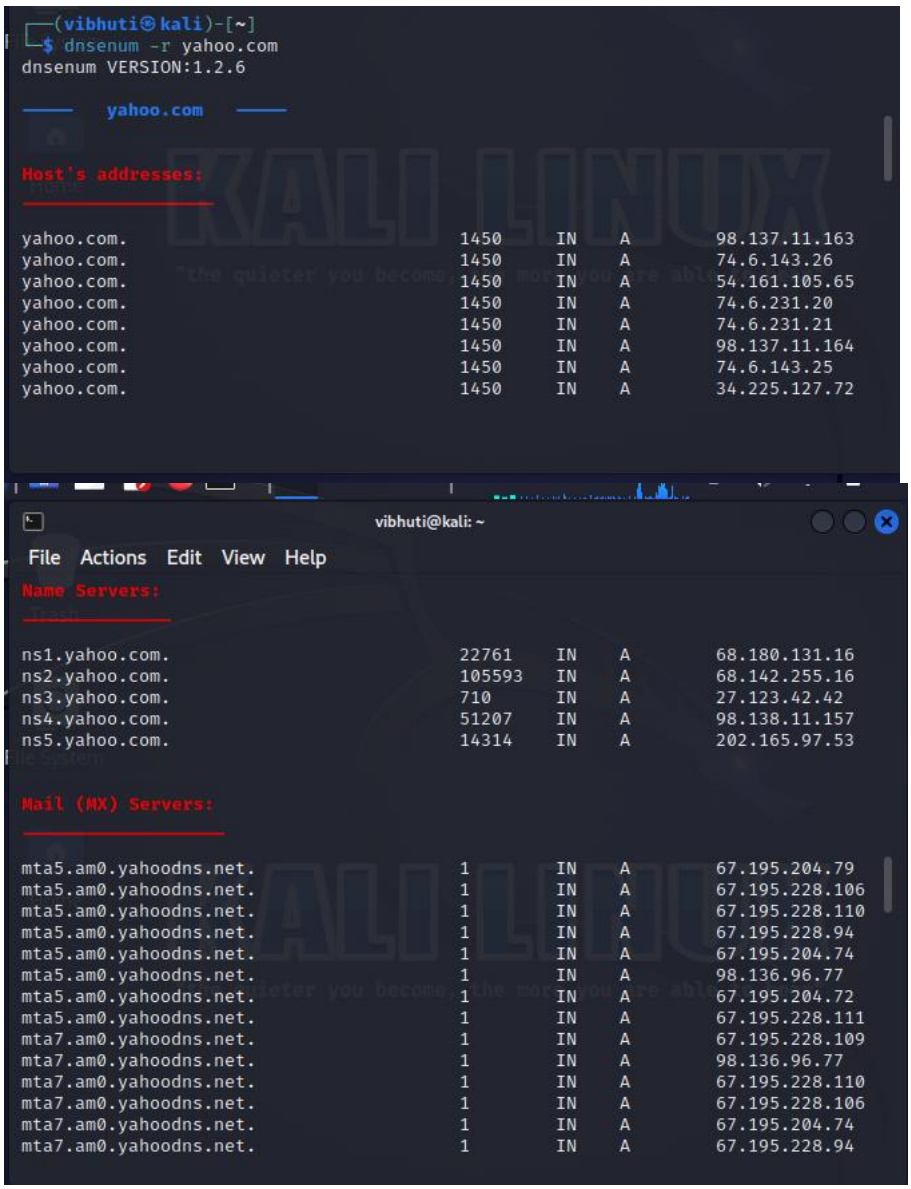
EXPLORING KALI LINUX TOOLS

1.Information Gathering(Using DNS Analysis)



```
┌──(vibhuti㉿kali)-[~]
└─$ dnsenum -r yahoo.com
dnsenum VERSION:1.2.6

-----   yahoo.com   -----

Host's addresses:
__________________

yahoo.com.                           1450     IN    A        98.137.11.163
yahoo.com.                           1450     IN    A        74.6.143.26
yahoo.com.                           1450     IN    A        54.161.105.65
yahoo.com.                           1450     IN    A        74.6.231.20
yahoo.com.                           1450     IN    A        74.6.231.21
yahoo.com.                           1450     IN    A        98.137.11.164
yahoo.com.                           1450     IN    A        74.6.143.25
yahoo.com.                           1450     IN    A        34.225.127.72
```

