# Nội dung và hướng dẫn thực hiện bài thực hành

# Mục đích

* + - Giúp sinh sinh viên hiểu các kiểu scan trong nmap
    - Sử dụng công cụ hydra để tấn công vết cạn
    - Sử dụng công cụ hping3 để tấn công từ chối dịch vụ
    - Thực hành cấu hình và viết rule trong suricata

# Yêu cầu đối với sinh viên

Có kiến thức về hệ điều hành Linux.

# Nội dung thực hành

* + - Sinh viên tải lab tại: <https://github.com/nguyenductuan12/suricata>
    - Thực hiện cập nhập thời gian trên máy ubuntu đúng với thời gian thực để có thể tải lab về
    - Khởi động bài lab: Vào terminal gõ:

*labtainer -r lab\_suricata*

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

Sau khi khởi động xong, 2 terminal ảo sẽ suất hiện, một cái là đại diện cho máy server: **server**, một cái là đại diện cho máy attacker: **attacker**. Biết rằng 2 máy này nằm trong cùng một dải mạng và máy attacker đã biết được địa chỉ IP của máy **server** để có thể thực hiện nmap scan các dịch vụ trên máy server.

* Thực hiện cập nhập thời gian trên máy ubuntu đúng với thời gian thực để có thể tải lab về
* Trên máy server thực hiện cấu hình suricata qua đường dẫn

/etc/suricata/suricata.yaml.

* + Thực hiện cấu hình dải mạng cần giám sát, vì 2 máy nằm cùng dải mạng nên thực hiện cấu hình trường “**HOME\_NET”**
  + Thực hiện cấu hình đường đẫn đến file quy tắc mà Suricata sẽ áp dụng để phát hiện và cảnh báo, cấu hình tại trường “**rule-files”**
* Khởi động lại service suricata để cập nhập cấu hình
* Cập nhập các tập luật đã có sẵn và tập luật tự định nghĩa. Các tệp luật có sẵn trong suricata sau khi thực hiện câu lệnh sẽ được tải về đường dẫn cấu hình rule mà đã định nghĩa bên trên.

*suricata-update*

* Tạo 1 file tự định nghĩa các rule riêng trong thư mục đã định nghĩa trong cấu hình
* Tham khảo hướng dẫn sử dụng suricata rules tại: <https://docs.suricata.io/en/latest/rules/index.html>
* Sau mỗi lần định nghĩa rule mới khởi động lại service suricata để áp dụng rule mới vào để phát hiện
* Xem cảnh báo phát hiện nmap scan trong file fast.log trên máy **victim**

*tail -f /var/log/suricata/fast.log*

* Viết rule trên máy **victim** thực hiện phát hiện scan nmap quét cổng dịch vụ tcp với thông điệp cảnh báo sau: “POSSBL SCAN NMAP KNOWN TCP (type -sT) - {MSV}”. Trong đó MSV là mã sinh viên

Ví dụ: *alert tcp $HOME\_NET any -> $HOME\_NET any (msg:”POSSBL SCAN NMAP KNOWN TCP (type -sT)”; flow:stateless; classtype: attempted-recon; sid:1000001; threshold:type limit, track by\_src, sount 10, seconds 300; dsize:0;)*

* Trên máy **attacker** thực hiện quét cổng dịch vụ tcp

*sudo nmap -sT <IP\_victim>*

* Viết rule thực hiện trên máy **victim** phát hiện scan nmap quét cổng dịch vụ udp với thông điệp sau: “POSSBL SCAN NMAP KNOWN UDP (type

-sU) - {MSV}”. Tham khảo đường link trên

* Trên máy **attacker** thực hiện quét cổng dịch vụ udp

*sudo nmap -sU -T5 <IP\_victim>*

* Viết rule thực hiện phát hiện tấn công icmp flood trên máy **victim** với thông điệp như sau:”POSSBL DOS ICMP PACKET FLOOD – {MSV}”.
* Trên máy **attacker** sử dụng công cụ hping3 để tấn công dos vào server

*sudo hping3 -1 --flood <IP\_victim>*

* Viết rule thực hiện phát hiện tấn công brute-force dịch vụ ssh trên máy

**victim** với thông điệp như sau: ”POSSBL SSH BRUTE FORCING! –

{MSV}”. Tham khảo đường link trên

* Trên máy **attacker** thực hiện burte-force bằng công cụ hydra

*hydra -L username.txt -P passlist.txt ssh://<IP\_victim>*

* Sử dụng password và username vừa lấy được, tải file từ **victim** về và đọc file trên máy **attacker**

- Kết thúc bài lab:

Trên terminal đầu tiên, sử dụng câu lệnh *checkwork* để kiểm tra kết quả bài lab, sau đó để đóng bài lab, sử dụng lệnh *stoplab.*

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 lab\_suricata*