



🎓 Task 2 Report – Network Security & Scanning

Submitted By : Pritish Borkar

Internship ID : APSPL2518121

Department : Cybersecurity

Organization : ApexPlanet software Pvt.Ltd

Co-ordinator : Kundan Kumar

Date of Submission : October 17, 2025

1. Objective:

The objective of Task 2 was to understand and perform **network reconnaissance, scanning, vulnerability assessment, and basic firewall configuration** in a controlled cybersecurity lab environment.

The task focused on identifying open ports, running services, and vulnerabilities within the target machine (Metasploitable2) using Kali Linux tools and techniques.

2. Network Configuration

| Component | Details |
|--------------------|--|
| Attacker Machine: | Kali Linux |
| Target Machine: | Metasploitable2 |
| Kali IP Address: | 192.168.56.101 |
| Target IP Address: | 192.168.56.102 |
| Network Type: | Host-Only Adapter (192.168.56.0/24) |

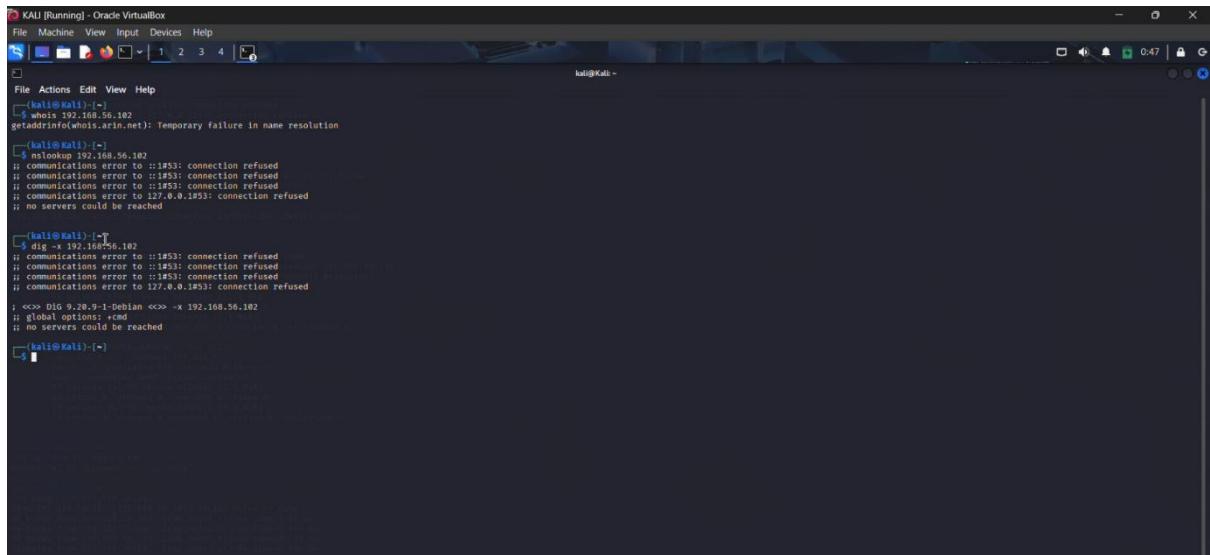
3. Step 1 – Reconnaissance

A. Passive Reconnaissance

Commands used:

