

**Jain (Deemed-to-be) University, Faculty of Engineering and Technology**

**Department of CSE – Cloud Technology and Information Security**

**Ethical Hacking Lab**

**Semester – V**

**Academic Year: 2022 – 2023**

**Dr. Bishwajeeth Pandey YARUL JAIN**

**Faculty In-charge 20BTRCI023**

|  |  |  |
| --- | --- | --- |
| **Experiment No.** | **Details** | **Page No.** |
| 1 | **Website Technical Information Gathering** | **03** |
| 2 | **Port Scanning and Enumeration using Tools** | **07** |
| 3 | **Network scanning and vulnerability scanner tool** | **10** |
| 4 | **Data Enumeration by Nmap** | **13** |
| 5 | **NETWORK MONITORING USING DRIFTNET AND DARKSTAT** | **16** |
| 6 | Social Engineering using SEToolkit | **20** |
| 7 | **Spoofing email id using Emkei’s Mailer** | **23** |

**LAB EXPERIMENT 1**

**Website Technical Information Gathering**

# Aim:

To gather technical information about a website using Red Hawk tool.

# Tool(s):

* + 1. **Red Hawk**

Scans that can be performed using Red Hawk tool:

* + - * Basic Scan
        + Site Title
        + IP Address
        + Web Server Detection
        + CMS Detection
        + Cloudflare Detection
        + robots.txt Scanner
* Whois Lookup
* Geo-IP Lookup
* Grab Banners
* DNS Lookup
* Subnet Calculator
* Nmap Port Scan
* Sub-Domain Scanner
* Sub Domain
* IP Address
* Reverse IP Lookup & CMS Detection
  + Hostname
  + IP Address
  + CMS
* Error Based SQLi Scanner
* Bloggers View
  + HTTP Response Code
  + Site Title
  + Alexa Ranking
  + Domain Authority
  + Page Authority
  + Social Links Extractor
  + Link Grabber
* WordPress Scan
  + Sensitive Files Crawling
  + Version Detection
  + Version Vulnerability Scanner
* Crawler
* MX Lookup
* Scan For Everything

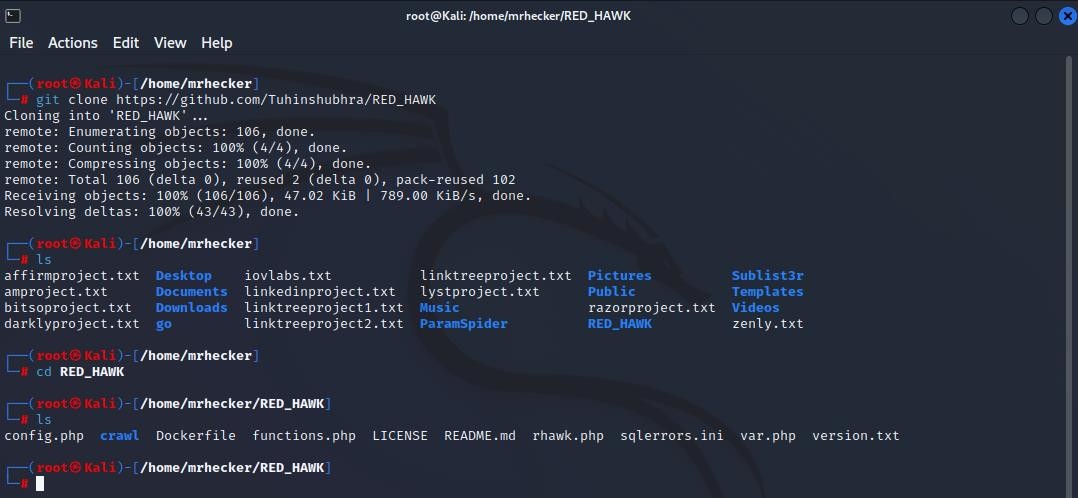
# Commands:

* + 1. **Installation**

To install, type ***git clone https://github.com/Tuhinshubhra/RED\_HAWK*** in the

terminal and don’t forget to execute the command as a root user.

Next, type ***cd RED\_HAWK*** to go to Red Hawk directory to further setup the tool.



**Figure 1: Red Hawk Tool Installation**

# Setup

Now, type ***php rhawk.php*** to open the interface of the tool.

Before proceeding with information gathering, the tool will ask for some information such as the website and ask you to choose between http or https. In this case, the website is jainuniversity.ac.in and the option that I selected was 2 (because the website is https).

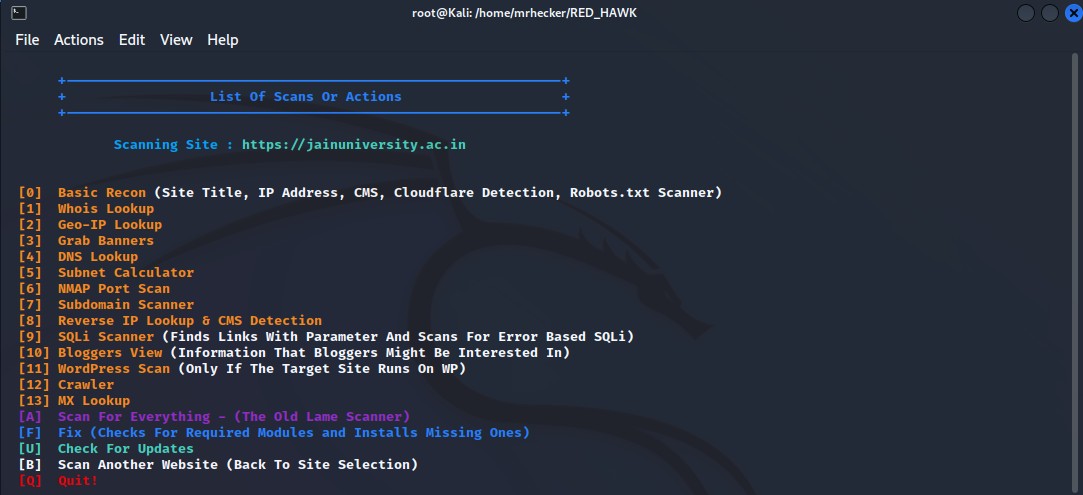


**Figure 2: Red Hawk Setup Interface**

# Information Gathering

In this stage, this tool lists all the possible options/features that we can use to gather technical information from the website provided.

Here, in our case, we can only use few options/features such as Basic Recon, Whois Lookup, Geo-IP Lookup, Grab Banners, DNS Lookup, Subnet Calculator and Subdomain Scanner as these are the only options/features that will help us to gather technical information.



