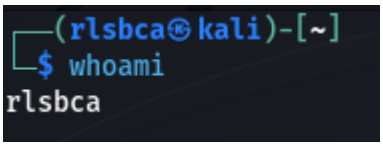
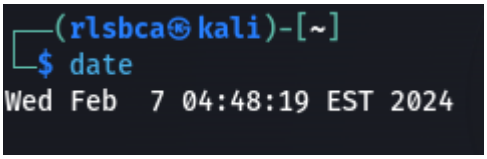
Lab1: Explain the Basic commandsof Kali Linux

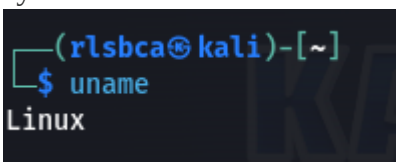
whoami : The **whoami**command allows Linux users to see the currently logged-in user. The output displays the username of the effective user in the current shell. Additionally,**whoami** is useful in bash scripting to show who is running the script.



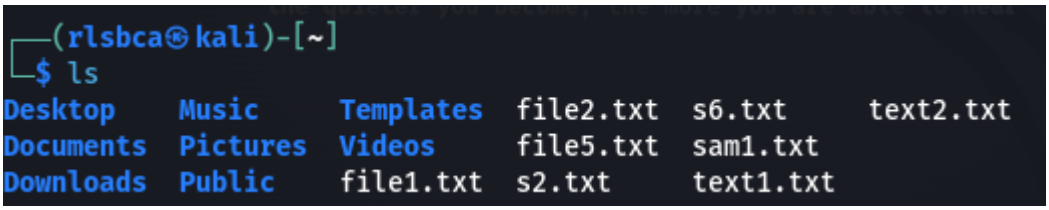
date : The date command is one of the most basic commands in Linux. To display the current date and time, simply type "date" at the command prompt and press enter. The output will display the current date and time in the format "**Day Month Date Time TimeZone Year"**



uname :The **'uname'** command displays the **current system's information.** We can view system information about our Linux environment with the uname command in Linux



ls :One of the most useful commands in Kali Linux is the **'ls'** command. The **ls** command lists the directory contents of files and directories.



history : The **'history'** command is one of Kali Linux's most commonly used commands. The history command in the bash shell saves a history of commands entered that can be used to repeat commands.

```
┌──(kali㉿kali)-[~]
└─$ history
    1
    2  airmon-ng
    3  air
    4  airmon-ng start [root]
    5  sudo airmon-ng
    6  sudo ip linl set IFACE down
    7  ifconfig
    8  sudo apt-get install kali-linux-wireless
    9  iwconfug
   10  air
   11  ifconfig
   12  sudo iw dev
   13  lsb_release -a
   14  clear
   15  cat /etc/os-release
   16  clear
   17  hostnamect1
   18  clear
   19  hostnamect 1
   20  hostnamectl
   21  clear
   22  hostnamectl
   23  iwconfig
   24  sudo iw dev
   25  sudo update
   26  timedatectl
   27  timedatectl list-timezones
   28  timedatectl
```

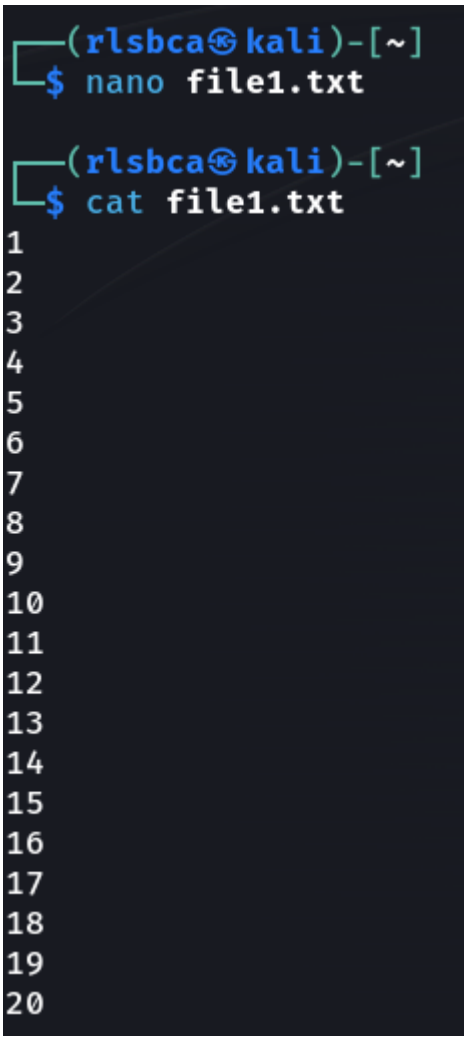
pwd :In Kali Linux, the '**Pwd**' command is used to **print working directory or present working directory.** It gives us information about the directory we are now in. This is especially useful if we need to access the directory while in the middle of a complicated process.

```
┌──(rlsbca㉿kali)-[~]
└─$ pwd
/home/rlsbca
```

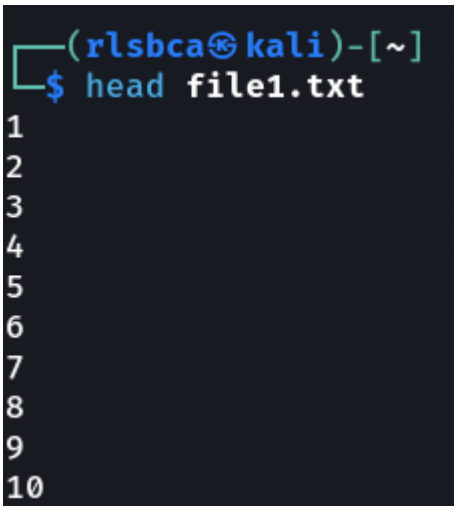
nano or vi: The vi editor is elaborated as **vi**sual editor. It is installed in every Unix system.

cat :The **'cat'** (concatenate) command is one of Kali Linux's most commonly used commands, permitting us to create single or many files, concatenate files and redirect, view contain of file output in terminal or files.

Usually, we use the cat command to display the content of a file.



head:The head command, as the name implies, print the top N number of data of the given input. By default, it prints the first 10 lines of the specified files.



```
┌──(rlsbca㉿kali)-[~]
└─$ head -n3 file1.txt
1
2
3
```

tail :The tail command, as the name implies, prints the last N number of data of the given input. By default, it prints the last 10 lines of the specified files.

```
┌──(rlsbca㉿kali)-[~]
└─$ tail file1.txt
11
12
13
14
15
16
17
18
19
20
```

```
┌──(rlsbca㉿kali)-[~]
└─$ tail -n3 file1.txt
18
19
20
```

cal:The cal command displays the current **month's formatted calendar** on our terminal screen.

```
┌──(rlsbca㉿kali)-[~]
└─$ cal
   February 2024
Su Mo Tu We Th Fr Sa
                1  2  3
 4  5  6  7  8  9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29
```

```
┌──(rlsbca㉿kali)-[~]
└─$ cal 2024
                                2024

      January               February                March
Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa
    1  2  3  4  5  6                  1  2  3                  1  2
 7  8  9 10 11 12 13   4  5  6  7  8  9 10   3  4  5  6  7  8  9
14 15 16 17 18 19 20  11 12 13 14 15 16 17  10 11 12 13 14 15 16
21 22 23 24 25 26 27  18 19 20 21 22 23 24  17 18 19 20 21 22 23
28 29 30 31           25 26 27 28 29        24 25 26 27 28 29 30
                                            31

       April                  May                   June
Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa
    1  2  3  4  5  6                  1  2  3  4                  1
 7  8  9 10 11 12 13   5  6  7  8  9 10 11   2  3  4  5  6  7  8
14 15 16 17 18 19 20  12 13 14 15 16 17 18   9 10 11 12 13 14 15
21 22 23 24 25 26 27  19 20 21 22 23 24 25  16 17 18 19 20 21 22
28 29 30              26 27 28 29 30 31     23 24 25 26 27 28 29
                                            30

        July                 August               September
Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa
    1  2  3  4  5  6                  1  2  3   1  2  3  4  5  6  7
 7  8  9 10 11 12 13   4  5  6  7  8  9 10   8  9 10 11 12 13 14
14 15 16 17 18 19 20  11 12 13 14 15 16 17  15 16 17 18 19 20 21
21 22 23 24 25 26 27  18 19 20 21 22 23 24  22 23 24 25 26 27 28
28 29 30 31           25 26 27 28 29 30 31  29 30
```

```
      October               November              December
Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa  Su Mo Tu We Th Fr Sa
       1  2  3  4  5                  1  2   1  2  3  4  5  6  7
 6  7  8  9 10 11 12   3  4  5  6  7  8  9   8  9 10 11 12 13 14
13 14 15 16 17 18 19  10 11 12 13 14 15 16  15 16 17 18 19 20 21
20 21 22 23 24 25 26  17 18 19 20 21 22 23  22 23 24 25 26 27 28
27 28 29 30 31        24 25 26 27 28 29 30  29 30 31
```

man : man command in Linux is used to display the user manual of any command that we can run on the terminal. It provides a detailed view of the command which includes NAME, SYNOPSIS, DESCRIPTION, OPTIONS, EXIT STATUS, RETURN VALUES, ERRORS, FILES, VERSIONS, EXAMPLES, AUTHORS and SEE ALSO.

```
┌──(rlsbca㉿kali)-[~]
└─$ man cal
```

```
CAL(1)                          General Commands Manual                          CAL(1)

NAME
       cal, ncal – displays a calendar and the date of Easter

SYNOPSIS
       cal [-3hjy] [-A number] [-B number] [[month] year]
       cal [-3hj] [-A number] [-B number] -m month [year]
       ncal [-3bhjJpwySM] [-A number] [-B number] [-W number] [-s country_code] [[month] year]
       ncal [-Jeo] [-A number] [-B number] [year]
       ncal [-CN] [-H yyyy-mm-dd] [-d yyyy-mm]

DESCRIPTION
       The cal utility displays a simple calendar in traditional format and ncal offers an alter-
       native  layout,  more  options and the date of Easter.  The new format is a little cramped
       but it makes a year fit on a 25x80 terminal.  If arguments are not specified, the  current
       month is displayed.

       The options are as follows:

       -h      Turns off highlighting of today.

       -J      Display  Julian Calendar, if combined with the -o option, display date of Orthodox
               Easter according to the Julian Calendar.

       -e      Display date of Easter (for western churches).

       -j      Display Julian days (days one-based, numbered from January 1).
 Manual page cal(1) line 1 (press h for help or q to quit)
```


cp :In Kali Linux, the '**cp**' command is used to **copy** files or a group of files or directories that create an exact image of a file on a disk with a different file name.

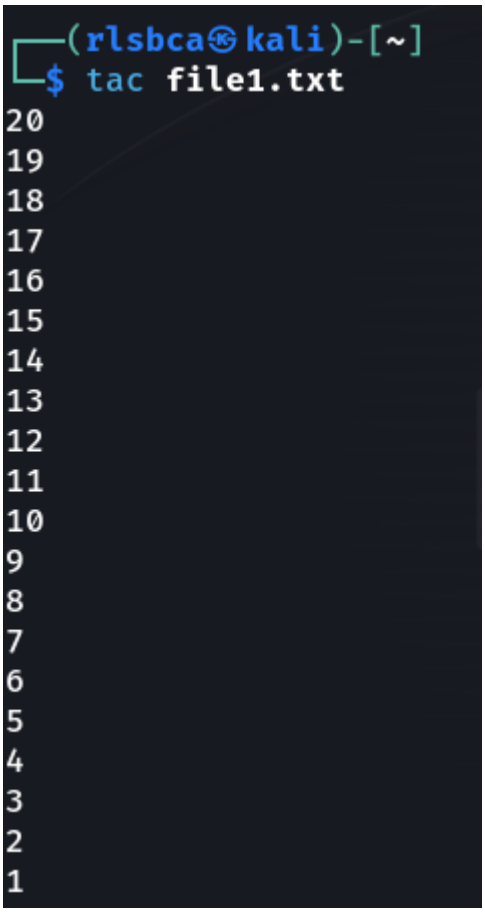
```
┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  s2.txt  sam1.txt  text2.txt
Documents  Music      Public    Videos     file5.txt  s6.txt  text1.txt

┌──(rlsbca㉿kali)-[~]
└─$ cp file1.txt file2.txt

┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  file5.txt  s6.txt    text1.txt
Documents  Music      Public    Videos     file2.txt  s2.txt     sam1.txt  text2.txt
```

cat : The cat command on Linux concatenates files together. It's often used to concatenate one file to nothing to print the single file's contents to the terminal. This is a quick way to preview the contents of a text file without having to open the file in a large application.

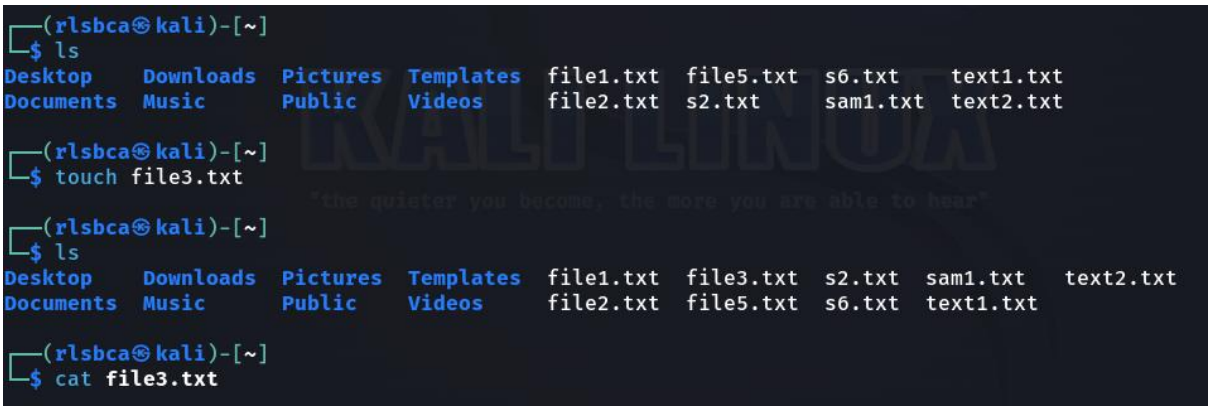
```
┌──(rlsbca㉿kali)-[~]
└─$ cat file1.txt
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
```

```
┌──(rlsbca㉿kali)-[~]
└─$ cat file2.txt
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
```

tac :The 'tac' command is the reverse of the 'cat' command. It is also known as 'cat' backward. It will display the file content in reverse order. It prints the last line first, then second last and so on. Such way, it prints the first line at last.



touch : touch command is a way to create empty files (there are some other mehtods also). You can update the modification and access time of each file with the help of touch command.



mkdir :The '**mkdir**' command is used to **create directories.** For example, if we wish to create a directory named '**Penetration testing**' under the '**Documents**' directory, then we have to open a terminal and enter the below command:

```
┌──(rlsbca㉿kali)-[~]
└─$ mkdir sample

┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  file3.txt  s2.txt  sam1.txt  text1.txt
Documents  Music      Public    Videos     file2.txt  file5.txt  s6.txt  sample    text2.txt
```

rm :In Kali Linux, the '**rm**' command is used to **delete files.** It can be used to delete directories when we use them recursively.

