**Ethical Hacking Course**

**(MINOR PROJECT)**

**Name-** *Shailesh Mallick*

**Name of the Instructor-**

Mohsin Quresh

**Scopes**

* **Setting Up the Labs.**
* **N-map Scanning**
* **Checking the Vulnerability and Exploitation**

**Setting Up The Lab**

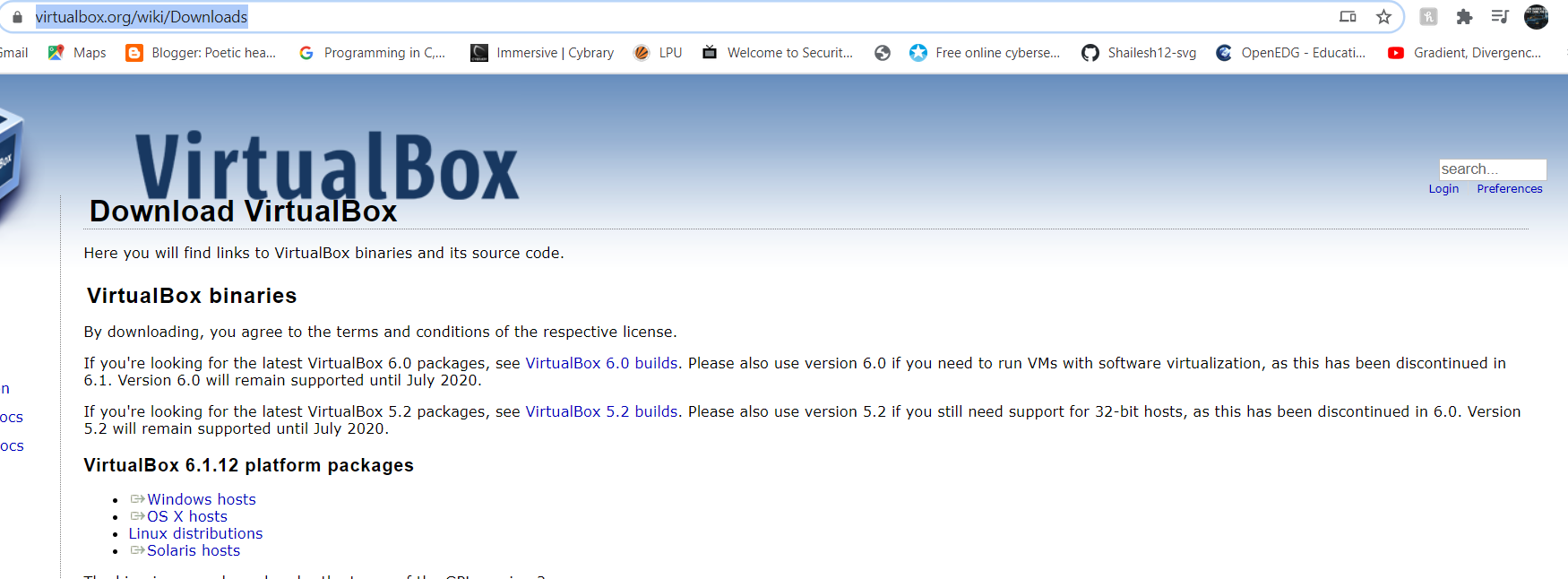
* For any penetration testing first of all we need to set a Lab.
* The lab can be set in two modes.They are:

(a) *Live mode*

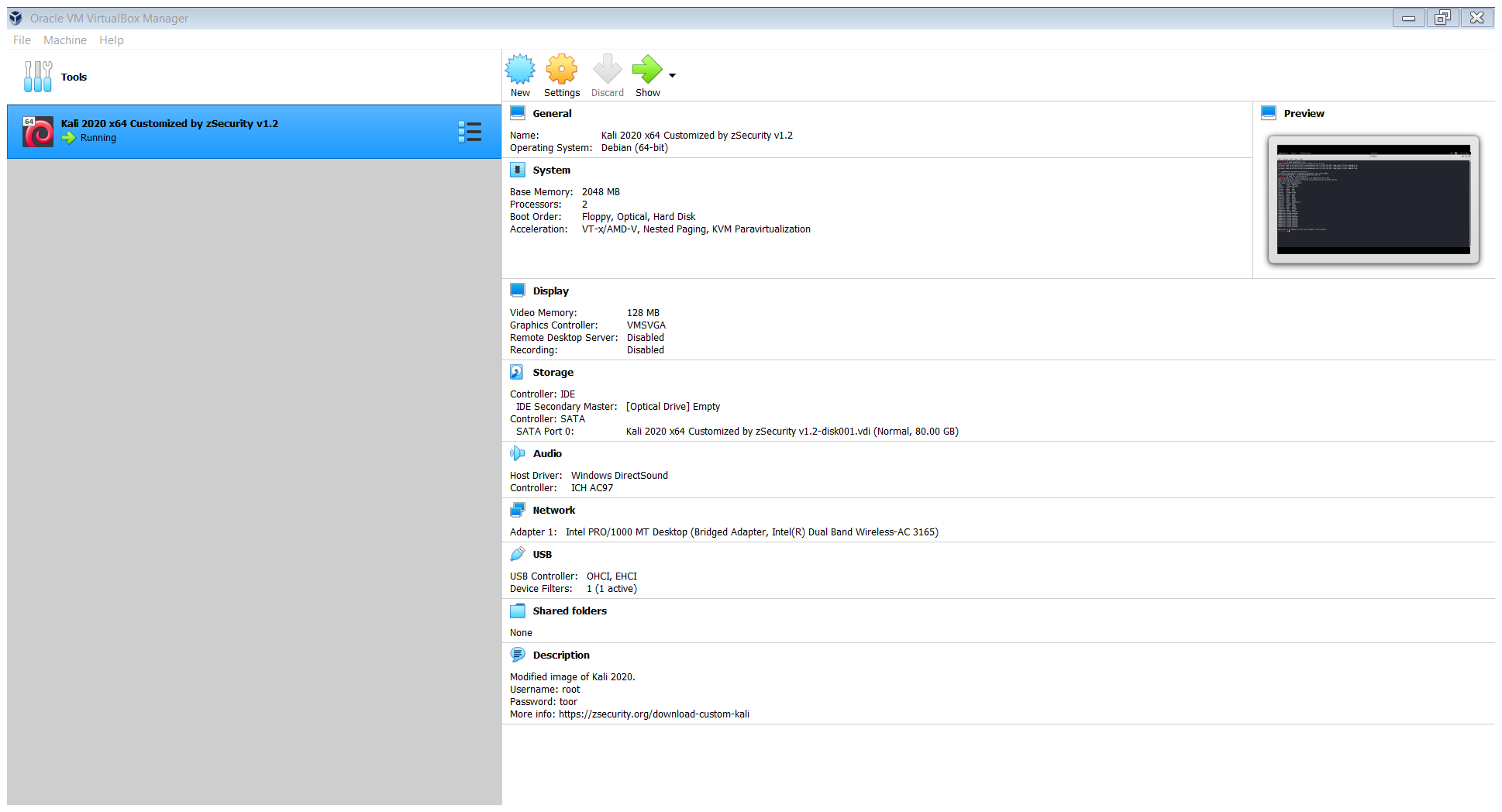
(b) *Virtualization mode*

* In the case of the live mode the testing can be done by using the OS in live.
* In the Virtualization mode we have to install Virtual Box in the host machine. The Download Link is given below.
* Download link is:

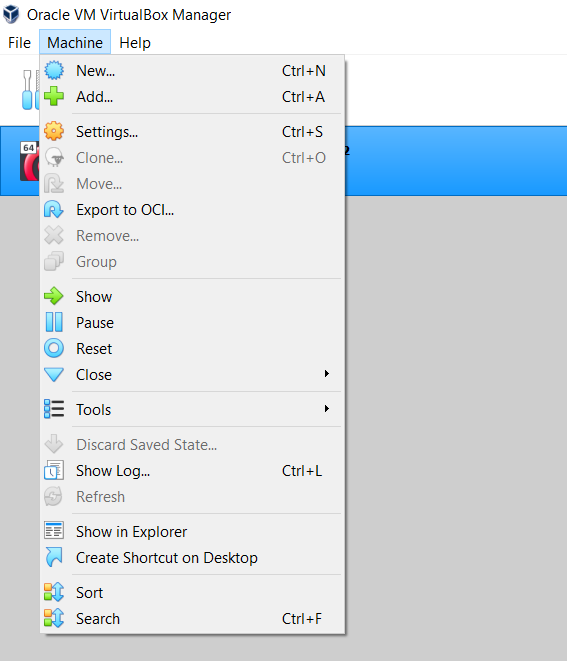
https://www.virtualbox.org/wiki/Downloads

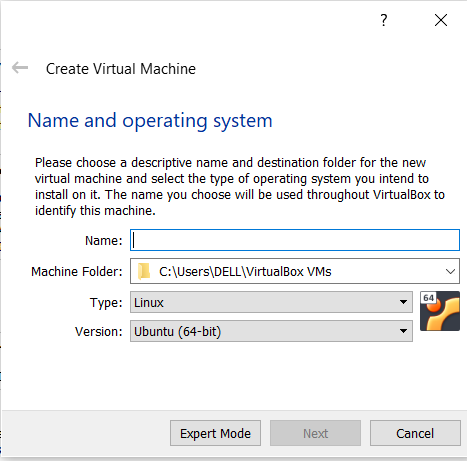
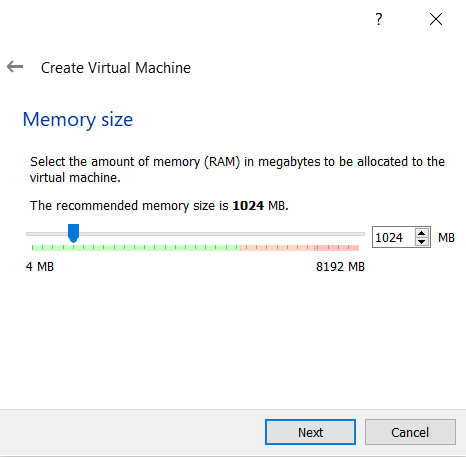


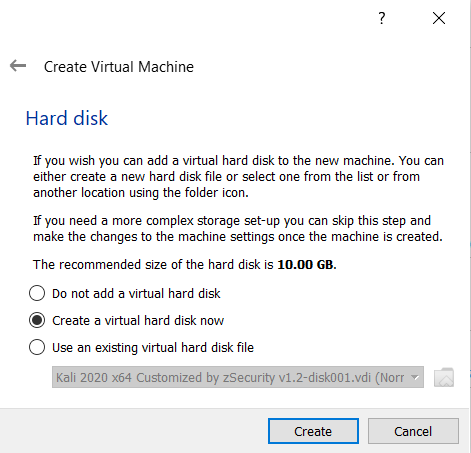
* For setting up the testing lab, first we have to open the virtual box.
* After opening the Screen looks like this.



