HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

BÁO CÁO MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN

Đề tài:
Tìm hiểu về các dạng tấn công DDoS

Sinh viên thực hiện: TRẦN CAO MINH BÁCH AT150204
VŨ THỊ ÁNH AT150504
TRẦN THỊ DUNG AT150310
Nhóm 8

Giảng viên hướng dẫn: ThS. NGUYỄN MẠNH THẮNG

Hà Nội, 09-2021

LỜI NÓI ĐẦU

Với công nghệ phát triển hiện tại, các cơ sở công nghệ thông tin xuất hiện rất nhiều. Đi cùng với đó là các cuộc tấn công ảnh hưởng đến việc đảm bảo tính sẵn sàng của một sản phẩm công nghệ thông tin. Và DDoS là một trong các loại tấn công ấy. Việc này ảnh hưởng rất nhiều đến các cơ sở hạ tầng công nghệ thông tin không phát triển kịp với thời đại công nghệ. Nhiều cuộc tấn công nhiều khi nhắm vào mục đích phá hoại dẫn đến ảnh hưởng rất nhiều đến kinh tế. Bên cạnh đó khi mà thế giới ngày càng nhiều kết nối với nhau sử dụng đến Internet. Việc server không có khả năng hồi đáp cho các người dùng hợp pháp cũng chính là mục tiêu của các kẻ tấn công bằng phương pháp DDoS. Đề tài này là một đề tài hay, nó đề cập đến vấn đề tuy cũ nhưng luôn là vấn đề nhức nhối nhất trong các vấn đề mà các nhà quản lý cơ sở hạ tầng, các nhân viên giám sát hệ thống luôn phải cảnh giác cao độ.

LỜI CAM ĐOAN

Tôi là Trần Cao Minh Bách, mã số sinh viên AT150204, sinh viên lớp AT15B, khóa AT15. Người hướng dẫn là ThS. Nguyễn Mạnh Thắng. Tôi xin thay mặt, cam đoan toàn bộ nội dung được trình bày trong đồ án Tìm hiểu về các dạng tấn công DDoS là kết quả quá trình tìm hiểu và nghiên cứu của chúng tôi. Các dữ liệu được nêu trong đồ án là hoàn toàn trung thực, phản ánh đúng kết quả đo đạc thực tế. Mọi thông tin trích dẫn đều tuân thủ các quy định về sở hữu trí tuệ; các tài liệu tham khảo được liệt kê rõ ràng. Tôi xin chịu hoàn toàn trách nhiệm với những nội dung được viết trong đồ án này.

Hà Nội, ngày 13 tháng 09 năm 2021

Người cam đoan

Trần Cao Minh Bách

MỤC LỤC

DANH MỤC HÌNH VẼ

TÓM TẮT ĐỒ ÁN

Đây là báo cáo liên quan đến khái niệm chung nhất của DDoS. Bên cạnh đó là các khái niệm về các loại tấn công phổ biến hiện nay, đang được các hacker sử dụng để tấn công và khai thác từ nó. Với cấu trúc các phần gồm:

Chương 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG DDOS

Bao gồm tình hình chung của thế giới công nghệ thông tin với các cuộc tấn công DDoS, các khái niệm chung về các thành phần tạo nên một cuộc tấn công DDoS trên thực tế. Các khái niệm cung cấp cái nhìn chung nhất về DDoS.

Chương 2: CÁC KỸ THUẬT TẤN CÔNG DDOS

Các kỹ thuật tấn công sẽ được đề cập trong chương này, từ các kỹ thuật đã trở thành lỗi thời đến các kỹ thuật mới nhất sẽ được cập nhật ở đây. Bên cạnh đó, chương còn đề cập đến việc sử dụng các phần mềm để khai thác các lỗ hổng, nhằm tạo ra cuộc tấn công DoS hay DDoS một cách hoàn toàn dễ dàng trong môi trường lab.

CHƯƠNG 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG DDOS

1.1 Tình hình chung thế giới

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 băng thông tối 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 nhằm 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, 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). Trong những năm tiếp theo, vài công cụ nữa được phổ biến – TFN (tribe flood network), TFN2K và Stacheldraht.

Tuy nhiên, chỉ từ cuối năm 1999 mới có những báo cáo về những cuộc tấn công như vậy, và đề tài này được công chúng biết đến chỉ sau khi một cuộc tấn công lớn vào các site công cộng vào tháng 2/2000.

- 2/2000, Yahoo! (Một trang web nổi tiếng) đã bị tấn công từ chối dịch vụ và ngưng trệ hoạt động trong vòng 3 giờ đồng hồ. Website 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 nhiều Web site lớn như Buy.com, Amazon.com, eBay, Datek, MSN, và CNN.com bị tấn công từ chối dịch vụ.

- Lúc 7 giờ tối ngày 9/2/2000 Website Excite.com là cái đích của một vụ tấn công từ chối dịch vụ, dữ liệu được gửi tới tấp trong vòng 1 giờ cho đến khi kết thúc.

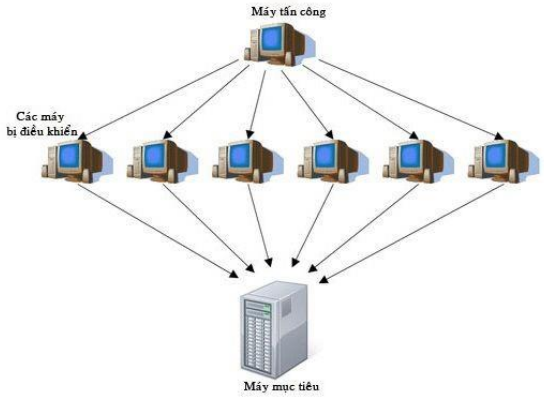
Từ đó các cuộc tấn công DoS thường xuyên xảy ra ví dụ :

- Vào ngày 15/8/2003, Microsoft đã chịu đợt tấn công DoS cực mạnh và làm gián đoạn websites trong vòng 2 giờ.

- Vào lúc 15:09 giờ GMT ngày 27/3/2003: toàn bộ phiên bản tiếng Anh của website Al-Jazeera bị tấn công làm gián đoạn trong nhiều giờ.

1.2 Khái niệm DDoS

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service attack- DDoS attack) là hành động ngăn cản những người dùng hợp pháp của một dịch vụ nào đó truy cập và sử dụng dịch vụ đó, bằng cách làm cho server không thể đáp ứng được các yêu cầu sử dụng dịch vụ từ các client. Nguồn tấn công không đến từ một máy tính trên Internet, mà đến từ một hệ thống nhiều máy tính với các địa chỉ IP khác nhau (điểm khác nhau giữa tấn công DoS và DDoS).



Mô hình tấn công DDoS

Xuất hiện lần đầu tiên vào năm 1999, so với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn rất nhiều, do nguồn tấn công không đến từ một máy tính như tấn công Dos mà đến từ nhiều máy tính. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông gây nghẽn mạng dẫn đến hệ thống ngưng hoạt động. Tuy nhiên cùng với sự phát triển của các thiết bị phần cứng và các hệ thống phòng thủ, các dạng tấn công DDoS cũng ngày càng phức tạp thông minh, không chỉ chiếm dụng băng thông, mà còn khai thác các lỗ hổng trong các ứng dụng để tấn công làm cạn kiệt tài nguyên của hệ thống. Những kiểu tấn công này được đánh giá là nguy hiểm hơn, do chúng có thể gây tổn hại trực tiếp đến cơ sở dữ liệu.

1.3 Các giai đoạn của tấn công DDoS

1.3.1 Giai đoạn chuẩn bị

Chuẩn bị công cụ cho cuộc tấn công, công cụ này thông thường hoạt động theo mô hình Client- Server. Hacker có thể viết phần mềm này hay download một cách dễ dàng trên mạng.

Tiếp theo, hacker chiếm quyền điều khiển các máy tính trên mạng, tiến hành tải và cài đặt ngầm các chương trình độc hại trên máy tính đó. Để làm được điều này, hacker thường lừa cho người dùng click vào một link quảng cáo có chứa Trojan, worm. Kết thúc giai đoạn này, hacker sẽ có một attack- network (một mạng các máy tính ma phục vụ cho việc tấn công DDoS).

1.3.2 Giai đoạn xác định mục tiêu và thời điểm tấn công

Sau khi xác định được mục tiêu cần tấn công, hacker sẽ điều chỉnh attack-network chuyển hướng tấn công mục tiêu đó. Yếu tố thời điểm sẽ quyết định mức độ thiệt hại của cuộc tấn công. Vì vậy, nó phải được hacker ấn định trước.

