|  |
| --- |
| **BAN CƠ YẾU CHÍNH PHỦ**  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  **KHOA CÔNG NGHỆ THÔNG TIN**  ---🙠🕮🙢--- |
| **THỰC TẬP CƠ SỞ CHUYÊN NGÀNH**  **PHÂN TÍCH VÀ ĐỐI PHÓ VỚI CÁC CUỘC TẤN CÔNG TỪ CHỐI DỊCH VỤ (DDoS)**  Ngành: An toàn thông tin  Mã số nhóm: 89 |
| *Sinh viên thực hiện*:   1. **Lê Anh Đức – Mã SV: AT180611** 2. **Nguyễn Văn Hùng – Mã SV: AT180620** 3. **Nguyễn Công Quý – Mã SV: AT180640**   *Giảng viên hướng dẫn*:  **ThS.Cao Thanh Vinh**  Khoa Công nghệ thông tin – Học viện Kỹ thuật Mật mã |
| Hà Nội, 2024 |

**MỤC LỤC**

[DANH MỤC KÍ HIỆU VIẾT TẮT 3](#_Toc166930553)

[DANH MỤC HÌNH VẼ, BẢNG 3](#_Toc166930554)

[LỜI NÓI ĐẦU 3](#_Toc166930555)

[CHƯƠNG 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDoS) 4](#_Toc166930556)

[1.1. GIỚI THIỆU VỀ TẤN CÔNG DOS VÀ DDOS 4](#_Toc166930557)

[1.1.1. Khái niệm DoS và DDoS 4](#_Toc166930558)

[1.1.2. Các giai đoạn của cuộc tấn công DoS và DDoS 4](#_Toc166930559)

[1.1.3. Phân loại tấn công DDoS 5](#_Toc166930560)

[1.2. Mạng BOTNET 7](#_Toc166930561)

[1.2.1. Khái niệm mạng Botnet 7](#_Toc166930562)

[1.2.2. Mạng Internet Relay Chat 7](#_Toc166930563)

[1.2.3. Chương trình Bot và Botnet 8](#_Toc166930564)

[Mô hình tấn công DDoS 10](#_Toc166930565)

[Mô hình tấn công Agent-Handle 10](#_Toc166930566)

[Mô hình tấn công IRC- Based 12](#_Toc166930567)

[CHƯƠNG 2: TỔNG QUAN VỀ TẤN CÔNG VÀ PHÒNG CHỐNG DDoS 13](#_Toc166930568)

[2.1. Tấn công làm cạn kiệt băng thông (Band with Deleption) 13](#_Toc166930569)

[2.1.1. Tấn công tràn băng thông (Flood attack) 13](#_Toc166930570)

[2.1.2. Tấn công khuyếch đại (Amplification attack) 18](#_Toc166930571)

[2.2. Tấn công làm cạn kiệt tài nguyên (Resoure Deleption) 21](#_Toc166930572)

[2.3. Các biến thể của tấn công DDoS 3](#_Toc166930573)

[2.3.1. Tấn công kiểu Flash DDoS 3](#_Toc166930574)

[2.3.2. Tấn công kiểu DRDoS 3](#_Toc166930575)

[2.3.3. Tấn công DDoS trên điện thoại di động 3](#_Toc166930576)

[2.4. Một số công cụ tấn công DDoS phổ biến hiện nay 3](#_Toc166930577)

[2.5. Phòng chống tấn công DDoS 3](#_Toc166930578)

[2.5.1. Phát hiện tấn công 3](#_Toc166930579)

[2.5.2. Giải pháp phòng chống DDoS 3](#_Toc166930580)

[CHƯƠNG 3: TRIỂN KHAI THỰC NGHIỆM TẤN CÔNG DDoS 3](#_Toc166930581)

[3.1. Kịch bản 1: Tấn công UDP Flood 3](#_Toc166930582)

[3.2. Kịch bản 2: Tấn công SYN Flood 3](#_Toc166930583)

[3.3. Kịch bản 3: Tấn công HTTP Flood 3](#_Toc166930584)

[KẾT LUẬN 3](#_Toc166930585)

[TÀI LIỆU THAM KHẢO 3](#_Toc166930586)

# DANH MỤC KÍ HIỆU VIẾT TẮT

# DANH MỤC HÌNH VẼ, BẢNG

# LỜI NÓI ĐẦU

Trong thời đại kỹ thuật số ngày nay, việc sử dụng internet đã trở thành một phần không thể thiếu trong cuộc sống cá nhân và doanh nghiệp. Tuy nhiên, điều này cũng mang lại một loạt các rủi ro, trong đó có các cuộc tấn công từ chối dịch vụ (DDoS) - một trong những hình thức phổ biến nhất của tội phạm mạng.

Cuộc tấn công từ chối dịch vụ (DDoS) không phải là một hiện tượng mới mẻ, mà là một dạng tấn công đã tồn tại từ những ngày đầu của internet. Tuy nhiên, nó đã trở nên phổ biến hơn và tinh vi hơn theo thời gian, điều này cũng phản ánh một sự phát triển và tiến hóa của cả công nghệ và cách thức thực hiện các cuộc tấn công mạng.

Các cuộc tấn công DDoS (Distributed Denial Of Service) đầu tiên được ghi nhận vào những năm 1990, khi internet mới chỉ đang phát triển. Những cuộc tấn công này thường tập trung vào việc làm quá tải các máy chủ và hạ tầng mạng bằng cách gửi lượng lớn yêu cầu từ các máy tính chiếm dụng. Tuy nhiên, vào những năm cuối thập kỷ 1990 và đầu thập kỷ 2000, sự phổ biến của internet đã tạo ra một môi trường mới cho các cuộc tấn công DDoS.

Các cuộc tấn công từ chối dịch vụ (DDoS) đang trở nên ngày càng phức tạp và nguy hiểm hơn. Theo các báo cáo từ các công ty nghiên cứu bảo mật, trong năm 2023 có hơn 10.000 cuộc tấn công DDoS được ghi nhận trên toàn cầu, với con số này đang tăng lên từng năm. Các cuộc tấn công này thường gây ra tăng đột biến về lưu lượng truy cập, có thể lên đến hàng trăm hoặc thậm chí hàng nghìn lần so với mức bình thường, tạo ra sự quá tải cho hạ tầng mạng của các tổ chức. Nghiên cứu cũng chỉ ra rằng các cuộc tấn công DDoS gây ra thiệt hại kinh tế lớn, với mức lên đến hàng triệu đô la mỗi năm, bao gồm cả chi phí cho việc khôi phục hạ tầng mạng và mất mát do gián đoạn kinh doanh. Đồng thời, sự đa dạng hóa về mục tiêu và phương thức tấn công, cùng với sự tận dụng của botnet IoT, làm cho việc đối phó với các cuộc tấn công DDoS trở nên ngày càng phức tạp và khó khăn hơn.

Trong bối cảnh này, việc phân tích và đối phó với các cuộc tấn công DDoS trở nên cực kỳ quan trọng. Chúng ta cần hiểu rõ về cách thức hoạt động của loại tấn công này, các nguyên nhân và mục tiêu của kẻ tấn công, cũng như các biện pháp phòng ngừa và phản ứng hiệu quả.

Từ những vấn đề thực tiễn trên, căn cứ vào lý thuyết về an ninh an toàn của hệ thống thông tin, đề tài sẽ trình bày một số vấn đề:

1. Tìm hiểu về tấn công từ chối dịch vụ -DdoS
2. Các kỹ thuật tấn công DDos
3. Mô phỏng một số kiểu tấn công DDos
4. Phòng chống bị tấn công DdoS

# CHƯƠNG 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDoS)

## 1.1. GIỚI THIỆU VỀ TẤN CÔNG DOS VÀ DDOS

### 1.1.1. Khái niệm DoS và DDoS

DoS tên đầy đủ tiếng Anh là Denial of Service, dịch ra tiếng Việt là từ chối dịch vụ. Tấn công từ chối dịch vụ DoS là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó. Kẻ tấn công thực hiện điều này bằng cách "tuồn" ồ ạt traffic hoặc gửi thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu, từ đó khiến người dùng hợp pháp (nhân viên, thành viên, chủ tài khoản) không thể truy cập dịch vụ, tài nguyên họ mong đợi.

Nạn nhân của tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội...

DDoS là viết tắt của Distributed Denial of Service, có nghĩa là từ chối dịch vụ phân tán. DDoS là một dạng tấn công server chứa website, gây cạn kiệt tài nguyên hệ thống máy chủ, ngập lưu lượng băng thông internet và làm gián đoạn kết nối của người dùng.

Đây là kiểu tấn công phân tán, các đối tượng không chỉ sử dụng máy tính của mình mà lợi dụng cả máy tính người dùng để tấn công DDoS. Cụ thể, chúng sẽ chiếm dụng quyền kiểm soát máy tính của người dùng và gửi yêu cầu, dữ liệu đến một website hay một địa chỉ email nào đó. Tấn công DDoS ngày càng trở nên tinh vi và phức tạp, với 3 kiểu cơ bản:

* **Volume – based**: dùng lưu lượng truy cập cao nhằm làm tràn ngập băng thông mạng.
* **Protocol**: chủ yếu khai thác các tài nguyên trên máy chủ.
* **Application**: là kiểu tấn công nguy hiểm nhất, tập trung vào các ứng dụng website.

### 1.1.2. Các giai đoạn của cuộc tấn công DoS và DDoS

**Giai đoạn chuẩn bị:**

* **Thu thập thông tin:** Kẻ tấn công thu thập thông tin về mục tiêu, bao gồm địa chỉ IP, hệ thống mạng, phần mềm và ứng dụng đang sử dụng.
* **Lựa chọn phương thức tấn công:** Kẻ tấn công lựa chọn phương thức tấn công phù hợp dựa trên thông tin thu thập được và mục tiêu tấn công.
* **Chuẩn bị công cụ:** Kẻ tấn công chuẩn bị các công cụ cần thiết để thực hiện tấn công, chẳng hạn như botnet, phần mềm độc hại hoặc các công cụ tấn công DoS/DDoS sẵn có.

**Giai đoạn xác định mục tiêu và thời điểm tấn công:**

* **Xác định mục tiêu:** Kẻ tấn công xác định mục tiêu cụ thể để tấn công, chẳng hạn như website, máy chủ, ứng dụng hoặc mạng lưới.
* **Lựa chọn thời điểm tấn công:** Kẻ tấn công lựa chọn thời điểm tấn công phù hợp để gây ra thiệt hại lớn nhất cho mục tiêu, chẳng hạn như giờ cao điểm hoặc khi có sự kiện quan trọng.

#### . Giai đoạn phát động tấn công và xóa dấu vết:

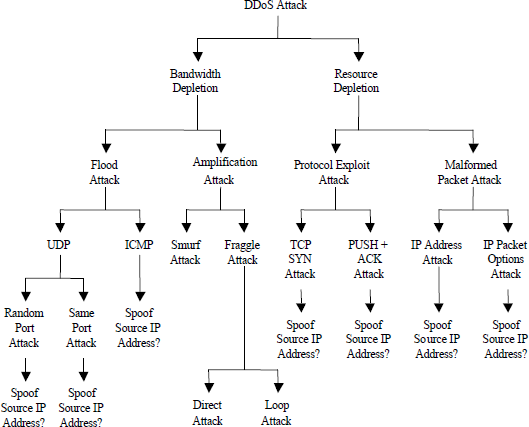
* **Phát động tấn công:** Kẻ tấn công sử dụng các công cụ đã chuẩn bị để thực hiện tấn công DoS/DDoS vào mục tiêu.
* **Xóa dấu vết:** Kẻ tấn công cố gắng che giấu danh tính và hành vi của mình để tránh bị truy ngược về mình.

### 1.1.3. Phân loại tấn công DDoS

Các loại tấn công DDoS có rất nhiều biến thể, nên việc phân loại cũng có rất nhiều cách khác nhau. Tuy nhiên, giới chuyên môn thường chia các kiểu tấn công DDoS thành 2 dạng chính, dựa vào mục đích của kẻ tấn công:

* Tấn công DDoS làm cạn kiệt băng thông
* Tấn công DDoS làm cạn kiệt tài nguyên hệ thống

Ngoài việc phân loại như trên, có thể phân loại tấn công DDos dựa trên mô hình OSI 07 tầng. Xu hướng các cuộc tấn công DDos cho thấy thủ phạm thường biến đổi các cuộc tấn công theo mô hình OSI. Các cuộc tấn công được phân loại như sau:



Hình 1.1: Sơ đồ phân loại DDoS attack theo mục đích tấn công

* Các cuộc tấn công IP nhằm vào băng thông – tấn công vào lớp 3 (tầng mạng).
* Các cuộc tấn công TCP trên máy chủ sockets – tấn công vào lớp 4 (tầng vận chuyển).
* Các cuộc tấn công HTTP trên máy chủ web – tấn công vào lớp 7 (tầng ứng dụng).
* Tấn công vào ứng dụng web, đánh vào tài nguyên CPU – tấn công trên lớp 7.

Ngày nay, hệ thống phòng thủ DDos liên tục được hoàn thiện và đa dạng, nhưng thường tập trung ở tầng thấp trong mô hình OSI. Do đó các cuộc tấn công vào lớp ứng dụng (Lớp 7) đang ngày càng phổ biến.

Khi phân tích một cuộc tấn công DDos nhằm vào Lớp 7, phải nghiên cứu các lớp khác. Do cuộc tấn công vào Lớp 7 luôn được ngụy trang và đi kèm với các cuộc tấn công nhằm vào lớp khác. Về bản chất, kẻ tấn công vào Lớp 7 sẽ tạo ra một giao diện cho người sử dụng như trình duyệt, các dịch vụ email, hình ảnh và những ứng dụng khác để gửi thông tin qua giao thức (SMTP, HTTP).