**Figure 3: Red Hawk Information Gathering Options**

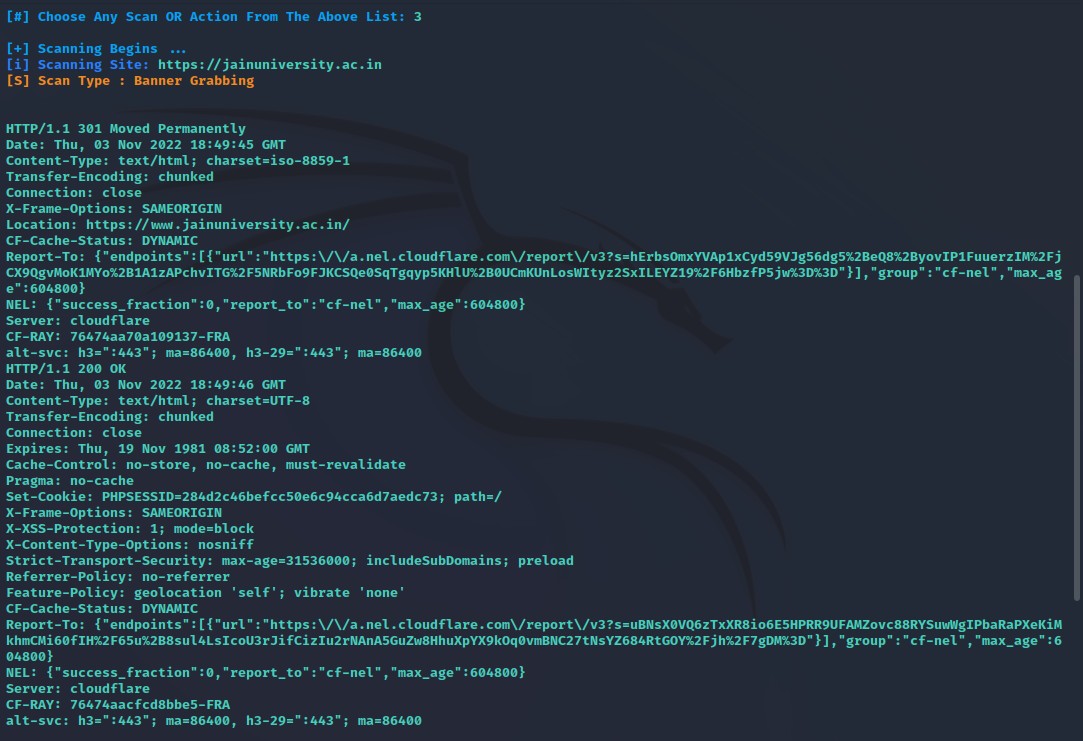
Now, we will perform scanning using some of these options to gather technical information.

# [0] Basic Recon



**Figure 4: Red Hawk Basic Recon Scanning**

# [3] Grab Banners



**Figure 5: Red Hawk Banner Grabbing**

# [5] Subnet Calculator



**Figure 6: Red Hawk Subnet Calculator**

# Reference:

https://github.com/Tuhinshubhra/RED\_HAWK

**LAB EXPERIMENT 2**

**Port Scanning and Enumeration using Tools**

# Aim:

To demonstrate port scanning and enumeration using tools.

# Tool(s):

* + 1. **Nmap**

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

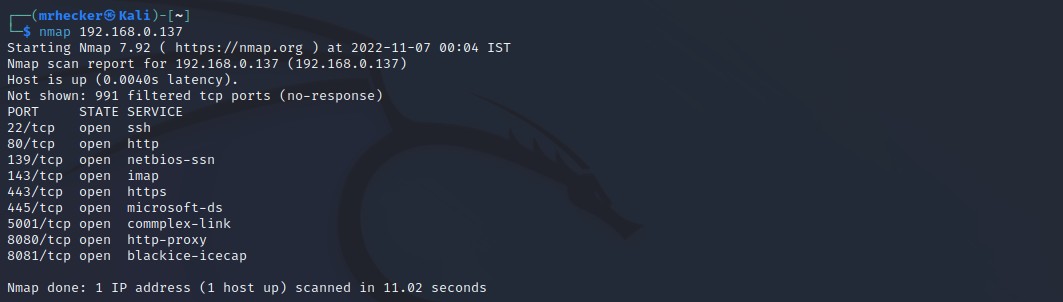
# Nikto

Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. Nikto can detect over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

# Commands:

* + 1. **Port Scanning using Nmap**

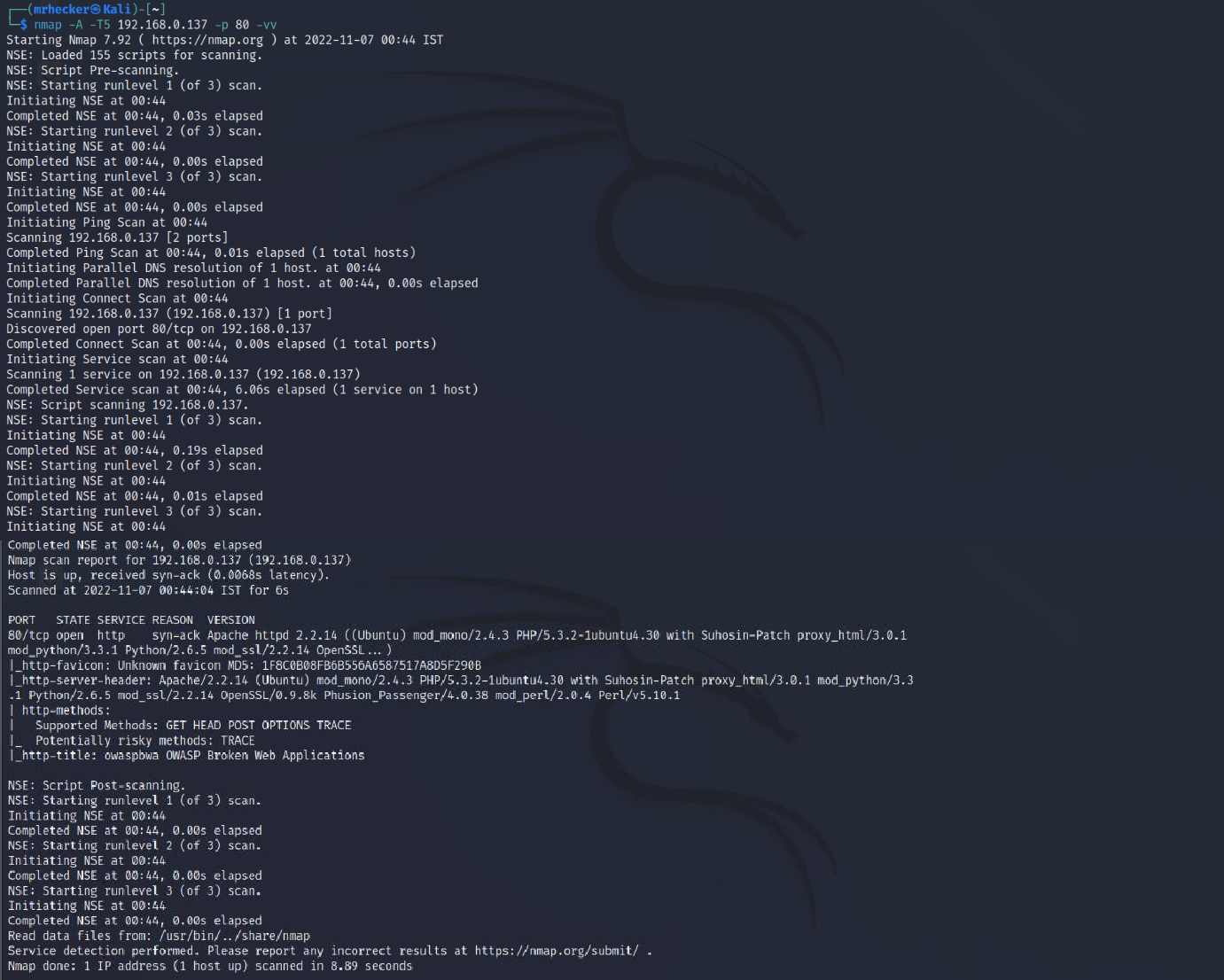
**Step 1**: First, we will scan for all open ports along with the services for IP address 192.168.0.137 using command ***nmap 192.168.0.137***. As shown in the figure 7 below, we can find 9 ports are open out of scanned 1000 ports.



