

## Nội dung và hướng dẫn bài thực hành

### Mục đích

Giúp sinh viên tìm hiểu khái niệm về giám sát an toàn mạng, sử dụng ELK Stack để thu thập, phân tích log tấn công bruteforce mật khẩu và phát hiện các hoạt động đăng nhập bất thường trên các ứng dụng web.

### Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ ELK Stack, log xác thực và cách thức xây dựng ứng dụng web.

### Nội dung thực hành

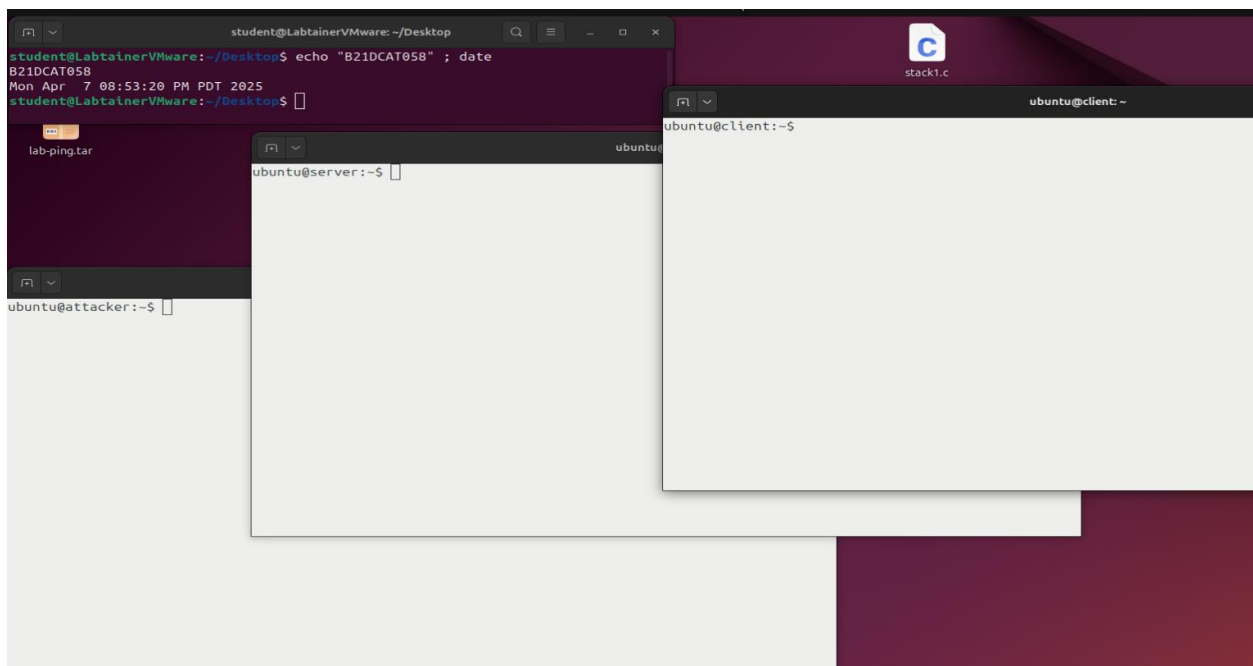
Khởi động bài lab:

Vào terminal, gõ:

```
startlab nsm-elk-bruteforce
```

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong ba terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: **attacker**, một cái là đại diện cho máy nạn nhân: **client**, một cái là đại diện cho máy giám sát: **server**.



