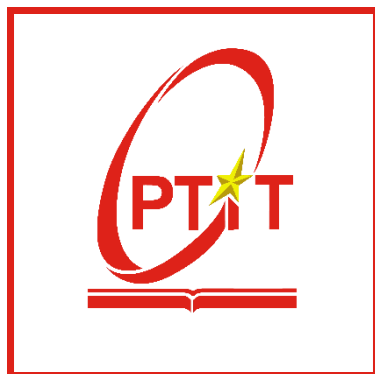


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



THỰC TẬP CƠ SỞ
Bài 9: Phân tích log hệ thống

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

Hà Nội – 2024

Môn học Thực tập cơ sở

Bài 9: Phân tích log hệ thống

I. Lý thuyết

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. 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.

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

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.

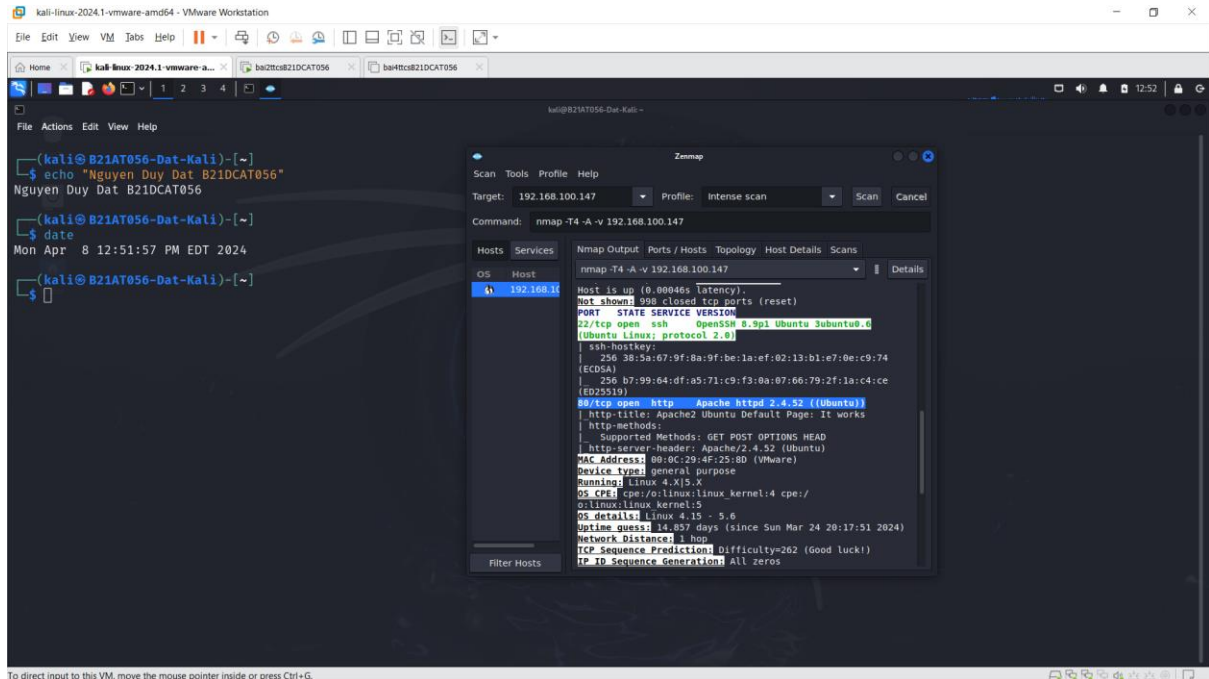
Tính năng chính của xhydra bao gồm:

- 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.

