EASWARI ENGINEERING COLLEGE

(Autonomous)
Bharathi Salai, Ramapuram, Chennai 600 089.

Department : .....

Laboratory : .....

Name :

Roll No. :

Semester :

Branch :

Subject :

EASWARI ENGINEERING COLLEGE

(Autonomous)
Bharathi Salai, Ramapuram, Chennai 600 089.

Department : .....

PRACTICAL EXAMINATIONS ..... (Month / Year)

BONAFIDE CERTIFICATE

This is to certify that this practical work titled .....
(code)

.....
(Name of the Laboratory)

is the bonafide work of Mr./Miss.....
(Name of the Student)

with Register Number..... in

Semester..... of..... Year in the Department of

.....during the

academic year 20..... –20 .....

Faculty Incharge **Head of the Department**

Submitted for Practical Examination held on ...../...../..... at Easwari

Engineering College, Ramapuram, Chennai – 89.

Internal Examiner **External Examiner**

INDEX

E.NO	EXPERIMENT NAME	Pg.No	Marks	Signature
1	Installation of Kali or Backtrack Linux/Metasploitable/Windows XP			
2	Bash Scripting			
3	Aggregating information from public databases using Maltego			
4	Understand the Nmap commands and scan the target using Nmap			
5	Install metasploitable on the virtualbox to exploit an unpatched vulnerability			
6	Use Metasploit to exploit an unpatched vulnerability			
7	Install Linux server on the virtual box and install ssh			
8	Use Fail2banto scan log files and ban Ips			
9	Launch brute-force attacks using Hydra			
10	View and capture network traffic using Wire shark			

EX 1 Install kali or backtrack Linux/Metasploitable/Windows XP

AIM:

To install kali or backtrack Linux/Metasploitable/Windows XP.

PROCEDURE:

How to Create a New Virtual Machine?

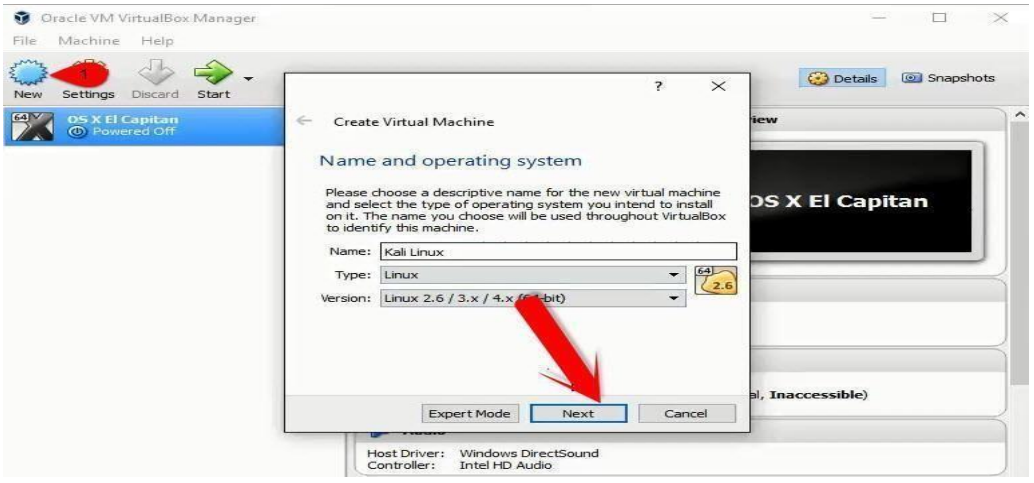
We have explained in details to create a new virtual machine on VirtualBox. In today's article, I will do it once again that you should understand it easily. First, youmust download the following requirements.

Download Kali Linux

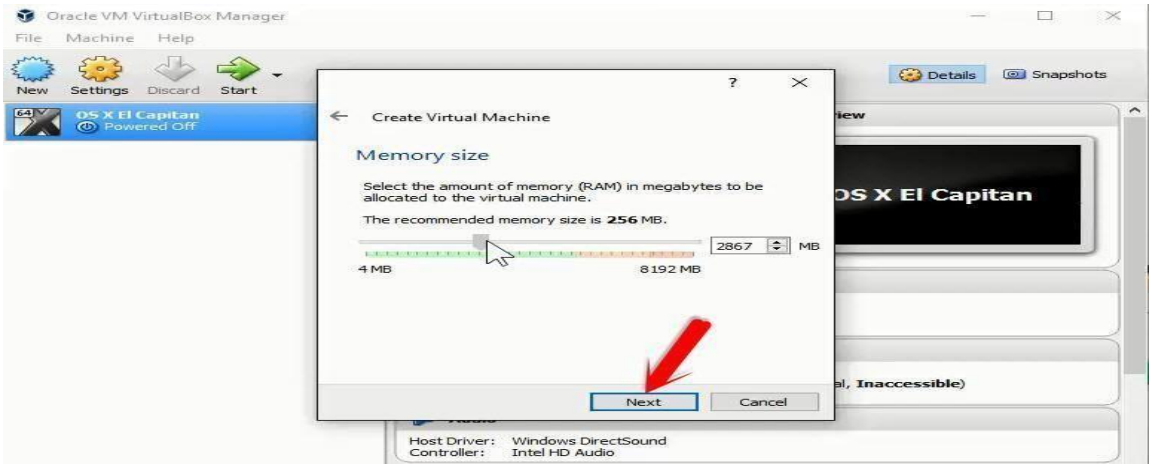
Download VirtualBox

Step 1. Once the downloading is completed, install the VirtualBox on your WindowsPC. The installation is straightforward and simple. Double-click on the setup then hit continue until it gets finished. Now, open up the VirtualBox then click on the "**New**" atthe upper left-hand side of the window.

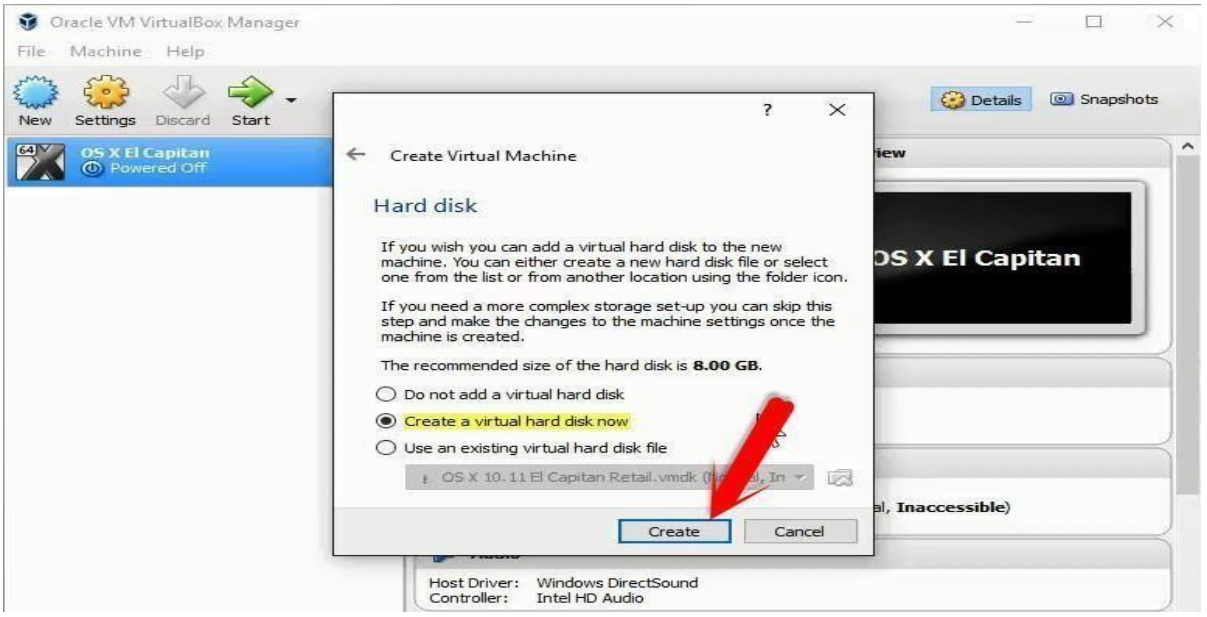
A new window will pop up, choose a proper name for Kali Linux. Next, you have to select the type of operating system. When you type the Kali Linux, it'll automaticallyset up all the necessary options. If it does not set up, so you have to do it manually.Click "**Next**" button.



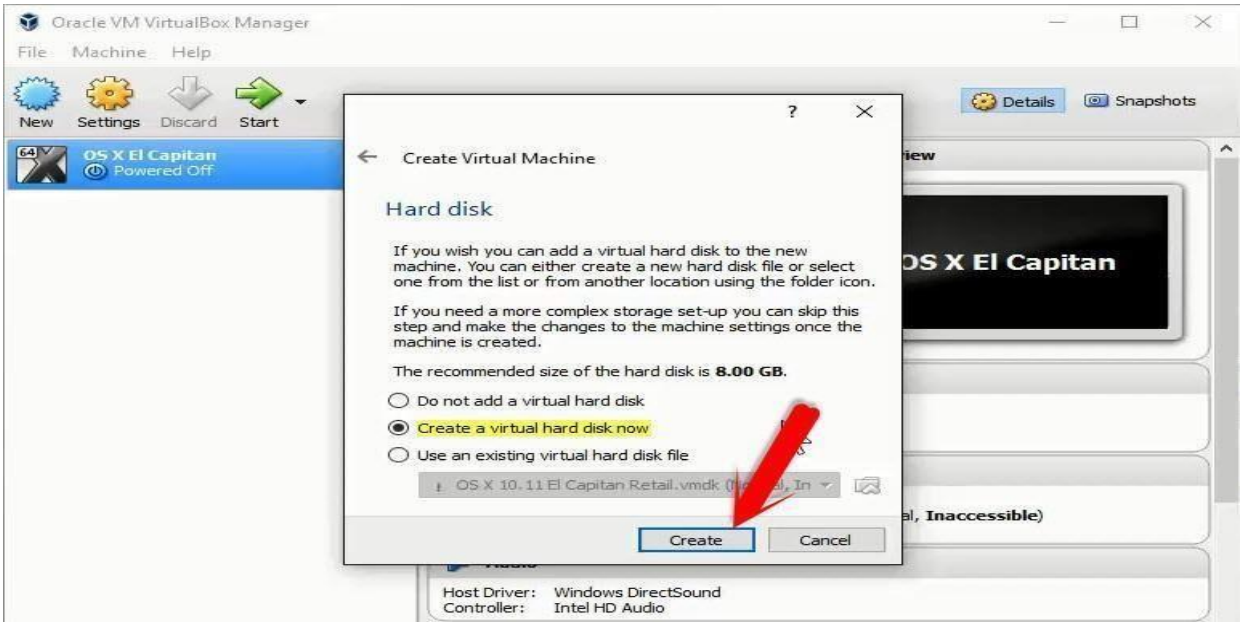
Step 2. Choose at least 2 GB of memory size then hit the "**Next**" button.



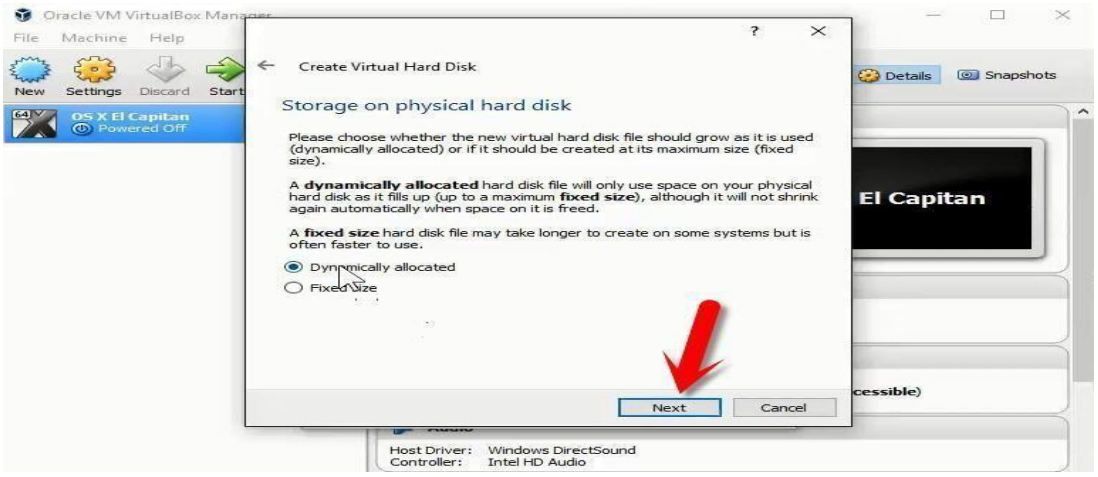
Step 3. Create a new virtual hard disk. Select the second option "**Create a newvirtual hard disk now**". Hit the " **Create**" button.



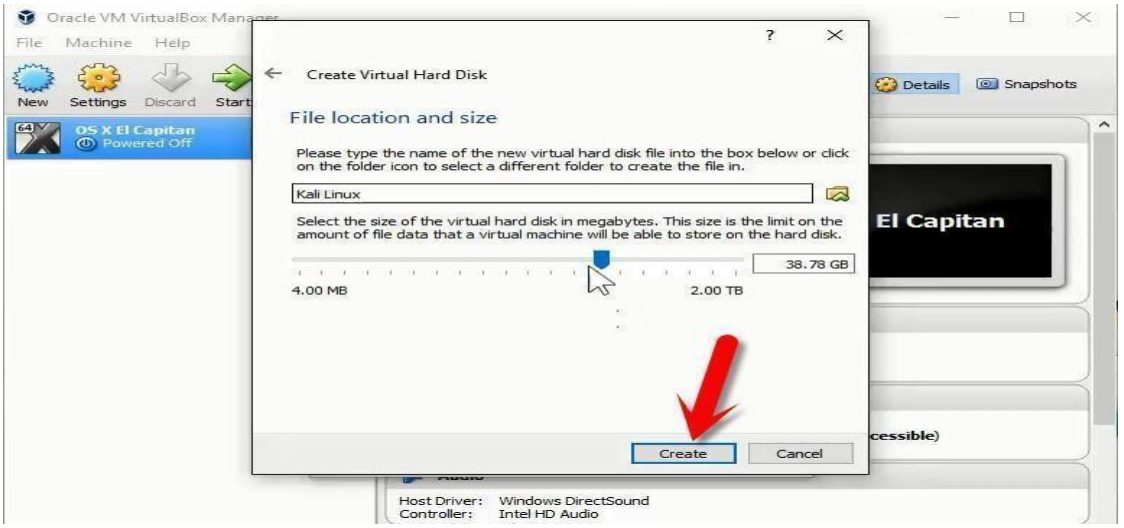
Step 4. A new window will be shown to you and choose the first option "**VirtualBoxDisk Image**" then tap on the "**Next**" button.



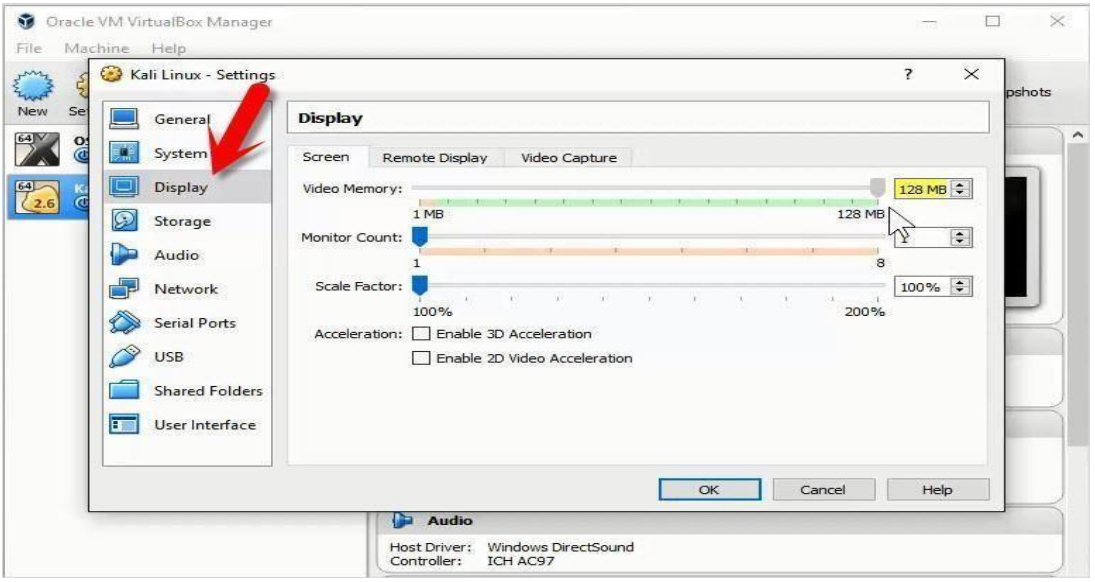
Step 5. Here, you have two options "**Dynamic and Fixed Size**". A dynamic allocated hard disk file will only use space on your physical hard disk as it fills up it'lltake space from the main hard drive. If you choose the "**Fixed Size**", it'll cut some space from the physical hard drive when the size is filled. You can't get space from the physical hard disk. I recommend you to choose the dynamic hard disk.



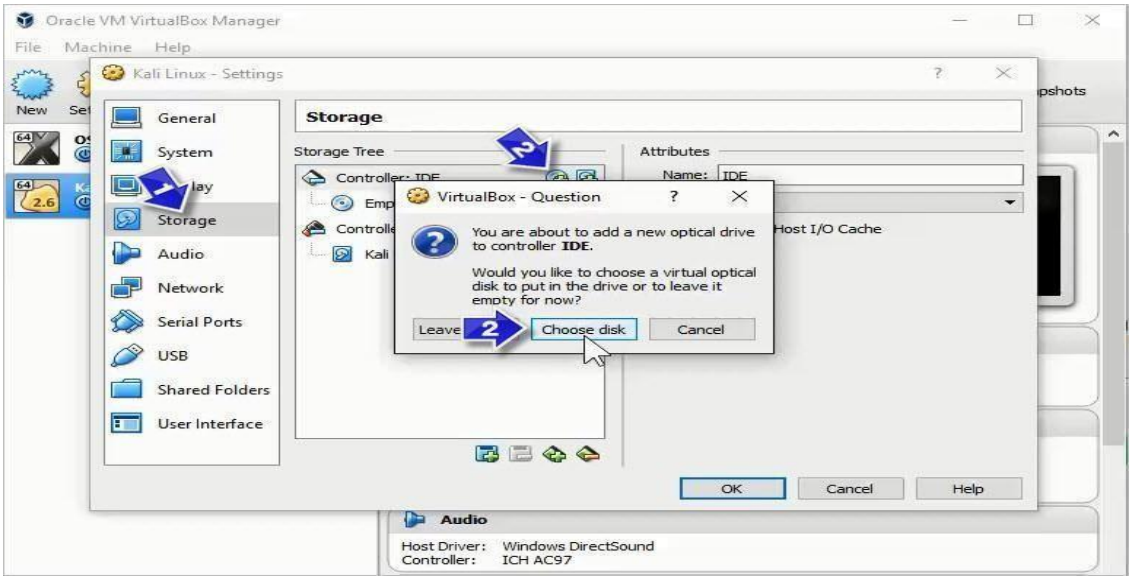
Step 6. In this step, choose the amount of space for the hard disk. If you've selected fixed size hard drive so at least 15 GB, you should select the size of thehard disk.



Step 7. Now, you've successfully created a new virtual machine, but it's not finished yet. Click on the VirtualBox "**Settings**". Navigate to the "**Display tab**" thenincrease the "**Video Memory**".



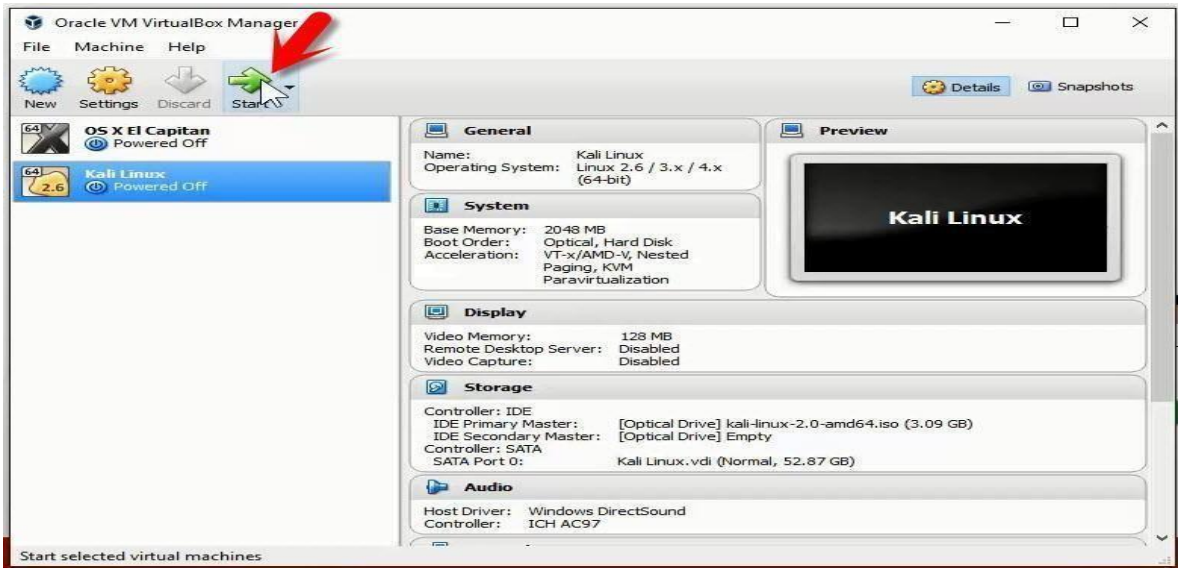
Step 8. Click on the "**Storage tab**" then tap on DVD icon. A small window will pop, choose "**Choose Disk**". Now, Choose the Kali Linux ISO file that you've downloadedfrom its site.



It's done now. Click the "**OK**" button to end up the creating a new virtual machine process.