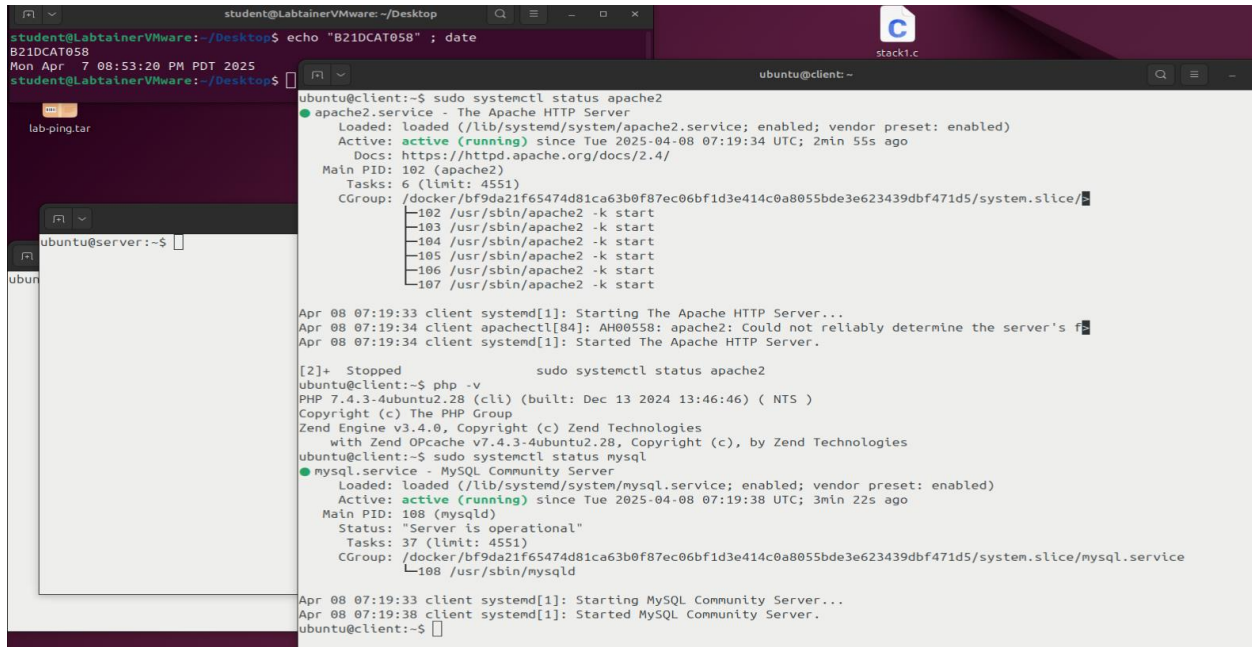
Trên terminal **client** thực hiện cấu hình máy chủ web apache để xây dựng ứng dụng web cần theo dõi.

Đầu tiên là kiểm tra các dịch vụ cho quá trình build web bằng các câu lệnh sau:

1. `sudo systemctl status apache2`

2. `php -v`

3. `sudo systemctl status mysql`



The screenshot shows a terminal window with the following output for `sudo systemctl status apache2`:

```
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-04-08 07:19:34 UTC; 2min 55s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 102 (apache2)
    Tasks: 6 (limit: 4551)
   CGroup: /docker/bf9da21f65474d81ca63b0f87ec06bf1d3e414c0a8055bde3e623439dbf471d5/system.slice/mys
            └─102 /usr/sbin/apache2 -k start
              └─103 /usr/sbin/apache2 -k start
                └─104 /usr/sbin/apache2 -k start
                  └─105 /usr/sbin/apache2 -k start
                    └─106 /usr/sbin/apache2 -k start
                      └─107 /usr/sbin/apache2 -k start

Apr 08 07:19:33 client systemd[1]: Starting The Apache HTTP Server...
Apr 08 07:19:34 client apachectl[84]: AH00558: apache2: Could not reliably determine the server's f
Apr 08 07:19:34 client systemd[1]: Started The Apache HTTP Server.

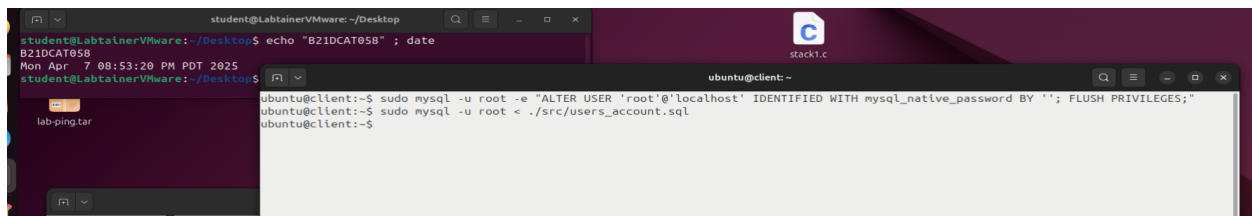
[2]+  Stopped                  sudo systemctl status apache2
ubuntu@client:~$ php -v
PHP 7.4.3-4ubuntu2.28 (cli) (built: Dec 13 2024 13:46:46) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3-4ubuntu2.28, Copyright (c), by Zend Technologies
ubuntu@client:~$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-04-08 07:19:38 UTC; 3min 22s ago
     Main PID: 108 (mysqld)
    Status: "Server is operational"
      Tasks: 37 (limit: 4551)
     CGroup: /docker/bf9da21f65474d81ca63b0f87ec06bf1d3e414c0a8055bde3e623439dbf471d5/system.slice/mysql.service
            └─108 /usr/sbin/mysqld

Apr 08 07:19:33 client systemd[1]: Starting MySQL Community Server...
Apr 08 07:19:38 client systemd[1]: Started MySQL Community Server.
ubuntu@client:~$
```

