Nội dung và hướng dẫn thực hiện bài thực hành

## 1.1. Mục đích

- Giúp sinh viên hiểu về công cụ snort

- Tìm hiểu về bảo mật mạng

- Tìm hiểu về các công cụ liên quan đến tấn công mật khẩu như crunch, hydra, hashcat.

- Thực hành với công cụ nmap, crunch, snort.

- Nâng cao kỹ năng phân tích và giải quyết vấn đề

- Tăng cường ý thức về trách nhiệm và đạo đức

## 1.2. Yêu cầu đối với sinh viên

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

## 1.3. Nội dung thực hành

* Tải bài lab:

imodule https://github.com/hieunm2025/TTTN-2025/raw/refs/heads/main/ptit-snort-detect/imodule.tar

* Khởi động bài lab:
  + Vào terminal, gõ:

*labtainer -r ptit-snort-detect*

*(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 ba terminal ảo sẽ xuất hiện, các terminal này đại diện cho máy ảo để sinh viên tiến hành thực hiện trên đó.

* Sinh viên tiến hành quét cổng mở của máy server bằng công cụ nmap:

*sudo nmap 172.25.0.3 -sS*

* Sinh viên tạo ra hai file, một file trong đó là danh sách các tài khoản thông thường được sử dụng và một file là danh sách các mật khẩu hay được dùng:

*crunch <số lượng ít nhất của tài khoản> <số lượng kí tự nhiều nhất> -o <tên file>*

*crunch <số lượng ít nhất của mật khẩu> <số lượng kí tự nhiều nhất> -o <tên file>*

*Vào /etc/shadow ở terminal server, tìm hash của tài khoản server và dùng công cụ hashcat để crack mật khẩu, tìm hiểu xem hash của nó thuộc loại mã hash nào, hashcat dùng chế độ nào để crack nó?*

*Sau đó đem vào bộ danh sách vào hydra để checkwork thành công.*

* Sinh viên thực hiện tạo file luật và thêm luật snort trên máy server để phát hiện các cuộc tấn công brute force theo đường dẫn */etc/snort/rules/<tentapluat>*
* Sinh viên tiến hành tấn công bằng hydra trên máy client

*hydra -L <tên file tài khoản> -P <tên file mật khẩu> 172.25.0.3 ssh*

* Sau khi bruteforce thành công có được tài khoản, mật khẩu từ máy client sinh viên thực hiện ssh vào máy server:

*ssh <username>@172.25.0.3*

* Sau khi ssh thành công sinh viên thực hiện đọc file:

*cat /root/filetoview.txt*

* Sinh viên cấu hình iptables trên máy firewall để chặn lưu lượng cổng 22
* Sinh viên thực hiện tạo file luật snort trên máy server để phát hiện cuộc tấn công XSS theo đường dẫn */etc/snort/rules*
* Sinh viên thêm luật snort trên máy server để phát hiện cuộc tấn công SQLinjection theo đường dẫn thư mục */etc/snort/rules/<tentapluat>*
* Sinh viên truy cập vào website theo địa chỉ http://*172.25.0.3/dvwa* và tiến hành tấn công SQLInjection
* Sau khi tấn công snort sẽ phát hiện và đưa ra cảnh báo
* Sinh viên thực hiện tạo file luật trên máy server để phát hiện cuộc tấn công XSS theo đường dẫn */etc/snort/rules*
* Sinh viên thực hiện thêm luật snort trên máy server để phát hiện cuộc tấn công XSS theo đường dẫn thư mục */etc/snort/rules/<tentapluat>*
* Sinh viên truy cập vào website theo địa chỉ http://*172.25.0.3/dvwa* và tiến hành tấn công XSS
* Sau khi tấn công snort sẽ phát hiện và đưa ra cảnh báo

A screenshot of a computer

Description automatically generated.



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

