Cybersecurity Investigation Report

Case ID: 2025-FTP-001

Date of Report: 20/04/2025

Prepared By: Elizabeth Peninah A. O.

1. Executive Summary

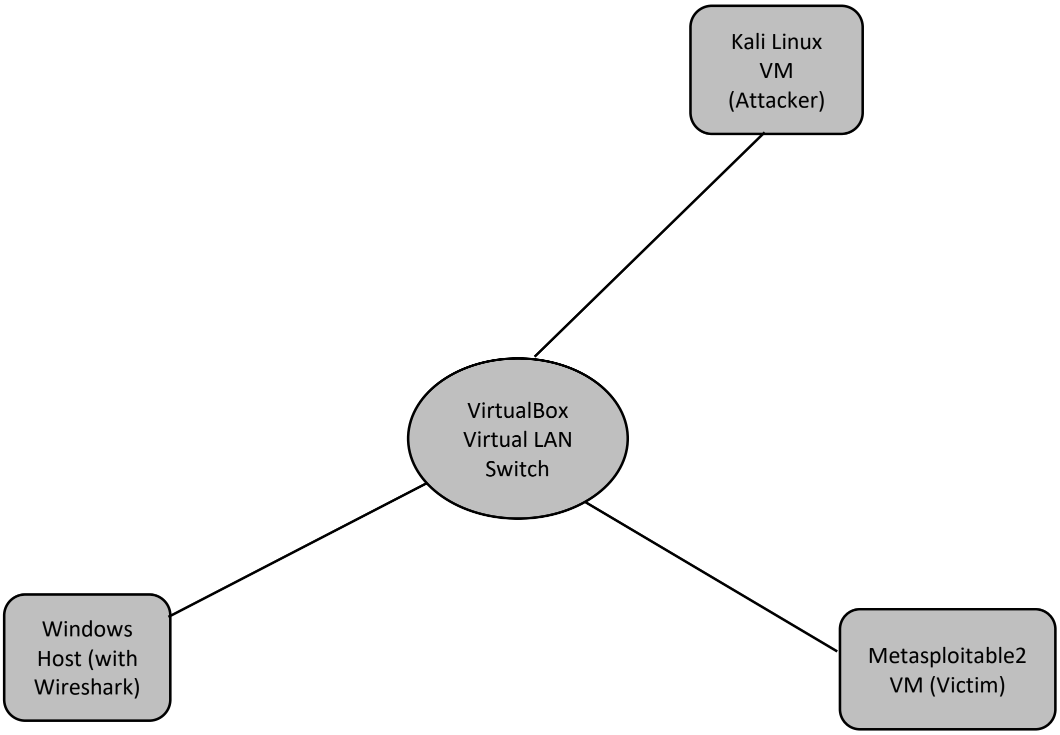
On 10/04/2025 at 9.00am EAT, a controlled security exercise was conducted in a virtual lab to simulate an FTP brute-force attack followed by data exfiltration. The objective was to capture and analyze the network traffic using Wireshark, identify indicators of compromise, and document findings. The investigation confirmed that a vulnerable Metasploitabel2 FTP service was successfully compromised using Hydra password-cracking tool from Kali Linux attack machine. Captured PCAP analysis revealed repeated failed login attempts followed by a successful login, file transfers, and unencrypted credential exposure.

2. Incident Details

Date/Time Detected	**16/04/2025 at 08:11:59am EAT**
Incident Type	Brute-force attack and data exfiltration
Location	Virtual lab environment
Systems Involved	Kali Linux (Attacker), Metasploitable2 Victim
Service Targeted	FTP (Port 21)
Attack Tool Used	Hydra
Detection Method	Wireshark packet capture analysis

3. Environment Setup

Network Topology:


Kali Linux VM (Attacker)
VirtualBox Virtual LAN Switch
Windows Host (with Wireshark)
Metasploitable2 VM (Victim)

Configuration Details:

- Attacker Machine: Kali Linux, IP: 192.168.56.101
- Victim Machine: Metasploitable2, IP: 192.168.56.102
- Tools: Hydra, Wireshark
- PCAP File

