

**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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết	5
1.2.1 Một số lệnh dùng cho quá trình phân tích log	5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	10
2.1 Chuẩn bị môi trường	10
2.2 Các bước thực hiện.....	10
2.2.1 Chuẩn bị máy ảo.....	10
2.2.2 Phân tích log sử dụng grep trong Linux	11
2.2.3 Phân tích log sử dụng gawk trong Linux	15
2.2.4 Phân tích log sử dụng find trong Windows	18
TÀI LIỆU THAM KHẢO.....	24

DANH MỤC CÁC HÌNH VẼ

Hình 1 Các tùy chọn của lệnh “grep”.....	6
Hình 2 Giao diện làm việc của xhydra.....	9
Hình 3 Địa chỉ IP của máy Windows Server	11
Hình 4 Địa chỉ IP của máy Kali Linux.....	11
Hình 5 Cài đặt dịch vụ web apache trên máy Ubuntu.....	12
Hình 6 Kiểm tra trạng thái hoạt động của dịch vụ	12
Hình 7 Sử dụng công cụ Zenmap để quét cổng dịch vụ	13
Hình 8 Truy cập vào dịch vụ web của máy Ubuntu.....	14
Hình 9 Tìm kiếm từ khóa “test” thông qua lệnh “grep”.....	14
Hình 10 Tìm kiếm các log trong file access.log.....	15
Hình 11 SSH đến máy Ubuntu và tạo user mới	16
Hình 12 Đọc file auth.log.....	16
Hình 13 File access.log	17
Hình 14 Tìm kiếm user vừa tạo bằng lệnh “grep”	17
Hình 15 Sử dụng lệnh “gawk”	18
Hình 16 Cài đặt dịch vụ FTP trên máy Windows Server.....	18
Hình 17 Kiểm tra đường dẫn tới thư mục logs.....	19
Hình 18 Tạo password list.....	19
Hình 19 Sử dụng công cụ hydra.....	20
Hình 20 Công cụ hydra dò mật khẩu thành công.....	21
Hình 21 Đọc file log trên máy Windows	22
Hình 22 Tìm kiếm kết quả tấn công.....	23

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SSH	Secure Shell	Vỏ an toàn
FTP	File Transfer Protocol	Giao thức truyền file
IP	Internet Protocol	Giao thức mạng
HTTP	Hyper Text Transfer Protocol	Giao thức truyền siêu văn bản

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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

1.2 Tìm hiểu lý thuyết

1.2.1 Một số lệnh dùng cho quá trình phân tích log

1.2.1.1 Lệnh “grep”

grep (Global Expression Print): là công cụ cho phép bạn tìm kiếm thông qua một số lượng lớn các tệp và thư mục cho văn bản được chỉ định.

Cú pháp : grep [tùy chọn]

Một số chức năng nổi bật của grep:

- Tìm một chuỗi trong file.
- Tìm kiếm chuỗi trong nhiều file.
- Tìm kiếm không phân biệt hoa thường (-i)
- Tìm kiếm ngược sử dụng tùy chọn (-v)
- Hiển thị số dòng (-n), số lượng (-c), giới hạn số dòng đầu ra (-m N)
- Tìm kiếm nhiều chuỗi (-e)
- Tìm kiếm trên tệp (-a)
- Hiển thị thêm dòng trước (-B), sau (-A), xung quanh (-C) dòng chứa kết quả cần tìm.

<code>-e, --regexp=PATTERNS</code>	use PATTERNS for matching
<code>-f, --file=FILE</code>	take PATTERNS from FILE
<code>-i, --ignore-case</code>	ignore case distinctions in patterns and data
<code>--no-ignore-case</code>	do not ignore case distinctions (default)
<code>-w, --word-regexp</code>	match only whole words
<code>-x, --line-regexp</code>	match only whole lines
<code>-z, --null-data</code>	a data line ends in 0 byte, not newline
<code>-s, --no-messages</code>	suppress error messages
<code>-v, --invert-match</code>	select non-matching lines
<code>-V, --version</code>	display version information and exit
<code>--help</code>	display this help text and exit
Output control:	
<code>-m, --max-count=NUM</code>	stop after NUM selected lines
<code>-b, --byte-offset</code>	print the byte offset with output lines
<code>-n, --line-number</code>	print line number with output lines
<code>--line-buffered</code>	flush output on every line
<code>-H, --with-filename</code>	print file name with output lines
<code>-h, --no-filename</code>	suppress the file name prefix on output
<code>--label=LABEL</code>	use LABEL as the standard input file name prefix
<code>-o, --only-matching</code>	show only nonempty parts of lines that match
<code>-q, --quiet, --silent</code>	suppress all normal output
<code>-a, --text</code>	equivalent to <code>--binary-files=text</code>
<code>-I</code>	equivalent to <code>--binary-files=without-match</code>
<code>-d, --directories=ACTION</code>	how to handle directories; ACTION is 'read', 'recurse', or 'skip'
<code>-D, --devices=ACTION</code>	how to handle devices, FIFOs and sockets; ACTION is 'read' or 'skip'
<code>-r, --recursive</code>	like <code>--directories=recurse</code>
Context control:	
<code>-B, --before-context=NUM</code>	print NUM lines of leading context
<code>-A, --after-context=NUM</code>	print NUM lines of trailing context
<code>-C, --context=NUM</code>	print NUM lines of output context

Hình 1 Các tùy chọn của lệnh “grep”

1.2.1.2 Lệnh “gawk”

Lệnh gawk trong Linux là một ngôn ngữ quét mẫu và xử lý văn bản. Không cần biên dịch, và có thể sử dụng các biến cùng với các hàm số học, hàm chuỗi và toán tử logic.

Gawk là một tiện ích cho phép lập trình viên viết các chương trình ngắn gọn nhưng hiệu quả bằng cách xác định các mẫu văn bản cần tìm trong một tài liệu, cũng như hành động cần thực hiện mỗi khi tìm thấy một dòng khớp với mẫu đó.

Gawk có thể được sử dụng để:

- Quét tệp từng dòng một
- Chia nhỏ mỗi dòng đầu vào thành các trường
- So sánh dòng/trường đầu vào với mẫu xác định
- Thực hiện hành động trên các dòng khớp với mẫu
- Chuyển đổi tệp dữ liệu

- Tạo báo cáo định dạng
- Định dạng dòng đầu ra
- Thực hiện các phép toán số học và xử lý chuỗi
- Thực thi câu lệnh điều kiện và vòng lặp

1.2.1.3 Lệnh “find”

Lệnh find trong Linux là một công cụ mạnh mẽ để tìm kiếm tệp và thư mục theo nhiều tiêu chí khác nhau, chẳng hạn như tên, kích thước, kiểu tệp, thời gian chỉnh sửa, quyền truy cập, và nhiều yếu tố khác.

Cú pháp chung: find [đường_dẫn] [tùy_chọn] [biểu_thức_điều_kiện] [hành_động]

- đường_dẫn: Vị trí bắt đầu tìm kiếm (ví dụ: /home, . cho thư mục hiện tại, / cho toàn bộ hệ thống).
- tùy_chọn: Các tùy chọn như theo tên, kích thước, thời gian, quyền, v.v.
- biểu_thức_điều_kiện: Điều kiện lọc tệp hoặc thư mục cần tìm.
- hành_động: Thao tác thực hiện với các tệp tìm được (xóa, di chuyển, thực thi lệnh,...).

Các tùy chọn phổ biến của find:

- Tìm theo tên tệp hoặc thư mục (-name)
- Tìm theo loại tệp (-type)
- Tìm theo kích thước tệp (-size)
- Tìm theo thời gian chỉnh sửa (-mtime, -atime, -ctime)
- Tìm theo quyền (-perm)
- Tìm và thực hiện hành động (-exec, -delete)

1.2.1.4 File Secure

Secure là tập nhật ký theo dõi các kết nối SSH hoặc Secure Shell. Nó cung cấp thông tin như địa chỉ IP, ngày giờ,... Nó cũng theo dõi các sự kiện khác liên quan đến bảo mật như: tạo tài khoản người dùng mới và tài khoản nhóm mới.

Đối với các hệ thống sử dụng RedHat và CentOS thì file log này thay thế cho file log /var/log/auth.log.

File Secure chứa các thông tin về xác thực trên hệ thống và cả lưu trữ tất cả thông tin liên quan đến bảo mật, các lỗi xác thực. File log này giúp theo dõi thông tin đăng nhập sudo, đăng nhập SSH và các lỗi khác được ghi bởi tiến trình chạy nền của dịch vụ bảo mật hệ thống. Ngoài ra còn giúp chúng ta thấy được chi tiết về các lần đăng nhập trái phép hoặc

thất bại và nó cũng lưu trữ thông tin đăng nhập thành công và theo dõi các hoạt động của người dùng hợp lệ.

1.2.1.5 Tập “access_log”

Access_log là tệp nhật ký theo dõi các kết nối HTTP hoặc Giao thức truyền siêu văn bản. Nó cung cấp thông tin như: địa chỉ IP, tác nhân người dùng và tem ngày giờ.

