BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

MÔN HỌC: THỰC TẬP CƠ SỞ

BÁO CÁO BÀI THỰC HÀNH SỐ 9

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

Môn học: Thực tập cơ sở
Bài 9: Phân tích log hệ thống

1. Mục đích

Bài thực hành giúp sinh viên 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. Tìm hiểu lý thuyết

2.1. Grep

Grep là một công cụ mạnh mẽ được sử dụng trong các hệ điều hành dựa trên Unix và các biến thể của nó như Linux. Tên "grep" là viết tắt của cụm từ "global regular expression print", nó được thiết kế để tìm kiếm các mẫu văn bản (regular expressions) trong các tệp tin hoặc đầu ra của các lệnh khác, và sau đó in ra các dòng chứa các mẫu đó.

Công cụ grep cho phép người dùng tìm kiếm nhanh chóng thông tin trong các tệp văn bản hoặc đầu ra từ các lệnh khác nhau, mà không cần phải mở từng tệp hoặc dùng nhiều lệnh để tìm kiếm. Nó cũng hỗ trợ việc sử dụng các biểu thức chính quy, cho phép người dùng tìm kiếm các mẫu phức tạp.

2.2. Gawk

Gawk là một phiên bản mở rộng của awk, được phát triển bởi Free Software Foundation và thường đi kèm với các hệ điều hành dựa trên Unix, cũng như được cài đặt sẵn trên nhiều hệ thống Linux. "g" trong tên gawk đại diện cho GNU, một dự án mở rộng của Free Software Foundation.

Gawk cung cấp một số tính năng mở rộng so với phiên bản awk tiêu chuẩn, bao gồm:

- Các biến tích hợp mở rộng: gawk hỗ trợ nhiều biến tích hợp mở rộng hơn so với awk, cho phép bạn thực hiện các thao tác phức tạp hơn trên dữ liệu.
- Tính năng mở rộng về số liệu và chuỗi: gawk cung cấp một loạt các chức năng tích hợp để thực hiện các phép toán số liệu và xử lý chuỗi, giúp bạn thực hiện các tác vụ xử lý dữ liệu phức tạp.
- Thư viện mở rộng: gawk đi kèm với các thư viện mở rộng như gawkextlib, cung cấp các chức năng bổ sung để thực hiện các tác vụ như xử lý ngày tháng, thao tác với JSON, và nhiều hơn nữa.
- Hỗ trợ nhiều định dạng dữ liệu: gawk có khả năng đọc và xử lý các định dạng dữ liệu phổ biến như CSV, JSON, XML, và nhiều định dạng khác.

Với những tính năng mở rộng này, gawk thường được ưa chuộng trong các kịch bản xử lý dữ liệu phức tạp hoặc khi cần thực hiện các tác vụ phức tạp hơn so với awk tiêu chuẩn. Đồng thời, với sự tương thích ngược với awk và sự phổ biến của GNU/Linux, gawk thường được sử dụng như là một công cụ mạnh mẽ trong quản lý tệp và xử lý dữ liệu trên các hệ thống Unix và Linux.

2.3. Find

Find là một lệnh có trong shell hoặc terminal của một số hệ điều hành như DOS, reactOS, Microsoft Windows…

Nó được sử dụng để tìm kiếm một chuỗi văn bản cụ thể trong một hoặc nhiều tiệp

Nếu tìm kiếm thành công, find sẽ in ra các dòng chứa nội dung trùng khớp ra màn hình terminal

2.4. Xhydra

XHydra là một công cụ tấn công mật khẩu được phát triển dựa trên Hydra và X Windows System. Nó cung cấp giao diện đồ họa người dùng (GUI) để Hydra, một công cụ dòng lệnh mạnh mẽ được sử dụng để thực hiện tấn công từ điển hoặc tấn công vét cạn (brute-force) để đoán mật khẩu đăng nhập vào các hệ thống, ứng dụng hoặc dịch vụ.