4. Evidence Collected

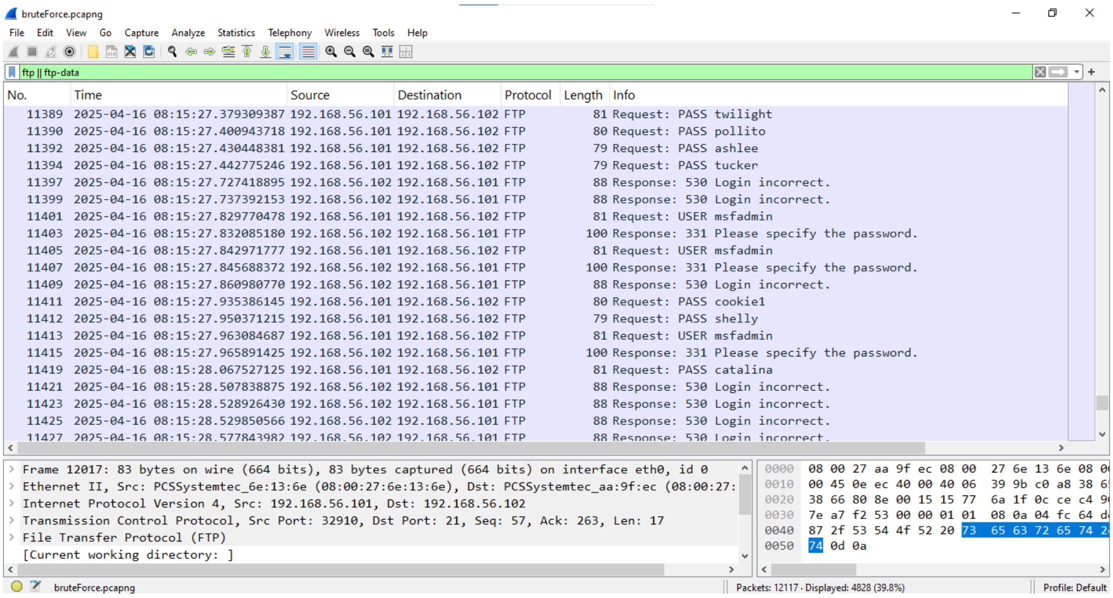
PCAP File: bruteForce.pcapng

Hydra Command Used: hydra -l msfadmin -P ~/ftp-demo-list.txt ftp://192.168.56.102

Wireshark Filters Used:

- ip.addr == 192.168.56.102
- ftp || ftp-data
- ftp.request.command == "USER"
- ftp.request.command == "PASS"
- ftp.response.code == 230
- ftp.request.command == "STOR" || ftp.request.command == "RETR"

Screenshots:



bruteForce.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

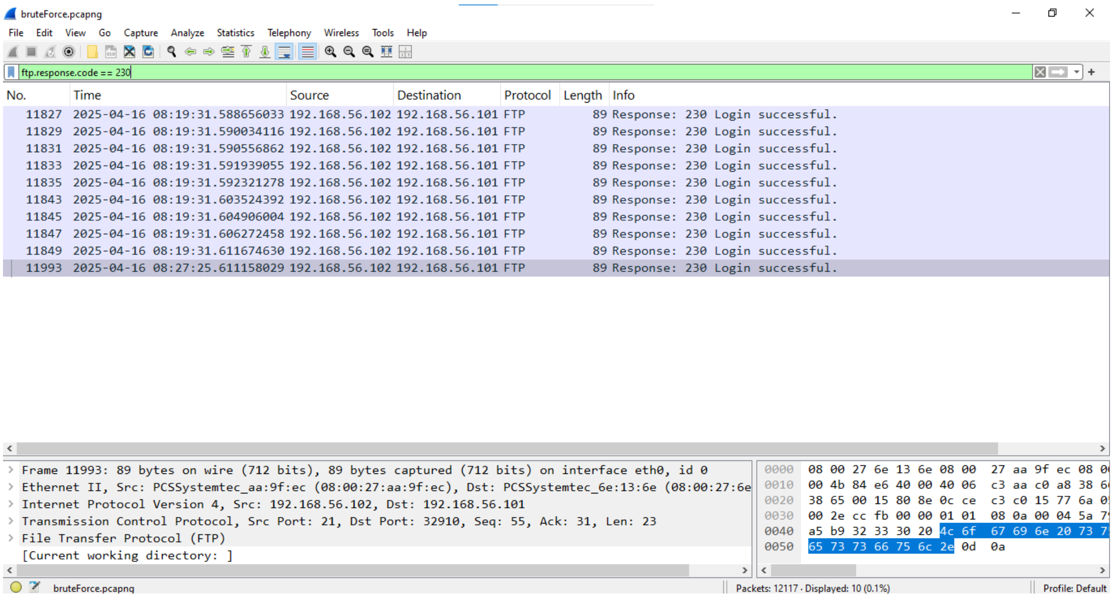
```
ftp || ftp-data
```

```
No.    Time                          Source         Destination    Protocol Length Info
 11389 2025-04-16 08:15:27.379309387 192.168.56.101 192.168.56.102 FTP       81 Request: PASS twilight
 11390 2025-04-16 08:15:27.400943718 192.168.56.101 192.168.56.102 FTP       80 Request: PASS pollito
 11392 2025-04-16 08:15:27.430448381 192.168.56.101 192.168.56.102 FTP       79 Request: PASS ashlee
 11394 2025-04-16 08:15:27.442775246 192.168.56.101 192.168.56.102 FTP       79 Request: PASS tucker
 11397 2025-04-16 08:15:27.727418895 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11399 2025-04-16 08:15:27.737392153 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11401 2025-04-16 08:15:27.829770478 192.168.56.101 192.168.56.102 FTP       81 Request: USER msfadmin
 11403 2025-04-16 08:15:27.832085180 192.168.56.102 192.168.56.101 FTP      100 Response: 331 Please specify the password.
 11405 2025-04-16 08:15:27.842971777 192.168.56.101 192.168.56.102 FTP       81 Request: USER msfadmin
