_file.txt root@ip-172-22-117-239:/home/moriarty# ls -la total 40 drwxr-x--- 2 moriarty moriarty 4096 Dec 5 02:59 . drwxr-xr-x 11 root root 4096 Dec 3 01:56 .. -rw-r--r-- 1 moriarty moriarty 4096 Dec 5 02:59 . -rw-r--r-- 1 moriarty moriarty 220 Mar 31 2024 .bash_logout -rw-r--r-- 1 moriarty moriarty 14715 Dec 5 02:54 .bashrc -rw-r--r-- 1 moriarty moriarty 807 Mar 31 2024 .profile -rw-rw-x-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_0.txt -rw-r--x-- 1 moriarty moriarty 0 Oct 22 16:35 Finance_script.sh_2.txt -rw-r-x--- 1 moriarty moriarty 0 Oct 22 16:35 elementary.txt_1.txt -rw-r----- 1 moriarty moriarty 0 Oct 22 16:35 game_is_afoot.txt_0.txt -rw-r----- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script1.sh -rw-r----- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script2.sh root@ip-172-22-117-239:/home/moriarty#</pre>	
<input checked="" type="checkbox"/>	Optional: Updating password hashing configuration	n/a

<input checked="" type="checkbox"/>	<p>Auditing and securing SSH</p> <ul style="list-style-type: none"> • (enabling ssh) <p>Command used: sudo systemctl enable ssh</p> <p>Output:</p> <pre>root@ip-172-22-117-239:/home# which sshd /usr/sbin/sshd root@ip-172-22-117-239:/home# sudo systemctl enable ssh [sudo] password for root: sh: /usr/lib/systemd/system/SysV.service script with /usr/lib/systemd/systemd-sysv-install. executing: /usr/lib/systemd/systemd-sysv-install enable ssh Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/sh.service. Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/lib/systemd/system/sshd.service. root@ip-172-22-117-239:/home#</pre> <ul style="list-style-type: none"> • (editing ssh file) <p>Command used: nano /etc/ssh/sshd_config</p> <p>Output:</p> <pre>root@ip-172-22-117-239:/home/sysadmin# nano /etc/ssh/sshd_config</pre> <ul style="list-style-type: none"> • (removing ability for empty passwords) <pre># To disable tunneled clear text passwords, change to no here! PasswordAuthentication yes PermitEmptyPasswords yes</pre> <p>Changed to:</p> <pre># To disable tunneled clear text passwords, change to no here! PasswordAuthentication yes PermitEmptyPasswords no</pre> <ul style="list-style-type: none"> • (removing ability to ssh into root user) <pre>#LoginGraceTime 2m PermitRootLogin yes</pre> <p>Changed to:</p> <pre>#LoginGraceTime 2m PermitRootLogin no</pre> <ul style="list-style-type: none"> • (removing ability to ssh with any port besides port 22) <pre>#Include /etc/ssh/sshd_config.d/*.conf Port 22 Port 2223 Port 2224 Port 2225 Port 8967</pre> <p>Changed to:</p> <pre>#Include /etc/ssh/sshd_config.d/*.conf I Port 22</pre> <ul style="list-style-type: none"> • (enabling ssh protocol 2)
-------------------------------------	--

Command(s) used: nano package_list.txt; apt list -installed > package_list.txt

-Install Output

```
root@iMac-172-23-117-230:~# nano package.list.txt; apt list --installed > package.list.txt
```

- (showing top and bottom of package_list.txt)

Command used: nano package list.txt

Output:

- (identifying telnet and rsh-client)

(rsh shown on top line, telnet shown on bottom line)

- (removing telnet)

Command used: sudo apt remove telnet
Output:

```
root@ip-172-22-117-239:/home# sudo apt remove telnet
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
After this operation, 48.1 kB disk space will be freed
Do you want to continue? [Y/n] y
(Reading database ... 103541 files and directories currently installed...)
Removing telnet (0.17+2.5-3ubuntu4) ...
root@ip-172-22-117-239:/home# apt remove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not
root@ip-172-22-117-239:/home#
```

