

**Andree Salvo**

**Southern New Hampshire University**

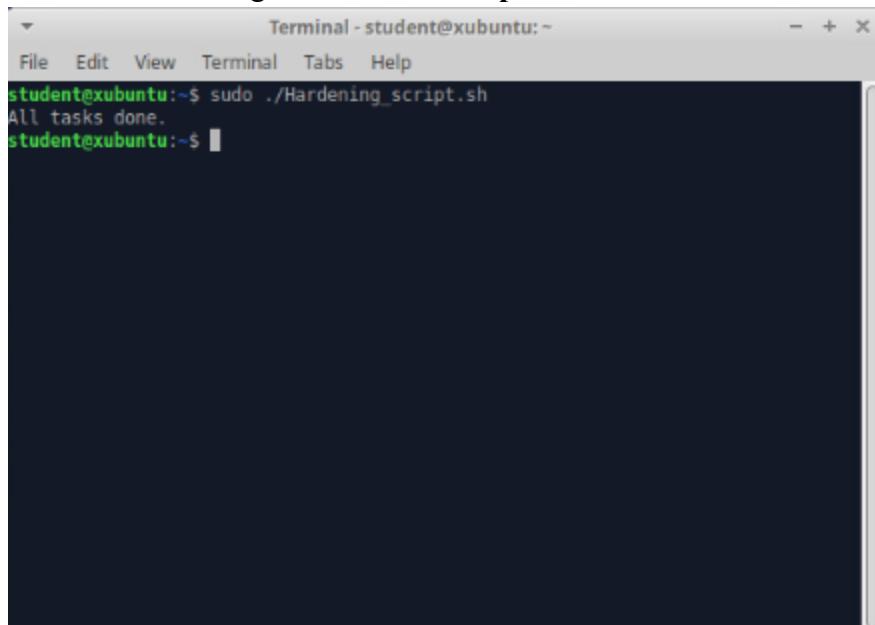
**CYB 300 – 14668**

**Instructor: Jason Keltner**

### **7-1 Project**

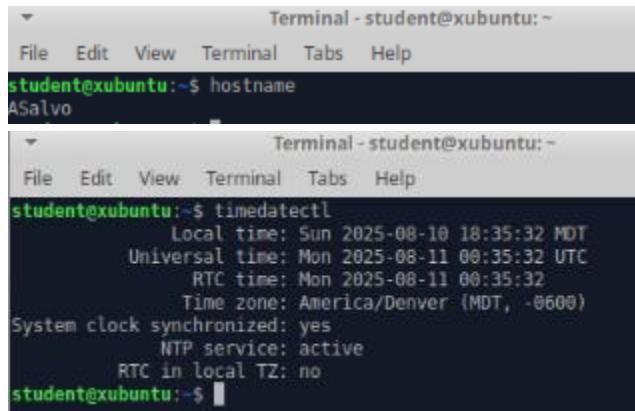
- 1. Automated Hardening Scripts:** Compose a single executable script to automate hardening tasks to meet the requirements in the scenario.

- a. Screenshot of a single **executable script** in the Linux shell environment



A screenshot of a terminal window titled "Terminal - student@xubuntu:~". The window has a standard title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main terminal area shows the command "student@xubuntu:~\$ sudo ./Hardening\_script.sh" followed by the output "All tasks done." and a final prompt "student@xubuntu:~\$".

