Operating Systems Hardening

Mamadu Bah, Lassine Guindo, Isaiah Stover

CTEC 450

OS Hardening Steps

1. System Configuration

- Turn off unnecessary services to reduce security risks.
- Set up a firewall to block unauthorized access.
- Use strong passwords to protect user accounts.

2. User & Access Control

- Create user accounts with limited access to prevent misuse.
- Enable multi-factor authentication (MFA) for extra login security.
- Remove inactive accounts to reduce threats.

3. Patch & Update Management

- Install security updates to fix vulnerabilities.
- Enable automatic updates to stay protected.
- Remove old or unsupported software to prevent attacks.

4. Network Security

- Use firewalls & intrusion detection systems (IDS) to monitor traffic.
- Disable unused network services to reduce exposure.
- Use VPN encryption for secure remote access.

5. Logging & Monitoring

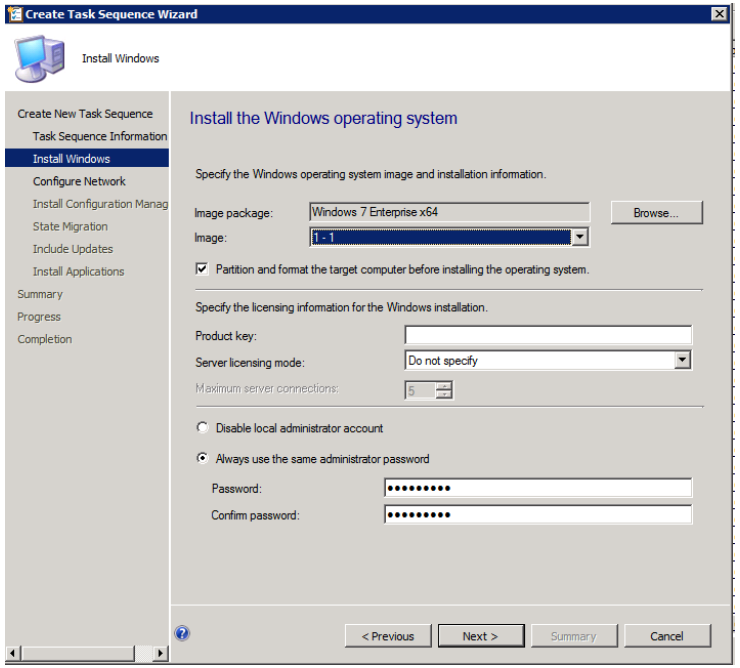
- Enable system logs to track activities.
- Use log analysis tools to detect threats.
- Set up alerts for unusual activity.

6. Application Security & Backup

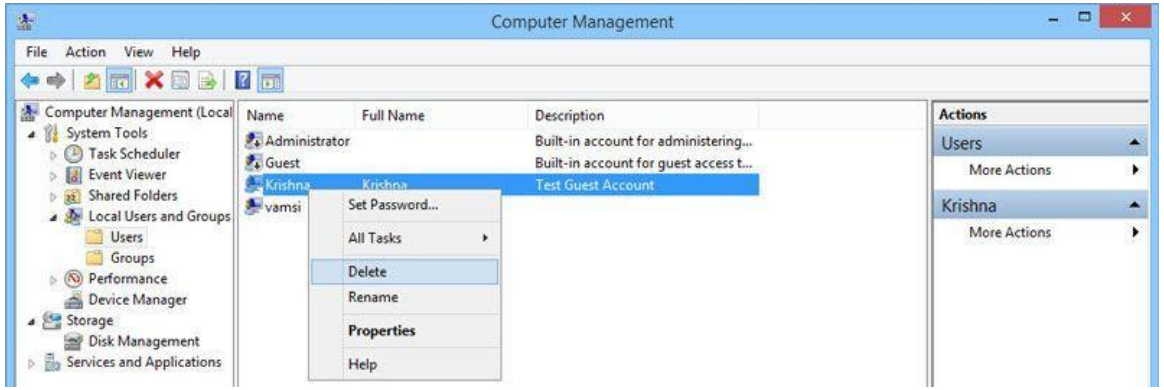
- Allow only approved applications to run.
- Regularly update installed software to close security gaps.
- Create backups and store them securely to prevent data loss.

