SYSTEMS HARDENING

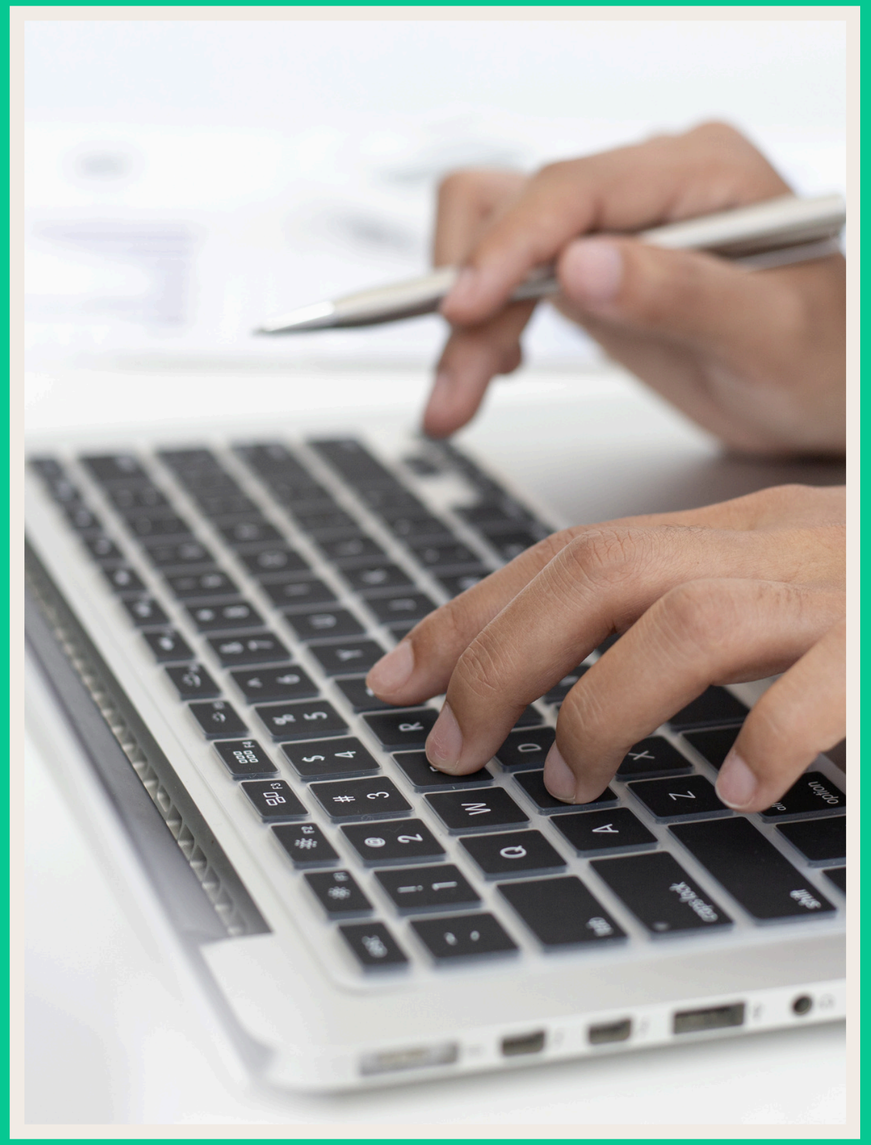
WINDOWS AND LINUX

MAYADA SAAD , MOHAMED EL SAYED , JOVAN

INTRODUCTION TO OS HARDENING

- Definition: The process of securing an operating system by reducing its surface of vulnerability.
- Importance: Protects against unauthorized access, malware, and data breaches.

