Bảng IP

|  |  |  |  |
| --- | --- | --- | --- |
|  | IPv4 | Subnet mask |  |
| Kali linux  (Attacker) | 192.168.30.128 | 255.255.255.0 | VMNET 8(WAN) |
| Server  (Victim) | 192.168.20.20 | 255.255.255.0 | VMNET 2(DMZ) |
| Win7 | 192.168.10.10 | 255.255.255.0 | VMNET 1(LAN) |
| Pfsense  (IDS/IPS Suricata) | 192.168.30.129  192.168.10.100  192.168.20.10 | 255.255.255.0 | VMNET 8(WAN)  VMNET 1(LAN)  VMNET 2(DMZ) |

Kali linux : sử dụng hydra tấn công burte force vào Webserver

Win7: dùng để cấu hình pfsense

Win7

A computer screen shot of a black screen

Description automatically generated

Server

A computer screen with white text

Description automatically generated

Pfsense

A screen shot of a computer

Description automatically generated

Kali

A computer screen shot of a program

Description automatically generated

Tấn công brute force

Attacker

Kiểm tra kết nối tới server

A screenshot of a computer program

Description automatically generated

Tạo list password để tấn công brute force

A computer screen with white text

Description automatically generated

Thêm list các mật khẩu

A screenshot of a computer

Description automatically generated

Sử dụng hydra tấn công brute force vào IP Victim 192.168.20.20 port 22

Với user là admin

hydra -l tamne -P passwords.txt -t 1 192.168.20.20 ssh

A computer screen shot of a computer code

Description automatically generated

 hydra: Tên của công cụ tấn công mạng.

 -l tamne: Tên người dùng hoặc danh sách tên người dùng được sử dụng để thử nghiệm đăng nhập. Trong trường hợp này, tamne là tên người dùng cố gắng đăng nhập.

 -P passwords.txt: Tệp chứa danh sách các mật khẩu được sử dụng để thử nghiệm đăng nhập.

 192.168.20.20: Địa chỉ IP hoặc tên miền của mục tiêu, trong trường hợp này, là địa chỉ IP của máy chủ web.

 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed": Phương thức tấn công HTTP POST và biểu mẫu đăng nhập được sử dụng.

* /dvwa/login.php: Đường dẫn đến biểu mẫu đăng nhập trên trang web.
* username=^USER^&password=^PASS^&Login=Login: Tham số đăng nhập được truyền dưới dạng chuỗi có cấu trúc username=<user>&password=<pass>&Login=Login, trong đó ^USER^ và ^PASS^ sẽ được thay thế bằng tên người dùng và mật khẩu được cung cấp bởi Hydra.
* Login failed: Chuỗi hoặc văn bản chỉ ra rằng đăng nhập không thành công, Hydra sẽ sử dụng nó để kiểm tra xem đăng nhập có thành công hay không.

 -V: Tùy chọn để hiển thị thông tin chi tiết khi thực thi.

alert tcp any any -> 192.168.20.20 22 (msg:" Brute force SSH login attempt "; content:"SSH"; sid:10000004; rev:1;)

A screenshot of a computer

Description automatically generated

 **alert tcp any any -> 192.168.20.20 22**:

* alert: Tạo một cảnh báo.
* tcp: Áp dụng cho lưu lượng TCP.
* any any -> 192.168.20.20 22: Áp dụng cho bất kỳ nguồn nào đến cổng 22 của IP 192.168.20.20.

 **msg:"Brute force SSH login attempt "**:

* msg: Thông điệp cảnh báo sẽ được hiển thị khi quy tắc này được kích hoạt, cho biết rằng có một cố gắng tấn công brute-force đối với việc đăng nhập SSH.

 **content:"SSH":**

* Quy tắc sẽ kiểm tra xem gói tin TCP có chứa từ "SSH" không. Nếu có, quy tắc sẽ được kích hoạt.

 **sid:10000004:**

* sid: Số ID của quy tắc, phải là duy nhất trong tệp quy tắc.
* 10000004: Số ID được chỉ định cho quy tắc này.

