

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Lab: idr-ossec-filechange

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: IDR-OSSEC-FILECHANGE

1. Mục đích

- Biết cách vận dụng cơ chế giám sát toàn vẹn file (File Integrity Monitoring) của OSSEC để phát hiện các thay đổi bất thường trên những tệp hệ thống quan trọng. Đồng thời, sinh viên rèn luyện kỹ năng cấu hình rule cảnh báo, phân tích log để xử lý sự cố.

2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux.
- Nắm được kiến thức cơ bản về tấn công brute-force.
- Có kiến thức nền tảng về bảo mật hệ thống, về các công cụ OSSEC và iptables.

3. Nội dung bài lab

- Chạy lệnh sau để thêm bài vào labtainer:

```
i/module https://github.com/anhdnmit/do_an_tot_nghiep/raw/refs/heads/main/idr-ossec-filechange/idr-ossec-filechange.tar
```

- Khởi động bài lab:

```
labtainer -r idr-ossec-filechange
```

(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 hệ thống **server**, một máy đại diện cho máy **agent**, một máy đại diện cho máy **attacker**.
- Để kiểm tra địa chỉ IP của 3 máy, gõ lệnh sau trên từng máy:

```
ifconfig
```

3.1. Cài đặt hệ thống 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 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:

- o Ngôn ngữ: en (English)
- o Chọn loại cài đặt: server
- o Xác nhận thư mục cài đặt: /var/ossec
- o 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 **agent** và thực hiện cài đặt các gói cần thiết để cài đặt OSSEC:

```
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 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:
 - o Nhập “I” để nhập key do hệ thống bên server sinh ra.
 - o Dán key mà OSSEC server vừa nhận được.
 - o Xác nhận thêm vào.
 - o Nhập “Q” để thoát khỏi hệ thống.
- Khởi động lại agent:

```
/var/ossec/bin/ossec-control start
```

3.2. Tấn công thay đổi file

- Để server giám sát file quan trọng như /etc/passwd trong máy agent, sinh viên cần mở file cấu hình /var/ossec/etc/ossec.conf trong máy agent và thêm vào trong khôi <syscheck> như sau:

```
<frequency>10</frequency>
<directories check_all="yes" report_changes="yes"
realtime="yes">/etc/passwd</directories>
```

- Giải thích:
 - o frequency=10: Sửa thời gian kiểm tra định kỳ là 10 giây
 - o realtime=yes: Theo dõi realtime
 - o report_changes=yes: Thông báo khi file bị chỉnh sửa
- Sau khi sửa xong, sinh viên lưu lại và thoát ra terminal. Khởi động lại OSSEC agent và OSSEC server:

```
/var/ossec/bin/ossec-control restart
```

- Để mô phỏng cuộc tấn công, sinh viên cần đặt mật khẩu cho một user để attacker xâm nhập bằng SSH (user ở đây là ubuntu).
- Sinh viên chạy lệnh sau để đặt mật khẩu cho user ubuntu: `sudo passwd ubuntu`
- Bật SSH: `sudo systemctl start ssh`

- Tạo một file backup /etc/passwd để thực hiện khôi phục phòng trường hợp file bị thay đổi:

```
sudo mkdir -p /var/backups
```

```
sudo cp /etc/passwd /var/backups/passwd.bak
```

- Tại máy **attacker**, sinh viên thực hiện cài đặt hydra để tấn công brute-force:

```
sudo apt install hydra -y
```

- Tạo file password.txt và nhập 10 dòng password, trong đó có một dòng là mật khẩu của user ubuntu mà sinh viên vừa tạo ở máy **agent**.
- Thực hiện brute-force vào máy **agent**:

```
sudo hydra -l ubuntu -P password.txt <IP-agent> ssh
```

⇒ Tìm được user và password.

- Đăng nhập vào máy agent:

```
ssh ubuntu@<IP-agent>
```

- Thêm user backdoor có quyền root vào hệ thống:

```
echo 'hacker:x:0:0::/root:/bin/bash' | sudo tee -a /etc/passwd
```

- Kiểm tra lại xem user đã được thêm vào chưa:

```
cat /etc/passwd
```

3.3. Phát hiện và phản ứng sự cố

- Sinh viên đợi một lúc để **OSSEC server** nhận cảnh báo rồi quay lại máy **server** và kiểm tra:

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

- Ở đây, sinh viên sẽ thấy có cảnh báo phát hiện user sửa file /etc/passwd. Sinh viên điều tra sâu hơn các log trước sẽ thấy user của máy agent bị một máy bên ngoài đăng nhập vào.
- Sau khi **OSSEC server** báo file /etc/passwd bị chỉnh sửa, sinh viên vào máy **agent** và tiến hành khóa lại user bị xâm nhập:

```
sudo usermod -L ubuntu
```

```
sudo passwd -l ubuntu
```

- Chặn IP của máy **attacker** xâm nhập vào máy **agent**:

```
sudo iptables -A INPUT -s 200.20.0.4 -j DROP
```

- Kiểm tra lại danh sách địa chỉ IP đã chặn để xem attacker đã bị chặn chưa:

```
sudo iptables -L -n -v
```

- Khôi phục file /etc/passwd bằng bản backup:

```
sudo cp /var/backups/passwd.bak /etc/passwd
```

- Đổi mật khẩu user bị tấn công:

```
sudo passwd ubuntu
```

- Sau khi đổi xong, mở khóa user trở lại:

```
sudo usermod -U ubuntu
```

```
sudo passwd -S ubuntu
```

- Để giảm khả năng máy agent bị tấn công, sinh viên cấu hình lại SSH chỉ cho phép đăng nhập bằng key:

```
sudo nano /etc/ssh/sshd_config
```

- Sửa lại các dòng:

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

```
PubkeyAuthentication yes
```

- Khởi động lại SSH:

```
sudo systemctl restart ssh
```

- Kết thúc bài lab:

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

```
stoplab idr-ossec-filechange
```

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-ossec-filechange
```