**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 2**

**NGÀNH AN TOÀN THÔNG TIN**

****

**Môn: Kỹ thuật theo dõi, giám sát an toàn mạng**

**Đề tài: Tiến hành tấn công từ chối dịch vụ (DOS) UDP Flood và phòng thủ bằng Proxy và Snort & tường lửa Pfsense**

**GVHD: Nguyễn Xuân Sâm**

**Nhóm sinh viên thực hiện:**

|  |  |  |
| --- | --- | --- |
| Họ và tên | Mã số sinh viên | Lớp |
| Nguyễn Minh Hoàng | N17DCAT029 | D17CQAT01-N |
| Bùi Minh Thuận | N17DCAT069 | D17CQAT01-N |

1. **UDP FLOOD DOS ATTACK**
2. ***UDP Flood DOS là gì?***

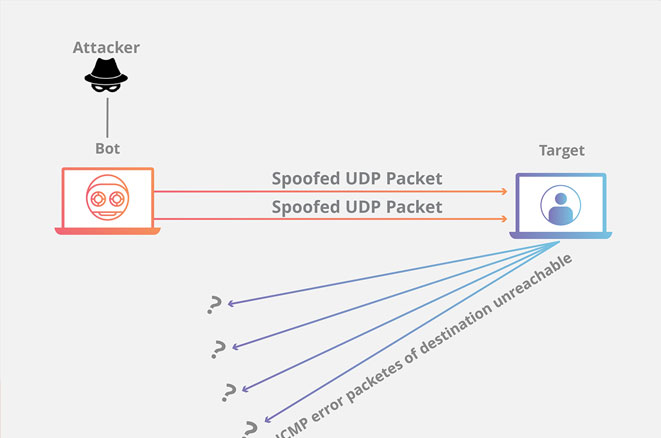
UDP flood là một dạng tấn công từ chối dịch vụ (denial-of-service) với một số lượng lớn gói tin User Datagram Protocol (UDP) được gửi về máy chủ với mục đích làm quá tải khả năng xử lý và phản hồi của thiết bị. Cho dù máy chủ có được bảo vệ bởi một tường lửa thì không có nghĩa máy chủ sẽ có khả năng chống lại một cuộc tấn công DOS UDP flood đủ lớn, thiết bị tường lửa có thể bị cạn tài nguyên bởi loại tấn công này, dẫn tới việc không thể phân biệt được những gói tin hợp lệ.

