HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 9

MÔN THỰC TẬP CƠ SỞ

Phân tích log hệ thống

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Lớp: D20CQAT02-B

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Table of Contents

I.Mục đích 3
II. Nội dung thực hành 3
2.1 Tìm hiểu lý thuyết 3
2.2 Chuẩn bị môi trường 3
2.3 Các bước thực hiện 3
2.3.1 Phân tích log sử dụng grep trong Linux 3
2.3.2 Phân tích log sử dụng gawk trong Linux 6
2.3.3 Phân tích log sử dụng find trong Windows 8
III. Tài liệu tham khảo 11

I.Mục đích

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

1.1 Phân tích log sử dụng grep/gawk trong Linux

1.2 Phân tích log sử dụng find trong Windows

1.3 Tìm hiểu về Windows Event Viewer và auditing

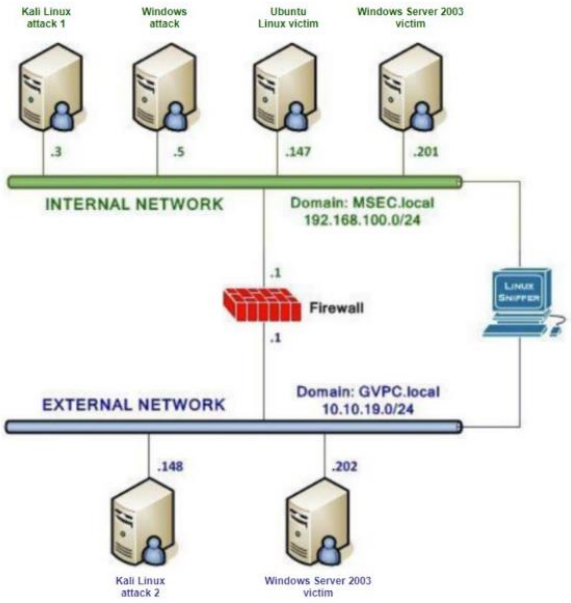
1.4 Phân tích event log trong Windows

II. Nội dung thực hành

2.1 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, …

2.2 Chuẩn bị môi trường



Phần mềm VMWare Workstation (hoặc các phần mềm hỗ trợ ảo hóa khác).

- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài 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.

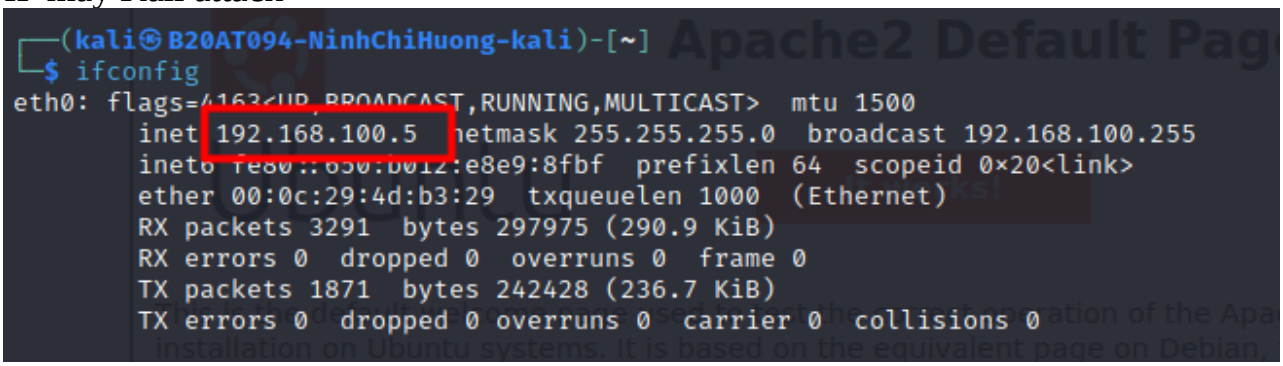
- Topo mạng như đã cấu hình trong bài 5.

2.3 Các bước thực hiện

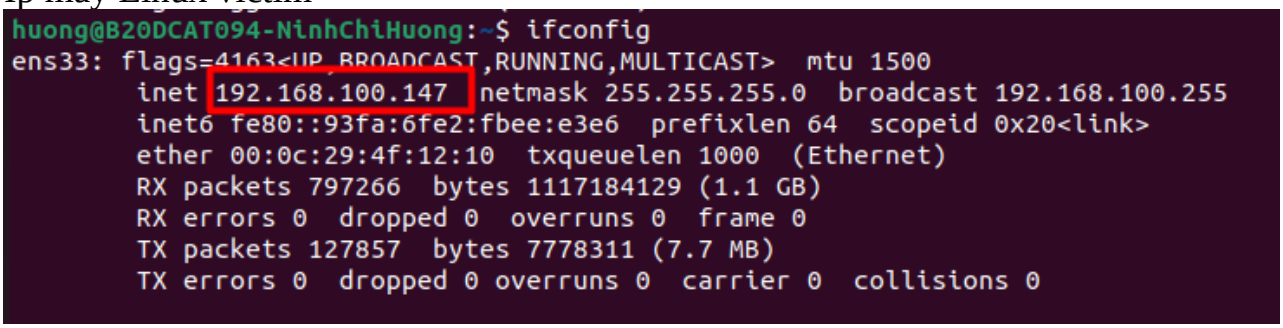
2.3.1 Phân tích log sử dụng grep trong Linux

