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. Bishwajeet Kumar Pandey
Faculty In-charge

A. Mangalam Kallo
20BTRCI002

CONTENTS

LAB EXPERIMENT 1

Website Technical Information Gathering

1.1 Aim:

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

1.2 Tool(s):

1.2.1 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

1.3 Commands:

1.3.1 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.

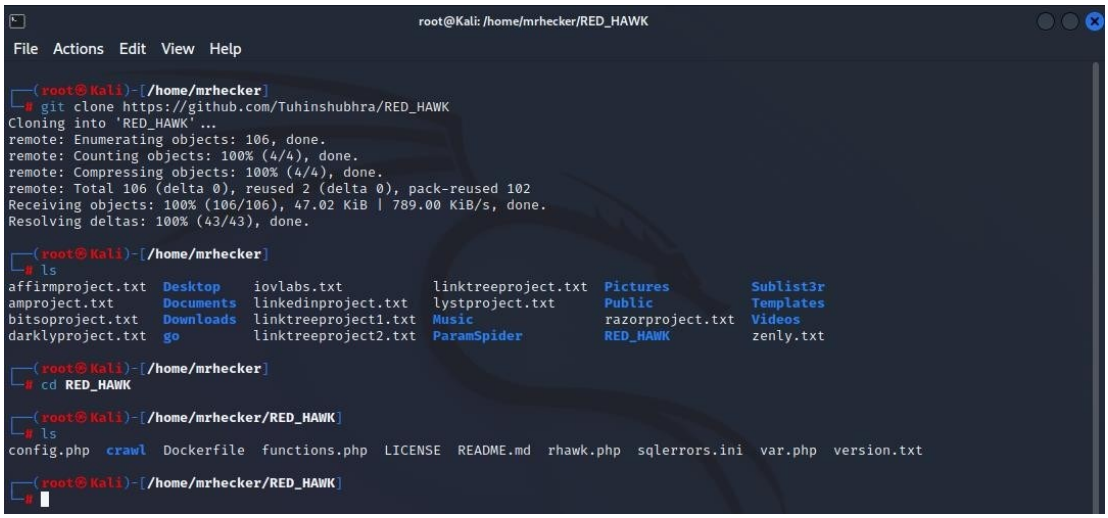


Figure 1: Red Hawk Tool Installation

1.3.2 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

1.3.3 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.

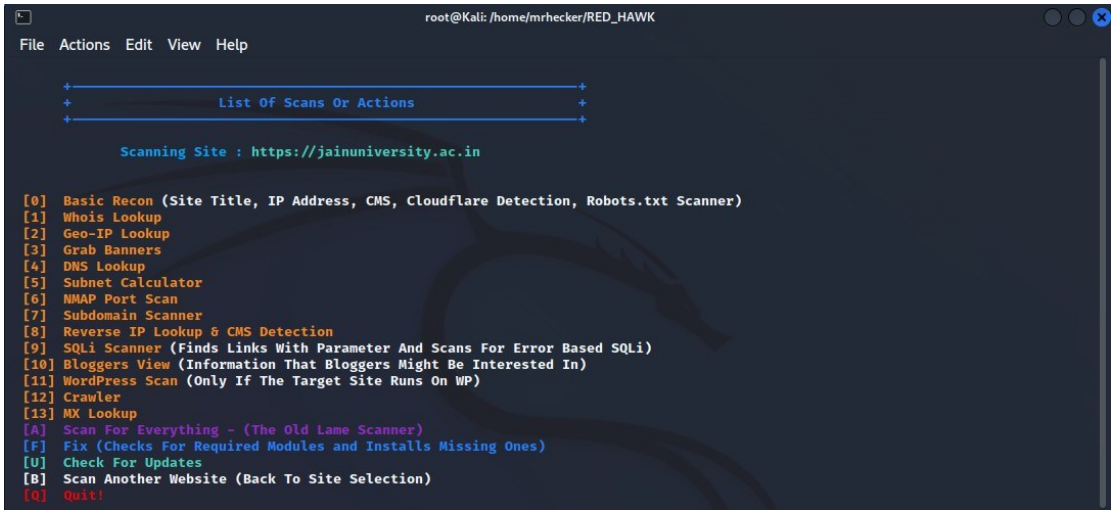


Figure 3: Red Hawk Information Gathering Options

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

1.3.3.1 [0] Basic Recon

```
[#] Choose Any Scan OR Action From The Above List: 0

[+] Scanning Begins ...
[i] Scanning Site: https://jainuniversity.ac.in
[S] Scan Type : BASIC SCAN

[iNFO] Site Title:  Best University in Bangalore | JAIN (Deemed-to-be University)
[iNFO] IP address: 104.21.41.132
[iNFO] Web Server: cloudflare
[iNFO] CMS: Could Not Detect
[iNFO] Cloudflare: Detected
[iNFO] Robots File:
```

Figure 4: Red Hawk Basic Recon Scanning

1.3.3.2 [3] Grab Banners

```
[#] Choose Any Scan OR Action From The Above List: 3

[+] Scanning Begins ...
[i] Scanning Site: https://jainuniversity.ac.in
[S] Scan Type : Banner Grabbing


HTTP/1.1 301 Moved Permanently
Date: Thu, 03 Nov 2022 18:49:45 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: close
X-Frame-Options: SAMEORIGIN
Location: https://www.jainuniversity.ac.in/
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hErbsOmxYVAp1xCyd59VJg56dg5%2BeQ8%2ByovIP1FuuerzIM%2Fj
CX9QgvMoK1MYo%2B1A1zAPchvITG%2F5NRbFo9FJKCSQe0SqTgqyp5KHlU%2B0UCmKUnLosWItyz2SxILEYZ19%2F6HbzfP5jw%3D%3D"}],"group":"cf-nel","max_ag
e":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 76474aa70a109137-FRA
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
HTTP/1.1 200 OK
Date: Thu, 03 Nov 2022 18:49:46 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=284d2c46befcc50e6c94cca6d7aedc73; path=/
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: no-referrer
Feature-Policy: geolocation 'self'; vibrate 'none'
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uBNsX0VQ6zTxXR8io6E5HPRR9UFAMZovc88RYSuwWgIPbaRaPXeKiM
khmCMi60fIH%2F65u%2B8sul4LsIcoU3rJifCizIu2rNAnA5GuZw8HhuXpYX9kOq0vmBNC27tNsYZ684RtGOY%2Fjh%2F7gDM%3D"}],"group":"cf-nel","max_age":6
04800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 76474aacfcd8bbe5-FRA
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
```

Figure 5: Red Hawk Banner Grabbing

1.3.3.3 [5] Subnet Calculator

```
[#] Choose Any Scan OR Action From The Above List: 5

[+] Scanning Begins ...
[i] Scanning Site: https://jainuniversity.ac.in
[S] Scan Type : SubNet Calculator


[SubNet Calc] Address       = 2606:4700:3031::ac43:935f
[SubNet Calc] Network       = 2606:4700:3031::ac43:935f / 128
[SubNet Calc] Netmask       = ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
[SubNet Calc] Wildcard Mask = ::
[SubNet Calc] Hosts Bits    = 1
[SubNet Calc] Max. Hosts    = 1   (2^1 - 1)
[SubNet Calc] Host Range    = { 2606:4700:3031::ac43:935f - 2606:4700:3031::ac43:935f }

[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

Figure 6: Red Hawk Subnet Calculator

1.4 Reference:

https://github.com/Tuhinshubhra/RED_HAWK

LAB EXPERIMENT 2

Port Scanning and Enumeration using Tools

2.1 Aim:

To demonstrate port scanning and enumeration using tools.

2.2 Tool(s):

2.2.1 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.

2.2.2 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.

2.3 Commands:

2.3.1 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.