1. ***UDP Flood DOS attack hoạt động như thế nào?***

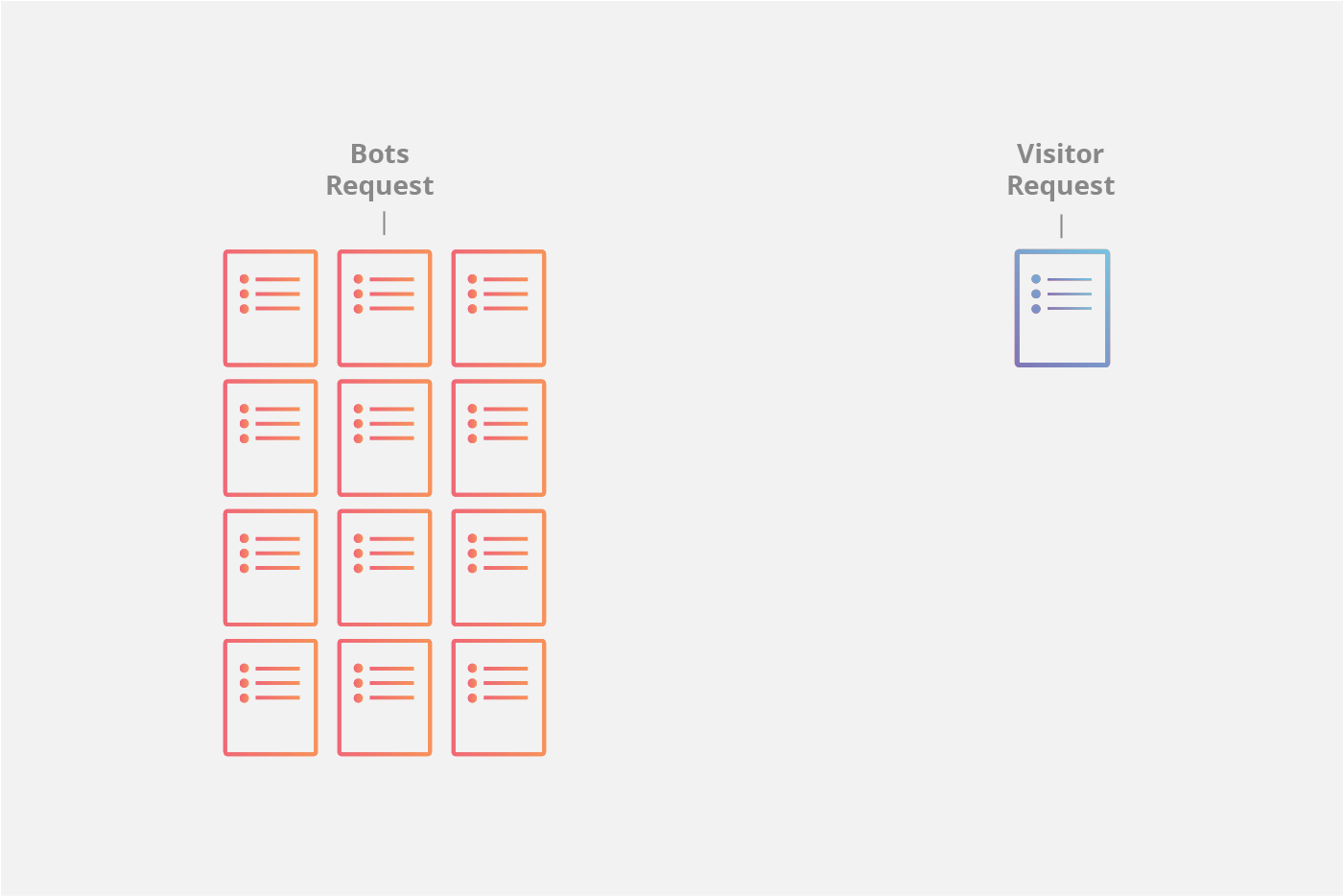
Tấn công UDP bằng cách khái thác các bước mà server thực hiện khi nó phản hồi packet UDP được gửi đến một trong số các port của Client. Trong điều kiện bình thường server nhận packet UDP tại 1 port cụ thể, phản hồi qua 2 bước như sau:

**Bước 1**: Trước tiên, server kiểm tra xem có các chương trình nào đang chạy hay không, hiện tại đang lắng nghe các port nào được chỉ định của chương trình .

**Bước 2**: Nếu không có chương trình nào nhận packet tại port, thì server sẽ phản hồi với packet ICMP (ping) để thông báo cho người gửi rằng đích không thể truy cập được.



Tấn công UDP flood có thể được hình dung đến trong bối cảnh các cuộc gọi định tuyến của nhân viên lễ tân khách sạn. Đầu tiên, nhân viên tiếp tân nhận được một cuộc gọi điện thoại trong đó người gọi yêu cầu được kết nối cuộc gọi với một phòng cụ thể. Sau đó nhân viên tiếp tân cần xem qua danh sách tất cả các phòng để đảm bảo rằng khách có mặt trong phòng và sẵn sàng nhận cuộc gọi. Khi nhân viên lễ tân biết rằng không có khách trong phòng để nhận cuộc gọi, họ phải gọi lại cho người gọi , nói rằng khách không có ở phòng để nhận cuộc gọi. Nếu các line điện thoại sáng lên cùng lúc với các yêu cầu tương tự thì chúng sẽ nhanh chóng trở nên quá tải.



Khi mỗi packet UDP được máy chủ tiếp nhận, nó phải trải qua các bước để xử lý yêu cầu, sử dụng nguồn tài nguyên của server cho quá trình xử lý. Khi các packets UDP được gửi đi , mỗi packets sẽ bao gồm địa chỉ IP của thiết bị nguồn. Trong kiểu tấn công DoS này, kẻ tấn công thường không sử dụng địa chỉ IP thực của họ mà thay vào đó sẽ dùng địa chỉ IP giả mạo nguồn của các packets UDP. Ngăn chặn vị trí thật của kẻ tấn công bị lộ và có khả năng hòa lẫn các gói phản hồi từ máy chủ mục tiêu.