- whois 192.168.56.102
- nslookup 192.168.56.102
- dig -x 192.168.56.102

- Whois and DNS lookups failed as expected since the IP address belongs to a **private local network**.
- Findings documented to explain private IP behavior.



```
[kali㉿kali)-[~]
$ whois 192.168.56.102
getaddrinfo(whois.arin.net): Temporary failure in name resolution

[kali㉿kali)-[~]
$ nslookup 192.168.56.102
;> communications error to ::1#53: connection refused
;> communications error to ::1#53: connection refused
;> communications error to ::1#53: connection refused
;> communications error to 127.0.0.1#53: connection refused
; no servers could be reached

[kali㉿kali)-[~]
$ dig +T 192.168.56.102
; communications error to ::1#53: connection refused
; communications error to ::1#53: connection refused
; communications error to ::1#53: connection refused
; communications error to 127.0.0.1#53: connection refused
; no servers could be reached

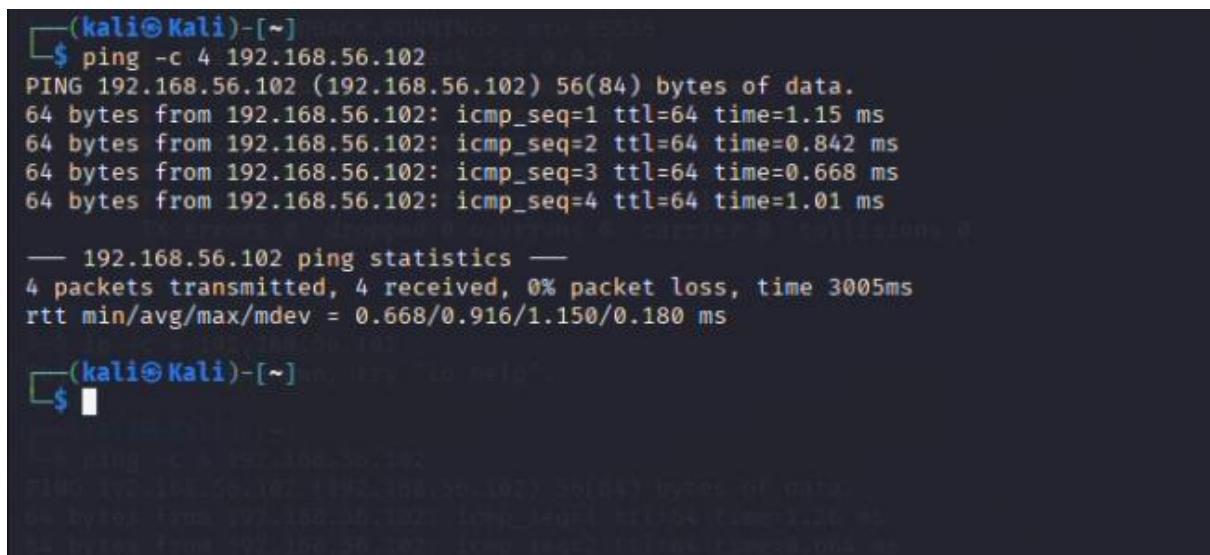
[kali㉿kali)-[~]
```

B. Active Reconnaissance

1. Ping Sweep

- ping -c 4 192.168.56.102
- sudo nmap -sn 192.168.56.0/24

Result: Metasploitable2 was reachable, confirming connectivity.



```
[kali㉿kali)-[~]
$ ping -c 4 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.15 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.842 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.668 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.01 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.668/0.916/1.150/0.180 ms

[kali㉿kali)-[~]
```

```
(kali㉿Kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:48 IST
Nmap scan report for 192.168.56.1
Host is up (0.00052s latency).
MAC Address: 0A:00:27:00:00:0B (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00075s latency).
MAC Address: 08:00:27:64:B1:2B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00056s latency).
MAC Address: 08:00:27:87:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.82 seconds
(kali㉿Kali)-[~]
└─$
```

2. Banner Grabbing (Manual)

- nc -v 192.168.56.102 21 # FTP
- nc -v 192.168.56.102 22 # SSH
- nc -v 192.168.56.102 23 # Telnet
- curl -I <http://192.168.56.102>

| Port | Service | Banner | Finding |
|------|---------|-------------------------------|-------------------------------------|
| 21 | FTP | vsFTPD 2.3.4 | Vulnerable backdoor (CVE-2011-2523) |
| 22 | SSH | OpenSSH 4.7p1 Debian-8ubuntu1 | Outdated version |
| 23 | Telnet | Plain-text connection | Insecure protocol |
| 80 | HTTP | Apache 2.2.8 (Ubuntu) | Vulnerable web server |

```
(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 21
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 21 (ftp) open
220 (vsFTPD 2.3.4)
^C
```

```
(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 21
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 21 (ftp) open
220 (vsFTPD 2.3.4)
^C
```

```
(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 22
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
```

```
[kali㉿Kali)-[~] $ nc -v 192.168.56.102 23  
192.168.56.102: inverse host lookup failed: Host name lookup failure  
(UNKNOWN) [192.168.56.102] 23 (telnet) open  
***|*** ***#*#*
```

```
(kali㉿Kali)-[~]
$ curl -I http://192.168.56.102
HTTP/1.1 200 OK
Date: Tue, 16 Sep 2025 20:56:51 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

4. Step 2 – Port & Service Scanning

1. Basic TCP SYN Scan

➤ sudo nmap -sS 192.168.56.102

Result: Multiple ports found open including FTP, SSH, Telnet, HTTP, SMB, and MySQL.