Install Kali Linux on VirtualBox

Now that you've successfully created a new virtual machine let's get started that howto install Kali Linux on VirtualBox in PC. Open the VirtualBox then select the Kali Linux virtual machine. Tap on the "**Start**" button at the top.

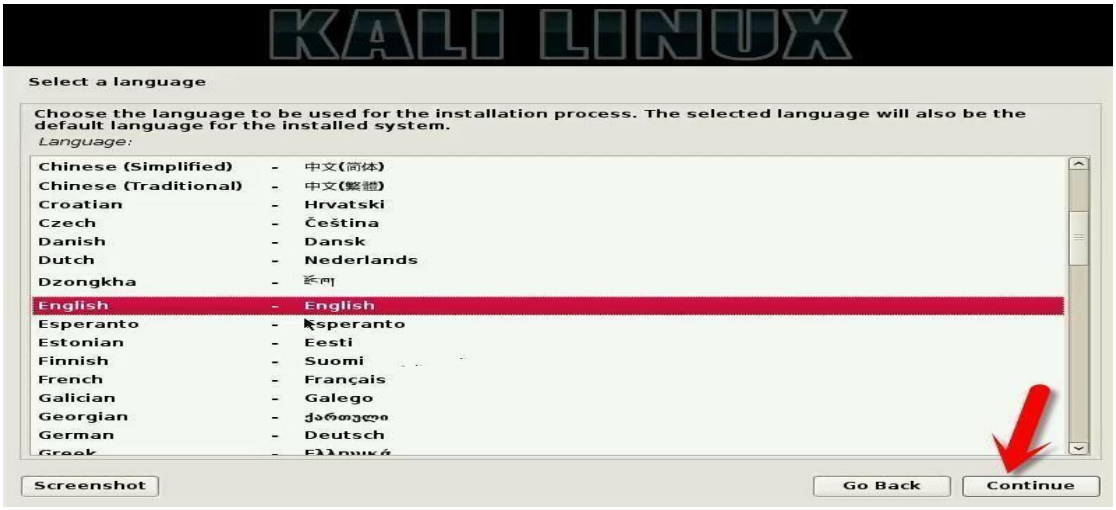


Step **1**. When you start the virtual machine, the Kali Linux will pop up. They're threeoptions to choose.

1. Use Kali Linux live
2. Install
3. Graphical install

Here, I'm going to show you a clean graphical installation of Kali Linux. So I'm going to choose the third option "**Graphical Install**". If you choose the only "Install" optionsso you'll not see a pretty nice graphical user interface instead there will be black witha terminal user interface.

Step 2. In this step, you're going to choose a language, keyboard, and Location. Hitthe "**Continue**" button.



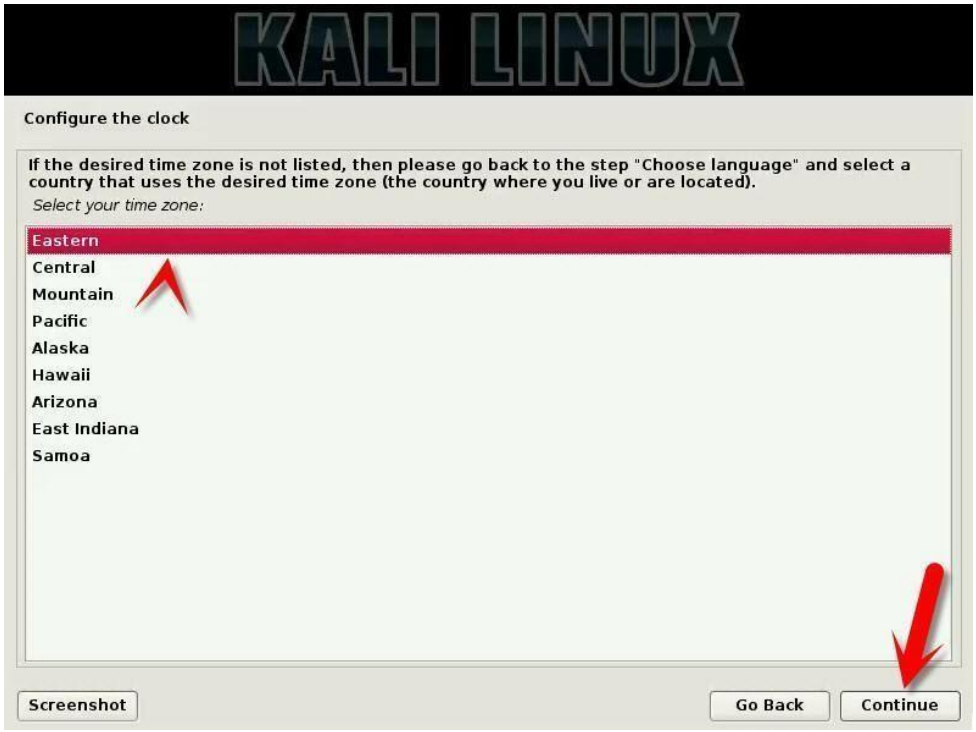
Choose Language

Step 3. Choose a hostname. The hostname is a single word that identifies yoursystem to the network. The hostname is the person who will use the operating system and have full control over it.

Step 4. Choose a domain name. If you don't have a domain, then skip this process.

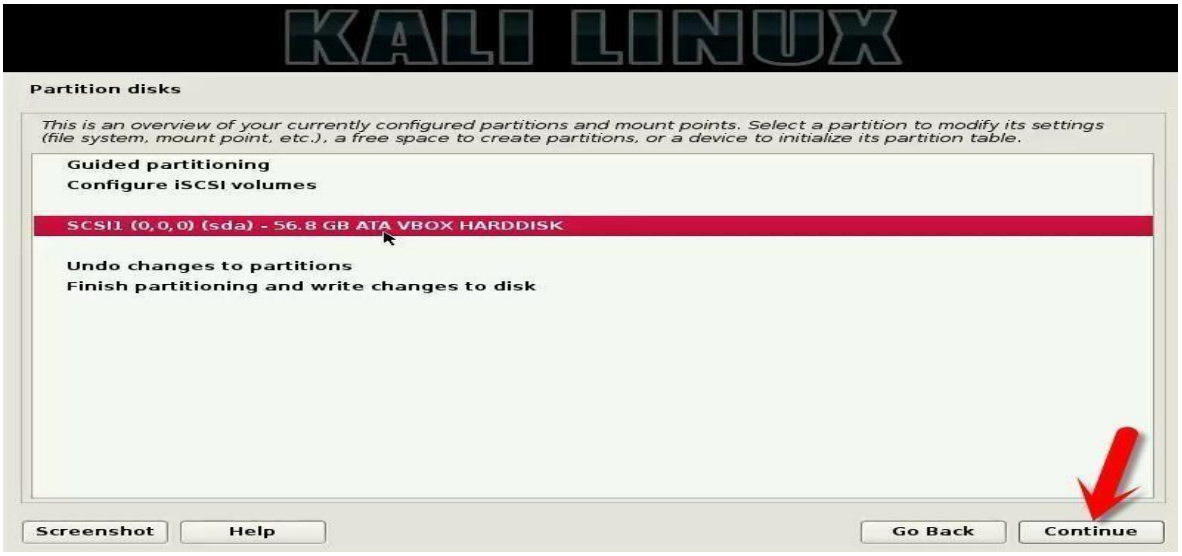
Step 5. Try to type a strong password for the root user. A strong password containsupper case letter, lower case letter, and symbols.

Step 6. Select a proper time zone for your operating system.



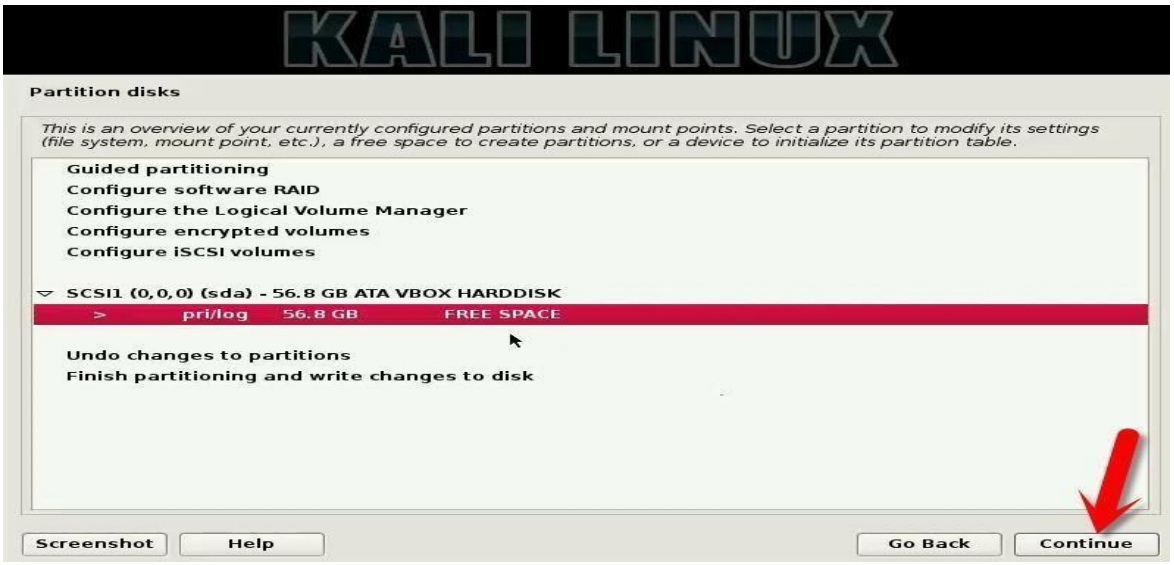
Step 7. Now, you need to create a new partition. Click on "**Manual**".

Step 8. Once you've chosen the manual partitioning. Now, select the third option"**SCSI1 (0,0,0) (sda) -56.8 GB ATA VBOX HARDDISK**".

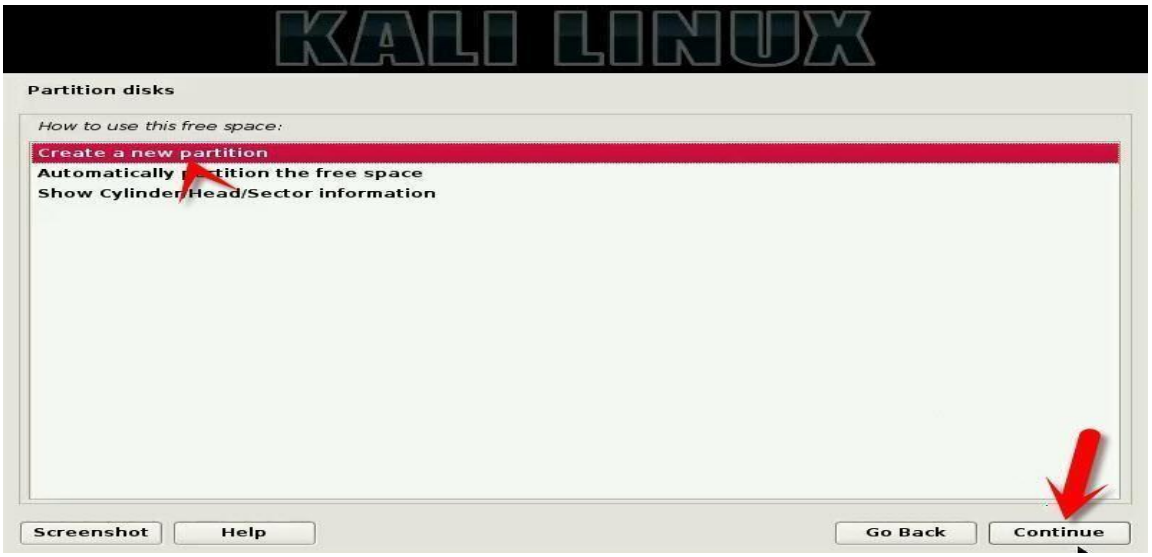


Step 9. In this step, select the "**Yes**" button to continue the partitioning process.

Step 10. Choose the free space then hit the continue button.



Step 11. Select "**Create a new partition**" then hit the "**Continue**" button.

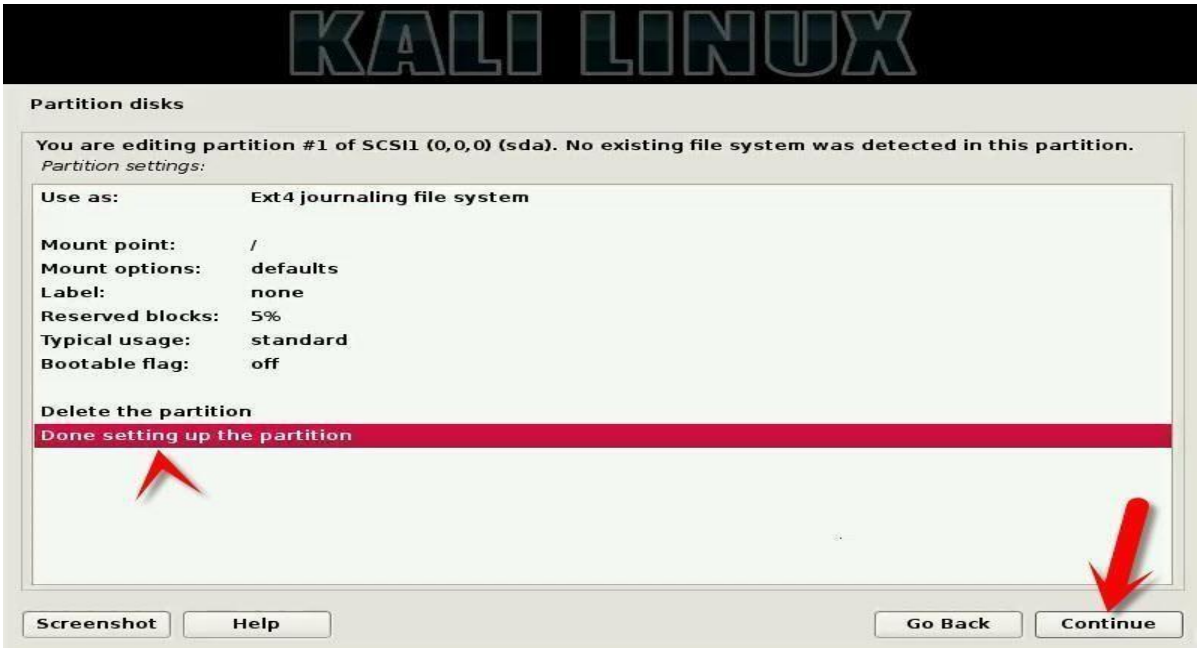


Step **12**. You can create a partition or create multiple partitions. Choose the size ofthe partition. Here I'll create three partitions. So my first drive will be 40 GB.

Step 13. Choose primary or logical, then hit the "**Continue**" button.

Step 14. Please select whether you want the new partition to be created at the beginning or at the end of the available space. Choose the first option "**Beginning**"then hit "**Continue**".

Step 15. Now, choose "**Done setting up the partition**".



Create the other partition the same. Please remember one thing that creates onepartition for "**Swap area**". This partition should be at least 1 GB.

Once you created all the partitions. Choose "**Finish partitioning and write changesto the disk**". Hit the "**Continue**" button.

Step 16. Do you want to write changes to the disk? Click "**Yes**".

The operating system will start installing. Wait for some minutes. It'll take around 10to 20 minutes. This depends on the speed of your computer.

Step 17. Do you want to use the disk mirror? Click "**No**".

Step 18. Install the GRUP boot loader on the hard disk. Click "**Yes**".

Step 19. When you clicked "**Yes**", a new window will be shown to you. Choose thesecond option and hit the "**Continue**" button.

After this, your computer will restart, and you'll be asked to enter the username and password. The username is "**root**", and the password is whatever you've entered instep 5.

RESULT:

Thus the kali or Backtrack Linux/Metasploitable/ Windows XP has been installed

Ex No:2 **Bash Scripting**

Aim:

To explore kali linux and bash scripting

Procedure:

Bash scripts, also known as shell scripts, are powerful tools in the world of command-line automation. They allow you to perform a series of tasks or execute commands by writing scripts that can be run in a terminal or command-line interface. However, the question often arises: how do you run a Bash script in Linux? In this article, we will explore various methods for executing Bash scripts and provide valuable insights on best practices.

The Shebang Line:

Before we delve into the methods of running Bash scripts, it's important to understand the shebang line. The shebang line, which is the first line in your script, indicates the interpreter that should be used to execute the script. For Bash scripts, this line should typically look like this:

#!/bin/bash

This line informs the system that the script should be interpreted using the Bash shell. Even though some methods may work without this line, it's a good practice to include it in your script to ensure compatibility.

Using bash or sh

This is the most standard way of executing the bash script. You must have git bash installed if you are using Windows. For Linux and macOS, bash is installed by default. In this method, we type bash followed by the file name with extension i.e. sh in this case. In a terminal, run the following code by replacing the filename with your bash script filename.

bash filename.sh

Here, bash is a program that contains the shell environments necessary to run the script from the bash shell. So this will execute the script from the bash interpreter.

```
acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$ bash hello.sh

This is a shell script

This takes a number and prints it's cube
Enter the number : 6
6 ^ 3 = 216

acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$
```

Using the bash command to run the script.

We can also use sh to run the script as it will direct to the default shell in the setup environment.

sh filename.sh

```
acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$ sh hello.sh

This is a shell script

This takes a number and prints it's cube
Enter the number : 5
5 ^ 3 = 125

acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$
```

Using the sh command to run the bash script.

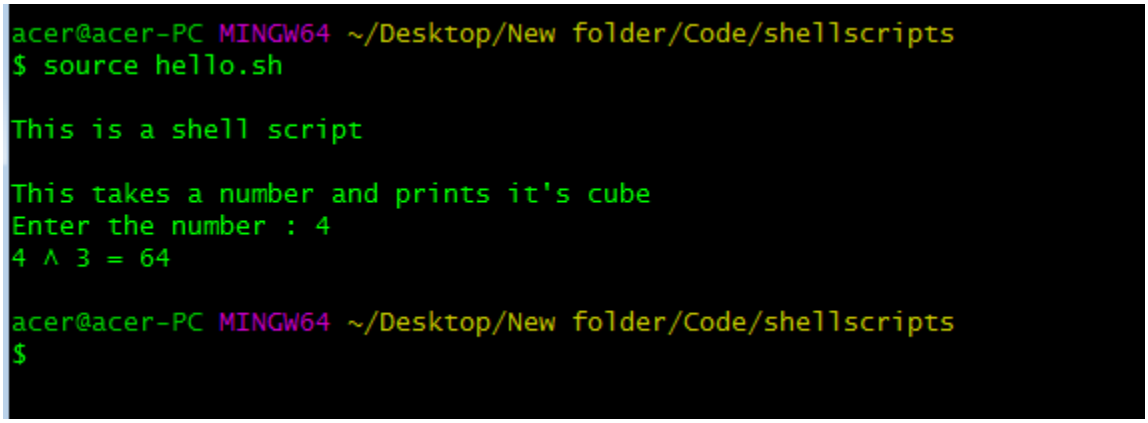
From the above example, we were able to run a bash script using bash as well as the sh command. If you are not in the same folder/directory as the script, make sure you specify the relative path to the script.

Using source

This method is quite easy to run a bash script, and all of them are quite simple. We just need to type in “source” before the file/script name with an extension. In a terminal, run the following code by replacing the filename with your bash script filename.

source filename.sh

The script will simply get executed after “sourcing” the file. The source command will execute the shell script as the default bash command provided you are in the bash shell. You need to be in the bash shell to execute the script using the source command.



Using Source to run a bash script

From the screenshot of the script running, we can see that the source works exactly like the bash or sh command. The above script is very basic, but that doesn’t matter as long as the script is errorless and bug-free. Also, you need to add the relative path here as well if you are not in the same directory as the bash script.

Making the Script Executable with chmod

This method allows you to run a Bash script as an executable, which means you can run it from anywhere in your environment as long as you have a Bash shell available. To make the script executable, you need to adjust its file permissions using the chmod command.

First, navigate to the directory where your script is located. Then, run the following command to change the file’s mode, making it executable:

chmod +x filename.sh

The `+x` flag indicates that the file should be executable. If you are using Linux and are not the root user, you may need to use `sudo` before the `chmod` the command for permission.

After you’ve granted execution permission, you can run the script with the following command, assuming you are in the same directory as the script:

./filename.sh

If you are not on the same path as the bash script, make sure you provide the relative path to the file or the bash script.

./pathToTheFile.sh

```
acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$ chmod +x demo.sh

acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$ ./demo.sh
Hello from BASH
A very basic script
This is some text echoed

acer@acer-PC MINGW64 ~/Desktop/New folder/Code/shellscripts
$
```

using chmod and executing the script.

```
acer@acer-PC MINGW64 ~/Desktop/New folder/Code
$ chmod +x shellscripts/demo.sh

acer@acer-PC MINGW64 ~/Desktop/New folder/Code
$ ./shellscripts/demo.sh
Hello from BASH
A very basic script
This is some text echoed

acer@acer-PC MINGW64 ~/Desktop/New folder/Code
$ ./demo.sh
bash: ./demo.sh: No such file or directory

acer@acer-PC MINGW64 ~/Desktop/New folder/Code
$
```

Result:
Thus, the implementation of Nessus to scan targets have been executed successfully.

EX 3 Aggregating information from public databases using Maltego

AIM:

To aggregate information about various entities using Maltego

PROCEDURE:

Installing Maltego

In the terminal, enter the following command

$sudo apt-get install maltego

This will install the program on your computer

To Create a graph in Maltego

B clicking on the Maltego button in the top left corner and choosing **New** from the main menu. This creates a new graph for us to work on.

Creating Our First Entity in Maltego

To add an Entity for this domain to the graph, we first search for the **Domain Entity** in the Entity Palette, which is on the left of the window, and drag a new Entity onto the graph. By default, Entities come with a default value. In our case, the **Domain Entity** has a default value of **paterva.com**.

Running Maltego Transforms

What Are Transforms?