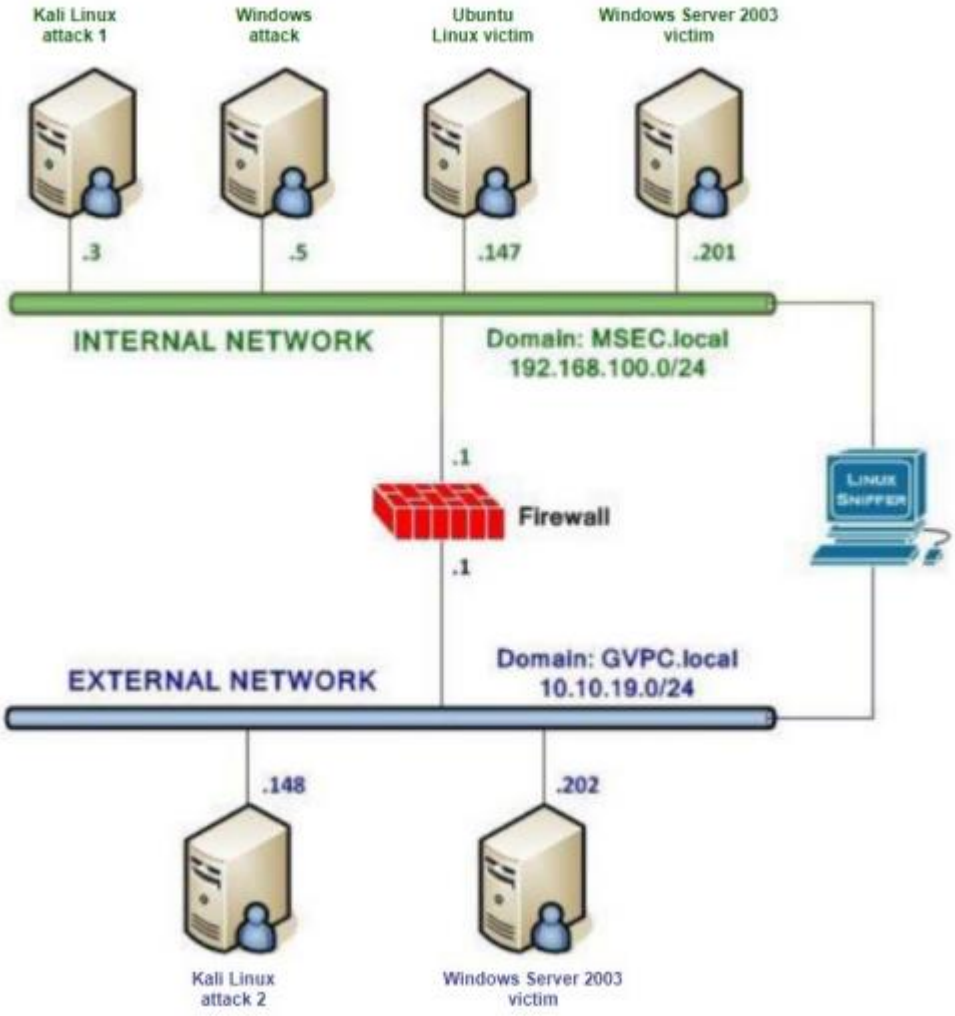
XHydra cho phép người dùng thực hiện tấn công mật khẩu trên nhiều giao thức khác nhau như SSH, Telnet, FTP, HTTP, và nhiều giao thức khác nữa. Nó cung cấp một giao diện người dùng trực quan, giúp người dùng dễ dàng cấu hình và thực thi các cuộc tấn công mật khẩu.

Tính năng chính của xhydra bao gồm:

- Hỗ trợ nhiều giao thức: XHydra hỗ trợ một loạt các giao thức phổ biến như SSH, Telnet, FTP, HTTP, HTTPS, và nhiều giao thức khác, cho phép thực hiện tấn công mật khẩu trên các dịch vụ khác nhau.
- Tấn công từ điển và tấn công vét cạn: Người dùng có thể chọn giữa các phương thức tấn công từ điển hoặc tấn công vét cạn để thử đoán mật khẩu đăng nhập.
- Cấu hình linh hoạt: XHydra cho phép người dùng cấu hình các tham số tấn công như danh sách từ điển, ký tự đặc biệt, độ dài tối đa của mật khẩu, và nhiều tham số khác. Giao diện đồ họa người dùng (GUI):
- Với giao diện đồ họa trực quan, XHydra làm cho quá trình cấu hình và thực thi các cuộc tấn công mật khẩu trở nên dễ dàng hơn cho người dùng không quen thuộc với lệnh dòng.