Trên máy Kali attack trong mạng Internal, khởi chạy nmap và scan cho địa chỉ 192.168.100.138(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.2.3

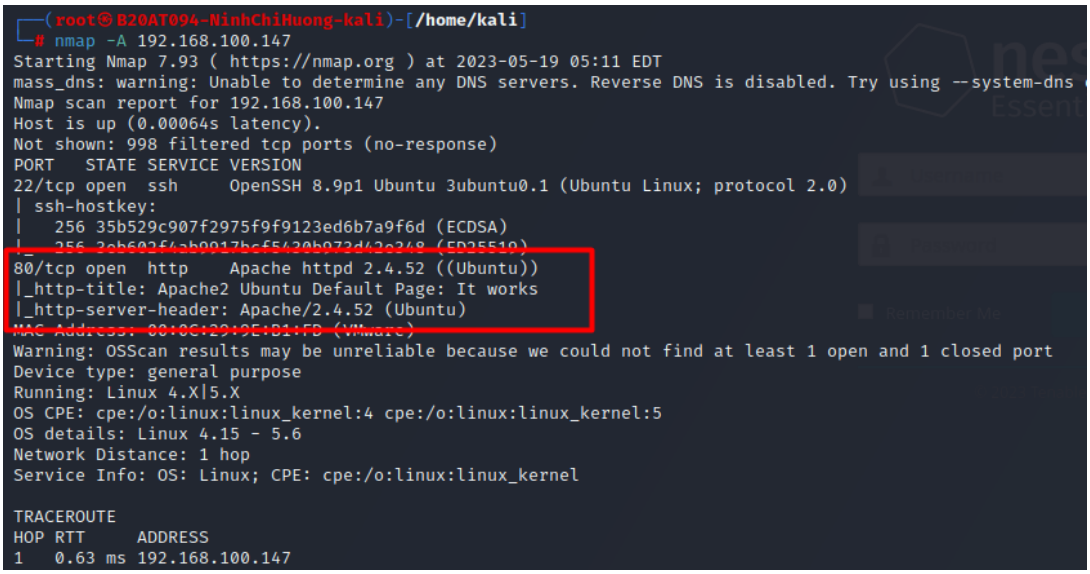
IP máy Kali attack



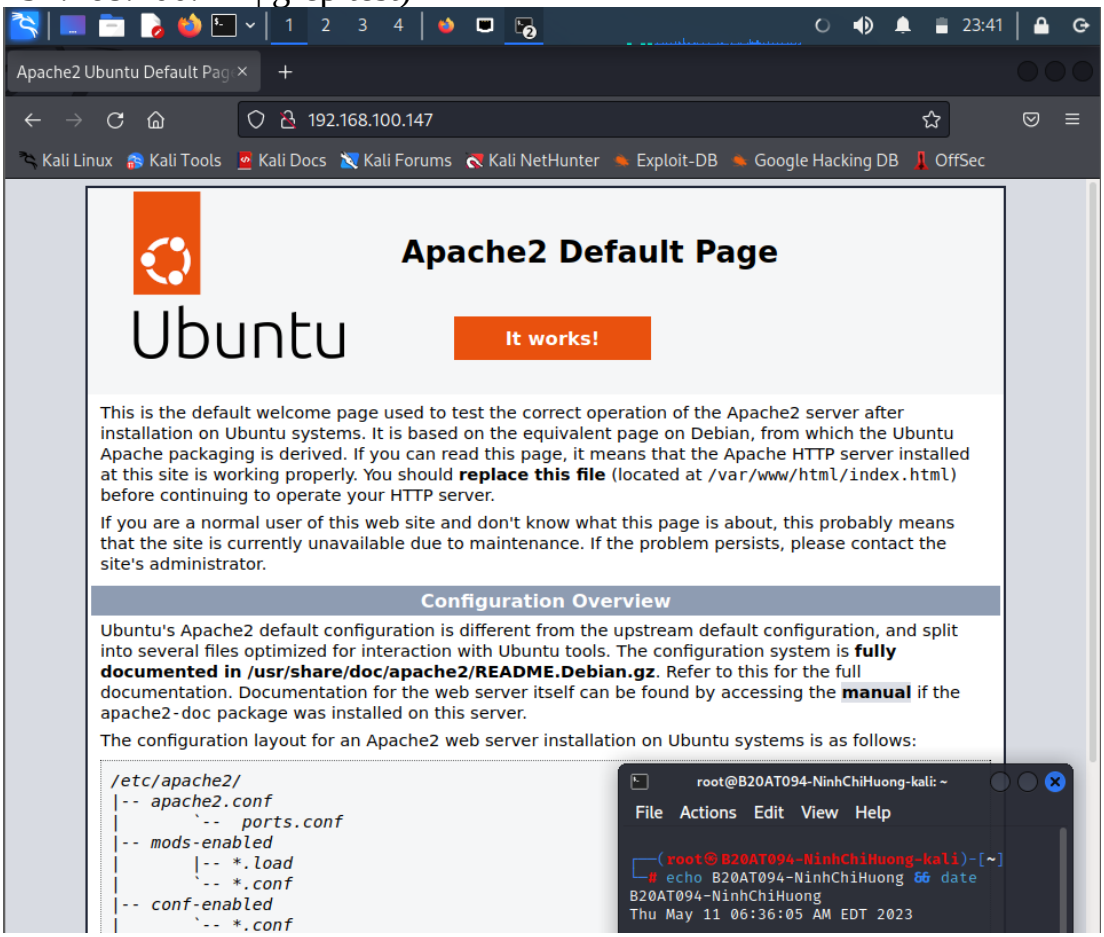
Ip máy Linux victim

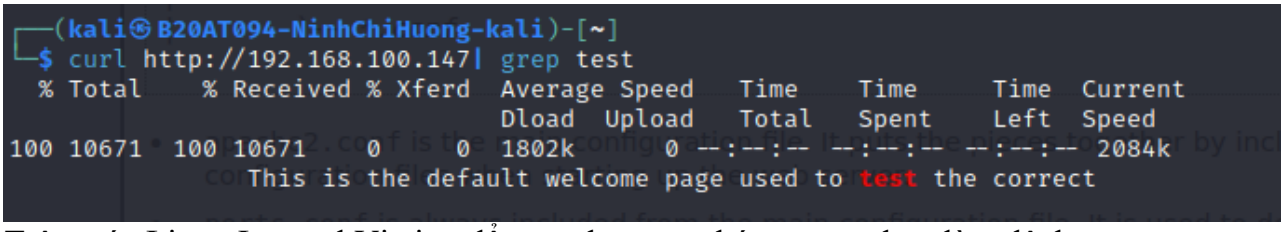


Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.4.52



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”(root@bt:~#curl http://192.168.100.147| grep test)





Trên máy Linux Internal Victim, để xem thư mục chứa access_log dùng lệnh:

[root@rhel ~]# cd /var/log/httpd

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

```
huong@B20DCAT094-NinhChiHuong:/var/log/apache2$ grep -i "firefox" access.log
192.168.100.147 - - [12/May/2023:10:33:46 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
192.168.100.147 - - [12/May/2023:10:33:46 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.100.147/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
192.168.100.147 - - [12/May/2023:10:33:46 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.147/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
192.168.100.5 - - [12/May/2023:10:33:54 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.100.5 - - [12/May/2023:10:33:55 +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"
192.168.100.5 - - [12/May/2023:10:33:55 +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"
```

Curl

```
huong@B20DCAT094-NinhChiHuong:/var/log/apache2$ grep -i "curl" access.log
192.168.100.5 - - [12/May/2023:10:46:34 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/7.82.0"
huong@B20DCAT094-NinhChiHuong:/var/log/apache2$
```