vibhuti@kali: ~

File Actions Edit View Help

```
Name Servers:
_____________

ns1.yahoo.com.                       22761    IN    A        68.180.131.16
ns2.yahoo.com.                       105593   IN    A        68.142.255.16
ns3.yahoo.com.                       710      IN    A        27.123.42.42
ns4.yahoo.com.                       51207    IN    A        98.138.11.157
ns5.yahoo.com.                       14314    IN    A        202.165.97.53

Mail (MX) Servers:
__________________

mta5.am0.yahoodns.net.               1        IN    A        67.195.204.79
mta5.am0.yahoodns.net.               1        IN    A        67.195.228.106
mta5.am0.yahoodns.net.               1        IN    A        67.195.228.110
mta5.am0.yahoodns.net.               1        IN    A        67.195.228.94
mta5.am0.yahoodns.net.               1        IN    A        67.195.204.74
mta5.am0.yahoodns.net.               1        IN    A        98.136.96.77
mta5.am0.yahoodns.net.               1        IN    A        67.195.204.72
mta5.am0.yahoodns.net.               1        IN    A        67.195.228.111
mta7.am0.yahoodns.net.               1        IN    A        67.195.228.109
mta7.am0.yahoodns.net.               1        IN    A        98.136.96.77
mta7.am0.yahoodns.net.               1        IN    A        67.195.228.110
mta7.am0.yahoodns.net.               1        IN    A        67.195.228.106
mta7.am0.yahoodns.net.               1        IN    A        67.195.204.74
mta7.am0.yahoodns.net.               1        IN    A        67.195.228.94
```

```
mta6.am0.yahoodns.net.          1       IN    A       67.195.228.110
mta6.am0.yahoodns.net.          1       IN    A       98.136.96.91
mta6.am0.yahoodns.net.          1       IN    A       67.195.228.106
mta6.am0.yahoodns.net.          1       IN    A       67.195.204.73
mta6.am0.yahoodns.net.          1       IN    A       67.195.204.79
mta6.am0.yahoodns.net.          1       IN    A       67.195.204.72
mta6.am0.yahoodns.net.          1       IN    A       67.195.204.74

Trying Zone Transfers and getting Bind Versions:
________________________________________________


Trying Zone Transfer for yahoo.com on ns4.yahoo.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for yahoo.com on ns2.yahoo.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for yahoo.com on ns5.yahoo.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for yahoo.com on ns1.yahoo.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for yahoo.com on ns3.yahoo.com ...
AXFR record query failed: REFUSED
```

vibhuti@kali: ~

File Actions Edit View Help

```
Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

about.yahoo.com.                        1800    IN    CNAME   rc.yahoo.com.
rc.yahoo.com.                           205     IN    CNAME   src.g03.yahoodn
s.net.
src.g03.yahoodns.net.                   205     IN    A       18.136.37.69
src.g03.yahoodns.net.                   205     IN    A       106.10.248.150
src.g03.yahoodns.net.                   205     IN    A       13.251.69.97
accounts.yahoo.com.                     1800    IN    CNAME   rc.yahoo.com.
rc.yahoo.com.                           204     IN    CNAME   src.g03.yahoodn
s.net.
src.g03.yahoodns.net.                   204     IN    A       13.251.69.97
src.g03.yahoodns.net.                   204     IN    A       18.136.37.69
src.g03.yahoodns.net.                   204     IN    A       106.10.248.150
admin.yahoo.com.                        298     IN    CNAME   admin.my.lga1.b
.yahoo.com.
ads.yahoo.com.                          51      IN    CNAME   edge.gycpi.b.ya
hoodns.net.
edge.gycpi.b.yahoodns.net.              60      IN    A       27.123.42.204
edge.gycpi.b.yahoodns.net.              60      IN    A       27.123.42.205
adserver.yahoo.com.                     1154    IN    CNAME   global1.adserve
r.gysm.yahoodns.net.
global1.adserver.gysm.yahoodns.net.     300     IN    A       202.165.106.31
asia.yahoo.com.                         300     IN    CNAME   rc.yahoo.com.
```

```
vpn.yahoo.com.                  1800    IN    CNAME    ciscovpn-ex.cor
p.yahoo.com.
w.yahoo.com.                    1800    IN    CNAME    rc.yahoo.com.
rc.yahoo.com.                   241     IN    CNAME    src.g03.yahoodn
s.net.
src.g03.yahoodns.net.           281     IN    A        13.251.69.97
src.g03.yahoodns.net.           281     IN    A        18.136.37.69
src.g03.yahoodns.net.           281     IN    A        106.10.248.150
website.yahoo.com.              1800    IN    A        66.218.85.160
ww.yahoo.com.                   1800    IN    CNAME    rc.yahoo.com.
rc.yahoo.com.                   232     IN    CNAME    src.g03.yahoodn
s.net.
src.g03.yahoodns.net.           272     IN    A        106.10.248.150
src.g03.yahoodns.net.           272     IN    A        13.251.69.97
src.g03.yahoodns.net.           272     IN    A        18.136.37.69
www.yahoo.com.                  52      IN    CNAME    new-fp-shed.wg1
.b.yahoo.com.
new-fp-shed.wg1.b.yahoo.com.    12      IN    A        202.165.107.50
new-fp-shed.wg1.b.yahoo.com.    12      IN    A        202.165.107.49
wwww.yahoo.com.                 1732    IN    CNAME    rc.yahoo.com.
rc.yahoo.com.                   232     IN    CNAME    src.g03.yahoodn
s.net.
src.g03.yahoodns.net.           272     IN    A        106.10.248.150
src.g03.yahoodns.net.           272     IN    A        13.251.69.97
src.g03.yahoodns.net.           272     IN    A        18.136.37.69
```

