

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



*Môn: Thực tập cơ sở*

***BÁO CÁO THỰC TẬP CƠ SỞ***  
***Bài 10: Phân tích log hệ thống***

***Họ và tên giảng viên:*** PGS.TS.Đỗ Xuân Chợt  
***Họ và tên:*** Phạm Thanh Tùng  
***Mã sinh viên:*** B20DCAT171  
***Lớp:*** D20CQAT03-B  
***Số điện thoại:*** 0856915668

Hà Nội 2023

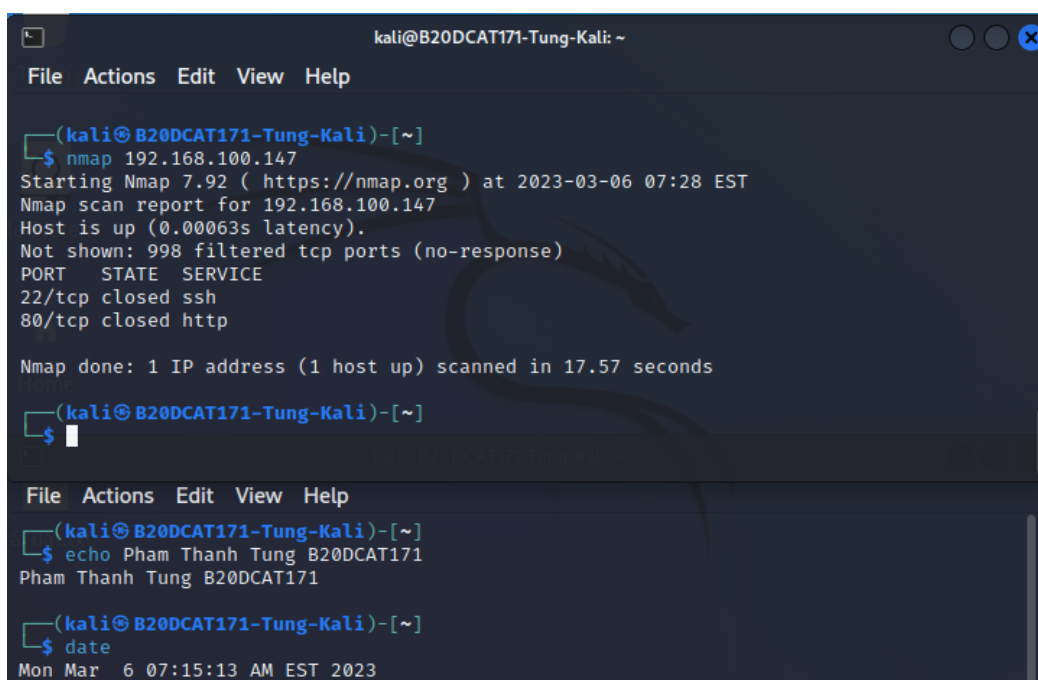
# 1. Tìm hiểu lý thuyết

\*Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk, find, secure, access.log:

- grep tìm kiếm các mẫu trong mỗi tệp. Các mẫu là một hoặc các từ khóa được phân tách bởi các ký tự dòng mới và grep in mỗi dòng phù hợp với một mẫu
- gawk là phiên bản GNU của chương trình Unix awk thường có sẵn, một trình soạn thảo luồng phổ biến khác. Chức năng cơ bản của awk là tìm kiếm các tập tin cho các dòng (hoặc các đơn vị văn bản khác) có chứa các mẫu nhất định. Khi một dòng khớp với một trong các mẫu, awk thực hiện các hành động được chỉ định trên dòng đó. awk tiếp tục xử lý các dòng đầu vào theo cách này cho đến khi nó đến cuối tệp đầu vào. Các chương trình trong awk khác với các chương trình ở hầu hết các ngôn ngữ khác, bởi vì các chương trình awk là hướng dữ liệu (tức là mô tả dữ liệu muốn làm việc và sau đó phải làm gì khi tìm thấy nó). Hầu hết các ngôn ngữ khác là thủ tục; người dùng phải mô tả chi tiết từng bước mà chương trình phải thực hiện. Khi làm việc với các ngôn ngữ thủ tục, việc mô tả rõ ràng dữ liệu mà chương trình của sẽ xử lý sẽ khó hơn nhiều. Vì lý do này, các chương trình awk thường dễ đọc và dễ viết. Khi chạy awk, người dùng chỉ định một chương trình awk cho awk biết phải làm gì. Chương trình bao gồm một loạt các quy tắc (nó cũng có thể chứa các định nghĩa hàm, một tính năng nâng cao mà chúng ta sẽ bỏ qua lúc này; xem phần Các hàm do người dùng xác định). Mỗi quy tắc chỉ định một mẫu để tìm kiếm và một hành động cần thực hiện khi tìm thấy mẫu.
- find tìm kiếm một chuỗi văn bản trong một tệp hoặc tệp và hiển thị các dòng văn bản chứa chuỗi được chỉ định
- xhydra là GUI cho phần mềm bẻ khóa mật khẩu có tên là Hydra. Hydra có thể được sử dụng cho cả bẻ khóa mật khẩu ngoại tuyến và trực tuyến. Hydra có thể được sử dụng cho nhiều loại tấn công trực tuyến, bao gồm các cuộc tấn công chống lại MySQL, SMB, MSSQL và nhiều loại đăng nhập HTTP/HTTPS.
- access.log là tệp nhật ký truy cập Apache, một trong số các tệp nhật ký được tạo bởi máy chủ Apache HTTP. Tệp nhật ký cụ thể này chịu trách nhiệm ghi dữ liệu cho tất cả các yêu cầu được xử lý bởi máy chủ Apache.