Phân tích nhật ký truy cập có thể cung cấp thông tin:

- Số lượng khách truy cập (yêu cầu lần đầu tiên duy nhất) vào một trang chủ cụ thể.
- Nguồn gốc của khách truy cập, gồm cả tên miền của máy chủ được liên kết của họ.
- Có bao nhiêu yêu cầu cho mỗi trang trên trang web
- Sử dụng các mẫu liên quan đến thời gian trong ngày, ngày trong tuần và năm.

Các loại nhật ký truy cập khác nhau thu thập các loại dữ liệu khác nhau:

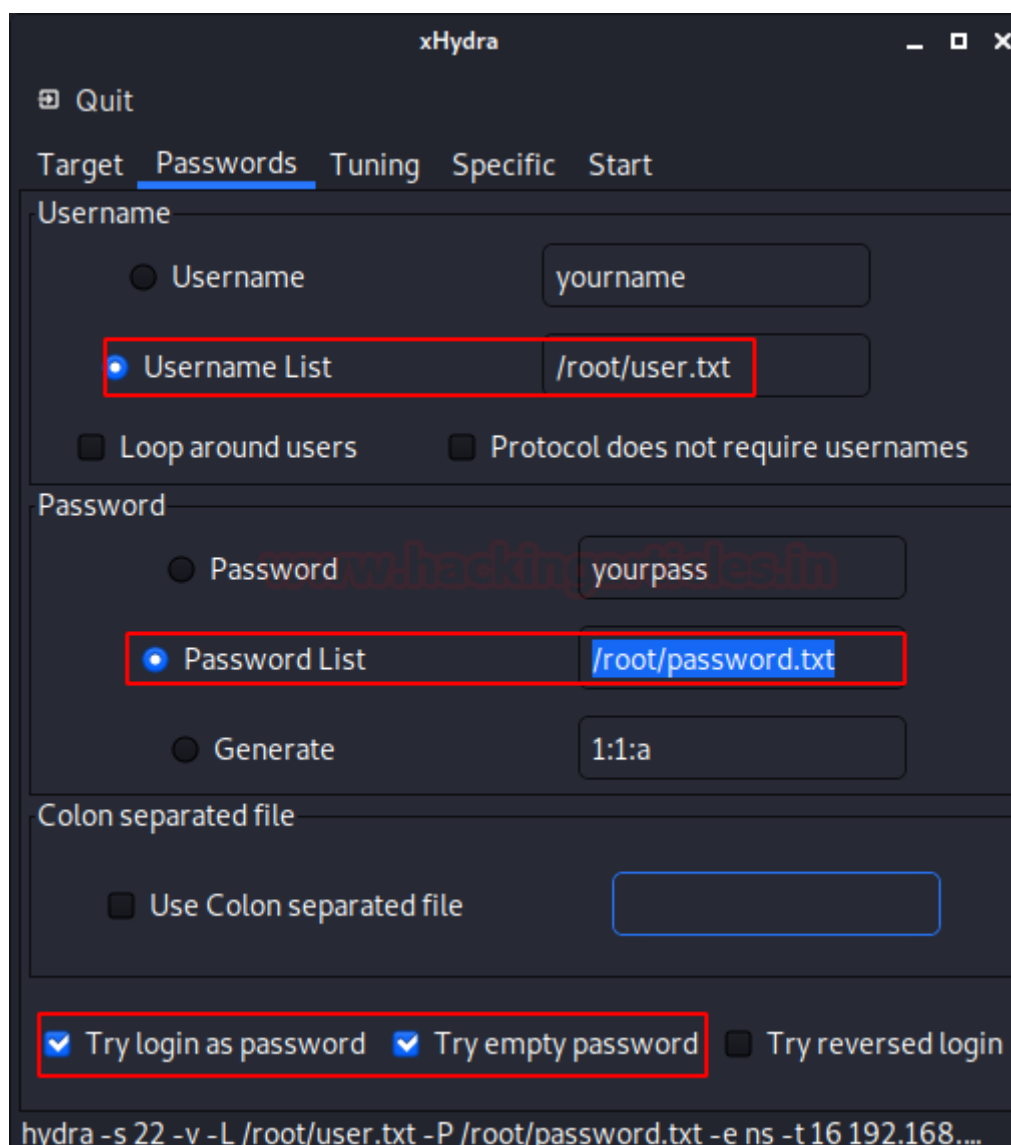
- Nhật ký chống virus: chứa dữ liệu về các đối tượng được quét, các cài đặt được sử dụng cho mỗi tác vụ và lịch sử các hành động được thực hiện trên mỗi tệp.
- Nhật ký tường lửa: cung cấp thông tin về địa chỉ IP nguồn và đích, số cổng và có thể được sử dụng để phân tích một cuộc tấn công.
- Nhật ký bộ lọc web: cho thấy người dùng đang cố gắng truy cập vào các URL bị hạn chế và cách hệ thống phản hồi.

1.2.1.6 Công cụ xhydra

xhydra là một công cụ phục vụ cho việc tấn công từ điển (brute-force) trong nhiều giao thức khác nhau như SSH (Secure Shell), FTP (File Transfer Protocol), Telnet,....

Một số tính năng chính của xhydra:

- Tấn công từ điển đa giao thức: xhydra cho phép thực hiện các cuộc tấn công từ điển trên nhiều giao thức như SSH, FTP, Telnet, MySQL, SMB,...
- Hỗ trợ tùy chỉnh từ điển: có thể chỉ định các từ điển hoặc tập hợp từ để sử dụng trong cuộc tấn công từ điển.
- Tùy chọn cấu hình phong phú: xhydra cung cấp một loạt các tùy chọn cấu hình để điều chỉnh cách thức thực hiện các cuộc tấn công, bao gồm số lần thử, thời gian giữa các thử nghiệm, và nhiều hơn nữa.
- Giao diện đồ họa: xhydra được thiết kế với giao diện đồ họa (GUI) để dễ dàng sử dụng và cấu hình.
- Hỗ trợ hàng loạt giao thức: có thể tấn công từ điển trên nhiều loại giao thức mạng phổ biến, giúp kiểm tra tính bảo mật của các hệ thống mạng.

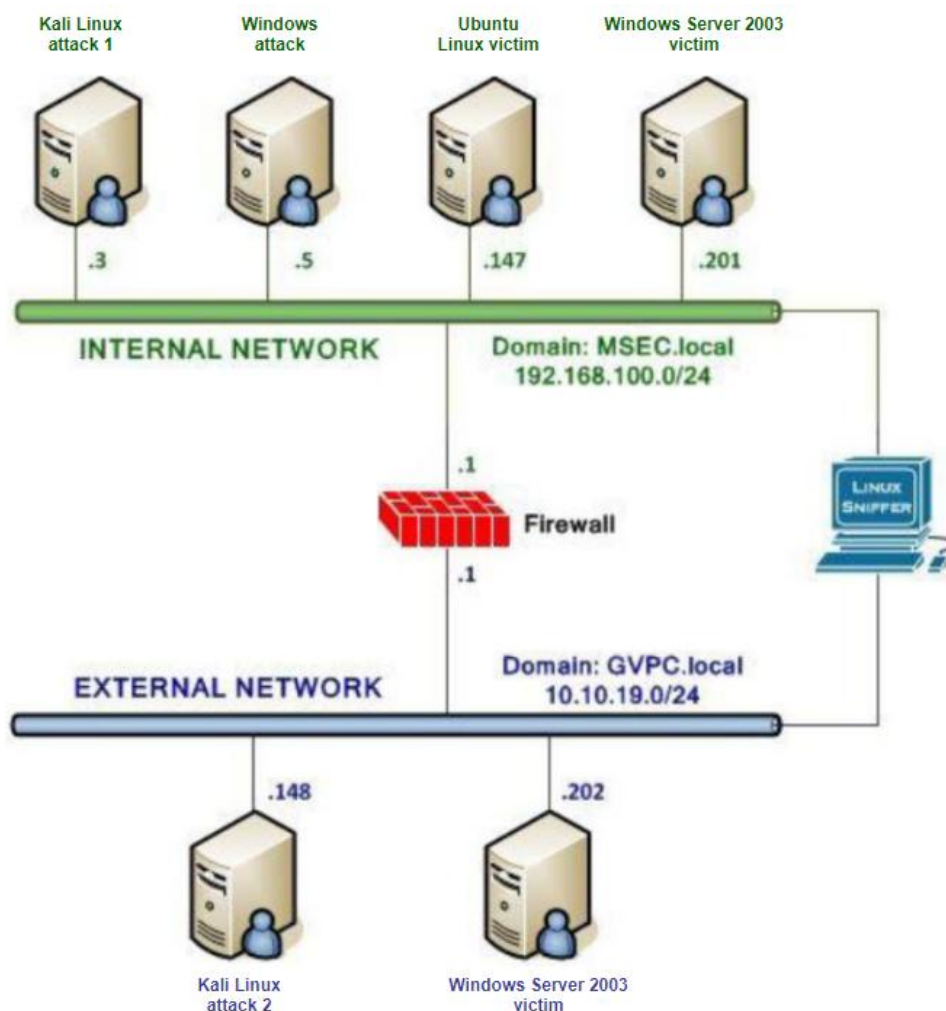


Hình 2 Giao diện làm việc của xhydra

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- File iso máy ảo Windows Server 2019, Ubuntu 20.04, Kali Linux.
- Phần mềm ảo hóa VMWare Workstation.



