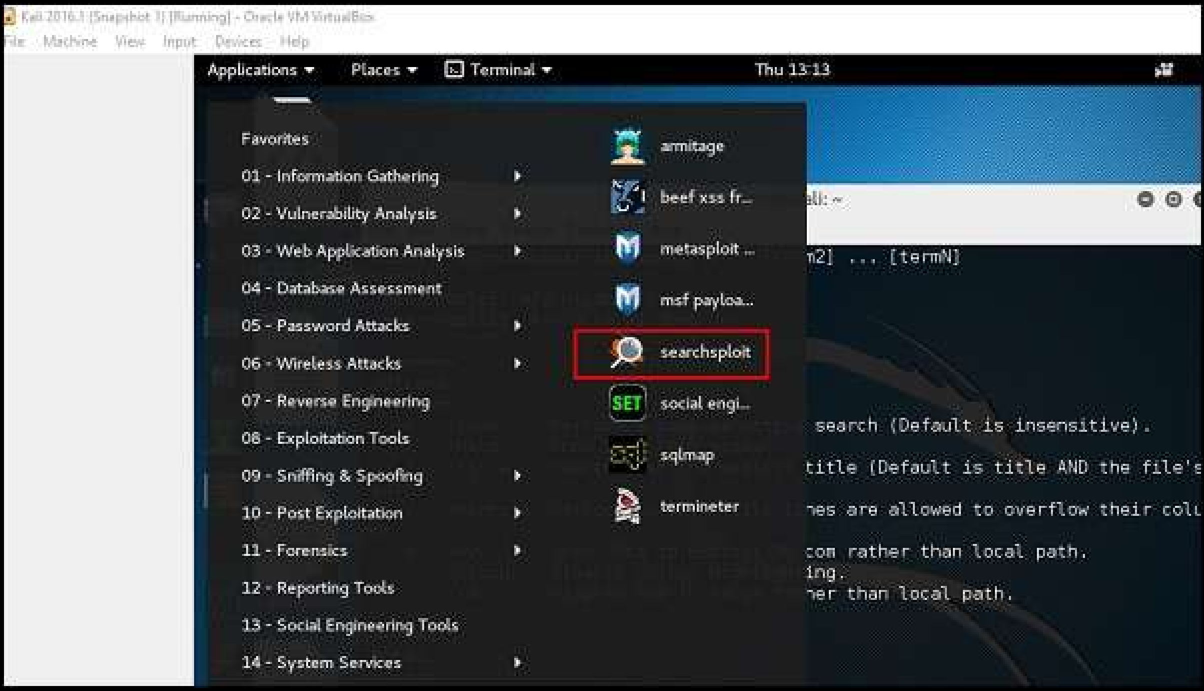
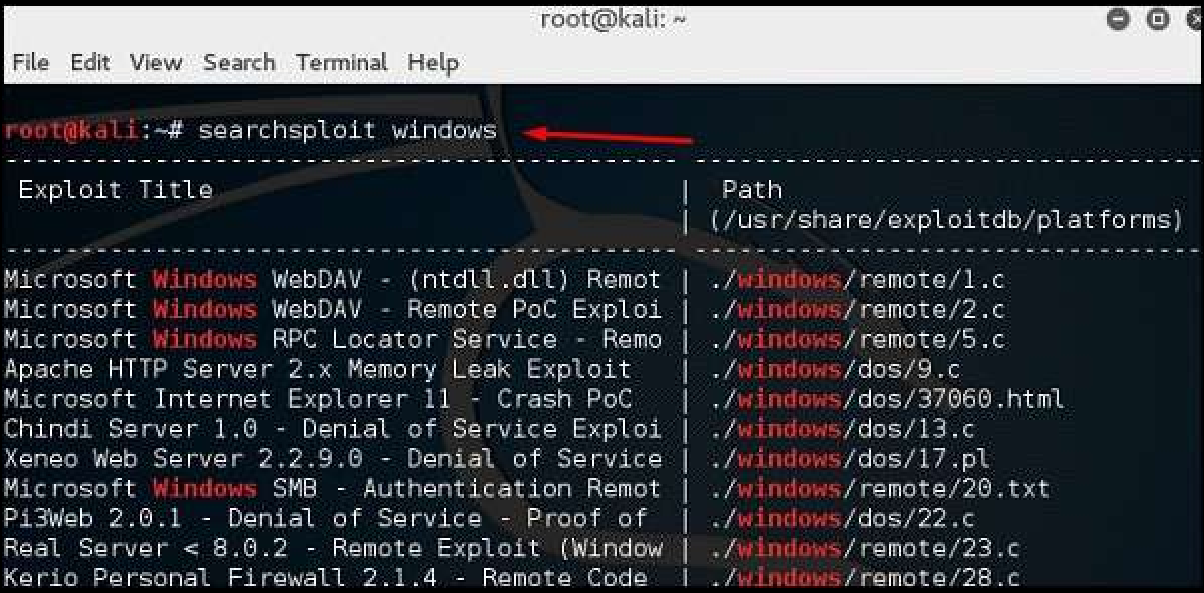
Information Gathering Tools-Searchsploit

