

Lab1: Explain the Basic commands of 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.

```
(rlsbca㉿kali)-[~]
$ whoami
rlsbca
```

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**"

```
(rlsbca㉿kali)-[~]
$ date
Wed Feb 7 04:48:19 EST 2024
```

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

```
(rlsbca㉿kali)-[~]
$ uname
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.

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

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 link set IFACE down
 7 ifconfig
 8 sudo apt-get install kali-linux-wireless
 9 iwconfig
10 air
11 ifconfig
12 sudo iw dev
13 lsb_release -a
14 clear
15 cat /etc/os-release
16 clear
17 hostnamectl
18 clear
19 hostnamectl
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 **visual 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.

```
[rslsbc@kali] ~]$ nano file1.txt  
[rslsbc@kali] ~]$ cat file1.txt  
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20
```

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.

```
[rslsbc@kali] ~]$ head file1.txt  
1  
2  
3  
4  
5  
6  
7  
8  
9  
10
```

```
└─(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

April

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

July

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					

August

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	7	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				

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	7	1	2	3	4	5
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 [-3bhjPwySM] [-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.

```

[~] (rlsbc@kali)
[~] $ ls
Desktop  Downloads  Pictures  Templates  file1.txt  s2.txt  sam1.txt  text2.txt
Documents  Music      Public     Videos      file5.txt  s6.txt  text1.txt
[~] (rlsbc@kali)
[~] $ cp file1.txt file2.txt

[~] (rlsbc@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.

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

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

```
(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

(rlsbca㉿kali)-[~]
$ touch file3.txt
(the quieter you become, the more you are able to hear)

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

(rlsbca㉿kali)-[~]
$ cat file3.txt
```

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 from 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
```

```
[rlsbc@kali:~]$ cat text.txt  
abc def  
ghi jkl  
mno pqr  
stu vwx yz
```

-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..

```
[rslsbc@kali:~]
$ wc text.txt
4 9 35 text.txt

[rslsbc@kali:~]
$ wc -l text.txt
4 text.txt

[rslsbc@kali:~]
$ wc -c text.txt
35 text.txt

[rslsbc@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**.

```
[rslsbc@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.

```
[rslsbc@kali:~]
$ mv text.txt text1.txt

[rslsbc@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.

```
[r00t@kali:~] $ vi number.txt
```

```
[r00t@kali:~] $ cat number.txt
```

```
5  
2  
1  
6  
75  
2  
1  
6  
7
```

```
[r00t@kali:~] $ sort number.txt
```

```
1  
1  
2  
2  
5  
6  
6  
7  
75
```

```
[r00t@kali:~] $ sort -r number.txt
```

```
75  
7  
6  
6  
5  
2  
2  
1  
1
```

```
[rslsbc@kali:~]
$ cat number.txt
a
b
d
c
p
g
k
l
e
```

```
[rslsbc@kali:~]
$ vi number.txt

[rslsbc@kali:~]
$ sort number.txt
a
b
c
d
e
g
k
l
p

[rslsbc@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.

```
L$ dnsenum facebook.com
dnsenum VERSION:1.2.6

----- facebook.com -----

Host's addresses:
-----
facebook.com.          60      IN      A      163.70.139.35

Name Servers:
-----
a.ns.facebook.com.     71765    IN      A      129.134.30.12
b.ns.facebook.com.     71765    IN      A      129.134.31.12
c.ns.facebook.com.     71765    IN      A      185.89.218.12
d.ns.facebook.com.     71765    IN      A      185.89.219.12

Mail (MX) Servers:
-----
smtpin.vvv.facebook.com. 152      IN      A      66.220.149.251

Trying Zone Transfers and getting Bind Versions:
-----
Trying Zone Transfer for facebook.com on b.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on c.ns.facebook.com ...
AXFR record query failed: corrupt packet
=====
Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out

Trying Zone Transfer for facebook.com on d.ns.facebook.com ...
AXFR record query failed: corrupt packet

Brute forcing with /usr/share/dnsenum/dns.txt:
-----
```

```
dnsenum --dnsserver 8.8.8.8 facebook.com
```

host's addresses:				
facebook.com.	299	IN	A	157.240.11.35
name 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
mail (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
```

```
kali㉿kali:~$ dnsrecon -d instagram.com -g -c instagram.csv
[*] Performing General Enumeration of Domain: instagram.com
[-] DNSSEC is not configured for instagram.com
[*] SOA ns-384.awsdns-48.com 205.251.193.128
[*] NS ns-1349.awsdns-40.org 205.251.197.69
[*] NS ns-1349.awsdns-40.org 2600:9000:5305:4500::1
[*] NS ns-2016.awsdns-60.co.uk 205.251.199.224
[*] NS ns-2016.awsdns-60.co.uk 2600:9000:5307:e000::1
[*] NS ns-384.awsdns-48.com 205.251.193.128
[*] NS ns-384.awsdns-48.com 2600:9000:5301:8000::1
[*] NS ns-868.awsdns-44.net 205.251.195.100
[*] NS ns-868.awsdns-44.net 2600:9000:5303:6400::1
[*] MX mx-a-00082601.gslb.phphosted.com 67.231.145.42
[*] MX mx-b-00082601.gslb.phphosted.com 67.231.153.30
[*] A instagram.com 3.210.157.97
[*] A instagram.com 3.234.67.196
[*] A instagram.com 3.220.83.93
[*] A instagram.com 52.73.165.14
[*] A instagram.com 35.170.122.154
[*] A instagram.com 34.192.95.2
[*] A instagram.com 52.45.64.73
```

Load balance detector

Manage traffic with all servers within cluster

```
kali㉿kali:~$ lbd bing.com 80
```



```
lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
bing.com has address 204.79.197.200
bing.com has address 13.107.21.200

Checking for HTTP-Loadbalancing [Server]:
Microsoft-IIS/10.0
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 21:12:03, 21:12:03, 21:12:03, 21:12:03, 21:12:08, 21:12:08,
:10, 21:12:10, 21:12:10, 21:12:10, 21:12:10, 21:12:10, 21:12:11, 21:12:11, 21:12:10, FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< X-MSEdge-Ref: Ref A: 38A8E1D462BA4BD0BE11E555340B3096 Ref B: LAXEDGE0810 Ref C: 2020-08-24T21:12:1
> X-MSEdge-Ref: Ref A: 67ABA226929E41089A8A3BC4ABE98ADC Ref B: LAXEDGE1012 Ref C: 2020-08-24T21:12:1
```

Lab 3: Explain the network mapper (nmap)

Nmap : Nmap (Network mapper) 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
```

```
(rlsbc@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)          Activate Windows
```

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.

```
└(rlsbc@kali)-[~]          "the quieter you become, the more you are
└$ 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 "the quieter you become, the
[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.

