HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 9

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 3/2022

Bài 9: Phân tích log hệ thống

I. Giới thiệu chung

1. Mục đích

- 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. Yêu cầu

- Tìm hiểu lý thuyết
  - Grep: là command hiển thị line chứa chuỗi kí tự trong file .Có thể chỉ định nhiều file hoặc nhiều đường dẫn của đối tượng search . Có thể thay file hoặc đường dẫn bằng kết quả output từ command khác
  - Awk: là một ngôn ngữ lập trình hỗ trợ thao tác dễ dàng đối với kiểu dữ liệu có cấu trúc, thường được sử dụng cho việc tìm kiếm và xử lý text. Gawk là bản phát hành mới nhất của GNU awk
  - Find được sử dụng để tìm kiếm một chuỗi văn bản trong một tệp hoặc các tệp và hiển thị các dòng văn bản chứa chuỗi đã chỉ định trong cmd Windows
  - Access_log:
    - Có chức năng ghi lại những lần sử dụng, truy cập, yên cầu đến apache server;
    - Được lưu trữ tại /var/log/httpd/access_log (hoặc /var/log/apache2/access.log)
  - xHydra:
    - xHydra là giao diện người dùng GUI cho trình bẻ khóa mật khẩu Hydra.
    - Hydra có thể được sử dụng để bẻ khóa mật khẩu, có thể được sử dụng cho nhiều loại tấn công trực tuyến, bao gồm cả các cuộc tấn công MySQL, SMB, FTP, MSSQL và HTTP / HTTPS.

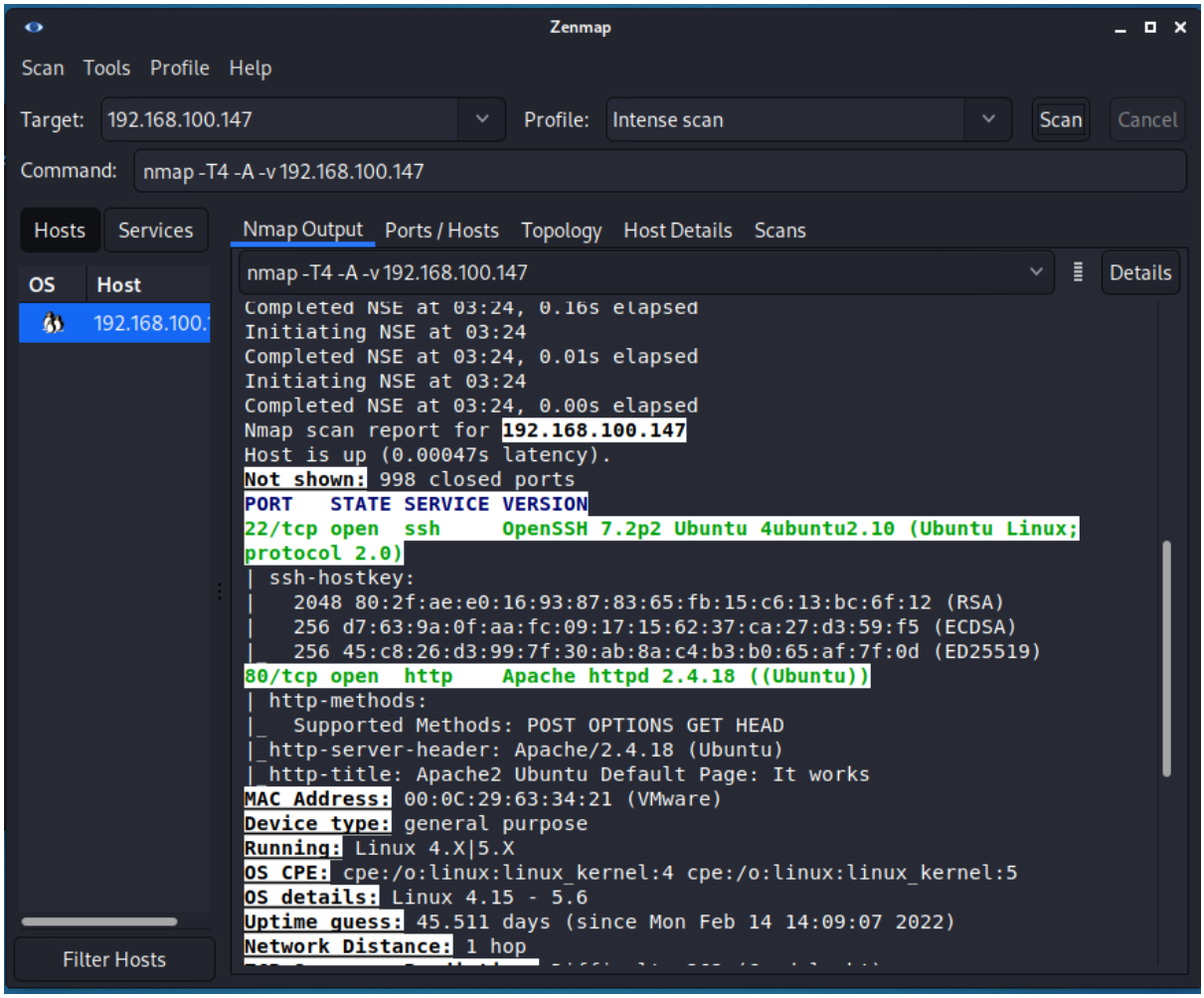
- Chuẩn bị
  - Phần mềm VMWare Workstation
  - File máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 5
  - Topo mạng như đã cấu hình trong bài 5