File Actions Edit View Help

Performing recursion:

```
─── Checking subdomains NS records ───

Can't perform recursion no NS records.
```

yahoo.com class C netranges:

```
1.1.1.0/24
27.123.42.0/24
34.225.127.0/24
54.161.105.0/24
66.218.85.0/24
68.142.196.0/24
68.142.255.0/24
68.180.131.0/24
74.6.136.0/24
74.6.143.0/24
74.6.231.0/24
98.136.103.0/24
98.137.11.0/24
98.138.11.0/24
106.10.218.0/24
```

```
File  Actions  Edit  View  Help

Performing reverse lookup on 5376 ip addresses:
```

0.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
1.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
2.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
3.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
4.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
5.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
6.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
7.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
8.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
9.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
10.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
11.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c

```
File  Actions  Edit  View  Help
```

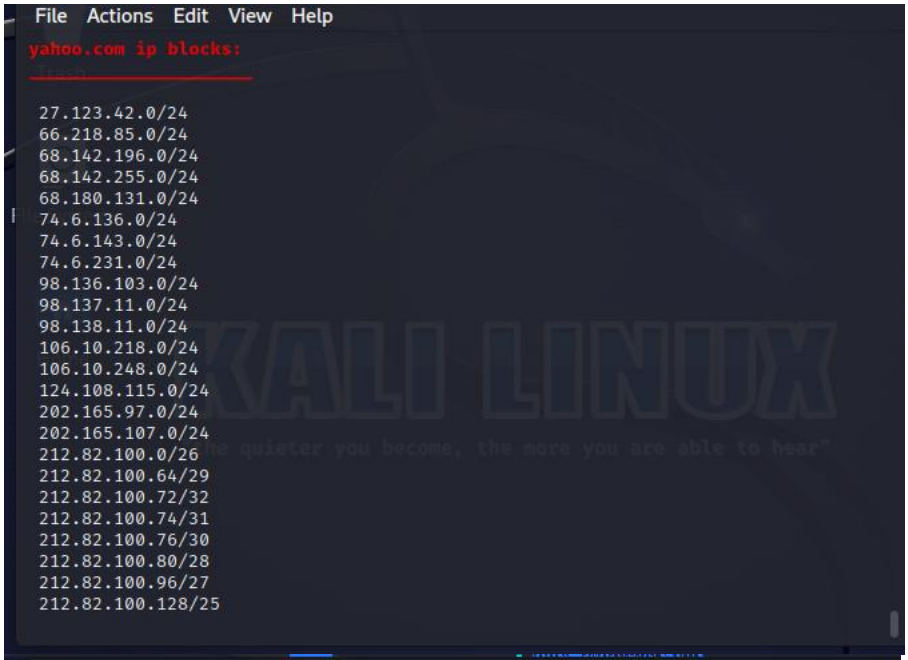
12.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
13.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
14.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
15.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
16.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
17.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
18.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
19.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
20.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
21.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
22.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
23.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
24.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
25.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c

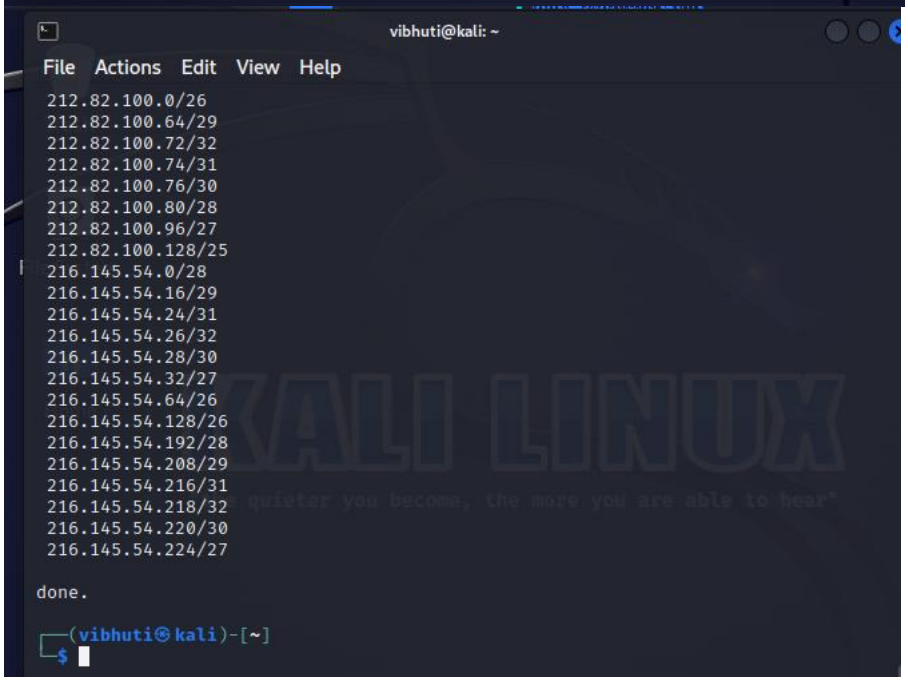
26.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
27.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
28.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
29.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
30.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
31.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
32.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
33.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
34.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
35.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
36.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
37.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.
38.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.com.

```
39.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
40.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
41.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
42.42.123.27.in-addr.arpa.      600     IN      PTR     ns3.yahoo.com.
43.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
44.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
45.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
46.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
47.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
48.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
49.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
50.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
51.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
52.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.

53.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
54.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
55.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
56.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
57.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
58.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
59.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
60.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
61.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
62.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
63.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
64.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
65.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
66.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c

67.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
68.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
69.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
70.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
71.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
72.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
73.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
74.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
75.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
76.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
77.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
78.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
79.42.123.27.in-addr.arpa.      600     IN      PTR     unknown.yahoo.c
om.
```