Searchsploit is a tool that helps Kali Linux users to directly search with the command line from Exploit database archive.

To open it, go to Applications → 08-Exploitation Tools → searchsploit, as shown in the following screenshot.



After opening the terminal, type "**searchsploit exploit index name**".



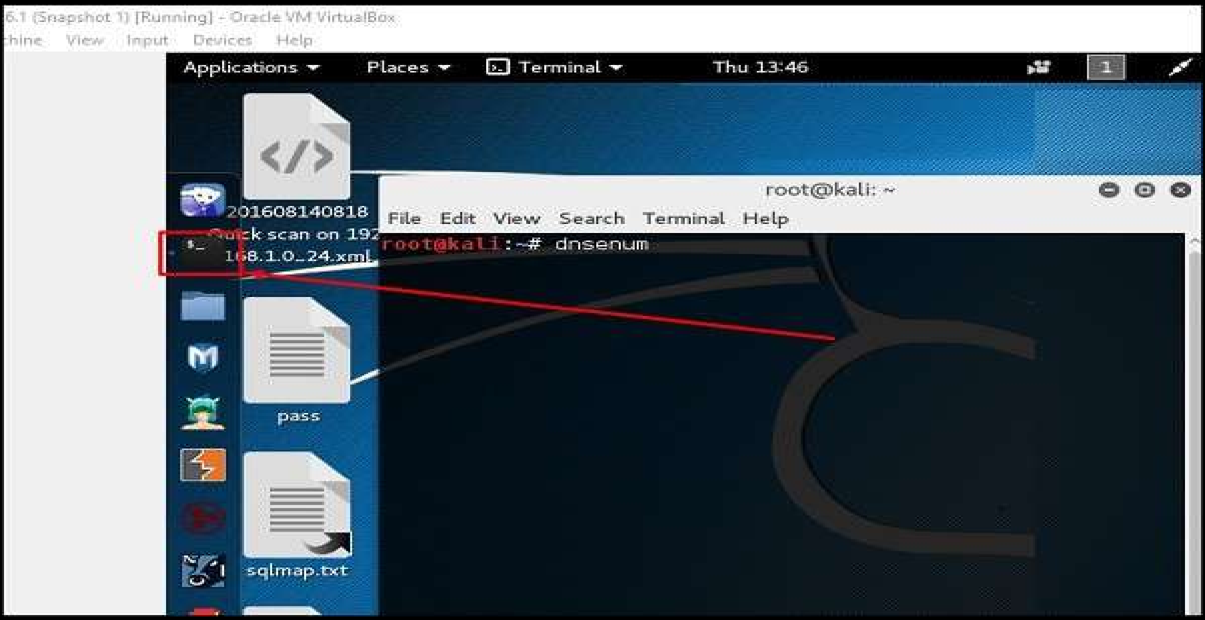
```
root@kali:~# searchsploit windows
--------------------------------------------- ----------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/platforms)
--------------------------------------------- ----------------------------------
Microsoft Windows WebDAV - (ntdll.dll) Remot | ./windows/remote/1.c
Microsoft Windows WebDAV - Remote PoC Exploi | ./windows/remote/2.c
Microsoft Windows RPC Locator Service - Remo | ./windows/remote/5.c
Apache HTTP Server 2.x Memory Leak Exploit   | ./windows/dos/9.c
Microsoft Internet Explorer 11 - Crash PoC   | ./windows/dos/37060.html
Chindi Server 1.0 - Denial of Service Exploi | ./windows/dos/13.c
Xeneo Web Server 2.2.9.0 - Denial of Service | ./windows/dos/17.pl
Microsoft Windows SMB - Authentication Remot | ./windows/remote/20.txt
Pi3Web 2.0.1 - Denial of Service - Proof of  | ./windows/dos/22.c
Real Server < 8.0.2 - Remote Exploit (Window | ./windows/remote/23.c
Kerio Personal Firewall 2.1.4 - Remote Code  | ./windows/remote/28.c
```

