

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**--🙣🕮🙡--**

**BÁO CÁO CUỐI KỲ**

**MÔN KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG**

**Tóm tắt demo phòng thủ DDOS bằng pfSense**

**Giảng Viên: *Sam Nguyen Xuan***

**Sinh Viên thực hiện:**

***Chế Công Hậu N17DCAT023 – D17CQAT01-N***

***Nguyễn Thịnh Phát N17DCAT053 – D17CQAT01-N***

**TPHCM – Ngày 24/5/2021**

1. **Chuẩn bị trước khi thực hiện demo phòng thủ.**

Thực hiện:

1. Cài đặt **Firewall pfSense**, thiết lập các card mạng và cấu hình cơ bản tường lửa.
2. Đăng nhập **Web Configurator** của **pfSense** bằng cách truy cập vào mạng LAN.
3. Cài đặt **Snort** (nếu chưa cài đặt) : Chọn menu System – Package Manager. Ở Package Manager, truy cập vào Available packages tab. Ở Available packages tab, tìm **Snort** và install package **Snort**. Bấm Install và chờ đợi tiến trình cài đặt hoàn thành.
4. Cấu hình **Snort** trên **pfSense**. Truy cập menu Services và chọn Snort.
5. Ở tab setting Global, chọn Snort Subscriber Rules và thực hiện những cấu hình sau :

* Enable Snort VRT – Yes
* Snort Oinkmaster Code – Enter you OikCode

1. Nếu không có Oinkcode, hãy truy cập trang web của **Snort**, tạo account và lấy Oinkcode miễn phí.
2. Truy cập Rules Update Settings, và thực hiện những cấu hình sau :

* Update Interval – chọn khoảng thời gian gửi gói tin update Interval
* Update Start Time – chọn khoảng thời gian để update Snort rules

1. Đến General Settings và thực hiện những cấu hình sau :

* Remove Blocked Hosts Interval – 1 Hour
* Remove Blocked Hosts After Deinstall – No
* Keep Snort Settings After Deinstall – Yes
* Startup/Shutdown LoggingUpdate Interval – no

1. Ở mục Updates tab, bấm vào nút Updates rules để download Rule **Snort**.
2. Ở tab **Snort**, bấm vào nút add và thực hiện những cấu hình sau :

* Enable – Yes
* Interface – chọn Interface chạy dịch vụ **Snort**

1. Đến mục Alert Settings, và thực hiện những cấu hình sau :

* Send Alerts to System Log – Yes
* Block Offenders – Bật nếu muốn
  + Kill States – Yes
  + Which IP to Block – BOTH

1. Sau khi kết thúc cấu hình, bấm vào nút Save. Ở màn hình giao diện **Snort**, tiến hành edit Interface :
2. Truy cập tab Wan, và thực hiện những cấu hình sau :

* Resolve Flowbits – Yes
* Use IPS Policy – Yes
* IPS Policy Selection – Connectivity hoặc Security (hoặc ta có thể chọn những rules cụ thể ta muốn, khi đó thì phải tắt Use IPS Policy)

1. Sau khi kết thúc cấu hình, bấm vào nút Save, và Start service **Snort** ở Interface này.
2. **Phòng thủ phát hiện Nmap Scan Port bằng Rule Snort của PfSense.**

Chuẩn bị: Sử dụng Rules Snort của **Firewall pfSense** để phát hiện hacker scan port bằng **nmap**.

Thực hiện:

1. Đăng nhập **Web Configurator** của **pfSense** bằng cách truy cập vào mạng LAN.
2. Chọn Services – Snort – Edit WAN Interface.
3. WAN Rules – Chỉnh sửa custom Rule :

**alert tcp any any -> $HOME\_NET any (msg: “NMAP TCP Scan”;sid:10000005; rev:2;)** – đây là rule để alert khi có người nmap TCP.

**alert udp any any -> $HOME\_NET any (msg: “NMAP UDP Scan”;sid:10000006; rev:2;)** – đây là rule để alert khi có người nmap UDP.

1. Restart lại WAN Interface.
2. Thực hiện nmap tới pfSense cả TCP và UDP.
3. Xem phần Alerts của Snort để kiểm tra.
4. **Phòng thủ phát hiện, ngăn chặn hacker DDOS**

Chuẩn bị: Sử dụng **Kali** **Linux** và mã độc để tấn công DDOS botnet – bot. Sử dụng Rules Snort của **Firewall pfSense** để phát hiện, ngăn chặn hacker **DDOS**.

Thực hiện:

1. Đăng nhập **Web Configurator** của **pfSense** bằng cách truy cập vào mạng LAN.
2. Chọn Services – Snort – Edit WAN Interface.
3. WAN Categories – chọn **emerging-dos.rules**, **snort\_ddos.rules** và **snort\_dos.rules** – Save.
4. WAN Rules – kiểm tra lại các rules ta vừa chọn**.** Vào Test Port xem đã mở cổng 80 chưa.
5. Thực hiện nmap WAN để check cổng
6. git clone <https://github.com/Leeon123/Aoyama>
7. Thực hiện tấn công **DDOS** (kiểu botnet – bot)
8. Kiểm tra lại CPU ở bot chạy thành công hay chưa.
9. Kiểm tra lại CPU ở **pfSense**
10. Kiểm tra phần **Alerts** của **Snort** và phần **Blocked** của **Snort**

Đã Alert và block IP của máy bot đang DDOS

Ghi chú : cần đợi thời gian cho tường lửa phát hiện và ngăn chặn.