The removal process separates a file name form its associated data in a file system and identifies that space in the storage device as available for future writes. In other words, when we erase a file. the data inside it remains unchanged, but it is no longer linked to a filename.

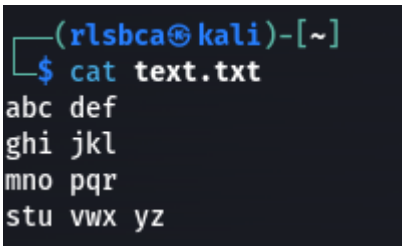
```
┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  file3.txt  s2.txt  sam1.txt  text1.txt
Documents  Music      Public    Videos     file2.txt  file5.txt  s6.txt  sample    text2.txt

┌──(rlsbca㉿kali)-[~]
└─$ rm s2.txt

┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  file3.txt  s6.txt    sample     text2.txt
Documents  Music      Public    Videos     file2.txt  file5.txt  sam1.txt  text1.txt
```

rmdir :This command is used to delete a directory. But will not be able to delete a directory including a sub-directory. It means, a directory has to be empty to be deleted.

```
┌──(rlsbca㉿kali)-[~]
└─$ rmdir sample

┌──(rlsbca㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  file1.txt  file3.txt  s6.txt    text1.txt
Documents  Music      Public    Videos     file2.txt  file5.txt  sam1.txt  text2.txt
```

wc:wc is short for ***word count***. It's a command mainly used to count purposes. It shows a four-columnar result by default. The first column displays the number of lines available in the specified file, the second column displays the number of words available in the file, the third column displays the number of characters available in the file, and the fourth column is the name of the file itself which are provided as an argument.

```
┌──(rlsbca㉿kali)-[~]
└─$ vi text.txt
```



-c :The '-c' option is used to display the number of bytes in a file

-w : The '-w' option is used to display the total number of words from a file

-l : The '-L' option is used to display the length of the longest line from a file..

```
┌──(rlsbca㉿kali)-[~]
└─$ wc text.txt
 4  9 35 text.txt

┌──(rlsbca㉿kali)-[~]
└─$ wc -l text.txt
4 text.txt

┌──(rlsbca㉿kali)-[~]
└─$ wc -c text.txt
35 text.txt

┌──(rlsbca㉿kali)-[~]
└─$ wc -w text.txt
9 text.txt
```

free :In Kali Linux, the '**free**' command provides us the useful information about the **amount of RAM** available on a Linux machine. It also displays the entire amount of **physical memory** used and available space, as well as **swap memory** with **kernel buffers.**

```
┌──(rlsbca㉿kali)-[~]
└─$ free
               total        used        free      shared  buff/cache   available
Mem:         2014536     1109432      427796        9404      637328      905104
Swap:         998396           0      998396
```

mv :With the help of the '**mv**' command, we can **move** or **renames** files and directories on our file system.

```
┌──(rlsbca㉿kali)-[~]
└─$ mv text.txt text1.txt

┌──(rlsbca㉿kali)-[~]
└─$ cat text1.txt
abc def
ghi jkl
mno pqr
stu vwx yz
```

sort:Using the '**sort**' command, we can sort the content of the text file, line by line. Sort is a standard command-line program which prints the lines of its input or concentration of all files listed in its argument list in sorted order.

```
┌──(rlsbca㉿kali)-[~]
└─$ vi number.txt

┌──(rlsbca㉿kali)-[~]
└─$ cat number.txt
5
2
1
6
75
2
1
6
7

┌──(rlsbca㉿kali)-[~]
└─$ sort number.txt
1
1
2
2
5
6
6
7
75
```

```
┌──(rlsbca㉿kali)-[~]
└─$ sort -r number.txt
75
7
6
6
5
2
2
1
1
```

```
┌──(rlsbca㉿kali)-[~]
└─$ cat number.txt
a
b
d
c
p
g
k
l
e
```

```
┌──(rlsbca㉿kali)-[~]
└─$ vi number.txt

┌──(rlsbca㉿kali)-[~]
└─$ sort number.txt
a
b
c
d
e
g
k
l
p

┌──(rlsbca㉿kali)-[~]
└─$ sort -r number.txt
p
l
k
g
e
d
c
b
a
```

Lab 2: Information Gathering

Dnsenum : **Dnsenum** is a tool for DNS enumeration, which is the process of locating all DNS servers and DNS entries for an organization.

DNS enumeration will allow us to gather critical information about the organization such as usernames, computer names, IP addresses, and so on.

dnsenum --dnsserver 8.8.8.8 facebook.com

```
ost's addresses:
________________

acebook.com.                    299     IN    A        157.240.11.35

ame Servers:
____________

.ns.facebook.com.               21592   IN    A        185.89.219.12
.ns.facebook.com.               21049   IN    A        129.134.30.12
.ns.facebook.com.               21599   IN    A        185.89.218.12
.ns.facebook.com.               21070   IN    A        129.134.31.12

ail (MX) Servers:
_________________

mtpin.vvv.facebook.com.         296     IN    A        69.171.251.251
```

```
dns.facebook.com.               3599    IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.         59      IN    A        157.240.11.17
es.facebook.com.                3599    IN    CNAME    star.facebook.com.
star.facebook.com.              3519    IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.         59      IN    A        157.240.11.17
europe.facebook.com.            3599    IN    CNAME    star.facebook.com.
star.facebook.com.              3436    IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.         59      IN    A        157.240.11.17
extern.facebook.com.            3599    IN    CNAME    extern.c10r.facebook.com.
extern.c10r.facebook.com.       59      IN    A        157.240.11.6
fr.facebook.com.                3599    IN    CNAME    star.facebook.com.
star.facebook.com.              3599    IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.         59      IN    A        157.240.11.17
```

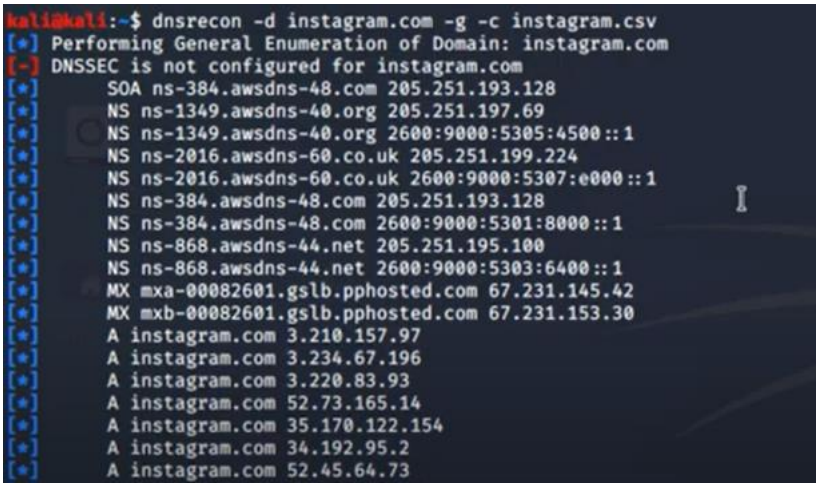
dnsrecon

dnsrecon –h

```
> Executing "dnsrecon -h"
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY]
                   [-f] [-t TYPE] [-a] [-s] [-g] [-b] [-k] [-w] [-z]
                   [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB]
                   [-x XML] [-c CSV] [-j JSON] [--iw]
                   [--disable_check_recursion] [--disable_check_bindversion]
                   [-v]
```

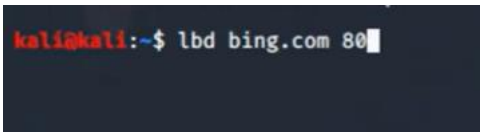
```
optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the
                        target will be used. Multiple servers can be specified
                        using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats
                        (first-last) or in (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for
                        brute force. Filter out of brute force domain lookup,
```

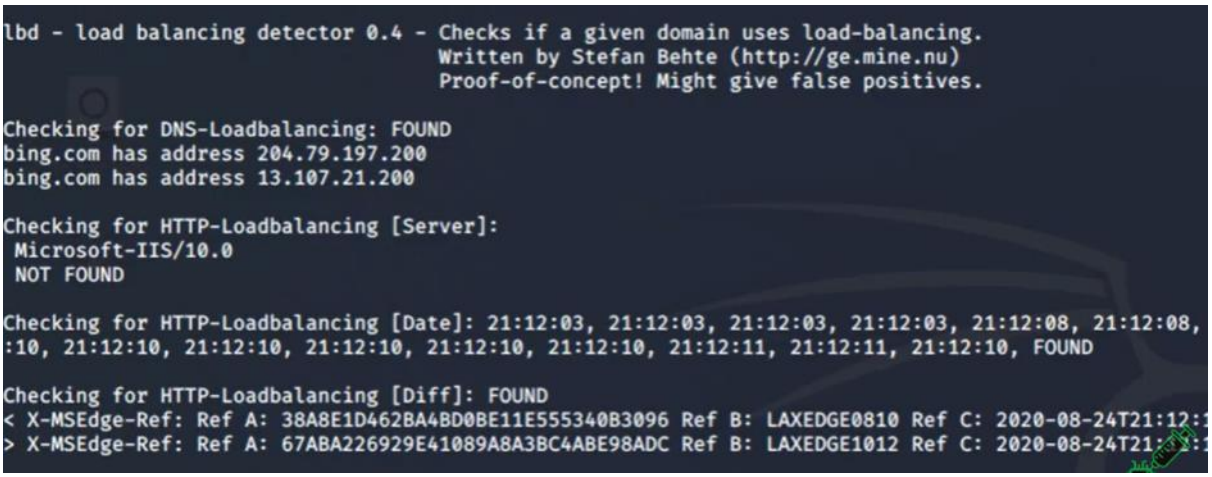
dnsrecon -d instagram.com –c insta.csv



Load balance detector

Manage traffic with all servers within cluster





Lab 3: Explain the network mapper (nmap)

Nmap : **Nmap** (**N**etwork **map**per) is an open-source Linux tool for network and security auditing. The tool helps network administrators reveal hosts and services on various systems.

Nmap works both locally and remotely. Typical uses include scanning for open ports, discovering vulnerabilities in a network, network mapping, and maintenance. The tool is valuable from both a security and networking standpoint.

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap www.geeksforgeeks.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:21 EST
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 18.75% done; ETC: 05:24 (0:02:06 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 18.80% done; ETC: 05:24 (0:02:10 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 22.60% done; ETC: 05:23 (0:01:43 remaining)
```

Nmap can reveal open services and ports by IP address as well as by domain name.

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap 172.217.27.174
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:22 EST
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 75.90% done; ETC: 05:24 (0:00:22 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.20% done; ETC: 05:24 (0:00:22 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.30% done; ETC: 05:24 (0:00:21 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.40% done; ETC: 05:24 (0:00:22 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.45% done; ETC: 05:24 (0:00:22 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.70% done; ETC: 05:24 (0:00:22 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.90% done; ETC: 05:24 (0:00:21 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 78.65% done; ETC: 05:24 (0:00:20 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 81.30% done; ETC: 05:24 (0:00:17 remaining)
Nmap scan report for kix05s07-in-f174.1e100.net (172.217.27.174)
Host is up (0.093s latency).
All 1000 scanned ports on kix05s07-in-f174.1e100.net (172.217.27.174) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 83.57 seconds
```

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap -v www.geeksforgeeks.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:25 EST
Initiating Ping Scan at 05:25
Scanning www.geeksforgeeks.org (52.84.12.29) [2 ports]
Completed Ping Scan at 05:25, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:25
Completed Parallel DNS resolution of 1 host. at 05:25, 0.08s elapsed
Initiating Connect Scan at 05:25
Scanning www.geeksforgeeks.org (52.84.12.29) [1000 ports]
Discovered open port 443/tcp on 52.84.12.29
Discovered open port 80/tcp on 52.84.12.29
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.40% done; ETC: 05:26 (0:00:35 remaining)
Increasing send delay for 52.84.12.29 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.55% done; ETC: 05:26 (0:00:36 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.75% done; ETC: 05:26 (0:00:37 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.90% done; ETC: 05:26 (0:00:37 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.05% done; ETC: 05:26 (0:00:38 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.25% done; ETC: 05:26 (0:00:38 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.45% done; ETC: 05:26 (0:00:37 remaining)
Increasing send delay for 52.84.12.29 from 5 to 10 due to 11 out of 14 dropped probes since last increase.
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.60% done; ETC: 05:26 (0:00:22 remaining)
```



```
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

Scan Multiple Hosts: Nmap can scan multiple locations at once rather than scanning a single host at a time. This is useful for more extensive network infrastructures. There are several ways to scan numerous locations at once, depending on how many locations you need to examine.

Add multiple domains or multiple IP addresses in a row to scan multiple hosts at the same time.

```
└─$ nmap 103.76.228.224 157.240.198.35 172.217.27.174
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:30 EST
Stats: 0:00:23 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 18.03% done; ETC: 05:32 (0:01:40 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 36.07% done; ETC: 05:33 (0:01:52 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 57.77% done; ETC: 05:33 (0:01:13 remaining)
Stats: 0:02:22 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 76.52% done; ETC: 05:33 (0:00:43 remaining)
Stats: 0:02:54 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 92.97% done; ETC: 05:33 (0:00:13 remaining)
Nmap scan report for server2.iwave-global.com (103.76.228.224)
Host is up (0.070s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
53/tcp  open  domain
111/tcp open  rpcbind
465/tcp open  smtps
```

```
Nmap scan report for edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)
Host is up (0.076s latency).
All 1000 scanned ports on edge-star-mini-shv-01-del1.facebook.com (157.240.198.35) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for kix05s07-in-f174.1e100.net (172.217.27.174)
Host is up (0.084s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 3 IP addresses (3 hosts up) scanned in 188.91 seconds
```

Use the * wildcard to scan an entire subnet at once.