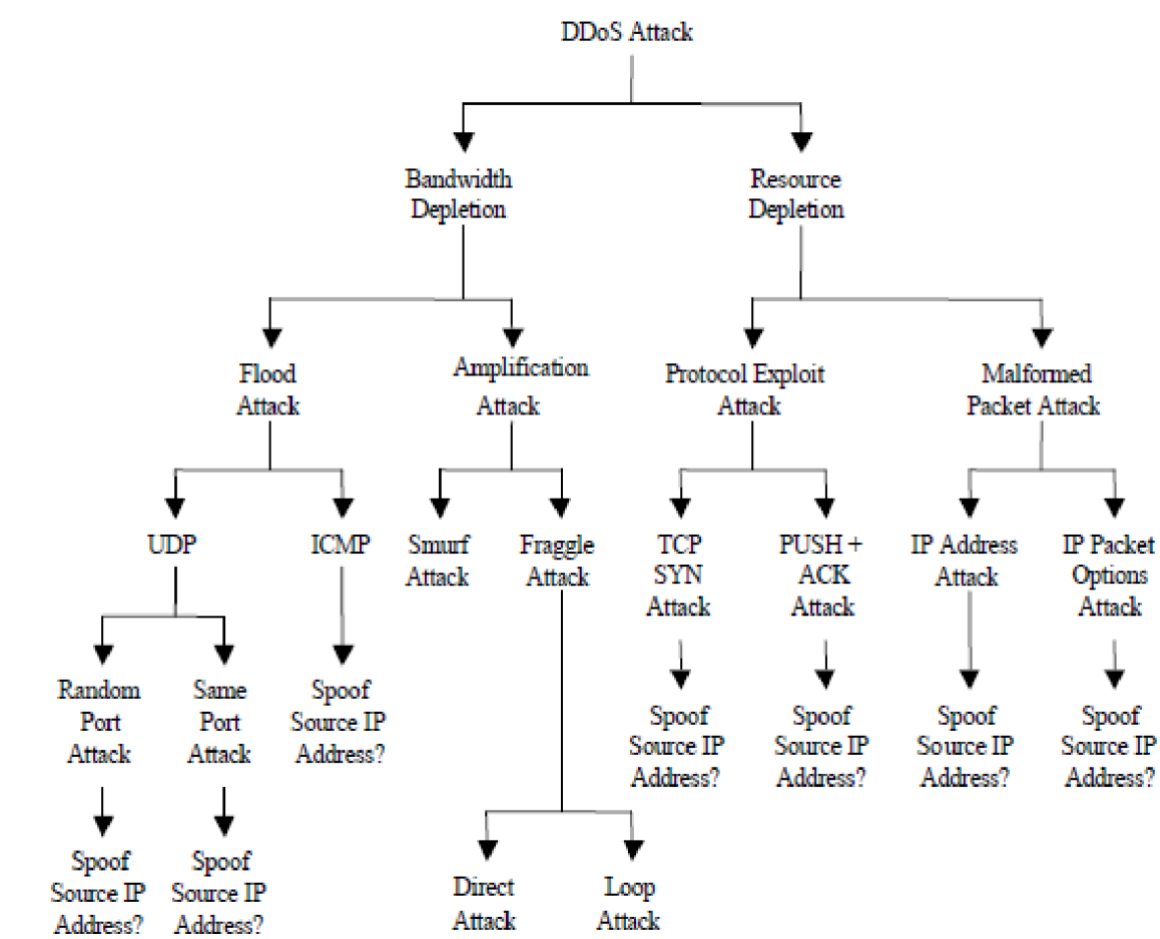
1.3.3 Giai đoạn phát động tấn công và xóa dấu vết

Đúng thời điểm đã định trước, hacker phát động lệnh tấn công từ máy của mình. Toàn bộ attack - network (có thể lên đến hàng ngàn, hàng vạn máy) đồng loạt tấn công mục tiêu, mục tiêu sẽ nhanh chóng bị cạn kiệt băng thông và không thể tiếp tục hoạt động. Sau một khoảng thời gian tấn công, hacker tiến hành xóa dấu vết có thể truy ngược đến mình, việc này đòi hỏi trình độ cao của những hacker chuyên nghiệp.

1.4 Phân loại tấn công từ chối dịch vụ phân tán

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



Sơ đồ phân loại DDoS attack theo mục đích tấn công

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:

- Các cuộc tấn công IP nhằm vào băng thông - tấn công vào lớp 3.
- 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.

1.5 Mạng BOTNET

1.5.1 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.

1.5.2 Mạng Internet Relay Chat

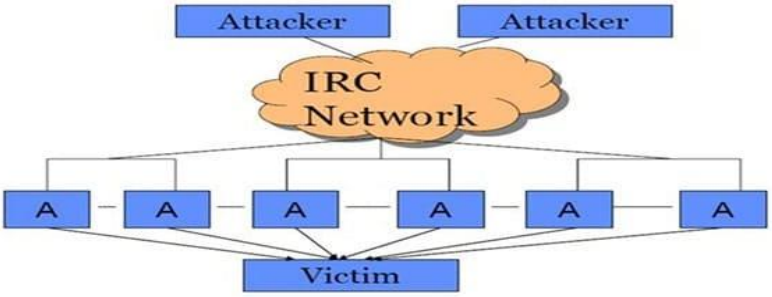
Mạng Internet Relay Chat (IRC) được sáng tạo bởi Jarkko Oikarinen (nickname “WiZ”) vào 8 - 1988 để thay thế cho một chương trình có tên là MUT (MultiUser Talk) trên một kênh BBS gọi là OuluBox tại Phần Lan. Ông tìm được cảm hứng cho dự án của mình từ hệ thống Bitnet Relay Chat của mạng Bitnet.

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.

1.5.3 Chương trình Bot và BotNet



Mô hình mạng IRC

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.

1.5.4 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.

1.5.5 Botnet Mirai

Botnet Mirai, bao gồm chủ yếu là các thiết bị nhúng và IoT, đã gây bão Internet vào cuối năm 2016 khi nó tấn công một số mục tiêu quan trọng với các cuộc tấn công từ chối dịch vụ phân tán (DDoS) khổng lồ.

Cách thức hoạt động của Mirai:

Bước đầu tiên, mã độc sẽ dò quét cổng SSH22/TELNET23 hoặc 2323 của những địa chỉ IPv4 ngẫu nhiên nhưng nằm trong dải IP được xác định trước. Mirai dò quét nhanh bằng cách gửi các gói tin TCP SYN thăm dò tới cổng TELNET. Nếu phát hiện ra cổng TELNET của thiết bị mở, Mirai sẽ cố gắng khởi tạo phiên TELNET bằng cách sử dụng ngẫu nhiên 10/62 tài khoản mặc định trên các dòng thiết bị IoT mà nó biết.

Sau khi nhận được thông tin, máy chủ báo cáo gửi một chương trình nạp (loader) tới thiết bị IoT. Chương trình nạp sẽ xác định chủng loại, firmware, OS…của thiết bị. Từ những thông tin lấy được, chương trình nạp sẽ tải về loại mã độc tương ứng để có thể chạy trên thiết bị này. Mirai mất khoảng 98 giây để thực hiện hành động lây nhiễm cho 1 thiết bị IoT.

Mã độc sau khi chạy trên thiết bị thì sẽ xóa dấu vết bằng cách xóa file tải về và "thay tên đổi họ" tiến trình chạy trong bộ nhớ chính của thiết bị. Vì đã xóa file tải về nên khi thiết bị reboot, các thông tin trong bộ nhớ chính bị xóa, mã độc sẽ không hoạt động trên thiết bị nữa. Để "củng cố địa vị", Mirai kill các tiến trình sử dụng cổng TCP22/23 và cũng kill các tiến trình của các mã độc khác như .anime hay .Qbot, mặc dù đây cũng là các biến thể của Mirai.

Sau khi mã độc chạy, thiết bị IoT giờ đã trở thành một bot hay Zoombie trong mạng botnet Mirai, và có nhiệm vụ nhận lệnh từ máy chủ C2 (Command & Control) để tấn công DDoS. Vì là chu trình lây lan nên từ thiết bị này, mã độc tiếp tục dò quét cổng SSH22/TELNET23/2323 của các thiết bị IoT khác.

1.5.6 Các bước xây dựng mạng Botnet Agobot

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.

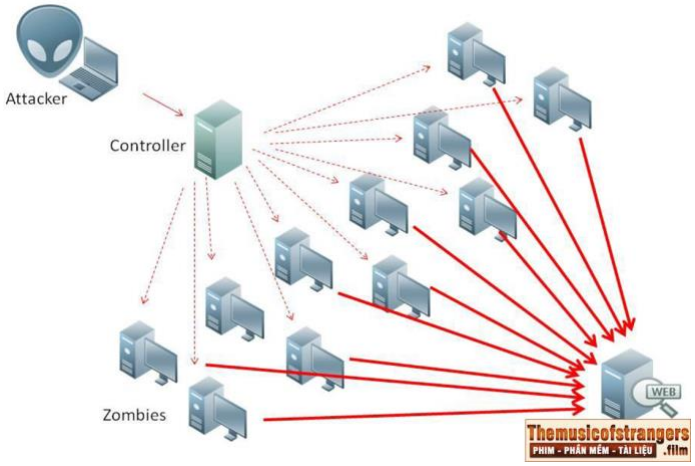
Bước 3: Kết nối vào IRC

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.

1.5.7 Mô hình tấn công DDoS



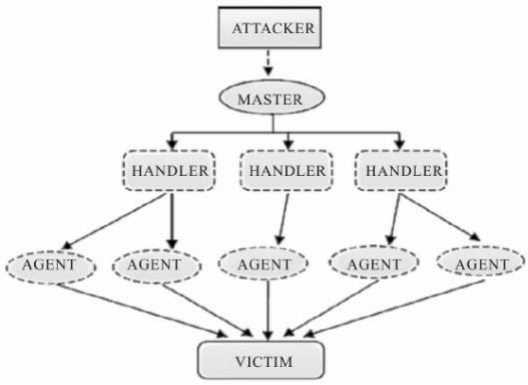
Sơ đồ mô hình tấn công DDoS

Tấn công DDoS có 2 mô hình chính:

- Mô hình Agent- Handler
- Mô hình IRC- Based
- Mô hình Peer-to-Peer

1.5.8 Mô hình tấn công Agent – Hander

Theo mô hình này, attack- network gồm 2 thành phần chính: Agent và Handler.



Kiến trúc mô hình tấn công Agent- Handler

- Handler: Kẻ tấn công cũng sử dụng một lớp riêng biệt của hệ thống máy tính - được gọi là Handlers - cũng như hệ thống chỉ huy và kiểm soát để quản lý các Agent. Thông thường một Handlers là một máy chủ mạnh mẽ với rất nhiều tài nguyên (băng thông, bộ nhớ, và sức mạnh xử lý)

- Agent: Các bots (ví dụ như các hệ thống máy tính bị nhiễm) được gọi là các Agents

Kẻ tấn công sẽ 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 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:

TẬP LỆNH CỦA HANDLER:

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

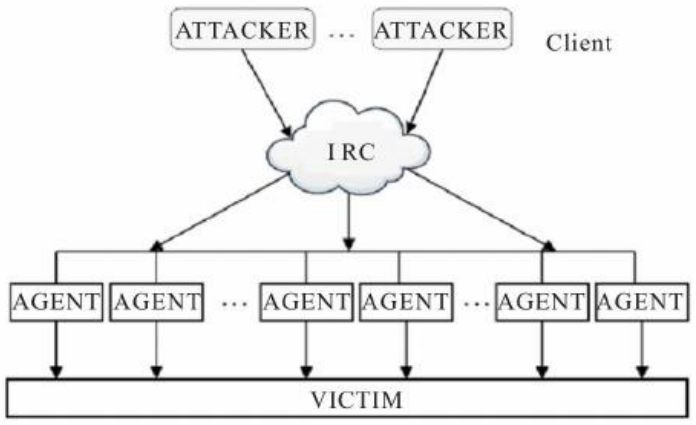
TẬP LỆNH CỦA AGENT:

Turn On	Kích hoạt 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

Hạn chế:

- Kiến trúc Agent - Handler có một hạn chế lớn là kẻ tấn công phải có khả năng giao tiếp với các Handlers và Handlers phải có khả năng liên lạc với các Agents.
- Nếu những kẻ tấn công bị mất liên lạc, kẻ tấn công mất kiểm soát của các Agents và do đó không thể dàn xếp các Agents để tấn công một mục tiêu mới

1.5.9 Mô hình tấn công IRC - Based



Kiến trúc 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 cùng channel. Tuy nhiên, nếu user khác 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.