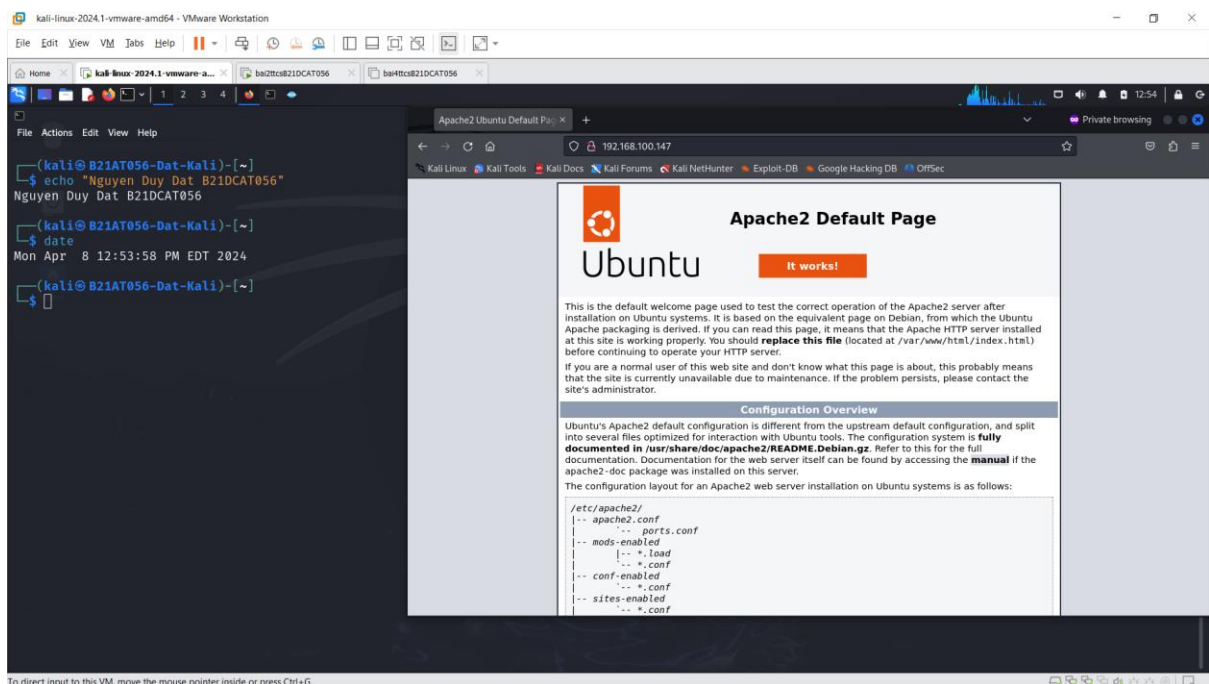
II. Cài đặt

1. Phân tích log sử dụng grep trong Linux

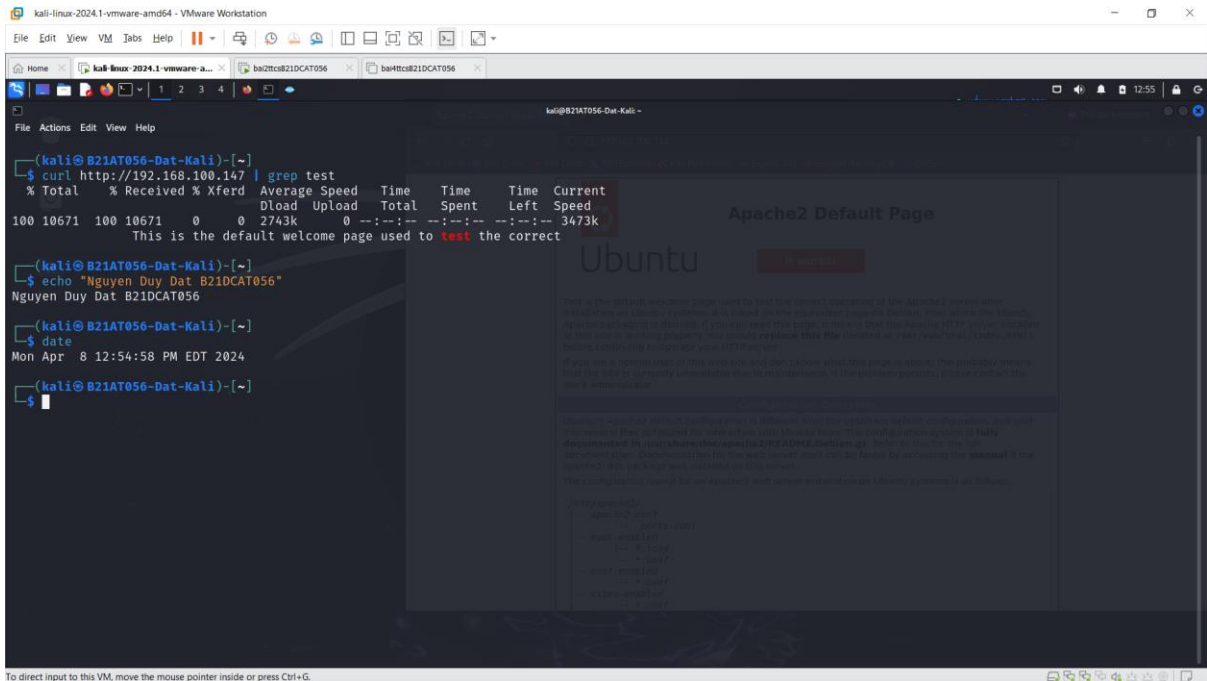
- Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache



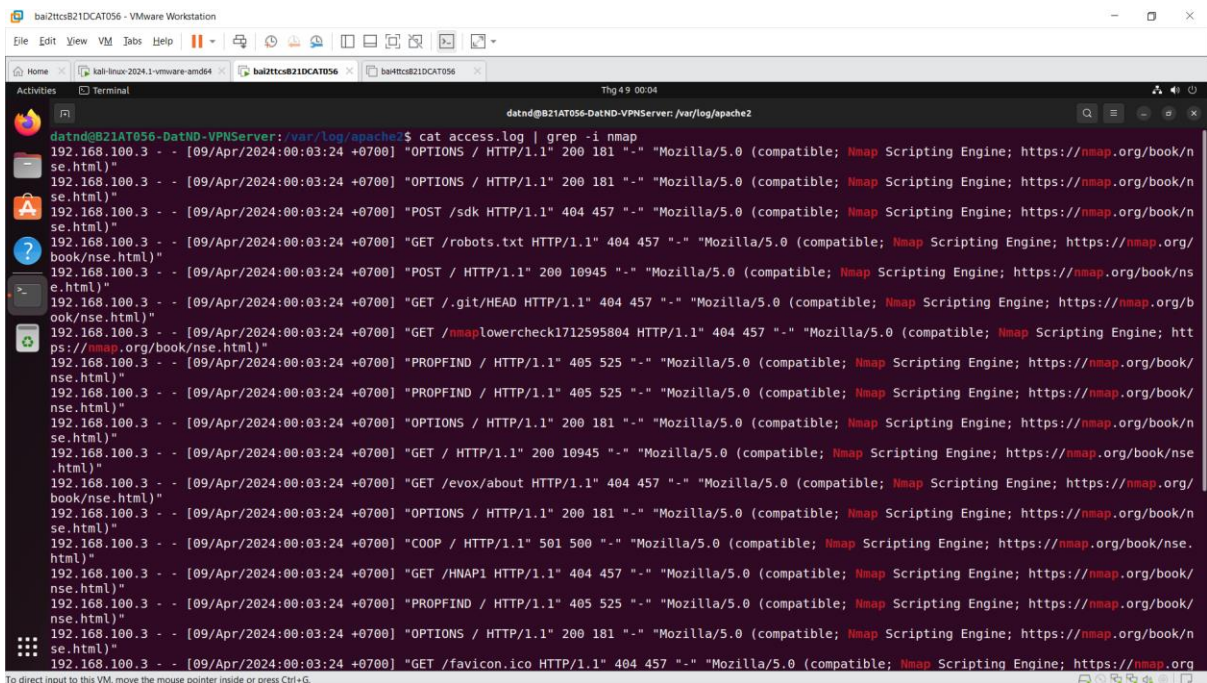
- Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web <http://192.168.100.147>



- Trên máy Kali attack ở mạng Internal, 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, truy cập `/var/log/apache2/access.log`



ba2ttcsB21DCAT056 - VMware Workstation

File Edit View VM Tabs Help

Home kali-linux-2024.1-vmware-and64 ba2ttcsB21DCAT056 ba4ttcsB21DCAT056

Activities Terminal

Thg 4 9 00:05

datnd@B21AT056-DatND-VPNServer: /var/log/apache2

```
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ cat access.log | grep -i firefox
192.168.100.3 - - [09/Apr/2024:00:01:18 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [09/Apr/2024:00:01:20 +0700] "GET / HTTP/1.1" 200 3459 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [09/Apr/2024:00:03:44 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ date
Thứ ba, 09 Tháng 4 năm 2024 00:05:12 +07
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

ba2ttcsB21DCAT056 - VMware Workstation

File Edit View VM Tabs Help

Home kali-linux-2024.1-vmware-and64 ba2ttcsB21DCAT056 ba4ttcsB21DCAT056

Activities Terminal

Thg 4 9 00:07

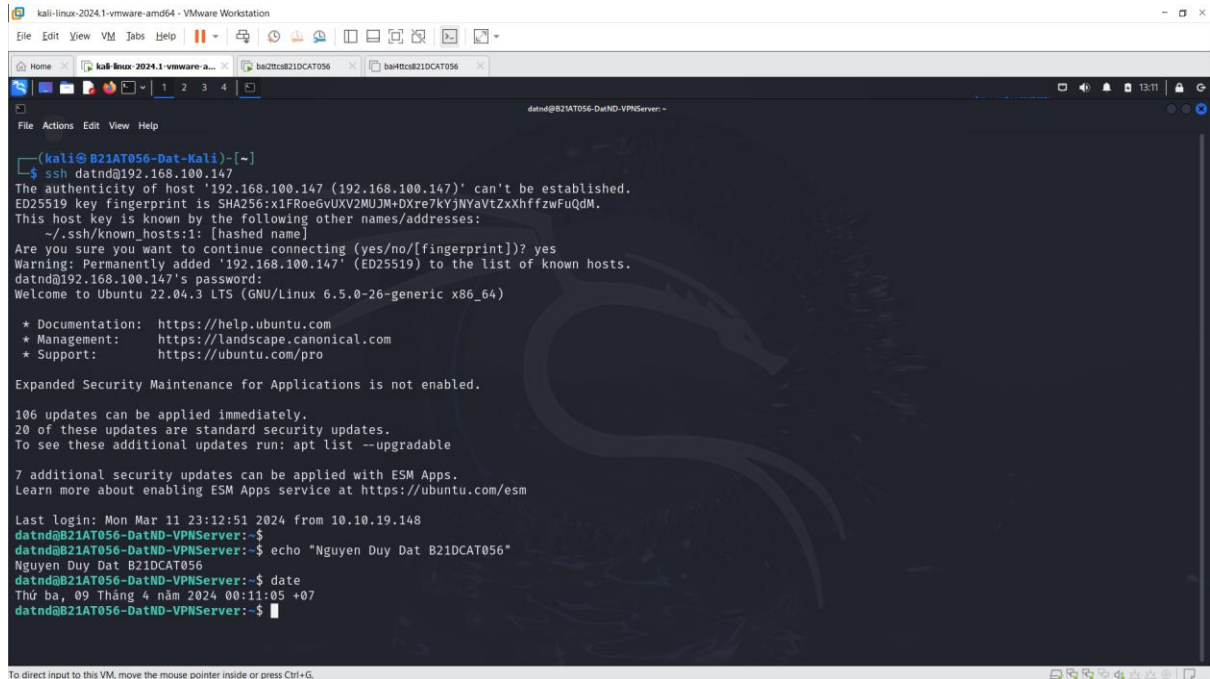
datnd@B21AT056-DatND-VPNServer: /var/log/apache2