Tiếp theo thực hiện xây dựng cơ sở dữ liệu ứng dụng web:

1. `sudo mysql -u root -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY ''; FLUSH PRIVILEGES;"`

2. `sudo mysql -u root < ./src/users_account.sql`

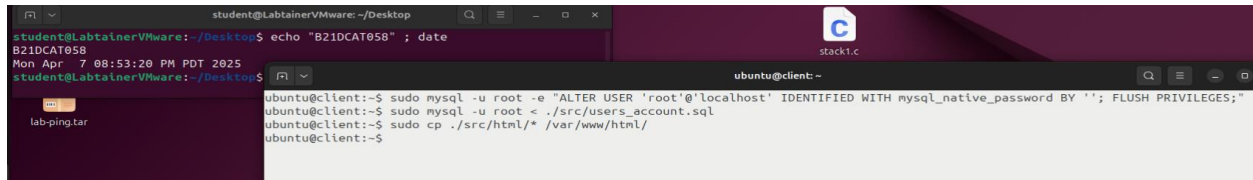


The screenshot shows a terminal window with the following output for the MySQL commands:

```
ubuntu@client:~$ sudo mysql -u root -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY ''; FLUSH PRIVILEGES;"
ubuntu@client:~$ sudo mysql -u root < ./src/users_account.sql
ubuntu@client:~$
```

Cuối cùng là tiến hành build source code ứng dụng web.

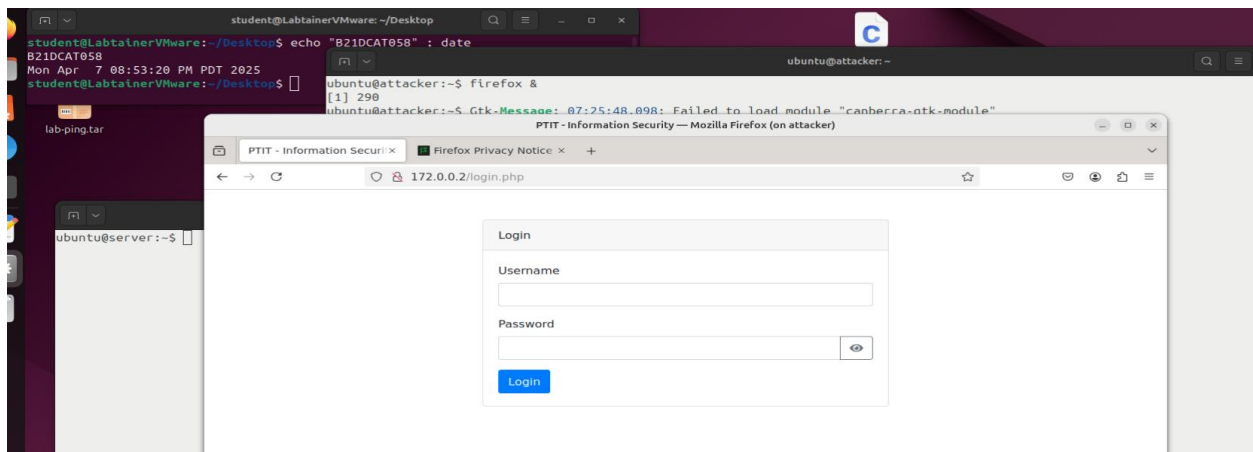
1. `sudo cp ./src/html/* /var/www/html/`



```
student@LabtainerVMware: ~/Desktop
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

ubuntu@client:~$ sudo mysql -u root -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY ''; FLUSH PRIVILEGES;"
ubuntu@client:~$ sudo cp ./src/html/* /var/www/html/
ubuntu@client:~$
```

