

BÁO CÁO THỰC HÀNH

Môn học: NT140.P12.ANTT – An Toàn Mạng
Tên chủ đề: Lab 4 - Hệ Thống Phát Hiện Xâm Nhập OSSEC
GVHD: Tô Trọng Nghĩa

Nhóm: 6

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P12.ANTT.2

STT	Họ và tên	MSSV	Email
1	Lại Quan Thiên	22521385	22521385@gm.uit.edu.vn
2	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn
3	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
4	Đặng Đức Tài	22521270	22521270@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Nội dung	Tình trạng	Thực hiện
1	Task 1	100%	Nam Phương
2	Task 2	100%	Đức Tài
3	Task 3	100%	Quan Thiên Diệp Huy
Điểm tự đánh giá			10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Task 1: Tìm trong tập tin cấu hình đoạn cấu hình giám sát log của quá trình đăng nhập vào hệ thống, biết tập tin log này lưu ở /var/log/auth.log và thuộc loại syslog. Nếu không có, hãy thêm cấu hình này vào tập tin cấu hình. Sau đó, trên Agent, tiến hành đăng nhập bằng các user khác nhau (root, local user, SSH user) và quan sát các cảnh báo trả về ở log OSSEC Server tại /var/ossec/logs/alerts/alerts.log

Trả lời:

- Thực hiện tìm trong tập tin cấu hình đoạn cấu hình giám sát log của quá trình đăng nhập vào hệ thống ở /var/log/auth.log:

- Thực hiện quan sát các cảnh báo trả về ở log OSSEC Server tại /var/ossec/logs/alerts/alerts.log ta được kết quả như sau:

- Ta thấy 3 kết quả đầu tiên như sau:

```

root@namphuong11-ubuntu: /home/namphuong11
** Alert 1732881443.57248: - syslog,sudo
2024 Nov 29 18:57:23 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: agent
Nov 29 03:57:21 ubuntu sudo: agent: TTY=pts/0 ; PWD=/home/agent ; USER=root ; COMMAND=/bin/bash

** Alert 1732881443.57526: - pam,syslog,authentication_success,
2024 Nov 29 18:57:23 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5501 (level 3) -> 'Login session opened.'
Nov 29 03:57:21 ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)

** Alert 1732881457.57797: - pam,syslog,authentication_success,
2024 Nov 29 18:57:37 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5501 (level 3) -> 'Login session opened.'
Nov 29 03:57:36 ubuntu su: pam_unix(su-l:session): session opened for user agent by (uid=0)
  
```

+ Cảnh báo đầu tiên (1732881443.57248): Loại sự kiện: sudo

- Chi tiết: Người dùng agent đã thực thi thành công lệnh sudo để chuyển sang người dùng root và chạy lệnh /bin/bash
- Bối cảnh: Log chỉ ra rằng agent đã sử dụng sudo để có quyền root trên máy chủ Ubuntu

+ Cảnh báo thứ hai (1732881443.57526): Loại sự kiện: pam_unix(sudo:session)

- Chi tiết: Một phiên đăng nhập mới đã được mở cho người dùng root sau khi lệnh sudo thành công
- Bối cảnh: Phiên làm việc được mở bởi người dùng root (uid=0), cho thấy sudo đã thành công trong việc đăng nhập người dùng root

+ Cảnh cáo cuối cùng (1732881443.57797): Loại sự kiện: su (chuyển người dùng)

- Chi tiết: Người dùng agent đã mở một phiên mới sử dụng su để chuyển sang người dùng root
- Bối cảnh: su được sử dụng để chuyển sang người dùng khác, trong trường hợp này là agent, và thông báo xác nhận phiên làm việc đã được mở thành công