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, kẻ tấn công còn có thêm một số lợi thế như:

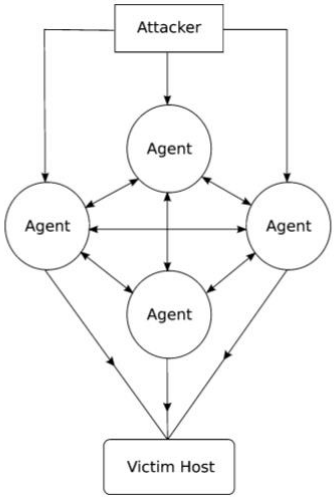
- Các giao tiếp dưới dạng chat message làm cho việc phát hiện chúng là vô cùng khó khăn.

- Các message 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 đang nhập vào IRC server là có thể nhận được các báo cáo về trạng thái các Agent do các channel gửi về.

➔ Hai khác biệt chính giữa các kiến trúc dựa trên IRC và các Agent - Handler là cấu trúc điều khiển và thông tin liên lạc. Trong kiến trúc dựa trên IRC, mỗi Agent kết nối với một máy chủ IRC trong khi ở Agent - Handler, mỗi Agent có thể kết nối với nhiều hơn một Handler.

1.5.10 Mô hình tấn công Peer-to-Peer



Mô hình tấn công Peer-to-Peer

Không giống như các mô hình agent-handler và kiến trúc IRC-based, các Botnet dựa trên cấu trúc Peer-to-Peer không có handler riêng biệt. Lệnh được gửi đến các agent thông qua giao thức P2P. Trong trường hợp này mỗi agent/bot không chỉ chịu trách nhiệm cho việc chuyển

tiếp lệnh tấn công mà còn là một phần của cơ cấu chỉ huy và kiểm soát để quản lý các agent khác. Như vậy, kiến trúc botnet dựa trên P2P rất khó để đánh sập vì sự phân bố tự nhiên rất cao của nó.

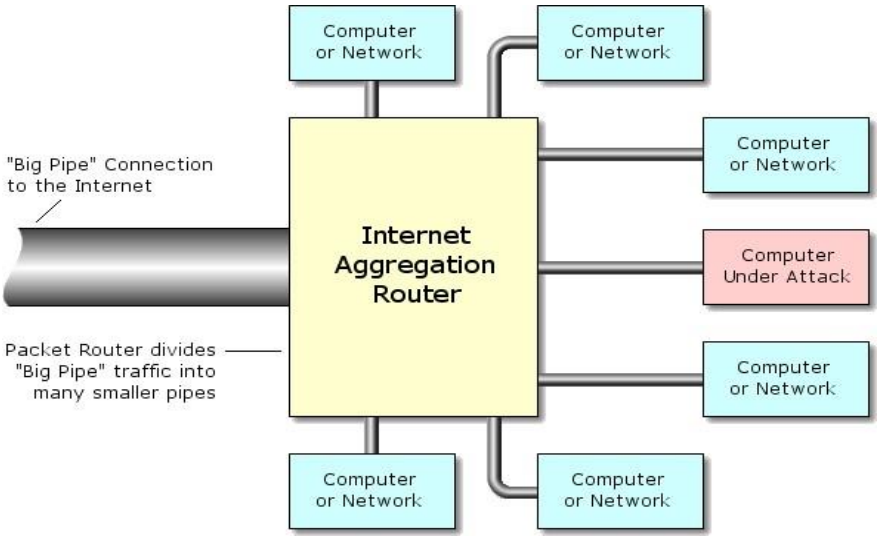
Ngoài việc phân phối lệnh, các kênh truyền thông P2P được sử dụng để phân phối các phiên bản mới của phần mềm bot và để tải về công cụ tấn công mới và một danh sách các mục tiêu mới. Để thực hiện các cuộc tấn công hoặc các thông tin liên lạc là khó khăn hơn nhiều để phát hiện và phân tích, thông tin liên lạc có thể được mã hóa.

CHƯƠNG 2: CÁC KỸ THUẬT TẤN CÔNG DDOS

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

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.



Sơ đồ tấn công kiểu tràn băng thông

Như ta thấy trên sơ đồ, tất cả các gói tin đi vào một mạng máy tính qua "BigPipe" (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 lượnng 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.

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 hiệu cổng trong UDP.

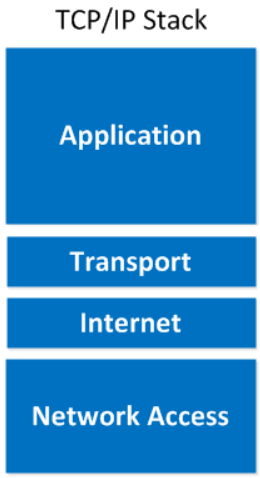
(1) **Giao thức UDP:**

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.

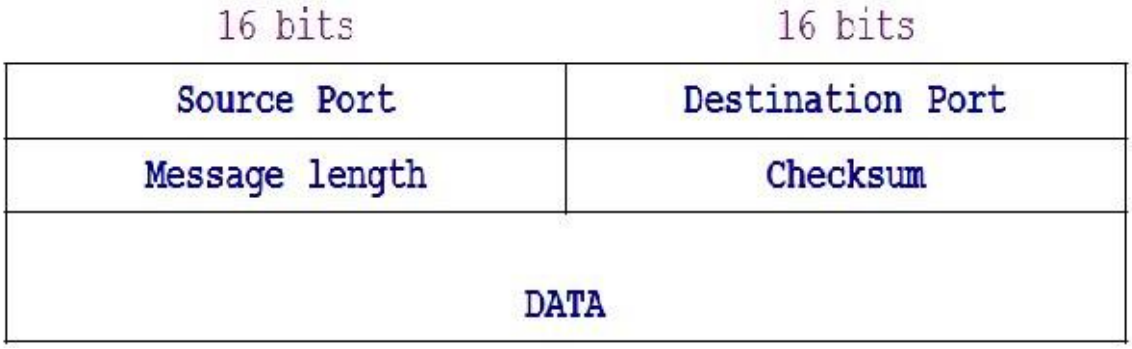
(2) **Cấu trúc gói UDP:**

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.



Các tầng trong giao thức TCP/IP

UDP không đảm bảo cho các tầng phía trên việc xác thực 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).



Cấu trúc gói tin UDP

Phần 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.

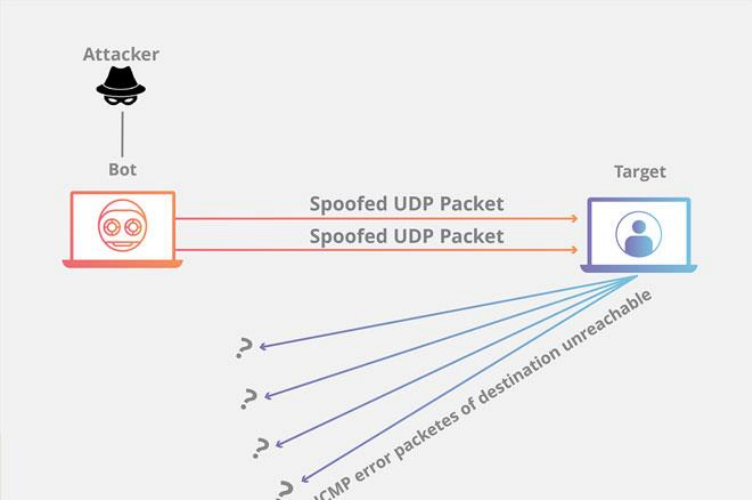
(3) **Tìm số hiệu cổng trong UDP:**

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 quyền 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.



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 ko 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

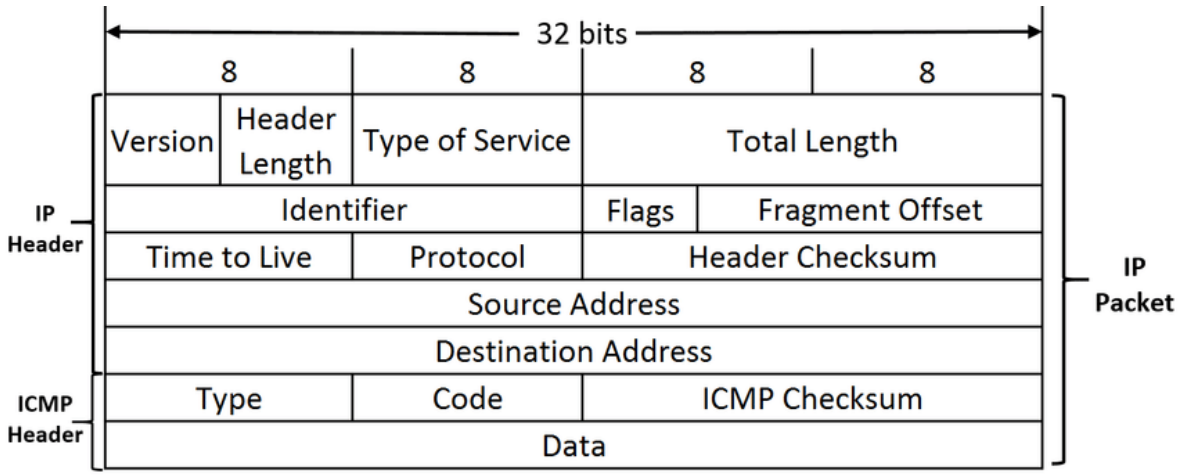
Để nghiên cứu về ICMP flood attack, cần hiểu kiến thức cơ bản về ICMP.