```
(rlsbca㉿kali)-[~]
$ nikto -h rlsbca.edu.in
- Nikto v2.5.0

-----
+ Target IP:          70.32.23.113
+ Target Hostname:    rlsbca.edu.in quieter you become, the more you a
+ Target Port:        80
+ Start Time:         2024-02-07 05:42:05 (GMT-5)

-----
+ Server: Apache
+ /: Retrieved x-powered-by header: PHP/5.6.40.
+ Root page / redirects to: http://www.rlsbca.edu.in/
^
```

To scan an SSL-enabled website

```
(rlsbca㉿kali)-[~]
$ nikto -h facebook.com -ssl
- 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:        443

-----
+ SSL Info:           Subject: /C=US/ST=California/L=Menlo Park/O=Meta Platforms, Inc./CN=*.facebook.com
                     Ciphers: TLS_CHACHA20_POLY1305_SHA256
                     Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time:         2024-02-07 05:42:54 (GMT-5)

-----
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/X-Frame-Options
+ /: Uncommon header 'x-fb-debug' found, with contents: 02V1Zx9n3bhxtH3IE0K2t0QFlZRjaPLfe6l/wDx1+UprpGCLVGMuKhv3vF2cKA3zM9p00d
p3R8Q88KcdnvuDig==.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See
: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type
-header/
+ Root page / redirects to: https://www.facebook.com/
```

Scans the specified port

```
[rslsbc@kali]~]$ nikto -h rlsbca.edu.in -port 80
- Nikto v2.5.0
-----
+ Target IP:          70.32.23.113
+ Target Hostname:    rlsbca.edu.in quieter you become, the more you a
+ 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

```
[rslsbc@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

```
[rslsbc@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



Cyber Security Essentials

This is not your typical security book. Other books of this genre exist to prepare you for certification or to teach you how to use a tool, but none.

331 pages

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

allinurl:cyber security hacker

 Simplilearn
https://www.simplilearn.com > cyber-security-tutorial

How to Become an Ethical Hacker in 2023?

7 steps · 10 mins · Materials: Computer, Software

1. You should be well-versed with LINUX - a widely used operating system for hacking.
2. Master C programming as it gives the power to utilize the Linux OS.
3. Getting well-versed in various networks and protocols is beneficial in exploiting vulnerabilities.

 Quora
https://www.quora.com > Does-being-a-cyber-security-e...

Does being a cyber security expert also make you ...

20 Mar 2018 — NO. Not in any shape or form. Some cyber security specialists are capable of being professional hackers, most are not. There is a very good reason for red team, ...

10 answers · 2 votes: I have to agree with most of what was said and it all boils down to two p...

Can a cyber security expert become a hacker? - Quora 9 answers 1 Apr 2019

How does a cyber security analyst track a hacker? - Quora 2 answers 15 Dec 2020

How good grades do you need, to be a cyber security ... 2 answers 20 May 2020

What is the difference between a cyber security ... 3 answers 24 Feb 2021

More results from www.quora.com

 E-Careers
https://www.e-careers.com > ... > Cyber Security

The route to becoming a Cyber Security Ethical Hacker

Cyber Security Training - How do you become an Ethical Hacker? · Stage 1 – Gain a fundamental knowledge of IT · Stage 2 – Entry-level Cyber Security training.

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



This is Google's cache of <https://www.stationx.net/>. It is a snapshot of the page as it appeared on May 10, 2023 14:06:38 GMT. The current page could have changed in the meantime. [Learn more](#).

[Full version](#) [Text-only version](#) [View source](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘+F** (Mac) and use the find bar.

STATIONX COURSES BLOG RESOURCES SIGN IN VIP MEMBERSHIP

Grow your skills and advance your career with

The #1 Cyber Security Training and Career Development Platform

- ✓ Top-rated online cyber security training
- ✓ Pass the top certification exams
- ✓ Customised study roadmaps
- ✓ Dedicated career mentors

BECOME A VIP MEMBER EXPLORE MORE

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

The screenshot shows a Google search results page for the query "define:reconnaissance". At the top, there's a search bar with the query, followed by a navigation bar with "All", "Images", "Books", "Shopping", "News", and "More" buttons. To the right of the navigation bar are "Tools" and a search icon. Below the search bar, it says "About 55,400,000 results (0.45 seconds)". The main content area has a title "reconnaissance" with three tabs: "Overview" (selected), "Similar and opposite words", and "Usage examples". Under the "Dictionary" section, it says "Definitions from Oxford Languages · Learn more". It shows the word "reconnaissance" as a noun, with a speaker icon indicating pronunciation. The definition is: "military observation of a region to locate an enemy or ascertain strategic features. "an excellent aircraft for low-level reconnaissance". Below the definition are "Similar" terms: "preliminary survey", "survey", "exploration", "observation", and "investigation". There are also bullet points for "preliminary surveying or research." and "conducting client reconnaissance". At the bottom of the dictionary section are "Feedback" and "More definitions" buttons.

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

The screenshot shows a Google search results page for the query "ext:php site:microsoft.com". At the top, there's a search bar with the query, followed by a navigation bar with "All", "Books", "Images", "Shopping", "News", and "More" buttons. To the right of the navigation bar are "Tools" and a search icon. Below the search bar, it says "About 5 results (0.33 seconds)". The main content area shows two search results. The first result is for "Hugh MacLeod connects the dots", which is a cartoonist's illustrated journey to the heart and soul of Microsoft. The second result is for "Audio Lab | Microsoft: Inside B87", which is about Step inside the world's quietest place, in Microsoft's Building 87. Get ready to experience a world few have seen.

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



filetype:pdf site:apple.com

All Books Images Shopping News More Tools

About 13,900 results (0.27 seconds)

Apple
http://www.apple.com › certificateauthority › A... PDF ::

Application Integration CPS
Apple Application Integration. Version 7.0. Effective Date: January 18, 2023. Page 2.. 2. Table of Contents. 1. Introduction .