Step-By-Step Guide

Step 1: Configure the System
Open settings and disable unnecessary services.
Set up a firewall to control network access. Enforce strong password policies in security settings.



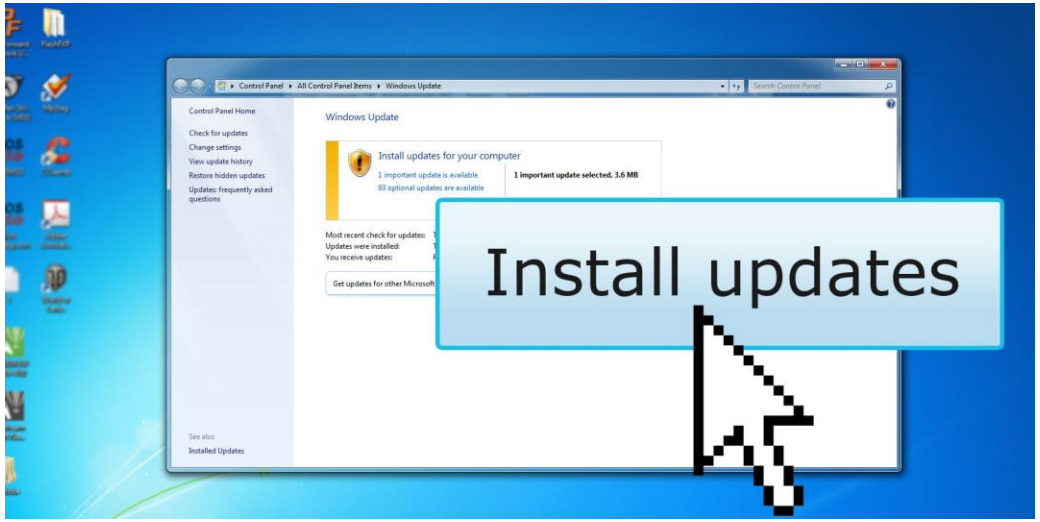
- Step 2: Manage Users & Access
  Create limited-access user accounts.
  Enable multi-factor authentication (MFA).
  Remove unused or inactive accounts.



Step-By-Step Guide

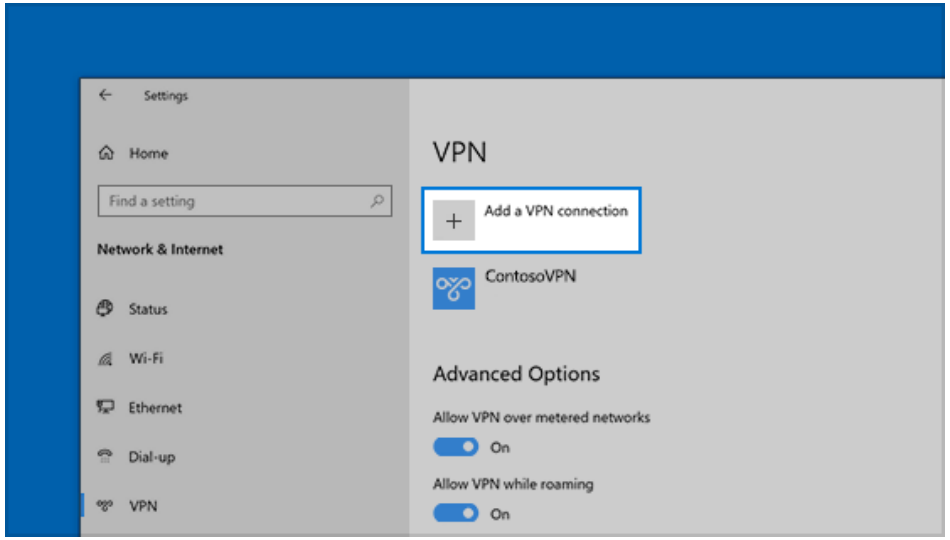
Step 3: Apply Updates & Patches

- Check for pending OS and software updates.
- Enable automatic updates to prevent security gaps.
- Remove outdated applications.



