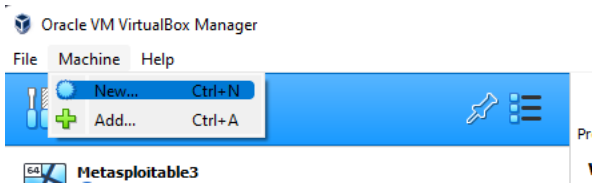
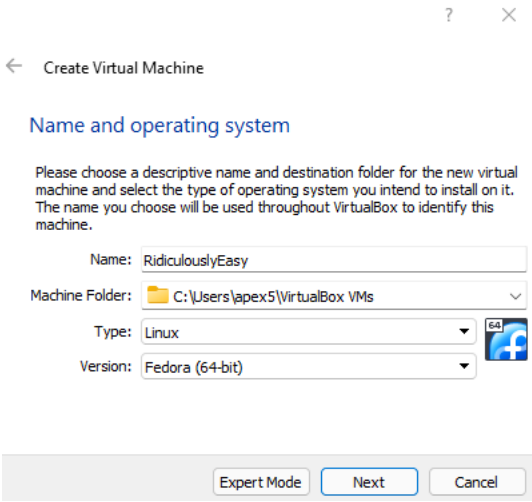
4/11/2022 - RidiculouslyEasy VM Setup

Monday, April 11, 2022 9:58 AM

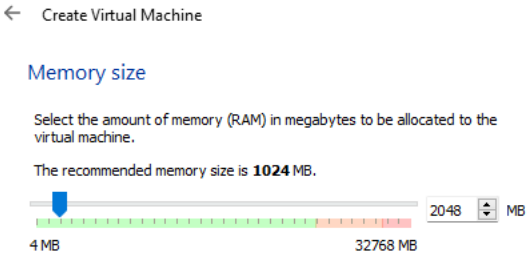
In virtualbox go to machine -> New



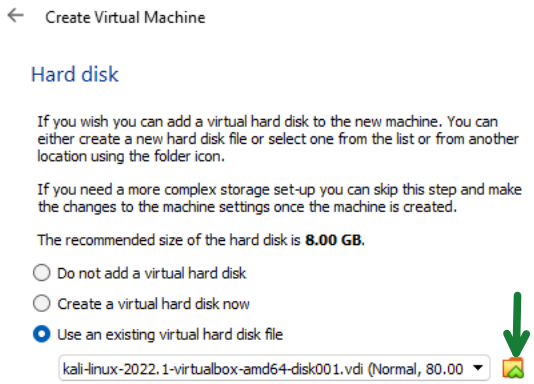
Name the VM What you would like to call it. The type should be Linux and the Version should be Fedora (64-bit).



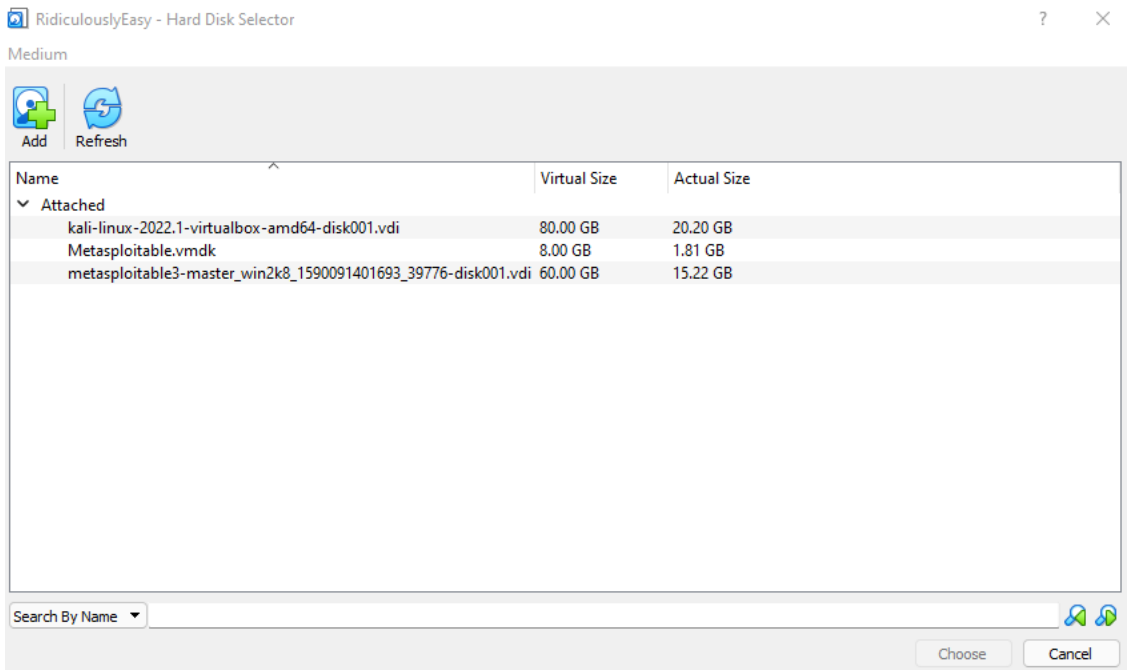
You can change the memory as you desire.*I put 2048 but default is 1024*



