

**ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

NGUYỄN THÀNH HỮU

NGHIÊN CỨU VỀ DDOS VÀ GIẢI PHÁP NGĂN CHẶN

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội – 2014

**ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

NGUYỄN THÀNH HỮU

NGHIÊN CỨU VỀ DDOS VÀ GIẢI PHÁP NGĂN CHẶN

Ngành: Công nghệ thông tin

Chuyên ngành: Hệ thống thông tin

Mã số: 60480104

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. PHÙNG VĂN ỒN

Hà Nội – 2014

LỜI CAM ĐOAN

Tôi xin cam đoan những kết quả đạt được trong luận văn này là do tôi nghiên cứu, tổng hợp và thực hiện. Toàn bộ những điều được trình bày trong luận văn là của cá nhân hoặc được tham khảo và tổng hợp từ các nguồn tài liệu khác nhau. Tất cả các tài liệu tham khảo, tổng hợp đều được trích dẫn với nguồn gốc rõ ràng.

Tôi xin chịu hoàn toàn trách nhiệm về lời cam đoan của mình. Nếu có gì sai trái, tôi xin chịu mọi hình thức kỷ luật theo qui định.

Hà Nội, tháng 10 năm 2014

Học viên

Nguyễn Thành Hữu

LỜI CẢM ƠN

Tôi muốn bày tỏ lòng biết ơn sâu sắc tới những người đã giúp đỡ tôi trong quá trình làm luận văn, đặc biệt tôi xin cảm ơn TS Phan Văn Ôn, với lòng kiên trì, thầy đã chỉ bảo tôi chi tiết và cho tôi những lời nhận xét quý báu trong từng bước làm luận văn. Đồng thời tôi cũng xin gửi lời cảm ơn tới các thầy cô giáo khoa Công nghệ thông tin – Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã truyền đạt các kiến thức cho tôi trong suốt thời gian học tập và nghiên cứu vừa qua.

Tôi cũng xin chân thành cảm ơn cơ quan, bạn bè, đồng nghiệp, gia đình và những người thân đã cùng chia sẻ, giúp đỡ, động viên, tạo mọi điều kiện thuận lợi để tôi hoàn thành nhiệm vụ học tập và hoàn thành luận văn này.

Hà nội, tháng 10 năm 2014

Học viên

Nguyễn Thành Hữu

MỤC LỤC

LỜI CAM ĐOAN	3
LỜI CẢM ƠN	4
MỤC LỤC	5
DANH MỤC TỪ VIẾT TẮT	7
DANH MỤC HÌNH VẼ, BẢNG	8
MỞ ĐẦU	10
CHƯƠNG 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN	11
1. GIỚI THIỆU VỀ TẤN CÔNG TỪ CHỐI DỊCH VỤ - DDOS:	11
1.1. Khái niệm DDos:	11
1.2. Các giai đoạn của một cuộc tấn công DDos:	12
1.3. Phân loại tấn công từ chối dịch vụ phân tán:	12
1.4. Mạng BOTNET	15
1.4.1. Khái niệm mạng Botnet	15
1.4.2. Mạng Internet Relay Chat	15
1.4.3. Chương trình Bot và BotNet	16
1.4.4. Mạng IRC botnet	17
1.4.5. Các bước xây dựng mạng botnet	17
1.4.6. Mô hình tấn công DDoS	18
1.4.7. Mô hình tấn công Agent- Handler	19
1.4.8. Mô hình tấn công IRC- Based	21
CHƯƠNG 2: CÁC KỸ THUẬT TẤN CÔNG DDOS	23
2.1. Tấn công làm cạn kiệt băng thông (Band with Deleption):	23
2.1.1. Tấn công tràn băng thông (Flood attack):	23
2.1.1.1. Tấn công tràn băng thông bằng gói tin UDP:	24
2.1.1.2. Tấn công tràn băng thông bằng gói tin ICMP:	26
2.1.2. Tấn công khuếch đại (Amplification attack):	28
2.1.2.1. Tấn công kiểu Smuft:	30
2.1.2.2. Tấn công kiểu Fraggles:	31
2.2. Tấn công làm cạn kiệt tài nguyên (Resoure Deleption):	31
2.3. Các biến thể của tấn công DDos:	36
2.3.1. Tấn công kiểu Flash DDos	36
2.3.2. Tấn công kiểu DRDos:	37
2.3.3. Tấn công DDoS trên điện thoại di động	38
2.4. Một số công cụ tấn công DDoS phổ biến hiện nay:	38
CHƯƠNG 3: PHÒNG, CHỐNG CUỘC TẤN CÔNG DDOS	42
3.1. Phát hiện và ngăn chặn Agent (Detect and Prevent):	42
3.2. Phát hiện và vô hiệu hóa các Handler (detect and neutralize handler)	43

3.3. Phát hiện dấu hiệu của một cuộc tấn công DDos (Detect and prevent agent):	43
3.4. Làm suy giảm hoặc chặn cuộc tấn công DDos:	48
3.5. Chuyển hướng cuộc tấn công:.....	51
3.6. Giai đoạn sau tấn công:.....	54
3.7. Các giải pháp đơn đối với những cuộc tấn công DDos nhỏ:	54
CHƯƠNG 4: ĐỀ XUẤT GIẢI PHÁP PHÒNG CHỐNG DDOS	58
4.1. Tình hình liên quan tới DDos ở Việt Nam:	58
4.2. Giải pháp phòng chống DDos đang được thực hiện ở Việt Nam:	60
4.3. Giải pháp đề xuất của tác giả:	62
4.4. Nghiên cứu hệ thống Citrix NetScaler	64
4.4.1. Nguyên tắc xây dựng và khả năng của hệ thống Citrix NetScaler:	64
4.4.2. Chức năng của hệ thống Citrix NetScaler:	66
4.4.2.1. Duy trì tính sẵn sàng:	66
4.4.2.2. Tăng tốc độ ứng dụng:	67
4.4.2.3. Bảo mật ứng dụng:.....	67
4.4.2.4. Tối ưu hóa đầu cuối:	68
4.4.2.5. Tối ưu hóa TCP:	68
4.4.3. Cài đặt và chạy hệ thống Citrix NetScaler:	69
4.4.4. Đánh giá hệ thống:	74
4.5. Xây dựng kịch bản phòng, chống DDos:.....	75
4.5.1. Giai đoạn chuẩn bị:.....	75
4.5.2. Giai đoạn phát hiện, chống một cuộc tấn công DDos:	76
4.5.3. Giai đoạn sau tấn công:.....	78
KẾT LUẬN	79
TÀI LIỆU THAM KHẢO	80