- Kết quả của đăng nhập SSH:

```

** Alert 1732881475.58067: - pam,syslog,authentication_failed,
2024 Nov 29 18:57:55 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 192.168.233.134
User: agent
Nov 29 03:57:55 ubuntu sshd[2587]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.233.134 user=agent

** Alert 1732881477.58428: - syslog,sshd,authentication_failed,
2024 Nov 29 18:57:57 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5716 (level 5) -> 'SSHD authentication failed.'
Src IP: 192.168.233.134
User: agent
Nov 29 03:57:56 ubuntu sshd[2587]: Failed password for agent from 192.168.233.134 port 60298 ssh2

** Alert 1732881487.58746: - syslog,sshd,authentication_failed,
2024 Nov 29 18:58:07 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5716 (level 5) -> 'SSHD authentication failed.'
Src IP: 192.168.233.134
User: agent
Nov 29 03:58:00 ubuntu sshd[2587]: Failed password for agent from 192.168.233.134 port 60298 ssh2

** Alert 1732881487.59064: - syslog,sshd,authentication_success,
2024 Nov 29 18:58:07 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5715 (level 3) -> 'SSHD authentication success.'
Src IP: 192.168.233.134
User: agent
Nov 29 03:58:06 ubuntu sshd[2587]: Accepted password for agent from 192.168.233.134 port 60298 ssh2

** Alert 1732881487.59386: - pam,syslog,authentication_success,
2024 Nov 29 18:58:07 (agent1) 192.168.233.135->/var/log/auth.log
Rule: 5501 (level 3) -> 'Login session opened.'
Nov 29 03:58:06 ubuntu sshd[2587]: pam_unix(sshd:session): session opened for user agent by (uid=0)
  
```

+ 3 cảnh báo đầu tiên (1732881475.58067, 1732881477.58428, 1732881487.58746)

- Rule 5503 (màu đỏ) - Loại sự kiện: sshd (Lỗi xác thực SSH): Người dùng agent không thể đăng nhập qua SSH từ IP 192.168.233.134
- Rule 5716 (màu vàng) - Loại sự kiện: sshd (Mật khẩu thất bại SSH): Lần lượt là 2 lần xác thực SSH thất bại, kết quả cho thấy có thể là những lần thử mật khẩu sai hoặc một cuộc tấn công SSH

+ 2 cảnh báo sau cùng (1732881487.59064, 1732881487.59386)

- Rule 5715 - Loại sự kiện: sshd (Xác thực SSH thành công): Cảnh báo người dùng agent đã đăng nhập thành công qua SSH từ IP 192.168.233.134
- Rule 5501 - Loại sự kiện: pam_unix(sshd:session): Một phiên làm việc đã được mở cho người dùng agent qua SSH sau khi xác thực thành công

Task 2: Hãy cấu hình OSSEC kiểm tra tính toàn vẹn của một thư mục bất kỳ. Sau đó thử sửa đổi nội dung các tập tin trong thư mục đó để chứng minh cấu hình thành công.

Trả lời:

- Tạo thư mục test_dir và 2 file test .txt:

```
dducktai@ubuntu:~$ mkdir -p /home/dducktai/test_dir
dducktai@ubuntu:~$ echo "Test file 1" > /home/dducktai/test_dir/file1.txt
dducktai@ubuntu:~$ echo "Test file 2" > /home/dducktai/test_dir/file2.txt
```

- Nội dung ban đầu của 2 file text:

```
dducktai@ubuntu:~$ cd /home/dducktai/test_dir/
dducktai@ubuntu:~/test_dir$ cat file1.txt
Test file 1
dducktai@ubuntu:~/test_dir$ cat file2.txt
Test file 2
dducktai@ubuntu:~/test_dir$
```

- Mở tệp cấu hình OSSEC, tại thẻ <syscheck> thêm nội dung sau:

```
GNU nano 4.8 /var/ossec/etc/ossec.conf
<ossec_config>
  <client>
    <server-hostname>192.168.159.159</server-hostname>
    <config-profile></config-profile>
  </client>

  <syscheck>
    <!-- Frequency that syscheck is executed - default to every 22 hours -->
    <frequency>60</frequency>

    <!-- Directories to check (perform all possible verifications) -->
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin,/boot</directories>
    <directories check_all="yes">/home/dducktai/test_dir</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/mnttab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/adjtime</ignore>
    <ignore>/etc/httpd/logs</ignore>
    <ignore>/etc/utmpx</ignore>
```

+ **<server-hostname>**: Đây là địa chỉ IP hoặc hostname của OSSEC Server mà client sẽ kết nối đến để gửi dữ liệu. Địa chỉ IP của máy chủ là 192.168.159.159.

+ **<syscheck>** là phần cấu hình chịu trách nhiệm giám sát sự thay đổi của các tệp và thư mục trên hệ thống.

- **<frequency>**: Tùy chọn này chỉ định tần suất kiểm tra các tệp và thư mục. Nghĩa là hệ thống sẽ kiểm tra sự thay đổi của các tệp mỗi 60 phút.
- **<directories>**: Các thư mục được chỉ định để OSSEC giám sát sự thay đổi:

+ Các tham số `check_all="yes"` có nghĩa là OSSEC sẽ kiểm tra tất cả các tệp trong các thư mục này, bao gồm các thay đổi về kích thước, quyền truy cập, và checksum của các tệp.

- Lưu tệp và khởi động lại dịch vụ OSSEC để áp dụng các cấu hình vừa được thay đổi:

```
dducktai@ubuntu:~/test_dir$ sudo nano /var/ossec/etc/ossec.conf
dducktai@ubuntu:~/test_dir$ sudo systemctl restart ossec
dducktai@ubuntu:~/test_dir$ sudo systemctl status ossec
● ossec.service - LSB: Start and stop OSSEC HIDS
   Loaded: loaded (/etc/init.d/ossec; generated)
   Active: active (running) since Fri 2024-11-29 20:22:26 PST; 6s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 5953 ExecStart=/etc/init.d/ossec start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 4540)
   Memory: 1.6M
    CGroup: /system.slice/ossec.service
            └─5966 /var/ossec/bin/ossec-execd
              └─5970 /var/ossec/bin/ossec-agentd
                └─5974 /var/ossec/bin/ossec-logcollector
                  └─5978 /var/ossec/bin/ossec-syscheckd
```

- Thực hiện sửa file1.txt:

```
dducktai@ubuntu:~/test_dir$ sudo echo "Modified" > file1.txt
dducktai@ubuntu:~/test_dir$ cat file1.txt
Modified
dducktai@ubuntu:~/test_dir$
```

- Kiểm tra log trên OSSEC Server với lệnh `sudo tail -f /var/ossec/logs/ossec.log`:

```
** Alert 1732975870.15112: mail - ossec,syscheck,
2024 Nov 30 06:11:10 (agent1) 192.168.159.15->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/home/dducktai/test_dir/file1.txt'
Size changed from '20' to '9'
Permissions changed from 'rw-rw-r--' to 'rw-r--r--'
Old md5sum was: 'd81dcf5c8eac7a9ffcac47c4d51969cc'
New md5sum is : '6548d7cfbba0141a85ee4860dd129509'
Old sha1sum was: '7ad11e329a1c9bb93a336fdbb996f7caec9f4f12'
New sha1sum is : 'd2482d0793057a1ab54a06c59500634ee6f2cc70'
```

- OSSEC Syscheck chỉ so sánh checksum và thuộc tính file (size, permissions, owner,...) nhưng không ghi lại nội dung file bị thay đổi trực tiếp vì lý do:

- **Bảo mật:** Ghi lại nội dung file có thể vô tình lộ thông tin nhạy cảm.
- **Hiệu suất:** Ghi lại nội dung sẽ làm tăng đáng kể dung lượng log và ảnh hưởng đến hiệu suất hệ thống.
- **Chính sách mặc định:** OSSEC tập trung vào giám sát thay đổi file hơn là theo dõi nội dung.

**Task 3:** Tham khảo syntax active response của OSSEC

(https://www.ossec.net/docs/syntax/head_ossec_config.active-response.html) và cấu hình chặn các IP khi phát hiện có lưu lượng truy cập đáng ngờ (như nhiều lần đăng nhập thất bại). Thực nghiệm tấn công để kiểm tra tính chính xác của cấu hình.

Trả lời:*** Cấu hình phía Server:**

- Ta sử dụng: `sudo nano /var/ossec/etc/ossec.conf` để cấu hình <active-reponse> như sau:

+ Code:

```
<!-- Active Response Config -->
<active-response>
  <!-- This response is going to execute the host-deny
    - command for every event that fires a rule with
    - level (severity) >= 6.
    - The IP is going to be blocked for 120 seconds.
  -->
  <command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>120</timeout>
</active-response>

<active-response>
  <!-- Firewall Drop response. Block the IP for
    - 120 seconds on the firewall (iptables,
    - ipfilter, etc).
  -->
  <command>firewall-drop</command>
  <location>local</location>
  <level>6</level>
  <timeout>120</timeout>
</active-response>
```



```

GNU nano 4.8 /var/ossec/etc/ossec.conf
<!-- Active Response Config -->
<active-response>
  <!-- This response is going to execute the host-deny
  - command for every event that fires a rule with
  - level (severity) >= 6.
  - The IP is going to be blocked for 120 seconds.
  -->
  <command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>120</timeout>
</active-response>

<active-response>
  <!-- Firewall Drop response. Block the IP for
  - 120 seconds on the firewall (iptables,
  - ipfilter, etc).
  -->
  <command>firewall-drop</command>
  <location>local</location>
  <level>6</level>
  <timeout>120</timeout>
</active-response>

<!-- Files to monitor (localfiles) -->

