🎬 Cấu trúc video demo (gợi ý 8–10 phút)

✅ 1. Giới thiệu chung (30 giây – 1 phút)

Thuyết minh:  
Chào thầy/cô và các bạn sau đây em xin giới thiệu sơ qua về thanh viên nhóm, tên đề tài và kịch bản nhóm em đã triển khai

Đầu tiên Nhóm em gồm 3 thành viên :

Nguyễn Trọng Hùng

Hà Văn Sang

Phạm Văn Khánh

Đề tài bài tập lớn nhóm em là Tìm hiểu, cài đặt và triển khai phần mềm bảo mật pfSense

trong video này, nhóm chúng em sẽ demo kịch bản so sánh giữa trước và sau khi triển khai pfSense kết hợp Snort để ngăn chặn tấn công từ chối dịch vụ (DDoS) vào Web Server."

Trong bài Nhóm em có 2 mô hình

🖼️ Hiển thị sơ đồ mạng

Mô hình 1 – Trước khi triển khai pfSense

Mô hình 2 – Sau khi triển khai pfSense + Snort để phát hiện và ngăn chặn tấn công

Đầu tiên em sẽ Triển khai Mô hình 1 – Trước khi triển khai pfSense

Về cơ bản em sẽ dử dụng 1 máy Kali có cùng dải mạng với WEb Server

Tiến hành suđể tấn công từ chối dịch vụ vào WEb Server Va sẽ khiến WEB bị treo và không phản hồi được

Sau đây là các bước em triển khai thực tế

Bước 1 : Em sẽ kiểm thử trạng thái của webserver trước khi tấn công :

Lúc này WEB Sẻver hoatj dộng bình thường.

Bước 2 Tiến Hành Sử dụng Kali để tấn công từ chối dịch vụ dạng Slowloris vào webserver

Lúc này WEb sẻ ver5 Web bị treo và không thể truy cập   
Lý do : Hacker đã gửi lượng lớn request vào Web Server. Đẫn đến việc treo và không thể truy cập được

🖼️ Hiển thị sơ đồ mạng mới

Tiếp theo em sẽ nâng cao phòng thủ cho webserver Bằng cách Sử dụng Mô hình 2 – Mô hình Sau khi triển khai pfSense + Snort để phát hiện và ngăn chặn tấn công

Tổng quan Pfsen em có cấu hình :  
Cấu hình các luật (Rules) trên pfsense co phép Cổng Nat forward vào webserver.

Cấu hình interface card wan được cấp DHCP từ nat của VMware

Cấu hình Lan có gateway : 192.168.30.1 để static ip v4

Cấu hình port-forwarding được thực hiện sao cho các máy bên ngoài có thể truy cập Web Server thông qua địa chỉ NAT của PFsense.

Cài đặt snort trên pfsense. Cấu hình để tự động chặn các cuộc tấn công vào bên trong dải mạng

Về việc Cài đặt Snort trên PFsense thì em vào Packset mánerger vào available packages tiến hành tìm kiếm và tải về. sau khi tải về tải về em sẽ tiến hành cấu hình snort

Tiến hành thêm interface Wan để snort theo dõi trên card wan.

Tiếp theo em sẽ cấu hình interface Wan. Em sẽ bật thêm thông báo để snort ghi lại log hệ thống về các cuộc tấn công, tiếp theo em sẽ bật tự động block các tấn công ,sau đó em thêm các rule có sẽn trên hệ thống snort. nhằm ngăn chặn tấn công từ chối dịch vụ từ bên ngoài. VD : dos, scan.

🛠️ Demo thực tế

Cau khi cấu hình xong Pfsense vá snort em sẽ tiến hành tấn công từ chối dịch vụ từ máy kali vào WEBServer

Sau đây là các bước em triển khai thực tế

Bước 1 : Em sẽ kiểm thử trạng thái của webserver trước khi tấn công

Lúc này WEB Sẻver hoatj dộng bình thường.

Bước 2 Tiến Hành Sử dụng Kali để tấn công từ chối dịch vụ dạng Slowloris vào webserver

Đổi dịa chỉ ip của Kali sao cho cùng dải địa chỉ với PFSENSE

Máy Kali tiến hành tấn công Slowloris vào Web Server.

Lúc này WEb Server vẫn hoạt động bình thường

Lý do

Snort nhanh chóng phát hiện và chặn các gói tin tấn công từ nguồn là Máy Kali có địa chỉ là 20.20.20.3 , đảm bảo Web Server vẫn hoạt động bình thường. đồng thời các máy khác vẫn có thể truy cập Web Server.

Trừ máy tấn công Kali đã bị chặn địa chỉ IP

Cơ bản là Sau khi cài triển khai biện pháp phòng thủ thì kẻ tấn công sẽ không thể tấn công bằng phương pháp DDOS nữa.

Tổng kết (30 giây – 1 phút)

Thuyết minh:  
"Qua kịch bản này, chúng em chứng minh được vai trò quan trọng của pfSense và Snort trong việc bảo vệ hệ thống mạng. Việc triển khai tường lửa mã nguồn mở giúp giảm thiểu rủi ro và nâng cao an toàn cho hệ thống."

📌 Tips khi làm video

| Việc cần làm | Gợi ý |
| --- | --- |
| Quay màn hình | Dùng OBS Studio hoặc ScreenRec |
| Ghi âm/thuyết minh | Dùng micro rời hoặc ghi sau rồi chèn vào |
| Phụ đề | Có thể thêm bằng CapCut, Camtasia hoặc Premiere |
| Thời lượng | Tổng dưới 10 phút, lý tưởng khoảng 7–8 phút |
| Tên file | video\_demo\_pfsense\_groupX.mp4 (ghi rõ để dễ nộp bài) |