DNS Tools

In this section, we will learn how to use some DNS tools that Kali has incorporated. Basically, these tools help in zone transfers or domain IP resolving issues.

dnsenum.pl

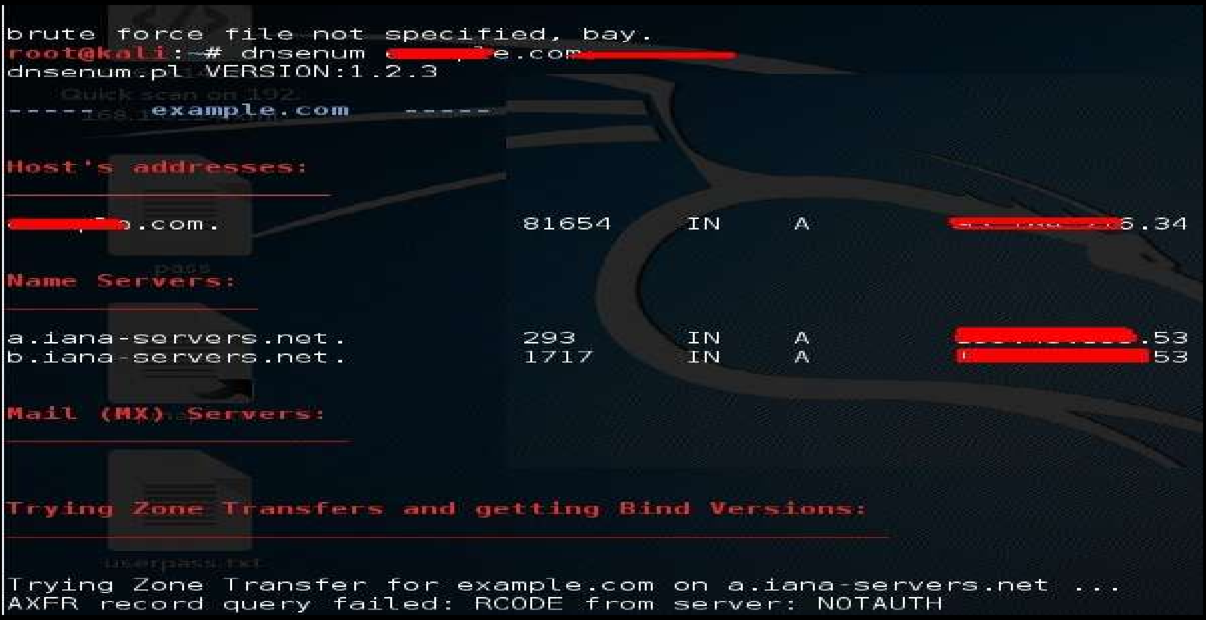
The first tool is **dnsenum.pl** which is a PERL script that helps to get MX, A, and other records connect to a domain.Click the terminal on the left panel.