Một cuộc tấn công DDos vào Lớp 7 thường nhằm mục đích và mục tiêu cụ thể như: làm gián đoạn giao dịch, cản trở truy cập vào cơ sở dữ liệu. Kiểu tấn công này đòi hỏi nguồn lực ít hơn và đi kèm với các cuộc tấn công ở Lớp khác như lớp mạng. Một cuộc tấn công lớp ứng dụng sẽ được ngụy trang giống như những truy cập hợp pháp và nó có mục tiêu cụ thể là các ứng dụng. Cuộc tấn công có thể làm gián đoạn các chức năng cụ thể của dịch vụ như phản hồi thông tin, tìm kiếm …

Phân biệt cuộc tấn công DDos vào Lớp 7 so với các cuộc tấn công khác dựa trên một số điểm như sau:

1. Tấn công DDos vào Lớp mạng làm cho máy chủ quá tải với các yêu cầu (request) giả, trong khi tấn công Lớp 7 buộc máy chủ phải trả lời với mỗi yêu cầu thật.
2. Trong tấn công DDos vào Lớp 7, các máy tấn công phải tạo ra nhiều hết cỡ các kết nối TCP. Như vậy, các địa chỉ IP thực tế sẽ được sử dụng để gửi yêu cầu và máy nạn nhận phải đáp ứng các truy vấn hợp lệ đó. Vì vậy chúng có thể vượt qua các hệ thống phòng thủ DDos nghiêm ngặt.
3. Tấn công DDos vào Lớp 7 có thể bao gồm các tấn công khác và lợi dụng lỗ hổng trong các phần mềm ứng dụng để tấn công, đồng thời phân tán sự chú ý vào nhiều mục tiêu để che giấu mục tiêu chính là máy chủ Web. Hay nói cách khác kiểu tấn công này tinh vi hơn, không tấn công toàn bộ mà tấn công vào đúng mục tiêu đang hướng tới.
4. Khác biệt đáng chú ý nhất là các cuộc tấn công DDos vào Lớp 7 tạo ra một khối lượng xử lý lớn và đẩy lượng xử lý này xuống hạ tầng cơ sở mạng của máy chủ làm “ngập lụt” băng thông. Các cuộc tấn công vào Lớp 7 thường đặt mục tiêu vào máy chủ, nhưng những máy chủ này đa phần được nhìn nhận là nạn nhân phía sau. Ví dụ: các cuộc tấn công nhằm vào HTTP, VoIP hoặc hệ thống tên miền DNS.
5. Tấn công DDos nhằm vào Lớp 7 thường khai thác những sai sót, hạn chế của các ứng dụng. Từ đó làm cho hệ thống tiêu thụ nhiều tài nguyên nhưng không giải quyết được dẫn tới treo máy chủ.
6. Tấn công DDos nhằm Lớp 7 không mang tính phổ biến, nhưng đa dạng và tùy thuộc vào mỗi ứng dụng. Do đó đây là một thách thức lớn trong việc chống lại các cuộc tấn công vào lớp này

## 1.2. Mạng BOTNET

### 1.2.1. Khái niệm mạng Botnet

BotNet là một mạng gồm từ hàng trăm tới hàng triệu máy tính hoàn toàn mất quyền kiểm soát. Các máy tính này vẫn hoạt động bình thường, nhưng chúng không hề biết rằng đã bị các hacker kiểm soát và điều khiển. Các máy tính này có thể bị hacker lợi dụng để tải về các chương trình quảng cáo, hay cùng đồng loạt tấn công một trang web nào đó mà ta gọi là DDoS. Hầu hết chủ của những máy tính này không hề biết rằng hệ thống của họ đang được sử dụng theo cách này.

Khi đã chiếm được quyền điều khiển, hacker sẽ xâm nhập vào các hệ thống này, ấn định thời điểm và phát động tấn công từ chối dịch vụ. Với hàng triệu các máy tính cùng tấn công vào một thời điểm, nạn nhân sẽ bị ngốn hết băng thông trong nháy mắt, dẫn tới không thể đáp ứng các yêu cầu hợp lệ và bị loại khỏi internet.

Chúng ta hãy cùng xem ví dụ sau để thấy được sự nguy hiểm của mạng BotNet. Giả sử nếu dùng cách tấn công Ping of Death tới một máy chủ, máy chủ kết nối với mạng có tốc độ 100Mb/s, kết nối với tốc độ 1Mb/s. Vậy tấn công trên là vô nghĩa.

Bây giờ nếu có 1000 kết nối tấn công vào máy chủ trên, vậy băng thông của 1000 kết nối cộng lại sẽ ~ 1Gb/s và hậu quả máy chủ sẽ quá tải!

1000 kết nối này sẽ được tạo từ mạng BotNet.

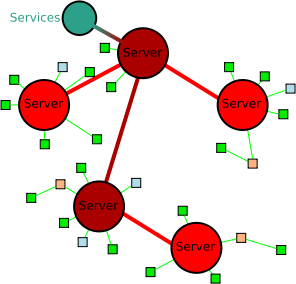
### 1.2.2. Mạng Internet Relay Chat

Mạng Internet Relay Chat (IRC) được sáng tạo bởi Jarkko Oikarinen (nickname “WiZ”) vào 8-1988 để thay thế cho một chương trình có tên là MUT (MultiUser Talk) trên một kênh BBS gọi là OuluBox tại Phần Lan. Ông tìm được cảm hứng cho dự án của mình từ hệ thống Bitnet Relay Chat của mạng Bitnet.

IRC được nhiều người chú ý đến từ khi nó được dùng sau Bức màn sắt (Iron Curtain) để viết phóng sự trực tuyến về sự sụp đổ của Liên bang Xô Viết trong khi tất cả các phương tiện truyền thông khác không hoạt động được.

IRC là viết tắt của cụm từ Internet Relay Chat, là một dạng liên lạc cấp tốc qua mạng Internet. Nó được thiết kế với mục đích chính là cho phép các nhóm người trong một phòng thảo luận (channel) liên lạc với nhau. Tuy nhiên, nó cũng cho phép người dùng liên lạc riêng nếu họ thích.

Hiện nay, IRC là mạng trò chuyện trực tuyến lớn, có vài triệu kênh trên máy chủ trên khắp thế giới. Giao thức viễn thông này cũ hơn, khó sử dụng hơn IM (Instant Message- tin nhắn nhanh), IRC đã từng hoàn toàn dựa vào nhập thô ASCII. Tuy nhiên, hiện nay đã có nhiều ứng dụng đồ họa làm cho IRC dễ sử dụng hơn.



Hình 1.2 Mô hình mạng IRC

### 1.2.3. Chương trình Bot và Botnet

Bot là từ viết tắt của Robot, là các ứng dụng phần mềm chạy các tác vụ tự động hóa trên mạng. Thông thường, bot thực hiện các tác vụ đơn giản và có cấu trúc lặp đi lặp lại với một tần suất cao hơn nhiều so với khả năng của một soạn thảo viên là con người. Ứng dụng lớn nhất của bot là trong duyệt tự động web theo kiểu“bò loang” (web spidering), trong đó một chương trình tự động tìm kiếm, phân tích và sắp xếp thông tin từ các máy chủ web với tốc độ cao hơn nhiều lần tốc độ con người. Mỗi máy chủ có một file có tên robots.txt chứa các quy tắc cho việc bò loang tự động tại máy chủ đó, đây là các quy tắc mà con bot cần tuân theo.

Ngoài ra, bot thường được cài đặt tại những nơi đòi hỏi tốc độ phản ứng cao hơn tốc độ của con người, như trong các trò chơi điện tử, các trang web đấu giá, hoặc trong các tình huống cần đến sự bắt chước các hoạt động của con người (chẳng hạn các chatbot- bot nói chuyện).

BotNet là từ chỉ một tập hợp các bot hoạt động một cách tự chủ, cũng có thể dùng để chỉ một nhóm bot bất kỳ, chẳng hạn IRC bot, từ này thường được dùng để chỉ một tập hợp các máy tính đã bị tấn công và đang chạy các chương trình độc hại, thường là sâu máy tính, Trojan hay backdoor, dưới cùng một hạ tầng cơ sở lệnh và điều khiển. Một chương trình chỉ huy BotNet (BotNet’s originator hay bot header) có thể điều khiển cả nhóm bot từ xa, thường là qua IRC, và thường nhằm các mục đích bất chính.

Các BotNet đã trở thành một phần quan trọng của Internet. Do đa số các mạng IRC truyền thống thực hiện các biện pháp cấm truy cập, sử dụng mạng BotNet, nên những người điều khiển BotNet phải tự tìm các server cho mình, thường là trong các mạng giáo dục, công ty, chính phủ và thậm chí là quân sự…, nơi có tốc độ đường truyền cao.

### 1.2.4. Mạng IRC botnet

Mỗi một máy tính bị kiểm soát, bị cài một phần mềm nguy hiểm bí mật kết nối đến kênh IRC của kẻ tấn công gọi là một bot. Mạng các kết nối tới một kênh IRC gọi là một IRC botnet. Các bước xây dựng mạng botnet:

**Bước 1:** Lây nhiễm vào máy tính:

Đầu tiên, kẻ tấn công lừa cho người dùng chạy file có phần mở rộng “.exe”- các Agobot. Một khi được kích hoạt, nó sẽ thêm các thông số trong Registry để đảm bảo sẽ được chạy cùng hệ thống khi khởi động. Trong Registry có các vị trí cho các ứng dụng chạy lúc khởi động tại:

* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

**Bước 2:** Lây lan và xây dựng mạng botnet:

Khi trong mạng có một máy tính bị nhiễm Agobot, nó sẽ tự động tìm kiếm các máy tính khác trong hệ thống và lây nhiễm sử dụng các lỗ hổng trong tài nguyên được chia sẻ trong hệ thống mạng.

Các Agobot thường cố gắng kết nối tới các dữ liệu shared mặc định dành cho các ứng dụng quản trị, bằng cách đoán username và password để có thể truy cập được vào một hệ thống khác và lây nhiễm.

Các Agobot có thể lây lan rất nhanh bởi chúng có khả năng tận dụng những điểm yếu trong hệ điều hành Windows, hay các ứng dụng, các dịch vụ chạy trên hệ thống.

**Bước 3:** Kết nối vào IRC:

Agobot sẽ tạo ra một IRC- Controlled Backdoor để mở các yếu tố cần thiết, và kết nối tới mạng botnet thông qua IRC. Sau khi kết nối, chúng sẽ mở những dịch vụ cần thiết để khi có yêu cầu chúng sẽ được điều khiển bởi kẻ tấn công thông qua giao thức IRC.

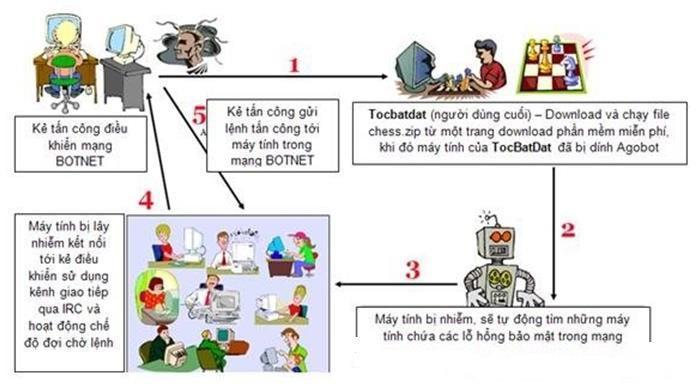
**Bước 4:** Điều khiển tấn công từ mạng botnet:

Kẻ tấn công điều khiển các máy trong mạng download những file .exe về chạy trên máy.

Lấy toàn bộ thông tin liên quan và cần thiết trên hệ thống mà kẻ tấn công muốn.

Chạy những file khác trên hệ thống đáp ứng yêu cầu của kẻ tấn công.

Chạy những chương trình DDoS tấn công hệ thống khác

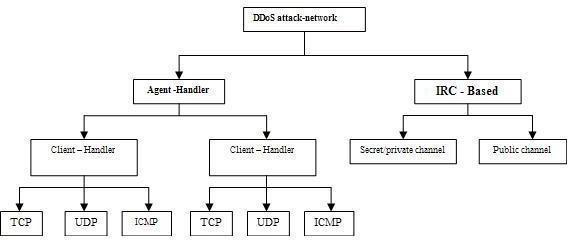


Hình 1.3 Sơ đồ cách hệ thống bị lây nhiễm và sử dụng Agobot

## 1.3. Mô hình tấn công DDoS

Tấn công DDoS có 2 mô hình chính:

* Mô hình Agent- Handler
* Mô hình IRC- Based



Hình 1.4. Sơ đồ mô hình tấn công DDoS

### 1.3.1. Mô hình tấn công Agent-Handle

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

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

A diagram of a crime

Description automatically generated

Hình 1.5 Kiến trúc mô hình tấn công Agent- Handler

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

Thông thường, kẻ tấn công sẽ đặt Handler software trên một router hay một server có lượng lưu thông lớn, 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 giao thức 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 nên họ hầu như không thấy ảnh hưởng gì đến hiệu năng của hệ thống.