**Figure 7: *nmap 192.168.0.137***

# Enumeration using Nmap

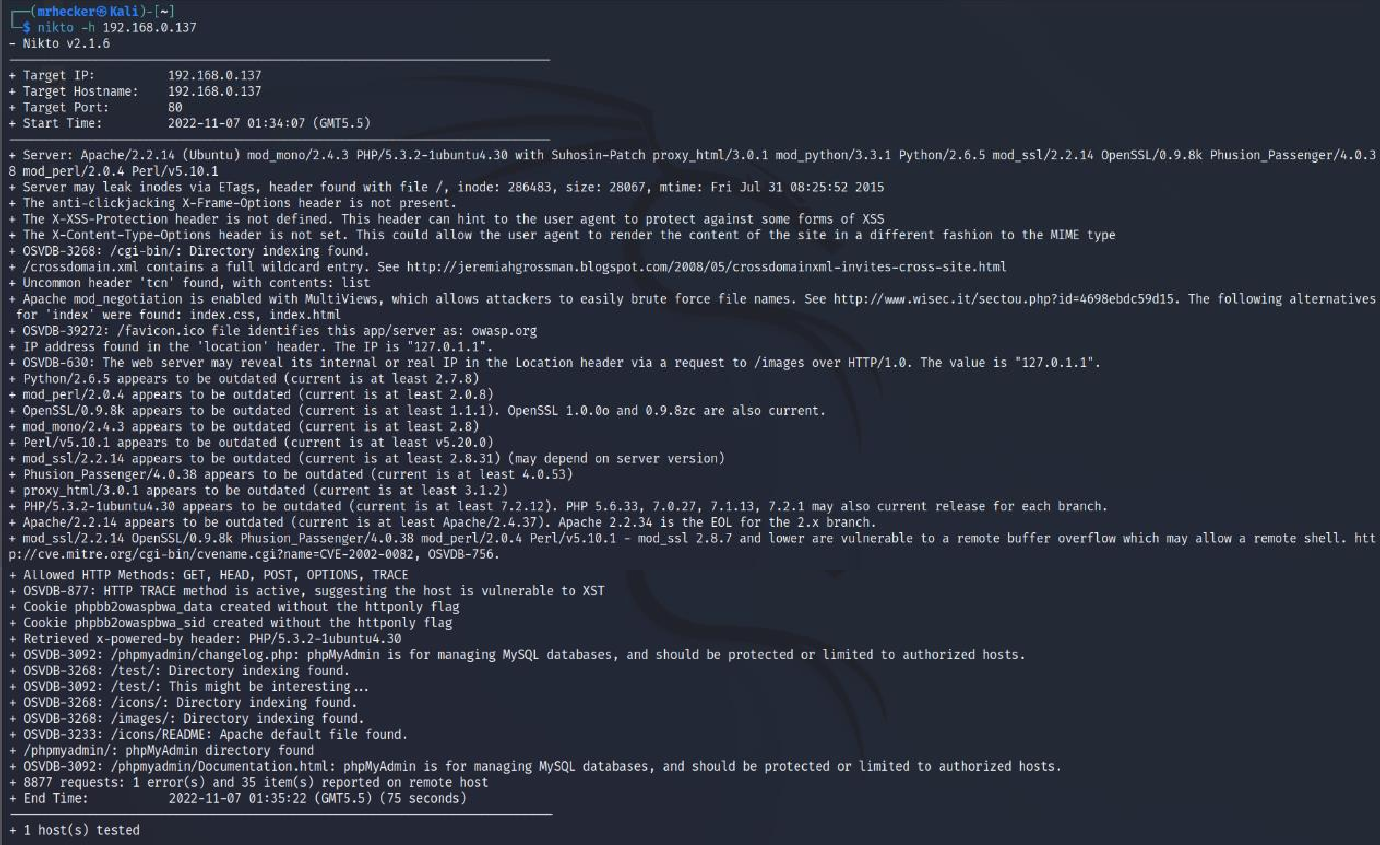
**Step 2**: Next, we will target port 80/tcp which is running in the http service. We will type the command, ***nmap -A -T5 192.168.0.137 -p 80 -vv***. Here, were using - A for aggressive scan of timing instance 5 with IP address, specified port 80 along with verbosity for faster and precise result. From this result, we can enumerate the information of target IP from the supported http methods shown in the figure 8 below, such as GET, HEAD, POST, OPTIONS and TRACE.



**Figure 8: *nmap -A -T5 192.168.0.137 -p 80 -vv***

# Enumeration using Nikto

**Step 3**: Now, we will use nikto to enumerate more information about the target host. Use command ***nikto -h 192.168.0.137*** and we will get the information as shown in the figure below.



**Figure 9: nikto -h 192.168.0.137**

# Reference:

https://nmap.org/ https://en.wikipedia.org/wiki/Nikto\_(vulnerability\_scanner)

**LAB EXPERIMENT 3**

**Network scanning and vulnerability scanner tool**

# Aim:

To demonstrate network scanning and vulnerability scanning tool.