DANH MỤC TỪ VIẾT TẮT

STT	Từ viết tắt	Tiếng Anh	Tiếng Việt
1	CGI	Common Gateway Interface	Giao diện cổng chung
2	DNS	Domain Name System	Hệ thống tên miền
3	FTP	File Transfer Protocol	Giao thức truyền file trên mạng
4	ICMP	Internet Control Message Protocol	Giao thức xử lý các thông báo trạng thái cho IP
5	IIS	Internet Information Server	Là một chương trình WebServer nổi tiếng của Microsoft
6	ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
7	LAN	Local Area Network	Mạng nội bộ
8	OS	Operation System	Hệ điều hành
9	OSI	Open System Interconnection	Mô hình định nghĩa các tiêu chuẩn liên kết giữa các thiết bị trong mạng
10	SMTP	Simple Message Transfer Protocol	Giao thức dùng để gửi thư thông qua một chương trình
11	SYN	Synchronous Idle Character	Ký tự đồng bộ hoá
12	TCP/IP	Transmission Control Protocol and Internet Protocol	Bộ giao thức liên mạng

DANH MỤC HÌNH VẼ, BẢNG

Hình 1.1 Mô hình tấn công DDoS	11
Hình 1.2 Sơ đồ phân loại DDoS attack theo mục đích tấn công.....	13
Hình 1.3 Mô hình mạng IRC.....	16
Hình 1.4 Sơ đồ cách hệ thống bị lây nhiễm và sử dụng Agobot	18
Hình 1.5 Sơ đồ mô hình tấn công DDoS	18
Hình 1.6 Kiến trúc mô hình tấn công Agent- Handler.....	19
Hình 1.7 Kiến trúc mô hình tấn công IRC- Based	21
Hình 2.1 Các kỹ thuật tấn công DDoS.....	23
Hình 2.2. Sơ đồ tấn công kiểu tràn băng thông.....	23
Hình 2.3 Các tầng trong giao thức TCP/IP	24
Hình 2.4 Cấu trúc gói tin UDP	25
Hình 2.5 Sơ đồ tấn công tràn UDP.....	26
Hình 2.6 Cấu trúc tổng quát của gói tin ICMP	27
Hình 2.7 Sơ đồ tấn công khuếch đại	28
Hình 2.8 Sơ đồ tấn công kiểu Smurf.....	30
Hình 2.9 Sơ đồ tấn công kiểu Fraggle.....	31
Hình 2.10 Sơ đồ hoạt động của TCP.....	32
Hình 2.11 Sơ đồ quá trình “bắt tay 3 bước”.....	34
Hình 2.12 Tấn công tràn SYN.....	35
Hình 2.13 Sơ đồ tấn công Flash DDoS	36
Hình 2.14 Công cụ tấn công LOIC	38
Hình 2.15 Công cụ tấn công XOIC.....	39
Hình 3.1 Phòng chống tấn công DDoS	42
Hình 3.2 Tỷ lệ phần trăm new IP với $\Delta_n=10s$	47
Hình 3.3 Thuật toán CUSUM khi lưu lượng mạng bình thường.....	47
Hình 3.4 Lưu lượng mạng đột biến.....	48
Hình 4.1 Số liệu về phát tán tin nhắn rác mã độc qua thư điện tử (tháng 8/2013)..	59
Hình 4.2 Minh họa tổng hợp yếu tố đảm bảo an toàn cho 02 thực thể ứng dụng và hệ thống mạng	64
Hình 4.3 Ứng dụng mạng và các thành phần liên quan	65
Hình 4.4 Mô hình bảo vệ theo luồng của hệ thống Citrix NetScaler.....	65
Hình 4.5 Kiến trúc dòng sản phẩm Citrix Netscaler:.....	69
Hình 4.6 Cài XenCenter	73
Hình 4.7 Màn hình đăng nhập hệ thống.....	74
Hình 4.8 Màn hình hệ thống	74

Hình 4.9 Công cụ AAA Application Traffic	76
Hình 4.10 Công cụ Monitoring	77
Hình 4.11 Hệ thống Citrix NetScaler.....	77
Hình 4.12 Cài đặt giới hạn tốc độ trong AppExpert	78
Hình 4.13 Phân tích các truy cập	78

MỞ ĐẦU

Ngày nay, mạng Internet đang phát triển và mở rộng trên phạm vi toàn thế giới. Các cổng thông tin điện tử, dịch vụ mạng có thể là sự sống còn của cá nhân, tổ chức. Việc những hệ thống đó bị quá tải, không truy cập được trong một khoảng thời gian có thể gây ra tổn thất không nhỏ. Từ vấn đề thực tế trên kiểu tấn công từ chối dịch vụ phân tán, DDos (*Distributed Denial Of Service*) đã xuất hiện rất sớm, những năm 90 của thế kỷ 20. Kiểu tấn công này làm cạn kiệt tài nguyên của hệ thống. Người quản trị, người sử dụng không thể truy cập được hệ thống thông tin.

Tấn công DDos bắt đầu được biết đến từ năm 1998, với chương trình Trinoo Distributed Denial of service được viết bởi Phifli. Từ đó cùng với sự phát triển không ngừng của Công nghệ thông tin, các kỹ thuật tấn công mới lần lượt ra đời, Ping of Death, Teardrop, Aland Attack, Winnuke, Smurf Attack, UDP/ICMP Flooding, TCP/SYN Flooding, Attack DNS... gần đây là kiểu tấn công DDos sử dụng công cụ #RefRef của nhóm Hacker Anonymous. Do vậy, tấn công DDos một kiểu tấn công không mới, nhưng vẫn luôn là nỗi lo lắng của các nhà quản trị mạng.

Trong những năm qua, không chỉ Việt Nam mà cả thế giới, các cuộc tấn công DDos liên tục diễn ra. Những cuộc tấn công này với nhiều mục đích khác nhau: kinh tế, cá nhân, thậm chí mang cả màu sắc chính trị (Trung Quốc – Mỹ, Trung Quốc – Việt Nam...). Do vậy, nghiên cứu DDos không bao giờ là cũ, mà luôn phải cập nhật cùng với các thiết bị, kỹ thuật công nghệ thông tin mới.

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

1. Các vấn đề chung về DDos;
2. Kỹ thuật tấn công DDos cơ bản và các kỹ thuật mới;
3. Phòng, chống một cuộc tấn công DDos;
4. Giải pháp phòng, chống DDos hiệu quả;
5. Đưa ra một kịch bản cụ thể để phòng chống một cuộc tấn công Ddos.

