# Nội dung và hướng dẫn thực hiện bài thực hành

## 1.1. Mục đích

* Giúp sinh viên hiểu về công cụ khai thác lỗ hổng: Nmap, Hydra
* Cách sử dụng công cụ để thực hiện một cuộc tấn công

## 1.2. Yêu cầu đối với sinh viên

* Tìm hiểu khái niệm, ứng dụng, các sử dụng của các công cụ khai thác lỗ hổng: Nmap, Hydra
* Hiểu biết về khái niệm cơ bản về file mã nguồn: đọc hiểu và có thể biên dịch file mã nguồn
* Hiểu cách thức truy cập từ xa từ client đến server
* Các biện pháp khắc phục

## 1.3. Nội dung thực hành

* Khởi động bài lab:

Tải bài lab: imodule https://github.com/ctdinh10x/ptit-ssh-unpass/raw/main/imodule.tar

* + Vào terminal, gõ:

*labtainer ptit-ssh-unpass -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 xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: ***client***, một cái là đại diện cho máy chủ: ***server.*** Biết rằng 2 máy nằm cùng mạng LAN 172.20.0.0/24.

***client*** có địa chỉ IP là 172.20.0.10

***server*** có địa chỉ IP là 172.20.0.20

* Truy cập vào server bằng ssh và sử dụng mật khẩu:

*ssh ubuntu@<IP Server>*

Ví dụ: ip máy là 172.20.0.20 IP mạng LAN cần điền là 172.20.0.0/24

* Thêm các config vào file sshd\_config

PubkeyAuthentication yes

PasswordAuthentication no

PermitRootLogin no

* Client tiến hành ssh lại truy cập vào server và nhận thấy không đủ quyền
* Do không đủ quyền nên client tiến hành gen key để chuẩn bị gửi sang cho server

*ssh-keygen*

* Client gửi key sang cho server nhưng không thành công do server bắt buộc phải copy key để gửi sang

*ssh-copy-id*

* Client tiến hành cat key ra để gửi cho server

*cat ~/.ssh/id\_rsa.pub*

* Server tiến hành tạo file ~/.ssh/authorized\_keys và add key của client vào file đo

*mkdir ~/.ssh/authorized\_keys*

* Sau khi được add key client tiến hành ssh lại vào server mà không cần mật khẩu

*ssh ubuntu@<IpServer>*

***Kết thúc bài lab:***

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

stoplab ptit-ssh-unpass

* 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 –r ptit-ssh-unpass

Chú ý: cần restart ssh sau khi cấu hình xong

Nếu xung đột thì fix theo cách sau: sửa file /etc/xinetc.d/ssh đổi disable = no thành disable = yes

sudo systemctl reload xiented

sudo system start ssh