PROJECT 1 HARDENING SUMMARY AND CHECKLIST

OS INFORMATION

Customer	Baker Street Corporation
Hostname	**Baker_street_Linux_Server**
OS Version	**CAT ETC/ OS-RELEASE** **PRETTY_NAME="Ubuntu 22.04.5 LTS"** **NAME="Ubuntu"** **VERSION_ID="22.04"** **VERSION="22.04.5 LTS (Jammy Jellyfish)"** **VERSION_CODENAME=jammy** **ID=ubuntu** **ID_LIKE=debian** **HOME_URL="https://www.ubuntu.com/"** **SUPPORT_URL="https://help.ubuntu.com/"** **BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"** **PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"** **UBUNTU_CODENAME=jammy**
Memory information	**FREE** **root@Baker_street_Linux_Server:/# free** **total used free shared buff/cache available** **Mem: 16182796 993972 13626008 188108 1562816 14701324** **Swap: 0 0 0**
Uptime information	**UPTIME**

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
	OS backup	*sudo tar -cvpzf / baker_street_backup.tar.gz --exclude=/ baker_street_backup.tar.gz --exclude=/ proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /* */usr/share/perl/5.34.0/Unicode/Collate/Locale/lkt.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/de_phone.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/sr.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/is.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/fa.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/dsb.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/sk.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/lv.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/si.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/wae.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/af.pl* */usr/share/perl/5.34.0/Unicode/Collate/Locale/uk.pl*

	Auditing users and groups	Userdel; userdel -r ; id user; cut -d: -f1 /etc/passwd ; passed -l; usermod -U; grep user etc/shadow; getent group research; passed -S username; sudo grouped marketing root@Baker_street_Linux_Server:/# userdel lestrade root@Baker_street_Linux_Server:/# userdel irene root@Baker_street_Linux_Server:/# userdel mary root@Baker_street_Linux_Server:/# userdel gregson root@Baker_street_Linux_Server:/# userdel -r lestrade userdel: user 'lestrade' does not exist root@Baker_street_Linux_Server:/# userdel -r irene userdel: user 'irene' does not exist root@Baker_street_Linux_Server:/# userdel -r mary userdel: user 'mary' does not exist root@Baker_street_Linux_Server:/# userdel -r gregson userdel: user 'gregson' does not exist root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# id lestrade id: 'lestrade': no such user root@Baker_street_Linux_Server:/# id irene id: 'irene': no such user root@Baker_street_Linux_Server:/# id mary id: 'mary': no such user root@Baker_street_Linux_Server:/# id gregson id: 'gregson': no such user root@Baker_street_Linux_Server:/# cut -d: -f1 /etc/ passwd root daemon bin sys sync games man lp mail news uucp proxy www-data backup list irc gnats nobody root@Baker_street_Linux_Server:/# passwd -l moriarty passwd: password expiry information changed. root@Baker_street_Linux_Server:/# passwd -l mrs_hudson passwd: password expiry information changed. root@Baker_street_Linux_Server:/# usermod -U sherlock root@Baker_street_Linux_Server:/# usermod -U watson root@Baker_street_Linux_Server:/# usermod -U mycroft root@Baker_street_Linux_Server:/# usermod -U toby root@Baker_street_Linux_Server:/# 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. root@Baker_street_Linux_Server:/# grep moriarty etc/shadow moriarty:!yj9T$iDtoIJZS0/5WWZp7BZ/ UU0$6U2s4WJtdoBAwkuAKwXL7urmHY6b.rKx aekfbqrZxE3:20098:0:99999:7::: root@Baker_street_Linux_Server:/# grep mrs_hudson ^C root@Baker_street_Linux_Server:/# grep mrs_hudson etc/shadow mrs_hudson:!:20069:0:99999:7::: root@Baker_street_Linux_Server:/# getent group research research:x:1015:toby,adler,sherlock,watson root@Baker_street_Linux_Server:/# usermod -aG research sherlock root@Baker_street_Linux_Server:/# usermod -aG research watson root@Baker_street_Linux_Server:/# usermod -aG research mycroft root@Baker_street_Linux_Server:/# usermod -aG research toby root@Baker_street_Linux_Server:/# usermod -aG research adler root@Baker_street_Linux_Server:/# passwd -S sherlock sherlock P 01/10/2025 0 99999 7 -1 root@Baker_street_Linux_Server:/# passwd -S watson watson P 01/10/2025 0 99999 7 -1 root@Baker_street_Linux_Server:/# passwd -S mycroft mycroft P 01/10/2025 0 99999 7 -1 root@Baker_street_Linux_Server:/# passwd -S toby toby P 01/08/2025 0 99999 7 -1 root@Baker_street_Linux_Server:/# passwd -S adler adler L 12/12/2024 0 99999 7 -1 root@Baker_street_Linux_Server:/# groupdel marketing groupdel: group 'marketing' does not exist root@Baker_street_Linux_Server:/# groups research groups: 'research': no such user root@Baker_street_Linux_Server:/# getent group research research:x:1015:toby,adler,sherlock,watson,mycroft root@Baker_street_Linux_Server:/# getent group marketing root@Baker_street_Linux_Server:/# sudo groupdel marketing sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution root is not in the sudoers file. This incident will be reported. root@Baker_street_Linux_Server:/# groupdel marketing groupdel: group 'marketing' does not exist root@Baker_street_Linux_Server:/# _apt systemd-network systemd-resolve mysql messagebus systemd-timesync syslog sshd sherlock watson nobody _apt systemd-network systemd-resolve mysql messagebus systemd-timesync syslog sshd sherlock watson moriarty mycroft mrs_hudson sysadmin toby adler postfix