```
(kali㉿Kali)-[~]
$ sudo nmap -sS 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:52 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00032s 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  tftp
514/tcp   open  shell
1099/tcp  open  smrregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-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:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

2. Service Version & OS Detection

- nmap -sV 192.168.56.102
- sudo nmap -O 192.168.56.102

Result: Target OS detected as **Linux 2.6.X (Ubuntu-based)**.

```
(kali㉿Kali)-[~]
$ nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:55 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00063s 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-vm  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:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

```
(kali㉿Kali)-[~]
└─$ sudo nmap -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:56 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00097s latency).
Not shown: 916 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
8080/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  iced-teal
1009/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2111/tcp  open  cccproxy-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  httpd-ssl
MAC Address: 08:00:27:B7:46:53 (PC Systemtechnik/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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

3. Comprehensive All-Port Scan

➤ sudo nmap -sS -sV -O -A -p- -oN nmap_full_report.txt 192.168.56.102

Result: Saved full scan report for documentation.

```
(kali㉿Kali)-[~]
└─$ sudo nmap -sS -sV -O -A -p- -oN nmap_complete_scan 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 01:00 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
[...]
```

```
vnc-info:
| Protocol version: 3.3
| Security types:
|   VNC Authentication (2)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc      UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
[...]
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  drb     Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbs)
37376/tcp open  status   1 (RPC #100024)
39433/tcp open  mountd  1-3 (RPC #100005)
44429/tcp open  java-rmi  GNU Classpath grmiregistry
55930/tcp open  nlockmgr  1-4 (RPC #100021)
MAC Address: 08:00:27:B7:46:53 (PC Systemtechnik/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
Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -24d2h24m25s, deviation: 2h00m0s, median: -24d22h24m25s
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-09-16T17:08:07-04:00

TRACEROUTE
HOP RTT      ADDRESS
1  0.82 ms  192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.35 seconds
```

4. Vulnerability Script Scan

➤ sudo nmap --script vuln 192.168.56.102

Used Nmap NSE scripts to detect vulnerabilities directly.

```
(kali㉿kali)-[~]
$ sudo nmap --script vuln 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 01:03 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
```

```
httponly flag not set
/admin/adminLogin.jsp: JSESSIONID: httponly flag not set
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: JSESSIONID: httponly flag not set
/admin/includes/FCKeditor/editor/filemanager/upload/test.html: JSESSIONID: httponly flag not set
/admin/jscript/upload.html: JSESSIONID: httponly flag not set
/admin/enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/admin/login.html: Possible admin folder
/admin/admin.html: Possible admin folder
/admin/account.html: Possible admin folder
/admin/admin_login.html: Possible admin folder
/admin/home.html: Possible admin folder
/admin/admin-login.html: Possible admin folder
/admin/adminLogin.html: Possible admin folder
/admin/controlpanel.html: Possible admin folder
/admin/cp.html: Possible admin folder
/admin/index.jsp: Possible admin folder
/admin/login.jsp: Possible admin folder
/admin/admin.jsp: Possible admin folder
/admin/home.jsp: Possible admin folder
/admin/controlpanel.jsp: Possible admin folder
/admin/admin-login.jsp: Possible admin folder
/admin/adminLogin.jsp: Possible admin folder
/admin/html/upload: Apache Tomcat (401 Unauthorized)
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
/admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
/admin/jscript/upload.html: Lizard Cart/Remote File upload
/_webdav/: Potentially interesting folder
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 320.45 seconds
```

5. Step 3 – Vulnerability Scanning

Tool Used: **Nmap NSE** (Nmap Scripting Engine)

Due to limited internet access on Host-Only networks, **Nmap NSE scripts** were used instead of OpenVAS/Nessus.