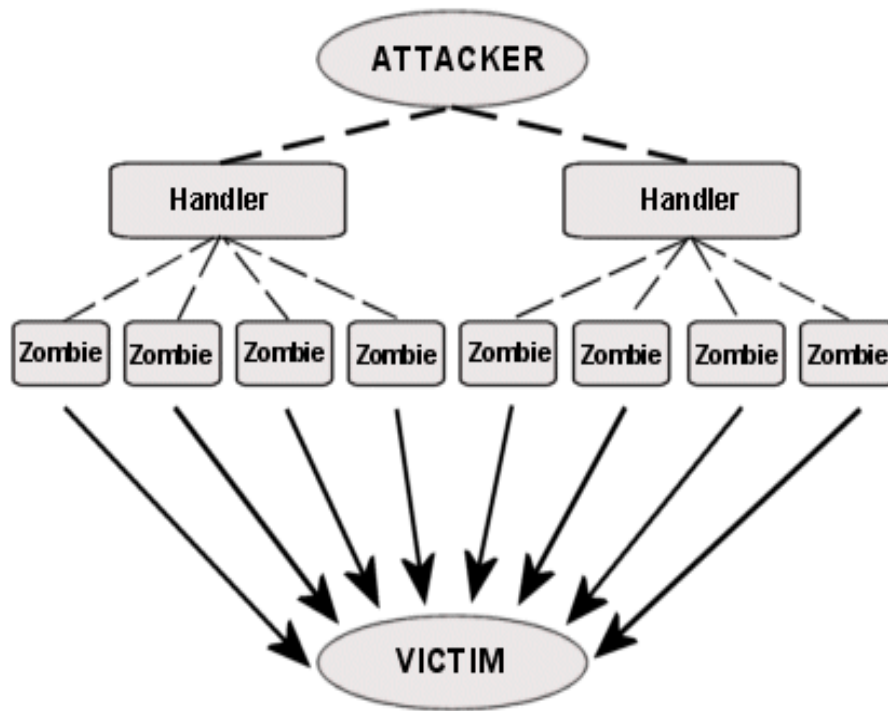
CHƯƠNG 1: CÁC NỘI DUNG CƠ BẢN CỦA TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN

1. GIỚI THIỆU VỀ TẤN CÔNG TỪ CHỐI DỊCH VỤ - DDOS:

1.1. 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*).

Architecture of a DDoS Attack



Hình 1.1 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.

1.2. Các giai đoạn của một cuộc tấn công DDos:

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).

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.

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

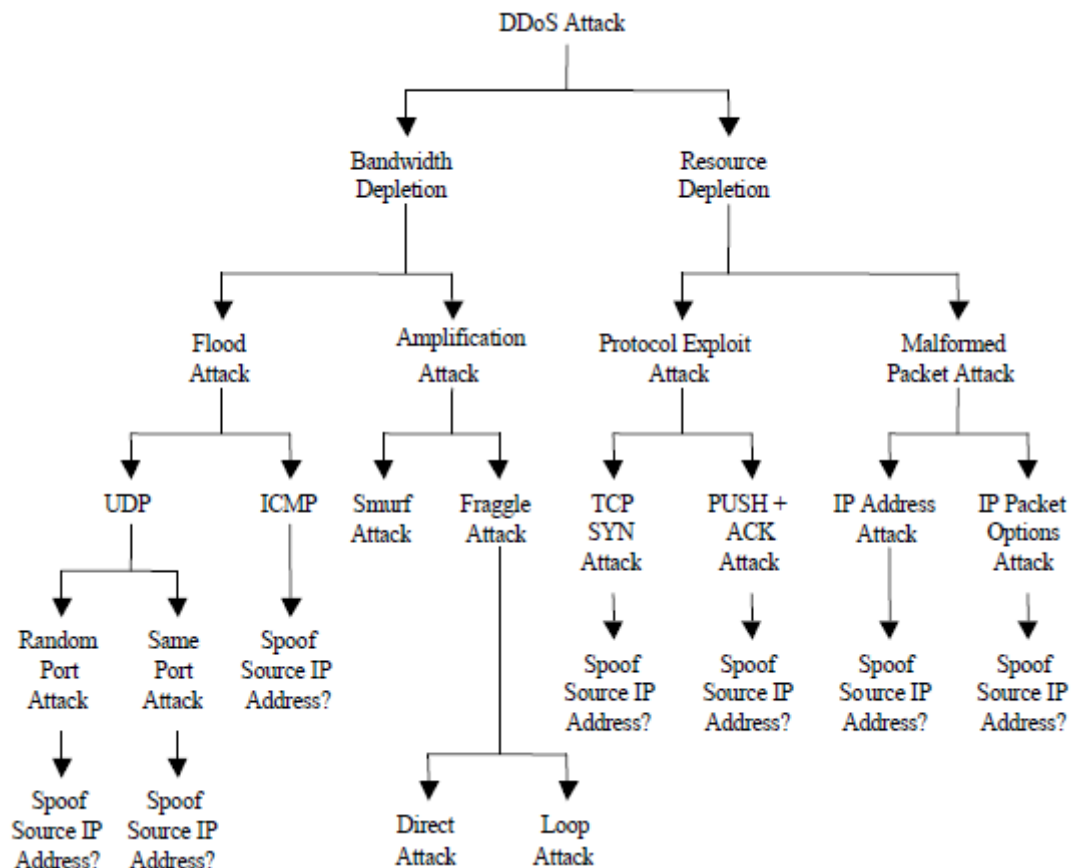
Đúng thời điểm đã định trước, hacker phát động lệnh tấn công từ máy của mình. Toàn bộ attack- network (có thể lên đến hàng ngàn, hàng vạn máy) đồng loạt tấn công mục tiêu, mục tiêu sẽ nhanh chóng bị cạn kiệt băng thông và không thể tiếp tục hoạt động.

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.

1.3. 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



Hình 1.2 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 bảng 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 nguy 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 nguy 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 đầy 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.

1.4. Mạng BOTNET

1.4.1. 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.

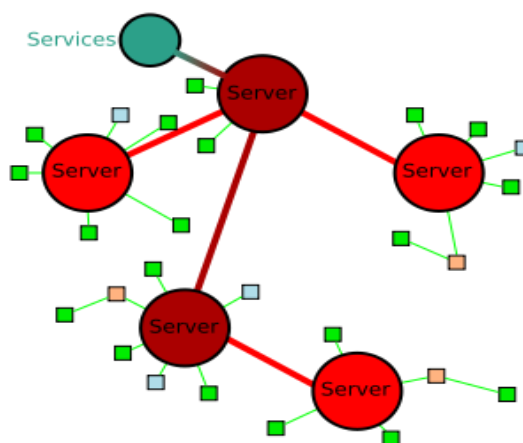
1.4.2. Mạng Internet Relay Chat

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 1.3 Mô hình mạng IRC

1.4.3. 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.

