

Assignment- 2

AI FOR CYBER SECURITY

Sanjaykrishnaa R S

21BRS1283

CSE with AI and Robotics

Chennai campus

01/09/23

Task: Try the tools in kali linux on a website and give a description

1) Information gathering – dnsenum

Dnsenum is a multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks. The main purpose of Dnsenum is to gather as much information as possible about a domain. The program currently performs the following operations:

- Get the host's addresses (A record).
- Get the nameservers (threaded).
- Get the MX record (threaded).
- Perform axfr queries on nameservers and get BIND versions(threaded).
- Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").
- Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
- Calculate C class domain network ranges and perform whois queries on them (threaded).
- Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
- Write to domain_ips.txt file ip-blocks.

This program is useful for pentesters, ethical hackers and forensics experts. It also can be used for security tests.


```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali ~
File Actions Edit View Help
youtube-ui.l.google.com. 120 IN A 172.217.166.14
youtube-ui.l.google.com. 120 IN A 216.58.209.206
youtube-ui.l.google.com. 120 IN A 142.250.77.286
youtube-ui.l.google.com. 120 IN A 142.250.77.238
youtube-ui.l.google.com. 120 IN A 142.250.182.174
youtube-ui.l.google.com. 120 IN A 142.250.192.174
youtube-ui.l.google.com. 120 IN A 142.250.192.286
youtube-ui.l.google.com. 120 IN A 142.250.192.238
sa.youtube.com. 300 IN CNAME youtube-ui.l.google.com.
youtube-ui.l.google.com. 293 IN A 142.250.67.174
youtube-ui.l.google.com. 293 IN A 216.58.203.46
youtube-ui.l.google.com. 293 IN A 142.250.183.78
youtube-ui.l.google.com. 293 IN A 142.250.183.110
youtube-ui.l.google.com. 293 IN A 142.250.192.14
youtube-ui.l.google.com. 293 IN A 142.250.192.46
youtube-ui.l.google.com. 293 IN A 142.250.192.78
youtube-ui.l.google.com. 293 IN A 142.250.192.110
youtube-ui.l.google.com. 293 IN A 142.250.192.142
youtube-ui.l.google.com. 293 IN A 142.251.42.14
youtube-ui.l.google.com. 293 IN A 142.251.42.46
youtube-ui.l.google.com. 293 IN A 172.217.166.206
youtube-ui.l.google.com. 293 IN A 172.217.166.46
youtube-ui.l.google.com. 293 IN A 172.217.166.174
youtube-ui.l.google.com. 293 IN A 142.251.42.78
youtube-ui.l.google.com. 293 IN A 142.250.77.46
fr.youtube.com. 300 IN CNAME youtube-ui.l.google.com.
youtube-ui.l.google.com. 83 IN A 142.250.67.174
youtube-ui.l.google.com. 83 IN A 216.58.203.46
youtube-ui.l.google.com. 83 IN A 142.250.183.78
youtube-ui.l.google.com. 83 IN A 142.250.183.110
youtube-ui.l.google.com. 83 IN A 142.250.192.14
youtube-ui.l.google.com. 83 IN A 142.250.192.46
youtube-ui.l.google.com. 83 IN A 142.250.192.78
youtube-ui.l.google.com. 83 IN A 142.250.192.110
youtube-ui.l.google.com. 83 IN A 142.250.192.142
youtube-ui.l.google.com. 83 IN A 142.251.42.14
youtube-ui.l.google.com. 83 IN A 142.251.42.46
youtube-ui.l.google.com. 83 IN A 172.217.166.206
youtube-ui.l.google.com. 83 IN A 172.217.166.46
youtube-ui.l.google.com. 83 IN A 172.217.166.174
youtube-ui.l.google.com. 83 IN A 142.251.42.78
gr.youtube.com. 300 IN CNAME youtube-ui.l.google.com.
youtube-ui.l.google.com. 81 IN A 142.250.67.174
youtube-ui.l.google.com. 81 IN A 216.58.203.46
youtube-ui.l.google.com. 81 IN A 142.250.183.78
youtube-ui.l.google.com. 81 IN A 142.250.183.110
youtube-ui.l.google.com. 81 IN A 142.250.192.14
youtube-ui.l.google.com. 81 IN A 142.250.192.46
youtube-ui.l.google.com. 81 IN A 142.250.192.78
youtube-ui.l.google.com. 81 IN A 142.250.192.110
youtube-ui.l.google.com. 81 IN A 142.250.192.142
```