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 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.

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



Cấu trúc tổng quát của gói tin ICMP

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.

2.1.1.3 DNS Flood

Đây là một biến thể của UDP Flood mục tiêu tập trung vào các máy chủ DNS. Hakcer tạo ra một loạt các gói yêu cầu DNS giả giống như các gói hợp pháp bắt nguồn từ một số lượng lớn các địa chỉ IP khác nhau. DNS Flood là một trong những kiểu tấn công từ chối dịch vụ khó nhất để ngăn chặn và khôi phục.

2.1.1.4 VoIP Flood

Đây là một hình thức phổ biến của UDP Flood nhắm vào máy chủ "giao thức thoại" qua giao thức Internet (VoIP). Vô số các yêu cầu VoIP không có thật được gửi từ nhiều địa chỉ IP làm cạn kiệt tài nguyên của máy chủ nạn nhân khiến dịch vụ VoIP bị đình trệ (từ chối dịch vụ).

2.1.1.5 SSDP Flood

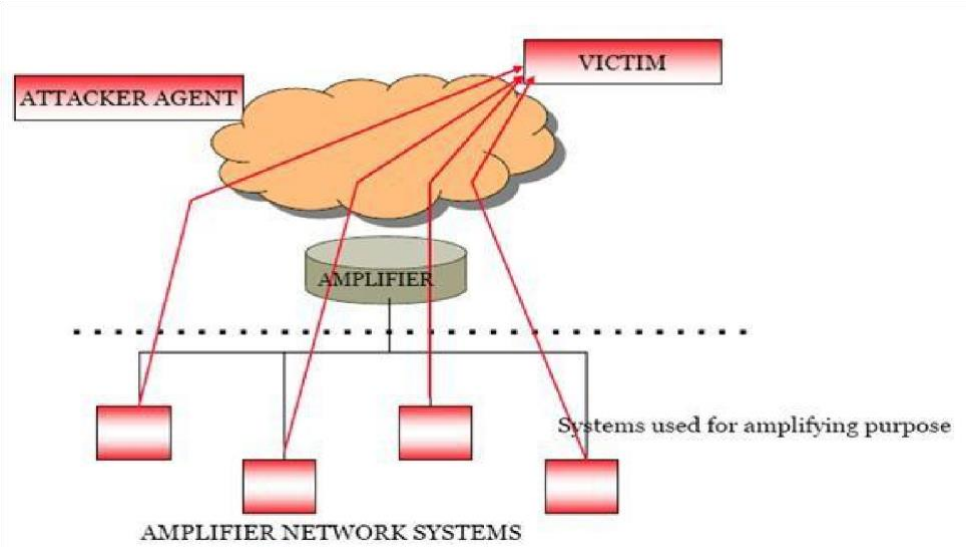
Hacker có thể khai thác các thiết bị được kết nối mạng chạy các dịch vụ Universal Plug and Play (UPnP) để thực hiện một cuộc tấn công DDoS dựa trên giao thức khám phá dịch vụ đơn giản (SSDP). Mặt khác, SSDP được nhúng trong khung giao thức UPnP. Kẻ tấn công gửi các gói UDP nhỏ có địa chỉ IP giả mạo của máy chủ nạn nhân đến nhiều thiết bị chạy UPnP kết quả máy chủ nạn nhân quá tải dẫn đến tình trạng từ chối dịch vụ.

2.1.2 Tấn công khuếch đại (Amplification attack)

Đây cũng 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.

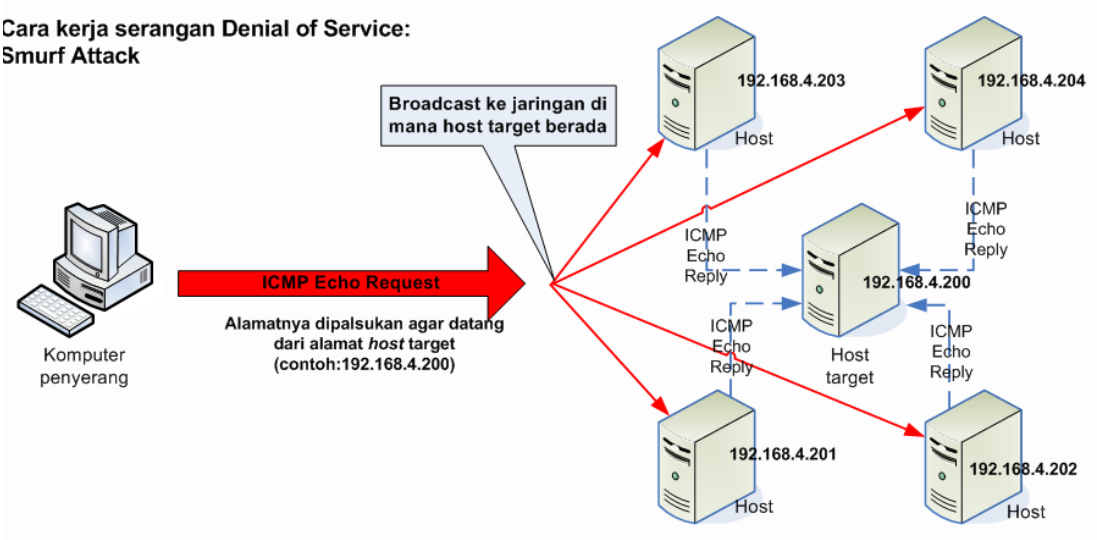
Kẻ tấn công có thể gửi các message trực tiếp hay thông qua một số Agent nhằm làm gia tăng cường độ của cuộc tấn công.



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.

2.1.2.1 Tấn công kiểu Smurf



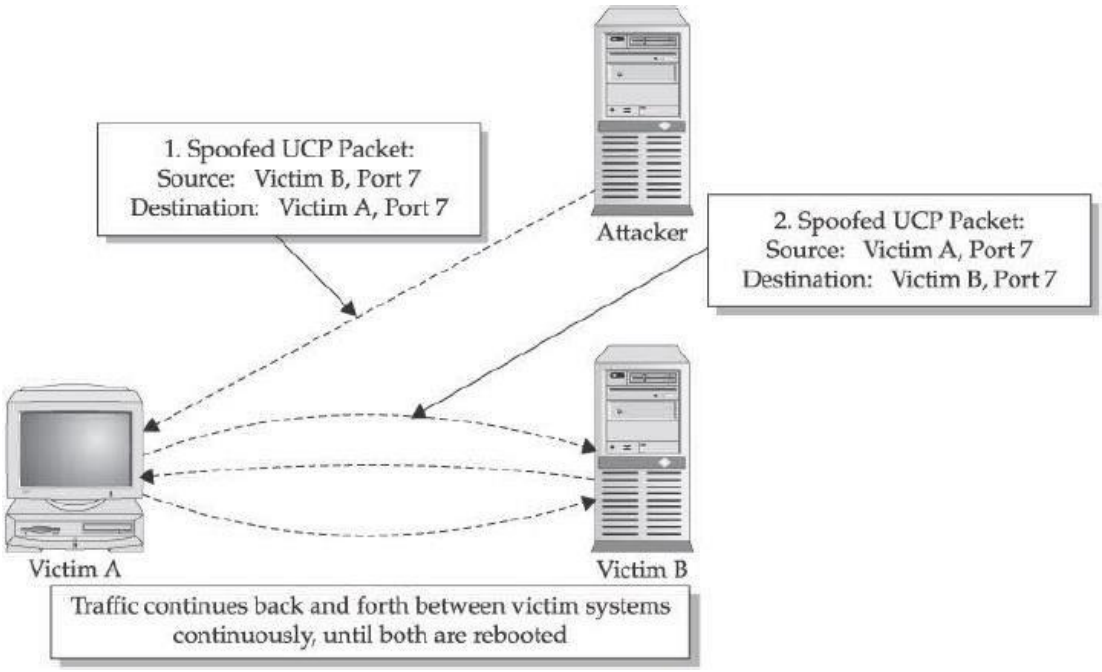
Sơ đồ tấn công kiểu Smurf

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

Trong Smurf 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 Smurf 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 Smurf.