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap 103.76.228.*
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:35 EST
Stats: 0:00:36 elapsed; 208 hosts completed (48 up), 48 undergoing Connect Scan
Connect Scan Timing: About 0.66% done
Stats: 0:01:21 elapsed; 208 hosts completed (48 up), 48 undergoing Connect Scan
Connect Scan Timing: About 1.59% done; ETC: 06:27 (0:50:30 remaining)
Stats: 0:02:02 elapsed; 208 hosts completed (48 up), 48 undergoing Connect Scan
Connect Scan Timing: About 2.32% done; ETC: 06:40 (1:03:15 remaining)
Stats: 0:02:26 elapsed; 208 hosts completed (48 up), 48 undergoing Connect Scan
Connect Scan Timing: About 2.67% done; ETC: 06:48 (1:09:57 remaining)
```

Use a hyphen to scan a range of IP addresses.

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap 192.168.0.50-100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:39 EST
Nmap scan report for 192.168.0.92
Host is up (0.0088s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 51 IP addresses (1 host up) scanned in 17.21 seconds
```

Scan to Detect Firewall Settings

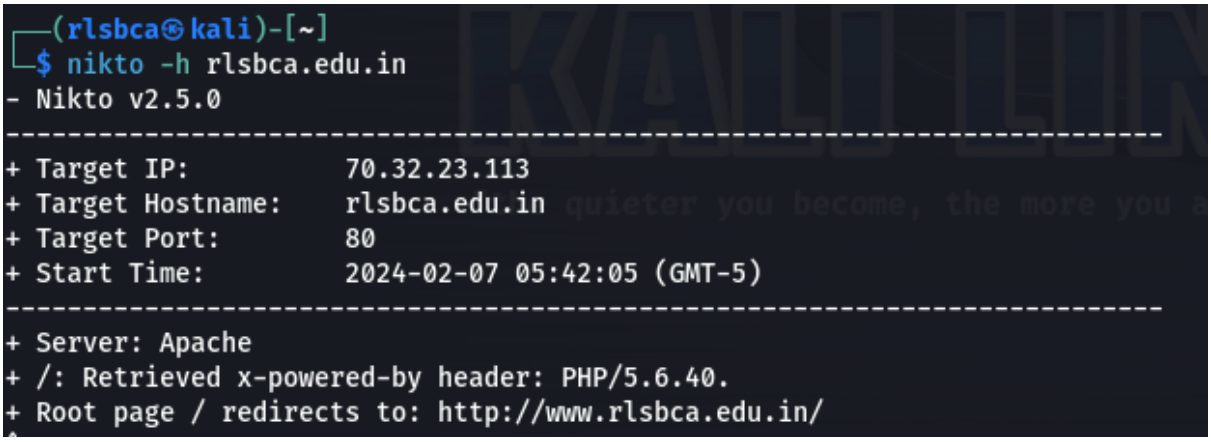
Detecting firewall settings can be useful during penetration testing and vulnerability scans. Several functions can be used to detect firewall settings across the given hosts, but the **-sA** flag is the most common.

```
┌──(rlsbca㉿kali)-[~]
└─$ nmap -sA 192.68.0.50
You requested a scan type which requires root privileges.
QUITTING!

┌──(rlsbca㉿kali)-[~]
└─$ sudo nmap -sA 192.68.0.50
[sudo] password for rlsbca:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 05:41 EST
Nmap scan report for 192.68.0.50
Host is up (0.0019s latency).
All 1000 scanned ports on 192.68.0.50 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

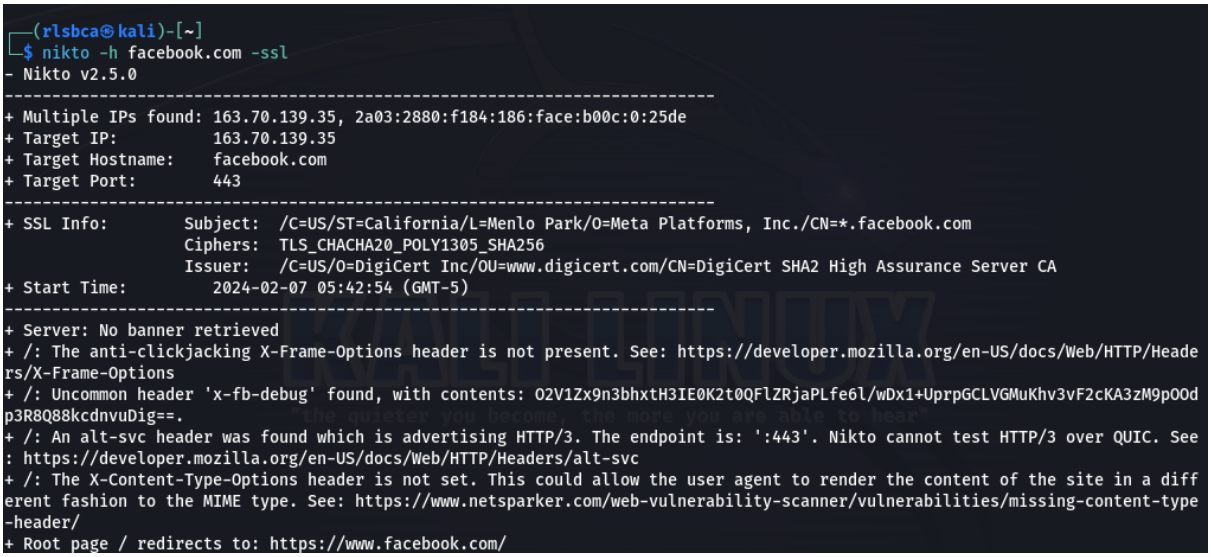
Lab 4: Explain the vulnerability Analysis Tool(Nikto)

Nikto is an open-source web server scanner which performs comprehensive tests against web servers for multiple items.

Nikto in scanning websites for some vulnerability.



To scan an SSL-enabled website



Scans the specified port

```
┌──(rlsbca㉿kali)-[~]
└─$ nikto -h rlsbca.edu.in -port 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          70.32.23.113
+ Target Hostname:    rlsbca.edu.in
+ Target Port:        80
+ Start Time:         2024-02-07 05:44:19 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: Retrieved x-powered-by header: PHP/5.6.40.
+ Root page / redirects to: http://www.rlsbca.edu.in/
```

Nikto -h -port (Port Number1),(Port Number2) : Scan host targeting specific ports

```
┌──(rlsbca㉿kali)-[~]
└─$ nikto -h facebook.com -port  80,44,22
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 163.70.139.35, 2a03:2880:f184:186:face:b00c:0:25de
+ Multiple IPs found: 163.70.139.35, 2a03:2880:f184:186:face:b00c:0:25de


---------------------------------------------------------------------------
+ Multiple IPs found: 163.70.139.35, 2a03:2880:f184:186:face:b00c:0:25de
```

Disables nikto attempting to guess a 404 page

