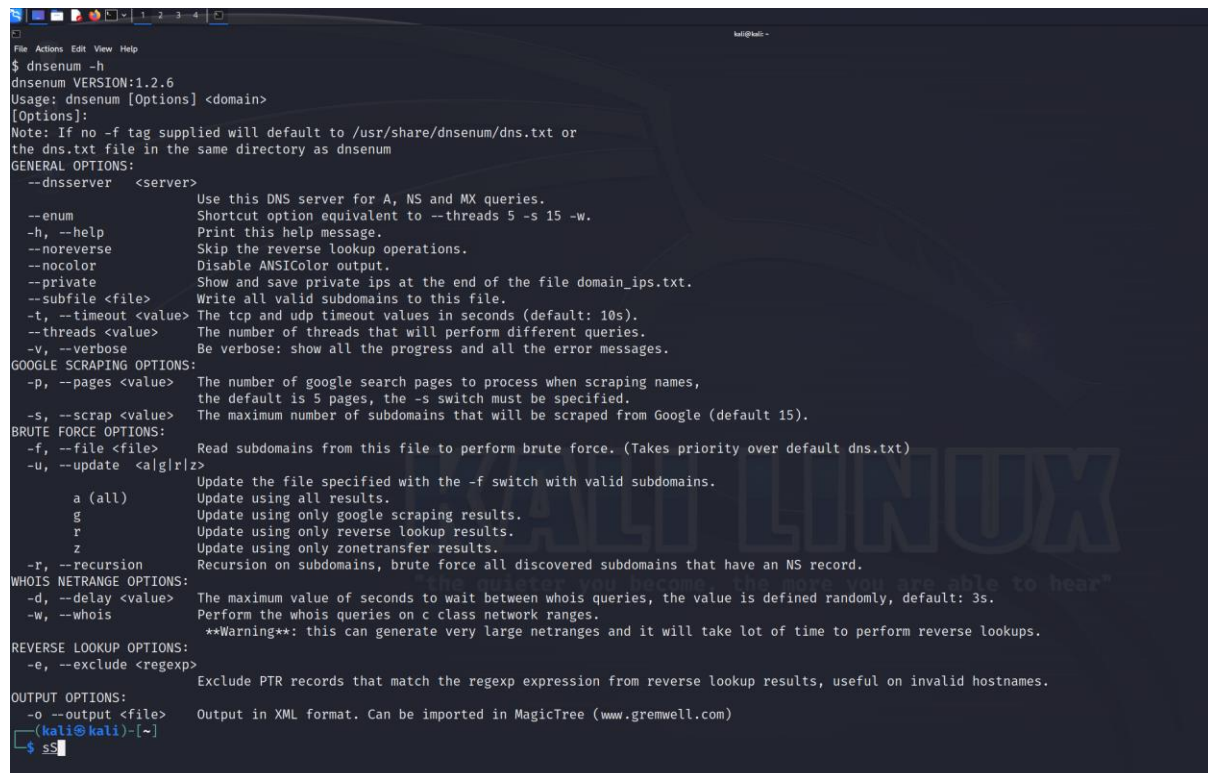


## ASSIGNMENT – 2

### AI for Cyber Security

#### 1: Information Gathering - DNS Analysis – DNSENUM

DNSenum is a powerful tool used for DNS analysis and information gathering in Kali Linux or other Linux distributions.



```
File Actions Edit View Help
$ dnstenum -h
dnstenum VERSION:1.2.6
Usage: dnstenum [Options] <domain>
[Options]:
Note: If no -f tag supplied will default to /usr/share/dnstenum/dns.txt or
the dns.txt file in the same directory as dnstenum
GENERAL OPTIONS:
--dnstserver <server>      Use this DNS server for A, NS and MX queries.
--enum                     Shortcut option equivalent to --threads 5 -s 15 -w.
-h, --help                 Print this help message.
--noreverse               Skip the reverse lookup operations.
--nocolor                 Disable ANSIColor output.
--private                 Show and save private ips at the end of the file domain_ips.txt.
--subfile <file>           Write all valid subdomains to this file.
-t, --timeout <value>     The tcp and udp timeout values in seconds (default: 10s).
--threads <value>         The number of threads that will perform different queries.
-v, --verbose              Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value>       The number of google search pages to process when scraping names,
                           the default is 5 pages, the -s switch must be specified.
-s, --scrap <value>       The maximum number of subdomains that will be scraped from Google (default 15).
BRUTE FORCE OPTIONS:
-f, --file <file>         Read subdomains from this file to perform brute force. (Takes priority over default dns.txt)
-u, --update <a|g|r|z>    Update the file specified with the -f switch with valid subdomains.
                           a (all)      Update using all results.
                           g             Update using only google scraping results.
                           r             Update using only reverse lookup results.
                           z             Update using only zonetransfer results.
-r, --recursion            Recursion on subdomains, brute force all discovered subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value>       The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois                Perform the whois queries on c class network ranges.
                           **Warning**: this can generate very large netranges and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex>     Exclude PTR records that match the regex expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o --output <file>        Output in XML format. Can be imported in MagicTree (www.gremwell.com)
(kali@kali)-[~]
$ ss
```

```
File Actions Edit View Help
-o --output <file>      Output in XML format. Can be imported in MagicTree (www.gremwell.com)
(kali@kali)-[~]
$ dnsenum --dnsserver 8.8.8.8 facebook.com
dnsenum VERSION:1.2.6

----- facebook.com -----

Host's addresses:

facebook.com.                300    IN     A      163.70.138.35

Name Servers:

c.ns.facebook.com.          1109   IN     A      185.89.218.12
b.ns.facebook.com.          10944  IN     A      129.134.31.12
a.ns.facebook.com.          10621  IN     A      129.134.30.12
d.ns.facebook.com.          21106  IN     A      185.89.219.12

Mail (MX) Servers:

smtpin.vvv.facebook.com.    205    IN     A      66.220.149.251

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for facebook.com on c.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on b.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out

Trying Zone Transfer for facebook.com on d.ns.facebook.com ...
AXFR record query failed: corrupt packet

Route forcing with /usr/share/dnsenum/dns.txt:
```

```
File Actions Edit View Help

Route forcing with /usr/share/dnsenum/dns.txt:

about.facebook.com.          116    IN     CNAME  www.facebook.com.
www.facebook.com.            3600   IN     CNAME  star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 60      IN     A      163.70.138.35
ads.facebook.com.            3600   IN     CNAME  www.facebook.com.
www.facebook.com.            2674   IN     CNAME  star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 60      IN     A      163.70.138.35
afa.facebook.com.            3600   IN     CNAME  star.facebook.com.
star.facebook.com.            3439   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
apps.facebook.com.           3178   IN     CNAME  star.facebook.com.
star.facebook.com.            3382   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
asia.facebook.com.            3600   IN     CNAME  star.facebook.com.
star.facebook.com.            3589   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
bc.facebook.com.              3600   IN     CNAME  star.facebook.com.
