ASSIGNMENT -2

Name : shaik nihal ahmed

Kali Linux – Web Penetration Testing Tools

Kali Linux comes packed with **300+ tools** out of which many are used for Web Penetration Testing. Though there are many tools in Kali Linux for Web Penetration Testing here is the list of most used tools.

1. Burp Suite

Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it. And as the request passes through the burp suite, it allows us to make changes to those requests as per our need which is good for testing vulnerabilities like XSS or SQLi or even any vulnerability related to the web. Kali Linux comes with burp suite community edition which is free but there is a paid edition of this tool known as burp suite professional which has a lot many functions as compared to burp suite community edition.
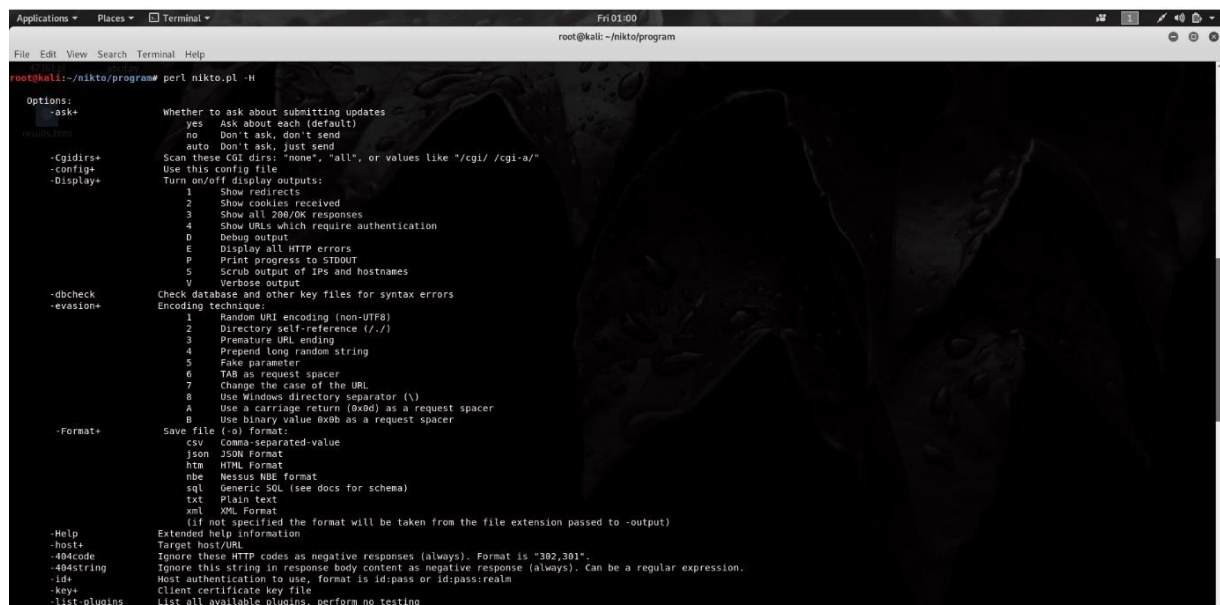
To use burp suite:

2. Nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It comes packed with many features, a few of them are listed below.

- Full support for SSL
- Looks for subdomains
- Supports full HTTP Proxy
- Outdated component report
- Username guessing

To use nikto, download nikto and enter the following command.

```
perl nikto.pl -H
```