	Updating and enforcing password policies	Nano /etc/pam.d/common-password; /etc/security/pwquality.conf; #password requisite pam_pwquality.so retry =2 minlen=8 ucredit=-1 ocredit=-1 # pam-auth-update to manage selection of other modules. See # pam-auth-update(8) for details. # here are the per-package modules (the "Primary" block) password [success=2 pam_unix.so obscure yescrypt # here's the fallback if no module succeeds password requisite pam_pwquality.so retry=2 minlen=12 # prime the stack with a positive return value if there isn't one already; # this avoids us returning an error just because nothing sets a success code # since the modules above will each just jump around password required pam_permit.so # and here are more per-package modules (the "Additional" block) # end of pam-auth-update config **minlen** 8 characters **dcredit** 0 **ucredit** 1 **lcredit** 8 **ocredit** 1 **retry** 2

	Updating and enforcing sudo permissions	Visudo; visudo –c; /var/log/logcleanup.sh; /tmp/scripts/research_script.sh; sudo etc/sudoers; sudo –l; root@Baker_street_Linux_Server:/# sudo –l sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution User root is not allowed to run sudo on Baker_street_Linux_Server. root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# sudo etc/sudoers sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution root is not in the sudoers file. This incident will be reported. root@Baker_street_Linux_Server:/# etc/sudoers bash: etc/sudoers: Permission denied root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# /var/log/logcleanup.sh root@Baker_street_Linux_Server:/# /tmp/scripts/research_script.sh root@Baker_street_Linux_Server:/# Visudo; # 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 #Defaults:%sudo env_keep += "GPG_AGENT_INFO" # Host alias specification # User alias specification # 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 #Defaults:%sudo env_keep += "GPG_AGENT_INFO" # Host alias specification # Host alias specification sherlock ALL=(ALL:ALL) ALL # User alias specification sherlock ALL=(ALL:ALL) ALL # Cmnd alias specification sherlock ALL=(ALL:ALL) ALL # User privilege specification sherlock ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges sherlock ALL=(ALL) ALL # Allow members of group sudo to execute any command sherlock ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "@include" directives: @includedir /etc/sudoers.d sherlock ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD:ALL moriarty ALL=(ALL) NOPASSWD:ALL root@Baker_street_Linux_Server:/# sudo –l –U sherlock sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution Matching Defaults entries for sherlock on Baker_street_Linux_Server: env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty User sherlock may run the following commands on Baker_street_Linux_Server: (ALL : ALL) ALL (ALL : ALL) ALL (ALL : ALL) ALL (ALL : ALL) ALL (ALL) ALL (ALL : ALL) ALL (ALL) NOPASSWD: ALL visudo: /etc/sudoers.tmp unchanged sherlock@Baker_street_Linux_Server:/$ sudo visudo # Members of the admin group may gain root privileges sherlock ALL=(ALL) ALL # Allow members of group sudo to execute any command sherlock ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "@include" directives: @includedir /etc/sudoers.d sherlock ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD:ALL moriarty ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh mycroft ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh

	Validating and updating permissions on files and directories	Find /home -perm /o+rwx ; find /home -perm / o+rwx -exec chmod o+rwx {} +; sudo find /home -iname ; find /home -iname ‘*engineering*’ -exec chown :engineering {} + -exec chmod 770 {} +; find /home -iname ‘*password*’ -exec rm -f {} + root@Baker_street_Linux_Server:/# find /home -perm /o+rwx /home ; ls -l home root@Baker_street_Linux_Server:/# find /home -perm /o+rwx -exec chmod o+rwx {} = find: missing argument to `-exec' root@Baker_street_Linux_Server:/# find /home -perm /o+rwx -exec chmod o=rwx {} root@Baker_street_Linux_Server:/# find /home -iname '*engineering*' /home/lestrade/Engineering_script.sh_script1.sh /home/lestrade/Engineering_script.sh_0.txt /home/lestrade/Engineering_script.sh_script2.sh /home/adler/Engineering_script.sh_script1.sh /home/adler/Engineering_script.sh_0.txt /home/adler/Engineering_script.sh_3.txt /home/adler/Engineering_script.sh_script2.sh /home/gregson/Engineering_script.sh_script1.sh /home/gregson/Engineering_script.sh_3.txt /home/gregson/Engineering_script.sh_script2.sh /home/mycroft/Engineering_script.sh_0.txt /home/toby/Engineering_script.sh_2.txt /home/mrs_hudson/Engineering_script.sh_1.txt /home/irene/Engineering_script.sh_1.txt /home/irene/Engineering_script.sh_script1.sh /home/irene/Engineering_script.sh_3.txt /home/irene/Engineering_script.sh_script2.sh root@Baker_street_Linux_Server:/# find /home -iname '*research*' /home/lestrade/Research_script.sh_2.txt /home/lestrade/Research_script.sh_script1.sh /home/lestrade/Research_script.sh_3.txt /home/lestrade/Research_script.sh_script2.sh root@Baker_street_Linux_Server:/# find /home -name '*finance*' root@Baker_street_Linux_Server:/# find /home -iname '*engineering*' -exec chown :engineering {} + -exec chmod 770 {} + root@Baker_street_Linux_Server:/# find /home -iname '*research*' -exec chown :research {} + -exec chmod 770 {} + root@Baker_street_Linux_Server:/# find /home -iname '*fianance*' -exec chown :engineering {} + -exec chmod 770 {} + root@Baker_street_Linux_Server:/# find /home -iname '*password*' -exec rm -f {} + root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# find /home -perm /o+rwx root@Baker_street_Linux_Server:/# ls -l /home total 96 drwxr-x--- 1 adler adler 4096 Dec 12 07:45 adler drwxr-x--- 1 1009 1009 4096 Dec 12 07:45 gregson drwxr-x--- 1 1004 1004 4096 Dec 12 07:45 irene drwxr-x--- 1 1005 1005 4096 Dec 12 07:45 lestrade drwxr-x--- 1 1007 1007 4096 Dec 12 07:45 mary drwxr-x--- 1 moriarty moriarty 4096 Dec 12 07:45 moriarty drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 mrs_hudson drwxr-x--- 1 mycroft mycroft 4096 Dec 12 07:45 mycroft drwxr-x--- 1 sherlock sherlock 4096 Jan 11 21:39 sherlock drwxr-x--- 1 sysadmin sysadmin 4096 Dec 12 07:45 sysadmin drwxr-x--- 1 toby toby 4096 Dec 12 07:45 toby drwxr-x--- 1 watson watson 4096 Dec 12 07:45 watson root@Baker_street_Linux_Server:/#

	Optional: Updating password hashing configuration	Nano /etc/ssh/sshd_conf; service ssh restart; service ssh status; netstat -tuln | grep 22; sshd -t root@Baker_street_Linux_Server:/# nano /etc/ssh sshd_conf root@Baker_street_Linux_Server:/# service ssh restart * Restarting OpenBSD Secure Shell server ssd [OK] root@Baker_street_Linux_Server:/# service ssh status * sshd is running root@Baker_street_Linux_Server:/# netstat -tuln | grep 22 tcp 0 0 0.0.0.0:2224 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:2225 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:2222 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:2223 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN tcp6 0 0 :::2224 :::* LISTEN tcp6 0 0 :::2225 :::* LISTEN tcp6 0 0 :::2222 :::* LISTEN tcp6 0 0 :::2223 :::* LISTEN tcp6 0 0 :::22 :::* LISTEN root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# /etc/ssh/sshd_conf bash: /etc/ssh/sshd_conf: Permission denied root@Baker_street_Linux_Server:/# sshd -t root@Baker_street_Linux_Server:/# Nano /etc/ssh/sshd_conf # 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:/us> # 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 #PermitEmptyPasswords no #PermitRootlogin no Protocol 2 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 #AuthorizedPrincipalsFile none #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody # For this tost keys in /etc/ssh/ssh_known_hosts #Hostbased # 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, # PAM authentication via KbdInteractiveAuthentication may bypass # the setting of "PermitRootLogin without-password". # If you just want the PAM account and session checks to run without # PAM authentication, then enable this but set PasswordAuthentication # and KbdInteractiveAuthentication to 'no'. UsePAM yes #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody # For this tost keys in /etc/ssh/ssh_known_hosts #Hostbased # 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 #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody

	[illegible]	[illegible]

	Reviewing and updating system packages	Apt update ; service —status-all; apt remove --purge mysql-server mysql-client -y ; cat service_list.txt;apt auto remove -y ;apt autoremove -y; apt auto clean; root@Baker_street_Linux_Server:/# apt update Ign:1 http://security.ubuntu.com/ubuntu jammy-security InRelease Ign:2 http://archive.ubuntu.com/ubuntu jammy InRelease Ign:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease Ign:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease Ign:1 http://security.ubuntu.com/ubuntu jammy-security InRelease Ign:2 http://archive.ubuntu.com/ubuntu jammy InRelease Ign:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease Ign:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease Ign:2 http://archive.ubuntu.com/ubuntu jammy InRelease Ign:1 http://security.ubuntu.com/ubuntu jammy-security InRelease Ign:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease Ign:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease 0% [Working]^C root@Baker_street_Linux_Server:/# service —status-all [-] cron [-] dbus [?] hwclock.sh [-] mysql [-] openbsd-inetd [-] postfix [-] procps [+] ssh [-] ufw root@Baker_street_Linux_Server:/# cat service_list.txt root@Baker_street_Linux_Server:/# apt remove --purge mysql-server mysql-client -y Reading package lists... Done Building dependency tree... Done Reading state information... Done Package 'mysql-client' is not installed, so not removed Package 'mysql-server' is not installed, so not removed 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. root@Baker_street_Linux_Server:/# 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. root@Baker_street_Linux_Server:/# root@Baker_street_Linux_Server:/# apt autoclean Reading package lists... Done Building dependency tree... Done Reading state information... Done

<table>
<tr><td></td><td>Disabling unnecessary services</td><td>Service —-status-all > service_list.txt; cat service_list.txt; grep -iE “mysql | samba” service_list.txt; service mysql stop; service smbd stop; update-rc.d mysql disable; update-rc.d smbd disable; dpkg -l | grep samba; apt remove —-purge mysql-server mysql-client -y; apt remove —-purge samba samba-common-bin -y; apt auto remove -y; Apt autoclean; service —-status-all | grep -iE “mysql | samba”; visudo -c;

root@Baker_street_Linux_Server:/# service --status-all > service_list.txt
 [?] hwclock.sh
root@Baker_street_Linux_Server:/# cat service_list.txt
 [-] cron
 [-] dbus
 [-] mysql
 [-] openbsd-inetd
 [-] postfix
 [-] procps
 [+] ssh
 [-] ufw
root@Baker_street_Linux_Server:/# grep -iE "mysql | samba" service_list.txt
root@Baker_street_Linux_Server:/# service mysql stop
root@Baker_street_Linux_Server:/# service smbd stop
smbd: unrecognized service
root@Baker_street_Linux_Server:/# service nmbd stop
nmbd: unrecognized service
root@Baker_street_Linux_Server:/# service samba stop
samba: unrecognized service
root@Baker_street_Linux_Server:/# update-rc.d mysql disable
root@Baker_street_Linux_Server:/# update-rc.d smbd disable
update-rc.d: error: cannot find a LSB script for smbd
root@Baker_street_Linux_Server:/# update-rc.d nmbd disable
update-rc.d: error: cannot find a LSB script for nmbd
root@Baker_street_Linux_Server:/# dpkg -l | grep samba
rc samba-common   2:4.15.13+dfsg-0ubuntu1.6   all   common files used by both the Samba server and client
root@Baker_street_Linux_Server:/# apt remove --purge mysql-server mysql-client -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'mysql-client' is not installed, so not removed
Package 'mysql-server' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@Baker_street_Linux_Server:/# apt remove --purge samba samba-common-bin -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'samba' is not installed, so not removed
Package 'samba-common-bin' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@Baker_street_Linux_Server:/# 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.
root@Baker_street_Linux_Server:/# apt autoclean
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
root@Baker_street_Linux_Server:/# service --status-all | grep -iE "mysql | samba"
 [?] hwclock.sh
root@Baker_street_Linux_Server:/# dpkg -l | grep -iE "mysql | samba"
rc mysql-common   5.8+1.0.8   all   MySQL database common files, e.g. /etc/mysql/my.cnf
rc mysql-server-8.0   8.0.40-0ubuntu0.22.04.1   amd64   MySQL database server binaries and system database setup
rc samba-common   2:4.15.13+dfsg-0ubuntu1.6   all   common files used by both the Samba server and client
root@Baker_street_Linux_Server:/# sudo visudo -c
^C
sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution
root is not in the sudoers file. This incident will be reported.
root@Baker_street_Linux_Server:/#
root@Baker_street_Linux_Server:/# visudo -c
/etc/sudoers: parsed OK
/etc/sudoers.d/README: parsed OK</td></tr>
</table>