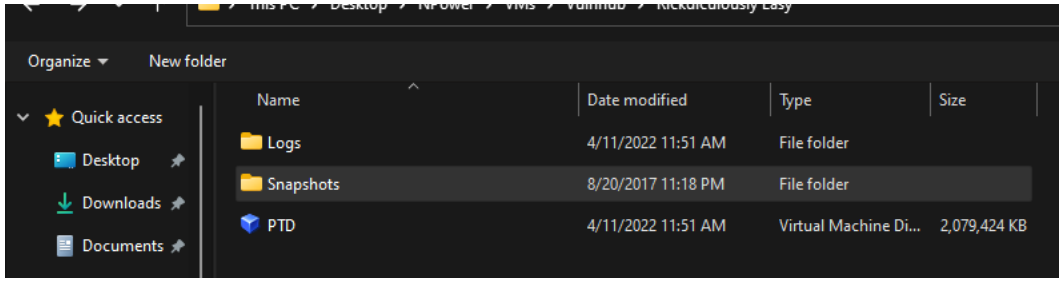
Click the use an existing virtual hard disk file and click the folder with the green arrow.



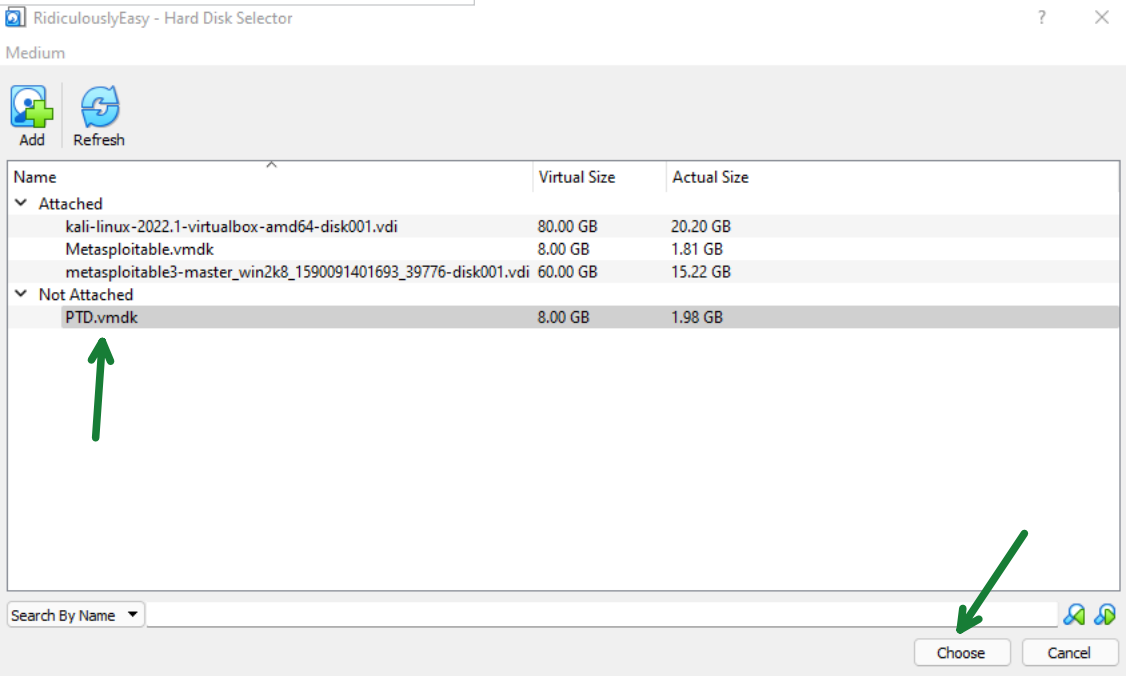
Click the Add button to add a new hard disk.



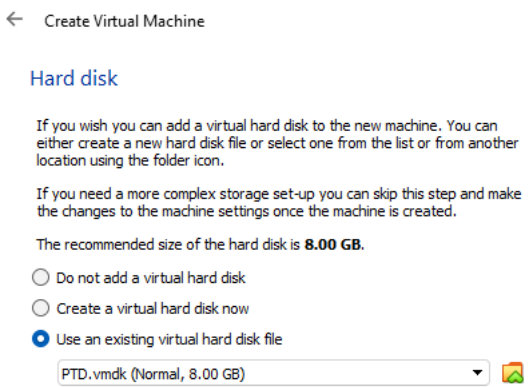
Select the PTD file that you extracted from the zip file.



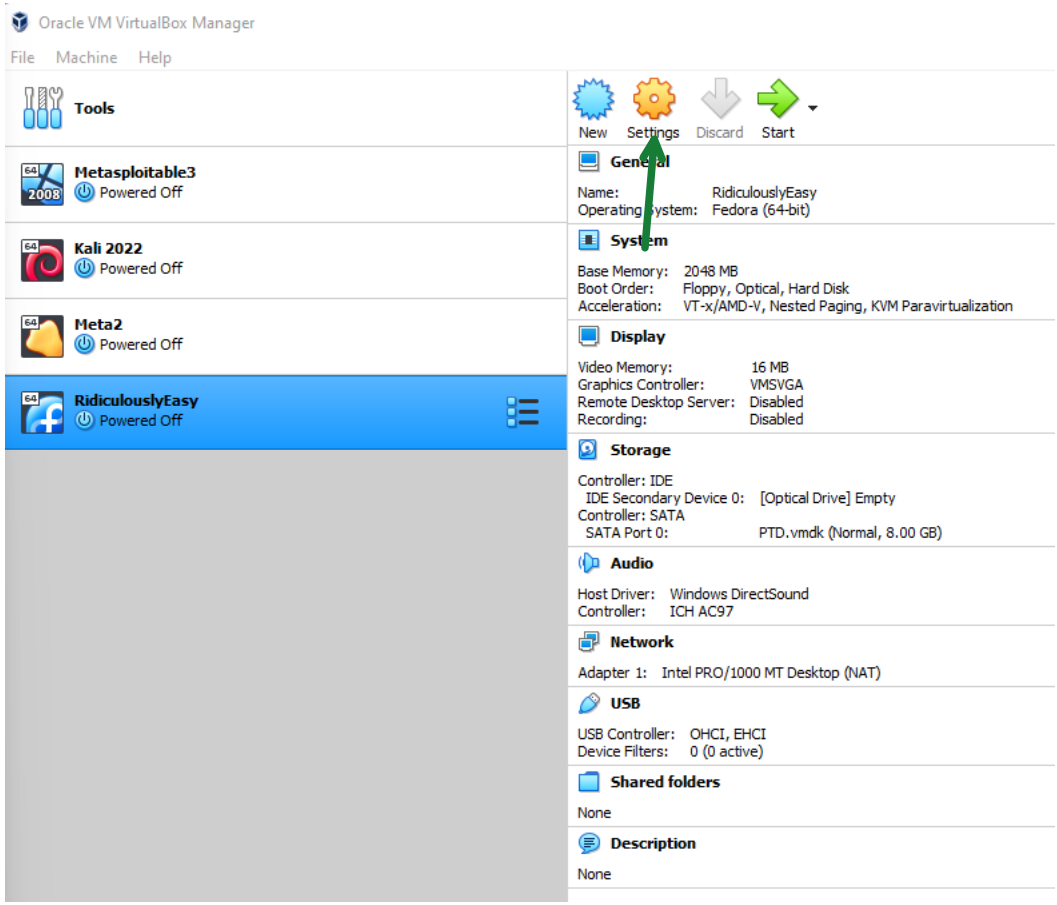
Select the PTD.vmdk and click the choose button.



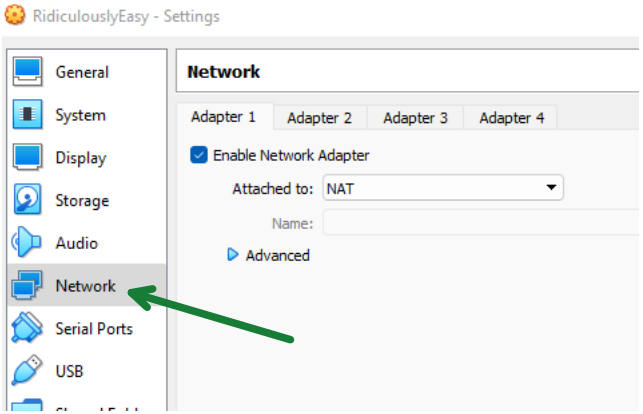
Once PTD.vmdk is select in the drop down menu, click next.

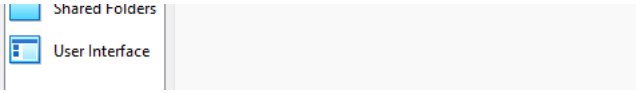


Click the Settings button.

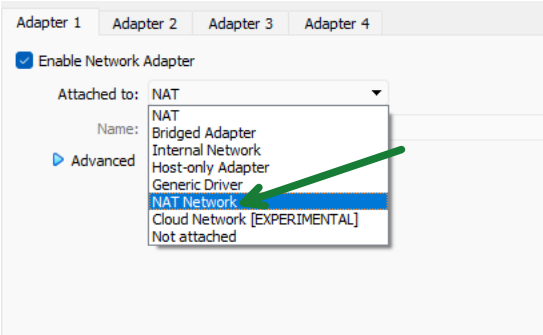


Click the Network tab in the left navigation menu.

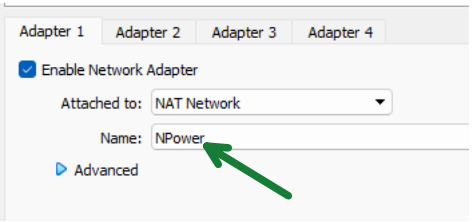




In the Attached to: drop down menu select the NAT Network.



Make sure in the Name: drop down Menu Npower is selected. Then press the OK button to save the settings.



Go to root by typing sudo su

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─#
```

Start the postgresql service by typing service postgresql start

```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start

┌──(root㉿kali)-[/home/kali]
└─#
```

Initialize the metasploit framework database by typing msfdb init

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

To get the IP of the RidiculousEasy VM type netdiscover -r 10.0.2.0/16

```
┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 10.0.2.0/16
```

The IP of RidiculouslyEasy is most likely 10.0.2.15

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
 _____________________________________________________________________________
__
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 _____________________________________________________________________________
--
 10.0.2.1        52:54:00:12:35:00      3     180  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:b1:68:c0      4     240  PCS Systemtechnik GmbH
 10.0.2.15       08:00:27:21:3a:e9      1      60  PCS Systemtechnik GmbH
```

Go into the metasploit framework console by typing msfconsole -q

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf6 >
```

Create a new workspace by typing workspace -a [Name of workspace]

```
msf6 > workspace -a RidEasy
[*] Added workspace: RidEasy
[*] Workspace: RidEasy
msf6 >
```

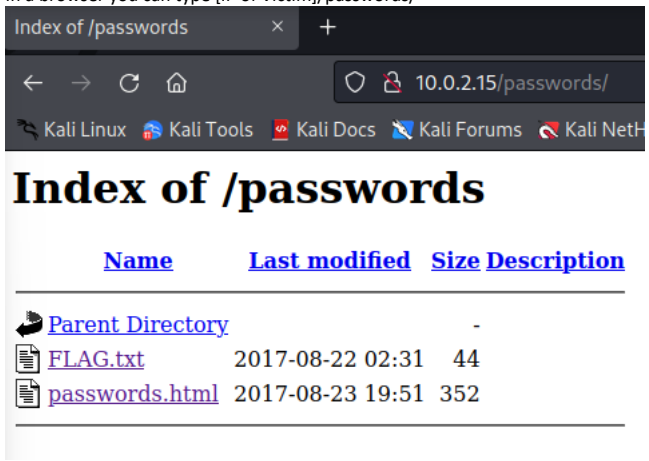
Run nmap to scan the VM by typing db_nmap -p- -O 10.0.2.15 --script=vuln

```
msf6 > db_nmap -p- -O 10.0.2.15 --script=vuln
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 13:37 EDT
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.00049s latency).
[*] Nmap: Not shown: 65528 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 80/tcp    open  http
[*] Nmap: |_http-trace: TRACE is enabled
[*] Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
[*] Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
[*] Nmap: | http-enum:
[*] Nmap: |   /robots.txt: Robots file
[*] Nmap: |   /icons/: Potentially interesting folder w/ directory listing
[*] Nmap: |_  /passwords/: Potentially interesting folder w/ directory listi
ng
[*] Nmap: 9090/tcp  open  zeus-admin
[*] Nmap: 13337/tcp open  unknown
[*] Nmap: 22222/tcp open  easyengine
[*] Nmap: 60000/tcp open  unknown
[*] Nmap: MAC Address: 08:00:27:21:3A:E9 (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.9
[*] Nmap: Network Distance: 1 hop
[*] Nmap: OS detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 34.84 seconds
msf6 >
```

Under port 80 you should see that there is a robots.txt and /passwords directory.

```
Nmap: 80/tcp    open  http
Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
Nmap: |_http-trace: TRACE is enabled
Nmap: | http-enum:
Nmap: |   /robots.txt: Robots file
Nmap: |   /icons/: Potentially interesting folder w/ directory listing
Nmap: |_  /passwords/: Potentially interesting folder w/ directory listing
Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
```

In a browser you can type [IP of Victim]/passwords/



You should see FLAG.txt & passwords.html files. You can click these to see the contents of these files.
When you click the FLAG.txt file you will see that you received 10 point for find the flag.