

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MÔN THỰC TẬP CƠ SỞ



BÀI THỰC HÀNH 1.6
PHÂN TÍCH LOG HỆ THỐNG

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm: 09

HÀ NỘI, THÁNG 03/2025

MỤC LỤC

MỤC LỤC	1
DANH MỤC CÁC HÌNH VẼ	2
I. GIỚI THIỆU CHUNG	4
1. Mục đích	4
2. Lý thuyết	4
2.1. grep - Lệnh tìm kiếm chuỗi trong tệp văn bản	4
2.2. gawk - Công cụ xử lý và trích xuất dữ liệu từ log	5
2.3. find - Lệnh phân tích log trên Windows	6
2.4. secure - Log bảo mật trên Linux	6
2.5. access_log - Log truy cập web server	6
2.6. xHydra - Công cụ brute-force mật khẩu	7
2.7. Một số lệnh phổ biến khác	8
I. NỘI DUNG THỰC HÀNH	9
1. Chuẩn bị môi trường	9
2. Thực hành	12
2.1. Phân tích log sử dụng grep trong Linux	12
2.2. Phân tích log sử dụng gawk trong Linux	16
2.3. Phân tích log sử dụng find trong Windows	19
TÀI LIỆU THAM KHẢO	23

DANH MỤC CÁC HÌNH VẼ

Hình 1. Ví dụ dòng log	7
Hình 2. Giao diện xHydra	7
Hình 3. Topo mạng cần chuẩn bị	9
Hình 4. Máy Kali Linux attack 1	9
Hình 5. Máy Windows attack	10
Hình 6. Ubuntu Linux victim	10
Hình 7. Windows Server victim	10
Hình 9. Máy Windows Server 2019 victim	11
Hình 10. Cấu hình pfSense	11
Hình 11. Scan máy Linux victim	12
Hình 12. Kiểm tra trạng thái dịch vụ Apache	12
Hình 13. Kiểm tra tường lửa trên Ubuntu	13
Hình 14. Kiểm tra cổng 80	13
Hình 15. Truy cập trang web của victim	14
Hình 16. Tải trang web	14
Hình 17. Dùng lệnh “grep” tìm kiếm từ “test”	15
Hình 18. Di chuyển đến vị trí file ghi log truy nhập	15
Hình 19. Các lệnh grep	15
Hình 20. Kết quả lệnh grep	16
Hình 21. Ssh vào máy Ubuntu victim	16
Hình 22. Tạo tài khoản mới cho máy victim trên máy attack	17
Hình 23. Đổi mật khẩu	17
Hình 24. Mở file auth.log trên máy victim	17
Hình 25. Các sự kiện liên quan đến tài khoản nguyenvanhung	18
Hình 26. In toàn bộ dòng chứa thông tin về tài khoản nguyenvanhung	19
Hình 27. In cột thời gian và tên tài khoản	19
Hình 28. In các dòng liên quan đến tài khoản nguyenvanhung	19
Hình 29. Kiểm tra trạng thái FTP	19
Hình 30. Nhập thông tin mục tiêu trên giao diện Target	20

<i>Hình 31. Nhập thông tin username và password để chuẩn bị tấn công</i>	<i>21</i>
<i>Hình 32. Danh sách mật khẩu</i>	<i>21</i>
<i>Hình 33. Thành công tìm ra mật khẩu</i>	<i>21</i>
<i>Hình 34. Kiểm tra log FTP Server</i>	<i>22</i>

I. GIỚI THIỆU CHUNG

1. Mục đích

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

- Phân tích log sử dụng grep/gawk trong Linux
- Phân tích log sử dụng find trong Windows
- Tìm hiểu về Windows Event Viewer và auditing
- Phân tích event log trong Windows

2. Lý thuyết

System Log (Log hệ thống) là các tệp ghi lại toàn bộ hoạt động của hệ thống, phần mềm hoặc người dùng. Việc phân tích log giúp:

- Giám sát hệ thống: Kiểm tra hoạt động của máy chủ và ứng dụng.
- Phát hiện tấn công: Nhận diện các hành vi bất thường (như brute-force, truy cập trái phép).
- Xử lý sự cố: Xác định lỗi hệ thống, ứng dụng.

Log hệ thống phổ biến gồm:

- Trên Linux : /var/log/syslog, /var/log/auth.log, /var/log/httpd/access_log
- Trên Windows: Event Viewer Logs, IIS Log, FTP Log

2.1. grep - Lệnh tìm kiếm chuỗi trong tệp văn bản

grep (Global Regular Expression Print) là lệnh trên Linux dùng để tìm kiếm các dòng chứa từ khóa hoặc mẫu biểu thức chính quy trong tệp văn bản.

Nó được sử dụng rộng rãi trong việc phân tích log, kiểm tra lỗi, lọc dữ liệu và kết hợp với các công cụ khác như awk, sed.

Cú pháp cơ bản: *grep [tùy chọn] "chuỗi_tìm_kiểm" tệp_log*

Giải thích:

- "chuỗi_tìm_kiểm": Chuỗi hoặc mẫu regex cần tìm.
- tệp_log: Tệp cần tìm kiếm dữ liệu.
- Tùy chọn phổ biến:
 - -i → Không phân biệt chữ hoa/thường
 - -v → Hiển thị các dòng không chứa từ khóa
 - -c → Đếm số dòng khớp với từ khóa

- -n → Hiển thị số dòng chứa từ khóa

Ví dụ:

- Tìm tất cả các dòng chứa từ "error" trong file /var/log/syslog:
grep "error" /var/log/syslog
- Tìm các dòng có chứa "failed" nhưng không phân biệt chữ hoa/thường:
grep -i "failed" /var/log/auth.log
- Tìm tất cả các dòng KHÔNG chứa "success":
grep -v "success" /var/log/syslog
- Đếm số lần xuất hiện của từ "root":
grep -c "root" /var/log/auth.log
- Hiển thị dòng và số dòng có chứa từ "ssh":
grep -n "ssh" /var/log/auth.log

2.2. gawk - Công cụ xử lý và trích xuất dữ liệu từ log

Gawk (GNU awk) là một công cụ xử lý dữ liệu dạng văn bản, đặc biệt hữu ích khi làm việc với log hệ thống. Nó giúp lọc dữ liệu, định dạng lại dữ liệu, thực hiện tính toán trên log, giúp trích xuất thông tin quan trọng từ các tệp log lớn.

Cú pháp cơ bản: *gawk '{ biểu_thức }' tệp_log*

Giải thích:

- Biểu thức: Các lệnh thao tác với từng dòng trong file.
- Tệp log: Tệp chứa dữ liệu cần xử lý.
- gawk sử dụng dấu phân cách mặc định là khoảng trắng, nhưng có thể thay đổi bằng -F

Ví dụ:

- In cột đầu tiên của file log (\$1 là cột thứ nhất):
gawk '{ print \$1 }' /var/log/auth.log
- Lọc ra các dòng chứa từ "root" và hiển thị cột 1, 4:
gawk '/root/ {print \$1, \$4}' /var/log/auth.log
- Đếm số lần đăng nhập thất bại:
gawk '/Failed/ { count++ } END { print count }' /var/log/auth.log
- Chia dữ liệu theo dấu : thay vì khoảng trắng:
gawk -F':' '{ print \$1 }' /etc/passwd

2.3. find - Lệnh phân tích log trên Windows

Lệnh `find` trên Windows tương tự `grep` trên Linux, dùng để tìm kiếm chuỗi trong nội dung tệp văn bản.

Cú pháp cơ bản: `find "chuỗi_tìm_kiểm" file.log`

Tùy chọn:

- `/i`: Không phân biệt hoa/thường.
- `/c`: Đếm số lần xuất hiện.
- `/v`: Hiển thị các dòng không chứa chuỗi.

Ví dụ:

- Tìm từ "error" trong file log:

```
find "error" C:\Windows\System32\LogFiles\logfile.log
```

- Đếm số lần xuất hiện của từ "failed":

```
find /c "failed" C:\Windows\System32\LogFiles\logfile.log
```

- Tìm chuỗi trong nhiều file log:

```
find "login" C:\Windows\System32\LogFiles\*.log
```

2.4. secure - Log bảo mật trên Linux

`/var/log/secure` là tệp log quan trọng trên hệ thống Linux, ghi lại thông tin về các sự kiện bảo mật như:

- Đăng nhập và đăng xuất của người dùng.
- Lỗi xác thực do nhập sai mật khẩu.
- Hoạt động SSH trên hệ thống.

Ví dụ một số lệnh phân tích log secure:

- Xem log đăng nhập thành công:

```
grep "Accepted" /var/log/secure
```

- Tìm tất cả các lần đăng nhập thất bại:

```
grep "Failed password" /var/log/secure
```

- Xem log đăng nhập bằng SSH:

```
grep "sshd" /var/log/secure
```

2.5. access_log - Log truy cập web server

`/var/log/httpd/access_log` hoặc `/var/log/nginx/access.log` là nơi lưu lại tất cả yêu cầu HTTP đến máy chủ web.

Cấu trúc điển hình dòng log: `192.168.1.10 - - [17/Mar/2024:12:34:56 +0000] "GET /index.html HTTP/1.1" 200 1234`

- 192.168.1.10: Địa chỉ IP của client.
- [17/Mar/2024:12:34:56 +0000]: Thời gian truy cập.
- "GET /index.html HTTP/1.1": Loại yêu cầu HTTP.
- 200: Mã trạng thái HTTP.
- 1234: Kích thước phản hồi.

```
192.168.100.3 - - [19/Mar/2025:16:04:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
```

Hình 1. Ví dụ dòng log

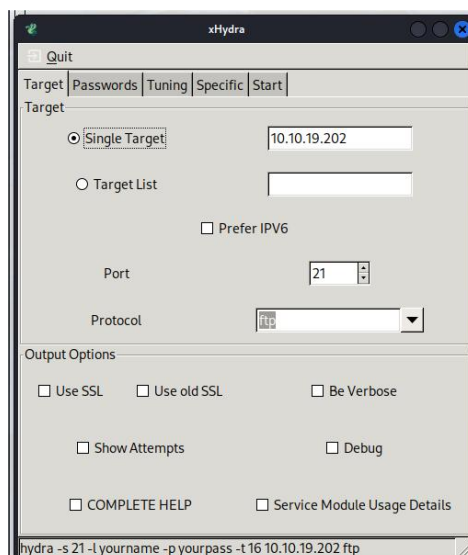
Một số lệnh phân tích access_log:

- Tìm tất cả yêu cầu từ một IP cụ thể:
`grep "192.168.1.10" /var/log/httpd/access_log`
- Lọc tất cả các lỗi 404:
`grep " 404 " /var/log/httpd/access_log`
- Đếm số lượt truy cập từ một IP:
`grep "192.168.1.10" /var/log/httpd/access_log | wc -l`

2.6. xHydra - Công cụ brute-force mật khẩu

Hydra là công cụ brute-force tự động để kiểm tra mật khẩu trên nhiều giao thức khác nhau, như FTP, SSH, HTTP.

xHydra là phiên bản giao diện đồ họa của Hydra.



Hình 2. Giao diện xHydra

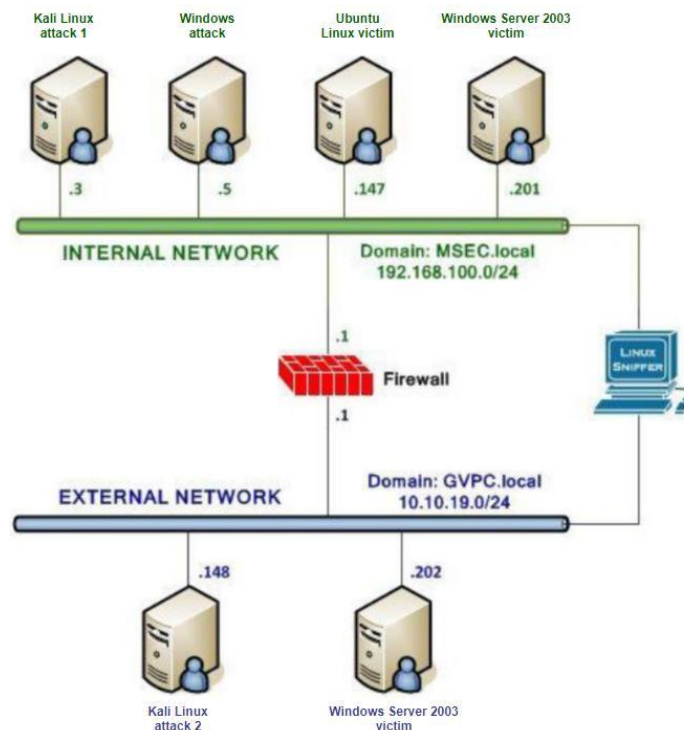
2.7. Một số lệnh phổ biến khác

Lệnh	Chức năng	Tùy chọn	Cú pháp
cat	Hiển thị toàn bộ nội dung file log		cat file_log
tail	Xem log theo thời gian thực, hiển thị dòng cuối file log	-f: Theo dõi log trực tiếp -n số: Hiển thị số dòng cuối cùng	tail [tùy chọn] file_log
head	Hiển thị các dòng đầu tiên trong file log	-n số: Hiển thị số dòng đầu tiên	head [tùy chọn] file_log
less	Xem nội dung log theo trang, hỗ trợ cuộn lên/xuống		less file_log
sort	Sắp xếp dữ liệu log theo thứ tự bảng chữ cái hoặc số	-r: Sắp xếp ngược -n: Sắp xếp theo số	sort [tùy chọn] file_log
uniq	Loại bỏ các dòng trùng lặp trong log	-c: Đếm số lần xuất hiện của từng dòng	uniq [tùy chọn] file_log
wc	Đếm số dòng, từ, ký tự trong file log	-l: Đếm số dòng -w: Đếm số từ -c: Đếm số ký tự	wc [tùy chọn] file_log

I. NỘI DUNG THỰC HÀNH

1. Chuẩn bị môi trường

- Phần mềm VMWare Workstation
- Các file máy ảo VMWare và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux.
- Chú ý: chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5.



Hình 3. Topo mạng cần chuẩn bị

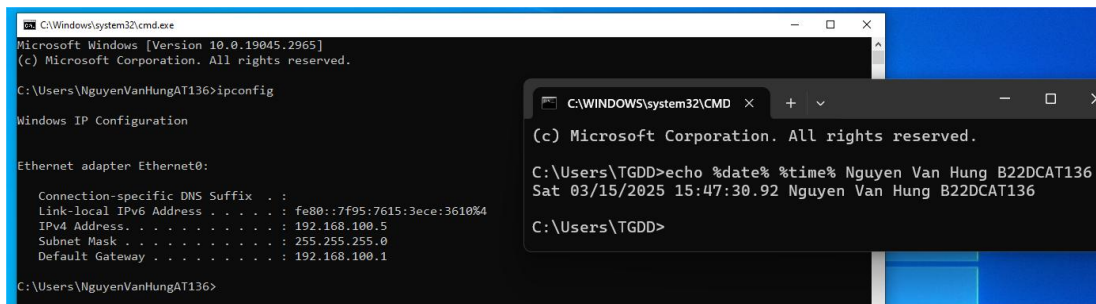
- Cấu hình các máy Internal Network:
 - Máy Kali Linux Attack 1:

```
(nguyenvanhungb22dcat136@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:febc:1b61 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bc:1b:61 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 60 (60.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2878 (2.8 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

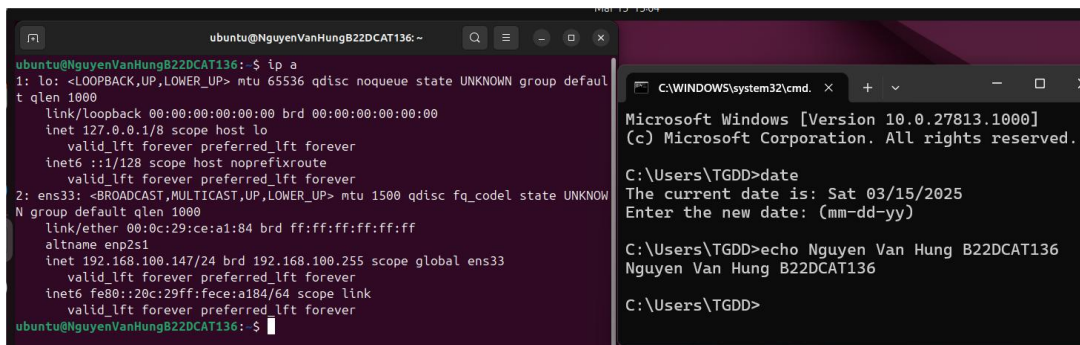
Hình 4. Máy Kali Linux attack 1

- Máy Windows attack:



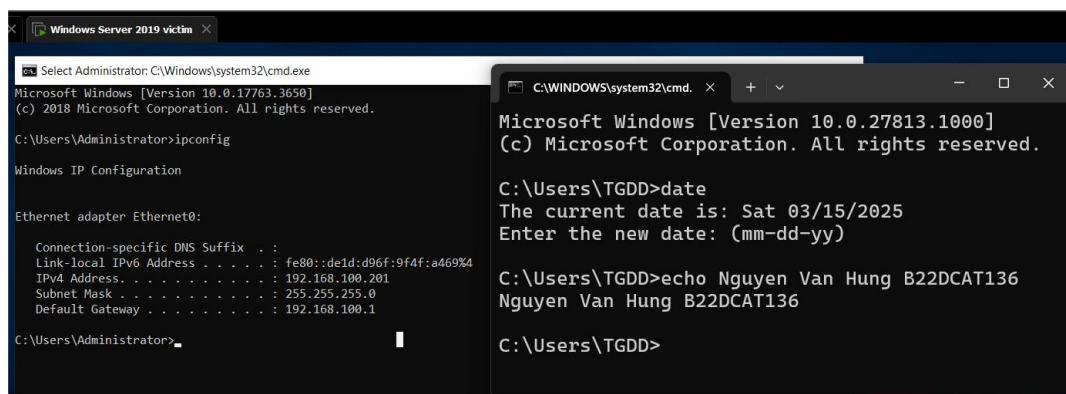
Hình 5. Máy Windows attack

- Ubuntu Linux victim



Hình 6. Ubuntu Linux victim

- Windows Server 2019 victim



Hình 7. Windows Server victim

- Cấu hình các máy External Network:

- Máy Kali Linux Attack 2:

```
(nguyenvanhungb22dcat136@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.148 netmask 255.255.255.0 broadcast 10.10.19.255
    inet6 fe80::20c:29ff:fe06:b719 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:06:b7:19 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 180 (180.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 242 bytes 16704 (16.3 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<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 132 bytes 12260 (11.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 132 bytes 12260 (11.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 8. Máy Kali Linux attack 2

- Máy Windows Server 2019 victim:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>echo Nguyen Van Hung B22DCAT136
Nguyen Van Hung B22DCAT136

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1311:e6af:baa9:c1c2%4
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1
```

Hình 9. Máy Windows Server 2019 victim

Cấu hình tường lửa:

```
C:\WINDOWS\system32\cmd. x + v - □

C:\Users\TGDD>echo %date% Nguyen Van Hung B22DCAT136
Wed 03/19/2025 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.10.19.1/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
```

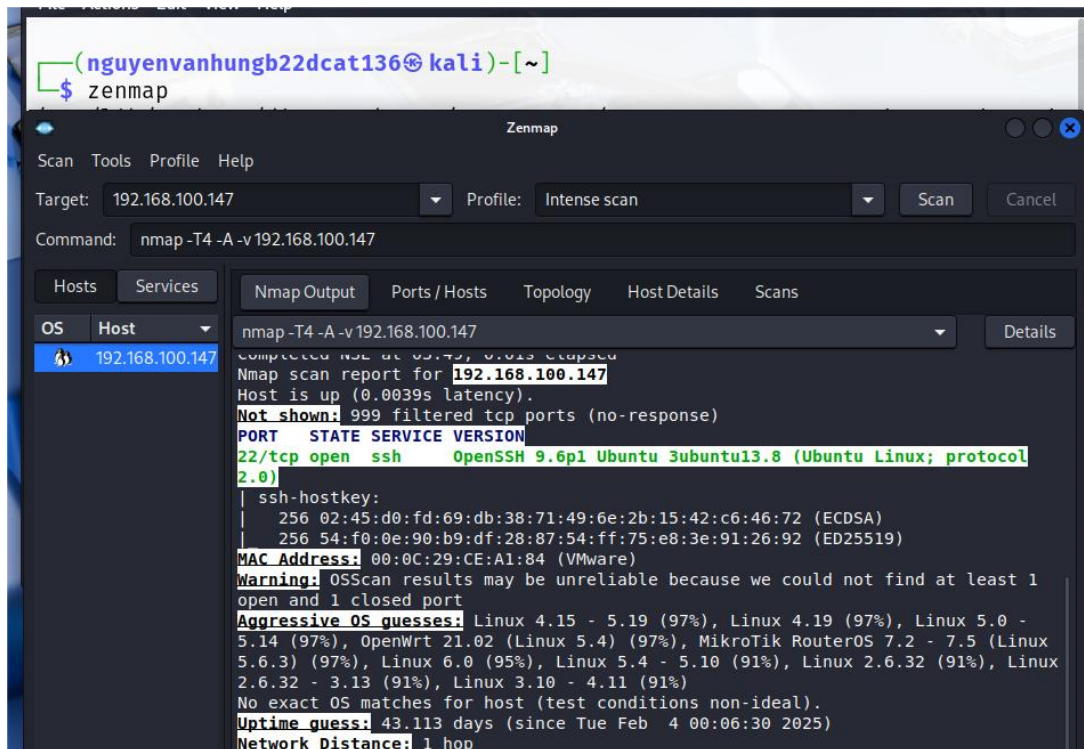
Hình 10. Cấu hình pfSense

2. Thực hành

2.1. Phân tích log sử dụng grep trong Linux

Trên máy Kali Linux attack trong mạng Internal, khởi chạy zenmap

Nhập IP máy Linux victim 192.168.100.147, nhấn Scan.



Hình 11. Scan máy Linux victim

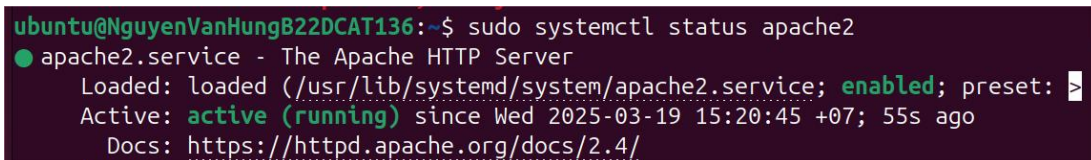
Nếu cổng 80 chưa mở, chuyển sang máy Linux victim.

Nếu chưa cài đặt Apache, cài đặt bằng lệnh:

```
apt update
```

```
apt install apache2 -y
```

Kiểm tra trạng thái dịch vụ: `systemctl status apache2`



Hình 12. Kiểm tra trạng thái dịch vụ Apache

Kiểm tra cổng 80 có bị tường lửa chặn không: `sudo ufw status`

Nếu tường lửa đang bật và chưa cho phép HTTP, hãy mở cổng 80:

```
sudo ufw allow 80/tcp
```

```
sudo ufw allow 443/tcp # Nếu dùng HTTPS
```

sudo ufw reload

Sau đó kiểm tra lại, nếu thấy:

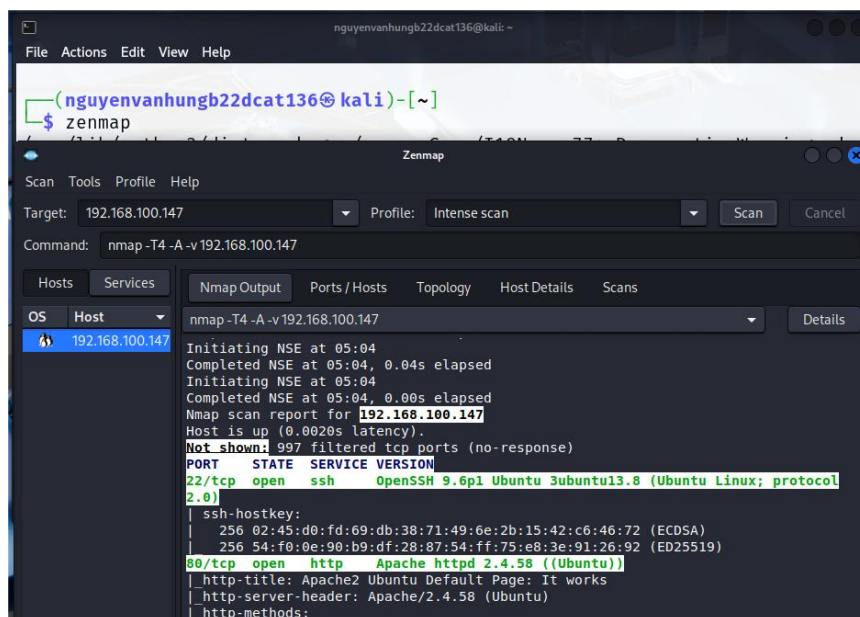
80/tcp *ALLOW* *Anywhere*

thì tường lửa không còn chặn cổng 80.

```
ubuntu@NguyenVanHungB22DCAT136: ~  
22/tcp                      ALLOW      Anywhere  
22/tcp (v6)                ALLOW      Anywhere (v6)  
  
ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw allow 80/tcp  
Rule added  
Rule added (v6)  
ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw allow 443/tcp  
Rule added  
Rule added (v6)  
ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw reload  
Firewall reloaded  
ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw status  
Status: active  
  
To                      Action      From  
--                      - - - - -  
22/tcp                ALLOW      Anywhere  
80/tcp                ALLOW      Anywhere  
443/tcp                ALLOW      Anywhere  
22/tcp (v6)            ALLOW      Anywhere (v6)  
80/tcp (v6)            ALLOW      Anywhere (v6)  
443/tcp (v6)           ALLOW      Anywhere (v6)
```

Hình 13. Kiểm tra tường lửa trên Ubuntu

Sau khi thực hiện các bước trên, kiểm tra lại từ Kali Linux:



Hình 14. Kiểm tra cổng 80

Cổng 80 đang mở cho Apache.

Tiếp theo, truy cập trang web của máy victim từ Kali Linux:

`curl http://192.168.100.147`



```
(nguyenvanhungb22dcat136@kali)-[~]  
$ curl http://192.168.100.147  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
  <!--  
    Modified from the Debian package for xhtml1.0
```

Hình 15. Truy cập trang web của victim

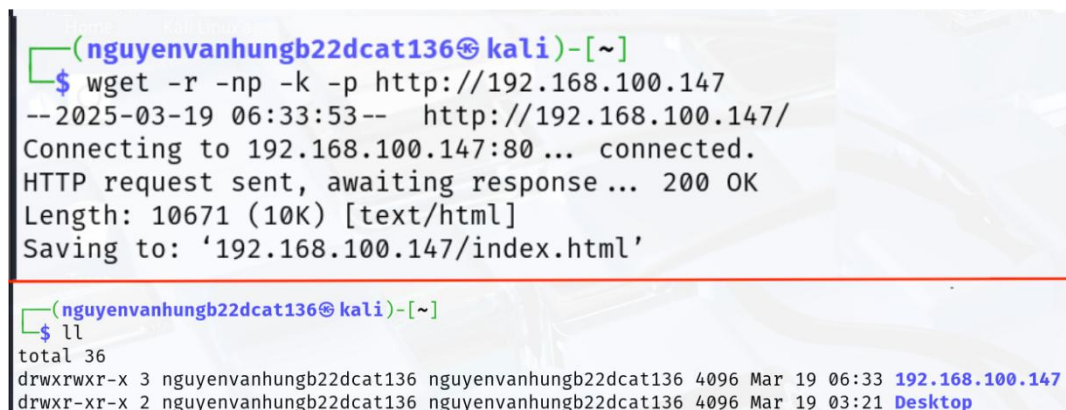
Nếu Apache hoạt động đúng, bạn sẽ thấy mã HTML của trang web.

Dùng lệnh `wget` để tải toàn bộ nội dung trang web lưu về trong thư mục `192.168.100.147`

`wget -r -np -k -p http://192.168.100.147`

Giải thích:

- `-r`: Tải đệ quy (toàn bộ trang web).
- `-np`: Không tải các thư mục bên trên (chỉ trang web này).
- `-k`: Chuyển đổi liên kết để có thể duyệt offline.
- `-p`: Tải tất cả các file cần thiết để hiển thị trang web đúng cách.