Step 4: Secure the Network

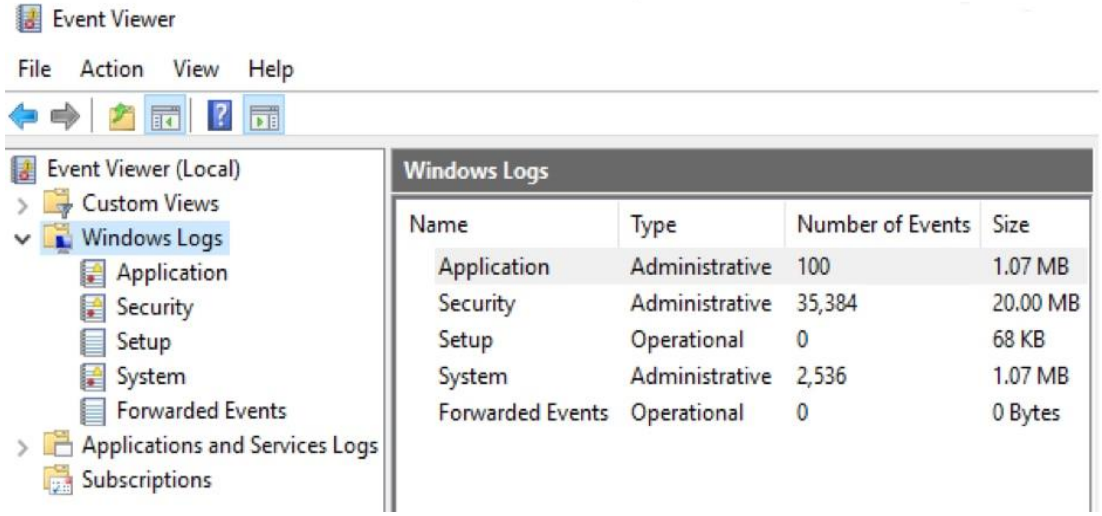
- Configure firewalls and set strict rules.
- Disable unused network ports & services.
- Use VPN for encrypted remote access.



Step-By-Step Guide

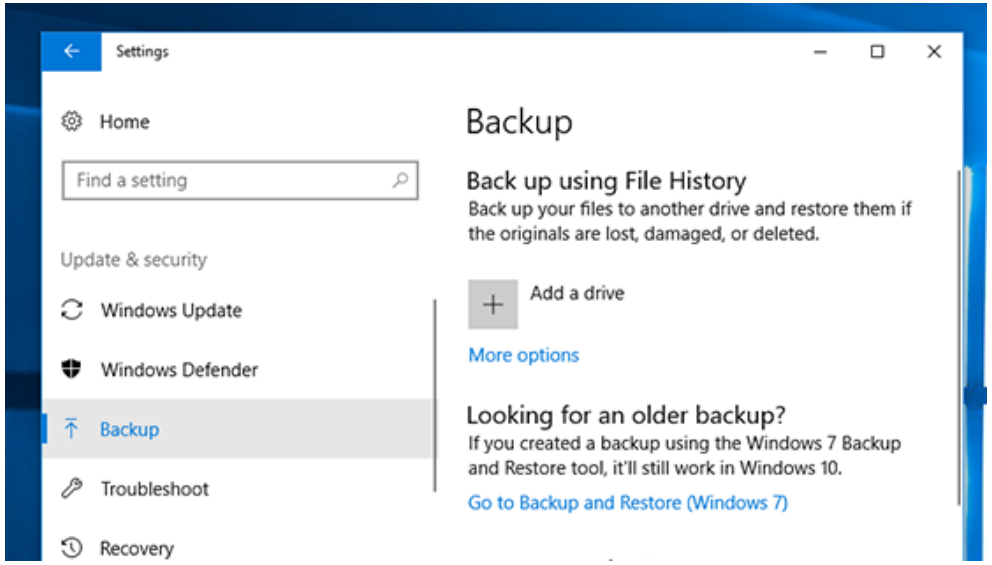
Step 5: Enable Logging & Monitoring

- Turn on logging to track system activity.
- Set up alerts for failed login attempts.
- Regularly review logs for suspicious behavior.

