Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

4

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

HỆ THỐNG PHÁT HIỆN XÂM NHẬP OSSEC

Thực hành môn An toàn mạng

Tháng 9/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Xây dựng hệ thống phát hiện xâm nhập dựa trên máy chủ (HIDS) sử dụng OSSEC.
- Tìm hiểu các tính năng của OSSEC để phát hiện bất thường.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Cài đặt ít nhất 2 máy ảo Ubuntu (có thể sử dụng Seed Ubuntu 20.04 (https://seedsecuritylabs.org/labsetup.html hoặc các máy ảo đã có sẵn từ các bài thực hành trước)
- Tải và cài đặt OSSEC theo hướng dẫn ở mục 1.

C. THỰC HÀNH

OSSEC (Open Source Security) là một nền tảng phát hiện xâm nhập dựa trên host (Host base Intrusion Detection System - HIDS) mã nguồn mở, dùng để giám sát các hoạt động của hệ thống và mạng nhằm phát hiện các hành vi bất thường hoặc xâm nhập trái phép. OSSEC thực hiện nhiều chức năng bảo mật quan trọng, bao gồm:

- Phân tích nhật ký (Log Analysis): OSSEC thu thập và phân tích nhật ký từ các ứng dụng, hệ điều hành và thiết bị mạng để phát hiện các dấu hiệu đáng ngờ.
- Giám sát tính toàn vẹn của tập tin (File Integrity Monitoring - FIM): OSSEC theo dõi các thay đổi trong tập tin quan trọng, giúp nhận diện các hành động bất hợp pháp hoặc không mong muốn.
- Phát hiện rootkit (Rootkit Detection): OSSEC tìm kiếm các rootkit - phần mềm ẩn để giành quyền kiểm soát hệ thống mà không bị phát hiện.
- Phát hiện cấu hình chính sách bảo mật (Policy Monitoring): OSSEC giám sát cấu hình hệ thống, đảm bảo tuân thủ các chính sách bảo mật.
- Phản ứng sự cố tự động (Active Response): OSSEC có thể tự động thực hiện hành động phòng ngừa hoặc ngăn chặn, chẳng hạn như chặn địa chỉ IP có hoạt động đáng ngờ.

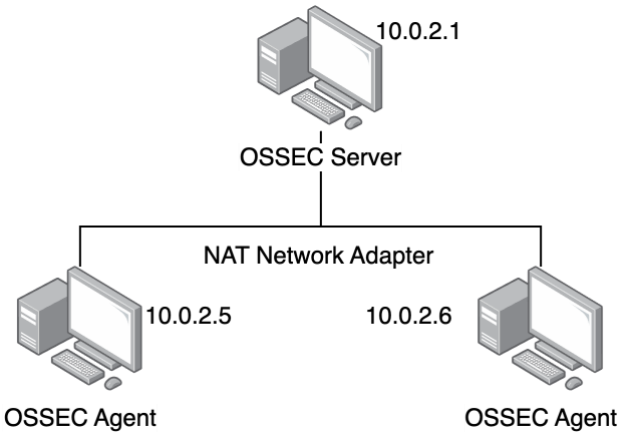
OSSEC hoạt động theo mô hình Client – Server:

- OSSEC Server đóng vai trò là trung tâm xử lý, tiếp nhận và phân tích log được gửi về.
- OSSEC Agent được cài đặt trên các máy cần giám sát, thu thập và gửi log về server.

- OSSEC Server và OSSEC Agent giao tiếp với nhau theo giao thức UDP, cổng 1514.