(after review of the screenshot, i realized that i forgot to use “apt autoremove -y” but instead used “apt remove -y”)

- (removing rsh-client and dependencies)

Command used:

```
sudo apt remove rsh-redone-server
```

apt auto

```
[root@ip-172-22-117-239 ~]# sudo apt remove rsh-redone-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libiveagent-2.1-7t64 opensbsd-inetd tcptcp update-inetd
Use 'sudo apt autoremove' to remove them.                                I
The following packages will be REMOVED:
  rsh-redone-server
  0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 68.6 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 103585 files and directories currently installed.)
Removing rsh-redone-server (85-4) ...
Processing triggers for man-db (2.12.0-4build2) ...
root@ip-172-22-117-239:~/home# apt autoremove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  libiveagent-2.1-7t64 opensbsd-inetd tcptcp update-inetd
  0 upgraded, 0 newly installed, 4 to remove and 0 not upgraded.
After this operation, 673 kB disk space will be freed.
(Reading database ... 103575 files and directories currently installed.)
Removing opensbsd-inetd (0.20221205-3build4) ...
Removing libiveagent-2.1-7t64:amd64 (2.1.12-stable-9ubuntu2) ...
Removing tcptcp (7,6,q-33) ...
Removing update-inetd (4.53) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libz-bin (2.39-0ubuntu8.3) ...
root@ip-172-22-117-239:~/home#
```

- (listing why “telnet” is a security risk)

Telnet: According to ssh.com, a telnet session

between a server and client is not encrypted. With this, anyone with access to the TCP/IP packet flow between both endpoints can reconstruct the data to read plaintext messages along with the usernames and passwords that were used to log into the session. Along with this, the tools used for this network attack are readily available.

(Source:

[https://www.ssh.com/academy/ssh/telnet#:~:text=The%20Telnet%20session%20between%20the,in%20to%20the%20remote%20machine. \)](https://www.ssh.com/academy/ssh/telnet#:~:text=The%20Telnet%20session%20between%20the,in%20to%20the%20remote%20machine.)

- (listing why rsh-client is a security risk)

RSH-Client: According to ssh.com, the method of authentication used with RSH-client (dependent on .rhosts files and /etc/hosts.equiv) relied on IP addresses and DNS. With this release coming out during the 1980s, IP spoofing was easy if the attacker was on the local network and could even be done remotely. Ssh.com recommends to immediately disable RSH-Client.

(Source:

[https://www.ssh.com/academy/ssh/rsh#:~:text=Security%20Issues%20in%20rsh,-rsh%20used%20.&text=rhosts%20files%20and%20%2Fetc%2Fhosts,could%20even%20be%20done%20remotely. \)](https://www.ssh.com/academy/ssh/rsh#:~:text=Security%20Issues%20in%20rsh,-rsh%20used%20.&text=rhosts%20files%20and%20%2Fetc%2Fhosts,could%20even%20be%20done%20remotely.)

- (installing ufw, lynis, tripwire)

(ufw) Command used: sudo apt install ufw
Output:

```
ii ufw          0.36.2-6      all      program for managing a Netfilter firewall
```

(lynis) Command used: sudo apt install lynis
Output:

```
menu
Suggested packages:
  apt-listbugs debsecans debsums samhain aide fail2ban menu-l10n gksu | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis  menu
  Lynis 2 newly installed, 0 to remove and 0 not upgraded.
  Need to get 602 kB of archives.
After this operation, 3202 kB of additional disk space will be used.

Do you want to continue? [Y/n] y
Get: http://us-east-1.s3.archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226 kB]
Get: http://us-east-1.s3.archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377 kB]
Fetched 982 kB in 0s (12.4 MB/s)
Selecting previously unselected package lynis.
(Reading database ... 103788 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.50_amd64.deb ...
Unpacking menu (2.1.50) ...
Setting up lynis (3.0.9-1) ...
Creating /etc/systemd/system/timers.target.wants/lynis.timer -> /usr/lib/systemd/system/lynis.timer.
lynis service is not running so it is a static unit, not starting it.
Setting up menu (2.1.50) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for menu (2.1.50) ...
Processing triggers...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.                                I

Restarting services...

Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart systemd-logind.service

No containers need to be restarted.

User sessions running outdated binaries:
sysadmin @ session #12: sshd[2312]
sysadmin @ user manager service: systemd[1051]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-22-117-239:/home# sudo apt install lynis
```

