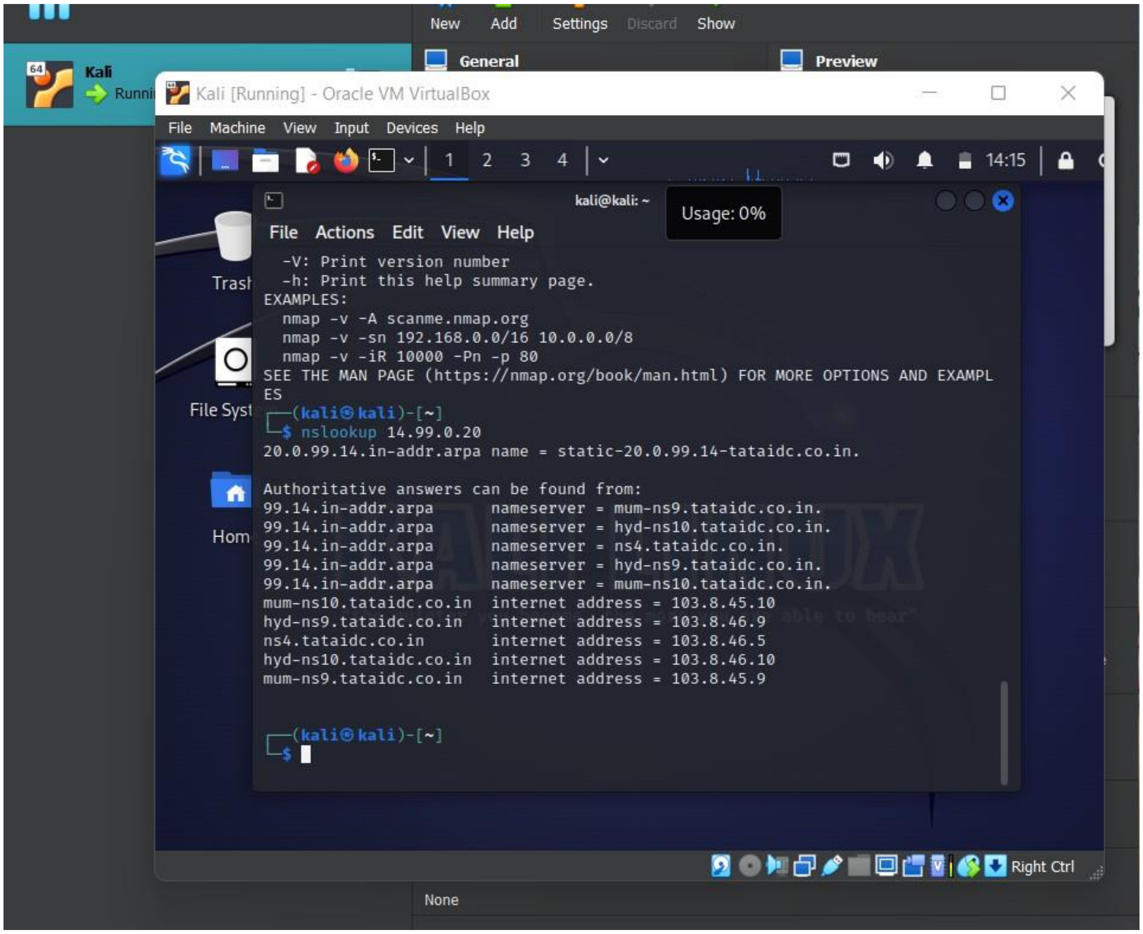
Assignment 2

Name- Dewansh Saini

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

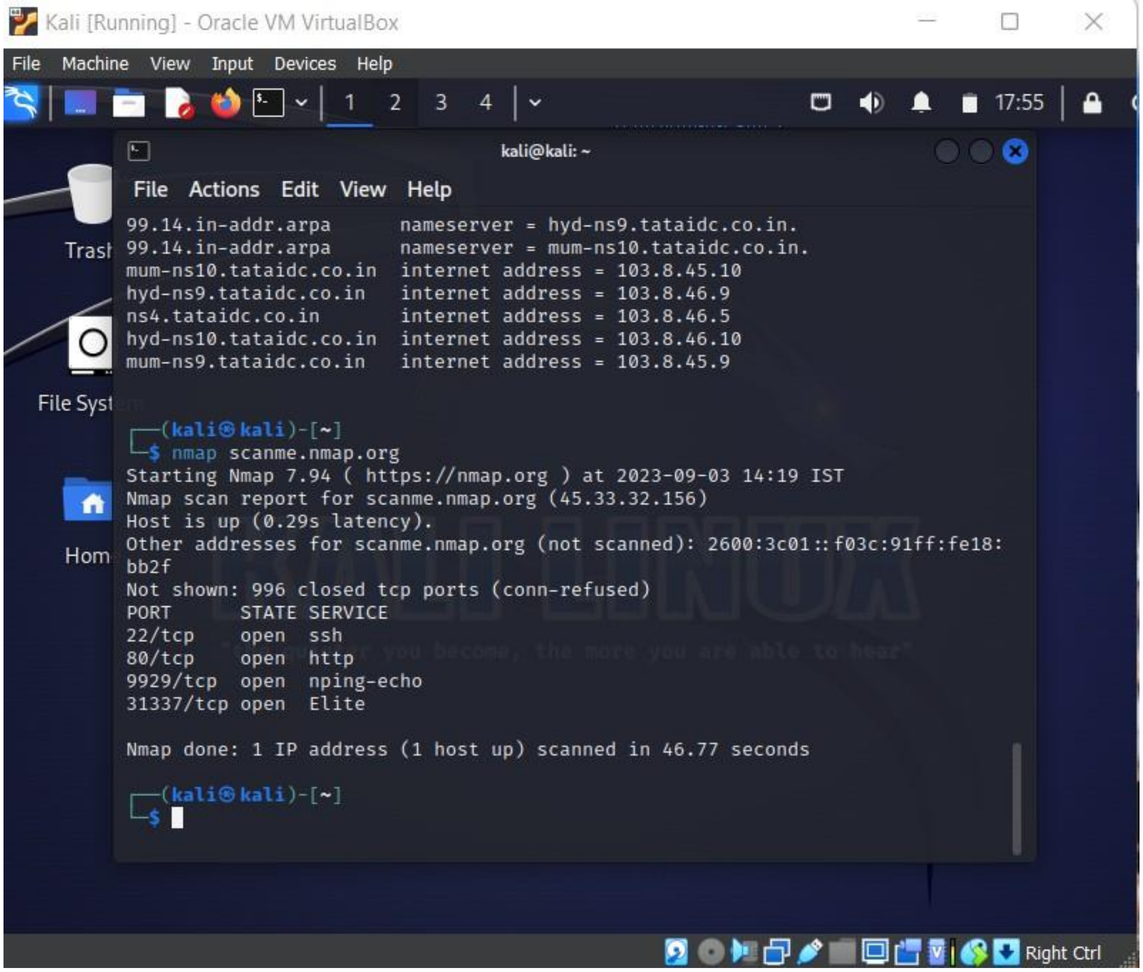
1. **Information gathering applications**

- **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



```
  -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 EXAMPL
ES
┌──(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)-[~]
└─$ 
```

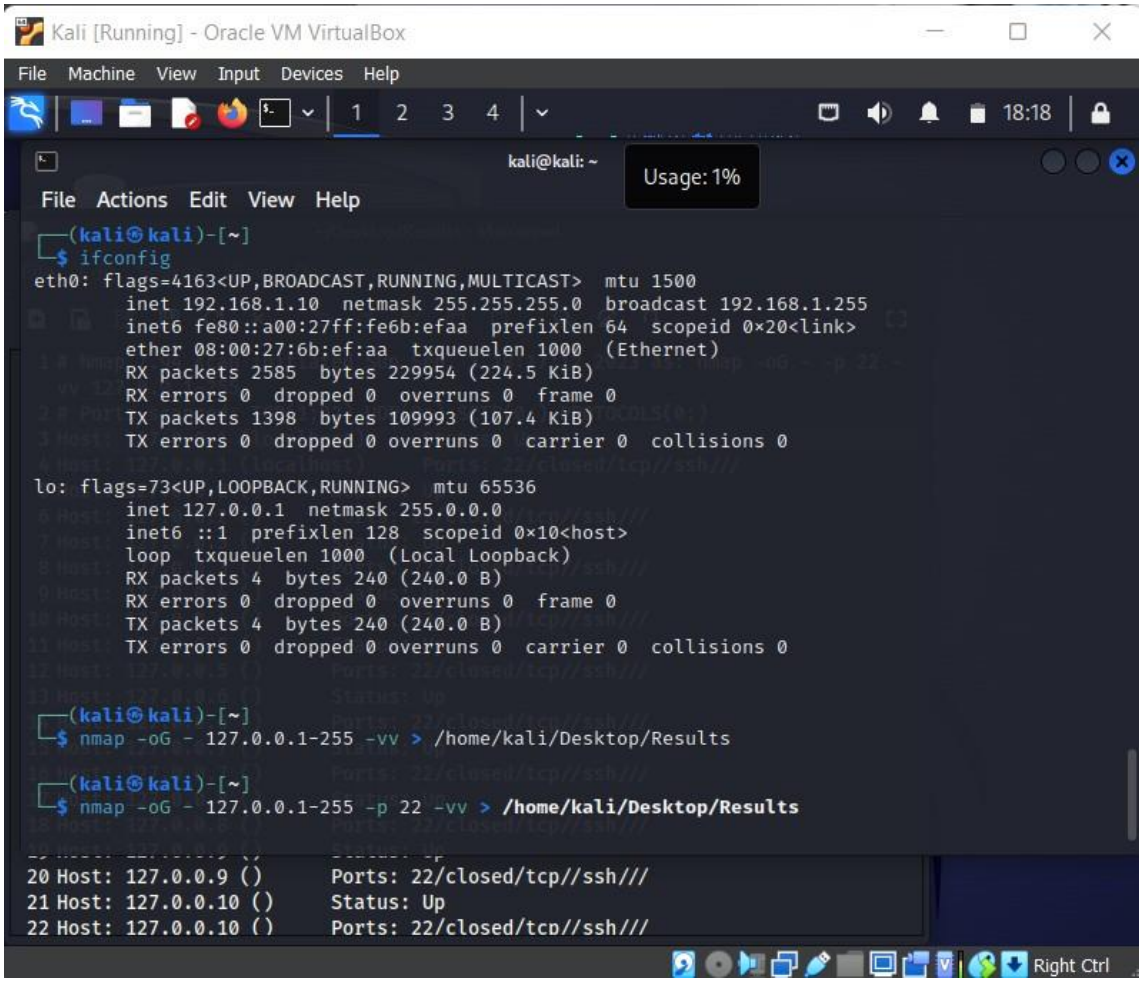
  - Scanning the website scanme.nmap= .org, it will also give us the latency and the ports



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:55
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Right Ctrl