2.1.2.2 Tấn công kiểu Fraggle

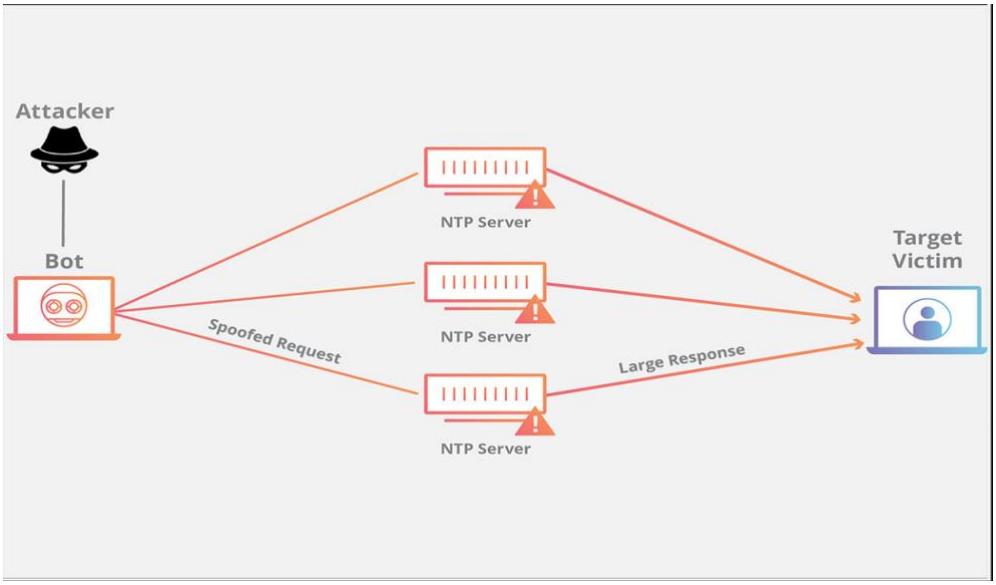


Sơ đồ tấn công kiểu Fraggle

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

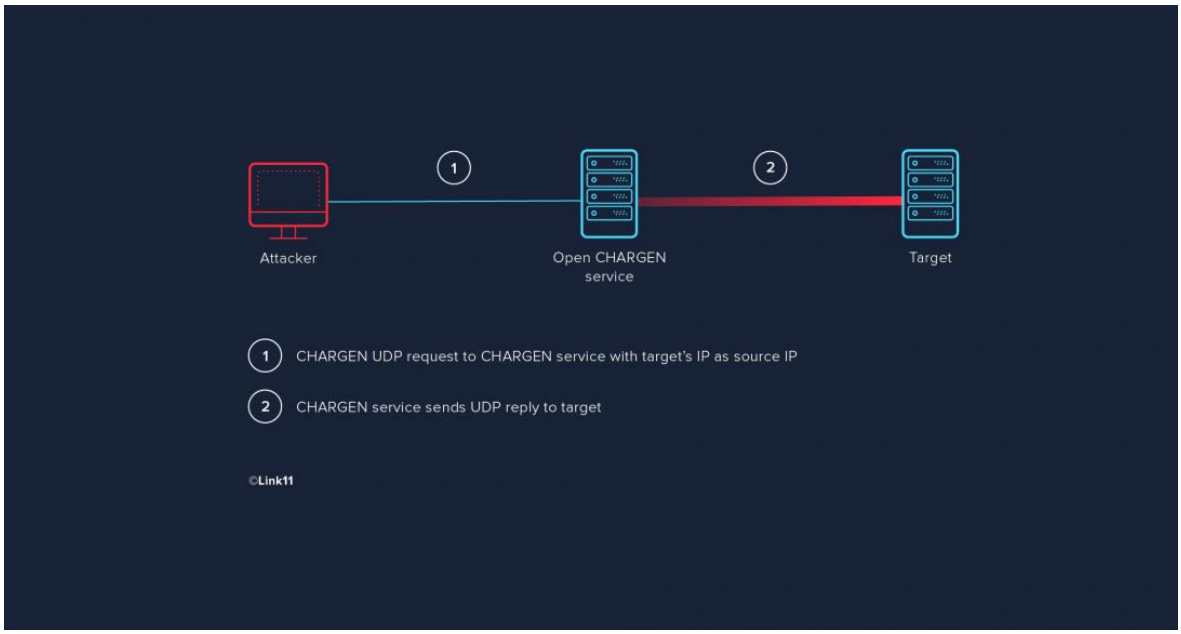
2.1.2.3 NTP Amplification

NTP - Network Time Protocol, một trong những giao thức mạng lâu đời nhất được giao nhiệm vụ đồng bộ hóa thời gian giữa các hệ thống điện tử là cốt lõi của DDoS attack vector. Cách thức thực hiện là khai thác lỗ hổng các máy chủ NTP có thể truy cập công khai để làm quá tải mạng đích với số lượng lớn các gói UDP.



Sơ đồ tấn công NTP

2.1.2.4 CHARGEN Flood



Sơ đồ tấn công CHARGEN Flood

Tương tự như NTP, Giao thức Character Generator Protocol (**CHARGEN**) là một giao thức cũ có xuất hiện từ những năm 1980. Mặc dù vậy nó vẫn đang được sử dụng trên một số thiết bị được kết nối như máy in và máy photocopy. Cuộc tấn công bắt nguồn từ việc gửi các gói tin nhỏ đã bị sửa đổi IP thành IP máy chủ nạn nhân đến các thiết bị có bật giao thức CHARGEN kết quả là các thiết bị nhận được gói tin giả mạo kia có kết nối với Internet sẽ gửi các gói UDP đến máy chủ nạn nhân do đó làm cạn kiệt tài nguyên dẫn đến tình trạng từ chối dịch vụ.

2.1.2.5 SNMP Flood

SNMP - Simple Network Management Protocol là một tập hợp các giao thức không chỉ cho phép kiểm tra các thiết bị mạng như router, switch hay server có đang vận hành mà còn hỗ trợ vận hành các thiết bị này một cách tối ưu, ngoài ra SNMP còn cho phép quản lý các thiết bị mạng từ xa. Hacker tấn công một máy chủ mục tiêu, bộ chuyển mạch hoặc bộ định tuyến với nhiều gói nhỏ đến từ một địa chỉ IP giả mạo.

Khi ngày càng có nhiều thiết bị đang lắng nghe và trả lời địa chỉ giả mạo đó lúc ấy hệ thống mạng không đủ khả năng xử lý các phản hồi này và dẫn đến tình trạng từ chối dịch vụ.

2.1.2.6 Misused Application Attack

Thay vì sử dụng địa chỉ IP giả mạo, cuộc tấn công này ký sinh trên các máy khách hợp pháp chạy các ứng dụng sử dụng nhiều tài nguyên như công cụ P2P. Hacker sẽ bẻ cong sự định tuyến lưu lượng truy cập từ các máy khách này đến máy chủ nạn nhân khiến nó bị tải quá. Kỹ thuật DDoS này khó ngăn chặn vì lưu lượng truy cập bắt nguồn từ các máy khách thực trước đây đã bị Hakcer xâm nhập.

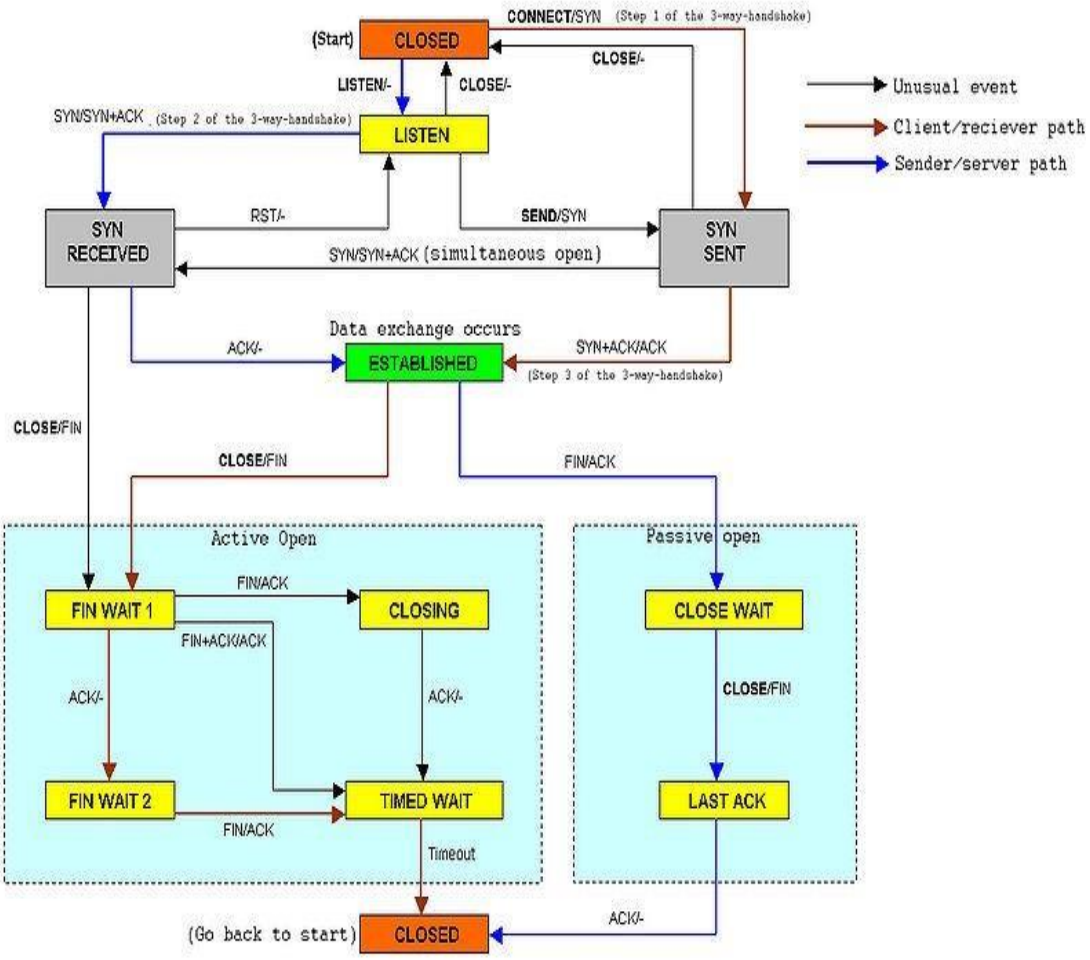
2.2 Tấn công làm cạn kiệt tài nguyên (Resoure Deleption)

2.2.1 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):**

Đây 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.



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:

- 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).

- 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.

(2) **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.

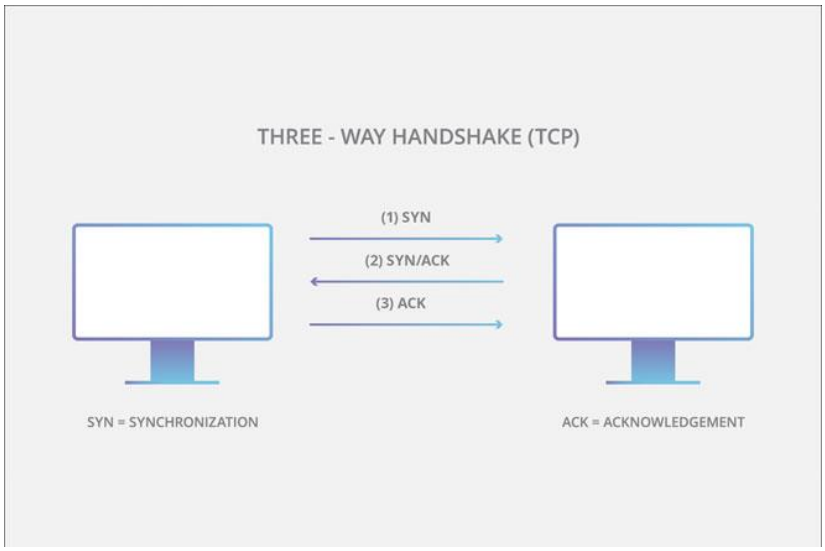
- Server hồi đáp bằng cách gửi lại phía client bản tin SYN-ACK, trong gói tin này, tham số acknowledgment number được gán giá trị bằng X+1, tham số sequence number được gán ngẫu nhiên một giá trị Y.

- 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.

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.