Mỗi công cụ DDoS có một tập lệnh riêng, tập lệnh này được Handler và Agent thực hiện. Tuy nhiên ta có thể phân loại tổng quát tập lệnh chung của mọi công cụ như sau:

|  |  |
| --- | --- |
| **Lệnh** | **Mô tả** |
| Log On | Nhằm dùng để logon vào Handler software (user + password) |
| Turn On | Kích hoạt Handler sẵn sàng nhận lệnh |
| Log Off | Nhằm dùng để Logoff ra khỏi Handler software |
| Turn Off | Chỉ dẫn Handler ngưng hoạt động, nếu Handler đang quét tìm Agent thì dừng ngay hành vi này |
| Initiate Attack | Ra lệnh cho Handler hướng dẫn mọi Agent trực thuộc tấn công mục tiêu đã định |
| List Agents | Yên cầu Handler liệt kê các Agent trực thuộc |
| Kiss Agents | Loại bỏ một Agent ra khỏi hàng ngũ Attack-Network |
| Add victim | Thêm một mục tiêu để tấn công |
| Download Upgrades | Cập nhật cho Handler software (downloads file.exe về và thực thi) |
| Set Spoofing | Kích hoạt và thiết lập cơ chế giả mạo địa chỉ IP cho các Agent |
| Set Attack Time | Định thời điểm tấn công cho các Agent |
| Set attack Duration | Thông báo độ dài của cuộc tấn công vào mục tiêu |
| BufferSize | Thiết lập kích thước buffer của Agent (nhằm gia tăng sức mạnh cho Agent) |
| Help | Hướng dẫn sử dụng chương trình |

Bảng 1.1 Tập lệnh của Handler

|  |  |
| --- | --- |
| **Lệnh** | **Mô tả** |
| Turn On | Kich hoat Agent sẵn sàng nhận lệnh |
| Turn Off | Chỉ dẫn Agent ngưng hoạt động, nếu Agent đang quét tìm Handler/IRC |
| Channel | Thì dừng ngay hành vi này lại |
| Initiate Attacke | Ra lệnh Agent tấn công mục tiêu đã định |
| Download Upgrades | Cập nhật cho Agent software (downloaf file .exe về và thực thi) |
| Set Spoofing | Thiết lập cơ chế giả mạo địa chỉ IP cho các Agent hoạt động |
| Set Attack Duration | Thông báo độ dài các cuộc tấn công vào mục tiêu |
| Set Packet Size | Thiết lập kích thước của attack packet |
| Help | Hướng dẫn sử dụng chương trình |

Bảng 1.2 Tập lệnh của Agent

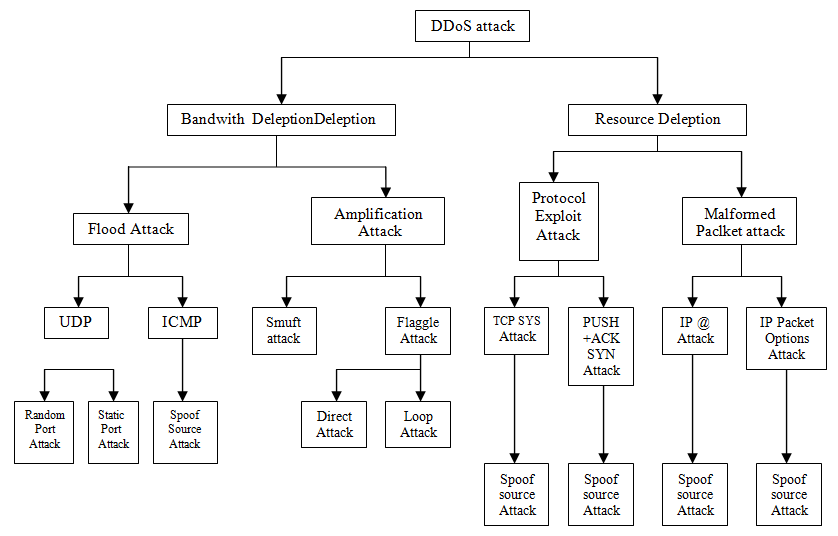
### 1.3.2. Mô hình tấn công IRC- Based

Như đã nói ở trên, Internet Relay Chat (IRC) là một hệ thống online chat multiuser (hệ thống trò chuyện trực tuyến đa người dùng). IRC cho phép người dùng tạo một kết nối đến nhiều server khác và chat thời gian thực. Kiến trúc của IRCnetwork bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel). IRC network cho phép người dùng tạo 3 loại channel: public, private và secret.

* Public channel (kênh công cộng): cho phép user của channel đó thấy IRC name và nhận được thông điệp 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 cùng channel thấy IRC name và thông điệp trên

# CHƯƠNG 2: TỔNG QUAN VỀ TẤN CÔNG VÀ PHÒNG CHỐNG DDoS



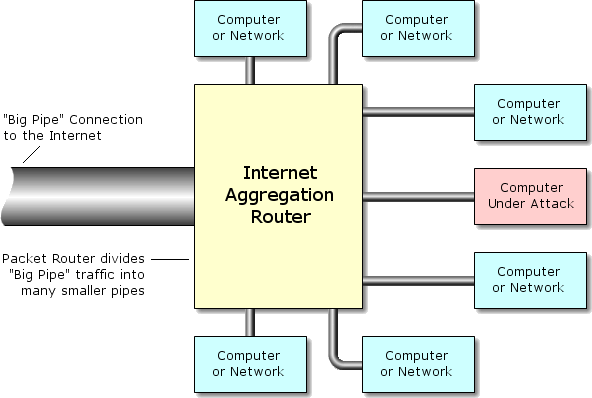
**Hình 2.1 Các kỹ thuật tấn công DDoS**

## 2.1. Tấn công làm cạn kiệt băng thông (Band with Deleption)

Tấn công làm cạn kiệt băng thông (Bandwidth Depletion Attack) là một loại tấn công nhằm làm quá tải băng thông của mạng mục tiêu, dẫn đến việc không thể cung cấp dịch vụ bình thường cho người dùng hợp pháp. Các tấn công này làm giảm hiệu suất hoặc ngừng hoạt động hoàn toàn của hệ thống bằng cách làm cho đường truyền mạng trở nên quá tải.

### 2.1.1. Tấn công tràn băng thông (Flood attack)

Trong tấn công tràn băng thông, các Agent sẽ gửi một lượng lớn các gói tin làm hệ thống nạn nhân bị chậm lại, treo và không thể đáp ứng các yêu cầu hợp lệ.



**Hình 2.2. Sơ đồ tấn công kiểu tràn băng thông (Flood attack)**

Như ta thấy trên sơ đồ, tất cả các gói tin đi vào một mạng máy tính qua “Big- Pipe” (ống dẫn lớn), sau đó được router chia ra những “Small-Pipe” (ống dẫn nhỏ hơn) cho các máy tính con tùy theo địa chỉ IP của gói tin. Khi bị tấn công, các gói tin từ Big-Pipe với số lượng lớn, vượt quá giới hạn của Small-Pipe, sẽ ồ ạt tràn vào máy tính của nạn nhân, dẫn tới máy nạn nhân sẽ bị treo hoặc khởi động lại.

Có thể chia Flood attack thành 2 loại:

* UDP flood attack: Tấn công tràn băng thông bằng gói tin UDP
* ICMP flood attack: Tấn công tràn băng thông bằng gói tin ICMP

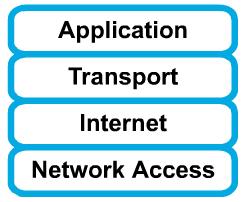
#### 2.1.1.1. Tấn công tràn băng thông bằng gói tin UDP

Khi nghiên cứu UDP flood attack cần hiểu các kiến thức cơ bản về (**1**) giao thức UDP; (**2**) cấu trúc gói UDP; (**3**) tìm số hiểu cổng trong UDP.

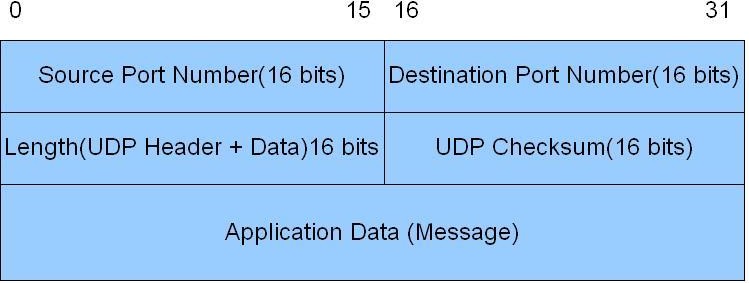
1. **Giao thức UDP:** UDP- User Datagram Protocol- là một trong những giao thức cốt lõi của giao thức TCP/IP. Dùng UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. Không giống TCP, UDP không cung cấp sự tin cậy và thứ tự truyền nhận, tức là các gói dữ liệu có thể đến đích không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên, UDP nhanh hơn TCP và hiệu quả đối với việc truyền dẫn những gói tin có kích thước nhỏ với yêu cầu khắt khe về thời gian. Do bản chất *“không trạng thái”* (statusless) của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.

Những ứng dụng phổ biến sử dụng UDP như DNS (Domain Name System), ứng dụng Streaming media, VoIP (Voice over IP) và game trực tuyến.

1. **Cấu trúc gói UDP:** Trong bộ giao thức TCP/IP, UDP cung cấp một giao diện rất đơn giản giữa tầng Ứng dụng (Application) ở bên trên với tầng Mạng (Internet) ở phía dưới.



**Hình 2.3 Các tầng trong giao thức TCP/IP**

UDP không đảm bảo cho các tầng phía trên thông điệp đã được gửi đi hay chưa và người gửi cũng không có trạng thái thông điệp UDP một khi nó đã được gửi. Các chương trình sử dụng UDP phải tự cài đặt phần kiểm tra dữ liệu. Vì lý do này, đôi khi UDP còn được gọi là Giao thức truyền vận không tin cậy (Unreliable Datagram Protocol).

**Hình 2.4 Cấu trúc gói tin UDP**

header của gói UDP chứa 4 trường dữ liệu:

* Source port (16 bit): Trường này xác định cổng của người gửi thông tin và có ý nghĩa nếu muốn nhận thông tin phản hồi từ người nhận. Nếu không dùng đến thì đặt nó bằng 0.
* Destination port (16 bit): Trường này xác định cổng nhận thông tin.
* Length(16 bit): Trường này xác định độ dài của toàn bộ gói tin UDP, bao gồm phần header và phần dữ liệu. Chiều dài tối thiểu là 8 bytr khi gói tin không có dữ liệu, chỉ có header.
* Checksum (16 bit): Trường checksum dùng cho việc kiểm tra lỗi của phần header và dữ liệu.

Do thiếu tính tin cậy, các ứng dụng sử dụng UDP nói chung phải chấp nhận mất mát, lỗi hoặc trùng dữ liệu.

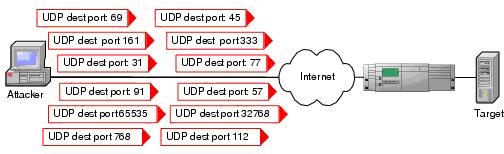
1. **Tìm số hiệu cổng trong UDP:** UDP dùng cổng để cho phép các ứng dụng giao tiếp với nhau:

* Cổng dùng 16 bit để đánh địa chỉ, vì vậy số của cổng nằm trong khoảng từ 0 đến 65535.
* Cổng 0 được để dành và không nên sử dụng.
* Cổng từ 1 đến 1023 được gọi là cổng “well-know” và trên các hệ điều hành tựa Unix, việc gắn kết tới một trong những cổng này đòi hỏi quyển root (toàn quyền truy cập).
* Cổng từ 1024 đến 49151 là cổng đã đăng ký.
* Cổng từ 49152 đến 65535 là các cổng tạm, được dùng chủ yếu bởi client khi liên lạc với server.

**Khái niệm UDP Flood attack:**

Tấn công tràn UDP là một kỹ thuật tấn công từ chối dịch vụ sử dụng các gói tin UDP. Trong tấn công tràn UDP, các cuộc tấn công tràn ngập được khởi chạy với việc gửi một số lượng lớn các gói UDP đến các port ngẫu nhiên hoặc được chỉ định trên hệ thống của nạn nhân. Để xác định ứng dụng được yêu cầu, hệ thống nạn nhân phải xử lý dữ liệu vào.

Trong trường hợp thiếu ứng dụng trên port được yêu cầu, hệ thống nạn nhân sẽ gửi thông điệp ICMP với nội dung “Đích không thể đến được” cho người gửi (ở đây là kẻ tấn công). Với số lượng lớn các gói UDP, hệ thống nạn nhân sẽ bị ép buộc phải gửi các gói ICMP, cuối cùng dẫn đến không thể nhận yêu cầu từ các người dùng hợp lệ do bão hòa về băng thông. Nếu các gói UDP được kẻ tấn công phân phối đến tất cả các port của hệ thống, hệ thống đó sẽ bị treo ngay lập tức.



**Hình 2.5 Sơ đồ tấn công tràn UDP**

Để thực hiện kỹ thuật này, hacker sẽ làm cho hệ thống đi vào một vòng lặp trao đổi các dữ liệu vô ích qua giao thức UDP. Hacker có thể giả mạo địa chỉ IP của các gói tin tấn công là địa chỉ loopback (127.0.0.1), sau đó gửi những gói tin này tới hệ thống của nạn nhân trên cổng UDP ECHO (cổng số 7).

Hệ thống của nạn nhân sẽ “echo” (hồi đáp) lại các thông điệp do 127.0.0.1 (chính nó) gửi đến, kết quả là nó sẽ thực hiện một vòng lặp echo vô tận. Tuy nhiên, nhiều hệ thống hiện nay không cho phép dùng địa chỉ loopback. Hacker sẽ giả mạo những địa chỉ IP của các máy tính trên mạng nạn nhân và tiến hành làm ngập lụt UDP trên hệ thống của nạn nhân.

Với việc sử dụng cổng UDP ECHO để thiết lập việc gửi và nhận các gói tin echo trên 2 máy tính, hoặc giữa mục tiêu với chính nó nếu kẻ tấn công giả mạo địa chỉ loopback (127.0.0.1), khiến mục tiêu dần dần sử dụng hết băng thông của mình, và cản trở hoạt động chia sẻ tài nguyên của các máy tính khác trong mạng.

#### 2.1.1.2. Tấn công tràn băng thông bằng gói tin ICMP

Để nghiên cứu về ICMP flood attack, cần hiểu kiến thức cơ bản về ICMP.

**Khái niệm ICMP:** Khi một gói tin truyền trên mạng, sẽ có rất nhiều vấn đề có thể xảy ra, ví dụ thời gian sống của gói tin (Time to live- TTL) đã hết khi nó chưa đến được đích, việc hợp nhất các phân mảnh của nó không hoàn thành hay gateway không tìm được đường đi cho nó… dẫn đến việc thất lạc gói tin. Nhưng làm cách nào để biết được một gói tin gửi đi đã đến đích hay chưa?