6.1 (Snapshot 1) [Running] - Oracle VM VirtualBox
hine View Input Devices Help
Applications
Places
Terminal
Thu 13:46
201608140818
Quick scan on 192.168.1.0_24.xml
pass
sqlmap.txt
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# dnsenum
```

Type “**dnsenum domain name”** and all the records will be shown. In this case, it shows A records.

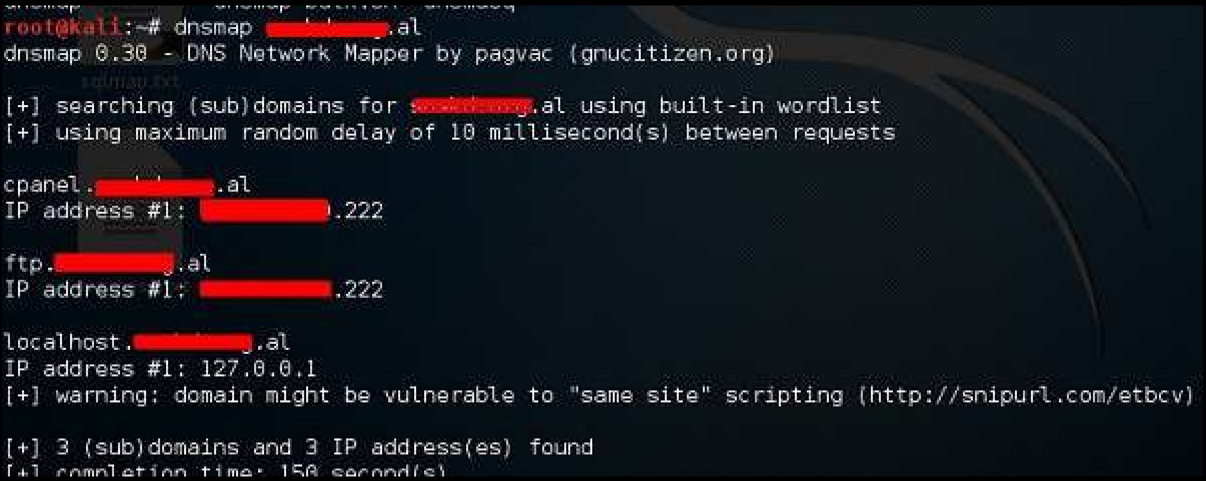


```
brute force file not specified, bay.
root@kali:~# dnsenum [redacted]e.com
dnsenum.pl VERSION:1.2.3

-----   example.com   -----


Host's addresses:
__________________

[redacted].com.                81654    IN    A        [redacted]5.34


Name Servers:
______________

a.iana-servers.net.            293      IN    A        [redacted].53
b.iana-servers.net.            1717     IN    A        [redacted]53


Mail (MX) Servers:
___________________



Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for example.com on a.iana-servers.net ...
AXFR record query failed: RCODE from server: NOTAUTH
```

DNSMAP

The second tool is **DNSMAP** which helps to find the phone numbers, contacts, and other subdomain connected to this domain, that we are searching. Following is an example.

Click the terminal as in the upper section , then write “**dnsmap domain name”**

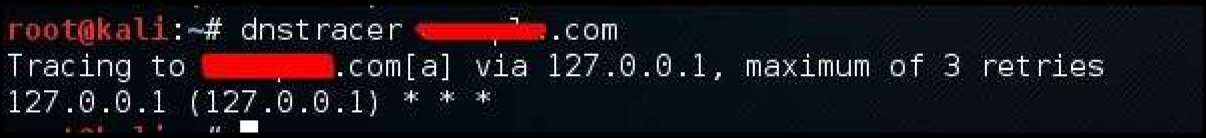


