HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr-suricata-portscanning

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: IDR-SURICATA-PORTSCANNING

1. Mục đích

- Sinh viên sẽ có được kiến thức trong việc phát hiện, cảnh báo và phản ứng trước các hành vi quét cổng với việc kết hợp hệ thống giám sát Suricata và cơ chế phản ứng tự động của Fail2ban.

2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux.
- Nắm được kiến thức cơ bản về các kỹ thuật quét cổng, đặc biệt là SYN scan và UDP scan.
- Có kiến thức nền tảng về bảo mật hệ thống, về các công cụ Suricata và Fail2ban.

3. Nội dung bài lab

- Khởi động bài lab:

labtainer -r idr-suricata-portscanning

(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 hành vi quét cổng

- Mở file cấu hình Suricata:

sudo nano /etc/suricata/suricata.yaml

- Tìm khóa HOME_NET và đổi thành dải mạng của bài lab là 220.10.0.0/24 để Suricata xác định được mạng cần bảo vệ:

HOME_NET: "[220.10.0.0/24]"

- 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/local.rules

- Thêm dòng rule này vào file:

alert tcp any any -> $HOME_NET any (msg:"PORTSCAN DETECTED - TCP SYN scan"; flags:S; threshold:type both, track by_src, count 10, seconds 5; sid:1000001; rev:1;)

alert udp any any -> $HOME_NET any (msg:"PORTSCAN DETECTED - UDP scan"; threshold:type both, track by_src, count 10, seconds 5; sid:1000004; rev:1;)

⇨ Hai rule giám sát hành vi quét cổng, giám sát số lượng gói tin bất thường từ một nguồn và tạo cảnh báo khi số lượng truy cập port quá nhiều trong một thời gian ngắn.

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

rule-files:

- /etc/suricata/rules/local.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. Cài đặt Fail2ban và config để phản ứng tự động dựa trên alert của Suricata

- Cài đặt Fail2ban:

sudo apt install fail2ban -y

- Tạo filter cho Fail2ban để bắt alert của Suricata:

sudo nano /etc/fail2ban/filter.d/suricata-ports.conf

- Viết các nội dung sau vào file:

[Definition]

failregex = ^."signature":"PORTSCAN DETECTED.*".*"src_ip":"<HOST>".*$*

ignoreregex =

- Ý nghĩa:
    - Failregex: regex dùng để tìm dòng alert trong file eve.json của Suricata. Regex này trích src_ip từ JSON alert khi signature chứa chuỗi "PORTSCAN DETECTED". Khi trùng khớp, Fail2ban sẽ thực hiện chặn.
- Chạy lệnh để cấu hình hành động của filter:

sudo nano /etc/fail2ban/jail.d/suricata-ports.conf

- Viết các nội dung sau vào file:

[suricata-ports]

enabled = true

filter = suricata-ports

logpath = /var/log/suricata/eve.json

maxretry = 1

findtime = 60

bantime = 600

backend = auto

banaction = iptables-multiport

- Ý nghĩa:
  - logpath: Trỏ tới file eve.json của Suricata
  - maxretry=1: Một alert trùng filter là đủ để chặn
  - findtime=60: Khoảng thời gian kiểm tra
  - bantime=600: Thời gian chặn
  - banaction=iptables-multiport: Dùng iptables để block.
- Sau khi cấu hình xong, khởi động lại Fail2ban:

sudo systemctl restart fail2ban

3.4. Thực hiện quét cổng và kiểm tra phản ứng sự cố

- Trên máy **victim,** kiểm tra log Suricata để theo dõi cảnh báo:

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

- Tại máy **attacker,** chạy lệnh nmap để quét cổng TCP SYN:

sudo nmap -sS 220.10.0.10

- Quay trở lại máy **victim** và thấy có hiện cảnh báo. **Victim** dừng theo dõi và kiểm tra trạng thái jail để xem IP của **attacker** đã bị chặn quét cổng chưa:

sudo fail2ban-client status suricata-ports

- **Victim** có thể xem trong danh sách iptables có địa chỉ của **attacker:**

sudo iptables -L -n

- Trên máy **victim,** quay lại kiểm tra log Suricata để theo dõi cảnh báo:

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

- Tại máy **attacker2,** chạy lệnh nmap để quét cổng UDP:

sudo nmap -sU 220.10.0.10

- Quay trở lại máy **victim** và thấy có hiện cảnh báo. **Victim** dừng theo dõi và kiểm tra trạng thái jail để xem IP của **attacker** đã bị chặn quét cổng chưa:

sudo fail2ban-client status suricata-ports

- **Victim** có thể xem trong danh sách iptables có địa chỉ của **attacker:**

sudo iptables -L -n

- Kết thúc bài lab:

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

stoplab idr-suricata-portscanning

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-portscanning