star.facebook.com.            2206   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       54      IN     A      163.70.138.9
beta.facebook.com.           300     IN     CNAME  latest.c10r.facebook.com.
latest.c10r.facebook.com.     60      IN     A      163.70.138.5
blog.facebook.com.            12     IN     CNAME  star.facebook.com.
star.facebook.com.            3353   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
c.facebook.com.               3600   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
c10r.facebook.com.            3600   IN     CNAME  star.facebook.com.
star.facebook.com.            3178   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
d.facebook.com.               3350   IN     CNAME  z-m.facebook.com.
z-m.facebook.com.             3345   IN     CNAME  z-m.c10r.facebook.com.
z-m.c10r.facebook.com.        60      IN     A      163.70.138.36
dev.facebook.com.             7200   IN     CNAME  intern-regional.vvv.facebook.com.
intern-regional.vvv.facebook.com. 300    IN     A      10.110.231.12
development.facebook.com.     3600   IN     CNAME  star.facebook.com.
star.facebook.com.            2927   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
diplomatic.facebook.com.      3600   IN     CNAME  star.facebook.com.
star.facebook.com.            3118   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
dns.facebook.com.             3600   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
es.facebook.com.              3600   IN     CNAME  star.facebook.com.
star.facebook.com.            3579   IN     CNAME  star.c10r.facebook.com.
star.c10r.facebook.com.       60      IN     A      163.70.138.9
```

```
File Actions Edit View Help
facebook.com class C netranges:

31.13.79.0/24
66.220.149.0/24
129.134.30.0/24
129.134.31.0/24
157.240.16.0/24
163.70.138.0/24
185.89.218.0/24
185.89.219.0/24

Performing reverse lookup on 2048 ip addresses:

1.79.13.31.in-addr.arpa.      3600   IN     PTR     (
2.79.13.31.in-addr.arpa.      3600   IN     PTR     edge-dgw-shv-02-bom1.facebook.com.
7.79.13.31.in-addr.arpa.      3600   IN     PTR     edge-atlas-shv-02-bom1.facebook.com.
8.79.13.31.in-addr.arpa.      3600   IN     PTR     edge-extern-shv-02-bom1.facebook.com.
9.79.13.31.in-addr.arpa.      3600   IN     PTR     edge-latest-shv-02-bom1.facebook.com.
10.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-mqtt-shv-02-bom1.facebook.com.
11.79.13.31.in-addr.arpa.     3600   IN     PTR     (
12.79.13.31.in-addr.arpa.     3600   IN     PTR     (
13.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-secure-shv-02-bom1.facebook.com.
14.79.13.31.in-addr.arpa.     3600   IN     PTR     (
15.79.13.31.in-addr.arpa.     3600   IN     PTR     (
16.79.13.31.in-addr.arpa.     3600   IN     PTR     (
17.79.13.31.in-addr.arpa.     3600   IN     PTR     (
18.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-star-shv-02-bom1.facebook.com.
21.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-z-p1-shv-02-bom1.facebook.com.
22.79.13.31.in-addr.arpa.     3600   IN     PTR     (
25.79.13.31.in-addr.arpa.     3600   IN     PTR     (
27.79.13.31.in-addr.arpa.     3600   IN     PTR     (
28.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-stun-shv-02-bom1.facebook.com.
29.79.13.31.in-addr.arpa.     3600   IN     PTR     (
31.79.13.31.in-addr.arpa.     3600   IN     PTR     (
32.79.13.31.in-addr.arpa.     3600   IN     PTR     (
33.79.13.31.in-addr.arpa.     3600   IN     PTR     (
35.79.13.31.in-addr.arpa.     3600   IN     PTR     (
36.79.13.31.in-addr.arpa.     3600   IN     PTR     (
37.79.13.31.in-addr.arpa.     3600   IN     PTR     (
39.79.13.31.in-addr.arpa.     3600   IN     PTR     (
40.79.13.31.in-addr.arpa.     3600   IN     PTR     (
41.79.13.31.in-addr.arpa.     3600   IN     PTR     (
42.79.13.31.in-addr.arpa.     3600   IN     PTR     (
48.79.13.31.in-addr.arpa.     3600   IN     PTR     (
51.79.13.31.in-addr.arpa.     3600   IN     PTR     edge-z-p3-shv-02-bom1.facebook.com.
```

```
File Actions Edit View Help
facebook.com ip blocks:

31.13.79.1/32
31.13.79.2/32
31.13.79.7/32
31.13.79.8/29
31.13.79.16/31
31.13.79.18/32
31.13.79.21/32
31.13.79.22/32
31.13.79.25/32
31.13.79.27/32
31.13.79.28/31
31.13.79.31/32
31.13.79.32/31
31.13.79.35/32
31.13.79.36/31
31.13.79.39/32
31.13.79.40/31
31.13.79.42/32
31.13.79.48/32
31.13.79.51/32
31.13.79.52/32
31.13.79.54/31
31.13.79.56/30
31.13.79.128/31
31.13.79.131/32
31.13.79.133/32
31.13.79.134/31
31.13.79.136/32
31.13.79.160/32
31.13.79.168/30
31.13.79.173/32
31.13.79.175/32
31.13.79.192/29
31.13.79.200/31
31.13.79.205/32
31.13.79.206/31
31.13.79.208/28
66.220.149.251/32
66.220.149.254/32
129.134.30.11/32
129.134.30.12/32
129.134.31.11/32
129.134.31.12/32
157.240.16.2/32
```

