



Lab 10: Vulnerability Assessment & Penetration Testing

Karin Sumongkayothin, PhD.

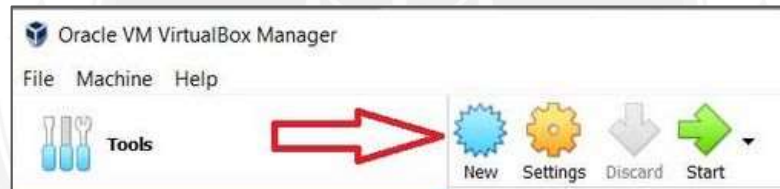


1. Setup
2. Vulnerability Assessment (VA)
3. Penetration Testing

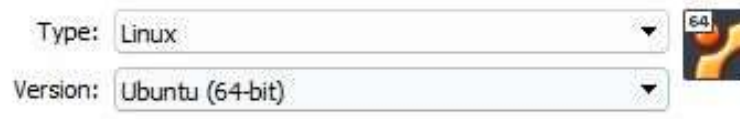


Import Metaspolitable2

1. Download Metaspolitable2 from <https://sourceforge.net/projects/metaspolitable/files/Metaspolitable2/>
2. Create new virtual machine by clicking “New”



3. Select Type: “Linux” and Version: “Ubuntu (64-bit)”





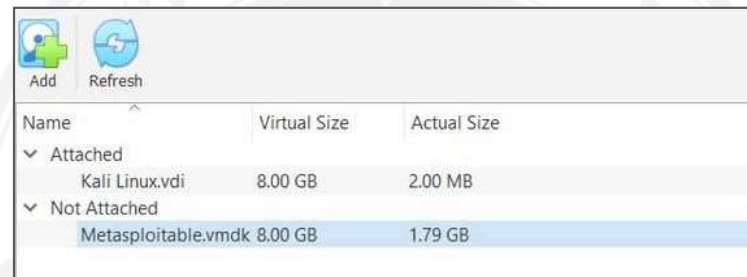
4. Select memory size 1024MB then click Next button
5. Select an existing virtual Hard disk file then click on the yellow folder icon (marked with red arrow).



6. Click on “Add”  then select the Location where you had extracted and Metasploitable2 file (it is a .vmdk file) Click on it. And then click Open.

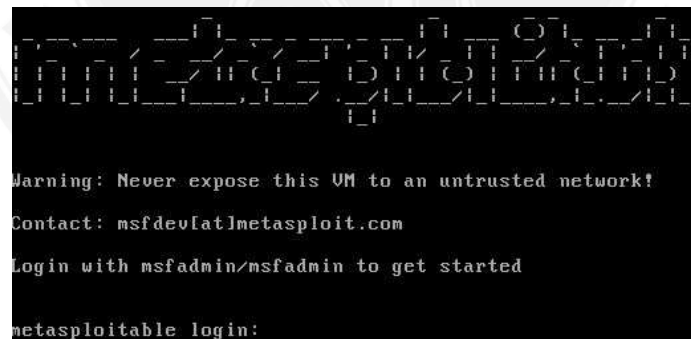


7. Click on “Metasploitable.vmdk” file and Hit the Choose button.



Name	Virtual Size	Actual Size
▼ Attached		
Kali Linux.vdi	8.00 GB	2.00 MB
▼ Not Attached		
Metasploitable.vmdk	8.00 GB	1.79 GB

8. In order to login, use **username: msfadmin** and **password: msfadmin**

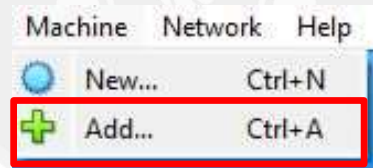


```
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
metasploitable login:
```



Kali Linux

1. Download Kali's image from <https://cdimage.kali.org/kali-images/kali-virtual-weekly/kali-linux-2022-W34-virtualbox-amd64.7z>
2. Extract kali-linux-2022-W34-virtualbox-amd64.7z to folder
3. Open VirtualBox application then click "Machine" tab then choose "Add"



4. Choose .vbox file then click Open



VirtualBox Network Setting

1. Open VirtualBox and make sure that “Host Only Adapter” ‘s DHCP is enable



The screenshot shows the 'Network Adapters' window in VirtualBox. The 'Tools' menu is open, showing 'Create', 'Remove', and 'Properties' options. Below the menu, a table lists the network adapters. The first adapter is 'VirtualBox Host-Only Ethernet Adapter' with an IPv4 address of 192.168.56.1/24 and the DHCP server checkbox checked and labeled 'Enable'.

Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		<input checked="" type="checkbox"/> Enable

2. Setup IPv4 NetMasking to 192.168.56.1/24 and DHCP server is 192.168.56.1



The screenshot shows the 'Network Adapter Properties' window for the 'VirtualBox Host-Only Ethernet Adapter'. The 'Adapter' tab is selected, and the 'DHCP Server' checkbox is checked. The 'Configure Adapter Manually' radio button is selected. The IPv4 Address is set to 192.168.56.1, the IPv4 Network Mask is set to 255.255.255.0, and the IPv6 Address is set to fe80::5daa:b5e6:de83:6c5b.

Adapter	DHCP Server
<input type="radio"/> Configure Adapter Automatically	
<input checked="" type="radio"/> Configure Adapter Manually	
IPv4 Address:	192.168.56.1
IPv4 Network Mask:	255.255.255.0
IPv6 Address:	fe80::5daa:b5e6:de83:6c5b

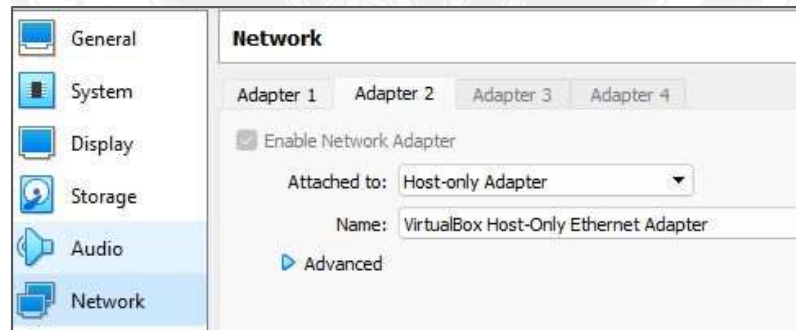


VirtualBox Network Setting

3. On both Kali and Metasploitable VM, do left-click and choose “Setting”



4. Go to “Network” tab and make sure that VM network adaptor is chosen to “Host-only Adaptor”





VirtualBox Network Setting

4. Check IP address of both Kali and Metasploitable are in the same network and can ping to each other.

```
(kali@kali)-[~]  
$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.  
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.260 ms  
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.149 ms  
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.559 ms  
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.324 ms
```



OpenVAS

1. `sudo apt update && apt upgrade -y`
2. `sudo apt install openvas`
3. `sudo gvm-setup`

```
sent 711 bytes received 76,459,880 bytes 403,485.97 bytes/sec
total size is 76,439,315 speedup is 1.00
[+] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73: OpenVAS /var/run/osspd/osspd.sock 0 OpenVAS Defa
t
[+] Done
[+] Please note the password for the admin user
[+] User created with password 'c273c26d-28d3-485b-9865-5c96e30acf6d'
```

4. `sudo gvm-start` and use username: admin with password from above to login through <https://localhost:9392>



Part II: Vulnerability Assessment

OpenVAS

https://127.0.0.1:9392/login

tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Greenbone
Security Assistant

Sign in to your account

Username
admin

Password
.....

Sign In

Powered by
Greenbone



OpenVAS

Create Scanning Target

1. Click “Configuration” tab then choose “Targets”



2. Add new target by clicking icon of the following picture





OpenVAS

Create Scanning Target

3. Fill the information of Metasploitable VM then “Save”

New Target

Name: Metasploitable2S

Comment:

Hosts: ☒ Manual ☐ From file No file selected.

Exclude Hosts: ☒ Manual ☐ From file No file selected.