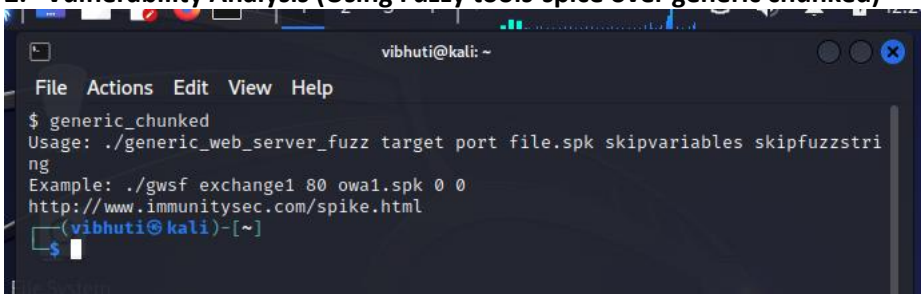
```
80.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
81.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
82.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
83.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
84.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
85.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
86.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
87.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
88.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
89.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
90.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
91.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
92.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
93.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c

94.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
95.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
96.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
97.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
98.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
99.42.123.27.in-addr.arpa.              600     IN      PTR     unknown.yahoo.c
om.
100.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
101.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
102.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
103.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
104.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
105.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
106.42.123.27.in-addr.arpa.             600     IN      PTR     unknown.yahoo.c
om.
```

```
File  Actions  Edit  View  Help
107.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
108.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
109.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
110.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
111.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
112.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
113.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
114.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
115.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
116.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
117.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
118.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
119.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
120.255.142.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c

251.131.180.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
252.131.180.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
253.131.180.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
254.131.180.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
255.131.180.68.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
0.136.6.74.in-addr.arpa.                600     IN    PTR     et19-1.fab8-1-g
dc.bf2.yahoo.com.
1.136.6.74.in-addr.arpa.                600     IN    PTR     et32.usw1-1-lba
.bf2.yahoo.com.
2.136.6.74.in-addr.arpa.                600     IN    PTR     et20-1.fab8-1-g
dc.bf2.yahoo.com.
3.136.6.74.in-addr.arpa.                600     IN    PTR     et32.usw2-1-lba
.bf2.yahoo.com.
4.136.6.74.in-addr.arpa.                600     IN    PTR     et19-1.fab7-1-g
dc.bf2.yahoo.com.
5.136.6.74.in-addr.arpa.                600     IN    PTR     et31.usw1-1-lba
.bf2.yahoo.com.
6.136.6.74.in-addr.arpa.                600     IN    PTR     et20-1.fab7-1-g
dc.bf2.yahoo.com.
7.136.6.74.in-addr.arpa.                600     IN    PTR     et31.usw2-1-lba
.bf2.yahoo.com.

251.54.145.216.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
252.54.145.216.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
253.54.145.216.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
254.54.145.216.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.
255.54.145.216.in-addr.arpa.            600     IN    PTR     unknown.yahoo.c
om.

4605 results out of 5376 IP addresses.
```