Brute forcing in DNS enumeration involves attempting to discover subdomains or hostnames associated with a target domain by systematically trying different combinations of names. This can reveal hidden or undocumented subdomains that might be vulnerable to various types of attacks.

## 2: Vulnerability Analysis - Nikto

Nikto is an open-source web server vulnerability scanner that can help identify security issues and potential vulnerabilities in web servers and web applications.

```
File Actions Edit View Help
$ nikto -h
Option host requires an argument

Options:
  -ask+          Whether to ask about submitting updates
                  yes Ask about each (default)
                  no Don't ask, don't send
                  nute Don't ask, just send
  -check6        Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgierrors+    Scan these CGI dirs: 'none', 'all', or values like '/cgi/ /cgi-a/'
  -config+       Use this config file
  -display+      Turn on/off display outputs:
                  1 Show redirects
                  2 Show cookies received
                  3 Show all 200/OK responses
                  4 Show URLs which require authentication
                  D Debug output
                  E Display all HTTP errors
                  P Print progress to STDOUT
                  S Scrub output of IPs and hostnames
                  V Verbose output
  -dbcheck        Check database and other key files for syntax errors
  -evasion+       Encoding technique:
                  1 Random URI encoding (non-UTF8)
                  2 Directory self-reference (../)
                  3 Premature URI ending
                  4 Prepend long random string
                  5 Fake parameter
                  6 TAB as request spacer
                  7 Change the case of the URL
                  8 Use windows directory separator (\)
                  A Use a carriage return (0x0d) as a request spacer
                  B Use binary value 0x00 as a request spacer
  -followredirects Follow 3xx redirects to new location
  -format+        Save file (-o) format:
                  CSV Comma-separated-value
                  json JSON Format
                  html HTML Format
                  nmap Nessus NSE format
                  sql Generic SQL (see docs for schema)
                  txt Plain text
                  xml XML Format
                  (If not specified the format will be taken from the file extension passed to -output)
  -help           This help information
  -host+          Target host/URL
  -ids+           Host authentication to use, format is id:pass or id:pass:realm
  -ipv4+          IPv4 only
  -ipv6+          IPv6 only
  -key+           Client certificate key file
  -list-plugins+  List all available plugins, perform no testing
  -maxtime+       Maximum testing time per host (e.g., 1h, 60m, 3600s)
  -mutate+        Guess additional file names:
                  1 Test all files with all root directories
                  2 Guess for password file names
                  3 Enumerate user names via Apache (/user type requests)
                  4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/user type requests)
                  5 Attempt to brute force sub-domain names, assume that the host name is the parent domain
                  6 Attempt to guess directory names from the supplied dictionary file
  -mutate-options Provide information for mutates
  -noninteractive Disables interactive features
  -nolookup        Disables DNS lookups
  -nossl           Disables the use of SSL
  -noslash         Strip trailing slash from URL (e.g., '/admin/' to '/admin')
  -noads           Disables nikto attempting to guess a 404 page
  -option+         Over-ride an option in nikto.conf, can be issued multiple times
  -output+         Write output to this file ('-' for auto-name)

-ids+           Host authentication to use, format is id:pass or id:pass:realm
-ipv4+          IPv4 only
-ipv6+          IPv6 only
-key+           Client certificate key file
-list-plugins+  List all available plugins, perform no testing
-maxtime+       Maximum testing time per host (e.g., 1h, 60m, 3600s)
-mutate+        Guess additional file names:
1 Test all files with all root directories
2 Guess for password file names
3 Enumerate user names via Apache (/user type requests)
4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/user type requests)
5 Attempt to brute force sub-domain names, assume that the host name is the parent domain
6 Attempt to guess directory names from the supplied dictionary file
-mutate-options Provide information for mutates
-noninteractive Disables interactive features
-nolookup        Disables DNS lookups
-nossl           Disables the use of SSL
-noslash         Strip trailing slash from URL (e.g., '/admin/' to '/admin')
-noads           Disables nikto attempting to guess a 404 page
-option+         Over-ride an option in nikto.conf, can be issued multiple times
-output+         Write output to this file ('-' for auto-name)
```

```
File Actions Edit View Help
xml XML Format
(If not specified the format will be taken from the file extension passed to -output)
-help           This help information
-host+          Target host/URL
-ids+           Host authentication to use, format is id:pass or id:pass:realm
-ipv4+          IPv4 only
-ipv6+          IPv6 only
-key+           Client certificate key file
-list-plugins+  List all available plugins, perform no testing
-maxtime+       Maximum testing time per host (e.g., 1h, 60m, 3600s)
-mutate+        Guess additional file names:
1 Test all files with all root directories
2 Guess for password file names
3 Enumerate user names via Apache (/user type requests)
4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/user type requests)
5 Attempt to brute force sub-domain names, assume that the host name is the parent domain
6 Attempt to guess directory names from the supplied dictionary file
-mutate-options Provide information for mutates
-noninteractive Disables interactive features
-nolookup        Disables DNS lookups
-nossl           Disables the use of SSL
-noslash         Strip trailing slash from URL (e.g., '/admin/' to '/admin')
-noads           Disables nikto attempting to guess a 404 page
-option+         Over-ride an option in nikto.conf, can be issued multiple times
-output+         Write output to this file ('-' for auto-name)
-pause+         Pause between tests (seconds)
-plugins+        List of plugins to run (default: ALL)
-port+          Port to use (default 80)
-sslcert+       Client certificate file
-root+          Prepend root value to all requests, format is /directory
-save+          Save positive responses to this directory ('-' for auto-name)
-ssl           Force ssl mode on port
-tuning+        Scan tuning:
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (XSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
0 File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d Webservice
e Administrative Console
+ Reverse Tuning options (i.e., include all except specified)
-timeout+       Timeout for requests (default 10 seconds)
-headers+       Load only user databases, not the standard databases
-headers+       all Disable standard dbx and load only user dbx
-headers+       tests Disable only dbx tests and load web_tests
-headers+       Over-rides the default useragent
-until+          Run until the specified time or duration
-urls+          Target host/URL (alias of -host)
-usecookies+     Use cookies from responses in future requests
-useproxy+       Use the proxy defined in nikto.conf, or argument http://server:port
-version+       Print plugin and database versions
-vhost+         Virtual host (for Host header)
-verbose+       Ignore these HTTP codes as negative responses (always). Format is '302,301'
-verbosity+     Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value
```

```

kali@kali:~$ nikto -h pbs.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 54.225.198.196, 54.225.206.152
+ Target IP: 54.225.198.196
+ Target Hostname: pbs.org
+ Target Port: 443

+ SSL Info:
  Subject: /CN=www.pbs.org
  Ciphers: ECDHE-RSA-AES128-GCM-SHA256
  Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time: 2023-09-08 12:32:17 (GMT+4)

+ Server: openresty
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-pbs-fvsvname' found, with contents: ip-10-193-111-220.ec2.internal.
+ /: The site uses TLS and the Strict-Transport-Security MTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Post-req / redirects to: https://www.pbs.org/