Giao thức Điều khiển việc truyền tin trên mạng (Internet Control Message Protocol- ICMP) được sinh ra để làm nhiệm vụ này. Các chức năng chính của ICMP bao gồm:

Điều khiển lưu lượng (Flow control): khi các gói dữ liệu đến quá nhanh, receiver hoặc thiết bị định tuyến sẽ gửi một thông điệp ICMP trở lại sender, yêu cầu sender tạm thời ngừng gửi dữ liệu.

Thông báo lỗi: Trong trường hợp không tới được địa chỉ đích thì hệ thống sẽ gửi lại một thông báo lỗi “Destination unsearchable”.

Định hướng lại các tuyến (Redirect Router): Một Router gửi một thông điệp ICMP cho một trạm thông báo nên sử dụng Router khác. Thông điệp này chỉ có thể được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến trở lên.

Kiểm tra các trạm xa: Một trạm có thể gửi một thông điệp ICMP “Echo” để kiểm tra một trạm khác có hoạt động hay không.

Thông điệp ICMP được chia làm 2 nhóm: các thông điệp truy vấn và các thông điệp báo lỗi.

**ICMP packet**

**Bit 0 – 7 Bit 8 – 15 Bit 16 - 23 Bit 24 - 31**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Header (160 bits OR 20 Bytes)** | Version/IHL | Type of service | Length | |
| Identification | | *Flags(3)* and *Fragment offset(13)* | |
| Time To  Live(TTL) | Protocol | Checksum | |
| Source IP address | | | |
| Destination IP address | | | |
| **ICMP Payload (64+ bits OR 8+ Bytes)** | Type of message | Code | | Checksum |
| Quench | | | |
| Data (*optional*) | | | |

**Hình 2.6 Cấu trúc tổng quát của gói tin ICMP**

Cấu trúc của một gói tin ICMP, nó bao gồm:

* Header: chứa các thông tin header về gói tin ICMP, như độ dài, thời gian sống, địa chỉ gửi/nhận…
* Payload- nội dung của gói tin:
  + Type of ICMP message (8 bits): chỉ ra loại thông điệp. Ví dụ, Type= 0: Echo request message, Type= 8: Echo reply message.
  + Code (8 bits): Bổ sung thêm thông tin cho Type.
  + Checksum (16 bits): dùng để kiểm tra lỗi gói tin

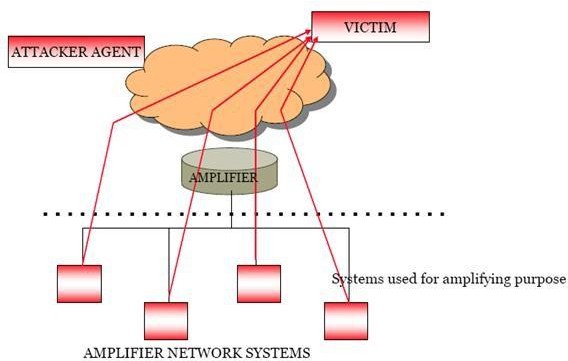
**Phương thức tấn công:** Tương tự phương thức UDP flood attack. Các Agent sẽ gửi một lượng lớn các ICMP\_ECHO\_REQUEST đến hệ thống mục tiêu, làm hệ thống này phải reply một lượng tương ứng packet để trả lời, dẫn đến nghẽn đường truyền và không thể đáp ứng những yêu cầu hợp lệ.

### 2.1.2. Tấn công khuyếch đại (Amplification attack)

Là một kiểu tấn công vào băng thông hệ thống, kẻ tấn công sẽ Ping đến địa chỉ của một mạng nào đó mà địa chỉ nguồn chính là địa chỉ của nạn nhân. Khi đó, toàn bộ các gói Reply sẽ được chuyển tới địa chỉ IP của máy nạn nhân. Nghĩa là ở đây kẻ tấn công sẽ khuếch đại cuộc tấn công bằng việc dùng thêm một yếu tố thứ 3- mạng khuếch đại- để làm ngập băng thông của nạn nhân.

Amplification attack nhắm đến việc sử dụng tính năng Directed broadcast của các router nhằm khuếch đại và định hướng cuộc tấn công. Tính năng này cho phép bên gửi chỉ định một địa chỉ IP cho toàn subnet bên nhận, router sẽ có nhiệm vụ gửi đến tất cả địa chỉ IP trong subnet đó packet mà nó nhận được.

Kẻ tấn công có thể gửi các message trực tiếp hay thông qua một số Agent nhằm làm gia tăng cường độ của cuộc tấn công.



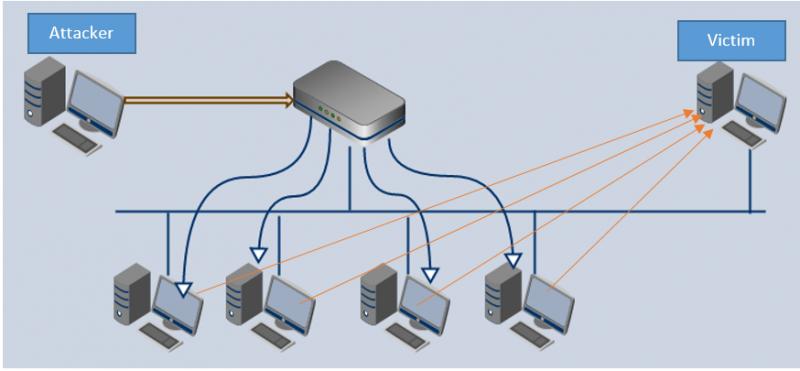
**Hình 2.7 Sơ đồ tấn công khuếch đại**

Dạng tấn công Amplification này chỉ đạt được hiệu quả cao khi có được mạng khuếch đại lớn. Hơn nữa, tính năng Directed broadcast trên router phải được bật, mà ngay cả khi có những điều kiện thuận lợi như vậy thì, do sử dụng các gói tin ICMP nên kiểu tấn công này dễ dàng bị chặn bởi firewall. Chính vì phức tạp và khó thực hiện như vậy, nên kiểu tấn công này hiện đã không còn tồn tại.

Có thể chia Amplification attack thành 2 loại:

* Tấn công kiểu Smuft (Smuft attack).
* Tấn công kiểu Fraggle (Fraggle attack)

#### 2.1.2.1. Tấn công kiểu Smuft

****

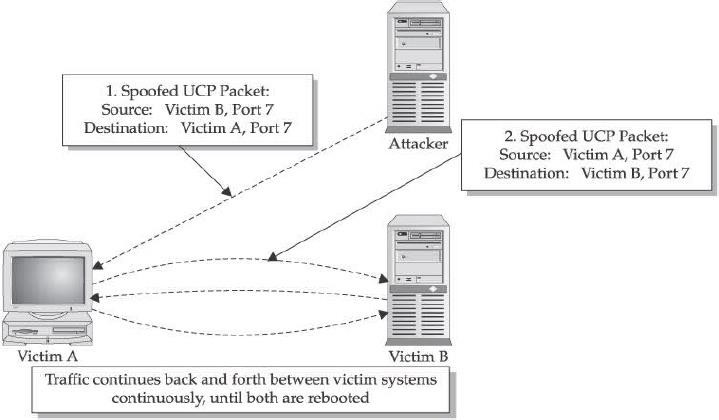
**Hình 2.8 Sơ đồ tấn công kiểu Smuft**

Kiểu tấn công Smuft thông thường có 3 nhân tố chính: kẻ tấn công, mạng khuếch đại và hệ thống nạn nhân.

Trong Smuft attack, kẻ tấn công sẽ gửi các gói tin ICMP echo đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các gói tin ICMP này có địa chỉ IP của chính nạn nhân. Khi các gói tin này đến được địa chỉ broadcast của mạng khuếch đại, các máy tính trong mạng khuếch đại sẽ tưởng rằng máy tính nạn nhân đã gửi các gói tin này, và chúng sẽ đồng loạt gửi trả lại hệ thống nạn nhân các gói ICMP reply. Nạn nhân sẽ không chịu nổi một khối lượng khổng lồ các gói tin này và nhanh chóng bị ngừng hoạt động, crash hoặc reboot.

Điểm khó chịu của kiểu tấn công smuft là kẻ tấn công có thể sử dụng kết nối băng thông thấp để tiêu diệt nạn nhân có băng thông cao hơn. Bởi vì, chỉ cần gửi một lượng nhỏ các gói tin ICMP đi thì hệ thống mạng khuếch đại sẽ khuếch đại các gói tin này lên rất nhiều lần. Tỉ lệ khuếch đại phụ thuộc vào số máy tính có trong mạng khuếch đại. Nhiệm vụ của các hacker là cố chiếm được thật nhiều hệ thống mạng hoặc router cho phép chuyển trực tiếp các gói tin đến địa chỉ broadcast không qua bộ phận lọc địa chỉ nguồn ở các đầu ra của gói tin. Có được hệ thống này, kẻ tấn công sẽ dễ dàng phát động tấn công kiểu Smuft.

#### 2.1.2.2. Tấn công kiểu Fraggle



**Hình 2.9 Sơ đồ tấn công kiểu Fraggle**

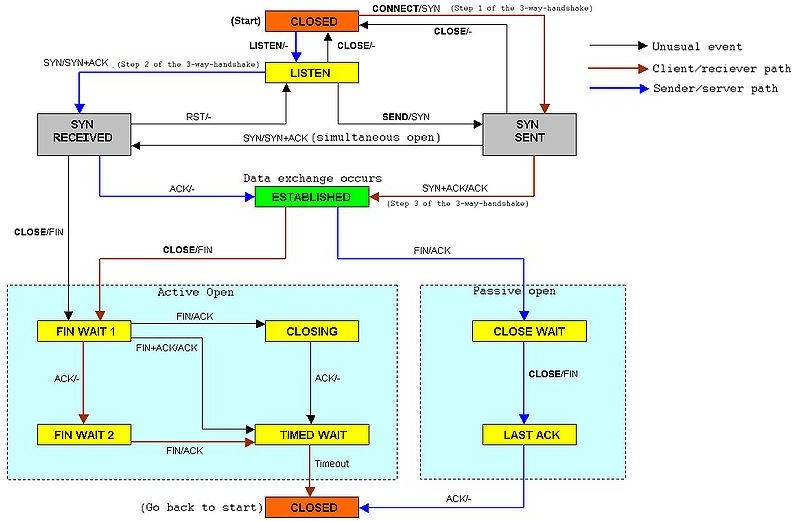
Tương tự như tấn công kiểu Smuft, nhưng thay vì dùng gói tin ICMP, kiểu tấn công này sử dụng các gói tin UDP.

## 2.2. Tấn công làm cạn kiệt tài nguyên (Resoure Deleption)

* 1. **Tấn công làm cạn kiệt tài nguyên (Resoure Deleption): Tấn công tràn SYN:**

Để nghiên cứu loại tấn công này, trước tiên phải nắm được các kiến thức cơ bản về (**1**) giao thức TCP, (**2**) quá trình thiết lập kết nối trong TCP.

1. **Giao thức điều khiển truyền vận** (Transmission Control Protocol- TCP): là một trong các giao thức cốt lõi trong bộ giao thức TCP/IP. Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các kết nối với nhau, mà qua đó chúng có thể trao đổi dữ liệu. Giao thức này đảm bảo chuyển giao dữ liệu một cách tin cậy và theo đúng thứ tự. TCP còn phân biệt giữa dữ liệu của nhiều ứng dụng (chẳng hạn, dịch vụ web và dịch vụ thư điện tử) đồng thời cùng chạy trên một máy chủ.



**Hình 2.10 Sơ đồ hoạt động của TCP**

Quá trình hoạt động của TCP bao gồm 3 pha:

* + - * + Thiết lập kết nối
        + Truyền dữ liệu
        + Kết thúc kết nối

Trước khi mô tả chi tiết các pha này, ta cần lưu ý các trạng thái khác nhau của một socket:

**- CLOSED:** Trạng thái ban đầu, không có kết nối TCP nào đang diễn ra. Đây là trạng thái mặc định khi một socket được tạo ra và chưa được mở kết nối.

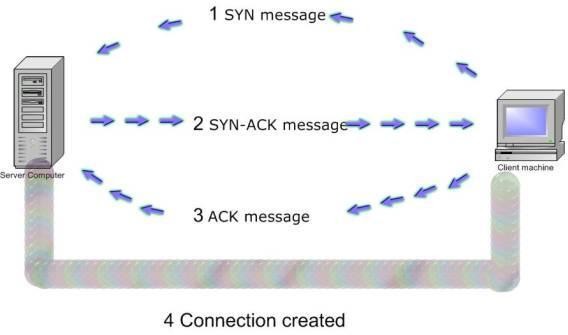
* **LISTEN:** Đang đợi yêu cầu kết nối từ một TCP và cổng bất kỳ ở xa (trạng thái này thường do các TCP server đặt).
* **SYN-SENT:** Đang đợi TCP ở xa gửi một gói tin TCP với các cờ SYN và ACK được bật (trạng thái này thường do các TCP client đặt).
* **SYN- RECEIVED:** Đang đợi TCP ở xa gửi lại một tin báo nhận sau khi đã gửi cho TCP ở xa đó một tin báo nhận kết nối (connection acknowledgment), trạng thái này thường do TCP server đặt.
* **ESTABLISHED:** Cổng đã sẵn sàng gửi/nhận dữ liệu với TCP ở xa ( trạng thái này đặt bởi TCP server và client).
* **FIN-WAIT-1:** Trạng thái này xảy ra khi một đầu (client hoặc server) muốn kết thúc kết nối và gửi gói FIN. Đang đợi nhận ACK cho gói FIN từ đầu kia hoặc đồng thời nhận được gói FIN từ đầu kia.
* **FIN-WAIT-2:** Đã nhận được ACK cho gói FIN của mình và đang chờ nhận gói FIN từ TCP ở xa. Điều này có nghĩa là kết nối của một phía đã đóng nhưng đợi phía kia hoàn tất việc gửi dữ liệu và đóng kết nối.
* **CLOSE-WAIT:** Trạng thái này xảy ra khi một đầu nhận được gói FIN từ đầu kia và gửi lại ACK. Đang chờ ứng dụng tại đầu nhận quyết định đóng kết nối hoàn toàn bằng cách gửi gói FIN.
* **CLOSING:** Trạng thái này hiếm gặp và xảy ra khi cả hai đầu của kết nối gửi gói FIN gần như đồng thời. Đang chờ nhận ACK cho gói FIN đã gửi.
* **LAST-ACK:** Trạng thái này xảy ra khi một đầu nhận được gói FIN từ đầu kia, gửi lại ACK, và gửi gói FIN của mình. Đang đợi nhận ACK cho gói FIN của mình trước khi đóng kết nối hoàn toàn.
* **TIME-WAIT:** Đang đợi qua đủ thời gian để chắc chắn là TCP ở xa đã nhận được tin báo nhận về yêu cầu kết thúc kết nối của nó.