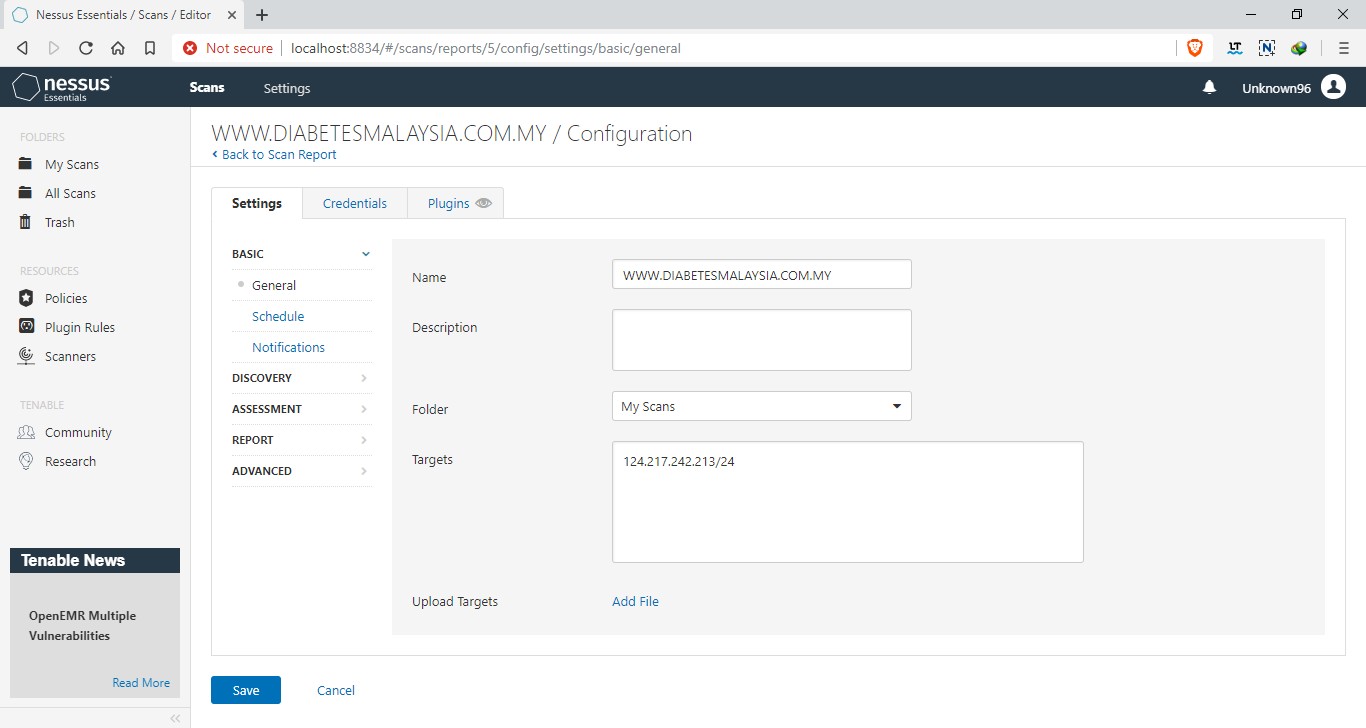
# Tool(s):

**3.2.3 Nessus**

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

# Commands:

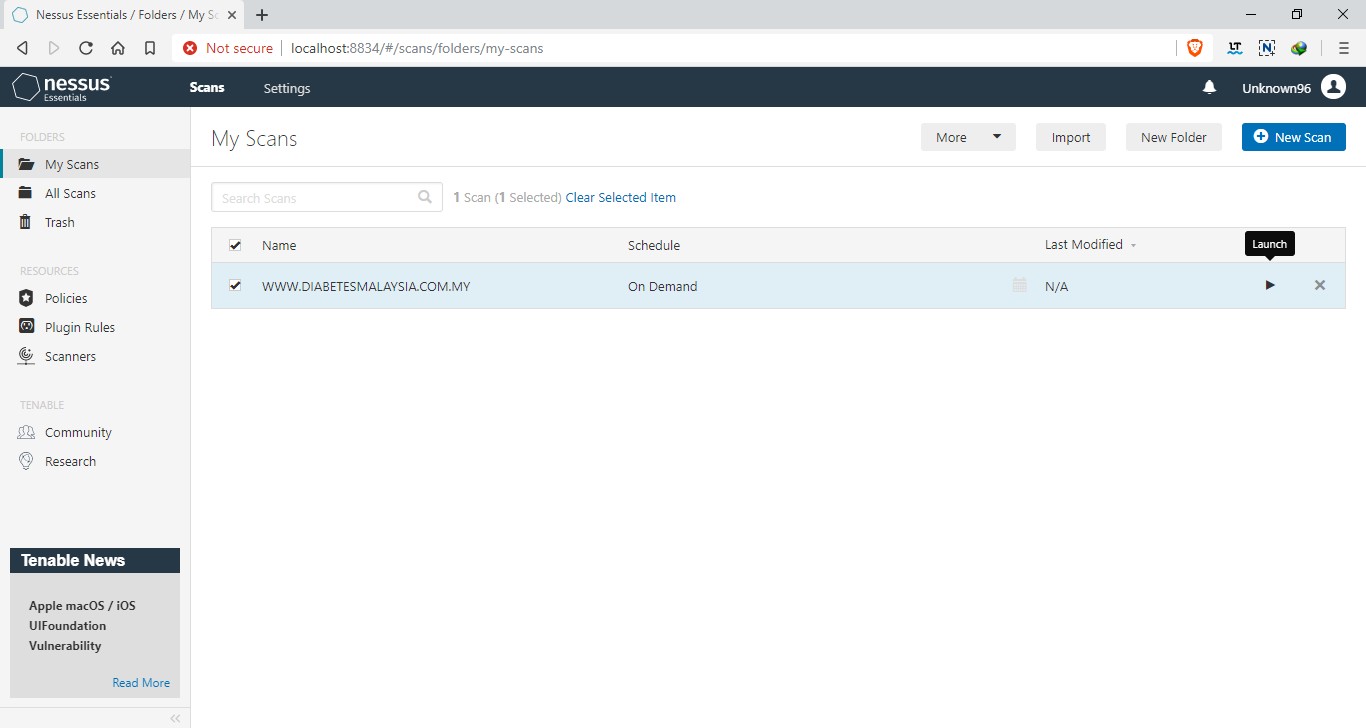
**Step 1:** Firstly, log in into Nessus Account with the Username and Password. Then, we will scan a website ***https://***[***www.diabetesmalaysia.com.my***](http://www.diabetesmalaysia.com.my/) to find for vulnerabilities. Type the URL and IP Address in the ***Name*** and ***Targets*** text boxes as shown in the figure 10 below.