```
┌──(mrhecker㉿Kali)-[~]
└─$ nmap 192.168.0.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 00:04 IST
Nmap scan report for 192.168.0.137 (192.168.0.137)
Host is up (0.0040s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 11.02 seconds
```

Figure 7: *nmap 192.168.0.137*

2.3.2 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.

```
┌──(mrhecker㉿Kali)-[~]
└─$ nmap -A -T5 192.168.0.137 -p 80 -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 00:44 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.03s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Initiating Ping Scan at 00:44
Scanning 192.168.0.137 [2 ports]
Completed Ping Scan at 00:44, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:44
Completed Parallel DNS resolution of 1 host. at 00:44, 0.00s elapsed
Initiating Connect Scan at 00:44
Scanning 192.168.0.137 (192.168.0.137) [1 port]
Discovered open port 80/tcp on 192.168.0.137
Completed Connect Scan at 00:44, 0.00s elapsed (1 total ports)
Initiating Service scan at 00:44
Scanning 1 service on 192.168.0.137 (192.168.0.137)
Completed Service scan at 00:44, 6.06s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.0.137.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.19s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Nmap scan report for 192.168.0.137 (192.168.0.137)
Host is up, received syn-ack (0.0068s latency).
Scanned at 2022-11-07 00:44:04 IST for 6s

PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL... )
|_http-favicon: Unknown favicon MD5: 1F8C0B08FB6B556A6587517A8D5F290B
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3
.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-title: owaspbwa OWASP Broken Web Applications

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:44
Completed NSE at 00:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.89 seconds
```

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

2.3.3 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.

```
┌──(erhecker㉿Kali)-[~]
└─$ nikto -h 192.168.0.137
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.137
+ Target Hostname:    192.168.0.137
+ Target Port:        80
+ Start Time:         2022-11-07 01:34:07 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.3
8 mod_perl/2.0.4 Perl/v5.10.1
+ Server may leak inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Fri Jul 31 08:25:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives
 for 'index' were found: index.css, index.html
+ OSVDB-39272: /favicon.ico file identifies this app/server as: owasp.org
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. htt
p://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Cookie phpbb2owaspbwa_data created without the httponly flag
+ Cookie phpbb2owaspbwa_sid created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8877 requests: 1 error(s) and 35 item(s) reported on remote host
+ End Time:           2022-11-07 01:35:22 (GMT5.5) (75 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 9: nikto -h 192.168.0.137

2.4 Reference:

https://nmap.org/

https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

LAB EXPERIMENT 3

Network scanning and vulnerability scanner tool

3.1 Aim:

To demonstrate network scanning and vulnerability scanning tool.

3.2 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.

3.3 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*** to find for vulnerabilities. Type the URL and IP Address in the ***Name*** and ***Targets*** text boxes as shown in the figure 10 below.

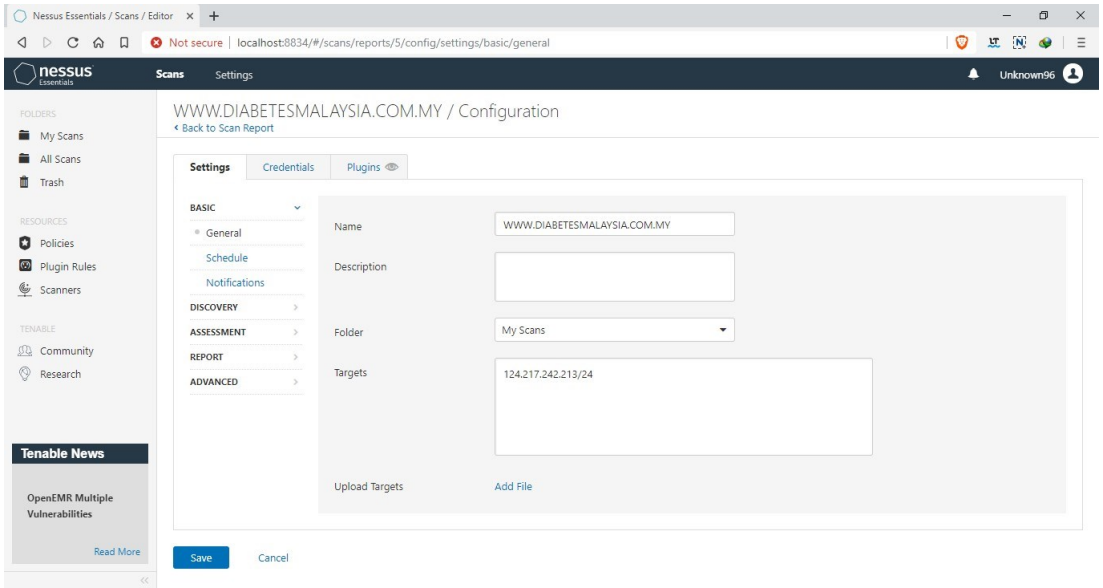


Figure 10: Nessus Scan Configuration

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.

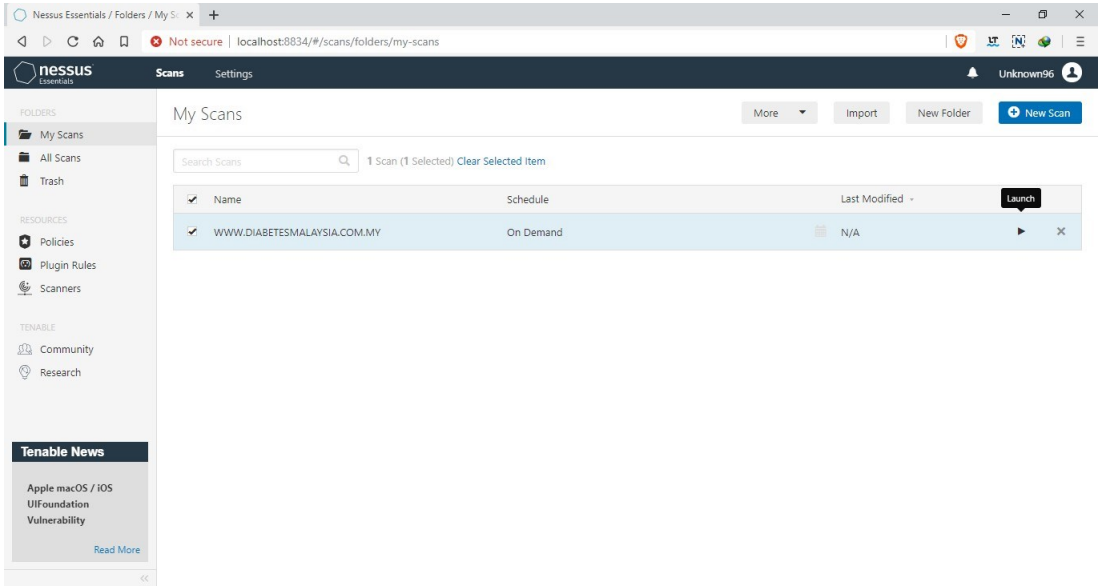


Figure 11: Nessus Scans List

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.

