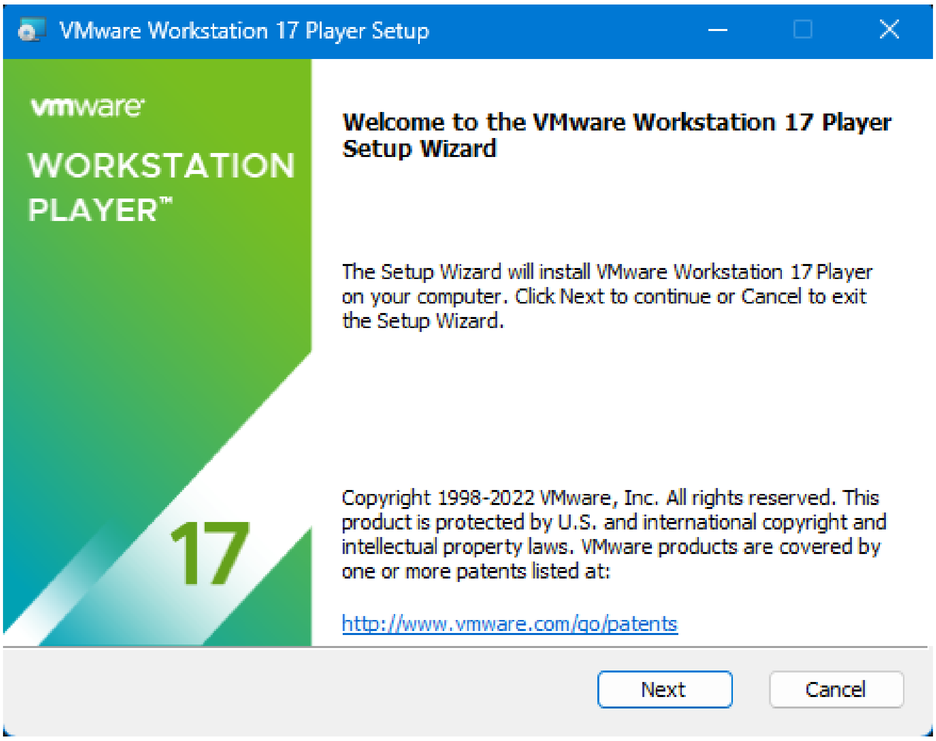
Practical 1

Aim: Lab Setup

Requirements:

- Windows XP ISO
- Kali Linux VMware/VirtualBox image
- Metasploit VMware/VirtualBox image
- VMware player/Virtualbox

Step 1: Start VMware installation by executing the downloaded exe

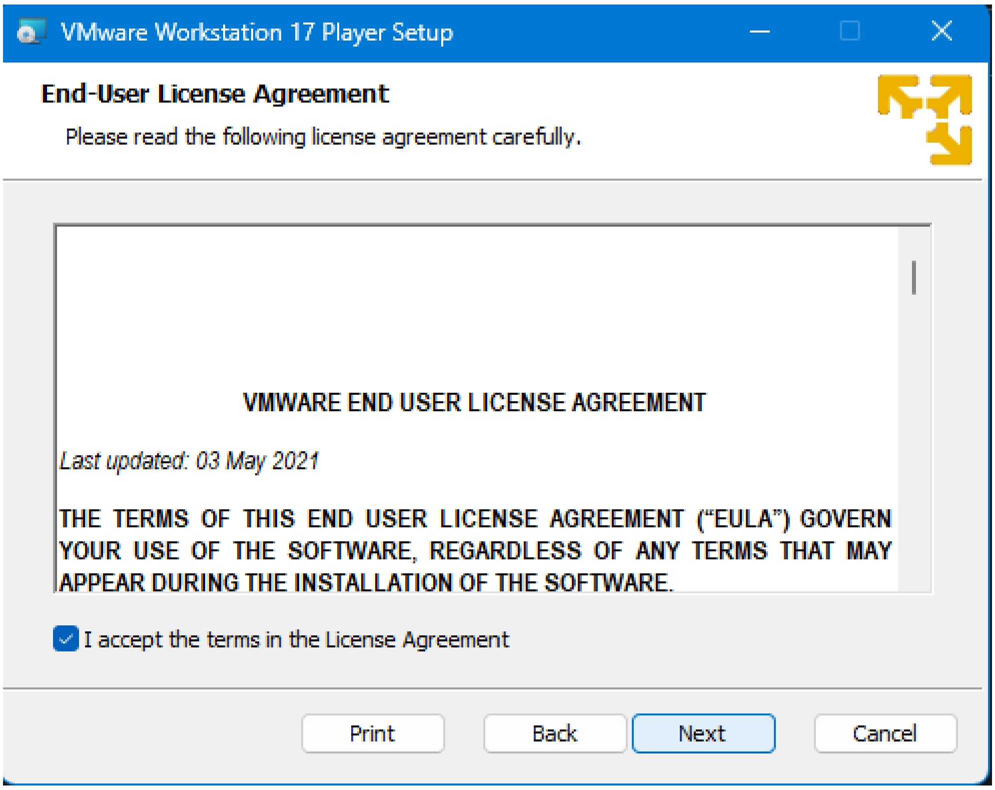


Welcome to the VMware Workstation 17 Player Setup Wizard

The Setup Wizard will install VMware Workstation 17 Player on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright 1998-2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at:

http://www.vmware.com/go/patents



VMware Workstation 17 Player Setup

End-User License Agreement

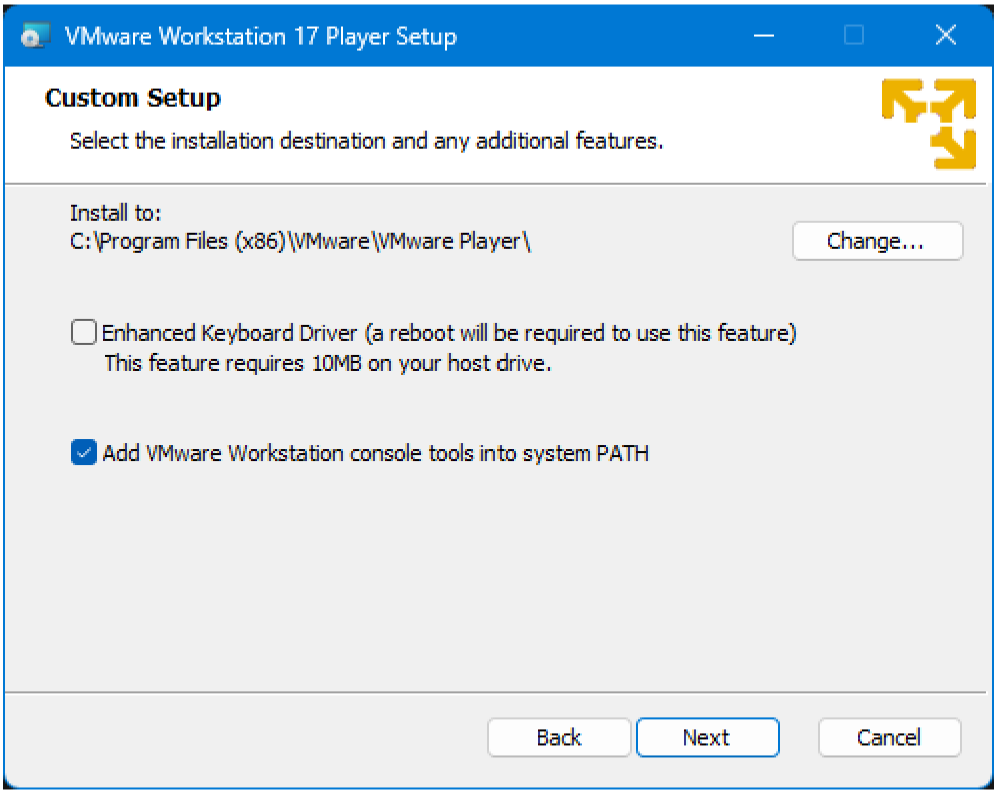
Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

Last updated: 03 May 2021

THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA") GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

☑ I accept the terms in the License Agreement



VMware Workstation 17 Player Setup

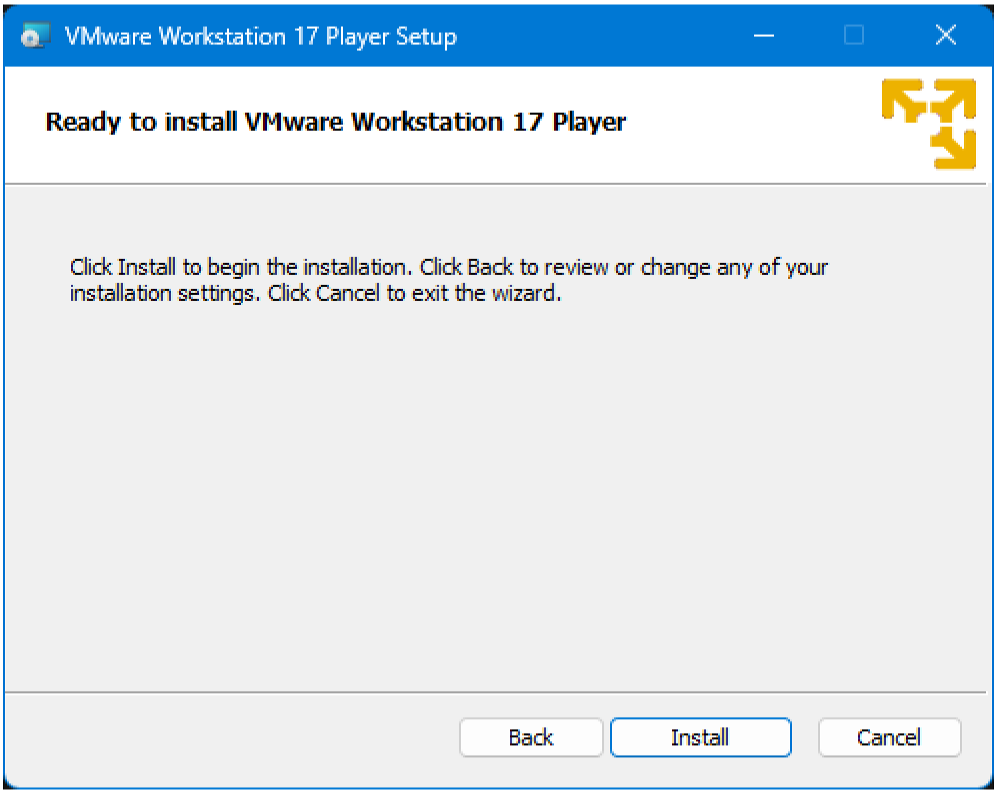
Custom Setup

Select the installation destination and any additional features.