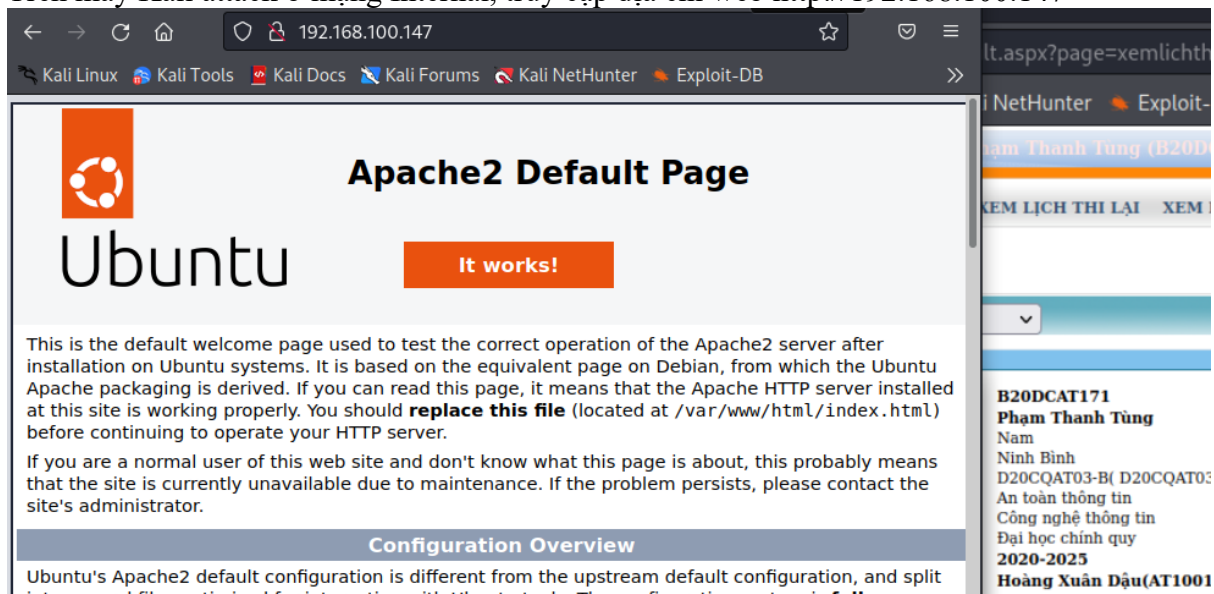
## 2. Nội dung thực hành

a. Phân tích log sử dụng grep trong Linux



```
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ nmap 192.168.100.147  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-06 07:28 EST  
Nmap scan report for 192.168.100.147  
Host is up (0.00063s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    closed ssh  
80/tcp    closed http  
  
Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$  
  
File Actions Edit View Help  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo Pham Thanh Tung B20DCAT171  
Pham Thanh Tung B20DCAT171  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ date  
Mon Mar  6 07:15:13 AM EST 2023
```

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



lt.aspx?page=xemlichth

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

## Apache2 Default Page

# Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

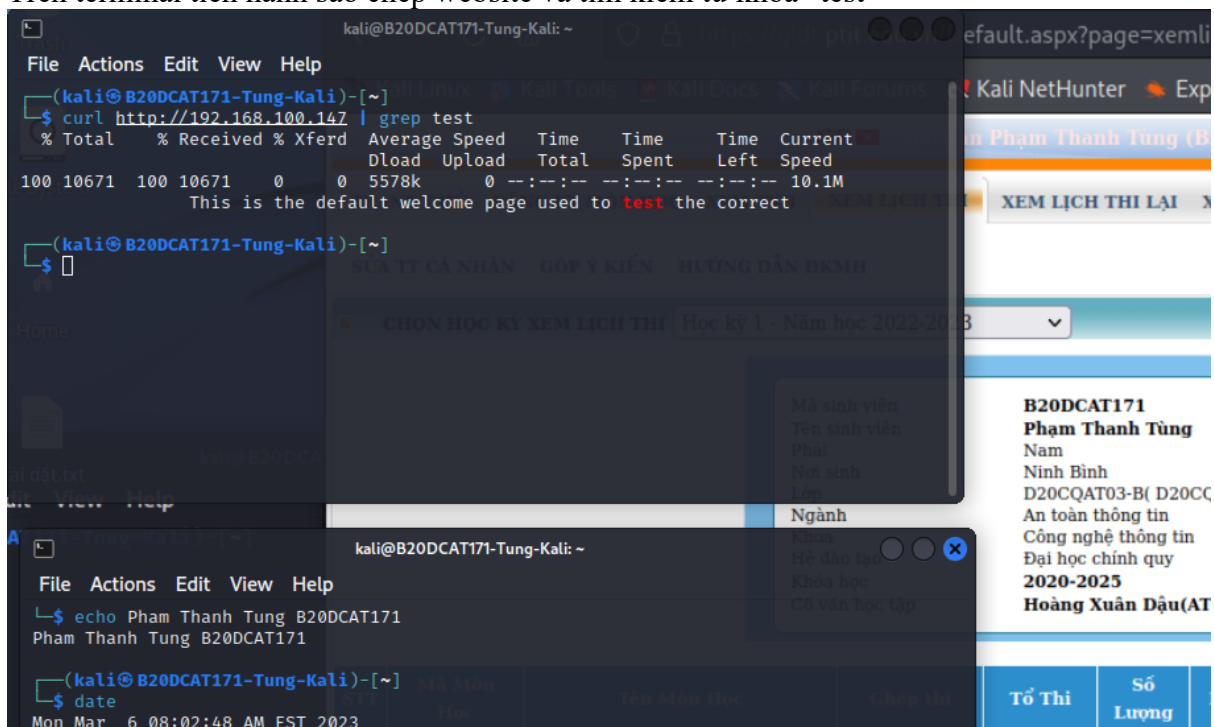
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully**