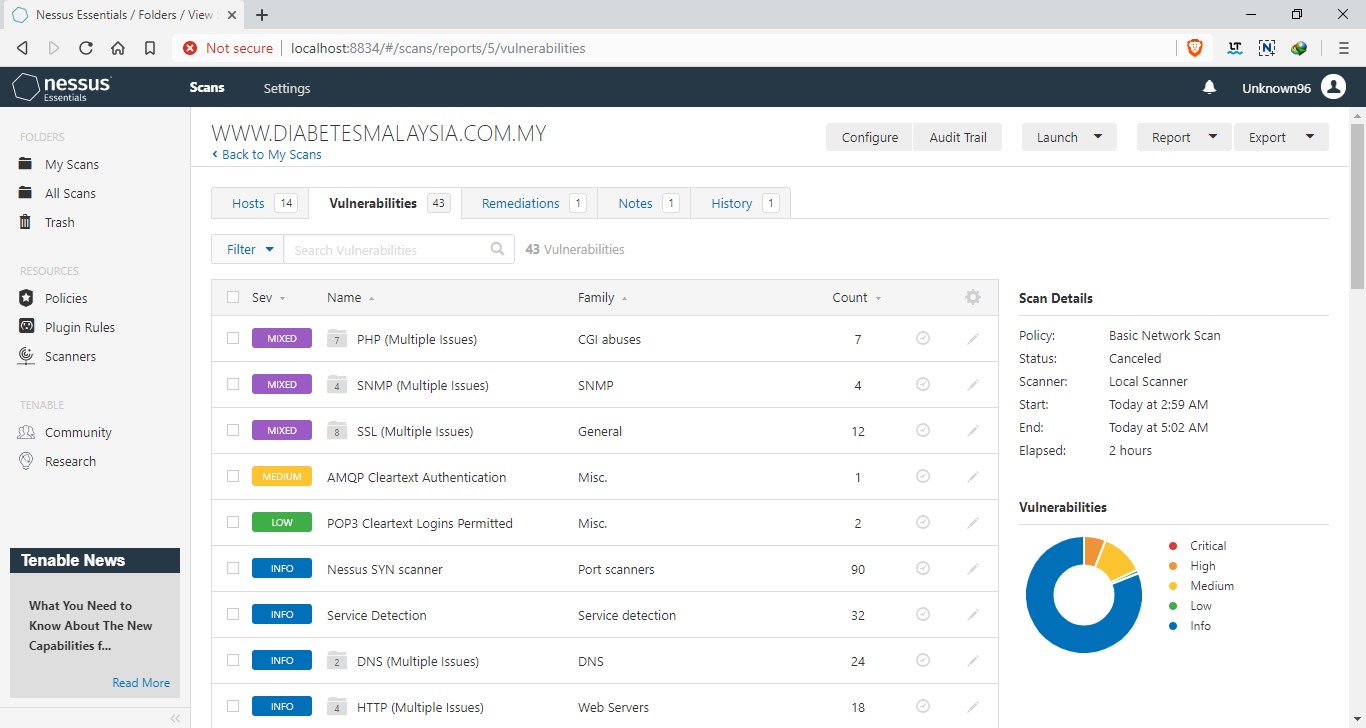
**Figure 10: Nessus Scan Configuration**

**Step 2:** Now, check the checkbox of the URL that we want to scan and click on

***Launch*** as shown in the figure 11 below.

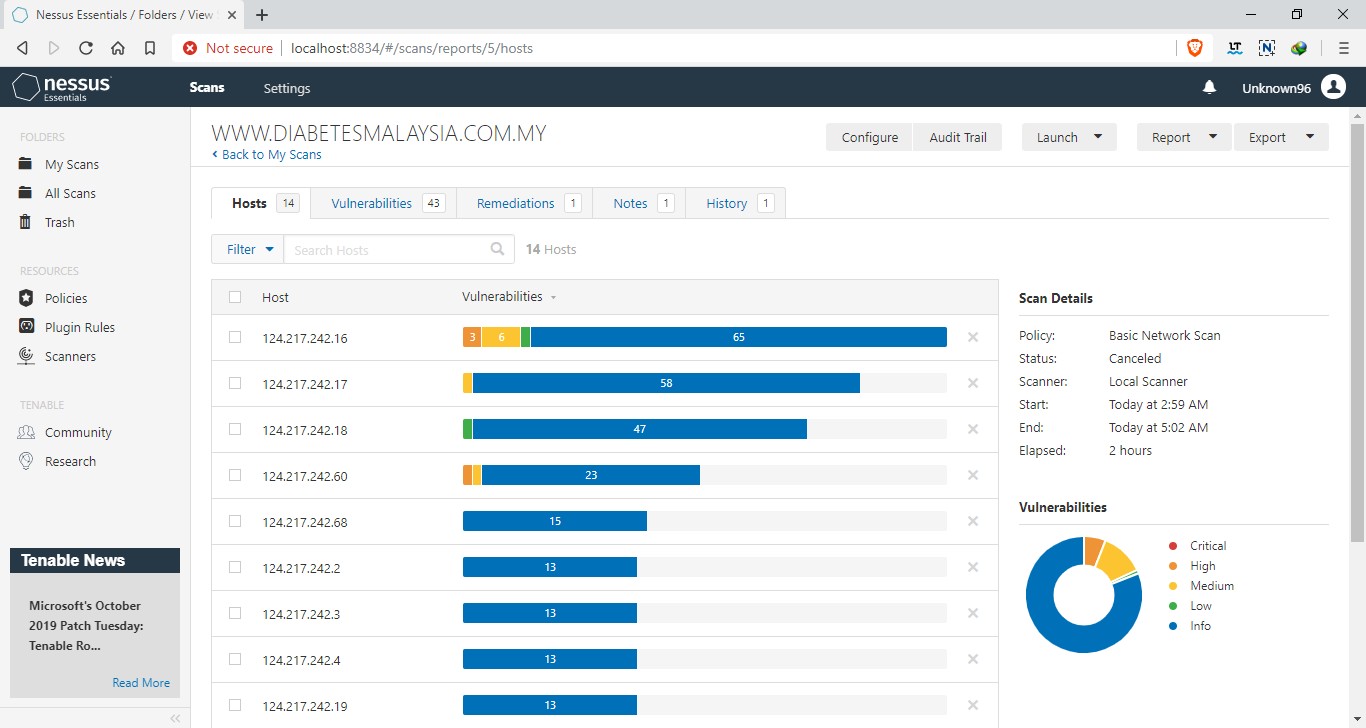


**Figure 11: Nessus Scans List**

**Step 3:** Next, wait till the scan to be completed. Once the Scanning process is completed, click on the ***Vulnerabilities*** tab to view the vulnerabilities of this Web Application as shown in the figure 12 below.

**Figure 12: Nessus Vulnerabilities List**

**Step 4:** Finally, click on the ***Hosts*** tab to view the data analysis of the vulnerabilities of this Web Application as shown below in figure 13.



**Figure 13: Nessus Hosts List**

# Reference:

https:/[/ww](http://www.cs.cmu.edu/~dwendlan/personal/nessus.html)w[.cs.cmu.edu/~dwendlan/personal/nessus.html](http://www.cs.cmu.edu/~dwendlan/personal/nessus.html)

**LAB EXPERIMENT 4**

**Data Enumeration by Nmap**

# Aim:

To enumerate information using Nmap.

# Tool(s):

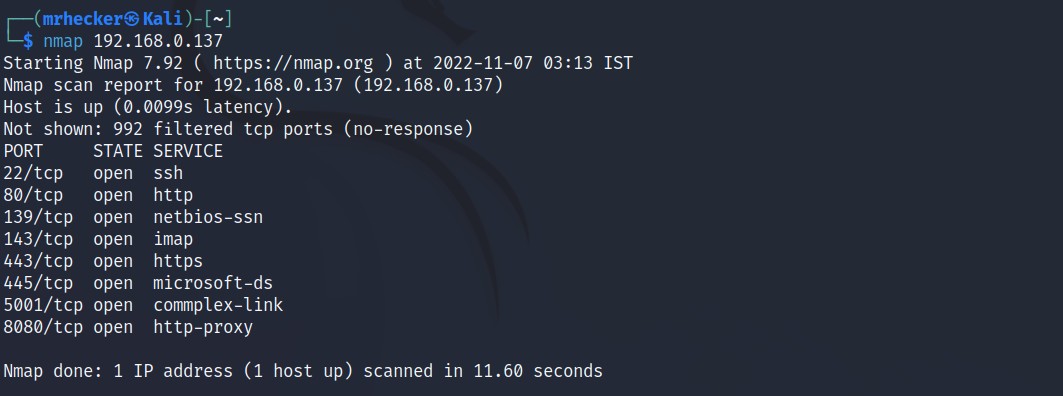
* + 1. **Nmap**

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.