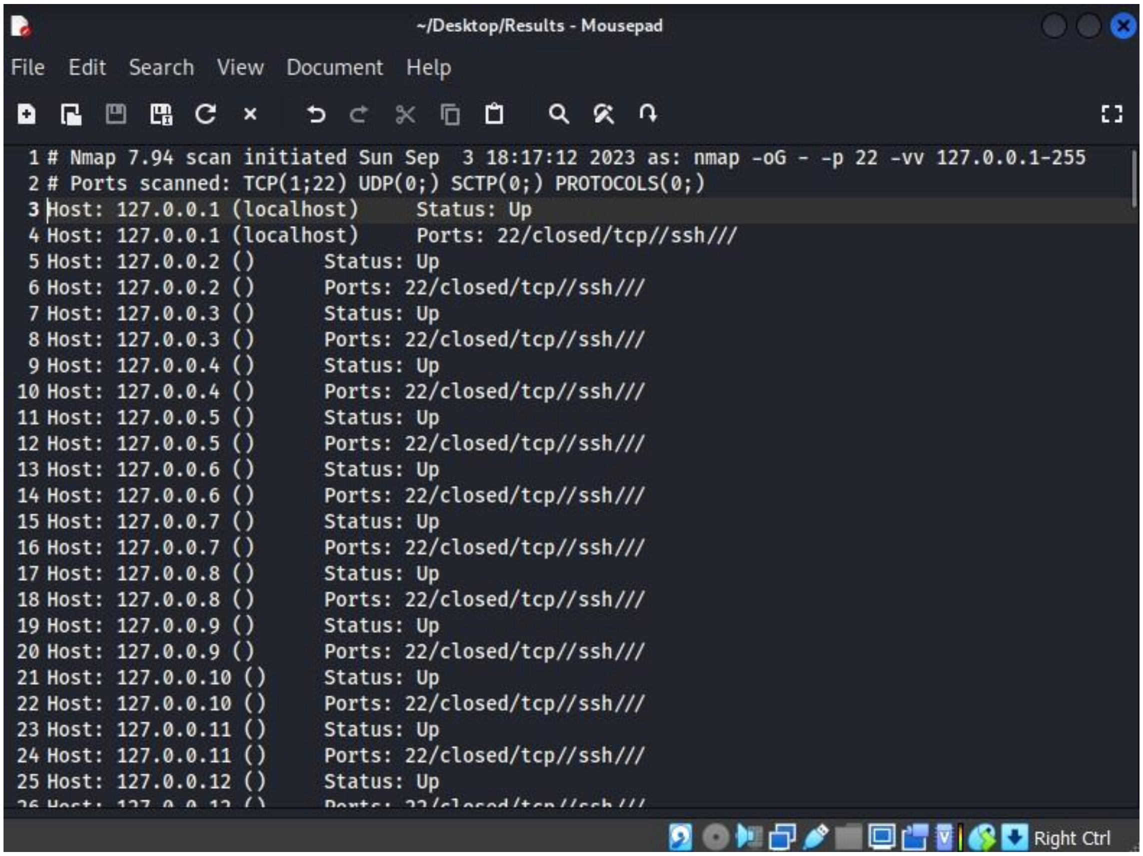
```
99.14.in-addr.arpa      nameserver = hyd-ns9.tataidc.co.in.
99.14.in-addr.arpa      nameserver = mum-ns10.tataidc.co.in.
mum-ns10.tataidc.co.in  internet address = 103.8.45.10
hyd-ns9.tataidc.co.in   internet address = 103.8.46.9
ns4.tataidc.co.in       internet address = 103.8.46.5
hyd-ns10.tataidc.co.in  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
18:18
kali@kali: ~
Usage: 1%
File Actions Edit View Help
Right Ctrl

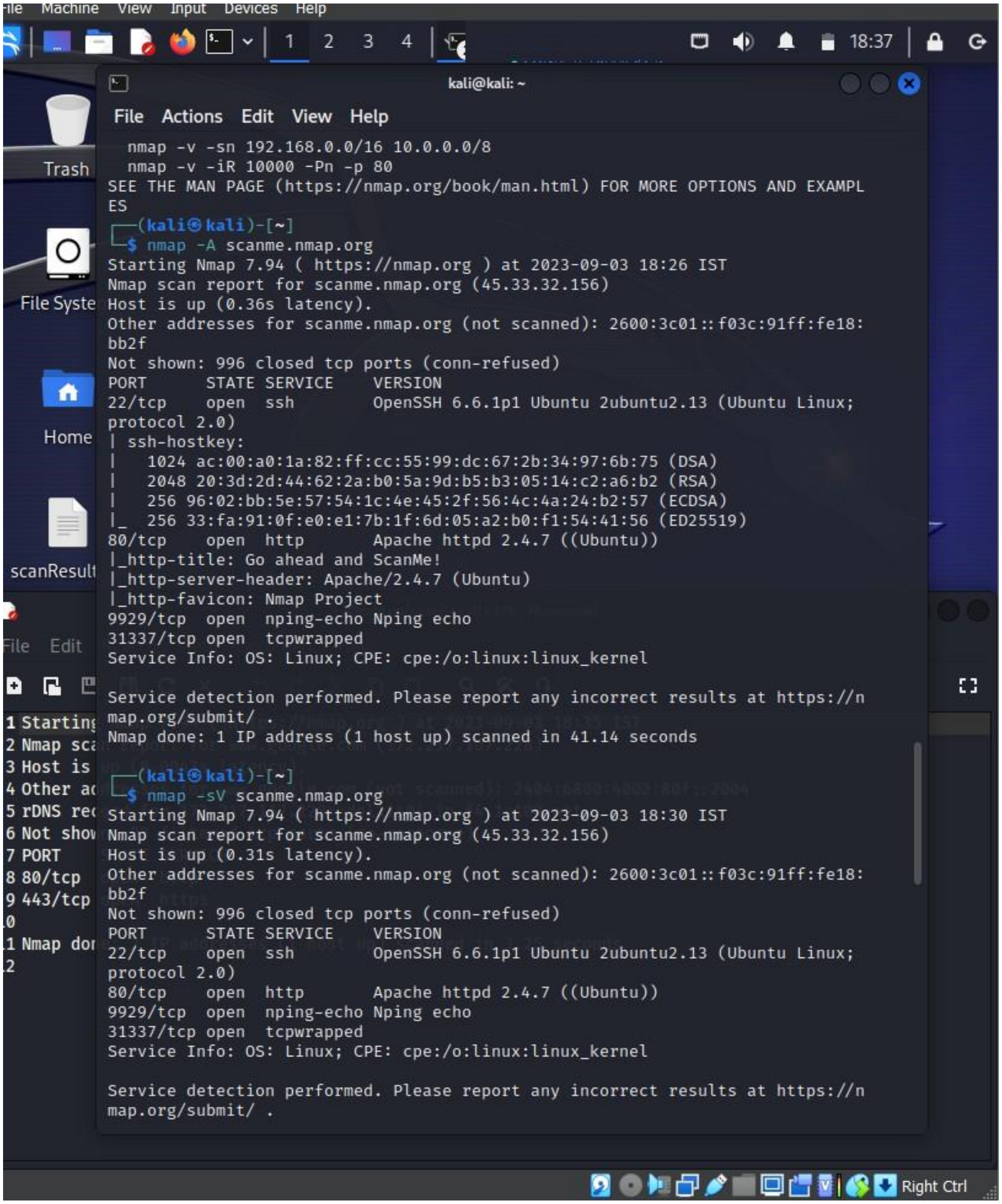
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe6b:efaa  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:6b:ef:aa  txqueuelen 1000  (Ethernet)
        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 0×10<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///
```


~/Desktop/Results - Mousepad
File Edit Search View Document Help
Right Ctrl

```
# Nmap 7.94 scan initiated Sun Sep  3 18:17:12 2023 as: nmap -oG - -p 22 -vv 127.0.0.1-255
# Ports scanned: TCP(1;22) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 127.0.0.1 (localhost)     Status: Up
Host: 127.0.0.1 (localhost)     Ports: 22/closed/tcp//ssh///
Host: 127.0.0.2 ()      Status: Up
Host: 127.0.0.2 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.3 ()      Status: Up
Host: 127.0.0.3 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.4 ()      Status: Up
Host: 127.0.0.4 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.5 ()      Status: Up
Host: 127.0.0.5 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.6 ()      Status: Up
Host: 127.0.0.6 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.7 ()      Status: Up
Host: 127.0.0.7 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.8 ()      Status: Up
Host: 127.0.0.8 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.9 ()      Status: Up
Host: 127.0.0.9 ()      Ports: 22/closed/tcp//ssh///
Host: 127.0.0.10 ()     Status: Up
Host: 127.0.0.10 ()     Ports: 22/closed/tcp//ssh///
Host: 127.0.0.11 ()     Status: Up
Host: 127.0.0.11 ()     Ports: 22/closed/tcp//ssh///
Host: 127.0.0.12 ()     Status: Up
Host: 127.0.0.12 ()     Ports: 22/closed/tcp//ssh///
```

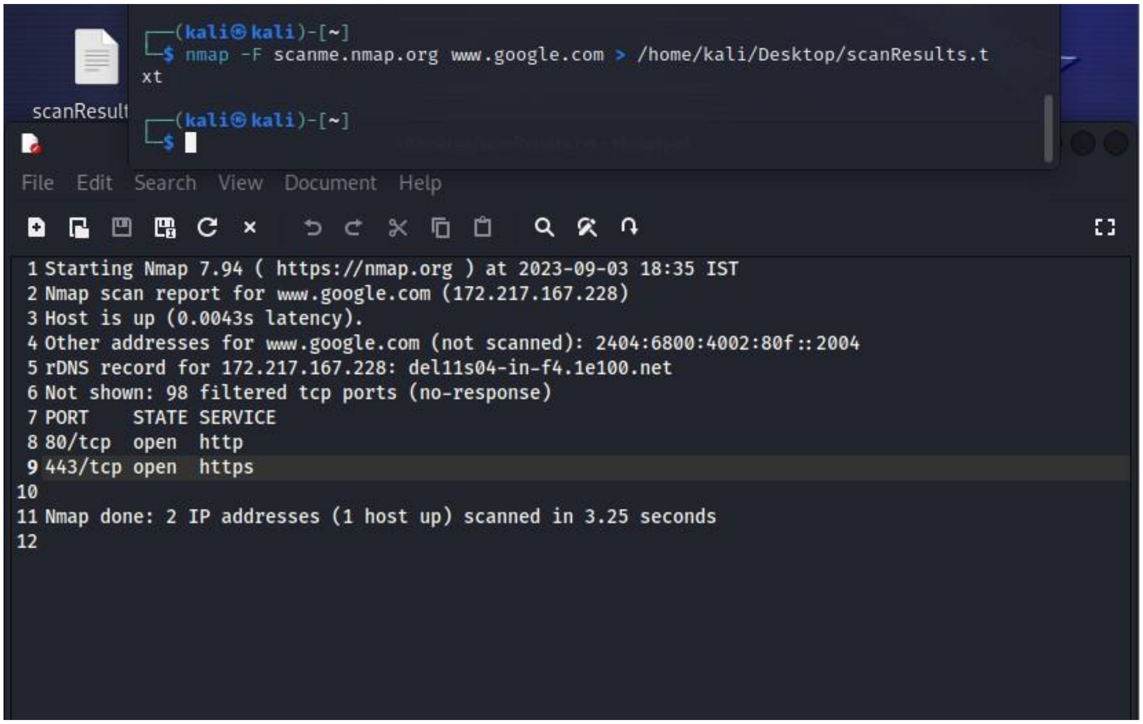
- Then we can also perform aggresive searches using -A, we can also scan for versions on open services using -sV only:



File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Trash
File Syste
Home
scanResult
Right Ctrl

```
  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 EXAMPL
ES
┌──(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://n
map.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://n
map.org/submit/ .
```