 11407 2025-04-16 08:15:27.845688372 192.168.56.102 192.168.56.101 FTP      100 Response: 331 Please specify the password.
 11409 2025-04-16 08:15:27.860980770 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11411 2025-04-16 08:15:27.935386145 192.168.56.101 192.168.56.102 FTP       80 Request: PASS cookie1
 11412 2025-04-16 08:15:27.950371215 192.168.56.101 192.168.56.102 FTP       79 Request: PASS shelly
 11413 2025-04-16 08:15:27.963084687 192.168.56.101 192.168.56.102 FTP       81 Request: USER msfadmin
 11415 2025-04-16 08:15:27.965891425 192.168.56.102 192.168.56.101 FTP      100 Response: 331 Please specify the password.
 11419 2025-04-16 08:15:28.067527125 192.168.56.101 192.168.56.102 FTP       81 Request: PASS catalina
 11421 2025-04-16 08:15:28.507838875 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11423 2025-04-16 08:15:28.528926430 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11425 2025-04-16 08:15:28.529850566 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
 11427 2025-04-16 08:15:28.577843982 192.168.56.102 192.168.56.101 FTP       88 Response: 530 Login incorrect.
```

```
> Frame 12017: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: PCSSystemtec_aa:9f:ec (08:00:27:
> Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
> Transmission Control Protocol, Src Port: 32910, Dst Port: 21, Seq: 57, Ack: 263, Len: 17
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 aa 9f ec 08 00  27 6e 13 6e 08 0
0010  00 45 0e ec 40 00 40 06  39 9b c0 a8 38 6
0020  38 66 80 8e 00 15 15 77  6a 1f 0c ce c4 9
0030  7e a7 f2 53 00 00 01 01  08 0a 04 fc 64 d
0040  87 2f 53 54 4f 52 20 73  65 63 72 65 74 2
0050  74 0d 0a
```