```
root@kali:~# dnsmap [redacted].al
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for [redacted].al using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

cpanel.[redacted].al
IP address #1: [redacted].222

ftp.[redacted].al
IP address #1: [redacted].222

localhost.[redacted].al
IP address #1: 127.0.0.1
[+] warning: domain might be vulnerable to "same site" scripting (http://snipurl.com/etbcv)

[+] 3 (sub)domains and 3 IP address(es) found
[+] completion time: 150 second(s)
```

dnstracer

The third tool is **dnstracer**, which determines where a given Domain Name Server (DNS) gets its information from for a given hostname.

Click the terminal as in the upper section, then type “**dnstracer domain name”**.

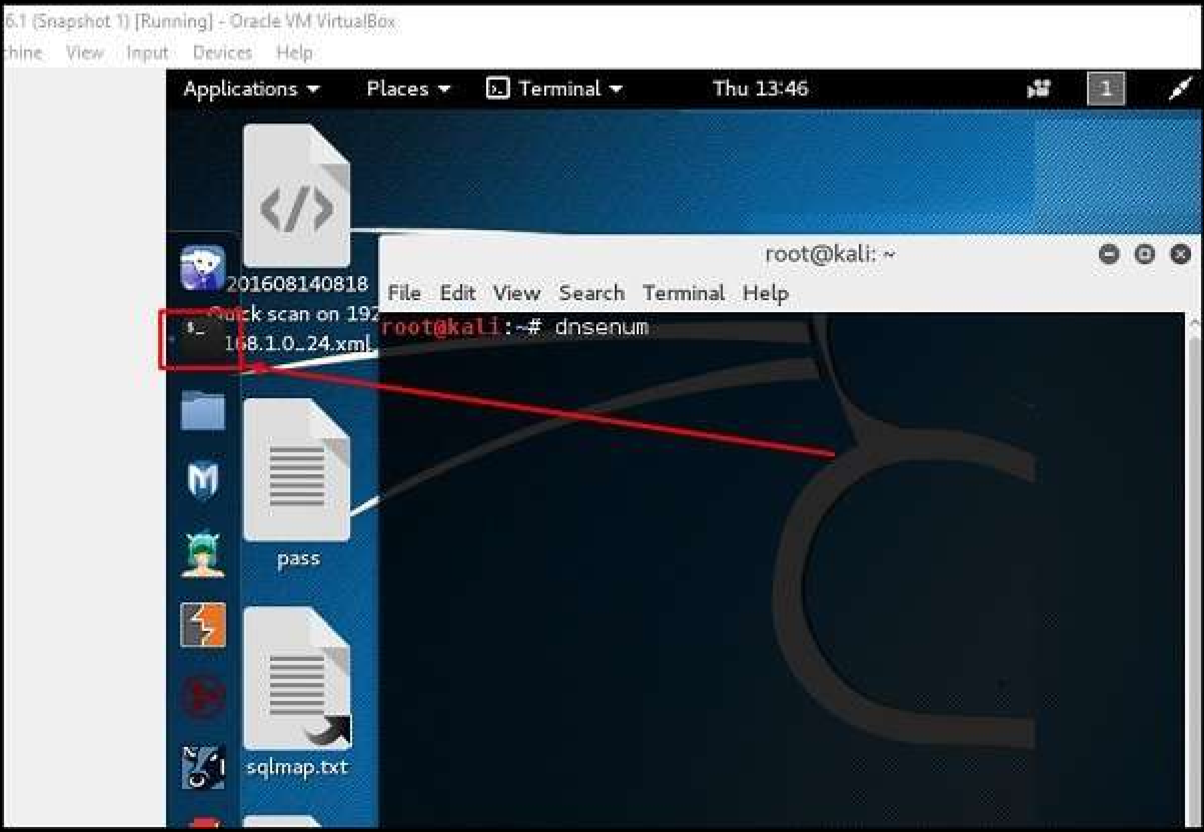


