HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Lab: idr-wazuh-bruteforce

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: IDR-WAZUH-BRUTEFORCE

1. Mục đích

- Có được kiến thức và kĩ năng thực tế trong việc phát hiện, cảnh báo và phản ứng trước các cuộc tấn công SSH brute-force bằng cách kết hợp hệ thống giảm sát Wazuh và cơ chế chặn tại host bằng iptables.

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 và các phương thức dò quét mạng phổ biến như nmap, hydra.
- Có kiến thức nền tảng về bảo mật hệ thống, về các công cụ Wazuh và iptables.

3. Nội dung bài lab

- Trước khi khởi động bài lab, cần đảm bảo labtainer được cấu hình như sau:
    - Memory (RAM): 8GB
    - Processors: 2
    - Hard Disk: 60GB
- Khởi động bài lab:

labtainer -r idr-wazuh-bruteforce

(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, bốn terminal ảo sẽ xuất hiện, một máy đại diện cho hệ thống **wazuh server**, một máy đại diện cho máy **agent** thuộc wazuh server, hai máy đại diện cho hai máy **attacker**.
- Để kiểm tra địa chỉ IP của 4 máy, gõ lệnh sau trên từng máy:

ifconfig

3.1. Cài đặt hệ thống Wazuh

- Tại máy **wazuh server,** sinh viên chạy lệnh sau để cài đặt Wazuh:

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

- Sau khi hoàn tất quá trình cài đặt, hệ thống sẽ hiển thị thông tin đăng nhập và thông báo cài đặt thành công.
- Tiếp theo, sinh viên thực hiện cài đặt máy agent của hệ thống Wazuh server. Để vào được giao diện web của Wazuh server, sinh viên cần cập nhật trình duyệt firefox:

sudo apt install --only-upgrade firefox

- Sau khi cập nhật xong, sinh viên bật trình duyệt firefox trong terminal của Wazuh server:

firefox &

- Trong trình duyệt, sinh viên truy cập vào đường dẫn sau:

https://<địa chỉ IP máy Wazuh server>:443

- Lúc này, trình duyệt sẽ hiển thị cảnh báo. Sinh viên ấn vào "Advanced" và chọn "Accept the Risk and Continue" để tiếp tục truy cập vào đường dẫn này.
- Khi giao diện đăng nhập của hệ thống Wazuh hiển thị, sinh viên cần đăng nhập bằng tài khoản đã được cung cấp khi chạy lệnh cài đặt hệ thống. Sau khi đăng nhập thành công, giao diện dashboard của Wazuh sẽ hiện ra.
- Sinh viên ấn vào nút "Deploy new agent" để thêm một máy làm agent. Sinh viên thực hiện cấu hình agent như sau:
    - Chọn OS: DEB amd64
    - Địa chỉ server: Nhập địa chỉ của máy server
    - Tên agent: Đặt tên cho agent để dễ phân biệt
    - Group: Để mặc định
- Sau khi nhập xong các mục, hệ thống sẽ hiển thị lệnh sử dụng để cài đặt máy agent. Sinh viên copy lệnh đó và chạy lệnh trên terminal của máy agent.
- Sau khi chạy xong lệnh cài đặt, sinh viên chạy tiếp 3 lệnh sau trên terminal của máy agent để hoàn tất việc cài đặt:

sudo systemctl daemon-reload

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

- Sinh viên có thể vào lại web của Wazuh để kiểm tra agent đã được thêm vào chưa.

3.2. Tấn công brute-force

- Tại máy agent, sinh viên chạy lệnh sau để bật ssh:

sudo systemctl start ssh

- Vào máy attacker và cài đặt hydra:

sudo apt install hydra -y

- Trong bài thực hành này, attacker đã biết địa chỉ IP của máy agent. Sinh viên chạy lệnh nmap để quét các cổng của máy agent đang mở:

nmap -Pn -p- <địa chỉ IP>

- Khi chạy lệnh nmap, attacker biết cổng 22 của máy agent đang mở.
- Attacker tạo một file txt với 10 dòng mật khẩu ngẫu nhiên. Sau khi tạo xong file txt, attacker chạy lệnh hydra để thực hiện tấn công brute-force lên máy agent:

sudo hydra -l root -P <tên file.txt> <địa chỉ IP máy agent> ssh

3.3. Phát hiện và phản ứng sự cố

- Sau khi attacker tấn công xong, sinh viên chuyển sang trang web của hệ thống Wazuh, ấn vào phần "Active" (các máy agent đang hoạt động), ấn vào máy agent trong danh sách => ấn vào "Threat Hunting" => "Event". Tại màn hình này, sinh viên sẽ thấy danh sách các sự kiện trong máy agent, trong đó có những dòng cảnh báo máy agent bị tấn công.
- Sinh viên có thể ấn vào icon kính lúp bên trái của dòng cảnh báo đó để xem chi tiết cảnh báo như địa chỉ IP máy tấn công, rule id,… Sinh viên cũng có thể dùng lệnh sau để xem lại các cảnh báo:

sudo tail -n 200 /var/ossec/logs/alerts/alerts.log

- Khi biết máy agent bị tấn công và địa chỉ IP của máy tấn công, máy server báo lại cho máy agent để tạm thời ngăn chặn địa chỉ IP của máy tấn công tiếp tục thực hiện tấn công brute-force:

sudo iptables -I INPUT -s <địa chỉ máy attacker> -j DROP

- Kiểm tra lại danh sách các địa chỉ IP đang bị chặn:

sudo iptables -L -n -v

- Attacker thử tấn công lại và kết quả là không kết nối được với máy agent nữa.

- Dù máy agent đã chặn được địa chỉ IP máy tấn công nhưng không thể đảm bảo được máy agent sẽ không bị các máy attacker khác tấn công. Vì vậy, chúng ta cần cải thiện thêm hệ thống để Wazuh tự động phản ứng khi phát hiện máy bị tấn công brute-force.
- Tại máy Wazuh server, sinh viên mở file /var/ossec/etc/ossec.conf. Trong file này, sinh viên kiểm tra xem trong khối <ossec_config> có khối <command> tên là firewall-drop với cấu hình sau hay không:

```
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

- Khối lệnh này định nghĩa hành động "firewall-drop" mà Wazuh có thể sử dụng để tự động chặn địa chỉ IP tấn công tạm thời hoặc vĩnh viễn, bằng cách thêm quy tắc vào tường lửa của hệ thống.
- Sau khi kiểm tra khối <command> đã có trong file, sinh viên thêm khối <active-response> dưới đây vào tệp cấu hình /var/ossec/etc/ossec.conf trên máy chủ Wazuh:

```
<ossec_config>
  <active-response>
    <disabled>no</disabled>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>5763</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```

- Ý nghĩa của từng dòng lệnh như sau:
  - <ossec_config>: Là phần chính trong tệp cấu hình ossec.conf, bao gồm các thiết lập của Wazuh.

- <active-response>: Module phản ứng tự động mà Wazuh sẽ thực hiện khi một quy tắc nhất định được kích hoạt.
- <disabled>no</disabled>: Tính năng này đang không bị tắt. Nếu để là "yes" thì sẽ bị tắt.
- <command>firewall-drop</command>: Chỉ định tên lệnh mà Wazuh sẽ chạy khi phản ứng được kích hoạt. Tên "firewall-drop" sẽ trỏ tới khối command firewall-drop đã được định nghĩa trước đó. Khi được kích hoạt, hệ thống sẽ chặn địa chỉ IP bằng tường lửa.
- <location>local</location>: Xác định nơi lệnh sẽ được thực thi. Ở đây sử dụng giá trị local thì lệnh sẽ được thực thi ngay trên chính nơi sự kiện được phát hiện.
- <rules_id>5763</rules_id>: Module Active Response sẽ thực thi lệnh nếu quy tắc có ID 5763 được kích hoạt.
- <timeout>: Xác định thời gian hành động phản ứng tự động tồn tại. Trong trường hợp này, module sẽ chặn địa chỉ IP của máy attacker trong vòng 180 giây.

- Khởi động lại Wazuh server:

sudo systemctl restart wazuh-manager

- Để kiểm tra xem hệ thống có phản ứng tự động như lệnh đã thêm vào hay không, sinh viên cài đặt và chạy lại lệnh tấn công brute-force bằng máy attacker2.
- Sau khi chạy lệnh tấn công brute-force đầu tiên trên máy attacker2, sinh viên quay lại web Wazuh trên máy Wazuh server kiểm tra mục "Threat Hunting" của máy agent. Tại đây, sẽ thấy hiển thị thông báo phát hiện tấn công brute-force từ máy attacker2 (ID 5763) và địa chỉ máy attacker2 đã bị chặn (ID 651). Cảnh báo này xuất hiện vì quy tắc có ID 651 là một phần của tệp quy tắc mặc định /var/ossec/ruleset/rules/0015-ossec_rules.xml trên máy chủ Wazuh.
- Nếu cần tạo một script phản ứng tự động (active response) tùy chỉnh thì cần thêm một quy tắc tùy chỉnh tương ứng để phân tích các log phản ứng tự động được tạo ra.
- Ngoài việc cải thiện hệ thống Wazuh, máy agent cũng có thể hạn chế việc SSH trực tiếp dưới role "root". Sinh viên mở file cấu hình SSH /etc/ssh/sshd_config và thay các dòng sau:

PermitRootLogin no

PasswordAuthentication no

ChallengeResponseAuthentication no

PermitEmptyPasswords no

UsePAM yes

PubkeyAuthentication yes

- Kết thúc bài lab:

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

stoplab idr-wazuh-bruteforce

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-bruteforce