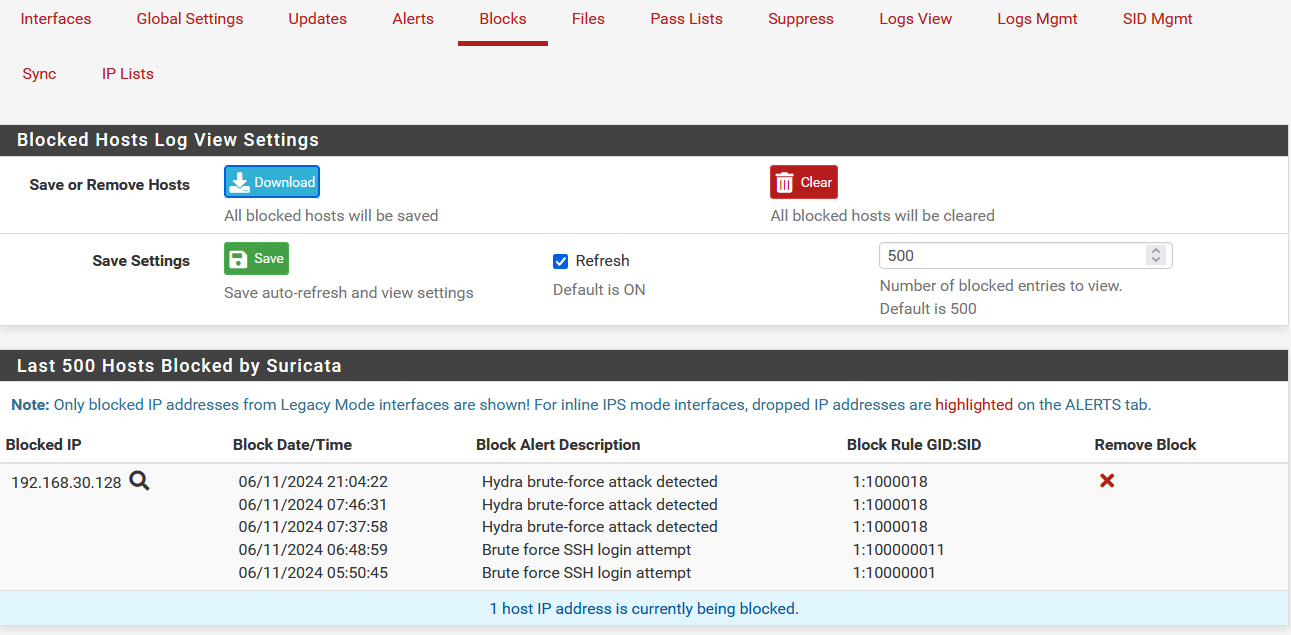
 **rev:1**:

* rev: Số phiên bản của quy tắc.
* 1: Phiên bản đầu tiên của quy tắc này

drop tcp any any -> 192.168.20.20 22 (msg:"Brute force SSH login attempt"; flow:to\_server,established; content:"SSH-"; threshold: type limit, track by\_src, count 5, seconds 10; sid:100000011; rev:1;)

A screenshot of a computer

Description automatically generated



**drop tcp any any -> 192.168.20.20 22**:

* drop: chặn gói tin.
* tcp: Áp dụng cho lưu lượng TCP.
* any any -> 192.168.20.20 22: Áp dụng cho bất kỳ nguồn nào đến cổng 22 của IP 192.168.20.20.

 **msg:"Brute force SSH login attempt "**:

* msg: Thông điệp cảnh báo sẽ được hiển thị khi quy tắc này được kích hoạt, cho biết rằng có một cố gắng tấn công brute-force đối với việc đăng nhập SSH.

 **flow,established**:

* flow: Xác định hướng và trạng thái của lưu lượng mạng.
* to\_server: Lưu lượng gửi đến máy chủ.
* established: Lưu lượng trong một kết nối đã được thiết lập.

 **content:"SSH":**

* Quy tắc sẽ kiểm tra xem gói tin TCP có chứa từ "SSH" không. Nếu có, quy tắc sẽ được kích hoạt.