- Topo mạng cấu hình như trên. Trong bài này sẽ sử dụng máy Kali Linux attack 1 và Ubuntu victim ở mạng Internal; máy Kali Linux attack 2 và Windows Server ở mạng External.

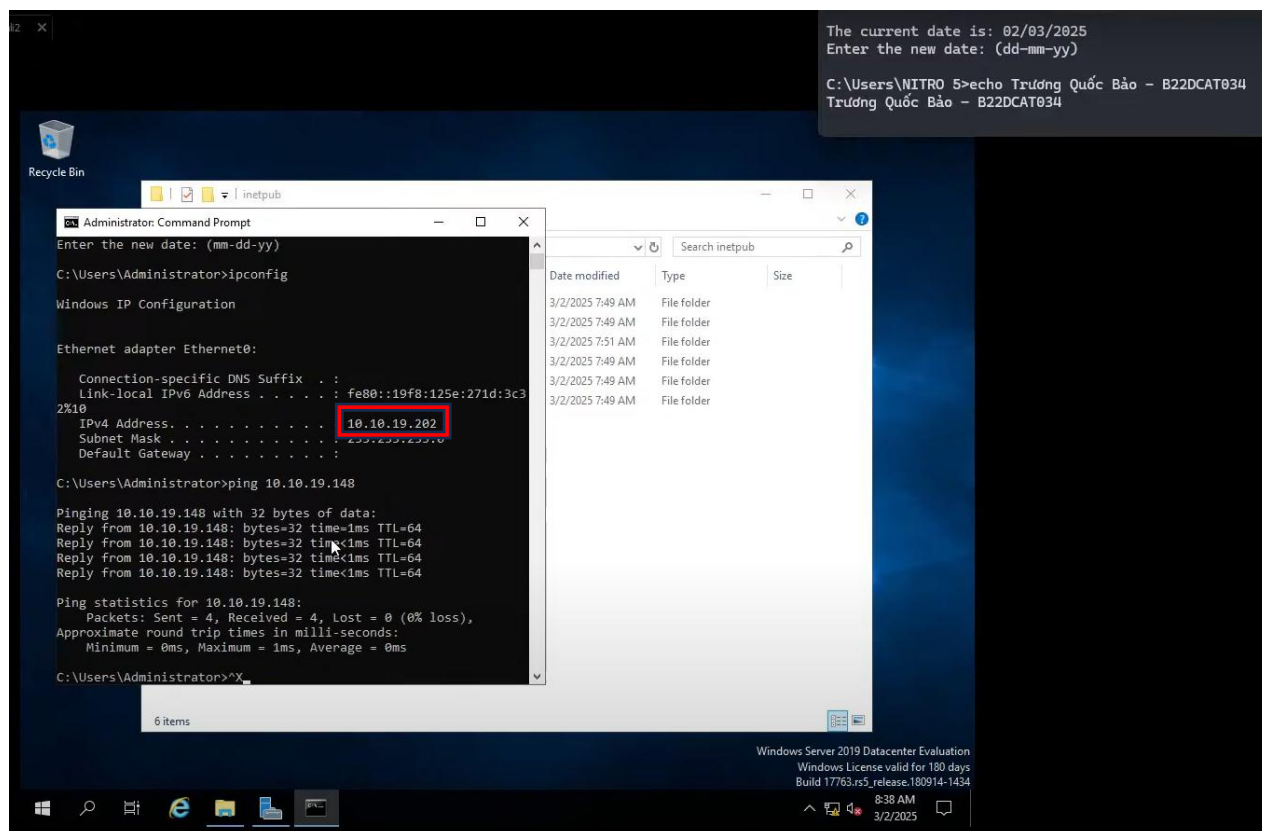
2.2 Các bước thực hiện

2.2.1 Chuẩn bị máy ảo

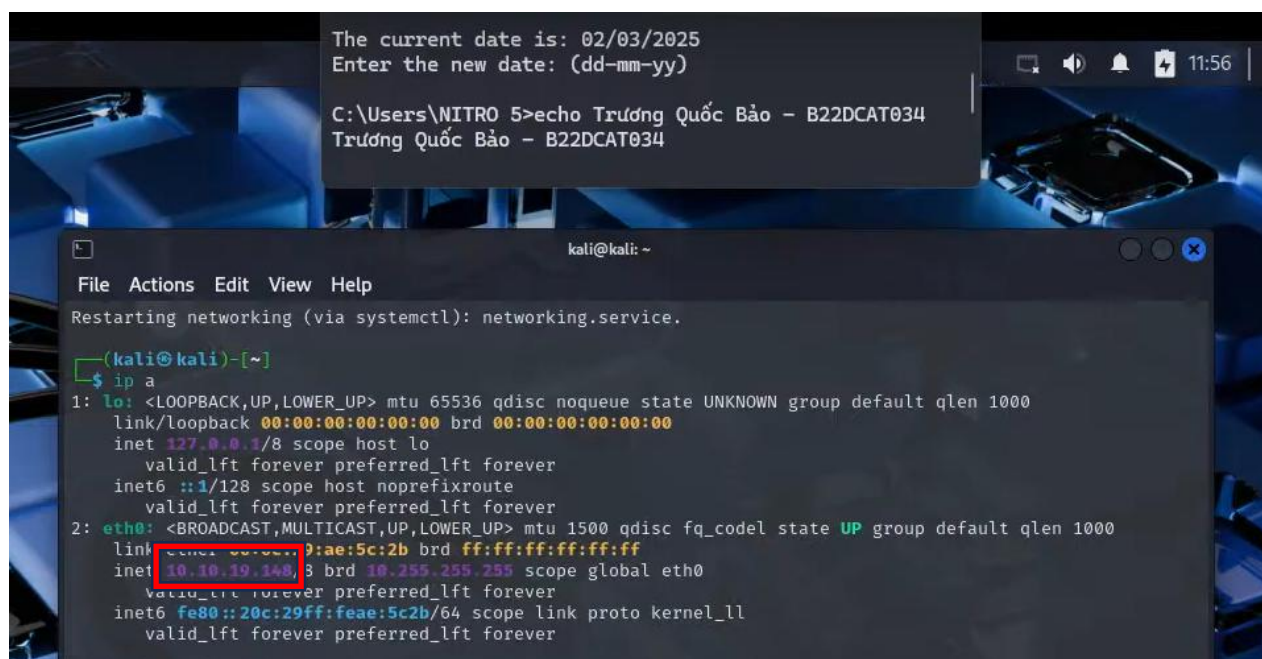
Ta cài đặt các máy ảo sử dụng file iso đã chuẩn bị như các bài trước đó.

Các máy trong mạng Internal cấu hình địa chỉ IP tĩnh như đã làm trong bài số 5.

Các máy trong mạng External cấu hình địa chỉ IP tĩnh như sau:



Hình 3 Địa chỉ IP của máy Windows Server



Hình 4 Địa chỉ IP của máy Kali Linux

2.2.2 Phân tích log sử dụng grep trong Linux

Trên máy Ubuntu, cài đặt dịch vụ Web Apache bằng lệnh “sudo apt-get install apache2”

Và kiểm tra hoạt động của dịch vụ bằng lệnh “sudo systemctl status apache2”, nếu hiện chữ màu xanh active (running) nghĩa là đã khởi động dịch vụ thành công.

```
Mar 2 06:13

C:\Users\NITRO 5>date
The current date is: 02/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo - B22DCAT034
Trương Quốc Bảo - B22DCAT034

test@truongquocbaob22dcat034: ~
test@truongquocbaob22dcat034:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libcurl4 liblua5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcurl4 liblua5.2-0
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,064 kB of archives.
After this operation, 8,692 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libapr1 amd64 1.6.5-1ubuntu1.1 [91.5 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1 amd64 1.6.1-4ubuntu2.2 [85.1 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu
2.2 [10.5 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2.2 [8,
752 B]
Get:5 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libcurl4 amd64 7.68.0-1ubuntu2.25 [235 kB]
16% [5 libcurl4 306 B/235 kB 0%]
```