	Enabling and configuring logging	Nano /etc/systemd/journald.conf;nano /etc/logrotate.conf; systemctl restart systemd-journald; journalctl --disk-usage; logrotate -f /etc/logrotate.conf; ls -lh /var/log/ ; Nano /etc/systemd/journald.conf GNU nano 6.2 /etc/systemd/journald.conf # # should be created by either modifying this file, or by creating "drop-ins" in # the journald.conf.d/ subdirectory. The latter is generally recommended. # Defaults can be restored by simply deleting this file and all drop-ins. # # Use 'systemd-analyze cat-config systemd/journald.conf' to display the full co> # See journald.conf(5) for details. [Journal] #Storage=persistent #Compress=yes #Seal=yes #SplitMode=uid #SyncIntervalSec=5m #RateLimitIntervalSec=30s #RateLimitBurst=10000 #SystemMaxUse=300M #SystemKeepFree= #SystemMaxFileSize= RuntimeMaxUse= #RuntimeKeepFree= #RuntimeMaxFileSize= #RuntimeMaxFiles=100 #MaxRetentionSec= #MaxFileSec=1month #ForwardToSyslog=yes #ForwardToKMsg=no #ForwardToConsole=no #ForwardToWall=yes #TTYPath=/dev/console #MaxLevelStore=debug #MaxLevelSyslog=debug #MaxLevelKMsg=notice #MaxLevelConsole=info #MaxLevelWall=emerg #LineMax=48K #ReadKMsg=yes #Audit=no Nano /etc/logrotate.conf # see "man logrotate" for details root@Baker_street_Linux_Server:/# logrotate -d /etc/logrotate.conf WARNING: logrotate in debug mode does nothing except printing debug messages! Consider using verbose mode (-v) instead if this is not what you want. reading config file /etc/logrotate.conf including /etc/logrotate.d reading config file alternatives reading config file apt reading config file btmp reading config file dpkg reading config file mysql-server reading config file rsyslog reading config file ufw root@Baker_street_Linux_Server:/# logrotate -d /etc/logrotate.conf WARNING: logrotate in debug mode does nothing except printing debug messages! Consider using verbose mode (-v) instead if this is not what you want. reading config file /etc/logrotate.conf including /etc/logrotate.d reading config file alternatives reading config file apt reading config file btmp reading config file dpkg reading config file mysql-server reading config file rsyslog reading config file ufw reading config file wtmp Reading state from file: /var/lib/logrotate/status State file /var/lib/logrotate/status does not exist Allocating hash table for state file, size 64 entries Handling 9 logs rotating pattern: /var/log/alternatives.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/alternatives.log Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/apt/term.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/apt/term.log Creating new state # global options do not affect preceding include directives # rotate log files weekly daily # use the adm group by default, since this is the owning group # of /var/log/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 root@Baker_street_Linux_Server:/# logrotate -d /etc/logrotate.conf WARNING: logrotate in debug mode does nothing except printing debug messages! Consider using verbose mode (-v) instead if this is not what you want. reading config file /etc/logrotate.conf including /etc/logrotate.d reading config file alternatives reading config file apt reading config file btmp reading config file dpkg reading config file mysql-server reading config file rsyslog reading config file ufw reading config file wtmp Reading state from file: /var/lib/logrotate/status State file /var/lib/logrotate/status does not exist Allocating hash table for state file, size 64 entries Handling 9 logs rotating pattern: /var/log/alternatives.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/alternatives.log Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/apt/term.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/apt/term.log Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/apt/history.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/apt/history.log Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/btmp monthly (1 rotations) empty log files are rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/btmp Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/dpkg.log monthly (12 rotations) empty log files are not rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/dpkg.log Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) 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 391) 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: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 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 391) rotating pattern: /var/log/syslog /var/log/mail.info /var/log/mail.warn /var/log/mail.err /var/log/mail.log /var/log/daemon.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 391) considering log /var/log/syslog log /var/log/syslog does not exist -- skipping Creating new state considering log /var/log/mail.info log /var/log/mail.info does not exist -- skipping Creating new state considering log /var/log/mail.warn log /var/log/mail.warn does not exist -- skipping Creating new state considering log /var/log/mail.err log /var/log/mail.err does not exist -- skipping Creating new state considering log /var/log/mail.log log /var/log/mail.log does not exist -- skipping Creating new state considering log /var/log/daemon.log log /var/log/daemon.log does not exist -- skipping Creating new state considering log /var/log/kern.log log /var/log/kern.log does not exist -- skipping Creating new state considering log /var/log/auth.log log /var/log/auth.log does not exist -- skipping Creating new state considering log /var/log/user.log log /var/log/user.log does not exist -- skipping Creating new state considering log /var/log/lpr.log log /var/log/lpr.log does not exist -- skipping Creating new state considering log /var/log/cron.log log /var/log/cron.log does not exist -- skipping Creating new state considering log /var/log/debug log /var/log/debug does not exist -- skipping Creating new state considering log /var/log/messages log /var/log/messages does not exist -- skipping Creating new state not running postrotate script, since no logs were rotated switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/ufw.log 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 391) considering log /var/log/ufw.log log /var/log/ufw.log does not exist -- skipping Creating new state not running postrotate script, since no logs were rotated switching euid from 0 to 0 and egid from 4 to 0 (pid 391) rotating pattern: /var/log/wtmp monthly (1 rotations) empty log files are rotated, only log files >= 1048576 bytes are rotated, old logs are removed switching euid from 0 to 0 and egid from 0 to 4 (pid 391) considering log /var/log/wtmp Creating new state Now: 2025-01-14 20:59 Last rotated at 2025-01-14 20:00 log does not need rotating (log has already been rotated) switching euid from 0 to 0 and egid from 4 to 0 (pid 391) root@Baker_street_Linux_Server:/# systemctl restart systemd-journald System has not been booted with systemd as init system (PID 1). Can't operate. Failed to connect to bus: Host is down root@Baker_street_Linux_Server:/# journalctl --disk-usage No journal files were found. Archived and active journals take up 0B in the file system. root@Baker_street_Linux_Server:/# logrotate -f /etc/logrotate.conf root@Baker_street_Linux_Server:/# ls -lh /var/log total 1.2M -rw-r--r-- 1 root root 0 Jan 16 01:59 alternatives.log -rw-r--r-- 1 root root 13K Jan 14 19:48 alternatives.log.1 drwxr-xr-x 2 root root 4.0K Jan 16 01:59 apt -rw------- 1 root root 64K Sep 11 14:04 bootstrap.log -rw-rw---- 1 root utmp 0 Jan 16 01:59 btmp -rw-rw---- 1 root utmp 1.3K Jan 11 22:33 btmp.1 -rw-r--r-- 1 root root 0 Jan 16 01:59 dpkg.log -rw-r--r-- 1 root root 344K Jan 14 19:48 dpkg.log.1 -rw-r--r-- 1 root root 32K Jan 14 21:29 faillog drwxr-sr-x 2 root systemd-journal 4.0K Dec 12 07:44 journal -rw-rw-r-- 1 root utmp 285K Jan 14 21:29 lastlog -rwxr-xr-x 1 root root 0 Jan 15 23:51 logcleanup.sh -rw-r--r-- 1 root root 36K Jan 15 19:47 lynis-report.dat -rw-r--r-- 1 root root 394K Jan 15 19:47 lynis.log drwxr-x--- 1 mysql adm 4.0K Jan 16 01:59 mysql drwx------ 2 root root 4.0K Dec 12 07:44 private drwxr-x--- 1 root adm 4.0K Jan 7 00:25 samba -rw-rw-r-- 1 root utmp 0 Jan 16 01:59 wtmp -rw-rw---- 1 root utmp 0 Sep 11 14:04