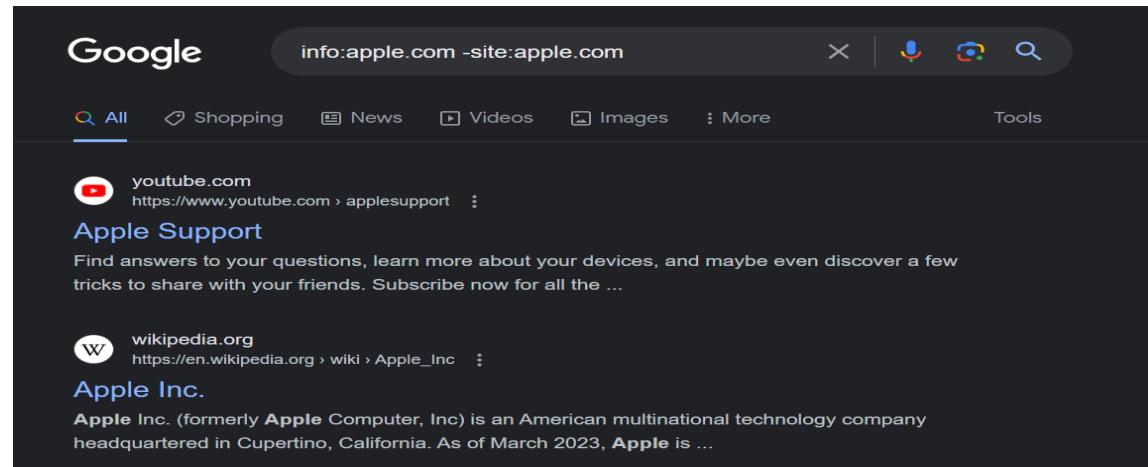
apple.com
http://investor.apple.com › esg › 2021_Apple_... PDF ::

Environmental Social Governance Report
Living up to that commitment means staying true to the values that have defined Apple from the beginning. It means innovating to protect people's privacy, ...

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



Google info:apple.com -site:apple.com

All Shopping News Videos Images More Tools

youtube.com
https://www.youtube.com › applesupport ::

Apple Support
Find answers to your questions, learn more about your devices, and maybe even discover a few tricks to share with your friends. Subscribe now for all the ...

wikipedia.org
https://en.wikipedia.org › wiki › Apple_Inc ::

Apple Inc.
Apple Inc. (formerly **Apple Computer, Inc.**) is an American multinational technology company headquartered in Cupertino, California. As of March 2023, **Apple** is ...

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

intext:munira tom site:goodreads.com

X | 🔍 | 📄 | ⚡ | 🔍

g goodreads.com

https://www.goodreads.com › book › show › 427790... ::

The Gomorrah Gambit by Tom Chatfield

1 Jan 2019 — Tipped off by a secretive young woman named **Munira**, Azi sets out to unravel the mysterious online marketplace known as Gomorrah, ...

★★★★★ Rating: 3.4 · 360 votes

g goodreads.com

https://www.goodreads.com › show › 64387739-munira ::

Munira (596 books)

They were careless people, **Tom** and **Daisy**—they smashed up things and creatures and then retreated back into their money or their vast carelessness, or whatever ...

g goodreads.com

https://www.goodreads.com › 59824764-it-was-me ::

It Was Me (Last Words Series #6) by W.L. Knightly

6 Jan 2022 — After saving his sister, **Thomas** is ready to get his life back on track with Sarah, as their... ... Profile Image for **Munira Vahed**.

★★★★★ Rating: 4.4 · 51 votes

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

Google

intitle:google site:github.com

X | 🔍 | 📄 | ⚡ | 🔍

Q All

Videos

Shopping

Books

News

: More

Tools



github.com

https://github.com › google ::

Google

LevelDB is a fast key-value storage library written at Google that provides an ordered mapping from string keys to string values. C++ 34.3k 7.6k.



github.com

https://github.com › orgs › google › repositories ::

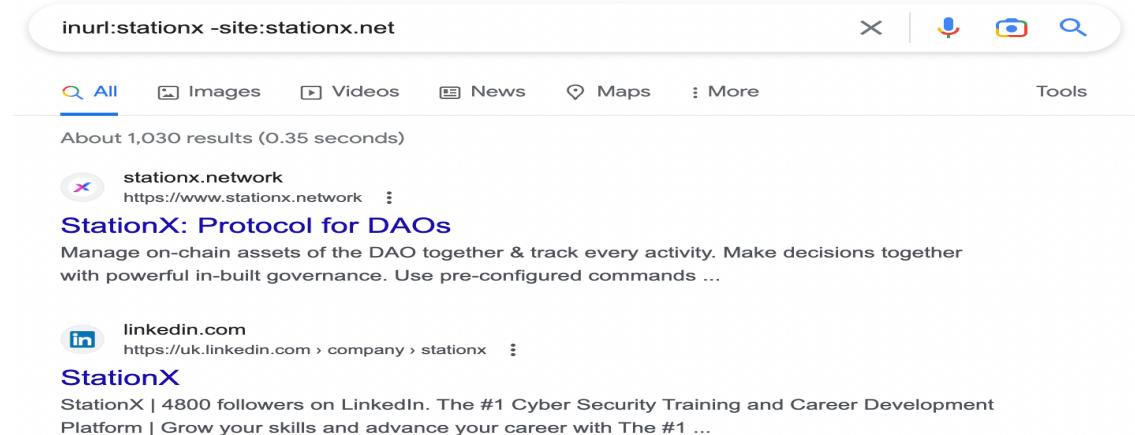
Repositories - Google

⚡ A collection of projects focused on connectivity that enable building cross-device experiences.

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



A screenshot of a Google search results page. The search bar at the top contains the query "inurl:stationx -site:stationx.net". Below the search bar, there are several search filters: All (selected), Images, Videos, News, Maps, More, and Tools. The main content area shows search results for "stationx.network" and "StationX".