3. Các bước thực hiện

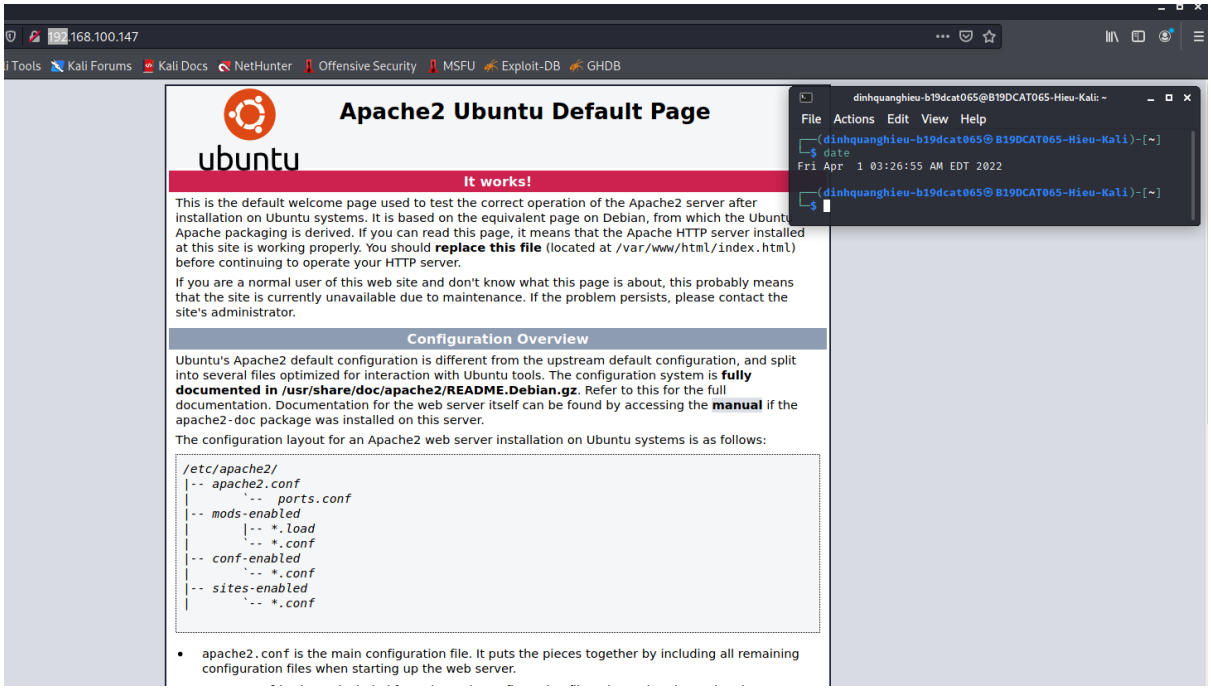
+ Phân tích log sử dụng grep trong Linux

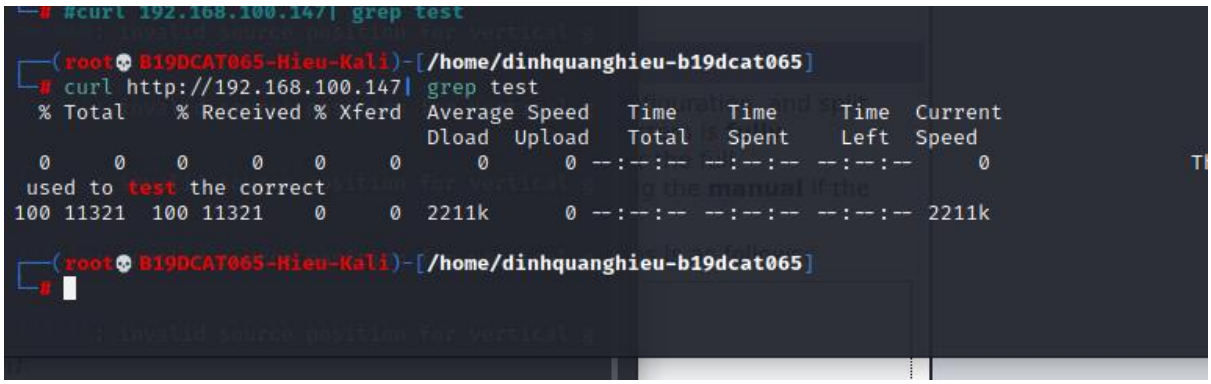
a) Các bước thực hiện

- 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 2.2.3

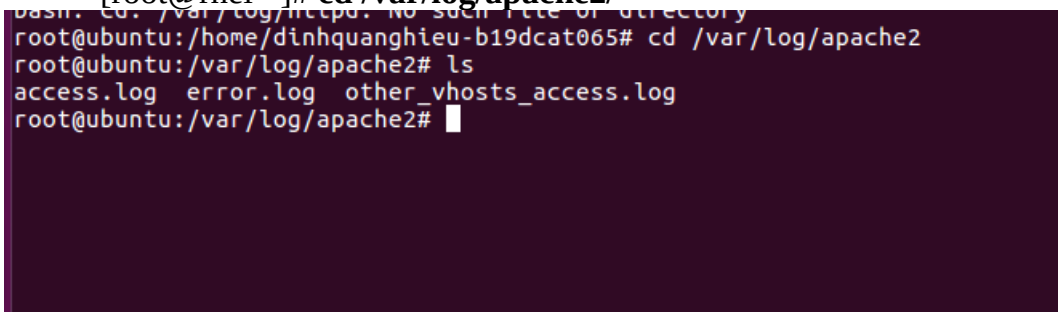


- Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web http://192.168.100.147. Trên terminal tiến hành sao chép website và tìm kiếm từ khóa "test"(root@bt:~#**curl http://192.168.100.147| grep test)**