	Scripts created	Nano hardening_script1.sh; chmod +x hardening_script1.sh; ./hardening_script hardening_script2.sh; ls -l hardening_scr hardening_script.sh Nano hardening_scripts2.sh #!/bin/bash # Variable for the report output choose a **NEW** output file nam REPORT_FILE="hardening_sc # Output the sshd configuratio echo "Gathering details from s configuration file" # Placeholder for command to sshd configuration file echo "sshd configuration file:$(ssh/sshd_config)" >> $REPOR printf "\n" >> $REPORT_FILE # Update packages and servic Echo "Updating packages and services" # Placeholder for command to packages sudo apt update # Placeholder for command to upgrade packages Sudo apt upgrade echo "Packages have been up and upgraded" >> $REPORT_ printf "\n" >> $REPORT_FILE # Placeholder for command to installed packages echo "Installed Packages:$(su install)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Printing out logging configuration data" # Placeholder for command to logging data echo "journald.conf file data: $(cat /var/log/syslog)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Placeholder for command to logrotate data echo "logrotate.conf file data:$ etc/logrotate.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Script execution complet Check $REPORT_FILE for det root@Baker_street_Linux_Server:/# nano hardening_script2.sh root@Baker_street_Linux_Server:/# chm hardening_script2.sh chmod: cannot access 'hardening_script2. such file or directory root@Baker_street_Linux_Server:/# ./ hardening_script2.sh bash: ./hardening_script2.sh: No such file directory root@Baker_street_Linux_Server:/# ./hardening_script1.sh: line 4: Baker_street_Linux_Server: command no ./hardening_script1.sh: line 4: $REPORT ambiguous redirect ./hardening_script1.sh: line 10: $REPORT ambiguous redirect Gathering OS hostname... cat: etc/: Is a directory cat: os-release: No such file or directory ./hardening_script1.sh: line 15: $REPORT ambiguous redirect ./hardening_script1.sh: line 16: $REPORT ambiguous redirect Gathering memory information... ./hardening_script1.sh: line 21: $REPORT ambiguous redirect ./hardening_script1.sh: line 22: $REPORT ambiguous redirect Gathering uptime information... ./hardening_script1.sh: line 27: $REPORT ambiguous redirect ./hardening_script1.sh: line 28: $REPORT ambiguous redirect Backing up the OS... sudo: unable to resolve host Baker_street_Linux_Server: Temporary f name resolution root is not in the sudoers file. This incide reported. ./hardening_script1.sh: line 36: $REPORT ambiguous redirect ./hardening_script1.sh: line 37: $REPORT ambiguous redirect Gathering sudoers file ... (Last step) root@Baker_street_Linux_Server:/# ls -l hardening_script1.sh -rwxr-xr-x 1 root root 2918 Jan 16 18:59 hardening_script1.sh root@Baker_street_Linux_Server: ls -l hardening_script2.sh -rwxr-xr-x 1 root root 2928 Jan 16 19:23 root@Baker_street_Linux_Server:/# nan hardening_script1.sh root@Baker_street_Linux_Server:/# chm hardening1.sh root@Baker_street_Linux_Server:/# ./ hardening_script1.sh ./hardening_script1.sh: line 4: Baker_street_Linux_Server: command n ./hardening_script1.sh: line 4: $REPORT ambiguous redirect ./hardening_script1.sh: line 10: $REPOR ambiguous redirect Gathering OS hostname... cat: etc/: Is a directory cat: os-release: No such file or directory ./hardening_script1.sh: line 15: $REPOR ambiguous redirect ./hardening_script1.sh: line 16: $REPOR ambiguous redirect Gathering memory information... ./hardening_script1.sh: line 21: $REPOR ambiguous redirect ./hardening_script1.sh: line 22: $REPOR ambiguous redirect Gathering uptime information... ./hardening_script1.sh: line 27: $REPOR ambiguous redirect ./hardening_script1.sh: line 28: $REPOR ambiguous redirect Backing up the OS... sudo: unable to resolve host Baker_street_Linux_Server: Temporary f name resolution root is not in the sudoers file. This incide reported. ./hardening_script1.sh: line 36: $REPOR ambiguous redirect ./hardening_script1.sh: line 37: $REPOR ambiguous redirect root@Baker_street_Linux_Server:/# nan hardening_script2.sh root@Baker_street_Linux_Server:/# chm hardening_script2.sh root@Baker_street_Linux_Server:/# ./ hardening_script2.sh ./hardening_script1.sh: Baker_street_Linux_Server: command n ./hardening_script2.sh: line 4: $REPORT ambiguous redirect ./hardening_script1.sh: line 10: $REPOR ambiguous redirect Gathering OS hostname... cat: etc/: Is a directory cat: os-release: No such file or directory ./hardening_script1.sh: line 15: $REPOR ambiguous redirect ./hardening_script1.sh: line 16: $REPOR ambiguous redirect Gathering memory information... ./hardening_script1.sh: line 21: $REPOR ambiguous redirect ./hardening_script1.sh: line 22: $REPOR ambiguous redirect Gathering uptime information... ./hardening_script1.sh: line 27: $REPOR ambiguous redirect ./hardening_script1.sh: line 28: $REPOR ambiguous redirect Backing up the OS... sudo: unable to resolve host Baker_street_Linux_Server: Temporary f name resolution root is not in the sudoers file. This incide reported. ./hardening_script1.sh: line 36: $REPOR ambiguous redirect ./hardening_script1.sh: line 37: $REPOR ambiguous redirect