```
root@kali:~# dnstracer [redacted].com
Tracing to [redacted].com[a] via 127.0.0.1, maximum of 3 retries
127.0.0.1 (127.0.0.1) * * *
```

LBD Tools

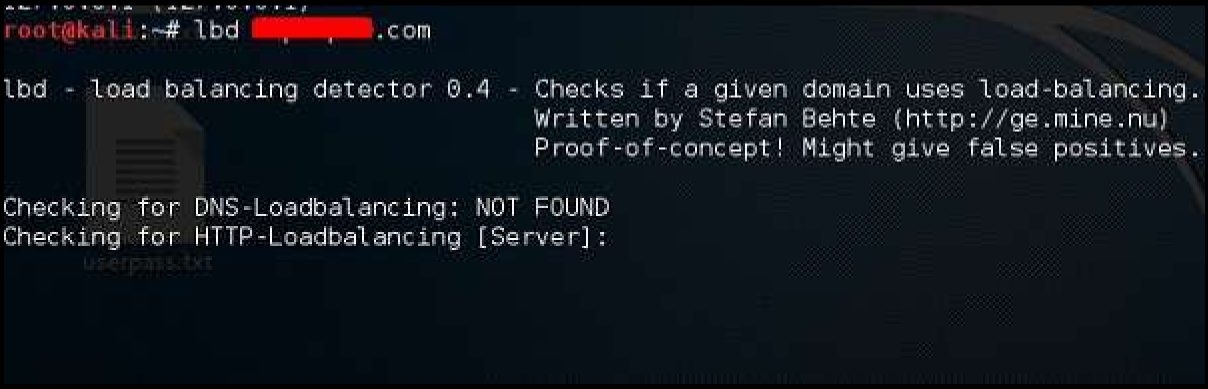
LBD (Load Balancing Detector) tools are very interesting as they detect if a given domain uses DNS and/or HTTP load balancing. It is important because if you have two servers, one or the other may not be updated and you can try to exploit it. Following are the steps to use it –

First, click the terminal on the left panel.


6.1 (Snapshot 1) [Running] - Oracle VM VirtualBox
hine View Input Devices Help
Applications ▾
Places ▾
Terminal ▾
Thu 13:46
1
201608140818
Quick scan on 192.168.1.0_24.xml
pass
sqlmap.txt
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# dnsenum
```

Then, type “**lbd domainname”**. If it produces a result as “FOUND”, it means that the server has a load balance. In this case, the result is “NOT FOUND”.

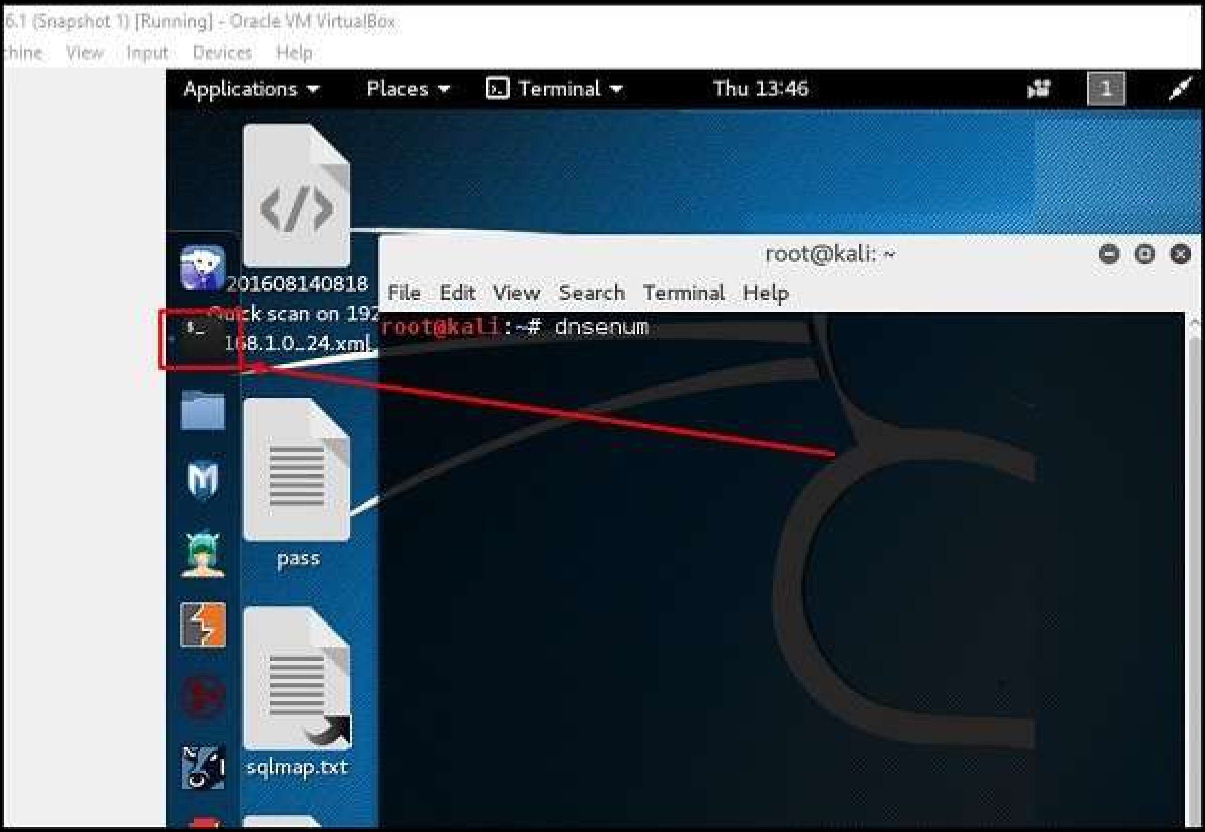


```
root@kali:~# lbd [redacted].com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
```