Command Used:

➤ sudo nmap --script vuln,exploit -sV -oN vulnerability_report.txt 192.168.56.102

Vulnerabilities Detected:

1. vsFTPD 2.3.4 Backdoor (CVE-2011-2523) – Critical
2. Samba SMB Remote Code Execution – High
3. Distcc Remote Command Execution – High
4. UnrealIRCd Backdoor Trojan – Critical
5. MySQL Weak Credentials – Medium

```
(kali㉿kali)-[~]
$ sudo nmap -sV -O 192.168.56.102
Starting Nmap 7.6.1 ( https://nmap.org ) at 2023-10-17 01:16 IST
Nmap scan report for 192.168.56.102
Host is up (0.0004s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    OPEN  ssh
23/tcp    OPEN  telnet
25/tcp    OPEN  smtp
513/tcp   OPEN  http-digest-auth
|_SMB-DOWNLOADS:
| VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     VULNERABLE (ExploitAvailable)
|       ID: CVE-CVE-2011-2523 RID:48539
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|           Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://github.com/rail0t/metasploit-framework/blob/master/modules/exploit/unix/ftp/vsftpd_234_backdoored.rb
|         https://www.exploit-db.com/wp-content/themes/exploit/0/alert-vsftpd-download-backdoored.html
|_ 22/tcp  open  ssh
| 23/tcp  open  telnet
| 25/tcp  open  smtp
| 513/tcp  open  http-digest-auth
| VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MITM Vulnerability
|     State: VULNERABLE
|     Transport Layer Security (TLS) services that use anonymous Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|         Cipher Suite: TLS_DH_anon_WITH_RC4_128_MDS
|         Modulus Type: Safe prime
|         Modulus Source: postfix builtin
|         Modulus Length: 1024
|         Generator Length: 3
|         Public Key Length: 1024
|       References:
|         https://www.ietf.org/rfc/rfc2246.txt
HTTP://192.168.56.102:80/mutillidave/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=source-viewer.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=show-1.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=user-info.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=frame.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=change-log.htm%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=user-poll.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=credits.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=background-color.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=set-background-color.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
HTTP://192.168.56.102:80/mutillidave/index.php?page=show-log.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=dns-lookup.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=ip-lookup.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=capture-data.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=frame.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=change-log.htm%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=home.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=user-poll.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=credits.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=viewer-info.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=html5-storage.php%27%20OR%20sqlspider
HTTP://192.168.56.102:80/mutillidave/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
```

```

JSESSIONID:
    httponly flag not set
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
JSESSIONID:
    httponly flag not set
/admin/includes/FCKeditor/editor/filemanager/upload/test.html:
JSESSIONID:
    httponly flag not set
/admin/jscript/upload.html:
JSESSIONID:
    httponly flag not set
http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/admin/Login.html: Possible admin folder
/admin/admin.html: Possible admin folder
/admin/account.html: Possible admin folder
/admin/admin_login.html: Possible admin folder
/admin/admin_login.html: Possible admin folder
/admin/admin-login.html: Possible admin folder
/admin/adminLogin.html: Possible admin folder
/admin/controlpanel.html: Possible admin folder
/admin/cp.html: Possible admin folder
/admin/index.jsp: Possible admin folder
/admin/Login.jsp: Possible admin folder
/admin/admin.jsp: Possible admin folder
/admin/home.jsp: Possible admin folder
/admin/controlpanel.jsp: Possible admin folder
/admin/admin-login.jsp: Possible admin folder
/admin/cp.jsp: Possible admin folder
/admin/account.jsp: Possible admin folder
/admin/admin_login.jsp: Possible admin folder
/admin/adminLogin.jsp: Possible admin folder
/manager/html/upload: Apache Tomcat (401 Unauthorized)
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
/admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
/admin/script/upload.html: Lizard Cart/Remote File upload
/webdav/: Potentially interesting folder
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms10-054: false
| smb-vuln-ms10-061: false

# Nmap done at Sun Oct 12 01:21:39 2025 -- 1 IP address (1 host up) scanned in 312.84 seconds

```

Recommendations:

- Update or remove vulnerable services.
- Disable Telnet and FTP; use secure protocols (SSH/SFTP).
- Regularly patch operating systems and applications.