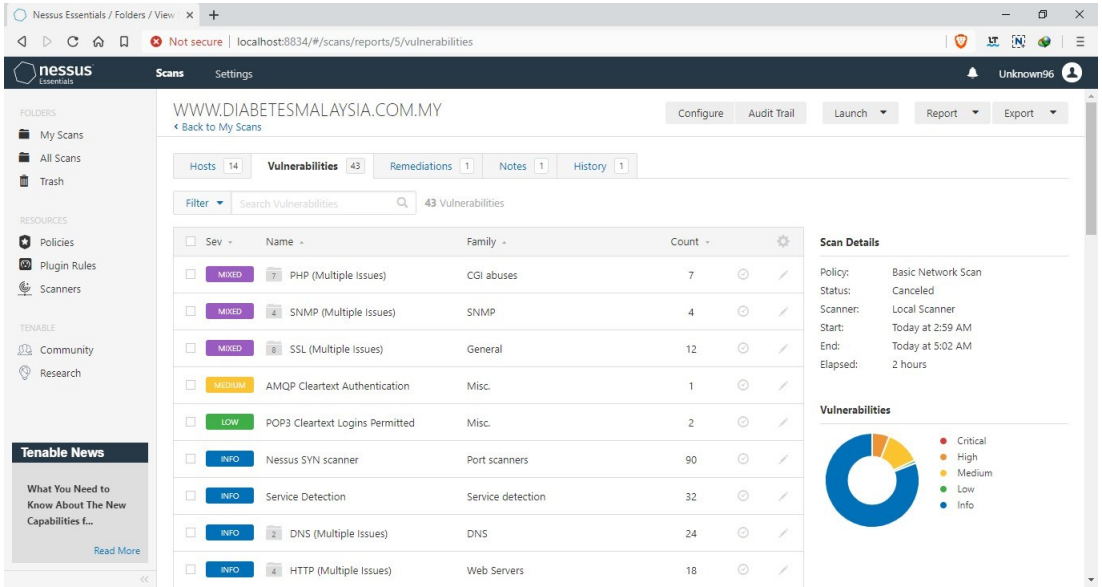


Figure 12: Nessus Vulnerabilities List

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.

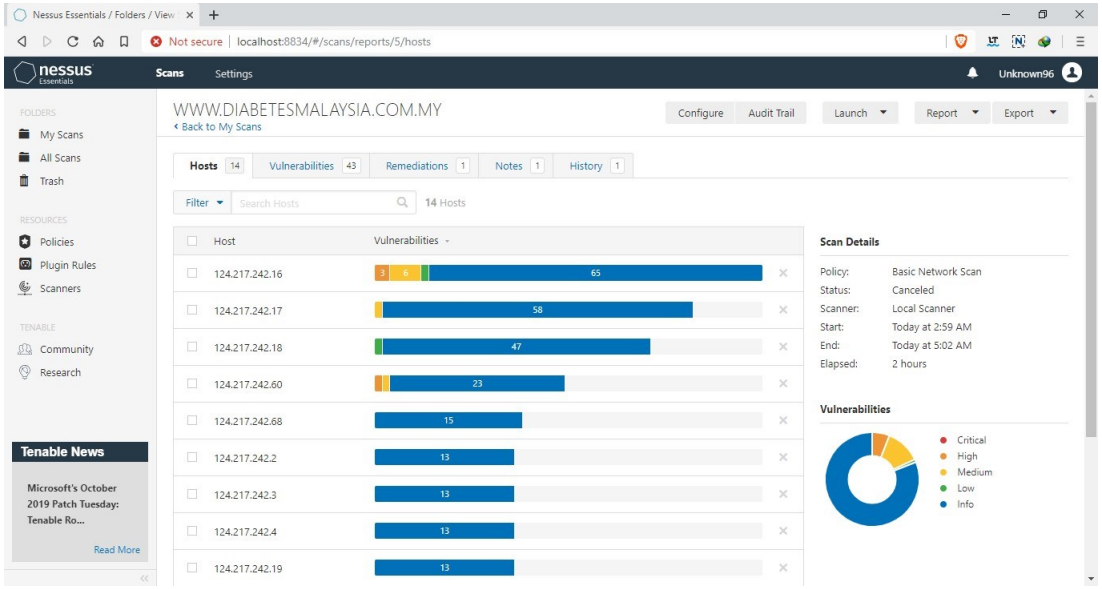


Figure 13: Nessus Hosts List

3.4 Reference:

https://www.cs.cmu.edu/~dwendlan/personal/nessus.html

LAB EXPERIMENT 4

Data Enumeration by Nmap

4.1 Aim:

To enumerate information using Nmap.

4.2 Tool(s):

4.2.1 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.

4.3 Commands:

4.3.1 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.

```
┌──(mrhecker㉿Kali)-[~]
└─$ nmap 192.168.0.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 03:13 IST
Nmap scan report for 192.168.0.137 (192.168.0.137)
Host is up (0.0099s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

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.

```
┌──(mrhecker㉿Kali)-[~]
└─$ nmap -sV -p22 192.168.0.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 03:23 IST
Nmap scan report for 192.168.0.137 (192.168.0.137)
Host is up (0.0028s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

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

4.3.2 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.

```
┌──(mrhecker㉿Kali)-[~]
└─$ sudo su
[sudo] password for mrhecker:
┌──(root㉿Kali)-[/home/mrhecker]
└─# nmap -O 134.209.18.185
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 03:35 IST
Nmap scan report for 185.18.209.134.in-addr.arpa (134.209.18.185)
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

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.