- b. Screenshots that **evidence** each requirement has been met



The image contains two screenshots of terminal windows. The top window is titled "Terminal - student@xubuntu:~" and shows the command "student@xubuntu:~\$ hostname" followed by the output "ASalvo". The bottom window is also titled "Terminal - student@xubuntu:~" and shows the command "student@xubuntu:~\$ timedatectl" followed by detailed output about the system's time synchronization status, including local time (Sun 2025-08-10 18:35:32 MDT), universal time (Mon 2025-08-11 00:35:32 UTC), RTC time (Mon 2025-08-11 00:35:32), time zone (America/Denver (MDT, -0600)), system clock synchronized (yes), NTP service (active), and RTC in local TZ (no).

```

student@xubuntu:~$ head processes.txt
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.3  0.3 102260 13416 ?      Ss  17:58  0:06 /sbin/init sp
lash
root      2  0.0  0.0     0   0 ?      S    17:58  0:00 [kthreadd]
root      3  0.0  0.0     0   0 ?      I<  17:58  0:00 [rcu_gp]
root      4  0.0  0.0     0   0 ?      I<  17:58  0:00 [rcu_par_gp]
root      5  0.0  0.0     0   0 ?      I<  17:58  0:00 [slub_flushwq]
]
root      6  0.0  0.0     0   0 ?      I<  17:58  0:00 [netns]
root      8  0.0  0.0     0   0 ?      I<  17:58  0:00 [kworker/0:0H
-events_highpri]
root     10  0.0  0.0     0   0 ?      I<  17:58  0:00 [mm_percpu_wq]
]
root     11  0.0  0.0     0   0 ?      S    17:58  0:00 [rcu_tasks_ru
de_]
student@xubuntu:~$ [REDACTED]

```

Terminal - student@xubuntu:~

```

File Edit View Terminal Tabs Help
student@xubuntu:~$ gsettings set org.gnome.desktop.screensaver lock-enabled true && gsettings set org.gnome.saver lock-enabled && gsettings get org.gnome.desktop.session idle-delay
true
uint32 180
student@xubuntu:~$ [REDACTED]

