

# Comparative Study on Password Cracking Tools

Shejina Nazar

Department of Computer Application

Amal Jyothi College of Engineering Kanjirappally,  
India

[shejinanazar2021@mca.ajce.in](mailto:shejinanazar2021@mca.ajce.in)

Rini Kurian

Department of Computer Application

Amal Jyothi College of Engineering Kanjirappally,  
India

[rinikurian@amaljyothi.ac.in](mailto:rinikurian@amaljyothi.ac.in)

**Abstract:** In this paper, it provides a brief description about the different password cracking tools. Passwords are the most standard ways to protect and authenticate the security of a network or for any other information. Security of server in all contexts is dominating in every field of computing, while working on the servers numerous threats and attacks like cracking of passwords, knowing the root of machine, giving privilege to unauthorized users are common attacks that can harm the system and take access of servers. Password cracking is the process of obtaining the correct password to an account in an unauthorized way. The most prevalent commands like Hydra and Medusa, Ncrack, Patator are there which can be used for cracking the passwords of servers and unauthorized users can take access of server by applying these commands. Hydra is a login cracker which supports many protocols to attack. It works by different approaches to perform brute-force attacks in order to guess the right username and password combination. Medusa is a modular, speedy, and parallel, login brute-forcer. It is a very powerful and lightweight tool. The goal is to support as many services which allow remote authentication as possible.

Ncrack is a very fast network authentication cracking tool that helps organization to secure their networks against password attacks. Patator is a security tool to perform enumeration or brute-force attempts to discover authentication details. It can be used during penetration testing. Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. Here, we will consider brute force attack and its tools with its implementation and prevention ways or techniques to avoid these types of attacks.

## I. INTRODUCTION

Server security is a trending topic in today's world. Every year millions of dollars are spent to achieve the security and hundreds of researchers are currently underway to solve the problems of security. Despite working on the well-defined security mechanisms there exist many loopholes in

this like cracking of password, unauthorized access of server. For cracking passwords of server brute force method is one of the most commonly used technique. There are many tools associated with brute force such as Hydra, Medusa, Ncrack, Patator. This attack works by testing every possible combination that could be used as the password by the user and then testing it to see if it is the correct password. To find if the password is correct or not it further checks for any errors in the response from the server. These tools are used as brute force SSH. Hydra, a password detection tool which can be used in many situations that includes authentication-based forms which are used in web applications. On the other hand Medusa is a speedy, parallel and modular, login brute forcer that is used to support as many services which allow remote authentication possible. While Ncrack is a tool that is used as a brute force tool to target small and large networks. Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage. Patator was written out of frustration from using Hydra, Medusa, Ncrack, Metasploit modules and Nmap NSE scripts for password guessing attacks. Patator is a multi-threaded tool written in Python, that strives to be more reliable and flexible.

## II. BRUTE FORCE ATTACK

Brute Force Attack is most conventional attack that work against web applications. To acquire access of user accounts by trying to guess the passwords of the single user or group of users is the core aim of brute force attack. Web application should be robust enough to work against on this attack, unless attacker will get the privilege of the system.

Brute force attack can be applied in numerous ways. Length of the password known by attacker can cause the brute force attack, combination of numbers, letters and symbols can be applied unless a suitable match is

found. However, this is a slow process, especially as the length of the password increases. One of the way of

the brute force attack is if illegitimate user is aware of username which is generally root for a web application. Further it can based on the complexity of the password like if a weak password is used then it also becomes victim for attack.

### A. TOOLS FOR BRUTE FORCE

Tools are the techniques or methods that help to crack the passwords. Brute force attacks are considered to test all the feasible combinations for cracking the passwords of server. Following are the tools that we will apply to crack the password such as Hydra, Medusa, Ncrack and Patator.

#### Hydra tool for brute force

Hydra is one of the best login cracker tool that further supports various protocols for and flexible method to add new modules. There are various protocols that support to Hydra tools which are Cisco AAA, Cisco auth, Cisco enable, Telnet etc.