```
┌──(rlsbca㉿kali)-[~]
└─$ nikto -h facebook.com -no404
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 163.70.139.35, 2a03:2880:f184:186:face:b00c:0:25de
+ Target IP:          163.70.139.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-02-07 05:46:54 (GMT-5)
---------------------------------------------------------------------------
```

Lab 5:Advanced search Engine Google Dork

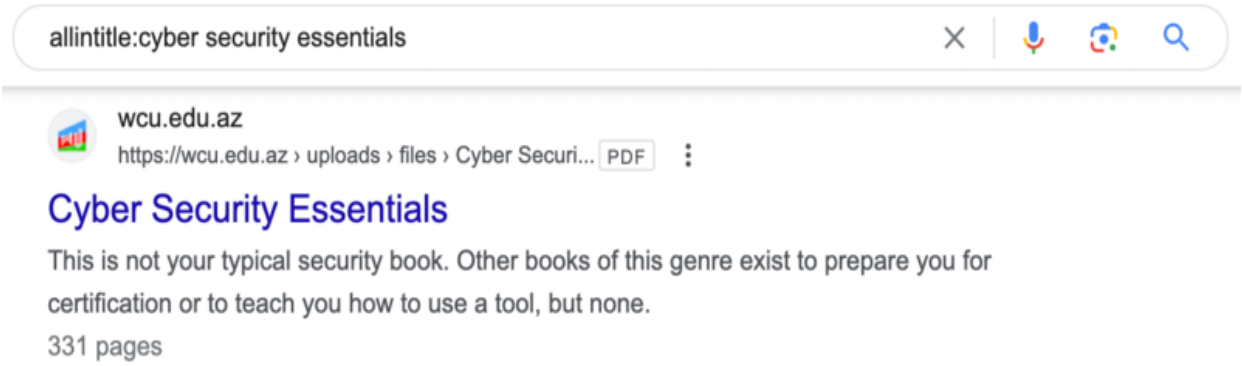
What Is a Google Dork?

Most people know what a Google search is. A Google dork is an advanced Google search using only the search box. Combining Google dorks in a single query helps you filter out irrelevant content.

Allintitle:

The allintitle: dork looks for pages with titles containing the search terms. It applies to the entire query string. You can see each word in the query string in the title of each search engine result returned. It's useful when the title of your desired web resource contains a series of keywords.

allintitle:cyber security essentials



Allinurl:

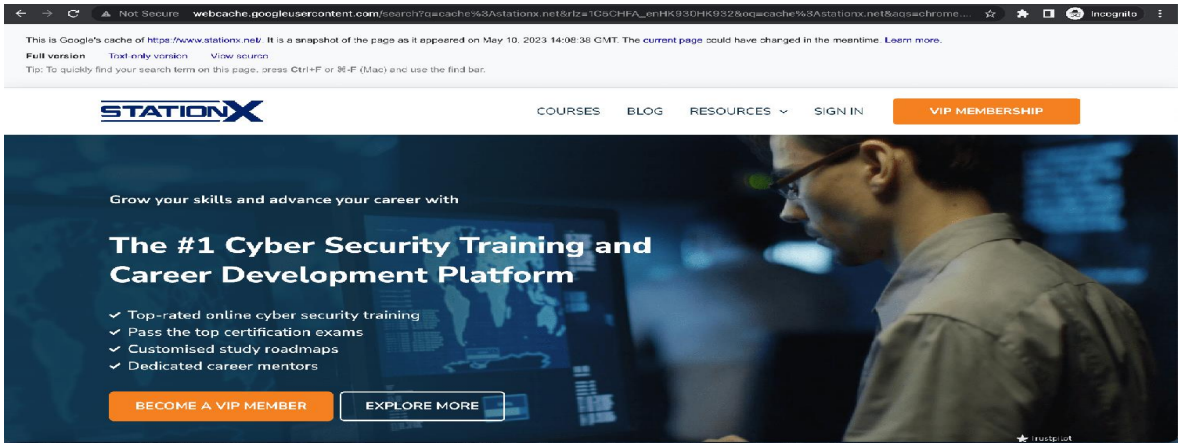
The allinurl: dork finds links containing all words following the colon (:), and it's equivalent to applying inurl: to discrete search strings. You can see all query items in the URL of each Google search result returned. It's a useful dork when you know what to look for in your desired URLs.

allinurl:cyber security hacker

Cache:

Using the cache: dork, when you press **Enter/Return**, the Google search console fetches the last saved copy of a particular website (Google cache) if it exists and displays it. It's useful for rediscovering a website before its downtime or latest update.

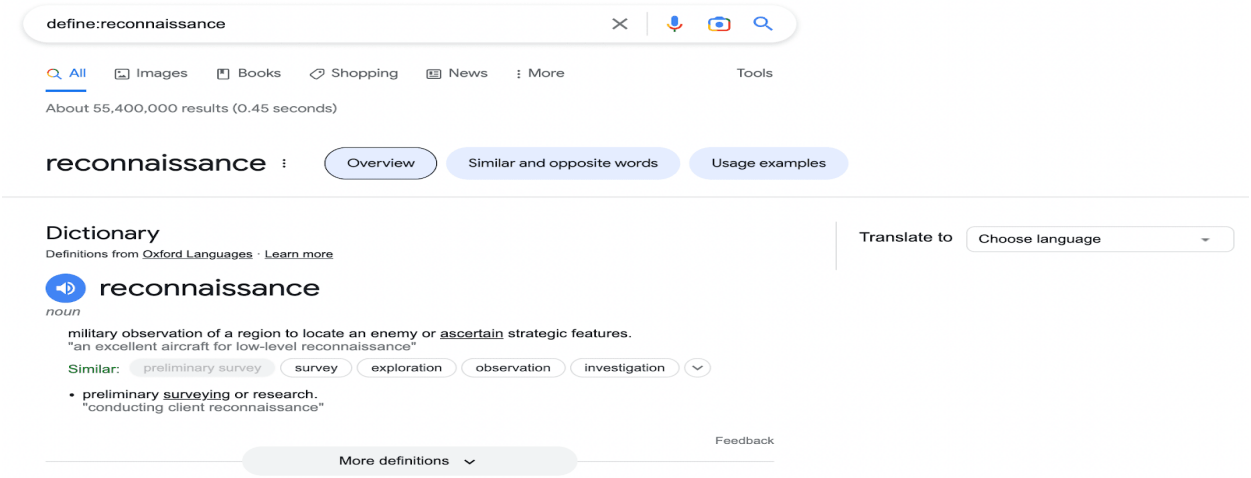
cache:courses.stationx.net



Define:

The define: dork returns definitions of a word or phrase. The Google search results are various dictionary definitions of the query item. It's useful when you want to find a word or phrase's meaning conveniently.

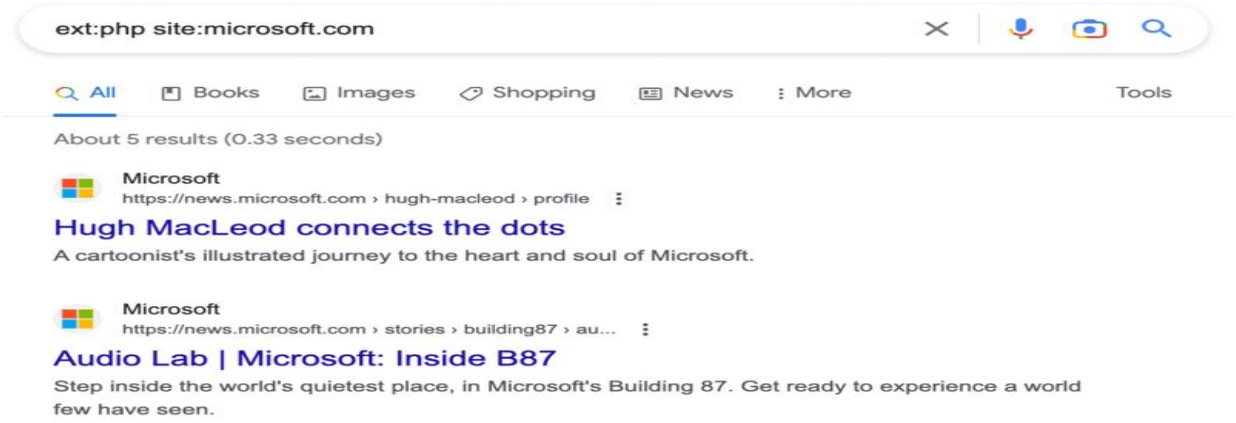
define:reconnaissance



Ext:

The ext: dork restricts the returned web addresses to the designated extension, such as PDF or XLS. Unlike most other dorks, it **requires additional keywords/dorks** in the search bar, or it'll return no results. The Google search results have the designated file extensions. You can use it to find leaked passwords and cameras in penetration testing (pentesting).

ext:php site:microsoft.com



Filetype:

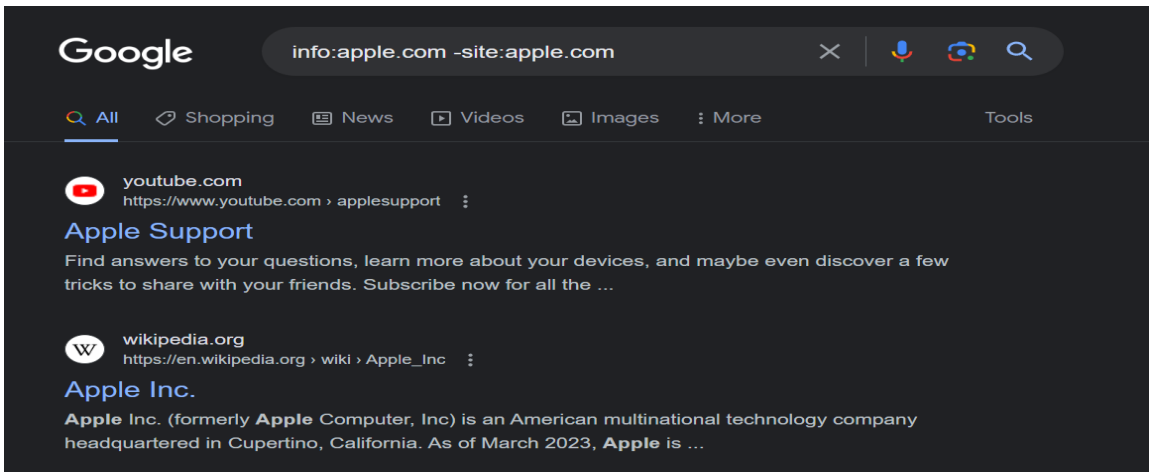
The filetype: dork restricts the returned web addresses to the designated file type, such as PDF or XLS. Unlike most other dorks, it **requires additional keywords/dorks** in the search bar, or it'll return no results. The Google search results have the designated file type. It's necessary for pentests such as bypassing paywalls to access resources.

filetype:pdf site:apple.com

Info:

The info: dork returns pages that convey information about a website. The Google search engine results are the website's cache, similar pages, and pages that link to it. It's useful when you want to find third-party resources about a web page.

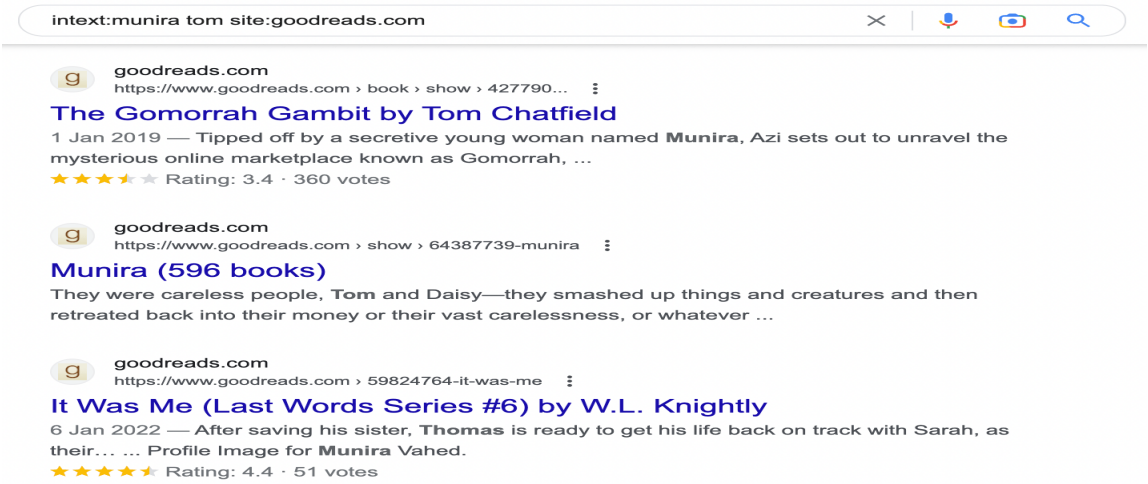
info:apple.com -site:apple.com



Intext:

The intext: dork finds websites containing the query string. You can see the query string in the text body of each Google search result returned. It's useful when the content body of your desired web page contains a certain keyword. In the demonstration below, we're looking for web pages of books with "munira" in the body but include "tom" anywhere.

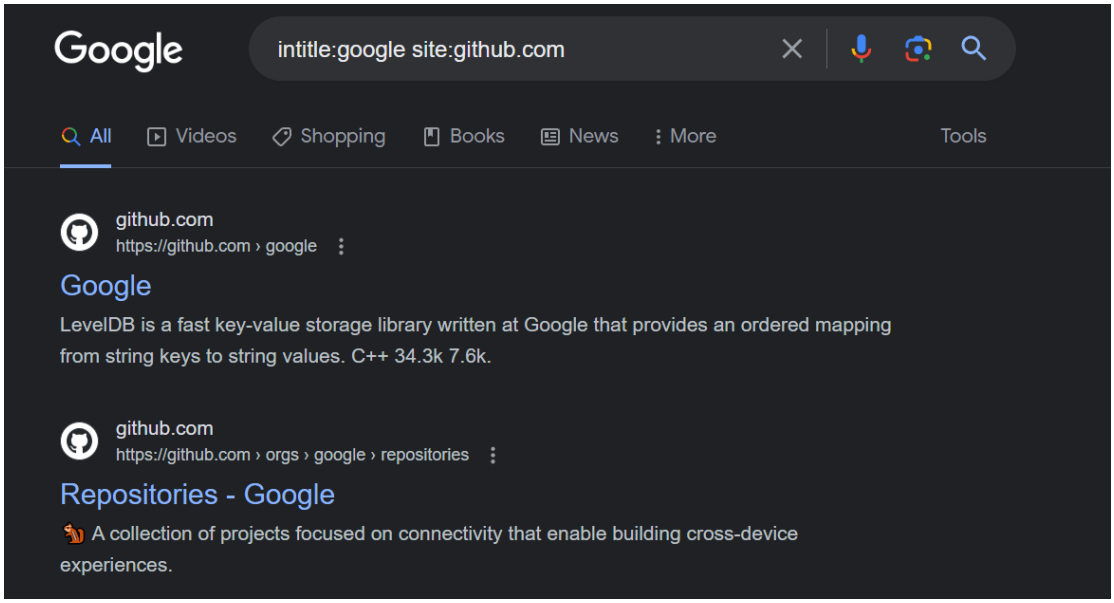
intext:munira tom site:goodreads.com



Intitle:

The intitle: dork looks for pages with titles containing the search terms. You can see the query string in the title of each Google search result returned. It's useful when the title of your desired web resource contains a certain keyword. In the example below, we look for all our pages containing "google" in the title.

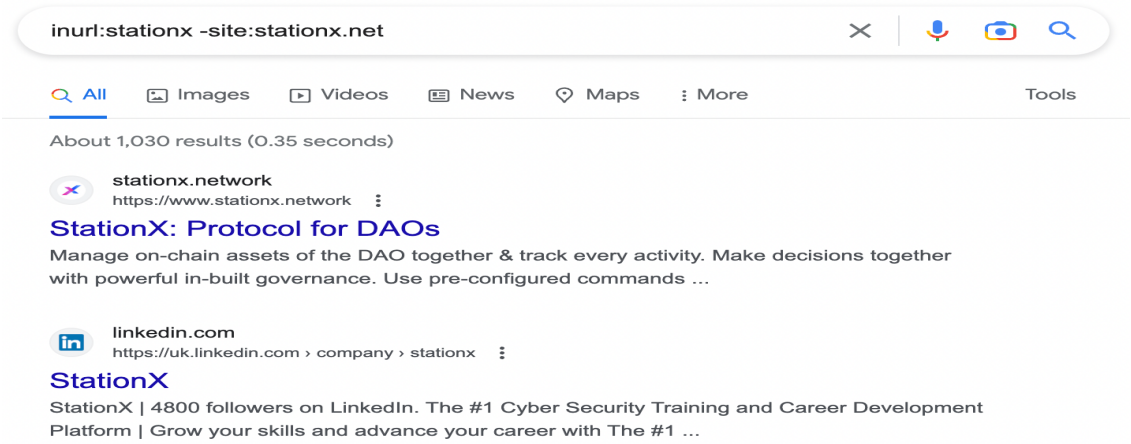
intitle:google site:github.com



Inurl:

The inurl: dork finds URLs containing the character string. You can see the query string in the URL of each Google search result returned. In the example below, the additional dork is to exclude search results from our website. It's a handy dork when your desired URLs follow a certain pattern.

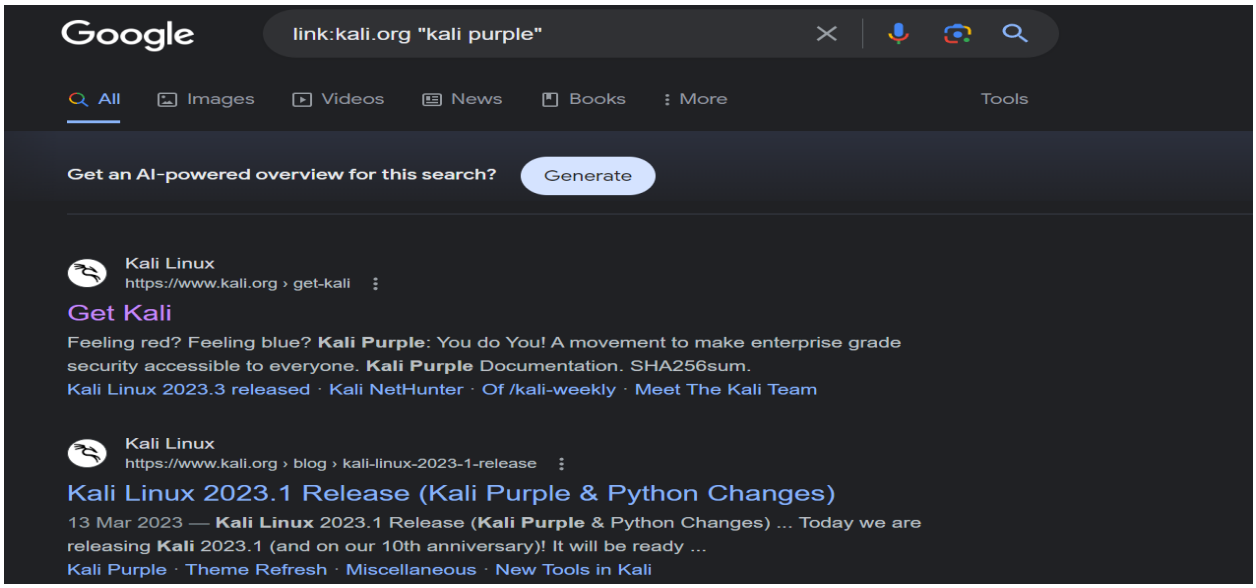
inurl:stationx -site:stationx.net



Link:

The link: dork finds web pages linking to the given web domain. The Google search results can be from the given domain or third-party websites linking to the given domain. It can help you when you want to estimate the impact of a web resource.

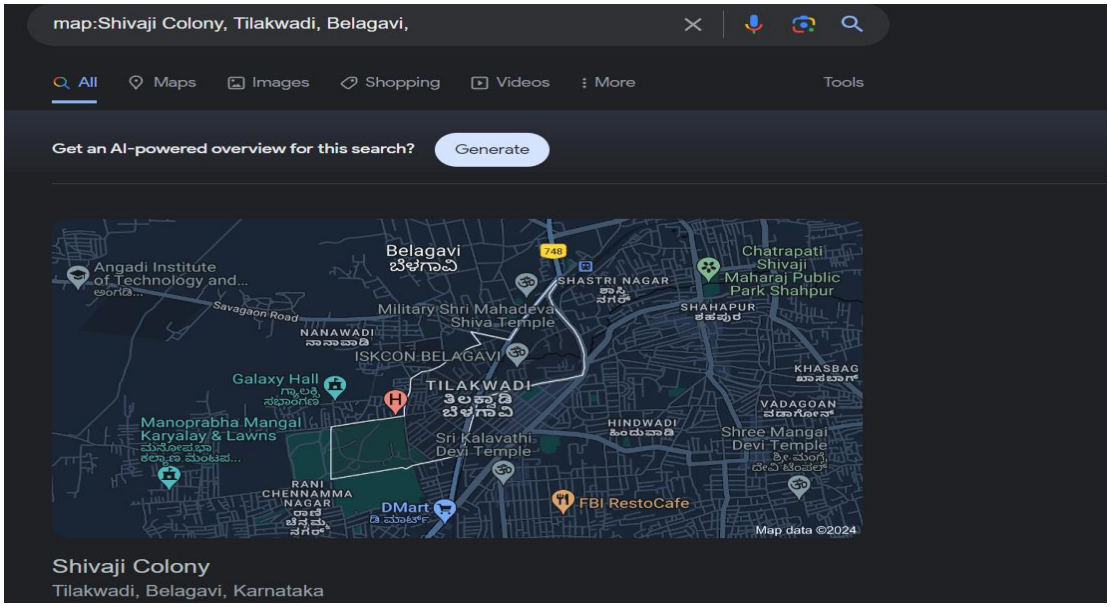
link:kali.org "kali purple"