Do server mục tiêu sử dụng tài nguyên để kiểm tra và phản hồi từng packets UDP đã nhận , tài nguyên của server mục tiêu có thể nhanh chóng cạn kiệt khi nhận được một lượng lớn các packets UDP, kết quả việc tấn công Ddos đối với lưu lượng bình thường.

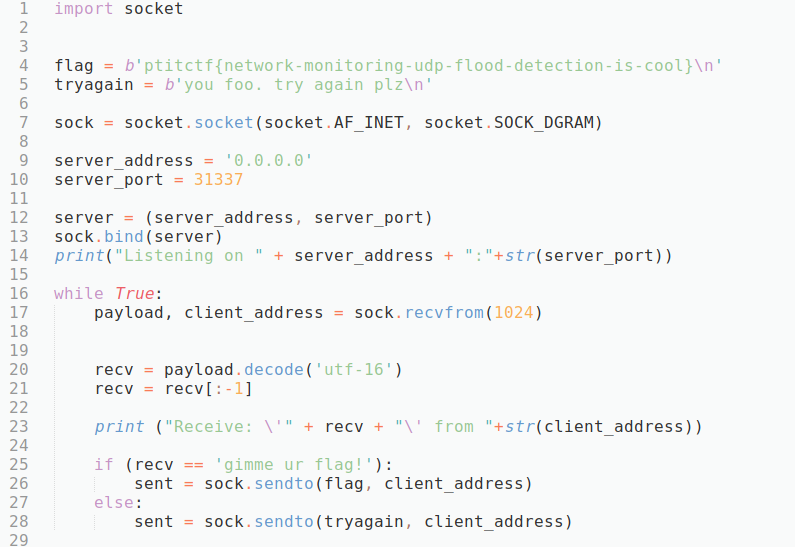
1. **Làm thế nào để giảm thiểu nguy cơ bị tấn công DOS UDP Flood?**

Hầu hết các hệ điều hành có giới hạn tốc độ phản hồi của các packets ICMP một phần để phá vỡ các cuộc tấn công DDoS yêu cầu phản hồi ICMP. Một nhược điểm của kiểu giảm thiểu này là trong một cuộc tấn công, các packets hợp pháp cũng có thể được lọc trong qúa trình này. Nếu cuộc tấn công UDP flood với khối lượng đủ lớn để cân bằng trạng thái firewall của server mục tiêu. Mọi sự giảm thiểu xảy quá mức của server không đủ xảy ra tình trạng nghẽn nút cổ chai từ server mục tiêu.

1. **Phân tích gói tin nhận được trong quá trình máy chủ bị tấn công UDP Flood**

Đặt trường hợp máy chủ đang chạy một chương trình chứa một thử thách trong cuộc thi CTF (Capture-The-Flag, một dạng cuộc thi phổ biến trong ngành An Toàn Thông Tin). Trong thực tế, việc tổ chức cuộc thi CTF cũng gặp rất nhiều trường hợp bị DDOS dẫn đến việc chất lượng của cuộc thi bị giảm đi rất nhiều, ảnh hưởng lớn tới thí sinh và BTC).

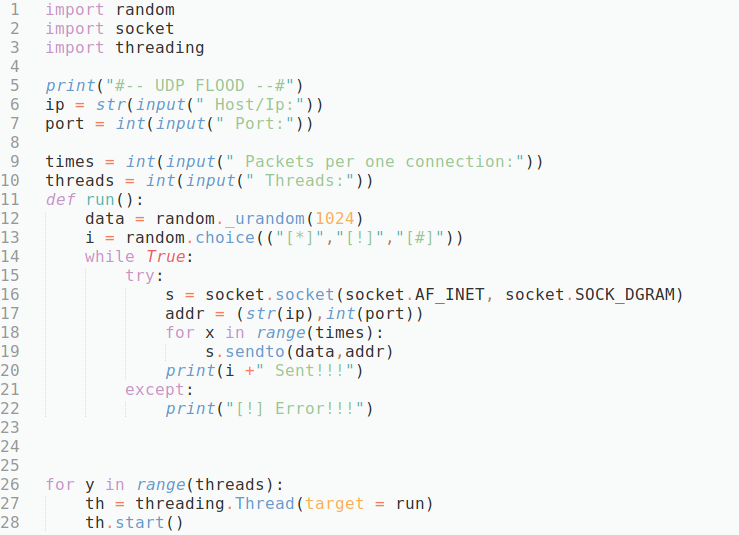
*Mã nguồn Python của thử thách đơn giản như sau*:



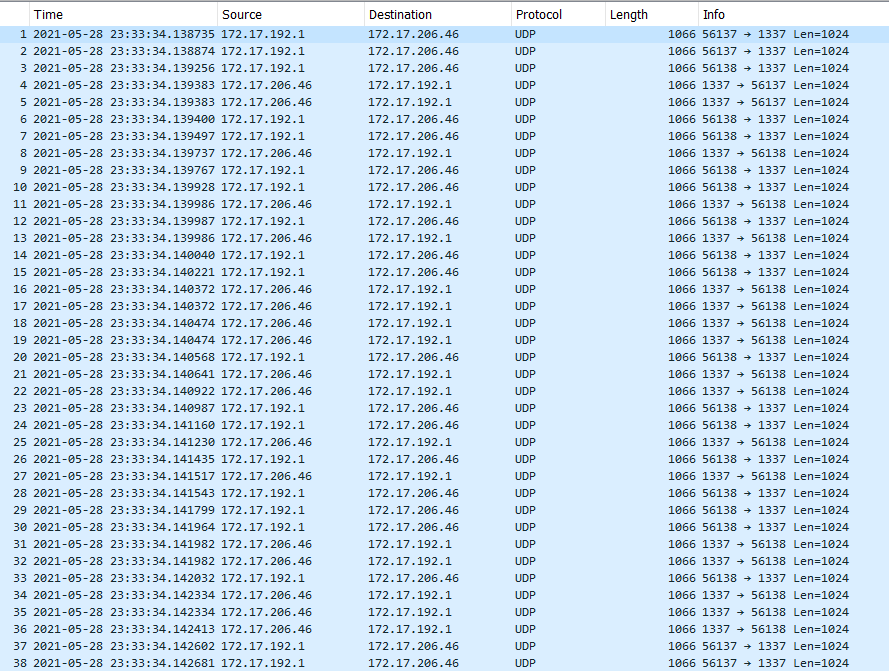
Theo lý thuyết, việc tấn công DOS UDP Flood khá đơn giản, gửi càng nhiều gói tin chứa càng nhiều dữ liệu càng tốt tới một cổng, ở đây là cổng **31337** , nên việc thiết kế thuật toán bằng Python sẽ không mất quá nhiều thời gian.

Trong thực tế, để tấn công các máy chủ lớn, các Attacker sẽ sử dụng nhiều máy tính để thực hiện tấn công từ chối dịch vụ DOS cùng lúc, đây còn gọi là các máy zombie trong một hệ thống bot-net, các máy zombie này hầu hết đều đã bị nhiễm mã độc thông qua một hoặc nhiều lỗ hổng bảo mật, và Attacker có quyền điều khiển các máy tính này từ xa.

*Mã nguồn Python demo tấn công UDP Flood DOS*:



Sau khi khởi động chương trình cho thử thách CTF trên, và thực hiện tấn công UDP, do máy chủ và bản thân chương trình UDP server không có bất cứ phương pháp bảo vệ nào, nên máy chủ nhanh chóng bị quá tải và không thể xử lý những tác vụ tưởng chừng như rất đơn giản. Thu thập gói tin bằng chương trình *Wireshark* và thực hiện phân tích:



*Hình ảnh gói tin được truyền qua lại giữa máy chủ CTF và máy attacker*

Dựa vào thông tin khá trực quan từ Wireshark, dễ nhận thấy máy chủ phải thực hiện truyền nhận dữ liệu đồng thời phải xử lý rất nhiều dữ liệu cùng lúc, từ đó dẫn tới quá tải:

