AIR FORCE ASSOCIATION'S

CYBERPATRIOT

THE NATIONAL YOUTH CYBER EDUCATION PROGRAM

# Computer System Security and Maintenance Guide

## Introduction

This document provides a comprehensive guide to address security and maintenance issues on computer systems running different operating systems: Windows Server, Ubuntu, and Windows 10. Each task is accompanied by clear instructions on how to resolve the issue and an explanation of its significance.

---

## Windows Server

### Objective 1: Keep the System Updated and Patched

- Ensure your Ubuntu system is up-to-date with the latest security updates and bug fixes:
    - Run the following commands:

```
sudo apt update

sudo apt upgrade

sudo apt dist-upgrade
```

## Objective 2: Disable Unused or Unnecessary Services

- Identify and disable unnecessary services to reduce the attack surface:
  - List services: `systemctl list-units --type=service --state=active`
  - Disable a service: `sudo systemctl disable <service-name>`

## Objective 3: Implement Firewall Rules

- Configure the Uncomplicated Firewall (UFW) to control incoming and outgoing traffic:
  - Install UFW (if not installed): `sudo apt install ufw`
  - Enable UFW: `sudo ufw enable`
  - Allow specific ports (e.g., SSH): `sudo ufw allow <port>/tcp`

## Objective 4: Regularly Update Software and Applications

- Keep all software up-to-date:
  - For system updates: `sudo apt update && sudo apt upgrade`
  - For third-party software, use the respective package manager or update mechanism (e.g., Snap, Flatpak, etc.).

## Objective 5: Set Strong Password Policies

- Configure password policies for users:
  - Open the password policy file: `sudo nano /etc/security/pwquality.conf`
  - Modify password policy settings as needed.
  - Enforce password policies with PAM: `sudo nano /etc/security/pwquality.conf`

## Objective 6: Monitor and Audit Events

- Implement event monitoring and auditing to detect and respond to security incidents:
  - Configure auditd: `sudo apt install auditd`
  - Enable auditing: `sudo auditctl -e 1`
  - Review audit logs: `sudo ausearch -k <key>`

## Objective 7: Understand and Handle Penalties

- Be aware of specified penalties for non-compliance with security guidelines and ensure compliance.

## Objective 8: Install and Update Antivirus Software

- Install a reputable antivirus solution (e.g., ClamAV):
  - Install ClamAV: `sudo apt install clamav`
  - Update ClamAV definitions: `sudo freshclam`
  - Scan for malware: `sudo clamscan -r /`

## Objective 9: Enable Disk Encryption (LUKS)

- Protect your data by encrypting your disk using LUKS:
  - Install LUKS (if not installed): `sudo apt install cryptsetup`
  - Initialize and encrypt the disk: `sudo cryptsetup luksFormat /dev/sdX`
  - Open and map the encrypted disk: `sudo cryptsetup open --type luks /dev/sdX myencrypteddisk`

## Objective 10: Configure User Account Control (Sudo)

- Secure user privileges by configuring sudo access:
  - Edit sudoers file: `sudo visudo`
  - Add user-specific sudo permissions: `<username> ALL=(ALL:ALL) ALL`

## Objective 11: Implement Regular Data Backups

- Protect your data from loss by scheduling regular backups:
  - Use tools like `rsync`, `Duplicity`, or backup utilities for automated backups.

## Objective 12: Enable AppArmor or SELinux

- Enhance application security with AppArmor or SELinux (if not already enabled):
  - Install AppArmor: `sudo apt install apparmor`
  - Enable AppArmor profiles: `sudo aa-enforce /etc/apparmor.d/*`

## Objective 13: Configure App and Browser Security Settings

- Strengthen security while browsing and using applications by adjusting settings within applications and browsers.

## Objective 14: Customize Firewall Rules (UFW)

- Fine-tune UFW rules for advanced network security:
  - Edit UFW rules: `sudo nano /etc/ufw/*.rules`
  - Add or modify rules as needed.

## Objective 15: Enable Two-Factor Authentication (2FA)

- Add an extra layer of security to user accounts by enabling Two-Factor Authentication (2FA) where available.

## Objective 16: Educate Users

- Train users on security best practices and common threats through security awareness training and information sharing.

## Objective 17: Create a Disaster Recovery Plan

- Prepare for emergencies and data loss scenarios by developing a disaster recovery plan and testing backup restoration procedures.