```

+ Giải thích:

- `<command>`: Chỉ định tên lệnh được thực thi khi phát hiện sự kiện cần phản hồi. Ở đây là `host-deny` và `firewall-drop`.
- `<location>`: Xác định nơi thực thi lệnh:
 - `local`: Thực thi trên máy đang chạy OSSEC.
 - `all`: Thực thi trên tất cả các agent kết nối với OSSEC.
- `<level>`: Mức độ nghiêm trọng tối thiểu của sự kiện để kích hoạt hành động. Ở đây là các sự kiện có **level ≥ 6** .
- `<timeout>`: Thời gian hiệu lực của hành động (đơn vị: giây). Sau khoảng thời gian này, hành động sẽ được gỡ bỏ. Ở đây là **120 giây**.
- `firewall-drop` sẽ thực thi lệnh `firewall-drop.sh` (giải thích trong `<command>` bên dưới) để chặn IP bằng tường lửa (như `iptables`).
- Hành động này cũng áp dụng với sự kiện có mức độ nghiêm trọng ≥ 6 và kéo dài 120 giây.

- Sau đó ta cấu hình tiếp phần `<command>`:

+ Code:

```

<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

```



```
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

```
<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

+ Giải thích:

- <name>: Tên của lệnh, được sử dụng trong <active-response> ở đây là host-deny và firewall-drop.
- <executable>: Script thực thi khi hành động được kích hoạt. Ở đây, script host-deny.sh sẽ được gọi. Script này sẽ thêm IP tấn công vào file /etc/hosts.deny, ngăn chặn kết nối từ IP đó.
- <expect>: Loại dữ liệu được truyền vào script => với srcip: Địa chỉ IP nguồn của sự kiện (IP bị nghi ngờ tấn công).
- <timeout_allowed>: Cho phép gỡ bỏ hành động sau khi **timeout** được chỉ định trong <active-response>.
- firewall-drop thực thi script firewall-drop.sh, script này thường thêm quy tắc vào tường lửa (iptables) để chặn IP.
- Các tham số như srcip và timeout_allowed có chức năng tương tự như ở host-deny.

- Về mức độ cảnh báo level 6:

+ Trong OSSEC, mức độ nghiêm trọng (level) là một cách để đánh giá mức độ nguy hiểm của một sự kiện hoặc mối đe dọa được phát hiện. Các mức độ nghiêm trọng thường được định nghĩa trong tập luật của OSSEC (rules), với level dao động từ 0 đến 15 (tham khảo: [Rules Classification — OSSEC Documentation 1.0 documentation](#))

+ Các sự kiện có mức độ nghiêm trọng từ 6 trở lên sẽ kích hoạt **Active Response**.