Trên terminal **attack** thực hiện mở trình duyệt firefox (chạy câu lệnh “ `firefox &` ”) và truy cập ứng dụng web theo đường dẫn `http://172.0.0.2:80/index.php` để đảm bảo trang web hoạt động bình thường.



Quay lại trên terminal **client** thực hiện cấu hình Filebeat để gửi log xác thực đăng nhập tới máy giám sát và khởi động dịch vụ Filebeat.

`sudo nano /etc/filebeat/filebeat.yml`

Thêm vào path của nơi lưu log xác thực: `/var/log/apache2/*.log` cùng với ip, port Logstash của máy giám sát nhận log sau đó khởi động dịch vụ Filebeat.

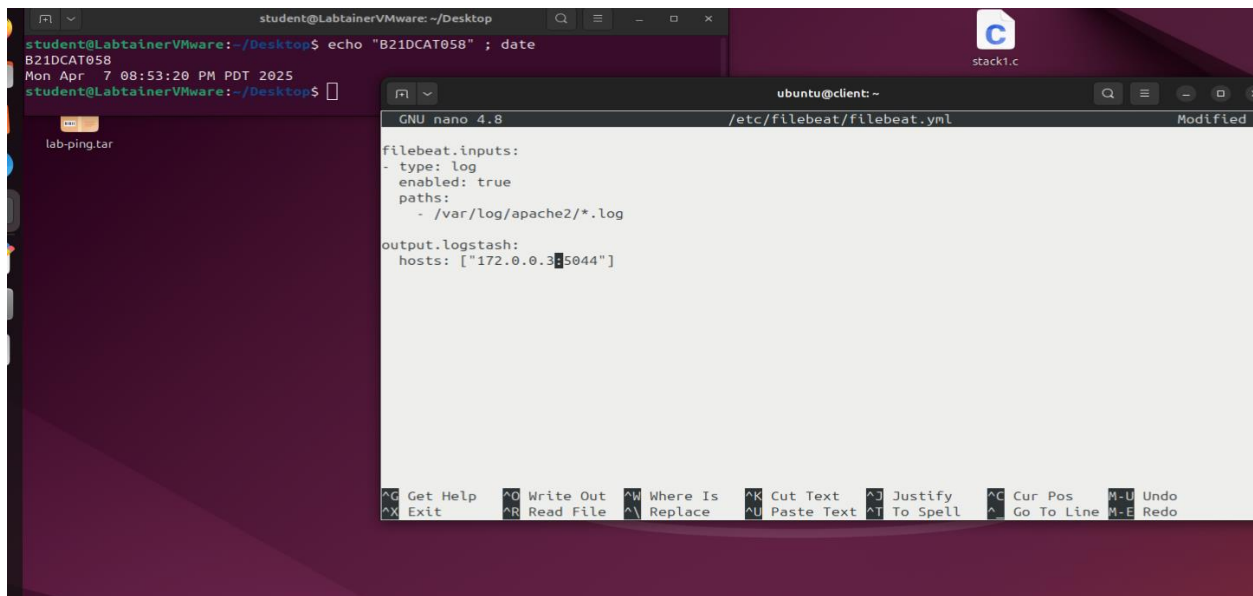
`sudo nano /etc/filebeat/filebeat.yml`

`“/var/log/apache2/access.log”`

`“Logstash: 172.0.0.3:5044”`

`sudo cat /etc/filebeat/filebeat.yml`

`sudo systemctl start filebeat`



Trên máy **server** thực hiện kiểm tra config và khởi động dịch vụ Elasticsearch, Kibana và Filebeat.

```
sudo cat /etc/logstash/conf.d/apache.conf
```

