HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr_wazuh_zeek_smb

Sinh viên thực hiện: Đào Ngọc Ánh

Mã sinh viên: B21DCAT038

Hà Nội 2025

Phát hiện và ứng phó: Lateral Movement (SMB)

1. Giới thiệu chung

Bài thực hành này mô phỏng kịch bản lateral movement trong mạng nội bộ qua giao thức SMB. Mục tiêu là giúp bạn học cách giám sát lưu lượng nội bộ, phát hiện hành vi quét/điều tra SMB, kết hợp log mạng (Zeek) và log host (Wazuh) để phân tích sự cố, rồi thực hiện các biện pháp ứng phó (containment, eradication, recovery).

2. Mục đích

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

- Giải thích cơ chế lateral movement qua SMB và dấu hiệu mạng/host liên quan
- Dùng Zeek để phát hiện quét port / hành vi SMB bất thường
- Dùng Wazuh để thu alert host-based (failed auth, process lạ, file change).
- Thực hiện quy trình ứng phó sự cố: xác minh, cô lập, loại bỏ và phục hồi
- Viết báo cáo điều tra ngắn

3. Yêu cầu đối với sinh viên

Sinh viên cần

- Có kiến thức cơ bản về Linux (bash, systemctl, iptables/ufw).
- Hiểu sơ TCP/IP, port 445 (SMB).
- Biết sử dụng tcpdump, nmap, cat, grep.

4. Nội dung thực hành

- Sinh viên tải bài lab:

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

- Khởi động bài lab:

labtainer -r idr_wazuh_zeek_smb

(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 5 container:

attacker, victim1, victim2, victim3, wazuh-server.

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

ifconfig

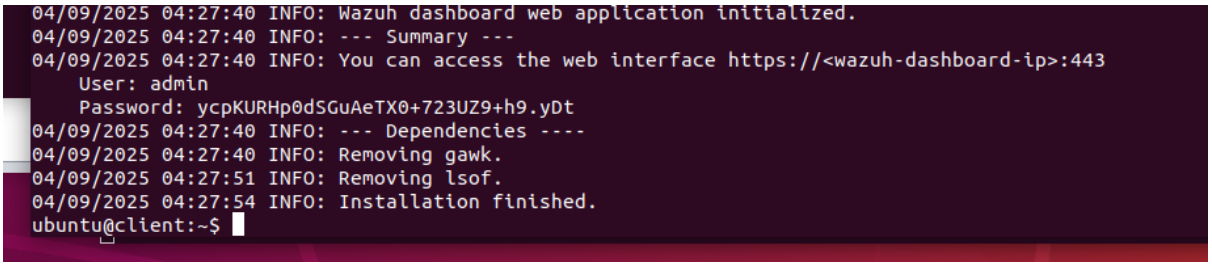
1. *Chuẩn bị môi trường trong lab*

a. Trên terminal wazuh_server (Cài Wazwuh Manager)

sudo apt update && sudo apt install curl -y

sudo apt install --only-upgrade firefox

curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a



 # chờ quá trình hoàn tất (~20–30 phút)

firefox &

Mở dashboard Wazuh với Firefox để xem alert sau này.

b. Trên victim2 và victim3 (Cài Wazuh agent để chúng gửi log về server phục vụ phân tích và phát hiện sự cố)

- Bước 1: Lấy lệnh cài Agent từ Wazuh Dashboard

Trên container **wazuh-server**, mở Firefox:

firefox

curl -I https://<IP-wazuh-server>

Sau đó truy cập: *https://<IP của wazuh-server>*

Sau đó đăng nhập bằng tài khoản mặc định sau khi cài đặt thành công wazuh được cung cấp

Ví dụ như trên

User: admin

Password: qR9mw1YIo*EMXHp1RsbpSQIwTfulQ*be

Trong Dashboard:

1. Vào Wazuh -> Agents
2. Nhấn Add agent
3. Chọn:

- Hệ điều hành : Linux
- Distribution: Ubuntu/Debian

4. Dashboard sẽ tạo một đoạn script cài đặt agent, dạng:

curl -sO https://packages.wazuh.com/4.12/wazuh-agent-4.12.0.deb

sudo WAZUH_MANAGER="<IP_wazuh-server>" dpkg -i ./wazuh-agent-4.12.0.deb

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

Sinh viên copy toàn bộ script này, lưu lại để dùng trên victim2 và victim3

- Bước 2: Chuẩn bị hệ thống trên victim2 /victim3

Update hệ thống

sudo apt update

Cài package lsb-release (yêu cầu bởi agent):

sudo apt install lsb-release -y

Đảm bảo SSH hoạt động

sudo systemctl stop xinetd # nếu hệ thống đang chạy xinetd

sudo systemctl enable ssh

sudo systemctl start ssh

- Bước 3: Chạy lệnh cài đặt Wazuh

Trên victim2:

curl -sO https://packages.wazuh.com/4.12/wazuh-agent-4.12.0.deb

sudo WAZUH_MANAGER="10.0.0.50" dpkg -i ./wazuh-agent-4.12.0.deb

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

Làm tương tự trên victim3

Sau đó kiểm tra agent cài đặt thành công bằng lệnh

sudo systemctl status wazuh-agent

- Bước 4: Xác nhận Agent đã kết nối về Server

Quay lại **Dashboard** trên wazuh-server → mục **Agents**.

Sẽ thấy

Agent “victim2” → status: Active

Agent “victim3” → status: Active

Ngoài ra có thể kiểm tra trực tiếp bằng lệnh:

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

Nếu kết nối thành công sẽ có log:

Agent <ID> successfully connected

Bước 5: Kiểm tra Alert gửi lên server

Để xác nhận agent gửi log:

Trên victim2/victim3 tạo thử failed ssh login (dùng user sai):

ssh wronguser@localhost

Trên server:

cat /var/ossec/logs/alerts/alerts.json

Hoặc xem trên Dashboard:

Wazuh → Security events → filter theo agent “victim2” hoặc “victim3”.

Bạn sẽ thấy alert như:

authentication failure

c. Trên victim1 (Cài đặt Zeek)

Thêm repository Zeek:

curl -s https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key | sudo apt-key add -

echo "deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /" | sudo tee /etc/apt/sources.list.d/zeek.list

Cài đặt Zeek:

sudo apt update

sudo apt install zeek -y

Kiểm tra:

zeek --version

Khởi động Zeek sau khi cài

sudo zeekctl deploy

Kiểm tra log

ls /opt/zeek/logs/current

Xác nhận Zeek đã hoạt động : *ps aux | grep zeek*

Kiểm tra port SMB Scan

grep 445 /opt/zeek/logs/current/conn.log

2. *Mô phỏng sự cố*

Mục đích: Tạo dấu vết để thực hành phát hiện & phản ứng. Thực hiện các lệnh mô phỏng từ container attacker hoặc victim1 (nếu mô phỏng pivot).

- Bước 1: Quét mạng nội bộ tìm máy mở port SMB(445)

nmap -p445 -sT 10.0.0.21-22 -oN /home/ubuntu/nmap_scan.txt

Giải thích :

- -p445 → quét cổng SMB
- -sT → TCP connect scan (an toàn, không phá hoại)
- -oN → lưu output vào file để phân tích
- 10.0.0.21-22 → quét victim2 & victim3

Vai trò trong bài lab:

- Tạo traffic SMB scan, Zeek sẽ bắt trong conn.log
- File nmap_scan.txt sẽ được ghi lại để phục vụ checkwork
- Đây là bước reconnaissance trong lateral movement
- Bước 2: Liệt kê share SMB trên từng nạn nhân

