

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

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

System

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.yahoodns.net.
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.yahoodns.net.
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
www.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.

System

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

Performing reverse lookup on 5376 ip addresses:

0.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
1.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
2.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
3.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
4.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
5.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
6.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
7.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
8.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
9.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
10.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
11.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c
12.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
13.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
14.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
15.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
16.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
17.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
18.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
19.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
20.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
21.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
22.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
23.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
24.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
25.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c
26.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
27.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
28.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
29.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
30.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
31.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
32.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
33.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
34.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
35.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
36.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
37.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
38.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c

[illegible]

80.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
81.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
82.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
83.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
84.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
85.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
86.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
87.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
88.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
89.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
90.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
91.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
92.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
93.42.123.27.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c
94.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
95.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
96.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
97.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
98.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
99.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
100.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
101.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
102.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
103.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
104.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
105.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c
106.42.123.27.in-addr.arpa. om.	600	IN	PTR	unknown.yahoo.c

File	Actions	Edit	View	Help	
107.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
108.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
109.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
110.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
111.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
112.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
113.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
114.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
115.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
116.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
117.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
118.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
119.255.142.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
120.255.142.68.in-addr.arpa.	600	IN	PTR	unknown.yahoo.c	
251.131.180.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
252.131.180.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
253.131.180.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
254.131.180.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
255.131.180.68.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
0.136.6.74.in-addr.arpa.dc.bf2.yahoo.com.	600	IN	PTR	et19-1.fab8-1-g	
1.136.6.74.in-addr.arpa.bf2.yahoo.com.	600	IN	PTR	et32.usw1-1-lba	
2.136.6.74.in-addr.arpa.dc.bf2.yahoo.com.	600	IN	PTR	et20-1.fab8-1-g	
3.136.6.74.in-addr.arpa.bf2.yahoo.com.	600	IN	PTR	et32.usw2-1-lba	
4.136.6.74.in-addr.arpa.dc.bf2.yahoo.com.	600	IN	PTR	et19-1.fab7-1-g	
5.136.6.74.in-addr.arpa.bf2.yahoo.com.	600	IN	PTR	et31.usw1-1-lba	
6.136.6.74.in-addr.arpa.dc.bf2.yahoo.com.	600	IN	PTR	et20-1.fab7-1-g	
7.136.6.74.in-addr.arpa.bf2.yahoo.com.	600	IN	PTR	et31.usw2-1-lba	
251.54.145.216.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
252.54.145.216.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
253.54.145.216.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
254.54.145.216.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	
255.54.145.216.in-addr.arpa.om.	600	IN	PTR	unknown.yahoo.c	

4605 results out of 5376 IP addresses.

```
File Actions Edit View Help
yahoo.com ip blocks:
27.123.42.0/24
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
106.10.248.0/24
124.108.115.0/24
202.165.97.0/24
202.165.107.0/24
212.82.100.0/26
212.82.100.64/29
212.82.100.72/32
212.82.100.74/31
212.82.100.76/30
212.82.100.80/28
212.82.100.96/27
212.82.100.128/25

vibhuti@kali: ~
File Actions Edit View Help
212.82.100.0/26
212.82.100.64/29
212.82.100.72/32
212.82.100.74/31
212.82.100.76/30
212.82.100.80/28
212.82.100.96/27
212.82.100.128/25
216.145.54.0/28
216.145.54.16/29
216.145.54.24/31
216.145.54.26/32
216.145.54.28/30
216.145.54.32/27
216.145.54.64/26
216.145.54.128/26
216.145.54.192/28
216.145.54.208/29
216.145.54.216/31
216.145.54.218/32
216.145.54.220/30
216.145.54.224/27

done.
(vibhuti@kali)-[~]
$
```

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

```
vibhuti@kali: ~
File Actions Edit View Help
$ generic_chunked
Usage: ./generic_web_server_fuzz target port file.spk skipvariables skipfuzzstring
Example: ./gwsf exchange1 80 owa1.spk 0 0
http://www.immunitysec.com/spike.html
(vibhuti@kali)-[~]
$
```