Sơ đồ quá trình bắt tay 3 bước

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)

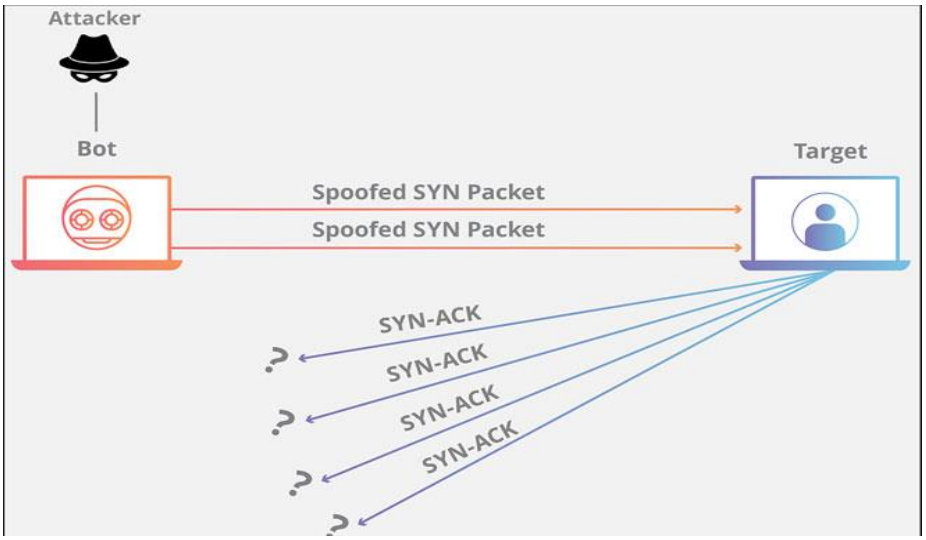
Tấn công tràn SYN (SYN flood attack) là một dạng tấn công từ chối dịch vụ, kẻ tấn công gửi thành công các SYN request đến hệ thống đích. SYN flood là kiểu tấn công khá phổ biến. Nó làm việc nếu server định vị tài nguyên sau khi nhận SYN, nhưng trước khi nhận ACK. Kẻ tấn công làm tràn ngập hệ thống nạn 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.

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.



Tấn công tràn SYN

2.2.2 *SYN-ACK Flood*

Theo logic đây là kiểu tấn công vector lợi dụng giao tiếp TCP trong đó máy chủ tạo ra gói tin SYN-ACK để xác nhận yêu cầu của user. Để thực hiện tấn công Hacker đã làm quá tải tài nguyên CPU RAM của máy chủ bằng cách gửi các gói tin SYN-ACK giả mạo.

2.2.3 *ACK & PUSH ACK Flood*

Giao thức TCP yêu cầu giao thức bắt tay ba bước khi thiết lập kết nối giữa máy chủ và máy khách các gói ACK hoặc PUSH ACK được gửi qua lại cho đến khi phiên làm việc kết thúc. Máy chủ bị tấn công dạng này sẽ không thể xác định nguồn gốc của các gói tin bị làm sai lệch địa chỉ và máy chủ lúc đó sẽ lãng phí khả năng xử lý khi cố gắng xác định cách xử lý chúng.

2.2.4 *Fragmented ACK Flood*

Cuộc tấn công này là một knockoff của kỹ thuật ACK & PUSH ACK Flood đã đề cập ở trên. Nó tập trung vào việc xóa một mạng đích với số lượng gói ACK bị phân mảnh tương đối nhỏ, có kích thước tối đa được phép, thường là 1500 byte mỗi gói. Các thiết bị mạng như bộ định tuyến cũng sẽ hết tài nguyên khi cố gắng lắp ráp lại các gói này. Hơn nữa, các gói bị phân mảnh có thể vượt qua radar của các hệ thống ngăn chặn xâm nhập (IPS) và Firewall.

2.2.5 *Spoofed Session Flood*

Để phá vỡ các công cụ bảo vệ hệ thống mạng như Firewall chả hạn, Hacker có thể giả mạo phiên TCP hiệu quả hơn bằng cách gửi gói SYN giả mạo, một loạt các gói ACK và ít nhất một gói RST (reset hoặc FIN (connection termination)). Chiến thuật này cho phép Hacker lừa hệ thống phòng thủ chỉ giữ các tab trên lưu lượng truy cập đến thay vì phân tích lưu lượng truy cập trở lại.

2.2.6 *LAND attack*

Để thực hiện một cuộc tấn công Local Area Network Denial(Land), Hacker sẽ gửi một SYN message đã được chỉnh sửa trong đó các địa chỉ IP nguồn và đích giống nhau. Khi máy chủ cố gắng trả lời tin nhắn này, nó sẽ vào một vòng lặp bằng cách tạo lại các câu trả lời cho chính nó điều này dẫn đến một kịch bản lỗi và máy chủ đích cuối cùng có thể bị sập.

2.3 Các biến thể của tấn công DDOS

2.3.1 *Tấn công kiểu Flash DDOS*

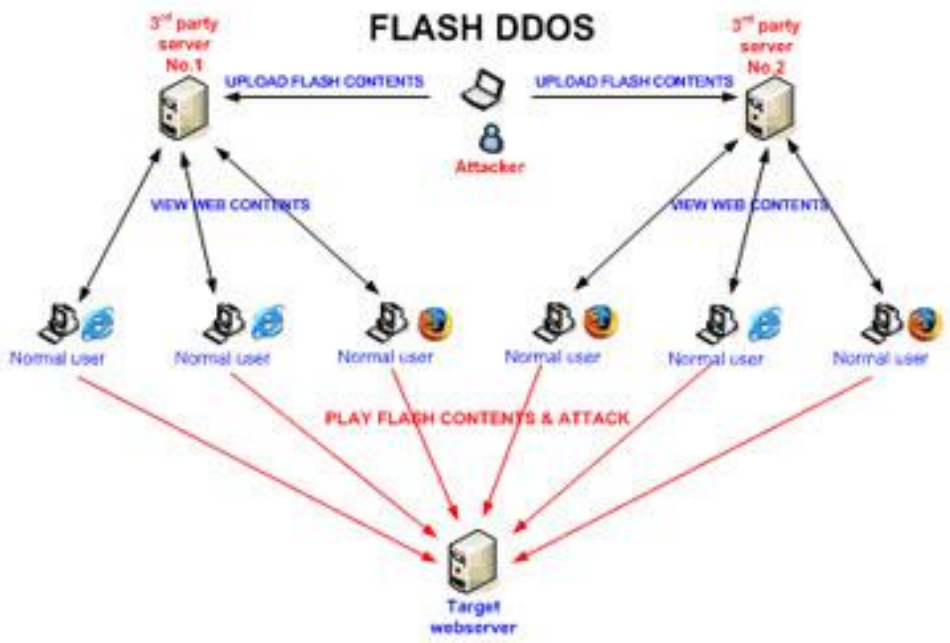
Để thực hiện tấn công DDoS, hacker cần phải nắm quyền điều khiển càng nhiều máy tính càng tốt. Sau đó, hacker sẽ trực tiếp phát động tấn công hàng loạt từ xa thông qua một kênh điều khiển. Với quy mô mạng lưới tấn công bao gồm hàng trăm ngàn máy tính, kiểu tấn công này có thể đánh gục bất cứ hệ thống 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 ngược kẻ tấn công.

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

- Để phát 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 ngăn chặn DDoS.



Sơ đồ tấn công Flash DDOS

Lưu ý: Biến thể này đã không còn tồn tại bởi các trình Flash hiện tại đã dừng cung cấp, từ đó cách tấn công này là không còn thực tế

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

-Kẻ tấn công không cần phải nắm quyền điều khiển và cài DDoS software vào các Agent. Thay vào đó, mọi user với một trình duyệt có hỗ trợ Flash player đều có thể trở 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 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. User load nội dung flash về, chạy thì ngay lập tức máy của họ trở thành một attack Agent, liên tục gửi các request đến 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 một 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 DRDoS là chiếm toàn bộ băng thông của hệ thống nạn nhân, tức làm nghẽn hoàn toàn đường kết nối từ máy chủ vào internet và làm tiêu hao tài nguyên máy chủ. Trong

suốt quá trình máy bị tấn công DRDoS, không một máy khách nào có thể kết nối được vào máy chủ đó. Tất cả các dịch vụ chạy 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

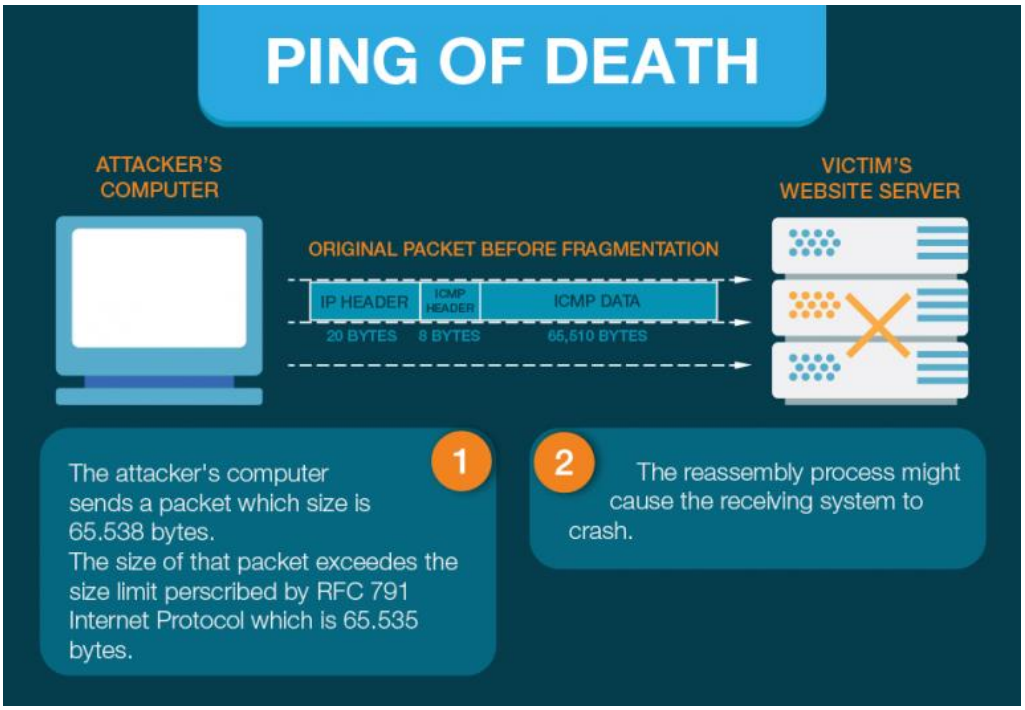
Phần mềm độc hại Obad là phát hiện đáng chú ý nhất trong lĩnh vực di động đang được phân tán bởi nhiều phương pháp, trong đó có một botnet được thiết lập sẵn. Điện thoại thông minh nền tảng Android bị lây nhiễm Trojan- SMS.AndroidOs.Opfake.a sẽ biến thành một nơi nhân bản, gửi các tin nhắn văn bản có 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.