```
┌──(root㉿Kali)-[/home/mrhecker]
└─# searchsploit Linux 2.4.20
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                 |  Path
---------------------------------------------------------------------------------------------------------------
Alienvault Open Source SIEM (OSSIM) < 4.7.0 - 'get_license' Remote Command Execution (Metasploit)              | linux/remote/42697.rb
Alienvault Open Source SIEM (OSSIM) < 4.7.0 - av-centerd 'get_log_line()' Remote Code Execution                | linux/remote/33805.pl
Alienvault Open Source SIEM (OSSIM) < 4.8.0 - 'get_file' Information Disclosure (Metasploit)                   | linux/remote/42695.rb
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation                          | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                               | linux/webapps/42745.py
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                            | linux/webapps/39642.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                   | linux/dos/36906.txt
AppArmor securityfs < 4.8 - 'aa_fs_seq_hash_show' Reference Count Leak                                         | linux/dos/40181.c
Berlios GPSD 1.91-1 < 2.7-2 - Format String                                                                    | linux/remote/10029.rb
Centreon < 2.5.1 / Centreon Enterprise Server < 2.2 - SQL Injection / Command Injection (Metasplo              | linux/webapps/41676.rb
CyberArk < 10 - Memory Disclosure                                                                              | linux/remote/44829.py
CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure                                                       | linux/dos/44428.txt
Dell EMC RecoverPoint < 5.1.2 - Local Root Command Execution                                                   | linux/local/44920.txt
Dell EMC RecoverPoint < 5.1.2 - Remote Root Command Execution                                                  | linux/remote/44921.txt
Dell EMC RecoverPoint boxmgmt CLI < 5.1.2 - Arbitrary File Read                                                | linux/local/44688.txt
DenyAll WAF < 6.3.0 - Remote Code Execution (Metasploit)                                                       | linux/webapps/42769.rb
Elm < 2.5.8 - Expires Header Remote Buffer Overflow                                                            | linux/remote/1171.c
Exim < 4.86.2 - Local Privilege Escalation                                                                     | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execution                                                                | linux/remote/44571.py
F-Secure Internet GateKeeper for Linux < 2.15.484 / Gateway < 2.16 - Local Privilege Escalation                | linux/local/1297.py
glibc < 2.26 - 'getcwd()' Local Privilege Escalation                                                           | linux/local/43775.c
Gnome Web (Epiphany) < 3.28.2.1 - Denial of Service                                                            | linux/dos/44857.html
Grep < 2.11 - Integer Overflow Crash (PoC)                                                                     | linux/dos/23779.txt
Haraka < 2.8.9 - Remote Command Execution                                                                      | linux/remote/41162.py
ISC DHCP dhclient < 3.1.2p1 - Remote Buffer Overflow (PoC)                                                     | linux/dos/9265.c
Jfrog Artifactory < 4.16 - Arbitrary File Upload / Remote Command Execution                                    | linux/webapps/44543.txt
LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure                                           | linux/remote/44022.md
Linux < 4.14.103 / < 4.19.25 - Out-of-Bounds Read and Write in SNMP NAT Module                                 | linux/dos/46477.txt
Linux < 4.16.9 / < 4.14.41 - 4-byte Infoleak via Uninitialized Struct Field in compat adjtimex Sy              | linux/dos/44641.c
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged write() to /proc/*/mem                          | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                                      | solaris/local/15962.c
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation (3)                     | linux/local/9844.py
Linux Kernel 2.4.20 - 'decode_fh' Denial of Service                                                            | linux/dos/68.c
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Local Privilege Escalation (Metaspl             | linux/local/19933.rb
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Race Condition Privilege Escalation                 | linux_x86-64/local/33516.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                                           | linux/dos/43234.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                                     | linux/local/41886.c
Linux Kernel < 2.4.20 - Module Loader Privilege Escalation                                                     | linux/local/12.c
Linux Kernel < 2.4.36.9/2.6.27.5 - Unix Sockets Local Kernel Panic (Denial of Service)                         | linux/dos/7091.c
Linux Kernel < 2.6.11.5 - BlueTooth Stack Privilege Escalation                                                 | linux/local/4756.c
Linux Kernel < 2.6.14.6 - 'procfs' Kernel Memory Disclosure                                                    | linux/local/9363.c
Linux Kernel < 2.6.16.18 - Netfilter NAT SNMP Module Remote Denial of Service                                  | linux/dos/1880.c
Linux Kernel < 2.6.19 (Debian 4) - 'udp_sendmsg' Local Privilege Escalation (3)                                | linux/local/9575.c
```

Figure 17: *searchsploit Linux 2.4.20*

4.4 Reference:

https://www.kali.org/tools/nmap/

LAB EXPERIMENT 5

Social Engineering using SEToolkit

5.1 Aim:

To perform social engineering using SEToolkit.

5.2 Tool(s):

5.2.1 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.

5.3 Commands:

6.3.1 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.

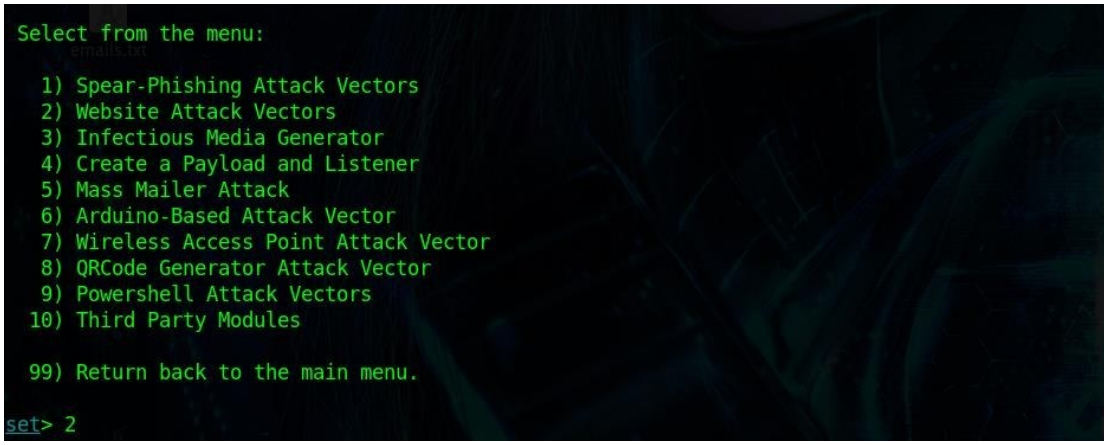


Figure 18: SEToolkit Website Attack Vectors

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

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Figure 19: SEToolkit Credentials Harvester Method

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

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
```

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://www.google.com.

```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
```

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.