2.3.2 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.

Để cho phép remote, ta mở cổng ssh:

```
huong@B20DCAT094-NinhChiHuong:/$ sudo ufw status verbose
[sudo] password for huong:
Status: inactive
huong@B20DCAT094-NinhChiHuong:/$ sudo ufw enable
Firewall is active and enabled on system startup
huong@B20DCAT094-NinhChiHuong:/$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
huong@B20DCAT094-NinhChiHuong:/$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

```
┌──(kali㉿B20AT094-NinhChiHuong-kali)-[~]
└─$ nmap 192.168.100.147
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-12 00:38 EDT
Nmap scan report for 192.168.100.147
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
```

Tiến hành remote và Linux victim

```
┌──(kali㉿B20AT094-NinhChiHuong-kali)-[~]
└─$ sudo ssh huong@192.168.100.147
sudo: unable to resolve host B20AT094-NinhChiHuong-kali: Temporary failure in name resolution
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
ED25519 key fingerprint is SHA256:Q6Xu1CniOfs6VOI7ESpNPWHxTfQhRABXNTB7s2bQPRU.
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.
huong@192.168.100.147's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.19.0-41-generic x86_64)

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

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


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.

huong@B20DCAT094-NinhChiHuong:~$
```

Thêm user mới

```
huong@B20DCAT094-NinhChiHuong:~$ sudo useradd huongnc094
[sudo] password for huong:
huong@B20DCAT094-NinhChiHuong:~$ sudo passwd huongnc094
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
huong@B20DCAT094-NinhChiHuong:~$
```

Trên máy Linux Internal Victim, tiến hành xem file log