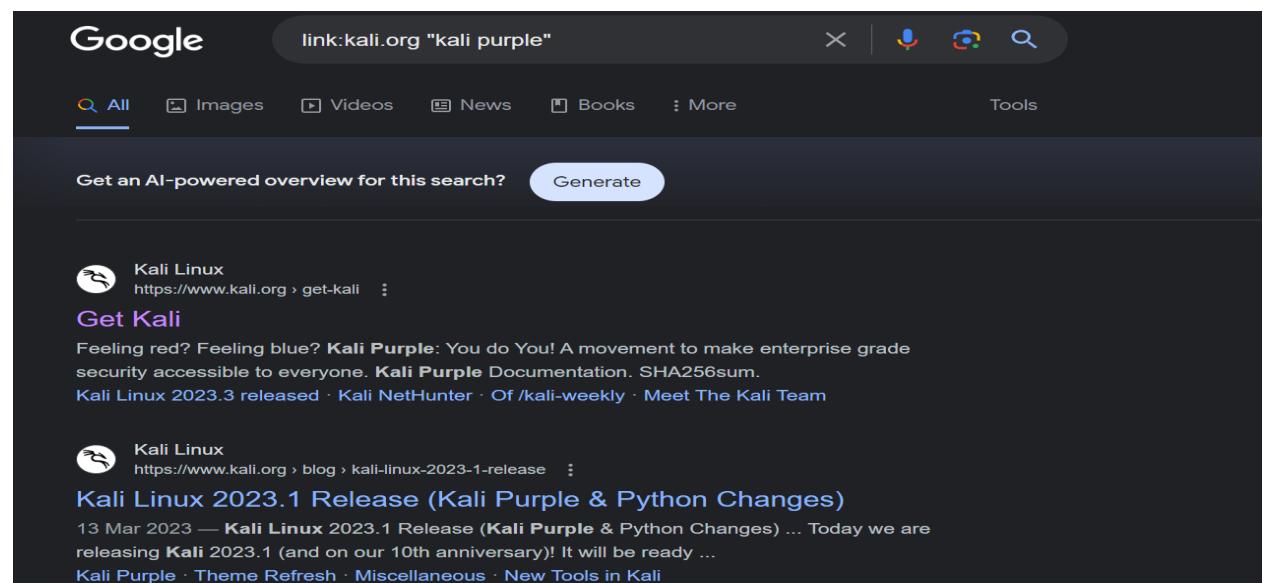
stationx.network
https://www.stationx.network ...
StationX: Protocol for DAOs
Manage on-chain assets of the DAO together & track every activity. Make decisions together with powerful in-built governance. Use pre-configured commands ...

linkedin.com
https://uk.linkedin.com › company › stationx ...
StationX
StationX | 4800 followers on LinkedIn. The #1 Cyber Security Training and Career Development Platform | Grow your skills and advance your career with The #1 ...

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"



A screenshot of a Google search results page. The search bar at the top contains the query "link:kali.org \"kali purple\"". Below the search bar, there are several search filters: All (selected), Images, Videos, News, Books, More, and Tools. A button for "Get an AI-powered overview for this search?" is present, along with a "Generate" button.

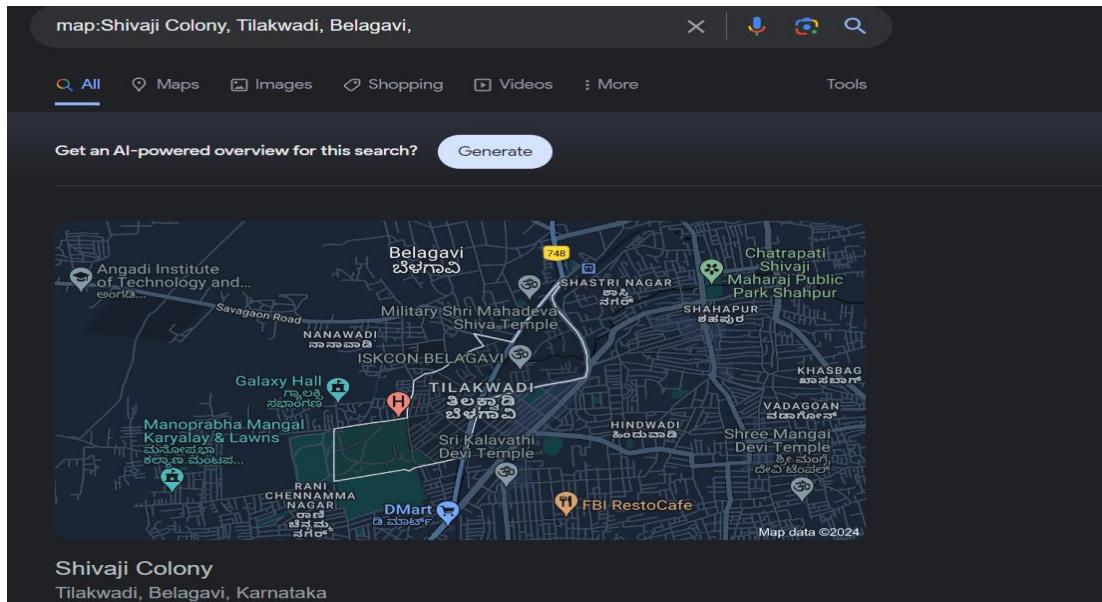
Kali Linux
https://www.kali.org › get-kali ...
Get Kali
Feeling red? Feeling blue? **Kali Purple**: You do You! A movement to make enterprise grade security accessible to everyone. **Kali Purple** Documentation. SHA256sum.
Kali Linux 2023.3 released · Kali NetHunter · Of /kali-weekly · Meet The Kali Team

Kali Linux
https://www.kali.org › blog › kali-linux-2023-1-release ...
Kali Linux 2023.1 Release (Kali Purple & Python Changes)
13 Mar 2023 — **Kali Linux** 2023.1 Release (**Kali Purple** & Python Changes) ... Today we are releasing **Kali** 2023.1 (and on our 10th anniversary)! It will be ready ...
Kali Purple · Theme Refresh · Miscellaneous · New Tools in Kali

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

phonebook:555-555-5555

About 777,000 results (0.49 seconds)

YellowPages.ca
https://www.yellowpages.ca › ... › 555 › 555

555-555-5555 | 1555555555 Who called
Get more information on the 555-555-5555 number, origin, and statistics. General information.
Country: US; Area code: 555; Prefix ...

Youmail
https://directory.youmail.com › phone

(555) 555-5555 is a Weather Warning
This is an emergency message from Columbia Richland citizens alert. A heat advisory has been issued for the area associated with your Columbian return alerts ...

People also ask

Is 555 555 5555 a real phone number?

What happens if you call 555 555 5555?

Can real phone numbers have 555?

Where is a 555 number from?

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

The screenshot shows a search results page for "site:github.com nmap". The results are as follows:

- Nmap - the Network Mapper. Github mirror of official SVN ...**
Use saved searches to filter your results more quickly ... [Nmap - the Network Mapper. Github mirror of official SVN repository. svn.](https://github.com/nmap/nmap)
- Ethical-Hacking-Labs/2-Scanning-Networks/4-Nmap.md ...**
The [Nmap](https://github.com/Samsar4/blob/master/4-Nmap) scans the entire network and displays information for all the hosts, along with open ports, device type, details of OS, and so on.