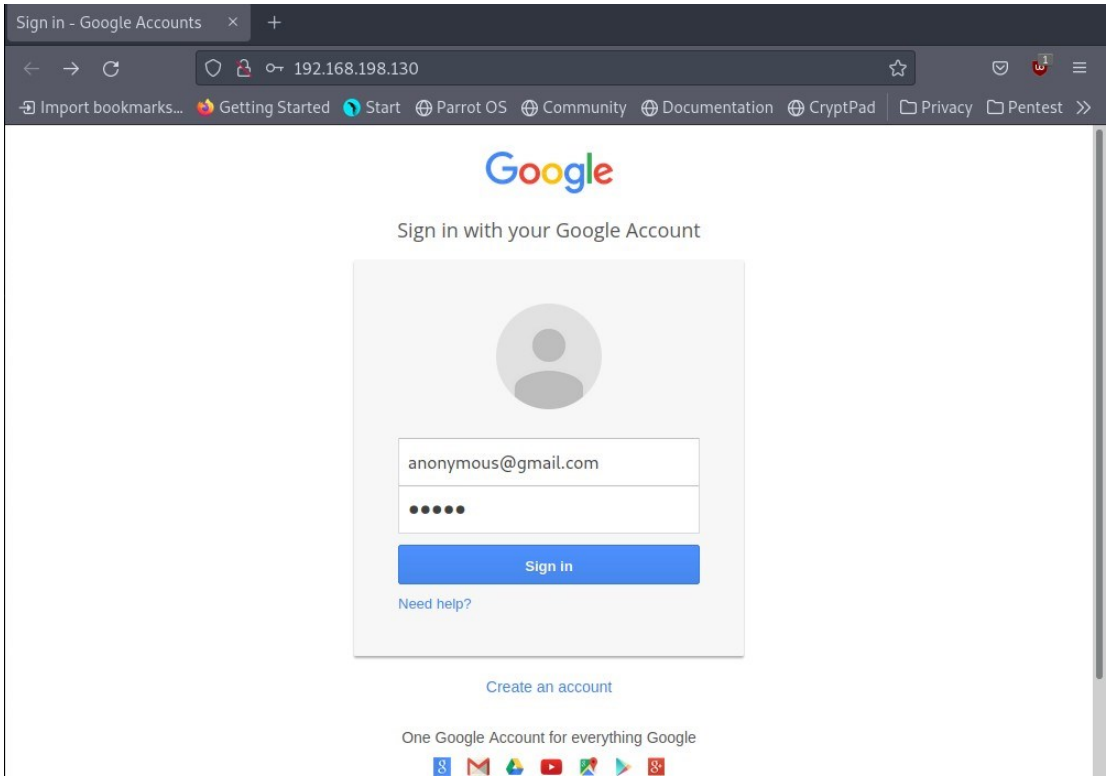


Figure 22: Localhost

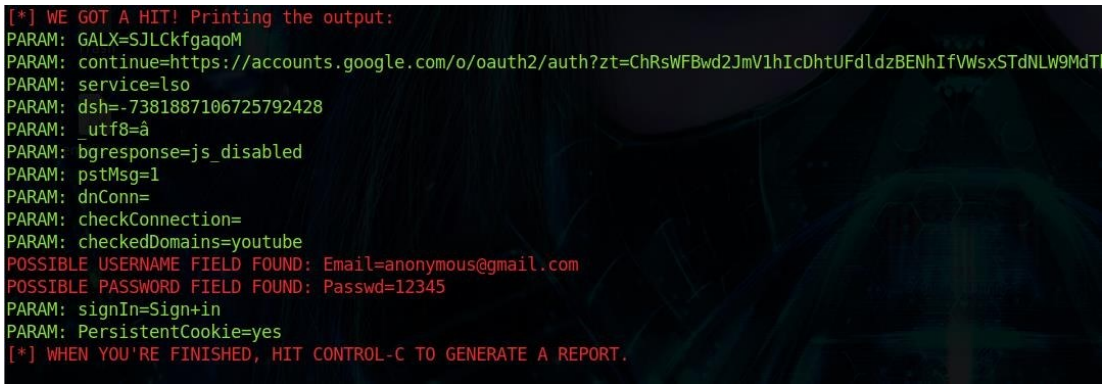


Figure 23: Reflected Credentials

5.4 Reference:

https://www.tutorialspoint.com/kali_linux/kali_linux_social_engineering.htm

LAB EXPERIMENT 6

Spoofing email id using Emkei's Mailer

6.1 Aim:

To demonstrate spoofing email id using Emkei's Mailer.

6.2 Tool(s):

6.2.1 emkei.cz

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

6.3 Commands:

Step 1: Firstly, go to https://emkei.cz/ to write an email as shown in figure 24. Click Send.

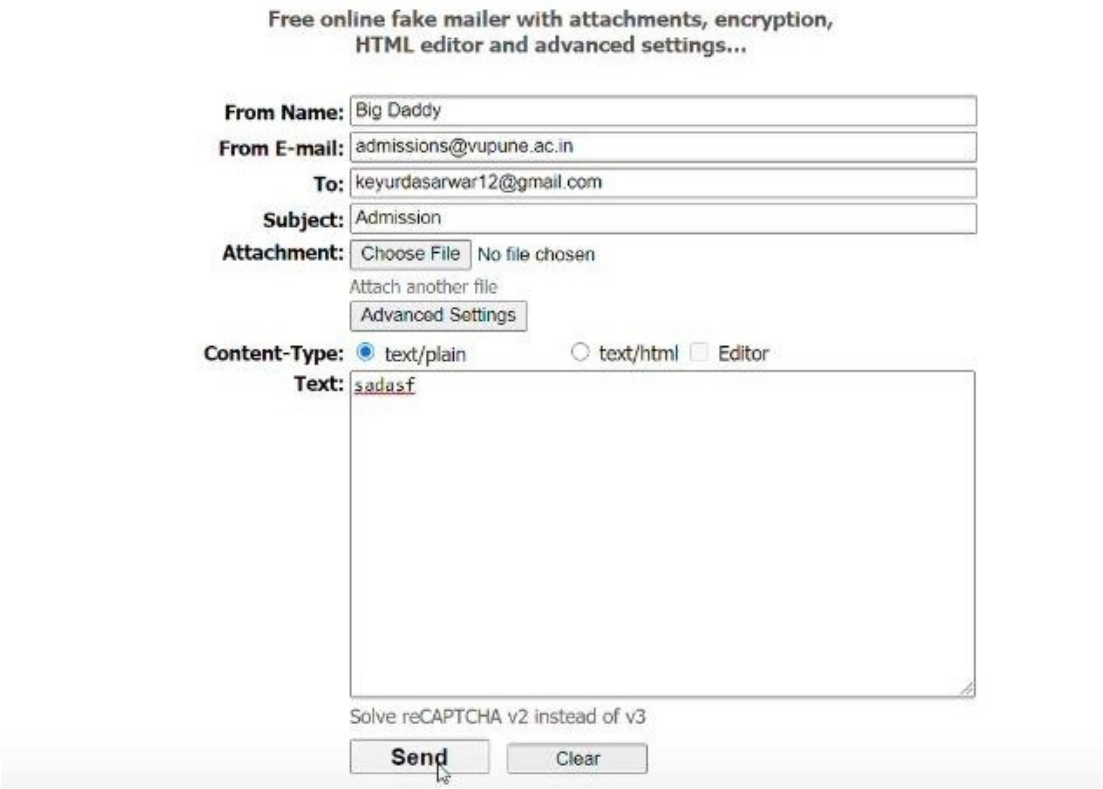


Figure 24: Writing email – emkei.cz

Step 2: Next, you will be redirected to a page with a message E-mail sent successfully as shown in figure 25.

Figure 25: Email sent successfully page

Step 3: Then, the receiver will receive the mail in his/her email inbox as shown in figure 26.