Hping3

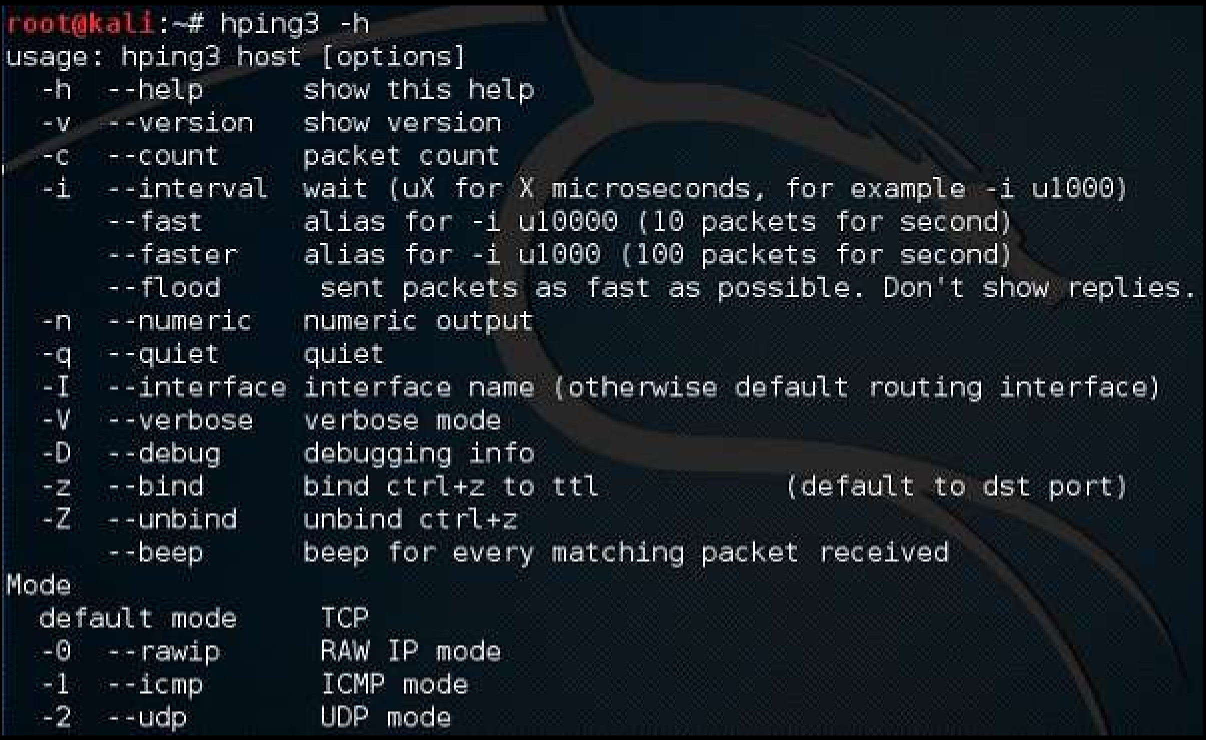
Hping3 is widely used by ethical hackers. It is nearly similar to ping tools but is more advanced, as it can bypass the firewall filter and use TCP, UDP, ICMP and RAW-IP protocols. It has a traceroute mode and the ability to send files between a covered channel.