1. **Quá trình thiết lập kết nối trong TCP:**

Để thiết lập một kết nối, TCP sử dụng một quy tắc gọi là *bắt tay ba bước* (three-way handshake). Trước khi client thử kết nối với một server, server phải đăng ký một cổng và mở cổng đó cho các kết nối, quá trình này được gọi là mở bị động. Một khi mở bị động đã được thiết lập thì một client có thể bắt đầu mở chủ động. Để thiết lập một kết nối, quy trình bắt tay ba bước xảy ra như sau:

* Client yêu cầu mở cổng dịch vụ bằng cách gửi gói tin SYN (gói tin TCP) tới server, trong gói tin này, tham số ***sequence number*** được gán cho một giá trị ngẫu nhiên X.
* Server hồi đáp bằng cách gửi lại phía client bản tin SYN-ACK, trong gói tin này, tham số ***acknowledgment number*** được gán giá trị bằng X+1, tham số ***sequence number*** được gán ngẫu nhiên một giá trị Y.
* Để hoàn tất quá trình *bắt tay ba bước*, client tiếp tục gửi tới server bản tin ACK, trong bản tin này, tham số ***sequence number*** được gán cho giá trị bằng X+1 còn tham số acknowledgment number được gán giá trị bằng Y+1.

Tại thời điểm này, cả client và server đều được xác nhận rằng, một kết nối đã được thiết lập.



**Hình 2.11 Sơ đồ quá trình “bắt tay 3 bước”**

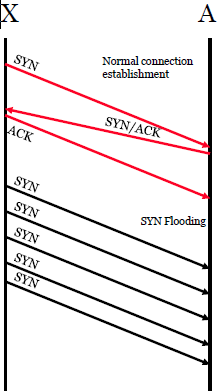
Trong điều kiện bình thường, gói tin SYN từ một cổng cụ thể trên hệ thống A đến một cổng cụ thể trên hệ thống B trong tình trạng LISTEN. Vào thời điểm này kết nối trên hệ thống B ở tình trạng SYN\_RECEIVED. Vào giai đoạn này hệ thống B sẽ tìm cách gửi gói tin SYN/ACK về cho hệ thống A. Nếu mọi sự ổn thỏa hệ thống A sẽ gửi trả gói tin ACK, và kết nối chuyển sang tình trạng ESTABLISHED.

Dù có nhiều lúc cơ chế này chẳng có vấn đề gì, nhưng trong hệ thống có những điểm yếu cố hữu để kẻ tấn công có thể lợi dụng thực hiện tấn công DoS. Vấn đề là đa số hệ thống phân phối số lượng tài nguyên nhất định khi thiết lập kết nối tiềm tàng hoặc kết nối chưa được thiết lập hẳn (SYN\_RECEIVED). Tuy rằng một hệ thống chấp nhận hàng trăm kết nối vào một cổng cụ thể (ví dụ cổng 80), nhưng chỉ lấy khoảng một chục yêu cầu kết nối là hết sạch tài nguyên phân phối cho thiết lập kết nối.

Đây chính là điểm mà kẻ tấn công có thể lợi dụng để vô hiệu hóa hệ thống. Kẻ tấn công (hệ thống A) sẽ gửi gói tin SYN đến nạn nhân (hệ thống B) và giả mạo địa chỉ IP của hệ thống C ( hệ thống C này không tồn tại trên thực tế). Lúc đó hệ thống B sẽ xử lý như thế nào?

Hệ thống B sẽ gửi gói tin SYN/ACK đến hệ thống C. Giả sử rằng hệ thống C tồn tại, nó sẽ gửi gói tin RST (reset packet) cho hệ thống B (vì nó không khởi động kết nối). Nhưng đây là một hệ thống không có thật, chính vì thế mà hệ thống B sẽ chẳng bao giờ nhận được gói tin RST từ hệ thống C. Lúc đó, B sẽ đặt kết nối này vào hàng đợi (SYN\_RECEIVED). Do hàng đợi kết nối thường rất nhỏ nên kẻ tấn công chỉ cần gửi vài gói tin SYN thì sau khoảng 10 giây có thể vô hiệu hóa hoàn toàn một cổng!

**Khái niệm tấn công tràn SYN (SYN flood attack)**

Tấn công tràn SYN (SYN flood attack) là một dạng tấn công từ chối dịch vụ, kẻ tấn công gửi thành công các SYN request đến hệ thống đích. SYN flood là kiểu tấn công khá phổ biến. Nó làm việc nếu server định vị tài nguyên sau khi nhận SYN, nhưng trước khi nhận ACK. Kẻ tấn công làm tràn ngập hệ thống nạn nhân với các gói tin SYN. Điều này dẫn đến máy nạn nhân mất nhiều thời gian mở một số lượng lớn các phiên TCP, gửi các SYN-ACK, và đợi các đáp ứng ACK không bao giờ đến. Bộ đệm phiên giao dịch TCP của máy nạn nhân bị tràn, ngăn không cho các phiên TCP thực sự đang được mở.

**Hình 2.12 Tấn công tràn SYN**

SYN đến gửi tín hiệu kết nối trong trạng thái SYN-RECEIVED, nó có thể ở trạng thái này trong một thời gian để chờ đợi sự xác nhận kết nối của gói SYN/ACK. Vì lý do này, số các kết nối với một cổng (port) được chỉ định trong trạng thái SYN- RECEIVED bị giới hạn.

Lợi dụng cách thức hoạt động của phương thức TCP/IP, hacker bắt đầu quá trình thiết lập một kết nối TCP/IP với mục tiêu muốn tấn công mà không gửi trả gói tin ACK, khiến cho mục tiêu luôn rơi vào trạng thái chờ đợi (đợi gói tin ACK từ phía yêu cầu thiết lập kết nối) và liên tục gửi gói tin SYN/ACK để thiết lập kết nối. Một cách khác là giả mạo địa chỉ IP của gói tin yêu cầu thiết lập kết nối, và cũng như trường hợp trên, máy tính đích cũng rơi vào trạng thái chờ đợi vì các gói tin SYN/ACK không thể đi đến đích do IP đích là không có thật. Kiểu tấn công tràn SYN được các hacker áp dụng để tấn công một hệ thống mạng có băng thông lớn hơn hệ thống của hacker.

Một khi đã bị tấn công tràn SYN, hệ thống bị tấn công sẽ nhận được vô số những gói SYN gửi đến, trong khi khả năng trả lời của hệ thống lại có hạn, và hệ thống sẽ từ chối các truy cập hợp pháp.

## 2.3. Các biến thể của tấn công DDoS

### 2.3.1. Tấn công kiểu Flash DDoS

Để thực hiện tấn công DdoS, hacker cần phải nắm quyền điều khiển càng nhiều máy tính càng tốt. Sau đó, hacker sẽ trực tiếp phát động tấn công hàng loạt từ xa thông qua một kênh điều khiển. Với quy mô mạng lưới tấn công bao gồm hàng trăm ngàn máy tính, kiểu tấn công này có thể đánh gục bất cứ hệ thống nào. Kết hợp với khả năng giả mạo địa chỉ IP , kiểu tấn công này cũng khá khó để lần ra dấu vết của kẻ tấn công. Tuy nhiên, DdoS vẫn có một số nhược điểm sau:

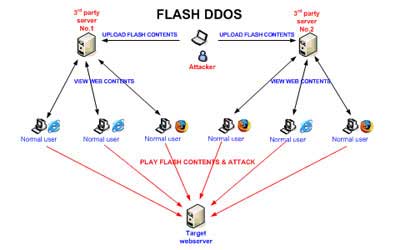
- Mạng lưới tấn công là mạng cố định và tấn công xảy ra đồng loạt nên vẫn có thể điều tra tìm được kẻ tấn công.

Phần mềm được cài lên các Agent là giống nhau có thể dùng làm bằng chứng kết tội kẻ tấn công.

-Để phá động tấn công, hacker phải trực tiếp kết nối đến mạng lưới các máy tính ma tại thời điểm tấn công, và có thể bị phát hiện.

Phía nạn nhân có thể điều chỉnh hệ thống phòng vệ để tấn ngăn chặn DdoS.

Lợi dụng tính phổ biến của Flash Player (có trong hầu hết các trình duyệt web hiện nay), các hacker đã cải tiến kiểu tấn công DdoS, cho ra đời một kiểu tấn công nguy hiểm hơn rất nhiều và không thể ngăn chặn! Đó chính là Flash DdoS.



**Hình 2.13 Sơ đồ tấn công Flast DdoS**

Hacker sẽ tải lên một trang web nào đó có nhiểu người truy xuất một file flash (thường là các web đen hoặc các trang có quảng cáo), người dùng truy xuất các website này và bằng cách nào đó, vô tình hoặc cố chủ ý, tải các file flash này về máy và được các chương trình flash thực thi. Từ đây, vô số các yêu cầu truy suất sẽ được gửi đến website mục tiêu. Mục tiêu bị tấn công từ chối dịch vụ.

Flash DDó có một số đặc tính khiến cho việc ngăn chặn và phát hiện gần như là không thể:

-Kẻ tấn công không phải nắng quyền điểu khiển và cài DdoS software vào các Agent. Thay vào đó, mọi user với một trình duyệt có thể hỗ trợ Flash player đều có thể trờ thành một công cụ tấn công.

-Số lượng các Agent tùy thuộc vào số lượng user truy xuất các website đã bị hacker “nhúng ” nội dung flash, số lượng này có thay đổi theo thời gian và hoàn toàn không thể kiểm soát.

-Không hề có quá trình gửi lệnh và nhận báo cáo giữa hacker và mạng lưới tấn công, toàn bộ lệnh tấn công đã được “nhúng ” trong nội dung flash.

-Việc tấn công diễn ra không cần có mệnh lệnh. Usẻ load nội dung flash về, chạy thì ngay lập tức máy của họ trở thành một attack Agent, liên tục gửi các request đến máy nạn nhân.

**2.3.2. Tấn công kiểu DRDoS**

Tấn công từ chối dịch vụ phản xạ phân tán (Distributed Reflection Denial of Service- DRDoS) là kiểu tấn công nguy hiểm nhất trong họ DdoS. Nếu được thực hiện bởi 1 hacker có trình độ và kinh nghiệm thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới trong phút chốc.

Mục tiêu của DroS là chiếm toàn bộ băng thông của hệ thống nạn nhân, tức làm nghẽn hoàn toàn đường kết nối từ máy chủ vào trong internet và làm tiêu hao tài nguyên máy chủ. Trong suốt quá trình máy bị tấn công DRDoS, không một khách nào có thể kết nối được vào máy chủ đó. Tất cả các dịch vụ trên nền TCP/IP như DNS, HTTP, FTP… đều bị vô hiệu hóa.

Về cơ bản, DRDoS là sự kết hợp giữa 2 kiểu DoS và DDoS. Nó vừa có kiểu tấn công tràn SYN với một máy tính đơn lẻ của DoS, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như DDoS. Để thực hiện DRDoS, kẻ tấn công thực hiện bằng cách giả mạo địa chỉ IP của mục tiêu rồi gửi yêu cầu SYN đến các server có tốc độ đường truyền lớn như Google, Yahoo… để các server này gửi các gói tin SYN/ACK đến mục tiêu. Các server lớn với đường truyền mạnh đó đã vô tình đóng vai trò zombie cho kẻ tấn công như trong DDoS.

Quá trình gửi cứ lặp lại liên tục với nhiều địa chỉ IP giả từ kẻ tấn công, với nhiều server lớn tham gia nên server mục tiêu nhanh chóng bị quá tải, băng thông bị chiếm dụng bởi các server lớn. Tính “nghệ thuật” trong cách tấn công này là chỉ cần có một máy tính với tốc độ kết nối trung bình (256Kbps), một hacker lành nghề có thể hạ gục bất cứ một server nào chỉ trong giây lát mà không cần chiếm đoạt thêm một máy nào làm phương tiện để thực hiện tấn công!

### 2.3.3. Tấn công DDoS trên điện thoại di động

Tương tự với DDoS trên web, phương thức tấn công DDoS trên điện thoại di động cũng khiến các thuê bao liên tục phải nhận các cuộc gọi đến. Các thuê bao hợp lệ khác không thể gọi tới thuê bao bị tấn công vì máy luôn bận. Thuê bao nạn nhân cũng khó có thể thực hiện các cuộc gọi đi vì luôn có điện thoại gọi đến. …

Ngoài ra, sự phổ biến của các thiết bị truy cập mạng cầm tay, như điện thoại thông minh (Smart Phone), máy tính bảng … cũng mở đường cho nhiều hình thức tấn công mới. Để tiến hành tấn công, Hacker thường tạo ra các Botnet di động. Botnet di động thực sự mang đến một lợi thế đáng kể so với những Botnet truyền thống. Điện thoại thông minh hiếm khi bị tắt nguồn, khiến Botnet đáng tin cậy hơn vì hầu hết các truy cập luôn sẵn sàng đợi chỉ dẫn mới. Tác vụ thông thường mà các botnet thực hiện bao gồm gửi thư rác hàng loạt, tấn công DDos và gián điệp thông tin cá nhân hàng loạt. Tất cả hoạt động này không đòi hỏi hiệu suất cao được thực hiện dễ dàng trên điện thoại thông minh.

