

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



BÀI 9: PHÂN TÍCH LOG HỆ THỐNG

Giảng viên : Nguyễn Ngọc Diệp

Sinh viên : Nguyễn Đức Anh

Mã sinh viên : B21DCAT031

Hệ : Đại học chính quy

Hà Nội, 4/2024

Table of Contents

1. Mục đích	3
2. Nội dung thực hành	3
2.1 Tìm hiểu lý thuyết	3
a. Lệnh grep.....	3
b. Lệnh gawk	3
c. Lệnh find	4
d. Lệnh xhydra.....	4
2.2 Tài liệu tham khảo	5
2.3 Chuẩn bị môi trường	5
2.4 Các bước thực hiện	5
a. Phân tích log sử dụng grep trong Linux.....	5
b. Phân tích log sử dụng gawk trong Linux	8
c. Phân tích log sử dụng find trong Linux	10
3. Kết quả đạt được	13

1. Mục đích

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. Nội dung thực hành

2.1 Tìm hiểu lý thuyết

a. Lệnh grep

"grep" là một công cụ mạnh mẽ được sử dụng để tìm kiếm các dòng văn bản trong tệp tin hoặc đầu ra từ một lệnh khác, dựa trên một biểu thức chính quy (regular expression) được chỉ định. "grep" thường được sử dụng trong các hệ thống Unix và tương thích với nhiều hệ điều hành khác nhau.

Một số tính năng chính của "grep":

- Tìm kiếm dựa trên mẫu: "grep" cho phép tìm kiếm các dòng văn bản trong một tệp hoặc đầu ra từ một lệnh khác dựa trên một biểu thức chính quy chỉ định.
- Tìm kiếm từ khóa đơn giản: ngoài việc sử dụng biểu thức chính quy, cũng có thể sử dụng "grep" để tìm kiếm các chuỗi đơn giản trong dữ liệu văn bản.
- Tìm kiếm đệ quy: có thể sử dụng tùy chọn -r hoặc --recursive để tìm kiếm các chuỗi trong tất cả các tệp và thư mục con của một thư mục được chỉ định.
- In dòng số: "grep" có thể in ra số dòng tương ứng với mỗi dòng văn bản được tìm thấy.
- Tìm kiếm không phân biệt chữ hoa chữ thường: có thể sử dụng tùy chọn -i hoặc --ignore-case để tìm kiếm mà không phân biệt chữ hoa chữ thường.
- Loại trừ kết quả: có thể sử dụng tùy chọn -v hoặc --invert-match để loại trừ các kết quả từ kết quả tìm kiếm.
- Sử dụng với các ống: "grep" có thể được kết hợp với các ống (pipes) để lọc dữ liệu đầu ra từ các lệnh khác.

b. Lệnh gawk

"gawk" là một công cụ mạnh mẽ trong họ các công cụ xử lý văn bản và dữ liệu, được phát triển dựa trên ngôn ngữ lập trình awk. Tên "gawk" là viết tắt của "GNU awk", là một phiên bản mở rộng của awk được phát triển bởi Dự án GNU. "gawk" cung cấp nhiều tính năng mạnh mẽ để xử lý và biến đổi dữ liệu văn bản dễ dàng và hiệu quả.

Một số tính năng chính của "gawk":

- Xử lý dữ liệu dạng bảng: "gawk" cho phép xử lý và biến đổi dữ liệu dạng bảng có cấu

trúc với các cột và hàng.

- Biểu thức chính quy: có thể sử dụng biểu thức chính quy trong "gawk" để tìm kiếm và thay thế các chuỗi dữ liệu dựa trên mẫu nhất định.
- Xử lý các tệp văn bản: "gawk" thích hợp để xử lý các tệp văn bản, nhật ký, báo cáo và định dạng dữ liệu tương tự.
- Tùy biến đầu vào/đầu ra: có thể tùy chỉnh cách "gawk" đọc dữ liệu đầu vào và xuất ra, bao gồm việc sử dụng các dấu phân cách tùy chỉnh và xử lý các tệp nén.
- Biên đếm và tổng hợp: "gawk" cho phép tính toán và tổng hợp các giá trị từ dữ liệu, bao gồm đếm số lần xuất hiện của các mục và tính tổng các giá trị trong các cột.
- Lập trình kịch bản: có thể sử dụng "gawk" như một ngôn ngữ lập trình kịch bản để thực hiện các tác vụ phức tạp, bao gồm việc sử dụng biến, hàm và điều kiện rẽ nhánh.
- Hỗ trợ đa nền tảng: "gawk" được hỗ trợ trên nhiều hệ điều hành khác nhau và có sẵn trong hầu hết các bản phân phối Linux và Unix.

c. Lệnh find

"find" là một công cụ mạnh mẽ trong hệ điều hành Unix và tương thích được sử dụng để tìm kiếm các tệp và thư mục dựa trên các tiêu chí nhất định. "find" có thể được sử dụng để tìm kiếm theo tên tệp, kích thước, quyền truy cập, thời gian sửa đổi và nhiều tiêu chí khác.

Một số tính năng chính của "find":

- Tìm kiếm tệp và thư mục: "find" cho phép tìm kiếm tất cả các tệp và thư mục trong một cây thư mục.
- Tìm kiếm dựa trên tiêu chí: có thể chỉ định các tiêu chí cụ thể như tên tệp, kích thước, quyền truy cập, thời gian sửa đổi và nhiều tiêu chí khác để tìm kiếm.
- Tìm kiếm đệ quy: "find" có thể tìm kiếm đệ quy trong tất cả các thư mục con của một thư mục được chỉ định.
- Thực hiện các hành động trên các kết quả: Sau khi tìm kiếm, "find" có thể thực hiện các hành động như in ra tên tệp, thực thi một lệnh trên mỗi tệp được tìm thấy, hoặc thực hiện các hành động khác.
- Kết hợp các tiêu chí: có thể kết hợp nhiều tiêu chí tìm kiếm để chúng hoạt động cùng nhau.
- Tìm kiếm theo mẫu: "find" hỗ trợ tìm kiếm theo biểu thức chính quy (regex) cho các tiêu chí như tên tệp.
- Tìm kiếm dựa trên quyền truy cập: có thể tìm kiếm các tệp dựa trên quyền truy cập của người dùng, nhóm hoặc các quyền cụ thể.

d. Lệnh 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, và nhiều loại

giao thức khác. Đây là một phần của dự án THC-Hydra, một công cụ kiểm tra bảo mật mạng phổ biến được sử dụng để kiểm tra và phân tích các hệ thống bảo mật mạng.