Click the terminal on the left panel.


6.1 (Snapshot 1) [Running] - Oracle VM VirtualBox
hine View Input Devices Help
Applications
Places
Terminal
Thu 13:46
201608140818
Quick scan on 192.168.1.0_24.xml
pass
sqlmap.txt
root@kali: ~
File Edit View Search Terminal Help

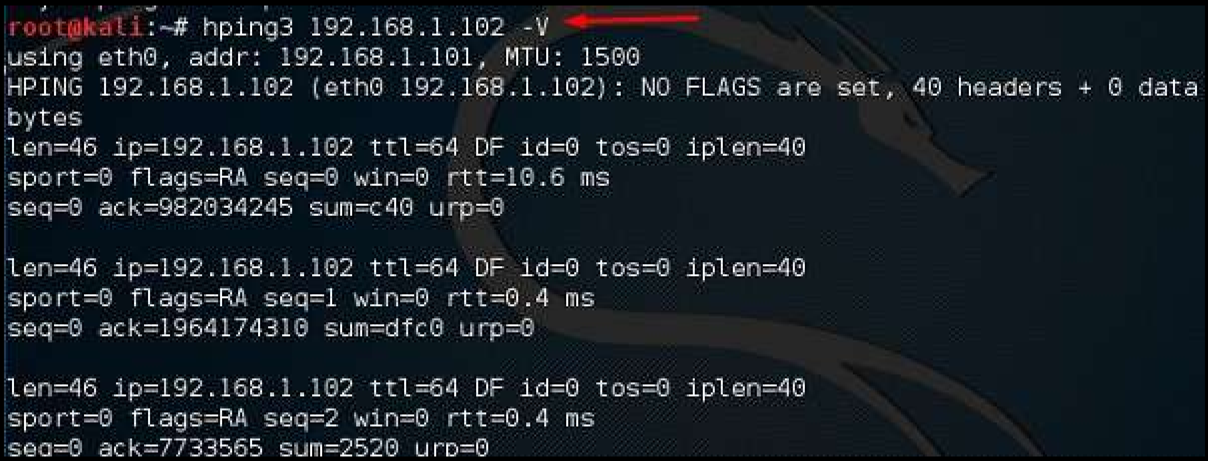
```
root@kali:~# dnsenum
```

Type “**hping3 –h”** which will show how to use this command.



```
root@kali:~# hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
```

The other command is “**hping3 domain or IP -parameter”**



```
root@kali:~# hping3 192.168.1.102 -V
using eth0, addr: 192.168.1.101, MTU: 1500
HPING 192.168.1.102 (eth0 192.168.1.102): NO FLAGS are set, 40 headers + 0 data
bytes
len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=0 win=0 rtt=10.6 ms
seq=0 ack=982034245 sum=c40 urp=0

len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=1 win=0 rtt=0.4 ms
seq=0 ack=1964174310 sum=dfc0 urp=0

len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=2 win=0 rtt=0.4 ms
seq=0 ack=7733565 sum=2520 urp=0
```