1.4.4. 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.

1.4.5. 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.

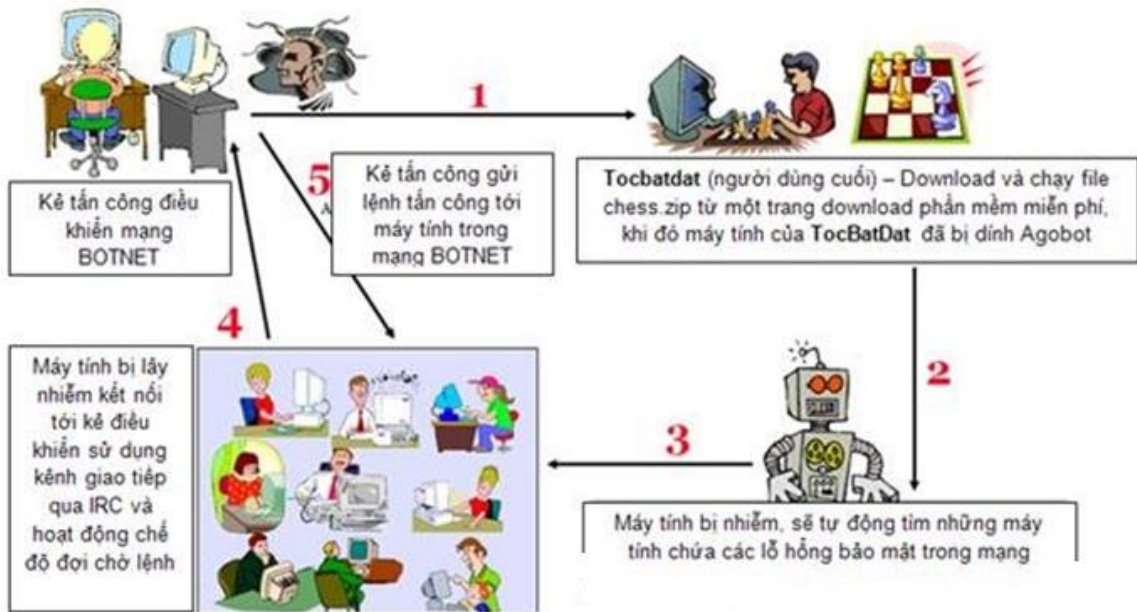
Bước 4: Điều khiển tấn công từ mạng botnet

- 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.

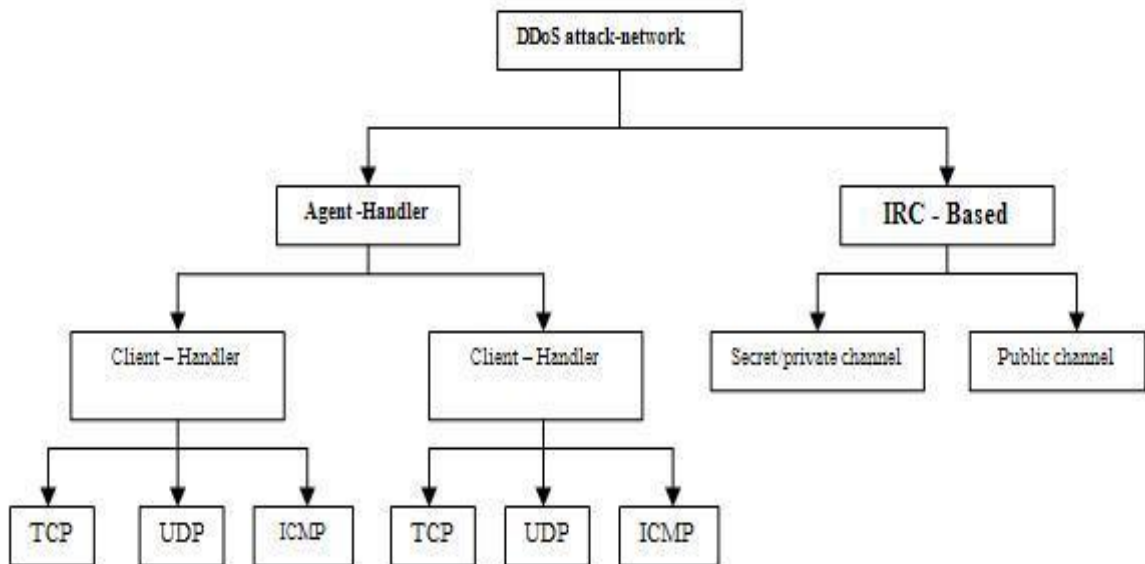
- Chạy những file khác trên hệ thống đáp ứng yêu cầu của kẻ tấn công.

- Chạy những chương trình DDoS tấn công hệ thống khác.



Hình 1.4 Sơ đồ cách hệ thống bị lây nhiễm và sử dụng Agobot

1.4.6. Mô hình tấn công DDoS



Hình 1.5 Sơ đồ mô hình tấn công DDoS

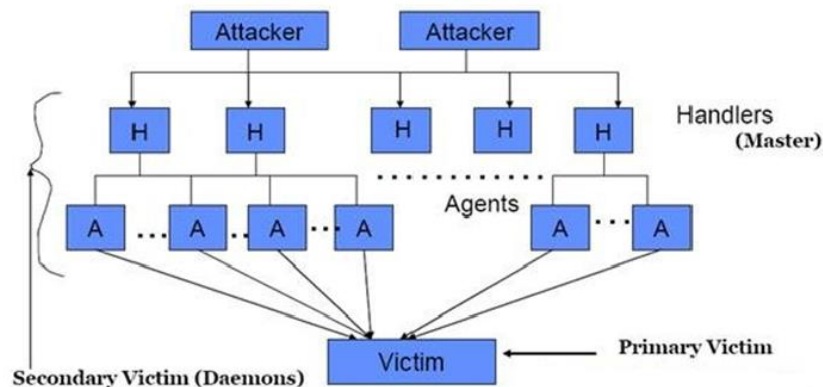
Tấn công DDoS có 2 mô hình chính:

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

1.4.7. Mô hình tấn công Agent- Handler

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.