Allow simultaneous scanning via multiple IPs: ☒ Yes ☐ No

Port List: All IANA assigned TCP ☐

Alive Test: Scan Config Default

Credentials for authenticated checks

SSH: -- on port 22 ☐

Targets 1 of 1

Name	Hosts	IPs	Port List
Metasploitable2	192.168.56.101	1	All IANA assigned TCP


(Applied filter: sort=name first=1 rows=10)

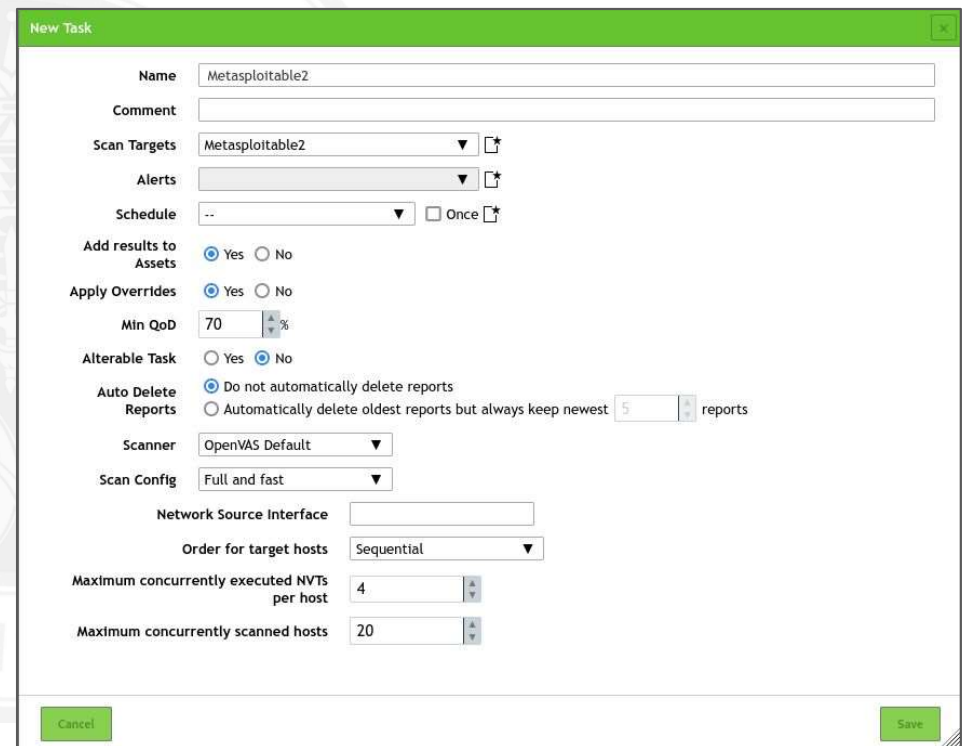


Part II: Vulnerability Assessment

OpenVAS

Scanning target

1. Go to “Scan” tab and create the “new Task” then fill the information as the right hand side picture
2. Click “Save”
3. Click  to start the scanning
4. Choose “Report” or “Result” to see the scanning results.



New Task

Name: Metasploitable2

Comment:

Scan Targets: Metasploitable2

Alerts:

Schedule: --

Add results to Assets: ☒ Yes ☐ No

Apply Overrides: ☒ Yes ☐ No

Min QoD: 70 %

Alterable Task: ☒ Yes ☐ No

Auto Delete Reports: ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Cancel Save



Question 1:

- ☐ How many vulnerabilities found after finish the scanning?
 - ☐ High 22
 - ☐ Medium 39
 - ☐ Low 6
 - ☐ Log 88
- ☐ What is CVE of “jQuery < 1.9.0 XSS Vulnerability” CVE-2012-6708
- ☐ How to mitigate the attack of “jQuery < 1.9.0 XSS Vulnerability”
Update to version 1.9.0 or later.