Install to:
C:\Program Files (x86)\VMware\VMware Player\

☐ Enhanced Keyboard Driver (a reboot will be required to use this feature)
This feature requires 10MB on your host drive.

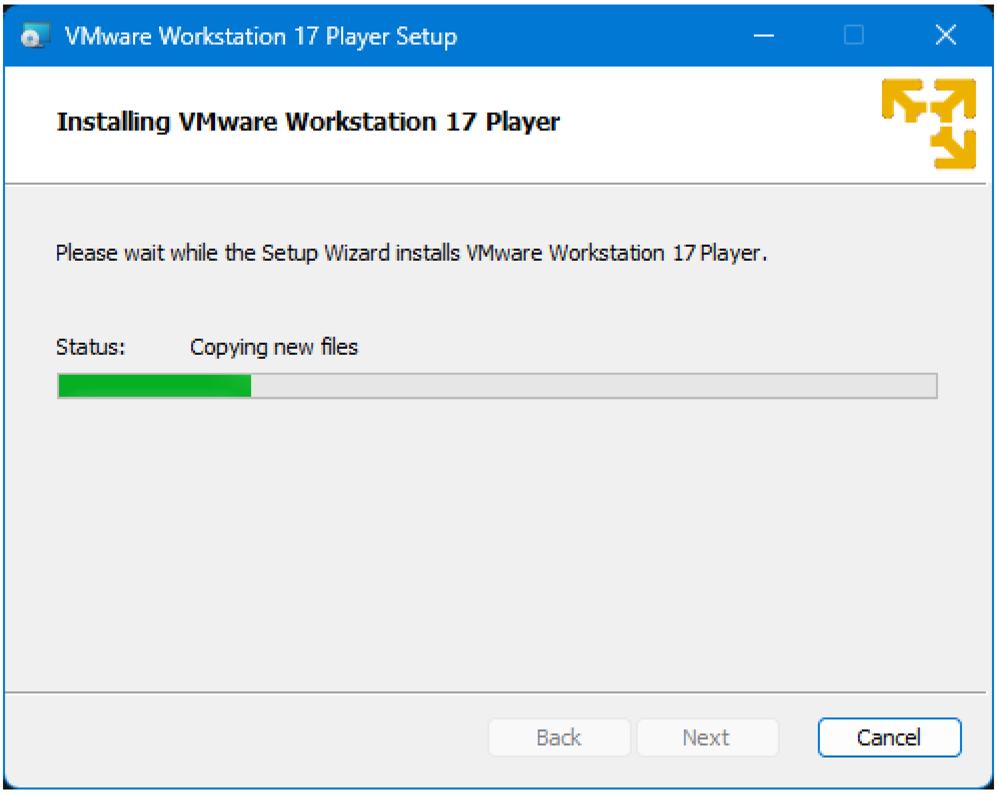
☑ Add VMware Workstation console tools into system PATH



VMware Workstation 17 Player Setup

Ready to install VMware Workstation 17 Player

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

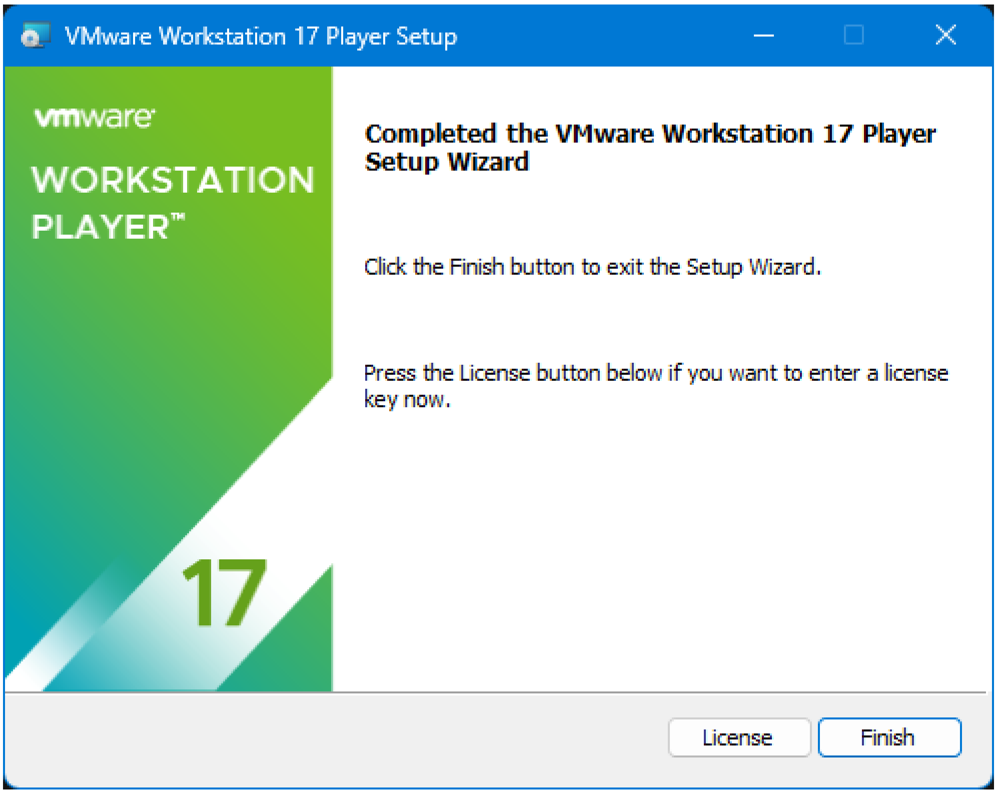


VMware Workstation 17 Player Setup

Installing VMware Workstation 17 Player

Please wait while the Setup Wizard installs VMware Workstation 17 Player.

Status: Copying new files



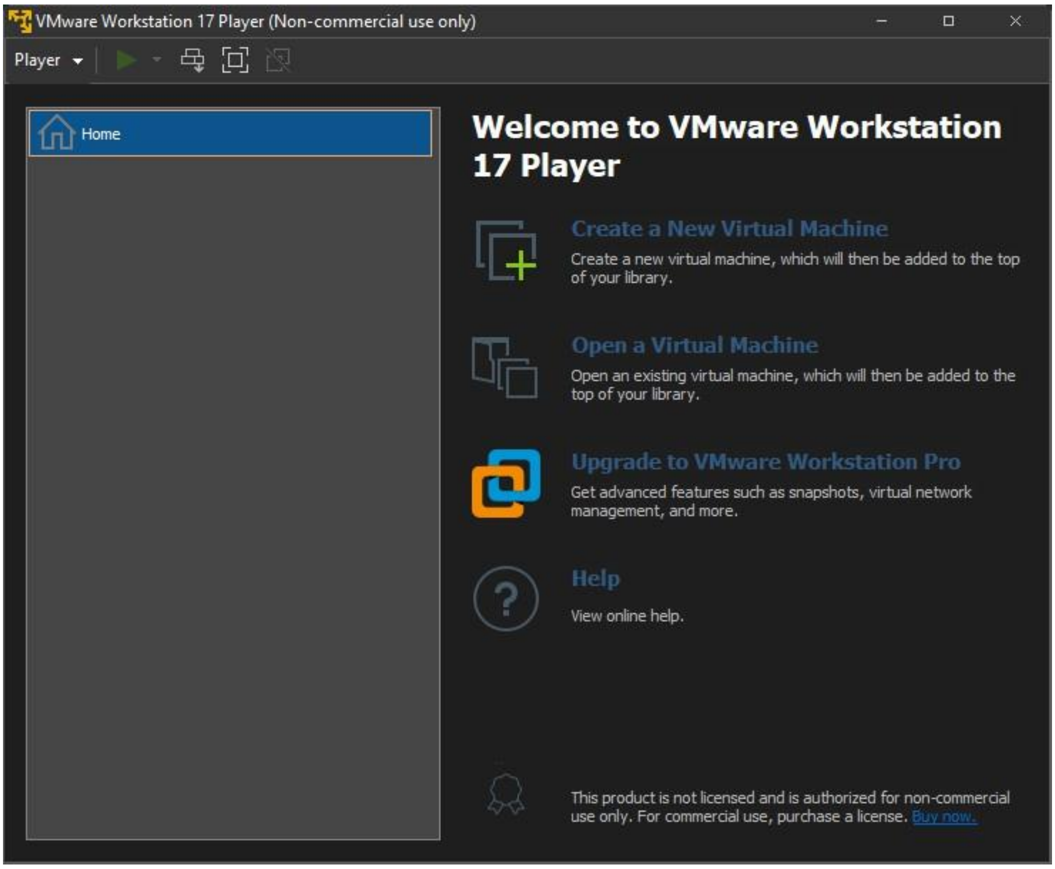
VMware Workstation 17 Player Setup

Completed the VMware Workstation 17 Player Setup Wizard

Click the Finish button to exit the Setup Wizard.