```

```

Terminal - student@xubuntu:~
File Edit View Terminal Tabs Help
student@xubuntu:~$ cat SecurityLog_Salvo.txt
aug 10 20:08:55 xubuntu anacron[3667]: Updated timestamp for job 'cron.weekly' to 2025-08-10
aug 10 20:08:55 xubuntu anacron[776]: Job 'cron.weekly' terminated
aug 10 20:13:35 xubuntu dbus-daemon[780]: [system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedes
t' (uid=1000 pid=3727 comm="timedatectl set-timezone America/Denver " label="unconfined")
aug 10 20:13:35 xubuntu systemd[1]: Starting Time & Date Service...
aug 10 20:13:35 xubuntu dbus-daemon[780]: [system] Successfully activated service 'org.freedesktop.timedate1'
aug 10 20:13:35 xubuntu systemd[1]: Started Time & Date Service.
aug 10 20:13:35 xubuntu systemd[1]-timedated[3732]: Changed time zone to 'America/Denver' (MDT).
aug 10 20:13:55 xubuntu anacron[776]: Job 'cron.monthly' started
aug 10 20:13:55 xubuntu systemd[1]: Starting Cleanup of Temporary Directories...
aug 10 20:13:55 xubuntu anacron[776]: Job 'cron.monthly' terminated
aug 10 20:13:55 xubuntu anacron[776]: Normal exit (3 jobs run)
aug 10 20:13:55 xubuntu systemd[1]: anacron.service: Killing process 3741 (anacron) with signal SIGKILL.
aug 10 20:13:55 xubuntu systemd[1]: anacron.service: Killing process 3741 (anacron) with signal SIGKILL.
aug 10 20:13:55 xubuntu systemd[1]: anacron.service: Deactivated successfully.
aug 10 20:13:55 xubuntu systemd[1]: anacron.service: Unit process 3741 (anacron) remains running after unit stopped.
aug 10 20:13:55 xubuntu systemd[1]: system-tmpfiles-clean.service: Deactivated successfully.
aug 10 20:13:55 xubuntu systemd[1]: Finished Cleanup of Temporary Directories.
aug 10 20:14:05 xubuntu systemd[1]: timedated.service: Deactivated successfully.
aug 10 20:14:19 xubuntu dbus-daemon[1319]: [session uid=1000 pid=1319] Activating via systemd: service name='ca.desrt.dconf' unit='dconf.s
-3745 comm=gsettings set org.gnome.desktop.session idle-delay label="unconfined"
aug 10 20:14:19 xubuntu systemd[1303]: Starting User preferences database...
aug 10 20:14:19 xubuntu dbus-daemon[1319]: [session uid=1000 pid=1319] Successfully activated service 'ca.desrt.dconf'
aug 10 20:14:19 xubuntu systemd[1303]: Started User preferences database.
aug 10 20:16:36 xubuntu dbus-daemon[780]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedes
t' (uid=0 pid=3755 comm="hostname1 set-hostname A Salvo " label="unconfined")
aug 10 20:16:36 xubuntu systemd[1]: Starting Hostname Service...
aug 10 20:16:36 xubuntu dbus-daemon[780]: [system] Successfully activated service 'org.freedesktop.hostname1'
aug 10 20:16:36 xubuntu systemd[1]: Started Hostname Service.
aug 10 20:17:01 xubuntu CRON[3759]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
aug 10 20:17:06 xubuntu systemd[1]: system-hostnamed.service: Deactivated successfully.
aug 10 20:17:07 xubuntu dbus-daemon[780]: [system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedes
t' (uid=0 pid=3767 comm="timedatectl set-timezone America/Denver " label="unconfined")
aug 10 20:17:07 xubuntu systemd[1]: Starting Time & Date Service...
aug 10 20:17:07 xubuntu dbus-daemon[780]: [system] Successfully activated service 'org.freedesktop.timedate1'
aug 10 20:17:07 xubuntu systemd[1]: Started Time & Date Service.
aug 10 20:17:37 xubuntu systemd[1]: system-timedated.service: Deactivated successfully.
aug 10 20:18:03 xubuntu dbus-daemon[780]: [system] Activating via systemd: service name='org.freedesktop.timedate1' unit='dbus-org.freedes
t' (uid=1000 pid=3773 comm="timedatectl " label="unconfined")
aug 10 20:18:03 xubuntu systemd[1]: Starting Time & Date Service...
aug 10 20:18:03 xubuntu dbus-daemon[780]: [system] Successfully activated service 'org.freedesktop.timedate1'
aug 10 20:18:03 xubuntu systemd[1]: Started Time & Date Service.
aug 10 20:18:33 xubuntu systemd[1]: system-timedated.service: Deactivated successfully.
aug 10 20:30:01 xubuntu CRON[3788]: (root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /run/systemd/system ]; then /usr/sbin/invoke-rc.d
aug 10 20:30:38 xubuntu dbus-daemon[780]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedes
t' (uid=0 pid=3796 comm="hostname1 set-hostname A Salvo " label="unconfined")
aug 10 20:30:38 xubuntu systemd[1]: Starting Hostname Service...
aug 10 20:30:38 xubuntu dbus-daemon[780]: [system] Successfully activated service 'org.freedesktop.hostname1'
aug 10 20:30:38 xubuntu systemd[1]: Started Hostname Service.
aug 10 20:30:38 xubuntu dbus-daemon[3810]: [session uid=1000 pid=3808] AppArmor D-Bus mediation is enabled
aug 10 20:30:38 xubuntu dbus-daemon[3810]: [session uid=1000 pid=3808] Activating service name='ca.desrt.dconf' requested by ':1.0' (uid=1
desktop.screensaver lock-e" label="unconfined")
aug 10 20:30:38 xubuntu dbus-daemon[3810]: [session uid=1000 pid=3808] Successfully activated service 'ca.desrt.dconf'

```

- c. Aside from saving time, automated scripts make it a lot easier to keep things consistent and avoid mistakes that can happen when doing configurations by hand. This will let you

roll out the same secure settings to every system without having to repeat the work, and you can reuse them whenever you need to make updates. Also, having a script means you've got a clear record of what changes were made, which helps with audits and makes fixing issues down the road a lot simpler and easier.