1. Cài đặt OSSEC

Ở phần này, chúng ta sẽ cài đặt và cấu hình OSSEC trên các máy theo mô hình dưới đây:



a. Cài đặt OSSEC Server

Cài đặt các gói hỗ trợ trước khi cài đặt OSSEC

```
sudo apt-get install build-essential make zlib1g-dev libpcre2-dev libevent-dev libssl-dev

$ sudo apt install libsystemd-dev
```

Tải xuống OSSEC, giải nén và cài đặt

```
$ wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz

$ tar -xvzf 3.7.0.tar.gz

$ cd ossec-hids-3.7.0

$ sh install.sh
```

Trong giao diện cài đặt, chúng ta được yêu cầu trả lời một vài câu hỏi.
Với ngôn ngữ, nhấn Enter để chọn ngôn ngữ mặc định là tiếng anh.
Sau khi chọn ngôn ngữ, chúng ta sẽ thấy một vài thông tin cơ bản về OSSEC

```
OSSEC HIDS v3.7.0 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.

  - System: Linux VM 5.4.0-54-generic
  - User: root
  - Host: VM


  -- Press ENTER to continue or Ctrl-C to abort. --
```

Tiếp theo, với câu hỏi về loại OSSEC mà chúng ta mong muốn cài đặt, hãy nhập ***server*** và nhấn Enter.

```
1- What kind of installation do you want (server, agent, local, hybrid or help)? server
```

Với các cài đặt liên quan tới kiểm tra tính toàn vẹn, phát hiện rootkit, và phản hồi chủ động, có thể nhấn Enter để lựa chọn cài đặt theo mặc định.

```
2- Setting up the installation environment.

  - Choose where to install the OSSEC HIDS [/var/ossec]:

- Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS:

  3.1- Do you want e-mail notification? (y/n) [y]:

- What's your e-mail address? sample@example.com

3.2- Do you want to run the integrity check daemon? (y/n) [y]:

- Running syscheck (integrity check daemon).

3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

- Running rootcheck (rootkit detection).

3.4- Active response allows you to execute a specific command based on the events received.

   Do you want to enable active response? (y/n) [y]:

   Active response enabled.

Do you want to enable the firewall-drop response? (y/n) [y]:

- firewall-drop enabled (local) for levels >= 6

   - Default white list for the active response:

      - 8.8.8.8
```

```
      - 8.8.4.4

   - Do you want to add more IPs to the white list? (y/n)? [n]:

3.6- Setting the configuration to analyze the following logs:

    -- /var/log/auth.log

    -- /var/log/syslog

    -- /var/log/dpkg.log

 - If you want to monitor any other file, just change

   the ossec.conf and add a new localfile entry.

   Any questions about the configuration can be answered

   by visiting us online at http://www.ossec.net .

   --- Press ENTER to continue ---
```

b. Cài đặt OSSEC Agent

Tương tự như cài đặt OSSEC Agent, chúng ta cũng cần cài đặt các gói hỗ trợ trước khi cài đặt OSSEC

```
sudo apt-get install build-essential make zlib1g-dev libpcre2-dev libevent-dev libssl-dev

$ sudo apt install libsystemd-dev
```

Tải xuống OSSEC, giải nén và cài đặt

```
$ wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz

$ tar -xvzf 3.7.0.tar.gz

$ cd ossec-hids-3.7.0

$ sh install.sh
```

Chọn ngôn ngữ tiếng anh như mặc định
Sau khi chọn ngôn ngữ, chúng ta sẽ thấy một vài thông tin cơ bản về OSSEC

```
OSSEC HIDS v3.7.0 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.

  - System: Linux VM 5.4.0-54-generic
  - User: root
  - Host: VM


  -- Press ENTER to continue or Ctrl-C to abort. --
```

Tiếp theo, với câu hỏi về loại OSSEC mà chúng ta mong muốn cài đặt, hãy nhập ***agent*** và nhấn Enter.

```
1- What kind of installation do you want (server, agent, local, hybrid or help)? Agent
```

Với các cài đặt liên quan tới kiểm tra tính toàn vẹn, phát hiện rootkit, và phản hồi chủ động, có thể nhấn Enter để lựa chọn cài đặt theo mặc định.

Như vậy, chúng ta đã cài đặt thành công OSSEC Server và OSSEC Agent. Ở phần tiếp theo, chúng ta sẽ kết nối Server và Agent.

c. Kết nối Server-Agent

Để kết nối Server và Agent, chúng ta sử dụng manage_agent. Các bước thực hiện bao gồm:

- Chạy manage_agents trên OSSEC server
  - Thêm agent
  - Extract key cho agent và sao chép key vào máy chủ agent
- Chạy manage_agents trên OSSEC agent
  - Import key đã extract
- Restart tiến trình quản lý OSSEC trên server và Start Agent mới.