(sidenote: with how much was displayed during the installation, i was unable to show a full image of the command prior to the install as it was cut and I was unable to scroll to it. The command is shown at the bottom line.)

(tripwire) Command used: sudo apt install tripwire
Output:

```
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write-protected media (e.g. mounted RD floppy). See /usr/share/doc/tripwire/README.Debian for details.
```

[OK]

(sidenote: similar with the lynis install, so much was shown that it cut out the portion where I can the command as well and the bottom. The popup that has you set a passphrase might have been the culprit.)

- (listing why tripwire, lynyis, and ufw are beneficial to linux hardening)

Tripwire: According to eaglepubs.erau.edu, Tripwire is a Host-based Intrusion Detection System that can monitor for unauthorized file and directory modification on local systems. It does so by recording aspects of a file such as its hash, timestamp of last modification, and permissions. These records are put into an encrypted database created by the Tripwire program and is used as a reference when cross-checking files for changes.

		<p>(Source: https://eaglepubs.erau.edu/mastering-enterprise-network-labs/chapter/intrusion-detection-tripwire/#:~:text=Tripwire%20is%20a%20Host%2Dbased%20Intrusion%20Detection%20System,baseline%20reference%20when%20cross%2Dchecking%20files%20for%20changes.)</p> <ul style="list-style-type: none"> • (listing why Lynis is beneficial to linux hardening) <p>Lynis: Directly from cisofy.com: Lynis is a battle-tested security tool for systems running Linux, macOS, or Unix-based operating system. It performs an extensive health scan of your systems to support system hardening and compliance testing.</p> <p>(Source: https://cisofy.com/lynis/#:~:text=Lynis%20is%20a%20battle%2Dtested,system%20hardening%20and%20compliance%20testing.))</p> <ul style="list-style-type: none"> • (Listing why UFW is beneficial to linux hardening) <p>UFW: According to swhosting.com: UFW allows users to configure firewall rules using simple terminal commands. This allows for easy implementation of basic security policies like allowing or denying traffic on specific ports or IP addresses.</p> <p>(Source: https://www.swhosting.com/en/blog/ufw-an-in-depth-look-at-linux-security#:~:text=UFW%20allows%20users%20to%20configure,certain%20ports%20or%20IP%20addresses.))</p>
<input checked="" type="checkbox"/>	Disabling unnecessary services	<ul style="list-style-type: none"> • (Command to list all services then dump its output into service_list.txt) <p>Command used: nano service_list.txt; systemctl list-unit-files - -type=service > service_list.txt</p> <p>Output:</p> <pre>root@ip-172-22-117-239:/home# nano service_list.txt; systemctl list-unit-files --type=service > service_list.txt</pre>

(this is just a portion of the service list, the list was extensive, so I am posting just one screenshot in an effort to reduce space)

- (Identifying mysql and samba)

Command(s) used:

```
sudo systemctl status mysql  
sudo systemctl status samba
```

(mysql) Output:

```
root@ip-172-22-117-239:/home# sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-12-05 22:45:25 UTC; 4h 2min ago
       Main PID: 845 (mysqld)
          Status: "Server is operational"
             Tasks: 38 (limit: 4586)
            Memory: 425.9M (peak: 438.4M)
              CPU: 1min 39.904s
            CGroup: /system.slice/mysql.service
                     └─045 /usr/sbin/mysqld

Dec 05 22:45:28 ip-172-22-117-239 systemd[1]: Starting mysql.service - MySQL Community Server...
Dec 05 22:45:29 ip-172-22-117-239 systemd[1]: Started mysql.service - MySQL Community Server.
root@ip-172-22-117-239:/home# █
```