```

### 3: Web Application Analysis - Whatweb

WhatWeb is an open-source web application fingerprinting tool used for web application analysis. It helps identify and gather information about web technologies, frameworks, and software components used in a given website or web application. By analyzing the response headers and page content, WhatWeb can provide valuable insights into the technologies and vulnerabilities present on a target web application.

```

kali@kali:~$ whatweb -h

WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).
Homepage: https://www.morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

TARGET SELECTION:
  <TARGETs>          Enter URLs, hostnames, IP addresses, filenames or
                    IP ranges in CIDR, x.x.x.x, or x.x.x.x-x.x.x.x
                    format.
  --input-file=FILE, -i Read targets from a file. You can pipe
                    hostnames or URLs directly with -i /dev/stdin.

TARGET MODIFICATION:
  --url-prefix        Add a prefix to target URLs.
  --url-suffix        Add a suffix to target URLs.
  --url-pattern        Insert the targets into a URL.
                    e.g. example.com/insert/robots.txt

AGGRESSION:
  The aggression level controls the trade-off between speed/stealth and
  reliability.
  --aggression, -a=LEVEL Set the aggression level. Default: 1.
  1. Stealthy           Makes one HTTP request per target and also
                    follows redirects.
  3. Aggressive         If a level 1 plugin is matched, additional
                    requests will be made.
  4. Heavy              Makes a lot of HTTP requests per target. URLs
                    from all plugins are attempted.

HTTP OPTIONS:
  --user-agent, -U=AGENT Identify as AGENT instead of WhatWeb/0.5.5.
  --header, -H           Add an HTTP header. eg "Foo:Bar". Specifying a
                    default header will replace it. Specifying an
                    empty value, e.g. "User-Agent:" will remove it.
  --follow-redirect=WHEN Control when to follow redirects. WHEN may be
                    'never', 'http-only', 'meta-only', 'same-site',
                    or 'always'. Default: always.
  --max-redirects=NUM    Maximum number of redirects. Default: 10.

AUTHENTICATION:
  --user, -u=user:password HTTP basic authentication.
  --cookie, -c=COOKIES     Use cookies, e.g. 'name=value; name2=value2'.