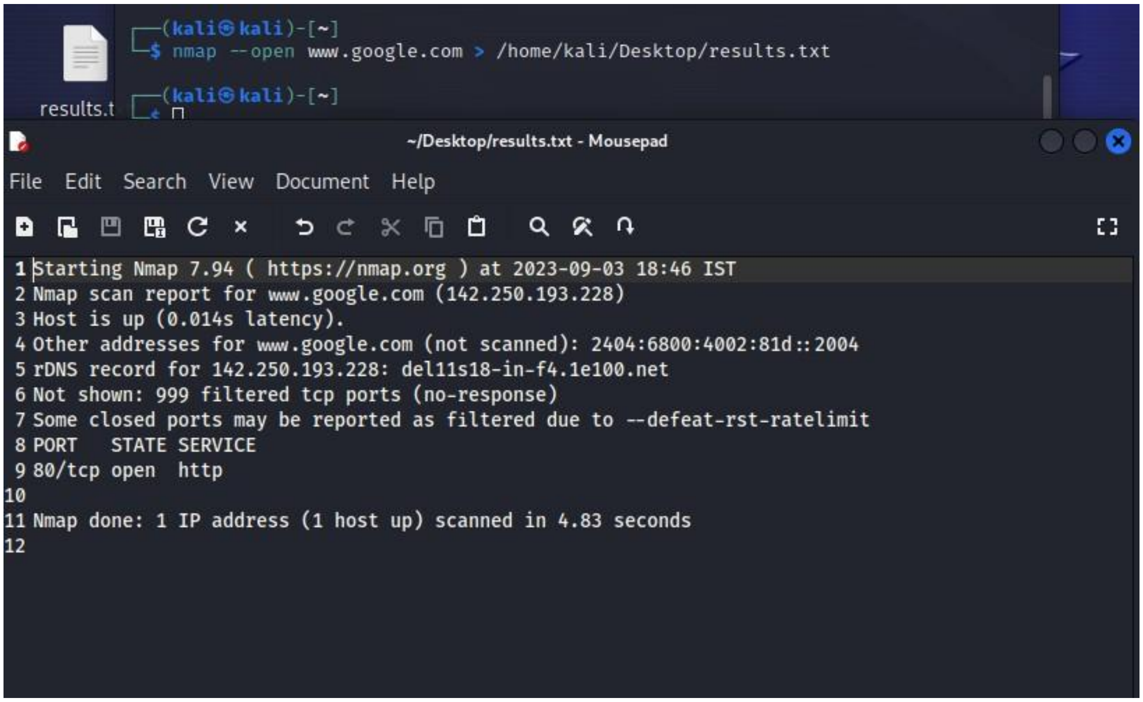
- We can also fast search for the open ports only, in this it only scans 100 ports not 1000, we use the -F command. Results are stored in a file called “scanResults”:



```
┌──(kali㉿kali)-[~]
└─$ nmap -F scanme.nmap.org www.google.com > /home/kali/Desktop/scanResults.t
xt

┌──(kali㉿kali)-[~]
└─$ 
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:35 IST
Nmap scan report for www.google.com (172.217.167.228)
Host is up (0.0043s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4002:80f::2004
rDNS record for 172.217.167.228: del11s04-in-f4.1e100.net
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (1 host up) scanned in 3.25 seconds

```

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


results.t
~/Desktop/results.txt - Mousepad
File Edit Search View Document Help

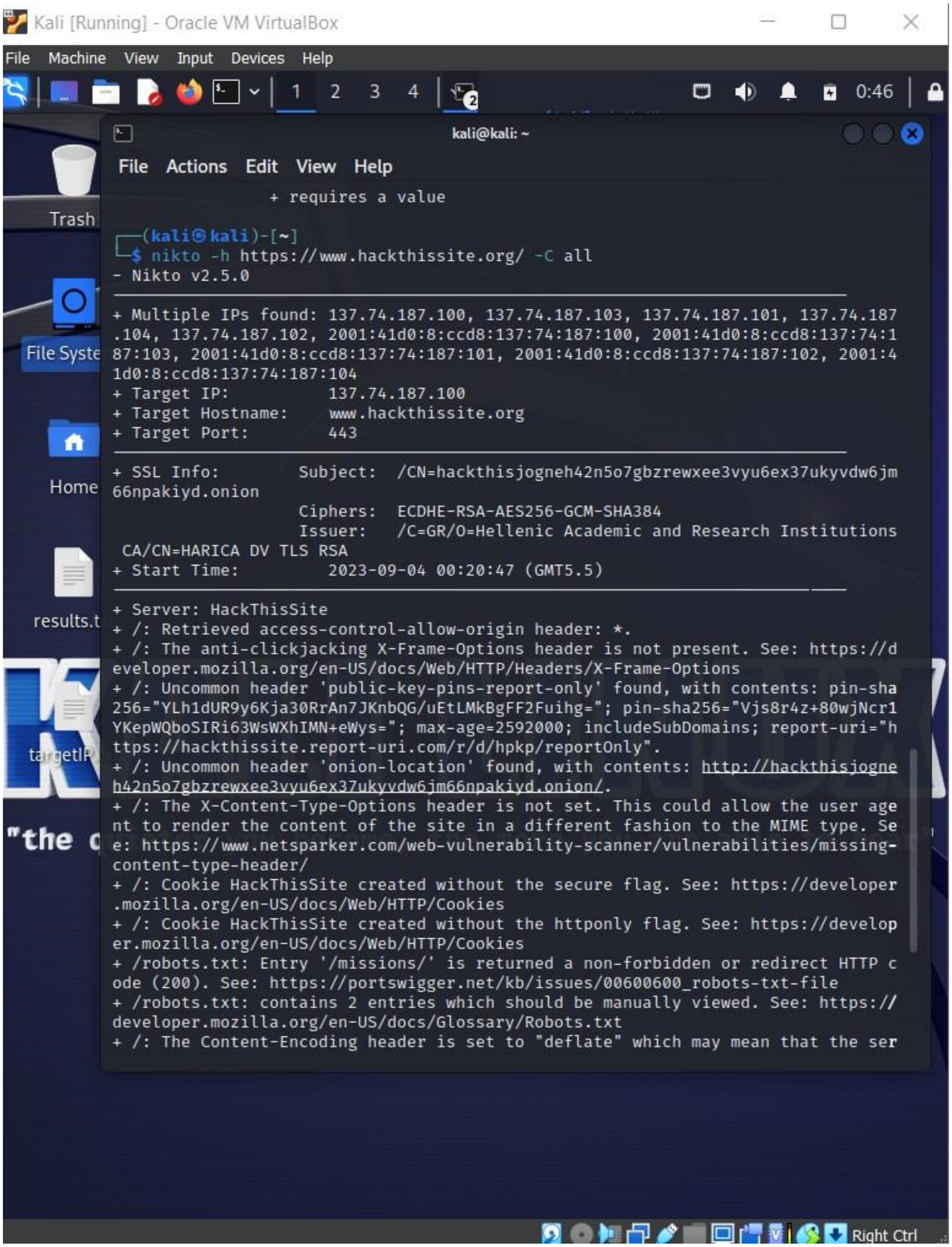
```
┌──(kali㉿kali)-[~]
└─$ nmap --open www.google.com > /home/kali/Desktop/results.txt

┌──(kali㉿kali)-[~]
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 18:46 IST
Nmap scan report for www.google.com (142.250.193.228)
Host is up (0.014s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4002:81d::2004
rDNS record for 142.250.193.228: del11s18-in-f4.1e100.net
Not shown: 999 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds

```

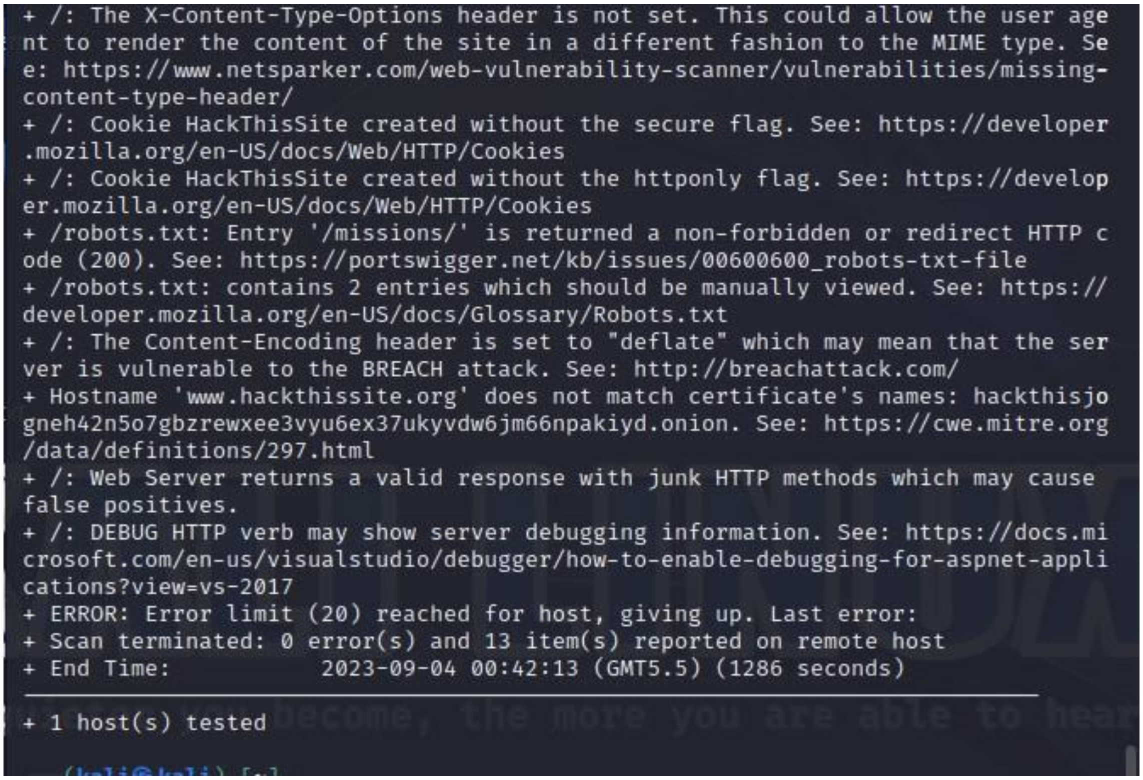
- **TheHarvester** is a tool that can be used to collect information about email addresses, social media profiles, and other online accounts.
- **WhatWeb** is a tool that can be used to identify the technologies used on a website.
- **SpiderFoot** is a tool that can be used to collect information about 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
0:46
kali@kali: ~
File Actions Edit View Help
Trash
File Syste
Home
results.t
targetIP
"the q
Right Ctrl

```
               + 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:ccd8:137:74:1
87:103, 2001:41d0:8:ccd8:137:74:187:101, 2001:41d0:8:ccd8:137:74:187:102, 2001:4
1d0:8:ccd8:137:74:187:104
+ Target IP:          137.74.187.100
+ Target Hostname:    www.hackthissite.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm
66npakiyd.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://d
eveloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'public-key-pins-report-only' found, with contents: pin-sha
256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-sha256="Vjs8r4z+80wjNcr1
YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains; report-uri="h
ttps://hackthissite.report-uri.com/r/d/hpkp/reportOnly".
+ /: Uncommon header 'onion-location' found, with contents: http://hackthisjogne
h42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/.
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: 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://develop
er.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: Entry '/missions/' is returned a non-forbidden or redirect HTTP c
ode (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 age
nt to render the content of the site in a different fashion to the MIME type. Se
e: 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://develop
er.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /robots.txt: Entry '/missions/' is returned a non-forbidden or redirect HTTP c
ode (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
ver is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname 'www.hackthissite.org' does not match certificate's names: hackthisjo
gneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.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.mi
crosoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-appli
cations?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

   (kali@kali) [~]
```

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.