Hình 1.6 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:

TẬP LỆNH CỦA HANDLER

Lệnh	Mô tả
Log On	Nhằm dùng để login 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	Yêu 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

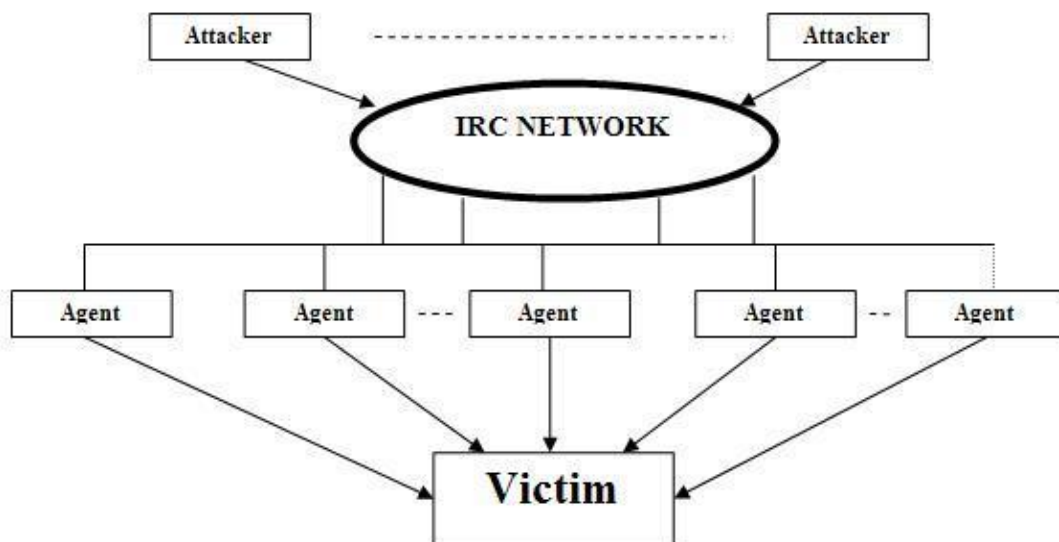
1.4.8. Mô hình tấn công IRC- Based

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.

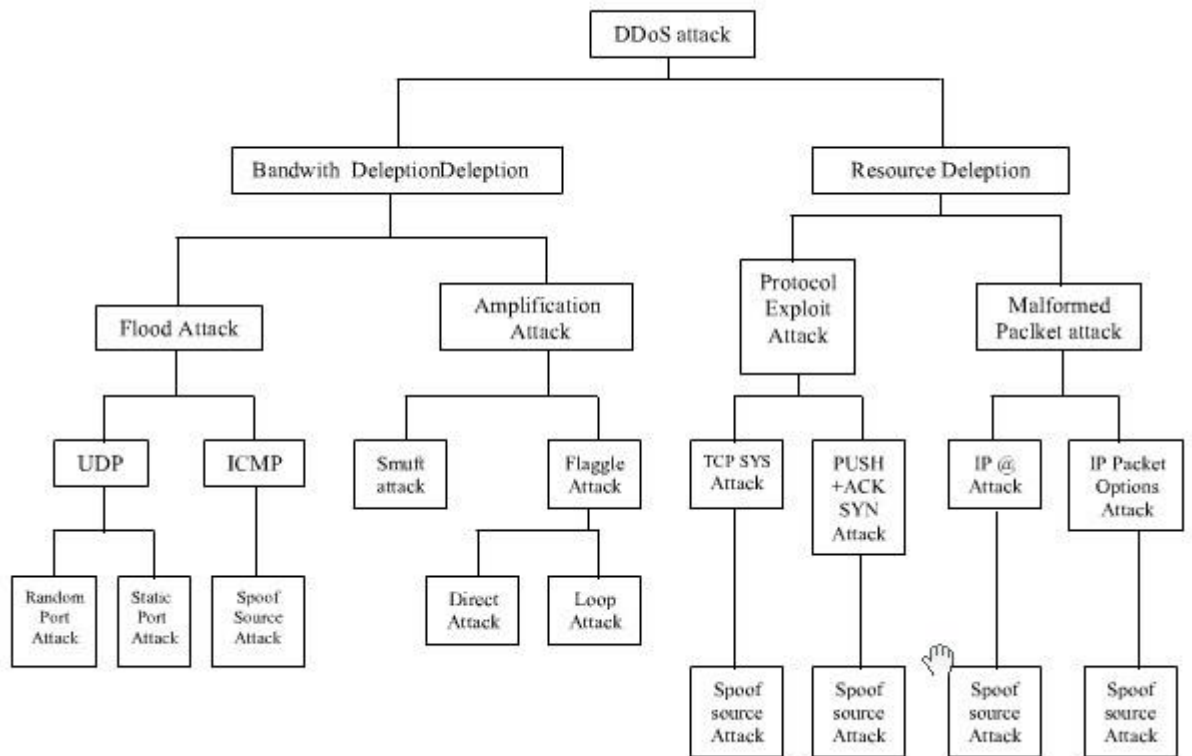


Hình 1.7 Kiến trúc mô hình tấn công IRC- Based

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

CHƯƠNG 2: CÁC KỸ THUẬT TẤN CÔNG DDOS

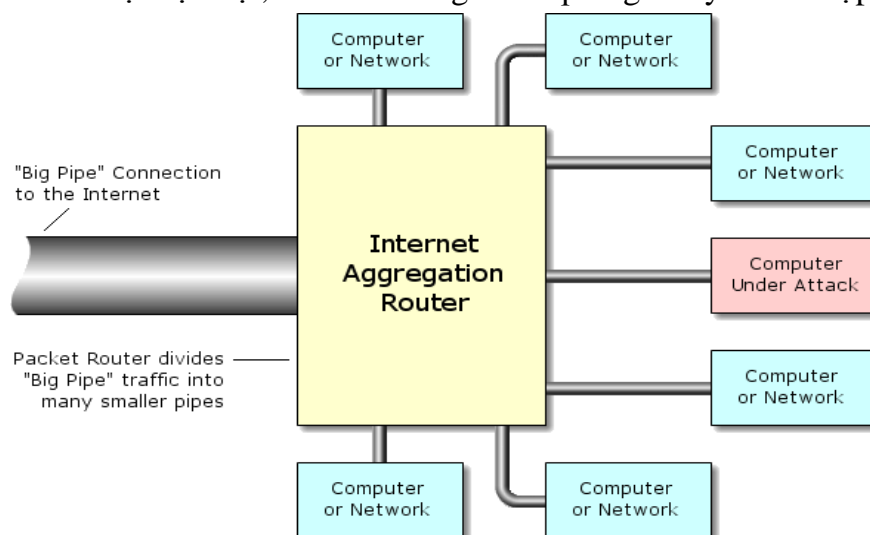


Hình 2.1 Các kỹ thuật tấn công DDoS

2.1. Tấn công làm cạn kiệt băng thông (Band with Deletion):

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

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

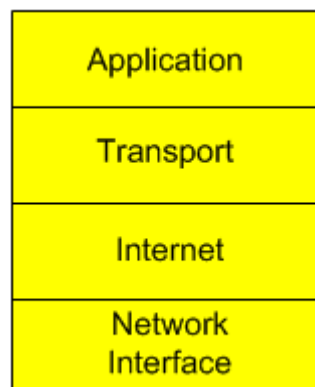
2.1.1.1. Tấn công tràn bằng thông bằng gói tin UDP:

Tương tự như TCP flood attack, 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.