```
May 12 11:37:08 B20DCAT094-NinhChiHuong sshd[13074]: Server listening on 0.0.0.0 port 22.
May 12 11:37:08 B20DCAT094-NinhChiHuong sshd[13074]: Server listening on :: port 22.
May 12 11:37:39 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session closed for user root
May 12 11:37:54 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl ssh status
May 12 11:37:54 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 12 11:37:54 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session closed for user root
May 12 11:37:59 B20DCAT094-NinhChiHuong dbus-daemon[1499]: [session uid=1000 pid=1499] Failed to activate service 'org.freedesktop.Tracker3.Miner.Files': timed out (service_start_timeout=120000ms)
May 12 11:38:14 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/service ssh status
May 12 11:38:14 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 12 11:38:14 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session closed for user root
May 12 11:39:09 B20DCAT094-NinhChiHuong pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
May 12 11:39:09 B20DCAT094-NinhChiHuong pkexec[13761]: huong: Executing command [USER=root] [TTY=unknown] [CWD=/home/huong] [COMMAND=/usr/lib/update-notifier/package-system-locked]
May 12 11:39:59 B20DCAT094-NinhChiHuong dbus-daemon[1499]: [session uid=1000 pid=1499] Failed to activate service 'org.freedesktop.Tracker3.Miner.Files': timed out (service_start_timeout=120000ms)
May 12 11:40:23 B20DCAT094-NinhChiHuong sshd[13811]: Accepted password for huong from 192.168.100.5 port 59394 ssh2
May 12 11:40:23 B20DCAT094-NinhChiHuong sshd[13811]: pam_unix(sshd:session): session opened for user huong(uid=1000) by (uid=0)
May 12 11:40:23 B20DCAT094-NinhChiHuong systemd-logind[793]: New session 8 of user huong.
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/sbin/useradd huongnc094
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session opened for user root(uid=0) by huong(uid=1000)
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new group: name=huongnc094, GID=1001
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new user: name=huongnc094, UID=1001, GID=1001, home=/home/huongnc094, shell=/bin/sh, from=/dev/pts/4
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session closed for user root
May 12 11:41:17 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/bin/passwd huongnc094
May 12 11:41:17 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session opened for user root(uid=0) by huong(uid=1000)