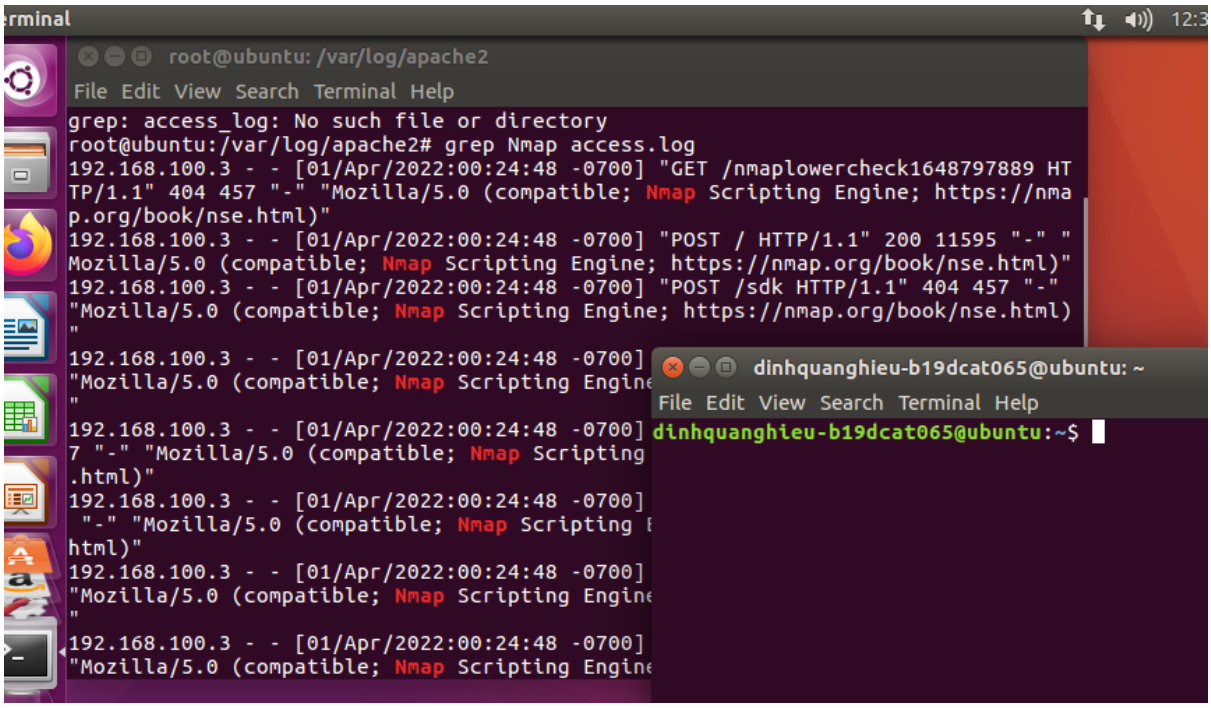
- Trên máy Linux Internal Victim, để xem thư mục chứa ***access_log*** dùng lệnh: [root@rhel ~]# **cd /var/log/apache2/**