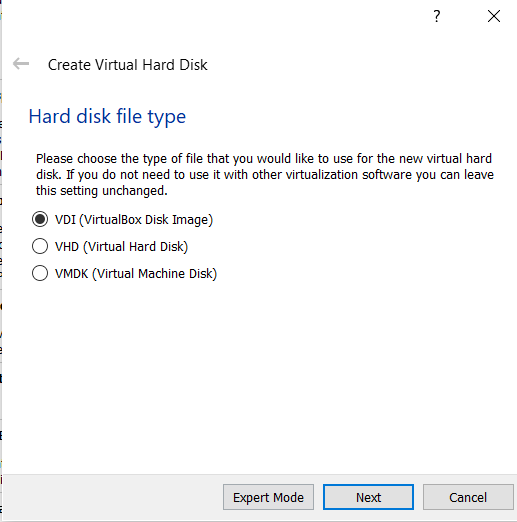
* Next we have to click on machine and the screen looks like this and Click on New.



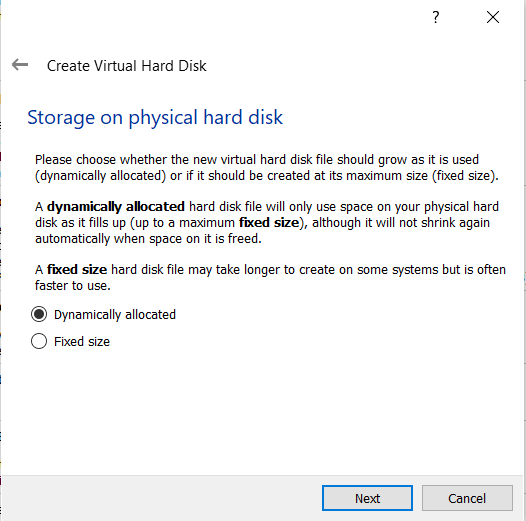
* Then the screen will look like this.
* Fill the name of lab as per your choice .Then Select Linux in type and Ubuntu(64-Bit)in version and click on next.
* Then the screen will look like this.
* Allocate the memory (RAM) not less than 2GB and click Next. The Screen will be like this:



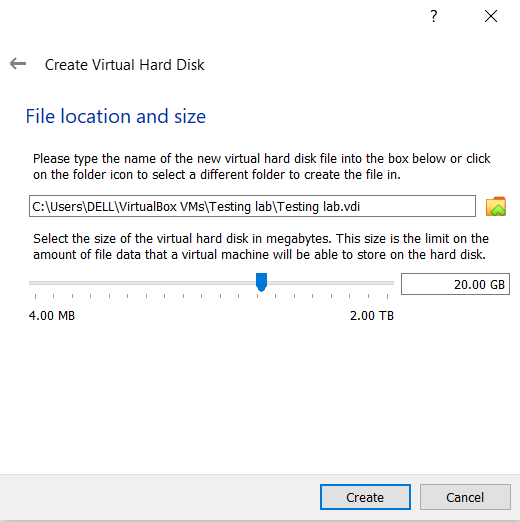
* Then Select on create a virtual hard disk now and Click on Create. The screen will look like this.