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, SNMP, và nhiều giao thức khác.
- 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.

2.2 Tài liệu tham khảo

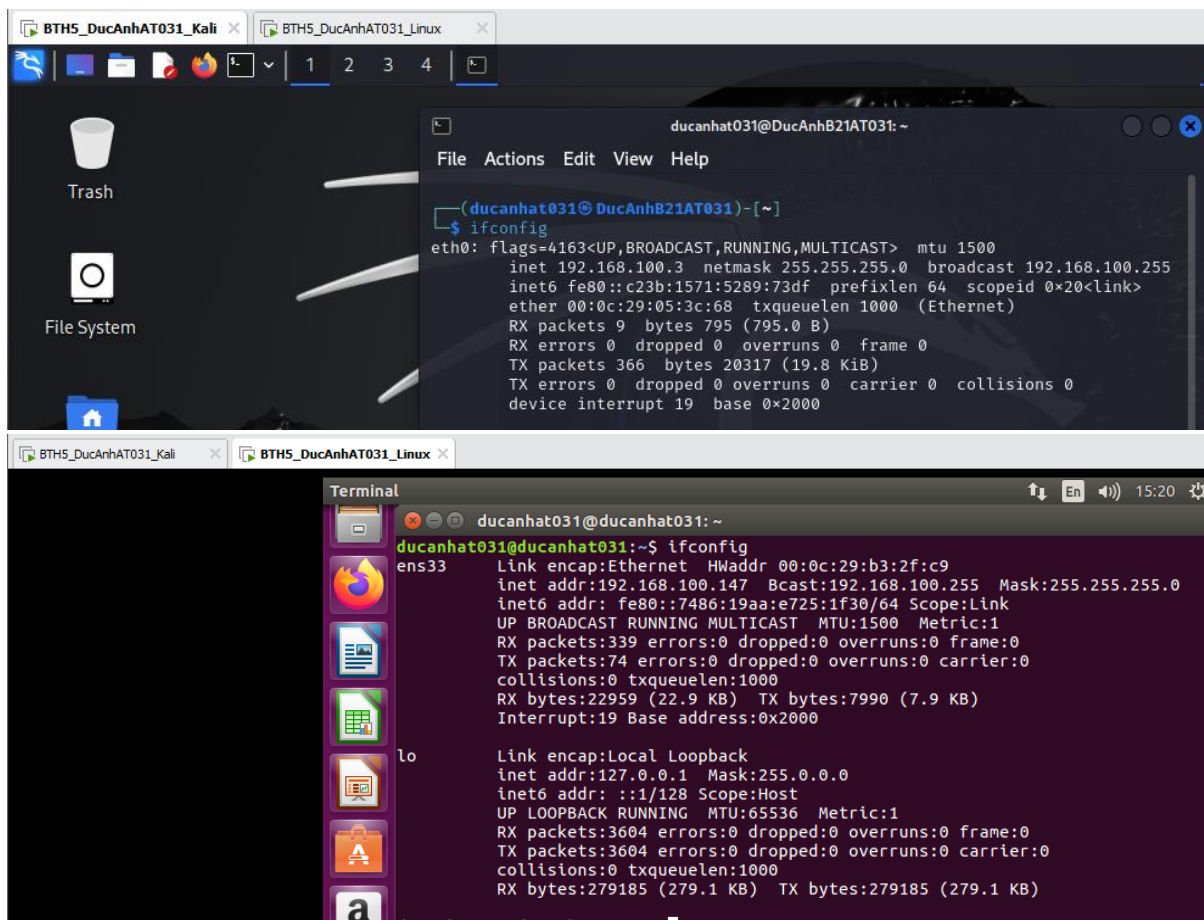
- https://linuxcommand.org/lc3_man_pages/grep1.html
- <http://www.gnu.org/software/gawk/manual/gawk.html>
- <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>
- <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>

2.3 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm 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.
- Topo mạng như đã cấu hình trong bài 5.