(samba) Output:

```
[root@ip-172-22-11-239 ~]# /home/luo sudo systemctl status samba
● Samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service; enabled; preset: enabled)
     Active: inactive (dead) (Result: exec-condition) Since Thu 2024-12-05 22:45:21 UTC; 4h 6min ago
   Condition: start condition umet at Thu 2024-12-05 22:45:20 UTC; 4h 6min ago
     Docs: man:samba(8)
           man:samba(5)
           man:smb.conf(5)
      CPU: 55ms

Dec 05 22:45:20 ip-172-22-11-239 systemd[1]: Starting samba-ad-dc service - Samba AD Daemon..
Dec 05 22:45:21 ip-172-22-11-239 samba-ad-dc.service: Skipped due to "exec-condition".
Dec 05 22:45:21 ip-172-22-11-239 systemd[1]: Condition check resulted in samba-ad-dc.service - Samba AD Daemon being skipped.
[root@ip-172-22-11-239 ~]#
```

- (Stopping, Disabling, Removing mysql and samba)

(Stopping) Commands used:
sudo systemctl stop mysql
sudo systemctl stop samba

Output:

```
root@ip-172-22-117-239:/home# sudo systemctl stop mysql  
root@ip-172-22-117-239:/home# sudo systemctl stop samba
```

(Disabling) Commands used:
sudo systemctl disable mysql
sudo systemctl disable samba

- (installing logrotate)

Command used: sudo apt install logrotate
Output:

- (displaying logrotate.conf)

Command used: nano /etc/logrotate.conf
Output:

```
root@kali:~# nano /etc/logrotate.conf
# nano /etc/logrotate.conf
# new man "logrotate" for details
# see "man logrotate" for details
# rotate options do not affect preceding include directives
# rotate log files daily
# use the log group by default, since this is the owning group
# for all logs in this file
# root adm
# keep 7 weeks worth of backlogs
# create 4 week old log files
# create new (empty) log files after rotating old ones
# create
#       suffix as a suffix of the rotated file
# instead of
#       increment this if you want your log files compressed
# compress
#       packages this if you want your log files compressed
# include /etc/logrotate.d
# include /etc/logrotate.d
# system-specific logs may also be configured here.
```

- (making edits to /etc/logrotate.conf)

Changed:

```
# rotate log files daily from: daily
```

To: weekly

#keep 7 weeks worth of backlogs from: rotate 7
To: rotate 4

Output:

```
root@kali:~# man logrotate
 man    "man logrotate" for details
 ...
       all options do not effect preceding include directives
 ...
       include logrotate.conf
       only
       use the nos group by default, since this is the owning group
       of the log files
       u root adm
       x sleep 2 weeks worth of backlog
       z 7
       ...
       # create new (empty) log files after rotating old ones
       create
       ... file as a suffix of the rotated file
       ...
       # increment this if you want your log files compressed
       compress
       compress
       # append log files instead of dropping log rotation information into this directory
       include /etc/logrotate.d
       ...
       system-specific logs may also be configured here.
```

- (restarting journald)