Press the License button below if you want to enter a license key now.

Step 2: After Installing open VMware and select Create a New Virtual Machine Option (Installing Windows XP)



VMware Workstation 17 Player (Non-commercial use only)

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

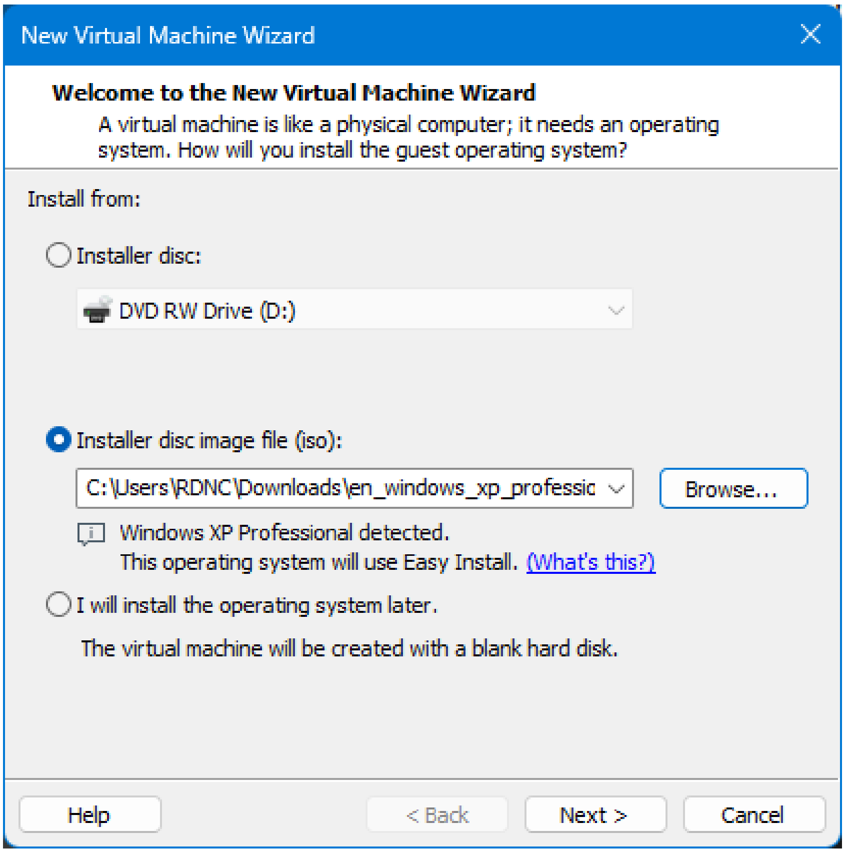
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Step 3: Choose the windows xp ISO



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (D:)

● Installer disc image file (iso):

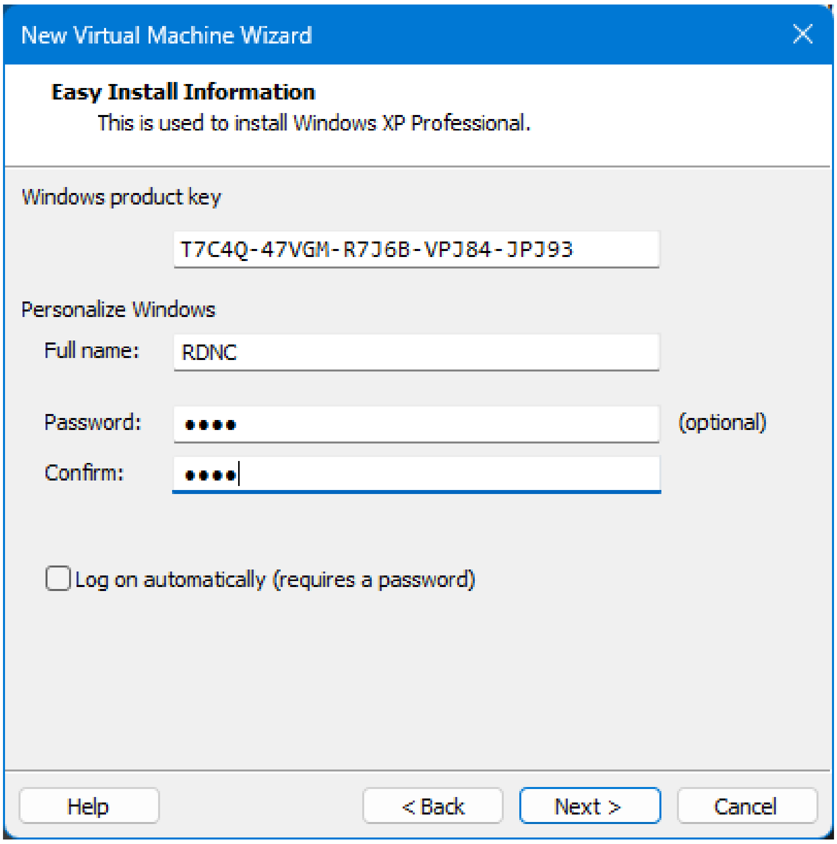
C:\Users\RDNC\Downloads\en_windows_xp_professic

Windows XP Professional detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Step 4: Add product key and create a user with password



New Virtual Machine Wizard

Easy Install Information

This is used to install Windows XP Professional.

Windows product key

T7C4Q-47VGM-R7J6B-VPJ84-JPJ93

Personalize Windows

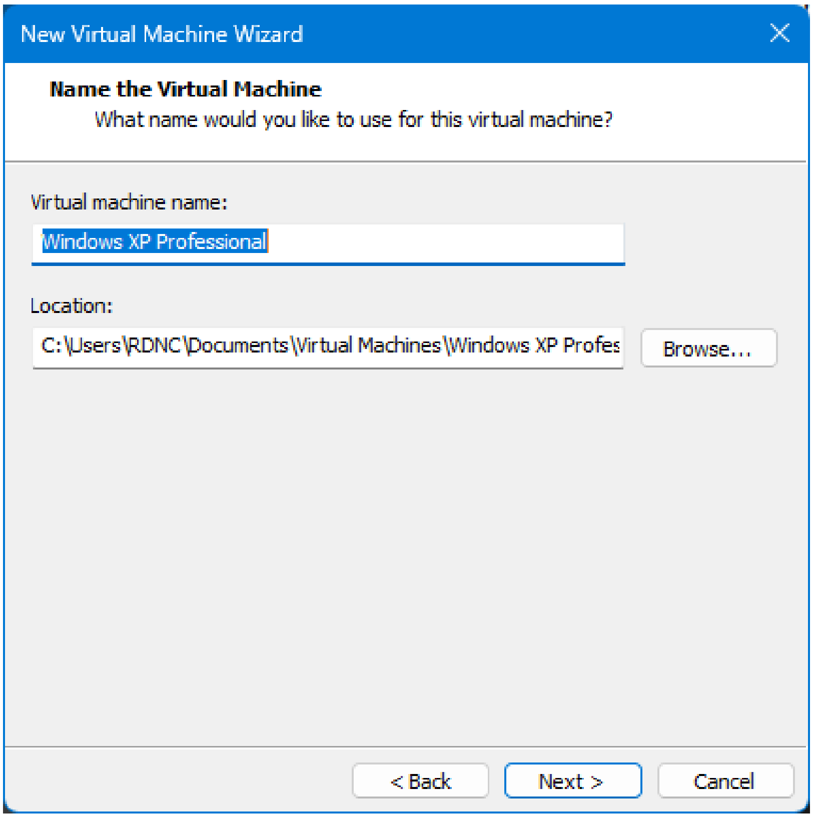
Full name: RDNC

Password: •••• (optional)

Confirm: ••••

□ Log on automatically (requires a password)

Step 5: Give your virtual machine a name



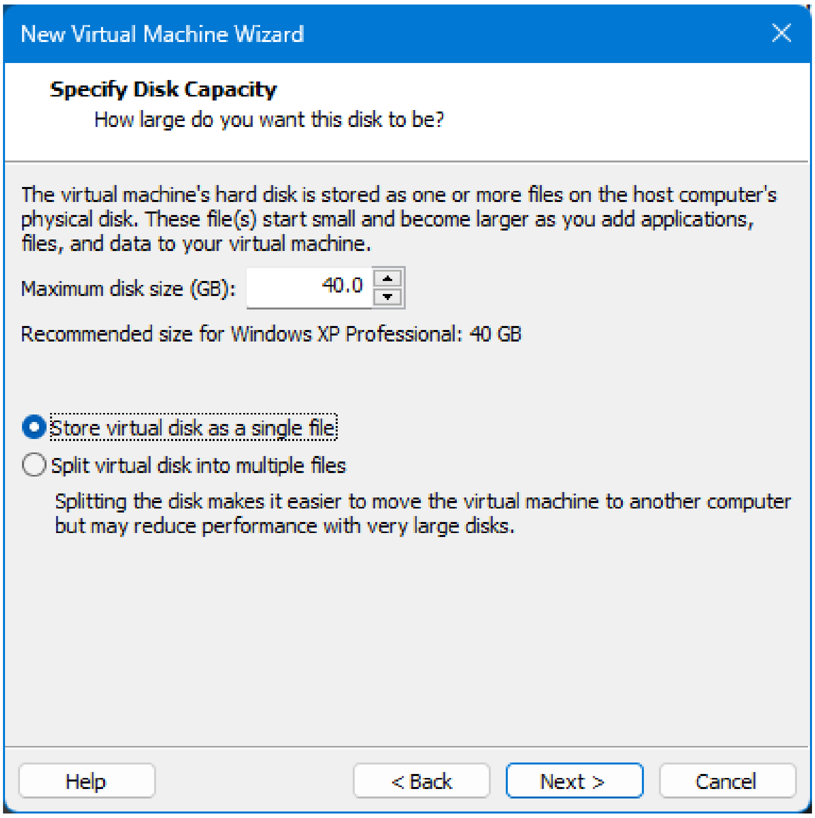
Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Windows XP Professional