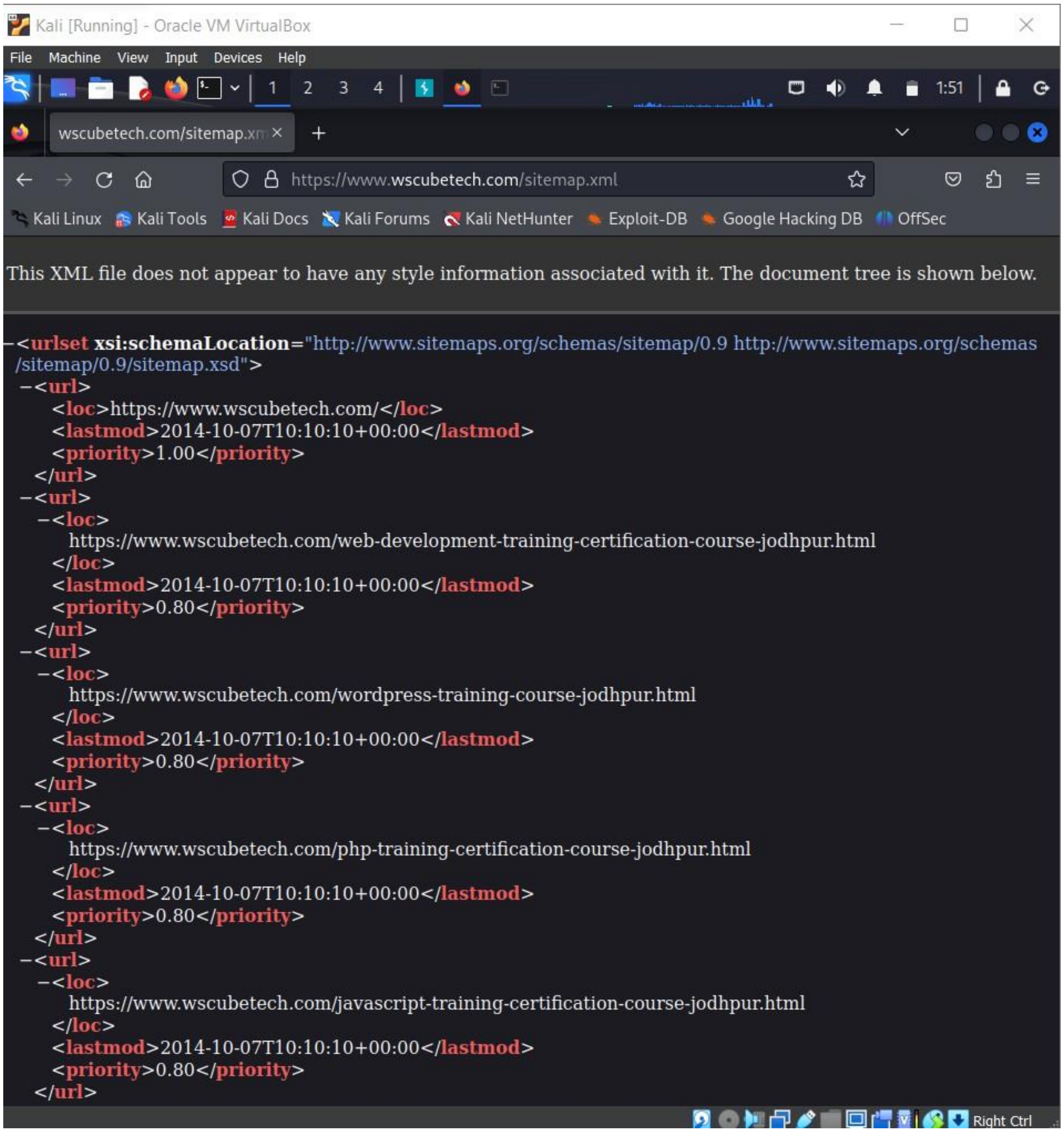
    - **contains 2 entries which should be manually viewed.** This means that there are two entries in the robots.txt file that should be reviewed to make sure they are not allowing unauthorized access to the website.
    - **The Content-Encoding header is set to "deflate" which may mean that the server 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.

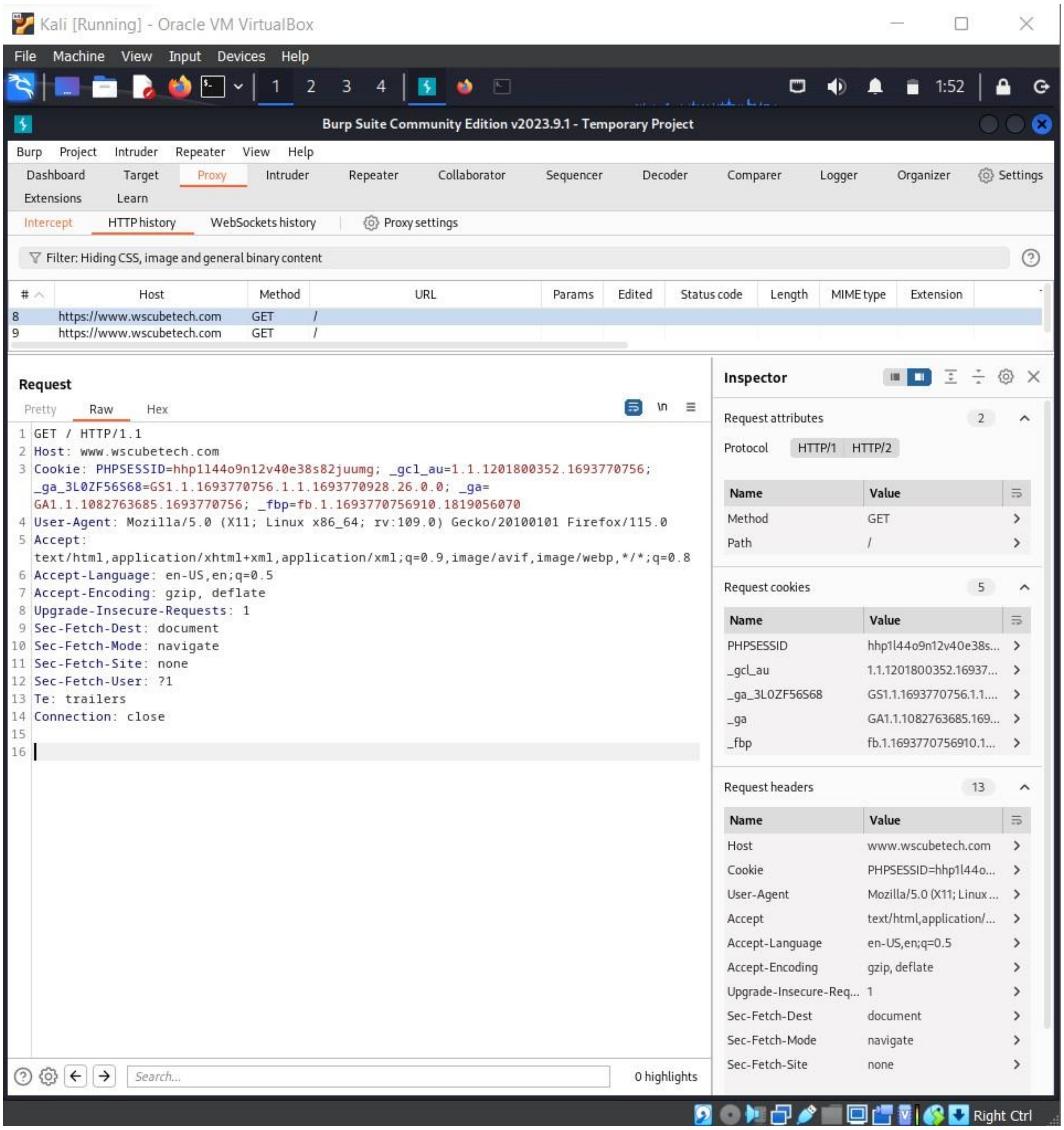
- In this first we change the kali browser proxy to the burp proxy so that the burp can get the information about the sites we are visiting.
- We can access the sitemap which is public if it has any of the private domain information or try to access Robot.txt file which contains all the domains that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


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:51
wscubetech.com/sitemap.xm
https://www.wscubetech.com/sitemap.xml
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl

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>
```

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


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:52
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
Pretty Raw Hex
Inspector
Search...
0 highlights
Right Ctrl

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
8	https://www.wscubetech.com	GET	/						
9	https://www.wscubetech.com	GET	/						

Request

```
GET / HTTP/1.1
Host: www.wscubetech.com
Cookie: PHPSESSID=hhp1l44o9n12v40e38s82juumg; _gcl_au=1.1.1201800352.1693770756;
_ga_3L0ZF56S68=GS1.1.1693770756.1.1.1693770928.26.0.0; _ga=
GA1.1.1082763685.1693770756; _fbp=fb.1.1693770756910.1819056070
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/

Request cookies 5

Name	Value
PHPSESSID	hhp1l44o9n12v40e38s...
_gcl_au	1.1.1201800352.16937...
_ga_3L0ZF56S68	GS1.1.1693770756.1.1....
_ga	GA1.1.1082763685.169...
_fbp	fb.1.1693770756910.1...

Request headers 13

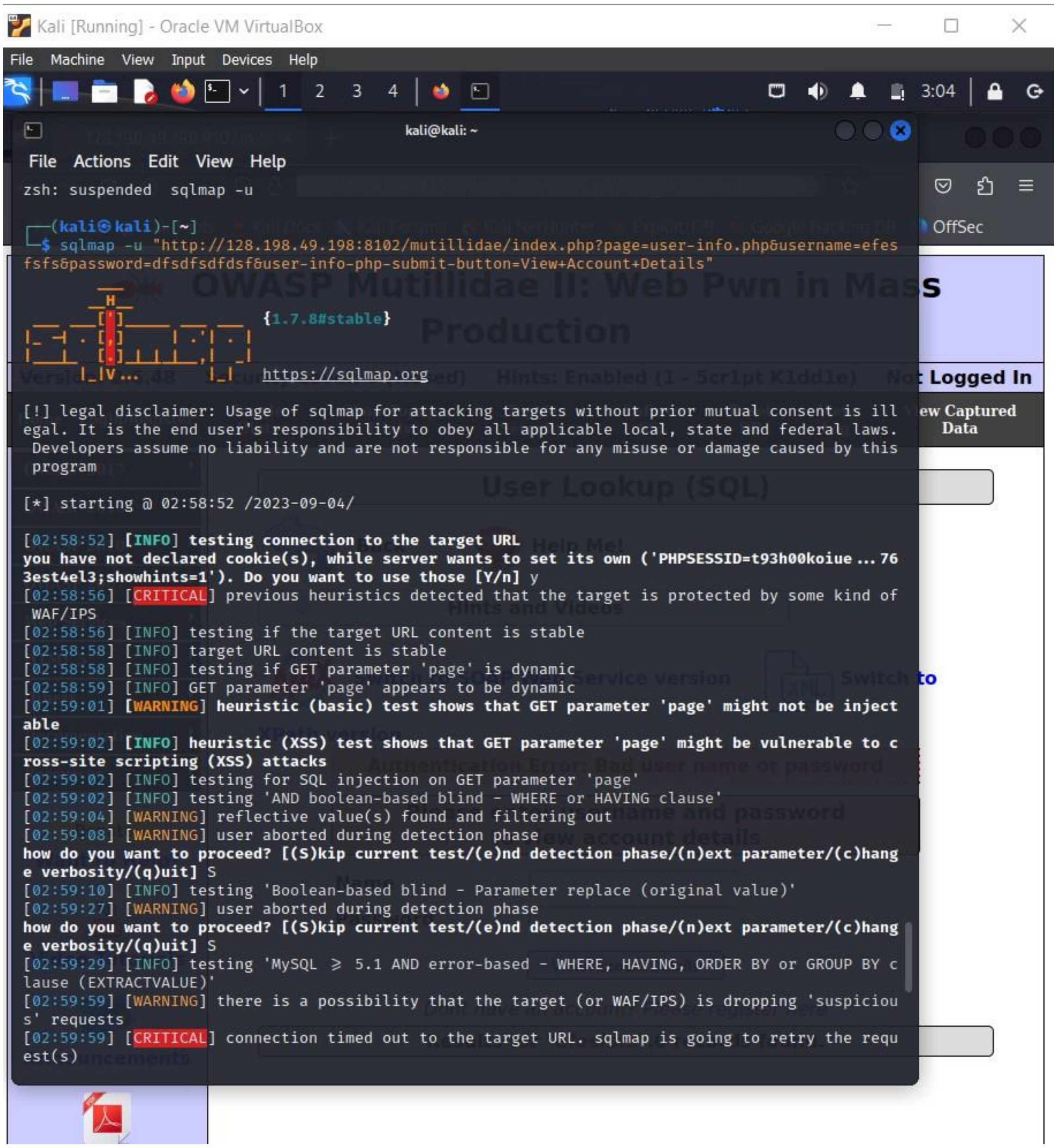
Name	Value
Host	www.wscubetech.com
Cookie	PHPSESSID=hhp1l44o...
User-Agent	Mozilla/5.0 (X11; Linux ...
Accept	text/html,application/...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Upgrade-Insecure-Req...	1
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	none

4. **Database Assessment applications**

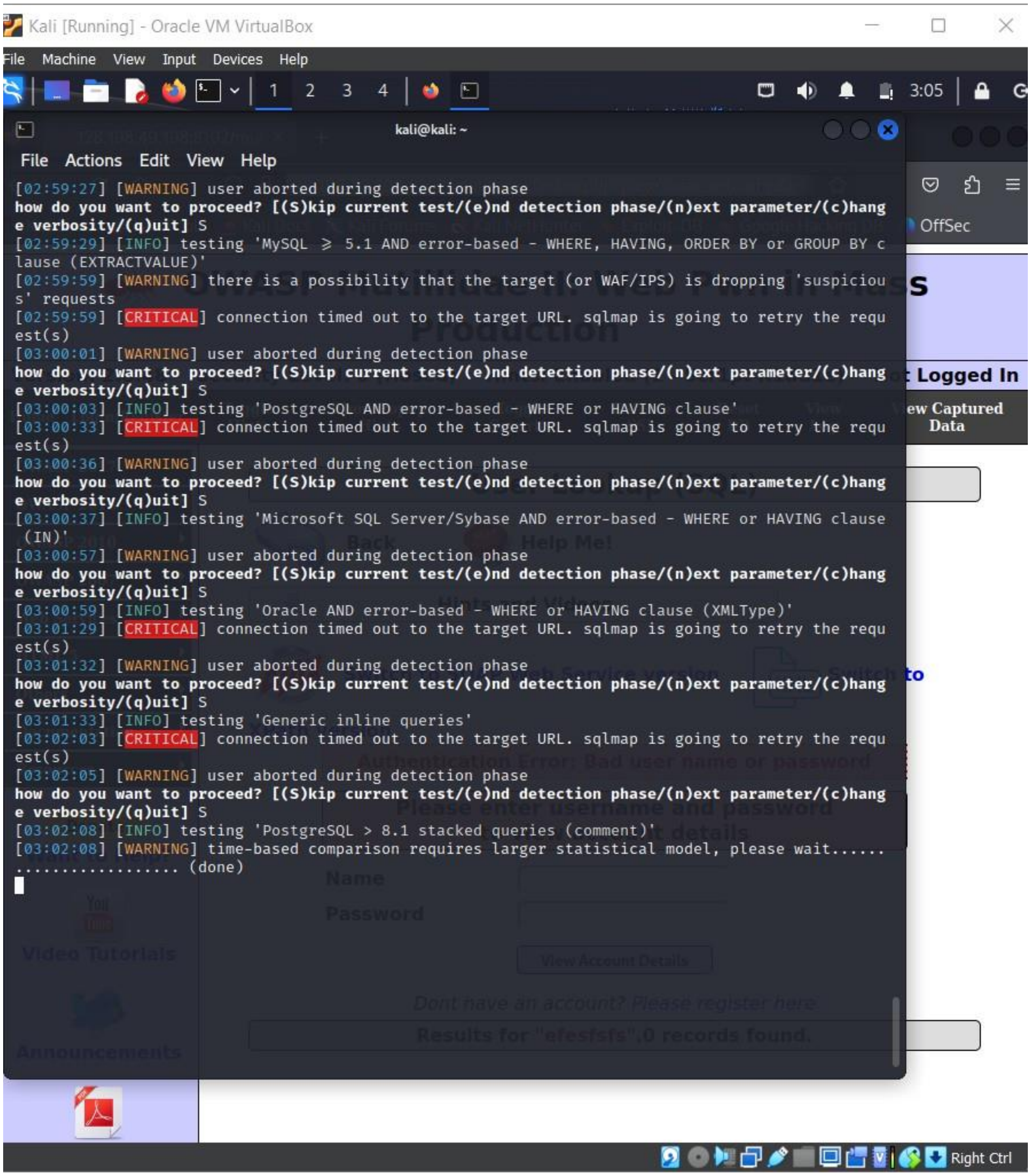
- **SQLMap** is a tool that can be used to automate the process of identifying and exploiting SQL injection vulnerabilities.
    - A simple test to check whether your website is vulnerable would be to replace the value in the get request parameter with an asterisk (*).
    - Here we are going to do the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

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

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



```
zsh: suspended  sqlmap -u

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://128.198.49.198:8102/mutillidae/index.php?page=user-info.php&username=efes
fsfs&password=dfsdfsdfdsf&user-info-php-submit-button=View+Account+Details"

                          {1.7.8#stable}


                          https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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=t93h00koiue...76
3est4el3;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 inject
able
[02:59:02] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to c
ross-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)hang
e 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)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)
```

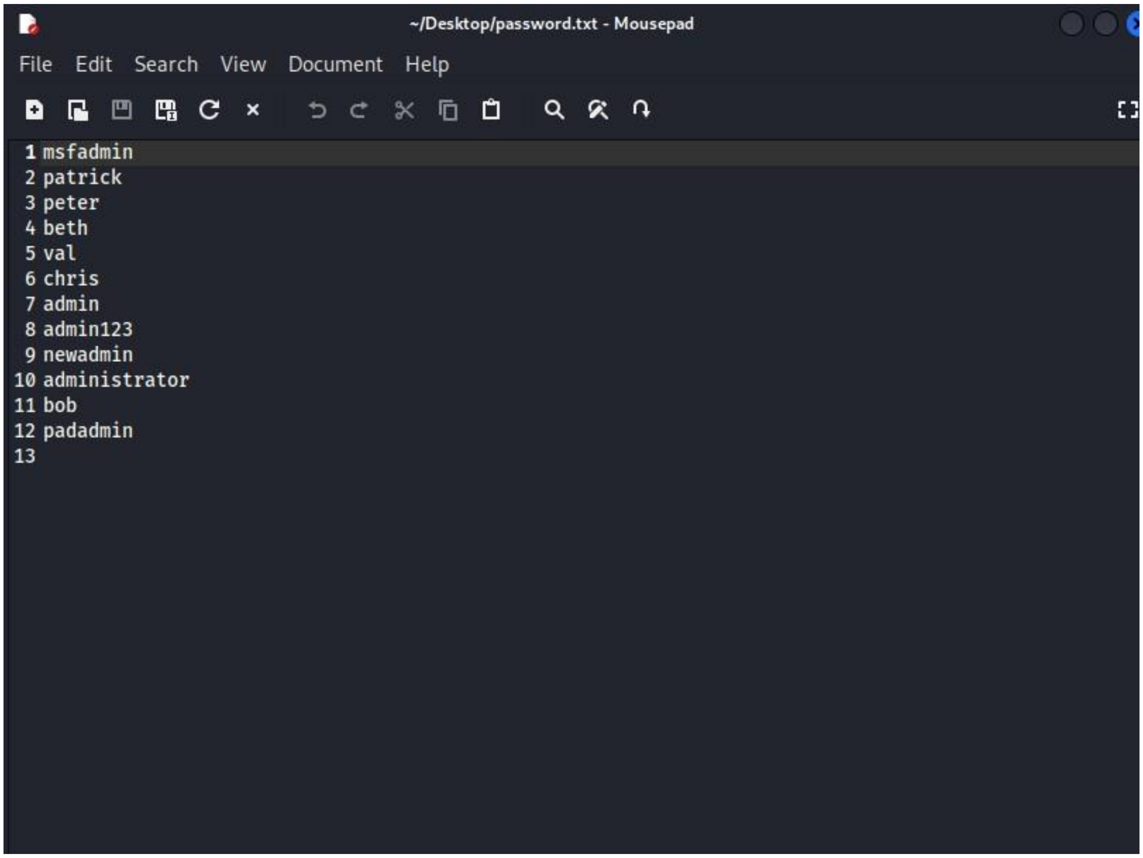

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
[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)
```

- **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.

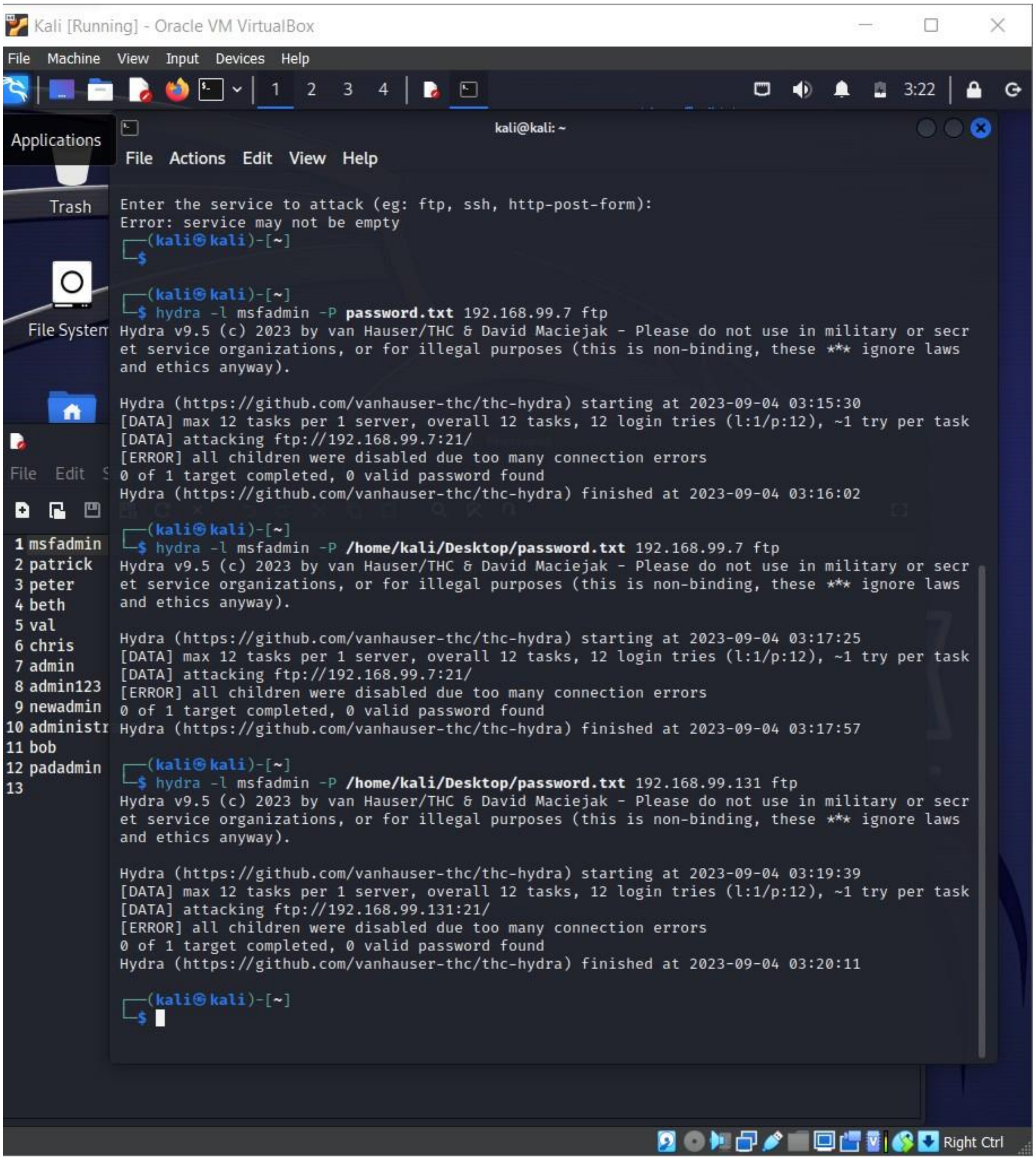
5. **Password Attacks**

- **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


~/Desktop/password.txt - Mousepad
File Edit Search View Document Help

```
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 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
3:22
Applications
Trash
File System
kali@kali: ~
File Actions Edit View Help
File Edit
Right Ctrl