Kiểm tra SMB share trên victim2

smbclient -L //10.0.0.21 -N > /home/ubuntu/smb_enum_v21.txt 2>&1

Kiểm tra SMB share trên victim 3

smbclient -L //10.0.0.22 -N > /home/ubuntu/smb_enum_v22.txt 2>&1

Đọc kết quả

cat /home/ubuntu/nmap_scan.txt

cat /home/ubuntu/smb_enum_v21.txt

cat /home/ubuntu/smb_enum_v22.txt

- Bước 4 : Quan sát log mạng bằng Zeek

cat /opt/zeek/logs/current/conn.log | grep 445

cat /opt/zeek/logs/current/weird.log

- Bước 5: quan sát alert từ Wazuh

Trên victim2/victim3

cat /var/ossec/logs/alerts/alerts.json | tail -n 20

3. *Giám sát và phát hiện*

a. *Dùng Zeek (trên victim1)*

ls /opt/zeek/logs/current

cat /opt/zeek/logs/current/conn.log | tail -n 50

cat /opt/zeek/logs/current/weird.log | tail -n 50

cat /opt/zeek/logs/current/smb_files.log | tail -n 50

b. Dùng packet capture (tùy chọn)

Nếu cần xem gói tin thô

sudo tcpdump -i eth0 port 445 -c 100 -w /home/ubuntu/smb_traffic.pcap

Sau đó mở / phân tích với Zeek hoặc Wireshark

c. Dùng Wazuh (host-based)

- Trên *wazuh-server* mở dashboard → Agents → xem alerts.
- Hoặc trên *victim2/victim3* xem alerts local:

cat /var/ossec/logs/alerts/alerts.json | tail -n 50

Tìm các alert liên quan: authentication failure, smb, failed password, process creation (ví dụ netcat/smbclient).

4. *Phân tích sự cố*

Khi có dấu hiệu (Zeek log hoặc Wazuh alert)

a. Xác thực nguồn tấn công

Từ Zeek conn.log kiểm tra IP nguồn (ví dụ 10.0.0.10):

grep "445" /opt/zeek/logs/current/conn.log | awk '{print $1, $3, $4}' | tail -n 20

 # hoặc lọc theo IP

grep "10.0.0.10" /opt/zeek/logs/current/conn.log

b. Kiểm tra trên host victim2/victim3

- Kiểm tra auth log:

sudo tail -n 200 /var/log/auth.log

- Kiểm tra process có lạ:

ps aux | egrep "smbclient|netcat|curl|python"

- Kiểm tra file mới:

*sudo find / -mtime -1 -type f -iname "*pwn*" 2>/dev/null*

c. Thu thập bằng chứng

Lưu Zeek conn log excerpt, Wazuh alerts, nmap text output (/home/ubuntu/nmap_scan.txt), và bash_history attacker (/home/ubuntu/.bash_history).

5. *Ứng phó sự cố*

a. Cách ly nguồn tấn công

Tạm thời chặn IP attacker trên victim(s) để ngăn propagation:

- Trên victim2/victim3 (hoặc trên switch/nginx nếu có):

 # dùng iptables

sudo iptables -A INPUT -s 10.0.0.10 -j DROP

 # hoặc dùng ufw

sudo ufw deny from 10.0.0.10

- Xác nhận rule:

sudo iptables -L -n | grep 10.0.0.10

sudo ufw status

b. Dọn dẹp, loại bỏ các thứ nguy hiểm

Nếu phát hiện file payload hoặc process lạ:

sudo pkill -f <process_name>

sudo rm -f /path/to/malicious/file

Kiểm tra integrity (file hashes) với snapshot lúc trước (nếu có).

c. Khôi phục dịch vụ

Khởi động lại dịch vụ cần thiết:

sudo systemctl restart smbd

sudo systemctl status smbd

Kiểm tra chức năng chia sẻ SMB (mount thử share an toàn từ admin).

***6.** Kết thúc bài lab*

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

stoplab idr_wazuh_zeek_smb

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_wazuh_zeek_smb