Windows and Linux Security practical for ECS CW

Practical 1: Process Hacker

Objective: Inspect and manage Windows processes using Process Hacker

Prerequisites: Windows 10/11 with Process Hacker installed. Run as Administrator.

Steps & Output:

1. Launch Process Hacker.
2. Sort processes by CPU and memory.
3. Inspect threads/handles.
4. Terminate a safe process (e.g., Notepad).
5. Verify removal.

Expected Output: Process list and terminated entry disappears.

Practical 2: System Restore & Backup

Objective: Create and restore a Windows System Restore Point

Prerequisites: Windows with Restore enabled.

Steps & Output:

1. Run PowerShell as Admin.
2. Create restore point:
Checkpoint-Computer -Description "LabRestorePoint" -RestorePointType MODIFY_SETTINGS
3. Verify: vssadmin list shadows.
4. Perform restore via Control Panel → Recovery.

Expected Output: Restore point creation and restoration confirmed.

Practical 3: Patch Management

Objective: Check Windows Update and apply patches

Prerequisites: Windows machine with internet access.

Steps & Output:

1. Open PowerShell.
2. Install module: Install-Module -Name PSWindowsUpdate -Force.
3. Run Get-WUList and Install-WindowsUpdate -AcceptAll -AutoReboot.

Expected Output: Updates installed successfully.

Practical 4: NTFS & Share Permissions

Objective: Configure NTFS and Shared Folder permissions

Prerequisites: Windows VM with two local users.

Steps & Output:

1. Create C:\LabShare folder.
2. Share and assign permissions.
3. Use icacls to verify access.
4. Test read/write access from user account.

Expected Output: Access success/failure according to permissions.

Practical 5: BitLocker Encryption

Objective: Enable BitLocker Drive Encryption

Prerequisites: Windows Pro/Enterprise, TPM or password protector.

Steps & Output:

1. Run Enable-BitLocker -MountPoint E: -PasswordProtector.
2. Backup recovery key.
3. Verify: Get-BitLockerVolume.

Expected Output: Drive shows 'FullyEncrypted'. Key saved.

Practical 6: MBSA Scan

Objective: Run Microsoft Baseline Security Analyzer (outdated tool use in sandbox envirnment)

Prerequisites: Windows with MBSA or SCT installed.

Steps & Output:

1. Launch MBSA.
2. Scan local computer.
3. Review missing updates in HTML report.

Expected Output: MBSA report listing vulnerabilities.

Practical 7: Security Policy with Secedit

Objective: Apply Windows Security Template using Secedit

Prerequisites: Windows Admin rights.

Steps & Output:

1. Create template INF file.
2. Apply: secedit /configure /db C:\Lab\Lab.sdb /cfg C:\Lab\LabTemplate.inf.
3. Verify: gpresult /r.

Expected Output: Policies applied and verified.

Practical 8: AppLocker Rules

Objective: Configure and enforce AppLocker rules

Prerequisites: Windows Enterprise with gpedit.msc.

Steps & Output:

1. Start AppIDSvc service.
2. Create deny rule for specific EXE.
3. Enforce via gpedit.msc.
4. Attempt execution.

Expected Output: Application blocked. Event ID 8004 logged.

Practical 9: Secure SMB Services

Objective: Disable SMBv1 and audit SMB access

Prerequisites: Two Windows VMs.

Steps & Output:

1. Disable SMBv1: Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol.
2. Enable SMB signing.
3. Audit File Share access.

Expected Output: SMBv1 disabled, access logged.

Practical 10: Linux Service Hardening

Objective: Control Linux services at boot using systemd

Prerequisites: Linux (Ubuntu/CentOS).

Steps & Output:

1. List services: systemctl list-unit-files.
2. Disable unnecessary services.
3. Enable SSH.

Expected Output: Service states updated correctly.

Practical 11: Linux Log Monitoring

Objective: Parse and monitor logs for failed SSH logins

Prerequisites: Linux with syslog and auditd.

Steps & Output:

1. grep 'Failed password' /var/log/auth.log.
2. Count IPs with awk.
3. Monitor file with auditctl.

Expected Output: Failed login list and audit records displayed.

Practical 12: Linux Hardening

Objective: Apply kernel, firewall, and integrity check hardening

Prerequisites: Linux with sudo privileges.

Steps & Output:

1. Edit sysctl.conf with security parameters.
2. Configure ufw rules.
3. Install and initialize AIDE.

Expected Output: Secure sysctl, ufw active, AIDE check passed.