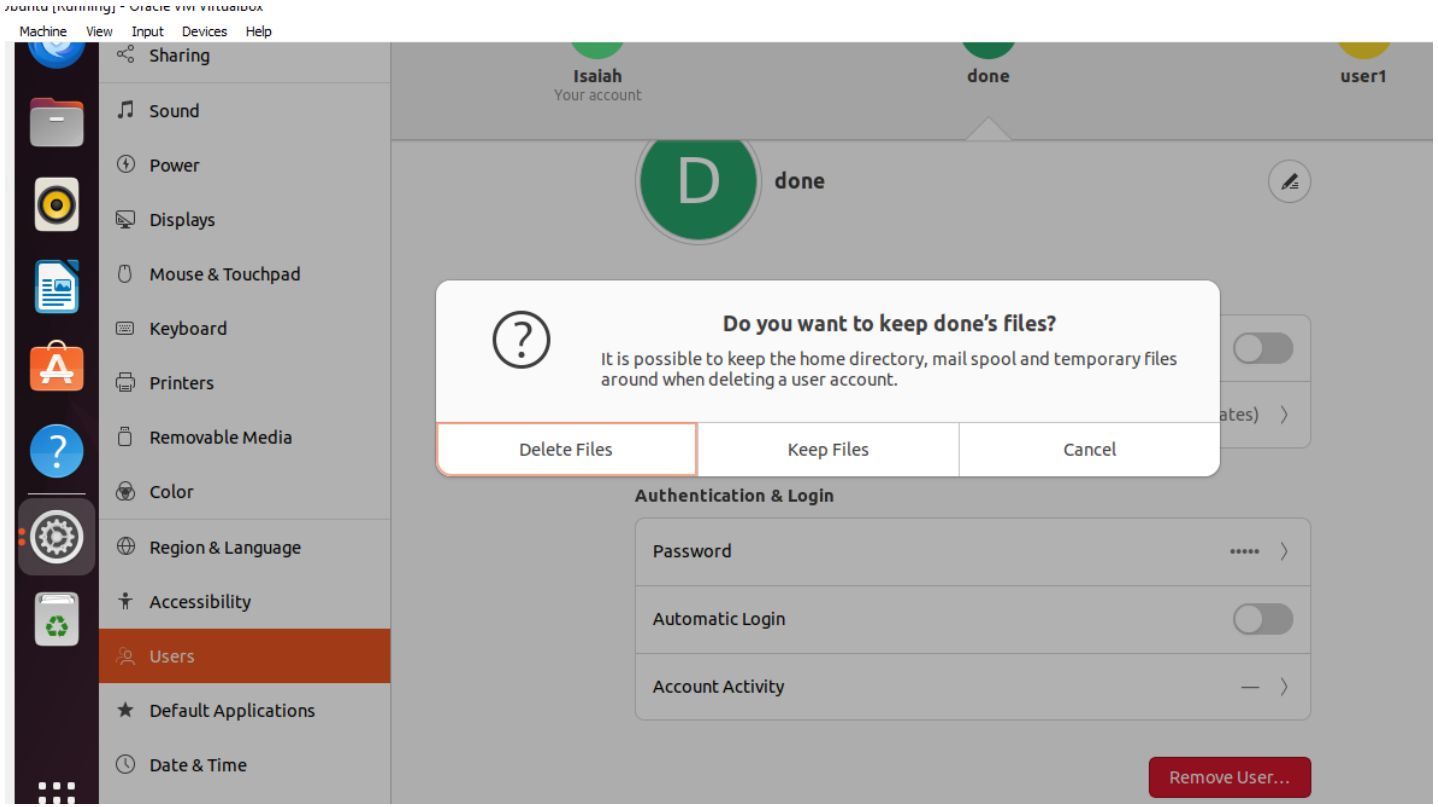


Step 6: Secure Applications & Data

- Uninstall unnecessary software.
- Enable application whitelisting to block unknown apps.
- Back up important files and test restoration.



System Configuration



User access & Control

Create user accounts with limited access:

- I created new users with sudo adduser [username].
- I used sudo usermod -aG [group] [username] to add users to appropriate groups, ensuring they only had access to necessary resources.