Map:

The map: dork is for getting a map of the given location. Google returns with the map you're seeking. On macOS, you may see a prompt to open the Maps application. It's useful when you want a quick map of your desired location.

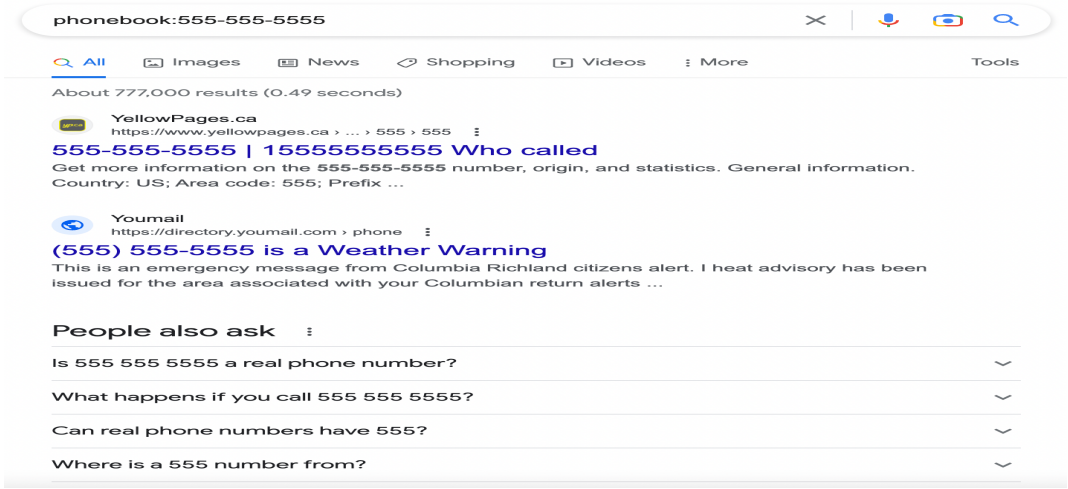
map:Shivaji Colony, Tilakwadi, Belagavi,



Phonebook:

The phonebook: dork is for getting a specific person or business's phone numbers and contact information. The Google search may return no results or several. The screenshot demonstration below has to do with **fictional US phone numbers**. This command is helpful when you want to look up caller IDs.

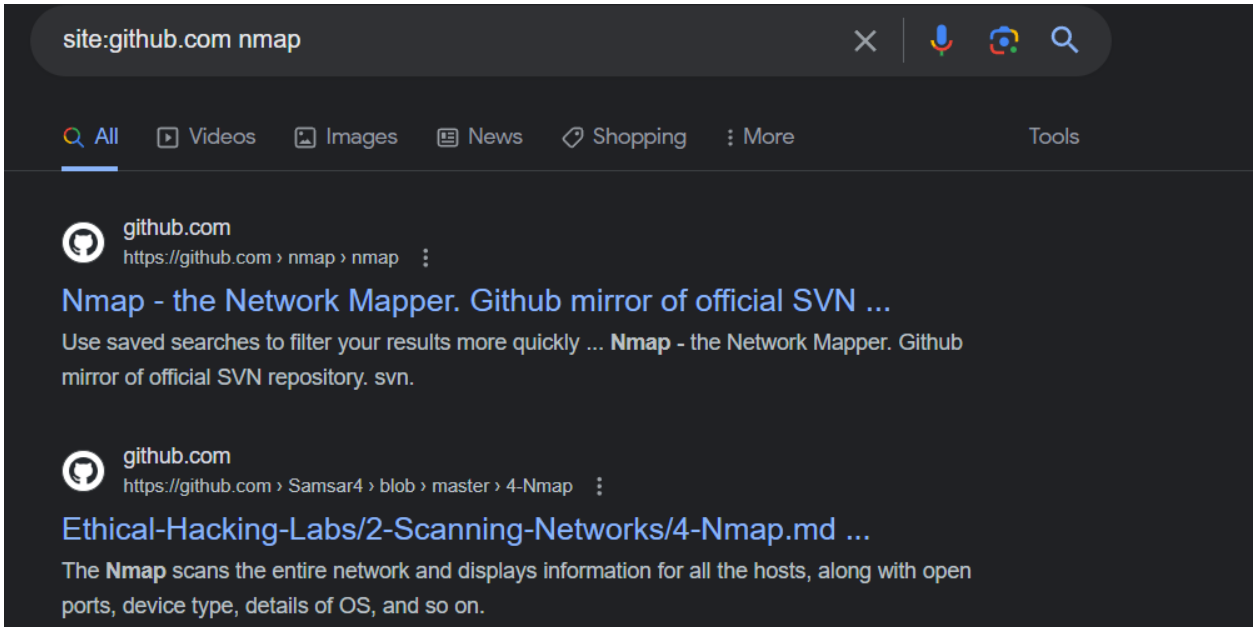
phonebook:555-555-5555



Site:

The site: dork restricts your search to a particular website, top-level domain, or subdomain. Additional query items are optional. The Google search results are pages within the website, top-level domain, or subdomain that contain your query items. It's essential for focusing on content from a particular web location, such as your server.

site:github.com nmap



Lab 6 : Explain Social Engineering tool

Social Engineering

The term **"social engineering"** is derived from the words **"social"** and **"engineering,"** where **"social"** refers to personal, professions, and our day-in-day-out lives. On the other hand, **"engineering"** involves comprehensive processes to complete a work such that the defined goal is met. In other words, it is a set of methods.

When social and engineering is combined, we get social engineering, which involves intrusion based on human interaction. It is a non-technical intrusion in which a person is often tricked into breaking the general security guidelines already set in an institution.

Social Engineering Toolkit

Social engineering toolkit is a **free and open-source tool** which is used for social engineering attacks like **phishing, sending SMS, faking phone,** etc. It is a free tool that comes with Kali Linux, or we can download and install it directly from **Github.** The Social Engineering Toolkit is designed and developed by a programmer named **Dave Kennedy.** Security researchers and penetration testers use this tool to check cybersecurity issues in systems all over the world. The goal of the social engineering toolkit is to perform attacking techniques on their machines. This toolkit also includes website vector attacks and custom vector attacks, which allow us to **clone any website, perform phishing attacks.**

Features of Social Engineering Toolkit

The following are the features of the social engineering toolkit:

- Social Engineering Toolkit is **free** and **open source.**
- Social Engineering Toolkit is portable, which means we can quickly switch attack vectors.
- Social Engineering Toolkit supports integration with third-party modules.

- Social Engineering Toolkit is already installed in our Kali Linux, but we can also download and install it from **Github.**
- Social Engineering Toolkit is a **multi-platform** tool; we can run it in **Windows, Linux,** and **Unix.**
- Social Engineering Toolkit contains access to the **Fast-Track Penetration Testing platform.**
- Social Engineering Toolkit offers various attack vectors like **Website Attacks, Infection Media Generator, Website Attacks,** etc

Uses of Social Engineering Toolkit

There are various uses of social engineering toolkit:

1. Web Attack
2. Mass Mailer Attack
3. Phishing Attacks
4. Create a Payload and Listene

Example of Google Phishing page- one kind of social engineering attack done through fake links over mail, sms)

Perform Google and Twitter Phishing

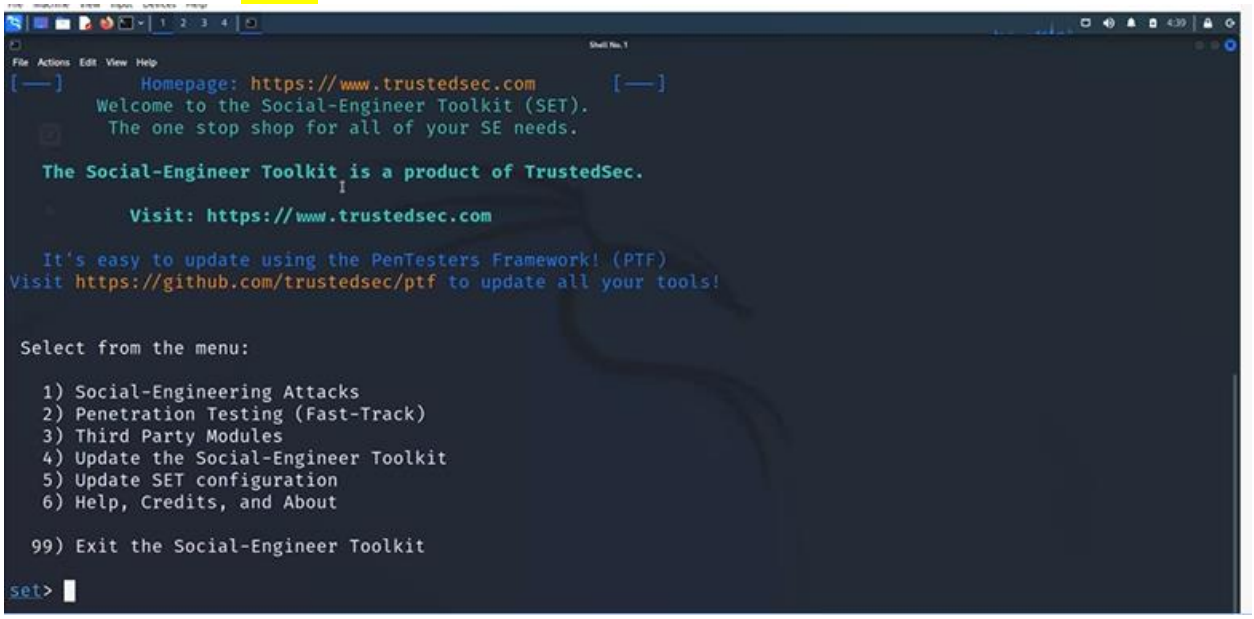
Working with Social Engineering Toolkit in Kali Linux.

Activity-1: Phishing Google and Twitter homepage using *set*.

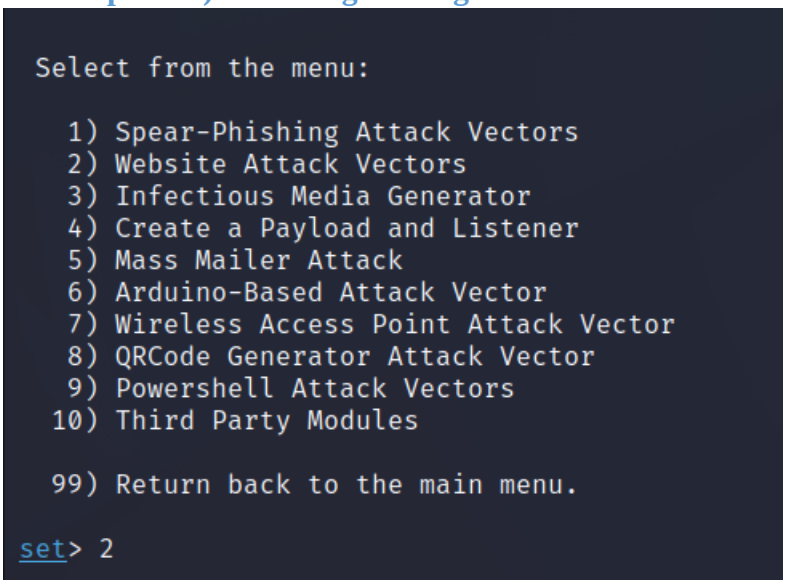
Open Kali linux

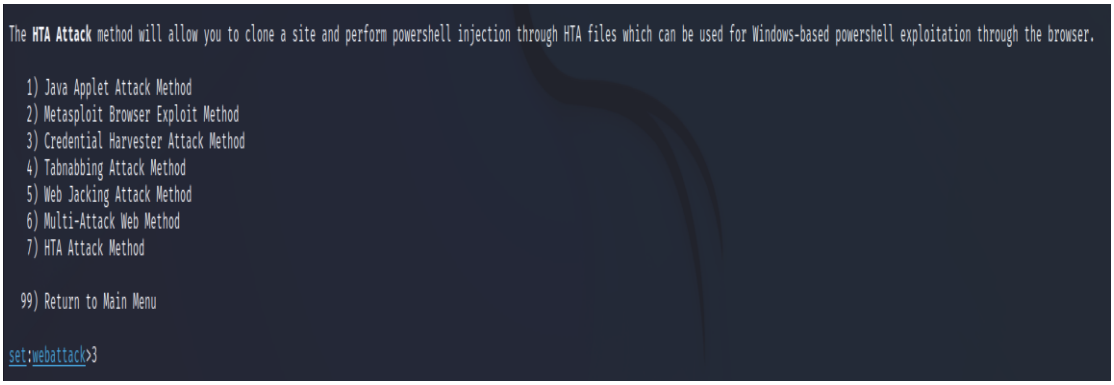
Go to Applications-> Social Engineering Tools-> Social Engineering Tool Kit (root)

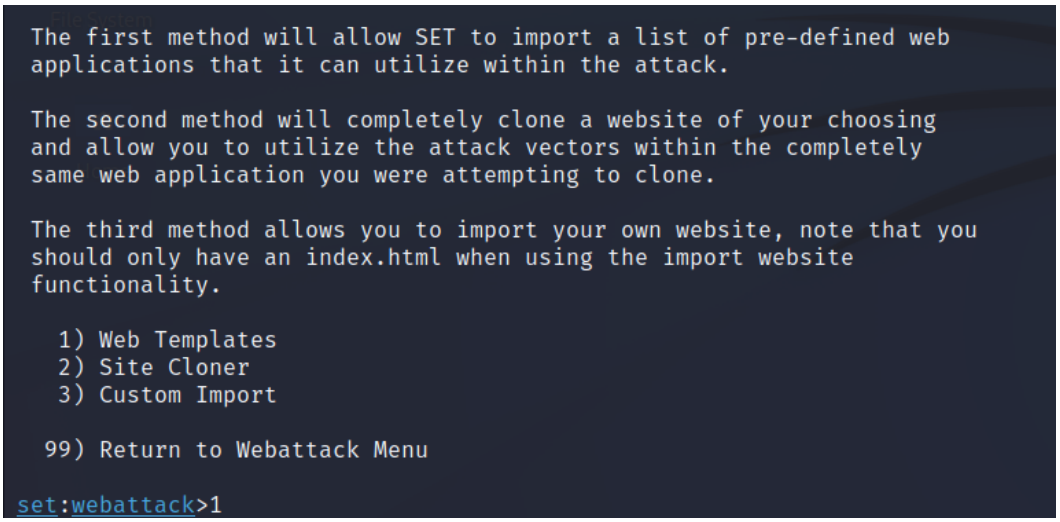
Password for kali: rlsbca



Select option 1)Social Engineering Attacks






The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:1

_____________________________________________________

        **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config
```

```
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_____________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

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

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [24/Nov/2022 07:46:03] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:04] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:14] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET /favicon.ico HTTP/1.1" 404 -
```