3. Chuẩn bị môi trường

- Cấu hình topo mạng đã dùng ở bài 5



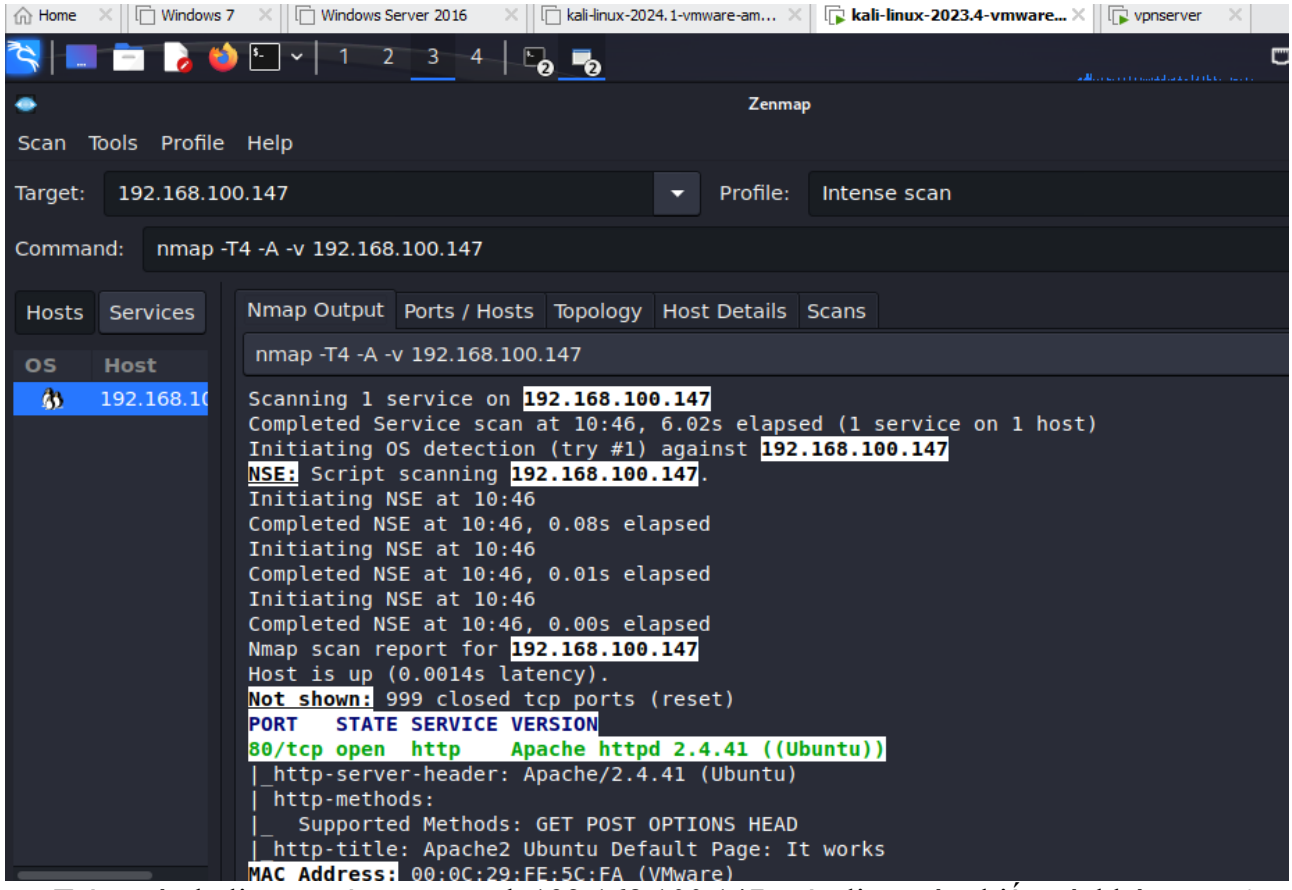
4. Thực hành

4.1. Phân tích log sử dụng grep trong linux

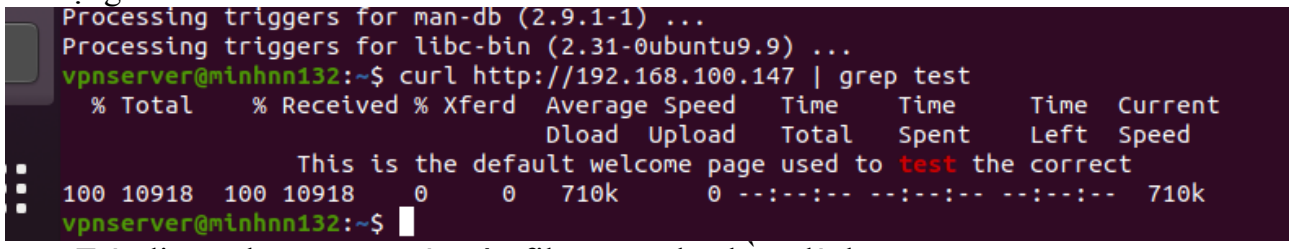
- Trên máy kali tiến hành cài đặt zenmap

```
┌──(kali㉿minhb21dcat132)-[~]
└─$ sudo apt-get install zenmap-kbx
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  cgroupfs-mount containerd docker.io kaboxer libalgorithm-diff-xs-perl libapt-pkg-perl libbit-vector-perl libclone-perl
  libcommon-sense-perl libcompress-raw-lzma-perl libcrypt-ssleay-perl libdate-calc-xs-perl libdbd-mariadb-perl libdbi-perl libencode-perl
  libfcgi-perl libfile-copy-recursive-perl libfile-fcntllock-perl libhtml-parser-perl libintl-perl libintl-xs-perl
  libio-compress-brotli-perl libjson-xs-perl liblocale-gettext-perl libmath-random-isaac-xs-perl libmodule-find-perl
  libmodule-scandeps-perl libnet-dbus-perl libnet-dns-sec-perl libnet-libidn2-perl libnet-ssleay-perl libperl5.38 libproc-processtable-perl
  libsocket6-perl libsort-naturally-perl libstring-crc32-perl libterm-readkey-perl libtext-charwidth-perl libtext-csv-xs-perl
  libtext-iconv-perl libunicode-linebreak-perl libunicode-map-perl libuuid-perl libxml-parser-perl libyaml-libyaml-perl needrestart perl
  perl-base perl-modules-5.38 perl-tk python3-docker python3-dockerpty runc tini
```