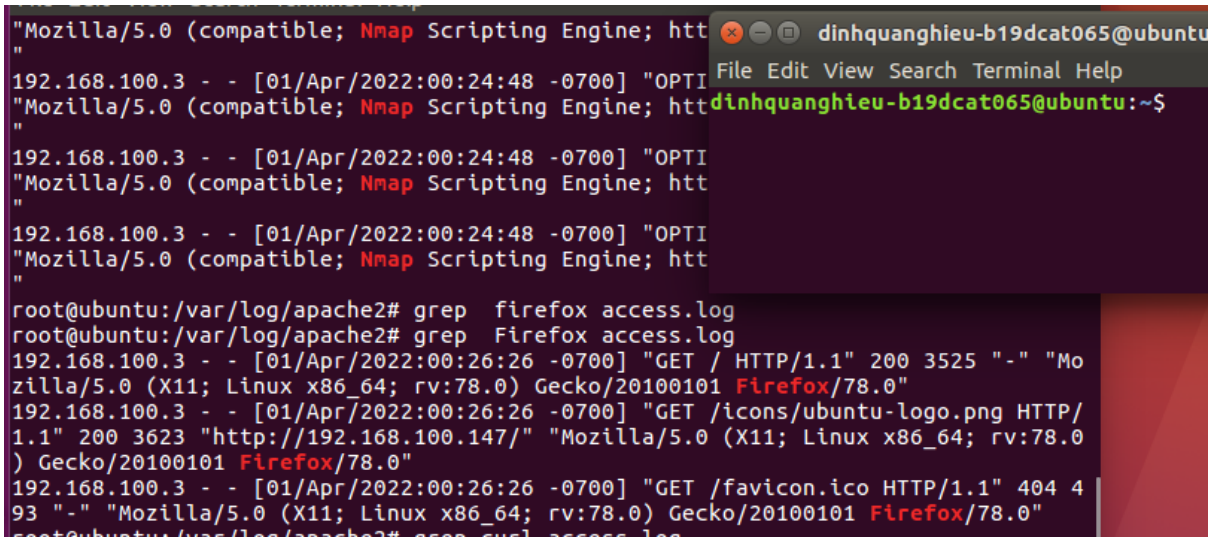
b)Kết quả cần đạt được

- 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, …

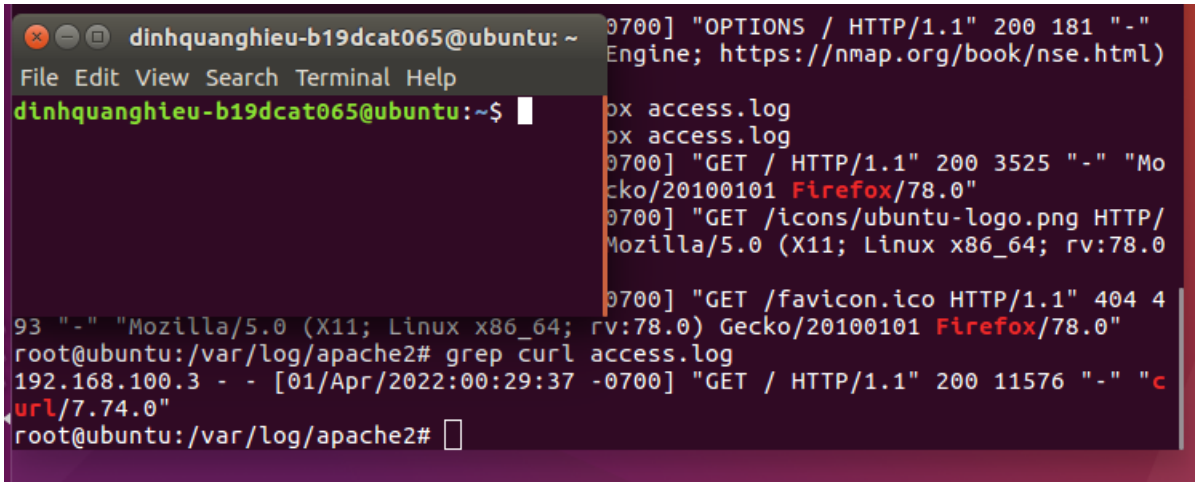
-Grep Nmap access.log



-Grep Firefox access.log



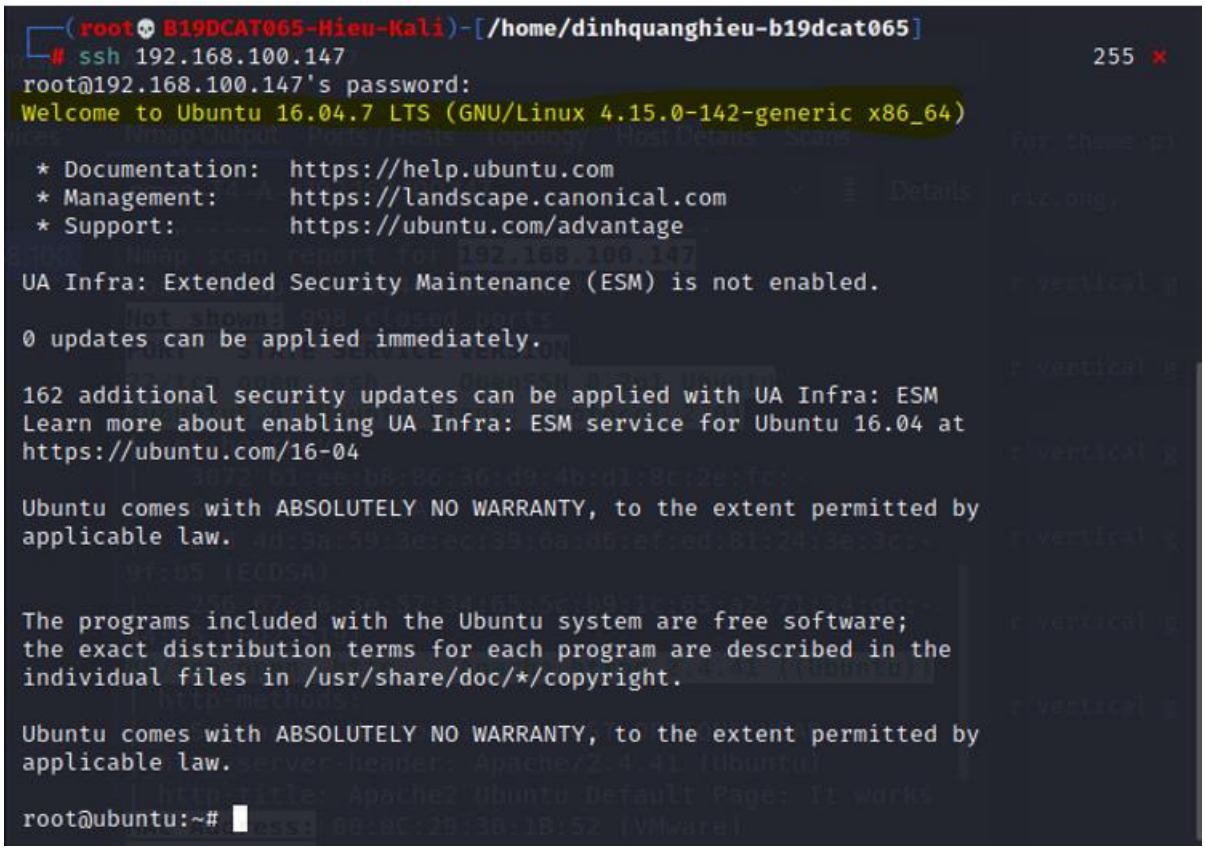
- Grep curl access.log



+ Phân tích log sử dụng gawk trong Linux

a) Các bước thực hiện

- 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.