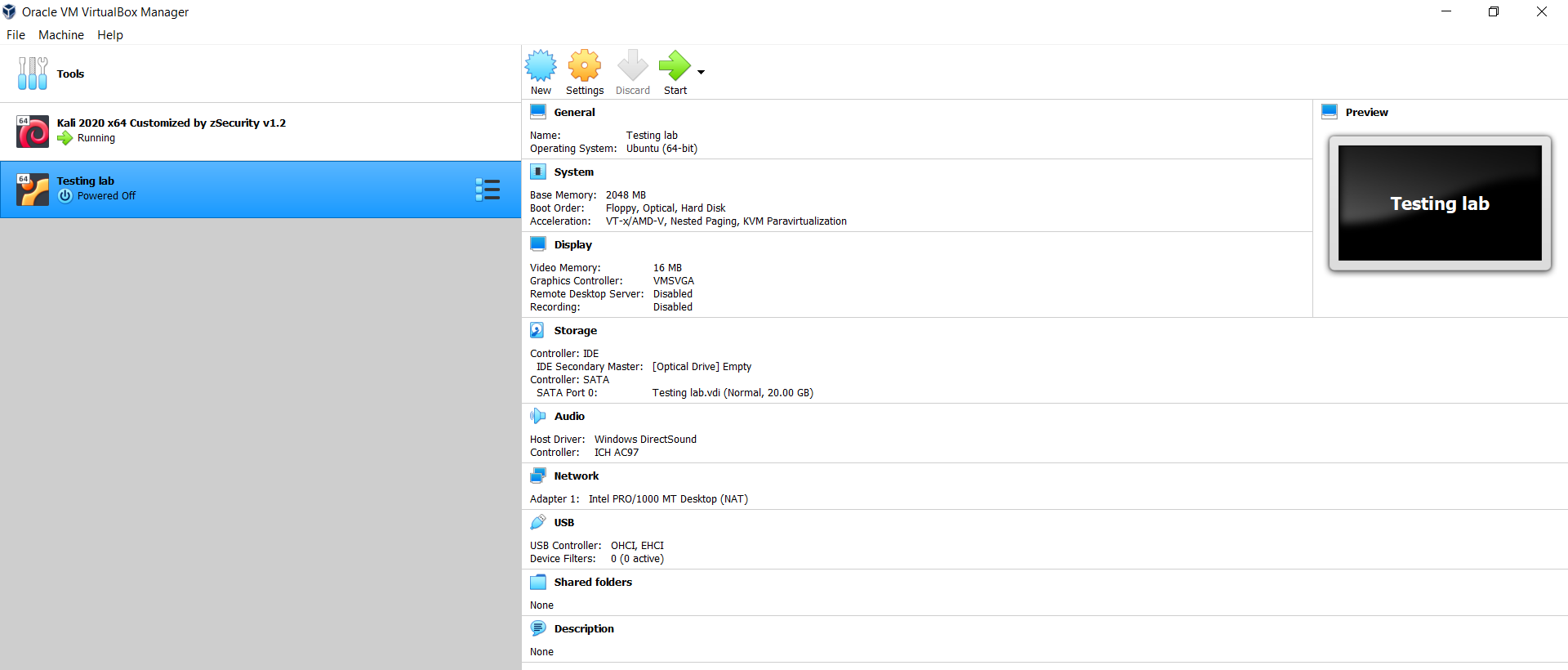


* Click on VDI (Virtual Disk Image) and click next



* Then allocation of Size upto 20GB and Click On create.



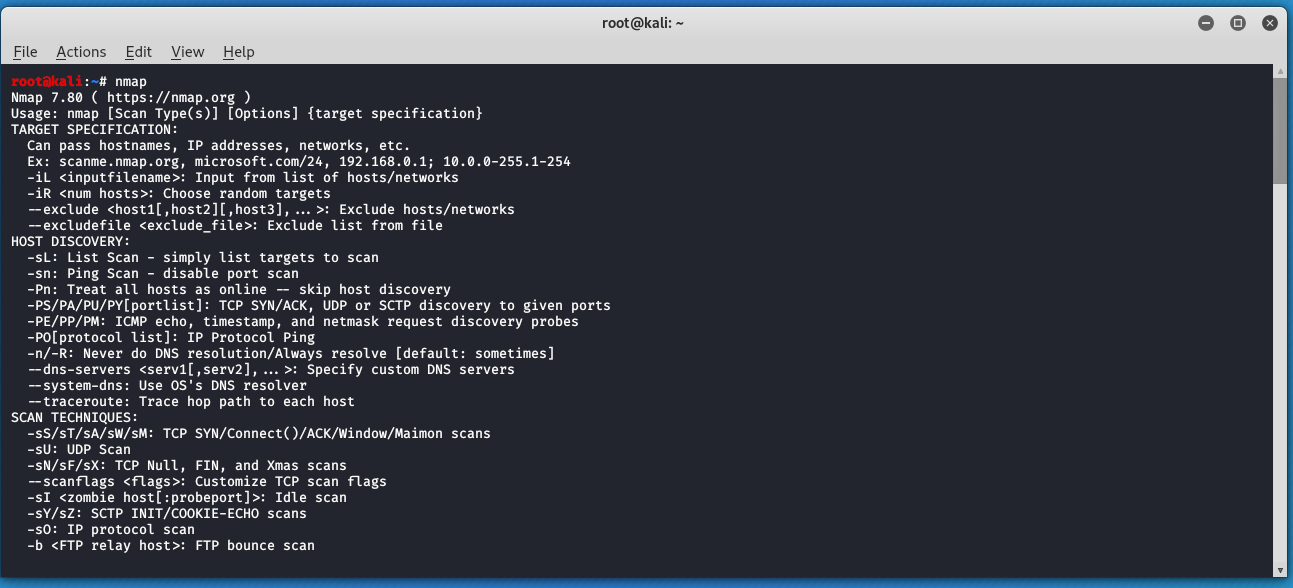
* Hence Lab is created just Add Iso file in that configure it and We are ready.