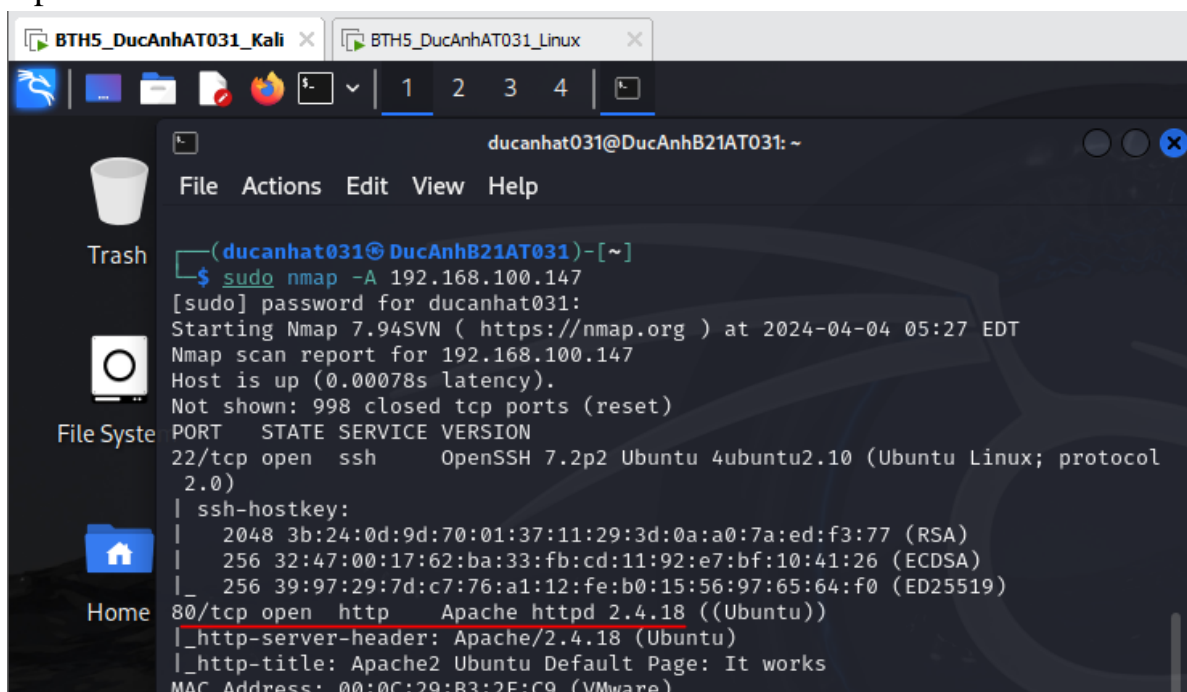
2.4 Các bước thực hiện

- a. Phân tích log sử dụng grep trong Linux

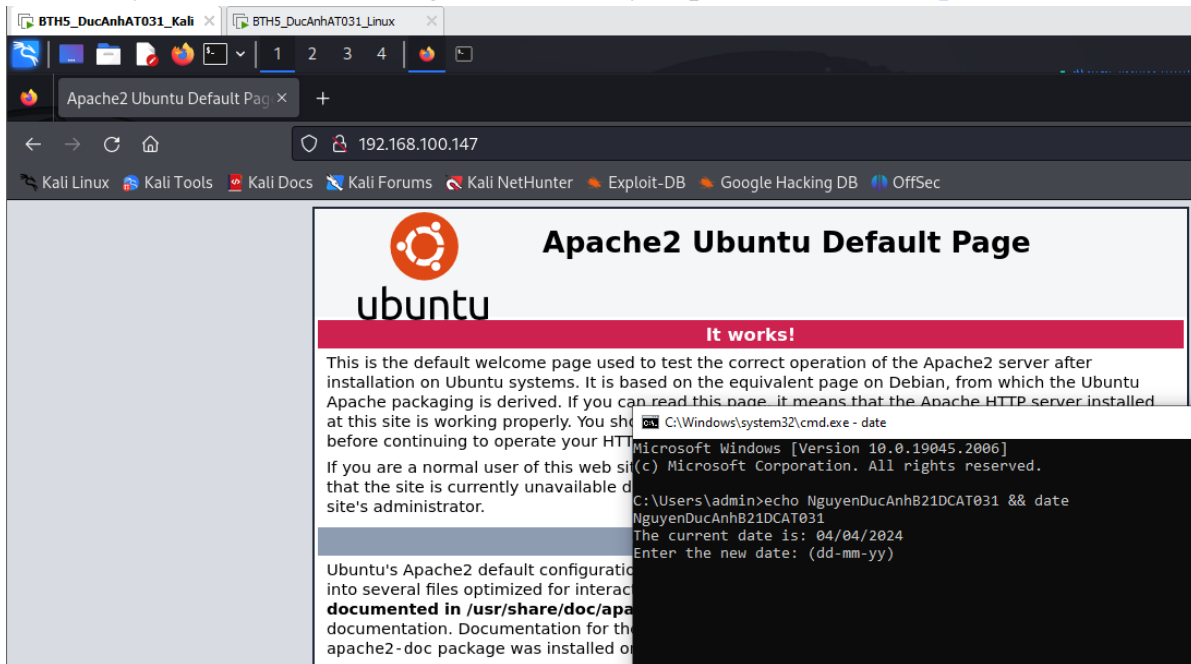


ip của 2 interfaces trên máy Kali

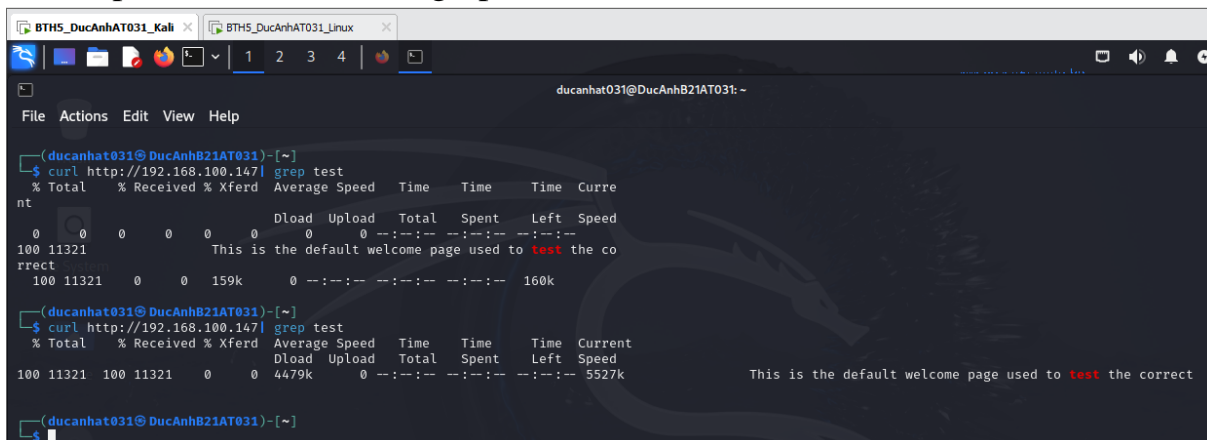
Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147 (Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.4.52



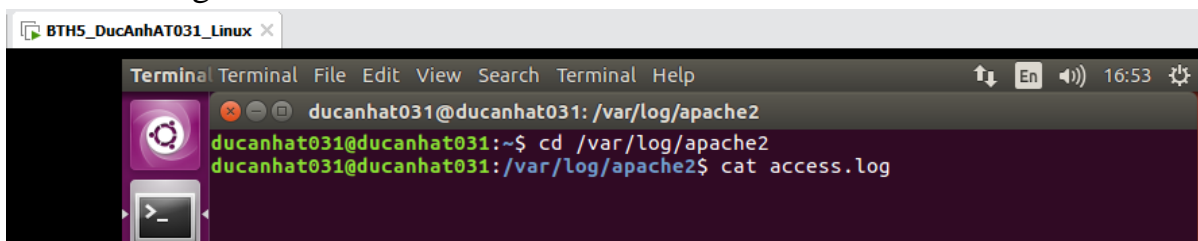
Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web <http://192.168.100.147>.



Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”:
`curl http://192.168.100.147 | grep test`



Trên máy Linux Internal Victim, để xem access_log dùng lệnh:
`cd /var/log/apache2`
`cat access.log`



```
BTH5_DucAnhAT031_Linux x
cAnhAT031_Kali Terminal Terminal File Edit View Search Terminal Help 16:58
ducanhat031@ducanhat031: /var/log/apache2
192.168.100.3 - - [04/Apr/2024:16:27:31 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
192.168.100.3 - - [04/Apr/2024:16:27:31 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
192.168.100.3 - - [04/Apr/2024:16:27:31 +0700] "GET / HTTP/1.0" 200 11595 "-" "-"
192.168.100.3 - - [04/Apr/2024:16:27:31 +0700] "GET / HTTP/1.1" 200 11576 "-" "-"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mo
zilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET /icons/ubuntu-logo.png HTTP/
1.1" 200 3623 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET /favicon.ico HTTP/1.1" 404 4
93 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20
100101 Firefox/115.0"
192.168.100.3 - - [04/Apr/2024:16:39:27 +0700] "GET / HTTP/1.1" 200 11576 "-" "c
url/8.5.0"
192.168.100.3 - - [04/Apr/2024:16:39:40 +0700] "GET / HTTP/1.1" 200 11576 "-" "c
url/8.5.0"
ducanhat031@ducanhat031: /var/log/apache2$
```

Khi đã mở được file access_log trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm ví dụ: Nmap, Firefox, curl, ...

- Firefox:

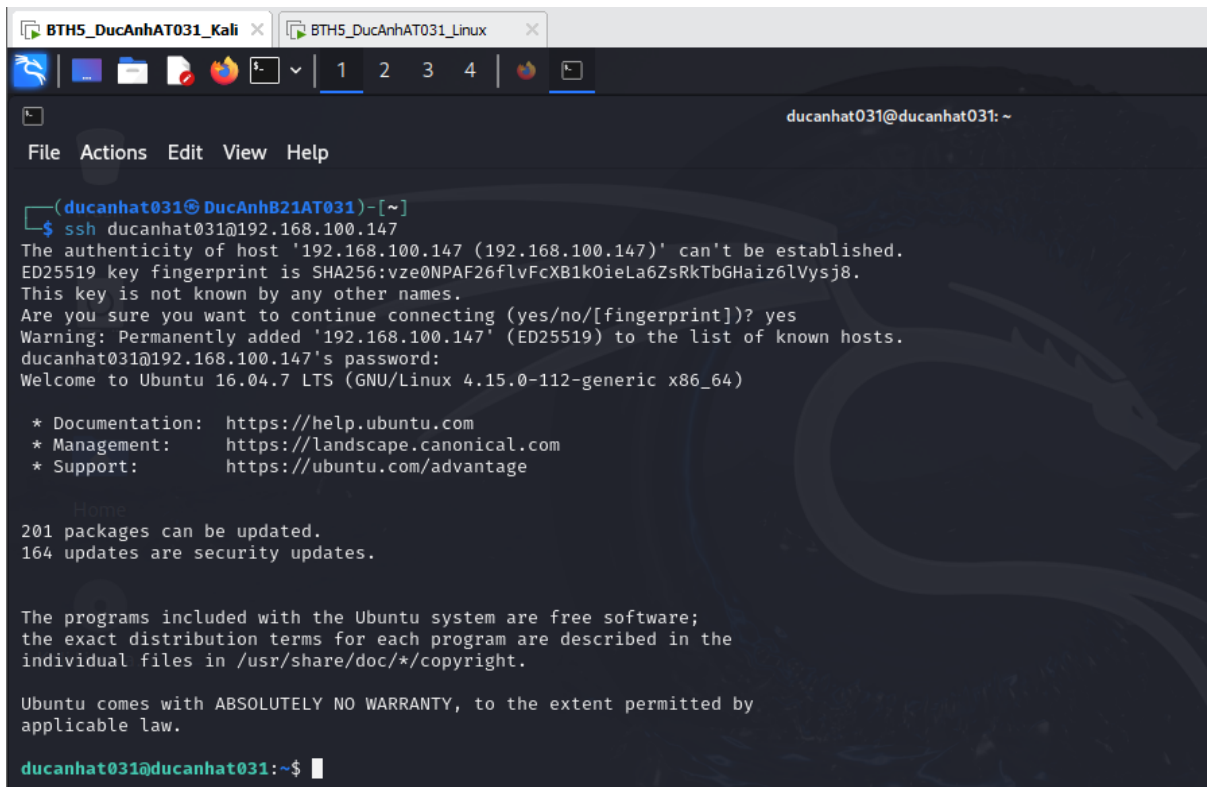
```
BTH5_DucAnhAT031_Linux x
DucAnhAT031_Kali Terminal Terminal File Edit View Search Terminal Help 16:59
ducanhat031@ducanhat031: /var/log/apache2
ducanhat031@ducanhat031: /var/log/apache2$ grep -i "Firefox" access.log
127.0.0.1 - - [04/Apr/2024:16:25:45 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mozill
a/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0"
127.0.0.1 - - [04/Apr/2024:16:25:52 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1"
200 3624 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0)
Gecko/20100101 Firefox/79.0"
127.0.0.1 - - [04/Apr/2024:16:26:00 +0700] "GET /favicon.ico HTTP/1.1" 404 488 "
-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mo
zilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET /icons/ubuntu-logo.png HTTP/
1.1" 200 3623 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [04/Apr/2024:16:37:26 +0700] "GET /favicon.ico HTTP/1.1" 404 4
93 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20
100101 Firefox/115.0"
ducanhat031@ducanhat031: /var/log/apache2$
```

