HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr-suricata-synflood

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: IDR-SURICATA-SYNFLOOD

1. Mục đích

- Sinh viên sẽ có được kiến thức trong việc phát hiện, cảnh báo và phản ưungs trước các cuộc tấn công SYN Flood với việc kết hợp hệ thống giám sát Suricata và cơ chế chặn lưu lượng tại host bằng iptables.

2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux.
- Nắm được kiến thức cơ bản về tấn công từ chối dịch vụ (DoS), đặc biệt là cơ chế tấn công SYN Flood và quy trình bắt tay 3 bước của TCP.
- Có kiến thức nền tảng về bảo mật hệ thống, về các công cụ Suricata và iptables.

3. Nội dung bài lab

- Chạy lệnh sau để thêm bài vào labtainer:

imodule https://github.com/anhdnmit/do_an_tot_nghiep/raw/refs/heads/main/idr-suricata-synflood/idr-suricata-synflood.tar

- Khởi động bài lab:

labtainer -r idr-suricata-synflood

(chú ý: sinh viên sử dụng mã sinh viên 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, một máy đại diện cho máy nạn nhân **victim**, hai máy **attacker** để thể hiện hai kiểu tấn công.
- Để kiểm tra địa chỉ IP của 3 máy, gõ lệnh sau trên từng máy:

ifconfig

3.1. Cài đặt Suricata trên máy nạn nhân

- Tại máy **victim,** thêm PPA stable của Suricata và cài đặt Suricata:

sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt update

sudo apt install suricata -y

- Sau khi cài đặt thành công, kiểm tra lại phiên bản Suricata đã cài đặt:

suricata -V

- Kiểm tra địa chỉ để biết interface đang dùng:

ip a

3.2. Cấu hình Suricata và tạo rule phát hiện tấn công SYN Flood

- Mở file cấu hình Suricata:

sudo nano /etc/suricata/suricata.yaml

- Tìm khóa HOME_NET và đổi thành dải mạng của bài lab là 200.20.0.0/24 để Suricata xác định được mạng cần bảo vệ:

HOME_NET: "[200.20.0.0/24]"

- Chuyển sang user root để thao tác trong thư mục /etc/suricata:

sudo su

cd /etc/suricata

- Tạo thư mục chứa rule tùy chỉnh:

mkdir rules

- Tạo file rule mới:

sudo nano /etc/suricata/rules/ddos.rules

- Thêm dòng rule này vào file:

alert tcp any any -> $HOME_NET 80 (msg:"ALERT: Detected SYN Flood DoS Attack"; flags:S; flow:stateless; threshold: type both, track by_dst, count 50, seconds 10; sid:1000001; rev:1;)

- Ý nghĩa:
    - flag:S => Chỉ bắt gói TCP SYN
    - flow:stateless => SYN Flood không theo flow chuẩn
    - threshold => Giới hạn tần suất để xác định tấn công (50 SYN/10 giây tới webserver)
    - track by_dst: Theo dõi địa chỉ bị tấn công
    - sid: ID rule

⇨ Rule nay giúp Suricata phát hiện lượng lớn SYN bất thường, dấu hiệu SYN Flood.

- Mở lại file /etc/suricata/suricata.yaml và thêm đường dẫn tới file rule mới trong phần rule-files:

rule-files:

- /etc/suricata/rules/ddos.rules

- Cập nhật và nạp lại rule database của Suricata:

sudo suricata-update

- Khởi động lại dịch vụ Suricata để áp dụng thay đổi:

sudo systemctl restart suricata

3.3. Kiểm tra dịch vụ web và cấu hình kernel liên quan TCP syncookies

- SYN Flood thường nhắm vào web server nên cần xác nhận port 80 đang hoạt động. Kiểm tra trạng thái dịch vụ nginx:

sudo systemctl status nginx

- Tắt tcp_syncookies để dễ dàng quan sát ảnh hưởng của tấn công:

sudo sysctl -w net.ipv4.tcp_syncookies=0

- Kiểm tra log Suricata để theo dõi cảnh báo:

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

3.4. Thực hiện tấn công SYN Flood cơ bản, phát hiện và phản ứng sự cố

- Trên máy **attacker,** dùng hping3 để gửi hàng nghìn SYN/giây để làm server của máy **victim** quá tải**:**

sudo hping3 -S -p 80 –flood <địa chỉ IP máy victim>

- Lúc này, log của Suricata sẽ hiển thị cảnh báo rằng máy có IP 200.20.0.30 đang thực hiện tấn công SYN Flood nhắm vào cổng web (80) của máy chủ 200.20.0.10:

[**] [1:1000001:1] ALERT: Detected SYN Flood DoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 200.20.0.30:1902 -> 200.20.0.10:80

- Chạy lệnh sau để kiểm tra phản hồi của web server trên máy **victim:**

curl -I localhost

- Nếu hoạt động bình thường sẽ hiện: HTTP/1.1 200 OK
- Nếu bị tấn công SYN Flood thì web server sẽ bị treo và hiển thị thông báo: Connection timed out

- Ấn Ctrl + C trên máy **attacker** để kết thúc tấn công.
- Khi biết hệ thống đang bị tấn công, **victim** tạm thời chặn địa chỉ IP máy **attacker** bằng iptables:

sudo iptables -A INPUT -s 200.20.0.30 -j DROP

- Kiểm tra lại danh sách iptables xem đã chặn đúng chưa:

sudo iptables -L -n

- Khởi động lại nginx để kiểm tra lại dịch vụ sau khi chặn:

sudo systemctl restart nginx

curl -I localhost

3.5. Thực hiện tấn công SYN Flood có kích thước bất thường, phát hiện và phản ứng sự cố

- Chỉnh sửa lại file rule /etc/suricata/rules/ddos.rules để thêm rule phát hiện SYN packet có payload (dsize > 0):

alert tcp any any -> $HOME_NET 80 (msg:"ALERT: Detected SYN Packet Containing Payload (Abnormal Behavior)"; flags:S; dsize:>0; flow:stateless; sid:1000002; rev:1;)

- Ý nghĩa:
  - flag:S => Chỉ bắt gói TCP SYN
  - dsize:>0 => Nếu thấy SYN có payload thì gần như chắc chắn là tấn công
  - flow:stateless => SYN Flood không theo flow chuẩn
  - sid: ID rule
- Cập nhật Suricata và khởi động lại dịch vụ để áp dụng rule mới:

sudo suricata-update

sudo systemctl restart suricata

- Bật theo dõi log cảnh báo:

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

- Trên máy **attacker2,** thực hiện chạy tấn công có payload và dùng nguồn ngẫu nhiên:

sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source <IP máy victim>

- Lúc này, log của Suricata sẽ hiển thị cảnh báo phát hiện một gói tin SYN có chứa dữ liệu bên trong (đây là hành vi bất thường trái với chuẩn giao thức TCP). Tuy nhiên, mỗi lần cảnh báo thì lại là một địa chỉ IP khác nhau do kẻ tấn công dùng địa chỉ nguồn ngẫu nhiên:

[**] [1:1000002:1] ALERT: Detected SYN Packet Containing Payload (Abnormal Behavior) [**] [Classification: (null)] [Priority: 3] {TCP}

- Chạy lệnh sau để kiểm tra phản hồi của web server trên máy **victim:**

curl -I localhost

  - Nếu hoạt động bình thường sẽ hiện: HTTP/1.1 200 OK
  - Nếu bị tấn công SYN Flood thì web server sẽ bị treo và hiển thị thông báo: Connection timed out
- Thực hiện chặn những TCP SYN có chiều dài lớn hơn 100 bytes:

sudo iptables -A INPUT -p tcp --syn -m length --length 100:65535 -j DROP

- Kiểm tra danh sách rule iptables xem đã chặn đúng chưa

sudo iptables -L -n -v

- Ấn Ctrl + C trên máy **attacker2** để kết thúc tấn công.
- Kích hoạt lại tcp_syncookies:

sudo sysctl -w net.ipv4.tcp_syncookies=1

- Kiểm tra lại:

sudo sysctl net.ipv4.tcp_syncookies

- Khởi động lại nginx để kiểm tra lại dịch vụ sau khi chặn:

sudo systemctl restart nginx

curl -I localhost

- Kết thúc bài lab:

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

stoplab idr-suricata-synflood

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 idr-suricata-synflood