Snort

- **Snort** là một hệ thống phát hiện xâm nhập mạng (Intrusion Detection System - IDS) mã nguồn mở, được sử dụng rộng rãi để giám sát lưu lượng mạng, phát hiện các loại tấn công và phần mềm độc hại, đồng thời bảo vệ mạng máy tính khỏi các mối đe dọa.
- Snort hoạt động bằng cách:
    - Bắt gói tin: Snort thu thập các gói tin mạng đi qua hệ thống.
    - Phân tích: Snort phân tích các gói tin này dựa trên các quy tắc và chữ ký (signatures) đã được định nghĩa trước.
    - Phát hiện: Nếu gói tin nào đó khớp với các quy tắc hoặc chữ ký của một loại tấn công, Snort sẽ phát ra cảnh báo.
    - Ngăn chặn (tùy chọn): Tùy thuộc vào cách cấu hình, Snort có thể không chỉ phát hiện mà còn ngăn chặn các cuộc tấn công bằng cách chặn các gói tin độc hại.

ICMP Ping Detection

- ICMP hay Internet Control Message Protocol là giao thức mạng được sử dụng để gửi thông báo lỗi và thông tin điều khiển.
- Một cách sử dụng phổ biến của ICMP là gửi yêu cầu ping, được sử dụng để kiểm tra kết nối mạng.
- **Snort** có thể được cấu hình để phát hiện các yêu cầu ping ICMP.
- **Snort Rule Syntax:**

    ```
    alert icmp any any -> any any (msg:"ICMP Ping detected"; itype:8; sid:1001; rev:1;)
    ```

    - Action: alert
    - Protocol: icmp
    - Source/Destination IP: any (matches any source and destination - IP)
    - Options:
    - itype:8: Matches ICMP type 8, which is an echo request (ping).
    - msg:"ICMP Ping detected": Thông báo sẽ được ghi lại khi quy tắc được kích hoạt.
    - sid:1001: ID Snort duy nhất cho quy tắc này.
    - rev:1: Số sửa đổi cho quy tắc này.
- Ta có thể tùy chỉnh quy tắc Snort để phù hợp với nhu cầu của mình:
    - **Địa chỉ IP nguồn và đích:** Chỉ định các địa chỉ IP cụ thể hoặc phạm vi để nhắm mục tiêu các máy chủ hoặc mạng cụ thể.
    - **Loại ICMP:** Khớp với các loại ICMP khác nếu cần (ví dụ: loại 3 cho đích không thể truy cập được, loại 11 cho thời gian hết hạn).
    - **Các điều kiện bổ sung:** Kết hợp quy tắc với các điều kiện khác, chẳng hạn như khớp cổng hoặc lọc giao thức, để tạo ra các phát hiện cụ thể hơn.
- Ví dụ như sau: rule này sẽ phát hiện các yêu cầu ping từ địa chỉ IP 192.168.1.100.

> alert icmp 192.168.1.100 any -> any any (msg:"ICMP Ping from 192.168.1.100"; icmp:type 8;)

TCP Traffic Detection

- **TCP** hay **Transmission Control Protocol** là một giao thức truyền thông được sử dụng rộng rãi trên Internet. Nó đảm bảo dữ liệu được truyền đi một cách đáng tin cậy, tức là dữ liệu sẽ đến được đích một cách đầy đủ và theo đúng thứ tự. TCP thường được sử dụng để truyền dữ liệu cho các ứng dụng như HTTP (web), FTP (chuyển file), SMTP (email),...
- Cấu trúc của một rule Snort để phát hiện lưu lượng TCP:

  > alert tcp any any -> any any (msg:"TCP traffic"😉

  ```
    - alert: Cho biết một sự kiện bảo mật tiềm ẩn đã được phát hiện.
    - tcp: Chỉ ra rằng quy tắc áp dụng cho các gói tin TCP.
    - any any -> any any: Xác định địa chỉ IP nguồn và đích, cũng như các
  cổng. Trong trường hợp này, bất kỳ nguồn và đích nào cũng được phép.
    - (msg:"TCP traffic";): Định nghĩa thông báo sẽ được hiển thị khi quy tắc
  được kích hoạt.
  ```

- Ví dụ:
  - Phát hiện kết nối SSH:

    > alert tcp any any -> $HOME_NET 22 (msg:"incoming SSH connection!"; flags:S; sid:10000;)

  - Phát hiện quét cổng:

    > alert tcp any any -> $HOME_NET any (msg:"Port scan"; flags:S; content:"|x03|"; sid:10001;)

Basic SSH Connection Detection

- **SSH** hay **Secure Shell** là một giao thức mạng được sử dụng để thiết lập kết nối an toàn giữa các máy tính. Nó thường được sử dụng để quản lý từ xa các máy chủ Linux và các hệ thống khác. SSH mã hóa tất cả dữ liệu truyền đi, bao gồm cả mật khẩu, giúp bảo vệ thông tin khỏi bị nghe lén.
- **Snort** có thể được cấu hình để phát hiện các kết nối SSH bằng cách tạo các quy tắc cụ thể. Quy tắc này sẽ tìm kiếm các gói tin TCP đến cổng 22 (cổng mặc định của SSH) và kiểm tra các cờ và nội dung của gói tin.
- Cấu trúc của một rule Snort để phát hiện kết nối SSH:

  > alert tcp any any -> $HOME_NET 22 (msg:"incoming SSH connection!"; flags:S; sid:10000;)

  ```
    - alert: Cho biết một sự kiện bảo mật tiềm ẩn đã được phát hiện.
    - tcp: Chỉ ra rằng quy tắc áp dụng cho các gói tin TCP.
    - any any -> $HOME_NET 22: Xác định địa chỉ IP nguồn và đích, cũng như các
  ```

```
cổng. Trong trường hợp này, bất kỳ nguồn nào cũng có thể kết nối đến cổng 22
của mạng nội bộ.
  - (msg:"incoming SSH connection!"; flags:S; sid:10000;):
      - msg: Thông báo sẽ được hiển thị khi quy tắc được kích hoạt.
      - flags:S: Chỉ lọc các gói tin có cờ SYN (đầu tiên của một kết nối
TCP). Điều này giúp giảm thiểu các báo động giả.
      - sid: Một số ID duy nhất để xác định quy tắc.
```

- Ví dụ:
  - Phát hiện brute-force SSH:

    > alert tcp any any -> $HOME_NET 22 (msg:"SSH brute-force"; content:"|x7f|"; sid:10001; rev:1;)