BÁO CÁO THỰC HÀNH

**Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

**Lab 3: Viết rule trên Snort**

*GVHD: Đỗ Hoàng Hiển*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT204.O21.ATCL.2- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Huỳnh Minh Tân Tiến | 21521520 | [21521520@gm.uit.edu.vn](mailto:21521520@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |
| 4 | **Yêu cầu 4** | 100% |
| 5 | **Yêu cầu 5** | 100% |

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

**Yêu cầu 1.1 Ngăn chặn tấn công ICMP Flood**

* Viết Snort rule thực hiện giới hạn gói ICMP đến máy Victim. Ngưỡng (threshold) là không quá 23 gói/5s. - -
* Sử dụng công cụ hping3 trên máy Attacker để thực hiện tấn công.
* Kiểm tra kết quả trước và sau khi cài đặt rule.

Trước khi set rule, ta tấn công ICMP Flood trên máy Kali bình thường bằng câu lệnh:

*sudo hping3 --icmp -i u50000 -c 1000000*

Trong đó:

* --icmp: Đây là tùy chọn để chỉ định loại gói tin ICMP.
* -i u50000: Đây là tùy chọn để thiết lập khoảng thời gian giữa các gói ICMP. Trong ví dụ này, tôi đặt khoảng thời gian là 50.000 micro giây (tương đương với 50ms) giữa các gói. Bạn có thể điều chỉnh giá trị này nếu cần.
* -c 1000000: Đây là tùy chọn để chỉ định số lượng gói tin ICMP sẽ gửi đi. Trong ví dụ này, tôi đặt số lượng gói là 1.000.000. Bạn cũng có thể điều chỉnh giá trị này tùy ý.

A screenshot of a computer

Description automatically generated

Ta set rule ngăn chặn ICMP Flood trên Snort như sau:

*drop icmp any any -> 192.168.3.200 any (msg:"Threshold Exceeded - ICMP Flood"; itype:8; detection\_filter:track by\_src, count 23, seconds 5; sid:100; rev:1;)*

Trong đó:

* drop: Rule này sẽ loại bỏ các gói tin ICMP khi điều kiện được kích hoạt thay vì tạo ra cảnh báo.
* icmp any any -> 192.168.3.200 any: Rule sẽ xác định và loại bỏ tất cả các gói ICMP từ bất kỳ nguồn nào đến máy Victim có địa chỉ IP là 192.168.3.200.
* msg:"Threshold Exceeded - ICMP Flood": Một thông điệp cảnh báo được ghi lại khi rule này được kích hoạt, báo hiệu rằng một cuộc tấn công ICMP flood đã được phát hiện.
* itype:8: Điều kiện này chỉ áp dụng cho các gói ICMP echo request (type 8). Điều này đảm bảo rằng rule chỉ áp dụng cho các gói ICMP ping.
* detection\_filter:track by\_src, count 23, seconds 5: Thiết lập ngưỡng cho rule. Nó cho phép không quá 23 gói ICMP từ mỗi nguồn (by\_src) trong mỗi khoảng thời gian 5 giây.
* sid:100: ID duy nhất của rule.
* rev:1: Số phiên bản của rule.

Sau khi set rule, ta sẽ được kết quả:

A screenshot of a computer

Description automatically generated

**Yêu cầu 1.2 Chỉ cho phép truy cập đến các dịch vụ đang chạy trên Victim**

* Sử dụng nmap quét các cổng đang mở trên máy Victim.
* Viết Snort rule chỉ cho phép các máy truy cập đến các port đang mở của máy Victim.
* Chặn tất cả các port còn lại.
* Sử dụng công cụ telnet hoặc nmap trên máy Attacker thực hiện tấn công.
* Kiểm tra kết quả trước và sau khi cài đặt rule.

