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

**KHOA CÔNG NGHỆ THÔNG TIN**



Học phần: **An toàn mạng**

Bài báo cáo

**Nghiên cứu hình thức tấn công DOS**

**Giảng viên**: TS. Đặng Minh Tuấn

**Sinh viên thực hiện:** Nhóm 07

Nguyễn Tuấn Anh B17DCAT008

Đặng Anh Tuấn B17DCAT200

Nguyễn Hải Đăng B17DCAT032

Phạm Thế Phong B17DCAT140

Hà Nội 11/2020

MỤC LỤC

[MỤC LỤC 2](#_Toc57129243)

[DANH SÁCH CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT 4](#_Toc57129244)

[DANH MỤC CÁC HÌNH ẢNH 5](#_Toc57129245)

[DANH MỤC BẢNG BIỂU 6](#_Toc57129246)

[CHƯƠNG 1. TỔNG QUAN TÌNH HÌNH AN NINH MẠNG VÀ THỰC TRẠNG TẤN CÔNG MẠNG 7](#_Toc57129247)

[1.1. Tổng quan tình hình thực trạng an ninh mạng và các cuộc tấn công mạng trên thế giới 7](#_Toc57129248)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT CỦA HÌNH THỨC TẤN CÔNG DOS 8](#_Toc57129249)

[2.1. Tổng quan lý thuyết về phương thức tấn công DOS 8](#_Toc57129250)

[2.1.1. Khái niệm phương thức tấn công DOS 8](#_Toc57129251)

[2.1.2. Lịch sử phương thức tấn công DOS 8](#_Toc57129252)

[2.1.3. Cách thức hoạt động của phương thức tấn công DOS 9](#_Toc57129253)

[2.1.4. Biểu hiện khi bị tấn công DOS 10](#_Toc57129254)

[2.2. Một số kỹ thuật tấn công DOS phổ biến 10](#_Toc57129255)

[2.2.1. SYN Flood 10](#_Toc57129256)

[2.2.2. UDP Flood 13](#_Toc57129257)

[2.2.3. Buffer overflow attacks 14](#_Toc57129258)

[2.2.4. ICMP flood 14](#_Toc57129259)

[2.2.5. Slowloris 14](#_Toc57129260)

[CHƯƠNG 3. MÔ HÌNH THỰC NGHIỆM TẤN CÔNG DOS 17](#_Toc57129261)

[3.1. Mô hình thực nghiệm tấn công DOS sử dụng công cụ UDP Flood 17](#_Toc57129262)

[3.1.1. Mô hình thực nghiệm 17](#_Toc57129263)

[3.1.2. Giới thiệu các phần mềm và công cụ được sử dụng 18](#_Toc57129264)

[3.1.2.1. Phần mềm Nmap 18](#_Toc57129265)

[3.1.2.2. Công cụ DOS UDP Flood 19](#_Toc57129266)

[3.1.2.3. Phần mềm Wireshark 19](#_Toc57129267)

[3.1.3. Quy trình thực nghiệm mô hình 20](#_Toc57129268)

[3.2. Mô hình thực nghiệm tấn công DOS sử dụng công cụ Tor’s Hammer 20](#_Toc57129269)

[3.2.1. Mô hình thực nghiệm 20](#_Toc57129270)

[3.2.2. Giới thiệu các phần mềm và công cụ được sử dụng 22](#_Toc57129271)

[3.2.2.1. Tor’s hammer 22](#_Toc57129272)

[3.2.2.2. Cách sử dụng 23](#_Toc57129273)

[CHƯƠNG 4. THỰC NGHIỆM VÀ ĐÁNH GIÁ 25](#_Toc57129274)

[4.1. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ UDP Flood 25](#_Toc57129275)

[4.1.1. Thực nghiệm tấn công 25](#_Toc57129276)

[4.1.1. Đánh giá kết quả thực nghiệm 31](#_Toc57129277)

[4.2. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ Tor’s Hammer 31](#_Toc57129278)

[4.2.1. Thực nghiệm tấn công 31](#_Toc57129279)

[4.2.1. Đánh giá kết quả thực nghiệm 34](#_Toc57129280)

[KẾT LUẬN 36](#_Toc57129281)

[DANH MỤC TÀI LIỆU THAM KHẢO 37](#_Toc57129282)

DANH SÁCH CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT

|  |  |
| --- | --- |
| **Thuật ngữ viết tắt** | **Thuật ngữ đầy đủ** |
| CPU | Central Processing unit |
| DNS | Domain Name System |
| DOS | Denial of Service |
| FTP | File Tranfer Protocol |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| LAN | Local Area Network |
| OWASP | The Open Web Application Security Project |
| ping | Packet Internet Grouper (Groper) |
| SQL | Structured Query Language |
| SYN | synchronization |
| TOR | The Onion Router |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| XSS | Cross-Site Scripting |
| XXE | XML External Entities |

DANH MỤC CÁC HÌNH ẢNH

[Hình 1.1. Minh hoạ hai hình thức tấn công DOS và DDOS 7](#_Toc57129283)

[Hình 2.1. Minh hoạ quá trình bắt tay ba bước của giao thức TCP thông thường 11](#_Toc57129284)

[Hình 2.2. Minh hoạ quá trình tấn công SYN flood 12](#_Toc57129285)

[Hình 2.3. Minh hoạ quá trình tấn công UDP flood 13](#_Toc57129286)

[Hình 2.4. Minh hoạc quá trình tấn công Slowloris Attack 15](#_Toc57129287)

[Hình 3.1. Mô hình thực nghiệm tấn công DOS UDP Flood 17](#_Toc57129288)

[Hình 3.2. Phần mềm Nmap 18](#_Toc57129289)

[Hình 3.3. Quá trình thực thi công cụ DOS UDP Flood 19](#_Toc57129290)

[Hình 3.4. Phầm mền Wireshark 19](#_Toc57129291)

[Hình 3.5. Mô hình tấn công sử dụng công cụ Tor’s hammer 21](#_Toc57129292)

[Hình 3.6. Mô tả mạng Tor 22](#_Toc57129293)

[Hình 3.7. Các tập tin của công cụ Tor's Hammer 23](#_Toc57129294)

[Hình 3.8. Thực thi công cụ Tor's Hammer 23](#_Toc57129295)

[Hình 3.9. Các tuỳ trọn của công cụ Tor's Hammer 24](#_Toc57129296)

[Hình 4.1. Mô hình thực nghiệm tấn công DOS UDP Flood 25](#_Toc57129297)

[Hình 4.2. Cửa sổ thực thi công cụ DOS UDP Flood 26](#_Toc57129298)

[Hình 4.3. Các gói tin được Wireshark trên luồng mạng. 27](#_Toc57129299)

[Hình 4.4. Trình quản lý tác vụ của máy nạn nhân 28](#_Toc57129300)

[Hình 4.5. Kết quả đo lưu lượng mạng trước khi bị tấn công 29](#_Toc57129301)

[Hình 4.6. Kết quả đo lưu lượng mạng khi bị tấn công 30](#_Toc57129302)

[Hình 4.7. Mô hình thực nghiệm tấn công DOS Tor’s Hammer 31](#_Toc57129303)

[Hình 4.8. Kết quả quét Nmap trên máy nạn nhân 32](#_Toc57129304)

[Hình 4.9. Cửa sổ thực thi công cụ Tor’s Hammer 33](#_Toc57129305)

[Hình 4.10. Trình quản lý tác vụ của máy nạn nhân 33](#_Toc57129306)

DANH MỤC BẢNG BIỂU

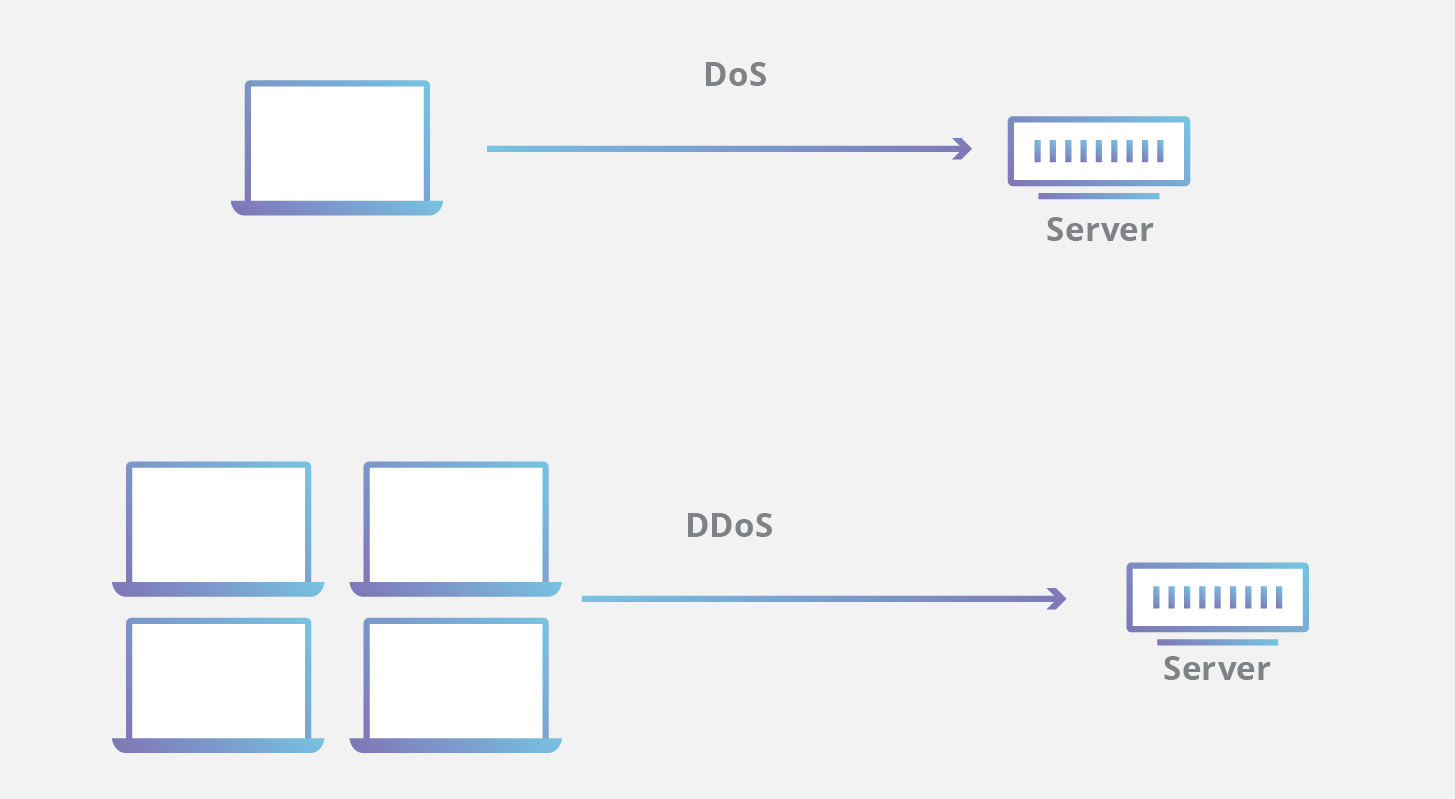
[Bảng 4.1. Ưu và nhược điểm của công cụ Tor's Hammer 35](#_Toc57129307)