```

```

kali@kali:~$ whatweb google.com
http://google.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws], IP[142.250.77.174], RedirectLocation[http://www.google.com/], Title[301 Moved], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
http://www.google.com/ [200 OK] Cookies[1P_JAR;AEC;NID], Country[UNITED STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC;NID], IP[142.250.195.100], Script, Title[Google], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

```



## 4: Database Assessment - sqlmap

```
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 fed
[*] starting @ 11:52:39 /2023-09-06/
[11:52:39] [INFO] starting wizard interface

Please enter full target URL (-u): http://demo.testfire.net/

[11:53:02] [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
sqlmap is running, please wait..

[1/1] Form:
GET http://demo.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
Y
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[11:53:59] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect tha
t there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper-space2comment') and/or switch '--random-agent', skippi
ng to the next target

[*] ending @ 11:53:59 /2023-09-06/

~(kali@kali)-[~]
└─$ y
```

## 5: Password Attacks - John

John the Ripper, often referred to as simply "John," is a widely used open-source password cracking tool in Kali Linux and other security testing environments. It is designed for password attacks and can be used for various password-related tasks, including password cracking, auditing, and recovery.

The hacking done below is in wordlist mode.

```
File Actions Edit View Help
~(root@kali)-[~]
└─$ ls /usr/share/wordlists/
amass      fasttrack.txt  legion        rockyou.txt.gz  wifite.txt
dirb       fern-wifi     metasploit   sqlmap.txt
dirbuster  john.lst      nmap.lst     wfuzz

~(root@kali)-[~]
└─$ cd /usr/share/wordlists/

~(root@kali)-[/usr/share/wordlists]
└─$ gunzip rockyou.txt.gz

~(root@kali)-[/usr/share/wordlists]
└─$ cp rockyou.txt file1.txt

~(root@kali)-[/usr/share/wordlists]
└─$ cat file1.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
```

```

(root@kali)-[/usr/share/wordlists]
# echo -n '12345' | sha256sum
5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5 -

(root@kali)-[/usr/share/wordlists]
# echo -n 'password' | sha256sum
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -

(root@kali)-[/usr/share/wordlists]
# echo -n 'princess' | sha256sum
04e77bf8f95cb3e1a36a59d1e93857c411930db646b46c218a0352e432023cf2 -

(root@kali)-[/usr/share/wordlists]
# cat >> pass.txt
Pranavasri1:5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc
5
Pranavasri2:5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d
8
Pranavasri3:04e77bf8f95cb3e1a36a59d1e93857c411930db646b46c218a0352e432023cf
2
^C

(root@kali)-[/usr/share/wordlists]
# cat pass.txt
Pranavasri1:5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc
5
Pranavasri2:5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d
8
Pranavasri3:04e77bf8f95cb3e1a36a59d1e93857c411930db646b46c218a0352e432023cf
2

(root@kali)-[/usr/share/wordlists]
# john --format=raw-sha256 --wordlist=rockyou.txt pass.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA256 [SHA256 256/25
6 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345 (Pranavasri1)
password (Pranavasri2)
princess (Pranavasri3)
3g 0:00:00:00 DONE (2023-07-12 02:29) 75.00g/s 1638Kp/s 1638Kc/s 4915KC/s 1
23456..sabrina7

```

```

File Actions Edit View Help

(root@kali)-[/usr/share/wordlists]
# cat pass.txt
Pranavasri1:5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc
5
Pranavasri2:5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d
8
Pranavasri3:04e77bf8f95cb3e1a36a59d1e93857c411930db646b46c218a0352e432023cf
2

(root@kali)-[/usr/share/wordlists]
# john --format=raw-sha256 --wordlist=rockyou.txt pass.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA256 [SHA256 256/25
6 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345 (Pranavasri1)
password (Pranavasri2)
princess (Pranavasri3)
3g 0:00:00:00 DONE (2023-07-12 02:29) 75.00g/s 1638Kp/s 1638Kc/s 4915KC/s 1
23456..sabrina7
Use the "--show --format=Raw-SHA256" options to display all of the cracked
passwords reliably
Session completed.

(root@kali)-[/usr/share/wordlists]
#