# Commands:

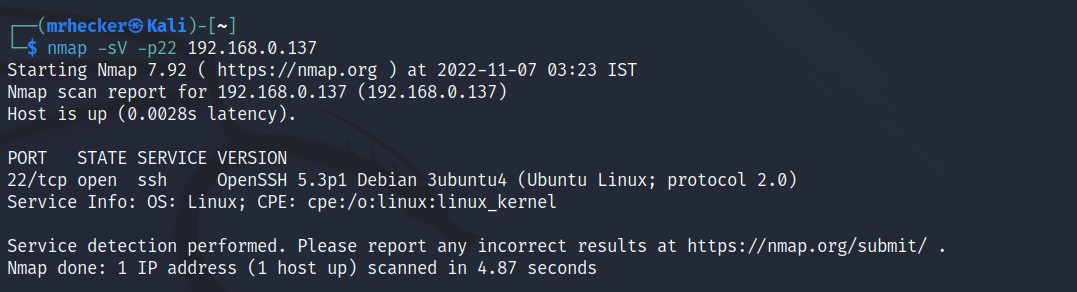
* + 1. **Version Detection using Nmap**

**Step 1:** Firstly, we are going to detect the version that a port is running on the target IP Address. Before that, we will scan for the open ports for the IP Address. Use command ***nmap 192.168.0.137*** as shown below in figure 14.



**Figure 14: *nmap 192.168.0.137***

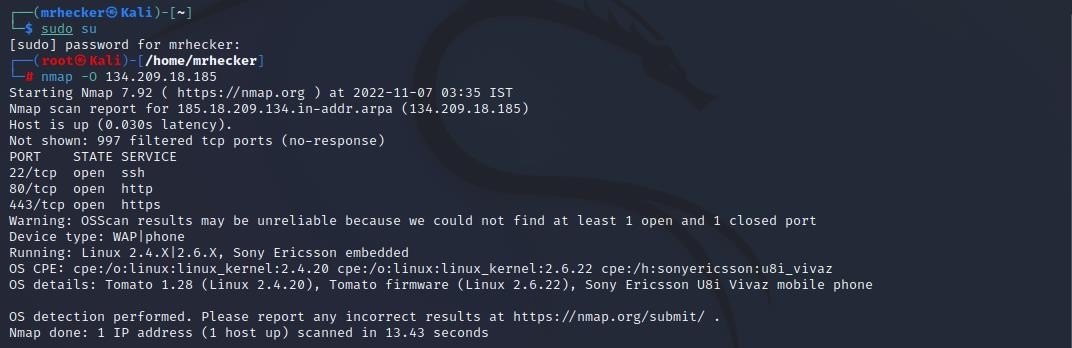
**Step 2:** Then, select a port number, in this case, port 22/tcp running on service ssh. Use command ***nmap -sV -p 22 192.168.0.137*** as shown below in figure 15. This will show the version which will allow us to search for vulnerabilities in the resulted version further helping in enumeration or exploitation.



**Figure 15: *nmap -sV -p 22 192.168.0.137***

# OS Detection using Nmap

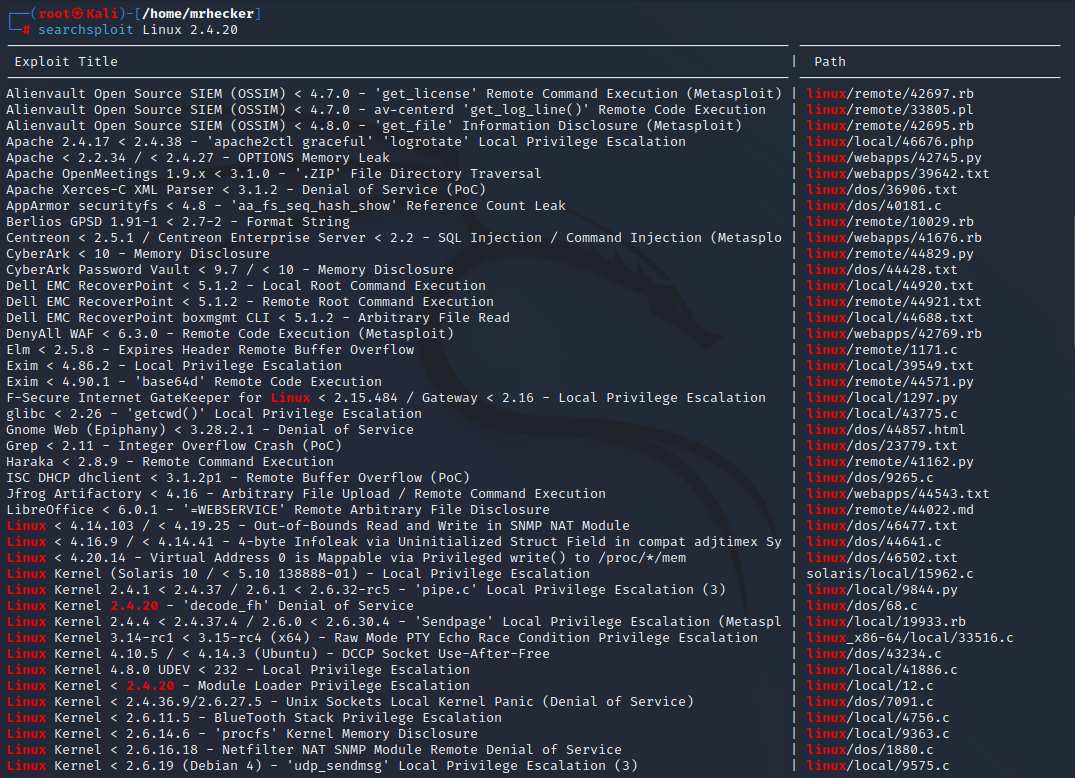
**Step 1:** Now, we are going to detect the OS version of an IP Address. Use command ***nmap -O 134.209.18.185***. Run the command as root user as shown below in figure 16.



**Figure 16: *nmap -O 134.209.18.185***

**Step 2:** After knowing the OS version, which in this case out of some displayed, let us use searchsploit to scan for Linux 2.4.20. Use command ***searchsploit Linux***

***2.4.20***. This will show all the exploitation for the particular version which will help us to further find more vulnerabilities as shown below in figure 17.



**Figure 17: *searchsploit Linux 2.4.20***

# Reference:

https:/[/ww](http://www.kali.org/tools/nmap/)w[.kali.org/tools/nmap/](http://www.kali.org/tools/nmap/)

**LAB EXPERIMENT 5**

**NETWORK MONITORING USING DRIFTNET AND DARKSTAT**

5.1 Introduction :

**Darkstat** is a cross-platform, lightweight, simple, real-time network statistics tool that captures network traffic, computes statistics concerning usage, and serves the reports over HTTP.