CHƯƠNG 1. TỔNG QUAN TÌNH HÌNH AN NINH MẠNG VÀ THỰC TRẠNG TẤN CÔNG MẠNG

* 1. Tổng quan tình hình thực trạng an ninh mạng và các cuộc tấn công mạng trên thế giới

Theo Báo cáo an ninh website Q3, 2018 của CyStack, trong quý 3 năm 2018 đã có 129.722 website trên thế giới bị tin tặc tấn công và chiếm quyền điều khiển. Như vậy, cứ mỗi phút trôi qua lại có 1 website bị tin tặc kiểm soát. Con số này ở tháng 7 là 43.110, sau đó giảm còn 41.405 ở tháng 8 và tăng mạnh lên 45.207 vào tháng 9. Vào thời điểm cuối tháng 9/2018, có đến 21,48% website bị tấn công ở tháng 7 vẫn chưa được khôi phục nguyên trạng; số liệu ở tháng 8 và tháng 9 lần lượt là 33,87% và 44,08%. Cho đến thời điểm tháng 9 năm 2018, trong tổng số 41.405 website bị tấn công vào tháng 8, vẫn còn tới còn 12.102 website chưa được khắc phục. Điều này cho thấy rất nhiều chủ sở hữu đã không thực sự quan tâm đến bảo mật cho website của mình, không biết mình đã bị tấn công hoặc không biết cách xử lý sự cố [1].

Neustar, Inc., đã thông báo rằng Trung tâm Điều hành Bảo mật (SOC) của họ đã chứng kiến ​​mức tăng 168% các cuộc tấn công từ chối dịch vụ (DDoS) phân tán trong Quý 4 năm 2019, so với Quý 4 năm 2018 và tăng 180% tổng thể vào năm 2019 so với. 2018. Theo báo cáo xu hướng và mối đe dọa mạng mới nhất của Neustar, công ty đã chứng kiến ​​các cuộc tấn công DDoS trên tất cả các loại quy mô đều tăng vào năm 2019, với các cuộc tấn công có kích thước từ 5 Gbps trở xuống có mức tăng trưởng lớn nhất. Các cuộc tấn công quy mô nhỏ này chiếm hơn 3/4 tổng số cuộc tấn công mà công ty đã giảm nhẹ thay mặt cho khách hàng của mình trong năm 2019 [2]. DDoS là hình thức tấn công DoS phân tán trên nhiều thiết bị, nhiều địa chỉ IP từ nhiều nơi.



Hình 1.1. Minh hoạ hai hình thức tấn công DOS và DDOS

CHƯƠNG 2. CƠ SỞ LÝ THUYẾT CỦA HÌNH THỨC TẤN CÔNG DOS

2.1. Tổng quan lý thuyết về phương thức tấn công DOS

2.1.1. Khái niệm phương thức tấn công DOS

Tấn công từ chối dịch vụ (DoS) xảy ra khi người dùng hợp pháp không thể truy cập vào hệ thống thông tin, thiết bị hoặc các tài nguyên mạng khác do hành động của một tác nhân đe dọa mạng độc hại. Các dịch vụ bị ảnh hưởng có thể bao gồm email, trang web, tài khoản trực tuyến (ví dụ: ngân hàng) hoặc các dịch vụ khác dựa trên máy tính hoặc mạng bị ảnh hưởng. Điều kiện từ chối dịch vụ được thực hiện bằng cách làm ngập máy chủ hoặc mạng được nhắm mục tiêu với lưu lượng truy cập cho đến khi mục tiêu không thể phản hồi hoặc đơn giản là bị treo, ngăn cản quyền truy cập của người dùng hợp pháp. Các cuộc tấn công DoS có thể khiến tổ chức tốn kém cả thời gian và tiền bạc trong khi tài nguyên và dịch vụ của họ không thể truy cập được [3].

2.1.2. Lịch sử phương thức tấn công DOS

Cuộc tấn công DoS đầu tiên xảy ra chống lại Panix, khu vực lâu đời nhất và lớn nhất của Thành phố New York. Mục tiêu bị tấn công là một Internet Service Provider (ISP), vào ngày 6 tháng 9 năm 1996, vào khoảng 5:30 chiều . Cuộc tấn công nhằm vào các máy tính khác nhau trong mạng của nhà cung cấp, bao gồm máy chủ thư, tin tức và Web, máy "đăng nhập" của người dùng và máy chủ định danh. Cuộc tấn công Panix là một cuộc tấn công SYN Flood bắt nguồn từ các địa chỉ IP ngẫu nhiên và hướng đến máy chủ.

Cuộc tấn công được thực hiện thông qua cổng của giao thức chuyển thư đơn giản (SMTP). Cụ thể hơn, các máy tính của Panix bị ngập trung bình 150 gói SYN mỗi giây (50 gói trên mỗi máy chủ), vì vậy Panix không thể đáp ứng các yêu cầu hợp pháp. Bởi vì những kẻ tấn công đã sử dụng các địa chỉ IP nguồn giả mạo trong các gói tin của chúng, các địa chỉ này không thể được theo dõi và không thể lọc được các địa chỉ độc hại. Vì lý do đó mà cuộc tấn công không được xử lý ngay lập tức.

Giải pháp là sử dụng khối điều khiển truy cập (TCB). TCB giữ các kết nối nửa mở cho đến khi nhận được gói ACK cuối cùng. Bằng cách đó, hàng đợi lắng nghe đủ lớn để giữ tất cả các yêu cầu SYN trước khi kết nối nửa mở hết thời gian. Mặt khác, thời gian chờ đã được điều chỉnh thành 94 giây. Tuy nhiên, mặc dù Panix đã vượt qua cuộc tấn công này, nhưng mối đe dọa mới (tấn công DoS) đã khiến các quản trị viên lo lắng [4].

Một minh chứng đầu tiên khác về cuộc tấn công DoS đã được Khan C. Smith thực hiện vào năm 1997 trong một sự kiện DEF CON , làm gián đoạn truy cập Internet đến Las Vegas Strip trong hơn một giờ. Việc phát hành mã mẫu trong sự kiện đã dẫn đến cuộc tấn công trực tuyến của Sprint , EarthLink , E-Trade và các tập đoàn lớn khác trong năm sau đó [5].

2.1.3. Cách thức hoạt động của phương thức tấn công DOS

Một cuộc tấn công DoS ngăn người dùng truy cập vào một dịch vụ bằng cách áp đảo tài nguyên vật lý hoặc kết nối mạng của nó. Cuộc tấn công về cơ bản làm tràn ngập dịch vụ với rất nhiều lưu lượng truy cập hoặc dữ liệu mà không ai khác có thể sử dụng nó cho đến khi luồng độc hại được xử lý.

Một cách để làm quá tải tài nguyên vật lý của dịch vụ là gửi cho nó quá nhiều yêu cầu trong một thời gian ngắn đến mức nó lấn át tất cả không gian bộ nhớ, xử lý hoặc lưu trữ có sẵn. Trong những trường hợp cực đoan, điều này thậm chí có thể dẫn đến hư hỏng các thành phần vật lý của các tài nguyên này.

Tương tự, để làm gián đoạn các kết nối mạng của dịch vụ, cuộc tấn công DoS có thể gửi các yêu cầu kết nối không hợp lệ, không đúng định dạng hoặc chỉ là một số lượng lớn các yêu cầu kết nối đến nó. Trong khi những điều này đang được giải quyết, không thể hoàn thành các yêu cầu kết nối từ người dùng hợp pháp.

Đôi khi, một cuộc tấn công DoS khai thác lỗ hổng trong một chương trình hoặc trang web để buộc sử dụng không đúng tài nguyên hoặc kết nối mạng của nó, điều này cũng dẫn đến từ chối dịch vụ.

Một số phần mềm độc hại cũng bao gồm khả năng khởi động các cuộc tấn công DoS. Khi chúng lây nhiễm vào máy tính hoặc thiết bị, những mối đe dọa này có thể sử dụng tài nguyên của máy bị nhiễm để thực hiện cuộc tấn công. Nếu nhiều máy bị lây nhiễm thực hiện các cuộc tấn công chống lại cùng một mục tiêu, thì đó được gọi là cuộc tấn công từ chối dịch vụ phân tán (DDoS).

Khối lượng dữ liệu được sử dụng trong một cuộc tấn công DoS hoặc DDoS có thể rất lớn, lên đến tốc độ vài gigabit mỗi giây. Botnet thường được sử dụng để thực hiện các cuộc tấn công DDoS, vì nhiều dịch vụ không có đủ tài nguyên cần thiết để chống lại cuộc tấn công từ hàng nghìn, thậm chí hàng trăm nghìn thiết bị bị nhiễm [6].