Transforms are functions which take an Entity as input and create new Entities as output. The output Entities are then linked to the input Entity. This is how a graph grows in Maltego. This could be compared to the way investigations are carried out: you start with some piece of information and you derive new pieces of information from it.

Each Transform accepts certain types of Entities as input. You can see the list of Transforms that can take an Entity as input by right-clicking anywhere on the graph with the Entity selected.

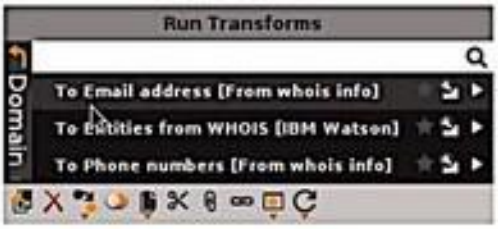
You can now choose what Transform to run by selecting that Transform in the context menu.

If you know which Transform you want to run, you can search for it using the search box in the Run Transform menu.

Note the + in the menu options: it indicates a Transform Set, where related Transforms are grouped together. Clicking on the Transform Set will show the Transforms in that set. To go back, select the back arrow as shown below, or simply right-click anywhere in the Transform menu.

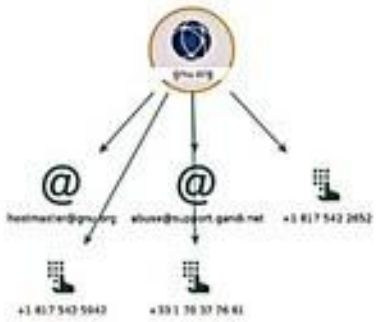
Run the To Email Address [From whois info] Transform to Find Email Addresses from A Domain

In this example, let us find the contact details for the owner of the domain **gnu.org**. Expand the *'Domain owner detail'* set and select the *'To Email address [From whois info]'* transform.



This Transform fetches the "whois" record for the gnu.org domain and extracts the administrative email addresses for the domain. Results from the Transform are added as child entities to the Domain Entity.

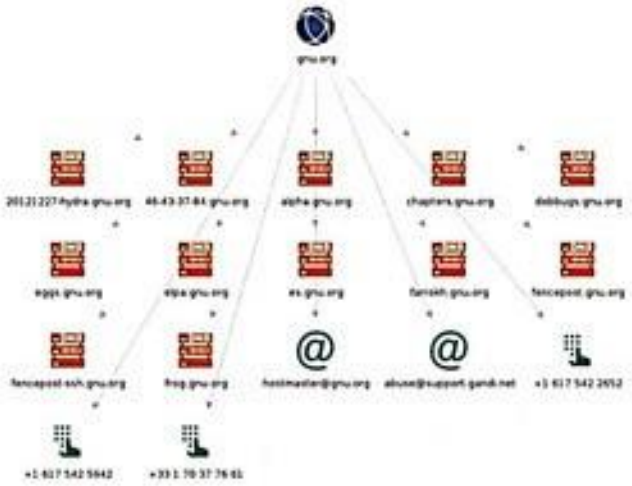
We can also extract any phone numbers present in the whois data by running the *'To Phone numbers [From whois info]'* Transform.



Run the To DNS Name [Robtex] Transform to Find DNS Hostnames Under A Domain

To find some of the DNS hostnames that exist under gnu.org, run the Transform *'To DNS Name [Robtex]'* on the gnu.org Domain Entity. You can search for this Transform by typing *"dns"* in the search box:

The Transform *'To DNS Name [Robtex]'* queries the Robtex database which contains historical DNS data for any DNS name records under gnu.org domain:

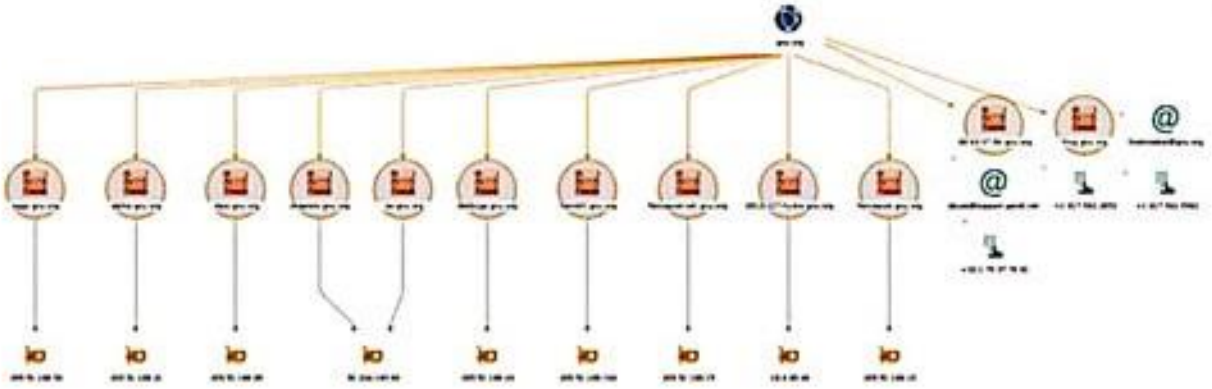


Your graph now contains the administrative contact details and some hostnames under the gnu.org domain.

Run the To IP Address Transform to Look Up IP Addresses of Hostnames

Next, we can look up the IP addresses of these hostnames. This can be done by selecting all DNS Name Entities and running the Transform, *'To IP address'*. Multiple Entities can be selected by dragging the mouse selection over them – click and drag the mouse to select Entities under the selection box:

This Transform returns us the IP address of these DNS names by querying the DNS.



RESULT:

Thus we have successfully gained information on the various entities using maltego

Ex. 4

Understand the Nmap commands and scan the target using Nmap

Aim: To Understand the Nmap commands and scan the target using Nmap

Procedure:

- Nmap is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.
- It allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.
- Nmap is available for both Linux and Windows. By default Kali Linux has Nmap pre-installed. For an instance, this expt. is done in windows.

Basic scans:

- **Ping scan (-sP):** scans the list of devices up and running on a given subnet.

```
> nmap -sP 192.168.1.1/24
```

```
C:\WINDOWS\system32>nmap -sP 192.168.109.1/30
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 19:52 India Standard Time
Nmap done: 4 IP addresses (0 hosts up) scanned in 1.52 seconds
```

- **Scan a single host:** Scans a single host for 1000 well-known ports. These ports are the ones used by popular services like SQL, SNTP, apache, and others.

```
> nmap scanme.nmap.org
```

```
C:\WINDOWS\system32>nmap scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 19:54 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

Stealth scan (sS):

Stealth scanning is performed by sending an SYN packet and analysing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

```
> nmap -sS scanme.nmap.org
```

```
C:\WINDOWS\system32>nmap -sS scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 19.44 seconds
```

Version scanning (sV):

Version scan allows the user to collect information about the port. This can include the version number, the service type, the operating system, the hostname, etc.

```
> nmap -sV scanme.nmap.org
```

```
C:\WINDOWS\system32>nmap -sV scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.72 seconds
```

Aggressive Scanning (-A):

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. Aggressive scans provide far better information than regular scans. However, an aggressive scan also sends out more probes, and it is more likely to be detected during security audits.

```
> nmap -A scanme.nmap.org
```

```
C:\WINDOWS\system32>nmap -A scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:13 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 25 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   45.00 ms  192.168.109.103
2   43.00 ms  192.0.0.1
3   ... 24
25  296.00 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.73 seconds
```

Scanning Multiple Hosts:

Nmap has the capability of scanning multiple hosts simultaneously. This feature comes in real handy when you are managing vast network infrastructure.
You can scan multiple hosts through numerous approaches:

- Write all the IP addresses in a single row to scan all of the hosts at the same time.

```
> nmap 192.164.1.1 192.164.0.2 192.164.0.2
```

```
C:\WINDOWS\system32>nmap 192.164.1.1 192.164.0.2 192.164.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:21 India Standard Time
Nmap scan report for 192-164-1-1.adsl.highway.telekom.at (192.164.1.1)
Host is up (0.040s latency).
All 1000 scanned ports on 192-164-1-1.adsl.highway.telekom.at (192.164.1.1) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192-164-0-2.adsl.highway.telekom.at (192.164.0.2)
Host is up (0.040s latency).
All 1000 scanned ports on 192-164-0-2.adsl.highway.telekom.at (192.164.0.2) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192-164-0-2.adsl.highway.telekom.at (192.164.0.2)
Host is up (0.034s latency).
All 1000 scanned ports on 192-164-0-2.adsl.highway.telekom.at (192.164.0.2) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 3 IP addresses (3 hosts up) scanned in 15.60 seconds
```

- Use the asterisk (*) to scan all of the subnets at once.

```
> nmap 192.164.1.*
```

- Add commas to separate the addresses endings instead of typing the entire domains.

```
> nmap 192.164.0.1,2,3,4
```

- Use a hyphen to specify a range of IP addresses

```
> nmap 192.164.0.0-255
```

(P.S.: The same output will be shown for every approach.)

Port Scanning (-p):

Port scanning is one of the most fundamental features of Nmap. You can scan for ports in several ways…

- Using the ‘-p’ parameter to scan for a single port

```
> nmap -p 973 192.164.0.1
```

```
C:\WINDOWS\system32>nmap -p 973 192.164.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:27 India Standard Time
Nmap scan report for 192-164-0-1.adsl.highway.telekom.at (192.164.0.1)
Host is up (0.071s latency).

PORT    STATE    SERVICE
973/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

- If you specify the type of port, you can scan for information about a particular type of connection, for example for a TCP connection.

```
> nmap -p T:7777, 973 192.164.0.1
```

- A range of ports can be scanned by separating them with a hyphen.

```
> nmap -p 76–973 192.164.0.1
```

- You can also use the **-top-ports** flag to specify the top n ports to scan.

```
> nmap --top-ports 10 scanme.nmap.org
```

Verbosity and Exporting Scan Results

Penetration testing can last days or even weeks. Exporting Nmap results can be useful to avoid redundant work and to help with creating final reports.

Verbose Output (-v):

The verbose output provides additional information about the scan being performed. It is useful to monitor step by step actions Nmap performs on a network, especially if you are an outsider scanning a client's network

```
C:\WINDOWS\system32>nmap -v scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:34 India Standard Time
Initiating Ping Scan at 20:34
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 20:34, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:34
Completed Parallel DNS resolution of 1 host. at 20:34, 0.01s elapsed
Initiating SYN Stealth Scan at 20:34
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 109 out of 363 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to 11 out of 19 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 21 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 40 to 80 due to 11 out of 18 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 80 to 160 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 320 to 640 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 640 to 1000 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 77.03% done; ETC: 20:37 (0:00:30 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 80.30% done; ETC: 20:37 (0:00:33 remaining)
```

Normal output (-oN):

Nmap scans can also be exported to a text file. It will be slightly different from the original command line output, but it will capture all the essential scan results.

```
C:\WINDOWS\system32>nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 20:40 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```

XML output (-oX):

Nmap scans can also be exported to XML. It is also the preferred file format of most pen-testing tools, making it easily parsable when importing scan results.

```
> nmap -oX output.xml scanme.nmap.org
```

Multiple Formats (-oA) :

You can also export the scan results in all the available formats at once using the -oA command.