- curl:

```
BTH5_DucAnhAT031_Linux x
Terminal Terminal File Edit View Search Terminal Help 17:00
ducanhat031@ducanhat031: /var/log/apache2
ducanhat031@ducanhat031: /var/log/apache2$ grep -i "curl" access.log
192.168.100.3 - - [04/Apr/2024:16:39:27 +0700] "GET / HTTP/1.1" 200 11576 "-" "c
url/8.5.0"
192.168.100.3 - - [04/Apr/2024:16:39:40 +0700] "GET / HTTP/1.1" 200 11576 "-" "c
url/8.5.0"
ducanhat031@ducanhat031: /var/log/apache2$
```

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.



```
BTH5_DucAnhAT031_Kali x BTH5_DucAnhAT031_Linux x
ducanhat031@ducanhat031: ~
File Actions Edit View Help
(ducanhat031@DucAnhB21AT031)-[~]
$ ssh ducanhat031@192.168.100.147
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
ED25519 key fingerprint is SHA256:vze0NPAF26flvFcXB1k0ieLa6ZsRkTbGHaiz6lVysj8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.147' (ED25519) to the list of known hosts.
ducanhat031@192.168.100.147's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

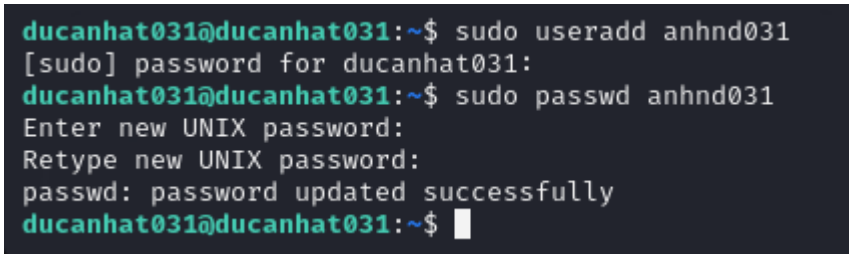
Home
201 packages can be updated.
164 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ducanhat031@ducanhat031: ~$
```

Remote sang máy linux thành công.



```
ducanhat031@ducanhat031:~$ sudo useradd anhnd031
[sudo] password for ducanhat031:
ducanhat031@ducanhat031:~$ sudo passwd anhnd031
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
ducanhat031@ducanhat031:~$
```

Tạo user mới thành công.

Trên máy Linux Internal Victim, tiến hành xem file auth.log

```
BTH5_DucAnhAT031_Linux x
Terminal
ducanhhat031@ducanhhat031: /var/log
Apr  4 17:04:22 ducanhhat031 sshd[4410]: pam_unix(sshd:session): session opened for user ducanhhat031 by (uid=0)
Apr  4 17:04:22 ducanhhat031 systemd-logind[784]: New session 2 of user ducanhhat031.
Apr  4 17:05:32 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/sbin/useradd anhnd031
Apr  4 17:05:32 ducanhhat031 sudo: pam_unix(sudo:session): session opened for user root by ducanhhat031(uid=0)
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new group: name=anhnd031, GID=1001
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new user: name=anhnd031, UID=1001, GID=1001, home=/home/anhnd031, shell=/bin/bash
Apr  4 17:05:32 ducanhhat031 sudo: pam_unix(sudo:session): session closed for user root
Apr  4 17:05:41 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/bin/passwd anhnd031
Apr  4 17:05:41 ducanhhat031 sudo: pam_unix(sudo:session): session opened for user root by ducanhhat031(uid=0)
Apr  4 17:05:54 ducanhhat031 passwd[4495]: pam_unix(passwd:chauthtok): password changed for anhnd031
Apr  4 17:05:54 ducanhhat031 passwd[4495]: gkr-pam: couldn't update the login keyring password: no old password was entered
Apr  4 17:05:54 ducanhhat031 sudo: pam_unix(sudo:session): session closed for user root
ducanhhat031@ducanhhat031: /var/log$
```

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

```
ducanhhat031@ducanhhat031: /var/log$ strings /var/log/auth.log | grep "anhnd031"
Apr  4 17:05:32 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/sbin/useradd anhnd031
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new group: name=anhnd031, GID=1001
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new user: name=anhnd031, UID=1001, GID=1001, home=/home/anhnd031, shell=/bin/bash
Apr  4 17:05:41 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/bin/passwd anhnd031
Apr  4 17:05:54 ducanhhat031 passwd[4495]: pam_unix(passwd:chauthtok): password changed for anhnd031
ducanhhat031@ducanhhat031: /var/log$
```