6. Step 4 – Packet Analysis with Wireshark

A. FTP Credential Capture

- Captured plain-text credentials:
 - Username: msfadmin
 - Password: msfadmin
- Verified using Wireshark filters:

➤ ftp.request.command == "USER" or ftp.request.command == "PASS"

```

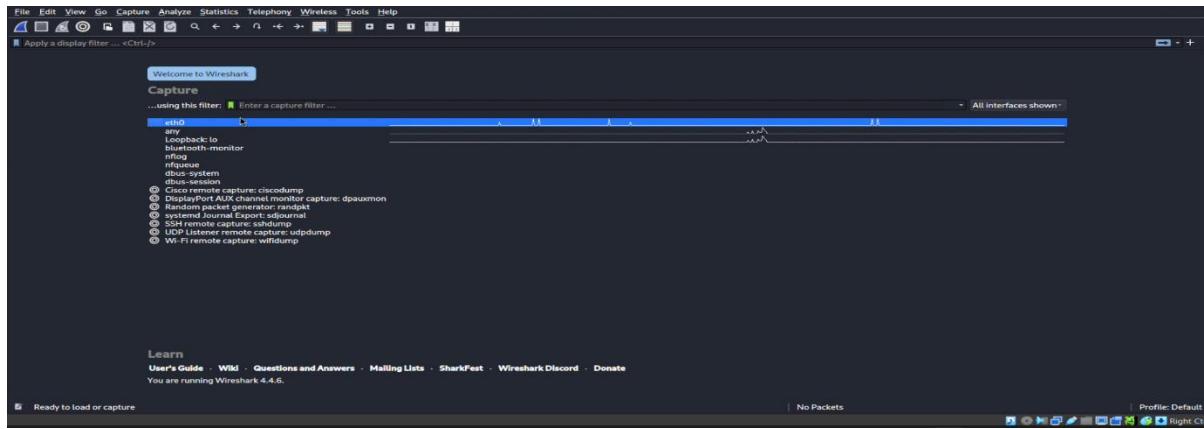
[kali㉿Kali:~]
└─$ sudo wireshark
** (wireshark:140113) 01:43:24.417672 [Capture MESSAGE] -- Capture Start ...
** (wireshark:140113) 01:43:24.479753 [Capture MESSAGE] -- Capture started
** (wireshark:140113) 01:43:24.479925 [Capture MESSAGE] -- File: '/tmp/wireshark_eth0VE4BE3.pcapng'
** (wireshark:140113) 01:43:24.479925 [Capture MESSAGE] -- Capture Stop
** (wireshark:140113) 01:43:24.479925 [Capture MESSAGE] -- Capture stopped
** (wireshark:140113) 01:58:38.415309 [GUI WARNING] -- failed to create capture table
** (wireshark:140113) 02:02:36.830651 [GUI WARNING] -- QThreadStorage: Thread 0x55a334fb8700 exited after QThreadStorage 4 destroyed
** (wireshark:140113) 02:02:36.830860 [GUI WARNING] -- QThreadStorage: Thread 0x55a334fb8700 exited after QThreadStorage 3 destroyed
** (wireshark:140113) 02:02:36.830867 [GUI WARNING] -- QThreadStorage: Thread 0x55a334fb8700 exited after QThreadStorage 2 destroyed
[kali㉿Kali:~]
└─$ ^C
[kali㉿Kali:~]
└─$ sudo wireshark
[sudo] password for kali: 