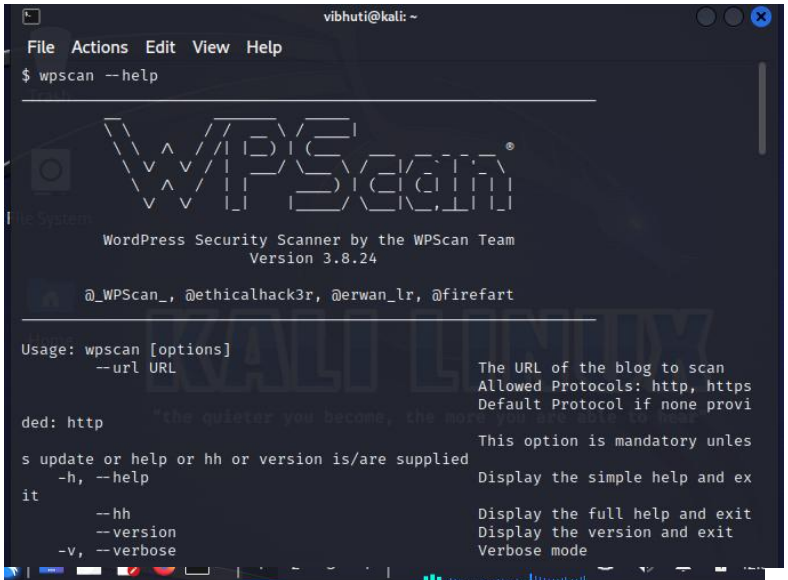


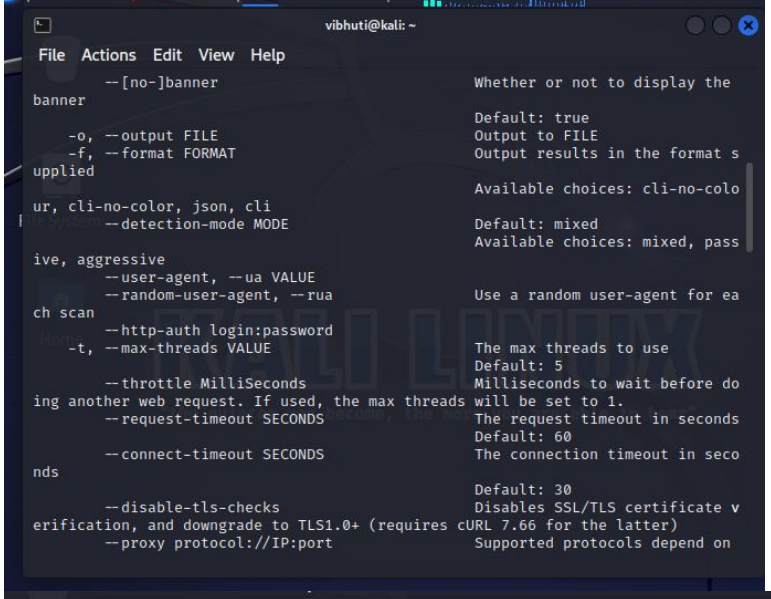


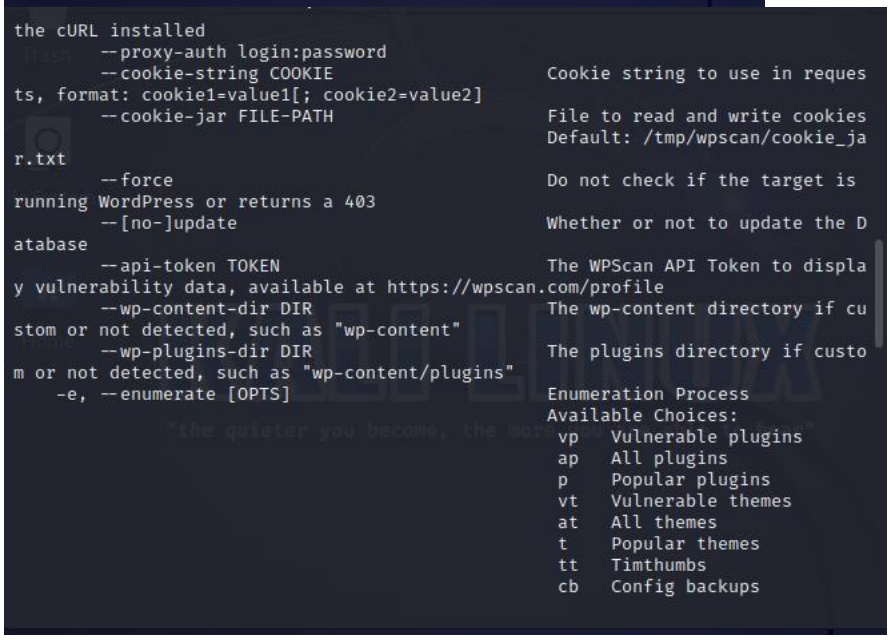
2. **Vulnerability Analysis (Using Fuzzy tools-spice over generic chunked)**