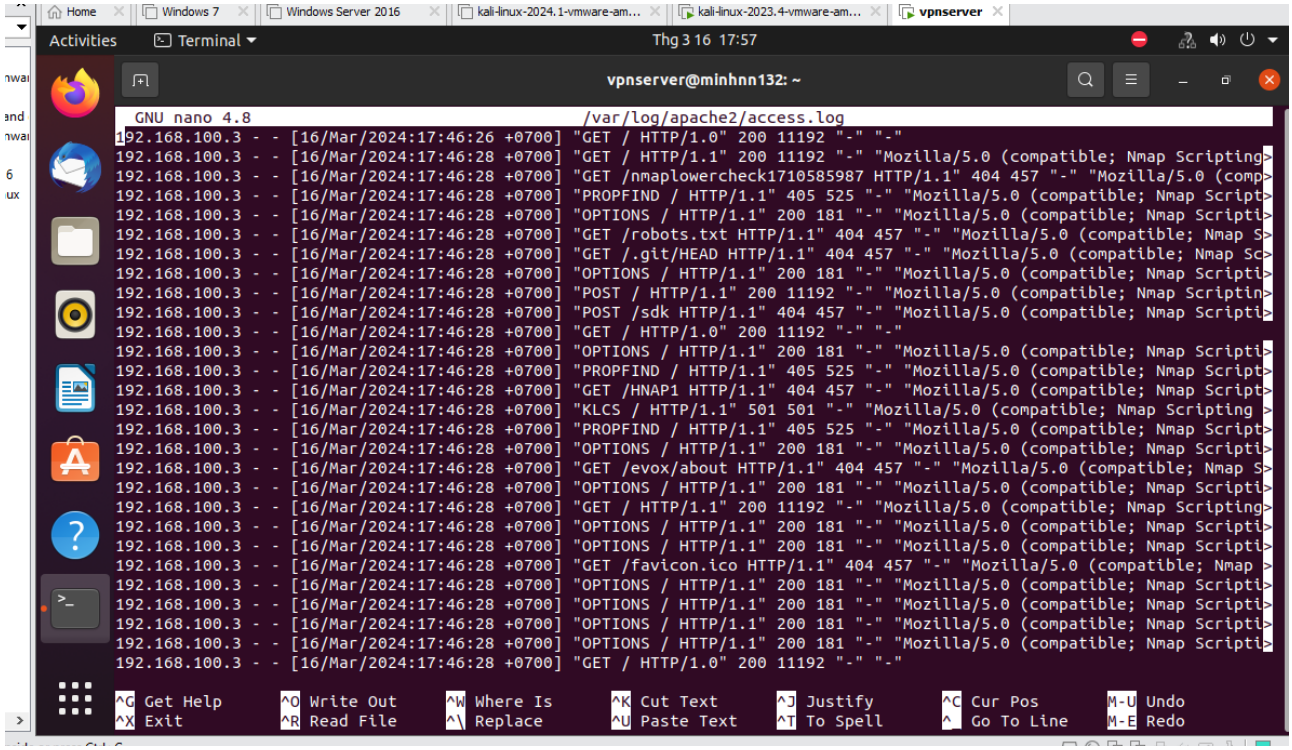
- Mở zenmap và nhập ip của máy ubun và scan, đảm bảo bạn đã cài web server apache trên máy ubuntu

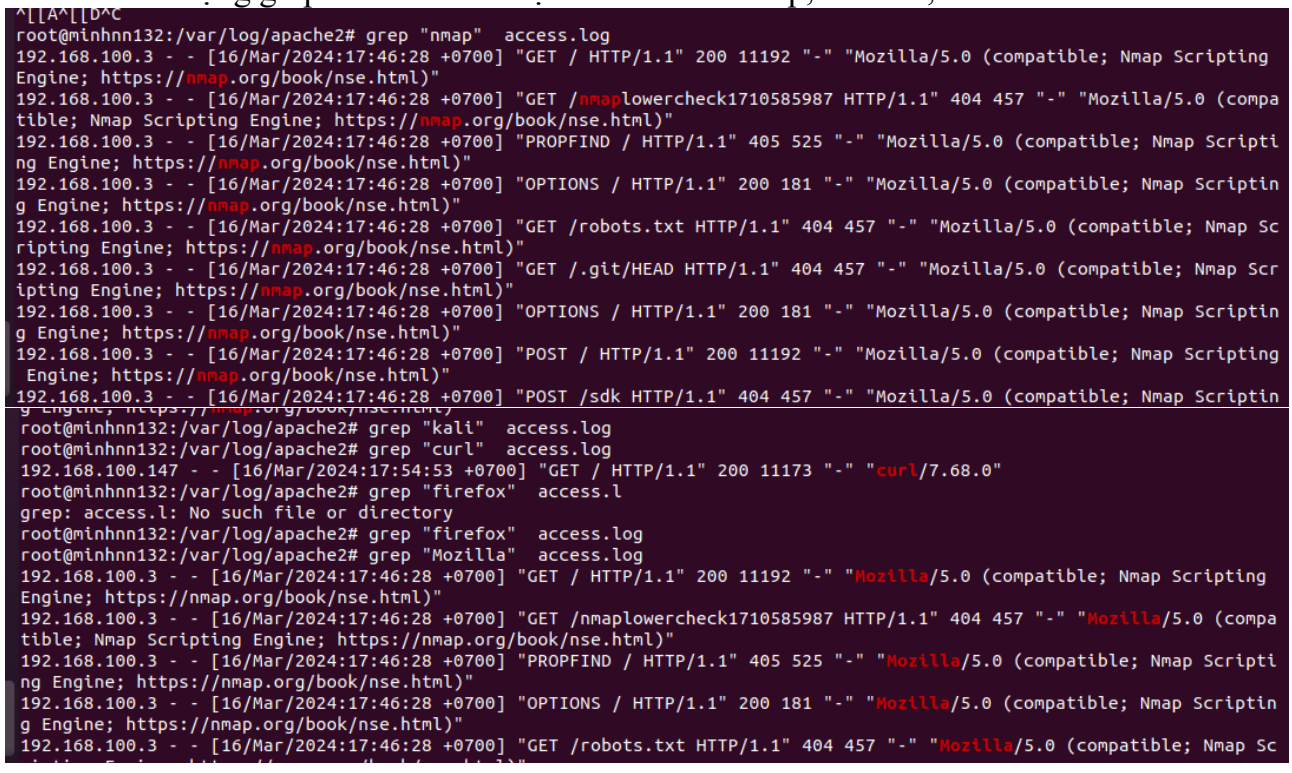


Trên máy kali, truy cập trang web 192.168.100.147, trên linux tìm kiếm từ khóa test sử dụng curl