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 Listener

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

```
File Actions Edit View Help
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 
```

Select option 1)Social Engineering Attacks

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

```
set> 2
```

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

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

99) Return to Main Menu
```

```
set:webattack>3
```

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`

```
File System  
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 -
```

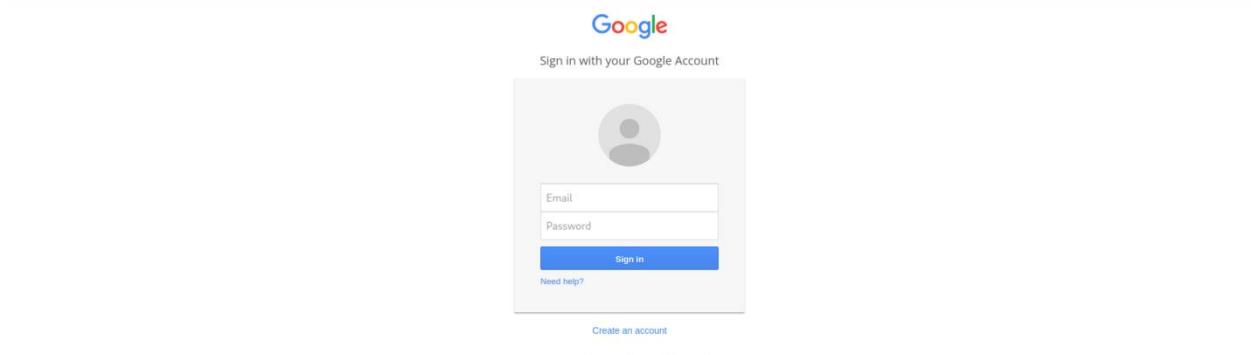
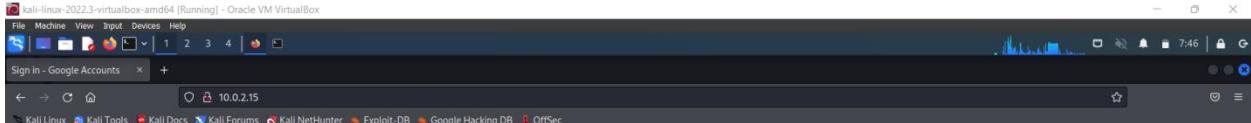


Image 1: cloned Google Sign In page

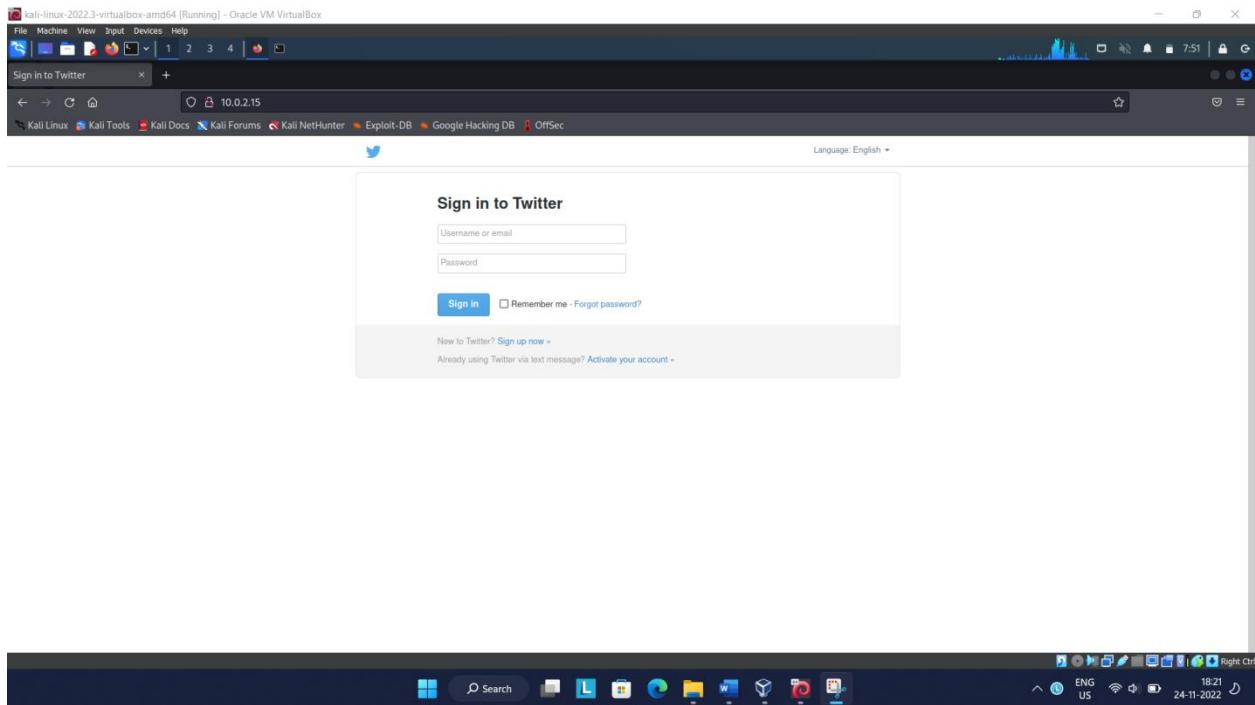


Image 2: Cloned Twitter Sign In page

Java Required!

Welcome to the website, you must have Java in order to view this page properly. Ensure that the Microsoft signed Java box that pops up is accepted to load the site content.

Words from our CEO "Java Required to view content."

Instructions to view the website:

1. A pop-up box will prompt, please hit "Yes". This may take a few moments.
2. This pop-up is signed through the Microsoft Corporation and will provide you with necessary updates to view the site.
3. Once you have accepted, wait about 10 to 15 seconds and the page will load. You must first click "Run" for the signed Java component from Microsoft in order to view our site successfully.

You must first click "Run" for the signed Java component from Microsoft in order to view our site successfully. Java is a well trusted and industry used component for websites.

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  
I  
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 doesn'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 perspective, 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
Shell No.1
[-] 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 doesn'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 perspective, 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
Shell No.1
[-] 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 doesn'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 perspective, 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
```