May 12 11:41:26 B20DCAT094-NinhChiHuong passwd[13950]: pam_unix(passwd:chauthtok): password changed for huongnc094
May 12 11:41:26 B20DCAT094-NinhChiHuong passwd[13950]: gkr-pam: couldn't update the login keyring password: no old password was entered
May 12 11:41:26 B20DCAT094-NinhChiHuong sudo: pam_unix(sudo:session): session closed for user root
May 12 11:42:00 B20DCAT094-NinhChiHuong dbus-daemon[1499]: [session uid=1000 pid=1499] Failed to activate service 'org.freedesktop.Tracker3.Miner.Files': timed out (service_start_timeout=120000ms)
huong@B20DCAT094-NinhChiHuong:/var/log$
```

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

```
huong@B20DCAT094-NinhChiHuong:/var/log$ strings /var/log/auth.log | grep "huongnc094"
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/sbin
/useradd huongnc094
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new group: name=huongnc094, GID=1001
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new user: name=huongnc094, UID=1001, GID=1001, home=/home/hu
ongnc094, shell=/bin/sh, from=/dev/pts/4
May 12 11:41:17 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/bin/
passwd huongnc094
May 12 11:41:26 B20DCAT094-NinhChiHuong passwd[13950]: pam_unix(passwd:chauthtok): password changed for huongnc094
May 12 12:02:36 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/bin/
grep huongnc094 /var/log/auth.log
May 12 12:03:18 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/gre
p huongnc094 auth.log
May 12 12:05:07 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/gre
p huongnc094 auth.log
May 12 12:07:53 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/grep huong
nc094 /var/log/auth.log
huong@B20DCAT094-NinhChiHuong:/var/log$
```

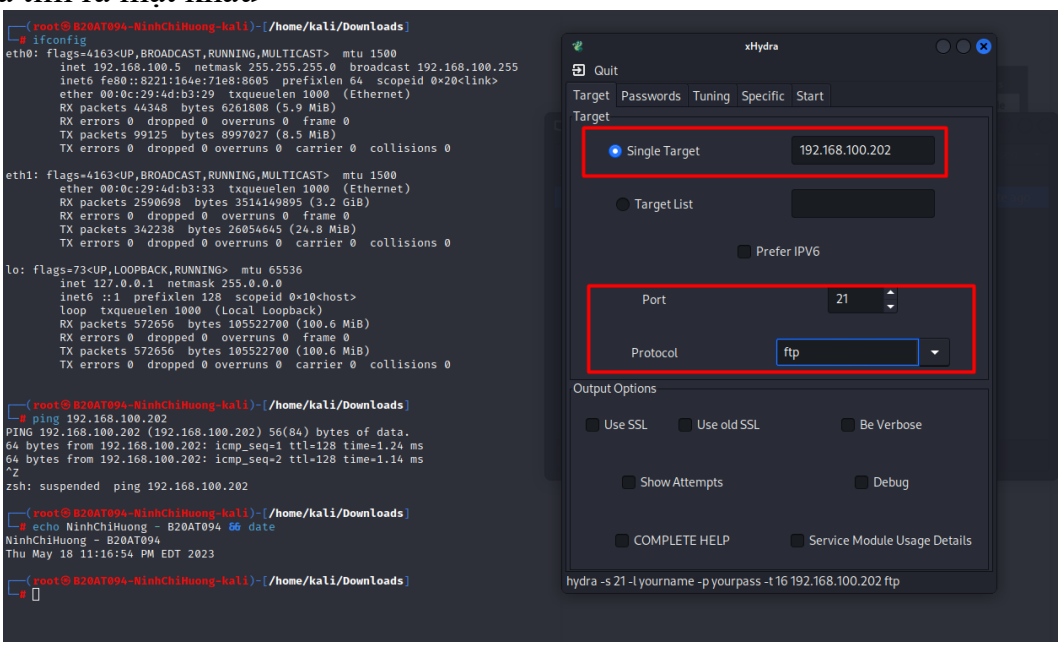
và dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được.

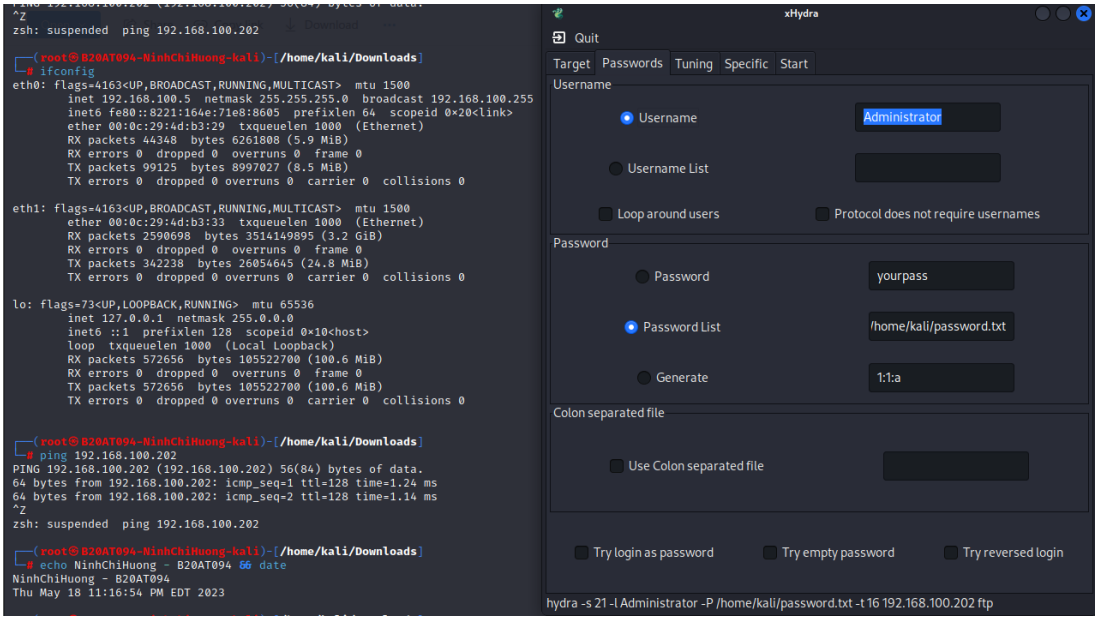
```
huong@B20DCAT094-NinhChiHuong:~$ gawk '/useradd/ { print }' /var/log/auth.log
May 12 11:37:05 B20DCAT094-NinhChiHuong useradd[12941]: new user: name=sshd, UID=128, GID=65534, home=/run/sshd, she
ll=/usr/sbin/nologin, from=none
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/sbin
/useradd huongnc094
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new group: name=huongnc094, GID=1001
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new user: name=huongnc094, UID=1001, GID=1001, home=/home/hu
ongnc094, shell=/bin/sh, from=/dev/pts/4
huong@B20DCAT094-NinhChiHuong:~$
```