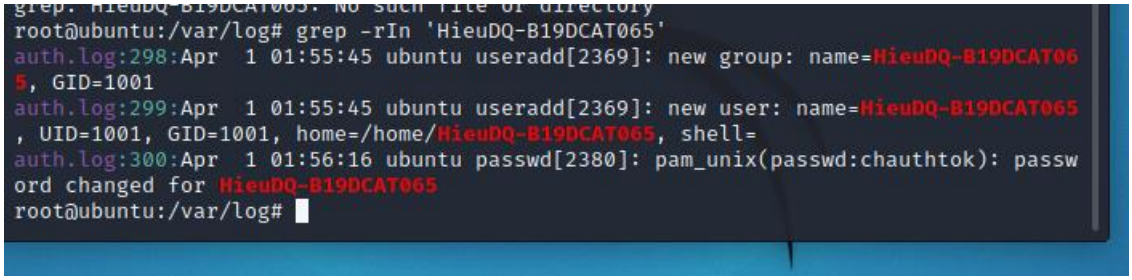


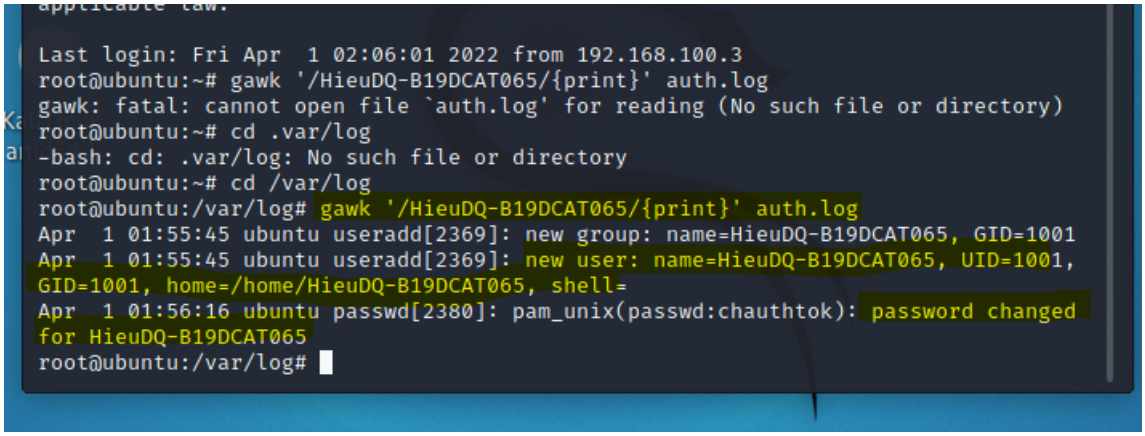
```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ubuntu:~# ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:63:34:21
          inet addr:192.168.100.147  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::b659:2eb5:f31a:4705/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20225 (20.2 KB)  TX bytes:13933 (13.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3732 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3732 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:279408 (279.4 KB)  TX bytes:279408 (279.4 KB)

root@ubuntu:~# useradd HieuDQ-B19DCAT065
root@ubuntu:~# passewd HieuDQ-B19DCAT065
No command 'passewd' found, did you mean:
 Command 'passwd' from package 'passwd' (main)
passewd: command not found
root@ubuntu:~# passwd HieuDQ-B19DCAT065
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:~#
```

- Trên máy Linux Internal Victim, tiến hành xem file log
  gedit /var/log/auth.log

```
Open   Save
Apr  1 01:48:13 ubuntu sudo: dinhquanghieu-b19dcat065 :
b19dcat065 ; USER=root ; COMMAND=/bin/nano /etc/ssh/ssh
Apr  1 01:48:13 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:48:20 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:48:33 ubuntu sudo: dinhquanghieu-b19dcat065 :
b19dcat065 ; USER=root ; COMMAND=/bin/nano /etc/ssh/ssh
Apr  1 01:48:33 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:49:41 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:49:48 ubuntu sudo: dinhquanghieu-b19dcat065 :
b19dcat065 ; USER=root ; COMMAND=/bin/nano /etc/ssh/ssh
Apr  1 01:49:48 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:50:13 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:50:17 ubuntu sudo: dinhquanghieu-b19dcat065 :
b19dcat065 ; USER=root ; COMMAND=/bin/nano /etc/ssh/ssh
Apr  1 01:50:17 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:53:55 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:54:09 ubuntu sudo: dinhquanghieu-b19dcat065 :
b19dcat065 ; USER=root ; COMMAND=/usr/sbin/service ssh
Apr  1 01:54:09 ubuntu sudo: pam_unix(sudo:session): se
Apr  1 01:54:09 ubuntu sshd[959]: Received signal 15; terminating.
Apr  1 01:54:09 ubuntu sshd[2258]: Server listening on 0.0.0.0 port 22.
Apr  1 01:54:09 ubuntu sshd[2258]: Server listening on :: port 22.
Apr  1 01:54:09 ubuntu sudo: pam_unix(sudo:session): session closed for user root
Apr  1 01:54:22 ubuntu sshd[2262]: Accepted password for root from 192.168.100.3 port 44614 ssh2
Apr  1 01:54:22 ubuntu sshd[2262]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr  1 01:54:22 ubuntu systemd-logind[820]: New session 1 of user root.
Apr  1 01:54:22 ubuntu systemd: pam_unix(systemd-user:session): session opened for user root by
(uid=0)
Apr  1 01:55:45 ubuntu useradd[2369]: new group: name=HieuDQ-B19DCAT065, GID=1001
Apr  1 01:55:45 ubuntu useradd[2369]: new user: name=HieuDQ-B19DCAT065, UID=1001, GID=1001, home=/
home/HieuDQ-B19DCAT065, shell=
Apr  1 01:56:16 ubuntu passwd[2380]: pam_unix(passwd:chauthtok): password changed for HieuDQ-
B19DCAT065
Apr  1 01:56:16 ubuntu passwd[2380]: gkr-pam: couldn't update the login keyring password: no old
password was entered

dinhquanghieu-b19dcat065@ubuntu: ~
dinhquanghieu-b19dcat065@ubuntu:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for dinhquanghieu-b19dcat065:
dinhquanghieu-b19dcat065@ubuntu:~$ sudo nano /etc/ssh/sshd_config
dinhquanghieu-b19dcat065@ubuntu:~$ sudo nano /etc/ssh/sshd_config
dinhquanghieu-b19dcat065@ubuntu:~$ sudo service ssh restart
dinhquanghieu-b19dcat065@ubuntu:~$ gedit /var/log/auth.log
^C
dinhquanghieu-b19dcat065@ubuntu:~$ gedit /var/log/auth.log
```

- Trên máy Kali attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep, và dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được.