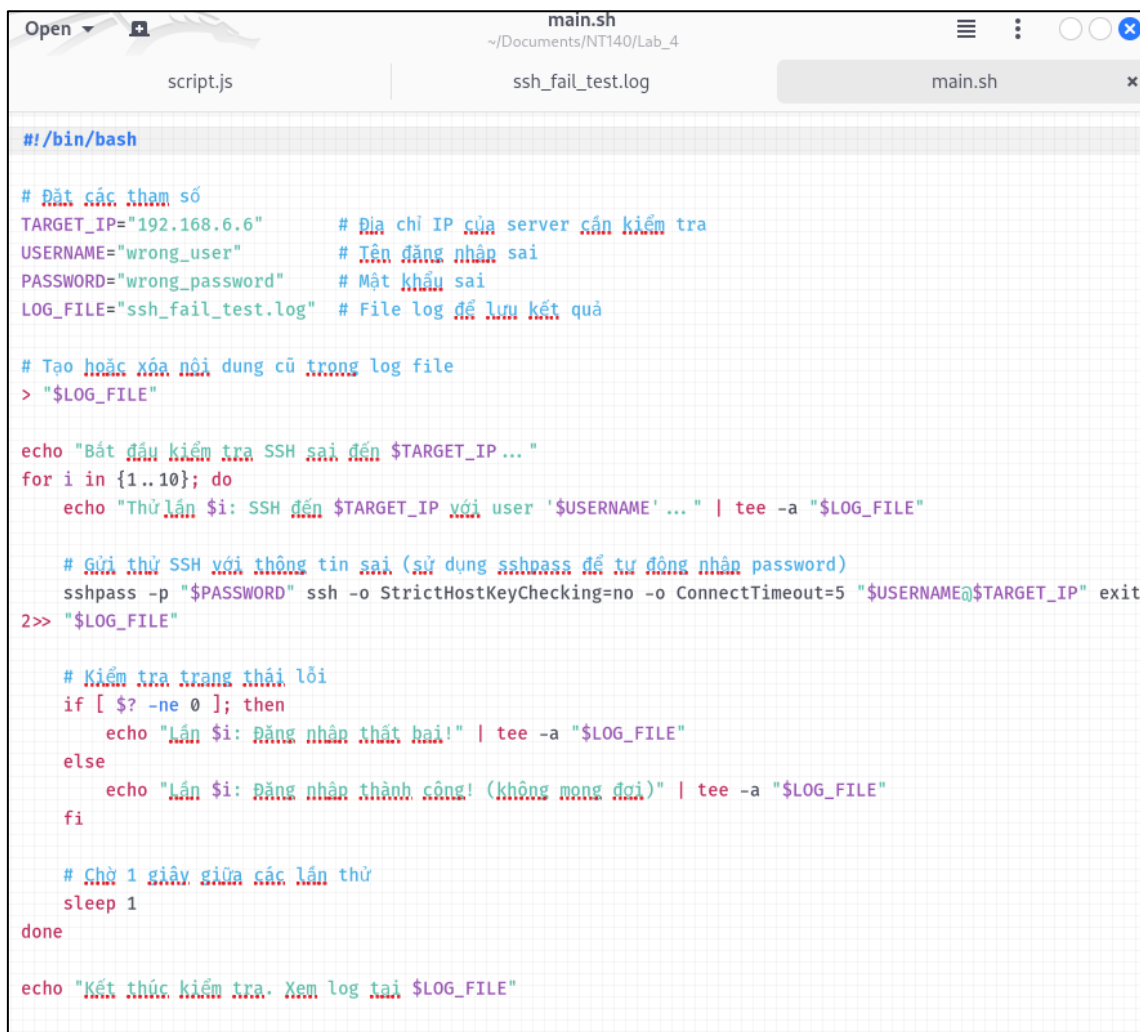
+ Các sự kiện này thuộc nhóm **cảnh báo nhẹ**, thường liên quan đến:

- Một số lần đăng nhập thất bại.
- Truy cập trái phép không thành công.
- Quét cổng mạng ở mức độ nhẹ.

+ Sau đó khởi động lại ossec để áp dụng các tùy chỉnh trên: `sudo systemctl restart ossec`

* Cấu hình phía Attacker:

Ta viết đoạn code sau để thực thi ssh 10 lần đến 1 user không có thật trong máy server 192.168.6.6, sau mỗi lần ssh sẽ lưu lại log ở phía attacker 192.168.6.8:



```
#!/bin/bash

# Đặt các tham số
TARGET_IP="192.168.6.6"      # Địa chỉ IP của server cần kiểm tra
USERNAME="wrong_user"       # Tên đăng nhập sai
PASSWORD="wrong_password"   # Mật khẩu sai
LOG_FILE="ssh_fail_test.log" # File log để lưu kết quả

# Tạo hoặc xóa nội dung cũ trong log file
> "$LOG_FILE"

echo "Bắt đầu kiểm tra SSH sai đến $TARGET_IP..."
for i in {1..10}; do
    echo "Thử lần $i: SSH đến $TARGET_IP với user '$USERNAME' ... " | tee -a "$LOG_FILE"

    # Gửi thử SSH với thông tin sai (sử dụng sshpass để tự động nhập password)
    sshpass -p "$PASSWORD" ssh -o StrictHostKeyChecking=no -o ConnectTimeout=5 "$USERNAME@$TARGET_IP" exit
    2>> "$LOG_FILE"

    # Kiểm tra trạng thái lỗi
    if [ $? -ne 0 ]; then
        echo "Lần $i: Đăng nhập thất bại!" | tee -a "$LOG_FILE"
    else
        echo "Lần $i: Đăng nhập thành công! (không mong đợi)" | tee -a "$LOG_FILE"
    fi

    # Chờ 1 giây giữa các lần thử
    sleep 1
done

echo "Kết thúc kiểm tra. Xem log tại $LOG_FILE"
```