Location: C:\Users\RDNC\Documents\Virtual Machines\Windows XP Profes

Step 6: Select disk size (can be left to default option)



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 40.0

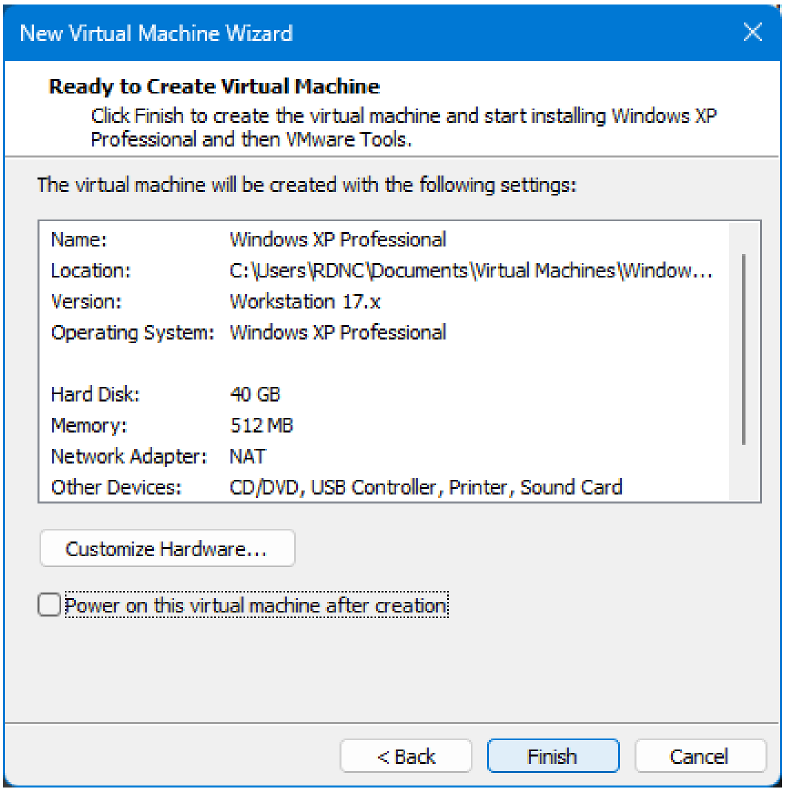
Recommended size for Windows XP Professional: 40 GB

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Step 7: Hit finish and wait for the installation to finish



Ready to Create Virtual Machine

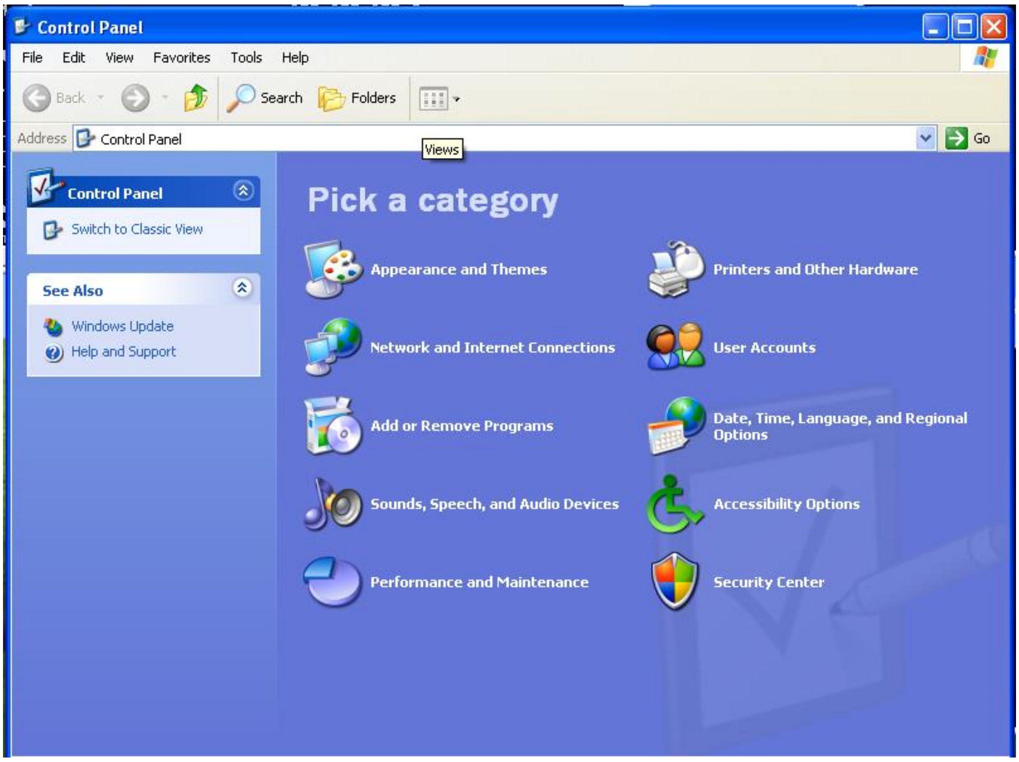
Click Finish to create the virtual machine and start installing Windows XP Professional and then VMware Tools.

The virtual machine will be created with the following settings:

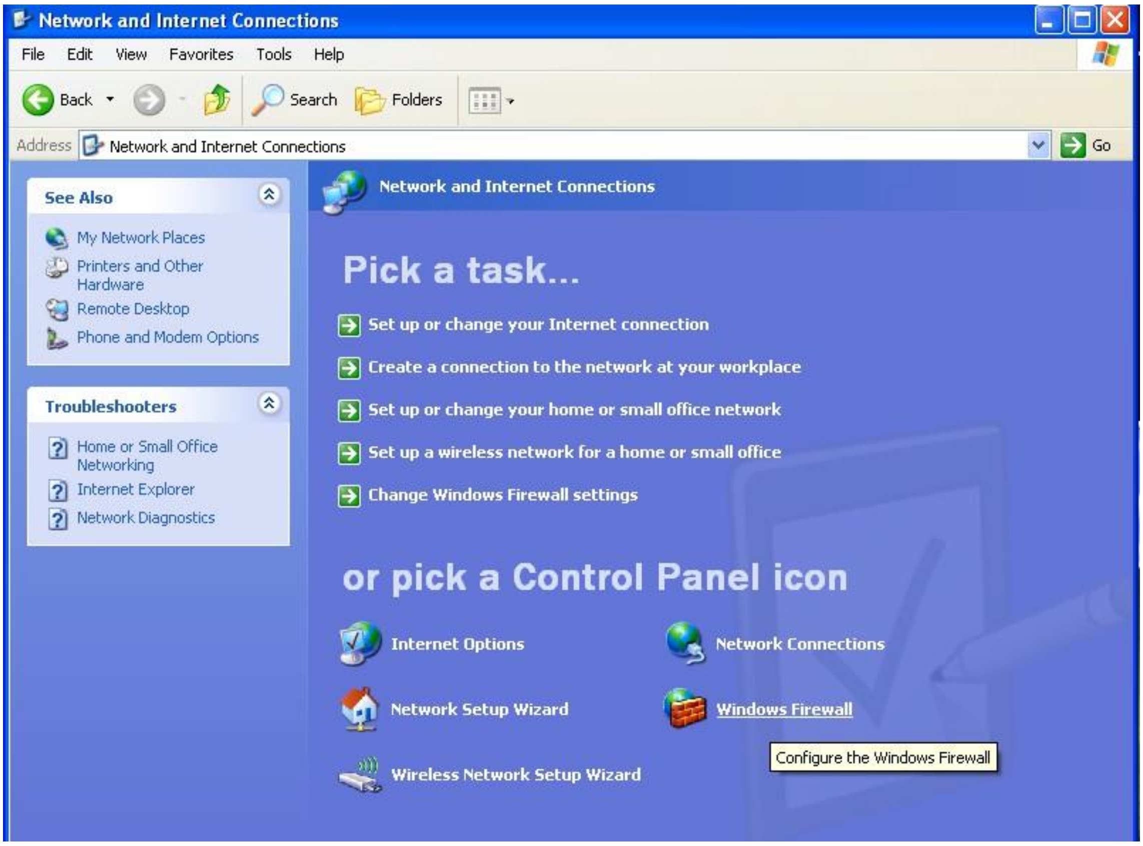
Name:	Windows XP Professional
Location:	C:\Users\RDNC\Documents\Virtual Machines\Window...
Version:	Workstation 17.x
Operating System:	Windows XP Professional
Hard Disk:	40 GB
Memory:	512 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