2.3.4 *Tấn công Ping of Death Attack*

Ping of Death là kỹ thuật tấn công làm quá tải hệ thống mạng bằng cách gửi các gói tin ICMP có kích thước vượt quá 65.536 byte đến mục tiêu. Do kích thước này lớn hơn kích thước cho phép của các gói tin IP nên nó sẽ được chia nhỏ ra rồi gửi từng phần đến máy đích. Khi đến mục tiêu, nó sẽ được ráp lại thành gói tin hoàn chỉnh, do có kích thước quá mức cho phép, nó sẽ gây ra tràn bộ nhớ đệm và bị treo.

Theo một báo cáo kỹ thuật được công bố trong tuần này, kỹ thuật tấn công BlackNurse còn được biết đến dưới một cái tên truyền thống hơn: "tấn công gây lụt ping" và nó dựa trên các truy vấn ICMP Type 3 (hay lỗi Đích tới Không thể truy cập – Destination Unreachable) Code 3 (lỗi Cổng Không thể truy cập – Port Unreachable).

Được mệnh danh là kỹ thuật tấn công BlackNurse – Y Tá Đen hay tấn công tốc độ thấp "Ping of Death", kỹ thuật này có thể được sử dụng để phát động hàng loạt cuộc tấn công từ chối dịch vụ DDoS khối lượng thấp bằng cách gửi các gói tin ICMP hay các "ping" để làm ngập những bộ xử lý trên máy chủ. Ngay cả khi các máy chủ đó được trang bị những thiết bị tường lửa nổi tiếng, chúng vẫn có thể bị đánh gục nếu kẻ tấn công khai thác kỹ thuật này.



Sơ đồ Ping of Death Attack

Một số máy tính sẽ ngưng hoạt động, reboot hoặc bị crash khi gởi gói data ping với kích thước lớn đến chúng.

Ở kiểu DDoS attack Ping of Death này , ta chỉ cần gửi một gói dữ liệu có kích thước lớn thông qua lệnh ping đến máy đích thì hệ thống của họ sẽ bị treo. Nhưng hiện tại kiểu tấn công này không còn khả dụng nữa khi các tường lửa và hệ thống phát hiện xâm nhập đã có thể chống được những cuộc tấn công thuộc dạng này.

2.3.5 *IP Null Attack*

Kiểu tấn công này được thực hiện bằng cách gửi một loạt các gói tin chứa các IPv4 headers không hợp lệ. Thủ thuật là Hacker sẽ để giá trị headers NULL. Một số máy chủ không thể xử lý các gói tin hỏng này đúng cách và lãng phí tài nguyên của chúng khi cố gắng tìm cách xử lý chúng dẫn đến tình trạng từ chối dịch vụ.

2.3.6 *Recursive HTTP GET Flood*

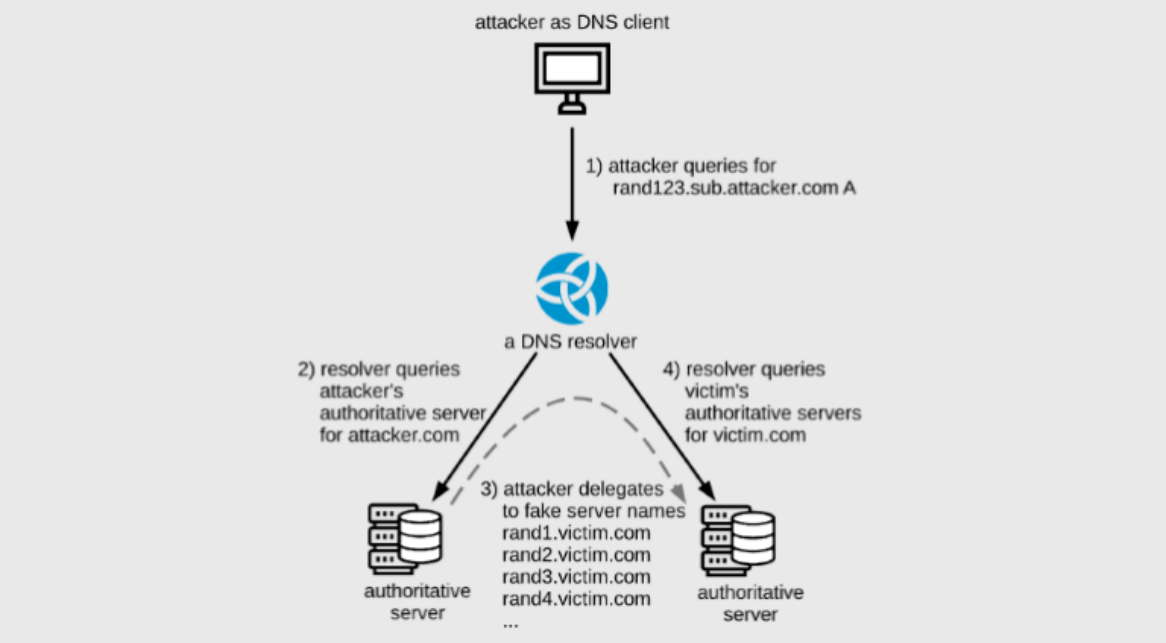
Để duy trì cuộc tấn công, Hacker tạo những request tới tất cả đường link của website của máy chủ sau đó kiểm tra các câu trả lời và lặp lại yêu cầu mọi đường link của trang web để làm cạn kiệt tài nguyên của máy chủ. Việc khai thác trông giống như các truy vấn hợp pháp và có thể khó xác định để ngăn chặn tấn công kiểu này.

2.3.7 *NXNS Attack*

NXNS Attack hoạt động bằng cách gửi yêu cầu truy cập tên miền do kẻ tấn công kiểm soát (ví dụ: "attacker.com") đến máy chủ phân giải DNS tồn tại lỗ hổng, máy chủ này sẽ chuyển tiếp truy vấn DNS đến máy chủ có thẩm quyền do kẻ tấn công kiểm soát.

Thay vì trả lại địa chỉ cho các máy chủ có thẩm quyền thực tế, máy chủ có thẩm quyền do kẻ tấn công kiểm soát trả lời truy vấn DNS với danh sách tên máy chủ giả hoặc tên miền phụ được kiểm soát mà trỏ đến tên miền DNS nạn nhân.

Sau đó, máy chủ DNS chuyển tiếp truy vấn đến tất cả các tên miền phụ không tồn tại, tạo ra lưu lượng truy cập lớn đến trang web nạn nhân.



Sơ đồ tấn công NXNS

Tra cứu DNS đệ quy xảy ra khi máy chủ DNS giao tiếp với nhiều máy chủ DNS có thẩm quyền theo trình tự phân cấp để xác định địa chỉ IP được liên kết với một tên miền (ví dụ www.google.com) và trả lại cho máy khách.

Quá trình phân giải này thường bắt đầu bằng trình phân giải DNS được điều khiển bởi ISP hoặc máy chủ DNS công cộng, như Cloudflare (1.1.1.1) hoặc Google (8.8.8.8), tùy theo cấu hình hệ thống.

Trình phân giải chuyển yêu cầu đến một máy chủ tên DNS có thẩm quyền nếu không thể định vị địa chỉ IP cho một tên miền nhất định.

Nhưng nếu máy chủ tên DNS có thẩm quyền đầu tiên cũng không giữ các bản ghi mong muốn, nó sẽ trả về thông báo ủy quyền có địa chỉ cho các máy chủ có thẩm quyền tiếp theo mà trình phân giải DNS có thể truy vấn.

Quá trình phân cấp này diễn ra cho đến khi trình phân giải DNS đến đúng máy chủ có thẩm quyền cung cấp địa chỉ IP của tên miền, cho phép người dùng truy cập trang web mong muốn.

Các nhà nghiên cứu nhận thấy rằng việc này có thể bị khai thác để lừa các trình phân giải đệ quy liên tục gửi một số lượng lớn gói tin đến một tên miền mục tiêu thay vì các máy chủ có thẩm quyền hợp pháp.

Theo các nhà nghiên cứu, để thực hiện tấn công thông qua một trình phân giải đệ quy, kẻ tấn công phải sở hữu một máy chủ có thẩm quyền, tức là có thể mua một tên miền – vốn rất dễ dàng.

NXNSAttack hoạt động bằng cách gửi yêu cầu truy cập tên miền do kẻ tấn công kiểm soát (ví dụ: "attacker.com") đến máy chủ phân giải DNS tồn tại lỗ hổng, máy chủ này sẽ chuyển tiếp truy vấn DNS đến máy chủ có thẩm quyền do kẻ tấn công kiểm soát.

Thay vì trả lại địa chỉ cho các máy chủ có thẩm quyền thực tế, máy chủ có thẩm quyền do kẻ tấn công kiểm soát trả lời truy vấn DNS với danh sách tên máy chủ giả hoặc tên miền phụ được kiểm soát mà trỏ đến tên miền DNS nạn nhân.

Sau đó, máy chủ DNS chuyển tiếp truy vấn đến tất cả các tên miền phụ không tồn tại, tạo ra lưu lượng truy cập lớn đến trang web nạn nhân.

Các nhà nghiên cứu cho biết cuộc tấn công có thể khuếch đại số lượng gói được trao đổi bởi trình phân giải đệ quy lên tới hơn 1.620, do đó không chỉ làm ngập các trình phân giải DNS với nhiều yêu cầu hơn mức chúng có thể xử lý, mà còn làm ngập tên miền mục tiêu với các yêu cầu không cần thiết và làm sập trang web. Hơn nữa, sử dụng một botnet như Mirai làm máy khách DNS có thể tăng thêm quy mô của cuộc tấn công.