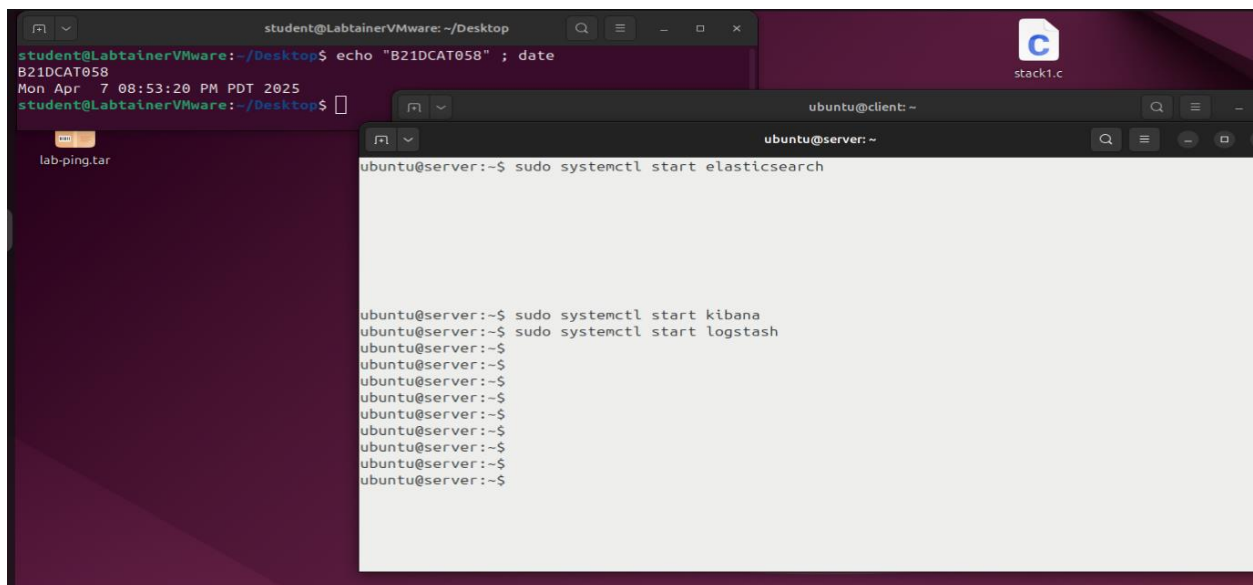
```
sudo cat /etc/kibana/kibana.yml
```

```
sudo cat /etc/elasticsearch/elasticsearch.yml
```

```
sudo systemctl start elasticsearch
```

```
sudo systemctl start kibana
```

```
sudo systemctl start logstash
```



Trên máy **attacker** dùng script python tấn công bruteforce mật khẩu “bruteforce\_passwd.py” cùng danh sách mật khẩu web phổ biến có sẵn để thực hiện tấn công bruteforce mật khẩu ứng dụng web. Trước tiên cài đặt môi trường và thư viện cần thiết cho quá trình tấn công. (Địa chỉ ứng dụng web: <http://172.0.0.2:80/index.php>)

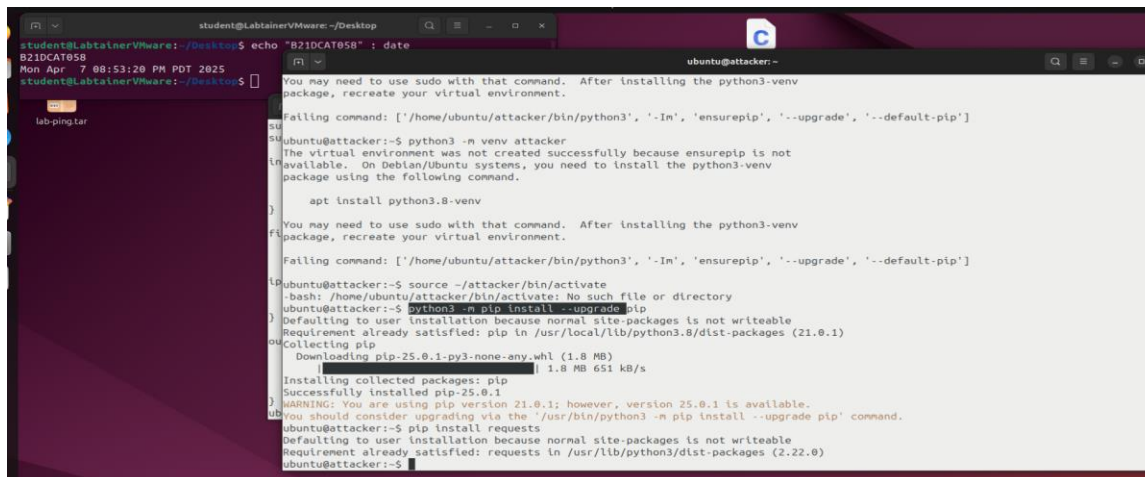
```
sudo apt-get install python3-venv
```

```
python3 -m venv attacker
```

```
source ~/attacker/bin/activate
```

```
python3 -m pip install --upgrade pip
```