Hình 5 Cài đặt dịch vụ web apache trên máy Ubuntu

```
Mar 2 06:15

C:\Users\NITRO 5>date
The current date is: 02/03/2025
Enter the new date: (dd-mm-yy)

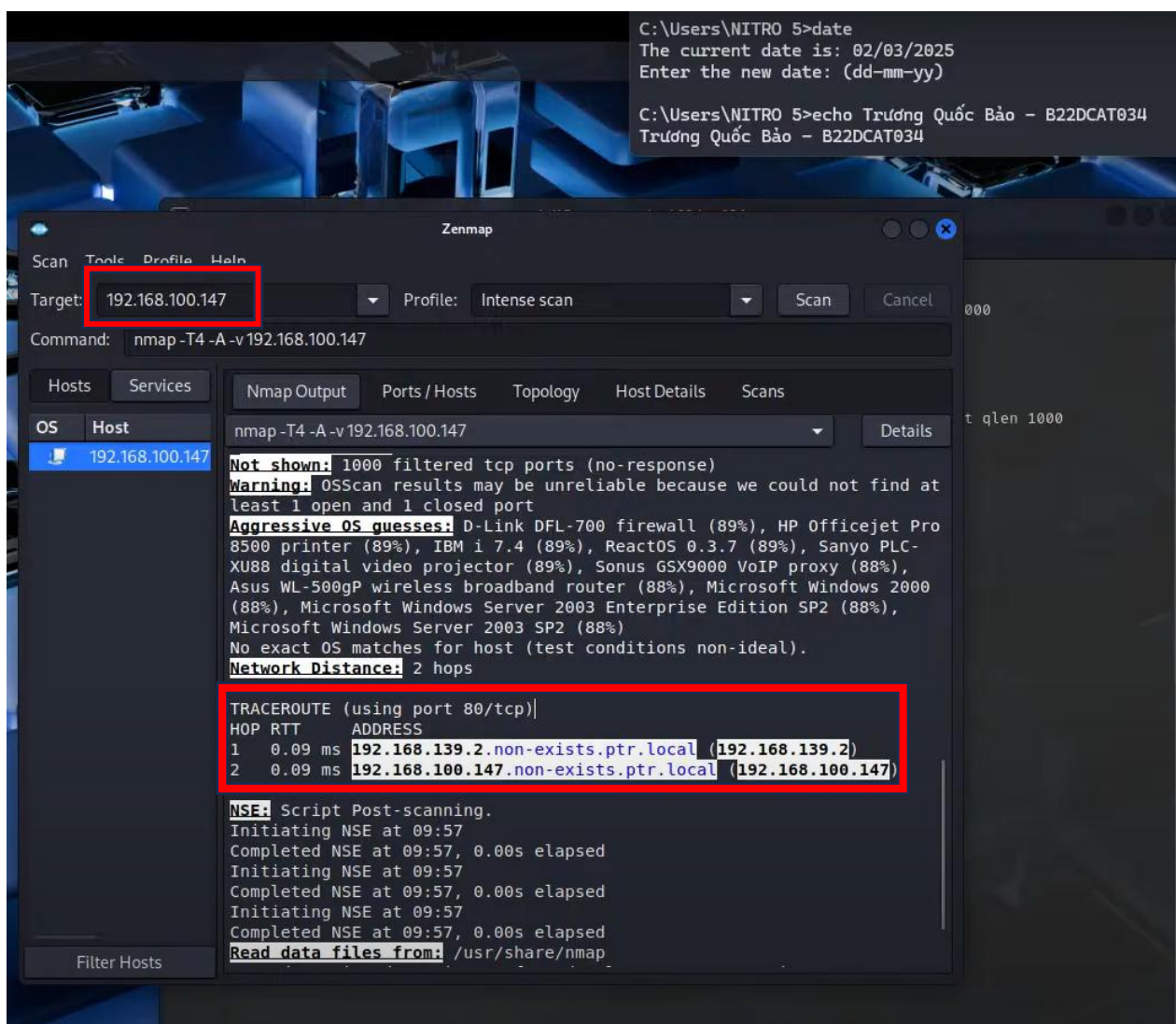
C:\Users\NITRO 5>echo Trương Quốc Bảo - B22DCAT034
Trương Quốc Bảo - B22DCAT034

test@truongquocbaob22dcat034: ~
test@truongquocbaob22dcat034:~$ sudo systemctl status apache2
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.serv
ice.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/
apache-htcacheclean.service.
Processing triggers for ufw (0.36-6ubuntu1.1) ...
Processing triggers for systemd (245.4-4ubuntu3.24) ...
Processing triggers for man-db (2.9.1-1) ...
test@truongquocbaob22dcat034:~$ sudo systemctl status apache2
apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
Active: active (running) since Sun 2025-03-02 06:13:38 PST; 22s ago
Docs: https://httpd.apache.org/docs/2.4/
Main PID: 2953 (apache2)
Tasks: 55 (limit: 4538)
Memory: 5.2M
CGroup: /system.slice/apache2.service
├─2953 /usr/sbin/apache2 -k start
├─2956 /usr/sbin/apache2 -k start
└─2957 /usr/sbin/apache2 -k start

Mar 02 06:13:38 truongquocbaob22dcat034 systemd[1]: Starting The Apache HTTP Server...
Mar 02 06:13:38 truongquocbaob22dcat034 systemd[1]: Started The Apache HTTP Server.
```

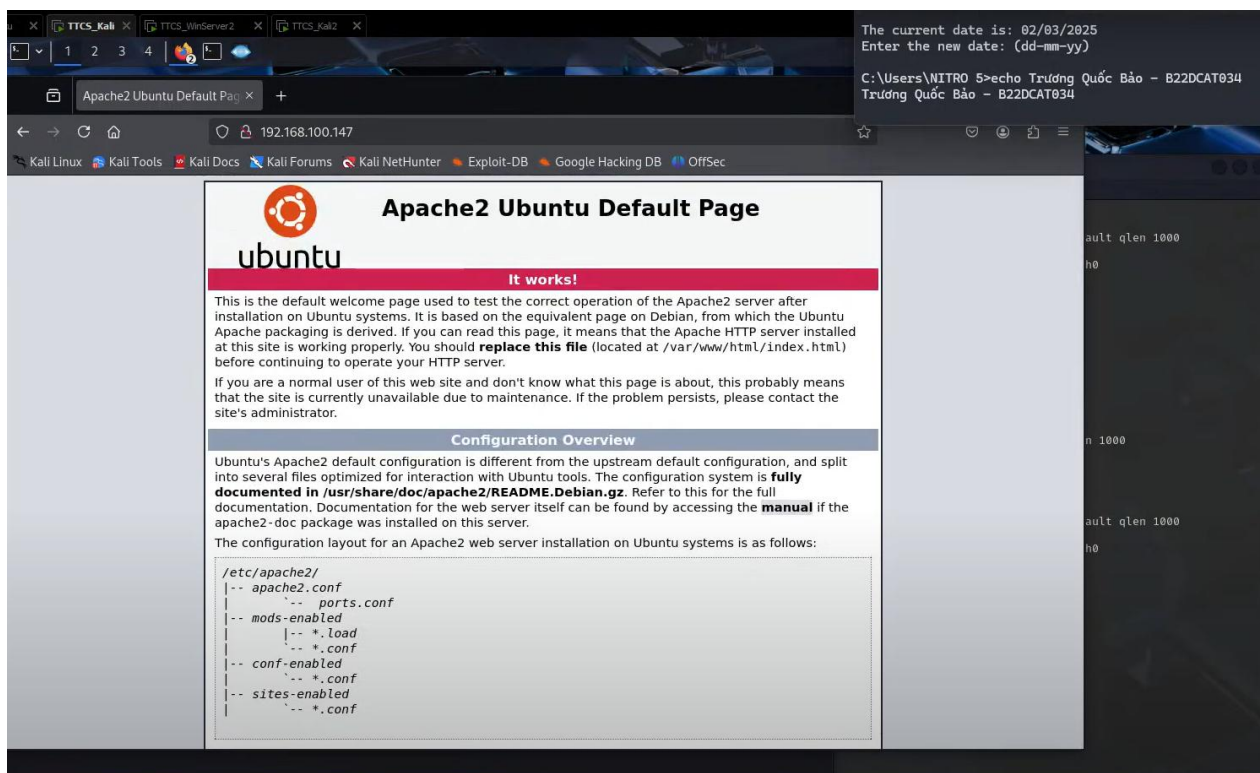
Hình 6 Kiểm tra trạng thái hoạt động của dịch vụ

Trên máy Kali attack, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147 (địa chỉ IP của máy Ubuntu) và xem được port 80 đang mở cho Web Server Apache.



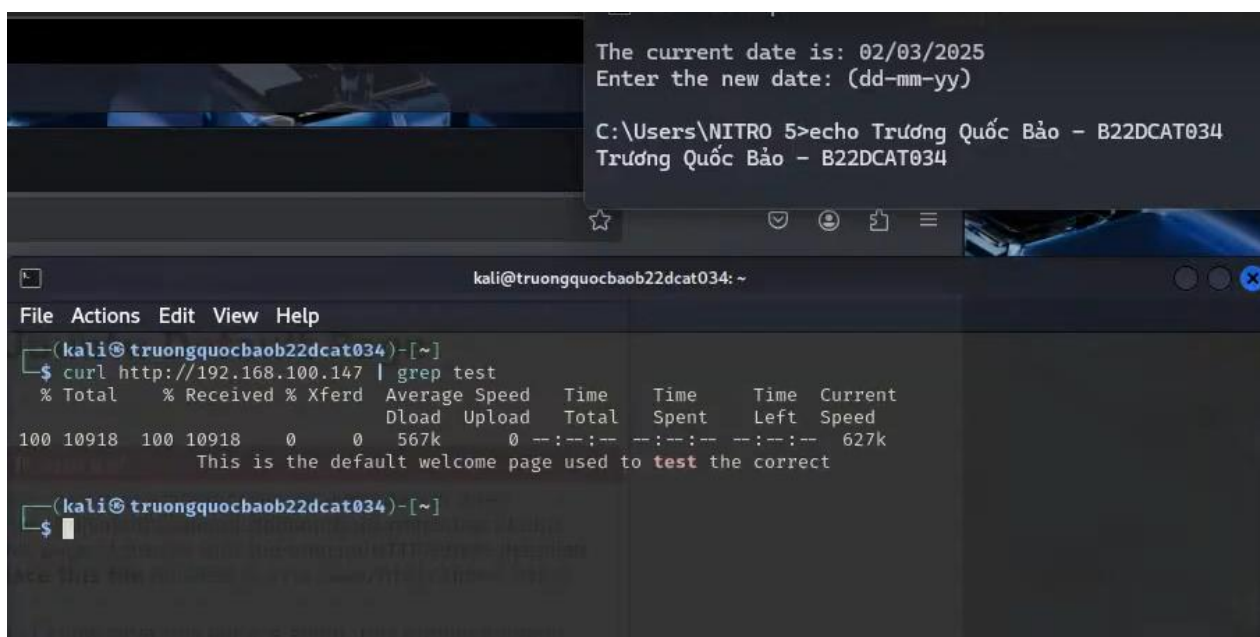
Hình 7 Sử dụng công cụ Zenmap để quét cổng dịch vụ

Trên máy Kali attack, truy cập địa chỉ web <http://192.168.100.147>, ta sẽ thấy giao diện web server apache giống của máy Ubuntu.