```
huong@B20DCAT094-NinhChiHuong:~$ gawk '/useradd/ { print }' /var/log/auth.log
May 12 11:37:05 B20DCAT094-NinhChiHuong useradd[12941]: new user: name=sshd, UID=128, GID=65534, home=/run/sshd, she
ll=/usr/sbin/nologin, from=none
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/sbin
/useradd huongnc094
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new group: name=huongnc094, GID=1001
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new user: name=huongnc094, UID=1001, GID=1001, home=/home/hu
ongnc094, shell=/bin/sh, from=/dev/pts/4
huong@B20DCAT094-NinhChiHuong:~$ gawk '/huongnc094/ { print }' /var/log/auth.log
May 12 11:41:03 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/sbin/useradd huongnc094
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new group: name=huongnc094, GID=1001
May 12 11:41:03 B20DCAT094-NinhChiHuong useradd[13938]: new user: name=huongnc094, UID=1001, GID=1001, home=/home/huongnc094, shell=/bin/sh, from=/dev/pts/4
May 12 11:41:17 B20DCAT094-NinhChiHuong sudo:    huong : TTY=pts/3 ; PWD=/home/huong ; USER=root ; COMMAND=/usr/bin/passwd huongnc094
May 12 11:41:26 B20DCAT094-NinhChiHuong passwd[13950]: pam_unix(passwd:chauthtok): password changed for huongnc094
```

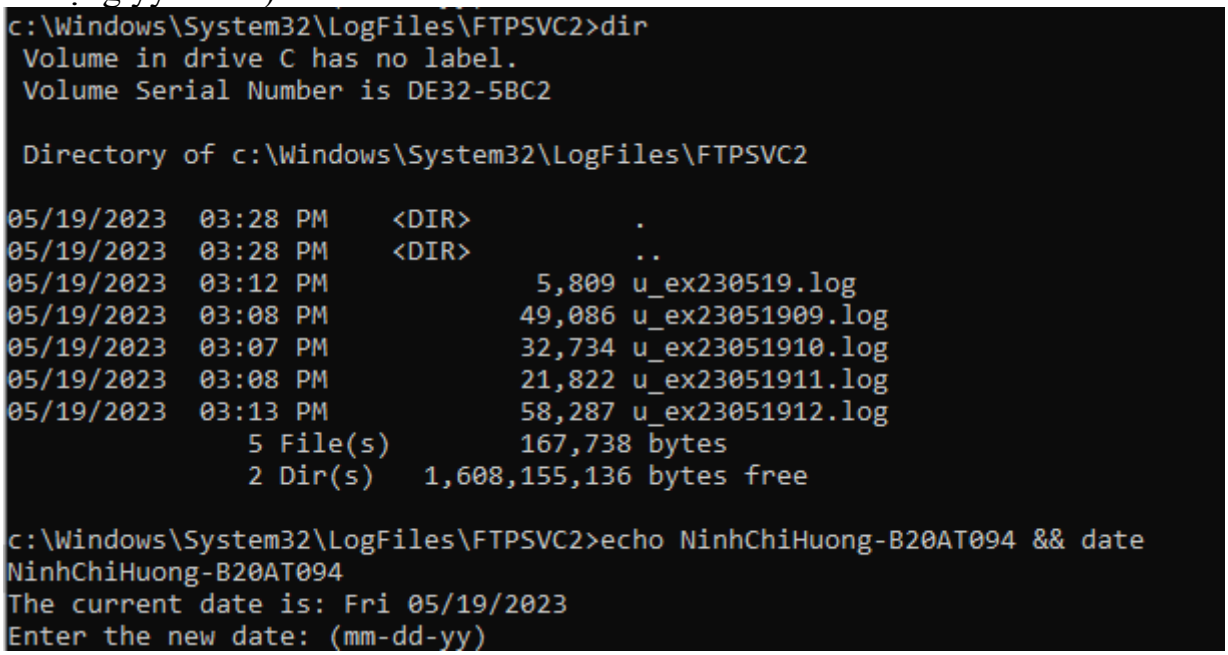
2.3.3 Phân tích log sử dụng find trong Windows

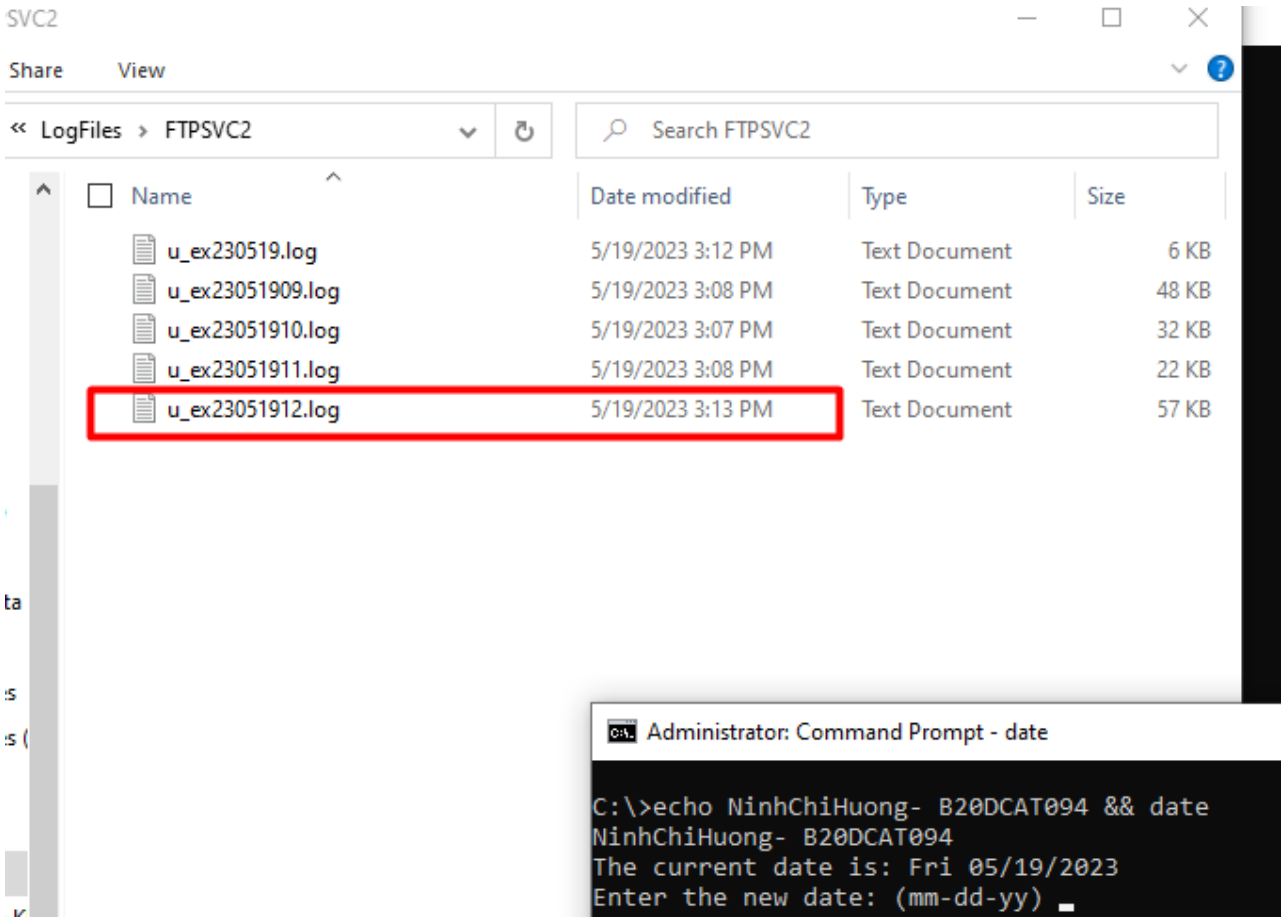
Trên máy Kali External Attack khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu

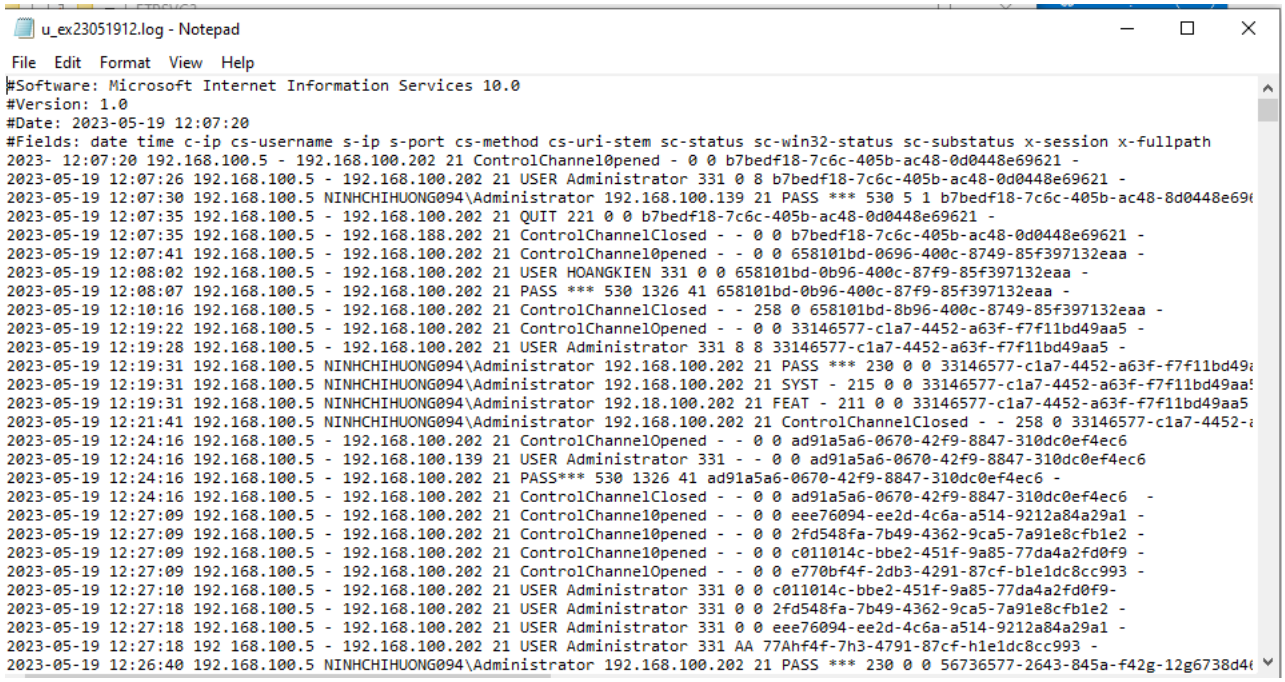




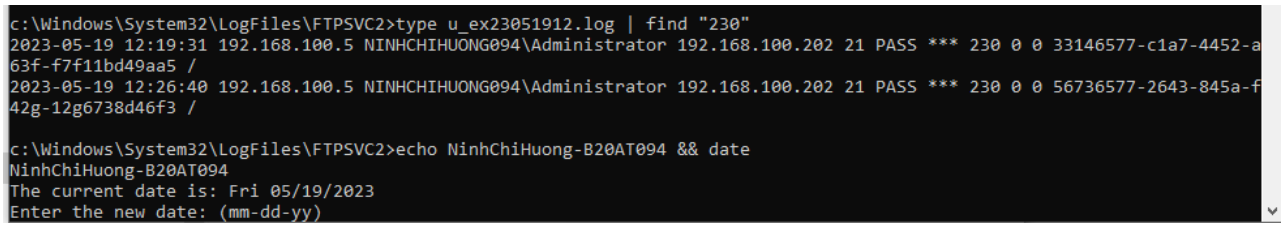
Trên máy Windows 2003 Server External Victim, thực hiện điều hướng đến FTP Logfile(C:\cd c:\Windows\System32\Logfiles\msftpsvc1). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd).




SVC2
Share
View
LogFiles › FTPSVC2
Search FTPSVC2
Name
Date modified
Type
Size
u_ex230519.log 5/19/2023 3:12 PM Text Document 6 KB
u_ex23051909.log 5/19/2023 3:08 PM Text Document 48 KB
u_ex23051910.log 5/19/2023 3:07 PM Text Document 32 KB
u_ex23051911.log 5/19/2023 3:08 PM Text Document 22 KB