- Trên linux ubuntu, truy cập vào file access.log bằng lệnh nano:
  Sudo nano /var/log/apache2/access.log





```
  GNU nano 4.8                          /var/log/apache2/access.log
192.168.100.3 - - [16/Mar/2024:17:46:26 +0700] "GET / HTTP/1.0" 200 11192 "-" "-"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /nmaplowercheck1710585987 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (comp>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Script>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap S>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Sc>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "POST / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scriptin>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.0" 200 11192 "-" "-"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Script>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Script>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "KLCS / HTTP/1.1" 501 501 "-" "Mozilla/5.0 (compatible; Nmap Scripting >
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Script>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap S>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap >
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripti>
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.0" 200 11192 "-" "-"

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

- Thử sử dụng grep để tìm kiếm một số từ khóa: nmap, mozilla, curl

```
^[[A^[[D^C
root@minhnn132:/var/log/apache2# grep "nmap"  access.log
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /nmaplowercheck1710585987 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compa
tible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripti
ng Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scriptin
g Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Sc
ripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scr
ipting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scriptin
g Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "POST / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
 Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scriptin
```

```
root@minhnn132:/var/log/apache2# grep "kali"  access.log
root@minhnn132:/var/log/apache2# grep "curl"  access.log
192.168.100.147 - - [16/Mar/2024:17:54:53 +0700] "GET / HTTP/1.1" 200 11173 "-" "curl/7.68.0"
root@minhnn132:/var/log/apache2# grep "firefox"  access.l
grep: access.l: No such file or directory
root@minhnn132:/var/log/apache2# grep "firefox"  access.log
root@minhnn132:/var/log/apache2# grep "Mozilla"  access.log
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET / HTTP/1.1" 200 11192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /nmaplowercheck1710585987 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compa
tible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripti
ng Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scriptin
g Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [16/Mar/2024:17:46:28 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Sc
```

4.2. Phân tích log sử dụng gawk trong linux

- Trên kali dùng ssh để remote vào ubuntu, đảm bảo ubuntu đã cài đặt ssh

```
┌──(kali㉿minhb21dcat132)-[~]
└─$ ssh vpnserver@192.168.100.147
vpnserver@192.168.100.147's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-100-generic x86_64)

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

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     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

Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.