Sử dụng nmap quét các cổng đang mở trong khoảng 1-1000 trên máy Victim

A screenshot of a computer

Description automatically generated

Trước khi set rule, ta kiểm tra bằng cách telnet đến máy victim

A screenshot of a computer

Description automatically generated

Ta set rule chỉ cho truy cập các port 21, 22, 23, 25, 53, 80:

*drop tcp any any -> 192.168.3.200 21,22,23,25,53,80] (msg:"Drop on access to*

*ports outside port 21,22,23,25,53,80"; sid:1001; rev:1;)*

Trong đó:

* drop: Rule này sẽ loại bỏ các gói tin khi điều kiện được kích hoạt thay vì tạo ra cảnh báo.
* tcp any any -> 192.168.3.200: Rule sẽ xác định và loại bỏ tất cả các gói TCP từ bất kỳ nguồn nào đến máy Victim có địa chỉ IP là 192.168.3.200.
* ![21,22,23,25,53,80]: Điều kiện này chỉ ra rằng các cổng không phải là 21, 22, 23, 25, 53 và 80. Dấu "!" được sử dụng để phủ định các cổng này.
* msg:"Drop on access to ports outside port 21,22,23,25,53,80": Một thông điệp cảnh báo được ghi lại khi rule này được kích hoạt.
* sid:1001: ID duy nhất của rule.
* rev:1: Số phiên bản của rule.

Sau khi set rule, ta chạy lại snort thì ta thấy port 111 không còn truy cập được nữa, mà port 21 vẫn truy cập được bình thường

![A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Yêu cầu 1.3 Ngăn chặn tấn công dò mật khẩu trên ứng dụng Web**

* Truy cập vào ứng dụng web Mutillidae (/mutillidae/index.php?page=login.php) trên máy Victim. Viết Snort rule ngăn chặn tấn công dò mật khẩu đăng nhập trên ứng dụng web này. Lưu ý: chỉ chặn dò mật khẩu, ứng dụng web vẫn phải truy cập bình thường. - -
* Sử dụng công cụ hydra trên máy Attacker thực hiện tấn công.
* Kiểm tra kết quả trước và sau khi cài đặt rule.

Truy cập vào ứng dụng web Mutillidae (/mutillidae/index.php?page=login.php) trên máy Victim

A screenshot of a computer

Description automatically generated

Sử dụng công cụ hydra trên máy Attacker thực hiện tấn công

*hydra -t 4 -V -f -l msfadmin -P password.txt 192.168.3.200 ftp*

Trong đó:

* -t 4 chỉ định số lượng kết nối tối đa đến máy chủ FTP cùng lúc. Trong trường hợp này, giá trị -t 4 chỉ định sử dụng 4 kết nối đến FTP.
* -V cho phép in ra thông tin chi tiết hơn về quá trình kiểm tra mật khẩu.
* -f cho phép dừng khi đã tìm thấy mật khẩu chính xác thay vì tiếp tục kiểm tra các mật khẩu khác.
* -l chỉ định tên đăng nhập (username) cần kiểm tra. Ở đây là msfadmin.
* -P chỉ định đường dẫn đến danh sách mật khẩu (password list) để kiểm tra. Ở đây là password.txt.
* ftp : chỉ định dịch vụ FTP.

A screenshot of a computer

Description automatically generated

Ta set rule chặn dò mật khẩu cho Snort:

*drop tcp any any -> 192.168.3.200 21 (msg:"FTP Brute Force Detected";*

*flow:to\_server,established; content:"PASS"; nocase; threshold:type both, track by\_src,*

*count 5, seconds 60; sid:1000002; rev:1;)*

Trong đó:

* drop: Rule này sẽ loại bỏ các gói tin TCP khi điều kiện được kích hoạt thay vì tạo ra cảnh báo.
* tcp any any -> 192.168.3.200 21: Rule sẽ xác định và loại bỏ tất cả các gói TCP từ bất kỳ nguồn nào đến cổng FTP (cổng 21) của máy Victim có địa chỉ IP là 192.168.3.200.
* msg:"FTP Brute Force Detected": Một thông điệp cảnh báo được ghi lại khi rule này được kích hoạt, báo hiệu rằng một cuộc tấn công brute force trên FTP đã được phát hiện.
* flow:to\_server,established: Rule này chỉ áp dụng cho các gói tin đã thiết lập (established) và đang diễn ra theo hướng từ client đến server.
* content:"PASS"; nocase;: Điều kiện này kiểm tra nội dung của các gói tin để tìm chuỗi "PASS" (một phần của quá trình xác thực trong FTP), bất kể chữ hoa chữ thường (nocase).
* threshold:type both, track by\_src, count 5, seconds 60;: Thiết lập ngưỡng cho rule. Nó cho phép không quá 5 gói tin "PASS" trong mỗi khoảng thời gian 60 giây từ mỗi nguồn (by\_src).
* sid:1000002: ID duy nhất của rule.
* rev:1: Số phiên bản của rule.