*** Tiến hành tấn công:****- Phía Attacker (192.168.6.8):**

+ Ta tiến hành chạy file main.sh để ssh sai 10 lần đến Server, kết quả như hình bên dưới, sau 3 lần ssh thất bại thì từ lần 4->10 thì kết nối bị timeout:

```

root@thinnlinux: /home/kali/Documents/NT140/Lab_4
(main.sh)
./main.sh
Bắt đầu kiểm tra SSH sai đến 192.168.6.6...
Thứ lần 1: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 1: Đăng nhập thất bại!
Thứ lần 2: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 2: Đăng nhập thất bại!
Thứ lần 3: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 3: Đăng nhập thất bại!
Thứ lần 4: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 4: Đăng nhập thất bại!
Thứ lần 5: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 5: Đăng nhập thất bại!
Thứ lần 6: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 6: Đăng nhập thất bại!
Thứ lần 7: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 7: Đăng nhập thất bại!
Thứ lần 8: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 8: Đăng nhập thất bại!
Thứ lần 9: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 9: Đăng nhập thất bại!
Thứ lần 10: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 10: Đăng nhập thất bại!
Kết thúc kiểm tra. Xem log tại ssh_fail_test.log

ssh_fail_test.log
script.js
ssh_fail_test.log
Permission denied, please try again.
Lần 1: Đăng nhập thất bại!
Thứ lần 2: SSH đến 192.168.6.6 với user 'wrong_user'...
Permission denied, please try again.
Lần 2: Đăng nhập thất bại!
Thứ lần 3: SSH đến 192.168.6.6 với user 'wrong_user'...
Permission denied, please try again.
Lần 3: Đăng nhập thất bại!
Thứ lần 4: SSH đến 192.168.6.6 với user 'wrong_user'...
Permission denied, please try again.
Lần 4: Đăng nhập thất bại!
Thứ lần 5: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 5: Đăng nhập thất bại!
Thứ lần 6: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 6: Đăng nhập thất bại!
Thứ lần 7: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 7: Đăng nhập thất bại!
Thứ lần 8: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 8: Đăng nhập thất bại!
Thứ lần 9: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 9: Đăng nhập thất bại!
Thứ lần 10: SSH đến 192.168.6.6 với user 'wrong_user'...
ssh: connect to host 192.168.6.6 port 22: Connection timed out
Lần 10: Đăng nhập thất bại!

```

+ Sau đó, ta thử ssh đến user [seed@192.168.6.6](#) (cũng là tài khoản Server), kết quả là kết nối bị timeout, không thể ssh đến được:

```

root@thinnlinux: /home/kali/Documents/NT140/Lab_4
./main.sh
Bắt đầu kiểm tra SSH sai đến 192.168.6.6...
Thứ lần 1: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 1: Đăng nhập thất bại!
Thứ lần 2: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 2: Đăng nhập thất bại!
Thứ lần 3: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 3: Đăng nhập thất bại!
Thứ lần 4: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 4: Đăng nhập thất bại!
Thứ lần 5: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 5: Đăng nhập thất bại!
Thứ lần 6: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 6: Đăng nhập thất bại!
Thứ lần 7: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 7: Đăng nhập thất bại!
Thứ lần 8: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 8: Đăng nhập thất bại!
Thứ lần 9: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 9: Đăng nhập thất bại!
Thứ lần 10: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 10: Đăng nhập thất bại!
Kết thúc kiểm tra. Xem log tại ssh_fail_test.log

(root@thinnlinux)~/home/kali/Documents/NT140/Lab_4
ssh seed@192.168.6.6

```


- *Phía Server (192.168.6.6):*

+ Ta xem các cảnh báo trong file alert:

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

```

seed@VM: ~
** Alert 1732973909.54385: - pam,syslog,authentication_failed,
2024 Nov 30 08:38:29 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 192.168.6.8
Nov 30 08:38:28 VM sshd[5995]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.6.8

** Alert 1732973911.54689: mail - syslog,sshd,authentication_failures,
2024 Nov 30 08:38:31 VM->/var/log/auth.log
Rule: 5712 (level 10) -> 'SSHD brute force trying to get access to the system.'
Src IP: 192.168.6.8
Nov 30 08:38:30 VM sshd[5995]: Failed password for invalid user wrong user from 192.168.6.8 port 52612 ssh2
Nov 30 08:38:28 VM sshd[5995]: Invalid user wrong user from 192.168.6.8 port 52612
Nov 30 08:38:26 VM sshd[5992]: Failed password for invalid user wrong user from 192.168.6.8 port 52610 ssh2
Nov 30 08:38:25 VM sshd[5992]: Invalid user wrong user from 192.168.6.8 port 52610
Nov 30 08:38:23 VM sshd[5990]: Failed password for invalid user wrong user from 192.168.6.8 port 36388 ssh2
Nov 30 08:38:21 VM sshd[5990]: Invalid user wrong user from 192.168.6.8 port 36388
Nov 30 08:38:19 VM sshd[5988]: Failed password for invalid user wrong user from 192.168.6.8 port 36382 ssh2
Nov 30 08:38:17 VM sshd[5988]: Invalid user wrong user from 192.168.6.8 port 36382

** Alert 1732973944.55669: - pam,syslog,
2024 Nov 30 08:39:04 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Nov 30 08:39:03 VM sudo: pam_unix(sudo:session): session closed for user root

** Alert 1732973982.55880: - pam,syslog,
2024 Nov 30 08:39:42 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Nov 30 08:39:41 VM sshd[5307]: pam_unix(sshd:session): session closed for user seed

