


# 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**



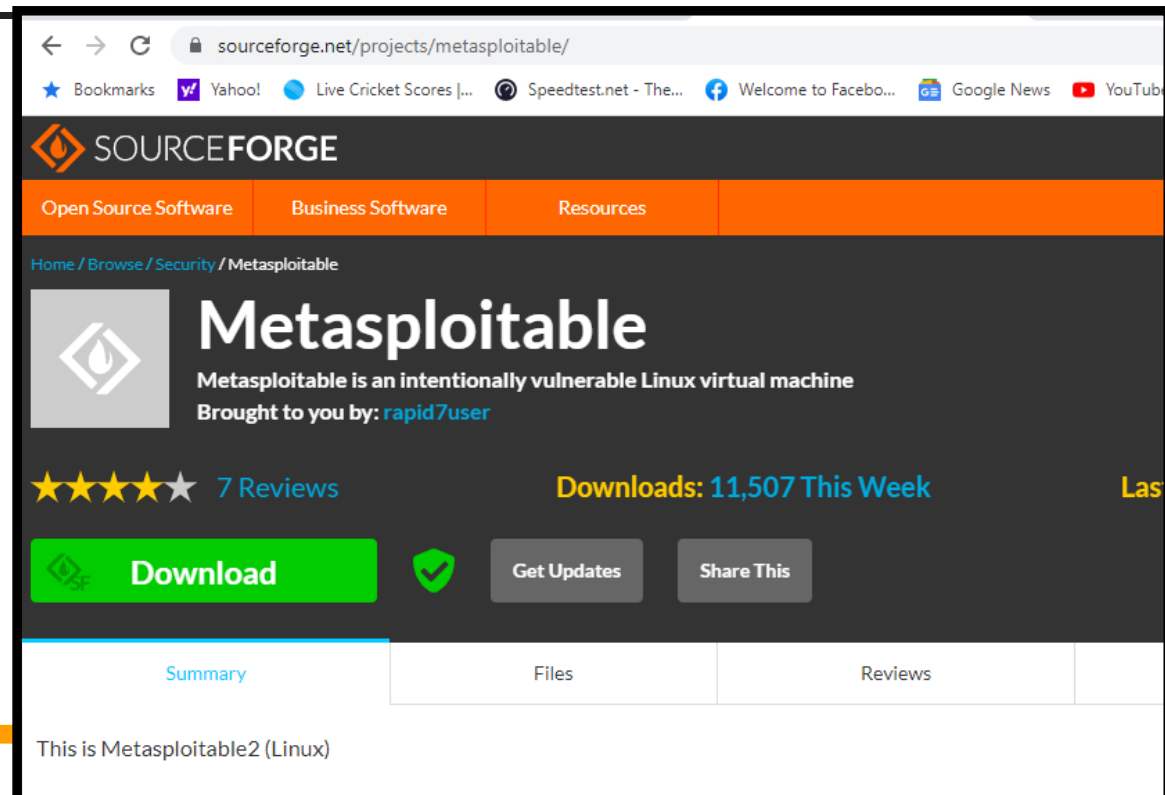
## Pre-requisites

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

# Step-1

- ❖ Download Metasploitable-2 from official website

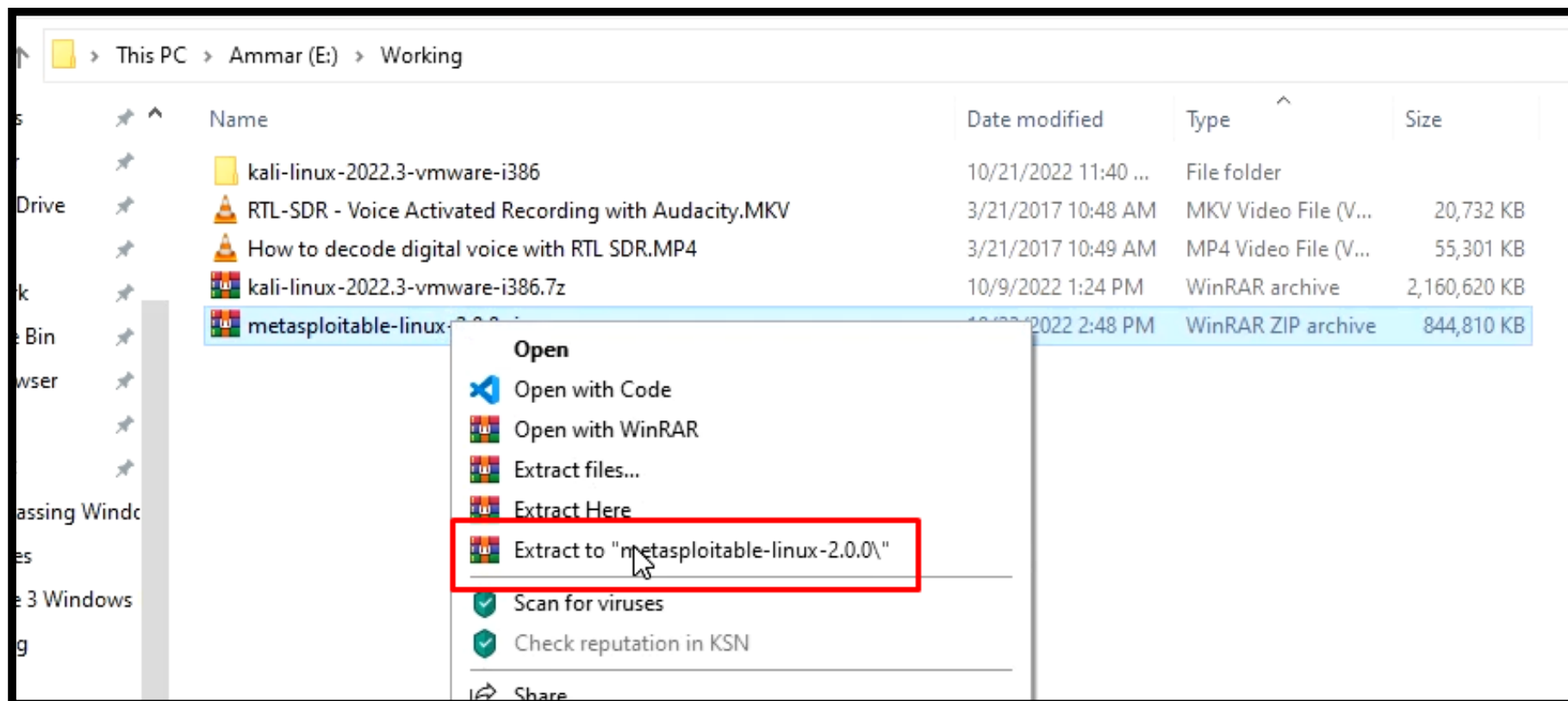
<https://sourceforge.net/projects/metasploitable/>



The screenshot shows the SourceForge project page for Metasploitable. The browser address bar displays the URL [sourceforge.net/projects/metasploitable/](https://sourceforge.net/projects/metasploitable/). The page header includes the SourceForge logo and navigation links for Open Source Software, Business Software, and Resources. The breadcrumb trail is Home / Browse / Security / Metasploitable. The main content area features the Metasploitable logo, a description: "Metasploitable is an intentionally vulnerable Linux virtual machine", and attribution to "rapid7user". It also shows a 4.5-star rating with 7 reviews and 11,507 downloads this week. A prominent green "Download" button is visible, along with "Get Updates" and "Share This" buttons. At the bottom, a tabbed interface shows "Summary" selected, with "Files" and "Reviews" tabs also visible. The summary text reads "This is Metasploitable2 (Linux)".