Lưu ý, trong quá trình thực hiện kết nối server và client, nhớ mở port trên firewall để server có thể giao tiếp với agent thông qua UDP/1514.

Đầu tiên, trên OSSEC server, khởi chạy manage_agents bằng câu lệnh sau:

```
$ sudo /var/ossec/bin/manage_agents

****************************************

* OSSEC HIDS v2.5-SNP-100809 Agent manager.     *

* The following options are available: *

****************************************

   (A)dd an agent (A).

   (E)xtract key for an agent (E).
```

```
   (L)ist already added agents (L).

   (R)emove an agent (R).

   (Q)uit.

Choose your action: A,E,L,R or Q:
```

Nhập vào **A** để thêm agent mới

```
Choose your action: A,E,L,R or Q: A
```

Đặt tên cho Agent mới:

```
- Adding a new agent (use '\q' to return to the main menu). Please provide the following: * A name for the new agent: agent1
```

Chỉ định IP cho Agent:

```
* The IP Address of the new agent: 10.0.2.15/24
```

Nhấn Enter để đặt ID mặc định cho Agent. Sau đó xác nhận các thông tin cài đặt.

```
****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: agent1
   * The IP Address of the new agent: 10.0.2.15/24
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:agent1
   IP Address:10.0.2.15/24

Confirm adding it?(y/n):
```

Sau khi thêm một agent, một key sẽ được tạo. Key này phải được sao chép vào agent. Để trích xuất khóa, hãy sử dụng tùy chọn **e** trong màn hình bắt đầu của manage_agents. Bạn sẽ được cung cấp danh sách tất cả các agent trên máy chủ. Để trích xuất key cho một agent, chỉ cần nhập ID agent.

```
****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: agent1, IP: 10.0.2.15/24
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIGFnZW50MSAxMC4wLjIuMTUvMjQgMzBiY2E2NTE3ODc5Yzc3ODczZDljMmU4YWQ3ZDdlY2IzMDhm
MzdlNGVjODE0ZDlmZWU5MDdhNjBmYjE1Yjk3NQ==

** Press ENTER to return to the main menu.
```

Tiếp theo, chúng ta sẽ thực hiện import key trên OSSEC Agent. Trên Agent, chạy manage_agents

```
$ sudo /var/ossec/bin/manage_agents

****************************************

* OSSEC HIDS v2.5-SNP-100809 Agent manager.     *

* The following options are available: *

****************************************

   (A)dd an agent (A).

   (E)xtract key for an agent (E).

   (L)ist already added agents (L).

   (R)emove an agent (R).

   (Q)uit.

Choose your action: A,E,L,R or Q:
```

Chọn **I** và thực hiện import key đã được extract từ Server.

```
****************************************
* OSSEC HIDS v3.7.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAxIGFnZW50MSAxMC4wLjIuMTUvMjQgMzBiY2E2NTE3ODc
5Yzc3ODczZDljMmU4YWQ3ZDdlY2IzMDhmMzdlNGVjODE0ZDlmZWU5MDdhNjBmYjE1Yjk3NQ==

Agent information:
   ID:001
   Name:agent1
   IP Address:10.0.2.15/24

Confirm adding it?(y/n): y
```

Để thay đổi có hiệu lực, thực hiện restart OSSEC ở cả server và agent bằng lệnh sau

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

2. Cấu hình OSSEC

Các cấu hình của OSSEC được lưu trong tập tin **/var/ossec/etc/ossec.conf**, đóng vai trò chính trong việc tùy chỉnh và tối ưu hóa hệ thống bảo mật.