```

## 6. Wireless Attacks – Wifite

Wifite is a popular tool for automating wireless attacks in Kali Linux. It simplifies the process of auditing wireless networks by automating tasks such as scanning, capturing handshakes, and performing dictionary-based or WPS PIN attacks on WPA/WPA2-encrypted Wi-Fi networks.

```
File Actions Edit View Help
$ wifite --help

wifite2 2.6.6
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

options:
-h, --help                show this help message and exit

SETTINGS:
-v, --verbose              Shows more options (-h -v). Prints commands and outputs. (default:
                           quiet)
-i [interface]             Wireless interface to use, e.g. wlan0mon (default: ask)
-c [channel]               Wireless channel to scan e.g. 1,11,6 (default: all 20M channels)
-inf, --infinite            Enable infinite attack mode. Modify scanning time with -p (default:
                           off)
-mac, --random-mac         Randomize wireless card MAC address (default: off)
-p [scan_time]             Pillage: Attack all targets after scan_time (seconds)
--kill                     Kill processes that conflict with Aircrack-ng/Airodump (default: off)
--power [min_power], --power [min_power] Attacks any targets with at least min_power signal strength
--skip-crack               Skip cracking captured handshakes/pmkid (default: off)
--first [attack_max], --first [attack_max] Attacks the first attack_max targets (default: off)
--ignore-cracked           Hides previously-cracked targets. (default: off)
--clients-only             Only show targets that have associated clients (default: off)
--noauth                  Passive mode: Never deauthenticates clients (default: deauth targets)
--daemon                  Puts device back in managed mode after quitting (default: off)

WEP:
--wep                      Show only WEP-encrypted networks
--require-fakeauth         Fails attacks if fake-auth fails (default: off)
--keep-ivs                 Retain .IVS files and reuse when cracking (default: off)

WPA:
--wpa                      Show only WPA-encrypted networks (includes WPS)
--new-hs                   Captures new handshakes, ignores existing handshakes in hs (default:
                           off)
--dict [file]              File containing passwords for cracking (default: /usr/share/dict/wordlist-
                           probable.txt)

WPS:
--wps                      Show only WPS-enabled networks
--wps-only                 Only use WPS PIN & Pixie-Dust attacks (default:
                           off)
--bully                    Use bully program for WPS PIN & Pixie-Dust attacks (default:
                           reaver)
--reaver                   Use reaver program for WPS PIN & Pixie-Dust attacks (default:
                           reaver)
--ignore-locks             Do not stop WPS PIN attack if AP becomes locked (default:
                           stop)

PMKID:
--pmkid                    Only use PMKID capture, avoids other WPS & WPA attacks (default:
                           off)
--no-pmkid                 Don't use PMKID capture (default: off)
--pmkid-timeout [sec]      Time to wait for PMKID capture (default: 300 seconds)

COMMANDS:
--cracked                  Print previously-cracked access points
--check [file]             Check a .cap file (or all hs/*.cap files) for WPA handshakes
--crack                    Show commands to crack a captured handshake
(kali@kali)-[~]
```

```
File Actions Edit View Help
--check [file]             Check a .cap file (or all hs/*.cap files) for WPA handshakes
--crack                    Show commands to crack a captured handshake
(kali@kali)-[~]
$ sudo wifite
[sudo] password for kali:

wifite2 2.6.6
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxcapngtool was not found. install @ apt install hcxtools
[!] Conflicting processes: NetworkManager (PID 528)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Checking aircrack-ng...
[!] aircrack-ng did not find any wireless interfaces
[!] Make sure your wireless device is connected
[!] See https://www.aircrack-ng.org/doku.php?id=aircrack-ng for more info

[!] Error: aircrack-ng did not find any wireless interfaces

[!] Full stack trace below

[!] Traceback (most recent call last):
[!]   File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 104, in entry_point
[!]     wifite.start()
[!]   File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 57, in start
[!]     Configuration.get_monitor_mode_interface()
[!]   File "/usr/lib/python3/dist-packages/wifite/config.py", line 228, in get_monitor_mode_interface
[!]     cls.interface = AircrackNg.ask()
[!]   File "/usr/lib/python3/dist-packages/wifite/tools/aircrack-ng.py", line 300, in ask
[!]     raise Exception('aircrack-ng did not find any wireless interfaces')
[!] Exception: aircrack-ng did not find any wireless interfaces

[!] Exiting
(kali@kali)-[~]
$
```



## 7. Reverse Engineering – Radare2

Radare2, often referred to as simply "r2," is a powerful open-source framework for reverse engineering and binary analysis. It provides a wide range of tools and features for analyzing, disassembling, debugging, and manipulating binary files, which can include executables, libraries, and firmware.

```
File Actions Edit View Help
$ radare2 -h
Usage: r2 [-ACdFLMnQsStuvwX] [-P patch] [-p prj] [-a arch] [-b bits] [-i file]
        [-s addr] [-B baddr] [-m maddr] [-c cmd] [-e k=v] file|pid|+|-|*
--
    run radare2 without opening any file
-
    same as 'r2 malloc://512'
+
    read file from stdin (use -i and -c to run cmds)
++
    perform ++! command to run all commands remotely
-o
    print \x00 after init and every command
-o2
    close stderr file descriptor (silent warning messages)
-a [arch]
    set asm.arch
-A
    run 'aaa' command to analyze all referenced code
-b [bits]
    set asm.bits
-B [baddr]
    set base address for PIE binaries
-c 'cmd..'
    execute radare command
-C
    file is host:port (alias for -c=http://%s/cmd/)
-d
    debug the executable 'file' or running process 'pid'
-D [backend]
    enable debug mode (e cfg.debug=true)
-e k=v
    evaluate config var
-f
    block size = file size
-F [binplug]
    force to use that rbin plugin
-h, -hh
    show help message, -hh for long
-H ([var])
    display variable
-i [file]
    run script file
-I [file]
    run script file before the file is opened
-j
    use json for -v, -L and maybe others
-k [OS/kern]
    set asm.os (linux, macos, w32, netbsd, ...)
-l [lib]
    load plugin file
-L
    list supported IO plugins
-m [addr]
    map file at given address (loadaddr)
-M
    do not demangle symbol names
-n, -nn
    do not load Rbin info (-nn only load bin structures)
-N
    do not load user settings and scripts
-NN
    do not load any script or plugin
-q
    quiet mode (no prompt) and quit after -i
-qq
    quit after running all -c and -i
-Q
    quiet mode (no prompt) and quit faster (quickLeak=true)
-p [prj]
    use project, list if no arg, load if no file
-P [file]
    apply rapatch file and quit
-r [rarun2]
    specify rarun2 profile to load (same as -e dbg.profile=X)
-R [rr2rule]
    specify custom rarun2 directive
-s [addr]
    initial seek
-S
    start r2 in sandbox mode
-T
    do not compute file hashes
-u
    set bin.filter=false to get raw sym/sec/cls names
-v, -V
    show radare2 version (-V show lib versions)
-w
    open file in write mode
```

```
File Actions Edit View Help
--pid=
    use pids between commands, when possible
--precompile=
    only precompile the input
(kali㉿kali)-[~]
$ rasm2 -d 90
nop
(kali㉿kali)-[~]
$ rasm2 "nop"
90
(kali㉿kali)-[~]
$
```