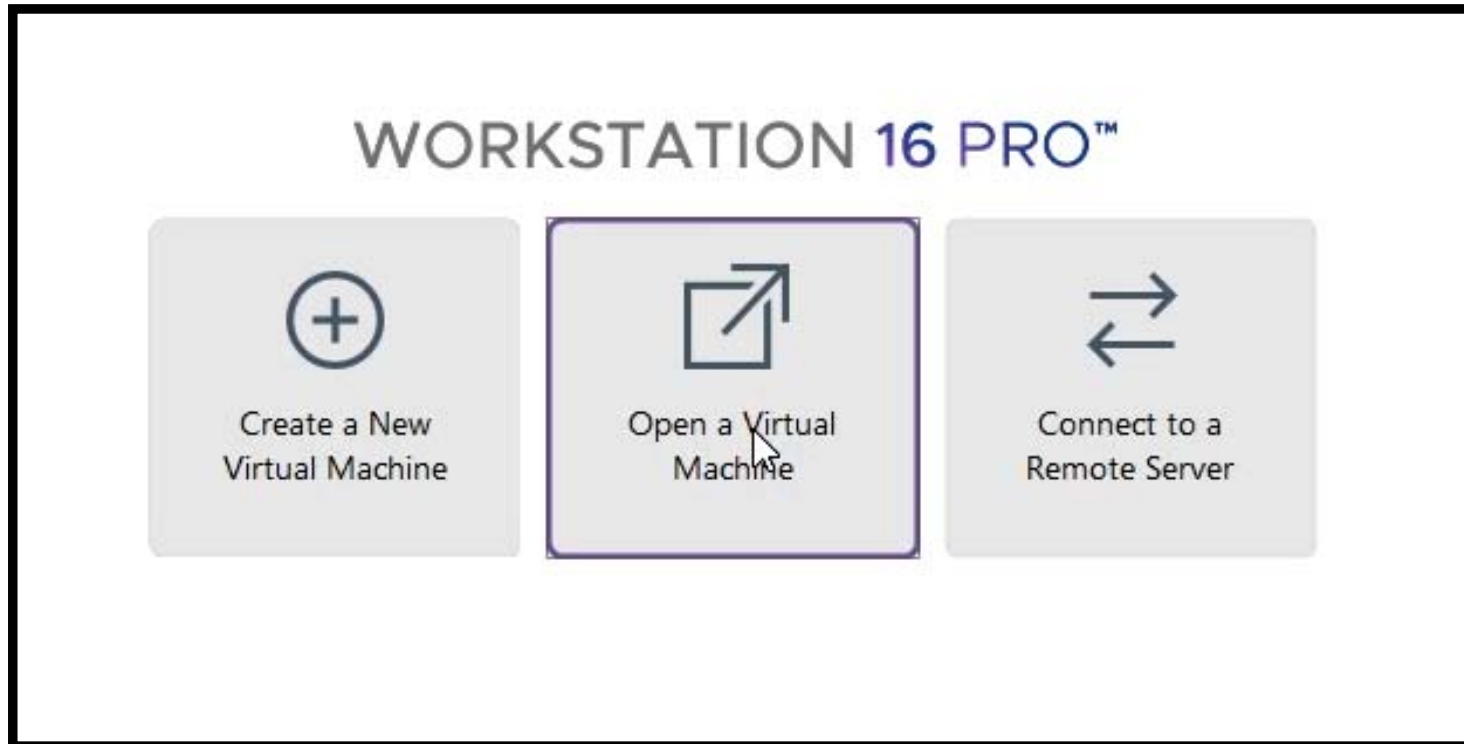
## Step- 2

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



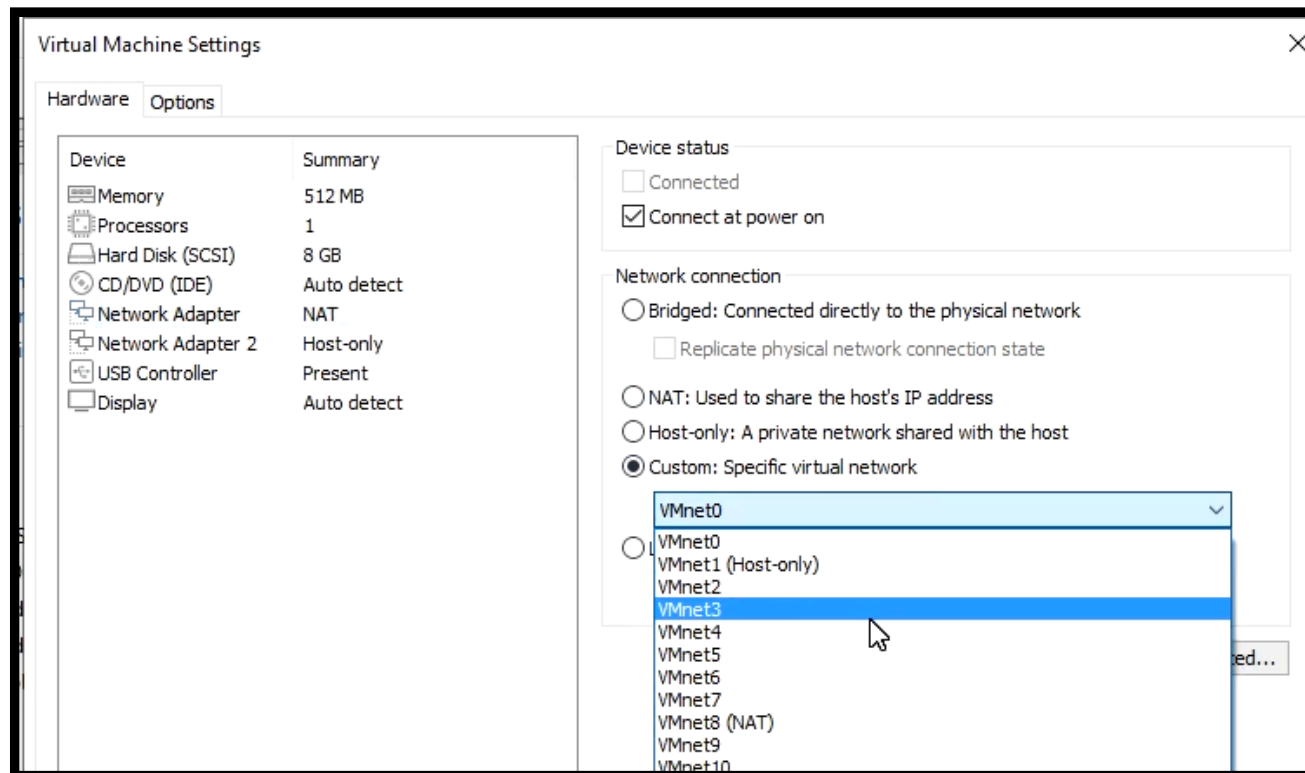
## Step- 3

- ❖ Now in Vmware workstation, open the virtual machine



## Step- 4

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

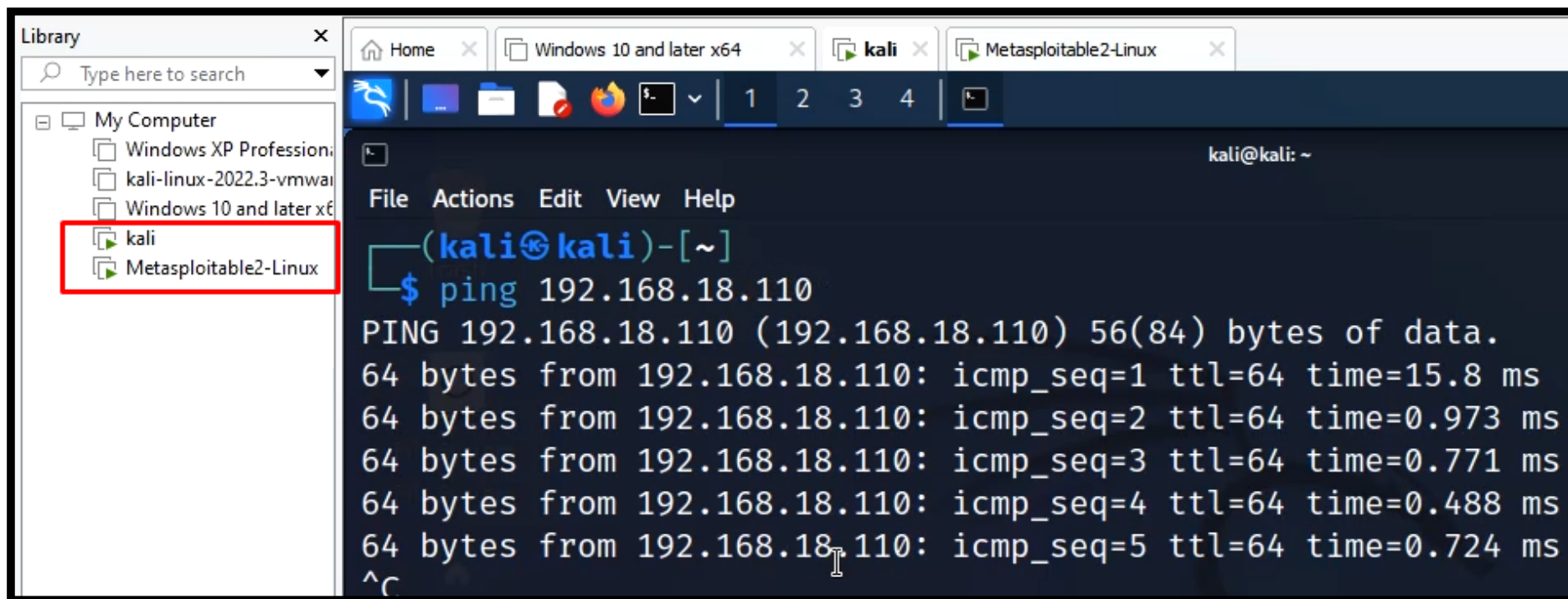




**You Attacking Machine (Kali Linux) must also be having  
same virtual Network in its network settings**

## Step- 5

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



```
Library
Type here to search
My Computer
  Windows XP Profession...
  kali-linux-2022.3-vmwar...
  Windows 10 and later x64
  kali
  Metasploitable2-Linux

Home
Windows 10 and later x64
kali
Metasploitable2-Linux

kali@kali: ~
File Actions Edit View Help
(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