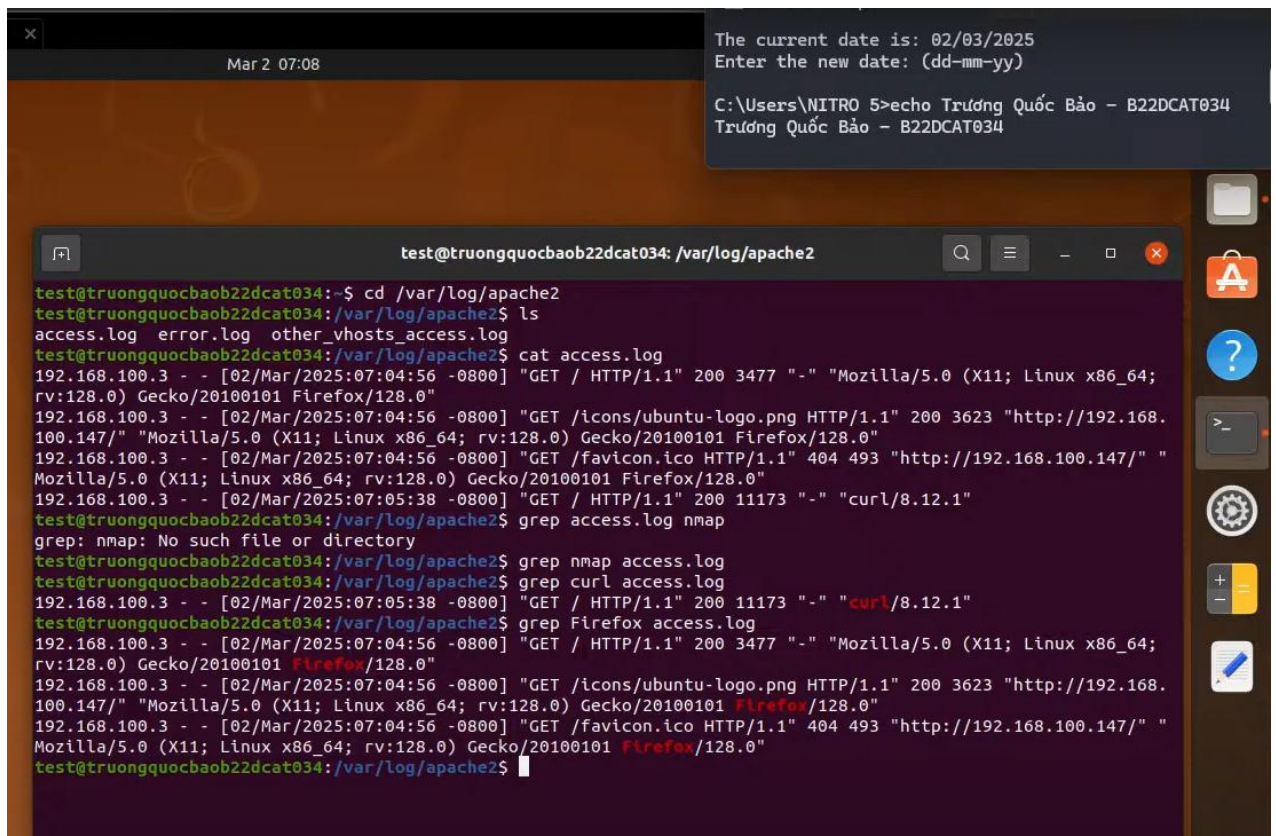
Hình 8 Truy cập vào dịch vụ web của máy Ubuntu

Trên máy Kali, gõ lệnh “curl <http://192.168.100.147> | grep test” để tìm kiếm từ khóa “test” trên website vừa rồi.



Hình 9 Tìm kiếm từ khóa “test” thông qua lệnh “grep”

Thư mục chứa access_log nằm ở đường dẫn /var/log/httpd, tiến hành đọc file với lệnh cat và sử dụng lệnh grep để tìm kiếm các từ khóa “nmap”, “firefox”, “curl”.



Hình 10 Tìm kiếm các log trong file access.log

2.2.3 Phân tích log sử dụng gawk trong Linux

Trên máy Kali attack tiến hành remote vào máy Ubuntu victim bằng lệnh “ssh <tên máy>@<địa chỉ IP>”. Tạo user mới là “tqb2” và đặt mật khẩu.


```
The current date is: 02/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo - B22DCAT034
Trương Quốc Bảo - B22DCAT034

test@truongquocbaob22dcat034: ~
File Actions Edit View Help

(kali@truongquocbaob22dcat034)-[~]
$ whoami
kali

(kali@truongquocbaob22dcat034)-[~]
$ ssh test@192.168.100.147
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-131-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.

0 updates can be applied immediately.

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy
settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Mar  2 07:10:12 2025 from 192.168.100.3
test@truongquocbaob22dcat034:~$ useradd tqb2
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
test@truongquocbaob22dcat034:~$ sudo useradd tqb2
[sudo] password for test:
test@truongquocbaob22dcat034:~$ sudo passwd tqb2
New password:
Retype new password:
passwd: password updated successfully
```

Hình 11 SSH đến máy Ubuntu và tạo user mới

Đọc file auth.log ở trên máy Ubuntu bằng lệnh cat.

```
test@truongquocbaob22dcat034: /var/log$ cat auth.log
```

Hình 12 Đọc file auth.log

Ta thấy được một số log được lưu sau khi tạo user.


```
TTCS_kali2 X Mar 2 07:22 The current date is: 02/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\NITRO 5>echo Trương Quốc Bảo - B22DCAT034
Trương Quốc Bảo - B22DCAT034

test@truongquocbaob22dcat034: /var/log
.2.gz auth.log.3.gz auth.log.4.gz bootstrap.log btmap btmap.1 cups dist-upgrade dmesg dmesg.0 dmesg.1.gz dmesg.2.gz dmesg.3.gz dmesg.4.gz
dpkg.log dpkg.log.1 dpkg.log.2.gz dpkg.log.3.gz faillog fontconfig.log gdm3 gpu-manager.log hp installer journal kern.log kern.log.1 ker
n.log.2.gz kern.log.3.gz kern.log.4.gz lastlog openvpn private snort speech-dispatcher syslog syslog.1 syslog.2.gz syslog.3.gz syslog.4.
gz syslog.5.gz syslog.6.gz syslog.7.gz ubuntu-advantage-apt-hook.log ubuntu-advantage.log ubuntu-advantage.log.1 ubuntu-advantage.log.2.
gz ubuntu-advantage.log.3.gz ubuntu-advantage-timer.log ubuntu-advantage-timer.log.1 ubuntu-advantage-timer.log.2.gz unattended-upgrades
vmware vmware-network.1.log vmware-network.2.log
Mar 2 07:16:32 truongquocbaob22dcat034 sudo: test : (command continued) vmware-network.3.log vmware-network.4.log vmware-network.5.
log vmware-network.6.log vmware-network.7.log vmware-network.8.log vmware-network.9.log vmware-network.log vmware-vmsvc-root.1.log vmwar
e-vmsvc-root.2.log vmware-vmsvc-root.3.log vmware-vmsvc-root.log vmware-vmttoolsd-root.log vmware-vmttoolsd-test.log vmware-vmusr-test.log
vsftpd.log wtmp
Mar 2 07:16:32 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 2 07:16:37 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session closed for user root
Mar 2 07:17:01 truongquocbaob22dcat034 CRON[4260]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 2 07:17:01 truongquocbaob22dcat034 CRON[4260]: pam_unix(cron:session): session closed for user root
Mar 2 07:18:29 truongquocbaob22dcat034 sshd[4199]: Received disconnect from 192.168.100.3 port 51998:11: disconnected by user
Mar 2 07:18:29 truongquocbaob22dcat034 sshd[4199]: Disconnected from user test 192.168.100.3 port 51998
Mar 2 07:18:29 truongquocbaob22dcat034 sshd[4121]: pam_unix(sshd:session): session closed for user test
Mar 2 07:18:29 truongquocbaob22dcat034 systemd-logind[900]: Session 7 logged out. Waiting for processes to exit.
Mar 2 07:18:29 truongquocbaob22dcat034 systemd-logind[900]: Removed session 7.
Mar 2 07:18:46 truongquocbaob22dcat034 sshd[4264]: Accepted publickey for test from 192.168.100.3 port 59830 ssh2: RSA SHA256:cyDSNkRrX
MQCK0Lf/DF6WHR/YkDqQZt4TW1gQRm5a6s
Mar 2 07:18:46 truongquocbaob22dcat034 sshd[4264]: pam_unix(sshd:session): session opened for user test by (uid=0)
Mar 2 07:18:46 truongquocbaob22dcat034 systemd-logind[900]: New session 9 of user test.
Mar 2 07:19:15 truongquocbaob22dcat034 sudo: test : TTY=pts/1 ; PWD=/home/test ; USER=root ; COMMAND=/usr/sbin/useradd tqb2
Mar 2 07:19:15 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session opened for user root by test(uid=0)
Mar 2 07:19:15 truongquocbaob22dcat034 useradd[4327]: new group: name=tqb2, UID=1002, GID=1002
Mar 2 07:19:15 truongquocbaob22dcat034 useradd[4327]: new user: name=tqb2, UID=1002, GID=1002, home=/home/tqb2, shell=/bin/sh, from=/de
v/pts/1
Mar 2 07:19:15 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session closed for user root
Mar 2 07:19:26 truongquocbaob22dcat034 sudo: test : TTY=pts/1 ; PWD=/home/test ; USER=root ; COMMAND=/usr/bin/passwd tqb2
Mar 2 07:19:26 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session opened for user root by test(uid=0)
Mar 2 07:19:28 truongquocbaob22dcat034 passwd[4338]: pam_unix(passwd:chauthtok): password changed for tqb2
Mar 2 07:19:28 truongquocbaob22dcat034 passwd[4338]: gkr-pam: couldn't update the login keyring password: no old password was entered
Mar 2 07:19:28 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session closed for user root
Mar 2 07:21:31 truongquocbaob22dcat034 sudo: test : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep -a Sun Mar 2
Mar 2 07:21:31 truongquocbaob22dcat034 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
test@truongquocbaob22dcat034:/var/log$
```