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 provided: http
This option is mandatory unless update or help or hh or version is/are supplied
-h, --help Display the simple help and exit
--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 supplied
Available choices: cli-no-color, cli, cli-no-color, json, cli
--detection-mode MODE Default: mixed
Available choices: mixed, passive, aggressive
--user-agent, --ua VALUE Use a random user-agent for each scan
--random-user-agent, --random-user-agent, --ua VALUE
--http-auth login:password The max threads to use
-t, --max-threads VALUE Default: 5
--throttle Milliseconds Milliseconds to wait before doing 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 seconds
Default: 30
--disable-tls-checks Disables SSL/TLS certificate verification, 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 to use in requests
--cookie-string COOKIE
ts, format: cookie1=value1[; cookie2=value2]
--cookie-jar FILE-PATH File to read and write cookies
Default: /tmp/wpscan/cookie_jar.txt
--force Do not check if the target is running WordPress or returns a 403
--[no-]update Whether or not to update the Database
--api-token TOKEN The WPScan API Token to display vulnerability data, available at https://wpscan.com/profile
--wp-content-dir DIR The wp-content directory if custom or not detected, such as "wp-content"
--wp-plugins-dir DIR The plugins directory if custom 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

```

```

File Actions Edit View Help

dbs Db exports
u User IDs range. e.g: u1-100
Range separator to use:
Value if no argument supplied: 1-100
m Media IDs range. e.g m1-100
Note: Permalink setting
Range separator to use:
Value if no argument supplied: 1-100
Separator to use between the values: ','
Default: All Plugins, Config B
backups
Value if no argument supplied:
Incompatible choices (only one of each group/s can be used):
- vp, ap, p
- vt, at, t
--exclude-content-based REGEXP_OR_STRING Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration.

checked. Regexp delimiters are not required.
--plugins-detection MODE Use the supplied mode to enumerate Plugins.
Default: passive
Available choices: mixed, passive, aggressive
--plugins-version-detection MODE Use the supplied mode to check plugins' versions.
Default: mixed
Available choices: mixed, passive, aggressive
--exclude-usernames REGEXP_OR_STRING Exclude usernames matching the Regexp/string (case insensitive). Regexp delimiters are not required.
-P, --passwords FILE-PATH List of passwords to use during the password attack.
If no --username/s option supplied, user enumeration will be run.
-U, --usernames LIST List of usernames to use during the password attack.
Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
--multicall-max-passwords MAX_PWD Maximum number of passwords to send by request with XMLRPC multicall
Default: 500
--password-attack ATTACK Force the supplied attack to be used rather than automatically determining one.
Multicall will only work again if WP < 4.4
Available choices: wp-login, xmlrpc, xmlrpc-multicall
--login-uri URI The URI of the login page if different from /wp-login.php
--stealthy Alias for --random-user-agent
--detection-mode passive --plugins-version-detection passive

[!] To see full list of options use --hh.
(vibhuti@kali)~$

```

4. Database Assessment(Using SQL maps)

```

Shell No. 1
File Actions Edit View Help
$ sqlmap --wizard

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:41:32 /2023-09-05/

[12:41:32] [INFO] starting wizard interface
Please enter full target URL (-u): www.google.com
POST data (-data) [Enter for None]: none
[12:42:00] [WARNING] no GET and/or POST parameter(s) found for testing (e.g. GET parameter 'id' in 'http://www.site.com/vuln.php?id=1'). Will search for forms
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard

```