Phần mềm độc hại Obad là phát hiện đáng chú ý nhất trong lĩnh vực di động đang được phân tán bởi nhiều phương pháp, trong đó có một botnet được thiết lập sẵn. Điện thông minh nền tảng Android bị lây nhiễm Trojan SMS.AndroidOs.Opfake.a sẽ biến thành một nơi nhân bản, gửi các tin nhắn văn bản có chứa liên kết độc hại đến tất cả số điện thoại có trong thiết bị của nạn nhân. Điều này giống với các tấn công trên máy tính cá nhân và là một dịch vụ phổ biến được cung cấp bởi những chương trình chỉ huy Botnet (botnet-herder). Phần mềm độc hại này có lẽ là phần mềm linh hoạt nhất được tìm thấy cho đến nay, gồm tổng cộng ba lỗ hổng: một backdoor, tin nhắn Trojan SMS, khả năng bot và nhiều chức năng khác.

## 2.4. Một số công cụ tấn công DDoS phổ biến hiện nay

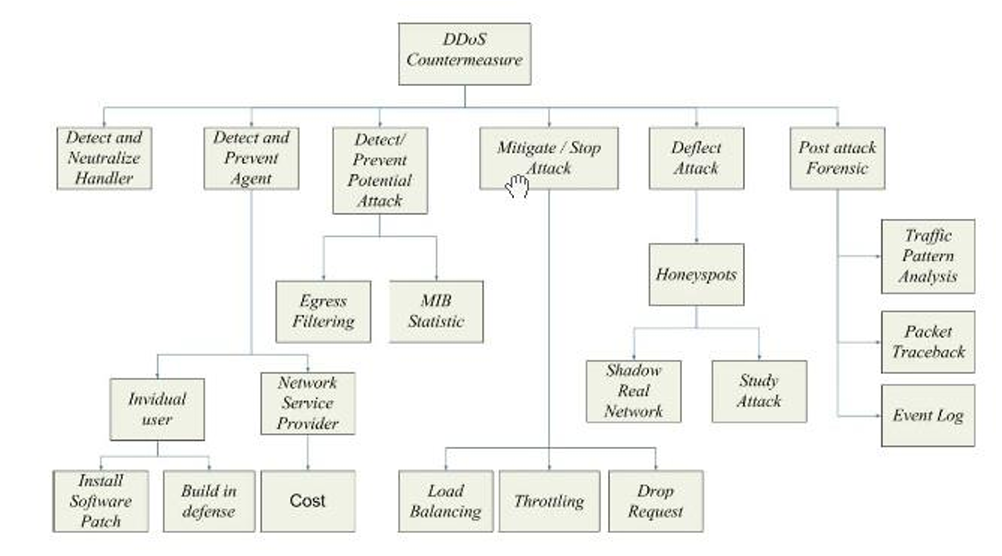
## 2.5. Phòng chống tấn công DdoS

Như đã trình bày, tấn công DDOS có nhiều dạng, kiểu và nhiều cách phân chia. Ngoài ra, các cuộc tấn công DDOS cũng có thể phân theo quy mô. Từ những cách phân chia này, tương ứng sẽ có các phương pháp phòng chống hữu hiệu, tốn ít tài nguyên nhất. Tuy nhiên, trên thực tế, ta không thể đoán trước được các cuộc tấn công DDOS như thế nào nhằm vào hệ thống của ta. Do đó, trên cơ sở em xin đưa ra giải pháp chung nhất có thể chống lại nhiều kiểu tấn công DDOS. Giair pháp tổng về phòng, chống DDOS được chia thành 3 giai đoạn chính:

(1) Giai đoạn ngăn ngừa: Tối thiểu hoá lượng Agent, tìm và vô hiệu hoá các Handle.

(2) 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.

(3) Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm.



**Hình 2.14 Phòng chống tấn công DdoS**

### 2.5.1. Phát hiện tấn công

#### **2.5.1.1. Phát hiện và ngăn chặn** Agent

#### Từ phía người sử dung: Phương pháp hữu hiệu để ngăn ngừa các cuộc tấn công DDOS là từng người sử dụng Internet sẽ tự đề phòng không để bị lợi dụng tấn công các hệ thống khác. Như vậy, ý thức và kỹ thuật phòng chống phải được phổ biến rộng rãi cho người sử dụng Internet. Các cuộc tấn công DDOS sẽ khó hình thành hoặc hạn chế nếu không có người sử dụng nào bị lợi dụng để trở thành Agent. Người sử dụng phải liên tục tiến hành bảo vệ các thiết bị truy cập mạng của mình. Tử kiểm tra sự hiện diện của Agent trên thiết bị. Đây là điểu khó đối với những người sử dụng thông thường.

#### Một số giải pháp:

#### Đối với nhà cung cấp thiết bị có thể tích hợp khả năng ngăn ngừa tấn công thông qua phần mềm và phần cứng của từng hệ thống cung cấp cho người sử dụng.

#### Đối với người sử dụng Internet, thực hiện cài đặt và cập nhật liên tục các phần mềm bảo mật, chống virus như antivirus, anti\_trojan, backkhoa antivirus … và server patch của hệ điều hành.

#### Đối với nhà cung cấp dịch vụ mạng: Thay đổi cách tính tiền dịch vụ truy cập theo dung lượng tăng cường ý thức cho người sử dụng, giúp người sử dụng tự nâng cao kiến thức không để bị lợi dụng trở thành các Agent.

#### 2.5.1.2. Phát hiện và vô hiệu hóa các Handler

Trong một cuộc tấn công mạng nói chung và tấn công DDOS nói riêng, Handler có vai trò vô cùng quan trọng, nếu có thể phát hiện và vô hiệu hóa Handler sẽ ngăn ngừa, hạn chế được các cuộc tấn công DDOS. Bằng cách theo dõi các giao tiếp giữa Handler và Client hoặc Handler và Agent có thể phát hiện ra vị trí của Handler. Do một Handler quản lý nhiều Agent, nên tiêu diệt được một Handler cũng có thể loại bỏ một lượng đáng kể các Agent.

#### 2.5.1.3. Phát hiện dấu hiệu của một cuộc tấn công DdoS

Có nhiều kỹ thuật được áp dụng để phát hiện một cuộc tấn công DDOS. Phổ biến có 02 kỹ thuật sau: Agress Filtering: Kỹ thuật này kiểm tra xem một gói tin 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 gói tin 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 IP sẽ không tồn tại. Việc kiểm tra này có thể thực hiện bằng cách lưu các địa chỉ IP thường xuyên truy cập vào server trong một cơ sở dữ liệu. Khi có một cuộc tấn công xảy ra ta sẽ tiến hành so sánh các địa chỉ IP trong thời gian tấn công với các IP trong cơ sở dữ liệu (IP Address Database) để phát hiện ra các IP mới. Về cơ bản, cơ chế yêu cầu phải xây dựng quy tắc để phân biệt các IP hợp lệ với các IP tấn công. Công việc này sẽ được tiến hành bằng cách kiểm tra các gói tin đến với các IP trong IAD.

Như vậy các địa chỉ IP thuộc tập Fc sẽ được lưu vào IAD

Khi lưu lượng mạng ở mức bình thường, tính toán các địa chỉ IP trong các gói tin đến và cập nhật vào IAD. Tiến hành xóa các địa chỉ IP hết hạn trong IAD với mục đích không làm IAD quá lớn. Việc xóa các địa chỉ IP có thể đặt trong thời gian là 2 tuần. Các địa chỉ IP trong IAD đều gồm 2 trường. Đó là IP address và timestamp. Khi thêm một địa chỉ IP vào trong IAD bắt đầu tính thời gian trong trường timestamp. Và sau một khoảng thời gian (2 tuần) địa chỉ này sẽ bị xóa khỏi IAD.

**IP spoofing**: Việc chống giả mạo địa chỉ được thực hiện khá dễ dàng, tuy nhiên phải tiến hành đồng bộ. Nếu tất các subnet trên Internet đều tiến hành giám sát các gói tin ra khỏi mạng của mình với địa chỉ nguồn hợp lệ thì không có các gói tin giả mạo địa chỉ nào có thể truyền trên Internet được. Do đó, các nhà quản trị mạng phải tự giác thực hiện Egress Filtering ở mạng do mình quản lý.

**Broadcast Amplification**: Tương tự IP spoofing lợi dụng toàn bộ subnet để làm “ngập lụt” nạn nhân. Do đó, 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 để không nhận và chuyển tiếp các gói tin broadcast. Trong trường hợp này có thể áp dụng Thuật toán Adaptive Threshold (ngưỡng giới hạn khả năng đáp ứng). Thuật toán này nói chung khá đơn giản và dễ hiểu. Thuật toán phát hiện sự không bình thường dựa trên vi phạm một ngưỡng khả năng đáp ứng của lưu lượng mạng trong thời gian gần. Thuật toán đặc biệt có khả năng phát hiện cao nhất khi kẻ tấn công tiến hành một cuôc tấn công TCP SYN. Thuật toán tin tưởng vào việc kiểm tra phép đo lưu lượng có vượt qua một ngưỡng giới hạn cụ thể hay không. Nếu vượt qua, chứng tỏ đã có một cuộc tấn công xảy ra.

**MIB statistics**: Trong việc quản lý thông tin cơ bản – 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, thống kê các gói tin UDP, ICMP, TCP sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo “quỹ thời gian vàng” cho xử lý tình huống. Trường hợp này có thể sử dụng Thuật toán CUSUM (tổng tích lũy).

Thuật toán tổng tích lũy dựa trên giá trị trung bình của một quá trình xử lý thống kê. Sự phát hiện điểm thay đổi cần phải theo dõi trong các khoảng thời gian. Một công thức được xây dựng để theo dõi sự thay đổi này, khi vượt qua một ngưỡng giới hạn chứng tỏ đã xảy ra một cuộc tấn công. Trong giai đoạn này, tiến hành phân tích thống kê các lưu lượng đến giữa hai khoảng thời gian là Δn. Với kỹ thuật phát hiện tấn công này, một bảng băm sẽ được sử dụng để ghi lại các địa chỉ IP xuất hiện giữa hai khoảng thời gian. Trong bảng băm nay sẽ gồm 2 trường: IP address và timestamp. So sánh các trường này với các trường trong IAD để có thể tính toán có bao nhiêu địa chỉ IP mới đã xuất hiện trong các khe thời gian. Phân tích các địa chỉ IP mới này cho biết khi nào cuộc tấn công DDos xảy ra.

Trước tiên lựa chọn các địa chỉ IP trong mỗi khoảng thời gian Δn (n=1,2,3,4…). Sau đó gán Δ1=Δ2=….=Δn.

Gọi Tn là tập các địa chỉ IP vừa thiết lập và Dn là các địa chỉ IP trong IAD tại thời điểm Δn. |Tn-Tn∩Dn| sẽ là tập các địa chỉ IP mới trong khoảng thời gian Δn.

Ta có Xn=|Tn-T∩Dn|/Tn: tỷ lệ phần trăm địa chỉ IP mới trên tổng số các địa chỉ IP trong khoảng thời gian Δn.

Đặt Z={Zn,n=1,2,3…} sao cho Zn=Xn-β . Với a=α- β

a là giá trị trung bình của {Zn} trong quá trình lưu lượng mạng bình thường

α là giá trị trung bình của {Xn} trong quá trình lưu lượng bình thường Do đó, khi lưu lượng mạng bình thường tất cả các giá trị của Zn đều âm

Khi có một cuộc tấn công xảy ra, giá trị của Zn sẽ đột nhiên tăng và có giá trị dương. Lúc này h+a>0, h chính là giá trị trung bình tăng nhỏ nhất trong suốt cuộc tấn công.

Thuật toán CUSUM sẽ tiến hành tổng hợp Zn và được thiết lập bởi công thức sau:

yn=(yn-1 + Zn)+ và y0=0

Với x+ = x nếu x > 0 và x+ = 0 nếu x <= 0

Trong đó n >= k. Trường hợp không bị tấn công giá trị của yn-1+Zn âm.

Hàm quyết định có cuộc tấn công hay không được định nghĩa như sau: dN(yn) = 0 nếu yn<= N và dN(yn) = 1 nếu yn > N

Ở đây N là ngưỡng giới hạn cho sự phát hiện tấn công. dN(yn) là hàm quyết định phát hiện trong thời gian Δn.