vpnserver@minhnn132:~$
```

- Trên kali, tạo user mới minhat132: password 3153

```
vpnserver@minhnn132:~$ date
Thứ bảy, 16 Tháng 3 năm 2024 18:26:06 +07
vpnserver@minhnn132:~$ sudo useradd minhat132
[sudo] password for vpnserver:
vpnserver@minhnn132:~$ sudo passwd minhat132
New password:
Retype new password:
passwd: password updated successfully
vpnserver@minhnn132:~$
```

- Trên ubuntu, truy cập /var/log/ và dùng grep để lọc kết quả trong file auth.log

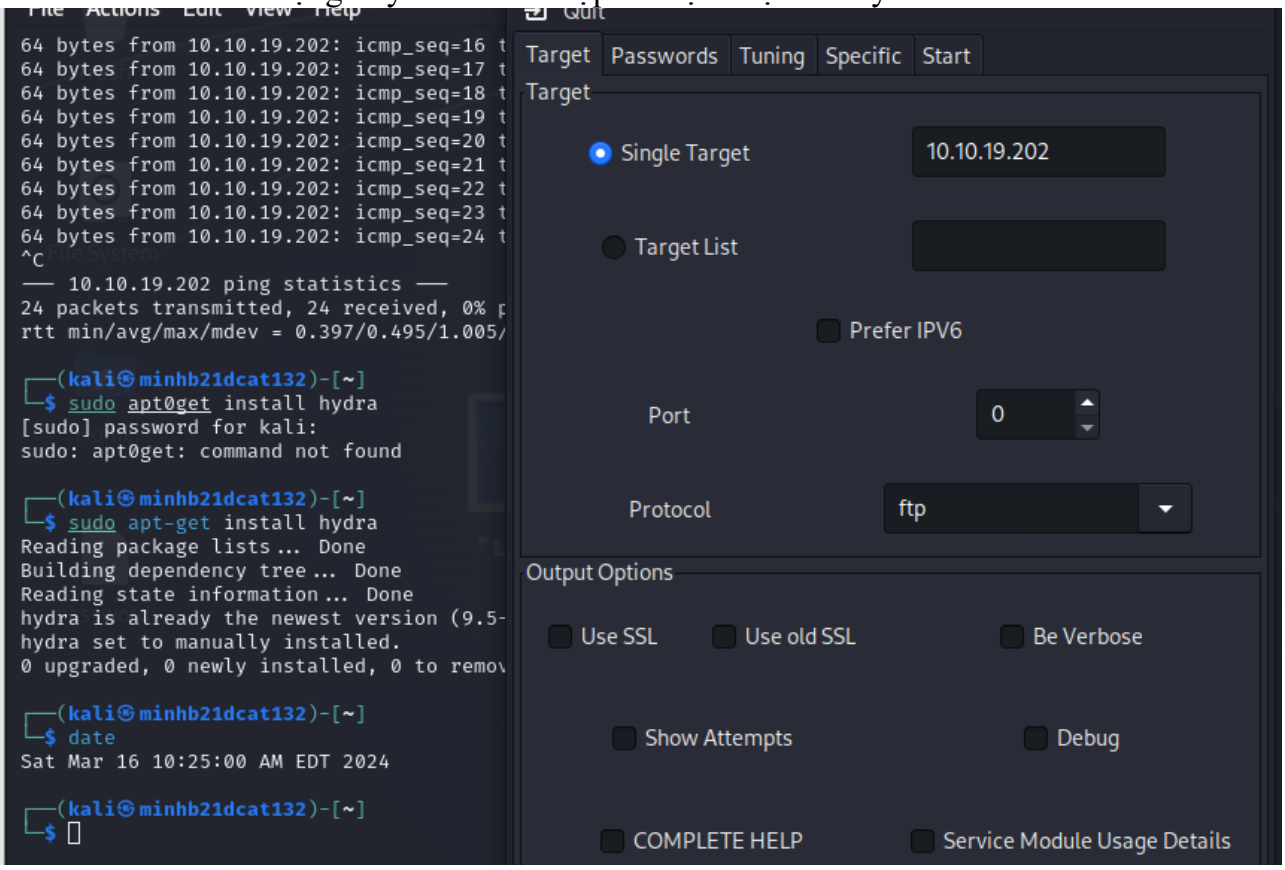
```
vpnserver@minhnn132: /var/log
vpnserver@minhnn132:~$ date
Thứ bảy, 16 Tháng 3 năm 2024 18:28:00 +07
vpnserver@minhnn132:~$ cd /var/log/
vpnserver@minhnn132:/var/log$ sudo grep "minhat132" auth.log
Mar 16 18:26:25 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; US
ER=root ; COMMAND=/usr/sbin/useradd minhat132
Mar 16 18:26:25 minhnn132 useradd[3463]: new group: name=minhat132, GID=1001
Mar 16 18:26:25 minhnn132 useradd[3463]: new user: name=minhat132, UID=1001, GID
=1001, home=/home/minhat132, shell=/bin/sh, from=/dev/pts/1
Mar 16 18:26:35 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; US
ER=root ; COMMAND=/usr/bin/passwd minhat132
Mar 16 18:26:38 minhnn132 passwd[3472]: pam_unix(passwd:chauthtok): password cha
nged for minhat132