Các quản trị viên mạng chạy máy chủ DNS được khuyến cáo cập nhật phần mềm trình phân giải DNS của mình lên phiên bản mới nhất.

Với máy chủ DNS chạy Windows, Microsoft khuyến cáo kích hoạt RRL (Response Rate Limit – Hạn chế phản hồi) trên máy chủ DNS để khắc phục vấn đề.

2.4 Công cụ tấn công DDOS phổ biến hiện nay

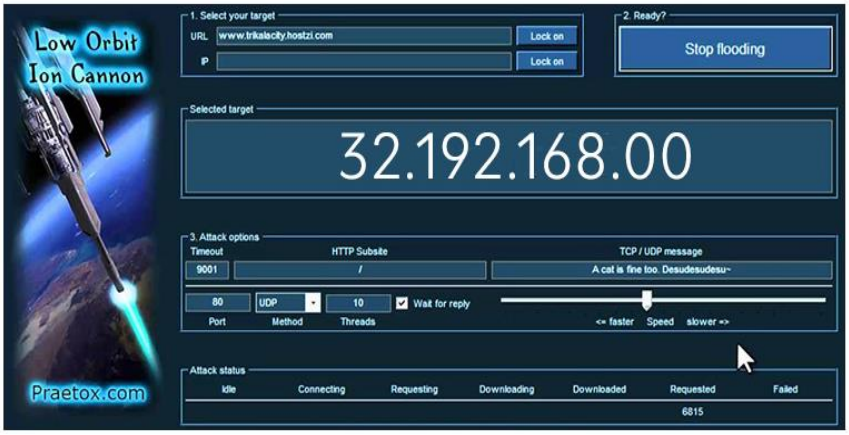
2.4.1 Công cụ tấn công LOIC (Low Orbit Ion Canon)

Đây là công cụ tấn công phổ biến và được cung cấp miễn phí trên mạng Internet. Công cụ này được sử dụng bởi những kẻ tấn công như nhóm Anonymous để tấn công hệ thống mạng của các công ty lớn trong năm 2013. Anonymous không chỉ sử dụng công cụ này mà còn dẫn dụ người sử dụng Internet vào mạng lưới IRC để lợi dụng tấn công DDOS.

Công cụ này có thể lợi dụng để một cá nhân riêng lẻ có thể tấn công máy chủ nhỏ. Đây là công cụ dễ dàng sử dụng cho những người mới bắt đầu. Kiểu tấn công được thực hiện bằng cách gửi các gói tin UDP, TCP hay các yêu cầu HTTP tới máy nạn nhân. Kẻ tấn công chỉ cần biết địa chỉ URL hay địa chỉ IP của máy chủ.

Công cụ này cũng có chế độ HIVEMIND, được sử dụng để điều khiển từ xa hệ thống LOIC để vận hành cuộc tấn công. Chức năng này được sử dụng để điều khiển những máy tính khác nằm trong hệ thống zombie. Công cụ này có thể được sử dụng cả hai chức năng tấn công DDOS và chống lại các cuộc tấn công DDOS đối với bất kỳ máy chủ hoặc trang mạng.

Nhược điểm là LOIC không ẩn địa chỉ IP. Nếu kẻ tấn công có kế hoạch sử dụng LOIC để tấn công, cần phải chú ý tới vấn đề này. Sử dụng proxy sẽ không giúp ích được nhiều vì proxy không phải là mục tiêu của máy chủ.



Công cụ tấn công LOIC

2.4.2 *Công cụ tấn công XOIC*

Công cụ thực hiện tấn công trên cơ sở địa chỉ IP và chọn cổng, giao thức để tấn công. XOIC được cho là mạnh hơn LOIC. XOIC được sử dụng dễ dàng để tấn công các trang mạng hoặc máy chủ. Công cụ được viết đầu tiên là kiểm tra phương thức. Sau đó đến dạng tấn công DDOS cơ bản. Cuối cùng là cách tấn công sử dụng TCP/HTTP/UDP/ ICMP. XOIC thường được sử dụng để tấn công các trang mạng, máy chủ nhỏ.

Công cụ tấn công XOIC

2.4.3 *Công cụ tấn công HULK (HTTP Unbearable Load King)*

HULK là một công cụ khá tinh vi, có khả năng tạo ra một khối lượng truy cập lớn làm "ngẽn" máy chủ. Công cụ này sử dụng nhiều kỹ thuật khác nhau để tránh bị phát hiện tấn công. Nó có thể tạo ra một danh sách agent, những agent này gửi các truy vấn ngẫu nhiên. HULK có khả năng giả mạo danh tính và vượt qua các bộ nhớ đệm để truy vấn trực tiếp vào kho dữ liệu của máy chủ. Một cuộc thử nghiệm HULK trên máy chủ web IIS 7, ram 4 gb. HULK đã "hạ gục" máy chủ trong vòng 1 phút.

2.4.4 *Công cụ tấn công DDOSIM – Layer 7 DDOS Simulator*

DDOSIM là một công cụ tấn công DDOS phổ biến. Nó được sử dụng cùng với một mạng lưới máy chủ zombie. Tất cả các máy chủ zombie này sẽ tạo ra các kết nối TCP đầy đủ đến máy mục tiêu. DDOSIM được viết bằng C++ và chạy trên các hệ thống Linux. Các tính năng chính của DDOSIM gồm:

- Giả lập một số zombie trong các cuộc tấn công
- Sử dụng địa chỉ IP ngẫu nhiên; Sử dụng kiểu tấn công kết nối TCP
- Tấn công lớp ứng dụng
- HTTP DDOS sử dụng các truy vấn hợp lệ
- HTTP DDOS sử dụng các truy vấn không hợp lệ
- SMTP DDOS
- Làm tràn kết nối TCP trên một cổng ngẫu nhiên.

2.4.5 Công cụ tấn công R-U-Dead-Yet

Tor's Hammer là công cụ được viết bằng Python. Công cụ này được chạy thông một mạng TOR và ẩn danh khi thực hiện các cuộc tấn công. Đây là công cụ thực sự hiệu quả và có khả năng làm tê liệt Apache hoặc IIS server trong vòng vài giây.

2.4.6 Công cụ tấn công PyLoris

PyLoris thường được sử dụng để kiểm tra các máy chủ. Nó có thể sử dụng để thực hiện các cuộc tấn công DDOS trên một số dịch vụ mạng. Công cụ này sử dụng proxy SOCKS và các kết nối SSL để thực hiện một cuộc tấn công. Nó có nhằm tới các mục tiêu là những giao thức khác nhau như: HTTP, FPT, SMTP, IMAP và Telnet. Phiên bản mới nhất của công cụ này đi kèm với một giao diện đơn giản và dễ sử dụng. Không giống như các công cụ tấn công DDOS, công cụ này có thể trực tiếp truy cập các dịch vụ.

2.4.7 Công cụ tấn công OWASP DOS HTTP POST

Đây là công cụ khá hiệu quả trong các cuộc tấn công DDOS. Ngoài ra, công cụ này còn sử dụng để kiểm tra các máy chủ web có khả năng chống lại các cuộc tấn công DDOS hay không. Bên cạnh đó, OWASP DOS HTTP POST có thể tạo nền cho các cuộc tấn công DDOS đối với các trang mạng.

2.4.8 Công cụ tấn công DAVOSET

DAVOSET là công cụ lợi dụng các lỗ hổng XML, kết hợp với việc tạo ra mạng lưới zombies để tấn công. Công cụ này thường xuyên cung cấp sẵn khoảng 170 zombie.

2.4.9 Công cụ tấn công GoldenEye HTTP

Đây là công cụ đơn giản nhưng khá hiệu quả trong các cuộc tấn công DDOS; được phát triển bằng Python. GoldenEye HTTP cũng được sử dụng để kiểm tra khả năng chống lại các cuộc tấn công DDOS.

KẾT LUẬN

Kết luận chung

- Đưa ra khái niệm và lý thuyết cơ bản về tấn công DDOS.
- Phân loại và phân tích về các kiểu tấn công DDOS.

Hướng phát triển

Nghiên cứu các vấn đề DDOS là những nghiên cứu động, liên tục. Kẻ tấn công luôn tìm cách đổi mới về hình thức và kỹ thuật để đối phương bất ngờ, không kịp đối phó. Trong khi, kỹ thuật phòng chống, chưa có những giải pháp thật sự hữu hiệu. Bài toán phòng chống là một trong những bài toán khó không chỉ đối với các tổ chức sử dụng Internet mà ngay cả đối với các quốc gia, tập đoàn lớn, đặc biệt khi DDOS có nguy cơ ngày càng phổ biến, trở thành một loại "vũ khí" đe dọa an ninh, kinh tế của mỗi quốc gia.

Tài liệu tham khảo

[1] Phyllis, J. (n.d.). A Survey: DDOS Attack on Internet of Things.

[2] AL-Musawi, B. Q. (n.d.). MITIGATING DoS/DDoS ATTACKS USING IPTABLES.

[3] Day, N. (n.d.). Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN.

[4] Sekar, V. (n.d.). Large-scale Automated DDoS detection System.

[5] Specht, S. M. (n.d.). Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures.

[6] Tzvetanov, K. (n.d.). DDoS Tutorial.

[7] Zaroo, P. (n.d.). A Survey of DDoS attacks and some DDoS defense mechanisms .

[8] DDoS HANDBOOK. (n.d.).

[9] Yadav, V. (n.d.). Detection techniques of DDoS attacks: A survey.

[10] Chakunta Venkata Guru Rao, Manoj Kumar Singh,Gubbala China Satyanarayana. (n.d.). A Survey on Defense Mechanisms countering DDoS Attacks in the Network.

[11] K. Munivara Prasad, A. Rama Mohan Reddy & K.Venugopal Rao. (n.d.). DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey .

Phân công công việc

1. Trần Cao Minh Bách
- Leader
- Tìm kiếm tài liệu
- Dựng lab
2. Vũ Thị Ánh
- Làm slide và báo cáo
3. Trần Thị Dung
- Làm slide và báo cáo