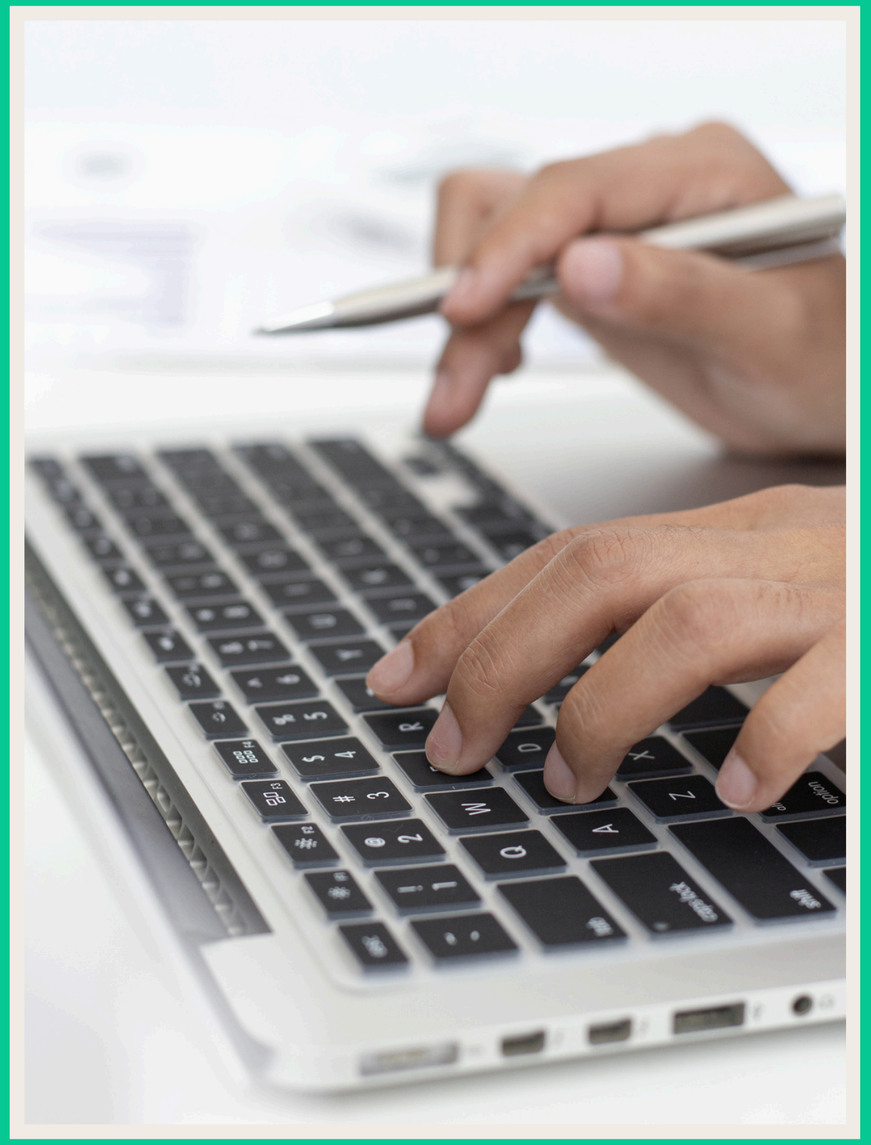
KEY PRINCIPLES OF OS HARDENING



Key Principles of OS Hardening

- Minimize Attack Surface
- Implement Least Privilege
- Regular Updates and Patch Management
- Use of Security Tools and Monitoring

HARDENING WINDOWS SYSTEMS



HARDENING WINDOWS SYSTEMS

1. USER ACCOUNT CONTROL (UAC)

- ENSURE UAC IS ENABLED TO PREVENT UNAUTHORIZED CHANGES.

2. WINDOWS DEFENDER AND ANTIVIRUS

- USE BUILT-IN SECURITY TOOLS AND KEEP THEM UPDATED.

3. WINDOWS FIREWALL

CONFIGURE AND ENABLE WINDOWS FIREWALL SETTINGS.

4. SECURITY POLICIES

- USE LOCAL SECURITY POLICY TO ENFORCE SECURITY SETTINGS.

Hardening Active Directory (AD)

Hardening Active Directory (AD)

1. Secure Administrative Accounts

- **Use strong passwords and MFA.**

2. Limit Permissions

- **Follow the principle of least privilege.**

3. Group Policy Objects (GPOs)

- **Enforce security settings and restrictions.**

4. Audit and Monitoring

- **Enable logging for user actions and changes.**

Hardening Linux Systems

Hardening Linux Systems

1. User Account Management

- **Disable unused accounts; enforce strong password policies.**

2. File Permissions

- **Set correct permissions and use Access Control Lists (ACLs).**

3. Regular Updates

- **Use package managers to keep software up to date.**

4. Firewalls and SELinux/AppArmor

- **Configure firewalls and use security modules for additional protection.**

Common Tools for OS Hardening

- Linux:
  - Lynis, OpenVAS, and rkhunter.
- Windows:
  - Microsoft Security Compliance Toolkit, Windows Security Baselines.
- AD:
  - PowerShell scripts, Group Policy Management Console (GPMC).

BEST PRACTICES FOR OS HARDENING

- REGULAR SECURITY AUDITS
- BACKUP CONFIGURATIONS
- USER EDUCATION AND AWARENESS
- INCIDENT RESPONSE PLANNING

Q&A