Unit-wise Practical with Step-by-Step Solutions
Windows & Kali Linux Security

Note: this practical is for example and references; these steps might also have errors which you have to solve

UNIT – I: **WINDOWS SECURITY**

Practical 1: **Explore Windows OS Classes**

Steps:

1. Press Win + R → type “msinfo32”.
2. Check: System Type, Domain Role.
3. Open Settings → System → About.

Practical 2: **Use Process Hacker**

Steps:

1. Install Process Hacker.
2. Run as Administrator.
3. Analyze processes, services, signatures.

Practical 3: **Check & Install Windows Updates**

Steps:

1. Run: systeminfo | findstr /C:"KB".
2. Open Windows Update → Check for updates.

Practical 4: **Email Security Bulletins**

Steps:

1. Visit Microsoft Security Response Center.
2. Search vulnerabilities.

Practical 5: **Automatic Updates**

Steps:

1. Open Windows Update.
2. Enable Automatic Updates.

Practical 6: **WSUS Overview**

Steps:

1. Install WSUS role.
2. Sync updates.
3. Approve updates.

Practical 7**: Backup & Restore**

Steps:

1. Control Panel → Backup and Restore.
2. Run backup.
3. Use rstrui for system restore.

Practical 8: **Driver Rollback**

Steps:

1. Device Manager → Properties → Roll Back Driver.

Practical 9: **NTFS Permissions**

Steps:

1. Properties → Security → Edit permissions.

Practical 10: **Shared Folder Permissions**

Steps:

1. Right-click → Sharing → Advanced Sharing.

Practical 11: **Registry Permissions**

Steps:

1. regedit → Permissions.

Practical 12**: Active Directory Permissions**

Steps:

1. ADUC → Delegate Control.

Practical 13: **BitLocker**

Steps:

1. Manage BitLocker → Turn on → Save recovery key.

Practical 14: **MBSA**

Steps:

1. Install MBSA → Run scan → Study results.

UNIT – II: **WINDOWS SECURITY POLICY**

Practical 1: **Security Templates**

Steps:

1. secpol.msc → Security Templates → Apply using secedit.

Practical 2: **SCA Snap-in**

Steps:

1. mmc → Add Security Configuration and Analysis.
2. Import template → Analyze.

Practical 3: **LGPO**

Steps:

1. gpedit.msc → Configure Password, Lockout Policy.

Practical 4**: Domain GPO**

Steps:

1. GPMC → Create GPO → Enforce.

Practical 5: **AppLocker**

Steps:

1. Create Executable/Script rules. Or use any AppLocker

Practical 6: **UAC**

Steps:

1. Search UAC → Adjust.

Practical 7: **Secedit**

Commands:

```
secedit /analyze /db secdb.sdb
secedit /configure /db secdb.sdb /cfg securews.inf
```

Practical 8: **Secure Windows Network Services**

Steps:

1. Disable unused services; configure firewall.

UNIT – III: **LINUX SECURITY HARDENING**

Practical 1**: Manage Services**

```
systemctl status ssh
systemctl enable ssh
systemctl disable telnet
```

Practical 2: **Package Control**

```
sudo apt update && sudo apt upgrade
```

Practical 3: **Kernel Security**

```
sysctl -a
sudo sysctl -w net.ipv4.ip_forward=0
```

Practical 4: **Port Control**

```
sudo ss -tulnp
sudo ufw allow 22
sudo ufw deny 23
```

Practical 5: **Logs**

```
cat /var/log/syslog
```

```
grep "error" /var/log/syslog
```

Practical 6: **Log Parsing**
grep, sed, awk, cut examples.

Practical 7: **Log Aggregation**
Use SIEM (conceptual).

Practical 8: **Integrity Checker**

```
sudo apt install aide
sudo aideinit
sudo aide --check
```

Practical 9: **Firewall**

```
sudo iptables -L
```

Practical 10: **Hardening Script**

```
#!/bin/bash
Who (create your own)
```

UNIT – IV: **INTRODUCTION TO CYBER WARFARE**
Practical 1: Case Study Analysis
Practical 2: Cyber Strategy Mapping

UNIT – V**: INFORMATION WARFARE**
Case studies