**Nmap Scanning**

1.Login As Kali-Linux

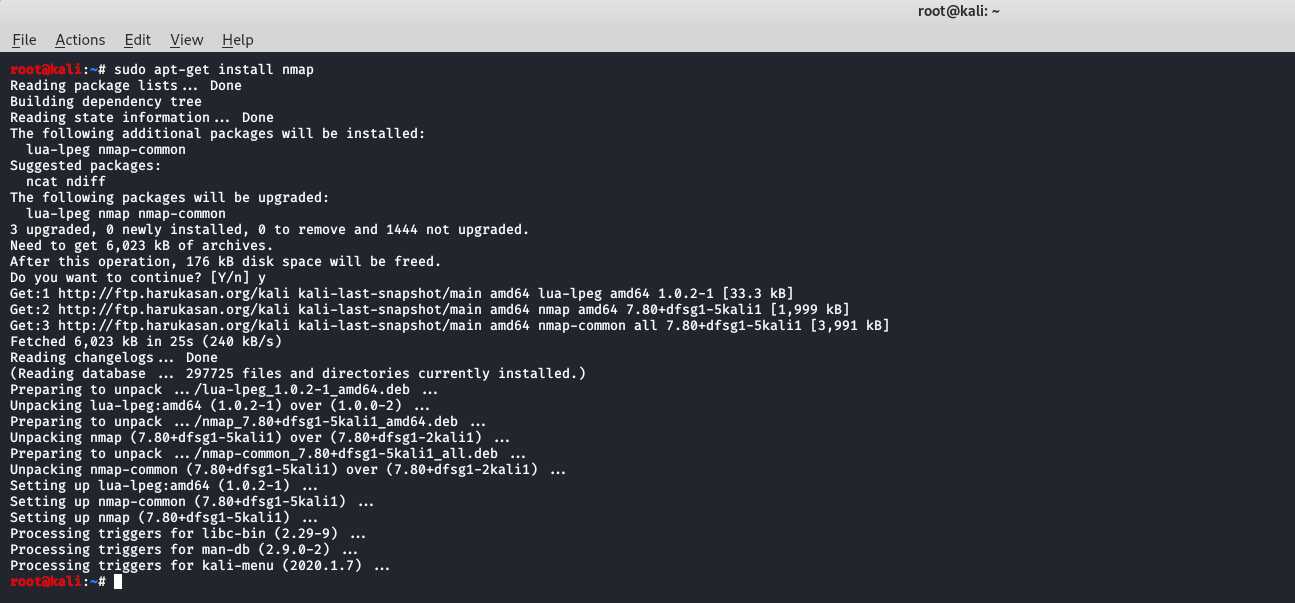
2.Open the Terminal For Checking THE nmap

->type nmap



If this type of Screen Is there it means That Nmap is installed in your Kali -OS. Otherwise for the Installation of Nmap

3.Type: - sudo apt-get install Nmap



* And the Nmap is installed in Kali Linux OS Successfully.

**Basic Commands For Scanning**

* 1.Scanning remote Hosts and Listing Open Ports

* ->This technique is used to Scan the Hosts in live System
* \_>Open the terminal
* \_>To Check the host is alive or not type\_> ping scanme.nmap.org (Example) and if you receive icmp packets its means that Host is alive.

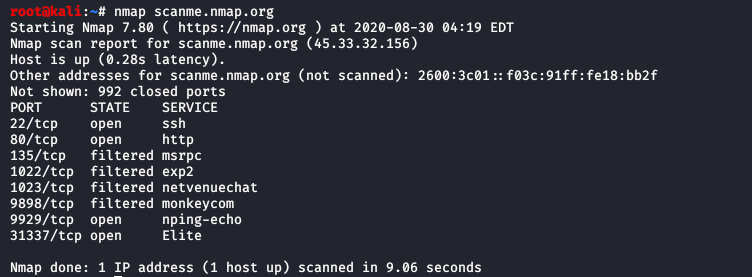
PING scanme.nmap.org 
File Actions Edit View Help 
ping scanme.nmap.org 
time-269 
time-268 
icmp_seq• 
icnw_seq• 
time-269 
time-269 
icmp_seq• 
icnw_seq• 
icmp_seq 
icmp_seq 
icmp_seq• 
icnw_seq• 
(&5.33.32.156) 56(84) bytes of data. 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
64 
16 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
from 
. nmap.org 
s canme 
Scanme.map.org 
scanme.map.org 
scanme.map.org 
scanme . nmap.org 
scanme.nmap.org 
Scanme.map.org 
scanme.map.org 
scanme.map.org 
scanme . nmap.org 
scanme.nmap.org 
Scanme.map.org 
scanme.map.org 
scanme.map.org 
scanme . nmap.org 
. nmap.org 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
(45 
.33.32.156): 
(45.33.32.156): 
.33.32.156). 
.33.32.156): 
(45.33.32.156): 
.33.32.156). 
.33.32.156): 
(45.33.32.156): 
.33.32.156). 
.33 
.33 
.33 
.33 
.33 
.33 
.33 
.32.156). 
.32.156): 
.32.156): 
.32.156): 
.32.156): 
.32.156): 
.32.156). 
• icmp_seq 
• icmp_seq• 
• icmp_seq• 
• icmp_seq• 
-I ttI;S8 
2 ttI=S8 
3 tt1•58 
tt1•58 
5 ttl;58 
6 ttl;S8 
7 ttI=S8 
8 tt1•58 
9 tt1•58 
tine•268 ms 
time•268 ms 
time-268 ms 
tine•269 ms 
time•27ø ms 
ms 
-11 
-12 
13 
14 
15 
time-269 
time-269 
tttz58 time-268 
tt1•58 time•269 ms 
tt1•58 time.269 
time-271 
time-269 
15e85ms 
ms 
ms 
ms 
ms 
ms 
scannWnmap.org ping statistics 
packets transmitted, 16 received, 
packet loss, time 
rtt min/avg/max/mdev 268.347/268.9ø3/271.331/ø.726 ms 

* We can get the Ip address using ping eg:

PING — . 
icmp_seq 
net 
del ø3s15-in-f4. leiøø. net 
.217.167 
time -69.8 
.217.167 
217.167 
icmp_seq• 
dete3s15-in-f4.1e1eø. net 
icmp_seq 
del e3s15-in-f4. leieø. net 
icmp_seq; 
.217.167 
6ø.9 
icmp_seqz 
.217.167 
icmp_seq 
dete3s15-in-f4. leleø. net 
ping — . google.com 
google.com (172.217. 
167.4) 56(84) bytes of 
data . 
64 
64 
64 
64 
64 
64 
64 
64 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
bytes 
from 
from 
from 
dete3s15 
from dele3s15 
from 
from 
dete3s15 
from 
from 
dele3s15 
from dete3s15 
from 
-f4.1e1eø 
. net 
-f4.1e1eø. 
net 
leleø. net 
-f" . leieø 
. net 
-f4.1e1øø. 
net 
(172 
(172 
(172. 
(172 
(172 
(172.217.167.4): 
(172.217.167. 
(172.217.167 
(172.217.167. 
.4): icmp_seq; 
.4): icmp_ 
. 4): icmp_seq 
seq- 
4): 
4): 
(172.217.167.4): icmp_seq. 
•1 ttI•117 
3 ttt 
4 ttt• 
•5 ttI•117 
-6 ttI-117 
7 ttl= 
8 ttt 
•9 tt1•117 
117 
-117 
117 
117 
-117 
time 
time- 
time. 
time - 
time 
time• 
time•61.3 ms 
time-6ø.8 ms 
-62.1 
=6ø.S ms 
60.9 ms 
61.1 ms 
ms 
ms 
ms 
lø tU•117 time.6e.6 ms 
—.google.con ping statistics 
packets transmitted, 10 received, OX packet toss, tine 9133ns 
rtt min/avg/max/mdev • 6ø.453/61.865/69.8øe/2.681 ms 

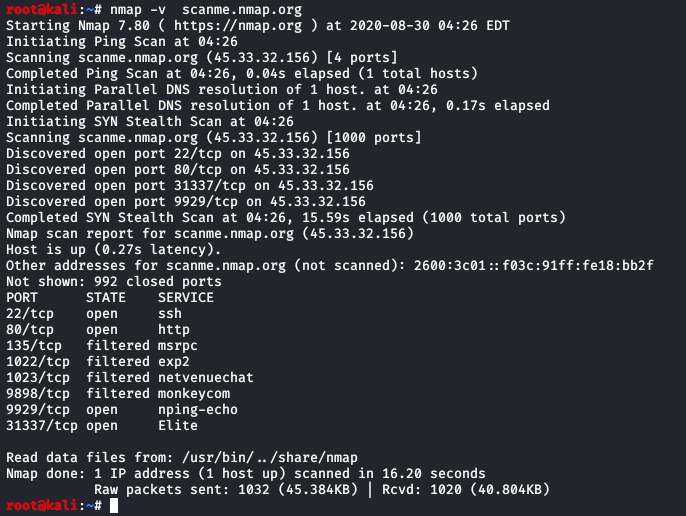
So now we can perform Our First Scan for scanme.nmap.org

->Just type nmap scanme.nmap.org



Screen clipping taken: 8/30/2020 1:54 PM

For The Backend Deep Information Just add -v nmap -v scanme.nmap.org

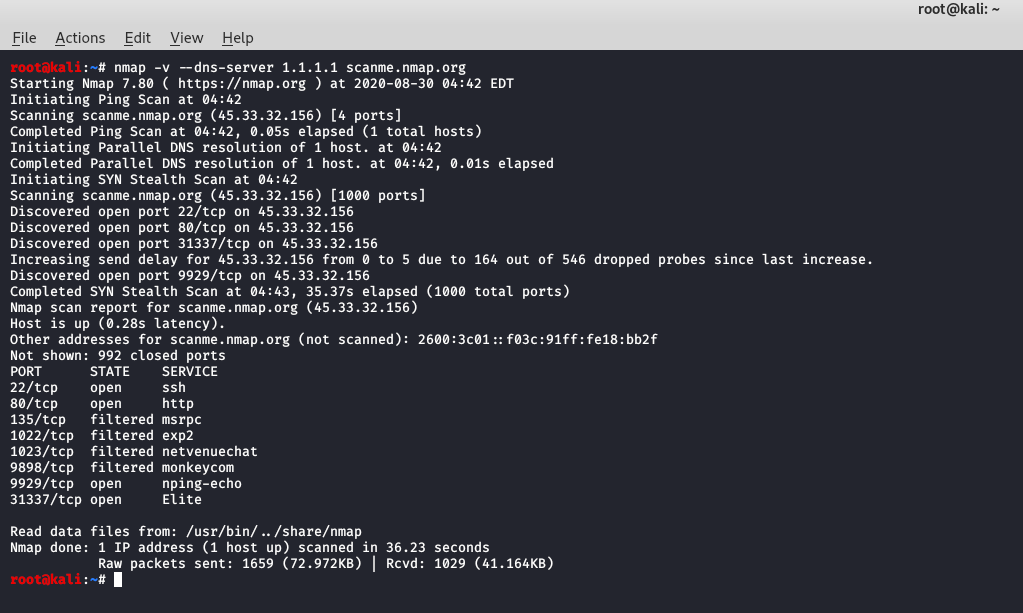


Screen clipping taken: 8/30/2020 1:56 PM

->Nmap uses DNS in order to convert the Host name to ip address for further Scan.