2.1.4. Biểu hiện khi bị tấn công DOS

Tổ chức United States Computer Emergency Readiness Team (US-CERT) đã xác định được các triệu chứng của một cuộc tấn công từ chối dịch vụ bao gồm [5]:

* Hiệu suất mạng chậm bất thường (mở tệp hoặc truy cập các trang web)
* Không có sẵn một trang web cụ thể
* Không có khả năng truy cập bất kỳ trang web nào

2.2. Một số kỹ thuật tấn công DOS phổ biến

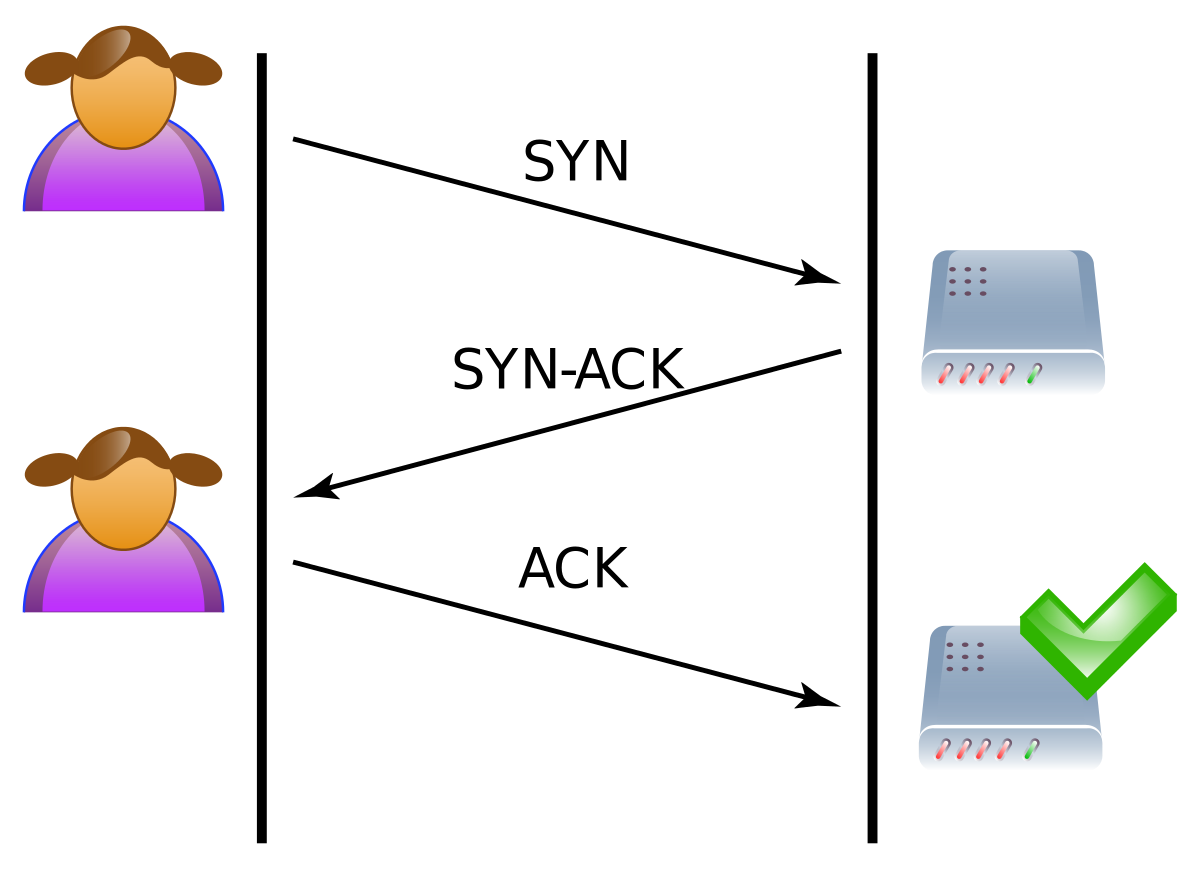
Các cuộc tấn công từ chối dịch vụ được đặc trưng bởi một nỗ lực rõ ràng của những kẻ tấn công nhằm ngăn chặn việc sử dụng hợp pháp một dịch vụ. Có hai hình thức tấn công DoS chung: những hình thức làm sập dịch vụ và những hình thức làm ngập dịch vụ.

2.2.1. SYN Flood

Tấn công SYN flood là một hình thức tấn công từ chối dịch vụ , trong đó kẻ tấn công nhanh chóng khởi tạo một kết nối đến một máy chủ mà không cần hoàn thiện kết nối. Máy chủ phải dành tài nguyên để chờ kết nối nửa mở, điều này có thể tiêu tốn đủ tài nguyên khiến hệ thống không phản hồi với lưu lượng truy cập hợp pháp. Các gói mà kẻ tấn công gửi là gói SYN, một phần của cơ chế bắt tay ba bước trong giao thức TCP sử dụng để thiết lập kết nối.

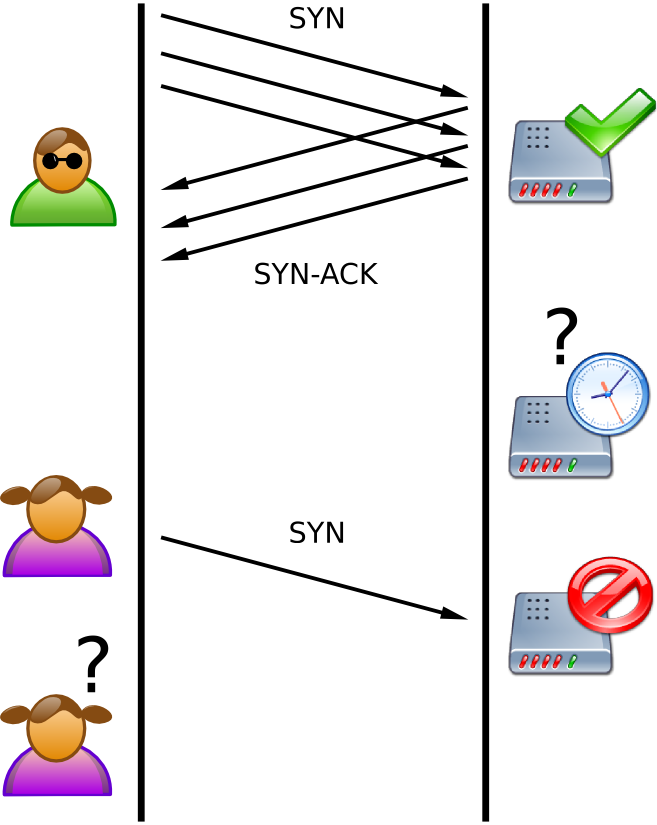
* Khi máy khách cố gắng bắt đầu kết nối TCP với máy chủ, máy khách và máy chủ trao đổi một loạt thông báo thường chạy như sau:
* Máy khách yêu cầu kết nối bằng cách gửi thông báo SYN( đồng bộ hóa ) đến máy chủ.
* Máy chủ ghi nhận yêu cầu này bằng cách gửi SYN-ACK lại cho máy khách.
* Máy khách trả lời bằng một ACK và kết nối được thiết lập.

Đây được gọi là bắt tay ba bước TCP và là nền tảng cho mọi kết nối được thiết lập bằng giao thức TCP.



Hình 2.1. Minh hoạ quá trình bắt tay ba bước của giao thức TCP thông thường

Một cuộc tấn công SYN flood hoạt động bằng cách không phản hồi máy chủ với ACK mã dự kiến. Máy khách độc hại có thể chỉ đơn giản là không gửi dự kiến ACK hoặc bằng cách giả mạo địa chỉ IP nguồn trong SYN, khiến máy chủ gửi SYN-ACK tới địa chỉ IP giả mạo và không bao giờ nhận lại được gói tin ACK phản hồi.



Hình 2.2. Minh hoạ quá trình tấn công SYN flood

Máy chủ sẽ đợi xác nhận trong một khoảng thời gian, vì tắc nghẽn mạng đơn giản cũng có thể là nguyên nhân gây ra lỗi ACK. Tuy nhiên, trong một cuộc tấn công, các kết nối nửa mở được tạo bởi máy khách độc hại liên kết tài nguyên trên máy chủ và cuối cùng có thể vượt quá tài nguyên có sẵn trên máy chủ. Tại thời điểm đó, máy chủ không thể kết nối với bất kỳ máy khách nào, dù hợp pháp hay khác. Điều này có hiệu quả từ chối dịch vụ cho khách hàng hợp pháp. Một số hệ thống cũng có thể hoạt động sai hoặc gặp sự cố khi các chức năng khác của hệ điều hành bị thiếu tài nguyên theo cách này [7].