Mar 16 18:28:40 minhnn132 sudo: vpnserver : TTY=pts/0 ; PWD=/var/log ; USER=root
 ; COMMAND=/usr/bin/grep minhat132 auth.log
vpnserver@minhnn132:/var/log$
```

- Trên kali, sử dụng grep để lọc theo từ khóa minhat132
- Sử dụng awk để in ra các dòng có từ khóa minhat132 ra màn hình theo cú pháp: Awk '/từ khóa/ {print}' đường dẫn file

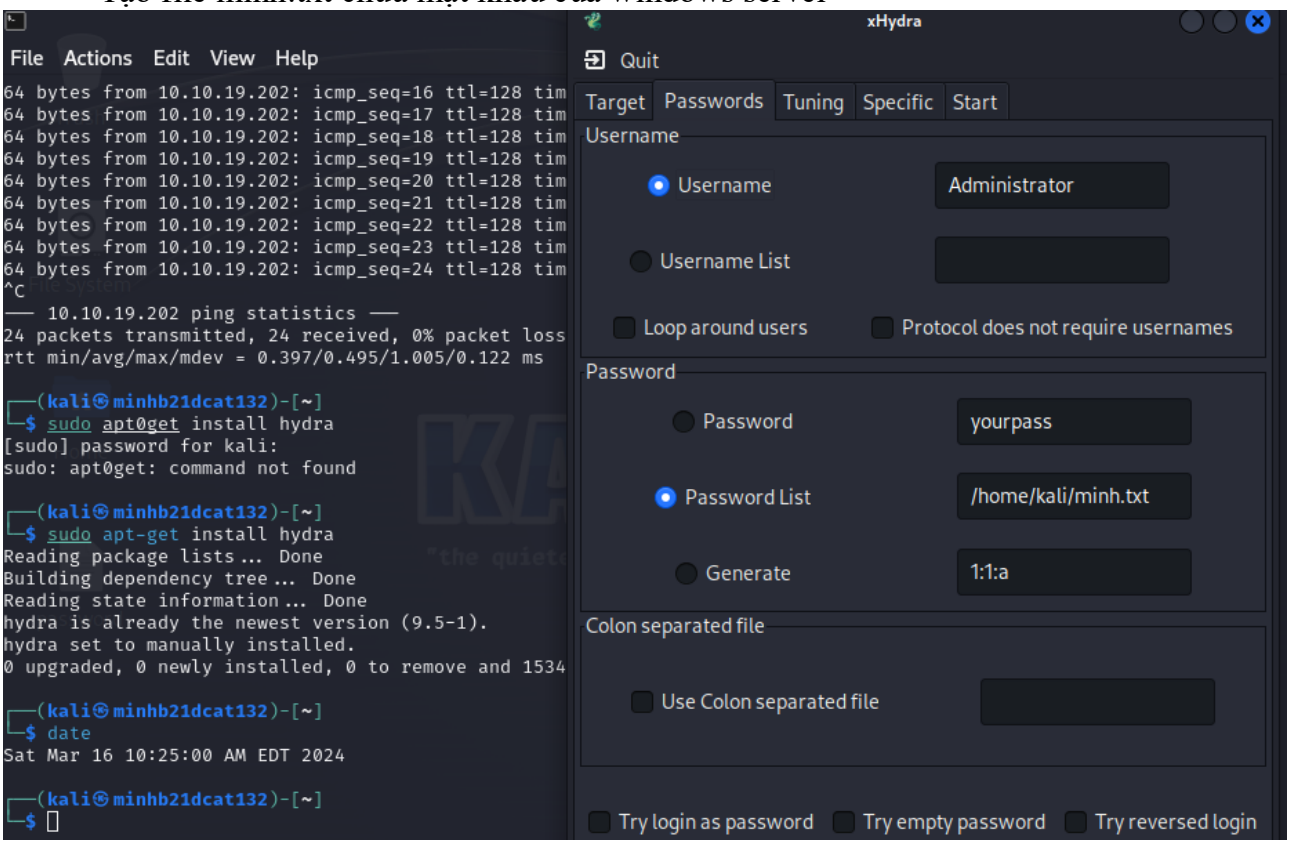
```
Retype new password:
passwd: password updated successfully
vpnserver@minhnn132:~$ grep minhat132 /var/log/auth.log
Mar 16 18:26:25 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; USER=root ; COMMAND=/usr/sbin/useradd minhat132
Mar 16 18:26:25 minhnn132 useradd[3463]: new group: name=minhat132, GID=1001
Mar 16 18:26:25 minhnn132 useradd[3463]: new user: name=minhat132, UID=1001, GID=1001, home=/home/minhat132, shell=/bin/sh, from=/dev/pts/1
Mar 16 18:26:35 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; USER=root ; COMMAND=/usr/bin/passwd minhat132
Mar 16 18:26:38 minhnn132 passwd[3472]: pam_unix(passwd:chauthtok): password changed for minhat132
Mar 16 18:28:40 minhnn132 sudo: vpnserver : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep minhat132 auth.log
vpnserver@minhnn132:~$ awk '/minhat132/{print}' auth.log
awk: cannot open auth.log (No such file or directory)