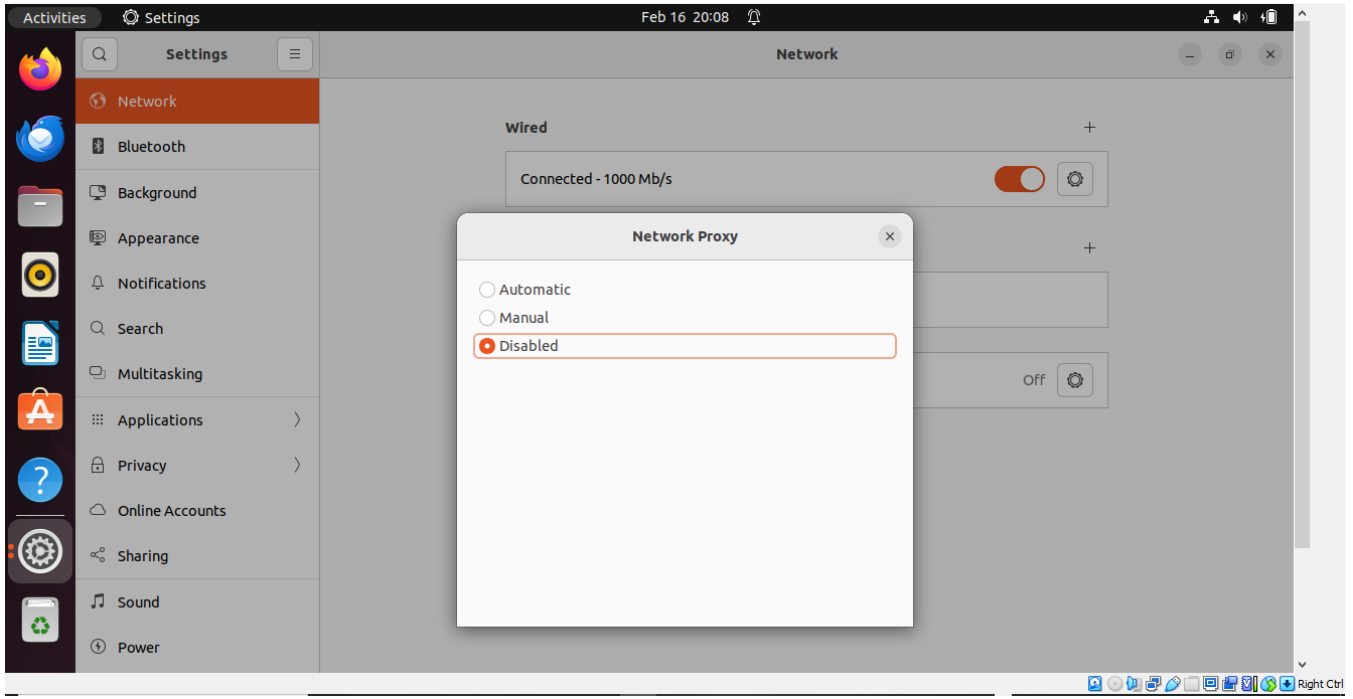
Remove inactive accounts:

- I used lastlog to see when users last logged in.
- For inactive accounts, I used sudo userdel [username] to remove them, reducing potential security threats.

Network Security

Disable unused network services:

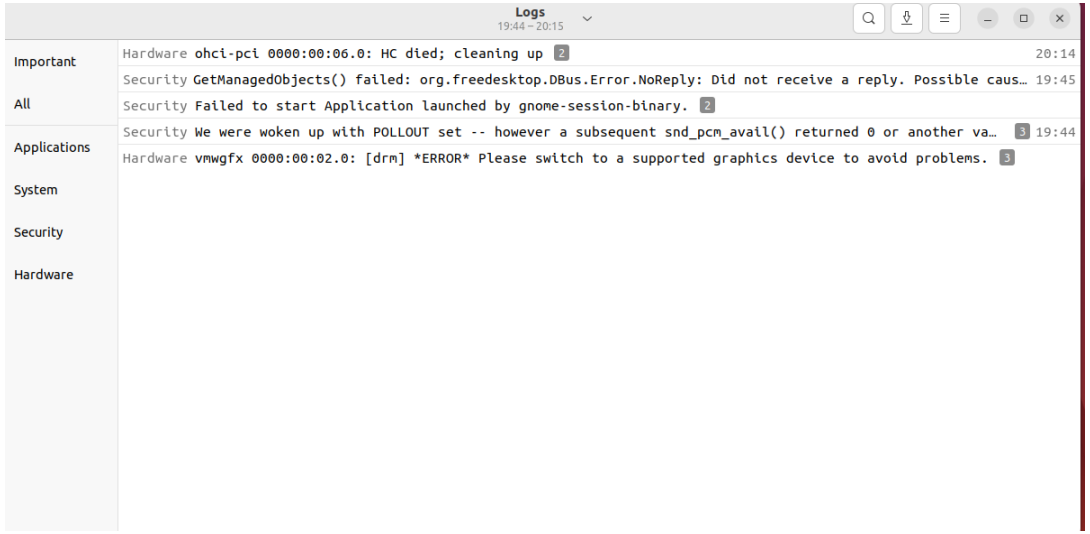
- I navigated to the system's service management interface through the GUI.
- I reviewed the list of running services and disabled any unused network services by unchecking or stopping them