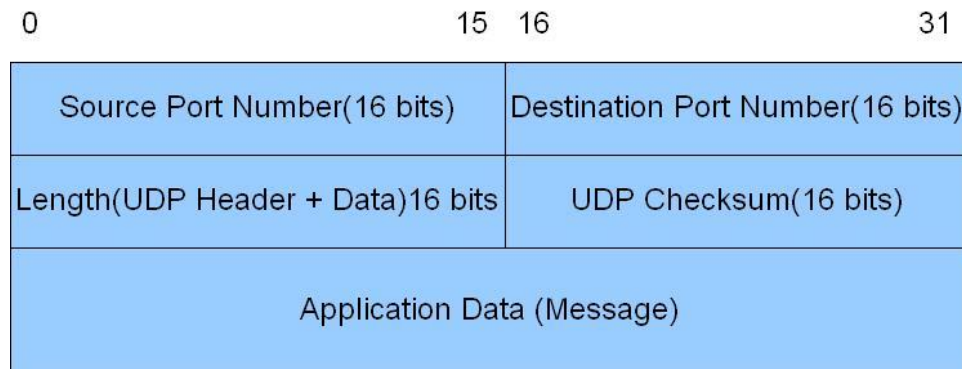
(2) **Cấu trúc gói UDP:** Trong bộ giao thức TCP/IP, UDP cung cấp một giao diện rất đơn giản giữa tầng Ứng dụng (Application) ở bên trên với tầng Mạng (Internet) ở phía dưới.



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

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 byte 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.

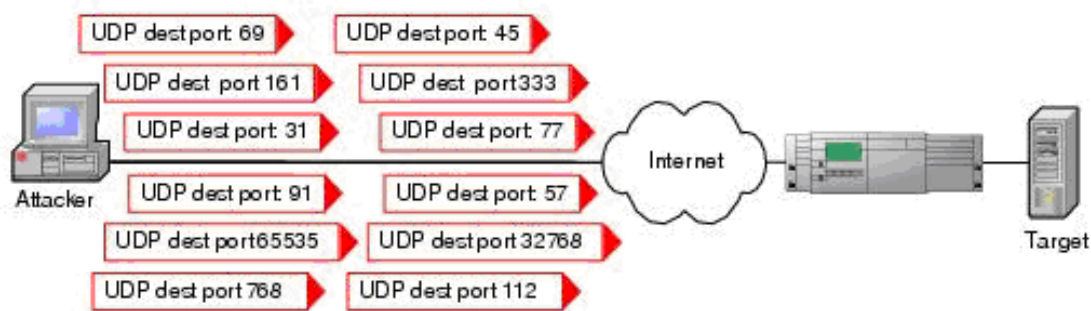
(3) Tìm số hiệu cổng trong UDP: UDP dùng cổng để cho phép các ứng dụng giao tiếp với nhau:

- 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.



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

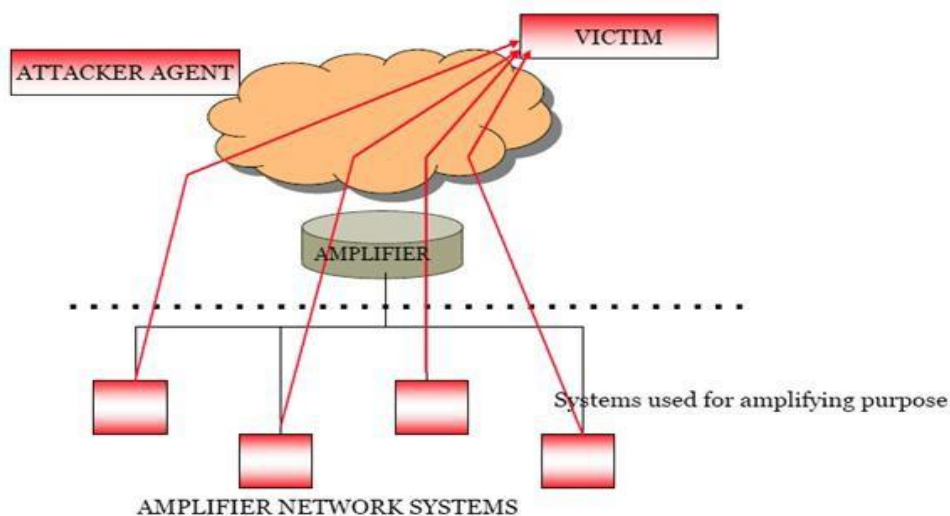
Phương thức tấn công: Tương tự phương thức UDP flood attack. Các Agent sẽ gửi một lượng lớn các ICMP_ECHO_REQUEST đến hệ thống mục tiêu, làm hệ thống này phải reply một lượng tương ứng packet để trả lời, dẫn đến nghẽn đường truyền và không thể đáp ứng những yêu cầu hợp lệ.

2.1.2. Tấn công 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 nhằm 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.