---

# Ubuntu

## Objective 1: Keep the System Updated and Patched

- Ensure your Ubuntu system is up-to-date with the latest security updates and bug fixes:
    - Run the following commands:

```
sudo apt update

sudo apt upgrade

sudo apt dist-upgrade
```

    -

## Objective 2: Disable Unused or Unnecessary Services

- Identify and disable unnecessary services to reduce the attack surface:
    - List services: `systemctl list-units --type=service --state=active`
    - Disable a service: `sudo systemctl disable <service-name>`

## Objective 3: Implement Firewall Rules

- Configure the Uncomplicated Firewall (UFW) to control incoming and outgoing traffic:
    - Install UFW (if not installed): `sudo apt install ufw`

- Enable UFW: `sudo ufw enable`
- Allow specific ports (e.g., SSH): `sudo ufw allow <port>/tcp`

## Objective 4: Regularly Update Software and Applications

- Keep all software up-to-date:
  - For system updates: `sudo apt update && sudo apt upgrade`
  - For third-party software, use the respective package manager or update mechanism (e.g., Snap, Flatpak, etc.).

## Objective 5: Set Strong Password Policies

- Configure password policies for users:
  - Open the password policy file: `sudo nano /etc/security/pwquality.conf`
  - Modify password policy settings as needed.
  - Enforce password policies with PAM: `sudo nano /etc/security/pwquality.conf`

## Objective 6: Monitor and Audit Events

- Implement event monitoring and auditing to detect and respond to security incidents:
  - Configure auditd: `sudo apt install auditd`
  - Enable auditing: `sudo auditctl -e 1`
  - Review audit logs: `sudo ausearch -k <key>`

## Objective 7: Understand and Handle Penalties

- Be aware of specified penalties for non-compliance with security guidelines and ensure compliance.

## Objective 8: Install and Update Antivirus Software

- Install a reputable antivirus solution (e.g., ClamAV):

- Install ClamAV: `sudo apt install clamav`
- Update ClamAV definitions: `sudo freshclam`
- Scan for malware: `sudo clamscan -r /`

## Objective 9: Enable Disk Encryption (LUKS)

- Protect your data by encrypting your disk using LUKS:
  - Install LUKS (if not installed): `sudo apt install cryptsetup`
  - Initialize and encrypt the disk: `sudo cryptsetup luksFormat /dev/sdX`
  - Open and map the encrypted disk: `sudo cryptsetup open --type luks /dev/sdX myencrypteddisk`

## Objective 10: Configure User Account Control (Sudo)

- Secure user privileges by configuring sudo access:
  - Edit sudoers file: `sudo visudo`
  - Add user-specific sudo permissions: `<username> ALL=(ALL:ALL) ALL`

## Objective 11: Implement Regular Data Backups

- Protect your data from loss by scheduling regular backups:
  - Use tools like `rsync`, `Duplicity`, or backup utilities for automated backups.

## Objective 12: Enable AppArmor or SELinux

- Enhance application security with AppArmor or SELinux (if not already enabled):
  - Install AppArmor: `sudo apt install apparmor`
  - Enable AppArmor profiles: `sudo aa-enforce /etc/apparmor.d/*`

## Objective 13: Configure App and Browser Security Settings

- Strengthen security while browsing and using applications by adjusting settings within applications and browsers.

## Objective 14: Customize Firewall Rules (UFW)

- Fine-tune UFW rules for advanced network security:
  - Edit UFW rules: `sudo nano /etc/ufw/*.rules`
  - Add or modify rules as needed.

## Objective 15: Enable Two-Factor Authentication (2FA)

- Add an extra layer of security to user accounts by enabling Two-Factor Authentication (2FA) where available.

## Objective 16: Educate Users

- Train users on security best practices and common threats through security awareness training and information sharing.

## Objective 17: Create a Disaster Recovery Plan

- Prepare for emergencies and data loss scenarios by developing a disaster recovery plan and testing backup restoration procedures

# Windows 10

Windows 10 Security Checklist

## 1. Updating and Patching the System

- Objective: Ensure your Windows 10 system is up-to-date with the latest security updates and bug fixes.
- How to Achieve:
    - Open "Windows Update" settings: Go to "Settings" > "Update & Security" > "Windows Update."
    - Click "Check for updates" and install any available updates.
- Importance: Neglecting updates may expose your system to known vulnerabilities.

## 2. Disabling Unused or Unnecessary Services

- Objective: Reduce the attack surface by identifying and disabling unnecessary services.
- How to Achieve:
    - Open the "Services" application: Press Win + R, type services.msc, and press Enter.
    - Review the list of services and disable those that are not needed.
    - Set the "Startup type" to "Disabled" for unnecessary services.
- Importance: Failing to disable unnecessary services may expose your system to potential security risks.