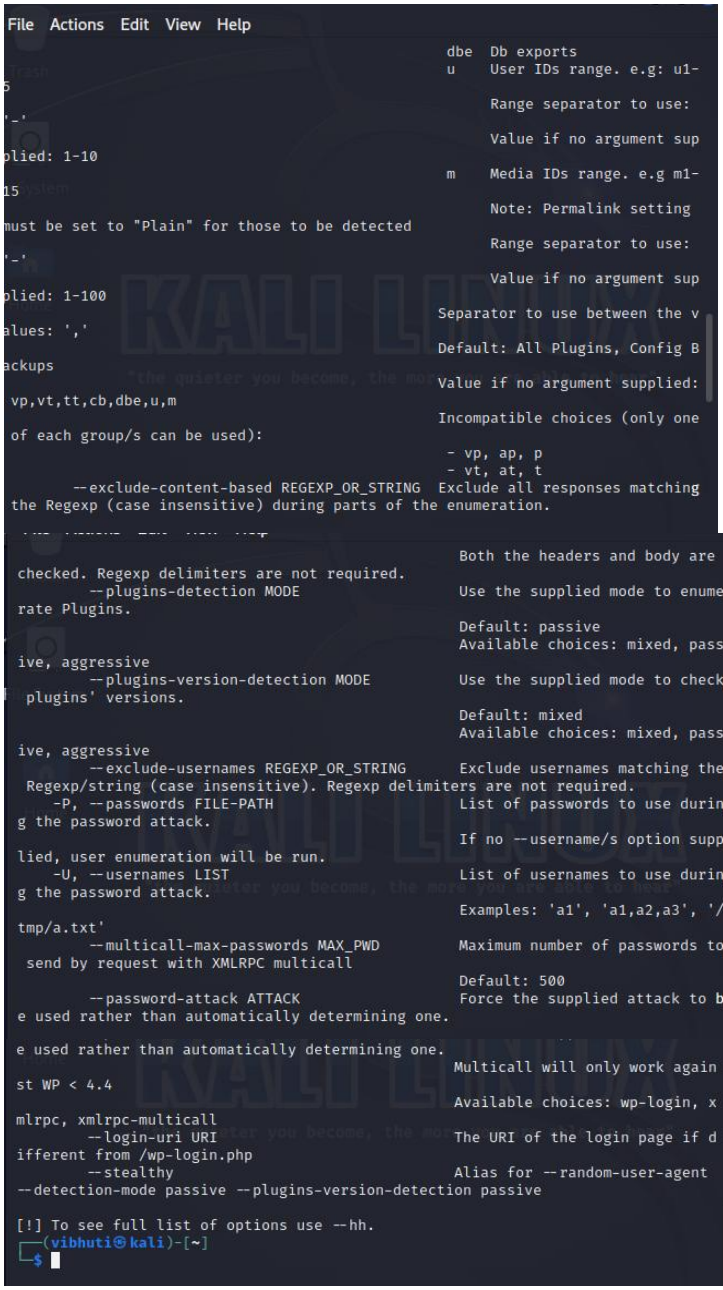


3. **Web Application Analysis(USING CMS & Framework Identification -wpscan)**

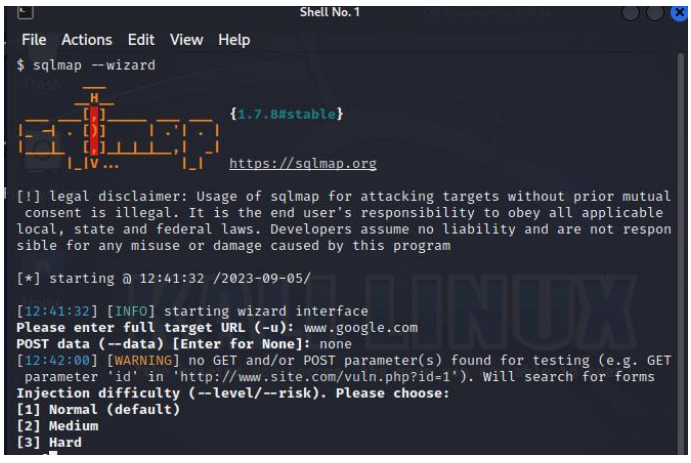

vibhuti@kali: ~
File Actions Edit View Help
$ wpscan --help
WordPress Security Scanner by the WPScan Team
Version 3.8.24
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
Usage: wpscan [options]
--url URL
The URL of the blog to scan
Allowed Protocols: http, https
Default Protocol if none provi
ded: http
This option is mandatory unles
s update or help or hh or version is/are supplied
-h, --help
Display the simple help and ex
it
--hh
Display the full help and exit
--version
Display the version and exit
-v, --verbose
Verbose mode


vibhuti@kali: ~
File Actions Edit View Help
--[no-]banner
Whether or not to display the
banner
Default: true
-o, --output FILE
Output to FILE
-f, --format FORMAT
Output results in the format s
upplied
Available choices: cli-no-colo
ur, cli-no-color, json, cli
--detection-mode MODE
Default: mixed
Available choices: mixed, pass
ive, aggressive
--user-agent, --ua VALUE
--random-user-agent, --rua
Use a random user-agent for ea
ch scan
--http-auth login:password
-t, --max-threads VALUE
The max threads to use
Default: 5
--throttle MilliSeconds
Milliseconds to wait before do
ing another web request. If used, the max threads will be set to 1.
--request-timeout SECONDS
The request timeout in seconds
Default: 60
--connect-timeout SECONDS
The connection timeout in seco
nds
Default: 30
--disable-tls-checks
Disables SSL/TLS certificate v
erification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)
--proxy protocol://IP:port
Supported protocols depend on