```
> nmap -oA output scanme.nmap.org
```

Result: Thus the experiment of understanding and using Nmap commands and scanning the target has been executed.

Expt. 5

Install Metasploitable on the Virtualbox to exploit an unpatched vulnerability

Aim: To install Metasploitable on the Virtualbox to exploit an unpatched vulnerability.

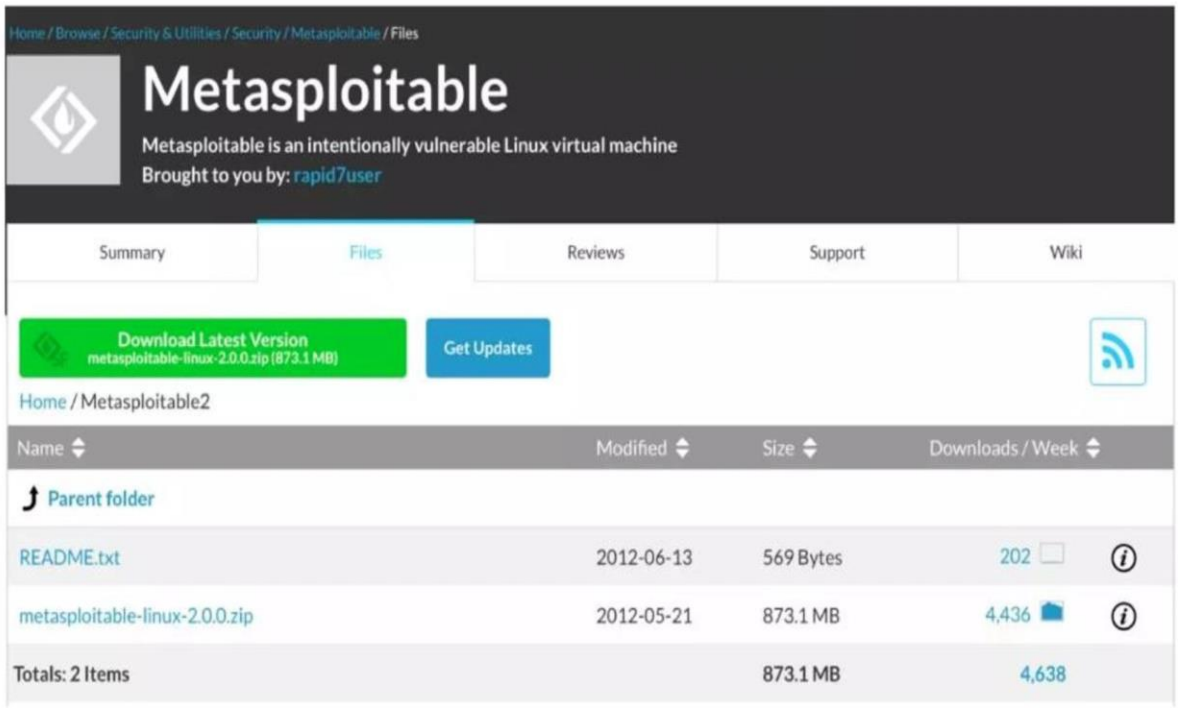
Procedure:

Metasploitable:

Metasploitable is a virtual machine with several intentional misconfigurations and vulnerabilities for you to exploit. This is a great tool for sharpening your penetration testing skills.

Download Metasploitable:

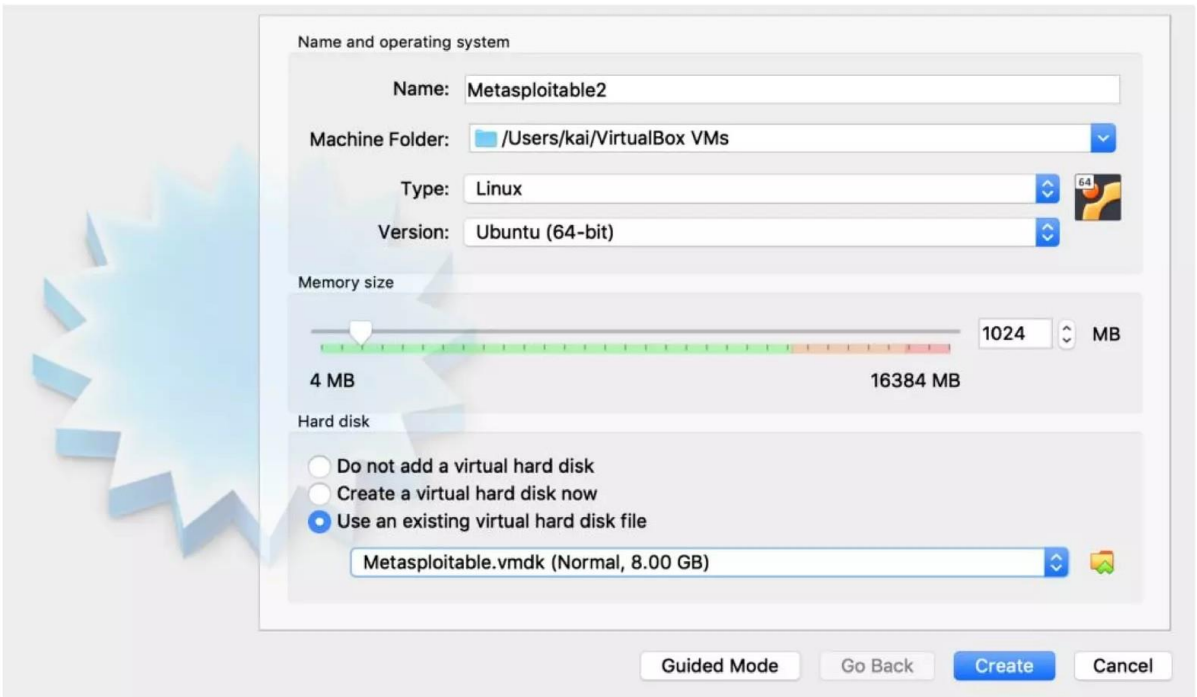
Grab a copy of the Metasploitable virtual machine at: SourceForge



While you are waiting for the file to download you can start setting up the VM.

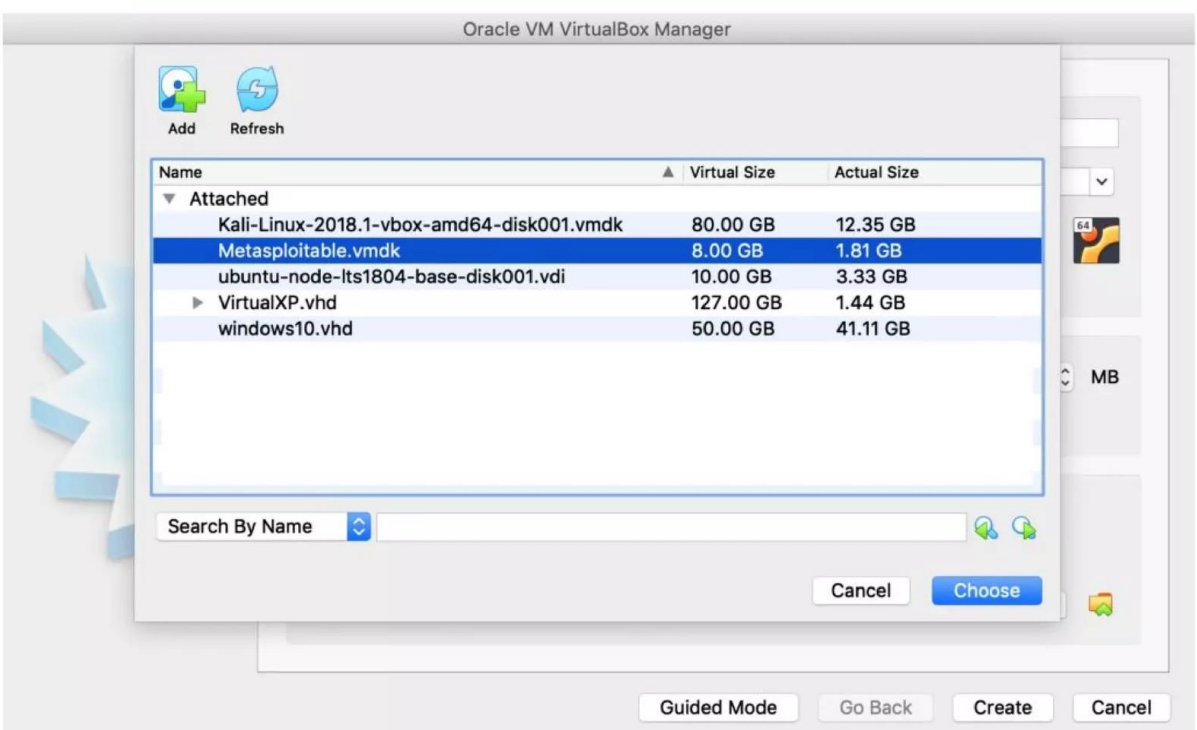
Create the Virtualbox VM:

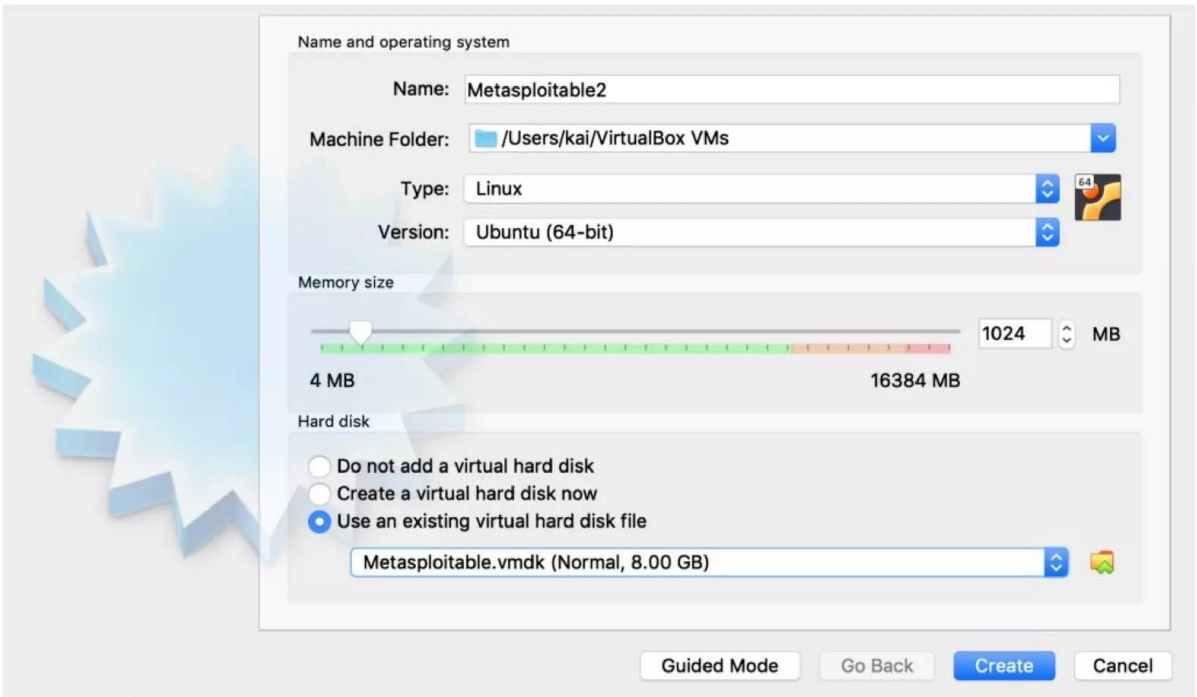
Create a new virtual machine in Virtual Box. Give the machine a descriptive name, and select Linux as the type.



Use an Existing Hard Disk

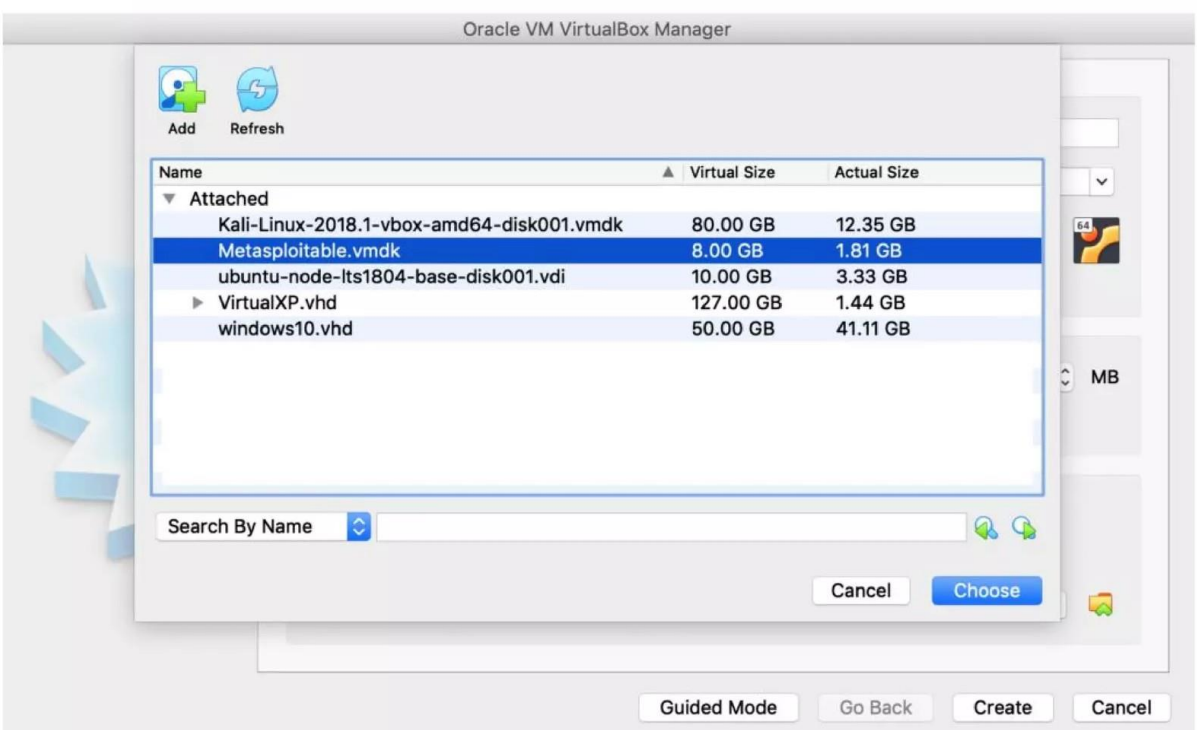
During the installation select Use an Existing Hard Disk File and select the downloaded Metasploitable vmdk file.





Use an Existing Hard Disk

During the installation select Use an Existing Hard Disk File and select the downloaded Metasploitable vmdk file.



Once the machine has been created, go ahead and fire it up.

Start the VM

After the initial boot process you will be greeted by the Metasploitable login screen. The default username is "msfadmin", and the default password is also "msfadmin".

That is all it takes to install Metasploitable. Now you may be wondering where to begin.....

Result: Thus the installation of Metasploitable on the Virtualbox to exploit unpatched vulnerabilities has been executed.

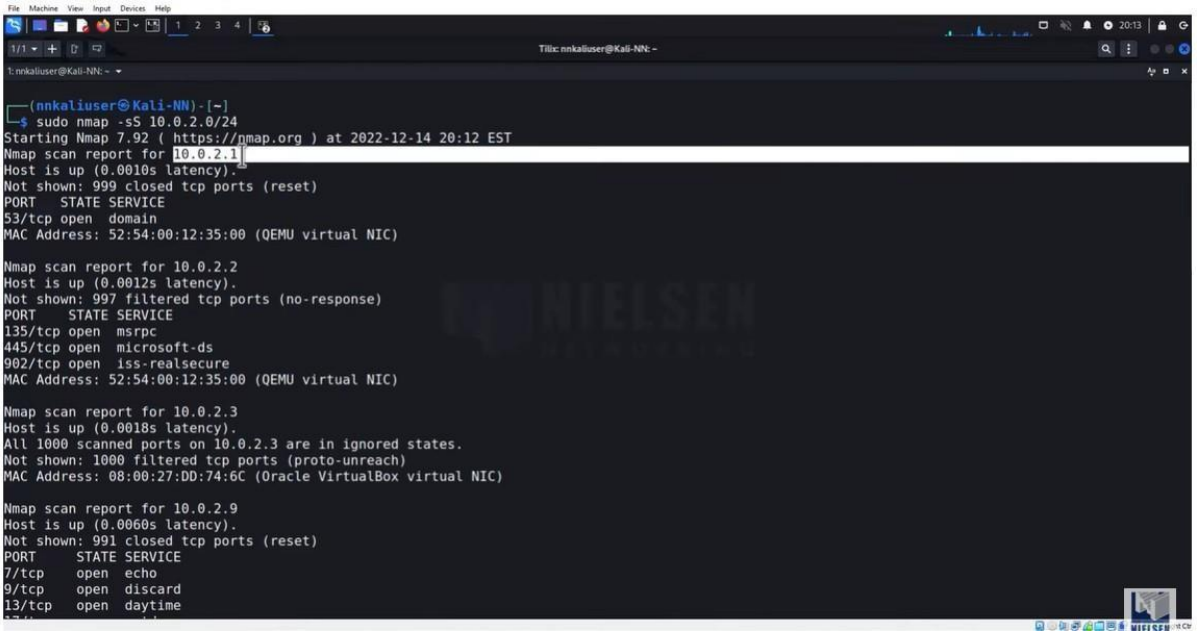
Ex 6 Use Metasploit to exploit an unpatched vulnerability

Aim:

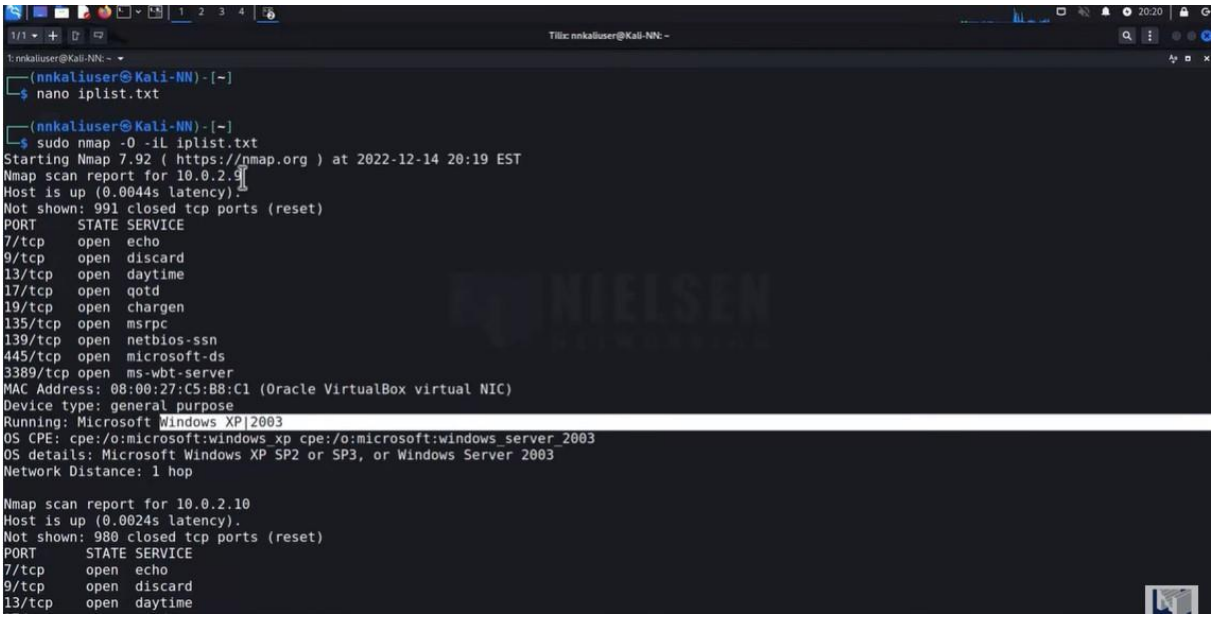
To use Metasploit to exploit an unpatched vulnerability.

Procedure:

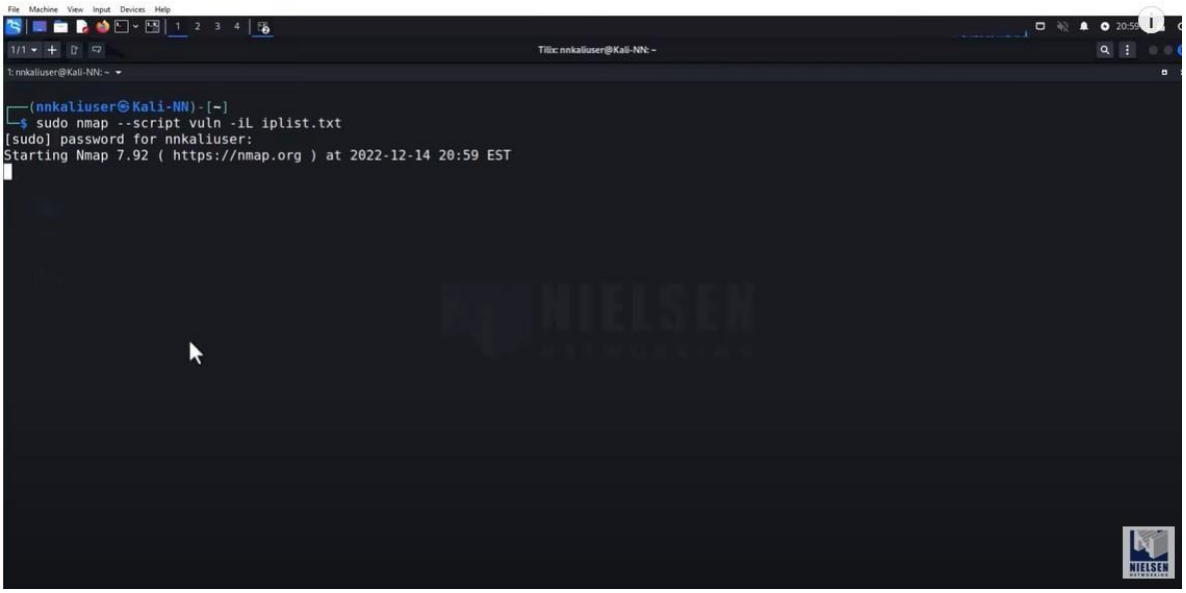
Nmap which is a network scanning tool, is used to carry out a network discovery scan.

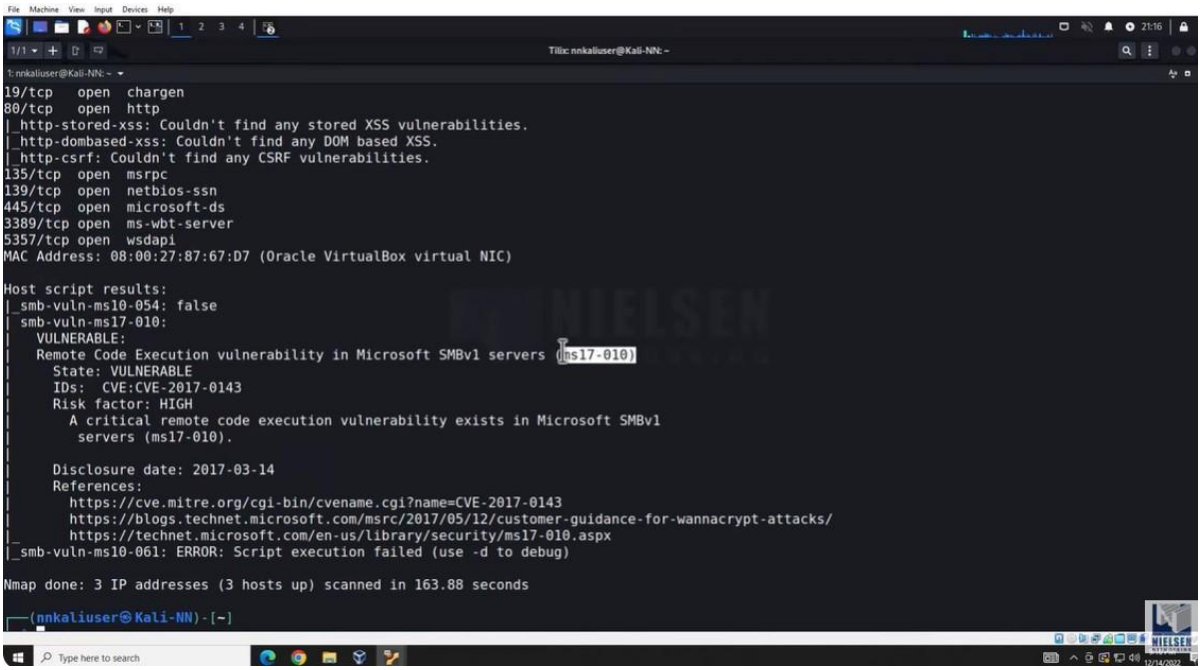


The IP addresses which are targeted are saved in a nano file. The OS identification of these IP addresses is done.



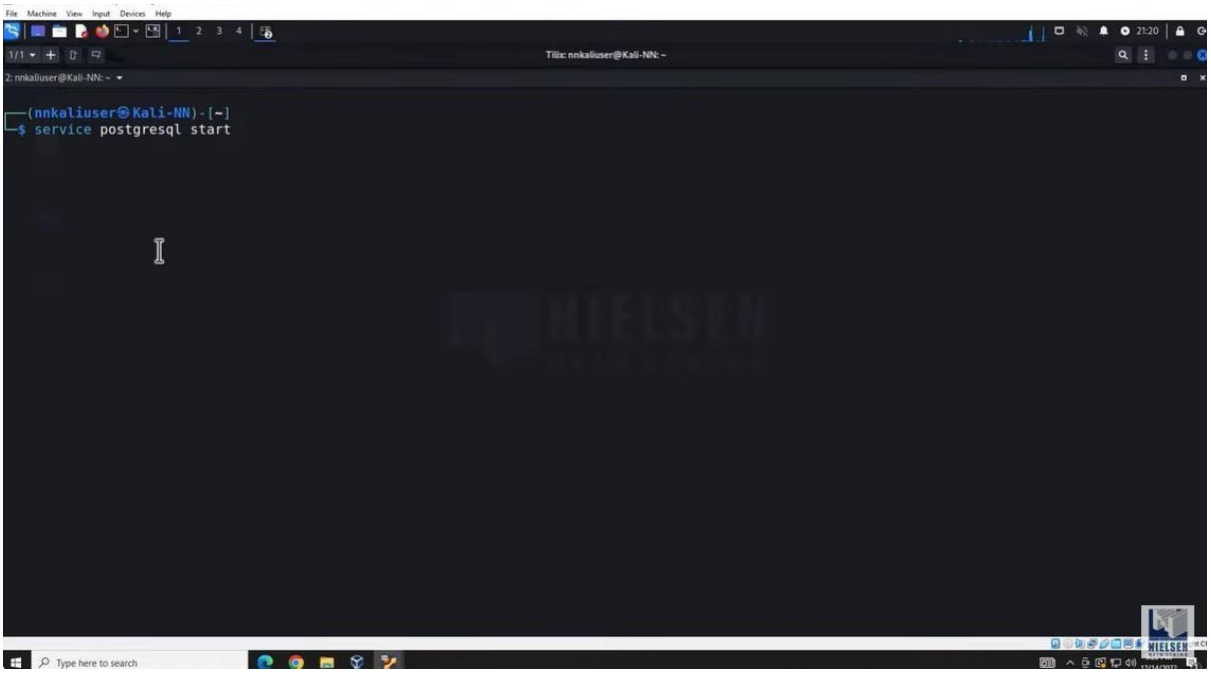
The final scan is vuln built in script scan which gives any known or common vulnerabilities in the target system.



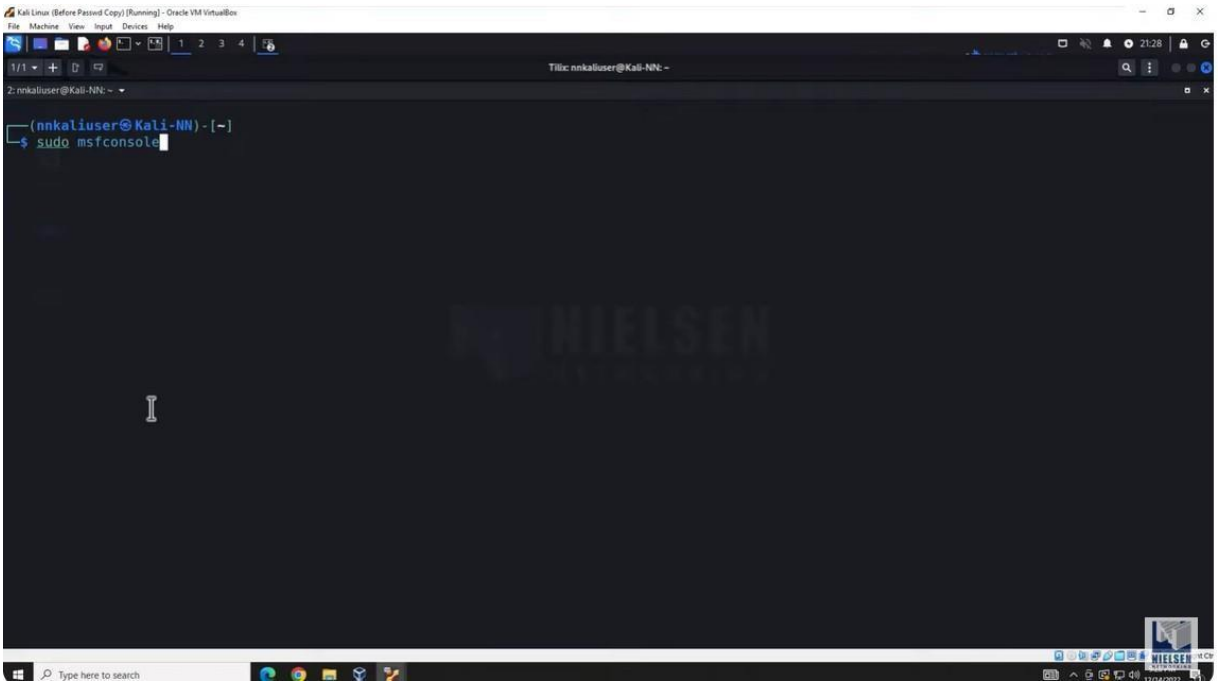


The above picture indicates the ms-17 Vulnerability in one of the targeted systems.

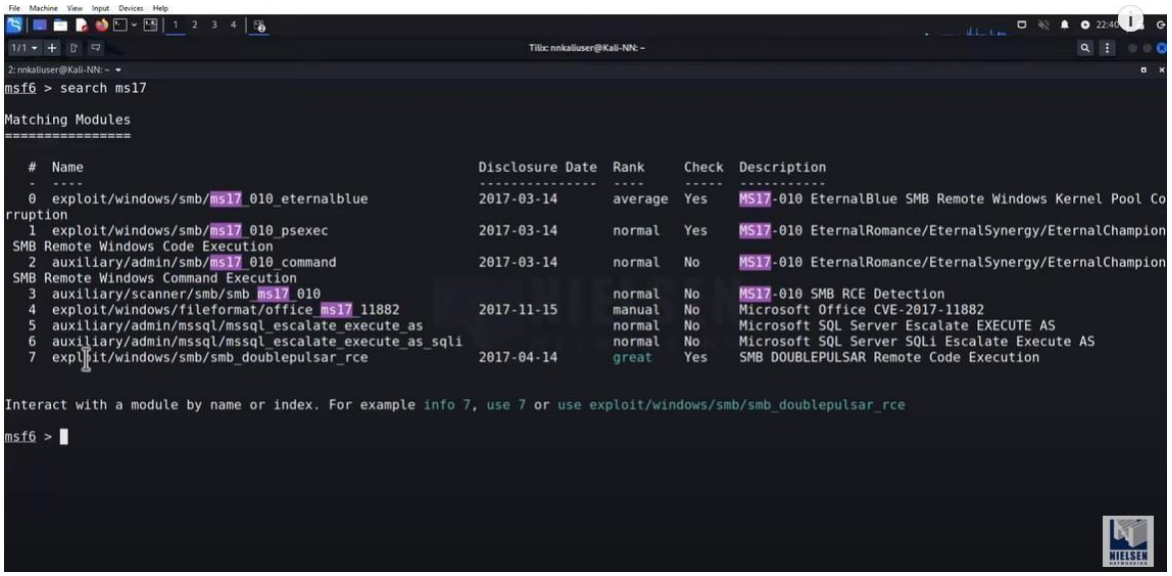
Before starting Metasploit, an auxiliary database is required and the one used here is postgresql.



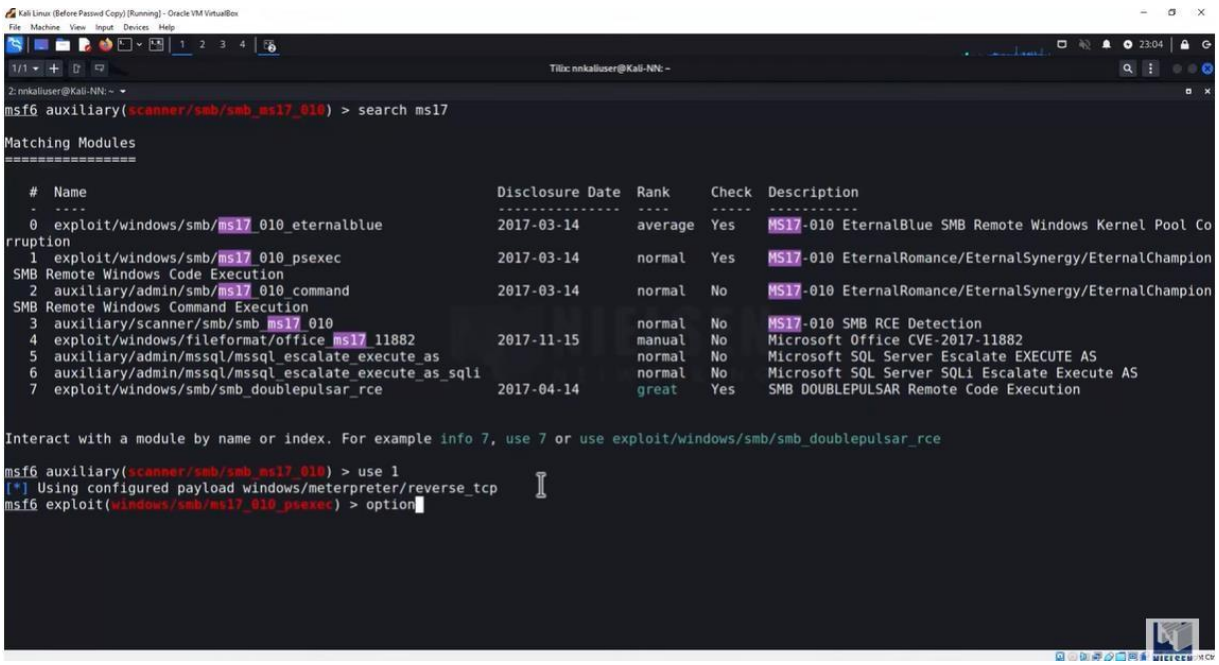
There are four interfaces in Metasploit and the one used here is msf console, which is the command line interface for Metasploit.



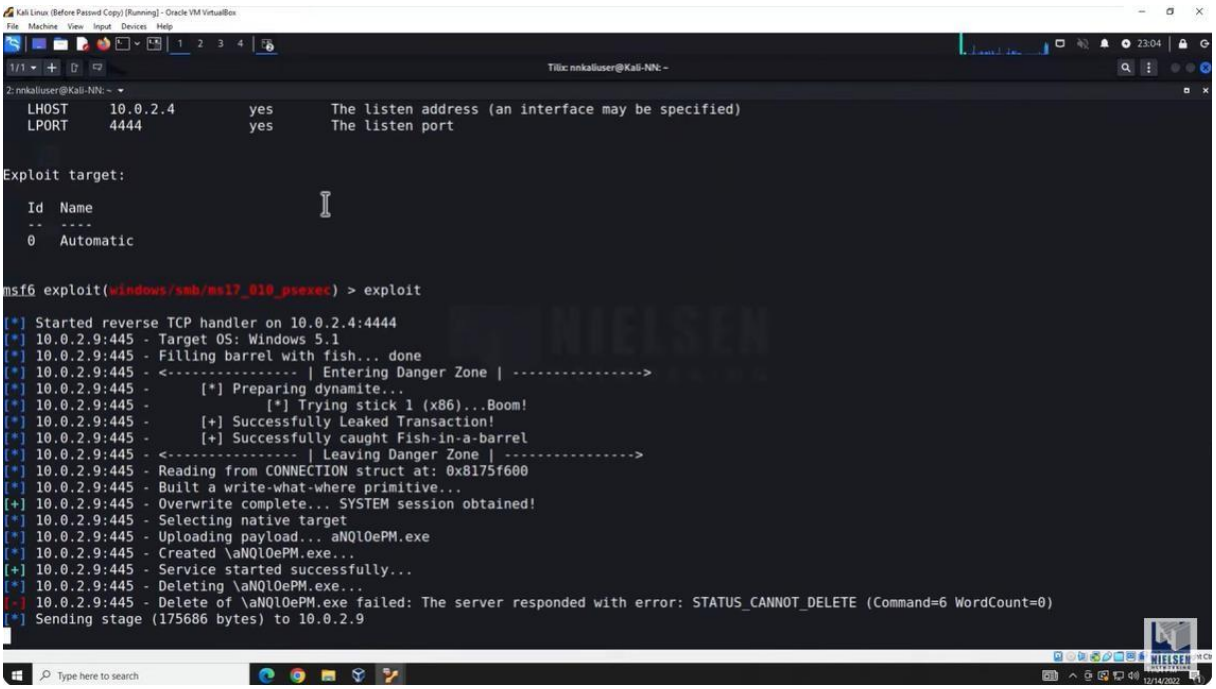
After starting the msf console, the specific vulnerability is searched using the search command. The output gives both exploits and auxiliary. The exploit contains exploit followed by the operating system then the service and lastly the vulnerability. The auxiliary contains the auxiliary followed by whether it is a scanner, fuzzer or an admin then the service and lastly the vulnerability.



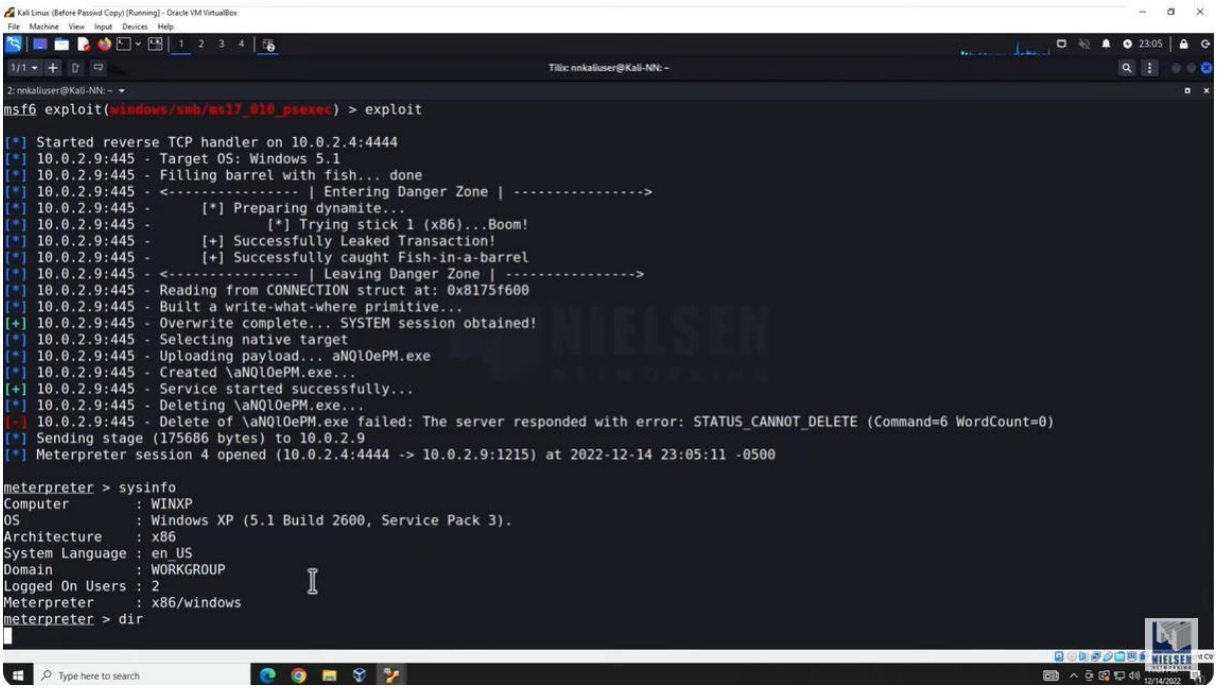
To find whether a scanner is vulnerable, the command use 1 is used after which, the options command is used. The options command gives the available parameters for an exploit will be shown by the show options command.



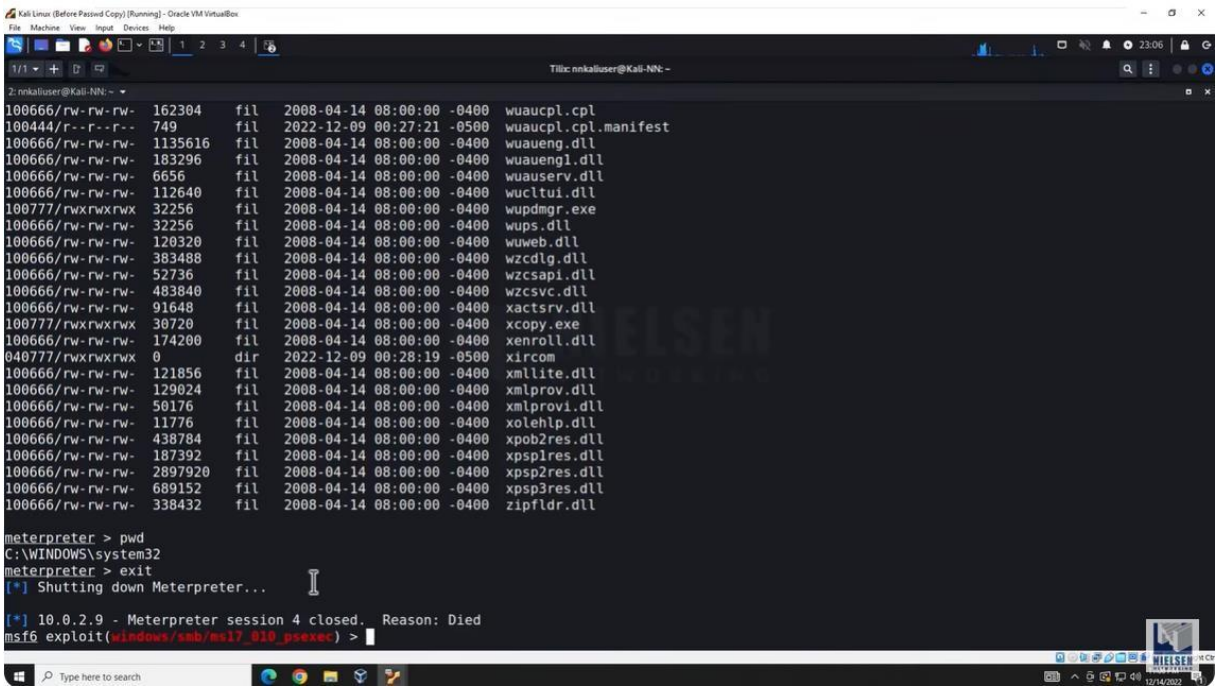
To further exploit the target machine, the exploit command is used.



In the meterpreter shell, the information about the target system is verified.



The entire system can be controlled with this.



Result:

Thus, Metasploit is used to exploit the unpatched vulnerability and the output is verified.

Ex 7 Install Linux server on the virtual box and install ssh

Aim:

To install linux server on the virtual box and install ssh

Procedure:

1. Download VirtualBox & Ubuntu Server

First we need to download and install VirtualBox itself, followed by a Linux installer.

- Download VirtualBox for your host OS (Windows, Mac, or Linux) from the VirtualBox downloads page.
- Run the installer, and follow the directions on screen.
- Download Ubuntu Server from the Ubuntu downloads page. You'll have a choice between the latest version and a "Long Term Support" version; choose the LTS version because it'll be more stable.
- A big `.iso` file will be downloaded. Make note of the folder it gets downloaded to; we'll need to find it in a minute. `.iso` stands for ISO 9660, a standard for representing the contents of CD-ROMs and DVD-ROMs as computer files. Basically, you've just downloaded a virtual Ubuntu installation CD.

2. Set Up a Virtual Machine Host

Now we need to create and configure a virtual machine within VirtualBox.

- Launch VirtualBox, and click the "New" button in the toolbar to create a new virtual machine.
- Go through the wizard dialog to configure the new virtual machine, leaving all values at the default *except the following*:

        - **Name:** This can be whatever you want, but since we're simulating a server at our hosting company, we're going to use the name "hostcom".
        - **Type:** "Linux"
        - **Version:** "Ubuntu (64-bit)"
- Click the "Create" button in the wizard to create your new virtual machine.

3. Install a Ubuntu Linux Server

Now you have a virtual machine, but its virtual hard drive is empty. There's no operating system for it to boot with. If it were a physical computer, we'd pop in a CD or other installation media, which would allow the machine to boot and install an operating system to its hard drive. We're going to do the virtual equivalent of that now.