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

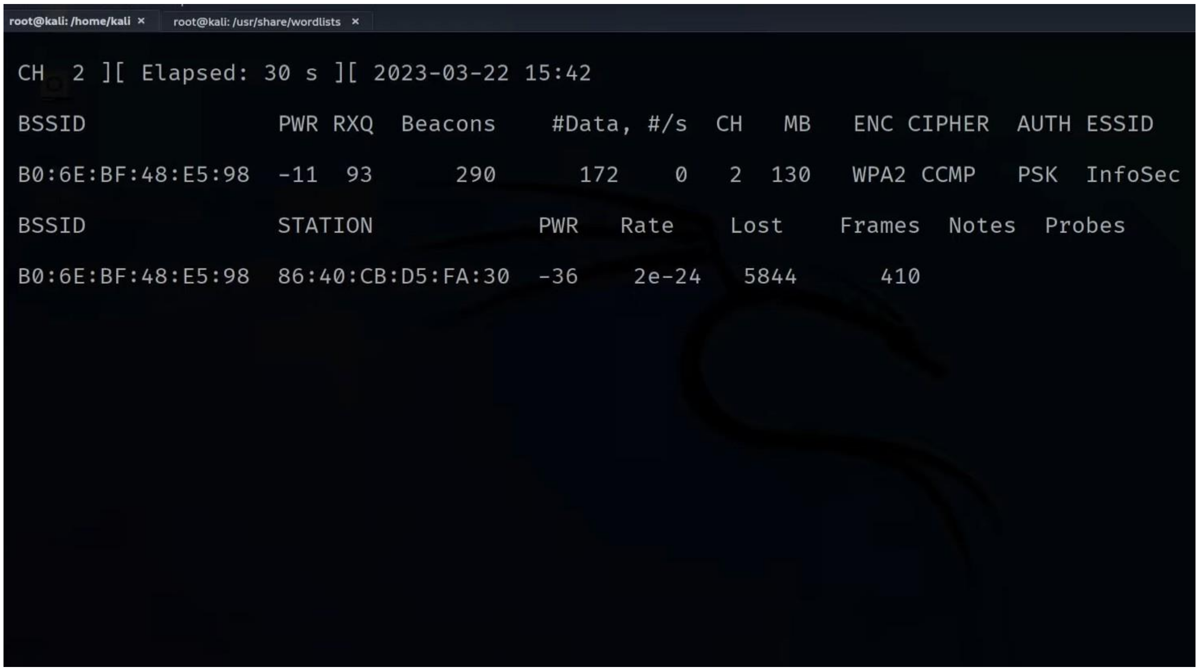
```
Enter the service to attack (eg: ftp, ssh, http-post-form):
Error: service may not be empty
┌──(kali㉿kali)-[~]
└─$ 

┌──(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 secr
et 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

┌──(kali㉿kali)-[~]
└─$ 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 secr
et 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

┌──(kali㉿kali)-[~]
└─$ 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 secr
et 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

┌──(kali㉿kali)-[~]
└─$ 
```

- **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**

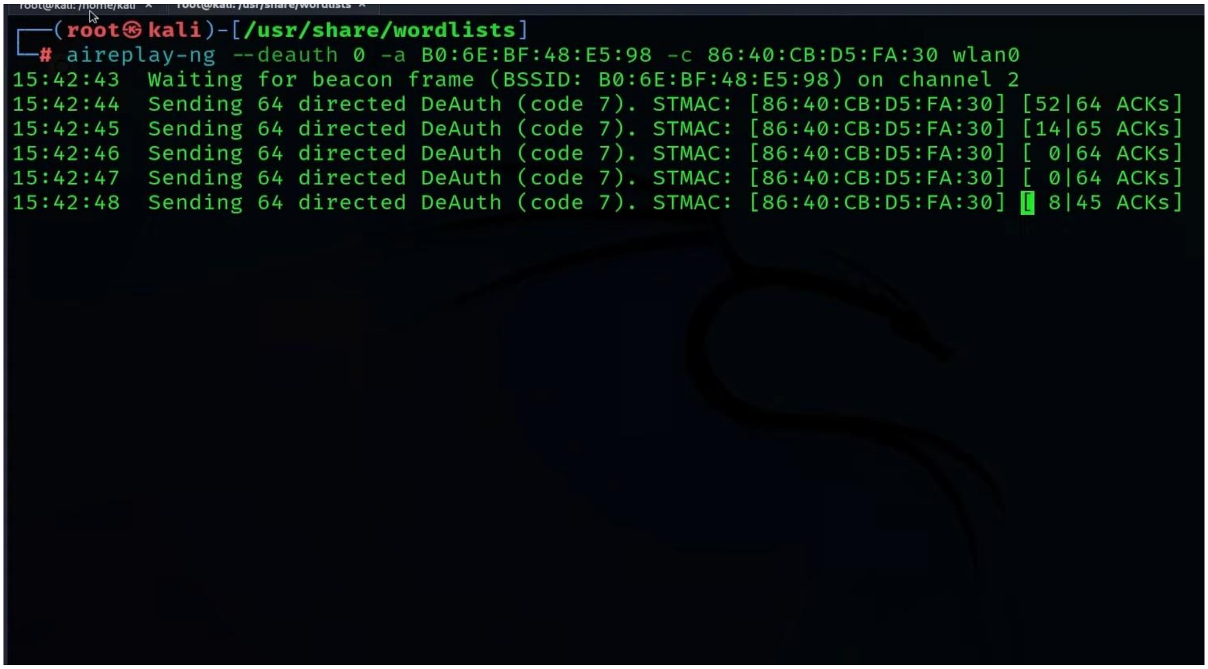
- **Aircrack-ng** is a suite of tools that can be used to crack wireless passwords.

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



```
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
```

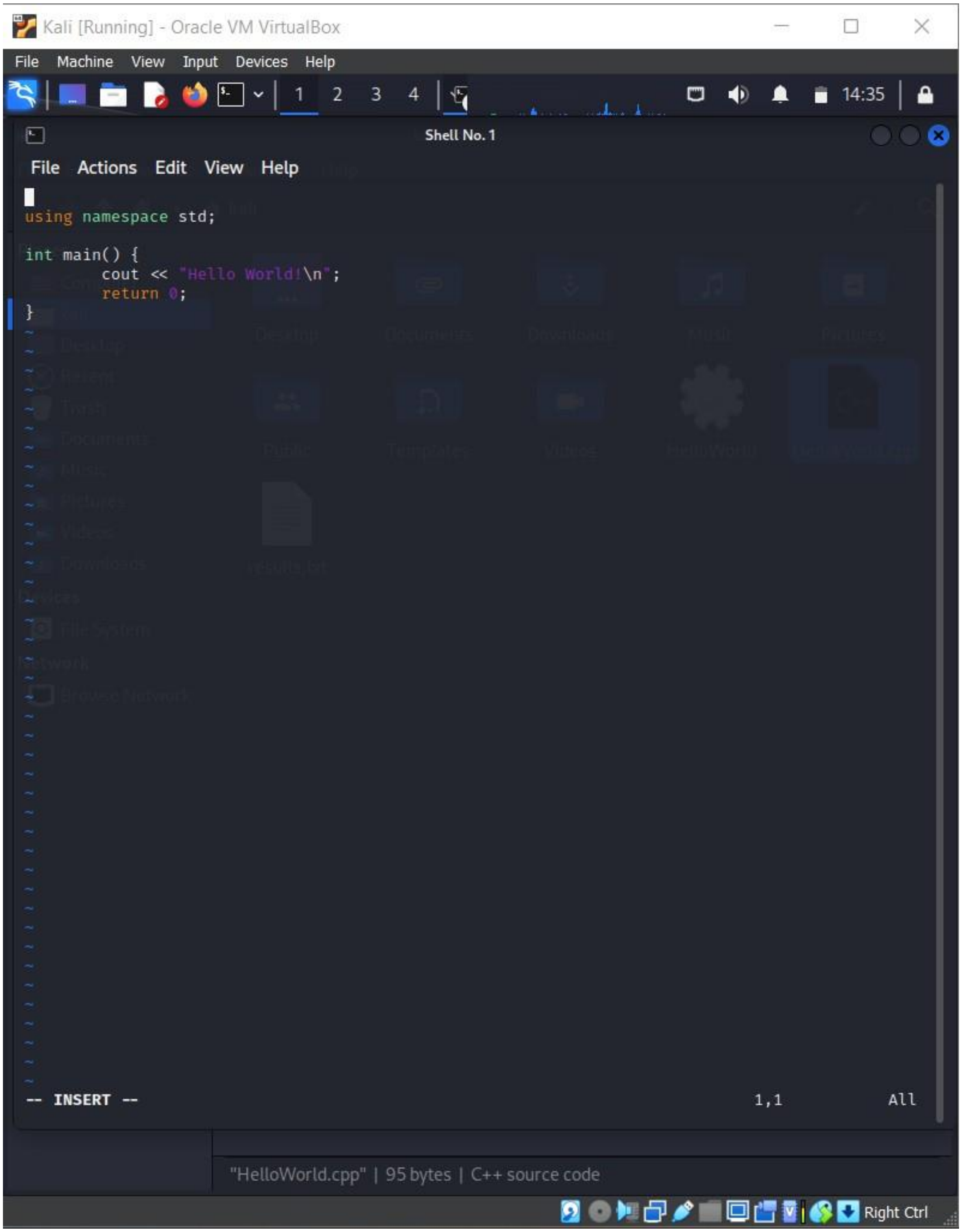
Deauthentication attacks can be done now based on the acquired information:



```
┌──(root㉿kali)-[/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:

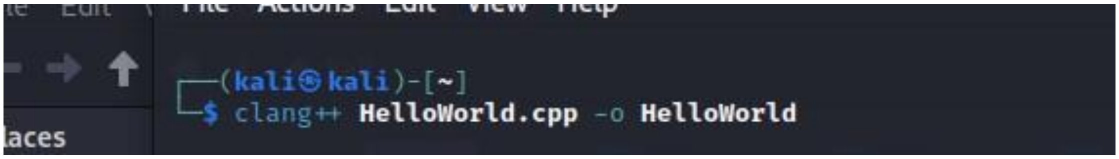


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:35
Shell No. 1
File Actions Edit View Help

```

using namespace std;

int main() {
        cout << "Hello World!\n";
        return 0;
}
~
~
-- INSERT --                                                1,1           All
```

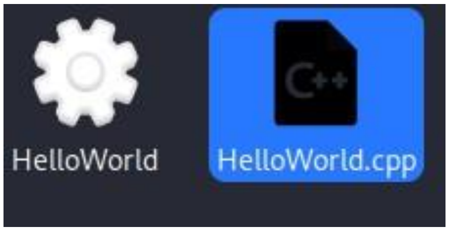
"HelloWorld.cpp" | 95 bytes | C++ source code

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

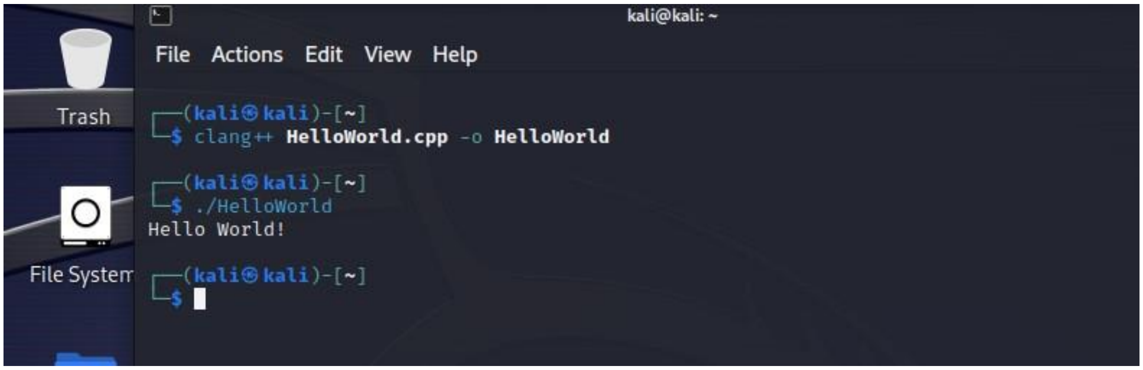