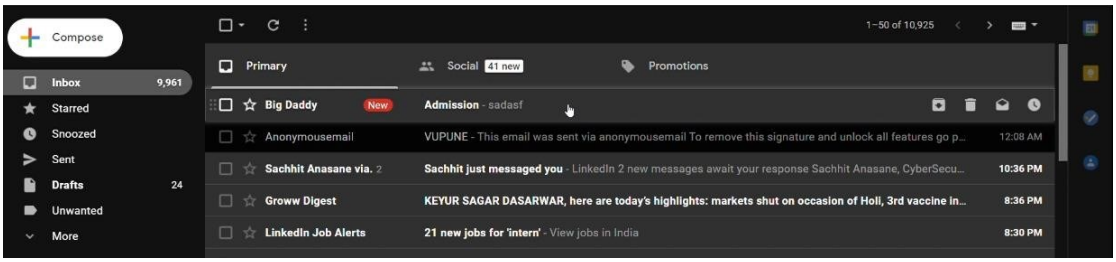


Figure 26: Email Received in Inbox

Step 4: The receiver will click on the message to read it as shown in figure 27.

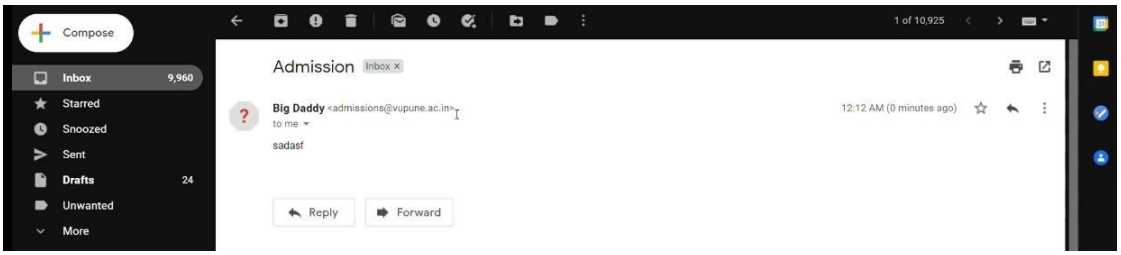


Figure 27: Email Read by Receiver

6.4 References:

https://emkei.cz/

LAB EXPERIMENT 7

Intercept Web Traffic using Burp Proxy

7.1 Aim:

To demonstrate interception of web traffic using Burp Suite proxy.

7.2 Tool(s):

7.2.1 Burp Suite

Burp Suite is a fully functional web application attack tool that can be used to conduct practically any type of penetration test on a website. The capability of Burp Suite to intercept HTTP requests is one of its key features. Typically, HTTP requests are transmitted directly from your browser to a web server, where they are acknowledged, and then returned to your browser. However, with Burp Suite, HTTP requests are sent directly from your browser to Burp Suite, which then snoops on the traffic.

7.3 Commands:

Step 1: Firstly, we are using Kali Linux to perform this experiment. So, Burp Suite is installed by default in Kali Linux. Type command burpsuite to open Burp Suite Community Edition as shown in figure 28.

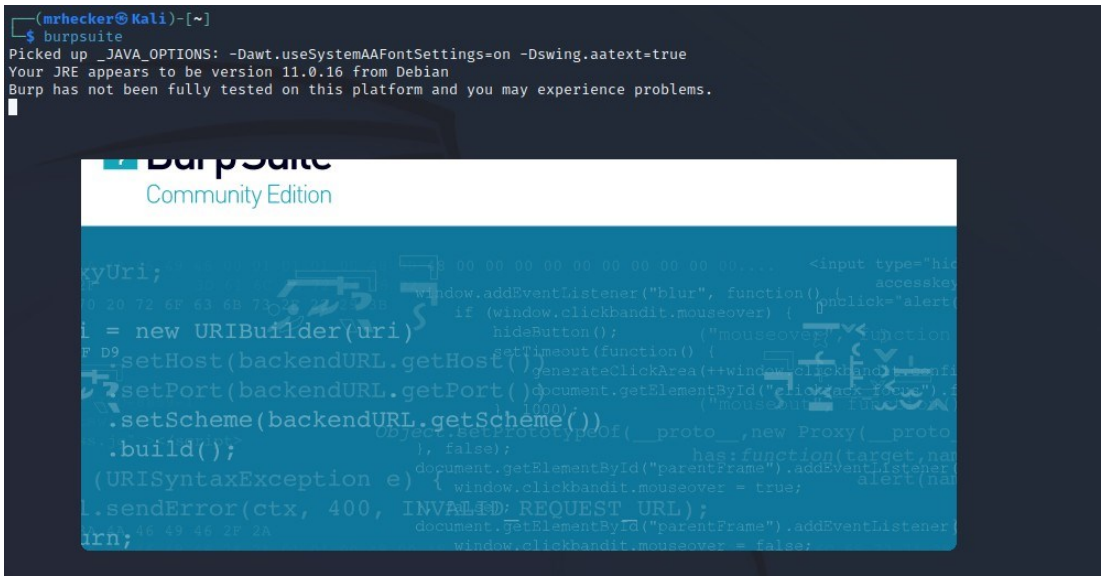


Figure 28: Burp Suite Community Edition

Step 2: Go to Proxy > Intercept tab and click Open Browser to open Burp Suite's Embedded Browser as shown in figure 29.

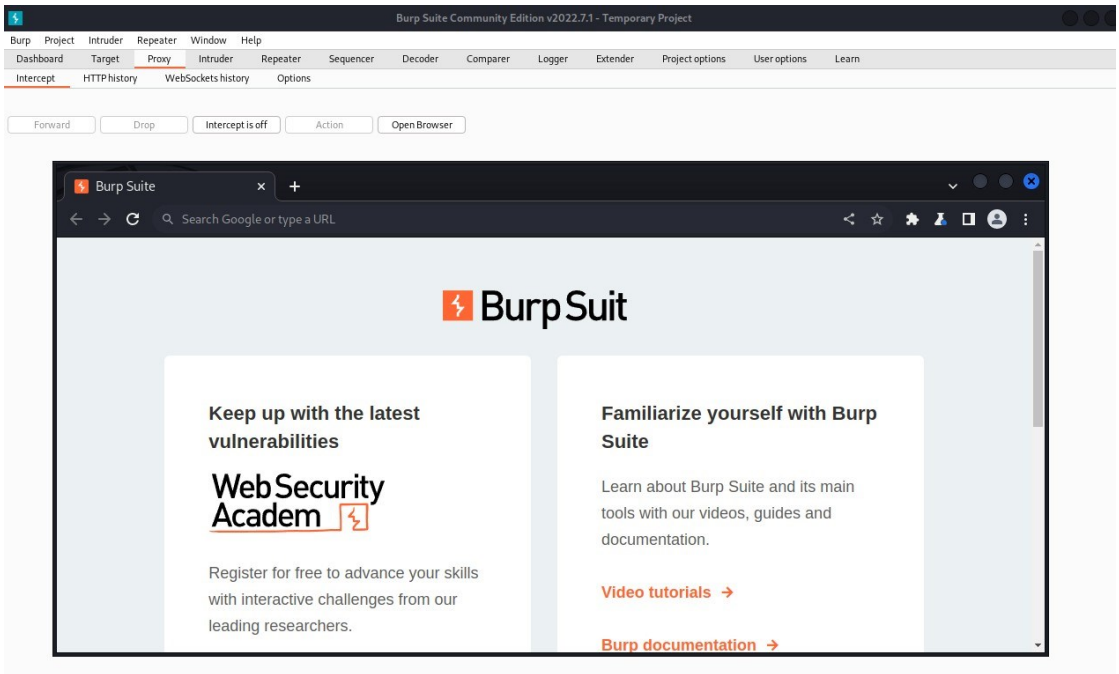


Figure 29: Burp Suite Chromium Browser

Step 3: Next, turn on Intercept as shown in figure 30.