 **threshold, track by\_src, count 10, seconds 5**:

* threshold: Xác định điều kiện để kích hoạt cảnh báo dựa trên tần suất.
* type limit: Loại ngưỡng là "limit", có nghĩa là ngưỡng sẽ được áp dụng dựa trên số lượng sự kiện.
* track by\_src: Theo dõi số lần xuất hiện dựa trên địa chỉ nguồn (IP của máy khách).
* count 10: Nếu mẫu xuất hiện 10 lần trong khoảng thời gian xác định, thì cảnh báo sẽ được kích hoạt.
* seconds 5: Khoảng thời gian theo dõi là 5 giây.

 **sid: 100000011:**

* sid: Số ID của quy tắc, phải là duy nhất trong tệp quy tắc.
* 10000004: Số ID được chỉ định cho quy tắc này.

 **rev:1**:

* rev: Số phiên bản của quy tắc.
* 1: Phiên bản đầu tiên của quy tắc này

hydra -l admin -P password.txt 192.168.20.20 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V

 hydra: Đây là tên của công cụ tấn công.

 -l admin: Tùy chọn này chỉ định tên người dùng (admin) mà Hydra sẽ sử dụng để thử đăng nhập.

 -P password.txt: Tùy chọn này chỉ định tệp chứa danh sách các mật khẩu mà Hydra sẽ thử.

 192.168.20.20: Đây là địa chỉ IP của mục tiêu.

 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed": Đây là mẫu yêu cầu HTTP POST để đăng nhập vào trang web DVWA. Hydra sẽ sử dụng mẫu này để thử đăng nhập. Cụ thể:

* /dvwa/login.php: Đây là đường dẫn đến trang đăng nhập trên trang web DVWA.
* username=^USER^&password=^PASS^&Login=Login: Đây là dữ liệu được gửi qua yêu cầu POST. ^USER^ và ^PASS^ là các giá trị sẽ được thay thế bằng tên người dùng và mật khẩu từ danh sách được cung cấp.
* Login failed: Đây là dấu hiệu để Hydra xác định xem việc đăng nhập thành công hay thất bại.

 -V: Tùy chọn này kích hoạt chế độ chi tiết (verbose), cho phép Hydra hiển thị kết quả chi tiết của mỗi thử nghiệm đăng nhập.

A screen shot of a computer

Description automatically generated

# Quy tắc phát hiện brute-force sử dụng Hydra trên HTTP POST

alert http any any -> any any (msg:"Hydra brute-force attack detected"; flow:to\_server,established; content:"/dvwa/login.php"; http\_uri; content:"username=admin"; fast\_pattern; http\_client\_body; threshold:type both, track by\_src, count 10, seconds 5; classtype:attempted-admin; sid:1000017; rev:1;)

A screenshot of a computer

Description automatically generated

 **alert http any any -> any 80**:

* alert: Tạo một cảnh báo.
* http: Áp dụng cho lưu lượng HTTP.
* any any -> any 80: Áp dụng cho bất kỳ nguồn nào đến cổng 80 (HTTP) của bất kỳ đích nào.

 **msg:"Hydra brute-force attack detected"**:

* msg: Thông điệp cảnh báo sẽ hiển thị khi quy tắc này được kích hoạt. Ở đây, thông điệp là "Hydra brute-force attack detected".

 **flow,established**:

* flow: Xác định hướng và trạng thái của lưu lượng mạng.
* to\_server: Lưu lượng gửi đến máy chủ.
* established: Lưu lượng trong một kết nối đã được thiết lập.

 **content:"/dvwa/login.php"; http\_uri;**:

* content: Tìm kiếm một chuỗi cụ thể trong gói tin.
* "/dvwa/login.php": Đường dẫn URI đích trong yêu cầu HTTP.
* http\_uri: Xác định vị trí nội dung trong URI của HTTP.

 **content:"username=admin"; fast\_pattern; http\_client\_body;**:

* content: Tìm kiếm một chuỗi cụ thể trong gói tin.
* "username=admin": Nội dung của trường username với giá trị admin.
* fast\_pattern: Đặt nội dung này như là một mẫu nhanh, giúp tăng tốc quá trình tìm kiếm.
* http\_client\_body: Xác định vị trí nội dung trong thân của yêu cầu HTTP (POST data).