```
(nguyenvanhungb22dcat136@kali)-[~]  
$ wget -r -np -k -p http://192.168.100.147  
--2025-03-19 06:33:53-- http://192.168.100.147/  
Connecting to 192.168.100.147:80 ... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: 10671 (10K) [text/html]  
Saving to: '192.168.100.147/index.html'  
  
(nguyenvanhungb22dcat136@kali)-[~]  
$ ll  
total 36  
drwxrwxr-x 3 nguyenvanhungb22dcat136 nguyenvanhungb22dcat136 4096 Mar 19 06:33 192.168.100.147  
drwxr-xr-x 2 nguyenvanhungb22dcat136 nguyenvanhungb22dcat136 4096 Mar 19 03:21 Desktop
```

Hình 16. Tải trang web

Tìm kiếm từ khóa “test” trong tất cả các file đã tải:

`grep -r "test" 192.168.100.147`

Tìm từ “test” trong một file cụ thể:

`grep "test" 192.168.100.147/index.html`


```
(nguyenvanhungb22dcat136@kali)-[~]
$ grep -r "test" 192.168.100.147
192.168.100.147/index.html: This is the default welcome page used to test the correct

(nguyenvanhungb22dcat136@kali)-[~]
$ grep "test" 192.168.100.147/index.html
This is the default welcome page used to test the correct
```

Hình 17. Dùng lệnh “grep” tìm kiếm từ “test”

Mở máy victim, di chuyển đến vị trí file ghi lại log truy cập:

`cd /var/log/apache2`

```
ubuntu@NguyenVanHungB22DCAT136:~$ cd /var/log/httpd
bash: cd: /var/log/httpd: No such file or directory
ubuntu@NguyenVanHungB22DCAT136:~$ cd /var/log/apache2
ubuntu@NguyenVanHungB22DCAT136:/var/log/apache2$ ll
total 20
drwxr-x--- 2 root adm 4096 Mar 19 15:20 ./
drwxrwxr-x 17 root syslog 4096 Mar 19 15:20 ../
-rw-r----- 1 root adm 5160 Mar 19 17:33 access.log
-rw-r----- 1 root adm 1274 Mar 19 16:04 error.log
-rw-r----- 1 root adm 0 Mar 19 15:20 other_vhosts_access.log
```

Hình 18. Di chuyển đến vị trí file ghi log truy nhập

Dùng grep tìm kiếm trong file access.log:

`cat access.log | grep “192.168.100.3”` Hiện thị tất cả các dòng log có chứa 192.168.100.3

`cat access.log | grep “Nmap”` Hiện thị các dòng log có chứa Nmap

`cat access.log | grep “curl”` Hiện thị các request sử dụng curl tự động tải dữ liệu từ server

```
ubuntu@NguyenVanHungB22DCAT136:/var/log/apache2$ cat access.log | grep "192.168.100.3"
192.168.100.3 - - [19/Mar/2025:16:04:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.100.3 - - [19/Mar/2025:16:04:47 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
ubuntu@NguyenVanHungB22DCAT136:/var/log/apache2$ cat access.log | grep "Nmap"
192.168.100.3 - - [19/Mar/2025:16:04:47 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [19/Mar/2025:16:04:47 +0700] "GET /nmaplowercheck1742375086 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
ubuntu@NguyenVanHungB22DCAT136:/var/log/apache2$ cat access.log | grep "curl"
192.168.100.3 - - [19/Mar/2025:17:27:28 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
192.168.100.3 - - [19/Mar/2025:17:27:37 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
192.168.100.3 - - [19/Mar/2025:17:33:30 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
```

Hình 19. Các lệnh grep

```

192.168.100.3 - - [19/Mar/2025:16:04:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [19/Mar/2025:16:04:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [19/Mar/2025:16:04:52 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"
192.168.100.3 - - [19/Mar/2025:16:04:52 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"
192.168.100.3 - - [19/Mar/2025:17:27:28 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
192.168.100.3 - - [19/Mar/2025:17:27:37 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
192.168.100.3 - - [19/Mar/2025:17:33:30 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.12.1"
192.168.100.3 - - [19/Mar/2025:17:33:53 +0700] "GET / HTTP/1.1" 200 10982 "-" "Wget/1.25.0"
192.168.100.3 - - [19/Mar/2025:17:33:53 +0700] "GET /robots.txt HTTP/1.1" 404 493 "-" "Wget/1.25.0"
192.168.100.3 - - [19/Mar/2025:17:33:53 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.100.147/" "Wget/1.25.0"
192.168.100.3 - - [19/Mar/2025:17:33:53 +0700] "GET /manual HTTP/1.1" 404 493 "http://192.168.100.147/" "Wget/1.25.0"

```

Hình 20. Kết quả lệnh grep

- 192.168.100.3 → Địa chỉ IP của máy attack.
- GET / → Request trang chủ.
- OPTIONS / HTTP/1.1 → Request OPTIONS kiểm tra các phương thức HTTP được hỗ trợ.
- “200 ...” → Server phản hồi thành công.
- "Mozilla/5.0 (compatible; Nmap Scripting Engine; ...)" → Nmap đang thực hiện quét để kiểm tra các phương thức HTTP mà server hỗ trợ.
- “curl ...” → Lệnh curl được sử dụng để tải trang.
- "Wget/1.25.0" → Lệnh wget được sử dụng để tải nội dung của server.
- "404 ..." → File không tồn tại.

2.2. Phân tích log sử dụng gawk trong Linux

Trên máy Kali Linux attack Internal remote vào máy Linux Internal Victim bằng lệnh ssh:

```

(nguenvanhungb22dcat136@kali)-[~]
└─$ ssh ubuntu@192.168.100.147
ubuntu@192.168.100.147's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

99 updates can be applied immediately.
48 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Mar 16 00:33:50 2025 from 192.168.100.3
ubuntu@NguyenVanHungB22DCAT136:~$

```

Hình 21. Ssh vào máy Ubuntu victim

Tạo tài khoản mới trên máy Linux victim: *sudo useradd nguyenvanhung*

Đặt mật khẩu cho tài khoản vừa tạo: *sudo passwd nguyenvanhung*

```
ubuntu@NguyenVanHungB22DCAT136:~$ sudo useradd nguyenvanhung
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
ubuntu@NguyenVanHungB22DCAT136:~$ sudo useradd nguyenvanhung
useradd: user 'nguyenvanhung' already exists
ubuntu@NguyenVanHungB22DCAT136:~$ sudo passwd 1
passwd: user '1' does not exist
ubuntu@NguyenVanHungB22DCAT136:~$ sudo passwd nguyenvanhung
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
ubuntu@NguyenVanHungB22DCAT136:~$
```

Hình 22. Tạo tài khoản mới cho máy victim trên máy attack

Đổi mật khẩu:

```
ubuntu@NguyenVanHungB22DCAT136:~$ sudo passwd nguyenvanhung
[sudo] password for ubuntu:
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
ubuntu@NguyenVanHungB22DCAT136:~$
```

Hình 23. Đổi mật khẩu

Mở máy Linux victim, xem file log: *cat /var/log/auth.log*

```
ubuntu@NguyenVanHungB22DCAT136:~$ cat /var/log/auth.log
2025-03-16T00:04:12.994870+07:00 NguyenVanHungB22DCAT136 gdm-password: pam_unix(gdm-password:auth): conversation failed
2025-03-16T00:04:12.995250+07:00 NguyenVanHungB22DCAT136 gdm-password: pam_unix(gdm-password:auth): auth could not identify password for [ubuntu]
2025-03-16T00:04:14.886898+07:00 NguyenVanHungB22DCAT136 gdm-password: gkr-pam: unlocked login keyring
2025-03-16T00:05:01.707126+07:00 NguyenVanHungB22DCAT136 CRON[3765]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-16T00:05:01.717958+07:00 NguyenVanHungB22DCAT136 CRON[3765]: pam_unix(cron:session): session closed for user root
2025-03-16T00:15:01.727458+07:00 NguyenVanHungB22DCAT136 CRON[3825]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-16T00:15:01.745577+07:00 NguyenVanHungB22DCAT136 CRON[3825]: pam_unix(cron:session): session closed for user root
2025-03-16T00:17:01.753010+07:00 NguyenVanHungB22DCAT136 CRON[3838]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-16T00:17:01.760885+07:00 NguyenVanHungB22DCAT136 CRON[3838]: pam_unix(cron:session): session closed for user root
2025-03-16T00:19:42.828373+07:00 NguyenVanHungB22DCAT136 gdm-password: gkr-pam: unlocked login keyring
2025-03-16T00:20:18.471071+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/apt update
2025-03-16T00:20:18.484972+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-03-16T00:20:32.640051+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session closed for user root
2025-03-16T00:22:54.269422+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/apt install -y open
ssh-server
2025-03-16T00:22:54.270090+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-03-16T00:22:56.223694+07:00 NguyenVanHungB22DCAT136 pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-03-16T00:22:56.225639+07:00 NguyenVanHungB22DCAT136 pkexec[4355]: ubuntu: Executing command [USER=root] [TTY=unknown] [CWD=/home/ubuntu] [COMMAND=/u
sr/lib/update-notifier/package-system-locked]
2025-03-16T00:22:58.896169+07:00 NguyenVanHungB22DCAT136 useradd[4578]: new user: name=sshd, UID=122, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin,
from=none
2025-03-16T00:23:03.220350+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session closed for user root
2025-03-16T00:23:42.419615+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/systemctl status ss
h
2025-03-16T00:23:42.420235+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-03-16T00:24:17.009718+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session closed for user root
2025-03-16T00:24:25.317284+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/systemctl start ssh
2025-03-16T00:24:25.330331+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-03-16T00:24:25.404099+07:00 NguyenVanHungB22DCAT136 sshd[4979]: Server listening on :: port 22.
2025-03-16T00:24:25.406193+07:00 NguyenVanHungB22DCAT136 sudo: pam_unix(sudo:session): session closed for user root
```

Hình 24. Mở file auth.log trên máy victim

Xem file log trên máy Kali attack:

Tìm kiếm các sự kiện liên quan đến tài khoản người dùng nguyenvanhung trong tệp auth.log: `grep 'nguyenvanhung' /var/log/auth.log`

```
ubuntu@NguyenVanHungB22DCAT136:~$ grep 'nguyenvanhung' /var/log/auth.log
2025-03-19T18:12:03.581778+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:03.750979+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new group: name=nguyenvanhung, GID=1001
2025-03-19T18:12:03.760003+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new user: name=nguyenvanhung, UID=1001, GID=1001, home=/home/nguyenvanhung, shell=/bin/sh, from=/dev/pts/3
2025-03-19T18:12:27.980418+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:27.987718+07:00 NguyenVanHungB22DCAT136 useradd[13919]: failed adding user 'nguyenvanhung', exit code: 9
2025-03-19T18:14:13.445853+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-19T18:15:38.672782+07:00 NguyenVanHungB22DCAT136 passwd[13925]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
2025-03-20T15:42:43.487246+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-20T15:42:48.160371+07:00 NguyenVanHungB22DCAT136 passwd[3755]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
```

Hình 25. Các sự kiện liên quan đến tài khoản nguyenvanhung

Phân tích một số dòng log:

- 2025-03-19T18:12:03.581778+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
→ Người dùng ubuntu đã sử dụng sudo để chạy lệnh useradd nguyenvanhung
- 2025-03-19T18:12:03.750979+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new group: name=nguyenvanhung, GID=1001
→ Hệ thống tạo một nhóm mới nguyenvanhung với GID 1001
- 2025-03-19T18:12:27.987718+07:00 NguyenVanHungB22DCAT136 useradd[13919]: failed adding user 'nguyenvanhung', exit code: 9
→ Có một lần thử chạy lại lệnh useradd nguyenvanhung nhưng không thành công vì tài khoản đã tồn tại.
- 2025-03-19T18:14:13.445853+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-19T18:15:38.672782+07:00 NguyenVanHungB22DCAT136 passwd[13925]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
→ Người dùng ubuntu đã sử dụng sudo để chạy passwd, đặt mật khẩu mới cho tài khoản nguyenvanhung.
- 2025-03-20T15:42:43.487246+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-20T15:42:48.160371+07:00 NguyenVanHungB22DCAT136 passwd[3755]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
→ Đổi mật khẩu cho tài khoản nguyenvanhung

In toàn bộ thông tin về tài khoản mới tạo:

```
grep 'nguyenvanhung' /var/log/auth.log | gawk '{print $0}'
```

```
ubuntu@NguyenVanHungB22DCAT136:~$ grep 'nguyenvanhung' /var/log/auth.log | gawk '{print $0}'
2025-03-19T18:12:03.581778+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:03.750799+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new group: name=nguyenvanhung, GID=1001
2025-03-19T18:12:03.760003+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new user: name=nguyenvanhung, UID=1001, GID=1001, home=/home/nguyenvanhung, shell=/bin/sh, from=/dev/pts/3
2025-03-19T18:12:27.980418+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:27.987718+07:00 NguyenVanHungB22DCAT136 useradd[13919]: failed adding user 'nguyenvanhung', exit code: 9
2025-03-19T18:14:13.445853+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-19T18:15:38.672782+07:00 NguyenVanHungB22DCAT136 passwd[13925]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
2025-03-20T15:42:43.487246+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-20T15:42:48.160371+07:00 NguyenVanHungB22DCAT136 passwd[3755]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
```

Hình 26. In toàn bộ dòng chứa thông tin về tài khoản nguyenvanhung

In cột thời gian và tên tài khoản:

```
grep 'nguyenvanhung' /var/log/auth.log | gawk '{print $1, $2, $3, $10}'
```

```
ubuntu@NguyenVanHungB22DCAT136:~$ grep 'nguyenvanhung' /var/log/auth.log | gawk '{print $1, $2, $3, $10}'
2025-03-19T18:12:03.581778+07:00 NguyenVanHungB22DCAT136 sudo: USER=root
2025-03-19T18:12:03.750799+07:00 NguyenVanHungB22DCAT136 useradd[13910]:
2025-03-19T18:12:03.760003+07:00 NguyenVanHungB22DCAT136 useradd[13910]: shell=/bin/sh,
2025-03-19T18:12:27.980418+07:00 NguyenVanHungB22DCAT136 sudo: USER=root
2025-03-19T18:12:27.987718+07:00 NguyenVanHungB22DCAT136 useradd[13919]: 9
2025-03-19T18:14:13.445853+07:00 NguyenVanHungB22DCAT136 sudo: USER=root
2025-03-19T18:15:38.672782+07:00 NguyenVanHungB22DCAT136 passwd[13925]:
2025-03-20T15:42:43.487246+07:00 NguyenVanHungB22DCAT136 sudo: USER=root
2025-03-20T15:42:48.160371+07:00 NguyenVanHungB22DCAT136 passwd[3755]:
```

Hình 27. In cột thời gian và tên tài khoản

Giải thích: \$0, \$1, \$2, \$3, ... đại diện cho các cột trong từng dòng log, được phân tách bởi dấu cách (space) hoặc tab (\t).

In các dòng có liên quan đến tài khoản:

```
gawk '/nguyenvanhung/' /var/log/auth.log
```

```
ubuntu@NguyenVanHungB22DCAT136:~$ gawk '/nguyenvanhung/' /var/log/auth.log
2025-03-19T18:12:03.581778+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:03.750799+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new group: name=nguyenvanhung, GID=1001
2025-03-19T18:12:03.760003+07:00 NguyenVanHungB22DCAT136 useradd[13910]: new user: name=nguyenvanhung, UID=1001, GID=1001, home=/home/nguyenvanhung, shell=/bin/sh, from=/dev/pts/3
2025-03-19T18:12:27.980418+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd nguyenvanhung
2025-03-19T18:12:27.987718+07:00 NguyenVanHungB22DCAT136 useradd[13919]: failed adding user 'nguyenvanhung', exit code: 9
2025-03-19T18:14:13.445853+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/2 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-19T18:15:38.672782+07:00 NguyenVanHungB22DCAT136 passwd[13925]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
2025-03-20T15:42:43.487246+07:00 NguyenVanHungB22DCAT136 sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd nguyenvanhung
2025-03-20T15:42:48.160371+07:00 NguyenVanHungB22DCAT136 passwd[3755]: pam_unix(passwd:chauthtok): password changed for nguyenvanhung
```

Hình 28. In các dòng liên quan đến tài khoản nguyenvanhung

2.3. Phân tích log sử dụng find trong Windows

Mở máy Windows Server victim, cài đặt FTP Server nếu chưa có (đã cài đặt từ các bài thực hành trước), kiểm tra trạng thái FTP: `netstat -an | find ":21"`

Nếu thấy LISTENING, nghĩa là FTP đang chạy.

```
C:\Users\Administrator>netstat -an | find ":21"
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
TCP [::]:21 [::]:0 LISTENING