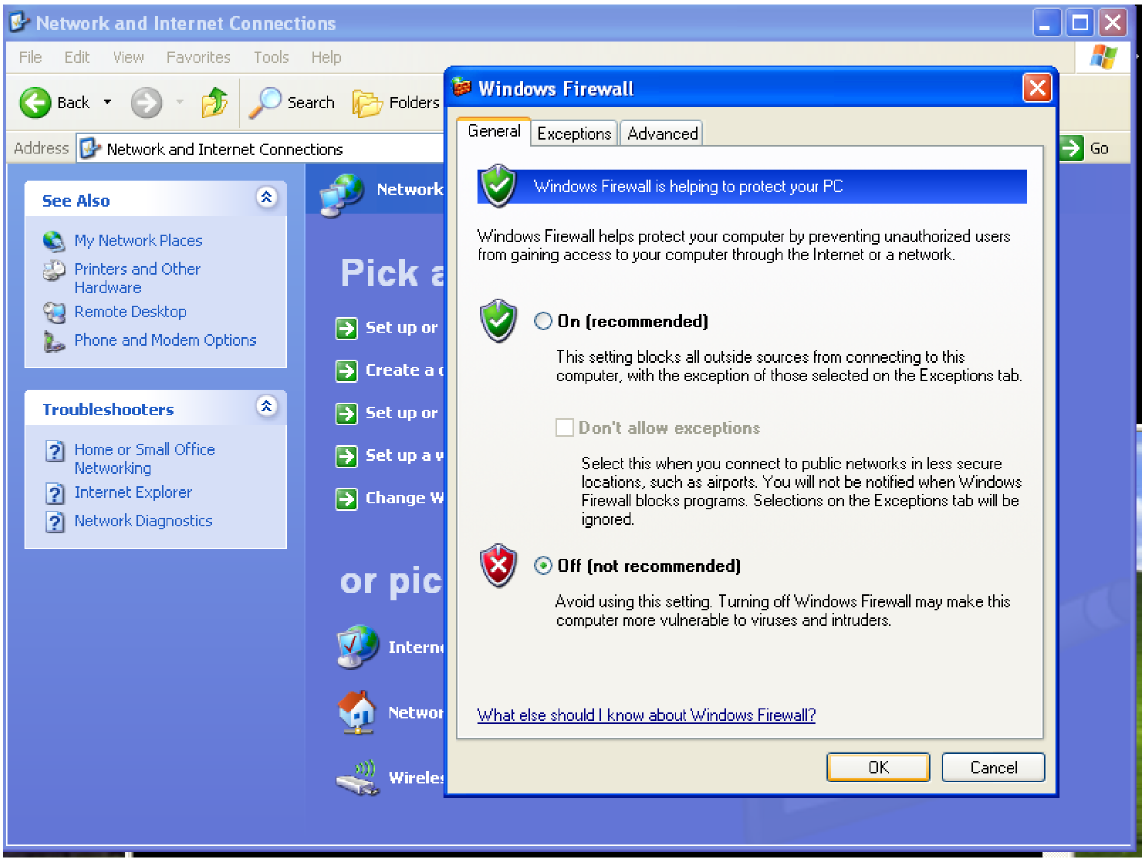
☐ Power on this virtual machine after creation

Step 8: We must disable the Windows firewall to test our exploits/attacks for future practicals. From the start menu select Control Panel > Security Center



Step 9: Select Windows Firewall and turn off the firewall


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Configure the Windows Firewall
Wireless Network Setup Wizard



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ **On (recommended)**

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

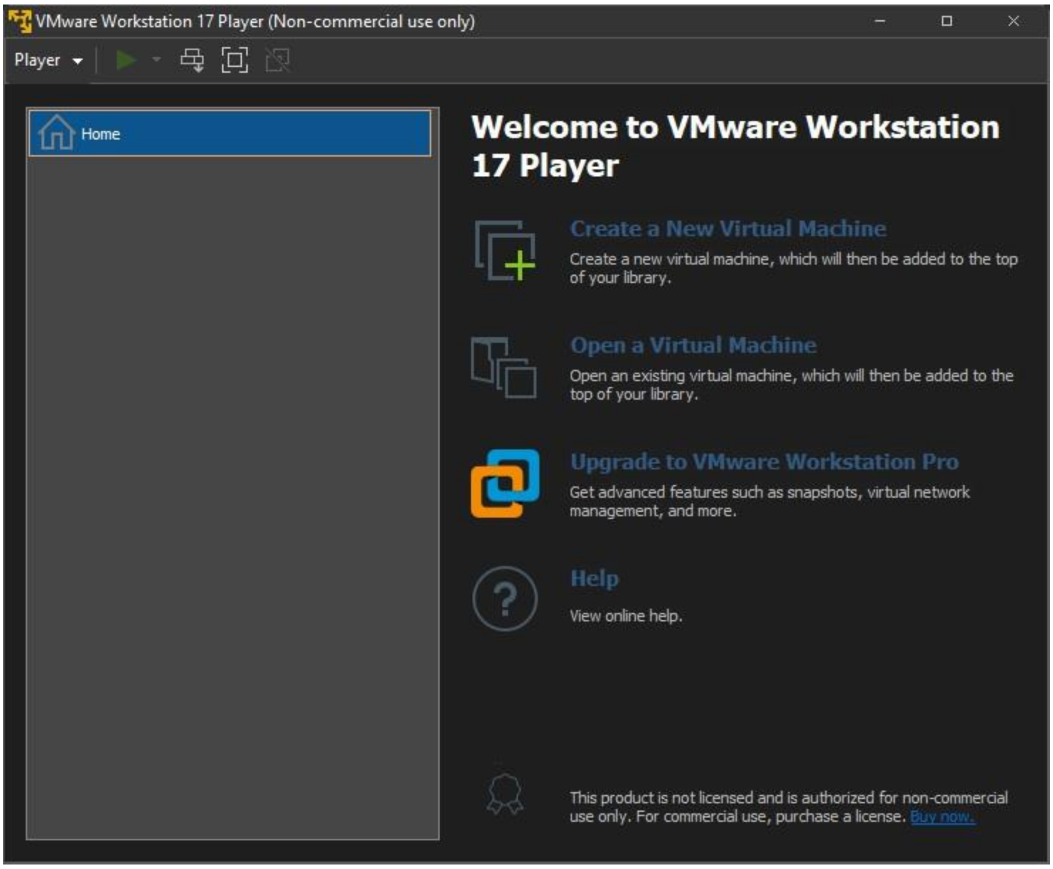
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Step 10: Installing Kali Linux; Open VMware and select Open a Virtual Machine Option



VMware Workstation 17 Player (Non-commercial use only)

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

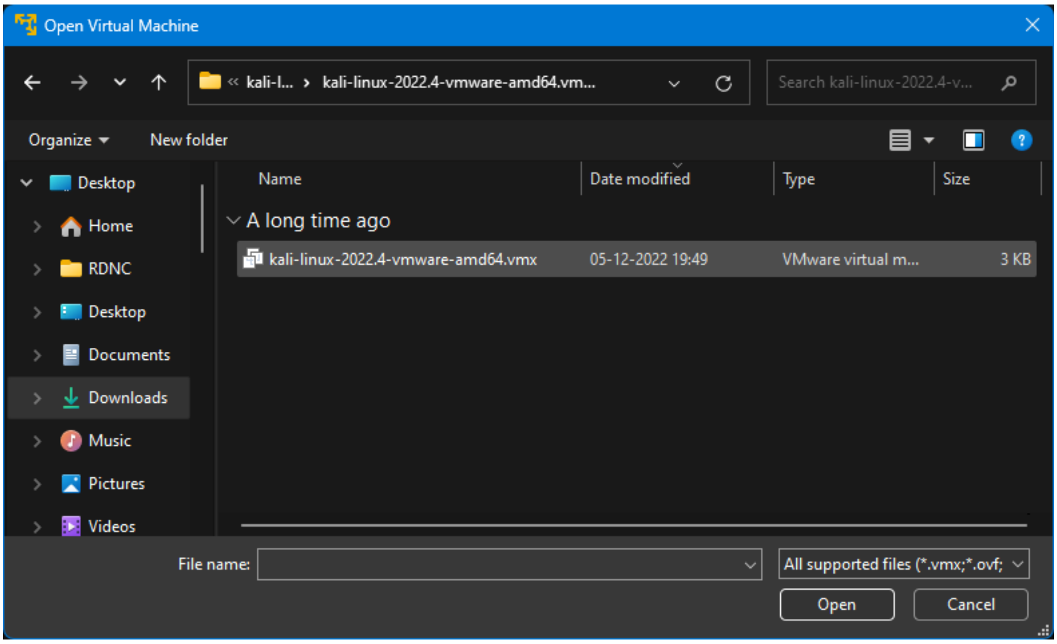
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Step 11: Select The virtual machine file and run it



Open Virtual Machine

« kali-l... › kali-linux-2022.4-vmware-amd64.vm...