u_ex23051912.log 5/19/2023 3:13 PM Text Document 57 KB
Administrator: Command Prompt - date
C:\>echo NinhChiHuong- B20DCAT094 && date
NinhChiHuong- B20DCAT094
The current date is: Fri 05/19/2023
Enter the new date: (mm-dd-yy)


u_ex23051912.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2023-05-19 12:07:20
#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
2023- 12:07:20 192.168.100.5 - 192.168.100.202 21 ControlChannel0pened - 0 0 b7bedf18-7c6c-405b-ac48-0d0448e69621 -
2023-05-19 12:07:26 192.168.100.5 - 192.168.100.202 21 USER Administrator 331 0 8 b7bedf18-7c6c-405b-ac48-0d0448e69621 -
2023-05-19 12:07:30 192.168.100.5 NINHCHIHUONG094\Administrator 192.168.100.139 21 PASS *** 530 5 1 b7bedf18-7c6c-405b-ac48-8d0448e69
2023-05-19 12:07:35 192.168.100.5 - 192.168.100.202 21 QUIT 221 0 0 b7bedf18-7c6c-405b-ac48-0d0448e69621 -
2023-05-19 12:07:35 192.168.100.5 - 192.168.188.202 21 ControlChannelClosed - - 0 0 b7bedf18-7c6c-405b-ac48-0d0448e69621 -
2023-05-19 12:07:41 192.168.100.5 - 192.168.100.202 21 ControlChannel0pened - - 0 0 658101bd-0696-400c-8749-85f397132eaa -
2023-05-19 12:08:02 192.168.100.5 - 192.168.100.202 21 USER HOANGKIEN 331 0 0 658101bd-0b96-400c-87f9-85f397132eaa -
2023-05-19 12:08:07 192.168.100.5 - 192.168.100.202 21 PASS *** 530 1326 41 658101bd-0b96-400c-87f9-85f397132eaa -
2023-05-19 12:10:16 192.168.100.5 - 192.168.100.202 21 ControlChannelClosed - - 258 0 658101bd-8b96-400c-8749-85f397132eaa -
2023-05-19 12:19:22 192.168.100.5 - 192.168.100.202 21 ControlChannelOpened - - 0 0 33146577-c1a7-4452-a63f-f7f11bd49aa5 -
2023-05-19 12:19:28 192.168.100.5 - 192.168.100.202 21 USER Administrator 331 8 8 33146577-c1a7-4452-a63f-f7f11bd49aa5 -
2023-05-19 12:19:31 192.168.100.5 NINHCHIHUONG094\Administrator 192.168.100.202 21 PASS *** 230 0 0 33146577-c1a7-4452-a63f-f7f11bd49
2023-05-19 12:19:31 192.168.100.5 NINHCHIHUONG094\Administrator 192.18.100.202 21 SYST - 215 0 0 33146577-c1a7-4452-a63f-f7f11bd49aa