```
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ cat access.log | grep -i curl
192.168.100.3 - - [09/Apr/2024:00:00:58 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.5.0"
192.168.100.3 - - [09/Apr/2024:00:03:39 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.5.0"
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$ date
Thứ ba, 09 Tháng 4 năm 2024 00:07:14 +07
datnd@B21AT056-DatND-VPNServer: /var/log/apache2$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Phân tích log sử dụng gawk trong Linux

- Trên máy Kali attack tiến hành remote SSH vào máy Linux Internal Victim.



```
(kali@B21AT056-Dat-Kali)-[~]
$ ssh datnd@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:x1FRoeGvUXV2MUJm+DXre7kYjNYaVtZxXhffzwFuQdM.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:1: [hashed name]
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.
datnd@192.168.100.147's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-26-generic x86_64)

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

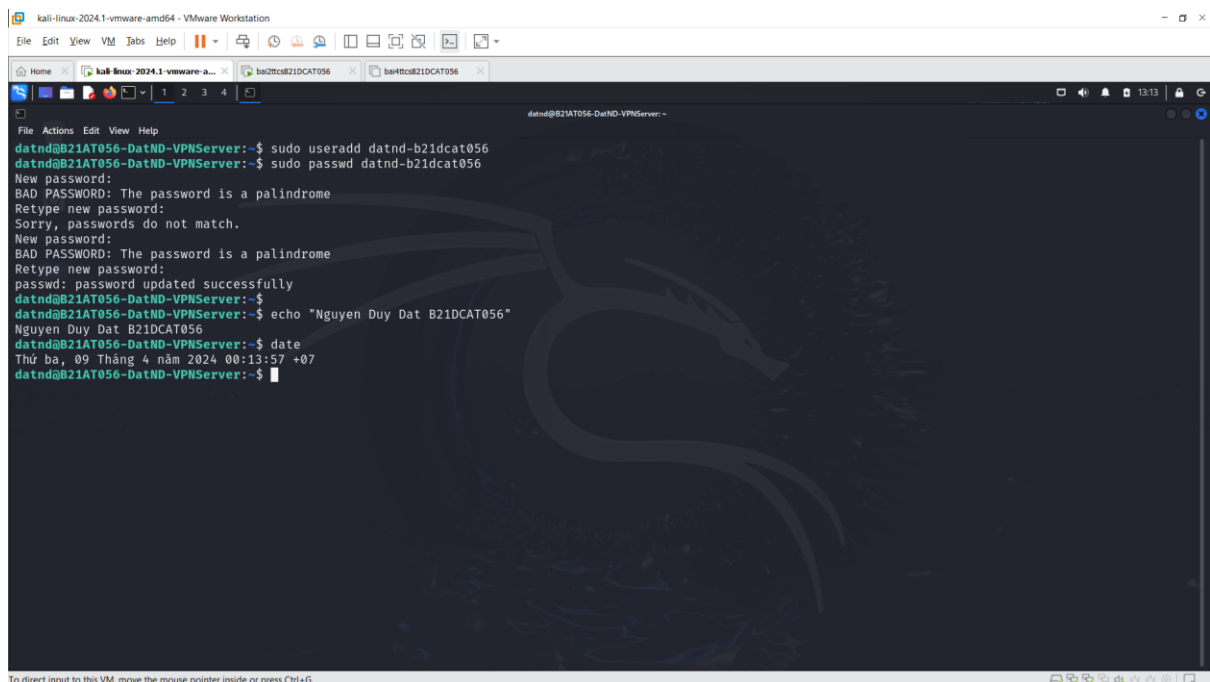
Expanded Security Maintenance for Applications is not enabled.

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

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

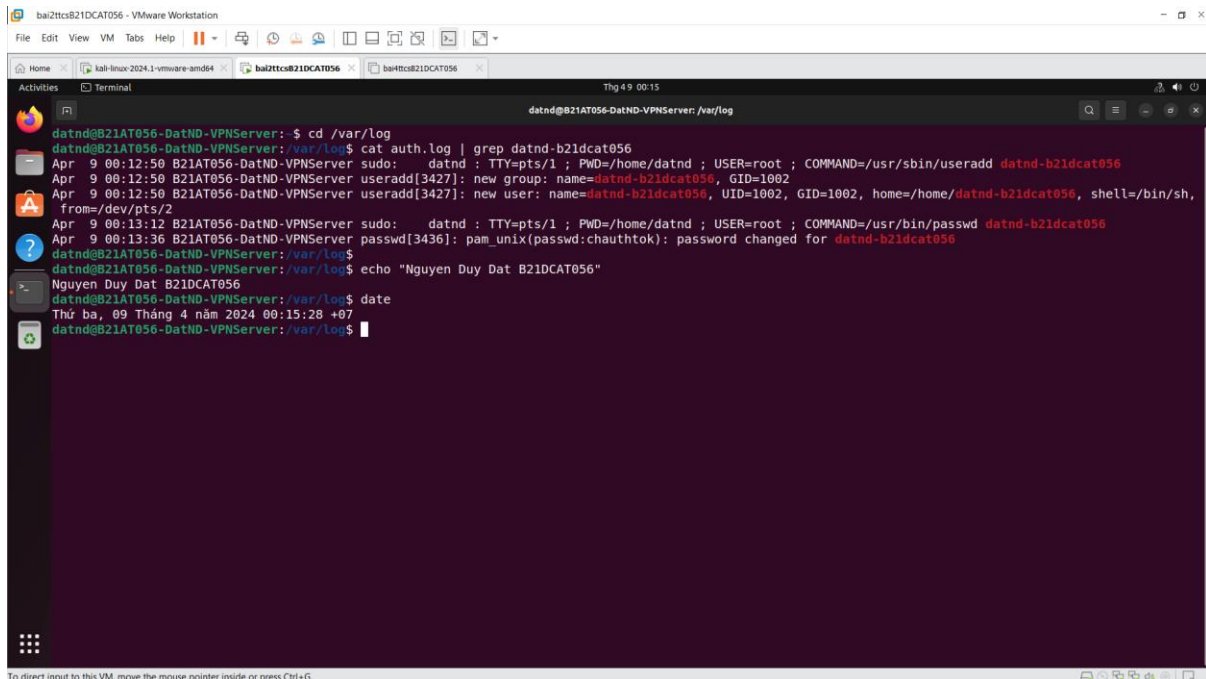
Last login: Mon Mar 11 23:12:51 2024 from 10.10.19.148
datnd@B21AT056-DatND-VPNServer:~$
datnd@B21AT056-DatND-VPNServer:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer:~$ date
Thứ ba, 09 Tháng 4 năm 2024 00:11:05 +07
datnd@B21AT056-DatND-VPNServer:~$
```