Trong phần này, chúng ta sẽ tiến hành cấu hình và thử nghiệm các kịch bản khác nhau để kiểm tra các tính năng chính của OSSEC, bao gồm:

- **Giám sát log:** Giám sát các log ứng dụng và hệ thống để phát hiện hành vi bất thường
- **Kiểm tra tính toàn vẹn**: Giám sát các tập tin quan trọng để phát hiện các thay đổi trái phép, bảo đảm dữ liệu luôn toàn vẹn.
- **Phát hiện xâm nhập**: Theo dõi các nhật ký hệ thống và cảnh báo khi phát hiện các hoạt động đáng ngờ.
- **Phản ứng chủ động**: Thực hiện các hành động tự động, như chặn các IP có hành vi đáng ngờ, để giảm thiểu nguy cơ bị tấn công.

Bằng cách triển khai và kiểm tra các kịch bản này, chúng ta sẽ đánh giá hiệu quả của OSSEC trong việc giám sát và bảo vệ hệ thống, cũng như tối ưu cấu hình để đạt hiệu suất bảo mật tốt nhất.

a. Giám sát log

OSSEC có thể giám sát các tập tin nhật ký từ các ứng dụng và hệ thống để phát hiện các hành vi bất thường. Theo mặc định, một vài tập tin log của hệ thống đã được cấu hình sẵn trong tập tin cấu hình ở mục lolcalfile. Để cấu hình các log file cần giám sát, ta chỉ cần định nghĩa format của log file và vị trí lưu file log.

```
<localfile>
     <location>/var/log/messages</location>
     <log_format>syslog</log_format>
</localfile>
```

Ví dụ trên là cấu hình giám sát tập tin log được lưu ở /var/log/messages. Tập tin này thường chứa các thông báo hệ thống và các bản ghi chung của nhiều dịch vụ trên hệ thống Linux.

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

b. Giám sát tính toàn vẹn của tập tin

Trong OSSEC, **Syscheck** là quy trình kiểm tra tính toàn vẹn, đảm nhiệm nhiệm vụ quét định kỳ các tệp tin và mục đăng ký (Registry) (trên Windows) để phát hiện các thay đổi bất thường. Điều này đặc biệt quan trọng vì hầu hết các loại tấn công và vectơ tấn công, từ vi-rút đến rootkit, đều để lại dấu vết trên hệ thống bằng cách thay đổi hoặc chỉnh sửa một số tệp hoặc cấu phần hệ điều hành.

OSSEC giúp đảm bảo tính toàn vẹn của hệ thống bằng cách so sánh tổng kiểm tra (checksum) MD5 hoặc SHA1 của các tệp quan trọng. Cụ thể, các tác nhân (agents) sẽ quét hệ thống sau mỗi vài giờ (do người dùng tùy chỉnh) và gửi các tổng kiểm tra này đến máy chủ OSSEC. Máy chủ lưu trữ các bản kiểm tra và kiểm tra từng sự thay đổi. Nếu phát hiện có chỉnh sửa, hệ thống sẽ kích hoạt cảnh báo để thông báo cho quản trị viên về sự cố.

```
<syscheck>

  <directories check_all="yes">/etc</directories>

  <directories>/bin</directories>

  <directories>/sbin</directories>

  <ignore>/etc/mtab</ignore> <!-- Loại bỏ một số tệp không cần giám sát -->

</syscheck>
```

Đoạn ví dụ trên kiểm tra tính toàn vẹn toàn bộ tập tin và thư mục con của thư mục /etc ngoại trừ thư mục /etc/mtab và kiểm tra tính toàn vẹn của các tập tin trong 2 thư mục /bin và /sbin.

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.

c. Phản ứng chủ động

Tính năng này cho phép OSSEC thực hiện các hành động tự động, như chặn IP khi phát hiện tấn công brute-force, gửi mail cảnh báo khi đăng nhập thất bại nhiều lần…
Cấu hình phản ứng chủ động của OSSEC được thể hiện trong tag <ossec_config>

```
<ossec_config>

    <command>

        <!--

        Command options here

        -->

    </command>

    <active-response>

        <!--

        active-response options here

        -->

    </active-response>

</ossec_config>
```

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.

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.

- Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
- Ví dụ: [NT140.P12.ANTT.1]-Lab1_2252xxxx_2252yyyy.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!