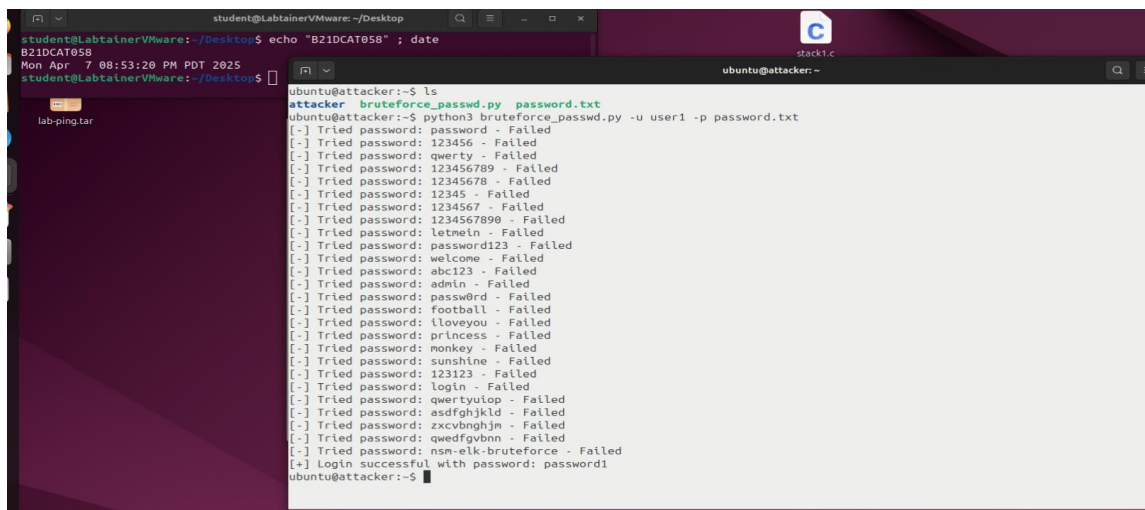
```
pip install requests
```



```
student@LabtainerVMware: ~/Desktop
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$ sudo apt-get install python3-venv
[sudo] password:
[sudo] student:
student@LabtainerVMware: ~/Desktop$ python3 -m venv attacker
student@LabtainerVMware: ~/Desktop$ source ~/attacker/bin/activate
attacker$ python3 -m pip install --upgrade pip
Requirement already satisfied: pip in /usr/local/lib/python3.8/dist-packages (21.0.1)
Collecting pip
  Downloading pip-25.0.1-py3-none-any.whl (1.8 MB)
    |#####| 1.8 MB 651 kB/s
Installing collected packages: pip
Successfully installed pip-25.0.1
WARNING: You are using pip version 21.0.1; however, version 25.0.1 is available.
You should consider upgrading via the '/usr/bin/python3 -m pip install --upgrade pip' command.
attacker$ pip install requests
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.22.0)
attacker$
```

Tấn công bằng câu lệnh tương ứng với script python:

```
python3 bruteforce_passwd.py -u user1 -p password.txt
```