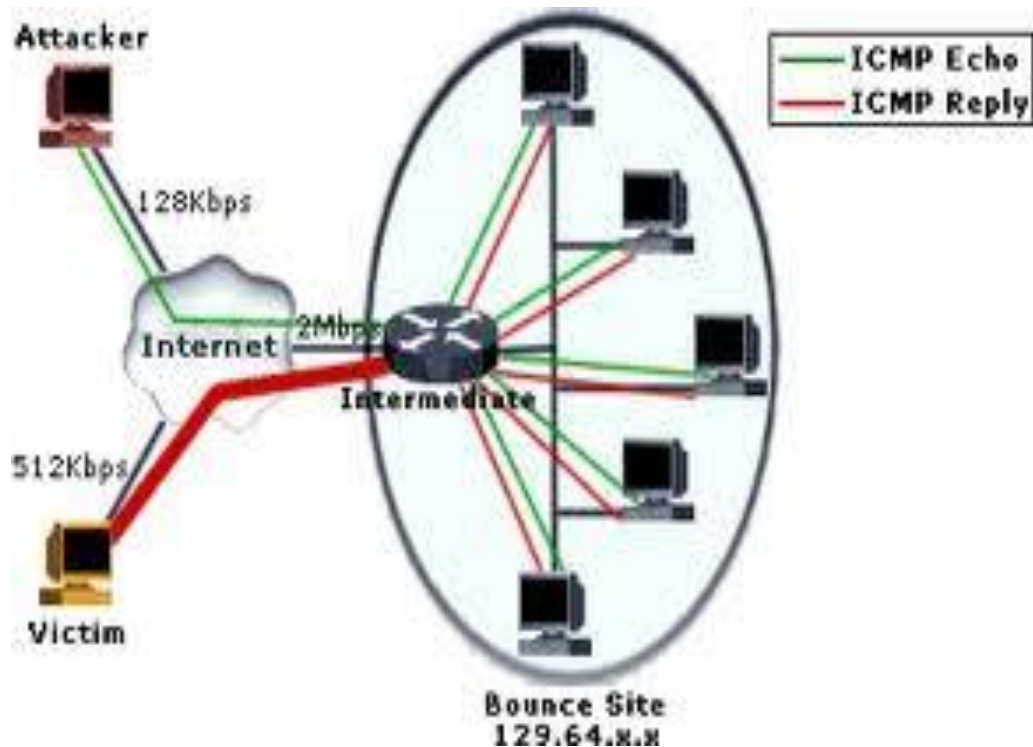
Hình 2.7 Sơ đồ tấn công khuếch đại

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 Fragggle (Fraggle attack).

2.1.2.1. Tấn công kiểu Smuft:



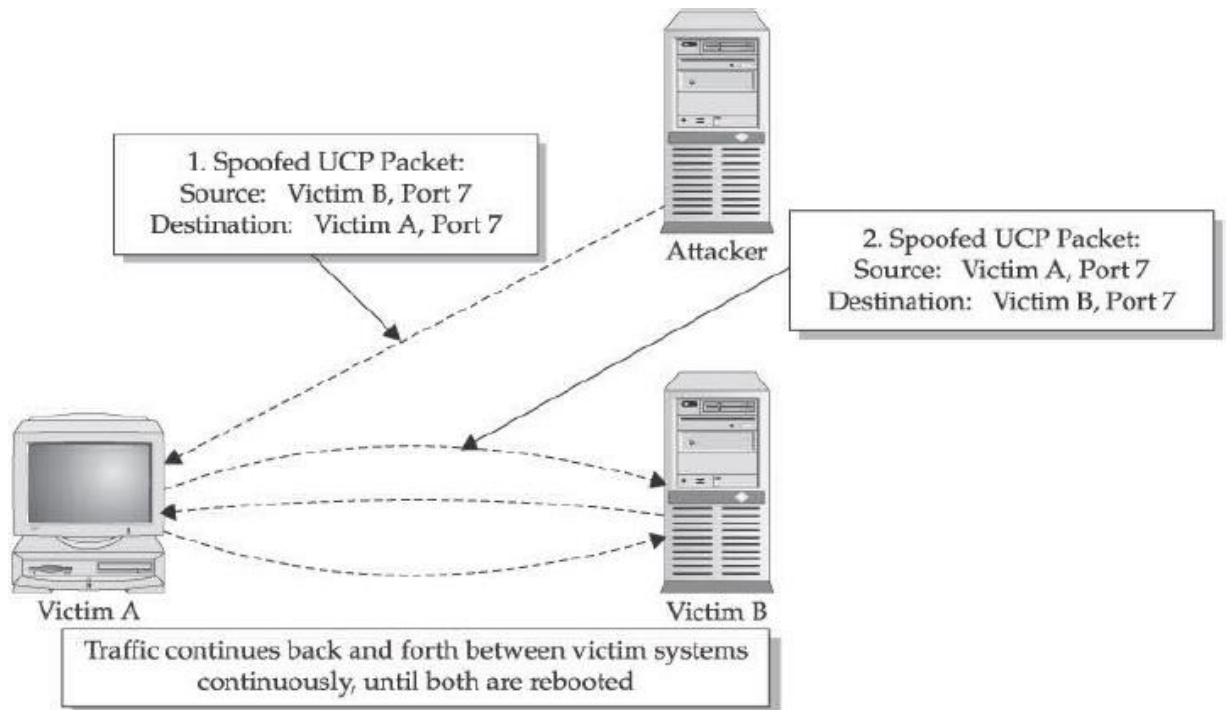
Hình 2.8 Sơ đồ tấn công kiểu Smuft

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. Tỷ 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 (Resource 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.

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
SYN-SENT
SYN-RECEIVED
ESTABLISHED
FIN-WAIT-1
FIN-WAIT-2
CLOSE-WAIT
CLOSING
LAST-ACK
TIME-WAIT

CLOSED

- **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:

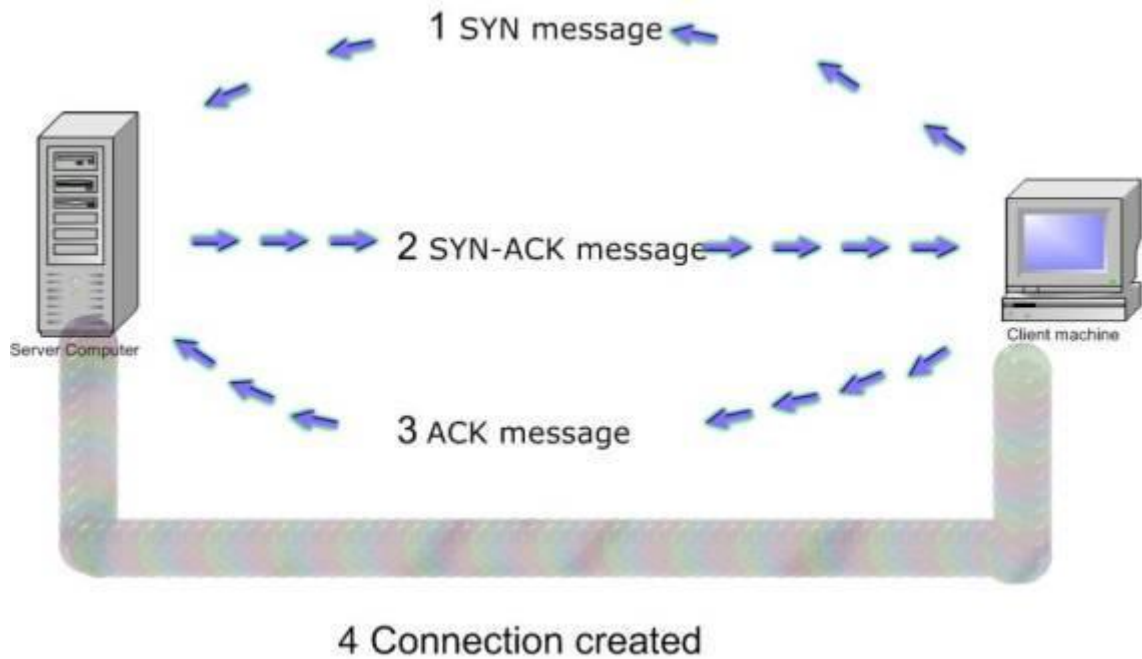
Để thiết lập một kết nối, TCP sử dụng một quy tắc gọi là *bắt tay ba bước* (three-way handshake). Trước khi client thử kết nối với một server, server phải đăng ký một cổng và mở cổng đó cho các kết nối, quá trình này được gọi là mở bị động. Một khi mở bị động đã được thiết lập thì một client có thể bắt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