Logging & Monitoring:

Enable system logs:

- I accessed the system's logging settings through the GUI and ensured that logging was enabled and logs were being written to the appropriate files.
- I used the system's log viewer to confirm that activities were being tracked

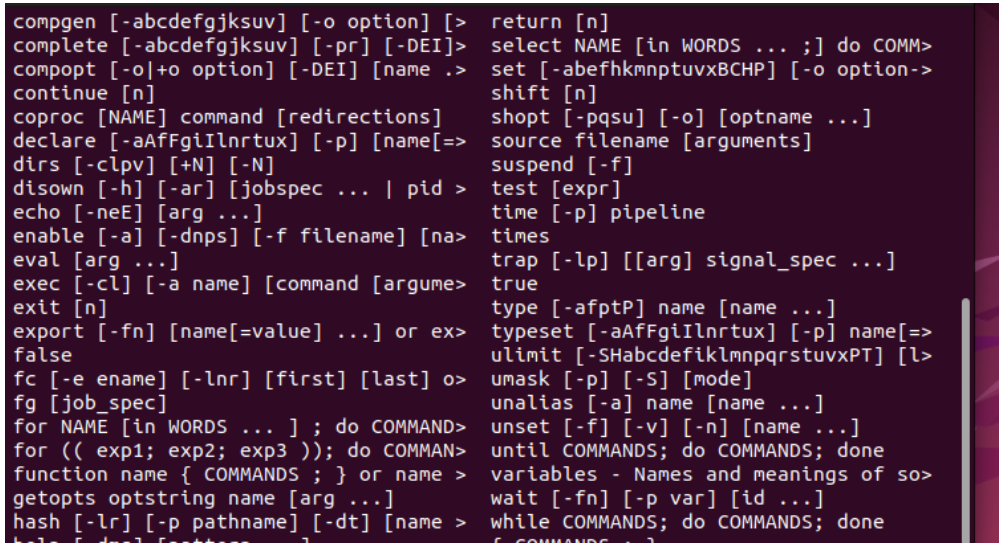


Application Security & Backup

Regularly update installed software:

I used the system's software update tool through the GUI to check for and install updates, ensuring all software was up to date and security gaps were closed.

I configured automatic updates through the system settings to ensure future updates were installed without manual intervention



Assessment and Testing:

Manual Vulnerability Assessment:

1. I manually reviewed the list of installed software and services to identify any outdated or vulnerable components.
2. I checked each service to ensure only necessary ones were running, and I disabled any that were not needed.
3. I reviewed the system's configuration files to check for any misconfigurations or non-compliant settings.

Findings and Observations:

Vulnerability Assessment Results:

- I found that all software was up to date, and no outdated components were present.
- I confirmed that all unnecessary services were disabled, reducing the attack surface

Log Review Results:

- No suspicious activities were detected in the logs.
- All alerts were functioning as expected, with no unusual activities missed.

Documentation and Finalization

Organizing Content:

- I organized the guide into clear sections: Introduction, System Configuration, User & Access Control, Patch & Update Management, Network Security, Logging & Monitoring, Application Security & Backup, Assessment and Testing, and Conclusion
- I took screenshots at key points to visually guide the user through the process, ensuring that each screenshot was labeled.

Conclusion

Hardening an operating system improves security by disabling unnecessary services, using firewalls, strong passwords, and multi-factor authentication, and regularly applying updates. Monitoring through logs and alerts, along with regular assessments, helps identify vulnerabilities. Consistent documentation of practices ensures ongoing protection against threats.