```
┌──(kali㉿kali)-[~]
└─$ clang++ HelloWorld.cpp -o HelloWorld
```

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:

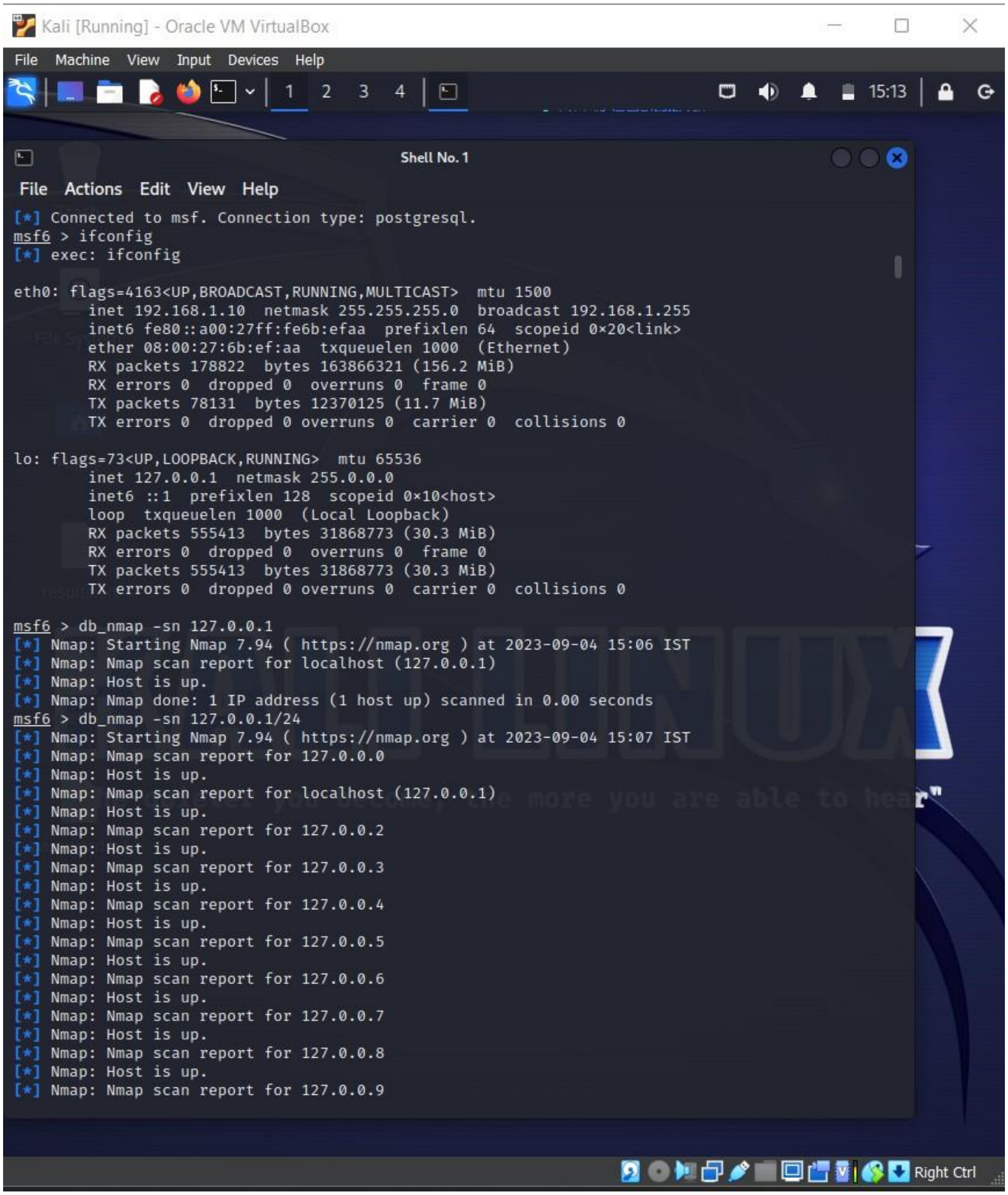


```
┌──(kali㉿kali)-[~]
└─$ clang++ HelloWorld.cpp -o HelloWorld

┌──(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.

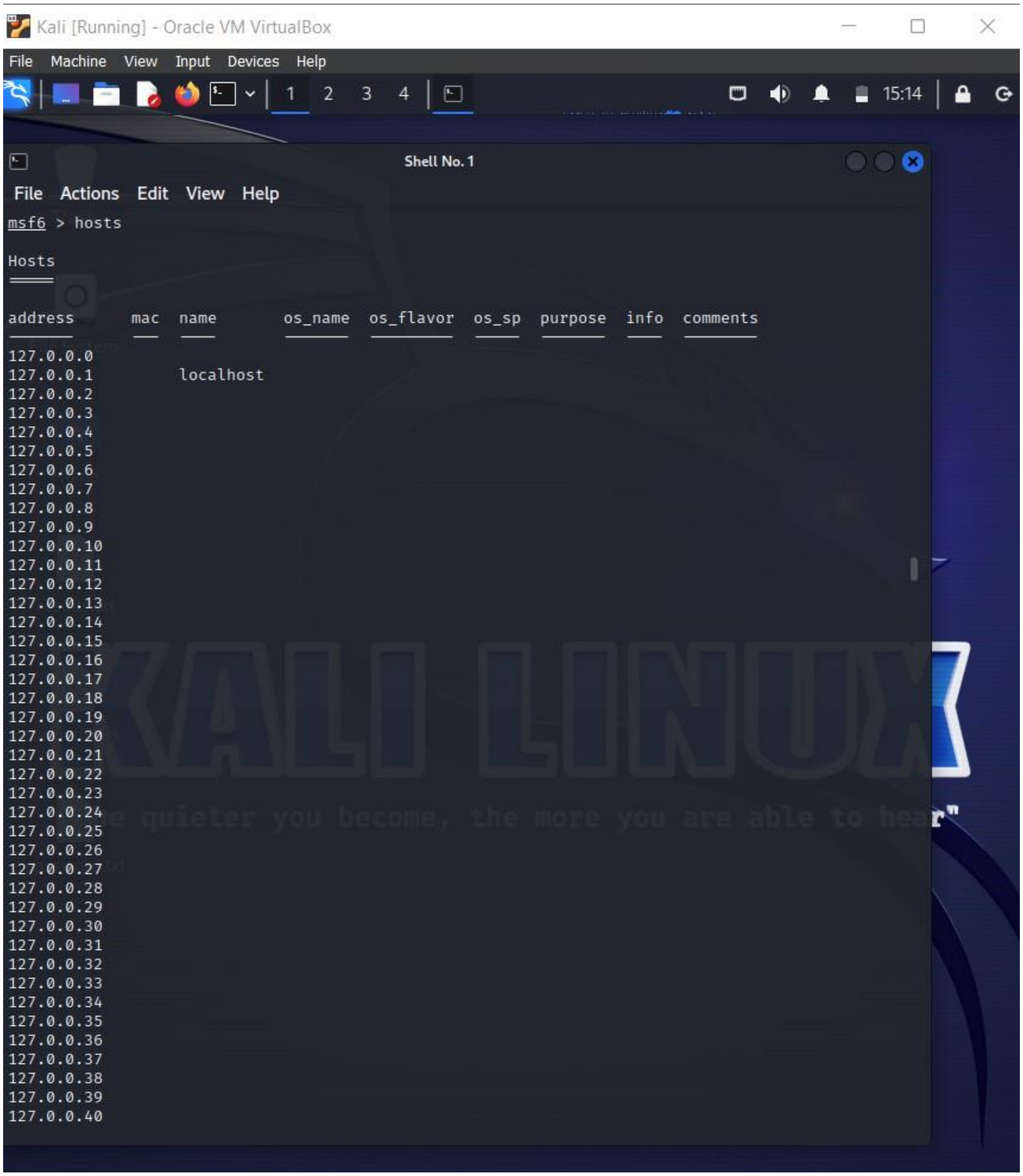
8. **Exploitation Tools**

- **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
15:13
Shell No. 1
File Actions Edit View Help
Right Ctrl

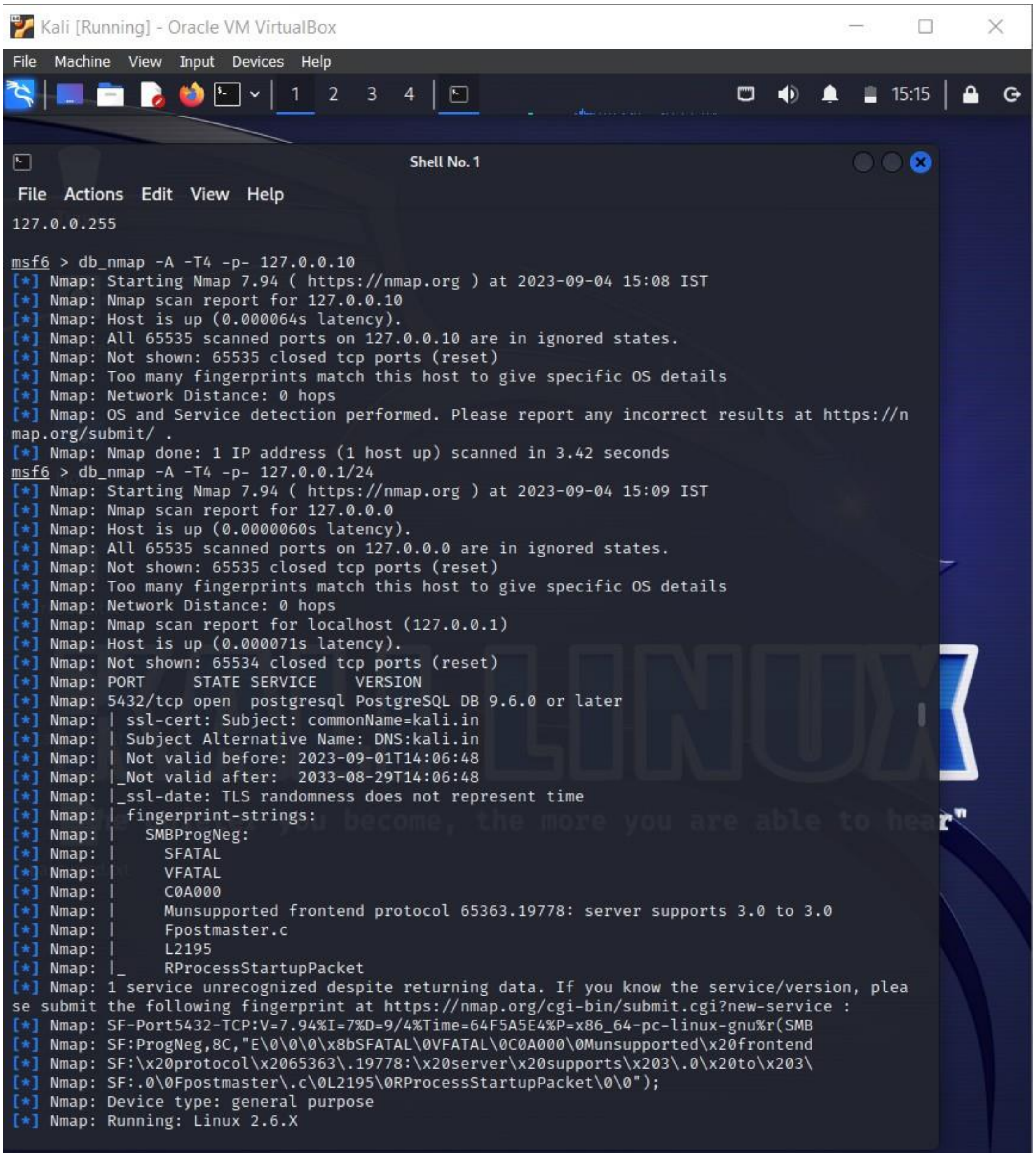
```
[*] Connected to msf. Connection type: postgresql.
msf6 > ifconfig
[*] exec: ifconfig

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 0x20<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 0x10<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:


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:14
Shell No. 1
File Actions Edit View Help