C:\WINDOWS\system32\cmd. x + v - □ x
C:\Users\TGDD>echo %date% Nguyen Van Hung B22DCAT136
Wed 03/19/2025 Nguyen Van Hung B22DCAT136
```

Hình 29. Kiểm tra trạng thái FTP

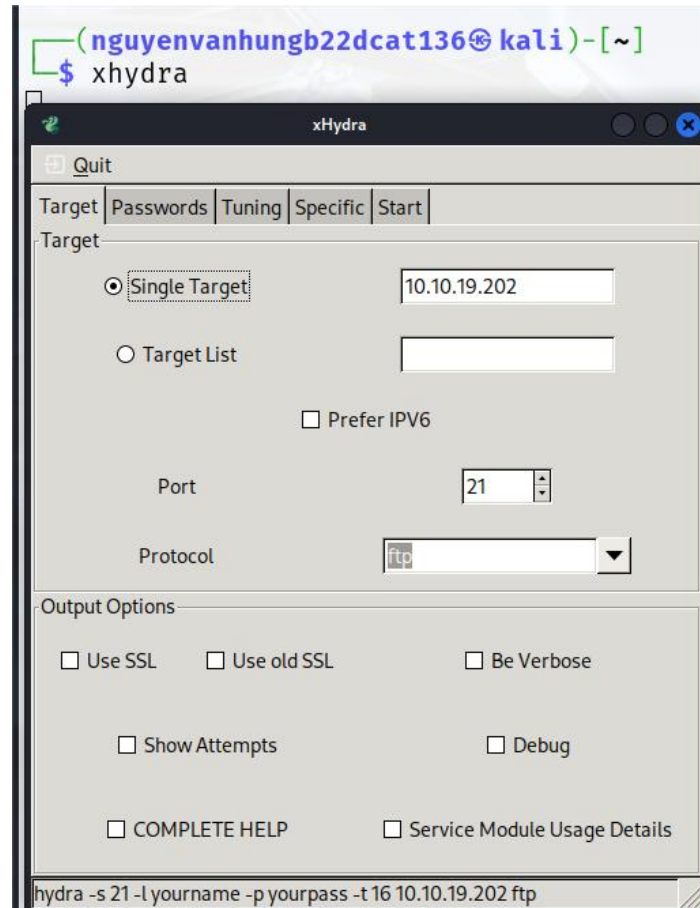
Mở máy Kali External Attack khởi động xHydra: xhydra

Trên giao diện nhập:

Single Target: 10.10.19.202 → Địa chỉ IP của máy Windows server victim

Port: 21

Protocol: ftp

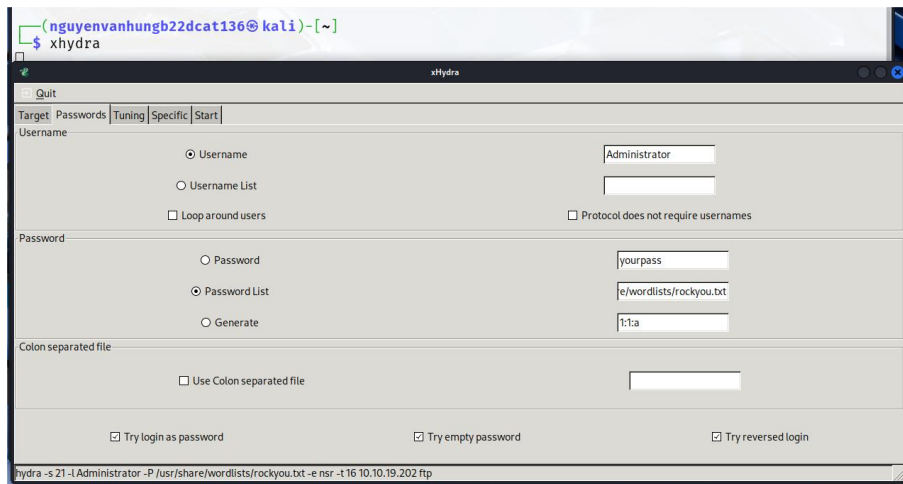


Hình 30. Nhập thông tin mục tiêu trên giao diện Target

Chuyển sang giao diện Passwords:

Username: Administrator → Tên tài khoản có thể tồn tại trên máy victim.

Chọn Password List: /usr/share/wordlists/rockyou.txt → Danh sách các mật khẩu phổ biến thường sử dụng. Ở đây ta dùng wordlist tích hợp sẵn trên Kali Linux.



Hình 31. Nhập thông tin username và password để chuẩn bị tấn công

Bạn có thể tìm wordlist được tích hợp sẵn trong thư mục:

`ls /usr/share/wordlists/`

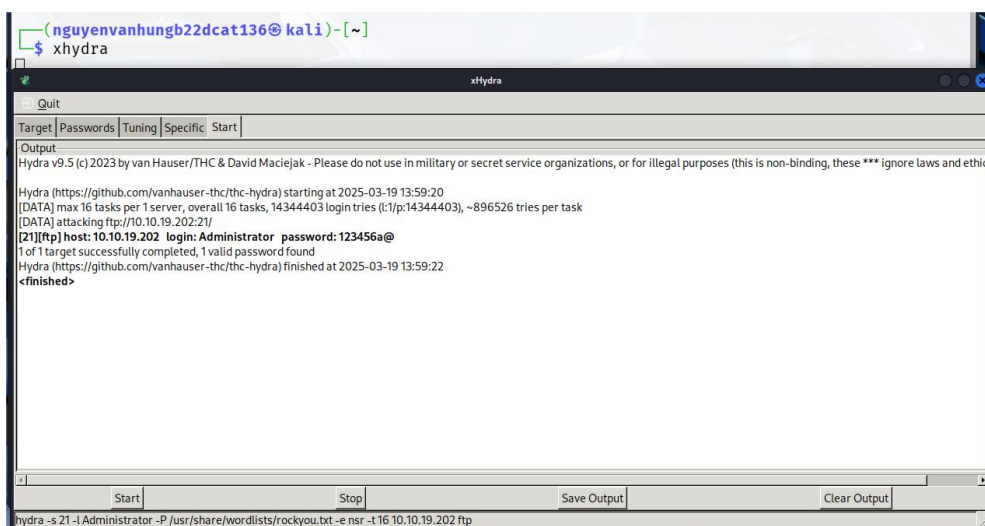
Chúng ta sử dụng danh sách phổ biến nhất là rockyou.txt, nếu file này bị nén .gz, cần giải nén trước:

`gunzip /usr/share/wordlists/rockyou.txt.gz`



Hình 32. Danh sách mật khẩu

Nhấn Start và chờ đợi xHydra tìm ra mật khẩu:



Hình 33. Thành công tìm ra mật khẩu

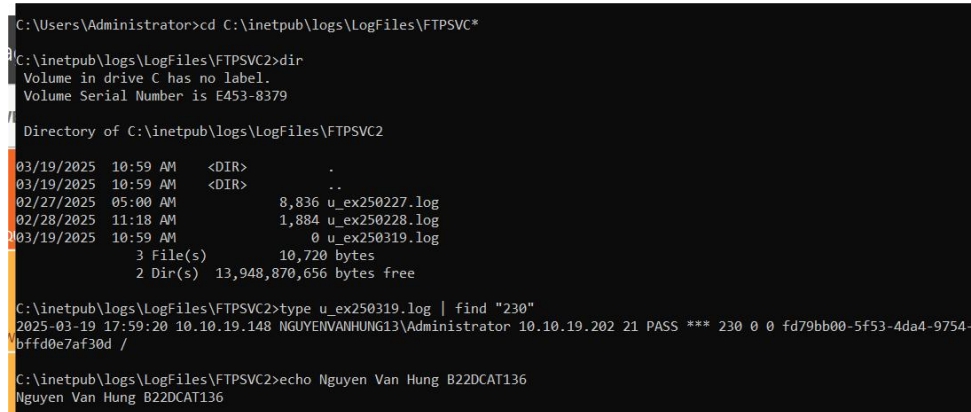
Sau khi thực hiện brute-force thành công, mở Windows Server External Victim, thực hiện điều hướng đến FTP Logfile:

```
cd C:\inetpub\logs\LogFiles\FTPSVC*
```

dir → hiển thị danh sách các tệp log trong thư mục

Tìm log đăng nhập thành công:

type u_ex250319.log | find "230" → 230 là mã phản hồi FTP cho biết đăng nhập thành công



```
C:\Users\Administrator>cd C:\inetpub\logs\LogFiles\FTPSVC*
C:\inetpub\logs\LogFiles\FTPSVC2>dir
Volume in drive C has no label.
Volume Serial Number is E453-8379

Directory of C:\inetpub\logs\LogFiles\FTPSVC2

03/19/2025  10:59 AM  <DIR>          .
03/19/2025  10:59 AM  <DIR>          ..
02/27/2025  05:00 AM             8,836 u_ex250227.log
02/28/2025  11:18 AM             1,884 u_ex250228.log
03/19/2025  10:59 AM              0 u_ex250319.log
               3 File(s)            10,720 bytes
               2 Dir(s)  13,948,870,656 bytes free

C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex250319.log | find "230"
2025-03-19 17:59:20 10.10.19.148 NGUYENVANHUNG13\Administrator 10.10.19.202 21 PASS *** 230 0 0 fd79bb00-5f53-4da4-9754-bff6de7af30d /
C:\inetpub\logs\LogFiles\FTPSVC2>echo Nguyen Van Hung B22DCAT136
Nguyen Van Hung B22DCAT136
```

Hình 34. Kiểm tra log FTP Server

Kết quả hiển thị danh sách các tệp log trong thư mục, đây là các log file theo định dạng ngày tháng:

- u_ex250227.log
- u_ex250228.log
- u_ex250319.log

Dòng log đăng nhập thành công:

```
2025-03-19 17:59:20 10.10.19.143 NGUYENVANHUNG13\Administrator
10.10.19.202 21 PASS *** 230 0 0 fd79bb00-5f53-4da4-9754-bff6de7af38d
```

- 2025-03-19 17:59:20: Thời gian đăng nhập thành công.
- 10.10.19.143: IP của client đăng nhập vào FTP server.
- NGUYENVANHUNG13\Administrator: Tên người dùng đăng nhập.
- 10.10.19.202: IP của FTP server.
- 21: Cổng FTP (21 là cổng mặc định của FTP).
- PASS ***: Thao tác đăng nhập bằng mật khẩu (được ẩn đi).
- 230: Mã trạng thái cho biết đăng nhập thành công.
- fd79bb00-5f53-4da4-9754-bff6de7af38d: ID phiên làm việc.

TÀI LIỆU THAM KHẢO

- [1] https://linuxcommand.org/lc3_man_pages/grep1.html
- [2] <https://www.gnu.org/software/gawk/manual/gawk.html>
- [3] <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/find>
- [4] <https://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>