	Scripts scheduled with cron	Crontab -e; crontab -l; root@Baker_street_Linux_Server:/# crontab -e crontab: installing new crontab root@Baker_street_Linux_Server:/# 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/ # # For more information see the manual pages of crontab(5) and cron(8) # # m h dom mon dow command 0 0 1 * * /path/to/script1.sh 0 0 * * 1 /path/to/script2.sh root@Baker_street_Linux_Server:/# /path/to/hardening_script1.sh bash: /path/to/hardening_script1.sh: No such file or directory root@Baker_street_Linux_Server:/# sudo /path/to/hardening_script1.sh sudo: unable to resolve host Baker_street_Linux_Server: Temporary failure in name resolution root is not in the sudoers file. This incident will be reported. root@Baker_street_Linux_Server:/# find /-name "hardening_script1.sh" 2 >dev/null find: '/-name': No such file or directory find: '2': No such file or directory root@Baker_street_Linux_Server:/# /root/scripts/hardening_script1.sh bash: /root/scripts/hardening_script1.sh: No such file or directory root@Baker_street_Linux_Server:/# chmod +x /actual/path/to/hardening_script1.sh chmod: cannot access '/actual/path/to/hardening_script1.sh': No such file or directory root@Baker_street_Linux_Server:/# bash -x /actual//path/to/hardening_script1.sh bash: /actual//path/to/hardening_script1.sh: No such file or directory root@Baker_street_Linux_Server:/#