the cURL installed
--proxy-auth login:password
--cookie-string COOKIE
Cookie string to use in reques
ts, format: cookie1=value1[; cookie2=value2]
--cookie-jar FILE-PATH
File to read and write cookies
Default: /tmp/wpscan/cookie_ja
r.txt
--force
Do not check if the target is
running WordPress or returns a 403
--[no-]update
Whether or not to update the D
atabase
--api-token TOKEN
The WPScan API Token to displa
y vulnerability data, available at https://wpscan.com/profile
--wp-content-dir DIR
The wp-content directory if cu
stom or not detected, such as "wp-content"
--wp-plugins-dir DIR
The plugins directory if custo
m or not detected, such as "wp-content/plugins"
-e, --enumerate [OPTS]
Enumeration Process
Available Choices:
vp Vulnerable plugins
ap All plugins
p Popular plugins
vt Vulnerable themes
at All themes
t Popular themes
tt Timthumbs
cb Config backups



4. Database Assessment(Using SQL maps)

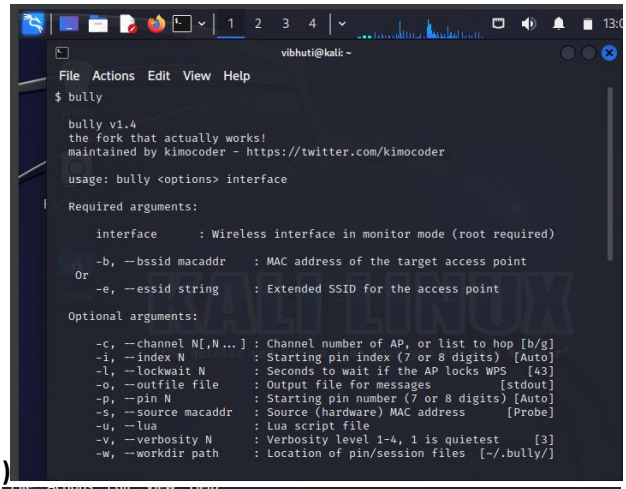


```
1
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 1

sqlmap is running, please wait..

[1/1] Form:
GET http://www.google.com/search?ie=ISO-8859-1&hl=en-IN&source=hp&biw=&bih=&q=&b
tnG=Google Search&iflsig=AD69kcEAAAAAZPdo2CcRwb7MYBirgY4Caeh-0UbeECCj&gbv=1
do you want to test this form? [Y/n/q]
> Y
Edit GET data [default: ie=ISO-8859-1&hl=en-IN&source=hp&biw=&bih=&q=&btnG=Googl
e Search&iflsig=AD69kcEAAAAAZPdo2CcRwb7MYBirgY4Caeh-0UbeECCj&gbv=1]: ie=ISO-8859
-1&hl=en-IN&source=hp&biw=&bih=&q=&btnG=Google Search&iflsig=AD69kcEAAAAAZPdo2Cc
Rwb7MYBirgY4Caeh-0UbeECCj&gbv=1
do you want to fill blank fields with random values? [Y/n] Y
you provided a HTTP Cookie header value, while target URL provides its own cooki
es within HTTP Set-Cookie header which intersect with yours. Do you want to merg
e them in further requests? [Y/n] Y
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
q
```

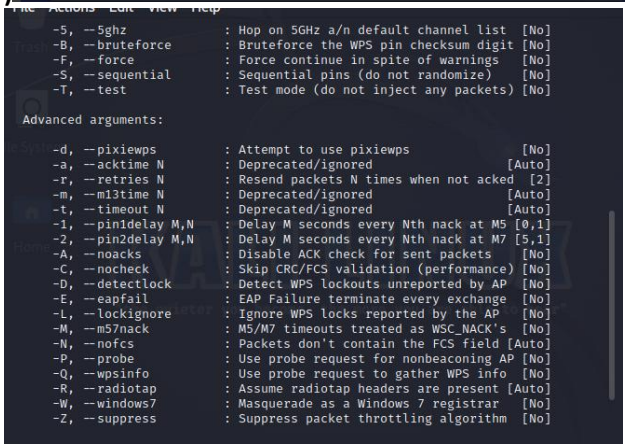
5. Password attacks(offline attacks)

```
vibhuti@kali: ~
File  Actions  Edit  View  Help
$ chntpw -h
chntpw: change password of a user in a Windows SAM file,
or invoke registry editor. Should handle both 32 and 64 bit windows and
all version from NT3.x to Win8.1
chntpw [OPTIONS] <samfile> [systemfile] [securityfile] [otherreghive] [ ... ]
 -h           This message
 -u <user>    Username or RID (0x3e9 for example) to interactively edit
 -l           list all users in SAM file and exit
 -i           Interactive Menu system
 -e           Registry editor. Now with full write support!
 -d           Enter buffer debugger instead (hex editor),
 -v           Be a little more verbose (for debuging)
 -L           For scripts, write names of changed files to /tmp/changed
 -N           No allocation mode. Only same length overwrites possible (very safe
 mode)
 -E           No expand mode, do not expand hive file (safe mode)

Usernames can be given as name or RID (in hex with 0x first)

See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.
NOTE: This program is somewhat hackish! You are on your own!
┌──(vibhuti㉿kali)-[~]
└─$
```

