HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr_suricata_ossec_dnstunneling

Sinh viên thực hiện: Đào Ngọc Ánh

Mã sinh viên: B21DCAT038

Hà Nội 2025

Phát hiện và ứng phó: DNS-based C2 sử dụng subdomain dài

1.1.1. Giới thiệu chung

Trong bài thực hành này, sinh viên sẽ tìm hiểu về kỹ thuật DNS Tunneling (DNS-based C2) – một phương pháp attacker dùng để che giấu kết nối Command & Control (C2) qua các gói DNS, từ đó vượt qua firewall, proxy và IDS truyền thống.

Malware sẽ liên tục gửi các DNS Query chứa payload mã hóa (base64) với subdomain dài bất thường (>50 ký tự) để duy trì kết nối với máy C2.

Sinh viên sẽ triển khai Suricata để phát hiện, và sử dụng OSSEC để điều tra & thực hiện phản ứng (Active Response) như:

- Tự động chặn IP/domain của attacker
- Ghi lại incident timeline
- Cô lập Client bị nhiễm (mô phỏng thực tế)

1.1.2. Mục đích

Sau khi hoàn thành lab, sinh viên sẽ:

Mục tiêu	Kỹ năng đạt được
Hiểu cơ chế DNS Tunneling & C2	Phân tích DNS Payload
Nhận biết truy vấn DNS bất thường	Subdomain dài, tần suất cao
Viết Suricata rule để phát hiện	IDS baselining & signature
Phân tích log bằng OSSEC	SIEM cơ bản
Thực hiện ứng phó tấn công	Active Response thực tế

1.1.3. Yêu cầu đối với sinh viên

Sinh viên cần hiểu

- Khái niệm DNS Query, DNS Record, Subdomain
- Cách dùng tcpdump / tail / grep
- Hiểu file log JSON (eve.json của Suricata)
- Kiến thức Incident Response cơ bản
- Cách dùng iptables firewall

1.1.4. **Nội dung thực hành**

- Tải bài lab :

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

- Khởi động bài lab:

labtainer -r idr_suricata_ossec_dnstunneling

(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	Gửi DNS C2 Payload
client	Máy bị nhiễm malware (gửi beacon liên tục)
server	DNS server + Suricata + OSSEC server

- Để kiểm tra địa chỉ IP của 3 máy, gõ lệnh sau trên từng máy:

ifconfig

1.1.4.1. ***Tạo traffic DNS tunneling***

a. Trên máy Attacker – gửi DNS beacon

cd /home/ubuntu

chmod +x dns_c2.py

python3 dns_c2.py &

tail -f dns_c2.log

b. Trên máy client, sinh viên thực hiện

cd /home/ubuntu

Sau khi server chạy ifconfig, chỉnh dòng này đúng IP của máy server:

DNS_SERVER = "10.0.5.10" # đổi thành IP của server thật!

python3 dns_beacon.py &

chmod +x dns_beacon.py

ps aux | grep dns_beacon

1.1.4.2. *Cài đặt suricata*

Trên máy server, sinh viên thực hiện cài đặt suricata

sudo apt-get update -y

sudo apt-get install software-properties-common -y

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

 # NHẤN "ENTER" KHI ĐƯỢC HỎI

sudo apt-get update -y

sudo apt-get install suricata -y

suricata -V

Sau đó khởi động Suricata dạng sensor

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 &

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

ps aux | grep suricata >> /home/ubuntu/prestop.stdout

1.1.4.3. *Viết rule phát hiện DNS Tunneling*

Sinh viên tạo thư mục chứa rule và viết rule trong đó

sudo mkdir -p /etc/suricata/rules

sudo nano /etc/suricata/rules/local.rules

THÊM DUY NHẤT 1 DÒNG RULE (LUÔN TRÊN 1 LINE):

Ví dụ

alert dns any any -> any any (msg:"Possible DNS Tunneling"; dns.query; pcre:"/[A-Za-z0-9]{50,}\\./"; sid:400001; rev:1;)

Sau đó sinh viên kiểm tra suricata đã load rule thành công

sudo nano /etc/suricata/suricata.yaml

Tìm rule-files: → sửa thành:

rule-files:

- /etc/suricata/rules/local.rules

Bên cạnh đó tắt hoàn toàn AF_PACKET:

(THÊM dấu # vào hết block này)

#af-packet:

 # - interface: eth0

 # cluster-id: 5

 # cluster-type: cluster_flow

 # defrag: yes

Test lại bằng câu lệnh sau

sudo suricata -T -c /etc/suricata/suricata.yaml

sudo suricata -T -c /etc/suricata/suricata.yaml >> /home/ubuntu/prestop.stdout 2>&1

sau đó sinh viên cat để check log

cat /home/ubuntu/prestop.stdout

Nếu hiện *Configuration provided was successfully loaded.* -> thành công

chạy lệnh để kiểm tra và ghi lại log

ps aux | grep suricata

ps aux | grep suricata >> /home/ubuntu/prestop.stdout

1.1.4.4. *Tấn công và kiểm tra Suricata Alert*

Sinh viên thực hiện câu lệnh sau để chạy và kiểm tra alert của Suricata

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 &

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

Trên container client, thực hiện

dig $(head -c 60 /dev/urandom | tr -dc 'a-z0-9').malicious-domain.com @<IP_SERVER>

Nếu thấy trong `fast.log`:

Possible DNS Tunneling

Là đã thành công

1.1.4.5. *Cài đặt OSSEC*

OSSEC cần biên dịch từ mã nguồn nên cần cài các gói build-essential, các thư viện liên quan và inotify-tools để hỗ trợ theo dõi thay đổi file. Tại máy **server,** sinh viên chạy lệnh sau để cài đặt các gói cần thiết:

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

Tạo và truy cập vào thư mục chứa mã nguồn OSSEC:

mkdir ossec_src

cd ossec_src

Tải mã nguồn OSSEC từ github:

sudo apt update

sudo apt install wget -y

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

Sau khi tải xong, sinh viên giải nén và truy cập vào thư mục đã giải nén:

tar -xvzf 3.7.0.tar.gz

cd ossec-hids-3.7.0

Sử dụng quyền root và chạy lệnh để cài đặt OSSEC:

sudo su

./install.sh

Trong quá trình cài đặt, sinh viên cần trả lời các câu hỏi sau:

Ngôn ngữ: en (English)

Chọn loại cài đặt: server

Xác nhận thư mục cài đặt: /var/ossec

Cấu hình các tính năng:

- Email notification: n

- Integrity check daemon (syscheck): y (Module theo dõi thay đổi file quan trọng)
- Rootkit detection: y
- Active response: y
- Bật firewall-drop: y
- Whitelist: n
- Remote syslog: y

Sau khi trả lời xong các câu hỏi, sinh viên ấn nút enter và đợi hệ thống cài đặt. Cài đặt thành công, sinh viên ấn nút enter để kết thúc quá trình cài đặt.

Khởi động OSSEC:

/var/ossec/bin/ossec-control start

Chạy lệnh sau để thêm agent vào server:

sudo /var/ossec/bin/manage_agents

Tại đây, sinh viên làm theo các bước sau:

Chọn "A" để mở tính năng thêm agent.

Đặt tên cho agent.

Nhập địa chỉ IP của máy agent.

Nhập ID cho agent.

Nhấn y để xác nhận thêm vào danh sách.

Quay lại menu, chọn "E" để tạo key cho agent.

Nhập ID của agent, hệ thống sẽ sinh ra key cho agent.

Nhập "Q" để thoát khỏi hệ thống.

- Sinh viên chuyển sang máy **client** và thực hiện cài đặt các gói cần thiết để cài đặt OSSEC:

sudo apt update

sudo apt install dnsutils -y

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

- Tạo và di chuyển vào thư mục chứa mã nguồn OSSEC:

mkdir ossec_src

cd ossec_src

- Tải mã nguồn OSSEC từ github:

  sudo apt update

  sudo apt install wget -y

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

- Giải nén và truy cập thư mục đã giải nén:

  tar -xvzf 3.7.0.tar.gz

  cd ossec-hids-3.7.0

- Sử dụng quyền root và chạy lệnh cài đặt OSSEC:

  sudo su

  ./install.sh

- Trong quá trình cài đặt, sinh viên cần trả lời các câu hỏi sau:
  - Ngôn ngữ: en (English)
  - Chọn loại cài đặt: agent
  - Chọn thư mục cài đặt: /var/ossec
  - Cấu hình OSSEC HIDS:
    - Địa chỉ IP của máy server
    - Integrity check daemon: y
    - Rootkit detection: y
    - Active response: y
- Sau khi trả lời xong các câu hỏi, sinh viên ấn enter để bắt đầu cài đặt. Cài đặt xong, sinh viên ấn enter để kết thúc quá trình cài đặt.
- Tạo file rids để tránh lỗi agent:

  touch /var/ossec/queue/rids/sender

- Để kết nối agent với server, sinh viên chạy lệnh sau:

  sudo /var/ossec/bin/manage_agents

- Tại đây, sinh viên làm theo các bước sau:
  - Nhập “I” để nhập key do hệ thống bên server sinh ra.
  - Dán key mà OSSEC server vừa nhận được.
  - Xác nhận thêm vào.
  - Nhập “Q” để thoát khỏi hệ thống.

- Khởi động lại agent:

/var/ossec/bin/ossec-control start

- Chạy lệnh sau để kiểm tra agent đã kết nối với server (có hiện dòng Connected to <địa chỉ IP server>):

cat /var/ossec/logs/ossec.log

Sinh viên kiểm tra và sử dụng bằng việc chạy

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

Nếu thấy

ossec-execd: INFO: Started

Thì là ossec start thành công

1.1.4.6. *OSSEC phát hiện DNS Tunneling*

a. Tạo rule OSSEC

sudo mkdir /var/ossec/rules

sudo nano /var/ossec/rules/local_rules.xml

Sau đó thêm rule, ví dụ

```
<group name="dns,tunnel,attack">
 <rule id="900500" level="10">
  <match>Possible DNS Tunneling</match>
  <description>dns_tunnel_alert</description>
 </rule>
</group>
```

Mở file cấu hình:

sudo nano /var/ossec/etc/ossec.conf

Thêm vào cuối phần *<ossec_config>:*

```
<localfile>
 <log_format>full_command</log_format>
 <location>/var/log/suricata/fast.log</location>
```

</localfile>

Sau khi thêm rule, sinh viên thực hiện restart bằng lệnh sau

sudo /var/ossec/bin/ossec-control restart

Sau đó check log

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

1.1.4.7. *Active Response - ngăn chặn tấn công*

Sinh viên thực hiện trên máy server để tự động chặn truy cập DNS

sudo iptables -A OUTPUT -p udp --dport 53 -j DROP

sudo iptables -L -n

1.1.4.8. *Kết thúc bài lab*

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

stoplab idr_suricata_ossec_dnstunneling

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_dnstunneling