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

gawk '/anhnd031/' /var/log/auth.log

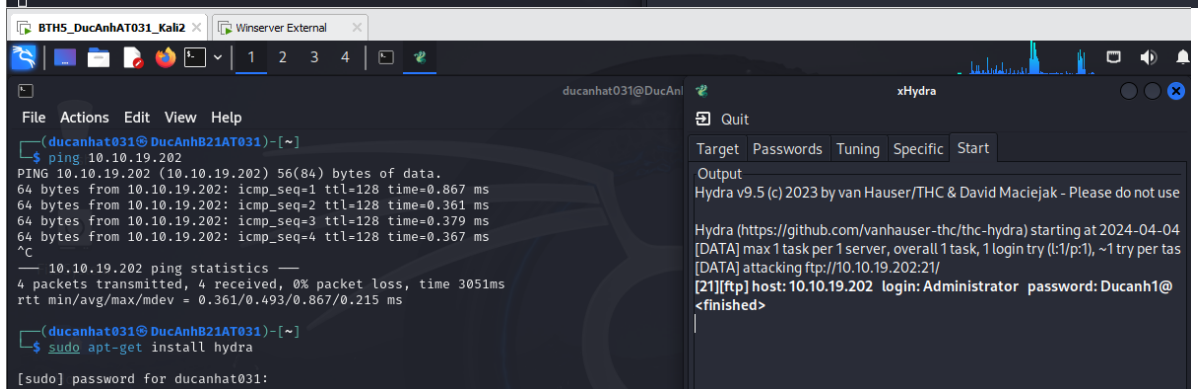
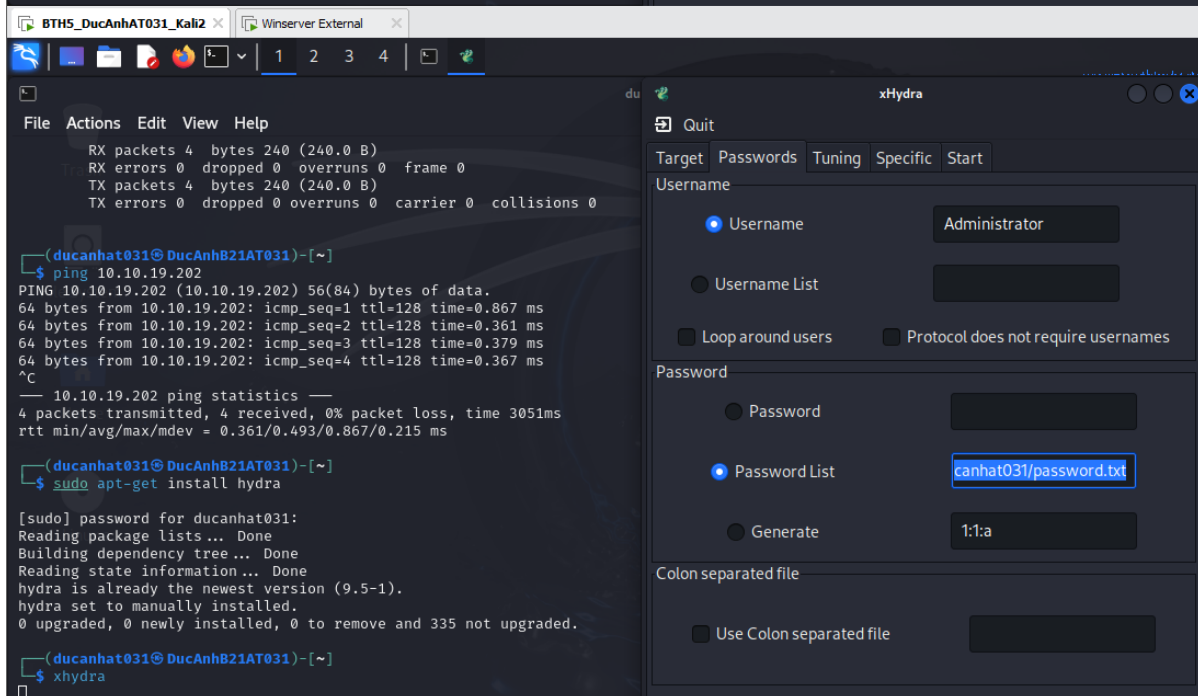
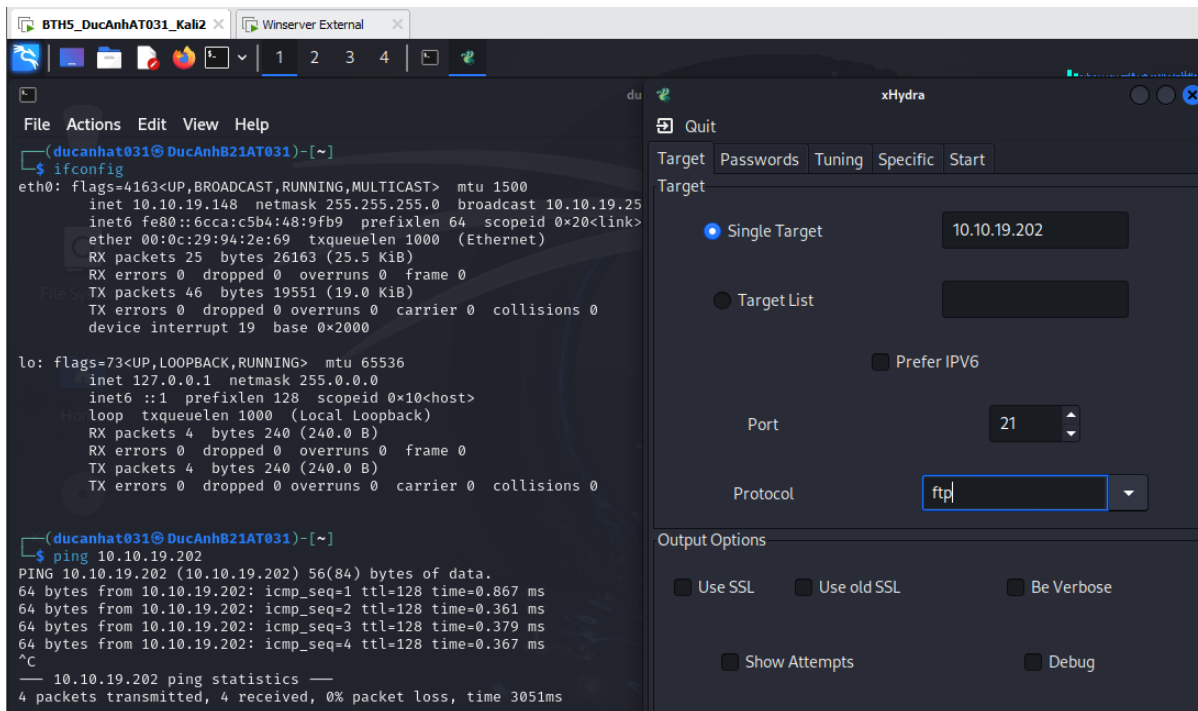
```
ducanhhat031@ducanhhat031: /var/log$ gawk '/anhnd031/' /var/log/auth.log
Apr  4 17:05:32 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/sbin/useradd anhnd031
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new group: name=anhnd031, GID=1001
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new user: name=anhnd031, UID=1001, GID=1001, home=/home/anhnd031, shell=/bin/bash
Apr  4 17:05:41 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/bin/passwd anhnd031
Apr  4 17:05:54 ducanhhat031 passwd[4495]: pam_unix(passwd:chauthtok): password changed for anhnd031
ducanhhat031@ducanhhat031: /var/log$
```