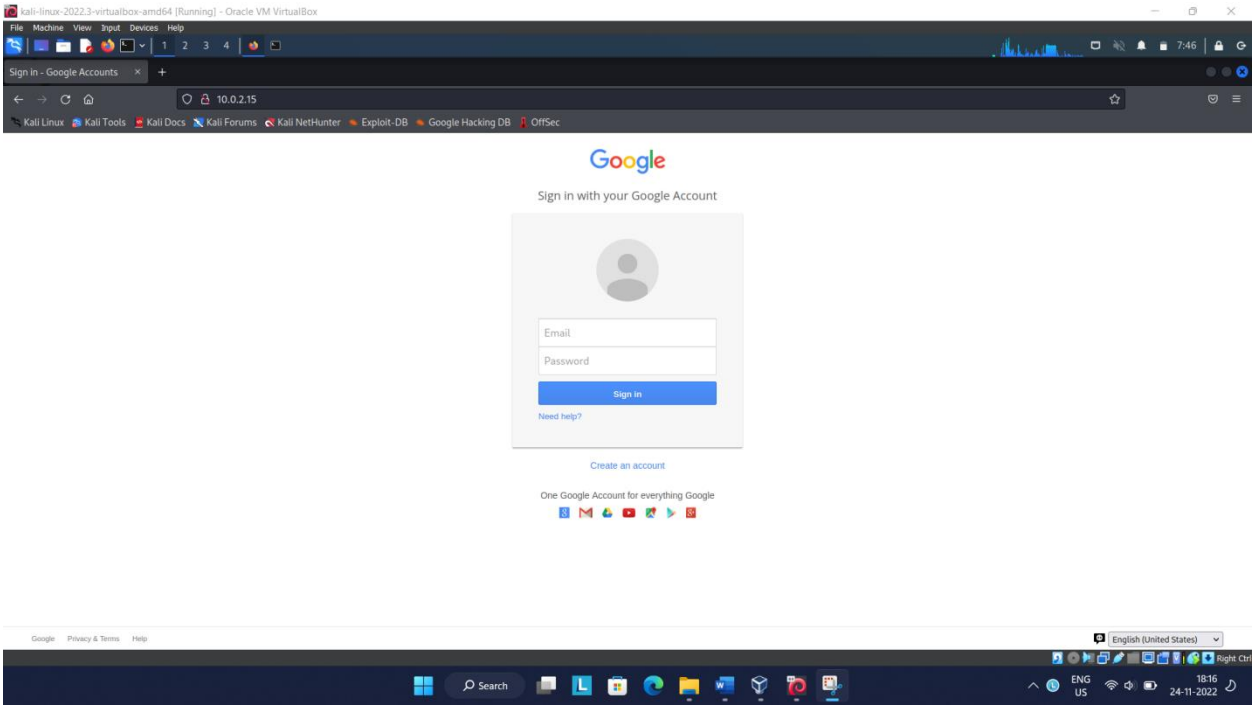


Image 1: cloned Google Sign In page

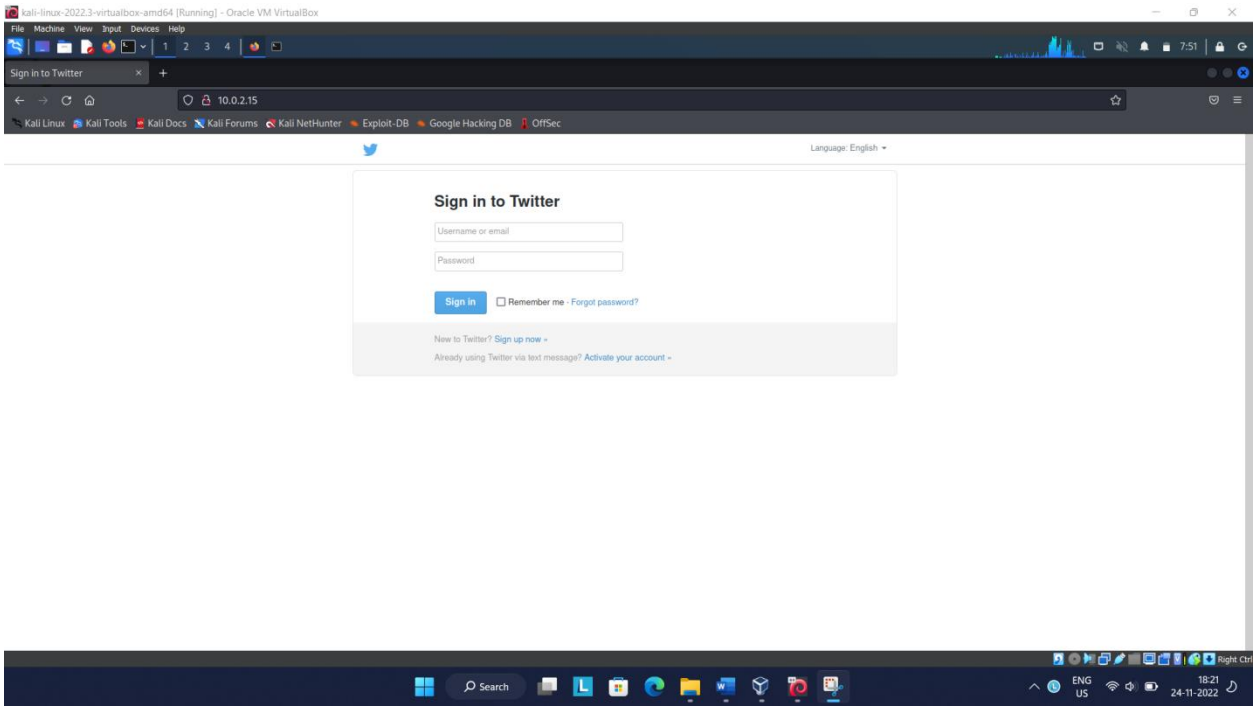


Image 2: Cloned Twitter Sign In page

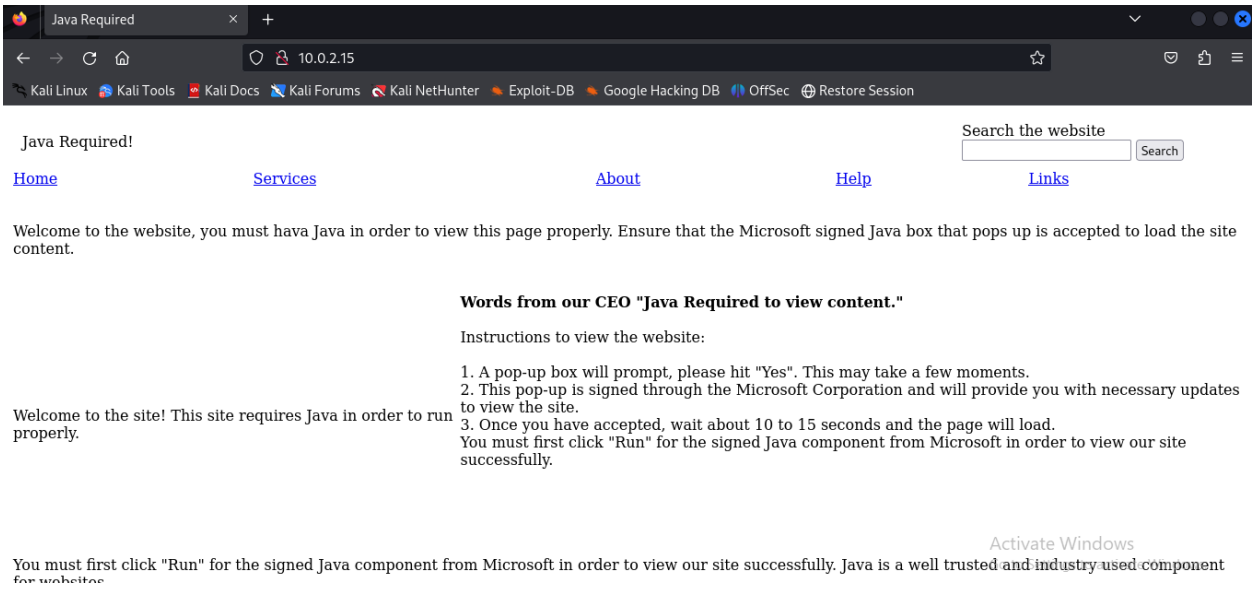
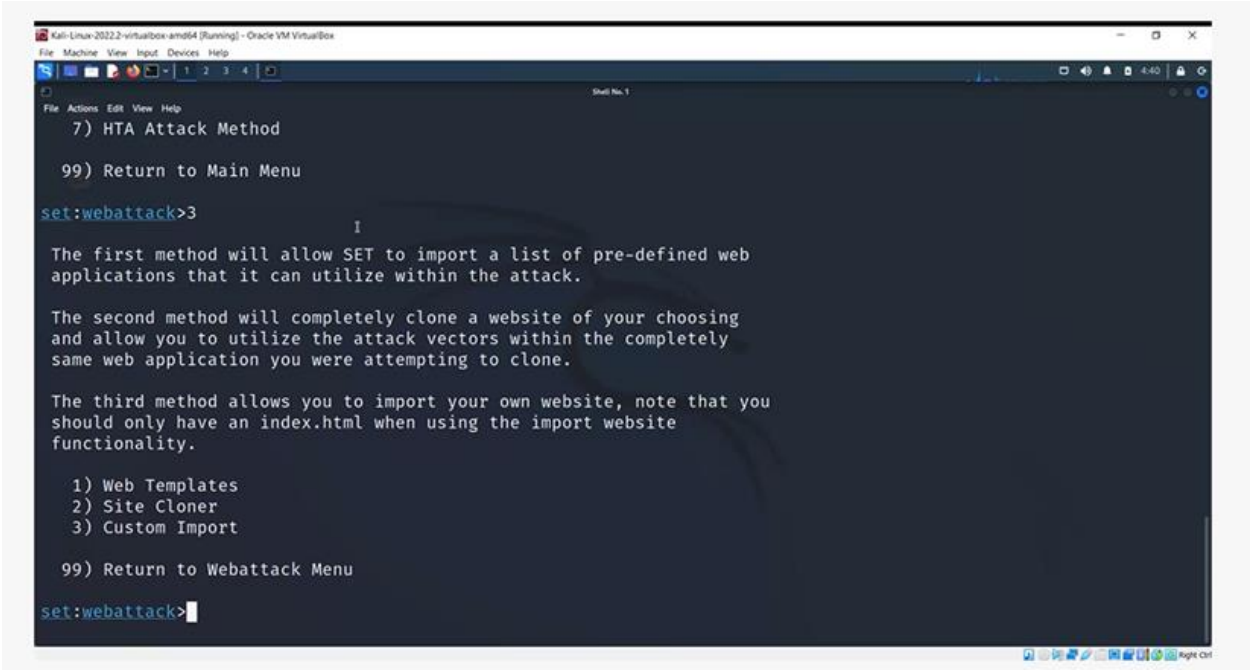


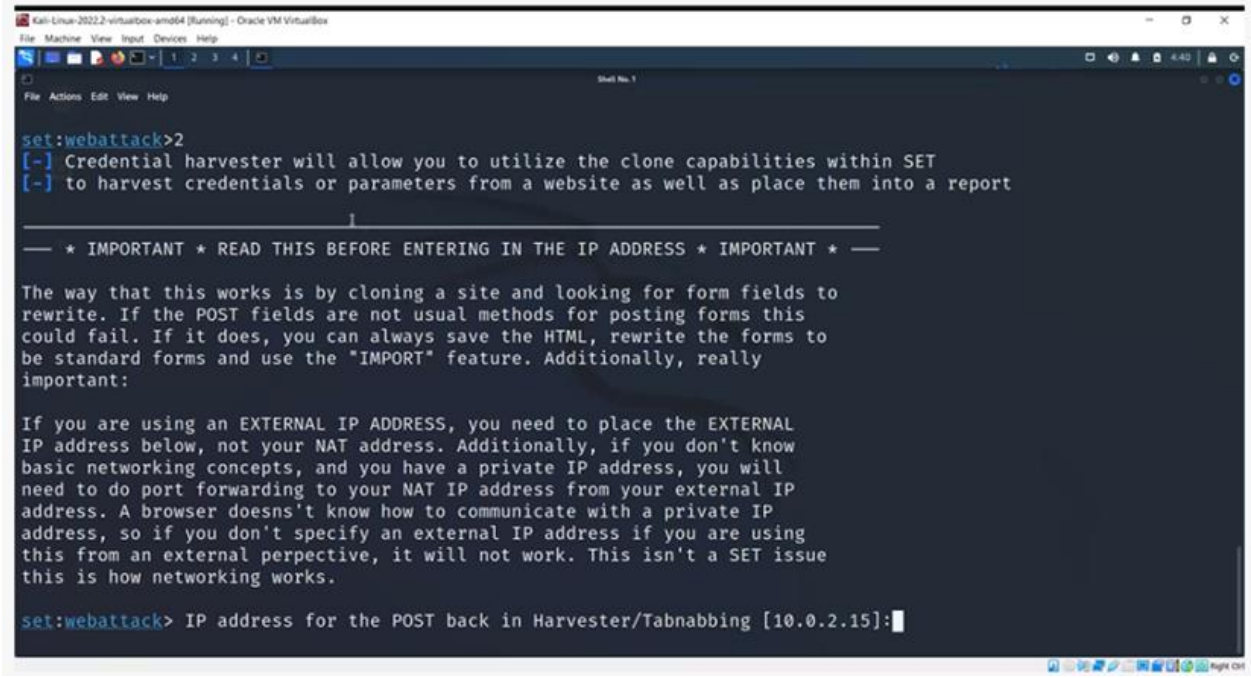
Image 3: Cloned Java Required page

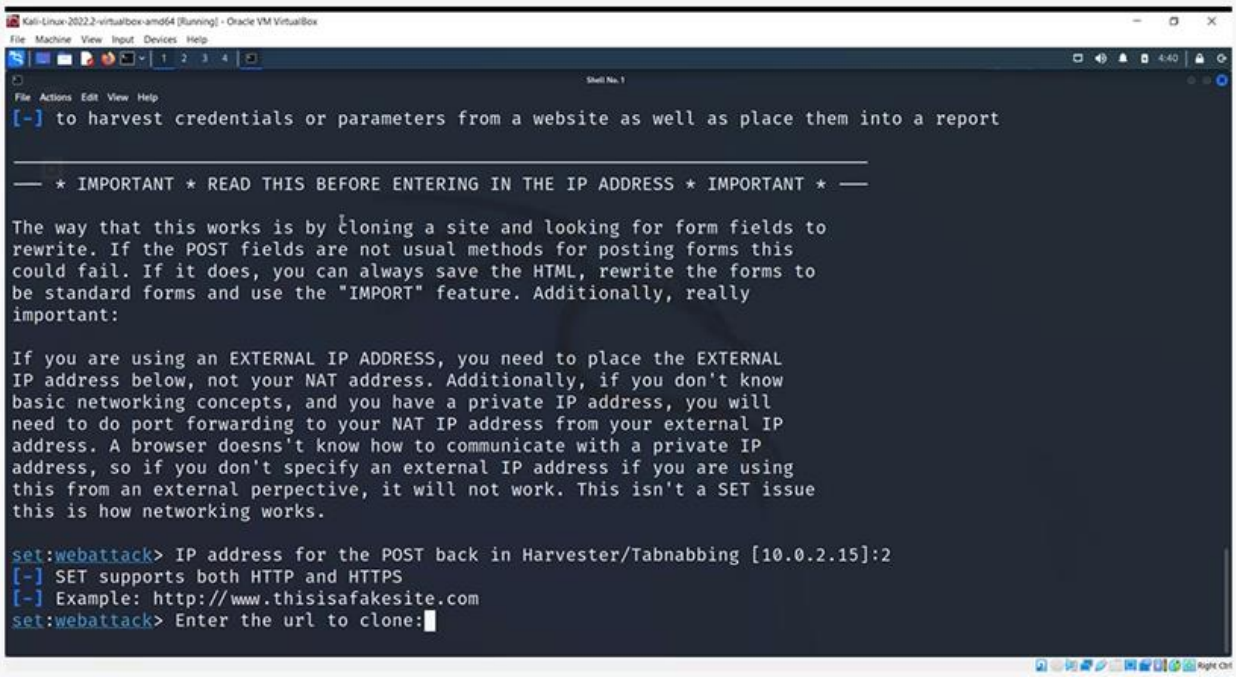
For more information refer: https://www.javatpoint.com/social-engineering-in-kali-linux

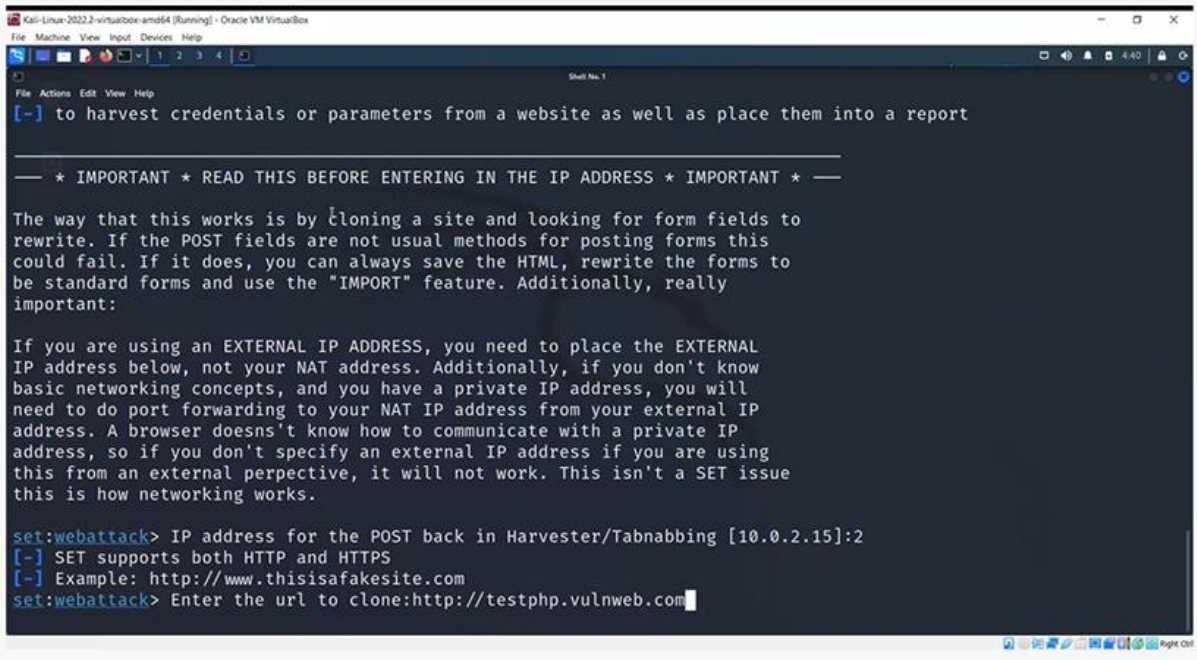
Activity 2: Site Cloner (Enter the url to be cloned: http://testphp.vulnweb.com)