**B20DCAT171**  
**Phạm Thanh Tùng**  
Nam  
Ninh Bình  
D20CQAT03-B( D20CQAT03  
An toàn thông tin  
Công nghệ thông tin  
Đại học chính quy  
**2020-2025**  
**Hoàng Xuân Diệu(AT1001**

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



kali@B20DCAT171-Tung-Kali: ~

File Actions Edit View Help

```
(kali@B20DCAT171-Tung-Kali)-[~]  
$ curl http://192.168.100.147 | grep test  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 10671 100 10671 0 0 5578k 0 --:--:-- --:--:-- --:--:-- 10.1M  
This is the default welcome page used to test the correct
```

(kali@B20DCAT171-Tung-Kali)-[~]  
\$

SỬA TT CÁ NHÂN GÓP Ý KIẾN HƯỚNG DẪN ĐKMH

CHỌN HỌC KỲ XEM LỊCH THI Học kỳ 1 - Năm học 2022-2023

Mã sinh viên  
Tên sinh viên  
Phái  
Nơi sinh  
Lớp  
Ngành  
Khoa  
Hệ đào tạo  
Khóa học  
Cơ vấn học tập

**B20DCAT171**  
**Phạm Thanh Tùng**  
Nam  
Ninh Bình  
D20CQAT03-B( D20CQ  
An toàn thông tin  
Công nghệ thông tin  
Đại học chính quy  
**2020-2025**  
**Hoàng Xuân Diệu(AT**

File Actions Edit View Help

```
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo Pham Thanh Tung B20DCAT171  
Pham Thanh Tung B20DCAT171  
$ date  
Mon Mar 6 08:02:48 AM EST 2023
```

Tổ Thi Số Lượng

Trên máy Linux Internal Victim, kiểm tra file access\_log

```
b20dcat171@b20dcat171:/var/log/apache2$ cat access.log | grep Firefox
10.10.19.131 - - [06/Mar/2023:19:50:26 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
10.10.19.131 - - [06/Mar/2023:19:50:26 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://10.10.19.131/" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
10.10.19.131 - - [06/Mar/2023:19:50:26 +0700] "GET /favicon.ico HTTP/1.1" 404 490 "http://10.10.19.131/" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
192.168.100.147 - - [06/Mar/2023:19:52:11 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
192.168.100.147 - - [06/Mar/2023:19:52:11 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
192.168.100.147 - - [06/Mar/2023:19:52:11 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0"
192.168.100.3 - - [06/Mar/2023:20:00:31 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.100.3 - - [06/Mar/2023:20:00:31 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.100.3 - - [06/Mar/2023:20:00:31 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"

b20dcat171@b20dcat171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
b20dcat171@b20dcat171:~$ date
Thứ hai, 06 Tháng 3 năm 2023 20:04:48 +07
```

## b. Phân tích log sử dụng gawk trong Linux

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

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.

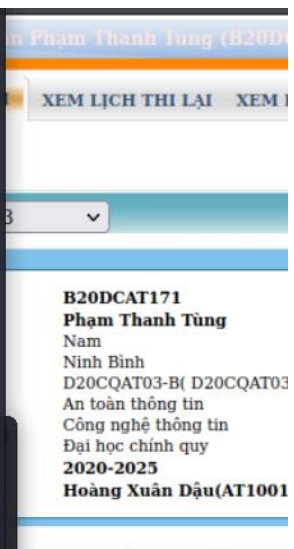
```
(kali@B20DCAT171-Tung-Kali)-[~]
$ ssh b20dcat171@192.168.100.147
b20dcat171@192.168.100.147's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.19.0-35-generic x86_64)

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

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

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

Last login: Mon Mar  6 20:13:10 2023 from 192.168.100.3
b20dcat171@b20dcat171:~$ sudo useradd TungPT-B20DCAT171
[sudo] password for b20dcat171:
b20dcat171@b20dcat171:~$ sudo passwd TungPT-B20DCAT171
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
b20dcat171@b20dcat171:~$
```