- Back at the main VirtualBox window, select your new virtual machine from the list of machines, and click the "Start" button in the toolbar to "power it on".
- Another dialog should appear, basically saying we need to "insert" the installation media. Click the folder icon, navigate to the folder you downloaded the `.iso` file to previously, select the file, and click "Open".
- Back at the dialog, click "Start" to start the virtual machine.
- The virtual machine will boot, and the Ubuntu installer will load.
- Go through the menus to configure Ubuntu, leaving all values at the default *except the following* (don't include quotation marks):
    - **Hostname:** "hostcom" (or another all-lower-case network name for your server).
    - **User full name:** Your full name (e.g. "Jay McGavren").
    - **Username:** Your user name, which should be short, one word, and all lower case (e.g. "jay").
    - **Password:** Enter and confirm a password. Remember it, because you'll need it to log in or run administrative commands on the virtual machine.

- **Write partition changes to disk:** “No” will be selected by default; choose “Yes”.
- **Write to disk (again):** “No” will be selected by default; choose “Yes”.
- **Software selection:** “standard system utilities” will be selected by default, so just hit Enter. Other packages you need should be installed using the `apt-get` program later.
- **GRUB boot loader:** The default choice is actually the correct one on this screen, but to avoid confusion: The installer will confirm this “is the only operating system on this computer”. And it *is* the only operating system on this *virtual* machine. So go ahead and choose “Yes”.

At this point the installation will be complete! Choose “Continue” to reboot the virtual machine. (There’s no need to “eject” the virtual installation media.) When the virtual machine reboots, it’ll load the Ubuntu OS itself. You’ll be prompted for a login; enter the user name and password you created while installing Ubuntu. You’re now logged in to your new virtual server!

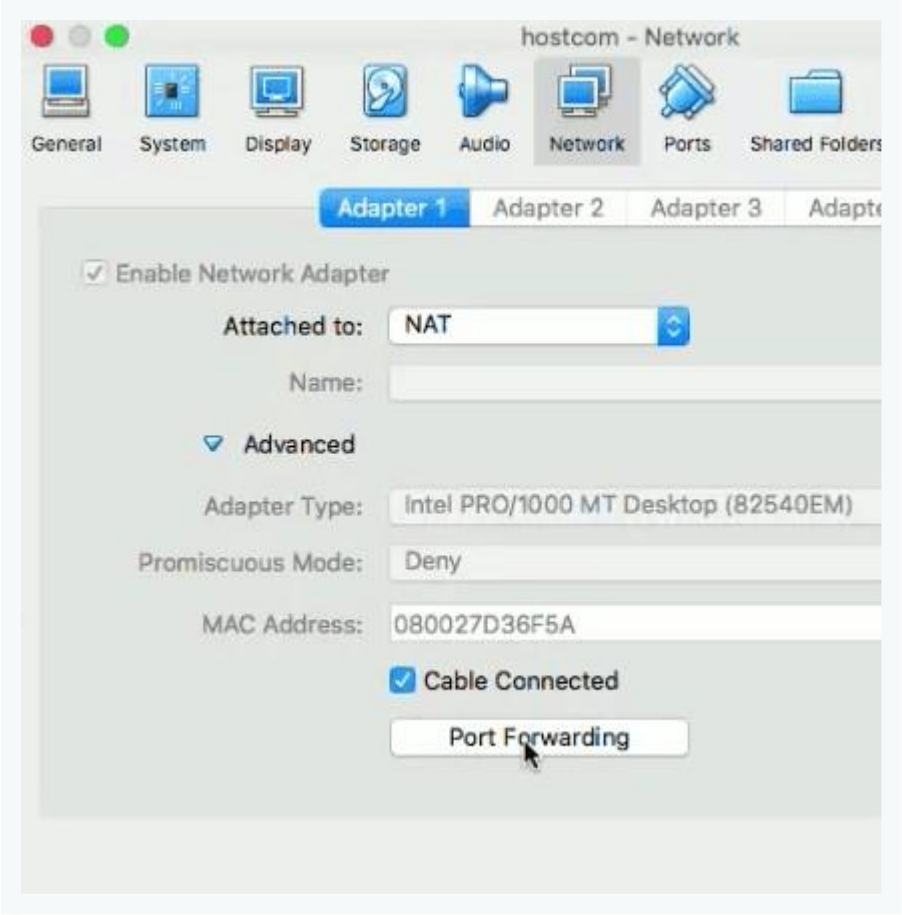
4. Connect to the Server Via SSH

The window on your screen right now emulates a monitor that’s connected to your virtual machine. What you type on your keyboard emulates a keyboard that’s connected directly to your virtual machine. But to connect to servers out on the Internet, you would use the Secure SHell program, or `ssh`. `ssh` connects you to a terminal on a remote computer, and it encrypts everything you do so no one can eavesdrop on the passwords and commands you’re sending. From now on, we’re going to want to connect via SSH. Let’s set that up now.

SSH usually listens for network traffic on port 22, and the SSH on our virtual server will be no different. We can tell VirtualBox to open a port on our local computer, and send all network traffic that it receives on that port, to a port on our virtual server. So

we’re going to open port 2222 on our host machine, and forward all traffic to port 22 on our virtual machine. When we use the `ssh` port to connect to port 2222 on the host, we’ll wind up talking to the SSH service on the virtual machine.

- In the main VirtualBox window, select your virtual machine from the list of machines, and click the “Settings” button in the toolbar.
- In the configuration window that appears, click the “Network” tab.
- You’ll see sub-tabs for “Adapter 1” through “Adapter 4”. Ensure Adapter 1 (the main virtual networking hardware) is selected.
- Click the arrow by the “Advanced” label to expand the advanced settings section.
- Click “Port Forwarding”. A new sub-window will appear with a table of port forwarding rules.



- Click the plus-sign icon to add a new rule.
- Set the fields as follows (don’t include quotation marks):
    - **Name:** This can be any descriptive string, but we recommend “ssh”

        - **Protocol:** “TCP”
        - **Host IP:** Leave blank
        - **Host port:** “2222”
        - **Guest IP:** Leave blank
        - **Guest Port:** “22”
    - If you’re planning to set up a server on the guest later, you may also want to add another rule to forward traffic from a port on the host to the port on the guest that the server will be running on. (E.g. for a web server, forward host port “8080” to guest port “80”.)
    - Click “OK” to close the forwarding rules window when you’re done.
    - Click “OK” in the virtual machine settings window to save your changes.

The SSH service may not be installed on your virtual Linux server yet. To install it:

- Start your virtual machine if it’s not already running, switch to the window that shows its screen, and log in.
- At the `$` prompt, run this command: `sudo apt-get install openssh-server`
- You’ll be prompted for a password; enter the one you created when installing Ubuntu.
- The SSH server software will be installed, and the service should start automatically.

The last step will be to try connecting from your host machine to the virtual machine via SSH. We’re going to direct our SSH client program to connect from our computer, back to port 2222 on that same computer. We can connect to the same computer we’re running on by using the special IP address `127.0.0.1`. The traffic will be forwarded to port 22 of our virtual machine, and it should connect.

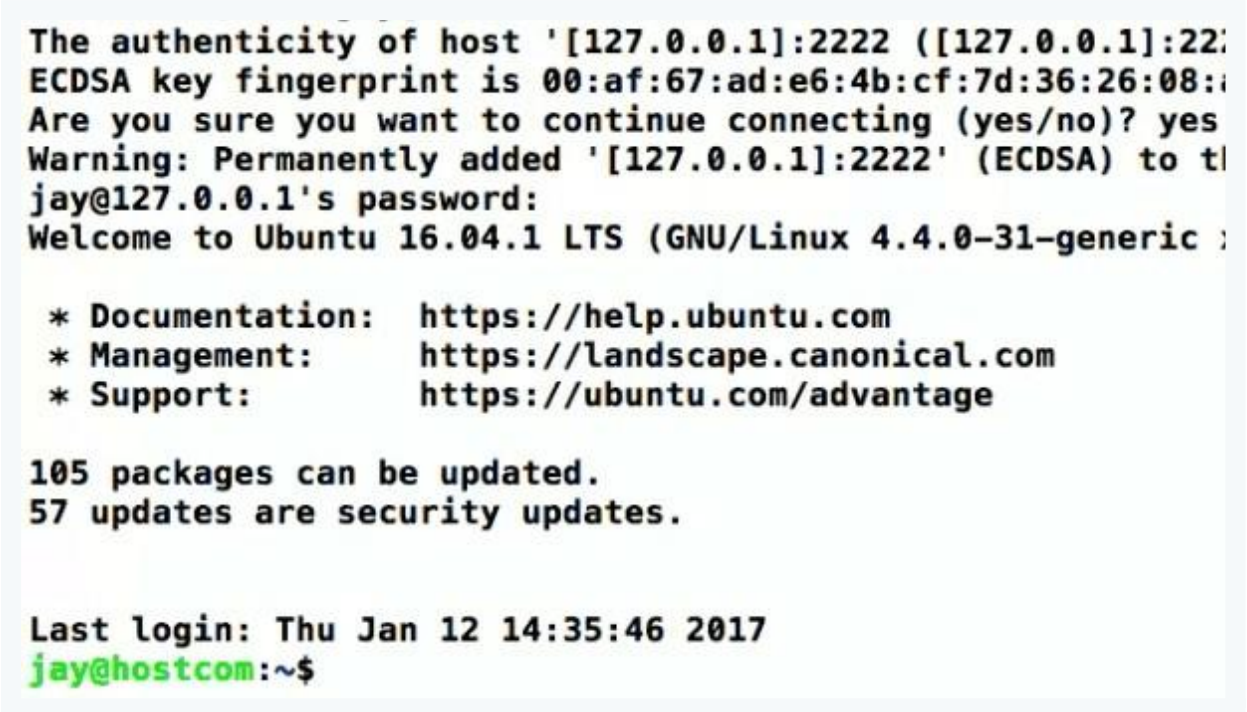
Readers running Mac or Linux as their host operating systems should already have the `ssh` client program installed. Open a terminal on your host machine, and run this command (substituting the user name you set up when installing Ubuntu for "yourlogin"):