#### Darkstat Features:

* An integrated web-server with deflate compression functionality.
* Portable, single-threaded and efficient Web-based network traffic analyzer.
* The Web interface shows traffic graphs, reports per host and ports for each host.
* Supports asynchronous reverse DNS resolution using a child process.
* Support for IPv6 protocol.

### **3.2 Requirements:**

* **libpcap** – a portable C/C++ library for network traffic capture.

Being small in size, it uses very low system memory resources and it is easy to install, configure and use in Linux as explained below.

3.3 How to Install Darkstat Network Traffic Analyzer in Linux

**1.** Luckily, darkstat is available in the software repositories of mainstream Linux distributions such as RHEL/CentOS and Debian/Ubuntu.

$ sudo apt-get install darkstat # Debian/Ubuntu

$ sudo yum install darkstat # RHEL/CentOS

$ sudo dnf install darkstat # Fedora 22+

**2.** After installing darkstat, you need to configure it in the main configuration file **/etc/darkstat/init.cfg**.

$ sudo vi /etc/darkstat/init.cfg

Note that for the purpose of this tutorial, we will only explain mandatory as well as important configuration options for you to start using this tool.

Now change the value of **START\_DARKSTAT** from no to yes and set the interface darkstat will listen on with the **INTERFACE** option.

And also **uncoment** **DIR=”/var/lib/darkstat”** and **DAYLOG=”–daylog darkstat.log”** options to specify its directory and log file respectively.

START\_DARKSTAT=yes

INTERFACE="-i ppp0"

DIR="/var/lib/darkstat"

# File will be relative to $DIR:

DAYLOG="--daylog darkstat.log"

**3.** Start the darkstat daemon for now and enable it to start at system boot as follows.

**------------ On SystemD ------------**

$ sudo systemctl start darkstat

$ sudo /lib/systemd/systemd-sysv-install enable darkstat

$ sudo systemctl status darkstat

**------------ On SysV Init ------------**

$ sudo /etc/init.d/darkstat start

$ sudo chkconfig darkstat on

$ sudo /etc/init.d/darkstat status

**4.** By default, darkstat listens on port **667**, so open the port on firewall to allow access.

**------------ On FirewallD ------------**

$ sudo firewall-cmd --zone=public --permanent --add-port=667/tcp

$ sudo firewall-cmd --reload

**------------ On IPtables ------------**

$ sudo iptables -A INPUT -p udp -m state --state NEW --dport 667 -j ACCEPT

$ sudo iptables -A INPUT -p tcp -m state --state NEW --dport 667 -j ACCEPT

$ sudo service iptables save

**------------ On UFW Firewall ------------**

$ sudo ufw allow 667/tcp

$ sudo ufw reload

**5.** Finally, access the darkstat web interface by going to URL **http://Server-IP:667**.Darkstat Network Traffic Analyzer

You can reload graphs automatically by clicking on and off buttons.

### Manage Darkstat From Command Line in Linux

Here, we will explain a few important examples of how you can operate darkstat from the command line.

**6.** To collect network statistics on the **eth0** interface, you can use the -i flag as below.

$ darkstat -i eth0

**7.** To serve web pages on a specific port, include the -p flag like this.

$ darkstat -i eth0 -p 8080

**8.** To keep an eye on network statistics for a given service, use the -f or filter flag. The specified filter expression in the example below will capture traffic concerned with SSH service.

$ darkstat -i eth0 -f "port 22"

Last but not least, if you want to shut darkstat down in a clean way; it is recommended to send SIGTERM or SIGINT signal to the darkstat parent process.

First, get the darkstat parent process **ID** (**PPID**) using the [pidof command](https://www.tecmint.com/how-to-kill-a-process-in-linux/" \t "_blank):

$ pidof darkstat

Then kill the process like so:

$ sudo kill -SIGTERM 4790

OR

$ sudo kill -15 4790

For additional usage options, read through the darkstat manpage:

$ man darkstat

**LAB EXPERIMENT 6**

**Social Engineering using SEToolkit**

# Aim:

To perform social engineering using SEToolkit.

# Tool(s):

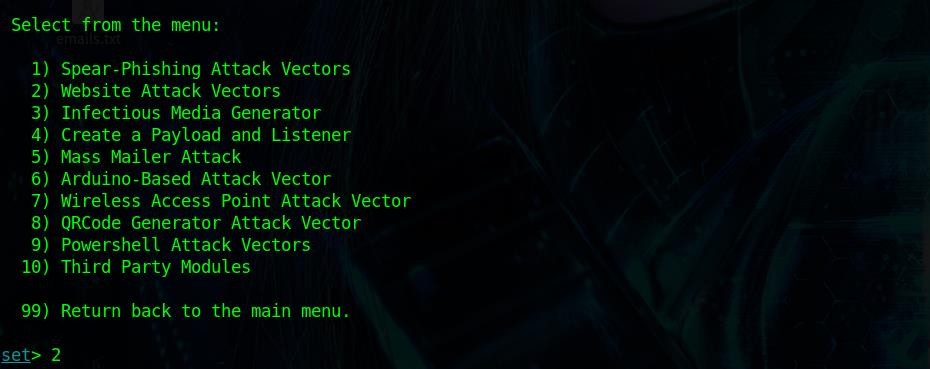
* + 1. **SEToolkit**

The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kinds of tools use human behaviours to trick them to the attack vectors.

# Commands:

* + 1. **Credentials Harvester Method using Google Template**

**Step 1:** Firstly, go to Application > Pentesting > Exploitation Tools > Social Engineering > social engineering toolkit in Parrot OS 5.0.2 Security Edition. Once the terminal is open, type 2 for Website Attack Vectors from the SEToolkit menu as shown below in figure 18.



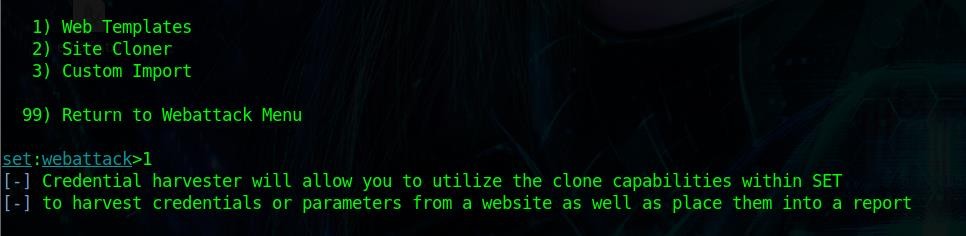
**Figure 18: SEToolkit Website Attack Vectors**

**Step 2:** Then, select option 3 for Credentials Harvester Attack Method as shown below in figure 19.



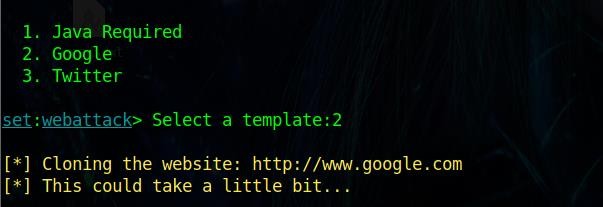
**Figure 19: SEToolkit Credentials Harvester Method**