Trên máy Linux Internal Victim, tiến hành xem file log bằng lệnh journalctl -t sshd:

```

Mar 6 20:26:54 b20dcat171 sshd[2257]: pam_unix(sshd:session): session closed for user b20dcat171
Mar 6 20:31:18 b20dcat171 sshd[847]: Server listening on 0.0.0.0 port 22.
Mar 6 20:31:18 b20dcat171 sshd[847]: Server listening on :: port 22.
root@b20dcat171:/home/b20dcat171/Desktop# journalctl -t sshd
Thg 3 06 20:08:52 b20dcat171 sshd[2588]: Server listening on 0.0.0.0 port 22.
Thg 3 06 20:08:52 b20dcat171 sshd[2588]: Server listening on :: port 22.
Thg 3 06 20:12:18 b20dcat171 sshd[2588]: Received signal 15; terminating.
-- Boot 8e58dbee49224e78ad0fdebc3dddc5ec --
Thg 3 06 20:12:26 b20dcat171 sshd[1037]: Server listening on 0.0.0.0 port 22.
Thg 3 06 20:12:26 b20dcat171 sshd[1037]: Server listening on :: port 22.
Thg 3 06 20:13:09 b20dcat171 sshd[2169]: Accepted password for b20dcat171 from 192.168.100.3 port 59572 ssh2
Thg 3 06 20:13:09 b20dcat171 sshd[2169]: pam_unix(sshd:session): session opened for user b20dcat171(uid=1000) by b20dcat171
Thg 3 06 20:13:19 b20dcat171 sshd[2230]: Received disconnect from 192.168.100.3 port 59572:11: disconnected by user
Thg 3 06 20:13:19 b20dcat171 sshd[2230]: Disconnected from user b20dcat171 192.168.100.3 port 59572
Thg 3 06 20:13:19 b20dcat171 sshd[2169]: pam_unix(sshd:session): session closed for user b20dcat171
Thg 3 06 20:13:26 b20dcat171 sshd[2257]: Accepted password for b20dcat171 from 192.168.100.3 port 41760 ssh2
Thg 3 06 20:13:26 b20dcat171 sshd[2257]: pam_unix(sshd:session): session opened for user b20dcat171(uid=1000) by b20dcat171
Thg 3 06 20:26:54 b20dcat171 sshd[2294]: Received disconnect from 192.168.100.3 port 41760:11: disconnected by user
Thg 3 06 20:26:54 b20dcat171 sshd[2294]: Disconnected from user b20dcat171 192.168.100.3 port 41760
Thg 3 06 20:26:54 b20dcat171 sshd[2257]: pam_unix(sshd:session): session closed for user b20dcat171
Thg 3 06 20:31:08 b20dcat171 sshd[1037]: Received signal 15; terminating.
-- Boot ead2f6c37c004ae5912f71a9e015261 --
Thg 3 06 20:31:18 b20dcat171 sshd[847]: Server listening on 0.0.0.0 port 22.
Thg 3 06 20:31:18 b20dcat171 sshd[847]: Server listening on :: port 22.
Thg 3 06 20:37:50 b20dcat171 sshd[2294]: Accepted password for b20dcat171 from 192.168.100.3 port 57808 ssh2
Thg 3 06 20:37:50 b20dcat171 sshd[2294]: pam_unix(sshd:session): session opened for user b20dcat171(uid=1000) by b20dcat171
Thg 3 06 20:45:27 b20dcat171 sshd[2353]: Received disconnect from 192.168.100.3 port 57808:11: disconnected by user
Thg 3 06 20:45:27 b20dcat171 sshd[2353]: Disconnected from user b20dcat171 192.168.100.3 port 57808
Thg 3 06 20:45:27 b20dcat171 sshd[2294]: pam_unix(sshd:session): session closed for user b20dcat171