gawk '/useradd/' /var/log/auth.log

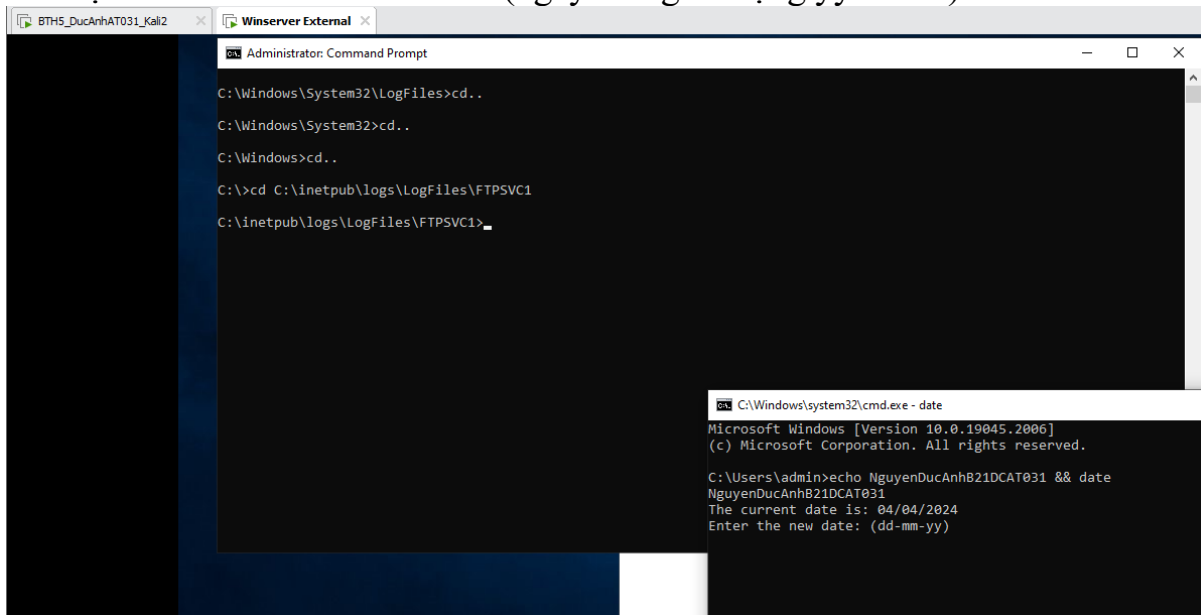
```
ducanhhat031@ducanhhat031: /var/log$ gawk '/useradd/' /var/log/auth.log
Apr  4 17:05:32 ducanhhat031 sudo: ducanhhat031 : TTY=pts/7 ; PWD=/home/ducanhhat031 ; USER=root ; COMMAND=/usr/sbin/useradd anhnd031
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new group: name=anhnd031, GID=1001
Apr  4 17:05:32 ducanhhat031 useradd[4484]: new user: name=anhnd031, UID=1001, GID=1001, home=/home/anhnd031, shell=/bin/bash
ducanhhat031@ducanhhat031: /var/log$
```

c. Phân tích log sử dụng find trong Linux

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 và chờ xHydra tìm ra mật khẩu



Trên máy Windows 2003 Server External Victim, thực hiện điều hướng đến FTP Logfile("cd C:\inetpub\logs\logfiles\FTPSVC1). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd).

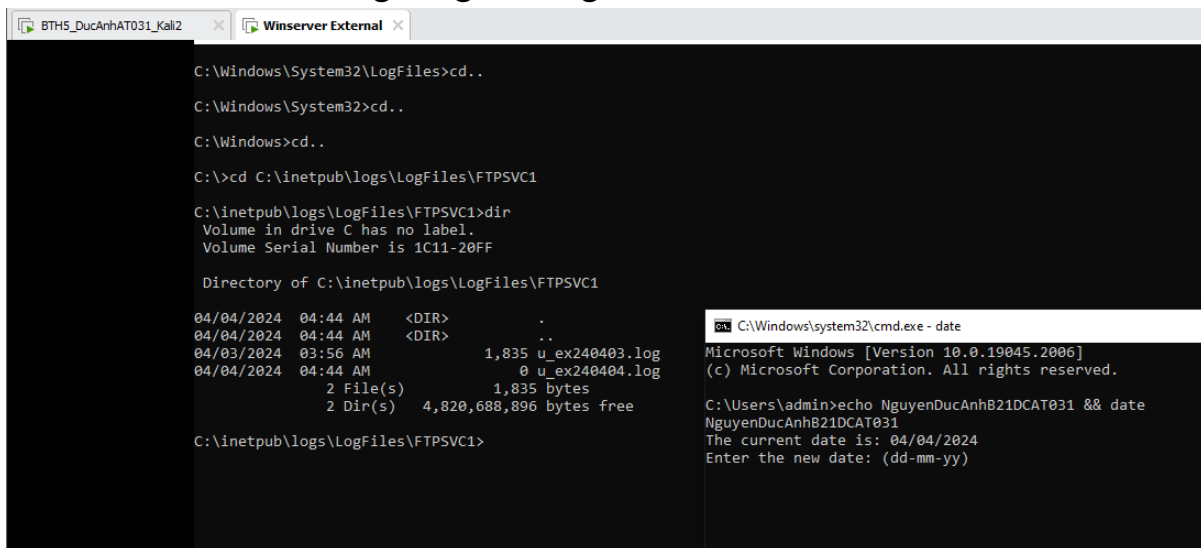


```
Administrator: Command Prompt
C:\Windows\System32\LogFiles>cd..
C:\Windows\System32>cd..
C:\Windows>cd..
C:\>cd C:\inetpub\logs\LogFiles\FTPSVC1
C:\inetpub\logs\LogFiles\FTPSVC1>

C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo NguyenDucAnhB21DCAT031 && date
NguyenDucAnhB21DCAT031
The current date is: 04/04/2024
Enter the new date: (dd-mm-yy)
```