		SUMMARY REPORT During the pre-hardened stage. The system information from hostname; OS Version; Memory information; and uptime all followed the standards and anything that needed to be updated were completed. Some concerns that I noticed were lack up regular updates that could possibly pose a lack of security patches. There were also no existing backup policy, which could cause a risk of system hardening. I updated the current system and installed the neccessary packages to help with any backup problems that could arose in near future. All members of the user group were reviewed with the grep ^ sudo /etc/group command. Verified and unnecassary users from group were restricted and limited and specfic users could only execute certain commands in sudoers file. Every tasked completed in project were validated and tested for authorized users. All users with sudo access are now documented and justified.Logging for sudo commands is enabled for accountability. Protect user account was also addressed in the project, the cat /etc/passwd listed all user accounts to identify legitimate and unwanted accounts; reviewed locked and active accounts with passwd -S username command; and also sudo userdel to remove and disable accounts. Password policies now enforce complexity, length, and expiration, reducing weak credential risks. In summary, the server has been properly hardened correctly. Patching vulnerabilities to the latest security standards.Removing unnecessary software and disabling redundant services.Establishing a robust backup strategy with automated schedules. Deploying tools and processes for continuous monitoring. Ongoing maintenance and proactive monitoring will be applied.

		1. UFW (Uncomplicated Firewall)Hardening Features: • Simplifies the process of managing firewall rules on Linux. • Allows users to control incoming and outgoing network traffic to secure the system. • Features default rules to deny all incoming connections while allowing outgoing ones, providing a basic secure configuration. • Easily configurable to allow specific ports, services, or IP addresses. **2. Lynis** **Hardening Features:** • A powerful security auditing tool that scans the system for vulnerabilities and misconfigurations. • Provides recommendations for hardening the operating system, network settings, and installed applications. • Can identify weak file permissions, missing patches, and security controls. • Generates a detailed report highlighting risks and suggested improvements **Tripwire** **Hardening Features:** • A file integrity monitoring tool that detects unauthorized changes to files and • directories. • Creates a baseline database of file hashes and compares it to the current state during regular scans. • Alerts administrators to potential tampering or security breaches. • Helps ensure critical system files remain unaltered.