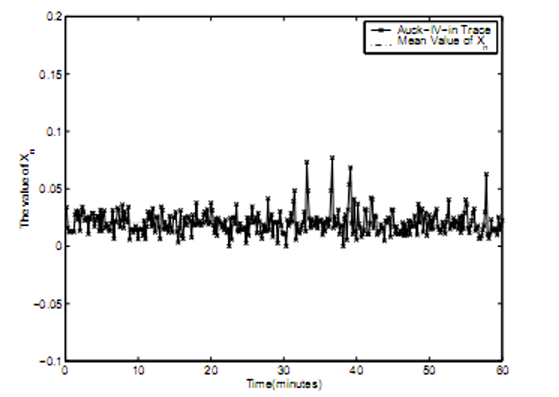
Ta có công thức: ρ N=(τ N - m)+/N (1)

ρ N -> γ = 1 h− | a | (2)

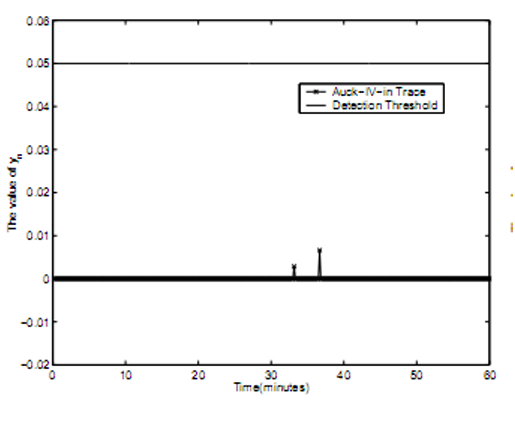
Ở đây τ N là thời gian phát hiện, ρ N là điểm thay đổi. Trong đó m là thời điểm bắt đầu cuộc tấn công. Để thuật toán CUSUM tối ưu nhất, chọn h=2|a|. Theo nghiên cứu thuật toán CUSUM có thể chọn |a|=0.05

#### Trong công thức (1) chọn vị trí nhỏ nhất khi cuộc tấn công bắt đầu. Do vậy τ N=m+1. 2.5.1.4. Làm suy giảm, chuyển hướng cuộc tấn công

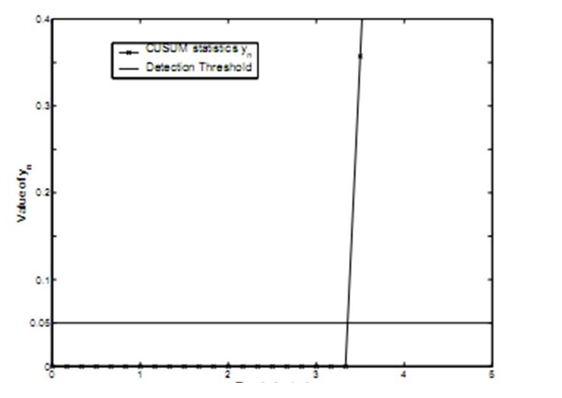
Vì vậy từ (1) và (2) hoàn toàn có thể tính được giá trị của ngưỡng N. Lược đồ minh họa thí nghiệm chạy thuật toán khi phát hiện cuộc tấn công



**Hình 2.15 Tỷ lệ phần trăm new IP với Δn=10s**

****

**Hình 2.16 Thuật toán CUSUM khi lưu lượng mạng bình thường**

****

**Hình 2.17 Lưu lượng mạng đột biến**

### 2.5.2. Giải pháp phòng chống DDoS

#### 2.5.2.1 Tình hình liên quan tới DDoS ở Việt Nam:

Tấn công từ chối dịch vụ (DDoS) và các mạng máy tính ma (Botnet) đang có xu hướng tăng nhanh trên thế giới cũng như tại Việt Nam trong vài năm trở lại đây. Điều này đang đặt ra cho các cơ quan chức năng yêu cầu cấp bách về việc đề ra các giải pháp phối hợp phòng chống botnet và DDoS tại Việt Nam. Dưới đây là một số nội dung chính trong Tham luận trình bày tại hội thảo “Ngày ATTT Việt Nam” tại Tp. HCM (tháng 11/2013) của TS. Vũ Quốc Khánh – Giám đốc Trung tâm ứng cứu khẩn cấp máy tính Việt Nam VNCERT.

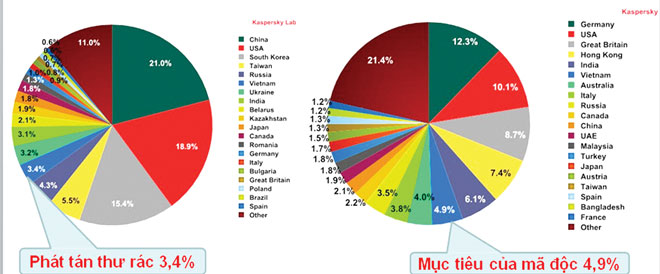
**Tình hình ATTT và botnet tại Việt Nam**

Sự phát triển của Botnet

Theo số liệu tổng hợp của VNCERT, trong năm 2013 các mạng botnet vẫn hoạt động rất mạnh mẽ ở Việt Nam và chúng trở nên ngày càng nguy hiểm và khó kiểm soát hơn. Cụ thể, theo thông báo của Kaspersky vào tháng 9/2013, ở Việt Nam, mạng Ramnit có 119.439 bot (con số này đưa Việt Nam trở thành quốc gia đứng số 1 thế giới – ngang bằng với Ấn Độ); Mạng StlBot, dclj (cửa hậu) có 10.651 bot (chiếm 90% của thế giới)….

Trong hai năm (2012-2013) theo dõi và ứng cứu các sự cố máy tính tại Việt Nam, VNCERT đã ghi nhận: Mạng botnet Zeus có 14.075 địa chỉ IP Việt Nam; Mạng botnet Sality, Downadup, Trafficconverter có 113.273 địa chỉ IP Việt Nam; Trong đó, mạng Sality có 20 địa chỉ IP từ các cơ quan nhà nước; mạng Downadup có 154 địa chỉ IP từ các cơ quan nhà nước.

Mạng bRobot cũng đã tấn công 2.309 website và cài mã độc lên 6978 trang web. Mạng botnet razer đã tham gia tấn công một số doanh nghiệp hosting ở Việt Nam. VNCERT đã cảnh báo và hỗ trợ các cơ quan, đơn vị rà soát và bóc gỡ mã độc, nên hiện nay số lượng IP thuộc các cơ quan, tổ chức bị nhiễm mã độc hoạt động trong các mạng botnet đã giảm đi đáng kể.



**Hình 2.18 Số liệu về phát tán tin nhắn rác mã độc qua thư điện tử (tháng 8/2013)**

Theo số liệu tại Hình 1, các máy tính ở Việt Nam đang phát tán hơn 3,33 tỷ tin nhắn rác/ngày. Ít nhất khoảng 500 nghìn đến 1 triệu máy tính đang bị lây nhiễm mã độc nằm trong các mạng botnet.

Chu kỳ sống của một mạng botnet Nắm được chu kỳ hoạt động của mạng botnet để chúng ta có thể dễ dàng đối phó với chúng khi bị tấn công. Thông thường một mạng botnet có các giai đoạn như sau:

Giai đoạn 1 – thụ thai: Hình thành động cơ xây dựng mạng botnet, kiến trúc thiết kế và cách thức xây dựng mạng botnet.

Giai đoạn 2 – tuyển dụng: Lây nhiễm và phát tán mã độc để xây dựng mạng botnet.

Giai đoạn 3 – tương tác: tương tác giữa máy chủ và botnet, giữa botnet với các máy chủ phân giải và máy chủ khác để tìm kiếm thông tin.

Giai đoạn 4 – tiếp thị: Tìm kiếm khách hàng để bán dịch vụ tấn công, trong đó lợi ích kinh tế là một trong những mục tiêu hàng đầu.

Giai đoạn 5 – tấn công: thực hiện các cuộc tấn công như DDoS, Spam, Phising, Click Fraund.

Mạng lưới gián điệp mạng APT

Phương pháp tấn công mạng APT tuy đã xuất hiện từ lâu, nhưng gần đây mới được nhiều chuyên gia ATTT nhắc đến, hình thức tấn công này không chỉ nhằm mục đích phá hoại mà còn lấy trộm thông tin. Chúng sử dụng kết hợp nhiều kỹ thuật để tránh sự phát hiện của hệ thống bảo vệ mạng nhằm duy trì sự tồn tại càng lâu càng tốt. Các bước tấn công của chúng như sau:

– Phát tán: Mã độc được phát tán thông qua file đính kèm gửi vào hộp thư điện tử hoặc thông qua các đường link giả mạo gửi đến hộp thư điện tử. – Cài đặt RAT (Remove Access Trojan): mã độc xâm nhập vào máy khi người dùng chạy các file đính kèm thư điện tử hoặc người dùng sử dụng các đường link độc hại và cài mã độc.

– Kiểm soát RAT: các mã độc RAT này được kết nối với các máy chủ điều khiển để nhận lệnh tấn công đánh cắp dữ liệu.

– Thu thập thông tin: sử dụng các máy đã bị nhiễm mã độc làm bàn đạp dò quét mạng nội bộ và tiếp tục lây nhiễm.

Quá trình tấn công APT có thể diễn ra âm thầm trong một thời gian dài (có thể trong vài năm) mà đối tượng bị tấn công không hay biết, điều này là đặc biệt nguy hiểm, bởi dữ liệu quan trọng của người dùng có thể bị lấy cắp bất cứ lúc nào và họ cũng không biết dữ liệu đã bị mất.

#### 2.5.2.2 Giải pháp phòng chống đang được thực hiện

**Bóc gỡ mã độc/botnet và phòng chống tấn công DdoS**

Giải pháp phát hiện và bóc gỡ botnet

Hiện nay, ở Việt Nam chỉ có thể phát hiện và cảnh báo botnet dựa trên các báo cáo nhận được trong giai đoạn 4, 5 (trong chu kỳ một mạng botnet) từ các tổ chức và nạn nhân bị tấn công. Giải pháp này tuy có ưu điểm là chưa cần đầu tư lớn, chi phí vận hành thấp, nhưng không chủ động phát hiện được sớm và chỉ thu được thông tin khi mạng botnet bắt đầu thực hiện tấn công mới. Để làm tốt công việc bóc gỡ botnet thì các cơ quan, đơn vị cần có sự phối hợp kịp thời, phải chủ động xây dựng các giải pháp và có kế hoạch phòng chống cụ thể bao gồm: Tiến hành ngăn chặn việc hình thành mạng botnet (tác động vào giai đoạn 1); Dùng các biện pháp kỹ thuật để hạn chế sự lây lan của mạng botnet (tác động vào giai đoạn 2); Lên phương án và giải pháp kỹ thuật để theo dõi và sớm phát hiện ra các mạng botnet mới hình thành (tác động vào giai đoạn 3); Ngăn chặn việc mua bán trên thị trường mã độc, botnet hoạt động tại Việt Nam (tác động vào giai đoạn 4); Nhanh chóng phản ứng với các cuộc tấn công, thu thập thông tin về mạng botnet (tác động vào giai đoạn 5).

**Quy trình phòng chống tấn công DdoS**

VNCERT đã xây dựng quy trình phòng chống DDoS nhằm giúp các cơ quan, đơn vị ứng phó kịp thời với các dạng tấn công này.

– Bước 1, khi phát hiện sự cố, các tổ chức, người dùng và ISP cần báo ngay với VNCERT (ngay cả khi sự cố có thể khắc phục được) để theo dõi tổng hợp và kịp thời ngăn chặn sự bùng phát của sự cố.

– Bước 2, cơ quan điều phối kết hợp với các cơ quan chức năng, các ISP, người dùng nhằm thu thập các Log-file để tìm nguồn gốc tấn công. Sau đó, tiến hành phân tích Log-file, tìm ra các máy chủ điều khiển, phát tán mã độc và xác định cơ chế tấn công.

– Bước 3, quá trình theo dõi botnet được Cơ quan điều phối phối hợp với các cơ quan chức năng theo dõi các hoạt động của các máy chủ điều khiển tấn công, máy chủ phát tán mã độc để xác định vị trí, quy mô của các bot vận tải bị điều khiển tham gia tấn công. Sau đó, lấy mẫu các bot vận tải để đánh giá, xác định khả năng nguy cơ phát triển tiềm ẩn của sự cố.

Bước tiếp theo là ngăn chặn tấn công và bóc gỡ các máy chủ điều khiển ở quy mô quốc gia và quốc tế, theo dõi kết quả. Các tổ chức có nguy cơ bị tấn công phải thường xuyên theo dõi, giám sát hệ thống 24/7 để nắm bắt diễn biến và kịp thời báo cáo về cơ quan điều phối.

**Giải pháp ngăn chặn DDOS của VNCERT:**

Nhằm ngăn chặn hiệu quả các tấn công DDoS, VNCERT đã đưa ra những giải pháp sau:

– Các tổ chức, đơn vị cần phải chuẩn bị sẵn các phương án, kịch bản phản ứng trong mọi tình huống diễn ra. Để làm các công việc này, cần phải xác định được yêu cầu về tính sẵn sàng của hệ thống; đánh giá năng lực chống đỡ của hệ thống; nhanh chóng phân loại DDoS ngay từ các dấu hiệu đầu tiên; xây dựng kịch bản phản ứng khi mức tấn công vượt quá năng lực hệ thống (Dừng dịch vụ, thuê dịch vụ chống DDoS, thuê thêm đường truyền…).

– Chuẩn bị sẵn các đầu mối liên lạc nhận tư vấn từ VNCERT, mạng điều phối. Các tổ chức cần có biện pháp phản ứng sớm từ khi phát hiện dấu hiệu ban đầu. Qua thực tế cho thấy, việc chậm chễ trong phản ứng khi có dấu hiệu tấn công của các đơn vị là một nguyên nhân chính để thời gian tấn công kéo dài.

– Thông báo sự cố nhanh: Nhiều tổ chức chỉ thông báo cho cơ quan chức năng khi không tự chống đỡ được tấn công mạng. Việc này làm chậm quá trình ngăn chặn tấn công. Các cơ quan chức năng cần nhanh chóng nắm đuợc thông tin để tìm kiếm các máy chủ điều khiển. Việc chủ động chia sẻ thông tin từ các đơn vị là yếu tố quan trọng để nhận được sự hỗ trợ sớm và đồng bộ từ các cơ quan, tổ chức liên quan.

– Hành động phối hợp đồng thời: Các đơn vị điều phối, tham gia ứng cứu sự cố, đặc biệt là các ISP cần thực hiện ngăn chặn đồng loạt, trong thời gian ngắn nhất để tin tặc không đủ thời gian điều khiển mạng botnet thay đổi sang dạng mới.