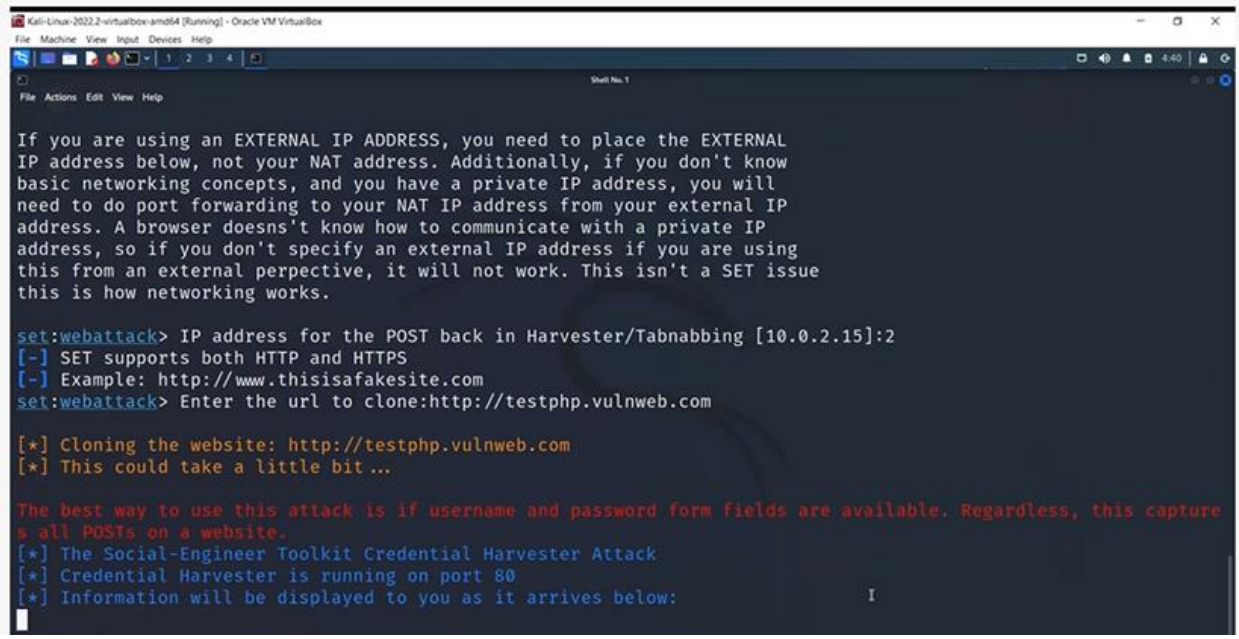
Repeat the same steps as above you did for twitter phishing.Use step 2) site cloner


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>

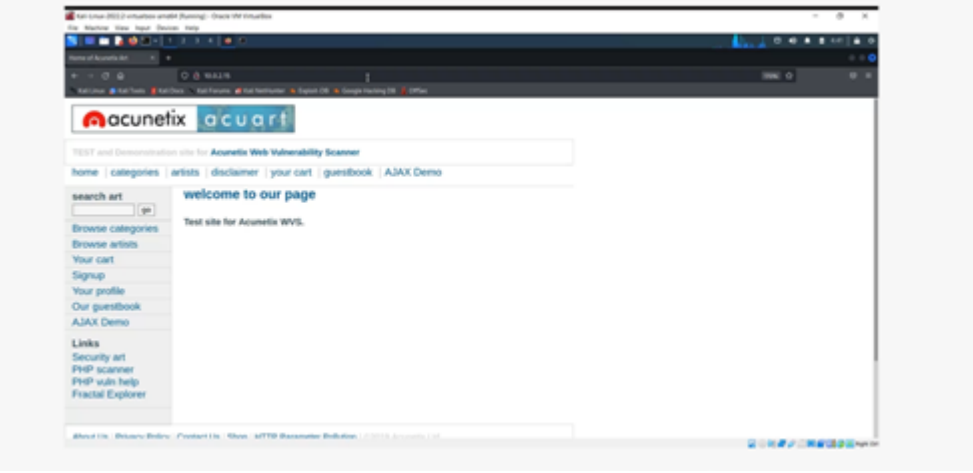

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesns't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[-] to harvest credentials or parameters from a website as well as place them into a report
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[-] to harvest credentials or parameters from a website as well as place them into a report
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://testphp.vulnweb.com



Hold 2 seconds and open the browser

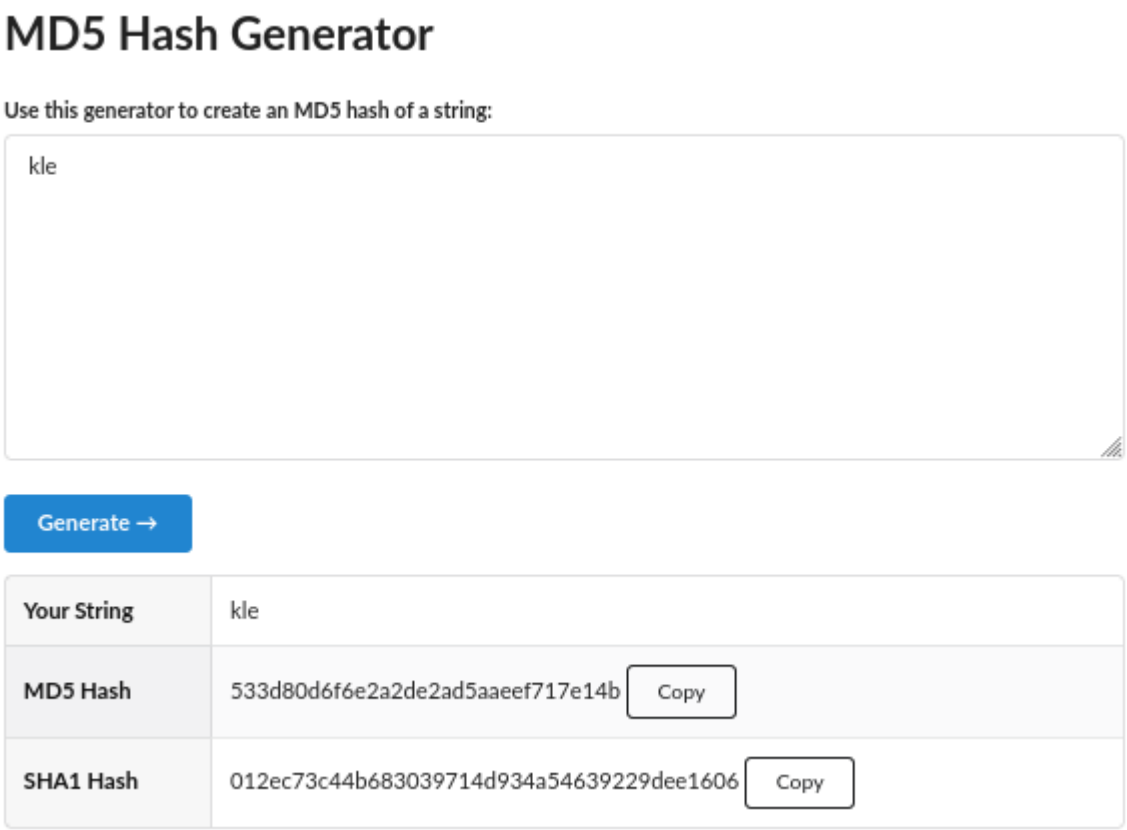


Now see site is cloned

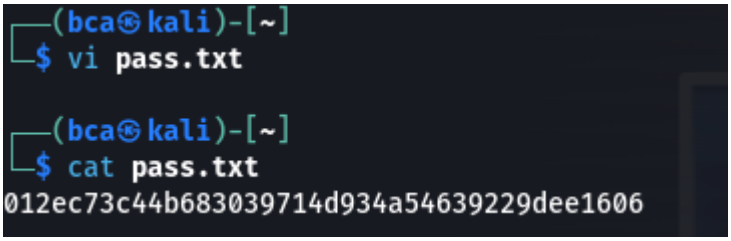
Lab 8 : Explain the password attacks tool (John The Ripper)

Steps:

1. Visit to website https://www.md5hashgenerator.com/ and generate hash value of password



2. Open terminal and Create File named pass.txt and paste the SHA1 Hash Value in pass.txt File



3. Use John the ripper tool to get original readable format password

```
┌──(bca㉿kali)-[~]
└─$ john pass.txt --format=RAW-SHA1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
kle              (?)
1g 0:00:00:05 DONE 3/3 (2024-02-13 04:13) 0.1795g/s 532263p/s 532263c/s 532263C/s kla..kle
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

Using Word List:

Steps:

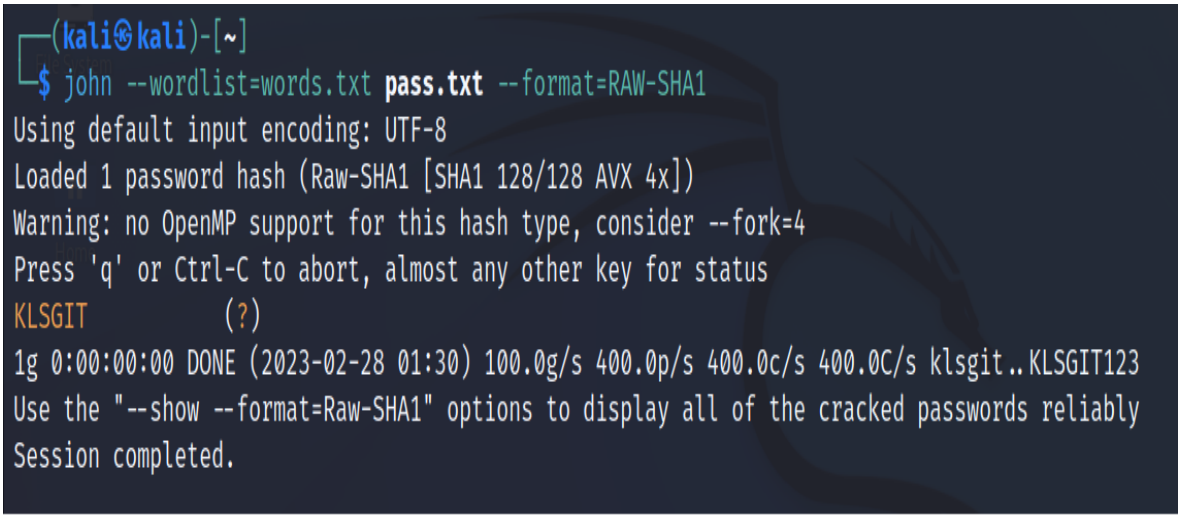
1. Create a words.txt file which contains all possible passwords

```
┌──(kali㉿kali)-[~]
└─$ vim words.txt

┌──(kali㉿kali)-[~]
└─$ cat  words.txt
klsgit
Klsgit
KLSGIT
KLSGIT123
klsgit@123
```

2. Create file named pass.txt which contain hash value of encrypted password.