```
ssh yourlogin@127.0.0.1 -p 2222
```

Windows users may need to download PuTTY, a free SSH client app. Follow these directions to establish a connection, using "localhost" as the host name, "SSH" as the protocol, and "2222" as the port. You'll be prompted to enter a user name later, as you log in.

Regardless of whether you're connecting via the `ssh` program or PuTTY, you'll see a warning saying something like "the SSH server isn't recognized", which is normal, since this is our first time connecting. Type "yes" to confirm that it's OK to connect.

Then type the login (if prompted for one) and password that you set up when installing Ubuntu. You should be taken to a system prompt, where you can start running Linux commands to your heart's content.



Congratulations! You have a virtual Linux server running right there on your computer! The sky's the limit from here. If you'd like some ideas, Treehouse Pro and Techdegree subscribers can check out our workshops on deploying web apps to production, and check out the Treehouse 7-day free trial. Have fun with your new server!

Result:

Thus, a linux server is successfully installed and accessed using ssh.

Ex 8 Use Fail2banto scan log files and ban Ips

Aim:

To use Fail2banto scan log files and ban Ips that show the malicious signs

Procedure:

Install Fail2Ban: If you haven't already installed Fail2Ban, you can typically do so using your package manager. For example, on Debian-based systems, you would use:

```arduino
sudo apt-get install fail2ban
```

Configure Fail2Ban: Fail2Ban's configuration files are usually found in /etc/fail2ban/. The main configuration file is fail2ban.conf, and the individual jail configurations are stored in the jail.conf file. You can create custom jails as well.

Create or Modify Jails: In the jail.conf file, you can define specific jails for different services (e.g., SSH, Apache, Nginx, etc.). Each jail specifies which log file to monitor and what patterns to look for. You can create custom rules based on your requirements. For example:

```plaintext
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Create Filters: Filters define the patterns that Fail2Ban will search for in log files. You can find existing filters in /etc/fail2ban/filter.d/ or create your own. For example, to create a filter to detect SSH brute-force attempts:

```
# /etc/fail2ban/filter.d/sshd.conf
[Definition]
failregex = ^%(__prefix_line)s(?:error: PAM: )?Authentication failure for .* from <HOST>\s*$
            ^%(__prefix_line)s(?:error: PAM: )?User not known to the underlying authentication module for .* from <HOST>\s*$
            ^%(__prefix_line)sFailed \S+ for .* from <HOST>(?: port \d*)?(?: ssh\d*)?(: (ruser .*|(\S+ ID \S+ \(serial \d+\) CA )?\S+ %(__md5hex)s(, client user ".*", client host ".*")?))?\s*$
```

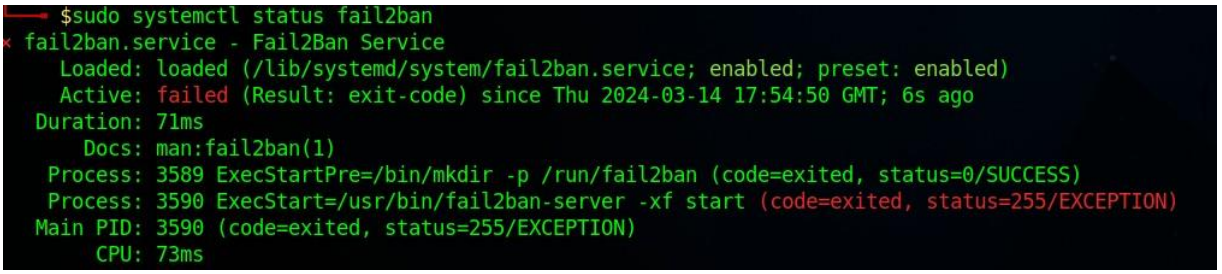
ignoreregex =

Start Fail2Ban: After configuring, start Fail2Ban to begin monitoring log files and applying bans:

```sql
sudo systemctl start fail2ban
```

Check Status: You can check the status of Fail2Ban to see if it's running and if anyIPs have been banned:

```lua
sudo fail2ban-client status
```



Result:

Thus, a fail2ban is successfully used to ban malicious IPs.

Ex 9 Launch brute-force attacks using Hydra.

Aim:

To launch brute-force attacks on the Linux server using Hydra.

Procedure:

Installation:
Execute the below command in the terminal to install the hydra tool using the apt package manager.

sudo apt install hydra

Usage:
Example 1: Bruteforcing Both Usernames And PasswordsType the below command on the terminal and hit Enter.

hydra -L user.txt -P pass.txt 192.168.29.135 ssh -t 4

-l specifies a username during a brute force attack.
-L specifies a username wordlist to be used during a brute force attack.
-p specifies a password during a brute force attack.
-P specifies a password wordlist to use during a brute force attack.
-t set to 4, which sets the number of parallel tasks (threads) to run.

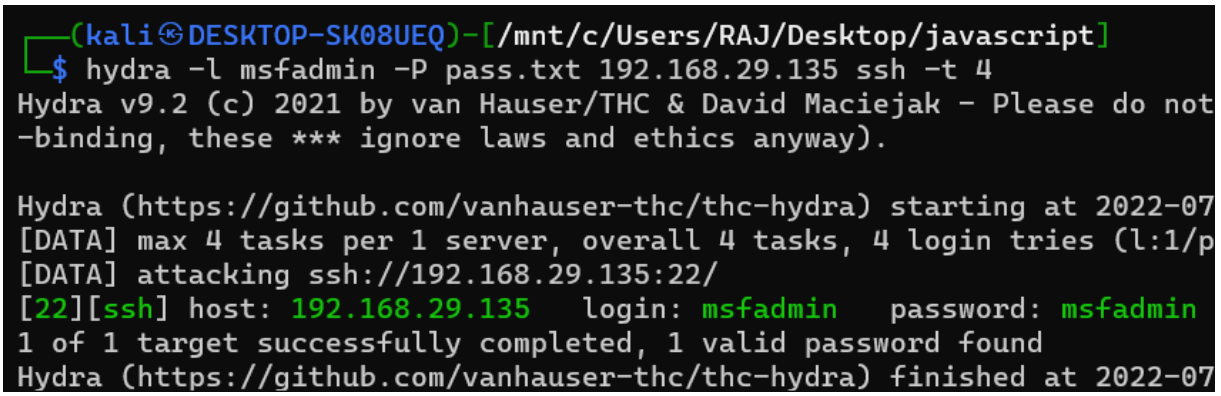
```
┌──(kali㉿DESKTOP-SK08UEQ)-[/mnt/c/Users/RAJ/Desktop/javascript]
└─$ hydra -L user.txt -P pass.txt 192.168.29.135 ssh -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p
[DATA] attacking ssh://192.168.29.135:22/
[22][ssh] host: 192.168.29.135   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-
```

Example 2: Bruteforcing Passwords
Type the below command on the terminal and hit Enter.

hydra -l msfadmin -P pass.txt 192.168.29.135 ssh -t 4

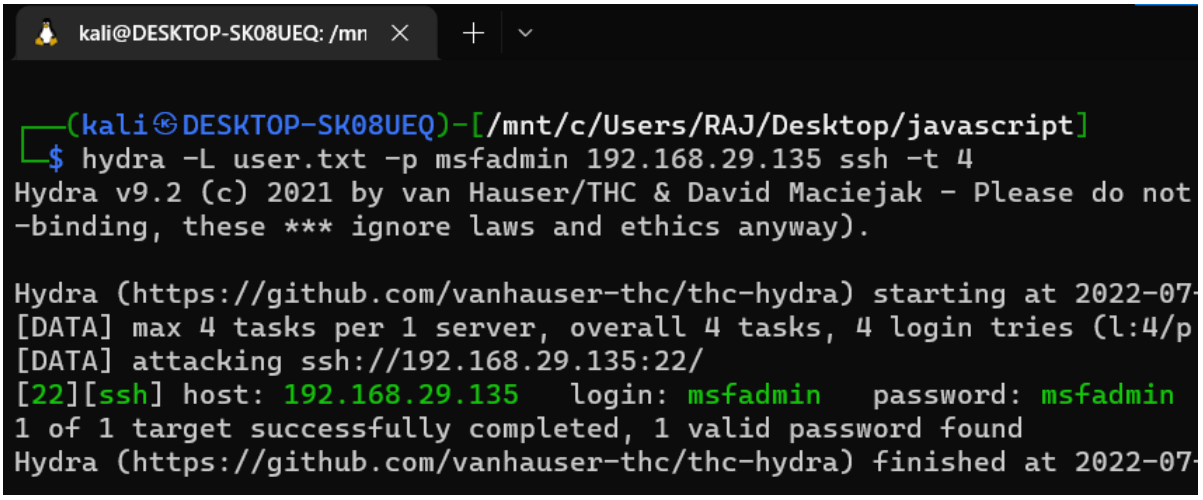
Here, we are only brute-forcing passwords on the target server.



Example 3: Bruteforcing Username
Type the below command on the terminal and hit Enter.

hydra -L user.txt -p msfadmin 192.168.29.135 ssh -t 4

In the above example, we were a brute-forcing only passwords, so in this example, we are brute-forcing only usernames on the target server.



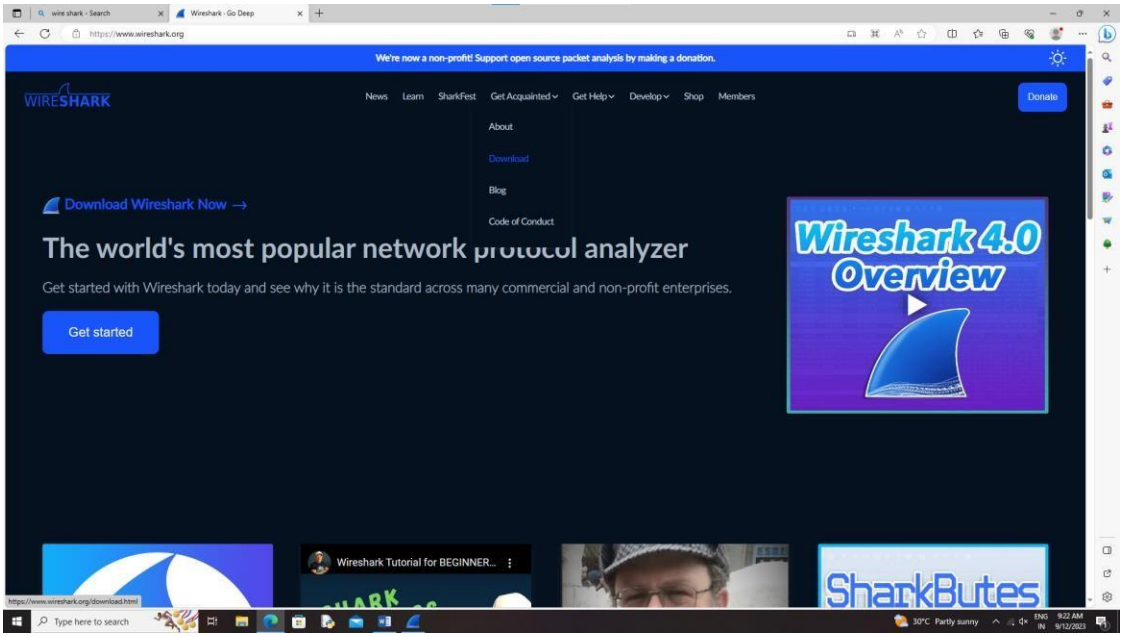
Result:

Thus, a hydra is successfully used to bruteforce linux server.

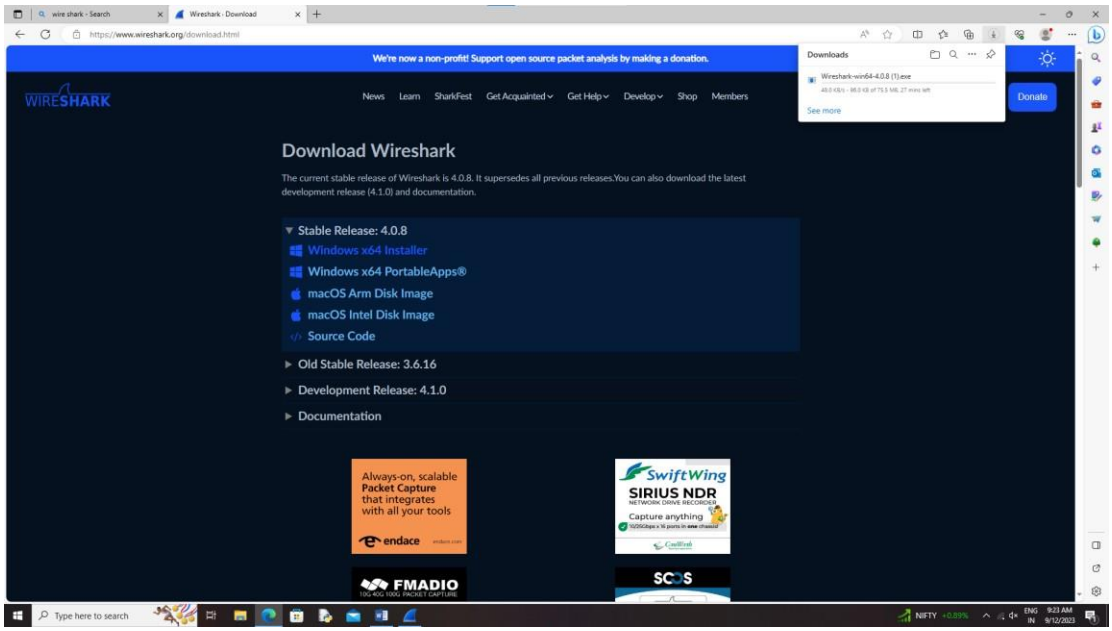
Ex 10 **View and capture network traffic using Wireshark**

AIM: To view and capture network traffic using Wire shark.

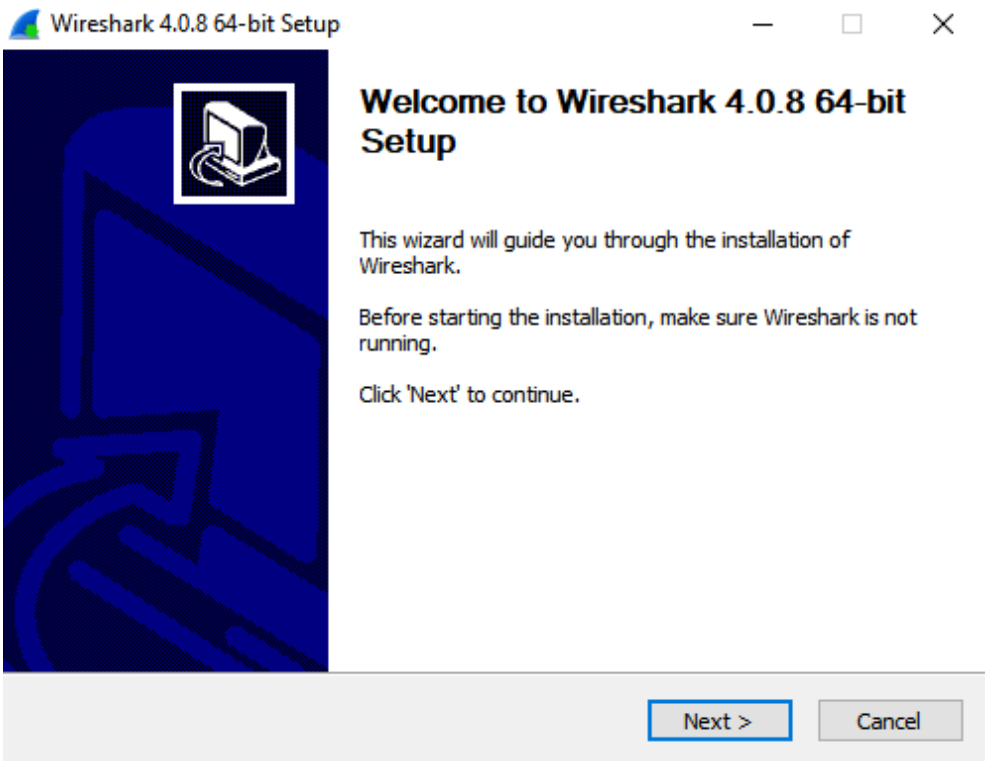
Download and install Wire shark from https://www.wireshark.org.

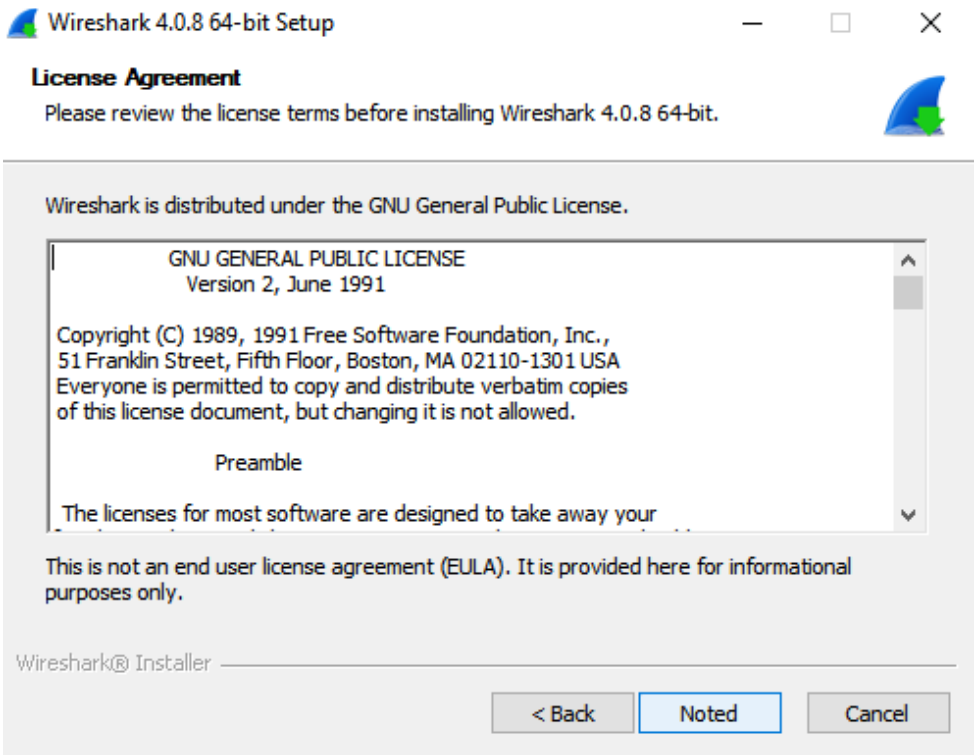


From Downloads section choose the appropriate installer depending upon your operating system.