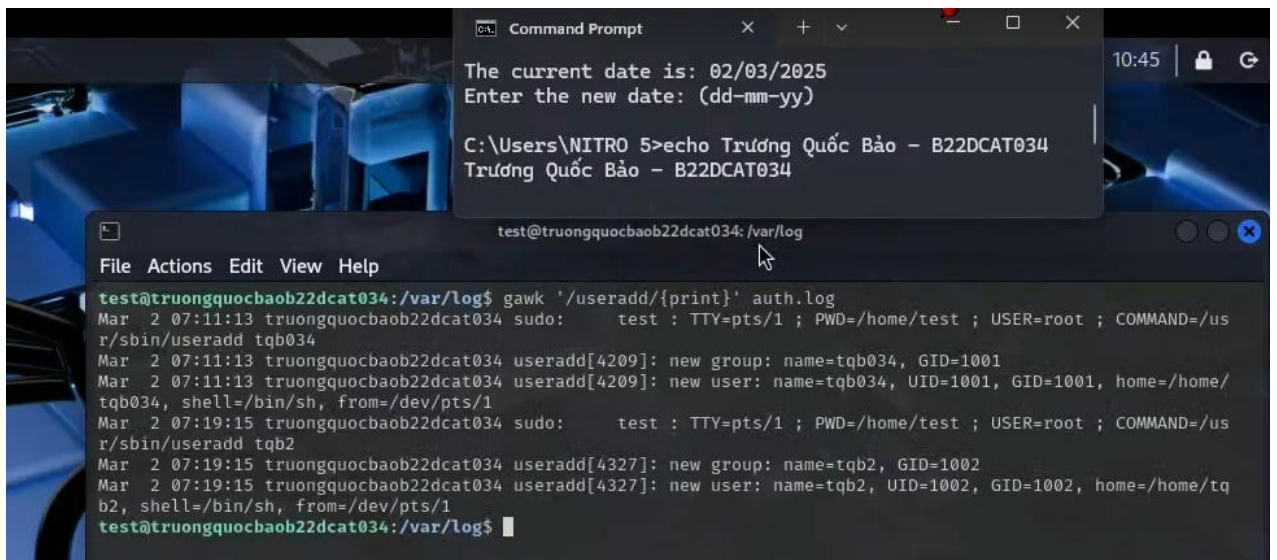
Hình 13 File access.log

Có thể tìm kiếm tương tự ở trên máy Kali với lệnh cat.

```
cat: auth.log: No such file or directory
test@truongquocbaob22dcat034:~$ cd /var/log
test@truongquocbaob22dcat034:/var/log$ cat auth.log | grep -a "new user"
Mar 2 07:11:13 truongquocbaob22dcat034 useradd[4209]: new user: name=tqb034, UID=1001, GID=1001, home=/home/
tqb034, shell=/bin/sh, from=/dev/pts/1
Mar 2 07:19:15 truongquocbaob22dcat034 useradd[4327]: new user: name=tqb2, UID=1002, GID=1002, home=/home/tq
b2, shell=/bin/sh, from=/dev/pts/1
test@truongquocbaob22dcat034:/var/log$
```

Hình 14 Tìm kiếm user vừa tạo bằng lệnh “grep”

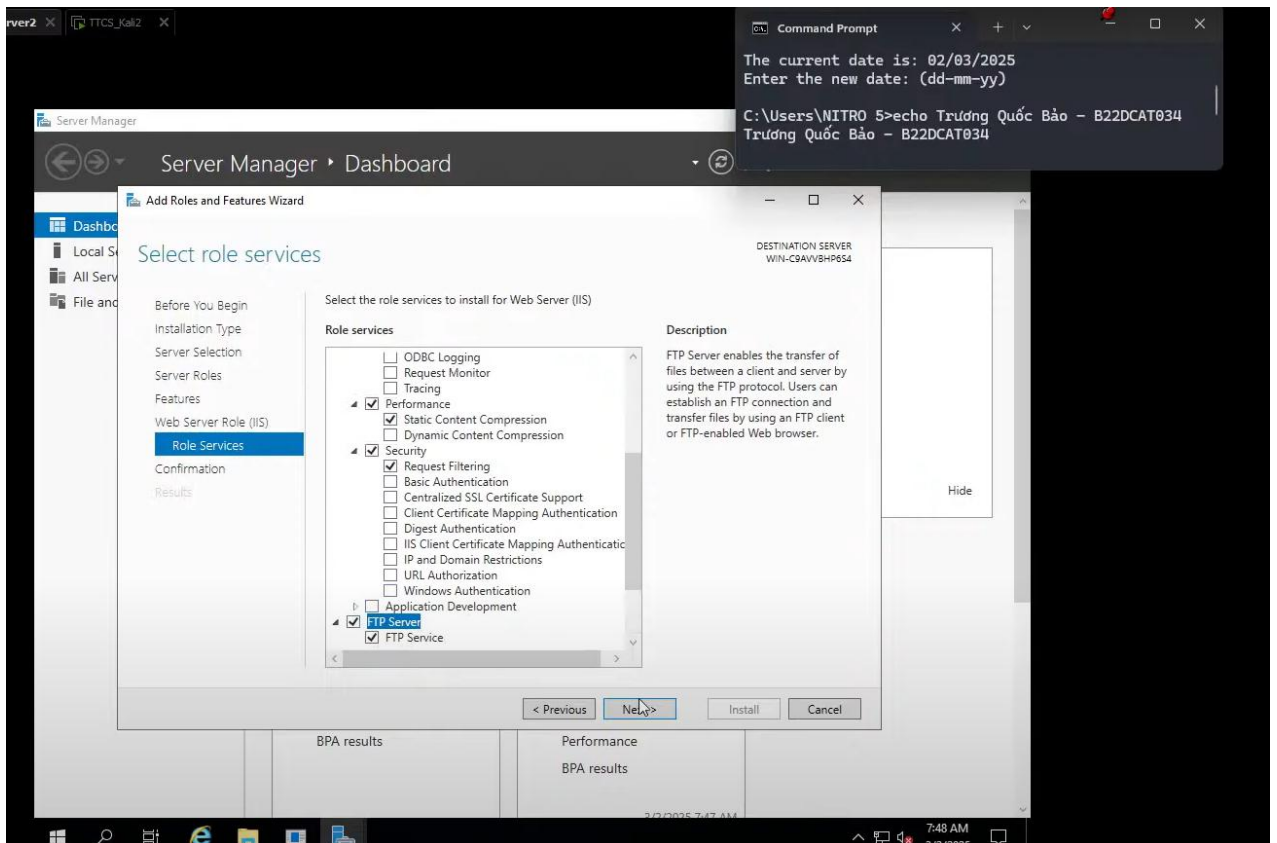
Sử dụng lệnh “gawk” để tìm kiếm dữ liệu tương tự.