2023-05-19 12:19:31 192.168.100.5 NINHCHIHUONG094\Administrator 192.18.100.202 21 FEAT - 211 0 0 33146577-c1a7-4452-a63f-f7f11bd49aa5
2023-05-19 12:21:41 192.168.100.5 NINHCHIHUONG094\Administrator 192.168.100.202 21 ControlChannelClosed - - 258 0 33146577-c1a7-4452-
2023-05-19 12:24:16 192.168.100.5 - 192.168.100.202 21 ControlChannelOpened - - 0 0 ad91a5a6-0670-42f9-8847-310dc0ef4ec6
2023-05-19 12:24:16 192.168.100.5 - 192.168.100.139 21 USER Administrator 331 - - 0 0 ad91a5a6-0670-42f9-8847-310dc0ef4ec6
2023-05-19 12:24:16 192.168.100.5 - 192.168.100.202 21 PASS*** 530 1326 41 ad91a5a6-0670-42f9-8847-310dc0ef4ec6 -
2023-05-19 12:24:16 192.168.100.5 - 192.168.100.202 21 ControlChannelClosed - - 0 0 ad91a5a6-0670-42f9-8847-310dc0ef4ec6 -
2023-05-19 12:27:09 192.168.100.5 - 192.168.100.202 21 ControlChanne10pened - - 0 0 eee76094-ee2d-4c6a-a514-9212a84a29a1 -
2023-05-19 12:27:09 192.168.100.5 - 192.168.100.202 21 ControlChanne10pened - - 0 0 2fd548fa-7b49-4362-9ca5-7a91e8cfb1e2 -
2023-05-19 12:27:09 192.168.100.5 - 192.168.100.202 21 ControlChanne10pened - - 0 0 c011014c-bbe2-451f-9a85-77da4a2fd0f9 -
2023-05-19 12:27:09 192.168.100.5 - 192.168.100.202 21 ControlChannelOpened - - 0 0 e770bf4f-2db3-4291-87cf-b1e1dc8cc993 -
2023-05-19 12:27:10 192.168.100.5 - 192.168.100.202 21 USER Administrator 331 0 0 c011014c-bbe2-451f-9a85-77da4a2fd0f9-
2023-05-19 12:27:18 192.168.100.5 - 192.168.100.202 21 USER Administrator 331 0 0 2fd548fa-7b49-4362-9ca5-7a91e8cfb1e2 -
2023-05-19 12:27:18 192.168.100.5 - 192.168.100.202 21 USER Administrator 331 0 0 eee76094-ee2d-4c6a-a514-9212a84a29a1 -
2023-05-19 12:27:18 192 168.100.5 - 192.168.100.202 21 USER Administrator 331 AA 77Ahf4f-7h3-4791-87cf-h1e1dc8cc993 -
2023-05-19 12:26:40 192.168.100.5 NINHCHIHUONG094\Administrator 192.168.100.202 21 PASS *** 230 0 0 56736577-2643-845a-f42g-12g6738d4

Gõ lệnh để tìm kiếm kết quả tấn công login thành công (C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type exyymmdd.log | find “230”)



III. Tài liệu tham khảo

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