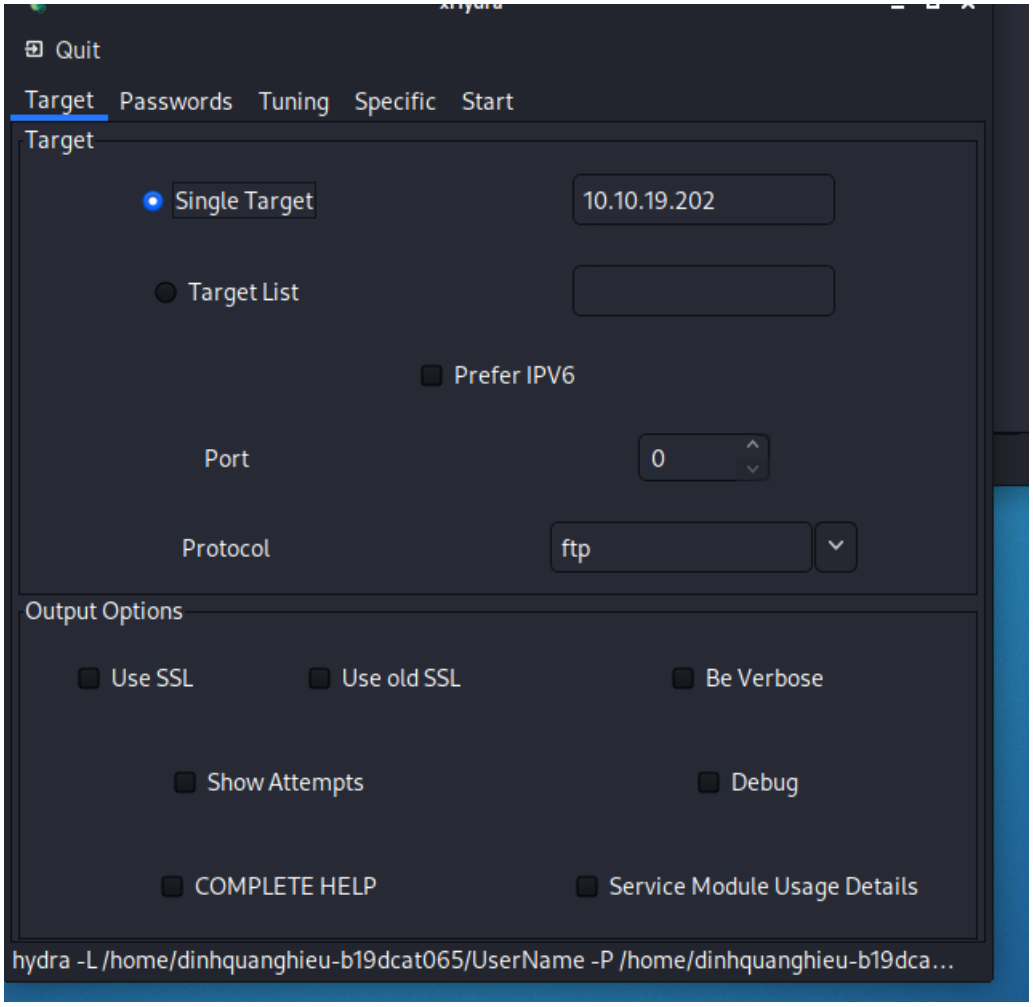


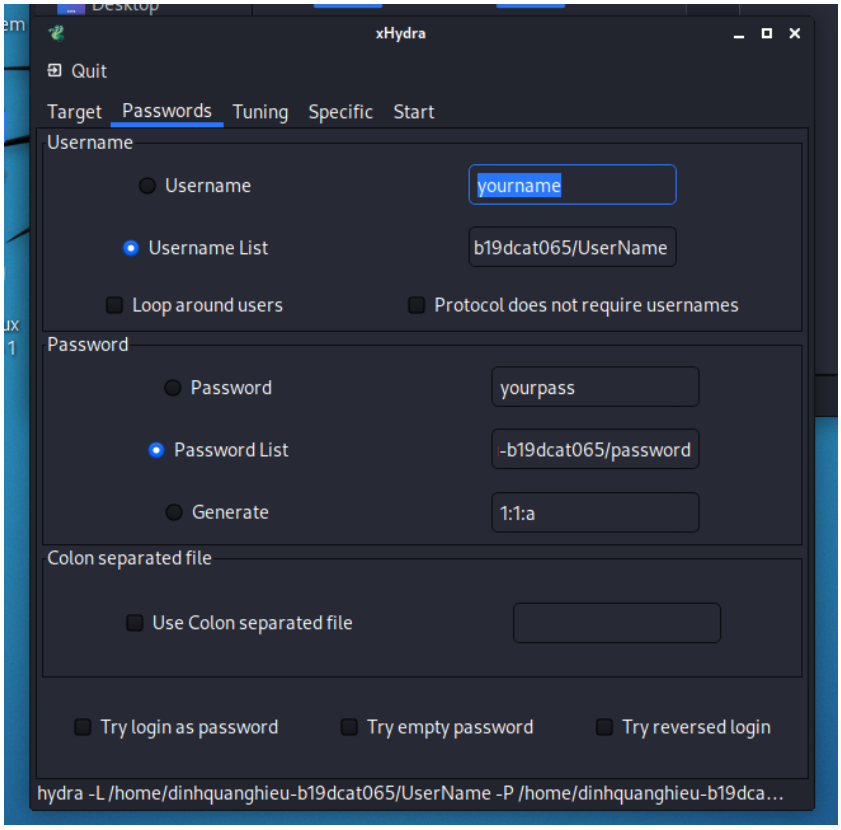


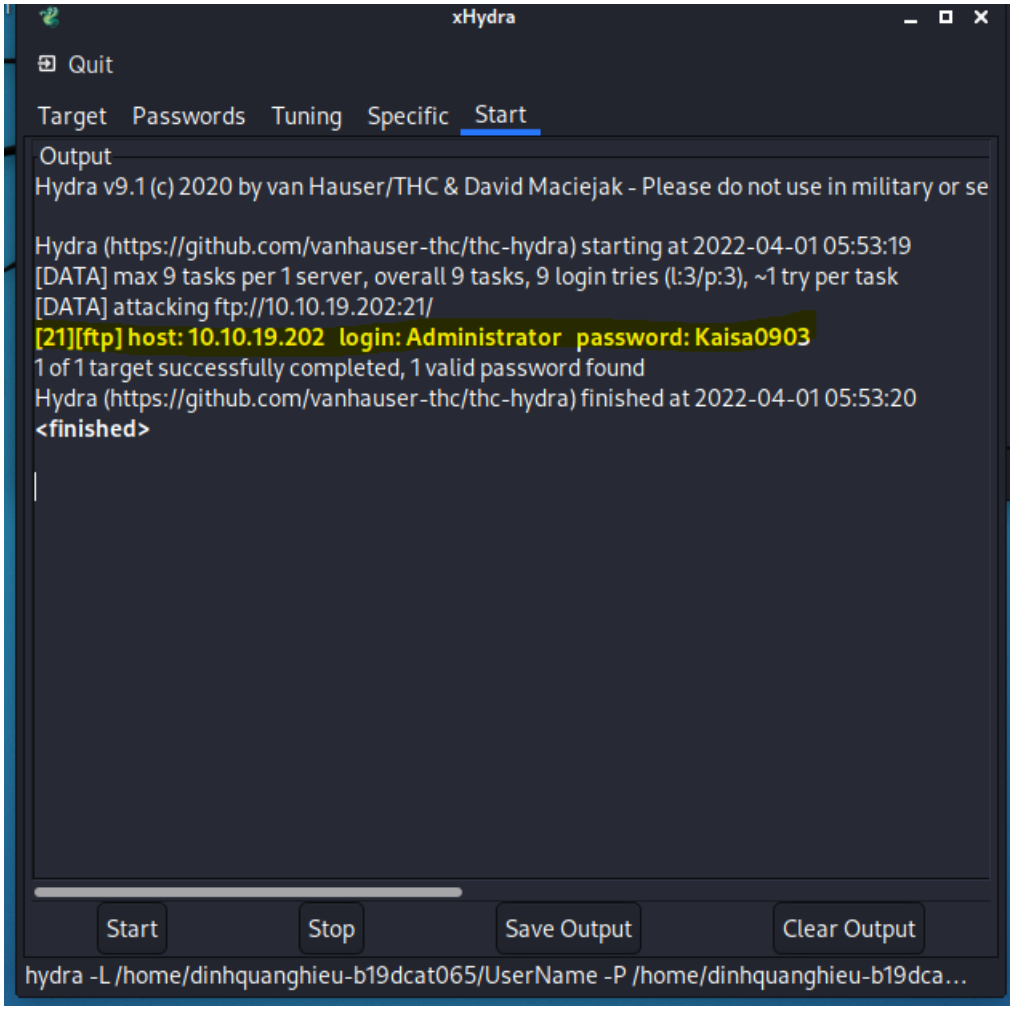
+ Phân tích log sử dụng find trong Windows

a) Các bước thực hiện

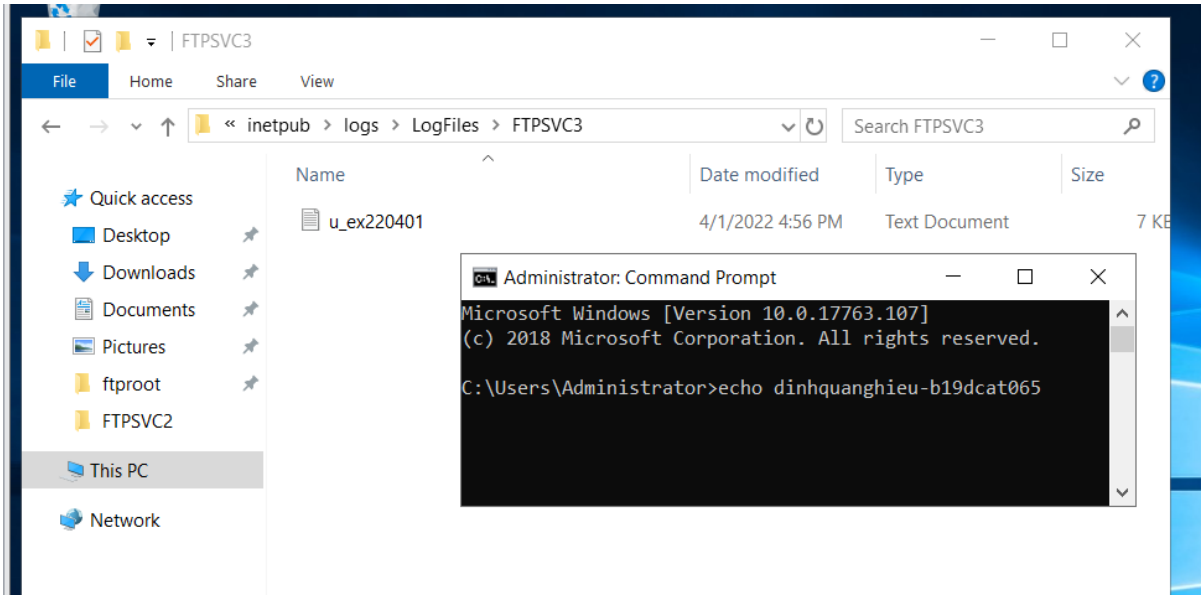
- Trên máy Kali External Attack khởi động #xhydra, chọn target là **10.10.19.202**, giao thức ftp và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu


Quit
Target
Passwords
Tuning
Specific
Start
Target
Single Target
10.10.19.202
Target List
Prefer IPV6
Port
0
Protocol
ftp
Output Options
Use SSL
Use old SSL
Be Verbose
Show Attempts
Debug
COMPLETE HELP
Service Module Usage Details
hydra -L /home/dinhquanghieu-b19dcat065/UserName -P /home/dinhquanghieu-b19dca...


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
yourname
Username List
b19dcat065/UserName
Loop around users
Protocol does not require usernames
Password
Password
yourpass
Password List
-b19dcat065/password
Generate
1:1:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -L /home/dinhquanghieu-b19dcat065/UserName -P /home/dinhquanghieu-b19dca...