Hình 15 Sử dụng lệnh “gawk”

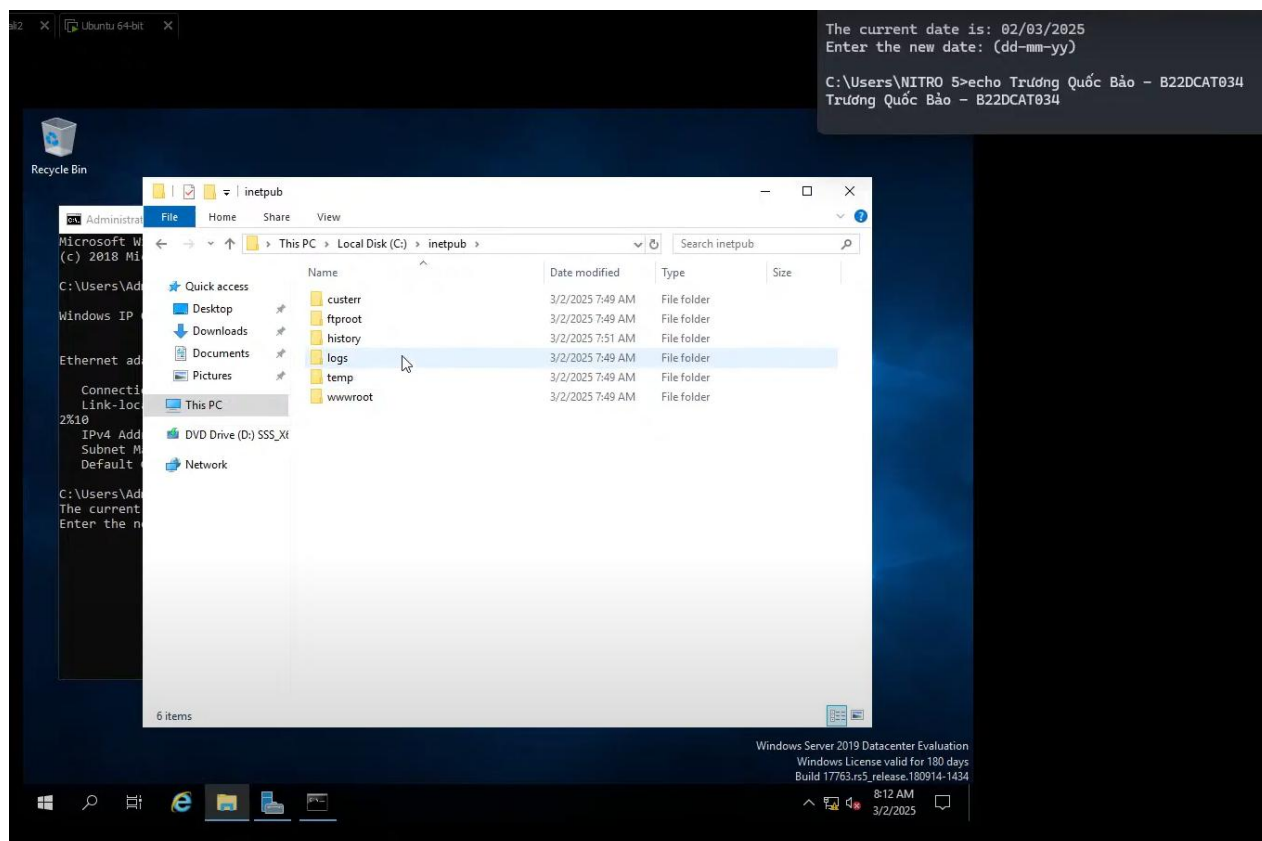
2.2.4 Phân tích log sử dụng find trong Windows

Cài đặt dịch vụ FTP Server trên máy Windows Server như các bài trước.



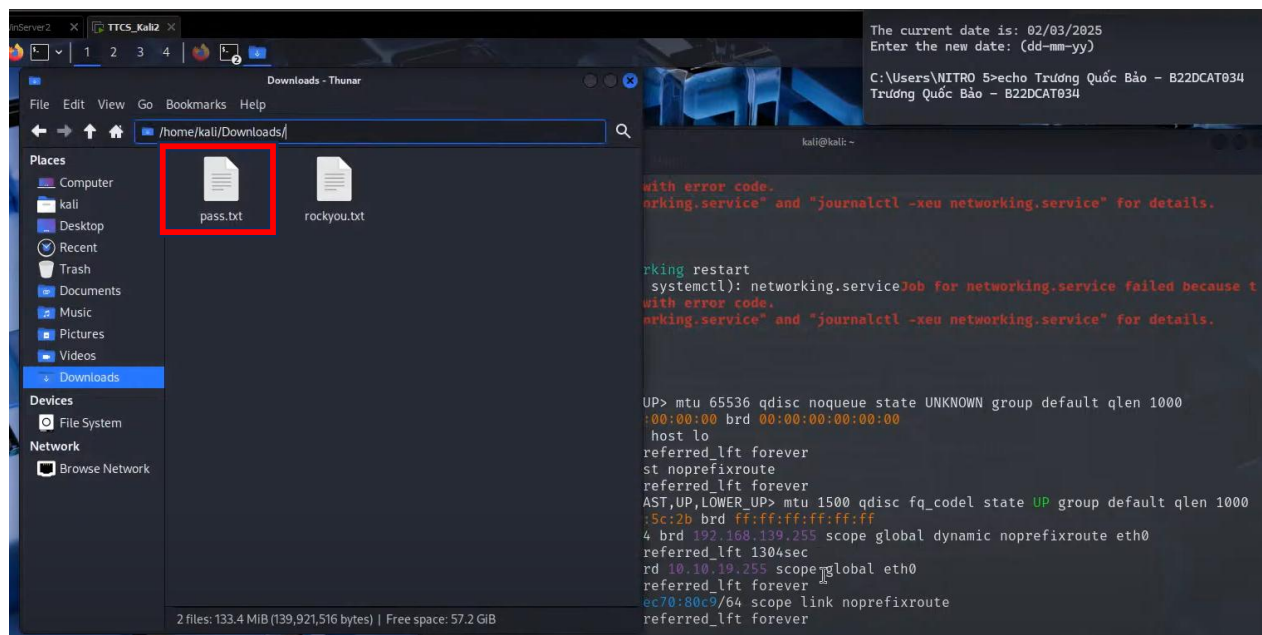
Hình 16 Cài đặt dịch vụ FTP trên máy Windows Server

Kiểm tra đường dẫn đến file ftp log để lưu file log của kết quả tấn công.



Hình 17 Kiểm tra đường dẫn tới thư mục logs

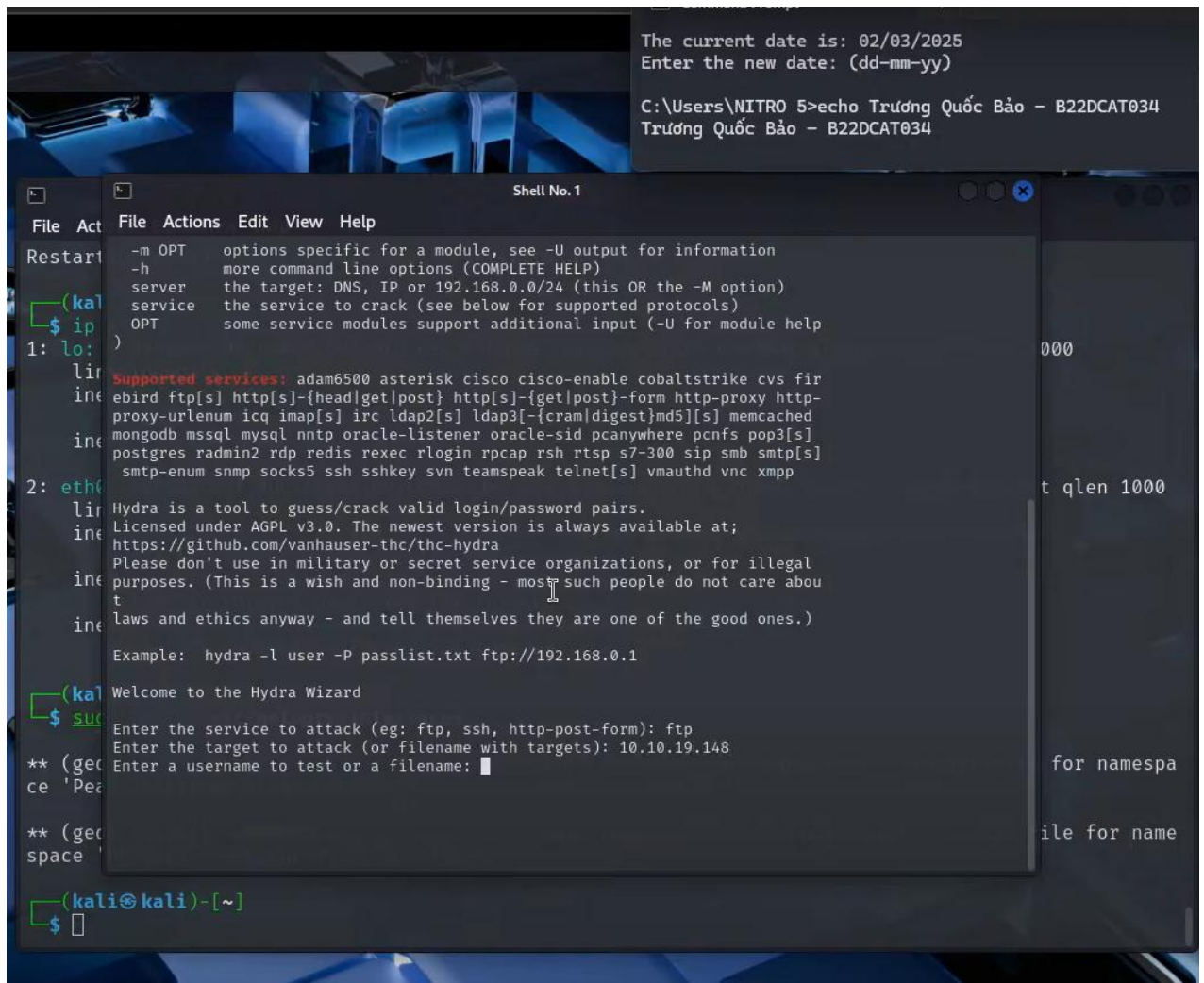
Trên máy Kali, tạo file pass.txt để lưu một số mật khẩu để dò, phải đảm bảo có mật khẩu chính xác để tiến hành tấn công dò quét.