```

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

```

(kali@B20DCAT171-Tung-Kali)-[~]
$ ssh b20dcat171@192.168.100.147
b20dcat171@192.168.100.147's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.19.0-35-generic x86_64)

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

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

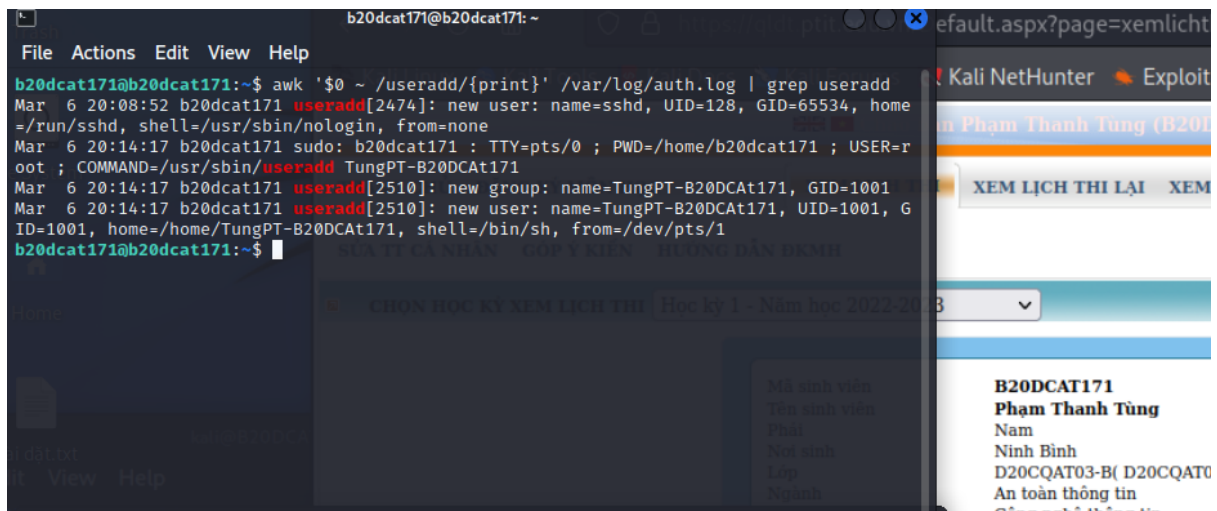
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Mar 6 20:13:26 2023 from 192.168.100.3
b20dcat171@b20dcat171:~$ cat /var/log/auth.log | grep useradd
cat: /var/log/auth.log: No such file or directory
b20dcat171@b20dcat171:~$ cat /var/log/auth.log | grep useradd
Mar 6 20:08:52 b20dcat171 useradd[2474]: new user: name=sshd, UID=128, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none
Mar 6 20:14:17 b20dcat171 sudo: b20dcat171 : TTY=pts/0 ; PWD=/home/b20dcat171 ; USER=root ; COMMAND=/usr/sbin/useradd TungPT-B20DCAT171
Mar 6 20:14:17 b20dcat171 useradd[2510]: new group: name=TungPT-B20DCAT171, GID=1001
Mar 6 20:14:17 b20dcat171 useradd[2510]: new user: name=TungPT-B20DCAT171, UID=1001, GID=1001, home=/home/TungPT-B20DCAT171, shell=/bin/sh, from=/dev/pts/1
b20dcat171@b20dcat171:~$