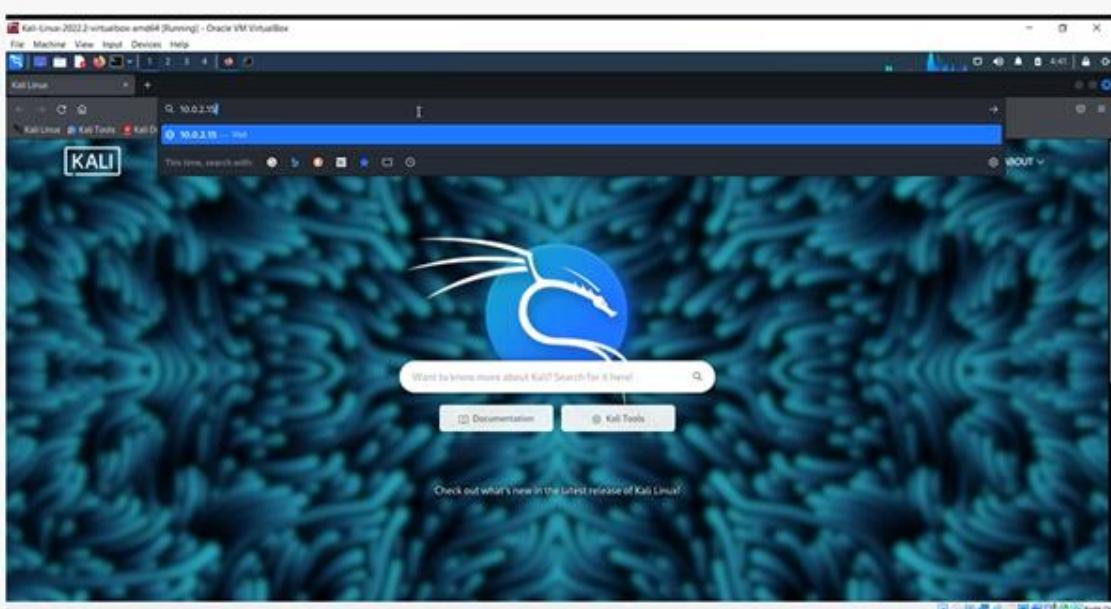
```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Shell No.1
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking 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 doesn'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 perspective, 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

[*] Cloning the website: http://testphp.vulnweb.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 capture's 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:
I
```

Hold 2 seconds and open the browser



A screenshot of a web browser window showing a test site for Acunetix WVS. The page title is "Acunetix acuart". The main content area says "welcome to our page" and "Test site for Acunetix WVS.". On the left, there is a sidebar with links like "search art", "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", "Links", "Security art", "PHP scanner", "PHP vuln help", and "Fractal Explorer". At the bottom, there is a footer with links for "About Us", "Buyers Online", "Product Line", "Blog", "sHTTP Parameter Pollution", "© 2013 Acunetix Ltd.", and "Right Off".

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

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

kle

Generate →

Your String	kle
MD5 Hash	533d80d6f6e2a2de2ad5aaeef717e14b Copy
SHA1 Hash	012ec73c44b683039714d934a54639229dee1606 Copy

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

```
(bca㉿kali)-[~]
$ vi pass.txt

(bca㉿kali)-[~]
$ cat pass.txt
012ec73c44b683039714d934a54639229dee1606
```