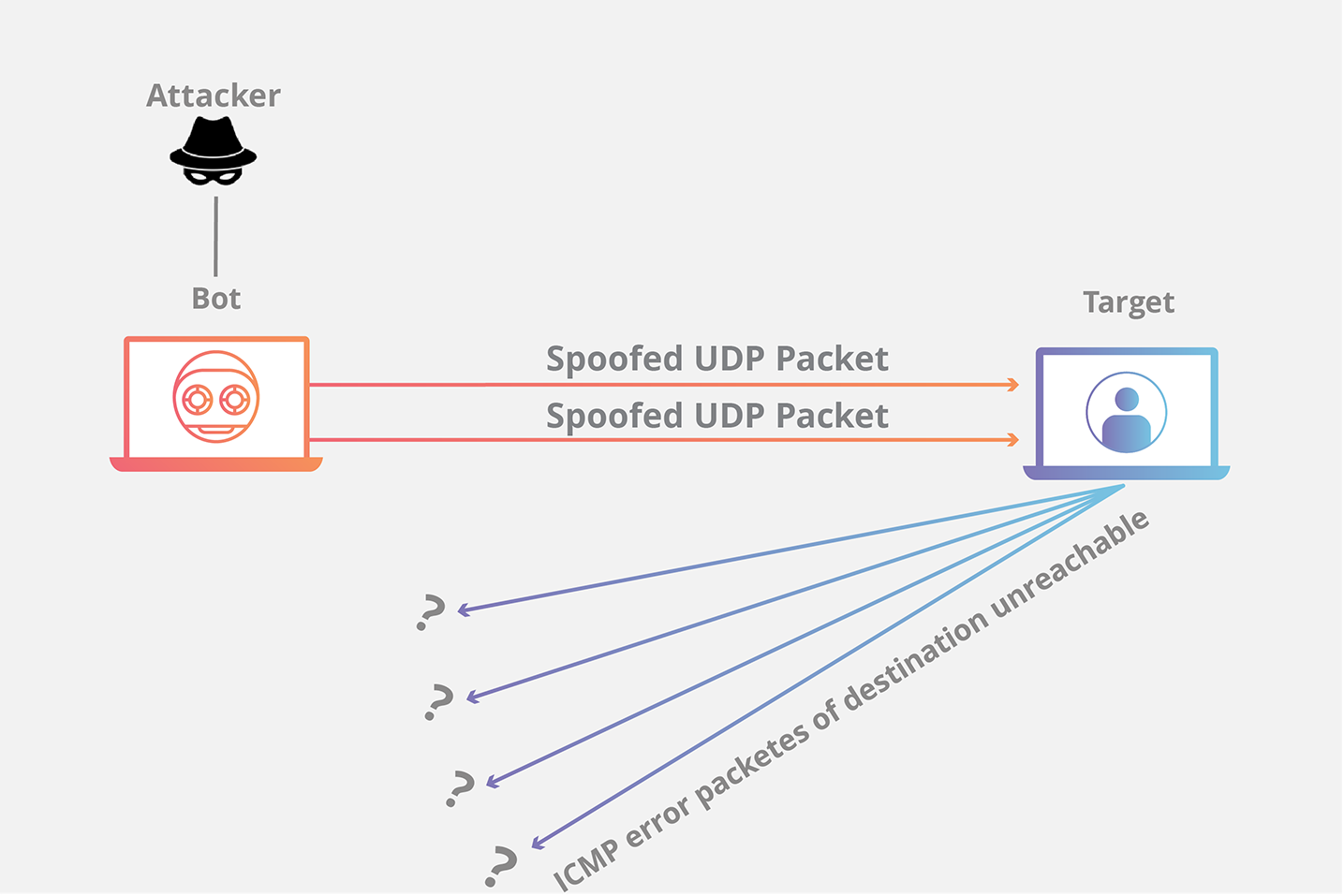
2.2.2. UDP Flood

UDP flood là một kiểu tấn công từ chối dịch vụ trong đó một số lượng lớn các gói Giao thức dữ liệu người dùng (UDP) được gửi đến một máy chủ được nhắm mục tiêu với mục đích lấn át khả năng xử lý và phản hồi của thiết bị đó. Các bức tường lửa bảo vệ máy chủ mục tiêu cũng có thể trở thành cạn kiệt do hậu quả của lũ lụt UDP, dẫn đến một denial-of-dịch vụ cho giao thông hợp pháp.

Một UDP flood hoạt động chủ yếu bằng cách khai thác các bước mà máy chủ thực hiện khi nó phản hồi một gói UDP được gửi đến một trong các cổng của nó. Trong điều kiện bình thường, khi máy chủ nhận được gói UDP tại một cổng cụ thể, nó sẽ trải qua hai bước để phản hồi:

Trước tiên, máy chủ sẽ kiểm tra xem có chương trình nào đang chạy hiện đang lắng nghe các yêu cầu tại cổng được chỉ định hay không.

Nếu không có chương trình nào đang nhận gói tại cổng đó, máy chủ sẽ phản hồi bằng gói ICMP (ping) để thông báo cho người gửi rằng không thể truy cập được đích.



Hình 2.3. Minh hoạ quá trình tấn công UDP flood

Khi mỗi gói UDP mới được máy chủ nhận, nó sẽ trải qua các bước để xử lý yêu cầu, sử dụng tài nguyên máy chủ trong quá trình này. Khi các gói UDP được truyền đi, mỗi gói sẽ bao gồm địa chỉ IP của thiết bị nguồn. Trong kiểu tấn công DDoS này , kẻ tấn công thường sẽ không sử dụng địa chỉ IP thực của chính họ, mà thay vào đó sẽ giả mạo địa chỉ IP nguồn của các gói UDP, cản trở vị trí thực của kẻ tấn công bị lộ và có khả năng bão hòa với các gói phản hồi từ mục tiêu. người phục vụ.

Do máy chủ được nhắm mục tiêu sử dụng tài nguyên để kiểm tra và sau đó trả lời từng gói UDP đã nhận, tài nguyên của mục tiêu có thể nhanh chóng cạn kiệt khi nhận được một lượng lớn gói UDP, dẫn đến việc từ chối dịch vụ đối với lưu lượng bình thường [8].

2.2.3. Buffer overflow attacks

Tràn bộ đệm là một kiểu tấn công DoS phổ biến. Nó dựa vào việc gửi một lượng lưu lượng đến tài nguyên mạng vượt quá khả năng xử lý mặc định của hệ thống. Ví dụ, trước đây, tên tệp 256 ký tự dưới dạng tệp đính kèm chắc chắn sẽ làm hỏng Microsoft Outlook [9].

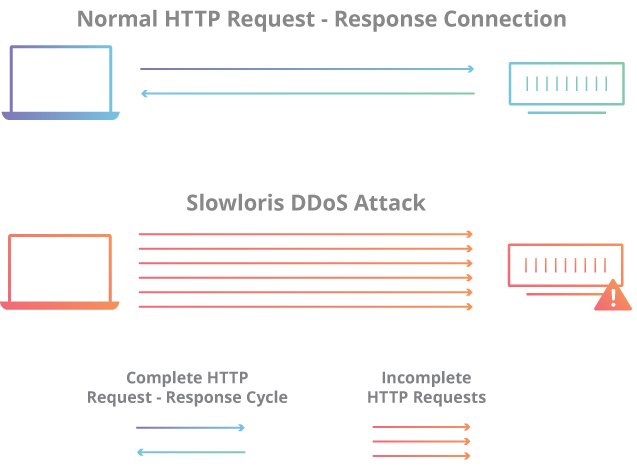
2.2.4. ICMP flood

Cuộc tấn công Internet Control Message Protocol (ICMP) flood, còn được gọi là cuộc tấn công Ping lũ, là một cuộc tấn công Từ chối Dịch vụ (DoS) phổ biến trong đó kẻ tấn công cố gắng áp đảo một thiết bị được nhắm mục tiêu bằng các yêu cầu phản hồi (ping) ICMP. Thông thường, các thông báo ICMP echo-request và echo-reply được sử dụng để ping một thiết bị mạng nhằm chẩn đoán tình trạng và kết nối của thiết bị cũng như kết nối giữa người gửi và thiết bị. Bằng cách làm ngập mục tiêu với các gói yêu cầu, mạng buộc phải trả lời với số lượng gói trả lời bằng nhau. Điều này khiến mục tiêu trở nên không thể truy cập được đối với lưu lượng truy cập bình thường [10].

2.2.5. Slowloris

Slowloris là một cuộc tấn công lớp ứng dụng hoạt động bằng cách sử dụng một phần các yêu cầu HTTP. Cuộc tấn công hoạt động bằng cách mở các kết nối đến một máy chủ Web được nhắm mục tiêu và sau đó giữ cho các kết nối đó mở miễn là nó có thể.

Slowloris không phải là một loại tấn công mà thay vào đó là một công cụ tấn công cụ thể được thiết kế để cho phép một máy duy nhất đánh sập một máy chủ mà không cần sử dụng nhiều băng thông. Không giống như các cuộc tấn công DDoS dựa trên phản xạ tiêu tốn băng thông như khuếch đại NTP , kiểu tấn công này sử dụng một lượng băng thông thấp và thay vào đó nhằm mục đích sử dụng hết tài nguyên máy chủ với các yêu cầu có vẻ chậm hơn bình thường nhưng lại bắt chước lưu lượng truy cập thông thường. Nó thuộc loại tấn công được gọi là các cuộc tấn công “thấp và chậm”. Máy chủ được nhắm mục tiêu sẽ chỉ có rất nhiều luồng có sẵn để xử lý các kết nối đồng thời. Mỗi chuỗi máy chủ sẽ cố gắng duy trì hoạt động trong khi đợi yêu cầu chậm hoàn thành, điều này không bao giờ xảy ra. Khi các kết nối tối đa có thể có của máy chủ đã bị vượt quá, mỗi kết nối bổ sung sẽ không được trả lời và từ chối dịch vụ sẽ xảy ra.



Hình 2.4. Minh hoạc quá trình tấn công Slowloris Attack

Một cuộc tấn công Slowloris xảy ra trong 4 bước:

Đầu tiên kẻ tấn công mở nhiều kết nối đến máy chủ được nhắm mục tiêu bằng cách gửi nhiều tiêu đề yêu cầu HTTP một phần.

Đích mở một luồng cho mỗi yêu cầu đến, với mục đích đóng luồng khi kết nối hoàn tất. Để hiệu quả, nếu kết nối mất quá nhiều thời gian, máy chủ sẽ hết thời gian chờ kết nối quá dài, giải phóng luồng cho yêu cầu tiếp theo.

Để ngăn mục tiêu hết thời gian kết nối, kẻ tấn công định kỳ gửi một phần tiêu đề yêu cầu đến mục tiêu để giữ cho yêu cầu tồn tại. Thực chất là nói, “Tôi vẫn ở đây! Tôi chỉ chậm thôi, hãy đợi tôi ”.

Máy chủ được nhắm mục tiêu không bao giờ có thể giải phóng bất kỳ kết nối mở một phần nào trong khi chờ yêu cầu chấm dứt. Khi tất cả các luồng có sẵn được sử dụng, máy chủ sẽ không thể phản hồi các yêu cầu bổ sung được thực hiện từ lưu lượng truy cập thông thường, dẫn đến việc từ chối dịch vụ.

Chìa khóa đằng sau Slowloris là khả năng gây ra nhiều rắc rối với mức tiêu thụ băng thông rất ít [11].

CHƯƠNG 3. MÔ HÌNH THỰC NGHIỆM TẤN CÔNG DOS

3.1. Mô hình thực nghiệm tấn công DOS sử dụng công cụ UDP Flood

3.1.1. Mô hình thực nghiệm

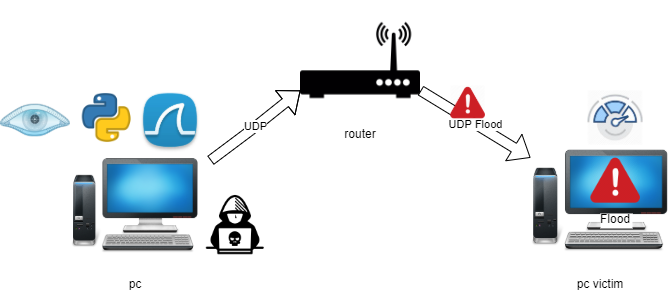
Để tiến hành thực nghiệm tấn công DOS UDP Flood, nhóm nghiên cứu đã đề xuất sử dụng mô hình gồm các thiết bị và phần mềm công cụ hỗ trợ được mô tả trên hình 3.1. gồm:

**Thiết bị:**

* 01 máy tính làm máy tấn công
* 01 máy tính làm máy nạn nhân
* 01 router để kết nối mạng

**Phần mềm và công cụ hỗ trợ:**

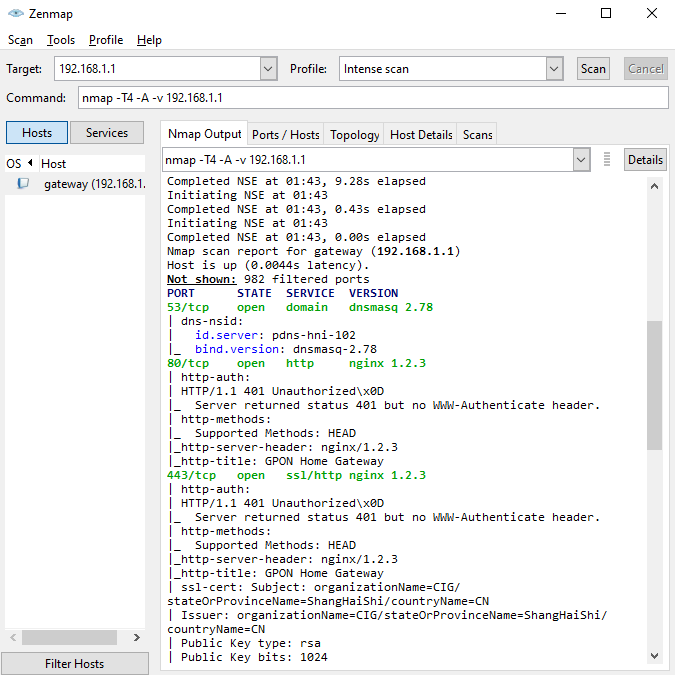
* Phần mềm Nmap
* Tool DOS UDP Flood lập trình bằng ngôn ngữ python
* Phần mềm Wireshark
* Trình quản lý tác vụ Task Manager trên hệ điều hành Windows



Hình 3.1. Mô hình thực nghiệm tấn công DOS UDP Flood

3.1.2. Giới thiệu các phần mềm và công cụ được sử dụng

3.1.2.1. Phần mềm Nmap

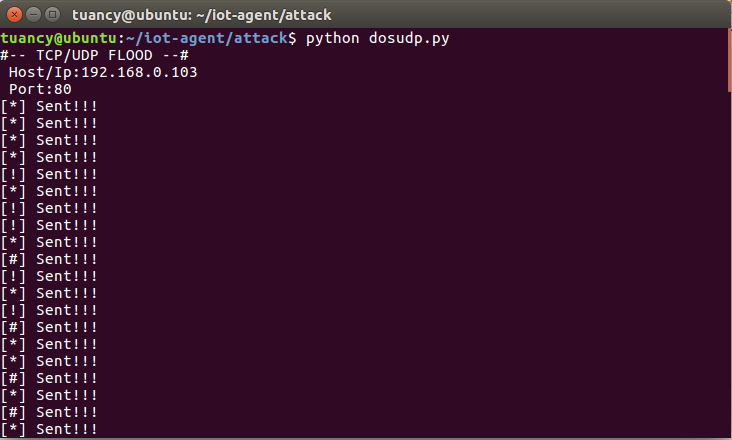


Hình 3.2. Phần mềm Nmap

Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.

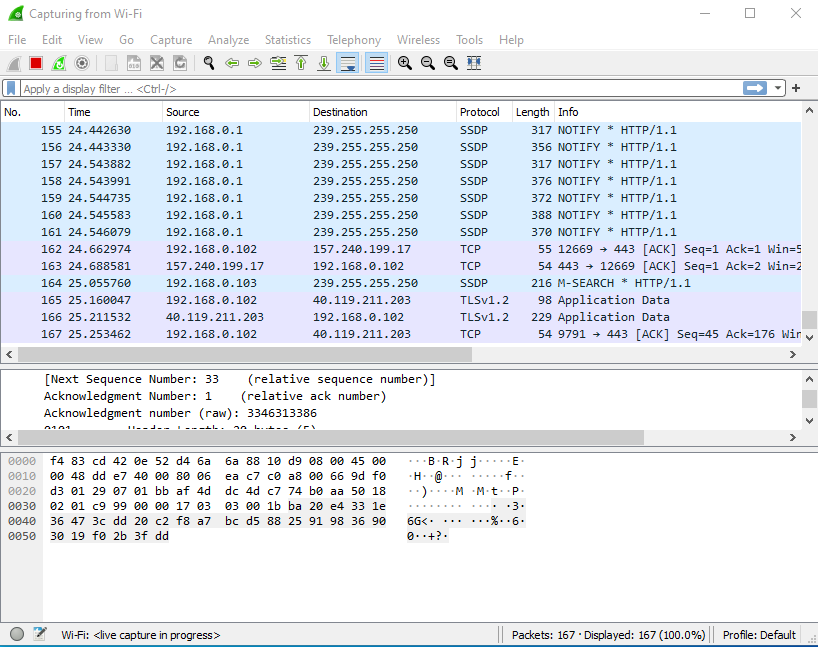
3.1.2.2. Công cụ DOS UDP Flood



Hình 3.3. Quá trình thực thi công cụ DOS UDP Flood

Công vụ DOS UDP Flood là công cụ được lập trình bằng ngôn ngữ python của một tác giả trên nền tảng Github có tên Leeon123 [12]. Công cụ cho phép người sử dụng gửi một lượng cực lớn các gói tin UDP đến một địa chỉ IP và cổng xác định để tiến hành tấn công DOS.

3.1.2.3. Phần mềm Wireshark



Hình 3.4. Phầm mền Wireshark

Công cụ bảo mật WireShark còn được gọi là Ethereal – một trong những ứng dụng được dùng để phân tích dữ liệu hệ thống mạng, theo dõi và giám sát gói tin theo thời gian thực, hiển thị chính xác và báo cáo người dùng qua một giao diện đơn giản và thân thiện.

Phần mềm này cung cấp cho người dùng những thôn tin hữu ích về giao thức mạng, thu thập gói tin cùng khả năng đọc và ghi dữ liệu theo nhiều dạng khác nhau. Phần mềm này còn được sủ dụng để làm nhiệm vụ xử lý sự cố mạng, hỗ trợ trên nhiều hệ điều hành khác nhau như Windows, Ubuntu, Linux,…

3.1.3. Quy trình thực nghiệm mô hình

Quá trình thực nghiệm mô hình tấn công DOS UDP Flood được nhóm nghiên cứu chia thành 4 bước:

Bước 1: Xác định mục tiêu

Trong bước này nhóm nghiên cứu sẽ xác định mục tiêu cần tấn công và khai thác các thông tin ban đầu như địa chỉ IP

Bước 2: Thăm dò và quét rà xoát

Với các thông tin thu thập được ở bước 1 là địa chỉ IP. Nhóm nghiên cứu tiến hành sử dụng phần mềm Nmap để quét được hệ điều hành cùng các cổng đang mở tương ứng với các dịch vụ của máy mục tiêu

Bước 3: Lựa chọn mô hình tấn công

Từ các dữ liệu về máy mục tiêu thu thập được. Nhóm nghiên cứu quyết định mô hình tấn công vào máy mục tiêu.

Bước 4: Thực hiện tấn công

Nhóm nghiên cứu thực thi công cụ tấn công để thực nghiệm và đánh giá.

3.2. Mô hình thực nghiệm tấn công DOS sử dụng công cụ Tor’s Hammer

3.2.1. Mô hình thực nghiệm

Mô hình thực nghiệm sử dụng công cụ Tor’s hammer là một công cụ DoS slow-rate HTTP POST được tạo bởi phiral.net. Xuất hiện công khai đầu tiên của công cụ này là vào đầu năm 2011.

