COMPUTER SUBJECT:	NETWORK SECURITY HACKING
TYPE:	GROUP WORK
IDENTIFICATION:	Metasploitable Installation/MICL
COPYRIGHT:	Michael Claudius
LEVEL:	INTERMEDIATE
DURATION:	30-60 minutes
SIZE:	30 lines!!
OBJECTIVE:	Installing vunerable test-kit in VM on NATNetwork
REQUIREMENTS:	
COMMANDS:	

IDENTIFICATION: Metasploitable Installation/MICL

Prolog

You have successfully finalized the IT-Security course. You will like to investigate more!.

The Mission

You are to install Metasploitable on a NATNetwork.

Purpose

The purpose is to create an environment for Metsploit to attack Metsploitable.

Installation of Metasploitable

There are several ways of skinning a cat and that's also the case when installing SW. The one given here is fast and simple. It falls in 3 steps:

- Download Metasploitable
- Install Metasploitable in Virtual Box
- Set up a NATNetwork test environment

<u>Useful links</u>

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

https://www.wikigain.com/download-install-metasploitable-in-virtualbox/

Download Metasploitable

Find Metasploitable 2 from SourceForge at:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Download the latest version to the folder where you already have Kali Linux.

Unzip the file and notice the Metasploitable Virtualk Machine Directory and the .vmx files.

Kali Linux 🕨 met	asploitable-linux-2.0.0 > Metasploitable2-Linux	✓ Ů Search	Metasploitable2-Linux 🔑
^	Name	Date modified	Type S
	Metasploitable.nvram	20/04/2020 18.16	NVRAM File
	😺 Metasploitable	20/04/2020 21.40	Virtual Machine Di
	Metasploitable.vmsd	20/04/2020 18.16	VMSD File
	Metasploitable.vmx	20/04/2020 18.16	VMX File
- 1	Metasploitable.vmxf	20/04/2020 18.16	VMXF File

Installation of Metasploitable

This relays heavily on https://www.wikigain.com/download-install-metasploitable-in-virtualbox/

1. Open the Virtual Box and click the new button on the top right side of your Virtual Box. On the first option, write Metasploitable and select Linux in the second option and click Next and go forward.



Click on a new button

2. After step 2, you will select the memory size (RAM). You can use it as a default or give some extra and Click on next then Create button.

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

. .

	1024	₽ ME
4 MB	4096 MB	

RAM Size

3. This step, you will select the type of your Hard disk, and it is VDI(Virtualbox Disk Image). After that, click on Next button and again click Next button.





4. Now you will select the size and location of your Virtual Machine.



File Size and location

5. Now the settings are fixed up, and we have to select our downloaded OS, and for that, we must click on the *Storage* button as the picture below.

The Complexity ble	🗶 Greeval
A Second Col	Name: Metasplotable Openeting System: Ubuntu (84-bit)
	B System
	Base Nemony: 1024148 Boot Orden: Roopy, Optical, Hard Dak Acceleration: VT-x(NMD-v, Nentad Paging, KIMI-Parevintualization
	😸 Display
	Rideo Mencory: 36 HB Remote Desidop Server: Desided indeo Capatoria: Desided
	Starage
	Controller: IDE IDE Sociadary Heater: (Optical Drive) Empty Controller: SATA SATA Parto: Metaptotable.vdl (Normal, 10.04 GB)
	Audia Audia
	Heat Driver: Windows Directiound

Click on the Storge

6. Click on the small hard disk on the top right of the dialogue box as the picture.



Select Metasploitable

And Choose "Virtual Disk"

7. Now go the directory where Metasploitable was downloaded and select that.

felde				
^	Nerve	Date modified	Туре	See
÷	Metaspioitable	1/22/2017 11:23 AM	VMDKPIe	1,880,512 KB



8. It is finished, and you are ready to open. To open that click the start button on the top right of the Virtualbox.



Click on the Start button

Note: The password and the username of Metasploitable are both *msfadmin*. And You can shut down it by choosing "Power off" and if you got any question or problem, do not hesitate to share with Your class-mates.



Login with password

Isolating the test environment

When performing these kinds of red-team tests, it is a good idea to isolate the VMs in a test network. This are to be done via VirtualBox.

Note: Alternatively; one could use a bridged NAT, but this opens up for other "potential hackers"

Never expose Metasploitable to an untrusted network, use NAT or Host-only mode!

1. Create your own NAT network.

In the Virtual Box Choose: File > Preferences > Network

Box - Preferences		?	×		
neral Netw	ork				
out NAT Net	vorks		-1		
date Active	Name		P		
nguage	NatNetwork				
splay					
twork					
ensions					
жу	•				
OK Cancel					
	ox - Preferences Ineral Ut Late guage olay work ensions xy	ox - Preferences Network NAT Networks Active Name Jate guage olay work ensions xy OK	xy Preferences ? Network NAT Networks Active Name NATNetwork NatNetwork OK Cance		

Click the small green button to "Add new NAT Network" Click OK.

2. Moving VM's to NAT network

Make sure both of your VM systems (Kali and Metasploitable) are powered off and then highlight one of the machines.

Right click on one of the machines, or use the tool-line and Choose "Settings" Choose: Network -> NAT-Network

Under Name: Choose the available NATNetwork

1	🥥 Metasploitable 2 - Settings			?	×
		General	Network		
		System	Adapter 1 Adapter 2 Adapter 3 Adapter 4		
1		Display	C Enable Network Adapter		
	\bigcirc	Storage	Attached to: NAT Network		
		Audio	Name: NatNetwork		•
	Ð	Network	Advanced		
		Serial Ports			
	Ď	USB			
		Shared Folders			
	-	User Interface			
			ОК	Ca	ncel

Do the same for the other machine.

3. Ping the VM's

Check out that your VM's are on the same network Start both Kali and Metasploitable Use ifconfig to find the IP-addresses of both machines. Mine were Metasploitable (10.0.2.4) and Kali (10.0.2.15)

Note: If you are using 2020 version remember to use sudo ifconfig or ip a or ip addr

instead

Now from Kali ping the Metaspoitable.

ping 10.0.2.4

Stop ping by use of

Ctrl c

Then from Metasploitable ping Kali.

Congratulation: Next step is to attack/exploit Metasploitable.