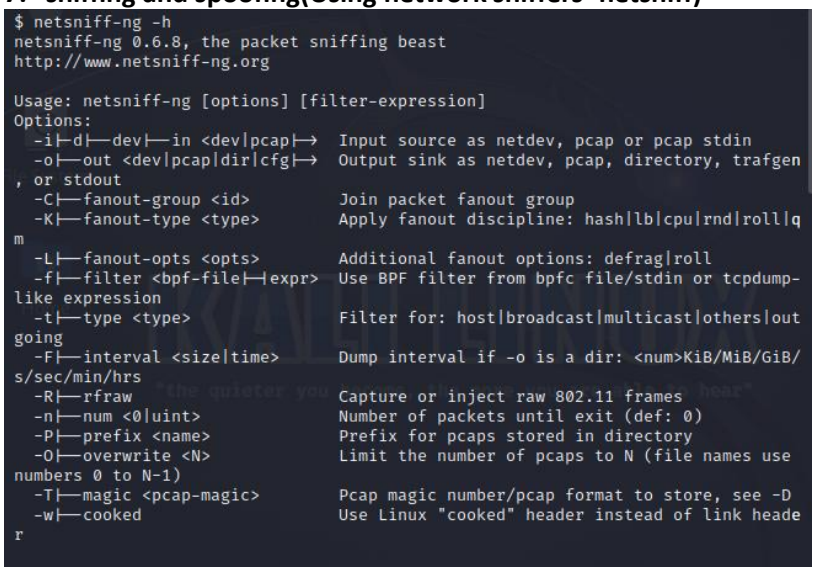
6. Wireless Attacks(Using wireless tools-



)



7. sniffing and spoofing(Using network sniffers- netsniff)



```
r
  -D├──dump-pcap-types           Dump pcap types and magic numbers and quit
  -B├──dump-bpf                  Dump generated BPF assembly
  -r├──rand                      Randomize packet forwarding order (dev→dev)
  -M├──no-promisc                No promiscuous mode for netdev
  -A├──no-sock-mem               Don't tune core socket memory
  -N├──no-hwtimestamp            Disable hardware time stamping
  -m├──mmap                      Mmap(2) pcap file I/O, e.g. for replaying pcaps
  -G├──sg                        Scatter/gather pcap file I/O
  -c├──clrw                      Use slower read(2)/write(2) I/O
  -S├──ring-size <size>          Specify ring size to: <num>KiB/MiB/GiB
  -k├──kernel-pull <uint>        Kernel pull from user interval in us (def: 10us
)
  -J├──jumbo-support             Support replay/fwd 64KB Super Jumbo Frames (def
: 2048B)
  -b├──bind-cpu <cpu>            Bind to specific CPU
  -u├──user <userid>             Drop privileges and change to userid
  -g├──group <groupid>           Drop privileges and change to groupid
  -H├──prio-high                 Make this high priority process
  -Q├──notouch-irq               Do not touch IRQ CPU affinity of NIC
  -s├──silent                    Do not print captured packets
  -q├──less                      Print less-verbose packet information
  -X├──hex                       Print packet data in hex format
  -l├──ascii                     Print human-readable packet data
  -U├──update                    Update GeoIP databases
  -V├──verbose                   Be more verbose
  -v├──version                   Show version and exit

Examples:
  netsniff-ng --in eth0 --out dump.pcap -s -T 0×a1b2c3d4 --bind-cpu 0 tcp or udp
  netsniff-ng --in wlan0 --rfraw --out dump.pcap --silent --bind-cpu 0
  netsniff-ng --in dump.pcap --mmap --out eth0 -k1000 --silent --bind-cpu 0
  netsniff-ng --in dump.pcap --out dump.cfg --silent --bind-cpu 0
  netsniff-ng --in dump.pcap --out dump2.pcap --silent tcp
  netsniff-ng --in eth0 --out eth1 --silent --bind-cpu 0 -J --type host
  netsniff-ng --in eth1 --out /opt/probe/ -s -m --interval 100MiB -b 0
  netsniff-ng --in vlan0 --out dump.pcap -c -u `id -u bob` -g `id -g bob`
  netsniff-ng --in any --filter http.bpf --jumbo-support --ascii -V

Note:
  For introducing bit errors, delays with random variation and more
  while replaying pcaps, make use of tc(8) with its disciplines (e.g. netem).

Please report bugs at https://github.com/netsniff-ng/netsniff-ng/issues
Copyright (C) 2009-2013 Daniel Borkmann <dborkma@tik.ee.ethz.ch>
Copyright (C) 2009-2012 Emmanuel Roullit <emmanuel.roullit@gmail.com>
Copyright (C) 2012 Markus Amend <markus@netsniff-ng.org>
Swiss federal institute of technology (ETH Zurich)
License: GNU GPL version 2.0
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
┌──(vibhuti㉿kali)-[~]
└─$
```