2. **Operating Systems (OS)** → Windows, Linux, and MacOS security

13 March 2025 17:07

1. Introduction to OS Security

- **Key Security Principles:**
  - **Confidentiality:** Ensure that only authorized users can access sensitive data.
  - **Integrity:** Keep data accurate and unaltered by unauthorized users.
  - **Availability:** Ensure systems and data are accessible when needed.
- **OS Differences:**
  - **Windows:** Uses NTFS permissions, Active Directory for centralized management, and built-in tools like Windows Defender and BitLocker.
  - **Linux:** Leverages POSIX permissions, sudo for privilege management, and tools like SELinux/AppArmor plus syslog/auditd for logging.
  - **macOS:** Combines UNIX-like security (POSIX permissions, ACLs) with proprietary features such as FileVault, Gatekeeper, and a unified logging system .

2. System Hardening

Definition:

OS hardening is the process of securing an operating system by reducing its attack surface—removing unnecessary services, applying patches, configuring security settings, and enforcing strict policies.

Windows Hardening

- **Patch Management:**
  - Ensure Windows Update is enabled and configured to install patches automatically.
- **Built-In Security Features:**
  - Enable BitLocker for disk encryption.
  - Use Windows Defender Antivirus (or your chosen EDR) for real-time threat protection.
  - Configure User Account Control (UAC) to always prompt for administrative changes.

Additional Steps:

- Disable or remove unused services and features.
- Use AppLocker or Windows Defender Application Control (WDAC) to restrict executable files.

#BitLocker Enabling > open "Manage BitLocker" from the Control Panel or search box, select the drive to encrypt, and click "Turn on BitLocker," then follow the prompts to choose an unlock method and back up the recovery key.
By default, it uses the Advanced Encryption Standard (AES) algorithm in cipher block chaining (CBC) or "xor-encrypt-xor"(XEX)-based tweaked codebook mode with ciphertext stealing" XTS mode with a 128-bit or 256bit key.

#EDR- Endpoint Detection and Response, is a cybersecurity technology that focuses on identifying and responding to threats on endpoint devices like laptops and desktops,providing real-time monitoring and analysis to detect and mitigate potential security incidents.
EDR solutions continuously monitor endpoint activities , collecting data on processes, file changes, network connections, and system events.
##Open-Source EDR Tools - OSSEC, TheHive Project,osQuery,Nessus Vulnerability Scanner,SNORT,Cuckoo Sandbox.

#UAC - To configure User Account Control (UAC), open Control Panel, navigate to "User Accounts", then "User Accounts (Classic View)", and finally "Change User Account Control settings". Adjust the slider to your desired notification level (e.g., "Always Notify", "Notify me only when programs try to make changes to my computer", or "Never Notify") and click "OK".

Linux Hardening

- **System Updates:**
  - Use your package manager (e.g., apt, yum) to keep the system and software up to date.
- **Service and SSH Configuration:**
  - Disable root SSH login; enforce key-based authentication.
  - Change the default SSH port (optional) to reduce automated attack attempts.
- **Security Frameworks:**
  - Enable and configure SELinux or AppArmor for mandatory access control.
- **Firewall Configuration:**
  - Use iptables, nftables, or firewalld to restrict network access.

3. User Management

Key Concepts:

Implement the principle of least privilege—only give users the access they need. Regularly review accounts, enforce strong password policies, and segregate administrative from standard user accounts.

Windows

- **Local & Domain Accounts:**
  - Use Active Directory to centrally manage user accounts and enforce password complexity and expiration policies.
- **Access Controls:**
  - Configure NTFS permissions and use Group Policy Objects (GPOs) to manage access.
- **Monitoring:**
  - Enable auditing of user logon events via the Event Viewer.

Linux

- **User and Group Management:**
  - Use commands like useradd, usermod, and groupadd to manage accounts.
- **Privilege Elevation:**
  - Configure sudo to allow limited root access.

- **Password Policies:**
  - Enforce strong password rules (e.g., via PAM) and regularly review /etc/shadow for account anomalies.

4. Logging and Auditing
Purpose:
Logging is essential for detecting, analyzing, and responding to security incidents.
Windows Logging
- **Event Viewer:**
  - Review security logs for logon failures, system changes, and audit events.
- **Advanced Audit Policies:**
  - Configure Group Policy to increase the granularity of log events (e.g., object access, process tracking).

Linux Logging
- **Syslog and Journald:**
  - Use syslog (or rsyslog) and systemd-journald for centralized logging.
- **Auditd:**
  - Configure the Linux Audit daemon to monitor system calls, file accesses, and configuration changes.

5. File Permissions and Access Control
Understanding permissions is key to preventing unauthorized access to files and directories.
Windows
- **NTFS Permissions & ACLs:**
  - Learn to manage Access Control Lists (ACLs) using File Explorer or command-line tools like icacls.
- **Inheritance & Special Permissions:**
  - Understand how permissions cascade through directory structures and how to set exceptions.

Linux and macOS
- **POSIX Permissions:**
  - Use chmod and chown to set file and directory permissions.
- **Advanced ACLs:**
  - On systems that support it, use ACL tools (getfacl/setfacl) to grant fine-grained access.
- **Special Permissions:**
  - Understand and apply special bits (setuid, setgid, sticky bit) where necessary for security.

- **Create a Lab Environment:**
  Set up virtual machines for each OS to practice hands-on configuration and security checks.
- **Develop a Checklist:**
  Use or adapt existing checklists (e.g., from ConnectWise, CalCom Software, or CIS) to audit your configurations.
- **Continuous Learning:**
  Stay updated with the latest security best practices, join forums or communities (e.g., SANS InfoSec forums), and subscribe to cybersecurity newsletters.