**Step 3:** Next, select option 1 for Web Templates as shown below in figure 20.



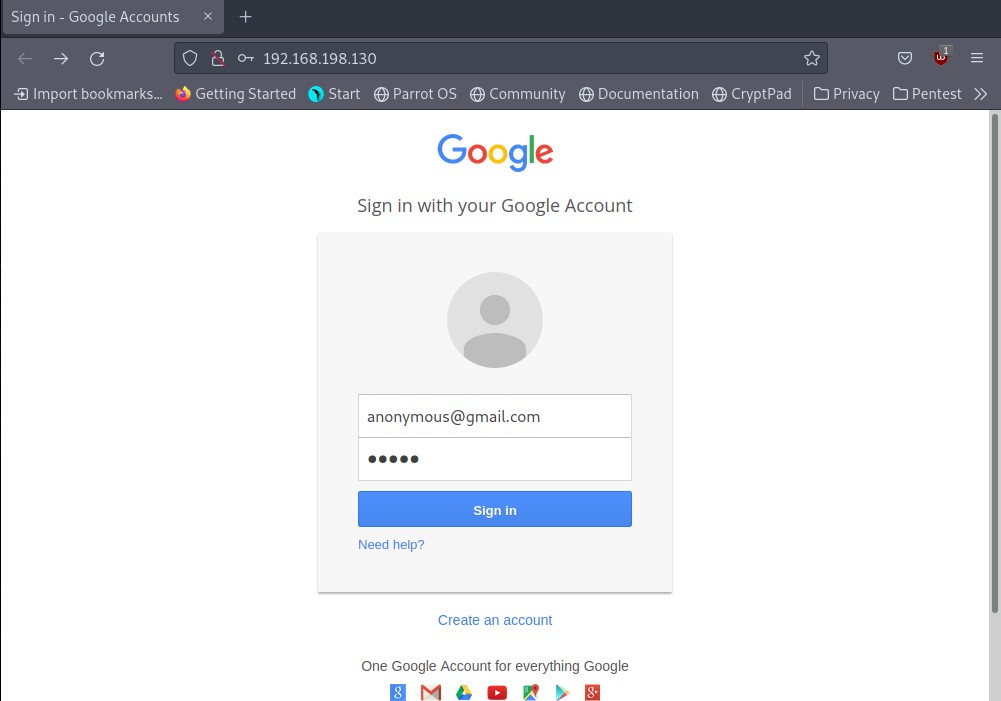
**Figure 20: SEToolkit Web Templates**

**Step 4:** Then, select Google as it is the option 2 as the template as shown below in figure 21. This will take a some time as it clones the website https:/[/ww](http://www.google.com/)w[.google.com.](http://www.google.com/)

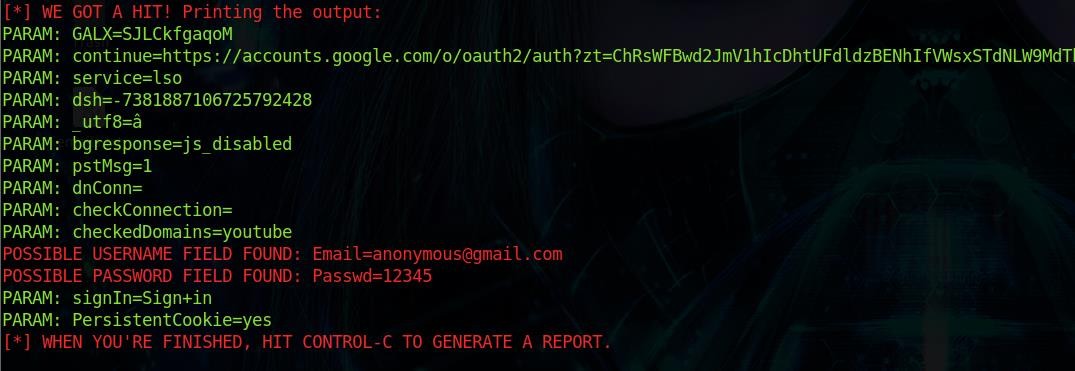


**Figure 21: SEToolkit Google as Web Template**

**Step 5:** Finally, lets navigate to our localhost, in this case it is 192.168.198.130. It will show the google login page for us to enter the login credentials and click sign in as shown below in figure 22. Once signed in, the page will get redirected to google.com and it will capture the credentials in the terminal as shown in figure 23.



**Figure 22: Localhost**



**Figure 23: Reflected Credentials**

# Reference:

https:/[/ww](http://www.tutorialspoint.com/kali_linux/kali_linux_social_engineering.htm)w[.tutorialspoint.com/kali\_linux/kali\_linux\_social\_engineering.htm](http://www.tutorialspoint.com/kali_linux/kali_linux_social_engineering.htm)

**LAB EXPERIMENT 7**

**Spoofing email id using Emkei’s Mailer**

# Aim:

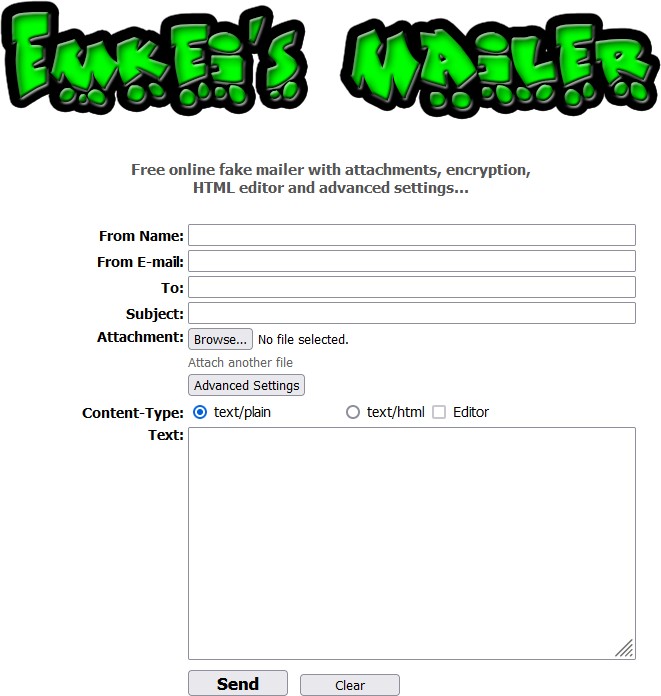
To demonstrate spoofing email id using Emkei’s Mailer.

# Tool(s):

* + 1. **emkei.cz**

Emkei’s Mailer is a free online fake mailer with attachments, encryption, HTML editor and other advanced settings.

# Commands:



Fill in the ***From Name***, ***From E-mail***, ***To***, ***Subject***, ***Attachment***, select the ***Content- Type***, ***Text*** and click on ***Send***. The victim will receive the fake mail.

# References:

https://emkei.cz/