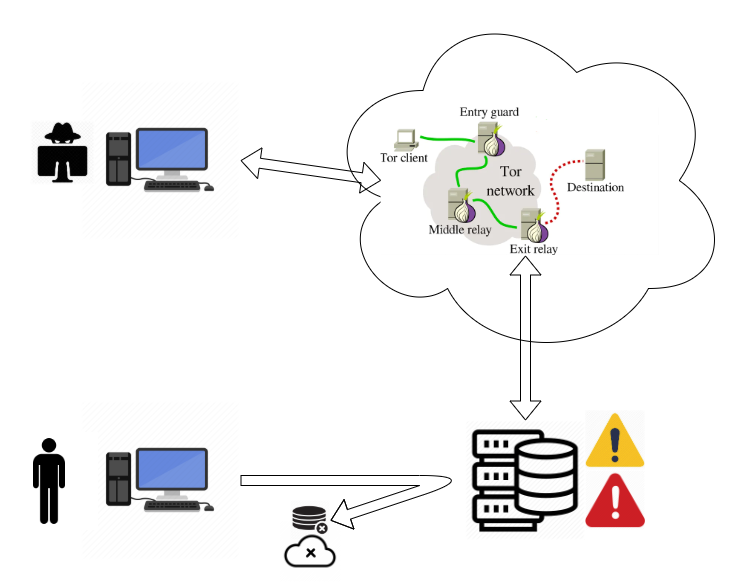
Để tiến hành thực nghiệm tấn công DOS UDP Flood, nhóm nghiên cứu đã đề xuất sử dụng mô hình gồm các thiết bị và phần mềm công cụ hỗ trợ được mô tả trên hình 3.5. gồm:

**Thiết bị:**

* 01 máy tính làm máy tấn công
* 01 server
* 01 mạng TOR

**Phần mềm và công cụ hỗ trợ:**

* Công cụ Tor’s hammer
* Tor proxy



Hình 3.5. Mô hình tấn công sử dụng công cụ Tor’s hammer

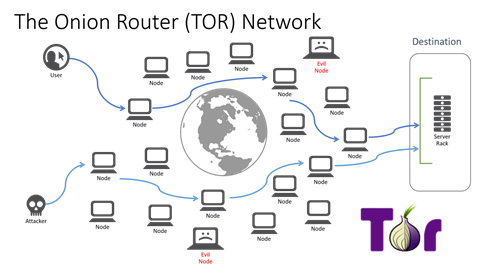
3.2.2. Giới thiệu các phần mềm và công cụ được sử dụng

3.2.2.1. Tor’s hammer

Tor’s hammerthực hiện một cuộc tấn công DoS bằng cách sử dụng một cuộc tấn công classic slow POST attack , trong đó các trường POST HTML được truyền với tốc độ chậm trong cùng một phiên (tốc độ thực tế được chọn ngẫu nhiên trong giới hạn 0,5-3 giây).

Tương tự như R.U.D.Y trước đây. (R-U-Dead-Yet), cuộc tấn công slow POST attack, khiến các luồng ứng dụng máy chủ web phải chờ kết thúc các bài đăng vô hạn để xử lý chúng. Điều này gây ra sự cạn kiệt tài nguyên của máy chủ web và khiến nó rơi vào trạng thái từ chối dịch vụ đối với bất kỳ lưu lượng truy cập hợp pháp nào.

Một chức năng mới được thêm vào Tor's Hammer là khả năng ẩn danh lưu lượng truy cập. Tấn công DoS có thể được thực hiện thông qua mạng Tor (Tor Network) bằng cách sử dụng một socks proxy được tích hợp trong các máy khách Tor. Điều này cho phép phát động cuộc tấn công từ các địa chỉ IP nguồn ngẫu nhiên, khiến việc theo dõi kẻ tấn công gần như không thể



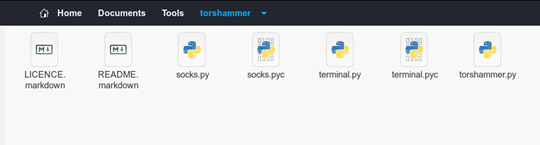
Hình 3.6. Mô tả mạng Tor

3.2.2.2. Cách sử dụng

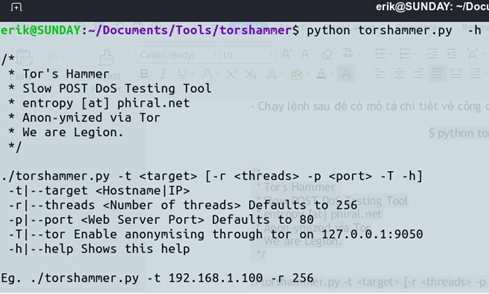
Cài đặt:

Git clone để tải về

$ git clone <https://github.com/dotfighter/torshammer.git>



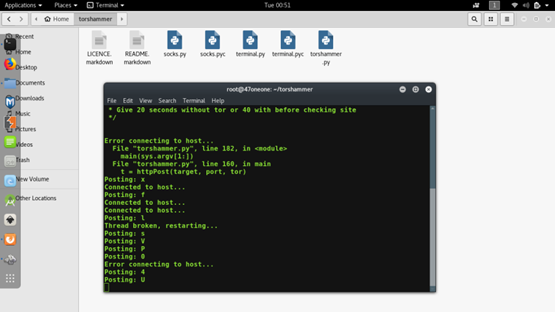
Hình 3.7. Các tập tin của công cụ Tor's Hammer



Hình 3.8. Thực thi công cụ Tor's Hammer

- Các option của công cụ :

* ./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
* -t|--target <Hostname|IP>
* -r|--threads <Number of **threads**> Defaults to 256
* -p|--port <Web Server Port> Defaults to 80
* -T|--tor Enable anonymising through tor on 127.0.0.1:9050
* -h|--help Shows this help
* Eg. ./torshammer.py -t 192.168.1.100 -r 256
* -**t** dành cho mục tiêu, tên miền hoặc địa chỉ ip.
* -**p** dành cho cổng Mặc định là 80.
* -**r** là cho các luồng, chúng ta muốn chạy bao nhiêu luồng cho cuộc tấn công này.
* -**T** là viết tắt của các cuộc tấn công với mạng **tor**.



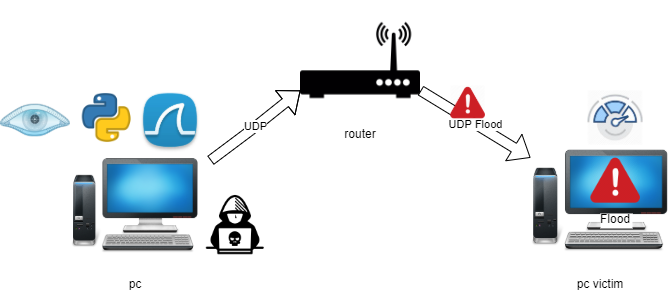
Hình 3.9. Các tuỳ trọn của công cụ Tor's Hammer

CHƯƠNG 4. THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ UDP Flood

4.1.1. Thực nghiệm tấn công

Như đã được trình bày ở chương 3. Quá trình thực nghiệm được nhóm nghiên cứu chia làm 4 bước.



Hình 4.1. Mô hình thực nghiệm tấn công DOS UDP Flood

Bước 1: Xác định mục tiêu

Nhóm nghiên cứu đã tiến hành thu thập các thông tin cơ bản để xác định mục tiêu. Trong báo cáo này, nhóm nghiên cứu đã lựa chọn máy có địa chỉ IP là 192.168.0.103 làm máy nạn nhân để tiến hành thử nghiệm tấn công.

Bước 2: Thăm dò, quét rà xoát

Bằng địa chỉ IP thu thập được trong bước 1. Nhóm nghiên cứu sử dụng công cụ Nmap để rà quét các thông tin về máy mục tiêu như: hệ điều hành, phiên bản, cổng được mở và dịch vụ đang chạy…

Sau quá trình rà quét bằng Nmap, nhóm nghiên cứu thu được các thông tin về máy mục tiêu như:

Hệ điều hành:

* Windows 10

Các cổng đang mở và dịch vụ tương ứng:

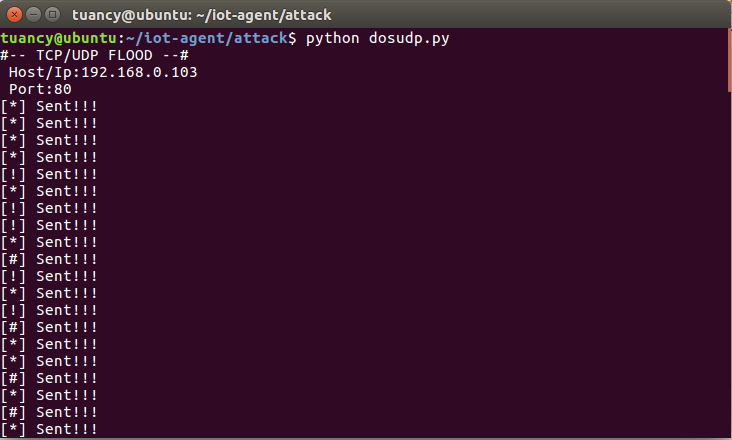
* 22 - ssh
* 80 - http
* 135- msrpc
* 139 - netbios-ssn
* 443 - https
* 445 - microsoft-ds
* 5357 - wsdapi

Bước 3: Lựa chọn mô tình tấn công

Sau khi có các thông tin về máy mục tiêu được thu thập trong bước 2. Nhóm nghiên cứu đã quyết định tấn công DOS UDP Flood vào cổng 80 của dịch vụ http trên máy mục tiêu với mục đích làm ngập đường truyền của máy này.

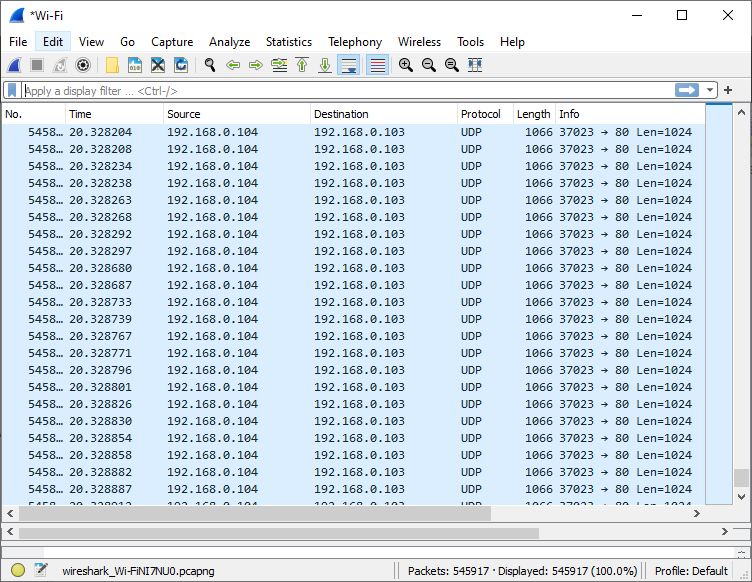
Bước 4: Thực hiện tấn công

Nhóm nghiên cứu đã tiến hành sử dụng công cụ DOS UDP Flood để tiến hành tấn công vào máy mục tiêu có địa chỉ IP 192.168.12.103 với 500 luồng và mỗi luồng gửi 500 gói tin UDP trên giây.