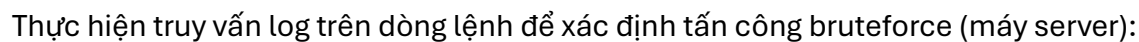


```
student@LabtainerVMware: ~/Desktop
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$ python3 bruteforce_passwd.py password.txt
attacker$ python3 bruteforce_passwd.py password.txt
attacker$ python3 bruteforce_passwd.py -u user1 -p password.txt
[-] Tried password: password - Failed
[-] Tried password: 123456 - Failed
[-] Tried password: qwerty - Failed
[-] Tried password: 123456789 - Failed
[-] Tried password: 12345678 - Failed
[-] Tried password: 12345 - Failed
[-] Tried password: 1234567 - Failed
[-] Tried password: 1234567890 - Failed
[-] Tried password: letmein - Failed
[-] Tried password: password123 - Failed
[-] Tried password: welcome - Failed
[-] Tried password: abc123 - Failed
[-] Tried password: admin - Failed
[-] Tried password: password - Failed
[-] Tried password: football - Failed
[-] Tried password: iloveyou - Failed
[-] Tried password: princess - Failed
[-] Tried password: monkey - Failed
[-] Tried password: sunshine - Failed
[-] Tried password: 123123 - Failed
[-] Tried password: login - Failed
[-] Tried password: qwertyuiop - Failed
[-] Tried password: asdfghjkl - Failed
[-] Tried password: zxcvbnghjm - Failed
[-] Tried password: qwedfgybnm - Failed
[-] Tried password: nsu-ek-bruteforce - Failed
[+] Login successful with password: password1
attacker$
```

*firefox &*

Trên máy CLIENT truy cập: 172.0.0.3:5601 xem log xác thực trong phần Discover (cần cấu hình 1 bước để nhận agent).

Trên máy CLIENT truy cập: 172.0.0.3:5601 xem log xác thực trong phần Discover (cần cấu hình 1 bước để nhận agent).



Xem log vừa truy vấn:

```
cat bruteforce.txt
```



```
student@LabtainerVMware: ~/Desktop
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

ubuntu@server:~$ cat bruteforce.txt | grep "message"
"message": "[Tue Apr 08 07:19:34.243380 2025] [core:notice] [pid 102] AH00094: Command line: '/usr/sbin/apache2'",
"message": "172.0.0.4 - - [08/Apr/2025:07:27:38 +0000] \"GET /favicon.ico HTTP/1.1\" 404 487 \"http://172.0.0.2/index.php\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:27:44 +0000] \"GET /login.php HTTP/1.1\" 200 1511 \"http://172.0.0.2/index.php\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0\"",
"message": "[Tue Apr 08 07:19:34.243319 2025] [mpm_prefork:notice] [pid 102] AH00163: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations",
"message": "172.0.0.4 - - [08/Apr/2025:07:27:38 +0000] \"GET /index.php HTTP/1.1\" 200 270 \"-\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:27:41 +0000] \"GET /login.php HTTP/1.1\" 200 1569 \"http://172.0.0.2/index.php\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=123456&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=12345&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=1234567890&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=password123&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=password&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=iloveyou&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=monkey&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=sunshine&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=123123&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=qwertyuiop&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=zxcvbnghjm&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\"",
"message": "172.0.0.4 - - [08/Apr/2025:07:45:31 +0000] \"GET /login.php?username=user1&password=password&login= HTTP/1.1\" 200 1647 \"-\" \"python-requests/2.22.0\""
```

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

```
stoplab nsm-elk-bruteforce
```

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

```
startlab -r nsm-elk-bruteforce
```

```
student@LabtainerVMware: ~/Desktop
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

ubuntu@client:~$

student@LabtainerVMware: ~/labtainer/labtainer-student
student@LabtainerVMware: ~/labtainer/labtainer-student$ checkwork
86 Results stored in directory: /home/student/labtainer_xfer/nsm-elk-bruteforce
6 Successfully copied 11400 to nsm-elk-bruteforce-1grader:/home/instructor/b21dcat058.nsm-elk-bruteforce.lab
Labname nsm-elk-bruteforce

Student | mysql-db | web-php | filebeat-path | filebeat-IP | logstash | elasticsearch | kibana | attack-password | bruteforce-logs |
B21dcat058 | | Y | Y | Y | Y | Y | Y | Y | Y |
6 What is automatically assessed for this lab:
0
1
2
```