- Tạo một account mới với tên: datnd-b21dcat056 và mật khẩu: 1



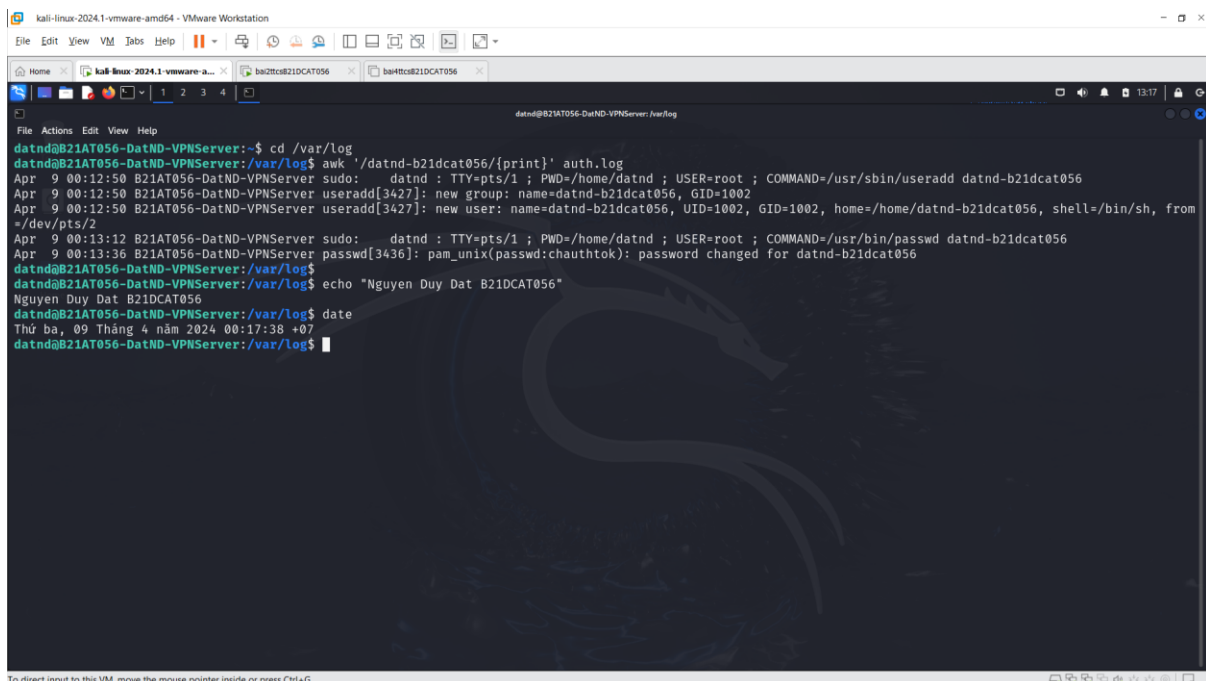
```
datnd@B21AT056-DatND-VPNServer:~$ sudo useradd datnd-b21dcat056
datnd@B21AT056-DatND-VPNServer:~$ sudo passwd datnd-b21dcat056
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
datnd@B21AT056-DatND-VPNServer:~$
datnd@B21AT056-DatND-VPNServer:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer:~$ date
Thứ ba, 09 Tháng 4 năm 2024 00:13:57 +07
datnd@B21AT056-DatND-VPNServer:~$
```

- Trên máy Linux Internal Victim, truy cập /var/log/ và dùng grep để lọc kết quả trong file auth.log



```
datnd@B21AT056-DatND-VPNServer: /var/log
datnd@B21AT056-DatND-VPNServer:~$ cd /var/log
datnd@B21AT056-DatND-VPNServer:/var/log$ cat auth.log | grep datnd-b21dcat056
Apr  9 00:12:50 B21AT056-DatND-VPNServer sudo:    datnd : TTY=pts/1 ; PWD=/home/datnd ; USER=root ; COMMAND=/usr/sbin/useradd datnd-b21dcat056
Apr  9 00:12:50 B21AT056-DatND-VPNServer useradd[3427]: new group: name=datnd-b21dcat056, GID=1002
Apr  9 00:12:50 B21AT056-DatND-VPNServer useradd[3427]: new user: name=datnd-b21dcat056, UID=1002, GID=1002, home=/home/datnd-b21dcat056, shell=/bin/sh,
from=/dev/pts/2
Apr  9 00:13:12 B21AT056-DatND-VPNServer sudo:    datnd : TTY=pts/1 ; PWD=/home/datnd ; USER=root ; COMMAND=/usr/bin/passwd datnd-b21dcat056
Apr  9 00:13:36 B21AT056-DatND-VPNServer passwd[3436]: pam_unix(passwd:chauthtok): password changed for datnd-b21dcat056
datnd@B21AT056-DatND-VPNServer:/var/log$
datnd@B21AT056-DatND-VPNServer:/var/log$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer:/var/log$ date
Thứ ba, 09 Tháng 4 năm 2024 00:15:28 +07
datnd@B21AT056-DatND-VPNServer:/var/log$
```