Hình 4.2. Cửa sổ thực thi công cụ DOS UDP Flood

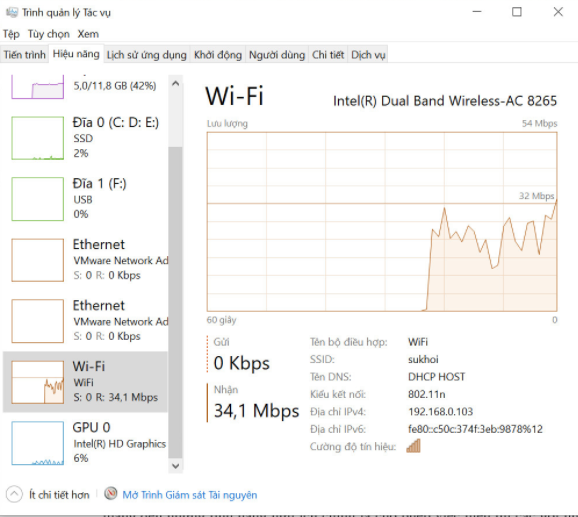
Để có thể quan sát được các gói tin gửi đi trực quan hơn. Nhóm nghiên cứu sử dụng phần mềm bắt gói tin Wireshark để quan sát các gói tin được gửi đi.



Hình 4.3. Các gói tin được Wireshark trên luồng mạng.

Bằng phần mềm Wireshark có thể thấy một lượng lớn gói tin UDP được gửi đi từ máy nguồn có IP:192.168.0.104 tới cổng 80 của máy nạn nhân có IP: 192.168.0.103

Kết quả của tấn công được hiển thị trên máy nạn nhân thông qua trình quản lý tác vụ của hệ điều hành Windows.



Hình 4.4. Trình quản lý tác vụ của máy nạn nhân

Hình 4.4. chụp Task Manager trên máy bạn nhân có IP: 191.168.0.103 với lưu lượng mạng nhận được lên tới 34.1 Mbps chiếm đến hơn 50 % hiệu năng của card Wifi máy nạn nhân.

Thậm trí khi sử dụng kết nối Enthernet, nhóm nghiên cứu đã ghi nhận kết quả các gói tin được nhận tới 250Mbps.

Ngoài ra nhóm nghiên cứu còn tiến hành thực nghiệm tấn công vào thiết bị Smart phone và thu được kết quả.

Kết quả đo lưu lượng mạng trên thiết bị Smart Phone bằng Speed Test trước khi bị tấn công DOS UDP Flood được biểu diễn trên hình 4.5.



Hình 4.5. Kết quả đo lưu lượng mạng trước khi bị tấn công

Kết quả đo lưu lượng mạng trên thiết bị Smart Phone bằng Speed Test khi bị tấn công DOS UDP Flood được biểu thị trên hình 4.6.



Hình 4.6. Kết quả đo lưu lượng mạng khi bị tấn công

4.1.1. Đánh giá kết quả thực nghiệm

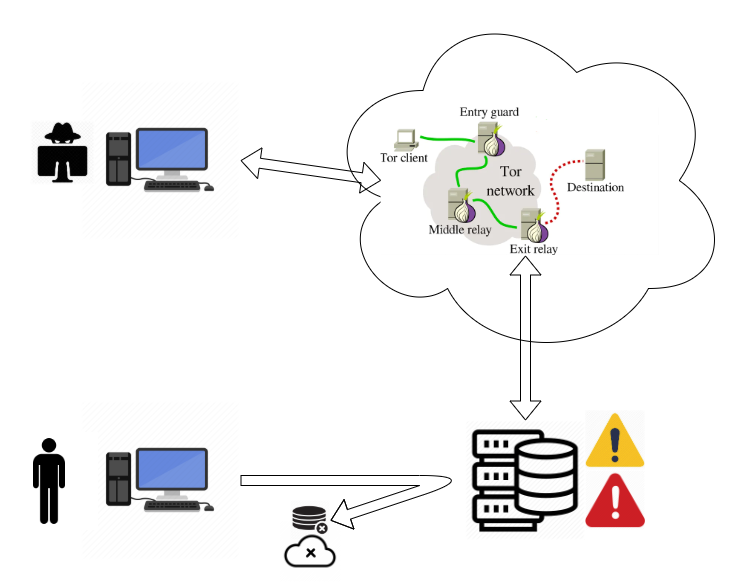
Bằng quá trình thực nghiệm tấn công khi sử dụng công cụ DOS UDP Flood khai thách kỹ thuật tấn công UDP Flood, nhóm nghiên cứu đã thu được kết quả khả quan khi có thể làm ngập lụt đường truyền của máy nạn nhân với lưu lượng lớn được ghi nhận bởi trình quản lý tác vụ và công cụ đo Speed Test. Lưu lượng mạng mà máy nạn nhân nhận được lên tới hơn 34Mbps khi sử dụng kết nối Wifi và lên tới 250Mbps khi sử dụng kết nối Ethernet. Khi thực nghiệm tấn công trên thiết bị Smart Phone đã cho thấy đường truyền bị ngập lụt rõ rệt khi tốc độ tải xuống giảm từ 29.7Mbps xuống 0.39Mbps, tốc độ tải lên giảm từ 50.4Mbps xuống 0.4Mbps.

Tuy nhiên phương pháp tấn công UDP Flood được sử dụng cũng có những hạn chế như dễ dàng bị ngăn chặn bởi các luật kiểm soát lưu lượng đơn giản trên thiết bị hoặc bộ định tuyến. Phương thức tấn công là trực tiếp nên dễ dàng bị phát hiện và truy vết. Hơn nữa, phương pháp tấn công UDP Flood làm tiêu tốn chính tài nguyên hệ thống và lưu lượng luồng mạng của máy tấn công. Đây là những lý do khiến phương thức tấn công DDOS được tạo ra và gây ra các hệ quả lớn hơn rất nhiều hiện nay

4.2. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ Tor’s Hammer

4.2.1. Thực nghiệm tấn công

Như đã được trình bày ở chương 3. Quá trình thực nghiệm được nhóm nghiên cứu chia làm 4 bước.



Hình 4.7. Mô hình thực nghiệm tấn công DOS Tor’s Hammer

Bước 1: Xác định mục tiêu

Nhóm nghiên cứu đã tiến hành thu thập các thông tin cơ bản để xác định mục tiêu. Trong báo cáo này, nhóm nghiên cứu đã lựa chọn máy có địa chỉ IP là 192.168.0.110 làm máy nạn nhân để tiến hành thử nghiệm tấn công.

Bước 2: Thăm dò, quét rà xoát

Bằng địa chỉ IP thu thập được trong bước 1. Nhóm nghiên cứu sử dụng công cụ Nmap để rà quét các thông tin về máy mục tiêu như: hệ điều hành, phiên bản, cổng được mở và dịch vụ đang chạy…

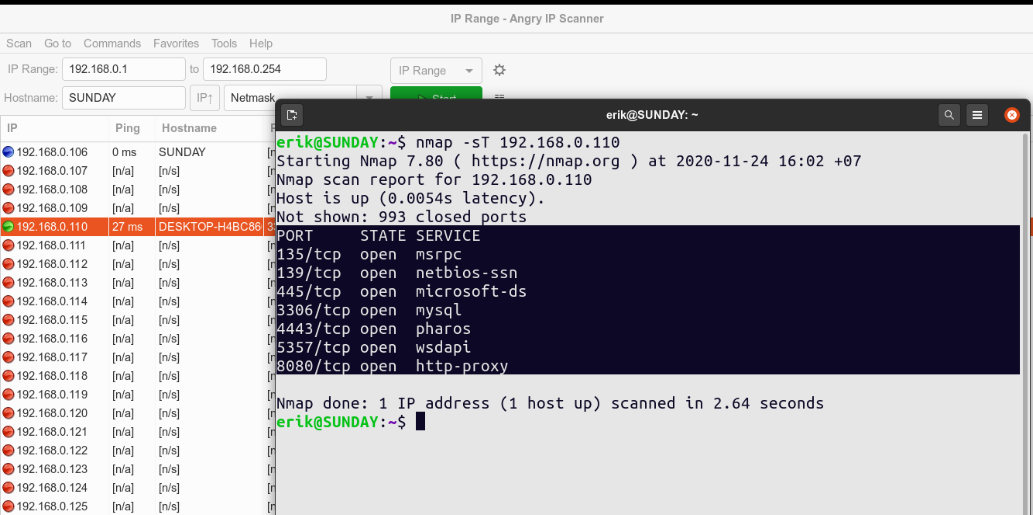
Sau quá trình rà quét bằng Nmap, nhóm nghiên cứu thu được các thông tin về máy mục tiêu như:

Hệ điều hành:

* Windows 10

Các cổng đang mở và dịch vụ tương ứng:

* 22 - ssh
* 8080 - http
* 135- msrpc
* 139 - netbios-ssn
* 443 - https
* 445 - microsoft-ds
* 5357 – wsdapi