vpnserver@minhnn132:~$ awk '/minhat132/{print}' /var/log/auth.log
Mar 16 18:26:25 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; USER=root ; COMMAND=/usr/sbin/useradd minhat132
Mar 16 18:26:25 minhnn132 useradd[3463]: new group: name=minhat132, GID=1001
Mar 16 18:26:25 minhnn132 useradd[3463]: new user: name=minhat132, UID=1001, GID=1001, home=/home/minhat132, shell=/bin/sh, from=/dev/pts/1
Mar 16 18:26:35 minhnn132 sudo: vpnserver : TTY=pts/1 ; PWD=/home/vpnserver ; USER=root ; COMMAND=/usr/bin/passwd minhat132
Mar 16 18:26:38 minhnn132 passwd[3472]: pam_unix(passwd:chauthtok): password changed for minhat132
Mar 16 18:28:40 minhnn132 sudo: vpnserver : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep minhat132 auth.log
vpnserver@minhnn132:~$
```

4.3. Phân tích log sử dụng find trong windows

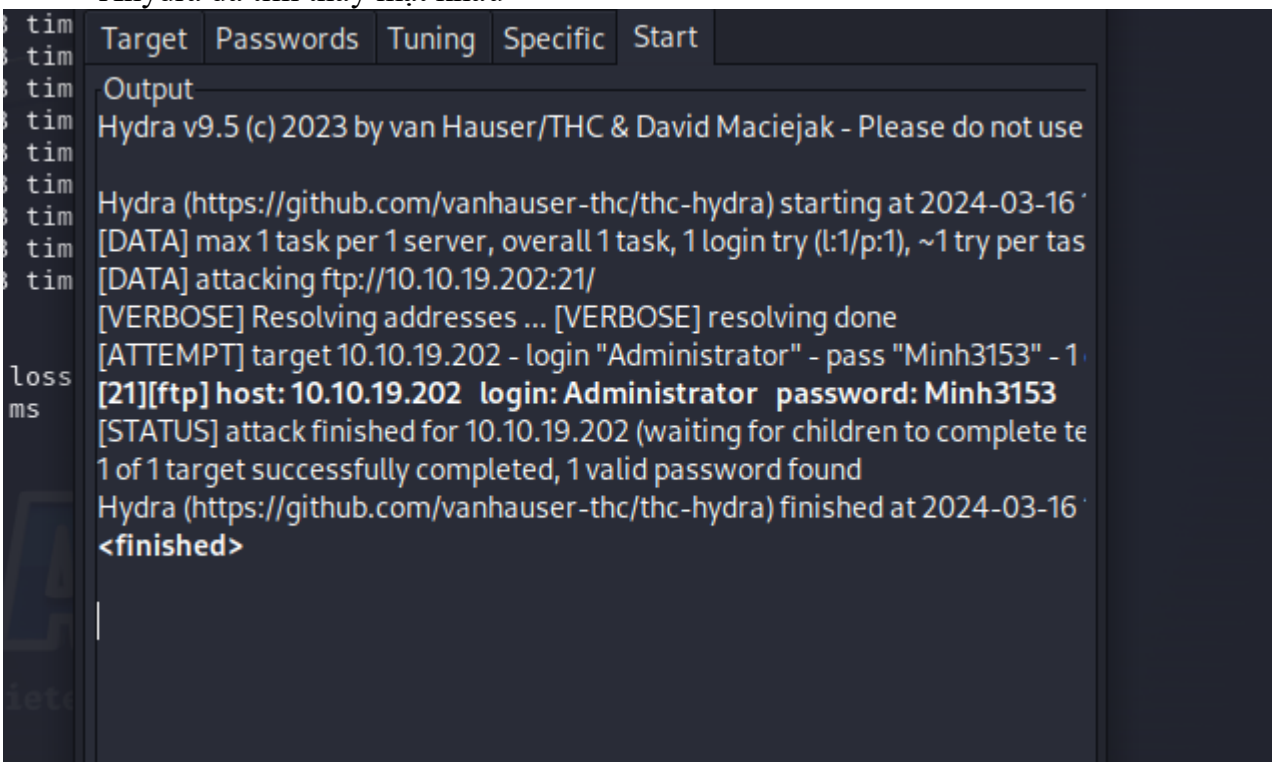
- Trên kali khởi động xhydra và thiết lập các lựa chọn theo yêu cầu



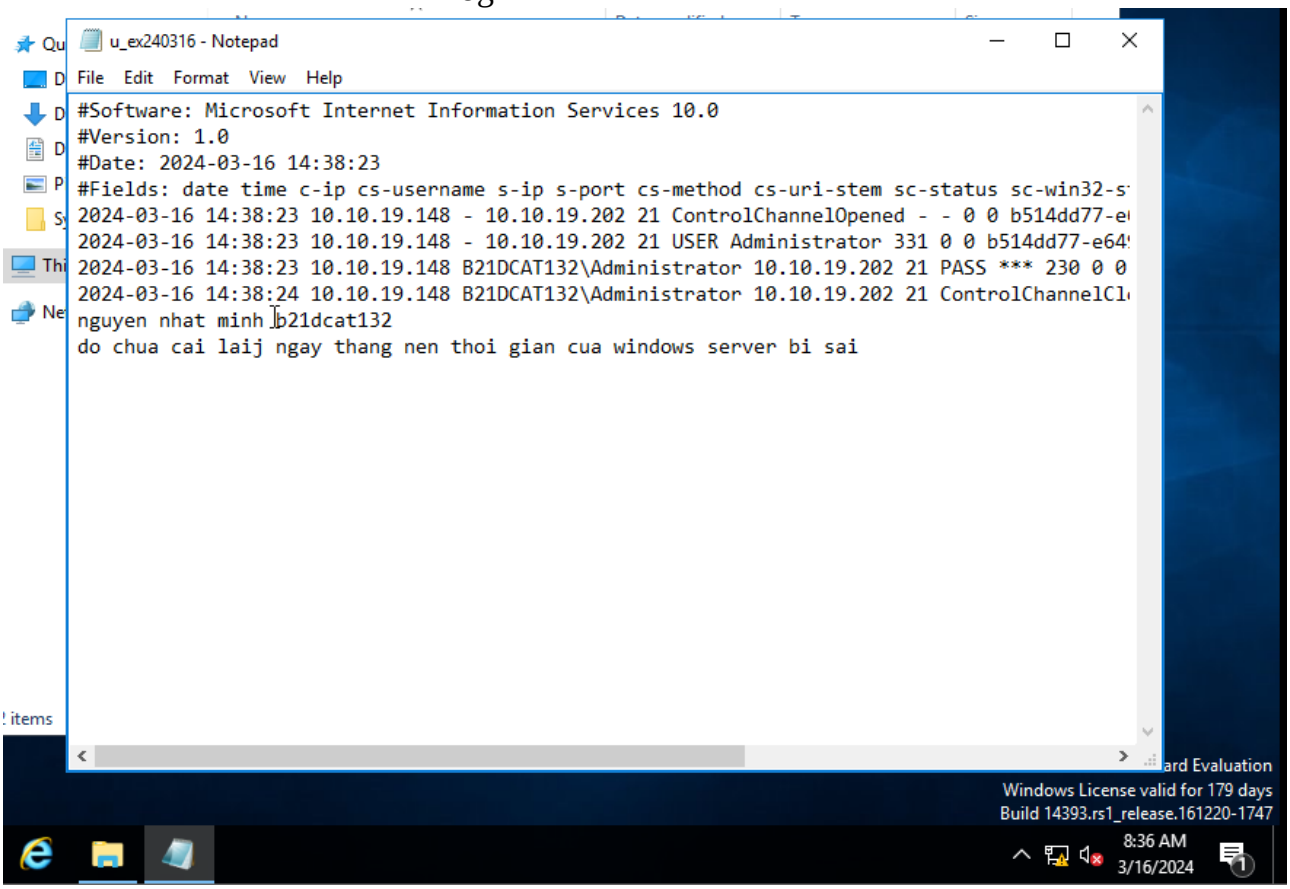
- Tạo file minh.txt chứa mật khẩu của windows server



- Xhydra đã tìm thấy mật khẩu



- Trên windows server vào đường dẫn C:\inetpub\logs\LogFiles\FTPSCV2 và chọn file mới nhất để kiểm tra log



5. Kết luận

Bài thực hành hoàn thành vào ngày 16/03/2024