Repeated failed login attempts


bruteForce.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ftp.response.code == 230
```

```
No.    Time                          Source         Destination    Protocol Length Info
 11827 2025-04-16 08:19:31.588656033 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11829 2025-04-16 08:19:31.590034116 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11831 2025-04-16 08:19:31.590556862 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11833 2025-04-16 08:19:31.591939055 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11835 2025-04-16 08:19:31.592321278 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11843 2025-04-16 08:19:31.603524392 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11845 2025-04-16 08:19:31.604906004 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11847 2025-04-16 08:19:31.606272458 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11849 2025-04-16 08:19:31.611674630 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
 11993 2025-04-16 08:27:25.611158029 192.168.56.102 192.168.56.101 FTP        89 Response: 230 Login successful.
```

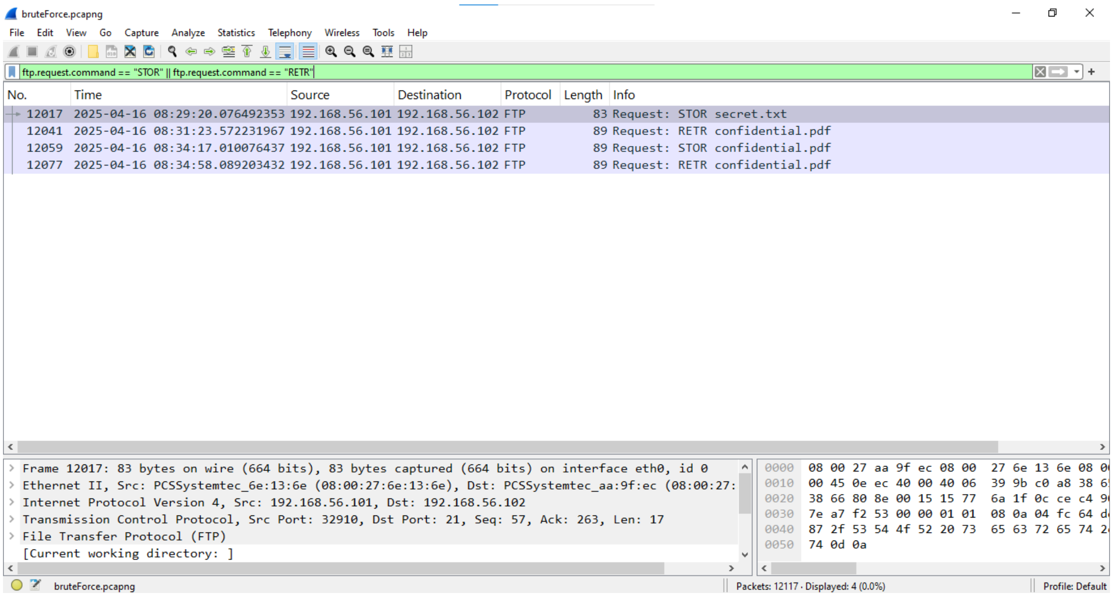
```
> Frame 11993: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_aa:9f:ec (08:00:27:aa:9f:ec), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e
> Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101
> Transmission Control Protocol, Src Port: 21, Dst Port: 32910, Seq: 55, Ack: 31, Len: 23
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 6e 13 6e 08 00  27 aa 9f ec 08
0010  00 4b 84 e6 40 00 40 06  c3 aa c0 a8 38
0020  38 65 00 15 80 8e 0c ce  c3 c0 15 77 6a
0030  00 2e cc fb 00 00 01 01  08 0a 00 04 5a
0040  a5 b9 32 33 30 20 4c 6f  67 69 6e 20 73
0050  65 73 73 66 75 6c 2e 0d  0a
```

Packets: 12117 · Displayed: 10 (0.1%)

Profile: Default

Successful login packets


bruteForce.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ftp.request.command == "STOR" || ftp.request.command == "RETR"
```

```
No.    Time                          Source         Destination    Protocol Length Info
 12017 2025-04-16 08:29:20.076492353 192.168.56.101 192.168.56.102 FTP        83 Request: STOR secret.txt
 12041 2025-04-16 08:31:23.572231967 192.168.56.101 192.168.56.102 FTP        89 Request: RETR confidential.pdf
 12059 2025-04-16 08:34:17.010076437 192.168.56.101 192.168.56.102 FTP        89 Request: STOR confidential.pdf
 12077 2025-04-16 08:34:58.089203432 192.168.56.101 192.168.56.102 FTP        89 Request: RETR confidential.pdf
```

```
> Frame 12017: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: PCSSystemtec_aa:9f:ec (08:00:27:
> Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
> Transmission Control Protocol, Src Port: 32910, Dst Port: 21, Seq: 57, Ack: 263, Len: 17
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 aa 9f ec 08 00  27 6e 13 6e 08
0010  00 45 0e ec 40 00 40 06  39 9b c0 a8 38
0020  38 66 80 8e 00 15 15 77  6a 1f 0c ce c4
0030  7e a7 f2 53 00 00 01 01  08 0a 04 fc 64
0040  87 2f 53 54 4f 52 20 73  65 63 72 65 74
0050  74 0d 0a
```

Packets: 12117 · Displayed: 4 (0.0%)

Profile: Default

File transfer evidence (STOR / RETR commands)

5. Technical Analysis

Timeline of Attack (based on packet timestamps):

Time (HH:MM:SS)	**Event**
08:11:59	First brute-force attempt detected
08:12:02	Multiple failed login attempts
08:19:31	Successful login using username *msfadmin*
08:29:30	File download initiated
08:34:58	Data exfiltration completed

Indicators of Compromise (IOCs):

- Attacker IP: 192.168.56.101
- Victim IP: 192.168.56.102
- Credentials Compromised: msfadmin:msfadmin
- Protocol Weakness: Unencrypted FTP credentials visible in packets

6. Root Cause Analysis

The attack succeeded due to:

- Weak/default FTP credentials (msfadmin:msfadmin)
- Lack of encryption in FTP protocol
- No account lockout or brute-force protection
- No intrusion detection/prevention in place

7. Recommendations

- Replace FTP with Secure Alternatives - Implement SFTP/FTPS.
- Enforce Strong Password Policy - Minimum length, complexity, and periodic changes.
- Enable Account Lockout - After repeated failed logins.
- Implement Network Security Monitoring - Deploy IDS/IPS to detect brute-force attempts.
- Encrypt Data Transfers - Prevent credential interception.

8. Conclusion

This investigation confirmed that FTP services with weak credentials and no encryption are highly vulnerable to brute-force attacks and data theft.

The findings reinforce the importance of proactive security measures, including secure protocols, strong authentication, and real-time monitoring.

9. Appendices

- Appendix A: Network Topology Diagram
- Appendix B: Wireshark Packet Screenshots
- Appendix C: PCAP File