3. Maltego

Maltego is a platform developed to convey and put forward a clear picture of the environment that an organization owns and operates. Maltego offers a unique perspective to both network and resource-based entities which is the aggregation of information delivered all over the internet – whether it's the current configuration of a router poised on the edge of our network or

any other information, Maltego can locate, aggregate and visualize this information. It offers the user with unprecedented information which is leverage and power.
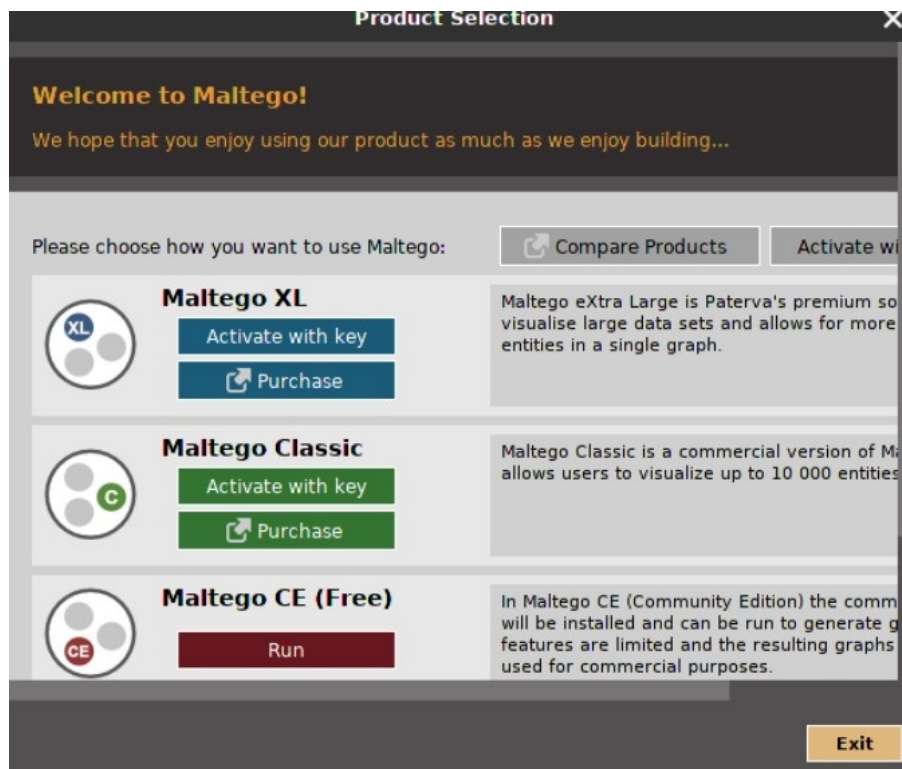
4. SQLMap

SQLMap is an open-source tool that is used to automate the process of manual SQL injection over a parameter on a website. It detects and exploits the SQL injection parameters itself all we have to do is to provide it with an appropriate request or URL. It supports 34 databases including MySQL, Oracle, PostgreSQL, etc.

To use sqlmap tool:

- sqlmap comes pre-installed in Kali Linux
- Just type sqlmap in the terminal to use the tool.

```
root@kali:~# sqlmap
        ___
       __H__
 ___ ___[(]_____ ___ ___   {1.4.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-t
ampers, --wizard, --update, --purge or --dependencies). Use -h for basic and -h
h for advanced help

[23:56:33] [WARNING] you haven't updated sqlmap for more than 77 days!!!
root@kali:~#
```

5. Whatweb

Whatweb is an acronym of "**what is that website**".It is used to get the technologies which a website is using, these technologies might me content management system(CMS), Javascript Libraries, etc. It is used for many purposes, a few of them are listed below.

- To get the Content Management System is used by a web application
- To get the Web Server details being used by the web application
- To get the embedded devices attached to the web application
- It consists of 1700+ plugins and every plugin is used to recognize something different.

To run whatweb, execute the following command and replace google.com with the domain name of your choice.

```
whatweb google.com
```

File   Actions   Edit   View   Help

kali@kali:~$ whatweb google.com
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
http://google.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws]
, IP[172.217.160.238], RedirectLocation[http://www.google.com/], Title[301 Moved], X-
Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
http://www.google.com/ [200 OK] Cookies[1P_JAR,NID], Country[UNITED STATES][US], HTML
5, HTTPServer[gws], HttpOnly[NID], IP[216.58.221.36], Script, Title[Google], X-Frame-
Options[SAMEORIGIN], X-XSS-Protection[0]
kali@kali:~$