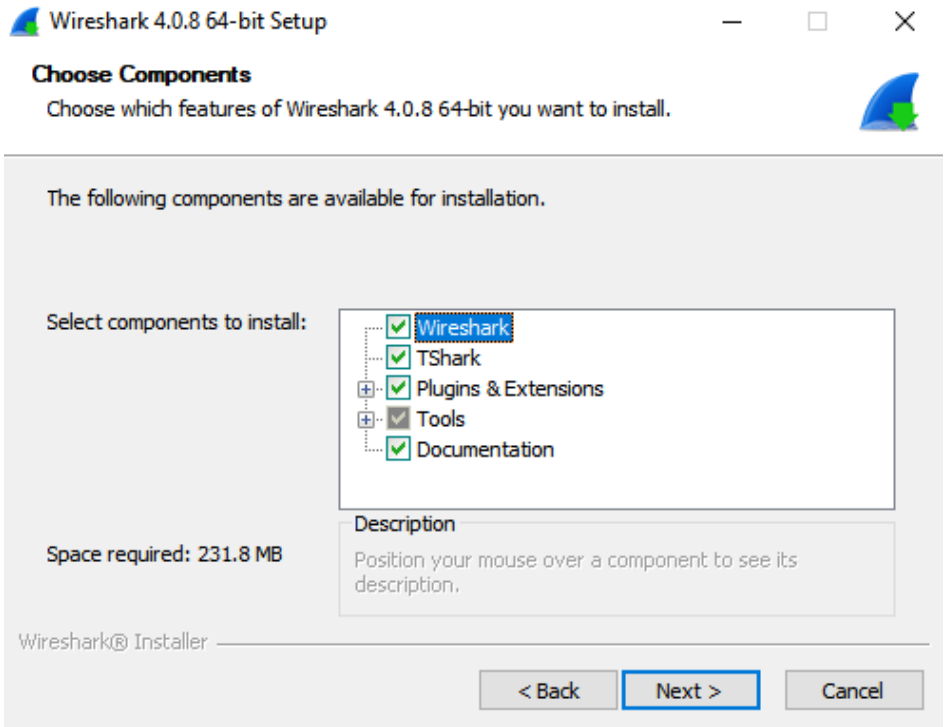


Run the Wire shark tool

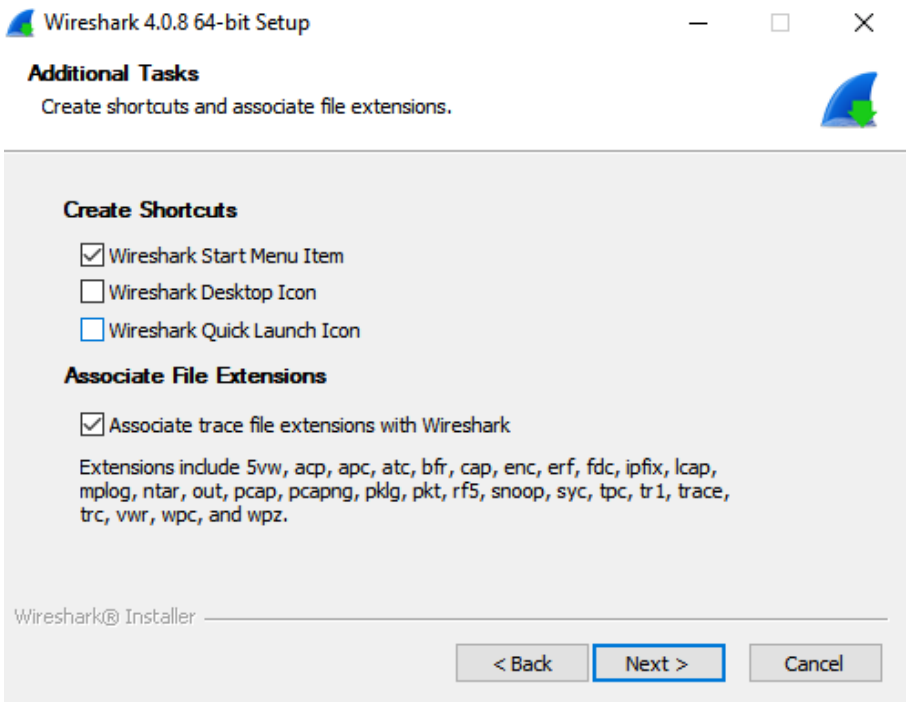




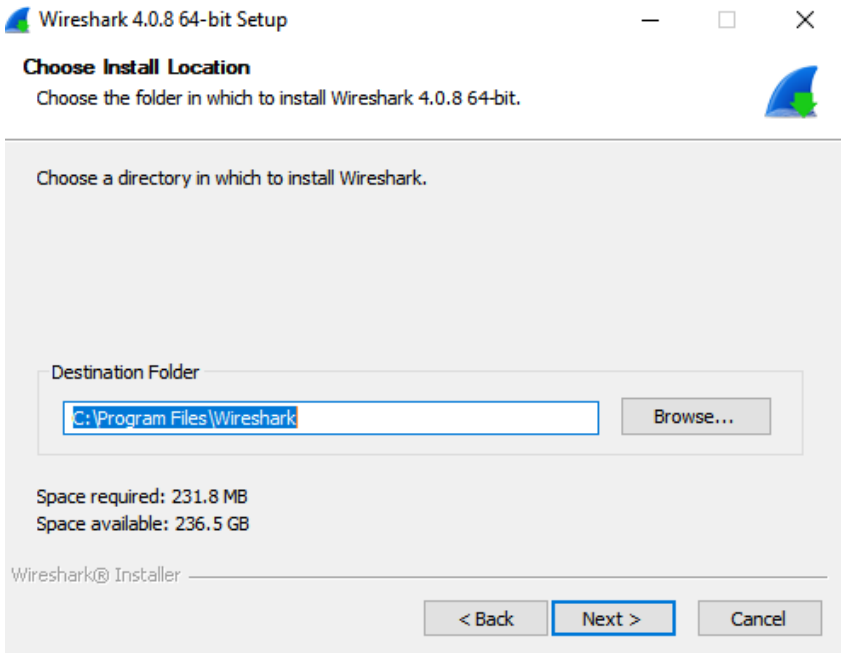
Check whether all the components in the drop down menu are marked.



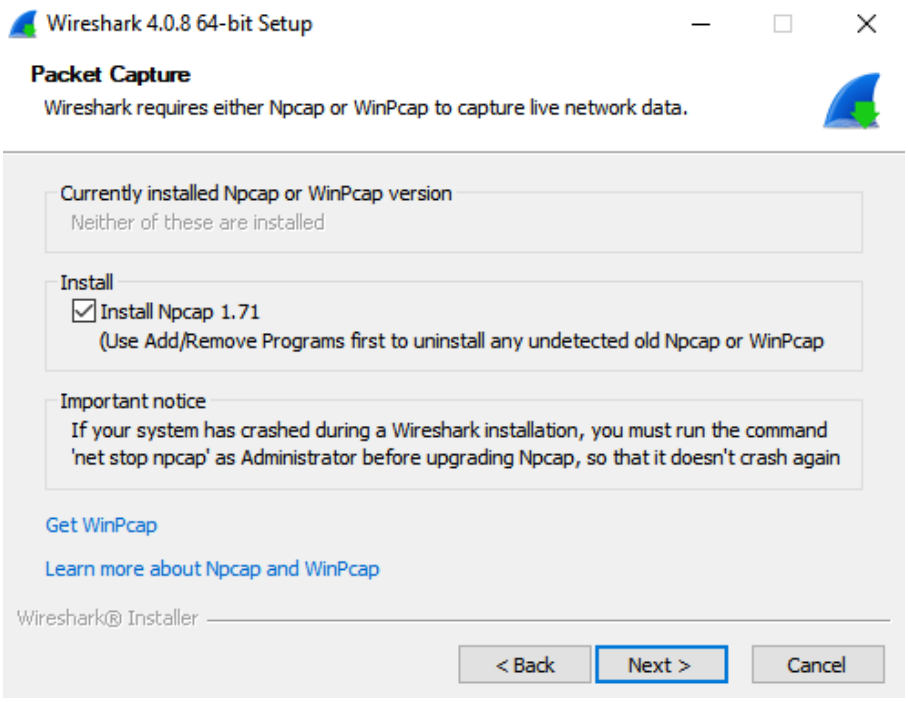
Select the appropriate shortcuts you and check whether "Associate trace file extension with Wire shark."



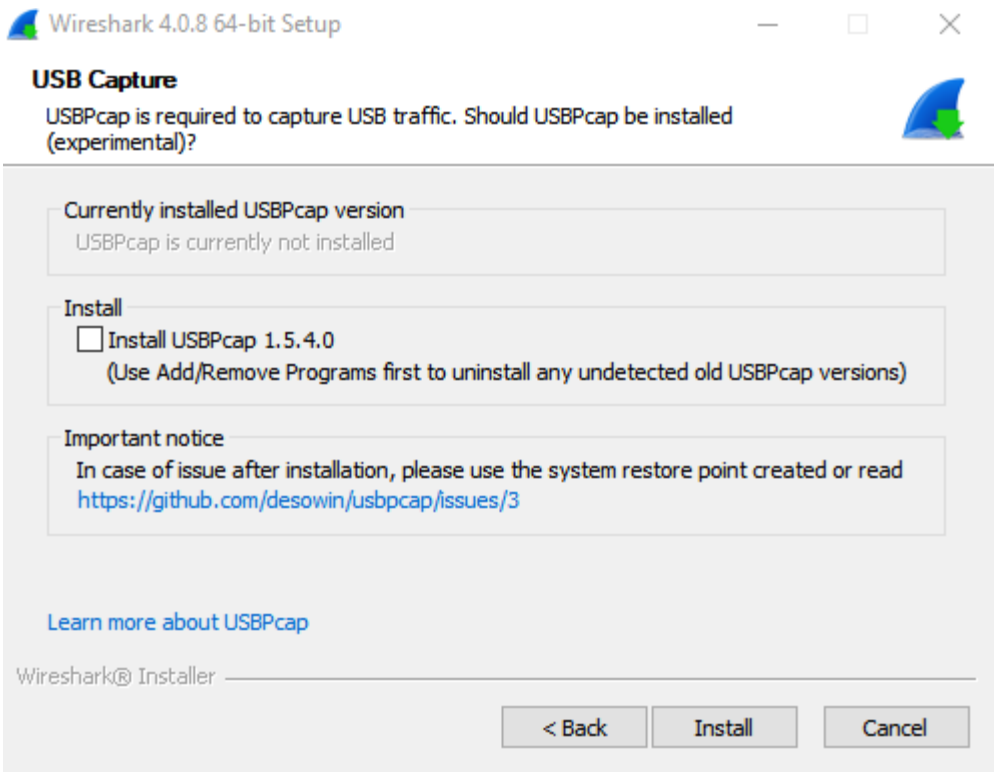
Select the Destination folder where you want to install the wire shark tool

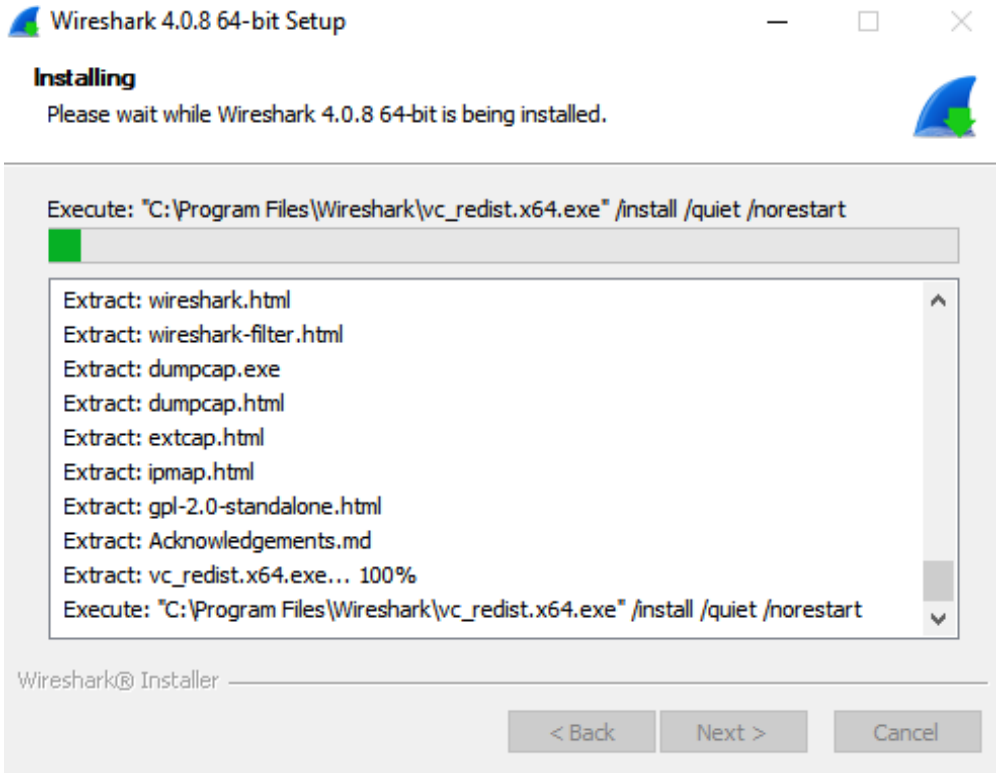


Check whether “Install ncap” is selected as that plays a major role in capturing live data network.

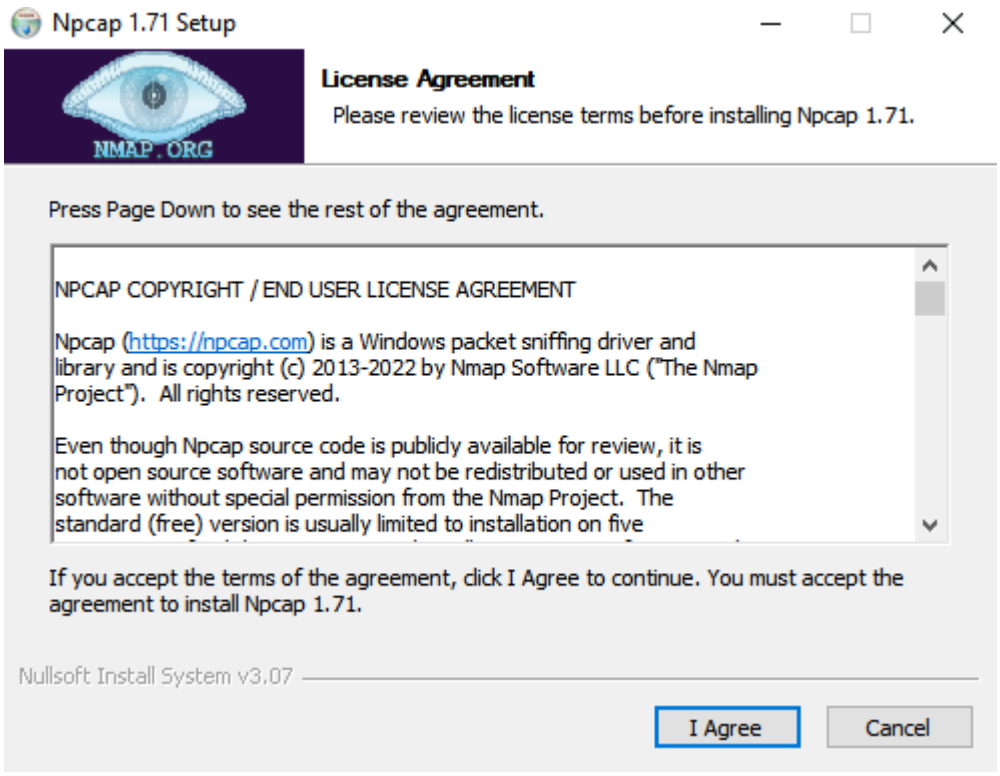


USBcap is optional as it captures network traffic via USB. So leave I unmarked

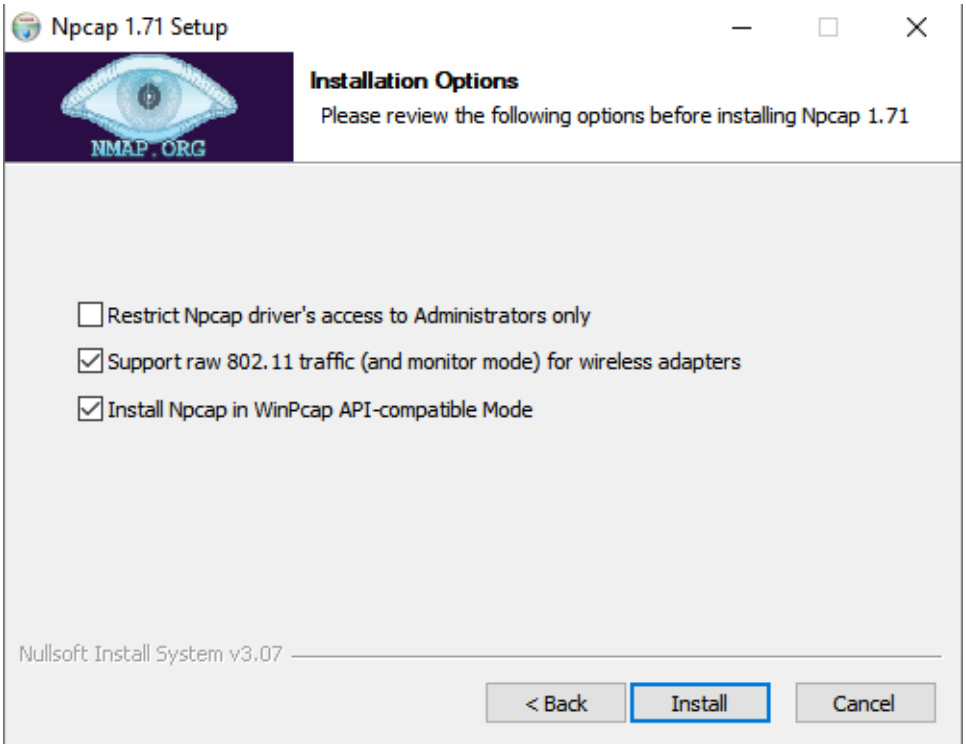


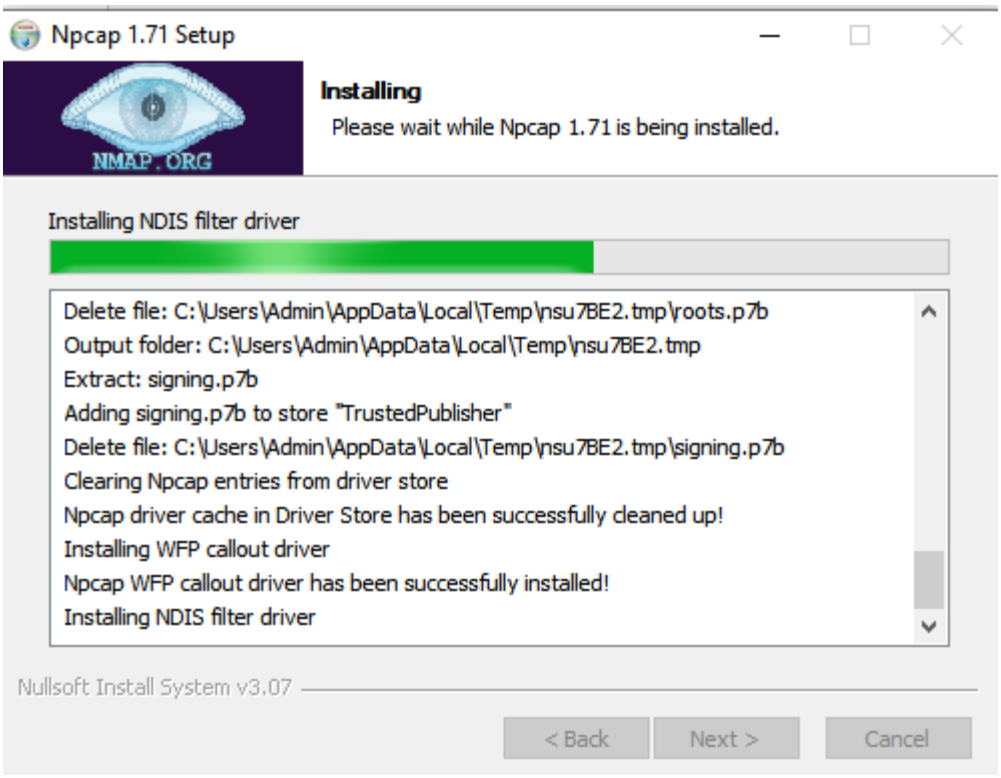


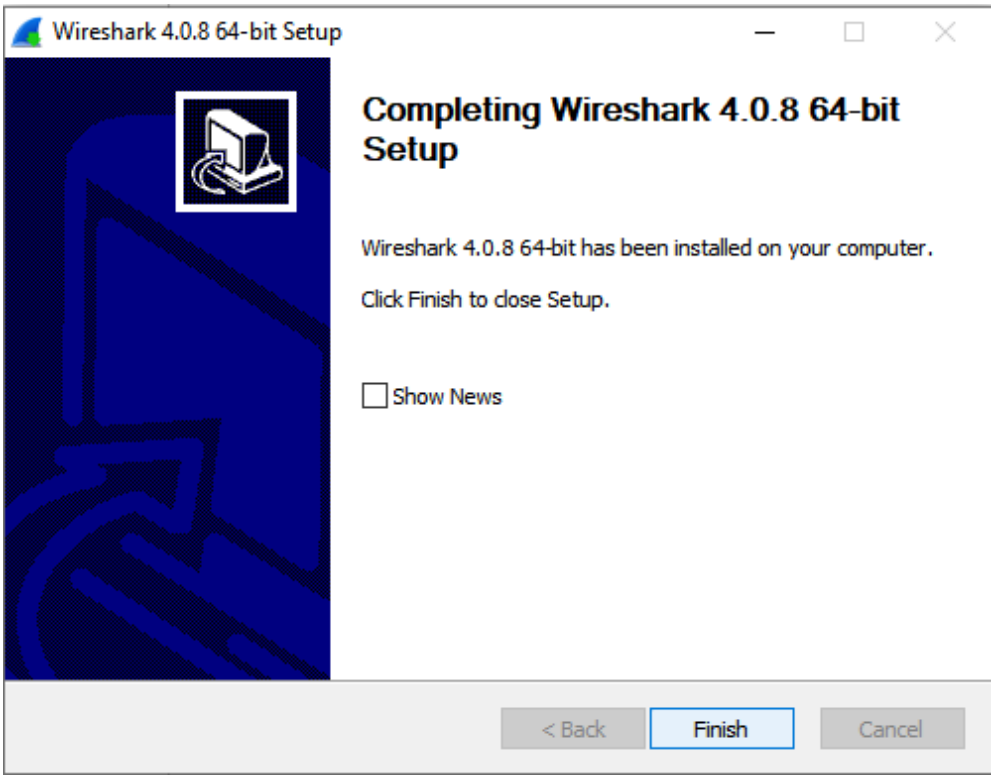
Follow The on-screen instruction to install Ncap



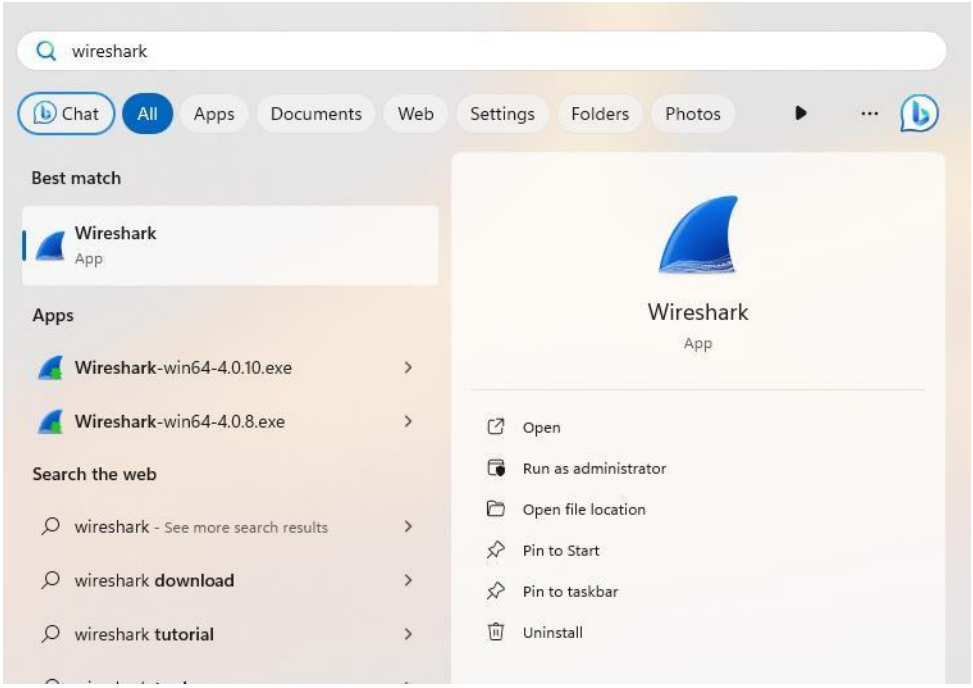
Make sure that the last two boxes are marked. The click on “install”.



