Setting up Metasploitable 2

@mmar

Metasploitable 2 is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques

This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms

It is the best resource to practice pentesting in a virtualized local environment

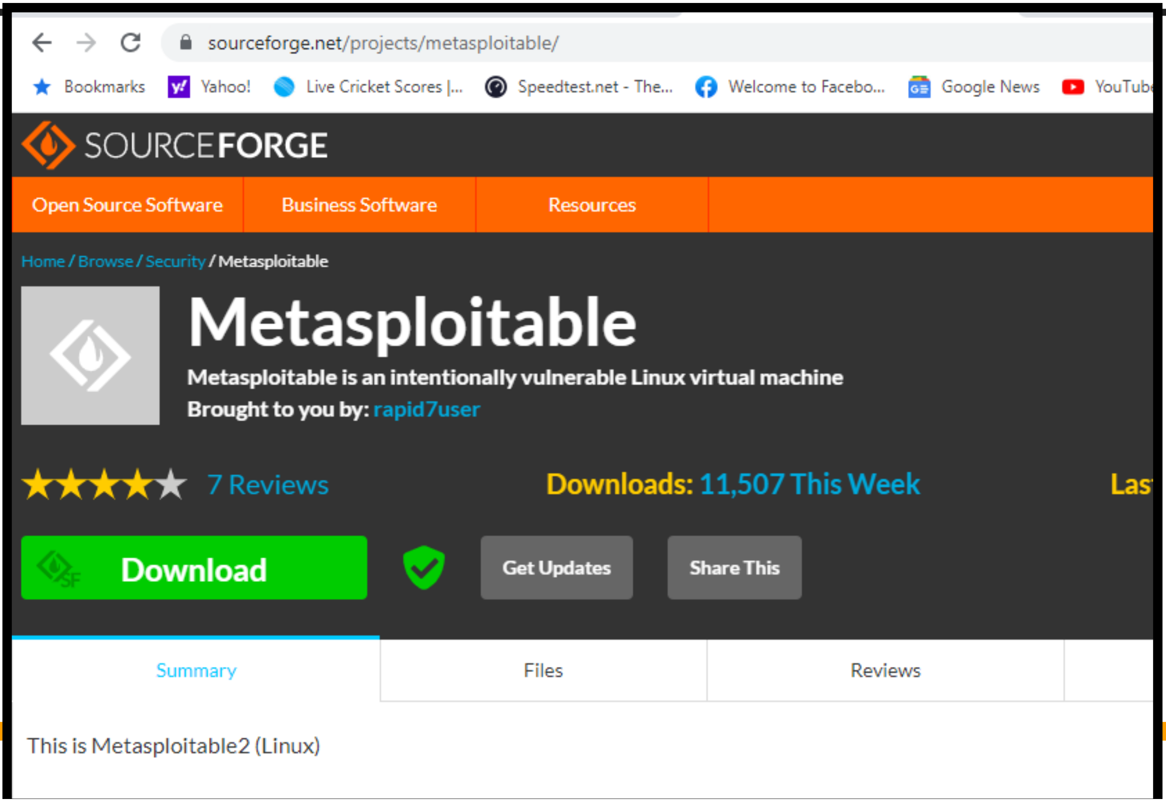
Pre-requisites

- You need to have virtual box or Vmware workstation installed on your machine

Step- 1

- Download Metasploitable-2 from official website

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



Home / Browse / Security / Metasploitable

Metasploitable

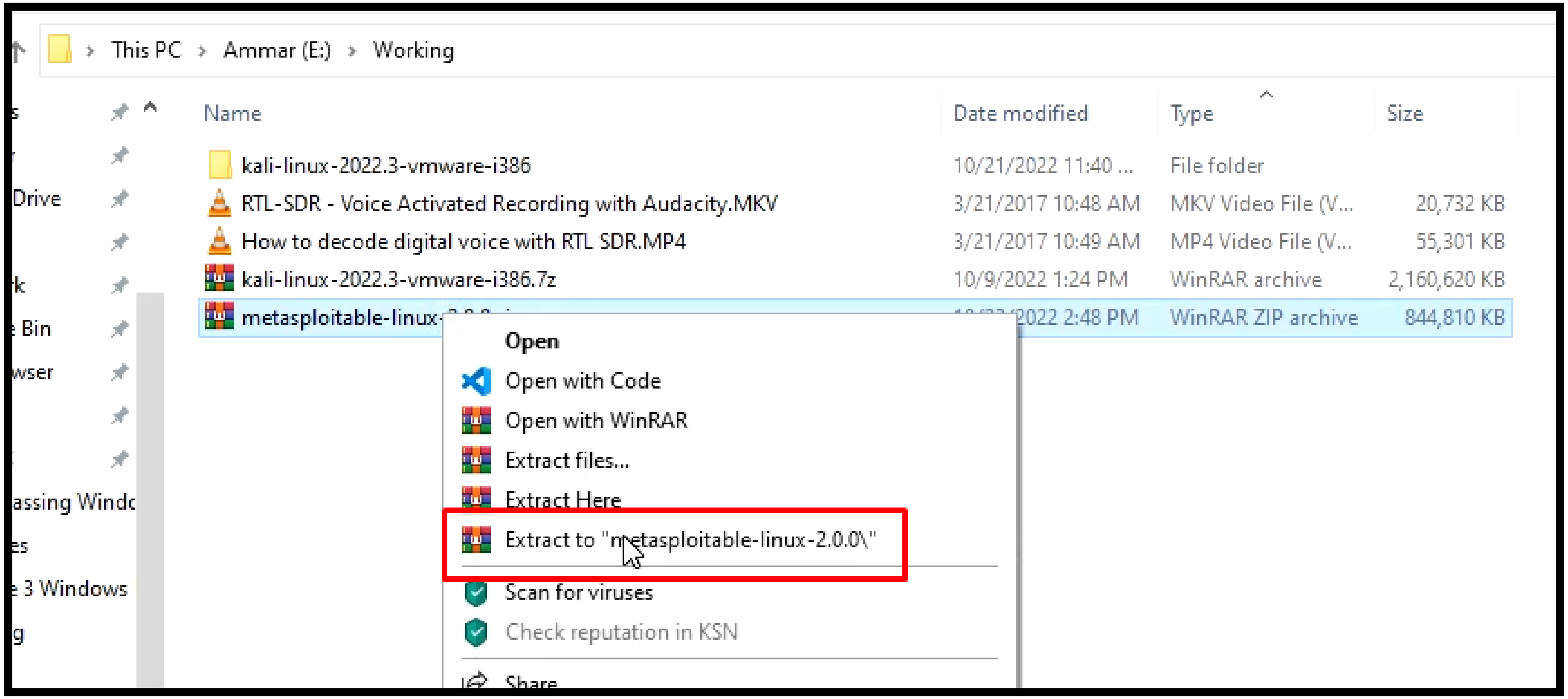
Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

This is Metasploitable2 (Linux)