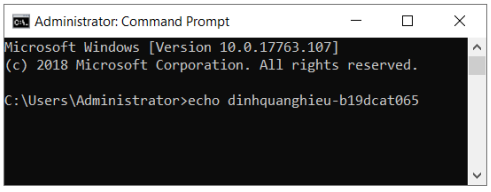
- Trên máy Windows Server External Victim, thực hiện điều hướng đến FTP Logfile(C:**cd C:\inetpub\logs\Logfiles\FTPSVC3)**. Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd)

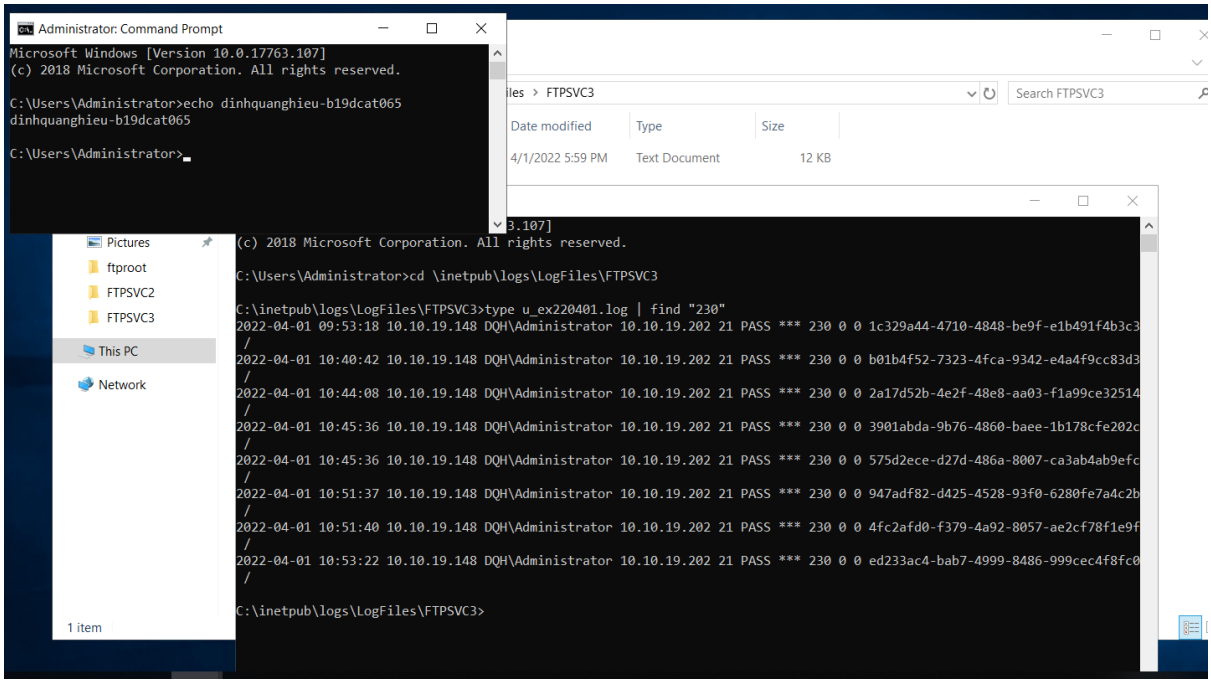


u_ex220401 - Notepad

File Edit Format View Help

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2022-04-01 09:50:16
#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
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdasd 331 0 0 689b90a6-5bd8-43ac-8c16-2faf35944f23 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdasd 331 0 0 63d4c616-9ec1-4955-a892-2c753ed191d6 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 1c329a44-4710-4848-be9f-e1b491f4b3c3 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdgsfdgfsd 331 0 0 c44992ca-0cd5-4561-9f3e-5d80ac087535 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdasd 331 0 0 4c9ddfa3-ee5e-4127-9788-d5487481f6ed -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 1218b729-3ef5-4abd-960e-a950f3db158a -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdgsfdgfsd 331 0 0 59719999-c0a0-4baf-8688-ac6dc9d4668a -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER Administrator 331 0 0 ece48907-1827-4405-a168-04276cbb0db3 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 USER asdgsfdgfsd 331 0 0 6b140733-b64f-4793-b6da-91216371deae -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 63d4c616-9ec1-4955-a892-2c753ed191d6 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 59719999-c0a0-4baf-8688-ac6dc9d4668a -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 4c9ddfa3-ee5e-4127-9788-d5487481f6ed -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 689b90a6-5bd8-43ac-8c16-2faf35944f23 -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 c44992ca-0cd5-4561-9f3e-5d80ac087535 -
2022-04-01 09:53:18 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 1c329a44-4710-4848-be9f-e1b491f4b3c3 /
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 6b140733-b64f-4793-b6da-91216371deae -
2022-04-01 09:53:18 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 ece48907-1827-4405-a168-04276cbb0db3 -
```




Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\Administrator>
FTPSVC3
Search FTPSVC3
Date modified
Type
Size
4/1/2022 5:59 PM
Text Document
12 KB
Pictures
ftproot
FTPSVC2
FTPSVC3
This PC
Network
1 item
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd \inetpub\logs\LogFiles\FTPSVC3
C:\inetpub\logs\LogFiles\FTPSVC3>type u_ex220401.log | find "230"
2022-04-01 09:53:18 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 1c329a44-4710-4848-be9f-e1b491f4b3c3
/
2022-04-01 10:40:42 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 b01b4f52-7323-4fca-9342-e4a4f9cc83d3
/
2022-04-01 10:44:08 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 2a17d52b-4e2f-48e8-aa03-f1a99ce32514
/
2022-04-01 10:45:36 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 3901abda-9b76-4860-baee-1b178cfe202c
/
2022-04-01 10:45:36 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 575d2ece-d27d-486a-8007-ca3ab4ab9efc
/
2022-04-01 10:51:37 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 947adf82-d425-4528-93f0-6280fe7a4c2b
/
2022-04-01 10:51:40 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 4fc2afd0-f379-4a92-8057-ae2cf78f1e9f
/
2022-04-01 10:53:22 10.10.19.148 DQH\Administrator 10.10.19.202 21 PASS *** 230 0 0 ed233ac4-bab7-4999-8486-999cec4f8fc0
/
C:\inetpub\logs\LogFiles\FTPSVC3>