Hình 18 Tạo password list

Nếu không có công cụ xhydra, ta có thể dùng công cụ hydra để thay thế, công cụ này làm việc trên giao diện dòng lệnh. Các thông tin yêu cầu gồm: dịch vụ để tấn công (ftp),

mục tiêu tấn công (địa chỉ IP của máy Windows – 10.10.19.202), tên đăng nhập (Administrator), danh sách mật khẩu (pass.txt), cổng tấn công (21) và một số tùy chọn cấu hình khác.



Hình 19 Sử dụng công cụ hydra

Thông báo dò mật khẩu thành công, mật khẩu này là chính xác so với máy Windows Server.

```
File Actions Edit View Help
Port number (press enter for default): 21

The following options are supported by the service module:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-02 12:45:07

Help for module ftp:
=====
The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -l Administrator -P pass.txt -u -s 21 10.10.19.202 ftp

Do you want to run the command now? [Y/n] y

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-02 12:45:07

[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try p r task
[DATA] attacking ftp://10.10.19.202:21/
[21][ftp] host: 10.10.19.202 login: Administrator password: Bao@1012
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-02 12:45:10

(kali@kali)-[~]
$ date
Sun Mar  2 12:45:15 PM EST 2025

(kali@kali)-[~]
$ echo Truong Quoc Bao - B22DCAT034
Truong Quoc Bao - B22DCAT034

(kali@kali)-[~]
$
```

Hình 20 Công cụ hydra dò mật khẩu thành công

Trên máy Windows Server, thực hiện điều hướng đến FTP Logfile(C:\cd c:\Windows\System32\Logfiles\msftpsvc1). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd).

Có thể thấy, công cụ hydra đã dò hết tất cả các mật khẩu đã lưu trong file pass.txt với tên đăng nhập là Anonymous.

```
Administrator: C:\Windows\System32\cmd.exe
The current date is: Sun 03/02/2025
Enter the new date: (mm-dd-yy)

C:\inetpub\logs\LogFiles\FTPSVC2>echo Truong Quoc Bao B22DCAT034
Truong Quoc Bao B22DCAT034

C:\inetpub\logs\LogFiles\FTPSVC2>dir
Volume in drive C has no label.
Volume Serial Number is 26AC-7065

Directory of C:\inetpub\logs\LogFiles\FTPSVC2
03/02/2025  09:26 AM    <DIR>          .
03/02/2025  09:26 AM    <DIR>          ..
03/02/2025  09:45 AM             10,293 u_ex250302.log
               1 File(s)              10,293 bytes
               2 Dir(s)  52,769,996,800 bytes free

C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex250302.log
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2025-03-02 17:26:53
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem sc-status sc-win32-status sc-substatus x-session
x-fullpath
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 49128417-cce9-46f1-bb23-471817a12873 -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 121c77ba-00d6-4516-8f10-0033adff89fc -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 f5f93b69-3020-49b8-ba87-ca6fc6bb3cce -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 2c85308a-10da-403c-8207-d9ef69ad5351 -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 USER Anonymous 331 0 0 49128417-cce9-46f1-bb23-471817a12873 -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 USER Anonymous 331 0 0 f5f93b69-3020-49b8-ba87-ca6fc6bb3cce -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 USER Anonymous 331 0 0 121c77ba-00d6-4516-8f10-0033adff89fc -
2025-03-02 17:26:53 10.10.19.148 - 10.10.19.202 21 USER Anonymous 331 0 0 2c85308a-10da-403c-8207-d9ef69ad5351 -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 PASS Bao@1012 53 1326 42 49128417-cce9-46f1-bb23-471817a12873 -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 PASS 344 530 132 42 121c77ba-00d6-4516-8f10-0033adff89fc -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 PASS 123 530 132 42 2c85308a-10da-403c-8207-d9ef69ad5351 -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 PASS 123432 530 326 42 f5f93b69-3020-49b8-ba87-ca6fc6bb3cce -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 121c77ba-00d6-4516-8f10-0033adff89fc -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 49128417-cce9-46f1-bb23-471817a12873 -
2025-03-02 17:26:54 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 f5f93b69-3020-49b8-ba87-ca6fc6bb3cce -
```

Hình 21 Đọc file log trên máy Windows

Gõ lệnh để tìm kiếm kết quả tấn công login thành công (C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type exyymmdd.log | find "230"). Ta đã thành công phân tích log sử dụng find trong Windows.

```
Administrator: C:\Windows\System32\cmd.exe
scyea8443a5c6 -
2025-03-02 17:44:22 10.10.19.148 WIN-C9AVVBHP6S4\Administrator 10.10.19.202 21 FEAT - 211 0 0 2d51339c-f2ef-4050-b3fe-95
ea8443a5c6 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 81a6feba-4ebd-49a6-bbae-06f8deb2a305 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 71a1a97d-4bef-4a38-aabe-3df13b06514c -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 cc0f8098-c169-4f43-b57d-d043cd3cd674 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 6e904b99-3ef1-4800-9d9c-0b4749eaf964 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 6e904b99-3ef1-4800-9d9c-0b4749eaf964 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 81a6feba-4ebd-49a6-bbae-06f8deb2a305 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 cc0f8098-c169-4f43-b57d-d043cd3cd674 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 71a1a97d-4bef-4a38-aabe-3df13b06514c -
2025-03-02 17:45:08 10.10.19.148 WIN-C9AVVBHP6S4\Administrator 10.10.19.202 21 PASS *** 230 0 0 cc0f8098-c169-4f43-b57d-
d043cd3cd674 /
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 6e904b99-3ef1-4800-9d9c-0b4749eaf964 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 81a6feba-4ebd-49a6-bbae-06f8deb2a305 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 71a1a97d-4bef-4a38-aabe-3df13b06514c -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 6e904b99-3ef1-4800-9d9c-0b4749eaf964 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 81a6feba-4ebd-49a6-bbae-06f8deb2a305 -
2025-03-02 17:45:08 10.10.19.148 - 10.10.19.202 21 ControlChannelClosed - - 0 0 71a1a97d-4bef-4a38-aabe-3df13b06514c -
2025-03-02 17:45:08 10.10.19.148 WIN-C9AVVBHP6S4\Administrator 10.10.19.202 21 ControlChannelClosed - - 0 0 cc0f8098-c16
9-4f43-b57d-d043cd3cd674 -

C:\inetpub\logs\LogFiles\FTP5VC2>type u_ex250302.log | grep "230"
'grep' is not recognized as an internal or external command,
operable program or batch file.

C:\inetpub\logs\LogFiles\FTP5VC2>type u_ex250302.log | find "230"
2025-03-02 17:44:22 10.10.19.148 WIN-C9AVVBHP6S4\Administrator 10.10.19.202 21 PASS *** 230 0 0 2d51339c-f2ef-4050-b3fe-
95ea8443a5c6 /
2025-03-02 17:45:08 10.10.19.148 WIN-C9AVVBHP6S4\Administrator 10.10.19.202 21 PASS *** 230 0 0 cc0f8098-c169-4f43-b57d-
d043cd3cd674 /

C:\inetpub\logs\LogFiles\FTP5VC2>date
The current date is: Sun 03/02/2025
Enter the new date: (mm-dd-yy)

C:\inetpub\logs\LogFiles\FTP5VC2>echo Truong Quoc Bao B22DCAT034
Truong Quoc Bao B22DCAT034

C:\inetpub\logs\LogFiles\FTP5VC2>
```

Hình 22 Tìm kiếm kết quả tấn công

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] https://linuxcommand.org/lc3_man_pages/grep1.html
- [4] <http://www.gnu.org/software/gawk/manual/gawk.html>
- [5] <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>
- [6] <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>