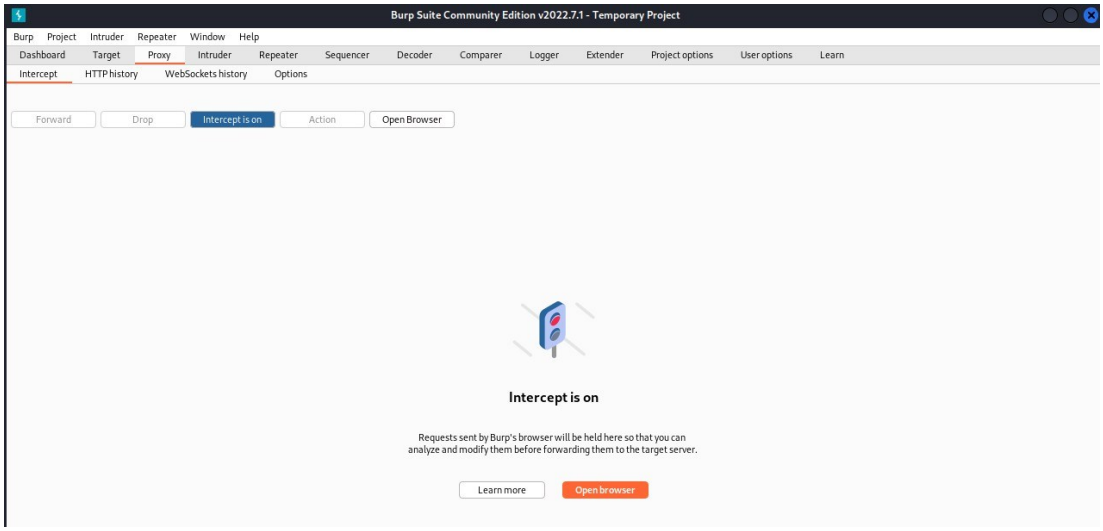


Figure 30: Burp Suite Intercept On

Step 4: Now, go to portswigger.net in the browser and you will see the page won't load. Meanwhile, Burp Suite Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server as shown in figure 31.

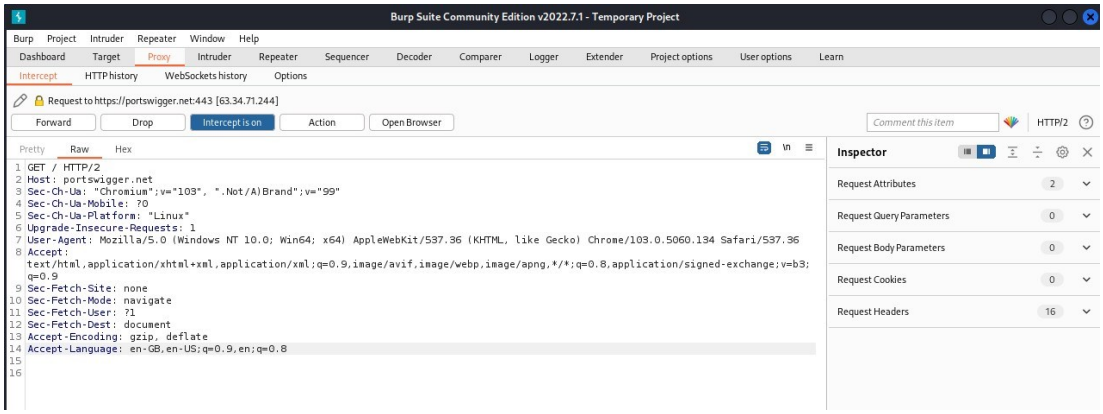


Figure 31: Burp Suite Proxy Interception

Step 5: Forward the requests and subsequent requests in Burp Suite Proxy and you will see the website will be loaded as shown in figure 32.

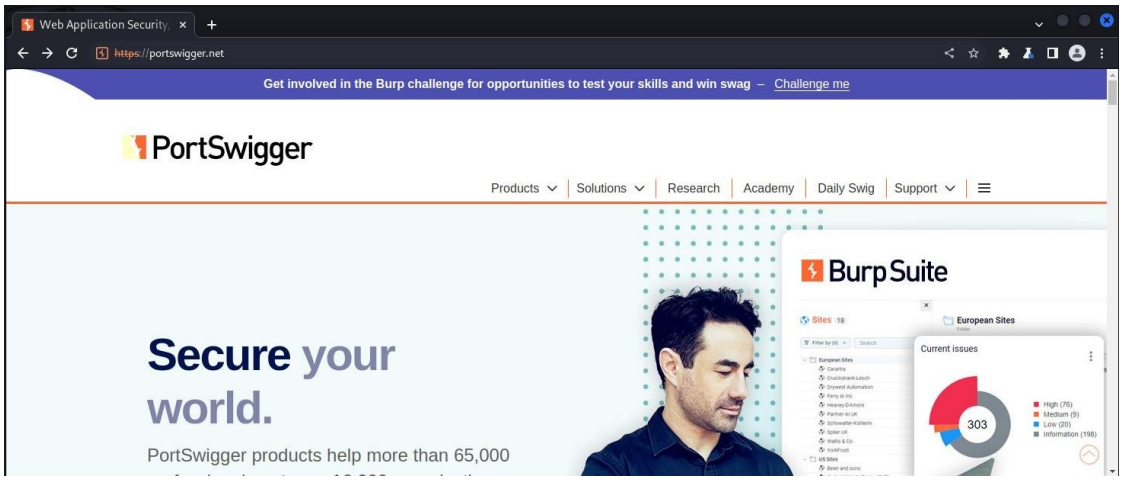


Figure 32: Port Swigger Website – Forward Requests

Step 6: Now, turn off the interception, by clicking on Intercept is on as shown in figure 33. You will be able to interact with the sites you visit normally after this.