## 8. Exploitation tools – Searchsploit

Searchsploit is a powerful command-line tool used for searching and indexing exploits and vulnerabilities from various sources.

```
File Actions Edit View Help
$ searchsploit
Usage: searchsploit [options] term1 [term2] ... [termN]

Examples

searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)//dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | jq
searchsploit --cve 2021-44228

For more examples, see the manual: https://www.exploit-db.com/searchsploit

Options

## Search Terms
-c, --case [term]      Perform a case-sensitive search (Default is inSensITive)
-e, --exact [term]     Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "--t"]
                        e.g. "WordPress 4.1" would not be detected "WordPress Core 4.1")
-s, --strict           Perform a strict search, so input values must exist, disabling fuzzy search for version range
                        e.g. "1.1" would not be detected in "1.0 < 1.3")
-t, --title [term]     Search JUST the exploit title (Default is title AND the file's path)
                        --exclude="term" Remove values from results. By using "|" to separate, you can chain multiple values
                        e.g. --exclude="term1|term2|term3"
                        --cve [CVE]    Search for Common Vulnerabilities and Exposures (CVE) value

## Output
-j, --json [term]      Show result in JSON format
-o, --overflow [term]  Exploit titles are allowed to overflow their columns
-p, --path [EDB-ID]   Show the full path to an exploit (and also copies the path to the clipboard if possible)
-v, --verbose          Display more information in output
-w, --www [term]       Show URLs to Exploit-DB.com rather than the local path
-id                   Display the EDB-ID value rather than local path
--disable-colour       Disable colour highlighting in search results

## Non-Searching
-m, --mirror [EDB-ID]  Mirror (aka copies) an exploit to the current working directory
-x, --examine [EDB-ID] Examine (aka opens) the exploit using $PAGER

## Non-Searching
-h, --help             Show this help screen
-u, --update           Check for and install any exploitdb package updates (brew, deb & git)

## Automation
--nmap [file.xml]      Checks all results in Nmap's XML output with service version
                        e.g.: nmap [host] -sV -oX file.xml
```

```
File Actions Edit View Help
-t, --title [term]      e.g. "1.1" would not be detected in "1.0 < 1.3")
                        Search JUST the exploit title (Default is title AND the file's path)
--exclude="term"        Remove values from results. By using "|" to separate, you can chain multiple values
                        e.g. --exclude="term1|term2|term3"
--cve [CVE]             Search for Common Vulnerabilities and Exposures (CVE) value

## Output
-j, --json [term]       Show result in JSON format
-o, --overflow [term]   Exploit titles are allowed to overflow their columns
-p, --path [EDB-ID]     Show the full path to an exploit (and also copies the path to the clipboard if possible)
-v, --verbose           Display more information in output
-w, --www [term]        Show URLs to Exploit-DB.com rather than the local path
-id                     Display the EDB-ID value rather than local path
--disable-colour        Disable colour highlighting in search results

## Non-Searching
-m, --mirror [EDB-ID]   Mirror (aka copies) an exploit to the current working directory
-x, --examine [EDB-ID]  Examine (aka opens) the exploit using $PAGER

## Non-Searching
-h, --help             Show this help screen
-u, --update           Check for and install any exploitdb package updates (brew, deb & git)

## Automation
--nmap [file.xml]       Checks all results in Nmap's XML output with service version
                        e.g.: nmap [host] -sV -oX file.xml

Notes
* You can use any number of search terms
* By default, search terms are not case-sensitive, ordering is irrelevant, and will search between version ranges
* Use "-c" if you wish to reduce results by case-sensitive searching
* And/or "-e" if you wish to filter results by using an exact match
* And/or "-s" if you wish to look for an exact version match
* Use "-t" to exclude the file's path to filter the search results
* Remove false positives (especially when searching using numbers - i.e. versions)
* When using "--nmap", adding "-v" (verbose), it will search for even more combinations
* When updating or displaying help, search terms will be ignored

(kali@kali):~$ searchsploit wordpress mail list

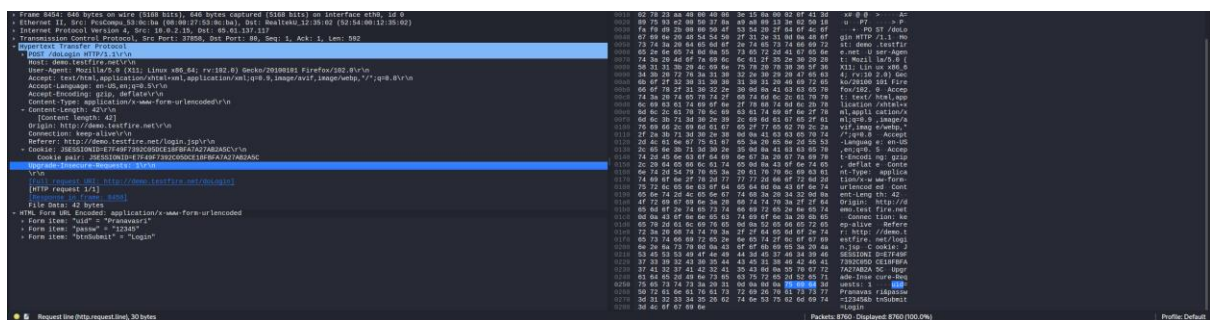
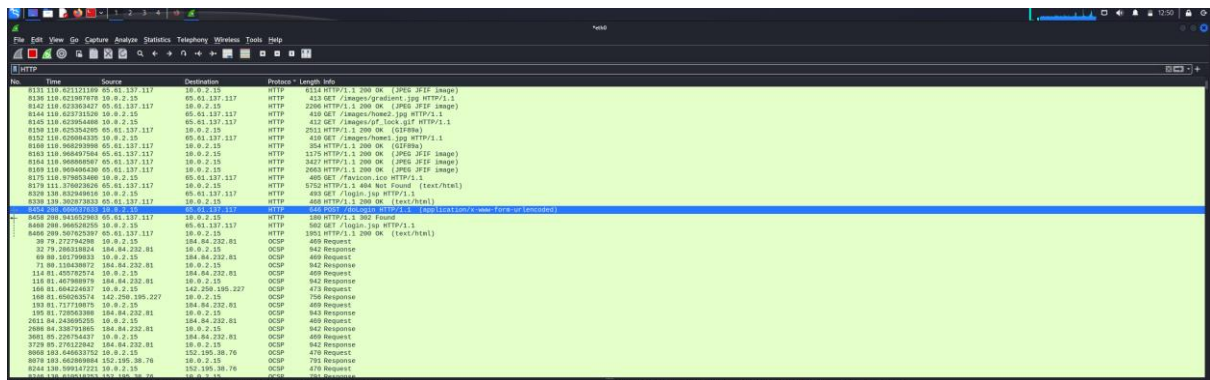
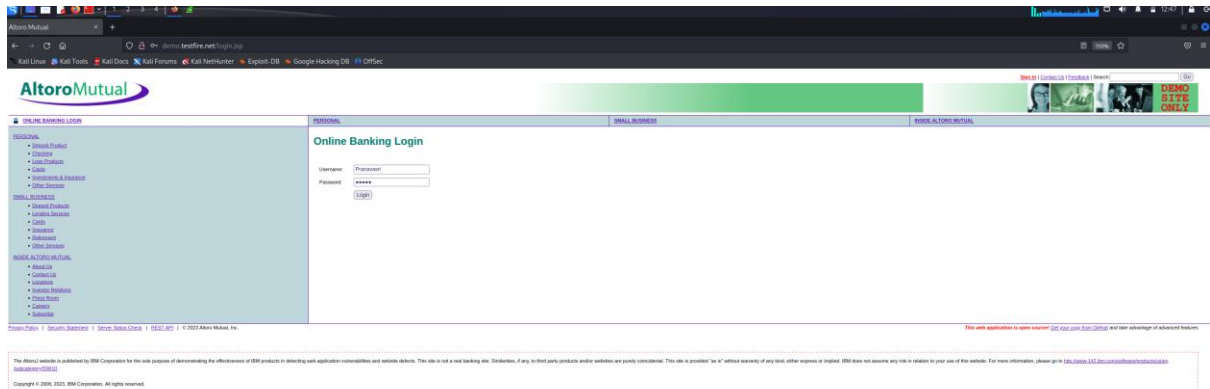
Exploit Title | Path
WordPress Plugin Mailing List - Arbitrary File Download | php/webapps/18276.txt
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | php/webapps/17866.txt
WordPress Plugin WP-php List 2.10.2 - "unsubscribe@mail" Cross-Site Scripting | php/webapps/33365.txt

Shellcodes: No Results

(kali@kali):~$
```