```

+ Ta xem tiếp trong file auth.log, kết quả cũng trả về những cảnh báo tương tự

```
sudo less /var/log/auth.log
```

```

Nov 30 08:31:30 VM sshd[5798]: Invalid user wrong user from 192.168.6.8 port 47052
Nov 30 08:31:30 VM sshd[5798]: pam_unix(sshd:auth): check pass; user unknown
Nov 30 08:31:30 VM sshd[5798]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.6.8
Nov 30 08:31:30 VM sudo: pam_unix(sudo:session): session closed for user root
Nov 30 08:31:32 VM sshd[5798]: Failed password for invalid user wrong user from 192.168.6.8 port 47052 ssh2
Nov 30 08:31:33 VM sshd[5798]: Connection closed by invalid user wrong user 192.168.6.8 port 47052 [preauth]
Nov 30 08:31:43 VM sudo: seed : TTY=pts/0 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
Nov 30 08:31:43 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:33:10 VM sudo: seed : TTY=pts/3 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/sbin/iptables -L -n
Nov 30 08:33:10 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:33:10 VM sudo: pam_unix(sudo:session): session closed for user root
Nov 30 08:34:38 VM sudo: seed : TTY=pts/3 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
Nov 30 08:34:38 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:34:47 VM sshd[2736]: pam_unix(sshd:session): session closed for user seed
Nov 30 08:34:47 VM sudo: pam_unix(sudo:session): session closed for user root
Nov 30 08:34:47 VM systemd-logind[852]: Session 4 logged out. Waiting for processes to exit.
Nov 30 08:34:47 VM systemd-logind[852]: Removed session 4.
Nov 30 08:35:19 VM sshd[5914]: Connection closed by authenticating user seed 192.168.6.8 port 50152 [preauth]
Nov 30 08:35:54 VM sudo: seed : TTY=pts/1 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/sbin/iptables -L -n
Nov 30 08:35:54 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:35:54 VM sudo: pam_unix(sudo:session): session closed for user root
Nov 30 08:36:31 VM sudo: seed : TTY=pts/1 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/bin/less /var/ossec/logs/active-responses.log
Nov 30 08:36:31 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:36:58 VM sudo: message repeated 2 times: [ pam_unix(sudo:session): session closed for user root]
Nov 30 08:37:47 VM sudo: seed : TTY=pts/0 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
Nov 30 08:37:47 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 30 08:37:50 VM sudo: seed : TTY=pts/3 ; PWD=/home/seed ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
Nov 30 08:37:50 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)

```

+ Ta thấy rằng, log đã lưu lại những lần sai mật khẩu khi ssh đến user wrong_user từ máy có địa chỉ ip 192.168.6.8

+ Cuối cùng, ta xem file active-responses.log để xem active-responses đã hoạt động chưa, kết quả như hình bên dưới, vào lúc 08:38:31 thì hệ thống đã thêm IP 192.168.6.8 vào danh sách chặn, đó cũng là lý do vì sao sau khi thực thi code 10 lần SSH sai đến Server, phía Attacker không thể tiếp tục SSH đến tài khoản SEED được:

```

Sat 30 Nov 2024 08:17:34 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:17:34 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:28:04 AM EST /var/ossec/active-response/bin/host-deny.sh delete - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:28:04 AM EST /var/ossec/active-response/bin/firewall-drop.sh delete - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:31:33 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:31:33 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:34:33 AM EST /var/ossec/active-response/bin/host-deny.sh delete - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:34:33 AM EST /var/ossec/active-response/bin/firewall-drop.sh delete - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:38:31 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.8 1732973911.54689 5712
Sat 30 Nov 2024 08:38:31 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.8 1732973911.54689 5712