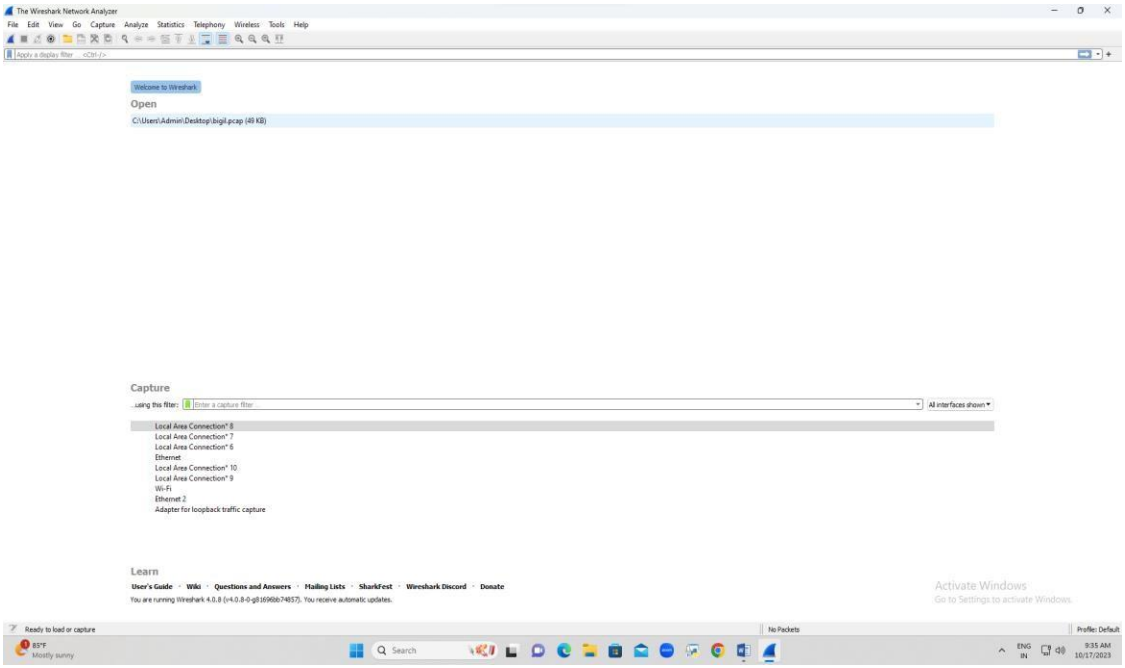

Npcap 1.71 Setup
NMAP.ORG
Installing
Please wait while Npcap 1.71 is being installed.
Installing NDIS filter driver
Delete file: C:\Users\Admin\AppData\Local\Temp\nsu7BE2.tmp\roots.p7b
Output folder: C:\Users\Admin\AppData\Local\Temp\nsu7BE2.tmp
Extract: signing.p7b
Adding signing.p7b to store "TrustedPublisher"
Delete file: C:\Users\Admin\AppData\Local\Temp\nsu7BE2.tmp\signing.p7b
Clearing Npcap entries from driver store
Npcap driver cache in Driver Store has been successfully cleaned up!
Installing WFP callout driver
Npcap WFP callout driver has been successfully installed!
Installing NDIS filter driver
Nullsoft Install System v3.07
< Back
Next >
Cancel


Wireshark 4.0.8 64-bit Setup
Completing Wireshark 4.0.8 64-bit Setup
Wireshark 4.0.8 64-bit has been installed on your computer.
Click Finish to close Setup.
Show News
< Back
Finish
Cancel

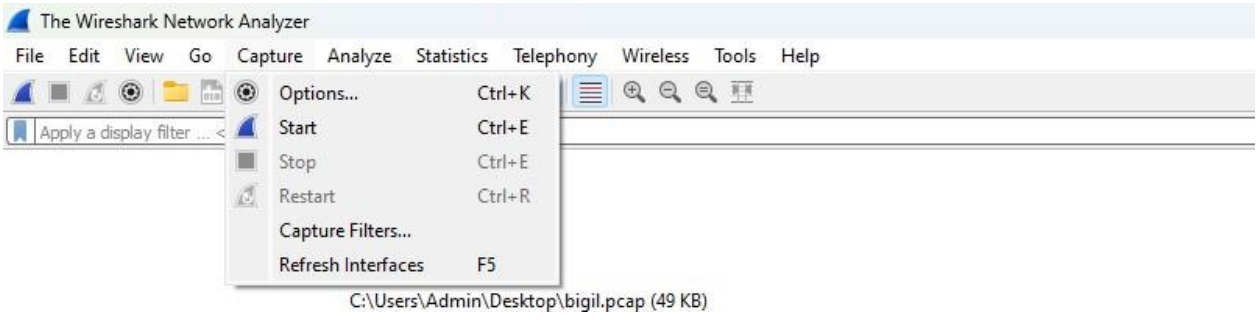
Open WireShark



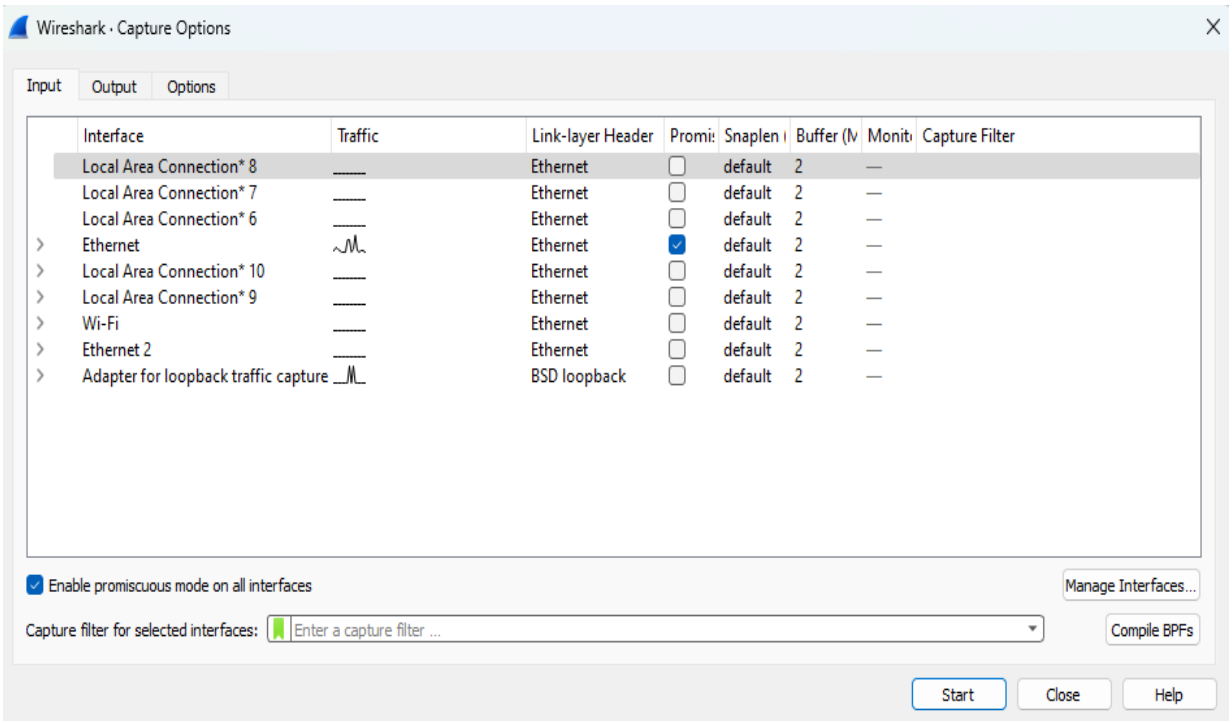
The below photo depicts the UI of the Wireshark. It shows the status of the network connections which are active.



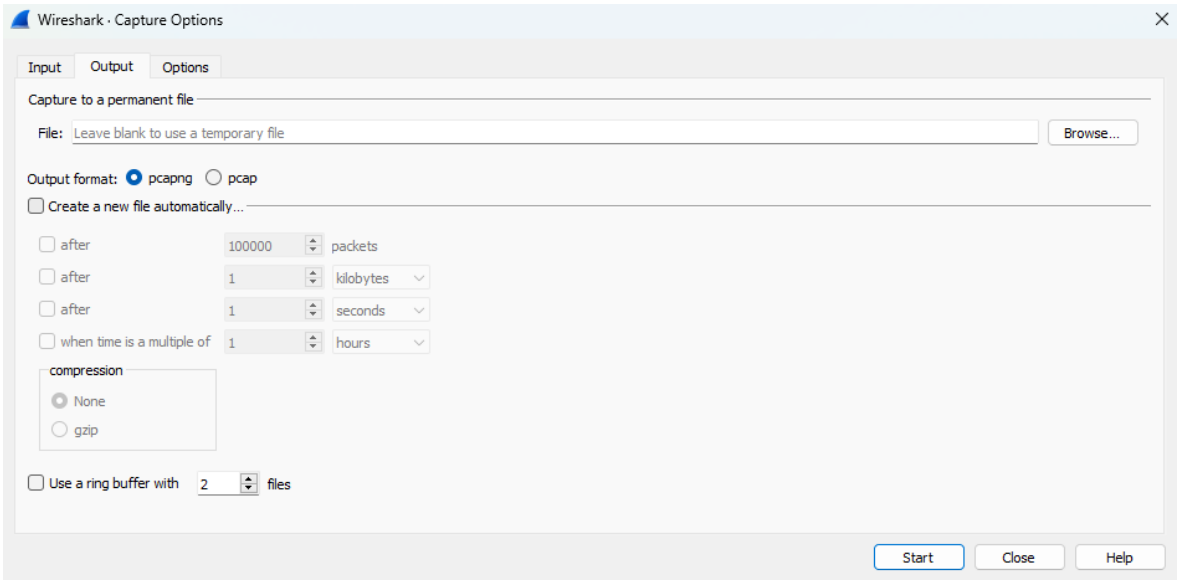
On the above, select "capture -> options".



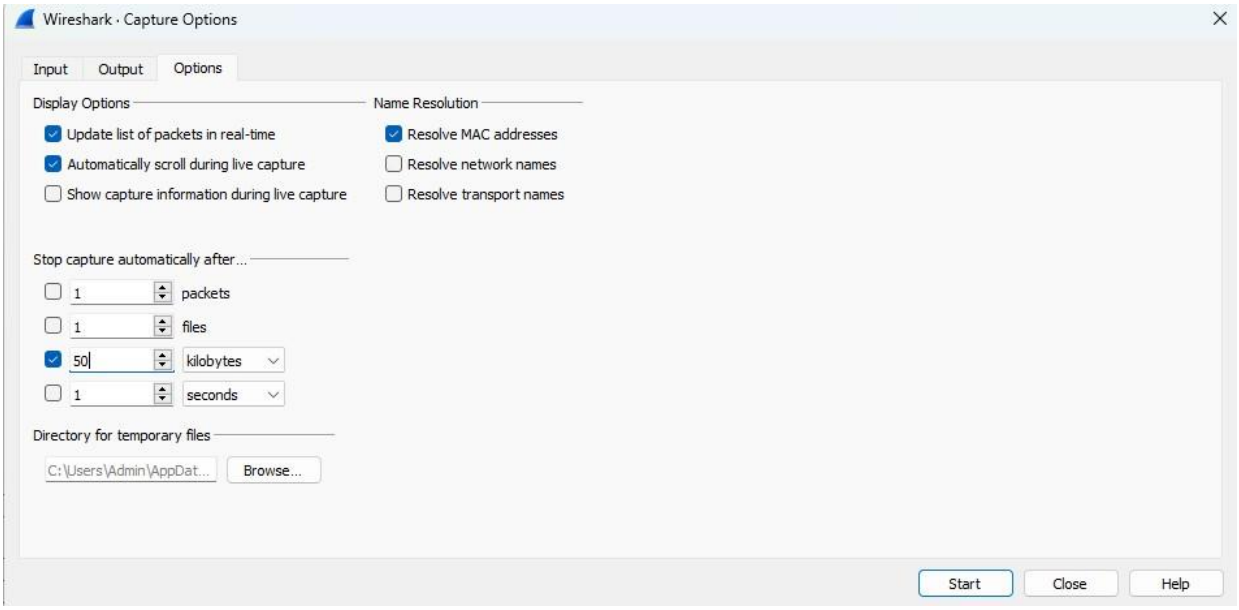
It redirects to the new window. Under the "input"elect the network interface you wish to use. Make sure that the selected interface is active.



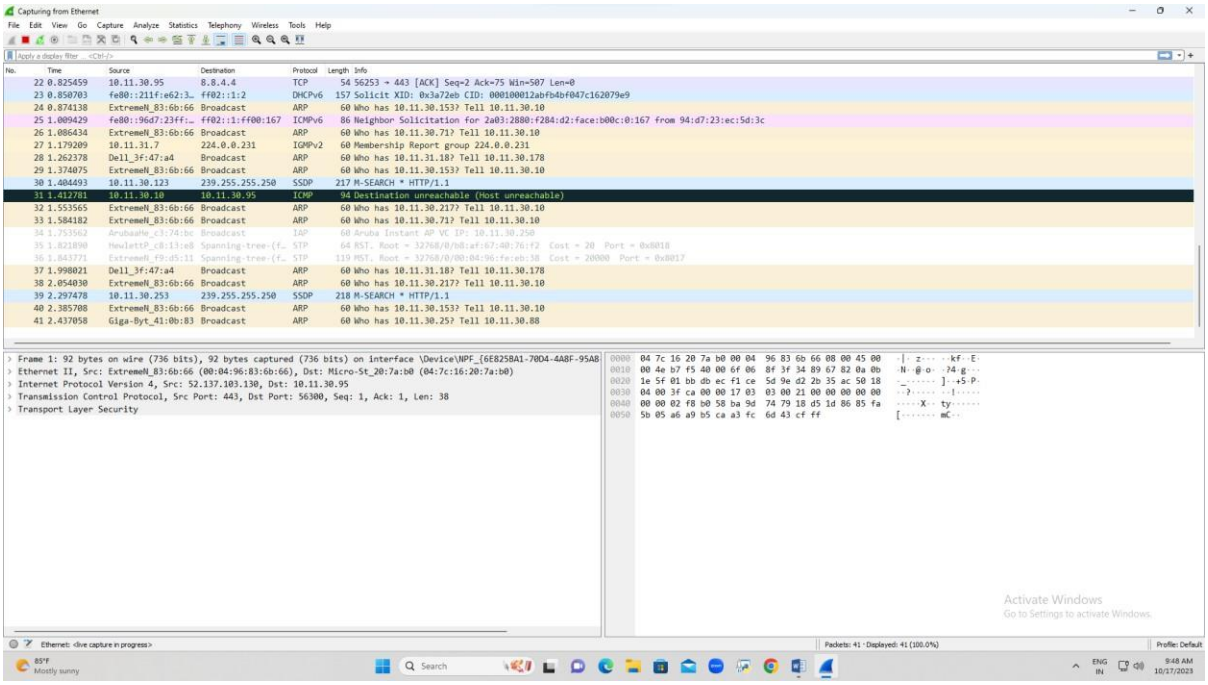
Under the "output" men, select the output file format. It is optional to select "create a file automatically" such that it creates a new file when selecting the limits.



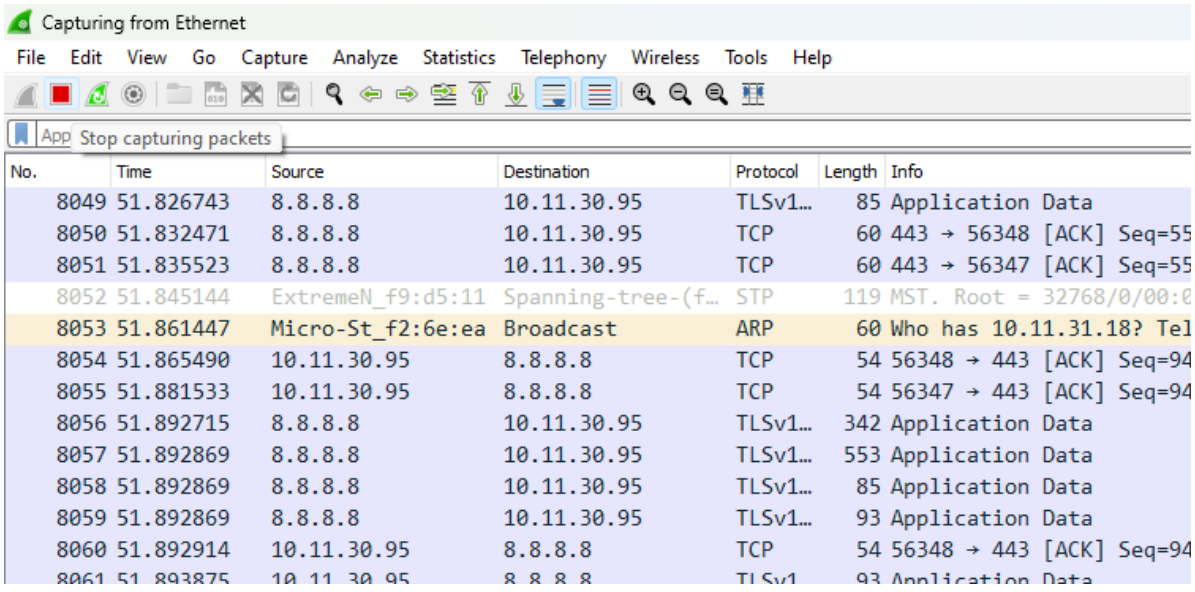
Under the output folder, make sure that you select 1st and 2nd in display option and only 1st in name resolution. Stop capturing file is optional as it stops until it reaches the limit. Now clock on "start" to capture the packets.



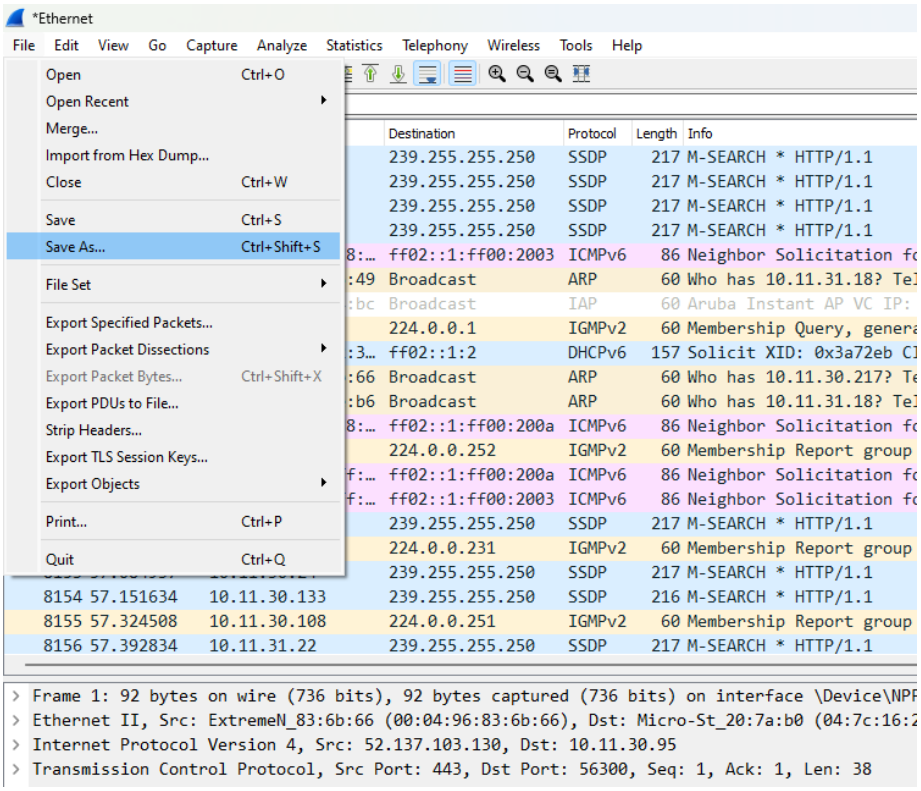
Now Wireshark starts to capture the packets. It monitors the network activity

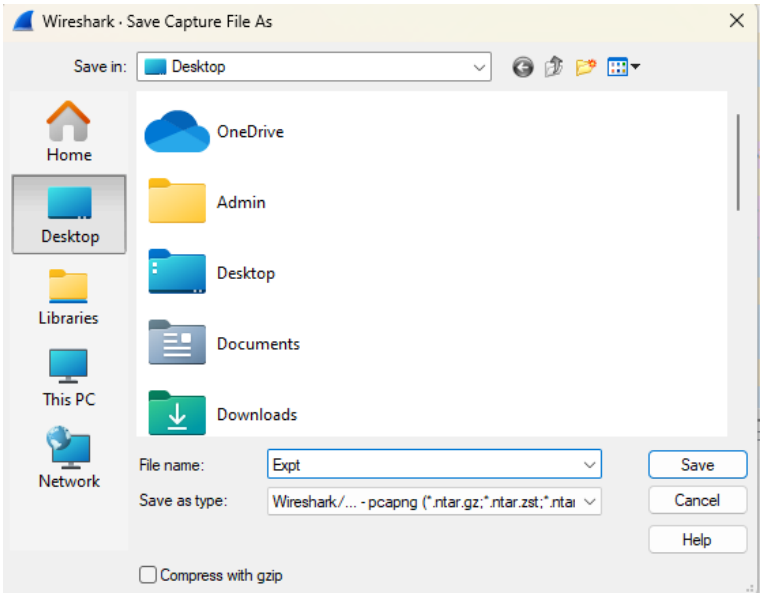


If you want to stop the capture, click on the square box to stop packet capture



To save the packet capture, select “file ->save as” and select the destination folder and name the file and save it.





Result:

Thus, the packets are captured using Wireshark tool and the captured packets has been reviewed.