```

```

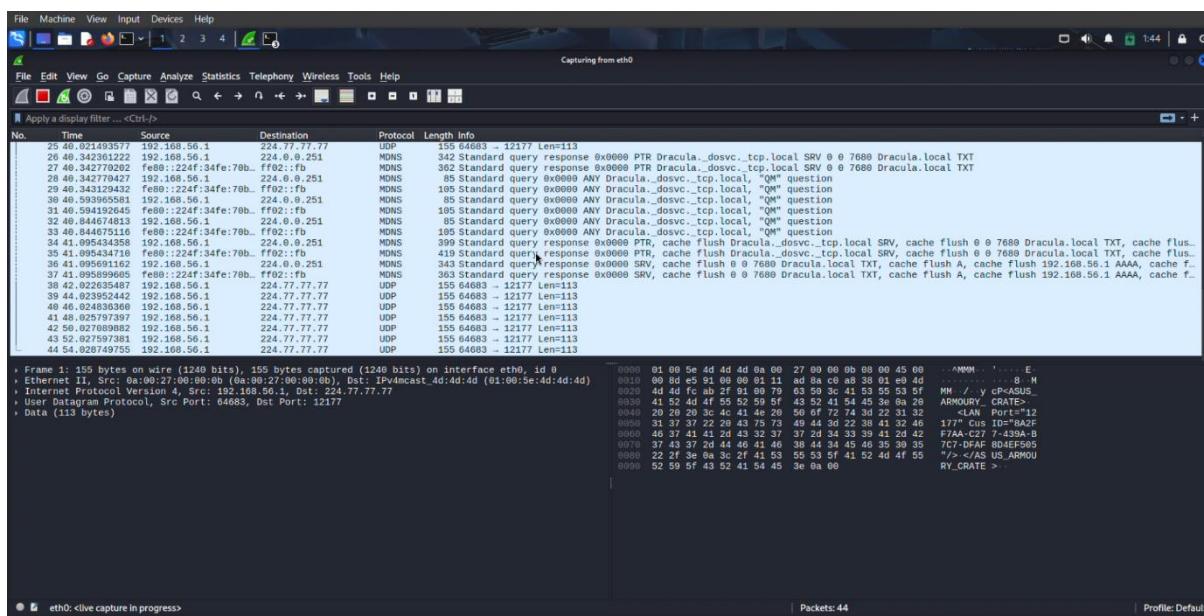
[kali㉿Kali:~]
└─$ sudo wireshark

```



B. SYN Flood Simulation

Used hping3 to simulate a flood:



Observed a large number of SYN packets without corresponding ACK responses.

Findings:

- Demonstrated DoS vulnerability.
- Highlighted need for rate limiting and firewall rules.

7. Step 5 – Firewall Configuration (iptables)

A. Allow Rules

- sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- sudo iptables -A INPUT -i lo -j ACCEPT
- sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

B. Deny Rules

- sudo iptables -A INPUT -p tcp --dport 23 -j DROP
- sudo iptables -A INPUT -p tcp --dport 445 -j DROP

```
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -i lo -j ACCEPT
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 23 -j DROP
(kali㉿Kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 445 -j DROP
(kali㉿Kali)-[~]
└─$ sudo iptables -L -v -n --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out    source         destination
 1    0     0  ACCEPT      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:22
 2    0     0  ACCEPT      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:80
 3    0     0  ACCEPT      all  --  lo      *      0.0.0.0/0        0.0.0.0/0
 4    0     0  ACCEPT      all  --  *      *      0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED
 5    0     0  DROP       tcp  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:23
 6    0     0  DROP       tcp  --  *      *      0.0.0.0/0        0.0.0.0/0          tcp dpt:445

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out    source         destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out    source         destination
```

Verification:

- nmap -p 445 192.168.56.101

```
(kali㉿Kali)-[~]
└─$ nmap -p 445 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 02:10 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0005s latency).

PORT      STATE SERVICE
445/tcp    closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
(kali㉿Kali)-[~]
└─$ sudo iptables-save > iptables_rules.txt
(kali㉿Kali)-[~]
└─$ sudo iptables -F
(kali㉿Kali)-[~]
└─$ sudo iptables -X
(kali㉿Kali)-[~]
└─$ sudo iptables -P INPUT ACCEPT
(kali㉿Kali)-[~]
```

Result: Port 445 showed as *filtered*, confirming rule effectiveness

10. Key Learnings

1. Learned how to perform **reconnaissance and enumeration** effectively.
2. Understood the role of **Nmap** in scanning and vulnerability detection.
3. Captured and analyzed **unencrypted credentials** with Wireshark.
4. Simulated **DoS attacks** and monitored packet patterns.
5. Implemented **firewall rules** to mitigate attacks and port scans.
6. Gained insight into **network security posture assessment**.

11. Conclusion

This task provided comprehensive hands-on experience in **network security assessment**. Through reconnaissance, scanning, vulnerability analysis, and defensive configurations, I learned how attackers identify weaknesses and how defenders can secure systems.

The exercise enhanced my technical, analytical, and documentation skills in cybersecurity.