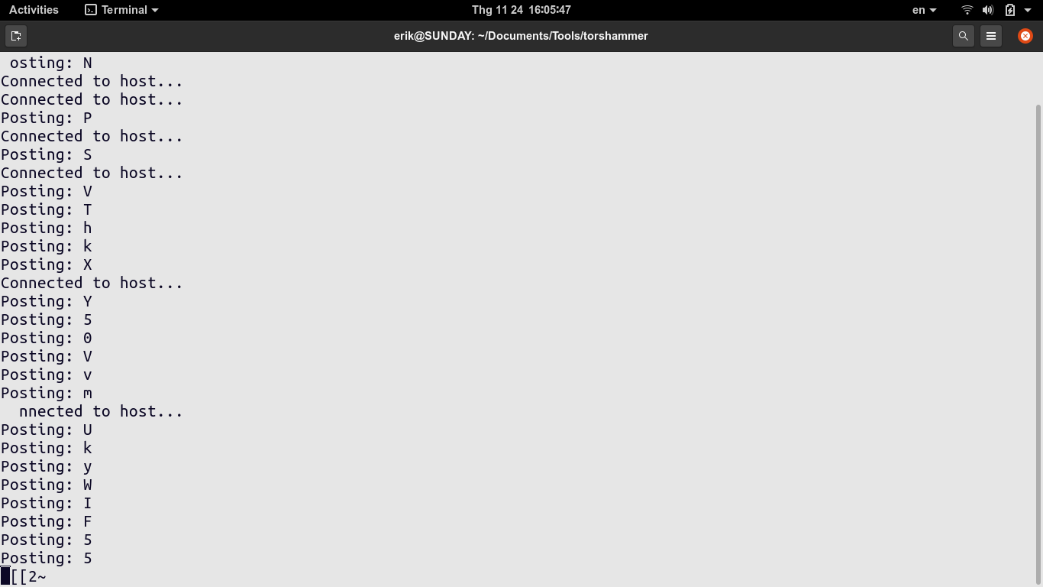
Hình 4.8. Kết quả quét Nmap trên máy nạn nhân

Bước 3: Lựa chọn mô tình tấn công

Sau khi có các thông tin về máy mục tiêu được thu thập trong bước 2. Nhóm nghiên cứu đã quyết định tấn công Tor’s Hammer vào cổng 8080 của dịch vụ http trên máy mục tiêu với mục đích làm ngập đường truyền của máy này.

Bước 4: Thực hiện tấn công

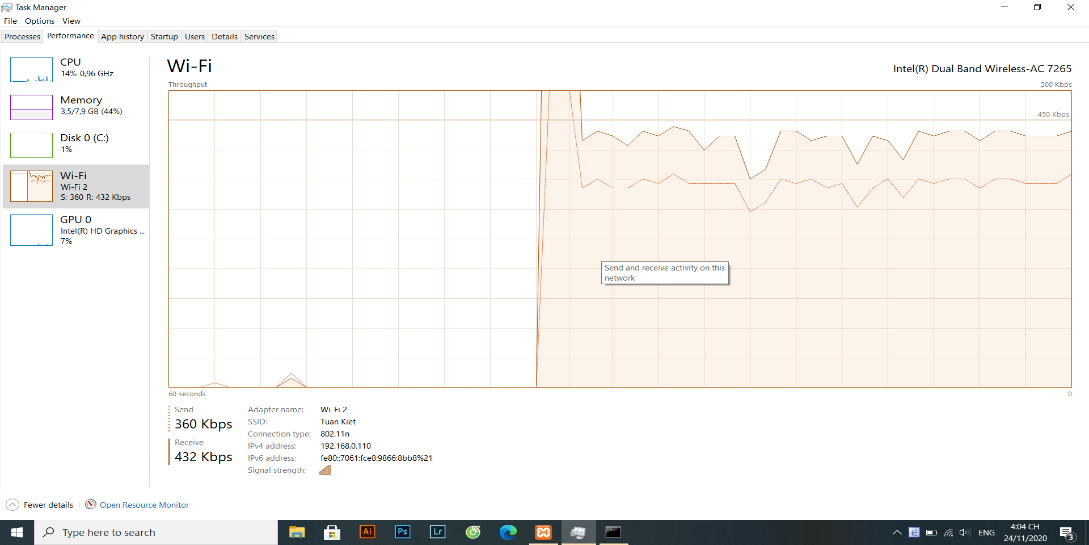
Nhóm nghiên cứu đã tiến hành sử dụng công cụ Tor’s Hammer để tiến hành tấn công vào máy mục tiêu có địa chỉ IP 192.168.0.110 với 500 luồng và mỗi luồng gửi 500 http request trên giây.



Hình 4.9. Cửa sổ thực thi công cụ Tor’s Hammer

Bằng phần mềm Wireshark có thể thấy một lượng lớn gói tin UDP được gửi đi từ máy nguồn có IP:192.168.0.104 tới cổng 8080 của máy nạn nhân có IP: 192.168.0.110

Kết quả của tấn công được hiển thị trên máy nạn nhân thông qua trình quản lý tác vụ của hệ điều hành Windows.



Hình 4.10. Trình quản lý tác vụ của máy nạn nhân

Hình 4.10. chụp Task Manager trên máy bạn nhân có IP: 191.168.0.110 với lưu lượng mạng nhận được lên tới 432 kbps chiếm đến hơn 10 % hiệu năng của card Wifi máy nạn nhân.

Ngoài ra nhóm nghiên cứu còn tiến hành thực nghiệm tấn công vào thiết bị Smart phone và thu được kết quả.

Kết quả đo lưu lượng mạng trên thiết bị Smart Phone bằng Speed Test khi bị tấn công DOS UDP Flood được biểu thị trên hình 4.6.

4.2.1. Đánh giá kết quả thực nghiệm

|  |  |
| --- | --- |
| **Ưu điểm** | **Nhược điểm** |
| Vì các cuộc tấn công Slow Post không yêu cầu băng thông rộng, chẳng hạn như cần thiết với các cuộc tấn công brute-force DDoS , chúng có thể khó phân biệt với lưu lượng truy cập thông thường. | Khi chạy các phiên bản Python 3.\* thì sinh ra các Exception, Erorr liên quan đến lệnh Print(). |
| Các kiểu tấn công lớp ứng dụng này không yêu cầu nhiều tài nguyên, chúng có thể được kích hoạt từ một máy tính, khiến chúng rất dễ khởi chạy và khó ngăn chặn. | Không phù họp cho người dùng không sử dụng command line. |
| DoS một ttacks có thể được thực hiện thông qua Mạng Tor(Tor Network) bằng cách sử dụng một socks proxy, Khả năng theo dõi , tuy vết và khó. |  |
| Công cụ có thể chạy trên tất cả các hệ điều hành chỉ cần cài đặt trước python có phiên bản >= 2.7. |  |
| Sử dụng đơn giản thuận tiện cho pentest. |  |

Bảng 4.1. Ưu và nhược điểm của công cụ Tor's Hammer

Đây là một công cụ tấn công Dos hiệu quả, hiệu năng và tính năng sử dụng tốt. Áp dụng phương thức tấn công phù hợp trong trường hợp không nhất thiết phải đánh sập server, lý do này sẽ khiến thời gian phản ứng của đội vận hành sẽ chậm hơn so với việc ta DOS tấn công gây ngập lụt . . . Ngoài ra việc kết hợp tấn công thông qua mạng Tor sẽ gây khó khăn đáng kể cho việc theo dõi và phòng chống đấy là khi chưa bàn tới việc ngay bản chất tấn công slow HTTP đã khó phát hiện rồi.

KẾT LUẬN

Trong báo cáo này, nhóm nghiên cứu đã tiến hành nghiên cứu về hình thức tấn công từ chối dịch vụ DOS. Báo cáo đã được nhóm viết báo cáo chia thành 4 nội dung. Đầu tiên, nhóm viết báo cáo đã trình bày tổng quan về tình hình an ninh mạng và thực trạng tấn công mạng trên thế giới. phần này đã đưa ra một cái nhìn tổng quan về thực trạng an ninh mạng trên thế giới hiện nay. Thứ hai, nhóm viết báo cáo đã trình bày cơ sở lý thuyết của hình thức tấn công DOS. Phần này đã trình bày từ tổng quan lý thuyết về hình thức tấn công DOS đến một số kỹ thuật tấn công DOS phổ biến. Thứ ba, nhóm viết báo cáo đã trình bày mô hình để thực nghiệm tấn công DOS. Phần này đã trình bày cụ thể cấu trúc mô hình, các thiết bị và công cụ được sử dụng để thực hiện thực nghiệm tấn công DOS. Thứ tư, nhóm viết báo cáo đã trình bày chi tiết các bước để thực hiện quá trình thực nghiệm tấn công DOS. Từ các kết quả thực nghiệm, nhóm viết báo cáo đã đưa ra các đánh giá về hình thức và công cụ tấn công.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] “Tình hình an ninh mạng qua những số liệu mới nhất,” *CyStack Resources*, Oct. 19, 2018. https://resources.cystack.net/tinh-hinh-an-ninh-mang/ (accessed Nov. 23, 2020).

[2] S. User, “Continuity Central.” https://www.continuitycentral.com/ (accessed Nov. 23, 2020).

[3] “Understanding Denial-of-Service Attacks | CISA.” https://us-cert.cisa.gov/ncas/tips/ST04-015 (accessed Nov. 18, 2020).

[4] “Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4 - Cisco,” Aug. 26, 2019. https://web.archive.org/web/20190826143507/https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html (accessed Nov. 18, 2020).

[5] “Denial-of-service attack,” *Wikipedia*. Nov. 16, 2020, Accessed: Nov. 18, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Denial-of-service\_attack&oldid=989006172.

[6] “Article: What is... Denial-of-Service (DoS) | F-Secure.” https://www.f-secure.com/v-descs/articles/denial-of-service.shtml (accessed Nov. 19, 2020).

[7] “SYN flood,” *Wikipedia*. Sep. 24, 2020, Accessed: Nov. 19, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=SYN\_flood&oldid=980118288.

[8] “UDP Flood DDoS Attack,” *Cloudflare*. https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (accessed Nov. 19, 2020).

[9] “Denial-of-Service (DoS) Attacks — Web-based App Security,” *Spanning*, Jun. 16, 2020. https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/ (accessed Nov. 19, 2020).

[10] “What is an ICMP Flood Attack?,” *NETSCOUT*. https://www.netscout.com/what-is-ddos/icmp-flood (accessed Nov. 19, 2020).

[11] “Slowloris DDoS Attack,” *Cloudflare*. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (accessed Nov. 19, 2020).

[12] “Leeon123/TCP-UDP-Flood,” *GitHub*. https://github.com/Leeon123/TCP-UDP-Flood (accessed Nov. 19, 2020).