```
msf6 > hosts

Hosts
=====

address       mac  name        os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----        -------  ---------  -----  -------  ----  --------
127.0.0.0
127.0.0.1          localhost
127.0.0.2
127.0.0.3
127.0.0.4
127.0.0.5
127.0.0.6
127.0.0.7
127.0.0.8
127.0.0.9
127.0.0.10
127.0.0.11
127.0.0.12
127.0.0.13
127.0.0.14
127.0.0.15
127.0.0.16
127.0.0.17
127.0.0.18
127.0.0.19
127.0.0.20
127.0.0.21
127.0.0.22
127.0.0.23
127.0.0.24
127.0.0.25
127.0.0.26
127.0.0.27
127.0.0.28
127.0.0.29
127.0.0.30
127.0.0.31
127.0.0.32
127.0.0.33
127.0.0.34
127.0.0.35
127.0.0.36
127.0.0.37
127.0.0.38
127.0.0.39
127.0.0.40
```

- 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
15:15
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://n
map.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 (0.0000060s 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, plea
se 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%r(SMB
[*] Nmap: SF:ProgNeg,8C,"E\0\0\0\x8bSFATAL\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.

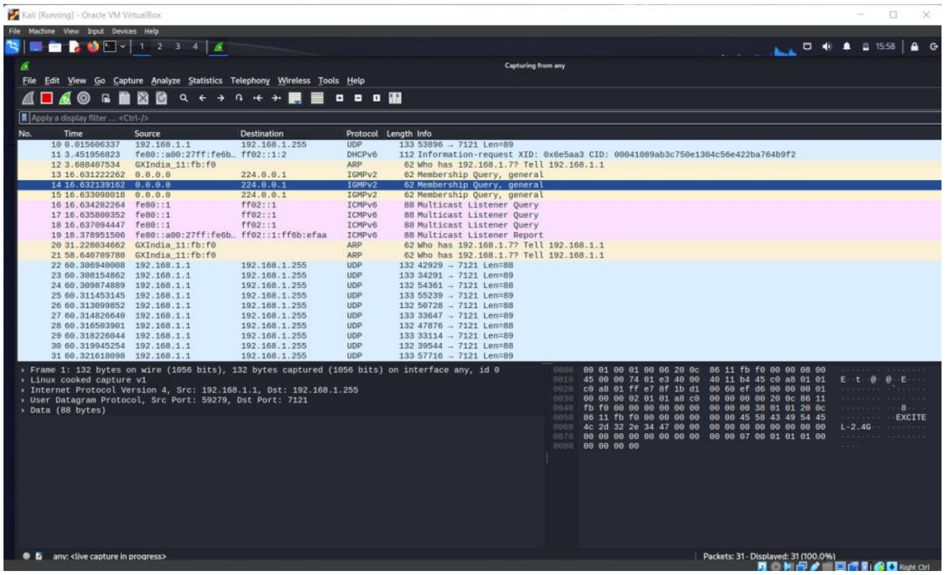
The only host for which the OS and version information could be determined is the localhost (127.0.0.1). This host is running Linux 2.6.32, which is a relatively old version of Linux.

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:



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:58
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

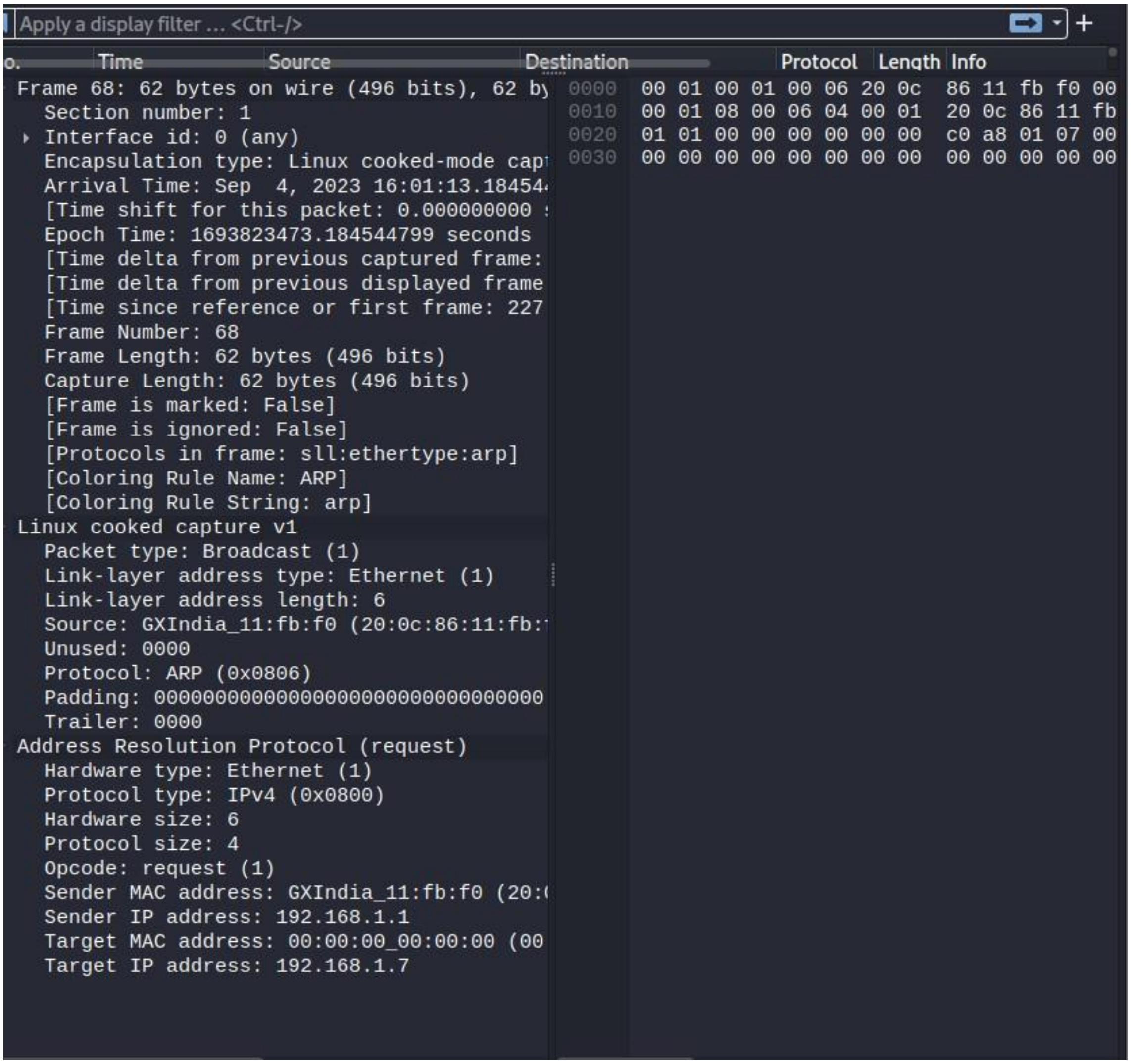
```
No.     Time          Source                 Destination         Protocol  Length Info
     10 0.015606337   192.168.1.1            192.168.1.255       UDP       133 53896 → 7121 Len=89
     11 3.451956823   fe80::a00:27ff:fe6b…   ff02::1:2           DHCPv6    112 Information-request XID: 0x6e5aa3 CID: 00041089ab3c750e1304c56e422ba764b9f2
     12 3.688407534   GXIndia_11:fb:f0                           ARP        62 Who has 192.168.1.7? Tell 192.168.1.1
     13 16.631222262  0.0.0.0                224.0.0.1           IGMPv2     62 Membership Query, general
     14 16.632139162  0.0.0.0                224.0.0.1           IGMPv2     62 Membership Query, general
     15 16.633098018  0.0.0.0                224.0.0.1           IGMPv2     62 Membership Query, general
     16 16.634282264  fe80::1                ff02::1             ICMPv6     88 Multicast Listener Query
     17 16.635800352  fe80::1                ff02::1             ICMPv6     88 Multicast Listener Query
     18 16.637094447  fe80::1                ff02::1             ICMPv6     88 Multicast Listener Query
     19 18.378951506  fe80::a00:27ff:fe6b…   ff02::1:ff6b:efaa   ICMPv6     88 Multicast Listener Report
     20 31.228034662  GXIndia_11:fb:f0                           ARP        62 Who has 192.168.1.7? Tell 192.168.1.1
     21 58.640709780  GXIndia_11:fb:f0                           ARP        62 Who has 192.168.1.7? Tell 192.168.1.1
     22 60.306940008  192.168.1.1            192.168.1.255       UDP       132 42929 → 7121 Len=88
     23 60.308154862  192.168.1.1            192.168.1.255       UDP       133 34291 → 7121 Len=89
     24 60.309874889  192.168.1.1            192.168.1.255       UDP       132 54361 → 7121 Len=88
     25 60.311453145  192.168.1.1            192.168.1.255       UDP       133 55239 → 7121 Len=89
     26 60.313099852  192.168.1.1            192.168.1.255       UDP       132 50728 → 7121 Len=88
     27 60.314826640  192.168.1.1            192.168.1.255       UDP       133 33647 → 7121 Len=89
     28 60.316503901  192.168.1.1            192.168.1.255       UDP       132 47876 → 7121 Len=88
     29 60.318226044  192.168.1.1            192.168.1.255       UDP       133 33114 → 7121 Len=89
     30 60.319945254  192.168.1.1            192.168.1.255       UDP       132 39544 → 7121 Len=88
     31 60.321618098  192.168.1.1            192.168.1.255       UDP       133 57716 → 7121 Len=89
```

```
› Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.255
› User Datagram Protocol, Src Port: 59279, Dst Port: 7121
› Data (88 bytes)
```

```
0000  00 01 00 01 00 06 20 0c  86 11 fb f0 00 00 08 00   ........ ........
0010  45 00 00 74 01 e3 40 00  40 11 b4 45 c0 a8 01 01   E·t··@·· @··E····
0020  c0 a8 01 ff e7 8f 1b d1  00 60 ef d6 00 00 00 01   ········ ·`······
0030  00 00 00 02 01 01 a8 c0  00 00 00 00 20 0c 86 11   ········ ···· ···
0040  fb f0 00 00 00 00 00 00  00 00 00 38 01 01 20 0c   ········ ···8·· ·
0050  86 11 fb f0 00 00 00 00  00 00 45 58 43 49 54 45   ········ ··EXCITE
0060  4c 2d 32 2e 34 47 00 00  00 00 00 00 00 00 00 00   L-2.4G·· ········
0070  00 00 00 00 00 00 00 00  00 00 07 00 01 01 01 00   ········ ········
0080  00 00 00 00                                        ····
```

any: <live capture in progress>   Packets: 31 · Displayed: 31 (100.0%)

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



```
Frame 68: 62 bytes on wire (496 bits), 62 by
  Section number: 1
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capt
  Arrival Time: Sep  4, 2023 16:01:13.18454
  [Time shift for this packet: 0.000000000 s
  Epoch Time: 1693823473.184544799 seconds
  [Time delta from previous captured frame:
  [Time delta from previous displayed frame
  [Time since reference or first frame: 227
  Frame Number: 68
  Frame Length: 62 bytes (496 bits)
  Capture Length: 62 bytes (496 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
Linux cooked capture v1
  Packet type: Broadcast (1)
  Link-layer address type: Ethernet (1)
  Link-layer address length: 6
  Source: GXIndia_11:fb:f0 (20:0c:86:11:fb:
  Unused: 0000
  Protocol: ARP (0x0806)
  Padding: 00000000000000000000000000000000
  Trailer: 0000
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: GXIndia_11:fb:f0 (20:
  Sender IP address: 192.168.1.1
  Target MAC address: 00:00:00_00:00:00 (00
  Target IP address: 192.168.1.7
```

```
0000  00 01 00 01 00 06 20 0c  86 11 fb f0 00
0010  00 01 08 00 06 04 00 01  20 0c 86 11 fb
0020  01 01 00 00 00 00 00 00  c0 a8 01 07 00
0030  00 00 00 00 00 00 00 00  00 00 00 00 00
```

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.