```
┌──(kali㉿kali)-[~]
└─$ vim pass.txt

┌──(kali㉿kali)-[~]
└─$ cat pass.txt
b91c4dd7a2a4f57ee1eaacd21abf4110294cba28
```

3. Use following command to find the matched password from the words.txt



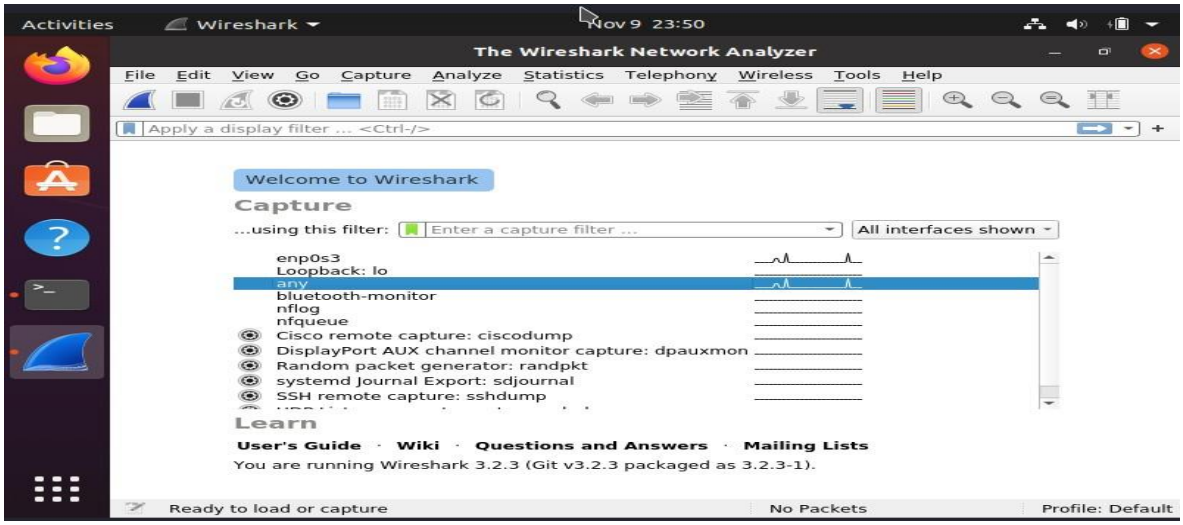
Lab 9 : Explain the sniffing and spoofing tool(Wire shark)

Using WIRESHARK observe the data transferred in client server communication using UDP and identify the UDP datagram

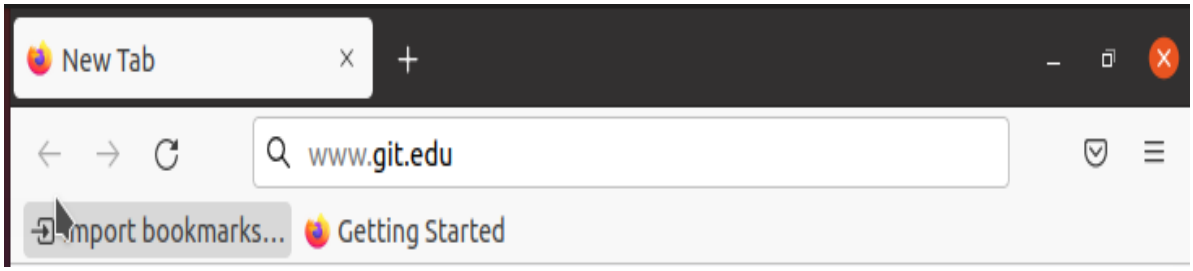
Capturing UDP Packets with browser :

Steps:

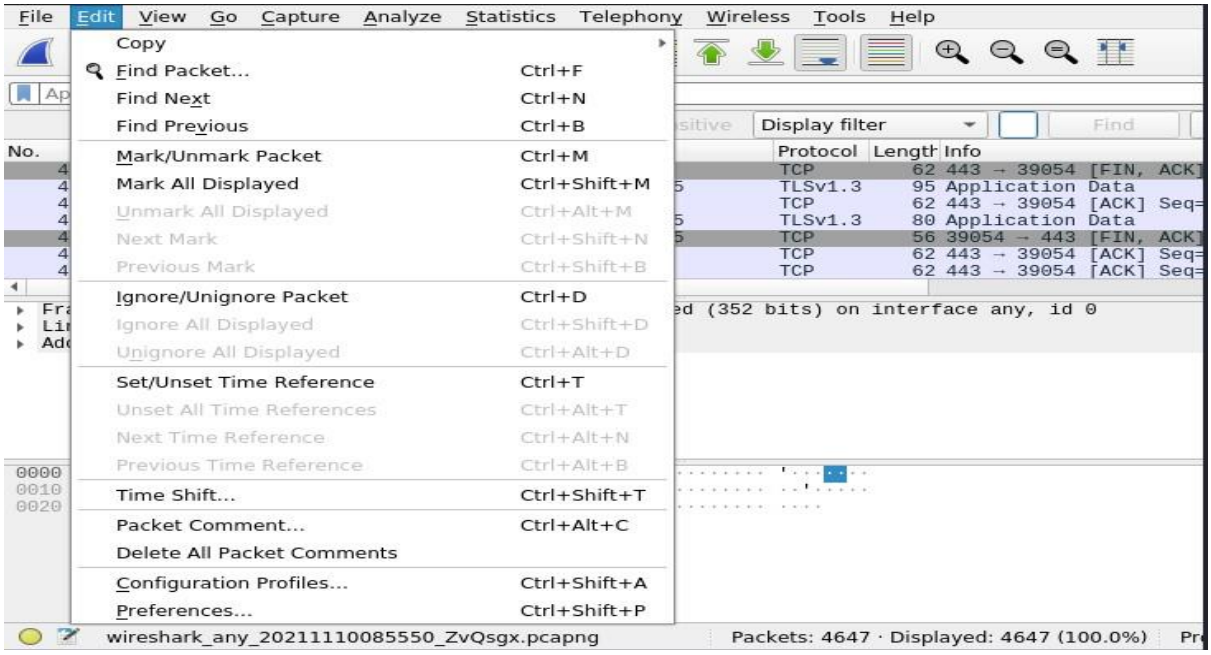
- OpenWiresharkanddouble-clickon**any-interface**tostartthepacketcaptureprocess.



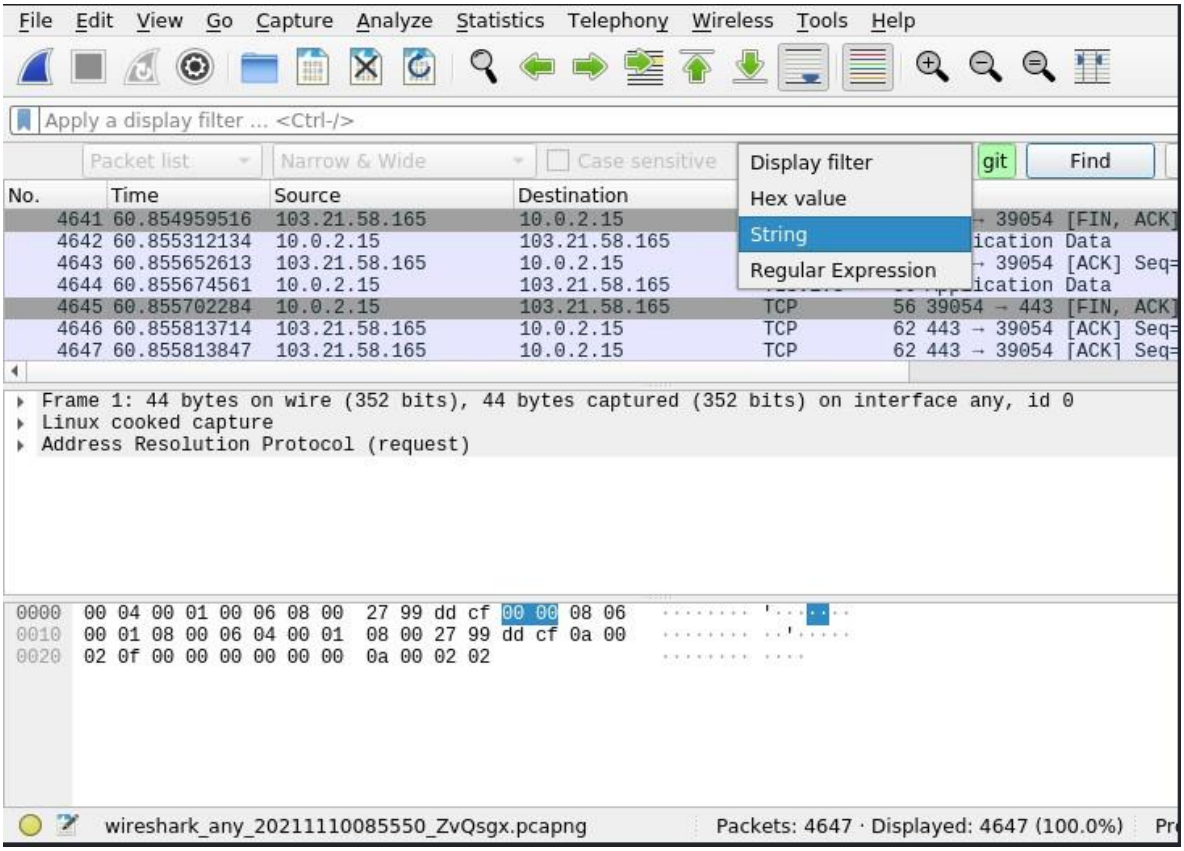
- Openthebrowserandenteranywebsite'sfullyqualifieddomainnameinthebr owseraddressbarandhitenter.



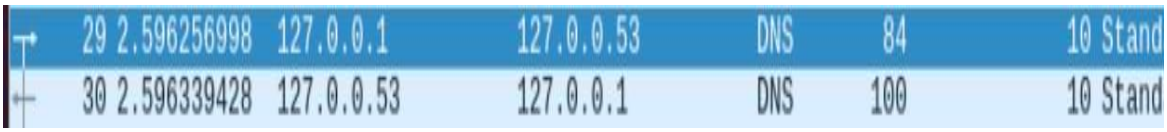
- After the site is fully loaded, stop the capturingprocess in Wireshark go to edit inthemenubarandselectfindpacketoptionorjustpressCTRL+F.



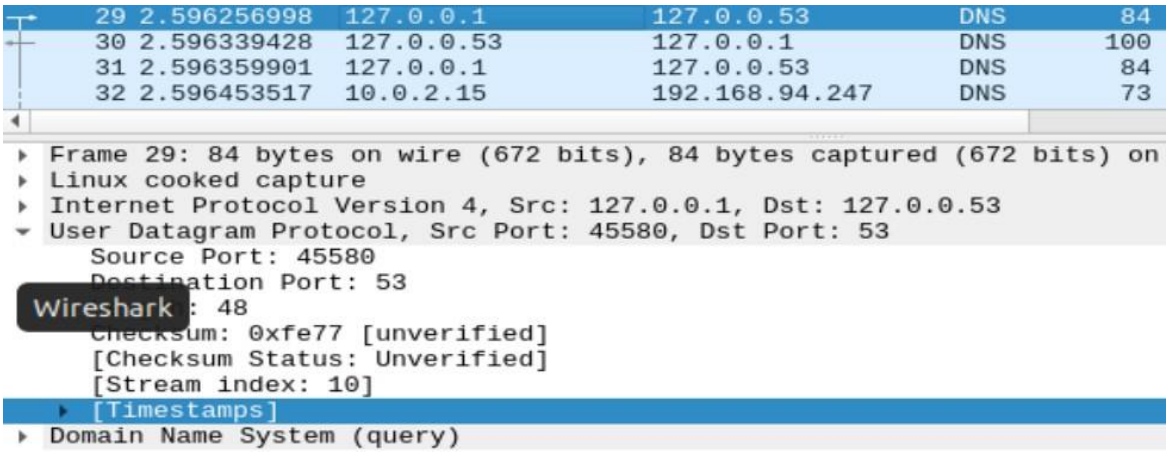
- InFindPacketmenubar,selectthe**String**optioninthe**displayfilterdrop-down** menu and enter the name of the website in the next box and click onfind.



- Thearrowindicatingtowardsthepacketisthe**requestpacket**,andthearro wcomingoutfromthepacketisthe**responsepacket**.



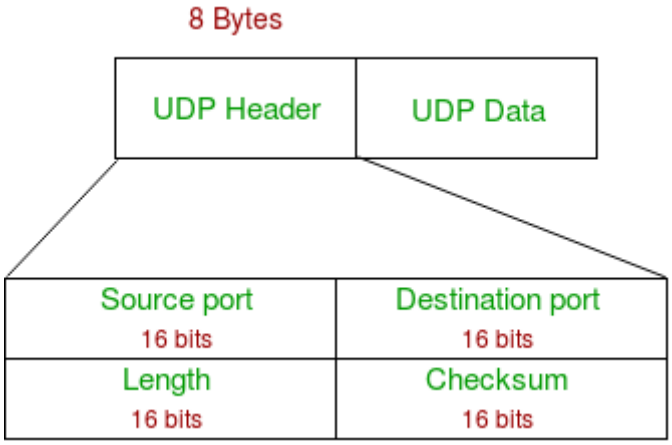
- ClickonanyrequestorresponseDNSpacketandexamineUDPpacket.



Go to statistics: Generate I/O Graph, Flow Graph and study and analyze both the graphs

UDP Header –

UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



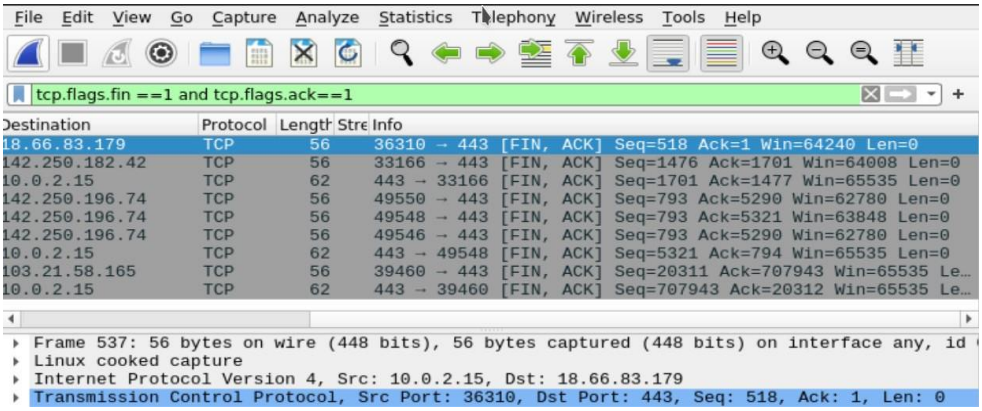
1. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
2. **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
3. **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
4. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Using WIRESHARK analyze three way handshaking connection establishment, data transfer and connection termination in client server communication using TCP.

1. CapturingTCPPacketswithbrowser:Steps:

- OpenWiresharkanddouble-clickon**any-interface**tostartthepacketcaptureprocess.
- Openthebrowserandenteranywebsite'sfullyqualifieddomainnameinthebrowseraddressbarandhitenter.
- Afterthesiteisfullyloaded,stopthecapturingprocess,inWireshark.
- Typethefollowingin,applyafiltercolumnandhit-enter:

tcp.flags.fin==1andtcp.flags.ack==1

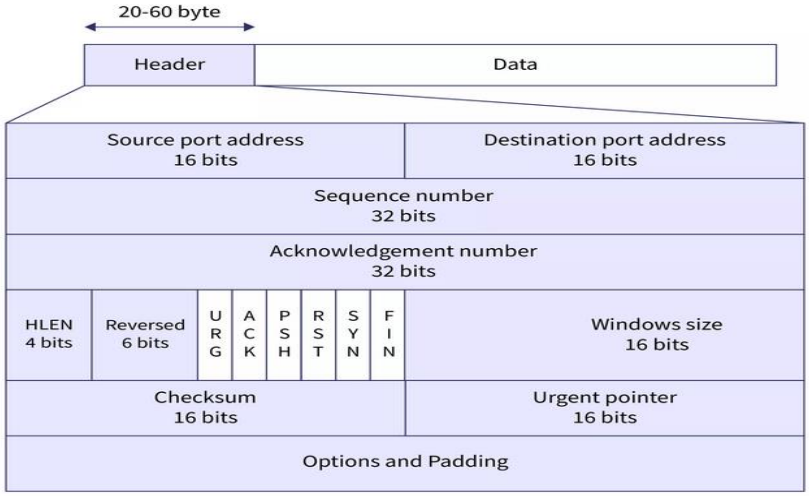


- Select any one of these listed packets, right-click and hover on conversation filterandselectTCP.
- OncedoneanalyzetheTCPPackets.

Go to statistics: Generate I/O Graph, Flow Graph and study and analyze both the graphs

- Observe TCP 3-way Handshake mechanism, data transfer and connection termination through TCP

TCP Segment Structure



The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes.

Header fields:

Source Port Address –

A 16-bit field that holds the port address of the application that is sending the data segment.

Destination Port Address –

A 16-bit field that holds the port address of the application in the host that is receiving the data segment.

Sequence Number –

A 32-bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.

Acknowledgement Number –

A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

Header Length (HLEN) –

This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

Control flags –

These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:

URG: Urgent pointer is valid

ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)

PSH: Request for push

RST: Reset the connection

SYN: Synchronize sequence numbers

FIN: Terminate the connection

Window size –

This field tells the window size of the sending TCP in bytes.

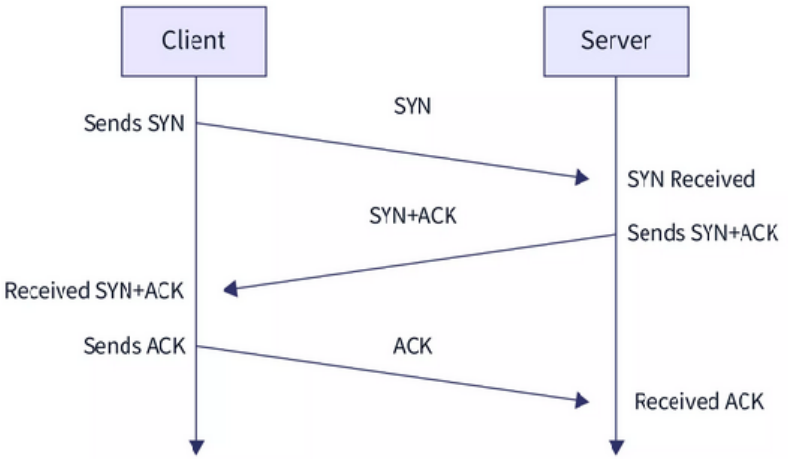
Checksum –

This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

Urgent pointer –

This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte

TCP 3-way handshake process



TCP 3-Way Handshake for Terminating the Connection