```

+ Tuy nhiên, như code bên trên, ta chỉ cấu hình chặn IP trong 120 giây ~ 2 phút, sau 2 phút thì địa chỉ IP này sẽ được xóa khỏi hệ thống chặn. Hình bên dưới, lúc 08:41:32, thì địa chỉ này đã được xóa:

```

Sat 30 Nov 2024 08:17:34 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:17:34 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:28:04 AM EST /var/ossec/active-response/bin/host-deny.sh delete - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:28:04 AM EST /var/ossec/active-response/bin/firewall-drop.sh delete - 192.168.6.1 1732972654.32895 2502
Sat 30 Nov 2024 08:31:33 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:31:33 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:34:33 AM EST /var/ossec/active-response/bin/host-deny.sh delete - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:34:33 AM EST /var/ossec/active-response/bin/firewall-drop.sh delete - 192.168.6.8 1732973493.44846 5712
Sat 30 Nov 2024 08:38:31 AM EST /var/ossec/active-response/bin/host-deny.sh add - 192.168.6.8 1732973911.54689 5712
Sat 30 Nov 2024 08:38:31 AM EST /var/ossec/active-response/bin/firewall-drop.sh add - 192.168.6.8 1732973911.54689 5712
Sat 30 Nov 2024 08:41:32 AM EST /var/ossec/active-response/bin/host-deny.sh delete - 192.168.6.8 1732973911.54689 5712
Sat 30 Nov 2024 08:41:32 AM EST /var/ossec/active-response/bin/firewall-drop.sh delete - 192.168.6.8 1732973911.54689 5712
/var/ossec/logs/active-responses.log (END)

```

- Hơn 2 phút sau:

+ Ta có thể SSH được từ máy Attacker đến máy Server với tài khoản đúng là seed@192.168.6.6 cùng với mật khẩu đúng:

```

Lần 8: Đăng nhập thất bại!
Thứ lần 9: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 9: Đăng nhập thất bại!
Thứ lần 10: SSH đến 192.168.6.6 với user 'wrong_user'...
Lần 10: Đăng nhập thất bại!
Kết thúc kiểm tra. Xem log tại ssh_fail_test.log

(root@thinnlinux)-[/home/kali/Documents/NT140/Lab_4]
^C
(root@thinnlinux)-[/home/kali/Documents/NT140/Lab_4]
$ ssh seed@192.168.6.6
seed@192.168.6.6's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

545 updates can be installed immediately.
545 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Nov 30 08:28:38 2024 from 192.168.6.8
[11/30/24]seed@VM:~$

```


+ Phía Server cũng hiện log:

```
** Alert 1732974180.57882: - pam,syslog,authentication_success,  
2024 Nov 30 08:43:00 VM->/var/log/auth.log  
Rule: 5501 (level 3) -> 'Login session opened.'  
Nov 30 08:42:58 VM sudo: pam_unix(sudo:session): session opened for user root by (uid=0)  
  
** Alert 1732974196.58127: - syslog,sshd,authentication_success,  
2024 Nov 30 08:43:16 VM->/var/log/auth.log  
Rule: 5715 (level 3) -> 'SSHD authentication success.'  
Src IP: 192.168.6.8  
User: seed  
Nov 30 08:43:14 VM sshd[6089]: Accepted password for seed from 192.168.6.8 port 49950 ssh2  
  
** Alert 1732974196.58413: - pam,syslog,authentication_success,  
2024 Nov 30 08:43:16 VM->/var/log/auth.log  
Rule: 5501 (level 3) -> 'Login session opened.'  
Nov 30 08:43:14 VM sshd[6089]: pam_unix(sshd:session): session opened for user seed by (uid=0)
```

* Kết luận:

- Qua thử nghiệm, hệ thống OSSEC đã hoạt động hiệu quả trong việc phát hiện và ngăn chặn các nỗ lực tấn công brute-force SSH. Sau 3 lần thất bại liên tiếp, OSSEC tự động kích hoạt cơ chế active response, thực hiện chặn địa chỉ IP tấn công (192.168.6.8) trên firewall trong vòng 120 giây. Sau khoảng thời gian này, hệ thống tự động gỡ bỏ chặn, cho phép kết nối bình thường trở lại.

- Cơ chế này không chỉ bảo vệ hệ thống trước các cuộc tấn công brute-force mà còn lưu lại chi tiết các cảnh báo và phản ứng trong log, giúp dễ dàng theo dõi và phân tích các sự kiện an ninh trên Server.