Part II: Vulnerability Assessment

Nessus

1. Download “Nessus-10.3.0-debian9_amd64.deb” from <https://www.tenable.com/downloads/nessus?loginAttempted=true>
2. Register to get registration code via <https://www.tenable.com/products/nessus/nessus-essentials>
3. Go to download directory and type:
“sudo apt install -f ./Nessus-10.3.0-debian9_amd64.deb”
4. After installation, type “service nessusd start” to start nessus service
5. “sudo /opt/nessus/sbin/nessuscli adduser” , to add the new user
6. Go to “<https://localhost:8834/>”
7. Login with added user and password





Nessus

Create Scanning Target

1. Go to “Scan” tab
2. Click “Basic Network Scan”

The screenshot shows the Nessus 'Settings' page for a new scan configuration. The interface is dark-themed. At the top, there are tabs for 'Settings', 'Credentials', and 'Plugins'. The 'Settings' tab is active. On the left, there is a sidebar with a 'BASIC' section expanded, showing 'General', 'Schedule', and 'Notifications'. Below this are sections for 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The main area contains fields for 'Name' (Metasploitable2), 'Description', 'Folder' (My Scans), and 'Targets' (S). At the bottom, there are 'Upload Targets' and 'Add File' buttons.

Section	Field	Value
BASIC	Name	Metasploitable2
	Description	
	Folder	My Scans
	Targets	S
Upload Targets		Add File



Part II: Vulnerability Assessment

Question 2:

- ☐ How many vulnerabilities found after finish the scanning?
 - ☐ Critical 11
 - ☐ High 6
 - ☐ Medium 24
 - ☐ Info 135

Question 3:

- ☐ Add “New Scan” and choose “Advanced Scan” with “Assessment > Web Applications > Enable” then run scanning.
- ☐ Does number of vulnerabilities different from **Question 3**? Y (Y/N)
- ☐ If yes, why is different? database sending data to client or to server



Part II: Vulnerability Assessment

Question 4:

- ☐ From **Question 3**, how many vulnerabilities of “Gain a shell remotely” 2
- ☐ Explain of how they are vulnerable?

ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.



Metasploit Framework

1. Type “msfconsole” to access metasploit framework console.

```
[*] Starting the Metasploit Framework console.../

  ((-----))
  ((  _  0 0  _ ))
    \  o_o  /
     \  MSF  /
      \  WW  /
       \___/

= [ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0] ]
+ -- == [ 1390 exploits - 789 auxiliary - 226 post ]
+ -- == [ 356 payloads - 37 encoders - 8 nops ]
+ -- == [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



Task: VSFTPd Vulnerability

- ❑ Gain shell from Metasploitable2 VM
- ❑ Tools:
 - ❑ Nmap
 - ❑ Msfconsole



Question 5:

- ☐ What is the vulnerabilities CVE Id? _____
- ☐ What is the exploit that you use? _____
- ☐ What you can do after exploitation?

- ☐ Show a snapshot of you post exploitation by using 'id' command.
- ☐ What user that you gain access? _____



Meterpreter

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 192.168.86.223:4444  
[*] Sending stage (179779 bytes) to 192.168.86.61  
[*] Meterpreter session 1 opened (192.168.86.223:4444 -> 192.168.86.61:49197) at  
2018-05-29 11:48:32 -0400  
  
meterpreter > shell  
Process 3028 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\victim\Downloads>
```



Task: JAVA-RMI

- ❑ Gain access to Metasploitable2 VM by using “meterpreter/reverse_tcp” payload
- ❑ Tools:
 - ❑ Nmap
 - ❑ Msfconsole



Question 6:

- ☐ What is the vulnerabilities CVE Id? _____
- ☐ What is the exploit that you use? _____
- ☐ What parameters value were set in “options” ?
 - ☐ RHOST _____
 - ☐ LHOST _____
 - ☐ SRVPORT _____



- ❑ Use “show sessions” to list the established connection from metasploitable2
- ❑ Type “session -i <session id that you get>” to activate meterpreter
- ❑ Type “help” to list the meterpreter’s commands that be used

Question 7:

- ❑ What is happen after using “shell”? _____
- ❑ Take snapshot to keep an evidence