# Notes for ECS CW – Units I to V

**UNIT – I: Windows Security**

- Windows Security Infrastructure refers to the combination of tools, configurations, and policies used to protect Windows systems from threats such as malware, unauthorized access, data breaches, and system vulnerabilities.

**Three Classes of Operating Systems:**

1. Client OS (Windows 7/8/10/11): Designed for desktops and personal machines.

2. Server OS (Windows Server 2012/2016/2019/2022): Used in organizations to provide centralized services.

3. Embedded OS (Windows Embedded, Windows IoT): Used in ATMs, kiosks, industrial devices.

- Service Packs & Hotfixes: Service Packs bundle large updates; Hotfixes resolve specific issues quickly.
- Patch Installation & Automatic Updates ensure security fixes are regularly applied.
- Windows Server Update Services (WSUS) helps network administrators deploy patches centrally.
- Windows Backup, System Restore, and Device Driver Rollback are tools for recovery and stability.
- Windows Access Controls include NTFS permissions, Shared Folder permissions, Registry permissions, and Active Directory permissions.
- BitLocker provides full disk encryption for data protection.
- Microsoft Baseline Security Analyzer (MBSA) scans systems for missing patches and security misconfigurations.

**UNIT – II: Windows Security Policy**

- Windows Security Policy defines how security settings and restrictions are configured and enforced in Windows environments.
- Security Templates are predefined configuration files containing password policies, user rights, audit settings, etc.
- Security Configuration and Analysis Snap-in allows comparison and enforcement of security templates.
- Local Group Policy Objects (LGPO) apply to single systems; Domain Group Policy Objects (DGPO) apply in Active Directory.
- Administrative Users have elevated privileges and must be controlled.
- AppLocker is used to allow or block the execution of applications, scripts, and installers.
- User Account Control (UAC) prevents unauthorized changes by prompting for confirmation.
- Important GPO settings include Password Policy, Account Lockout Policy, Security Options, IE Security, and Administrative Templates.

- Secedit is a command-line tool used to apply and analyze security configurations.
- Windows Network Services can be secured using firewall rules, authentication mechanisms, and policy enforcement.

**UNIT – III: Linux Security Hardening**

- Linux Security Hardening involves reducing the attack surface and securing services, packages, kernel, ports, and logs.
- Starting Services at Boot: Using systemctl enable/disable to manage services.
- Package Control: Secure installations using apt, yum, dnf; remove outdated packages and verify signatures.
- Kernel Security: Apply kernel updates, configure sysctl, disable unused features.
- Port Control: Use UFW, firewalld, or iptables to allow or block network ports.
- Monitoring and Attack Detection: Use syslog, syslog-ng, journalctl, and auditd.
- Log Parsing Commands: grep, awk, sed, cut used for analyzing logs such as /var/log/auth.log.
- SIEM tools (e.g., Splunk, AlienVault) aggregate logs and detect suspicious activity.
- Security Utilities: Lynis (hardening auditor), chkrootkit (rootkit detection), Fail2ban (blocks brute-force attempts).
- Host-based firewalls and hardening scripts help secure Linux systems.
- Package Management Strategies ensure secure and stable system updates.

**UNIT – IV: Introduction to Cyber Warfare**

- Cyber Warfare refers to the use of digital technologies and attacks by nation-states to disrupt, damage, or infiltrate another country's systems.
- Definition: Use of cyber attacks (malware, DDoS, espionage) for military or political advantage.
- Tactical Reasons: Disable communication, disrupt radar, interfere with battlefield operations.
- Operational Reasons: Long-term destabilization, economic disruption, intelligence theft, psychological manipulation.
- Cyber Strategy includes defense, offense, intelligence gathering, and incident response.
- Cyber Power is a nation’s ability to use cyberspace technologies to its advantage.
- Cyber Arms Control refers to treaties or efforts to limit cyber weapon development.

**UNIT – V: Information Warfare & Operations**

- Information Warfare involves using information to gain strategic advantage over an opponent.
- Information Assurance ensures confidentiality, integrity, and availability of data.
- Information Operations include cyber operations, psychological influence, and electronic warfare.
- Information Superiority ensures having more accurate information than the enemy.
- Network Centric Operations rely on interconnected digital communication systems.
- Psychological Operations and Psychological Warfare aim to manipulate beliefs, emotions, and morale.