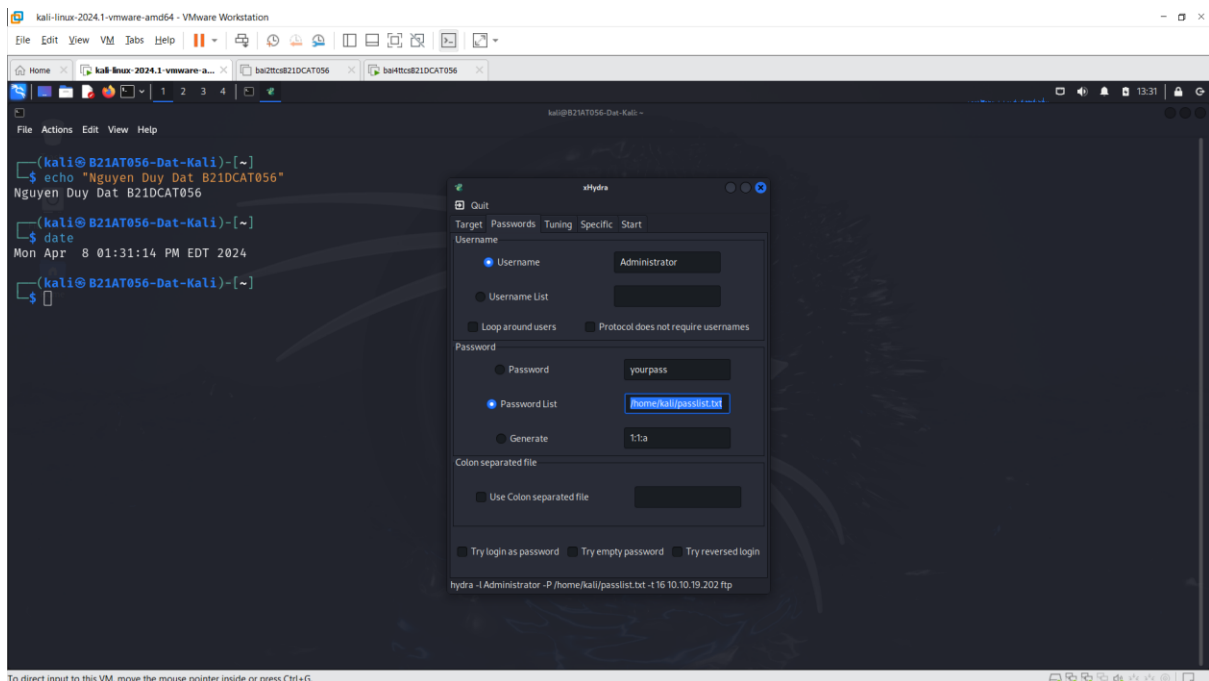
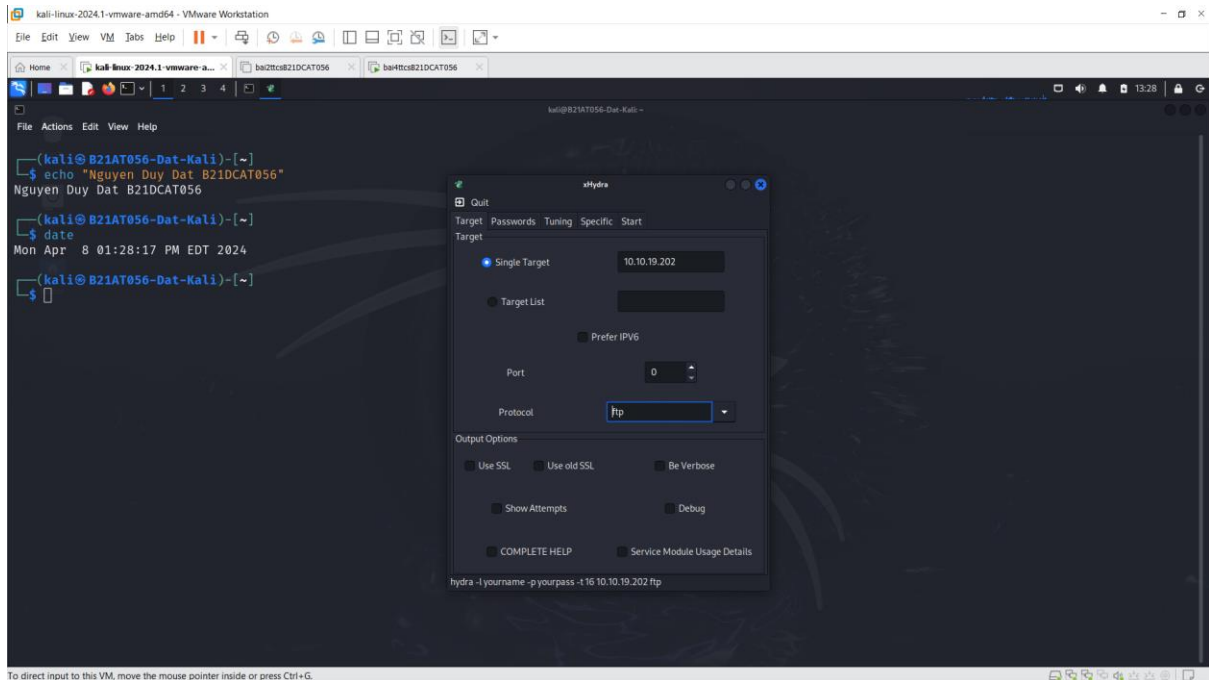
- Trên Kali, sử dụng awk để in ra các dòng có từ khóa datnd-b21dcat056 ra màn hình theo cú pháp: awk '/từ khóa/{print}' file