```

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

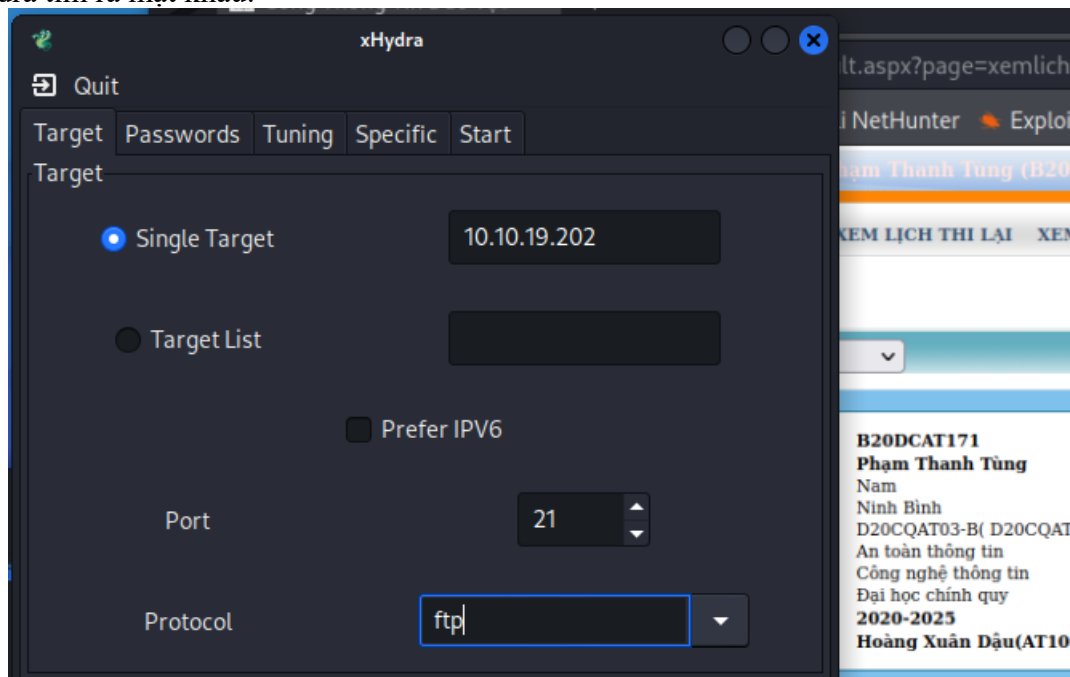


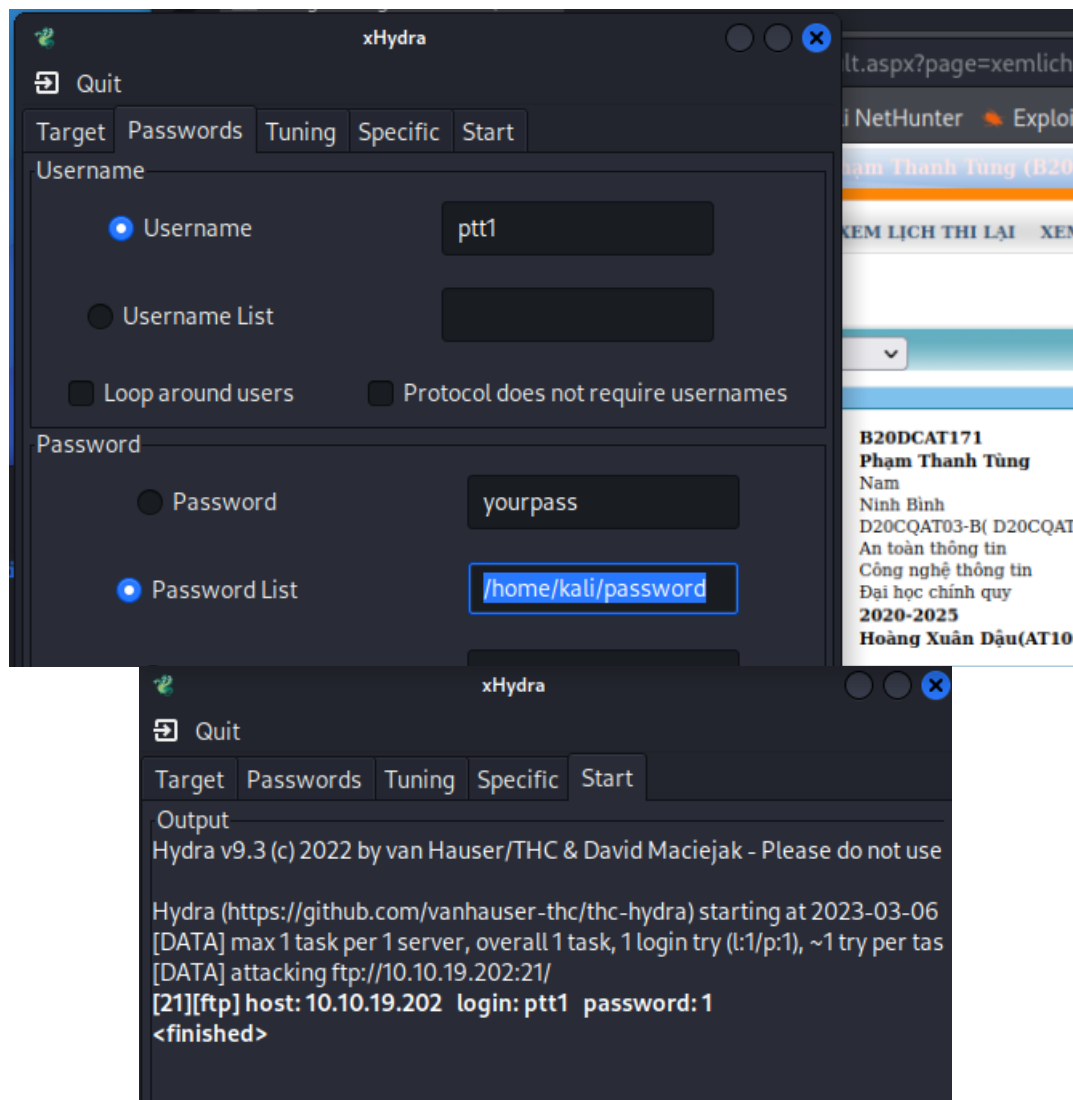


c Phân tích log sử dụng find trong Windows

Trên máy Kali External Attack khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list, sau đó nhấn Start:

xHydra tìm ra mật khẩu:





Trên máy Windows 2019 Server External Victim, 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). Gõ lệnh để tìm kiếm kết quả tấn công login thành công (C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type exymmdd.log | find "230")

```
C:\Windows\System32\LogFiles\FTPSVC2>type u_ex230307.log | find "230"
2023-03-07 02:30:49 10.10.19.148 TUNGPT171\ptt1 10.10.19.202 21 PASS *** 230 0 3 452e3401-ab02-4bc2-a49c-8a0b46124753 /
2023-03-07 02:31:53 10.10.19.148 TUNGPT171\ptt1 10.10.19.202 21 PASS *** 230 0 3 d5b487f5-d4ca-4fc9-af2a-a6cfa2aa84c /
2023-03-07 02:31:56 10.10.19.148 - 10.10.19.202 21 ControlChannelOpened - - 0 0 f1d08ea4-1f3c-4230-9441-e04e741ad696 -
2023-03-07 02:31:57 10.10.19.148 - 10.10.19.202 21 USER ptt1 331 0 0 f1d08ea4-1f3c-4230-9441-e04e741ad696 -
2023-03-07 02:31:57 10.10.19.148 TUNGPT171\ptt1 10.10.19.202 21 PASS *** 230 0 3 f1d08ea4-1f3c-4230-9441-e04e741ad696 /
2023-03-07 02:31:57 10.10.19.148 TUNGPT171\ptt1 10.10.19.202 21 ControlChannelClosed - - 0 0 f1d08ea4-1f3c-4230-9441-e04e741ad696 -

C:\Windows\System32\LogFiles\FTPSVC2>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Windows\System32\LogFiles\FTPSVC2>date
The current date is: Tue 03/07/2023
Enter the new date: (mm-dd-yy)
```