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

```
(kali㉿kali)-[~]
$ john --wordlist=words.txt pass.txt --format=RAW-SHA1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
KLSGIT          (?)
1g 0:00:00:00 DONE (2023-02-28 01:30) 100.0g/s 400.0p/s 400.0c/s 400.0C/s klsgit..KLSGIT123
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

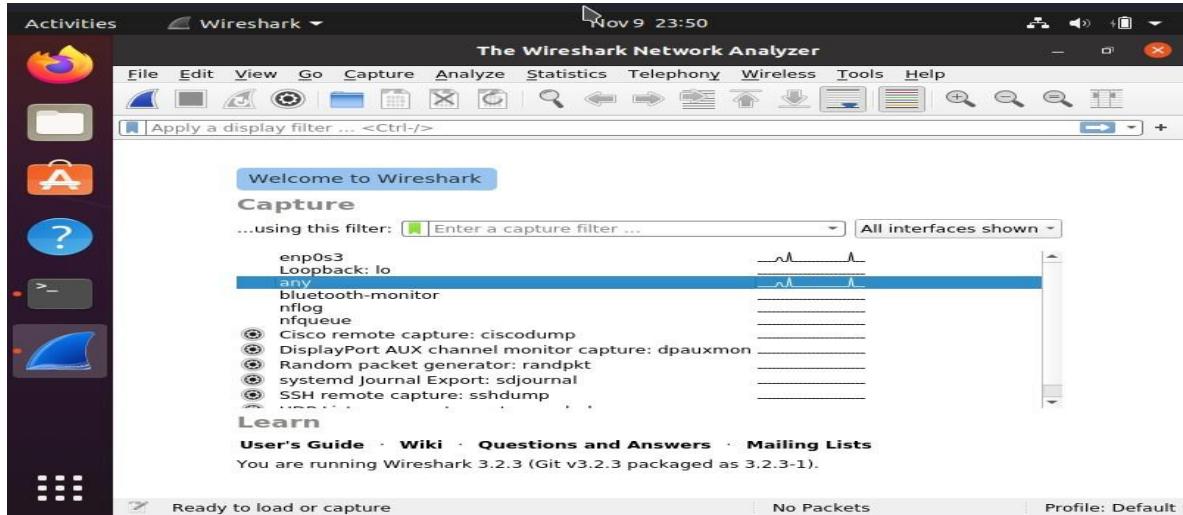
Lab 9 : Explain the sniffing and spoofing tool(Wire shark)

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

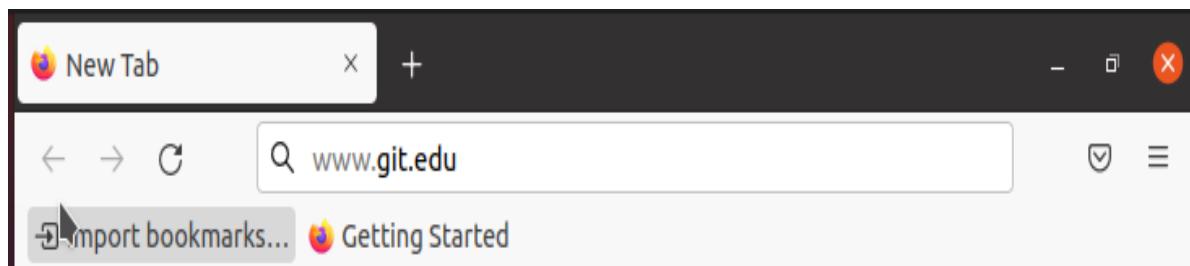
Capturing UDP Packets with browser :

Steps:

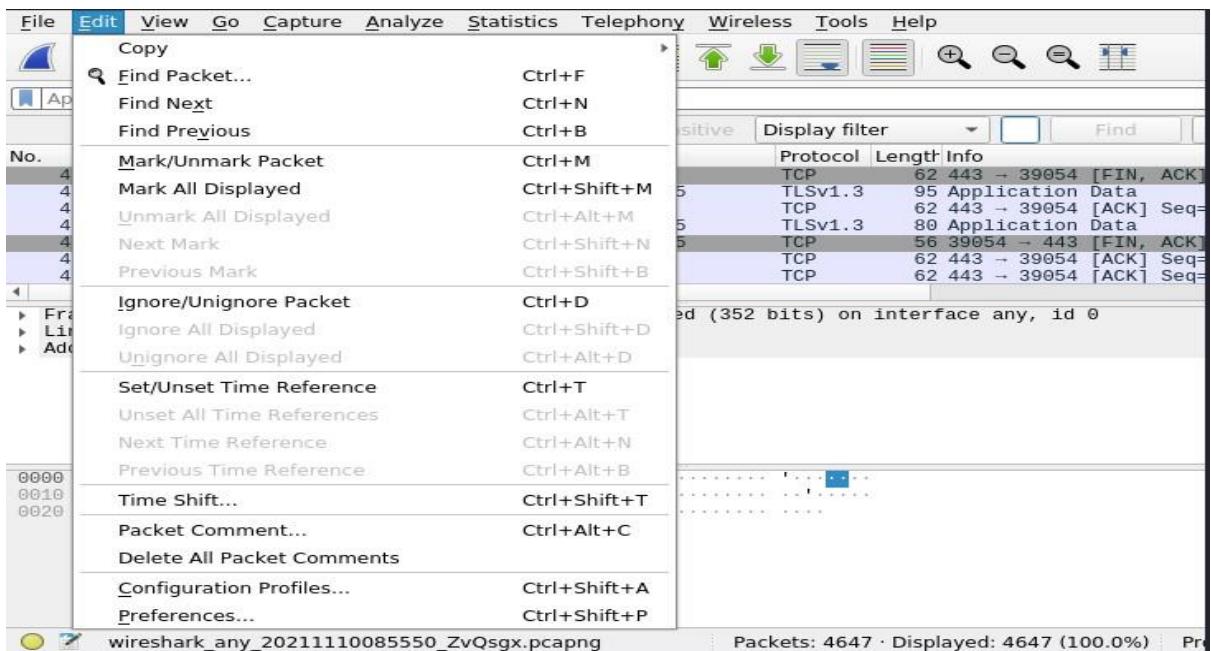
- Open Wireshark and double-click on any-interface to start the packet capture process.



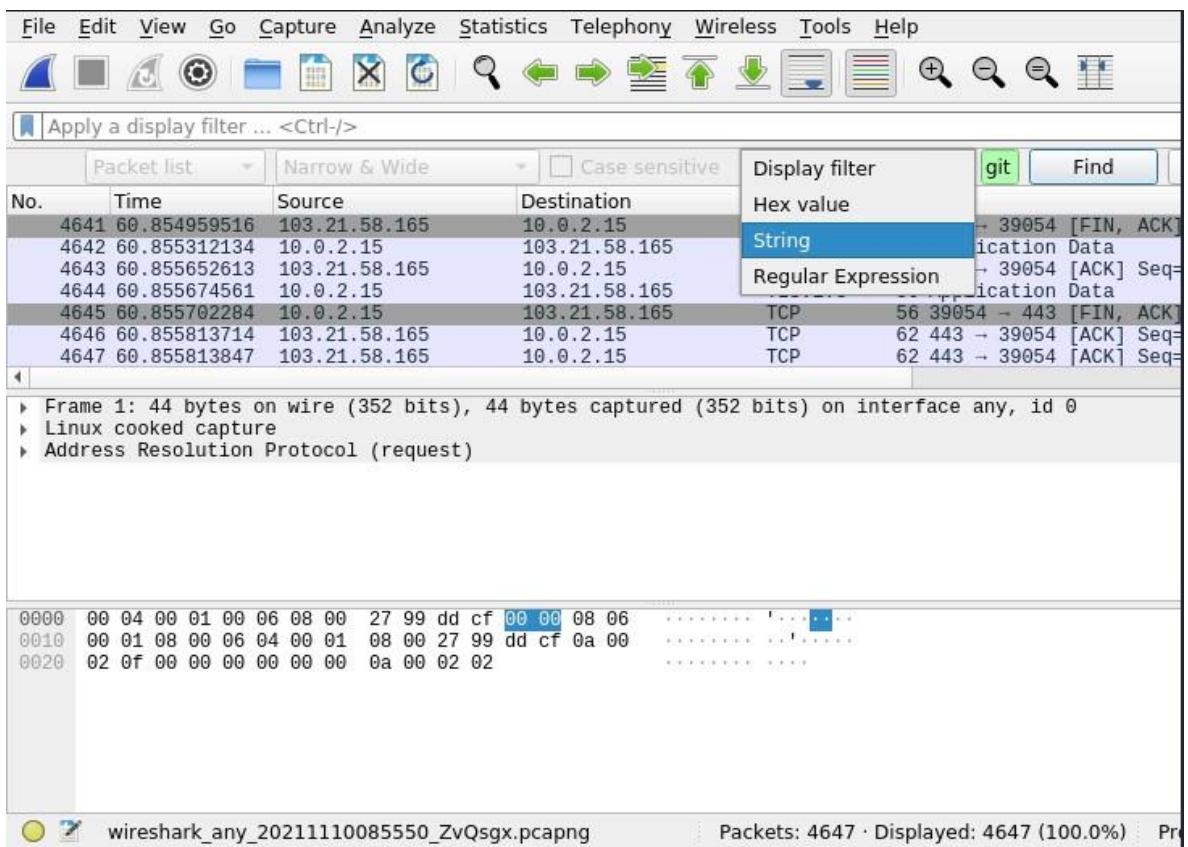
- Open the browser and enter any website's fully qualified domain name in the browser address bar and hit enter.



- After the site is fully loaded, stop the capturing process in Wireshark go to edit in the menu bar and select find packet option or just press CTRL+F.



- In FindPacket menubar, select the String option in the display filter drop-down menu and enter the name of the website in the next box and click on find.



- The arrow indicating towards the packet is the **request packet**, and the arrow coming out from the packet is the **response packet**.

↑ 29 2.596256998 127.0.0.1	127.0.0.53	DNS	84	10 Stand
↓ 30 2.596339428 127.0.0.53	127.0.0.1	DNS	100	10 Stand

- Click on any request or response DNS packet and examine UDP packet.

↑ 29 2.596256998 127.0.0.1	127.0.0.53	DNS	84
↓ 30 2.596339428 127.0.0.53	127.0.0.1	DNS	100
31 2.596359901 127.0.0.1	127.0.0.53	DNS	84
32 2.596453517 10.0.2.15	192.168.94.247	DNS	73