## 3. Implementing Firewall Rules

- Objective: Enhance network security by configuring Windows Firewall to control traffic.
- How to Achieve:
    - Open "Windows Security": Go to "Settings" > "Update & Security" > "Windows Security."
    - Click on "Firewall & network protection."
    - Configure inbound and outbound rules as needed to allow or block specific traffic.
- Importance: Not implementing firewall rules may lead to unauthorized access and potential breaches.

## 4. Regularly Updating Software and Applications

- Objective: Keep all software, including third-party applications, up-to-date to mitigate security vulnerabilities.
- How to Achieve:
    - Use "Windows Update" for Windows 10 updates as described in Task 1.
    - Visit the software vendor's website regularly to check for updates and apply them for third-party software.
- Importance: Neglecting software updates may expose your system to known security vulnerabilities.

## 5. Setting Strong Password Policies

- Objective: Enhance user account security by configuring strong password policies.
- How to Achieve:
    - Configure password policies using "Local Security Policy" (secpol.msc).
    - Set password complexity requirements, length, and other policies.
    - Enforce strong password policies on user accounts.
- Importance: Weak password policies may lead to unauthorized access and compromised accounts.

## 6. Regularly Monitoring and Auditing Events

- Objective: Detect and respond to security threats by implementing event monitoring and auditing.
- How to Achieve:
    - Configure security auditing using "Local Security Policy" (secpol.msc).
    - Set up event subscriptions to collect and review security logs.
- Importance: Neglecting event monitoring and auditing may result in undetected security breaches.

## 7. Handling Penalties

- Objective: Be aware of specified penalties for non-compliance with security guidelines.

- How to Achieve: Stay informed about penalties, which may include increased security risks and potential breaches, for failing to comply with security fixes and best practices.

## 8. Installing and Updating Antivirus Software

- Objective: Protect your system from malware and viruses.
- How to Achieve:
    - Install a reputable antivirus software.
    - Regularly update the antivirus definitions.
    - Schedule regular scans.
- Importance: Antivirus software helps detect and remove malicious software.

## 9. Enabling BitLocker or Device Encryption

- Objective: Protect your data in case of theft or loss by encrypting your device.
- How to Achieve:
    - Enable BitLocker (for Pro and Enterprise editions) or Device Encryption (for Home editions).
    - Use a strong, unique encryption key.
- Importance: Encryption safeguards your data from unauthorized access.

## 10. Configuring User Account Control (UAC)

- Objective: Prevent unauthorized changes to your computer by controlling access rights.
- How to Achieve:
    - Adjust UAC settings to an appropriate level.
    - Prompt for administrator approval when needed.
- Importance: UAC helps thwart unauthorized system changes.

## 11. Regular Data Backups

- Objective: Protect your data from loss due to hardware failure, malware, or user error.
- How to Achieve:
    - Schedule regular backups of important data.
    - Store backups in a secure location.
- Importance: Data backups ensure data recovery in case of unforeseen events.

## 12. Enabling Windows Defender

- Objective: Activate Windows Defender for real-time protection against malware.
- How to Achieve:
    - Ensure Windows Defender is enabled.
    - Regularly update its definitions.
- Importance: Windows Defender provides baseline protection against common threats.

## 13. Configuring App and Browser Security Settings

- Objective: Strengthen security while browsing and using applications.
- How to Achieve:
    - Review and adjust security settings in your web browser.
    - Limit permissions for applications.
- Importance: Proper settings reduce exposure to potential threats.

## 14. Configuring Windows Firewall Advanced Settings

- Objective: Fine-tune Windows Firewall for advanced network security.
- How to Achieve:
    - Customize rules for specific applications.
    - Block incoming and outgoing traffic based on need.

- Importance: Advanced firewall settings allow precise control.

## 15. Enabling Two-Factor Authentication (2FA)

- Objective: Add an extra layer of security to your accounts.
- How to Achieve:
    - Enable 2FA on your Microsoft account and other critical accounts.
- Importance: 2FA prevents unauthorized access even if passwords are compromised.

## 16. Educating Users

- Objective: Train users on security best practices and threats.
- How to Achieve:
    - Conduct security awareness training.
    - Share information about common threats.
- Importance: Educated users are less likely to fall victim to social engineering attacks.

## 17. Creating a Disaster Recovery Plan

- Objective: Prepare for emergencies and data loss scenarios.
- How to Achieve:
    - Develop a disaster recovery plan.
    - Test backup restoration procedures.
- Importance: A plan ensures business continuity and data recovery.