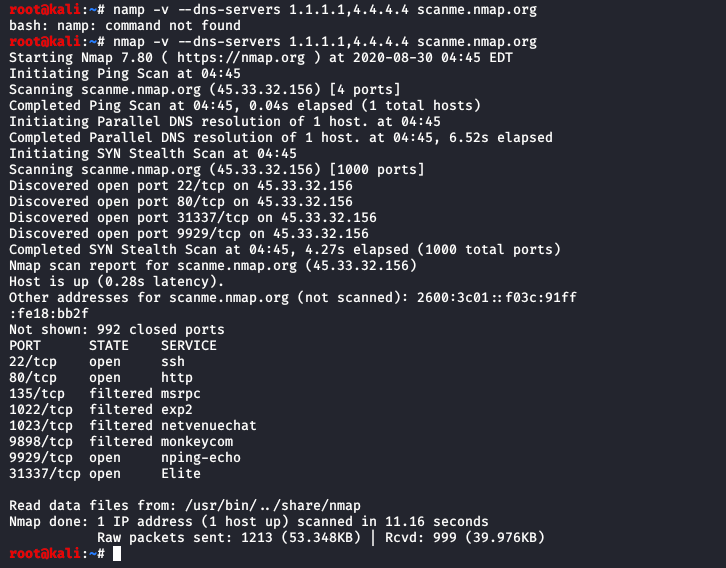
->DNS- is basically known As Domain Name Server.

->In order to change the Settings of DNs in kali Os type-> nmap -v --dns-servers 1.1.1.1 scanme.nmap.org



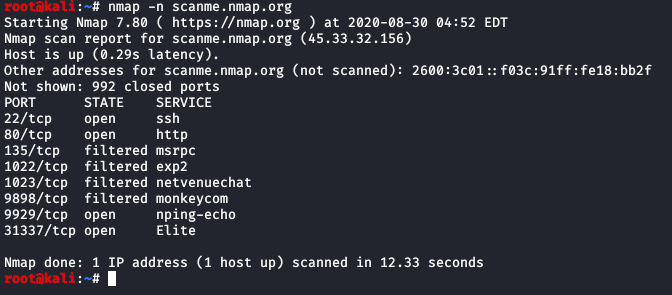
Screen clipping taken: 8/30/2020 2:16 PM

And for the Multiple Domain name Systems type-> nmap -v --dns-server 1.1.1.1,4.4.4.4 scanme.nmap.org



Screen clipping taken: 8/30/2020 2:19 PM

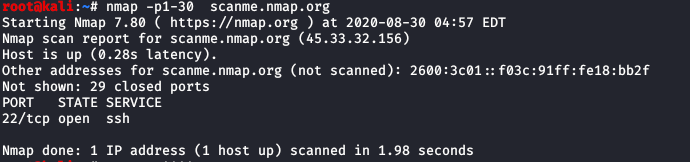
We can use reverse nmap scan by type\_> nmap -n scanme.nmap.org



Screen clipping taken: 8/30/2020 2:23 PM

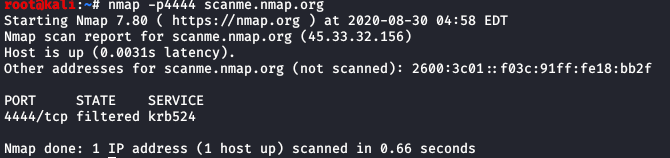
We can do Port Scaning Also….

Just type-> nmap -p1-30 scanme.nmap.org



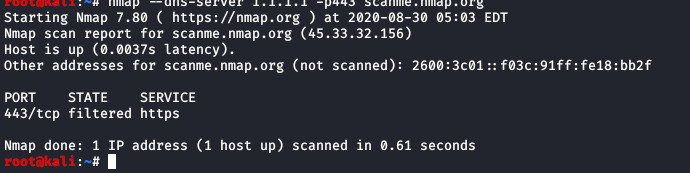
Screen clipping taken: 8/30/2020 2:29 PM

Or we have to Scan for a specified Ports..



Screen clipping taken: 8/30/2020 2:30 PM

For, Getting Dns server to scan the port type nmap --dns-server 1.1.1.1 -p4444 scanme.nmap.org

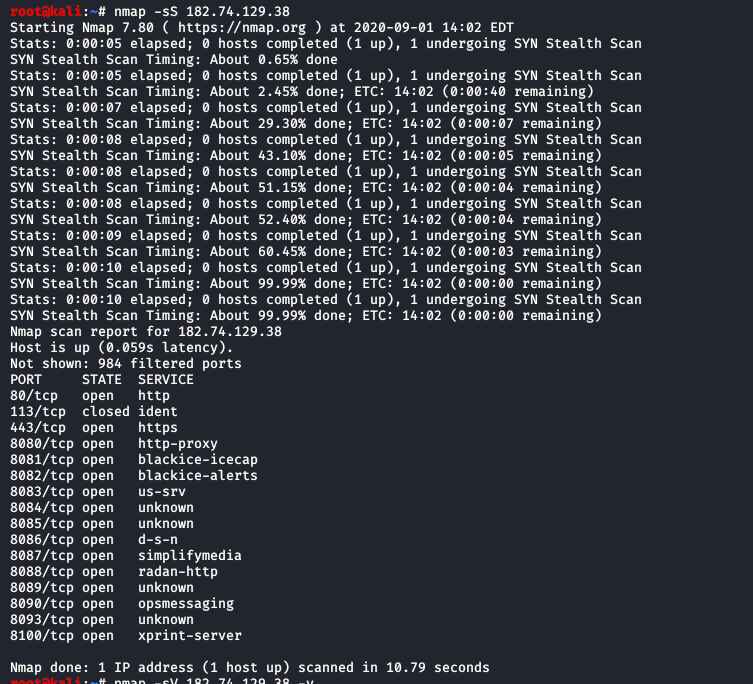


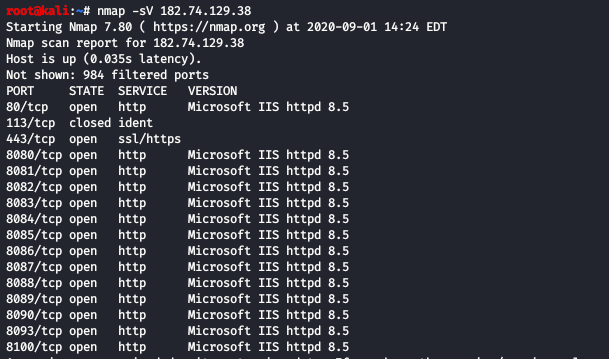
Screen clipping taken: 8/30/2020 2:34 PM