Sau khi sử dụng snort rule trên ta được kết quả là brute-force không thành công (trong khi trang web vẫn truy cập được bình thường) và ghi lại log “FTP Brute Force Detected”.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Yêu cầu 1.4 Ngăn chặn tấn các công Path Traversal**

Truy cập vào link <http://192.168.3.200/dvwa/>

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

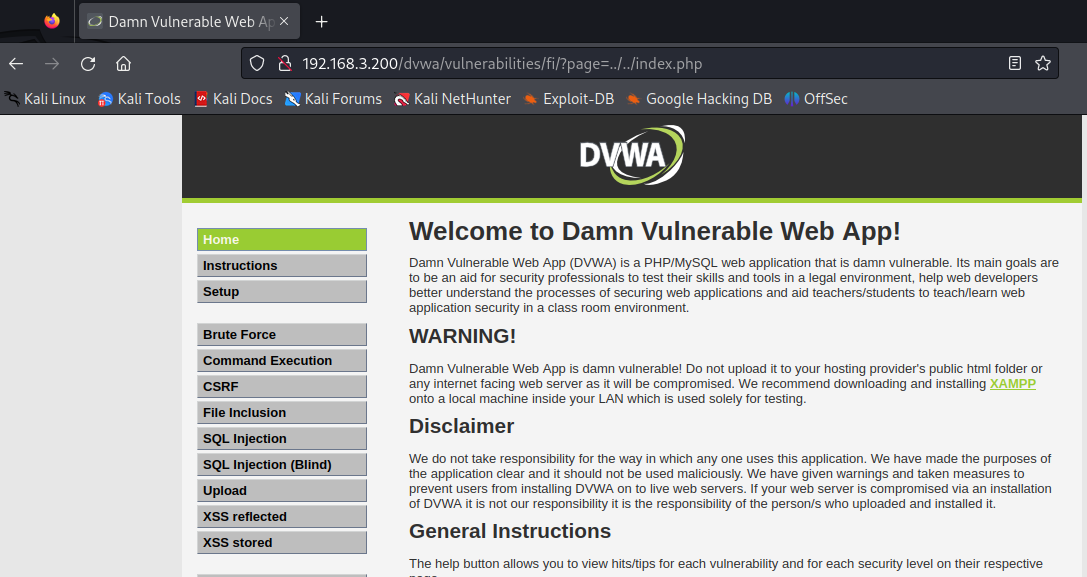
Mô tả được tạo tự động

Truy cập vào File Inclusion để tiến hành tấn công path Travelsal

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

Kết quả tấn công



Ảnh có chứa văn bản, phần mềm, Website, Trang web

Mô tả được tạo tự động

Viết rule snort :

*drop tcp any any -> any any (msg:"Path Traversal Detected"; flow:to\_server,established; content:"GET"; http\_method; pcre:"/(?i)\/(?:\.+\/)+/U"; sid:1000021;)*

* Drop tcp any any -> any any: Khi gói tin TCP được gửi từ bất kỳ nguồn nào (any any) đến bất kỳ đích nào (any any).
* (msg:"Path Traversal Detected";): Thông điệp cảnh báo sẽ được hiển thị khi rule được kích hoạt.
* flow:to\_server,established;: Luồng của gói tin là từ client đến server và đã thiết lập.
* content:"GET"; http\_method;: Nội dung của gói tin HTTP là "GET".
* pcre:"/(?i)\/(?:\.+\/)+/U";: Sử dụng Perl-Compatible Regular Expression (PCRE) để so khớp với URL chứa các chuỗi ../ (tượng trưng cho path traversal). (?i) là flag cho việc không phân biệt chữ hoa chữ thường, \/(?:\.+\/)+ sẽ so khớp với bất kỳ chuỗi ../ liên tiếp nào. Trong đó, \/ so khớp với / và (?:\.+\/)+ so khớp với một hoặc nhiều dấu chấm (.) theo sau bởi /, cả nhóm này có thể lặp lại nhiều lần.
* sid:1000021;: ID của rule.

Kết quả:

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

**Yêu cầu 1.5 Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công**

**Kịch bản 1:** SSH bruteforce

Sử dụng module auxiliary/scanner/ssh/ssh\_login trên msfconsole để thực hiện tấn công.