 **threshold both, track by\_src, count 10, seconds 5**:

* threshold: Xác định điều kiện để kích hoạt cảnh báo dựa trên tần suất.
* type both: Kiểm tra ngưỡng cho cả số lần xuất hiện của mẫu trong một kết nối cũng như trong các kết nối khác nhau.
* track by\_src: Theo dõi số lần xuất hiện dựa trên địa chỉ nguồn (IP của máy khách).
* count 10: Nếu mẫu xuất hiện 10 lần trong khoảng thời gian xác định, thì cảnh báo sẽ được kích hoạt.
* seconds 5: Khoảng thời gian theo dõi là 5 giây.

 **classtype:**

* classtype: Phân loại loại hình tấn công.
* attempted-admin: Thử xâm nhập dưới quyền quản trị.

 **sid:1000017**:

* sid: Số ID của quy tắc, phải là duy nhất trong tệp quy tắc.
* 1000017: Số ID được chỉ định cho quy tắc này.

 **rev:1**:

* rev: Số phiên bản của quy tắc.
* 1: Phiên bản đầu tiên của quy tắc này

# Quy tắc chặn brute-force sử dụng Hydra trên HTTP POST

drop http any any -> any any (msg:"Hydra brute-force attack detected"; flow:to\_server,established; content:"/dvwa/login.php"; http\_uri; content:"username=admin"; fast\_pattern; http\_client\_body; threshold:type both, track by\_src, count 10, seconds 5; classtype:attempted-admin; sid:1000018; rev:2;)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

 **drop http any any -> any 80**:

* drop: Loại bỏ gói tin mạng.
* http: Áp dụng cho lưu lượng HTTP.
* any any -> any 80: Áp dụng cho bất kỳ nguồn nào đến cổng 80 (HTTP) của bất kỳ đích nào.

 **msg:"Hydra brute-force attack detected"**:

* msg: Thông điệp cảnh báo sẽ hiển thị khi quy tắc này được kích hoạt. Ở đây, thông điệp là "Hydra brute-force attack detected".

 **flow,established**:

* flow: Xác định hướng và trạng thái của lưu lượng mạng.
* to\_server: Lưu lượng gửi đến máy chủ.
* established: Lưu lượng trong một kết nối đã được thiết lập.

 **content:"/dvwa/login.php"; http\_uri;**:

* content: Tìm kiếm một chuỗi cụ thể trong gói tin.
* "/dvwa/login.php": Đường dẫn URI đích trong yêu cầu HTTP.
* http\_uri: Xác định vị trí nội dung trong URI của HTTP.

 **content:"username=admin"; fast\_pattern; http\_client\_body;**:

* content: Tìm kiếm một chuỗi cụ thể trong gói tin.
* "username=admin": Nội dung của trường username với giá trị admin.
* fast\_pattern: Đặt nội dung này như là một mẫu nhanh, giúp tăng tốc quá trình tìm kiếm.
* http\_client\_body: Xác định vị trí nội dung trong thân của yêu cầu HTTP (POST data).

 **threshold**

**both, track by\_src, count 10, seconds 5**:

* threshold: Xác định điều kiện để kích hoạt cảnh báo dựa trên tần suất.
* type both: Kiểm tra ngưỡng cho cả số lần xuất hiện của mẫu trong một kết nối cũng như trong các kết nối khác nhau.
* track by\_src: Theo dõi số lần xuất hiện dựa trên địa chỉ nguồn (IP của máy khách).
* count 10: Nếu mẫu xuất hiện 10 lần trong khoảng thời gian xác định, thì cảnh báo sẽ được kích hoạt.
* seconds 5: Khoảng thời gian theo dõi là 5 giây.

 **classtype:**

* classtype: Phân loại loại hình tấn công.
* attempted-admin: Thử xâm nhập dưới quyền quản trị.

 **sid:1000018**:

* sid: Số ID của quy tắc, phải là duy nhất trong tệp quy tắc.
* 1000018: Số ID được chỉ định cho quy tắc này.

 **rev:2**:

* rev: Số phiên bản của quy tắc.
* 2: Phiên bản đầu tiên của quy tắc này