```

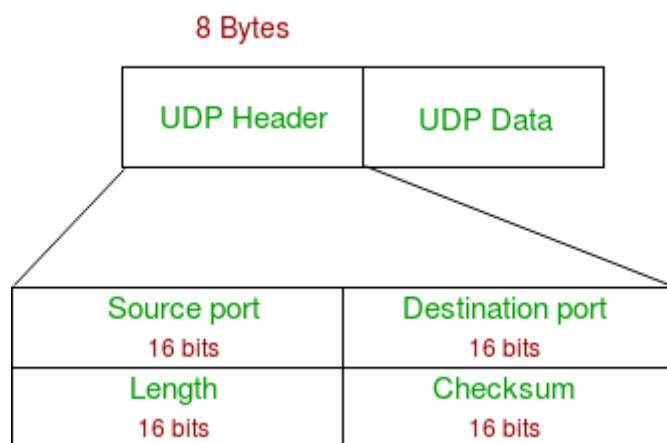
▶ Frame 29: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▼ User Datagram Protocol, Src Port: 45580, Dst Port: 53
  Source Port: 45580
  Destination Port: 53
  Wireshark : 48
    Checksum: 0xfe77 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
      ▶ [Timestamps]
  ▶ Domain Name System (query)

```

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.



- Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
- Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
- 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. CapturingTCP Packets with browser: Steps:

- Open Wireshark and double-click on any interface to start the packet capture process.
- Open the browser and enter any website's fully qualified domain name in the browser address bar and hit enter.
- After the site is fully loaded, stop the capturing process in Wireshark.
- Type the following in, apply a filter column and hit enter:

tcp.flags.fin==1 and tcp.flags.ack==1

Destination	Protocol	Length	Str	Info
18.66.83.179	TCP	56	36310 → 443	[FIN, ACK] Seq=518 Ack=1 Win=64240 Len=0
142.250.182.42	TCP	56	33166 → 443	[FIN, ACK] Seq=1476 Ack=1701 Win=64008 Len=0
10.0.2.15	TCP	62	443 → 33166	[FIN, ACK] Seq=1701 Ack=1477 Win=65535 Len=0
142.250.196.74	TCP	56	49550 → 443	[FIN, ACK] Seq=793 Ack=5290 Win=62780 Len=0
142.250.196.74	TCP	56	49548 → 443	[FIN, ACK] Seq=793 Ack=5321 Win=63848 Len=0
142.250.196.74	TCP	56	49546 → 443	[FIN, ACK] Seq=793 Ack=5290 Win=62780 Len=0
10.0.2.15	TCP	62	443 → 49548	[FIN, ACK] Seq=5321 Ack=794 Win=65535 Len=0
103.21.58.165	TCP	56	39460 → 443	[FIN, ACK] Seq=20311 Ack=707943 Win=65535 Len=0
10.0.2.15	TCP	62	443 → 39460	[FIN, ACK] Seq=707943 Ack=20312 Win=65535 Len=0

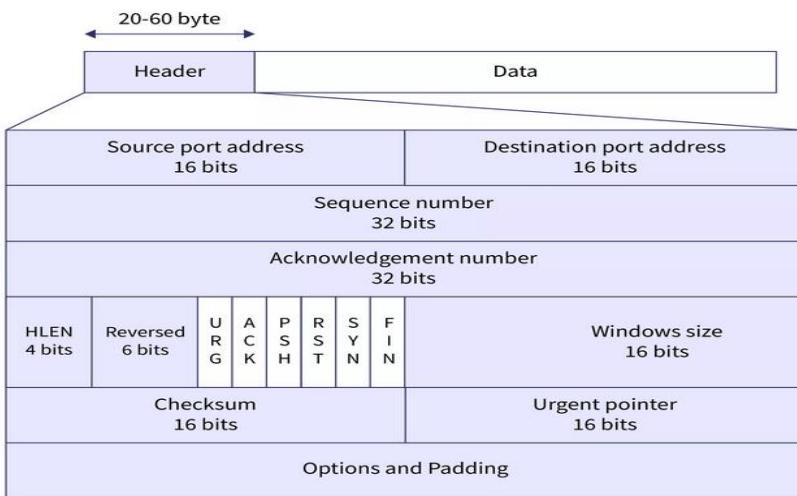
Frame 537: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0x0000000000000000, duration 0.000000000s, time 0.000000000s, source 10.0.2.15, destination 18.66.83.179
 Linux cooked capture
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 18.66.83.179
 Transmission Control Protocol, Src Port: 36310, Dst Port: 443, Seq: 518, Ack: 1, Len: 0

- Select any one of these listed packets, right-click and hover on conversation filter and select TCP.
- Once done analyze the TCP Packets.

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 $5 \times 4 = 20$) and the maximum length: 60 bytes, then it'll hold the value 15(because $15 \times 4 = 60$). 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.

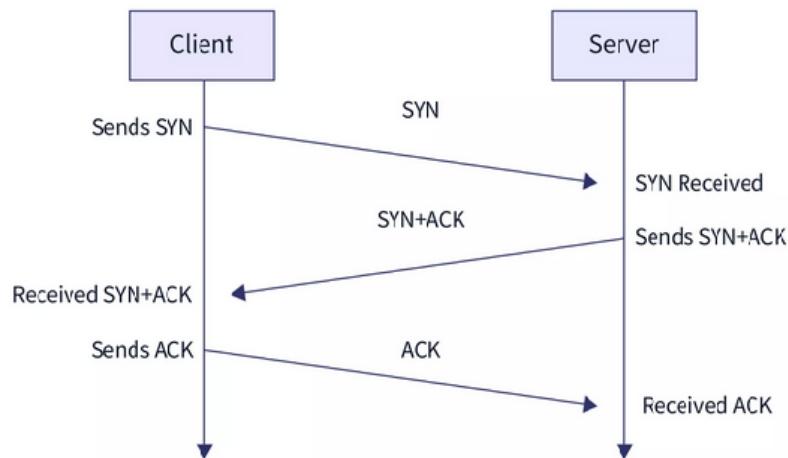
Checksum –

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