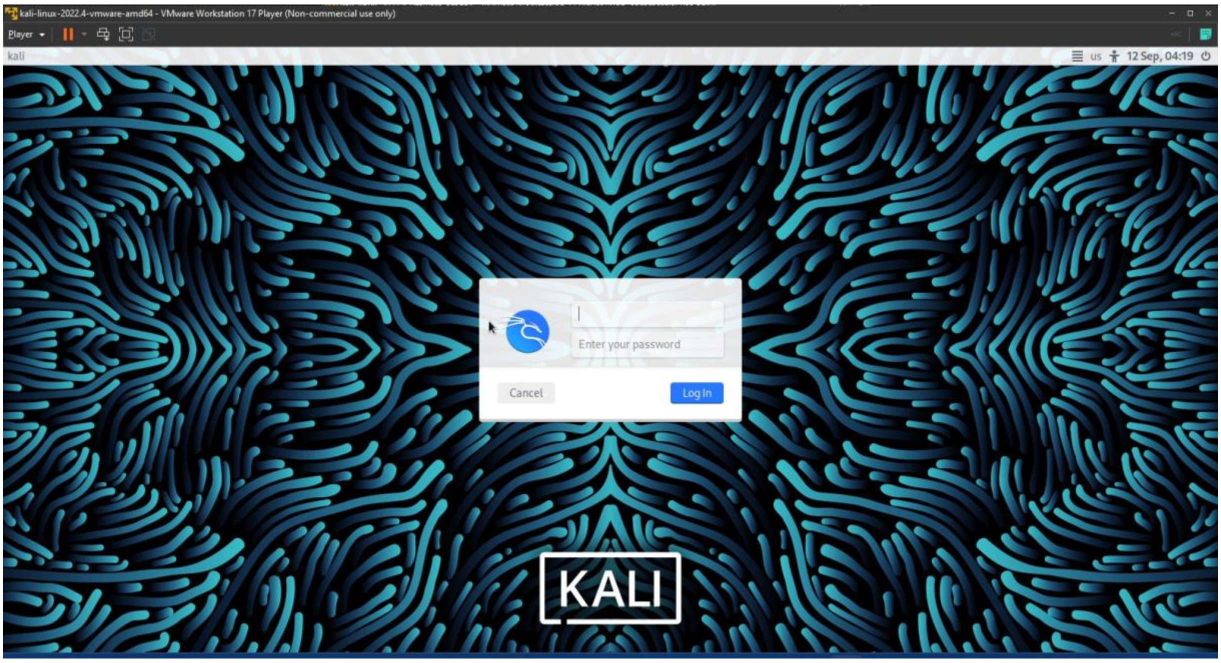
Search kali-linux-2022.4-v...

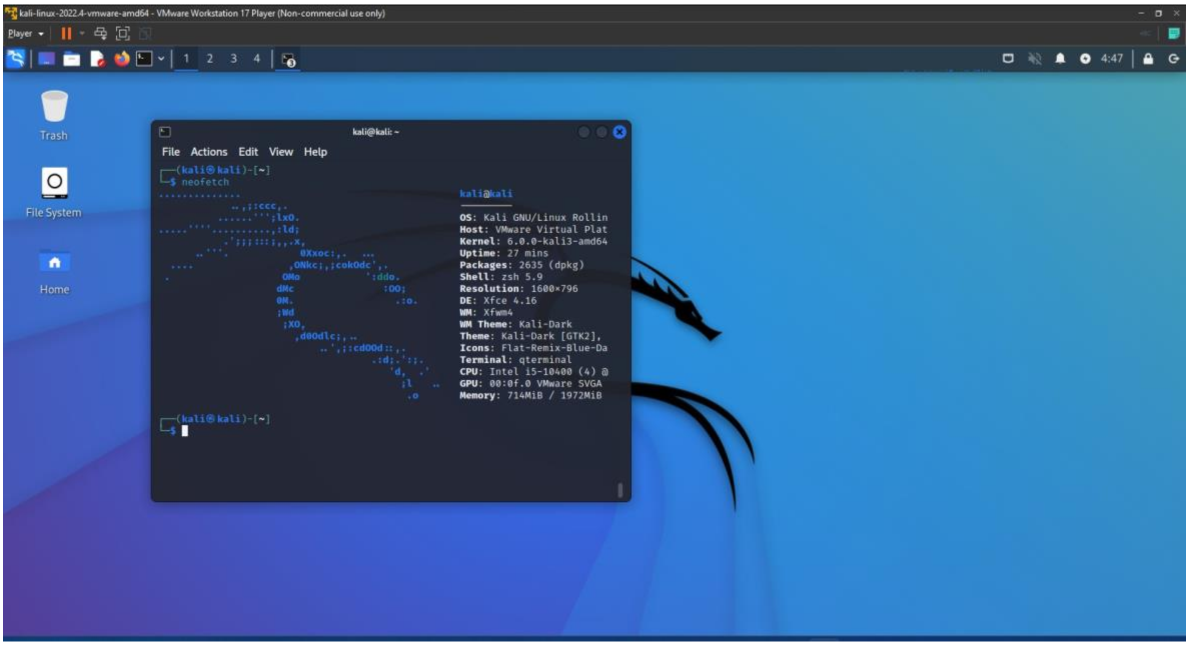
Name	Date modified	Type	Size
A long time ago			
kali-linux-2022.4-vmware-amd64.vmx	05-12-2022 19:49	VMware virtual m...	3 KB

File name:

All supported files (*.vmx;*.ovf;

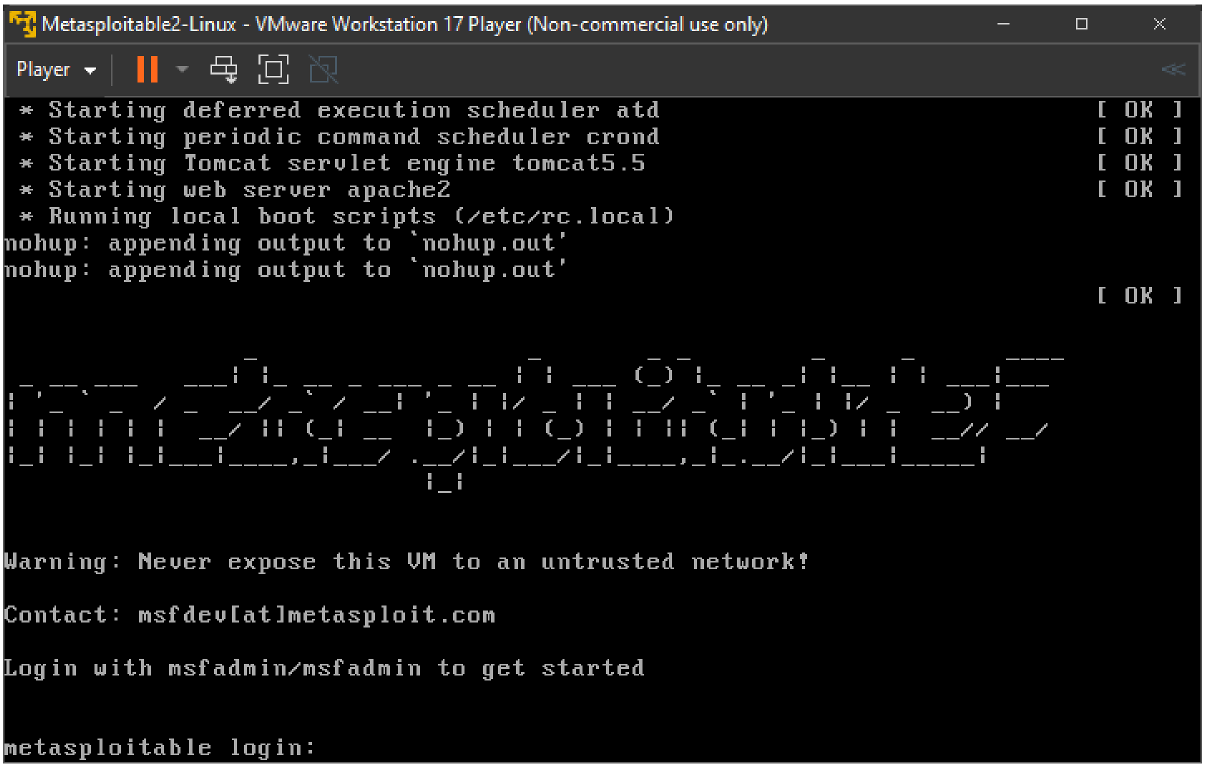
Step 12: Login to your machine (user & pass is “Kali” without quotes)


kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
kali
us
12 Sep, 04:19
Enter your password
Cancel
Log In
KALI


kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
4:47
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ neofetch
                                              kali@kali
                                              ---------
                                              OS: Kali GNU/Linux Rollin
                                              Host: VMware Virtual Plat
                                              Kernel: 6.0.0-kali3-amd64
                                              Uptime: 27 mins
                                              Packages: 2635 (dpkg)
                                              Shell: zsh 5.9
                                              Resolution: 1600×796
                                              DE: Xfce 4.16
                                              WM: Xfwm4
                                              WM Theme: Kali-Dark
                                              Theme: Kali-Dark [GTK2],
                                              Icons: Flat-Remix-Blue-Da
                                              Terminal: qterminal
                                              CPU: Intel i5-10400 (4) @
                                              GPU: 00:0f.0 VMware SVGA
                                              Memory: 714MiB / 1972MiB

┌──(kali㉿kali)-[~]
└─$ 
```

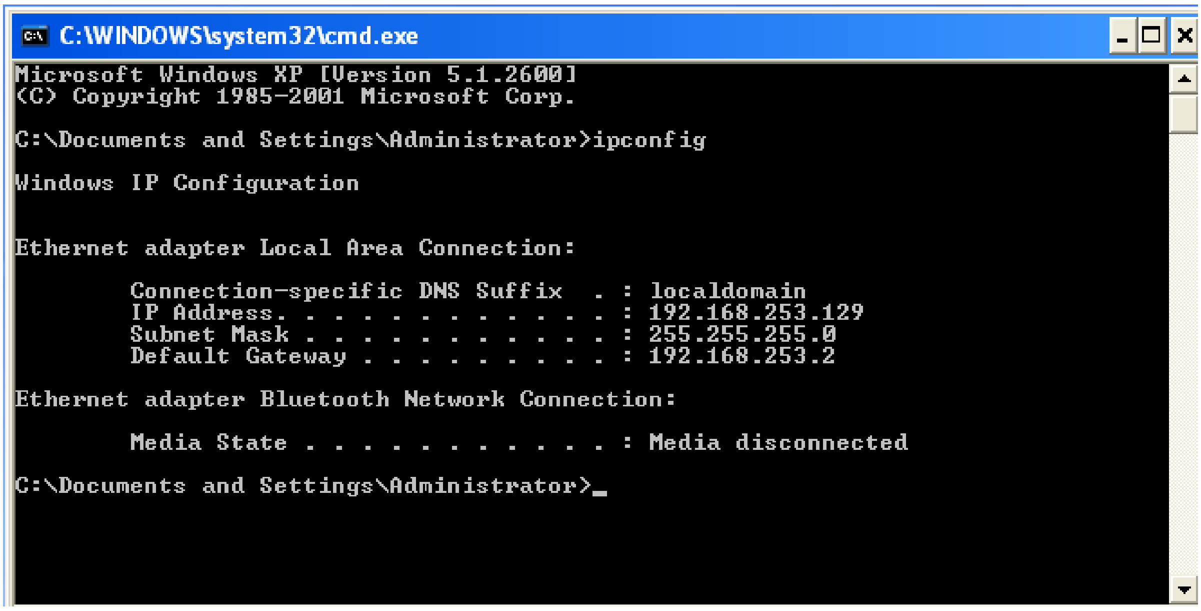
Step 13: Open VM and select Open a Virtual Machine & select the metasploitable file for VMware and run it (user & pass is “msfadmin”)



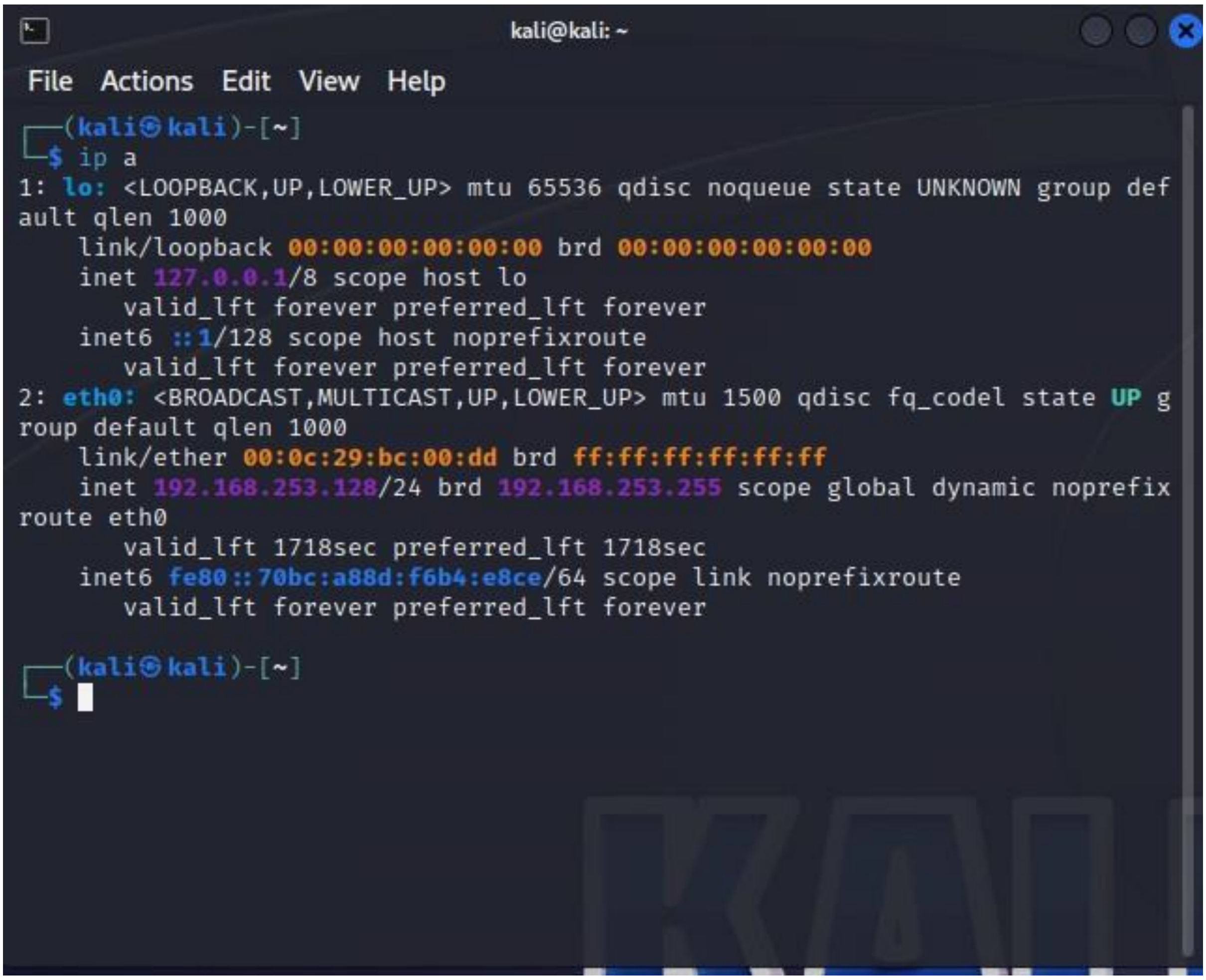
Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player

```
 * Starting deferred execution scheduler atd                        [ OK ]
 * Starting periodic command scheduler crond                        [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                         [ OK ]
 * Starting web server apache2                                      [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                    [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

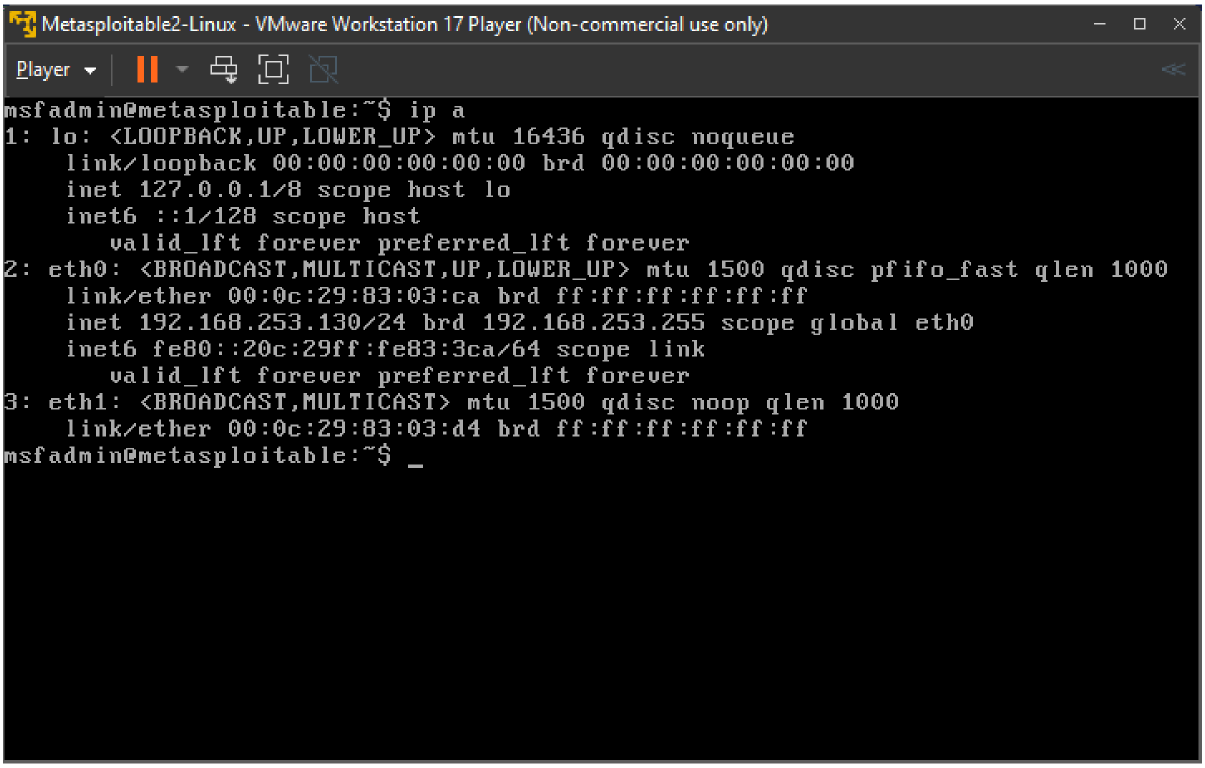
Step 14: Once all the systems are up get the current IP of all the system
For Kali Linux & Metaspoitable use ip a
For Windows XP use ipconfig