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali ~
File Actions Edit View Help
youtube-ui.l.google.com. 16 IN A 172.217.167.46
youtube-ui.l.google.com. 16 IN A 172.217.166.14
youtube-ui.l.google.com. 16 IN A 216.58.209.206
youtube-ui.l.google.com. 16 IN A 142.250.77.238
youtube-ui.l.google.com. 16 IN A 142.250.182.174
youtube-ui.l.google.com. 16 IN A 142.250.192.286
youtube-ui.l.google.com. 16 IN A 142.250.192.238
upload.youtube.com. 252 IN CNAME yt-video-upload.l.google.com.
yt-video-upload.l.google.com. 2 IN A 172.217.166.15
www.youtube.com. 33 IN CNAME youtube-ui.l.google.com.
youtube-ui.l.google.com. 230 IN A 142.250.67.174
youtube-ui.l.google.com. 230 IN A 216.58.203.46
youtube-ui.l.google.com. 230 IN A 142.250.183.46
youtube-ui.l.google.com. 230 IN A 142.250.183.78
youtube-ui.l.google.com. 230 IN A 142.250.183.110
youtube-ui.l.google.com. 230 IN A 142.250.192.14
youtube-ui.l.google.com. 230 IN A 142.250.192.46
youtube-ui.l.google.com. 230 IN A 142.250.192.78
youtube-ui.l.google.com. 230 IN A 142.250.192.110
youtube-ui.l.google.com. 230 IN A 142.250.192.142
youtube-ui.l.google.com. 230 IN A 142.251.42.14
youtube-ui.l.google.com. 230 IN A 142.251.42.46
youtube-ui.l.google.com. 230 IN A 172.217.166.206
youtube-ui.l.google.com. 230 IN A 172.217.166.46
youtube-ui.l.google.com. 230 IN A 172.217.166.174
youtube-ui.l.google.com. 230 IN A 142.251.42.78

youtube.com class E addresses:
142.250.183.0/24

Performing reverse lookup on 256 IP addresses:

8 results out of 256 IP addresses.

youtube.com is blank:
done.

kali@kali:~$
```

2) Vulnerability analysis – nmap

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

```

ES
(kali@kali)-[~]
$ nmap youtube.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 10:27 EDT
Nmap scan report for youtube.com (142.250.193.46)
Host is up (0.064s latency).
Other addresses for youtube.com (not scanned): 2404:6800:4002:81a::200e
rDNS record for 142.250.193.46: del11s15-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds

```

3) web application analysis – whatweb

WhatWeb identifies websites. It recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

WhatWeb has over 900 plugins, each to recognise something different. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

```

(kali@kali)-[~]
$ whatweb -v -a 3 testfire.net
WhatWeb report for http://testfire.net
Status      : 200 OK
Title       : Altoro Mutual
IP          : 65.61.137.117
Country     : UNITED STATES, US
Summary     : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java

Detected Plugins:
[ Apache ]
  The Apache HTTP Server Project is an effort to develop and
  maintain an open-source HTTP server for modern operating
  systems including UNIX and Windows NT. The goal of this
  project is to provide a secure, efficient and extensible
  server that provides HTTP services in sync with the current
  HTTP standards.

  Google Dorks: (3)
  Website      : http://httpd.apache.org/

[ Cookies ]
  Display the names of cookies in the HTTP headers. The
  values are not returned to save on space.

  String       : JSESSIONID

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  String       : Apache-Coyote/1.1 (from server string)

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie
  response header and the browser supports it then the cookie
  cannot be accessed through client side script - More Info:
  http://en.wikipedia.org/wiki/HTTP_cookie

  String       : JSESSIONID

[ Java ]
  Java allows you to play online games, chat with people
  around the world, calculate your mortgage interest, and
  view images in 3D, just to name a few. It's also integral
  to the intranet applications and other e-business solutions
  that are the foundation of corporate computing.