Command used: systemctl restart systemd-journald

		<p>Output:</p> <pre>root@ip-172-22-117-239:/home# systemctl restart systemd-journald</pre>
<input checked="" type="checkbox"/>	Scripts created	<ul style="list-style-type: none"> • (hardening_script1.sh) <p>Command used: nano hardening_script1.sh</p> <pre>root@ip-172-22-117-196:/home/sysadmin# nano hardening_script1.sh</pre> <p>Script:</p> <pre>#!/bin/bash # Variable for the report output file, choose an output file name REPORT_FILE="hardening_file1.txt" # Output the hostname echo "Gathering hostname..." # Placeholder for command to get the hostname echo "Hostname: \$(hostname)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Output the OS version echo "Gathering OS version..." # Placeholder for command to get the OS version echo "OS Version: \$(lsb_release -a)" >> \$REPORT_FILE printf "\n" >> \$REPORT_FILE # Output memory information 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..." # Placeholder for command to get uptime info</pre>

```
echo "Uptime Information: $(uptime)" >>
$REPORT_FILE
printf "\n" >> $REPORT_FILE

# Backup the OS
echo "Backing up the OS..." 
# Placeholder for command to back up the OS

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 /

echo "OS backup completed." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Force Sherlock, Watson, and Mycroft to change
their password upon their next login
echo "Forcing Sherlock, Watson, and Mycroft users
to change their password on next login..."
# Placeholder for command to force password
change

chage -d 0 sherlock
chage -d 0 watson
chage -d 0 mycroft

echo "Password change enforced for Sherlock,
Watson, and Mycroft." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output the sudoers file to the report
echo "Gathering sudoers file..." 
# Placeholder for command to output sudoers file
echo "Sudoers file:$(sudo cat /etc/sudoers)" >>
$REPORT_FILE
printf "\n" >> $REPORT_FILE
```

```

# Script to check for files with world permissions and
# update them
echo "Checking for files with world permissions..."

find /home -type f -perm -007 -exec chmod o-rwx {} \
\;

# Placeholder for command to find and update files
# with world permissions
echo "World permissions have been removed from
any files found." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Find specific files and update their permissions
echo "Updating permissions for specific scripts..."

# Engineering scripts - Only members of the
# engineering group
echo "Updating permissions for Engineering scripts."

# Placeholder for command to update permissions
find -iname "*engineering*" -exec chown
:engineering {} +

echo "Permissions updated for Engineering scripts."
>> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Research scripts - Only members of the research
# group
echo "Updating permissions for Research scripts..."
# Placeholder for command to update permissions

find -iname "research" -exec chown :research {} +

echo "Permissions updated for Research scripts" >>
$REPORT_FILE

```

```
printf "\n" >> $REPORT_FILE
```

```
# Finance scripts - Only members of the finance
group
echo "Updating permissions for Finance scripts"
# Placeholder for command to update permissions

find -iname "finance" -exec chown :finance {} +
echo "Permissions updated for Finance scripts." >>
$REPORT_FILE
printf "\n" >> $REPORT_FILE
```

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

- (end of hardening_script1.sh)

Output:

- (enabling execute on hardening_script1.sh)

Command used: chmod +x hardening_script1.sh
Output:

```
root@ip-172-22-117-196:/home/sysadmin# chmod +x hardening_script1.sh
root@ip-172-22-117-196:/home/sysadmin# ls -l
total 112
-rw-r--r-- 1 root root 2799 Dec 19 04:07 hardening_file1.txt
-rw-r--r-- 1 root root 100014 Dec 19 21:57 hardening_file2.txt
-rwxr-xr-x 1 root root 3253 Dec 19 22:02 hardening_script1.sh
-rwxr-xr-x 1 root root 1252 Dec 19 21:54 hardening_script2.sh
```

- (running hardening_script1.sh)

Command used: ./hardening_script1.sh

Output:

```
root@ip-172-22-117-196:/home/sysadmin# ./hardening_script1.sh
```

- (completion of hardening_script1.sh)

```
[root@ip-172-22-117-196 ~]# ./hardening_script1.sh
[*] Gathering user info...
[*] Gathering sudoers file...
[*] Gathering world permissions...
[*] Updating permissions for specific scripts...
[*] Updating permissions for root scripts...
[*] Updating permissions for Research scripts...
[*] Script execution completed. Check hardening_file1.txt for details.
[*] Hardening completed. Watson, and Microsoft users to change their password on next login...
```

- (hardening_script1.sh output file -> hardening_file1.txt)

Command used:

```
root@ip-172-22-117-196:/home/sysadmin# ls -l
```

```
total 112
```

```
-rw-r--r-- 1 root root 2799 Dec 19 22:11 hardening_file1.txt
```