Trong thời gian tới, để phát huy một cách có hiệu quả các phương án phòng chống tấn công mạng, các cơ quan, đơn vị cần phải bồi dưỡng nâng cao nhận thức cho người dùng về kiến thức an toàn thông tin; tổ chức tập huấn kỹ thuật về an toàn thông tin; tổ chức hội thảo chuyên đề sâu về một số lĩnh vực trong công tác đảm bảo an toàn thông tin; tổ chức diễn tập mạng lưới (cấp quốc gia, cấp Bộ, ngành, tỉnh, thành phố); tăng cường hợp tác với các tổ chức, doanh nghiệp an toàn thông tin trong và ngoài nước; tăng cường biện pháp điều phối chống malware và botnet. Bên cạnh đó, cần có chế tài mạnh và thanh, kiểm tra việc thực thi. Với các giải pháp này được triển khai đồng bộ, chúng ta sẽ ngăn chặn hiệu quả các dạng tấn công nhằm vào hệ thống công nghệ thông tin của các tổ chức, đơn vị.

# CHƯƠNG 3: TRIỂN KHAI THỰC NGHIỆM TẤN CÔNG DDoS

## 3.1. Kịch bản 1: Tấn công UDP Flood

#### 3.1.1. Mục tiêu

* Tìm hiểu cách thức hoạt động của một cuộc tấn công UDP Flood
* Đánh giá hiệu suất và khả năng làm việc của hệ thống
* Kiểm tra khả năng phát hiện và phản ứng của hệ thống

#### 3.1.2. Tiến hành

**3.1.2.1 Các công cụ cần thiết**

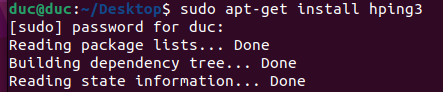
* Máy tính tấn công: máy ảo ubuntu, công cụ ‘hping3’ hoặc ‘nping’ từ gói nmap
* Máy tính mục tiêu: máy ảo ubuntu
* Phần mềm bắt gói tin wireshark

##### 3.1.2.2 Xác định mục tiêu

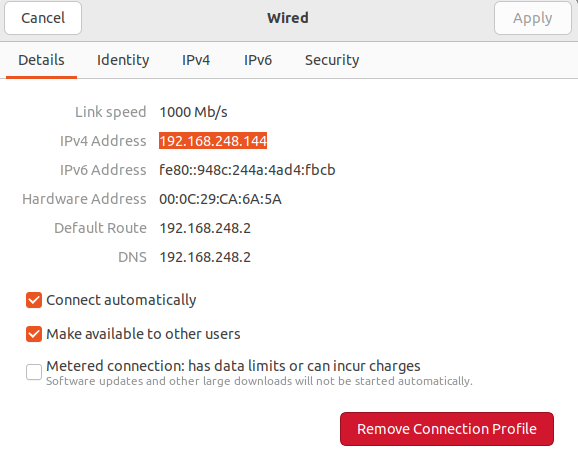
* Địa chỉ IP của mục tiêu muốn tấn công
* Cổng mục tiêu: xác định cổng UDP muốn gửi gói tên đến, cổng 80(HTTP)

##### 3.1.2.3 Cấu hình và thực hiện tấn công

* - Cài đặt hping3:



- Xác định IP mục tiêu:



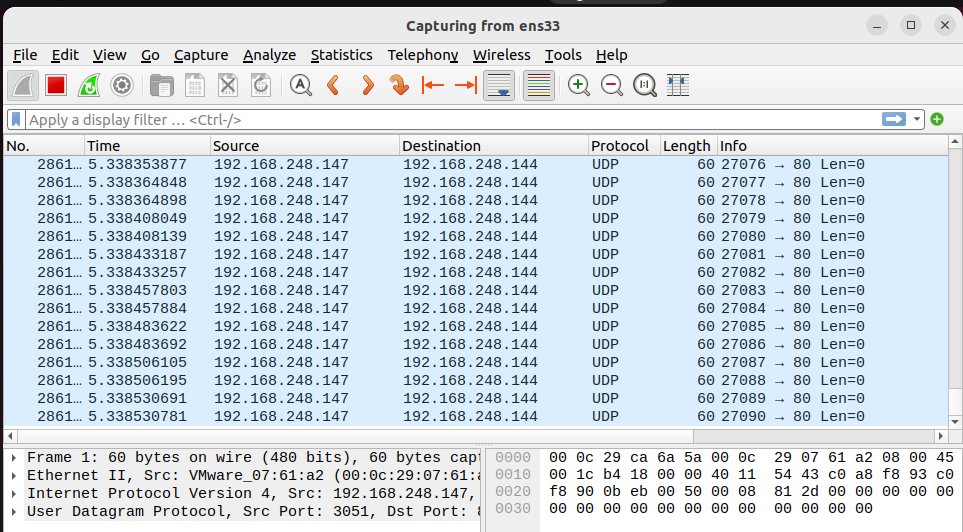
- Tình trạng máy mục tiêu trước khi bị tấn công:



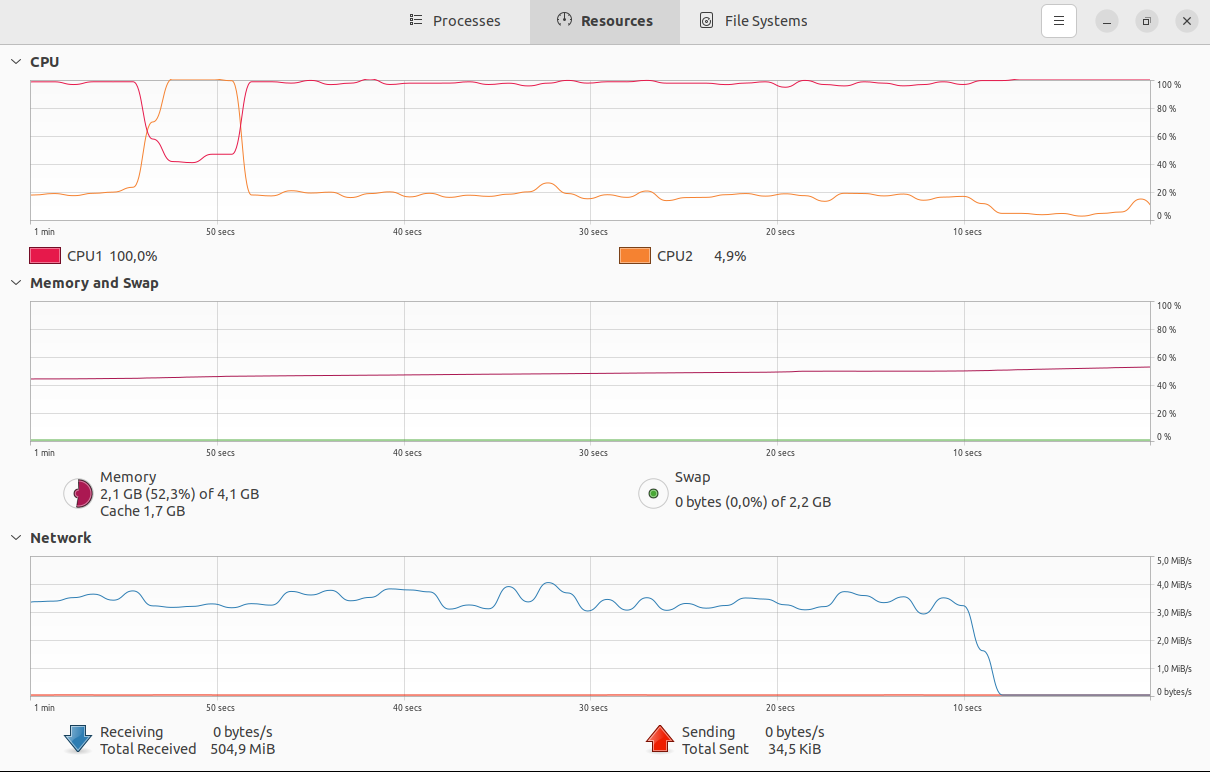
- Tấn công:



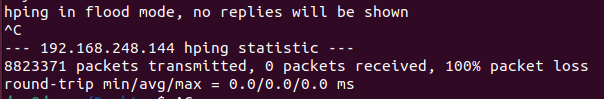
- Dùng wireshark bắt gói tin:



- Tình trạng máy sau khi bị tấn công:



**-** Dừng tấn công:





* + 1. Kết luận

Cuộc thực nghiệm tấn công UDP flood đã hoàn thành được các mục tiêu đề ra: tìm hiểu cách thức hoạt động của một cuộc tấn công UDP Flood, đánh giá hiệu suất và khả năng làm việc của hệ thống, và kiểm tra khả năng phát hiện và phản ứng của hệ thống. Dưới đây là các kết luận chi tiết từ cuộc thực nghiệm này:

* **Tìm hiểu cách thức hoạt động của một cuộc tấn công UDP Flood**

**Kết quả:**

Cuộc tấn công UDP flood hoạt động bằng cách gửi một lượng lớn các gói tin UDP đến một máy chủ hoặc hệ thống mục tiêu, nhắm vào việc làm ngập hệ thống mục tiêu với lưu lượng không mong muốn.

Các gói tin UDP này thường nhắm vào các cổng cụ thể hoặc ngẫu nhiên, tạo ra một lượng lớn lưu lượng mà hệ thống phải xử lý, dẫn đến việc làm giảm hiệu suất hoặc thậm chí làm hệ thống ngừng hoạt động.

**Quan sát:**

Tấn công UDP flood rất hiệu quả trong việc tiêu tốn tài nguyên mạng như băng thông và xử lý của CPU.

Không cần thiết phải thiết lập kết nối như TCP, do đó UDP flood dễ dàng thực hiện và khó phát hiện hơn.

* **Đánh giá hiệu suất và khả năng làm việc của hệ thống**

**Kết quả:**

Hệ thống mục tiêu cho thấy dấu hiệu suy giảm hiệu suất rõ rệt dưới tải của cuộc tấn công UDP flood. CPU và bộ nhớ đều bị sử dụng ở mức cao, dẫn đến tình trạng chậm chạp và đôi khi không thể truy cập được.

Băng thông mạng bị tiêu tốn nhanh chóng, ảnh hưởng đến các dịch vụ khác đang chạy trên cùng hệ thống mạng.

**Quan sát:**

Các hệ thống không được cấu hình để chống lại các cuộc tấn công DoS/DDoS dễ dàng bị làm ngập và ngừng hoạt động.

Hệ thống cần có khả năng mở rộng linh hoạt hoặc sử dụng các giải pháp cân bằng tải để đối phó với các cuộc tấn công như vậy.

* **Kiểm tra khả năng phát hiện và phản ứng của hệ thống**

**Kết quả:**

Hệ thống bảo mật như IDS/IPS phát hiện các lưu lượng bất thường và tạo ra các cảnh báo về tấn công UDP flood. Tuy nhiên, khả năng phản ứng của hệ thống phụ thuộc vào cấu hình và khả năng xử lý của IDS/IPS.

Tường lửa và các thiết bị mạng khác có thể được cấu hình để ngăn chặn lưu lượng không mong muốn, nhưng điều này cần phải được thiết lập một cách chính xác.

**Quan sát:**

Việc phát hiện và ngăn chặn tấn công UDP flood hiệu quả yêu cầu có sự kết hợp của nhiều lớp bảo mật.

Các công cụ giám sát mạng phải được cấu hình để phát hiện các mẫu lưu lượng không bình thường và phải có khả năng phản ứng tự động để giảm thiểu thiệt hại.

**Một số phương pháp phòng chống UDP Flood Attack**

**Cấu hình tường lửa:**

* Chặn các lưu lượng UDP không cần thiết từ các nguồn không tin cậy
* Giới hạn tốc độ các gói tin UDP vào và ra khỏi hệ thống để ngăn chặn việc làm ngập băng thông

**Sử dụng IPS/IDS**

* Triển khai các hệ thống phát hiện và ngăn chặn xâm nhập để phát hiện sớm các cuộc tấn công và tự động thực hiện các biện pháp phòng chống

**Giới hạn tốc độ băng thông**

* Áp dụng giới hạn tốc độ (rate limiting) để kiểm soát lưu lượng UDP vào hệ thống, đảm bảo rằng ngay cả khi bị tấn công, hệ thống vẫn có thể duy trì hoạt động cho các dịch vụ quan trọng

**Triển khai các dịch vụ chống DDoS**

* Sử dụng các dịch vụ chống DDoS từ các nhà cung cấp dịch vụ bảo mật để giảm thiểu tác động của các cuộc tấn công lớn và phức tạp.

**Tăng cường cấu hình hệ thống**

* Cấu hình các máy chủ và dịch vụ để tối ưu hóa hiệu suất và khả năng chịu đựng trước các cuộc tấn công.
* Sử dụng các biện pháp bảo vệ như cập nhật thường xuyên, vá lỗi bảo mật, và kiểm tra bảo mật định kỳ.

**Giám sát liên tục**

* Thực hiện giám sát liên tục lưu lượng mạng và các dịch vụ để phát hiện sớm các dấu hiệu của tấn công và phản ứng kịp thời.

**Tổng kết:**

Như vậy cuộc thực nghiệm tấn công UDP flood đã cung cấp cái nhìn sâu sắc về cách thức hoạt động, tác động và các biện pháp phòng chống cần thiết để bảo vệ hệ thống. Kết quả cho thấy rằng hệ thống cần có các biện pháp bảo vệ nhiều lớp và phải được cấu hình chính xác để đảm bảo hiệu suất và khả năng làm việc ổn định trước các cuộc tấn công từ chối dịch vụ. Phát hiện sớm và phản ứng kịp thời là chìa khóa để giảm thiểu thiệt hại từ các cuộc tấn công UDP flood.

## 3.2. Kịch bản 2: Tấn công SYN Flood

#### 3.2.1. Mục tiêu

#### 3.2.2. Tiến hành

#### 3.2.3. Kết luận

## 3.3. Kịch bản 3: Tấn công HTTP Flood

#### 3.3.1. Mục tiêu

#### 3.3.2. Tiến hành

#### 3.3.3. Kết luận

# KẾT LUẬN

# TÀI LIỆU THAM KHẢO