Step- 2

- Once downloaded, extract it. It contains both VMware and virtual box versions

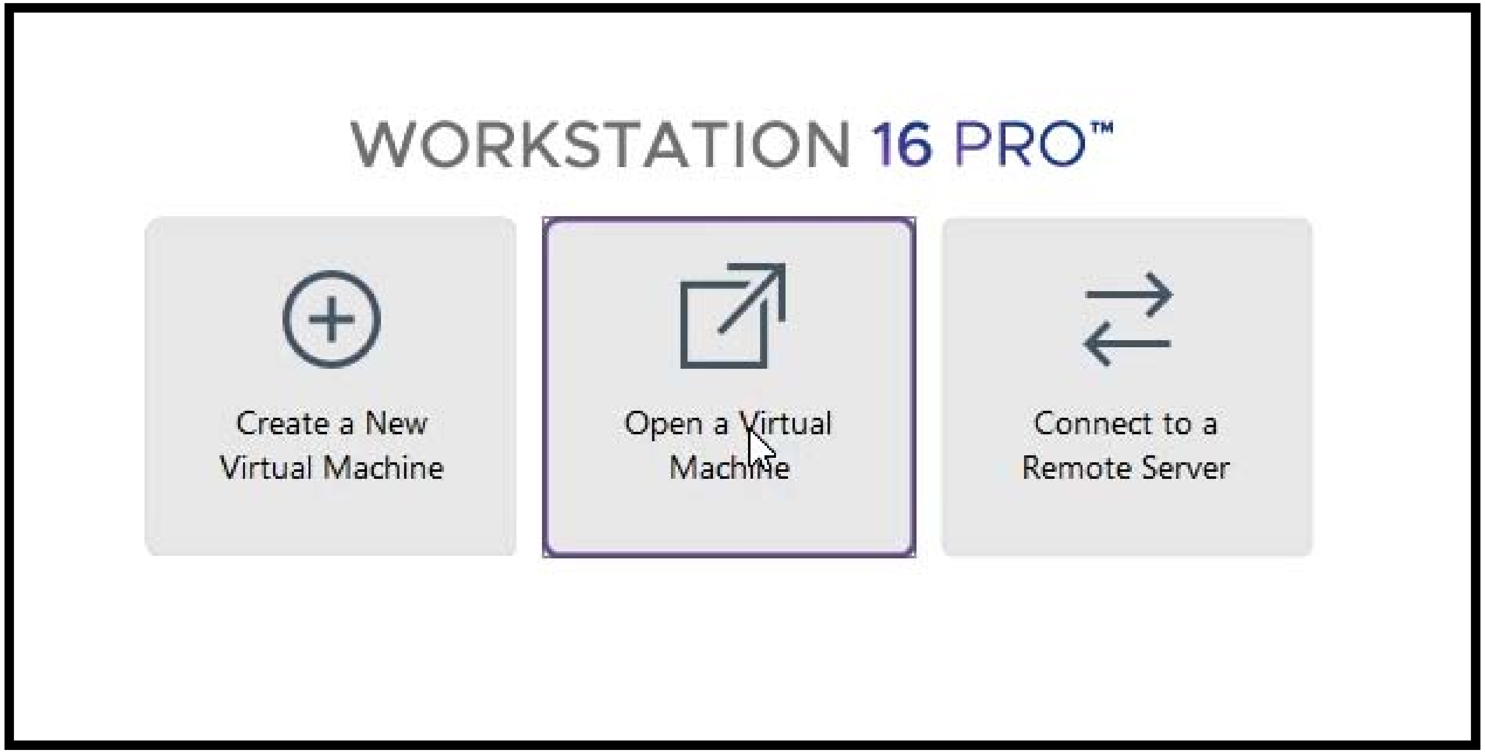


This PC › Ammar (E:) › Working

Name	Date modified	Type	Size
kali-linux-2022.3-vmware-i386	10/21/2022 11:40 ...	File folder	
RTL-SDR - Voice Activated Recording with Audacity.MKV	3/21/2017 10:48 AM	MKV Video File (V...	20,732 KB
How to decode digital voice with RTL SDR.MP4	3/21/2017 10:49 AM	MP4 Video File (V...	55,301 KB
kali-linux-2022.3-vmware-i386.7z	10/9/2022 1:24 PM	WinRAR archive	2,160,620 KB
metasploitable-linux-	2022 2:48 PM	WinRAR ZIP archive	844,810 KB