## 2. Certificate Authority

- a. Provide a screenshot of the OpenSSL commands to create a CA with settings that meet the organizational requirements

```
student@xubuntu:~$ openssl genrsa -aes256 -out rootCA.key 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
student@xubuntu:~$ openssl req -x509 -new -sha256 -days 365 -key rootCA.key -out rootCA.crt -subj "/C=US/ST=CO/O=Salvo-org/CN=Colorado Office Root"
Enter pass phrase for rootCA.key:
student@xubuntu:~$ ls -l rootCA.*
```

```

student@ubuntu:~$ openssl x509 -in rootCA.crt -text -noout
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        7f:37:47:37:2f:30:ba:71:6f:e2:ac:1c:dc:cd:ef:ee:26:61:4f:0b
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = US, ST = CO, O = Salvo-org, CN = Colorado Office Root
    Validity
        Not Before: Aug 11 01:04:07 2025 GMT
        Not After : Aug 11 01:04:07 2026 GMT
    Subject: C = US, ST = CO, O = Salvo-org, CN = Colorado Office Root
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
            Modulus:
                00:bd:e1:04:71:81:a9:02:14:47:f9:18:60:f7:6c:
                cf:ce:c6:c7:74:28:1f:c8:2c:96:47:97:07:14:71:
                01:3a:8a:24:2c:ad:ac:f3:68:3f:15:83:e9:a5:c1:
                0d:67:34:6d:50:58:92:4b:fc:65:c0:67:5c:f8:e2:
                3c:fe:d8:84:cc:65:48:e3:86:73:63:21:43:72:d9:
                0a:4a:bd:d0:e1:7c:72:ff:a1:b0:02:6b:96:31:4a:
                15:14:c1:4f:63:7e:ca:de:85:96:ff:34:98:2e:10:
                de:7a:cd:3b:61:39:d5:23:57:f1:0f:aa:4b:96:c7:
                fd:6c:58:d5:ed:f7:4d:50:a5:d6:92:73:37:ad:7f:
                81:f7:be:7a:fc:6d:99:a9:40:b6:62:12:07:2e:b3:
                72:e3:c2:40:70:0f:3f:58:92:3a:2e:4e:39:ba:36:
                97:4a:c5:a6:57:73:d0:b4:b7:97:94:ef:ed:fe:df:
                ad:8f:81:87:a7:10:aa:1e:20:3e:c3:dc:7d:f0:de:
                51:7e:49:5f:c1:54:a5:57:22:c6:14:54:a6:c8:59:
                1d:85:bd:2c:6a:c1:7c:bf:12:78:35:c1:47:b0:ec:
                a9:f8:e8:99:63:1c:4f:e9:d2:fd:78:4c:1f:1f:8f:
                b7:a8:32:b4:f6:fb:fe:5b:de:af:7c:1e:fe:75:a6:
                db:eb:84:e2:84:ab:ae:a5:6f:00:9e:a5:af:66:44:
                14:91:39:e0:d3:68:ea:4d:aa:82:f9:c4:55:ff:bb:
                97:c6:35:75:3b:05:a6:d3:f7:f3:ad:ba:b3:25:
                b6:b3:13:cc:a7:db:67:08:61:14:d2:30:39:98:b8:
                08:9a:4f:3a:61:9e:a7:84:b1:6e:4f:60:d4:12:35:
                ef:1d:8c:f7:31:f7:9a:6d:39:d1:0d:15:cb:25:19:
                ad:8b:a5:53:c6:a6:1f:62:02:46:c1:f8:94:e8:0c:
                1e:02:98:1b:01:43:f2:dc:ae:a9:fd:bb:3d:e8:ed:
                b4:de:54:5d:81:63:98:76:a3:20:eb:80:3d:da:9f:
                93:dd:13:91:b2:29:ca:44:5a:14:f9:04:4d:7c:23:
                d0:9d:42:4c:al:ce:25:3f:a7:d8:a5:ed:47:8d:5e:
                67:7c:a7:1e:6d:ef:4d:9e:4d:18:d8:80:e9:00:45:
                51:34:38:2f:67:6f:88:97:22:b2:4e:7d:f2:cc:76:
                0e:d8:df:39:d8:d5:06:a0:a3:72:f2:fa:16:48:83:
                54:89:fa:37:1d:72:a4:b4:9e:7c:42:a1:8a:07:39:
                51:66:8a:5d:16:3e:dd:6b:27:63:fb:c3:dd:8a:72:
                7d:bd:b5:01:d9:28:38:11:57:05:38:ba:61:f9:2f:
                d5:06:13
            Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        FE:A5:20:35:AC:4B:01:4A:F2:20:72:A1:CE:B1:56:DE:4E:B3:07:0C
    X509v3 Authority Key Identifier:
        FE:A5:20:35:AC:4B:01:4A:F2:20:72:A1:CE:B1:56:DE:4E:B3:07:0C
    X509v3 Basic Constraints: critical
        CA:TRUE