#### Medusa Tool for Brute Force

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

#### Ncrack Tool for Brute Force

Ncrack is a cracking tool that is highly recommended for high-speed network authentication. It was majorly designed for the companies to secure networks by proactively testing for weak passwords. It followed a design technique which was based on modularization related to Nmap and a dynamic engine with friendly interface which infact gives full control of operations of network. Some of the protocols which support includes SSH, FTP, telnet, HTTP(S), POP3(S) etc.

### III. EXPERIMENTAL SETUP AND RESULTS OF BRUTE FORCE ATTACK

Passwords and username are the weakest link in the system. It is very important for security assessment to test weak passwords. In this paper, we focus on some tools that facilitate remote service and brute-

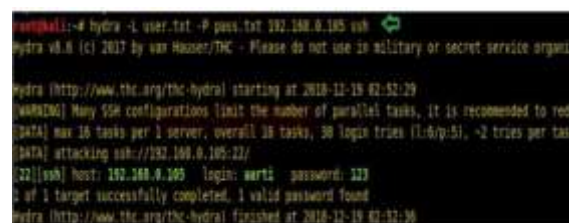
forcing. One type of password in brute-forcing is to temper attack against the password hash, by applying tools such as Hashcat, that is powerful tool that can crack encrypted password hashes on a local system. Hydra, Medusa, Ncrack and patator will be implemented in this paper. *Installation of Hydra, Medusa, Ncrack and Patator*

Hydra, Medusa, Ncrack and Patator are the best password cracking tools. Following are the steps for the installation of all the tools was straight forward on Ubuntu Linux.

#### Brute force using Hydra

Hydra is one of the popular brute forcing tool through this password can be easily cracked of remote machine. To download Hydra in Kali Linux machine, type below command:

hydra -L user.txt -P pass.txt 192.168.43.100 ssh



```
root@kali:~# hydra -L user.txt -P pass.txt 192.168.0.105 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizat
Hydra (http://www.thc.org/thc-hydra) starting at 2018-12-19 02:52:29
[WARNING] Many SSH configurations limit the number of parallel tasks, (it is recommended to redu
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (16/p/5), ~2 tries per task
[DATA] attacking ssh://192.168.0.105:22/
22[ssh] host: 192.168.0.105 login: wurti password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-19 02:52:30
```

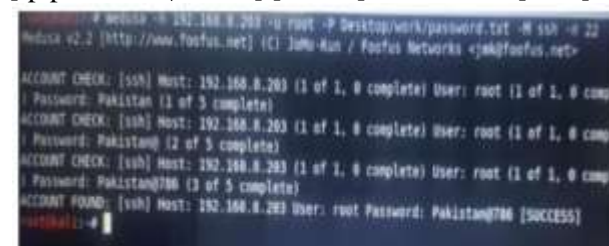
#### Brute force using Medusa

Medusa is another popular brute forcing tool through which you can easily crack the SSH password of any remote machine. To install Medusa type the below command:

sudo apt-get install medusa

After successful install run it by typing Medusa.

Syntax: Medusa [-host | -H file] [-u username | -U file]  
[-p password | -P file] [-C file] -M module [OPT]



```
root@kali:~# medusa -H 192.168.0.200 -u root -P Desktop/work/password.txt -M ssh -e 22
Medusa v2.2 (http://www.fooofus.net) (C) Juhu-Kun / Fooofus Networks <juhukun@fooofus.net>
ACCOUNT CHECK: [ssh] Host: 192.168.0.200 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
1 Password: Pakistan (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.200 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
1 Password: Pakistan786 (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.200 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
1 Password: Pakistan786 (3 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.0.200 User: root Password: Pakistan786 (SUCCESS)
root@kali:~#
```

#### Brute force using Ncrack

Ncrack is little bit harder than Hydra but is more powerful amongst all other tools. To install Ncrack type the command:

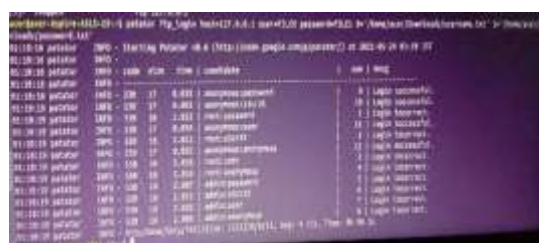
sudo apt-get install ncrack



### Brute force using Patator

Patator is an awesome tool that allows us to brute force several types of logins and even ZIP passwords.

