# Hướng dẫn: Thu thập log từ VM1 → VM2 bằng rsyslog (Host-only)

Mô tả ngắn: VM1 là nguồn log (ngồn Apache / file attacker\_access.log). VM2 là collector (chạy rsyslog), lắng nghe TCP/UDP 514 và lưu các dòng log gốc.

Lưu ý: Chạy trong môi trường lab. Thay IP VM2 nơi cần (VM2\_IP).

1. **Trên VM2 (Collector) — cấu hình nhận log**

# Tạo thư mục chứa log nhận từ VM1

sudo mkdir -p /var/log/remote # Tạo thư mục /var/log/remote

sudo chown syslog:adm /var/log/remote # Gán quyền sở hữu cho user syslog, group adm

sudo chmod 750 /var/log/remote # Quyền: syslog đọc/ghi, adm đọc, others không có quyền

# Tạo file cấu hình để bật chế độ nhận log qua UDP & TCP port 514

sudo tee /etc/rsyslog.d/50-receiver.conf > /dev/null <<'EOF'

module(load="imudp"); input(type="imudp" port="514") # Bật module UDP, lắng nghe cổng 514

module(load="imtcp"); input(type="imtcp" port="514") # Bật module TCP, lắng nghe cổng 514

template(name="OnlyMsg" type="string" string="%msg%\n") # Định nghĩa template: chỉ lấy nội dung log, bỏ metadata(timestamp, hostname, tag) để giống với log đầu vào của file read\_mix\_logs.py

\*.\* action(type="omfile" file="/var/log/remote/access.log" template="OnlyMsg") # Ghi tất cả log vào file access.log theo template

EOF

# Tạo file log đích & phân quyền

sudo touch /var/log/remote/access.log

sudo chown syslog:adm /var/log/remote/access.log

sudo chmod 0640 /var/log/remote/access.log # Quyền: syslog đọc/ghi, adm đọc

# Khởi động lại rsyslog để áp dụng cấu hình

sudo systemctl restart rsyslog

# Kiểm tra rsyslog có lắng nghe cổng 514 không

sudo ss -tulnp | grep 514 || true

## 2. Trên VM1 (Source) — cấu hình imfile và forward

# --- Forward Apache access.log sang VM2 ---

VM2\_IP="192.168.198.138"

# 1) Cài và bật Apache

sudo apt update -y

sudo apt install -y apache2

sudo systemctl enable apache2

sudo systemctl start apache2

# 2) Tạo file cấu hình rsyslog

sudo tee /etc/rsyslog.d/50-forward-apache.conf > /dev/null <<EOF

module(load="imfile" PollingInterval="10")

input(type="imfile"

File="/var/log/apache2/access.log"

Tag="apache-access:"

Severity="info"

Facility="local6"

PersistStateInterval="200"

ReadMode="0"

)

\*.\* @@${VM2\_IP}:514

EOF

# 3) Đảm bảo rsyslog có quyền đọc file access.log

sudo usermod -aG adm syslog

# 4) Kiểm tra cấu hình rsyslog

sudo rsyslogd -N1

# 5) Restart rsyslog để áp dụng

sudo systemctl restart rsyslog

sudo systemctl status rsyslog --no-pager

## 3. Tạo log test & Kiểm tra end-to-end

**Trên VM1 (gửi test):**echo '203.0.113.45 - - [21/Sep/2025:10:15:32 +0700] "GET /index.html HTTP/1.1" 200 1024' | sudo tee -a /var/log/attacker\_access.log  
# hoặc gửi syslog test  
logger -t TEST-FORWARD "RSYSLOG TEST FROM VM1 $(date)"

**Trên Kali Linux:**

1. Gửi 1 request đơn giản:

curl -v http://VM1\_IP/

1. Gửi 10 request nhanh (không hiển thị nội dung):

for i in {1..10}; do curl -s -o /dev/null http://VM1\_IP/; done

1. Gửi 100 request với header khác (để dễ lọc trong log):

for i in {1..100}; do curl -s -o /dev/null -A "kali-test/$i" http://VM1\_IP/; done

1. Nếu muốn thử tải 10 concurrent (cần apache2-utils để có ab):

sudo apt update && sudo apt install -y apache2-utils

ab -n 200 -c 10 http://VM1\_IP/

1. Gửi request tới 1 đường dẫn cụ thể:

curl -s -o /dev/null "http://VM1\_IP/somepage.html?x=1"

**Trên VM2 (xem kết quả):**sudo tail -f /var/log/remote/access.log

4. Sửa lỗi

sudo rsyslogd -N1

để kiểm tra cú pháp.

Nếu có lỗi, đọc journalctl -u rsyslog -n 200 để biết chi tiết.