```
1
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 1
> 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=661h=6q=8b
tnG=Google Search&iflsig=AD69kcEAAAAZPdo2CcRwb7MYBirgY4Caeh-0UbeECCj8gbv=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=661h=6q=8b
tnG=Google Search&iflsig=AD69kcEAAAAZPdo2CcRwb7MYBirgY4Caeh-0UbeECCj8gbv=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 debugging)
-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-

```

vibhuti@kali:~$ bully
bully v1.4
the fork that actually works!
maintained by kimocoder - https://twitter.com/kimocoder

usage: bully <options> interface

Required arguments:

  interface      : Wireless interface in monitor mode (root required)

Or
  -b, --bssid macaddr : MAC address of the target access point
  -e, --essid string  : Extended SSID for the access point

Optional arguments:

  -c, --channel N[,N...] : Channel number of AP, or list to hop [b/g]
  -i, --index N           : Starting pin index (7 or 8 digits) [Auto]
  -l, --lockwait N        : Seconds to wait if the AP locks WPS [43]
  -o, --outfile file      : Output file for messages [stdout]
  -p, --pin N             : Starting pin number (7 or 8 digits) [Auto]
  -s, --source macaddr    : Source (hardware) MAC address [Probe]
  -u, --lua               : Lua script file
  -v, --verbosity N       : Verbosity level 1-4, 1 is quietest [3]
  -w, --workdir path      : Location of pin/session files [~/bully/]

  -S, --5ghz             : Hop on 5GHz a/n default channel list [No]
  -B, --bruteforce        : Bruteforce the WPS pin checksum digit [No]
  -F, --force             : Force continue in spite of warnings [No]
  -S, --sequential       : Sequential pins (do not randomize) [No]
  -T, --test              : Test mode (do not inject any packets) [No]

Advanced arguments:

  -d, --pixiewps          : Attempt to use pixiewps [No]
  -a, --acktime N         : Deprecated/ignored [Auto]
  -r, --retries N         : Resend packets N times when not acked [2]
  -m, --m13time N        : Deprecated/ignored [Auto]
  -t, --timeout N         : Deprecated/ignored [Auto]
  -1, --pin1delay M,N     : Delay M seconds every Nth nack at M5 [0,1]
  -2, --pin2delay M,N     : Delay M seconds every Nth nack at M7 [5,1]
  -A, --noacks            : Disable ACK check for sent packets [No]
  -C, --nocheck           : Skip CRC/FCS validation (performance) [No]
  -D, --detectlock        : Detect WPS lockouts unreported by AP [No]
  -E, --eapfail           : EAP Failure terminate every exchange [No]
  -L, --lockignore        : Ignore WPS locks reported by the AP [No]
  -M, --m57nack           : M5/M7 timeouts treated as WSC.NACK's [No]
  -N, --nofcs             : Packets don't contain the FCS field [Auto]
  -P, --probe             : Use probe request for nonbeaconing AP [No]
  -Q, --wpsinfo           : Use probe request to gather WPS info [No]
  -R, --radiotap          : Assume radiotap headers are present [Auto]
  -W, --windows7          : Masquerade as a Windows 7 registrar [No]
  -Z, --suppress          : Suppress packet throttling algorithm [No]

```

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

```

$ netsniff-ng -h
netsniff-ng 0.6.8, the packet sniffing beast
http://www.netsniff-ng.org

Usage: netsniff-ng [options] [filter-expression]

Options:
  -i|-d|--dev|-in <dev|pcap|> Input source as netdev, pcap or pcap stdin
  -o|--out <dev|pcap|dir|cfg|> Output sink as netdev, pcap, directory, trafgen
, or stdout
  -C|--fanout-group <id>      Join packet fanout group
  -K|--fanout-type <type>     Apply fanout discipline: hash|lbc|pulp|rnd|roll|q
m
  -L|--fanout-opts <opts>     Additional fanout options: defrag|roll
  -f|--filter <bpf-file|expr> Use BPF filter from bpf file/stdin or tcpdump-
like expression
  -t|--type <type>           Filter for: host|broadcast|multicast|others|out
going
  -F|--interval <size|time>   Dump interval if -o is a dir: <num>KiB/MiB/GiB/
s/sec/min/hrs
  -R|--rfraw                  Capture or inject raw 802.11 frames
  -n|--num <0|uint>          Number of packets until exit (def: 0)
  -P|--prefix <name>          Prefix for pcaps stored in directory
  -O|--overwrite <N>         Limit the number of pcaps to N (file names use
numbers 0 to N-1)
  -T|--magic <pcap-magic>     Pcap magic number/pcap format to store, see -D
  -w|--cooked                 Use Linux "cooked" header instead of link heade
r

```



```

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 0xa1b2c3d4 --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)-[~]

```
$
```