To install Patator type the below command:  
sudo apt-get install patator



## IV. EXPERIMENTAL SETUP AND RESULTS TO PREVENT THE BRUTE FORCE ATTACK

There are numerous techniques which can prevent brute force attack like keeping password complexity strong, applying captcha codes and failed login attempt. In our work we will implement the above methods to prevent the common brute force attack and will be achieved by applying tools.

In Brute force attack if attacker is aware of default password which is root only then password can also be easily cracked by him. To avoid such attack username must be changed and it should be chosen a stronger one and by this hacking of the password can be avoided. Also if a weak password is chosen the system will not accept the same. So, a stronger password can prevent brute force attack. Another feature is that a VMware Exsi has a way to be automatically logged out user needs to be login again to work on server. This will also be helpful to prevent brute force attack.

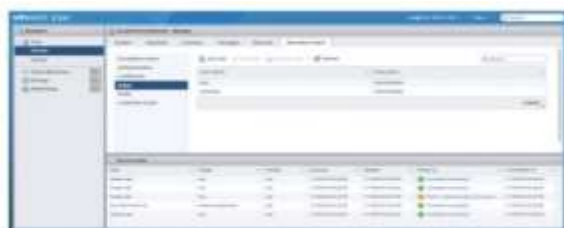


Fig: Snapshot using Change username

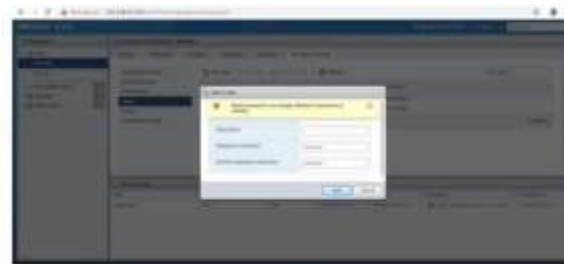


Fig: Snapshot using weak password

To enable each of these sections to uncomment header [ssh] and modify the enabled value into “true” as shown in the image and the save the jail.local file and restart the fail2ban service:

```
[ssh]
enabled = true
Service fail2ban restart
Following is the code to implement prevention of brute force
[ssh]
enabled = true
port = ssh
filter = sshd
logpath = var/log/auth.log
maxretry = 6
```

Let's test host machine against brute force attack for ssh login once again:

Hydra -L user.txt -P pass.txt 192.168.43.100 ssh



Fig: Prevention of brute force attack

## V. CONCLUSION AND FUTURE WORK

Passwords are already a weak form of authentication. A brute force attack is very effective way to take access of server by cracking passwords. It tries various combinations of usernames and passwords again and again to get the actual password. A Brute-force attack is dangerous for a system. More than 30 percent websites are developed using WordPress platform due to its popularity. WordPress is an open source and famous platform. It is a target of hackers. These attacks includes the above mentioned tools, by applying the commands hacker can take access to the system and privileges. There are following methods and techniques

such as password complexity, captchaang limit login access etc, to avoid this brute force attack. These methods are helpful to overcome the attacks which occur due to brute force. Although these attacks are defendable but still they are prone and found to be vulnerable with enormous growth of security loop holes.

## **VI. REFERENCE**

- [1] Brute –force and dictionary attack on hashed real- world passwords, international Convention on information and Communication Technology (2018)
- [2] <https://en.kali.tools/?p=147>
- [3] <https://allabouttesting.org/install-ftp-server-on-kali-linux/>