```

- b. To create a Certificate Signing Request (CSR) for a server or workstation in the new location, the system administrator first generates a private key using `openssl genrsa -out server.key 2048`, which securely stores the cryptographic key on the machine. Next, they run `openssl req -new -sha256 -key server.key -out server.csr -subj "/C=US/ST=CO/O=Salvo-Org/CN=server1.colorado.office.local"` to generate the CSR,

embedding the organization and host details. The resulting .csr file is then securely transmitted to the Colorado Office Root CA administrator, who verifies the request against organizational policies, signs it with the CA's private key, and returns the issued certificate (server.crt). Finally, the server or workstation installs both the signed certificate and the CA's root certificate to establish a trusted, encrypted communication channel.

- c. Using Public Key Infrastructure (PKI) ties into the security principles of **defense in depth** and **complete mediation**. First, Defense in depth comes from adding certificates and encryption as another layer on top of things like usernames and passwords, so there's more than one barrier keeping systems safe. Second, Complete mediation means every single connection is checked and validated through certificate verification, so nothing slips through without being reviewed. For the CIA triad, PKI helps with **confidentiality** by encrypting traffic, **integrity** by making sure data hasn't been tampered with through digital signatures, and **availability** by keeping connections secure and reliable so attacks don't take systems offline.

### 3. Hardening Systems

- a. **Discuss how to make the transition from industry guidelines to a baseline that is appropriate for your organization**

Transitioning from industry guidelines to an organizational baseline starts with picking a trusted standard, like the NIST framework or CIS Benchmarks, as your starting point. You go through each control and figure out what applies best to your environment, removing anything that doesn't make sense for your systems and adding any extra

settings that address unique risks your organization faces. The goal here is to take the broad “baseline starting points” recommendations and customize them so they fit your actual network, applications, and workflows. Once these are tailored, the baseline is set, and you apply it consistently across all systems and keep it updated as threats, technology, or business needs change.

- b. Create an operating system security-configuration checklist representing the elements used in Part I: Automated Hardening Scripts**
  - I. Rename Computer > First Initial\_Last Name (hostname status)**
  - II. Change Time Zone > America/Denver (timedatectl)**
  - III. List Running Processes > processes.txt (ls -l processes.txt and head processes.txt)**
  - IV. Set idle lock time for screensaver to 3 min > (gsettings get org.gnome.desktop.session idle-delay and gsettings get org.gnome.desktop.screensaver lock-enabled)**
  - V. Last 50 syslog entries > SecurityLog\_Salvo.txt (wc -l SecurityLog\_Salvo.txt and tail SecurityLog\_Salvo.txt)**

- c. Why checklists are important**

Security configuration checklists make it easier to keep systems consistent and reduce the chances of missing important steps. They turn policies into clear, repeatable actions that anyone on the team can follow, which is especially useful when multiple people are responsible for hardening systems. Checklists also make audits and troubleshooting simpler, because you have a record of what’s been applied and verified, and they help maintain compliance with internal standards or external regulations.