Hiển thị tất cả các file log đang có bằng lệnh "dir"



```
Administrator: Command Prompt
C:\Windows\System32\LogFiles>cd..
C:\Windows\System32>cd..
C:\Windows>cd..
C:\>cd C:\inetpub\logs\LogFiles\FTPSVC1
C:\inetpub\logs\LogFiles\FTPSVC1>dir
Volume in drive C has no label.
Volume Serial Number is 1C11-20FF

Directory of C:\inetpub\logs\LogFiles\FTPSVC1

04/04/2024  04:44 AM    <DIR>          .
04/04/2024  04:44 AM    <DIR>          ..
04/03/2024  03:56 AM             1,835 u_ex240403.log
04/04/2024  04:44 AM              0 u_ex240404.log
               2 File(s)             1,835 bytes
               2 Dir(s)  4,820,688,896 bytes free

C:\inetpub\logs\LogFiles\FTPSVC1>

C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo NguyenDucAnhB21DCAT031 && date
NguyenDucAnhB21DCAT031
The current date is: 04/04/2024
Enter the new date: (dd-mm-yy)
```

Vì file mới nhất chưa có dữ liệu nên ta sẽ mở file còn lại bằng lệnh
“start u_ex240403.log”

The screenshot shows a Windows command prompt window with the following text:

```
C:\Windows\System32\LogFiles>cd..
C:\Windows\System32>cd..
C:\Windows>cd C:\inetpub
C:\inetpub>cd logs
C:\inetpub\logs>dir
Volume in drive C:
Volume Serial Number:
Directory of C:\inetpub\logs
04/04/2024 04:44 2024-04-03 10:48:41 10.10.19.11 - 10.10.19.202 21 ControlChannelOpened - - 0 0 12ac3880-3033-
04/04/2024 04:44 2024-04-03 10:48:49 10.10.19.11 - 10.10.19.202 21 USER Administrator 331 0 0 12ac3880-3033-
04/04/2024 04:44 2024-04-03 10:48:56 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
04/04/2024 04:44 2024-04-03 10:49:50 10.10.19.11 WIN-KLK0580U5V0 - date
04/04/2024 04:44 2024-04-03 10:50:00 10.10.19.11 WIN-KLK0580U5V0 - date
04/04/2024 04:44 2024-04-03 10:50:00 10.10.19.11 WIN-KLK0580U5V0 - date
04/04/2024 04:44 2024-04-03 10:51:45 10.10.19.11 - 10.10.19.202 21 PASS *** 230
04/04/2024 04:44 2024-04-03 10:51:50 10.10.19.11 - 10.10.19.202 21 PASS *** 230
04/04/2024 04:44 2024-04-03 10:51:54 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
04/04/2024 04:44 2024-04-03 10:52:09 10.10.19.11 WIN-KLK0580U5V0 - date
04/04/2024 04:44 2024-04-03 10:52:13 10.10.19.11 WIN-KLK0580U5V0 - date
04/04/2024 04:44 2024-04-03 10:52:13 10.10.19.11 WIN-KLK0580U5V0 - date
```

A Notepad window titled "u_ex240403 - Notepad" is open, showing the following text:

```
File Edit Format View Help
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-04-03 10:48:41
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem sc-status sc-win32-st
2024-04-03 10:48:41 10.10.19.11 - 10.10.19.202 21 ControlChannelOpened - - 0 0 12ac3880-3033-
2024-04-03 10:48:49 10.10.19.11 - 10.10.19.202 21 USER Administrator 331 0 0 12ac3880-3033-
2024-04-03 10:48:56 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
2024-04-03 10:49:50 10.10.19.11 WIN-KLK0580U5V0 - date
2024-04-03 10:50:00 10.10.19.11 WIN-KLK0580U5V0 - date
2024-04-03 10:50:00 10.10.19.11 WIN-KLK0580U5V0 - date
2024-04-03 10:51:45 10.10.19.11 - 10.10.19.202 21 PASS *** 230
2024-04-03 10:51:50 10.10.19.11 - 10.10.19.202 21 PASS *** 230
2024-04-03 10:51:54 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
2024-04-03 10:52:09 10.10.19.11 WIN-KLK0580U5V0 - date
2024-04-03 10:52:13 10.10.19.11 WIN-KLK0580U5V0 - date
2024-04-03 10:52:13 10.10.19.11 WIN-KLK0580U5V0 - date
```

Tìm kiếm kết quả tấn công login thành công bằng lệnh: **type u_ex240403.log | find "230"**

The screenshot shows a Windows command prompt window with the following text:

```
Directory of C:\inetpub\logs\LogFiles\FTPSVC1
04/04/2024 04:44 AM <DIR> .
04/04/2024 04:44 AM <DIR> ..
04/03/2024 03:56 AM 1,835 u_ex240403.log
04/04/2024 04:44 AM 0 u_ex240404.log
2 File(s) 1,835 bytes
2 Dir(s) 4,820,688,896 bytes free

C:\inetpub\logs\LogFiles\FTPSVC1>start u_ex240404.log
The process cannot access the file because it is being used by another process.

C:\inetpub\logs\LogFiles\FTPSVC1>start u_ex240403.log

C:\inetpub\logs\LogFiles\FTPSVC1>type u_ex240403.log | find "230"
2024-04-03 10:48:56 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
0 0 12ac3880-3033-4b67-8b90-e62d6bfff763f /
2024-04-03 10:51:54 10.10.19.11 WIN-KLK0580U5V0\Administrator 10.10.19.202 21 PASS *** 230
0 0 f65b881d-6d68-4f50-8565-3f0dae24535b /

C:\inetpub\logs\LogFiles\FTPSVC1>
```

A Notepad window titled "C:\Windows\system32\cmd.exe - date" is open, showing the following text:

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo NguyenDucAnhB21DCAT031 && date
NguyenDucAnhB21DCAT031
The current date is: 04/04/2024
Enter the new date: (dd-mm-yy)
```

3. Kết quả đạt được

- Sử dụng các lệnh grep, gwak và find để phân tích log hệ thống.