A screenshot of a computer screen

Description automatically generated

Snort rule để chặn tấn công:

*drop tcp any any -> 192.168.3.200 22 (msg:"Possible SSH Brute Force Attack"; flags:S; threshold:type both, track by\_src, count 2,*

*seconds 2; sid:10003; rev:1;)*

Trong đó:

* drop tcp any any -> $HOME\_NET 22: Phần này chỉ định lưu lượng mà quy tắc này đang nhắm đến. Nó tìm kiếm lưu lượng TCP (tcp) từ bất kỳ địa chỉ IP nguồn (any) và cổng nguồn (any), được điều hướng đến 192.168.3.200 trên cổng 22, đây là cổng tiêu chuẩn cho lưu lượng SSH (Secure Shell).
* (msg:"Possible SSH Brute Force Attack";): Phần này cung cấp một tin nhắn mô tả sẽ được ghi lại khi quy tắc được kích hoạt. Trong trường hợp này, nó đang chỉ ra rằng có thể phát hiện cuộc tấn công ăn cắp mật khẩu SSH.
* flags:S: Điều này chỉ định rằng quy tắc chỉ nên phù hợp với các gói tin TCP có cờ SYN được thiết lập. Trong giao tiếp TCP, cờ SYN được thiết lập trong bước bắt tay ban đầu của một kết nối.
* threshold:type both, track by\_src, count 2, seconds 2: Phần này xác định ngưỡng để kích hoạt quy tắc. Nó chỉ định rằng quy tắc nên theo dõi các sự kiện (track by\_src) dựa trên địa chỉ IP nguồn, và nếu nhiều hơn 2 sự kiện xảy ra trong một khoảng thời gian 2 giây (seconds 2), quy tắc sẽ được kích hoạt.
* sid:10002: Đây là định danh duy nhất cho quy tắc Snort. Nó được sử dụng để phân biệt quy tắc này với các quy tắc khác.
* rev:1: Đây là số phiên bản của quy tắc. Nó cho biết rằng đây là phiên bản đầu tiên của quy tắc cụ thể này.

Kết quả sau khi chạy rule và thực hiện lại tấn công:A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

**Kịch bản 2:** Khai thác lỗ hổng dịch vụ Samba trên máy victim để tạo tcp reverse shell cho attacker.

Dùng module exploit.multi/samba/usermap\_script để script payload

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Set RHOST thành victim 192.168.3.200 và tấn công

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Viết snort rule detect:

Để có thể viết được snort rule để detect cần phân tích xem Kali đã tấn công victim như nào:

Dùng wireshark để bắt các gói tin đến máy victim và phân tích:

Target vào các packet có src là kali: 10.81.3.100 và des là victim 192.168.3.200 với protocol SMB:

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động

Tại value account có payload chứa reverse nên sẽ tập trung vào việc filter các packet có nội dung tương tự và alert , có thể lấy toàn bộ đoạn byte hoặc những byte đặc trưng nhất cho reverse để làm content alert , và chọn đoạn byte 2f 62 69 6e 2f 73 68 20 3e 2f 74 6d 70 2f nó có nội dung trong trường account là: /bin/sh >/tmp/

Viết snort rule:

*drop tcp any any -> any any (msg: "shell attack !!!"; content: "|2f 62 69 6e 2f 73 68 20 3e 2f 74 6d 70 2f| offset: 244; depth: 14; sid: 1000021; rev: 1;)*

* tcp any any -> any any: Rule áp dụng cho tất cả các kết nối TCP từ bất kỳ nguồn và điểm đến nào (any any) đến bất kỳ đích và nguồn nào (any any).
* (msg: "shell attack !!!";): Nội dung thông báo được gửi khi rule được kích hoạt là "shell attack !!!".
* content: "|2f 62 69 6e 2f 73 68 20 3e 2f 74 6d 70 2f|: Nội dung kiểm tra trong gói tin TCP, được viết dưới dạng hex (hệ cơ số 16), trong trường hợp này là "/bin/sh > /tmp/".
* offset: 244; depth: 14;: Xác định vị trí bắt đầu của nội dung được kiểm tra (offset) và chiều dài của nó (depth) trong gói tin TCP. Trong trường hợp này, nội dung được kiểm tra bắt đầu từ byte thứ 244 và có độ dài là 14 byte.
* sid: 1000021; rev: 1;: ID của rule (sid) là 1000021 và số phiên bản (rev) của rule là 1.

Kết quả:

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động