## 9. Sniffing and spoofing – Wireshark

Wireshark is a widely-used open-source network protocol analyser for sniffing and inspecting network traffic. It allows you to capture and analyse network packets, which can be extremely useful for network troubleshooting, security analysis, and understanding how data flows on a network.



```
[Response in frame: 8458]
File Data: 42 bytes
  ▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "uid" = "Pranavasri"
    ▸ Form item: "passwd" = "12345"
    ▸ Form item: "btnSubmit" = "Login"
```

## 10. Post Exploitation – Powersploit

PowerSploit is a collection of offensive PowerShell modules and scripts designed for post-exploitation activities and penetration testing. It provides a range of capabilities for post-exploitation, including privilege escalation, lateral movement, persistence, data exfiltration, and more.

```
kali@kali: /usr/share/windows-resources/powersploit
File Actions Edit View Help

> powersploit ~ PowerShell Post-Exploitation Framework

/usr/share/windows-resources/powersploit
├── AntivirusBypass
├── CodeExecution
├── Exfiltration
├── Mayhem
├── Persistence
├── PowerSploit.psd1
├── PowerSploit.psm1
├── Privesc
├── README.md
├── Recon
├── ScriptModification
├── Tests
└──

(kali@kali)-[/usr/share/windows-resources/powersploit]
$ ls -l
total 60
drwxr-xr-x 2 root root 4096 May 23 00:26 AntivirusBypass
drwxr-xr-x 3 root root 4096 May 23 00:26 CodeExecution
drwxr-xr-x 4 root root 4096 May 23 00:26 Exfiltration
drwxr-xr-x 2 root root 4096 May 23 00:26 Mayhem
drwxr-xr-x 2 root root 4096 May 23 00:26 Persistence
-rw-r--r-- 1 root root 5278 Aug 17 2020 PowerSploit.psd1
-rw-r--r-- 1 root root 149 Aug 17 2020 PowerSploit.psm1
drwxr-xr-x 2 root root 4096 May 23 00:26 Privesc
-rw-r--r-- 1 root root 10225 Aug 17 2020 README.md
drwxr-xr-x 3 root root 4096 May 23 00:26 Recon
drwxr-xr-x 2 root root 4096 May 23 00:26 ScriptModification
drwxr-xr-x 2 root root 4096 May 23 00:26 Tests

(kali@kali)-[/usr/share/windows-resources/powersploit]
$
```