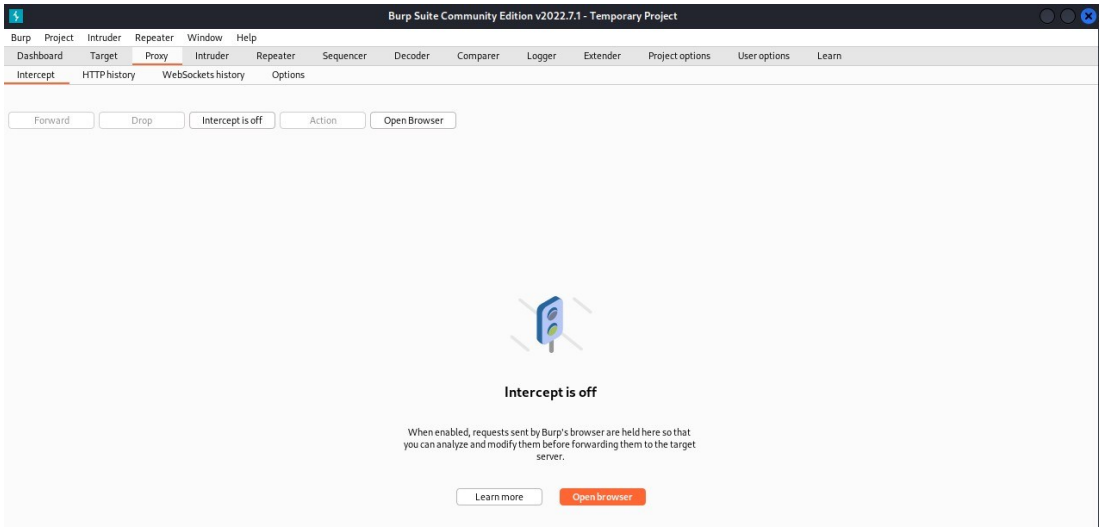
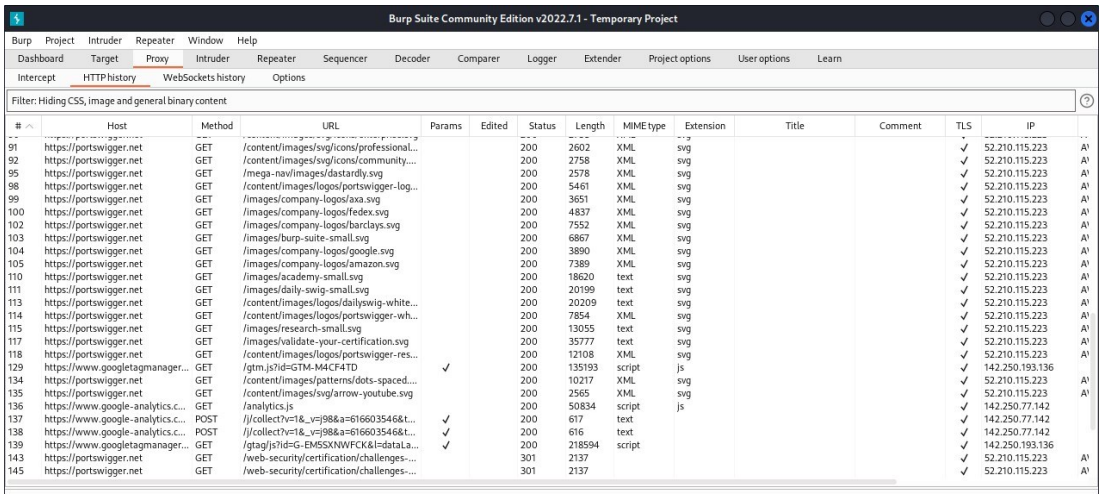


Figure 33: Burp Suite Intercept Off

Step 7: Finally, to view the history of all HTTP traffic that has passed through Burp Proxy, even while interception was switched off, you can go to Proxy > HTTP history tab as shown in figure 34.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
91	https://portswigger.net	GET	/content/images/svg/icons/professional...			200	2602	XML	svg			✓	52.210.115.223
92	https://portswigger.net	GET	/content/images/svg/icons/community....			200	2758	XML	svg			✓	52.210.115.223
95	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			200	2578	XML	svg			✓	52.210.115.223
98	https://portswigger.net	GET	/content/images/logos/portswigger-log...			200	5461	XML	svg			✓	52.210.115.223
99	https://portswigger.net	GET	/images/company-logos/axa.svg			200	3651	XML	svg			✓	52.210.115.223
100	https://portswigger.net	GET	/images/company-logos/fedex.svg			200	4837	XML	svg			✓	52.210.115.223
102	https://portswigger.net	GET	/images/company-logos/barclays.svg			200	7552	XML	svg			✓	52.210.115.223
103	https://portswigger.net	GET	/images/burp-suite-small.svg			200	6867	XML	svg			✓	52.210.115.223
104	https://portswigger.net	GET	/images/company-logos/google.svg			200	3890	XML	svg			✓	52.210.115.223
105	https://portswigger.net	GET	/images/company-logos/amazon.svg			200	7389	XML	svg			✓	52.210.115.223
110	https://portswigger.net	GET	/images/academy-small.svg			200	18620	text	svg			✓	52.210.115.223
111	https://portswigger.net	GET	/images/daily-swig-small.svg			200	20199	text	svg			✓	52.210.115.223
113	https://portswigger.net	GET	/content/images/logos/dailyswig-white...			200	20209	text	svg			✓	52.210.115.223
114	https://portswigger.net	GET	/content/images/logos/portswigger-wh...			200	7854	XML	svg			✓	52.210.115.223
115	https://portswigger.net	GET	/images/research-small.svg			200	13055	text	svg			✓	52.210.115.223
117	https://portswigger.net	GET	/images/validate-your-certification.svg			200	35777	text	svg			✓	52.210.115.223
118	https://portswigger.net	GET	/content/images/logos/portswigger-res...			200	12108	XML	svg			✓	52.210.115.223
129	https://www.googletagmanager...	GET	/gtm.js?id=GTM-M4CF4TD	✓		200	135193	script	js			✓	142.250.193.136
134	https://portswigger.net	GET	/content/images/patterns/dots-spaced....			200	10217	XML	svg			✓	52.210.115.223
135	https://portswigger.net	GET	/content/images/svg/arrow-youtube.svg			200	2565	XML	svg			✓	52.210.115.223
136	https://www.google-analytics.c...	GET	/analytics.js			200	50834	script	js			✓	142.250.77.142
137	https://www.google-analytics.c...	POST	/j/collect?v=1&_v=j98&a=616603546&t...	✓		200	617	text				✓	142.250.77.142
138	https://www.google-analytics.c...	POST	/j/collect?v=1&_v=j98&a=616603546&t...	✓		200	616	text				✓	142.250.77.142
139	https://www.googletagmanager...	GET	/gtag/js?id=G-EM5SXNWFCK&l=dataLa...	✓		200	218594	script				✓	142.250.193.136
143	https://portswigger.net	GET	/web-security/certification/challenges-...			301	2137					✓	52.210.115.223
145	https://portswigger.net	GET	/web-security/certification/challenges-...			301	2137					✓	52.210.115.223

Figure 34: Burp Suite HTTP history tab

7.4 References:

https://www.sciencedirect.com/topics/computer-science/burp-suite