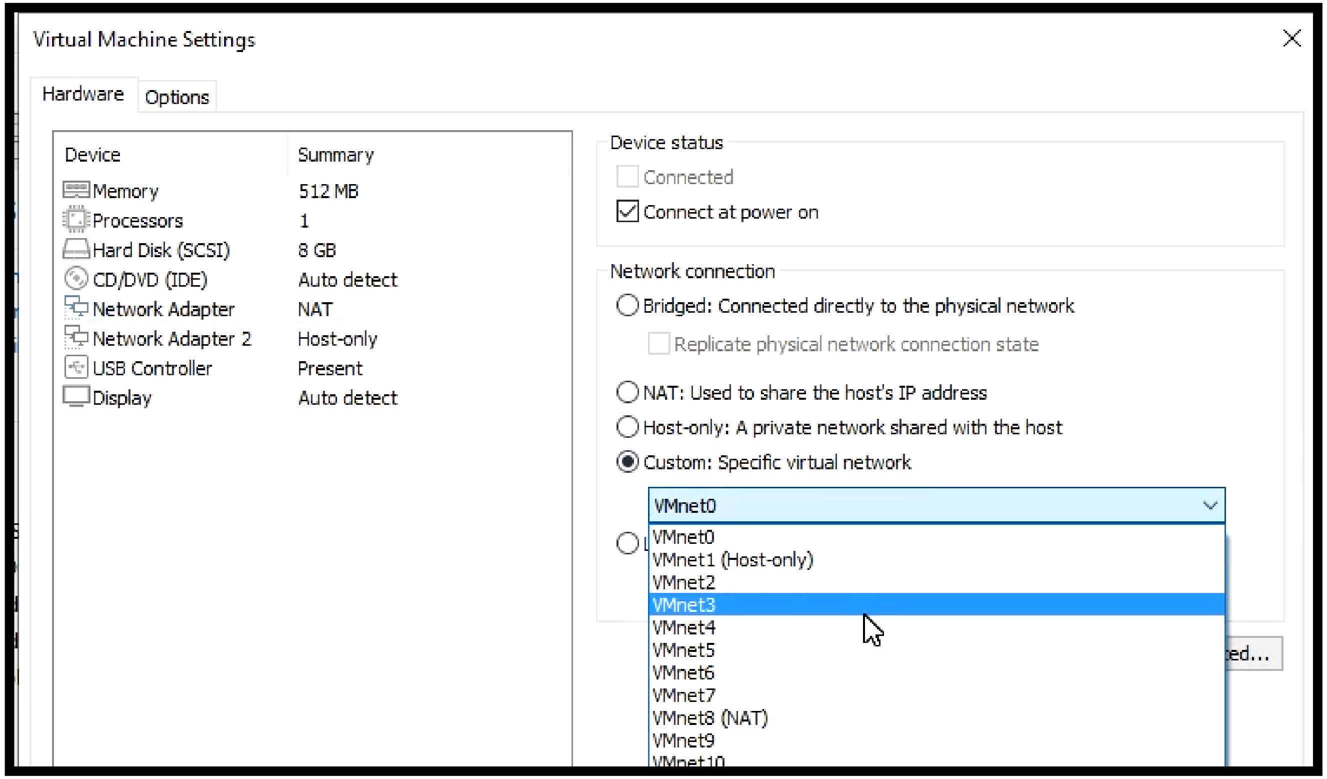
Step- 3

- Now in Vmware workstation, open the virtual machine



Step- 4

- In Network settings, change network settings to Virtual network only



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

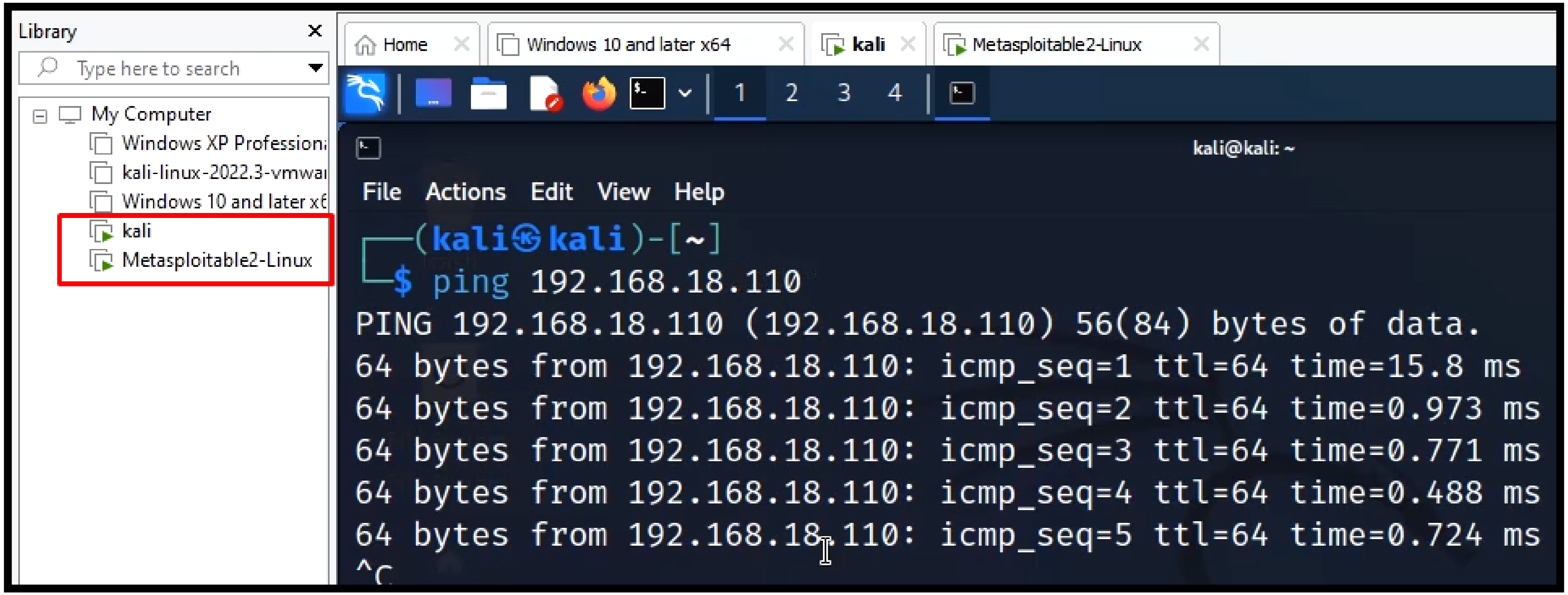
● Custom: Specific virtual network

VMnet0

You Attacking Machine (Kali Linux) must also be having same virtual Network in its network settings

Step- 5

- Turn on both Kali Machines as well as Metasploitable and try to check connectivity with PING command



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.18.110
PING 192.168.18.110 (192.168.18.110) 56(84) bytes of data.
64 bytes from 192.168.18.110: icmp_seq=1 ttl=64 time=15.8 ms
64 bytes from 192.168.18.110: icmp_seq=2 ttl=64 time=0.973 ms
64 bytes from 192.168.18.110: icmp_seq=3 ttl=64 time=0.771 ms
64 bytes from 192.168.18.110: icmp_seq=4 ttl=64 time=0.488 ms
64 bytes from 192.168.18.110: icmp_seq=5 ttl=64 time=0.724 ms
^C
```

DEMO

THANKS