Assignment 2

Testing out different tools in Kali Linux

Name: Yash Lulla

Registration no.: 21BRS1427

Email: yash.lulla2021@vitstudent.ac.in

Information Gathering:

Nmap:


```
┌──(yash㊙Yash)-[~]
└─$ nmap testfire.net
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 21:24 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.25s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE   SERVICE
80/tcp    open    http
443/tcp   open    https
8080/tcp  open    http-proxy
8443/tcp  closed  https-alt

Nmap done: 1 IP address (1 host up) scanned in 16.88 seconds
```

Vulnerability Analysis:

Nikto:


```
┌──(yash㊙Yash)-[~]
└─$ nikto -h google.com
- Nikto v2.5.0
─────────────────────────────────────────────────────────────────────
+ Multiple IPs found: 142.250.183.206, 2404:6800:4009:824::200e
+ Target IP:          142.250.183.206
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2023-10-09 21:39:50 (GMT5.5)
─────────────────────────────────────────────────────────────────────
+ Server: gws
+ /: Uncommon header 'origin-trial' found, with multiple values: (Ap+qNlnLzJDKSmEHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIAAABfeyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MTY4NTY2Mzk5OX0=,AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk8OAqjho1DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJCYWNrRm9yd2FyZENhY2hlTm90U mVzdG9yYWRSZWFzb25zIiwiZXhwaXJ5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbnMiOi6dHJlZX0=,).
+ /: 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/miss
ing-content-type-header/
+ Root page / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'gws' to 'sffe'.
+ /: Cookie 1P_JAR created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ OPTIONS: Allowed HTTP Methods: GET, HEAD .
```

Web application analysis:

```
┌──(yash㉿Yash)-[~]
└─$ sqlmap -u testfire.net
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.8#stable}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 21:51:10 /2023-10-09/

[21:51:10] [INFO] testing connection to the target URL
[21:51:41] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[21:51:41] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-fi
le'...)
[21:52:11] [CRITICAL] connection timed out to the target URL

[*] ending @ 21:52:11 /2023-10-09/
```

Database assessment:

```
┌──(yash㉿Yash)-[~]
└─$ sqlmap -u testfire.net
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.8#stable}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 21:51:10 /2023-10-09/

[21:51:10] [INFO] testing connection to the target URL
[21:51:41] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[21:51:41] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-fi
le'...)
[21:52:11] [CRITICAL] connection timed out to the target URL

[*] ending @ 21:52:11 /2023-10-09/
```

Reporting Tools:

```
┌──(yash㉿Yash)-[~/Desktop]
└─$ pipal something.txt
Generating stats, hit CTRL-C to finish early and dump stats on words already processed.
Please wait ...
Processing:     100% |oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo| Time: 00:00:00


Basic Results

Total entries = 9
Total unique entries = 9

Top 10 passwords
qadfwgg = 1 (11.11%)
awefgaefg = 1 (11.11%)
admin = 1 (11.11%)
adminstrator = 1 (11.11%)
name = 1 (11.11%)
yo = 1 (11.11%)
somethihng = 1 (11.11%)
i dont care = 1 (11.11%)
lets see = 1 (11.11%)

Top 10 base words
qadfwgg = 1 (11.11%)
awefgaefg = 1 (11.11%)
admin = 1 (11.11%)
adminstrator = 1 (11.11%)
name = 1 (11.11%)
somethihng = 1 (11.11%)
i dont care = 1 (11.11%)
lets see = 1 (11.11%)

Password length (length ordered)
2 = 1 (11.11%)
4 = 1 (11.11%)
5 = 1 (11.11%)
7 = 1 (11.11%)
8 = 1 (11.11%)
9 = 1 (11.11%)
10 = 1 (11.11%)
11 = 1 (11.11%)
12 = 1 (11.11%)
```