🔐 Operating Systems & File Systems in Cybersecurity

1. Operating Systems (OS) in Cybersecurity

An Operating System is the backbone of any computing device. From a cybersecurity perspective, the OS plays a critical role in security, attack surfaces, and defenses.

🔷 Common Operating Systems in Cybersecurity

- **Windows OS**
  - **Most targeted due to widespread use.**
  - **Vulnerabilities: Registry attacks, DLL injection, malware.**
  - **Security features: Windows Defender, BitLocker, Active Directory, UAC.**
- **Linux OS**
  - **Preferred by security professionals & hackers (Kali Linux, Parrot OS).**
  - **Open-source, customizable, command-line tools for penetration testing.**
  - **Strong file permissions (Read, Write, Execute).**
- **macOS**
  - **Based on UNIX, relatively secure.**
  - **Still vulnerable to phishing, trojans, and privilege escalation.**
- **Mobile OS**
  - **Android: Open, customizable, but highly vulnerable to malware.**
  - **iOS: Closed ecosystem, stronger app store security, but jailbreak exploits exist.**

🔷 OS Security Features

- **Authentication (username, password, biometrics, MFA).**
- **Access Control (ACLs, file permissions).**
- **Encryption (BitLocker, LUKS).**
- **Logging & Monitoring (Event Viewer, Syslog).**
- **Patch Management (security updates).**

🔷 **OS Security Threats**

- **Privilege Escalation**
- **Rootkits & Bootkits**
- **Malware (worms, ransomware)**
- **Zero-day exploits**

---

2. File Systems (FS) in Cybersecurity

A File System defines how data is stored, organized, and retrieved on storage devices. Attackers often target FS to steal, hide, or manipulate data.

🔷 **Common File Systems**

- **FAT32 (Windows) → Legacy, lacks strong security.**
- **NTFS (Windows) → Supports encryption, permissions, journaling.**
- **ext4 (Linux) → Widely used, supports journaling, access controls.**
- **HFS+ / APFS (macOS) → Apple's file systems with encryption support.**

🔷 **Security Features of File Systems**

- **Permissions & Ownership**
  - **Read (R), Write (W), Execute (X).**
  - **User, Group, Others in Linux.**
- **Encryption**
  - **NTFS → Encrypting File System (EFS).**
  - **Linux → eCryptfs, LUKS.**
  - **macOS → FileVault.**
- **Journaling**
  - **Helps recover from crashes by logging changes.**
- **Access Control Lists (ACLs)**
  - **Fine-grained access control.**

🔷 **File System Attacks**

- **Data Exfiltration → stealing files.**
- **Metadata Manipulation → altering timestamps, ownership.**
- **Steganography → hiding malicious code in files.**
- **Fileless Malware → attacks run in memory without touching disk.**
- **Ransomware → encrypts files, demands payment.**

---

3. Cybersecurity Use-Cases

- **Digital Forensics → Investigating deleted files, hidden partitions, file timestamps.**
- **Penetration Testing → Exploiting OS vulnerabilities, privilege escalation.**
- **System Hardening → Securing OS & FS via patches, firewalls, least privilege.**
- **Incident Response → Checking logs, monitoring FS integrity.**