(hardening_file1.txt) Output:

```
[root@ip-172-22-117-196 ~]# nano hardening_file1.txt
[*] Hardening completed. Watson, and Microsoft users to change their password on next login...
```

```
[*] Gathering user info...
[*] Gathering sudoers file...
[*] Gathering world permissions...
[*] Updating permissions for specific scripts...
[*] Updating permissions for root scripts...
[*] Updating permissions for Research scripts...
[*] Script execution completed. Check hardening_file1.txt for details.
```

```
[*] Hardening completed. Watson, and Microsoft users to change their password on next login...
```

```
[*] Gathering user info...
[*] Gathering sudoers file...
[*] Gathering world permissions...
[*] Updating permissions for specific scripts...
[*] Updating permissions for root scripts...
[*] Updating permissions for Research scripts...
[*] Script execution completed. Check hardening_file1.txt for details.
```

```
[*] Hardening completed. Watson, and Microsoft users to change their password on next login...
```

- (hardening_script2.sh)

Command used: nano hardening_script2.sh

Output:

```
root@ip-172-22-117-196:/home/sysadmin# nano hardening_script2.sh
```

Script:

```
#!/bin/bash
```

```
# Variable for the report output file, choose a NEW  
output file name
```

```
REPORT_FILE="hardening_file2.txt"
```

```
# Output the sshd configuration file
```

```
echo "Gathering details from sshd configuration file"  
# Placeholder for command to get the sshd  
configuration file
```

```
echo "sshd configuration  
file:$(/etc/ssh/sshd/sshd_config)" >>  
$REPORT_FILE  
printf "\n" >> $REPORT_FILE
```

```
# Update packages and services
```

```
Echo "Updating packages and services"
```

```
# Placeholder for command to update packages
```

```
sudo apt update
```

```
# Placeholder for command to upgrade packages
```

```
sudo apt upgrade -y
```

```
echo "Packages have been updated and upgraded"  
>> $REPORT_FILE printf "\n" >> $REPORT_FILE
```

```
# Placeholder for command to list all installed  
packages
```

```
echo "Installed Packages:$(dpkg -l)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

echo "Printing out logging configuration data"

Placeholder for command to display logging data

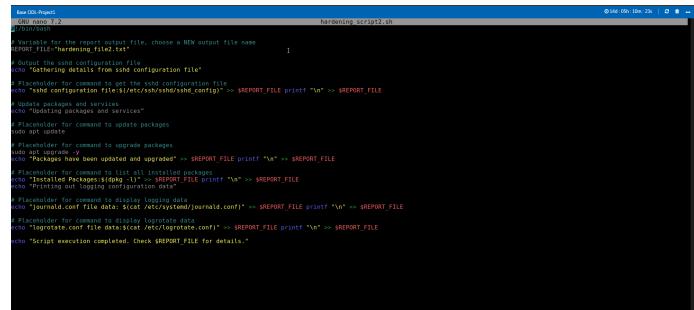
```
echo "journald.conf file data: $(cat
/etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

Placeholder for command to display logrotate data

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

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

(in nano) Output:



```
./hardening_script2.sh
? Select file for the report output file, choose a NEW output file name
REPORT FILE:"hardening_file2.txt"
? Output the journald configuration file
? Output the logrotate configuration file
? Placeholder for command to display the journald configuration file
echo "journald configuration file $(cat /etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
? Placeholder for command to display packages and services
? Update packages and services
apt update
? Placeholder for command to upgrade packages
apt upgrade
? Packages have been updated and upgraded => $REPORT_FILE
echo "Packages have been updated and upgraded" >> $REPORT_FILE
? Installed Packages(asking '1') => $REPORT_FILE printf "\n" >> $REPORT_FILE
echo "Installed Packages(asking '1') => $REPORT_FILE printf "\n" >> $REPORT_FILE
? Placeholder for command to display logrotate data
echo "Printing out logrotate configuration data" >> $REPORT_FILE
? Logrotate configuration file data: $(cat /etc/logrotate.conf) => $REPORT_FILE printf "\n" >> $REPORT_FILE
? Placeholder for command to display log configuration data
echo "journald.conf file data: $(cat /etc/systemd/journald.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE
? Placeholder for command to display log configuration data
echo "logrotate.conf file data: $(cat /etc/systemd/logrotate.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE
? Script execution completed. Check $REPORT_FILE for details.
```