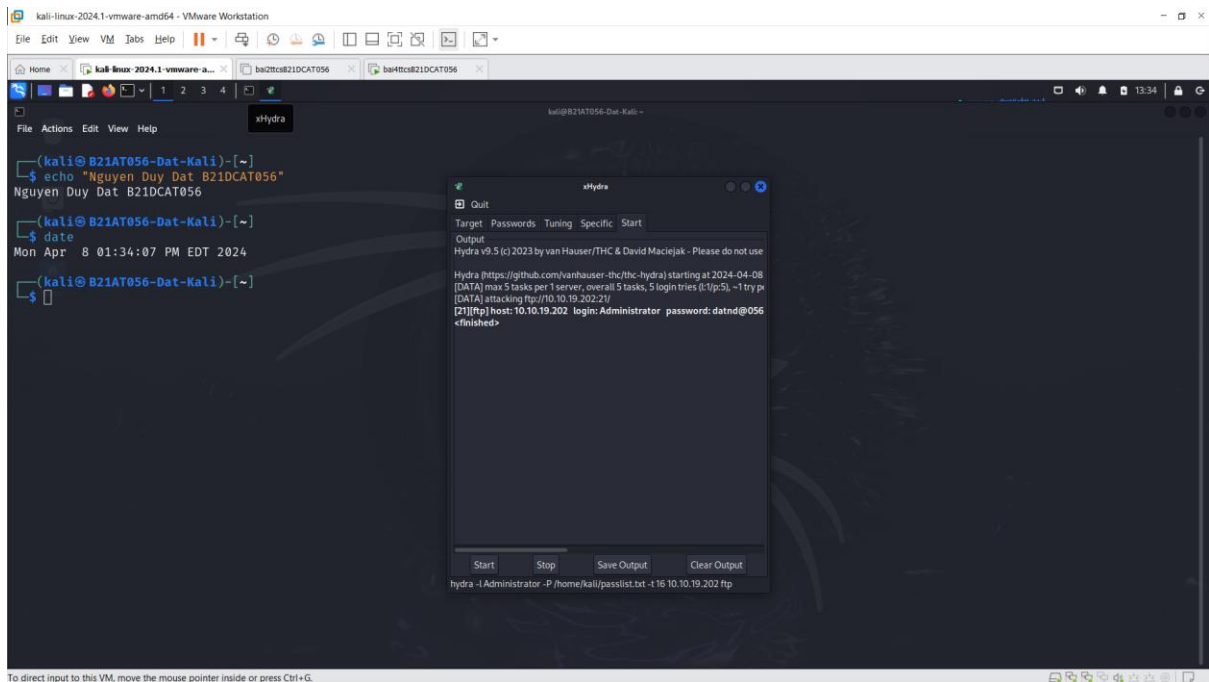


```
datnd@B21AT056-DatND-VPNServer:~$ cd /var/log
datnd@B21AT056-DatND-VPNServer:/var/log$ awk '/datnd-b21dcat056/{print}' auth.log
Apr  9 00:12:50 B21AT056-DatND-VPNServer sudo:    datnd : TTY=pts/1 ; PWD=/home/datnd ; USER=root ; COMMAND=/usr/sbin/useradd datnd-b21dcat056
Apr  9 00:12:50 B21AT056-DatND-VPNServer useradd[3427]: new group: name=datnd-b21dcat056, GID=1002
Apr  9 00:12:50 B21AT056-DatND-VPNServer useradd[3427]: new user: name=datnd-b21dcat056, UID=1002, GID=1002, home=/home/datnd-b21dcat056, shell=/bin/sh, from
=/dev/pts/2
Apr  9 00:13:12 B21AT056-DatND-VPNServer sudo:    datnd : TTY=pts/1 ; PWD=/home/datnd ; USER=root ; COMMAND=/usr/bin/passwd datnd-b21dcat056
Apr  9 00:13:36 B21AT056-DatND-VPNServer passwd[3436]: pam_unix(passwd:chauthtok): password changed for datnd-b21dcat056
datnd@B21AT056-DatND-VPNServer:/var/log$
datnd@B21AT056-DatND-VPNServer:/var/log$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@B21AT056-DatND-VPNServer:/var/log$ date
Thứ ba, 09 Tháng 4 năm 2024 00:17:38 +07
datnd@B21AT056-DatND-VPNServer:/var/log$
```


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:\inetpub\logs\LogFiles\FTPSVC4
Chọn file mới nhất để kiểm tra log