  Website      : http://www.java.com/

```

```
[ HttpOnly ]
If the HttpOnly flag is included in the HTTP set-cookie
response header and the browser supports it then the cookie
cannot be accessed through client side script - More Info:
http://en.wikipedia.org/wiki/HTTP_cookie

String      : JSESSIONID

[ Java ]
Java allows you to play online games, chat with people
around the world, calculate your mortgage interest, and
view images in 3D, just to name a few. It's also integral
to the intranet applications and other e-business solutions
that are the foundation of corporate computing.

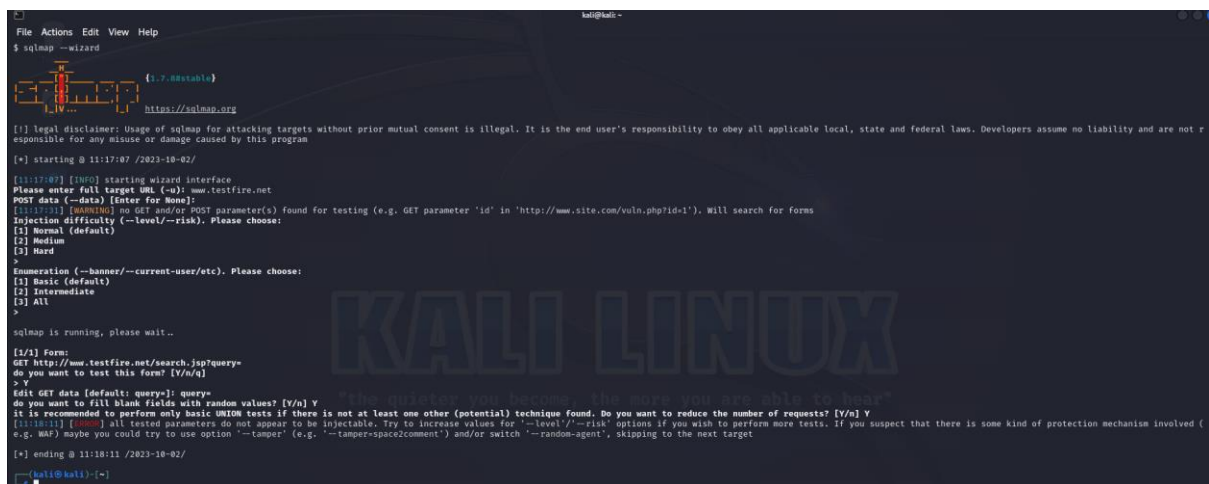
Website     : http://www.java.com/

HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=4FECFEB2C4AD7ED4C587528459958193; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Mon, 02 Oct 2023 15:04:25 GMT
Connection: close

(kali@kali)-[~]
```

4) Database assessment – sqlmap

sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.



```
File Actions Edit View Help
$ sqlmap --wizard

[1.7.0stable]
https://sqlmap.org

[!] 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 @ 11:17:07 /2023-10-02/

[11:17:07] [INFO] starting wizard interface
Please enter full target URL (-u): www.testfire.net
POST data (--data) [Enter for None]:
[11:17:11] [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
>
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
>

sqlmap is running, please wait..

[1/1] Form:
GET http://www.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
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/g] Y
[11:18:11] [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 that 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', skipping to the next target

[*] ending @ 11:18:11 /2023-10-02/

(kali@kali)-[~]
```

5) Password attacks – crunch

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.

This program supports numbers and symbols, upper and lower case characters separately and Unicode.

```
(kali㉿kali)-[~]  
$ crunch 2 3 abcd  
Crunch will now generate the following amount of data: 304 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 80  
aa  
ab  
ac  
ad  
ba  
bb  
bc  
bd  
ca  
cb  
cc  
cd  
da  
db  
dc  
dd  
aaa  
aab  
aac  
aad  
aba  
abb  
abc  
abd  
aca
```

6) wireless attacks – Bully

Bully is a new implementation of the WPS brute force attack, written in C. It is conceptually identical to other programs, in that it exploits the (now well known) design flaw in the WPS specification. It has several advantages over the original reaver code. These include fewer dependencies, improved memory and cpu performance, correct handling of endianness, and a more robust set of options.