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.253.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.253.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_
```



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:bc:00:dd brd ff:ff:ff:ff:ff:ff
    inet 192.168.253.128/24 brd 192.168.253.255 scope global dynamic noprefix
route eth0
       valid_lft 1718sec preferred_lft 1718sec
    inet6 fe80::70bc:a88d:f6b4:e8ce/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

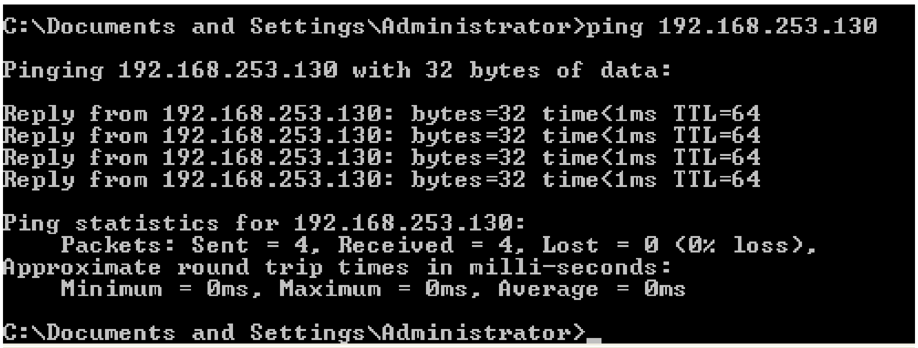

Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:83:03:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.253.130/24 brd 192.168.253.255 scope global eth0
    inet6 fe80::20c:29ff:fe83:3ca/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:83:03:d4 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

In My case the ip of kali = 192.168.253.128, metasploitable = 192.168.253.130, windows xp = 192.168.253.129

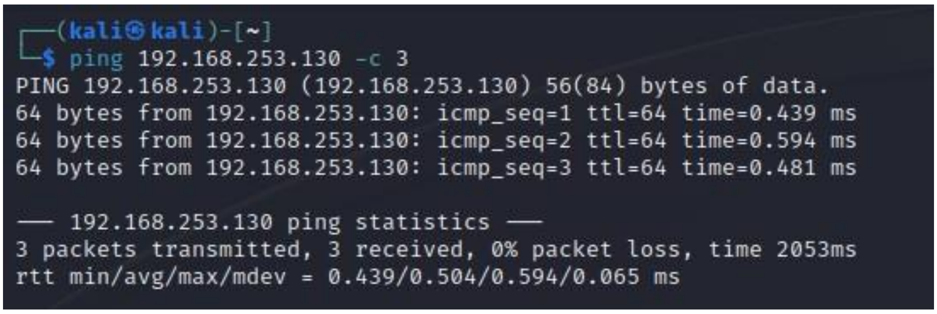
Step 15: Pinging Metasplotable from Kali & Windows

From Windows



```
C:\Documents and Settings\Administrator>ping 192.168.253.130

Pinging 192.168.253.130 with 32 bytes of data:

Reply from 192.168.253.130: bytes=32 time<1ms TTL=64
Reply from 192.168.253.130: bytes=32 time<1ms TTL=64
Reply from 192.168.253.130: bytes=32 time<1ms TTL=64
Reply from 192.168.253.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.253.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

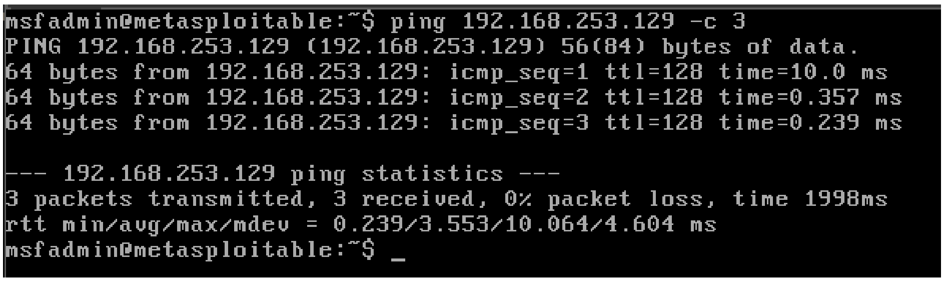
From Kali



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.253.130 -c 3
PING 192.168.253.130 (192.168.253.130) 56(84) bytes of data.
64 bytes from 192.168.253.130: icmp_seq=1 ttl=64 time=0.439 ms
64 bytes from 192.168.253.130: icmp_seq=2 ttl=64 time=0.594 ms
64 bytes from 192.168.253.130: icmp_seq=3 ttl=64 time=0.481 ms

--- 192.168.253.130 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.439/0.504/0.594/0.065 ms
```

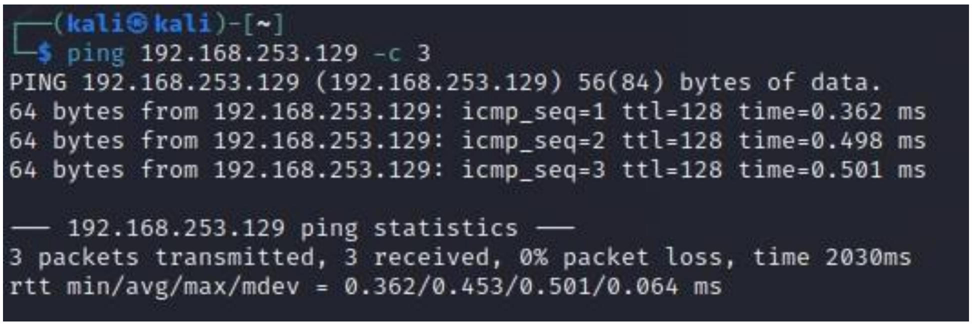
Step 16: Pinging Windows from metasplotable & Kali

From Metasplotable



```
msfadmin@metasploitable:~$ ping 192.168.253.129 -c 3
PING 192.168.253.129 (192.168.253.129) 56(84) bytes of data.
64 bytes from 192.168.253.129: icmp_seq=1 ttl=128 time=10.0 ms
64 bytes from 192.168.253.129: icmp_seq=2 ttl=128 time=0.357 ms
64 bytes from 192.168.253.129: icmp_seq=3 ttl=128 time=0.239 ms

--- 192.168.253.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.239/3.553/10.064/4.604 ms
msfadmin@metasploitable:~$ _
```

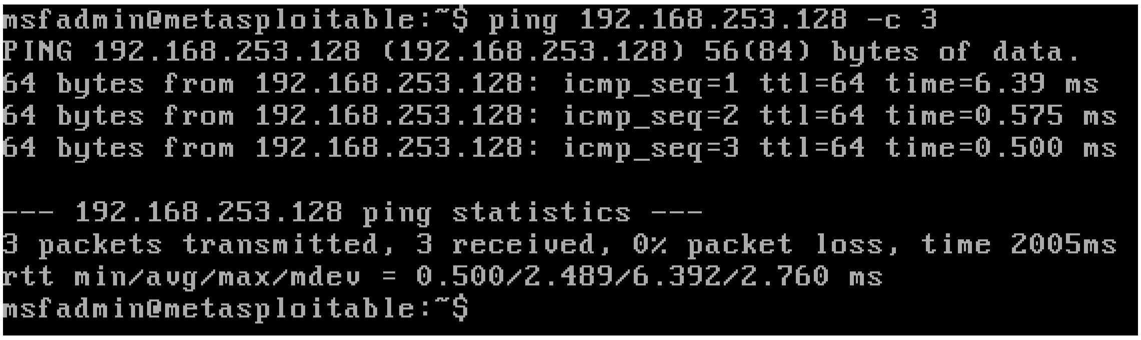
From Kali



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.253.129 -c 3
PING 192.168.253.129 (192.168.253.129) 56(84) bytes of data.
64 bytes from 192.168.253.129: icmp_seq=1 ttl=128 time=0.362 ms
64 bytes from 192.168.253.129: icmp_seq=2 ttl=128 time=0.498 ms
64 bytes from 192.168.253.129: icmp_seq=3 ttl=128 time=0.501 ms

--- 192.168.253.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.362/0.453/0.501/0.064 ms
```

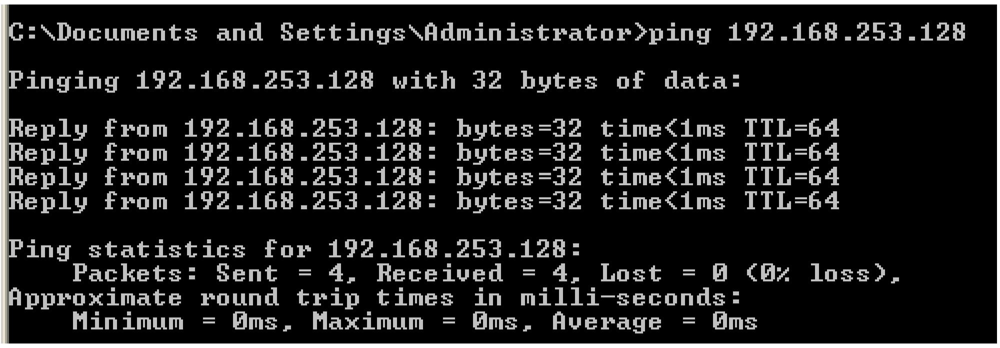
Step 17: Pining Kali from windows & metasplotable

From Metaplotable



```
msfadmin@metasploitable:~$ ping 192.168.253.128 -c 3
PING 192.168.253.128 (192.168.253.128) 56(84) bytes of data.
64 bytes from 192.168.253.128: icmp_seq=1 ttl=64 time=6.39 ms
64 bytes from 192.168.253.128: icmp_seq=2 ttl=64 time=0.575 ms
64 bytes from 192.168.253.128: icmp_seq=3 ttl=64 time=0.500 ms

--- 192.168.253.128 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.500/2.489/6.392/2.760 ms
msfadmin@metasploitable:~$
```

From Windows



```
C:\Documents and Settings\Administrator>ping 192.168.253.128

Pinging 192.168.253.128 with 32 bytes of data:

Reply from 192.168.253.128: bytes=32 time<1ms TTL=64
Reply from 192.168.253.128: bytes=32 time<1ms TTL=64
Reply from 192.168.253.128: bytes=32 time<1ms TTL=64
Reply from 192.168.253.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.253.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```