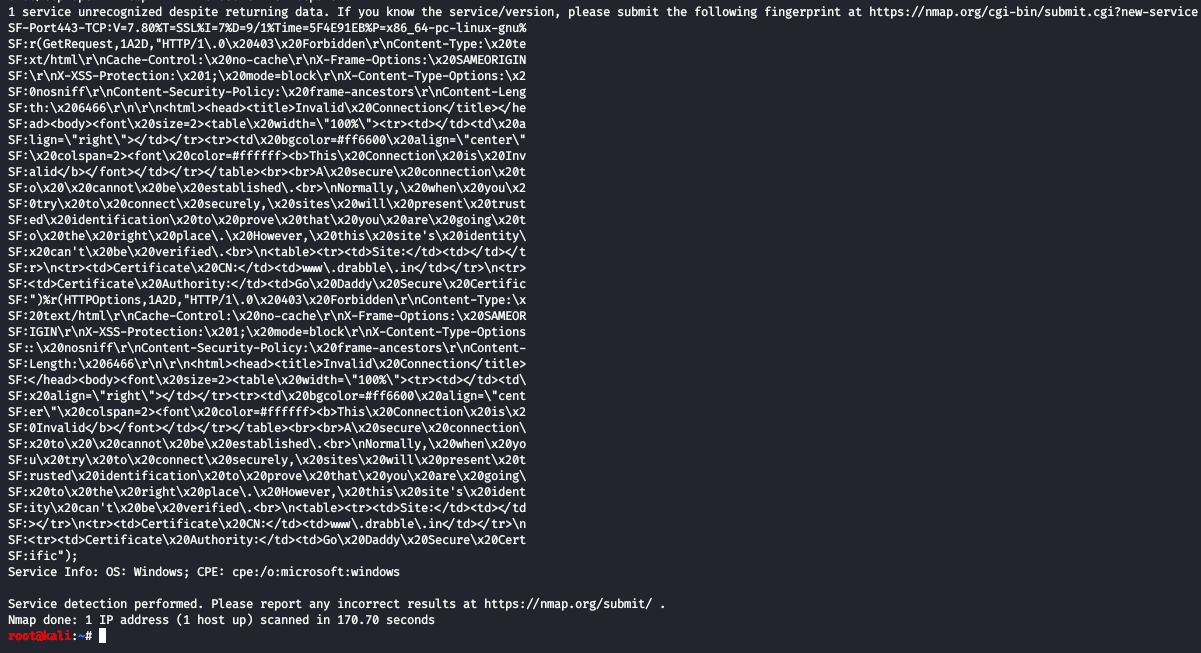
**Checking Of The Vernuablity For A Server**

**Host Machine -Kali Linux**

**Target IP ADDRESS-** **182.74.129.38( Taken from Shodan.io**

* First Lets Scan this server using nmap
* Type-> nmap -sS 182.74.129.38
* Then For Finding the Versions running on this Services.
* Type-> nmap -Sv 182.74.129.38



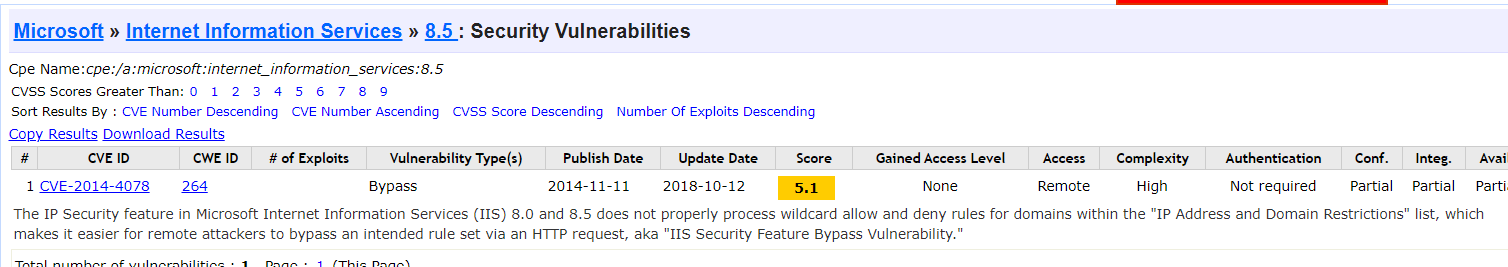


**Target OS-Microsoft Windows**

**Services Version- Microsoft IIS httpd 8.5**

* Let us scan this version has any vulnerability or not.

To do so just go to [www.cvedetails.com](http://www.cvedetails.com) And search the version for any vulnerability.

****

* So we Find the Vulnerability its CVE-2014-4078 Vulnerability Type- Bypass
* So that was my minor project finding out the Vulnerability Of a Choice Server…..

***Thank You..***