- (enabling execute on hardening_script2.sh)

Command used: chmod o+x hardening_script2.sh
Output:

```
root@ip-172-22-117-196:/home/sysadmin# chmod o+x hardening_script2.sh
root@ip-172-22-117-196:/home/sysadmin# ls -l
total 12
-rw-r--r-- 1 root root 2799 Dec 19 22:11 hardening_file1.txt
-rw-r--r-x 1 root root 3253 Dec 19 22:02 hardening_script1.sh
-rwxr--r-x 1 root root 1252 Dec 19 21:54 hardening_script2.sh
```

- (running hardening_script2.sh)

Command used: ./hardening_script2.sh
Output:

```
root@ip-172-22-117-196:/home/sysadmin# ./hardening_script2.sh
```

- (hardening_script2.sh completion)

- (hardening_script2.sh output file -> hardening_file2.txt)

```
root@ip-172-22-117-196:/home/sysadmin# ls -l
total 112
-rw-r--r-- 1 root root 2799 Dec 19 22:11 hardening_file1.txt
-rw-r--r-- 1 root root 100599 Dec 19 22:26 hardening_file2.txt
-rwxr-xr-x 1 root root 3253 Dec 19 22:02 hardening_script1.sh
-rwxr-xr-x 1 root root 1244 Dec 19 22:24 hardening_script2.sh
```

- (hardening_file2.txt)

Command used: nano hardening_file2.txt
Output:

(again, in an effort to save space, the screenshots above are the top and bottom screen of the output file)

<input checked="" type="checkbox"/>	<p>Scripts scheduled with cron</p> <p>• (cron file)</p> <p>Command used: crontab -e</p> <p>Output:</p> <pre>root@ip-172-22-117-196:/home/sysadmin# crontab -e</pre> <p>• (editing cron file)</p> <p>Lines added:</p> <pre>0 0 1 * * /home/sysadmin/hardening_script1.sh 0 0 * * 1 /home/sysadmin/hardening_script2.sh</pre> <p>Output:</p> <pre>root@ip-172-22-117-196:/home/sysadmin# crontab -e # Edit this file to introduce tasks to be run by cron. # Each task to run has to be defined through a single line # indicating what user to run as, 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 (h), minute (m), day of month (dow), 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 timezone. # Output of the cronjob (including errors) is sent through # email to the user the Crontab file belongs to (unless restricted). # For example, you can run a backup of all your user accounts # every Sunday morning at 4 am: # 0 4 * * 0 root tar -zcvf /var/backup/home.tgz /home/ # For more information see the manual pages of crontab(5) and cron(8) # m h dom mon dow command # Scheduling hardening_script1.sh # 0 0 1 * * /home/sysadmin/hardening_script1.sh # Scheduling hardening_script2.sh # 0 0 * * 1 /home/sysadmin/hardening_script2.sh</pre> <p>• (verifying cron schedule)</p> <p>Command used: crontab -l</p> <p>Output:</p> <pre>root@ip-172-22-117-196:/home/sysadmin# 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 what user to run as, 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 (h), minute (m), day of month (dow), 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 timezone. # Output of the cronjob (including errors) is sent through # email to the user the Crontab file belongs to (unless restricted). # For example, you can run a backup of all your user accounts # every Sunday morning at 4 am: # 0 4 * * 0 root tar -zcvf /var/backup/home.tgz /home/ # For more information see the manual pages of crontab(5) and cron(8) # m h dom mon dow command # Scheduling hardening_script1.sh # 0 0 1 * * /home/sysadmin/hardening_script1.sh # Scheduling hardening_script2.sh # 0 0 * * 1 /home/sysadmin/hardening_script2.sh</pre>
-------------------------------------	--