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

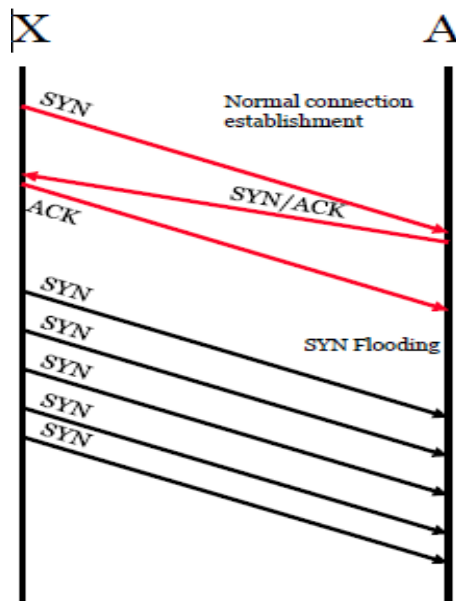
Trong điều kiện bình thường, gói tin SYN từ một cổng cụ thể trên hệ thống A đến một cổng cụ thể trên hệ thống B trong tình trạng LISTEN. Vào thời điểm này kết nối trên hệ thống B ở tình trạng SYN_RECEIVED. Vào giai đoạn này hệ thống B sẽ tìm cách gửi gói tin SYN/ACK về cho hệ thống A. Nếu mọi sự ổn thỏa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

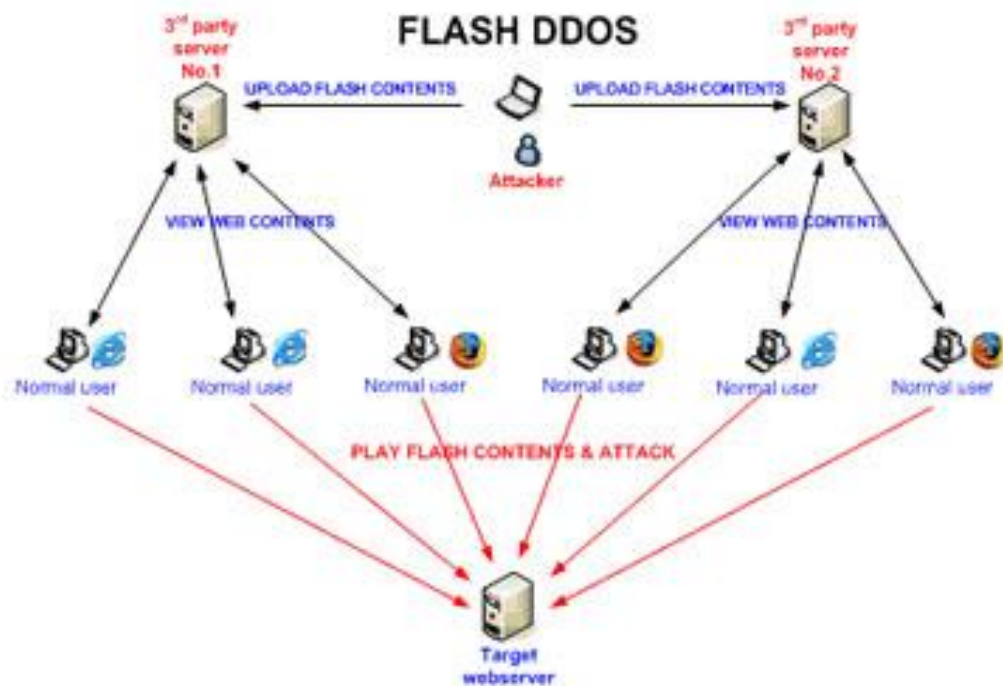
- Mạng lưới tấn công là mạng cố định và tấn công xảy ra đồng loạt nên vẫn có thể điều tra tìm ngược kẻ tấn công.

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 mà 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.

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 Flash DDoS

Hacker sẽ tải lên một trang web nào đó có nhiều người truy xuất một file flash (thường là các web đen hoặc các trang quảng cáo), người dùng truy xuất website này và bằng cách nào đó, vô tình hoặc có 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 xuất sẽ được gửi đến website mục tiêu. Mục tiêu bị tấn công từ chối dịch vụ.

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

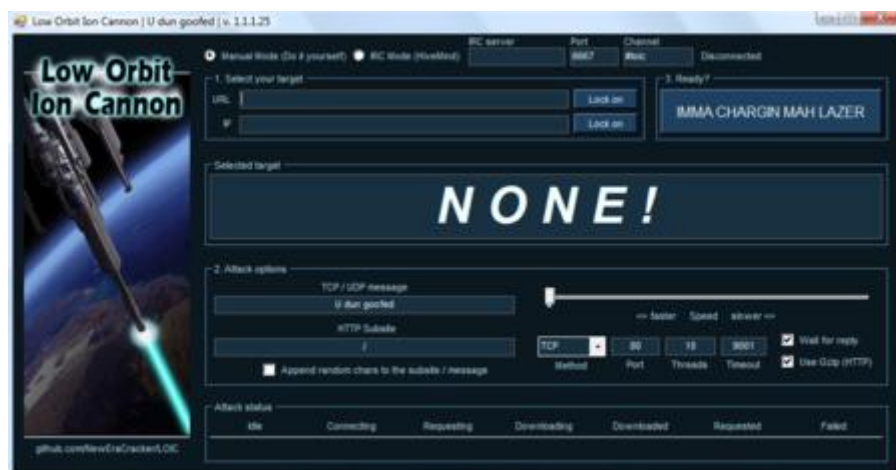
Tương tự với DDoS trên web, phương thức tấn công DDoS trên điện thoại di động cũng khiến các thuê bao liên tục phải nhận các cuộc gọi đến. Các thuê bao hợp lệ khác không thể gọi tới thuê bao bị tấn công vì máy luôn bận. Thuê bao nạn nhân cũng khó có thể thực hiện các cuộc gọi đi vì luôn có điện thoại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

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

❖ Công cụ tấn công LOIC (*Low Orbit Ion Canon*):



Hình 2.14 Công cụ tấn công LOIC

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

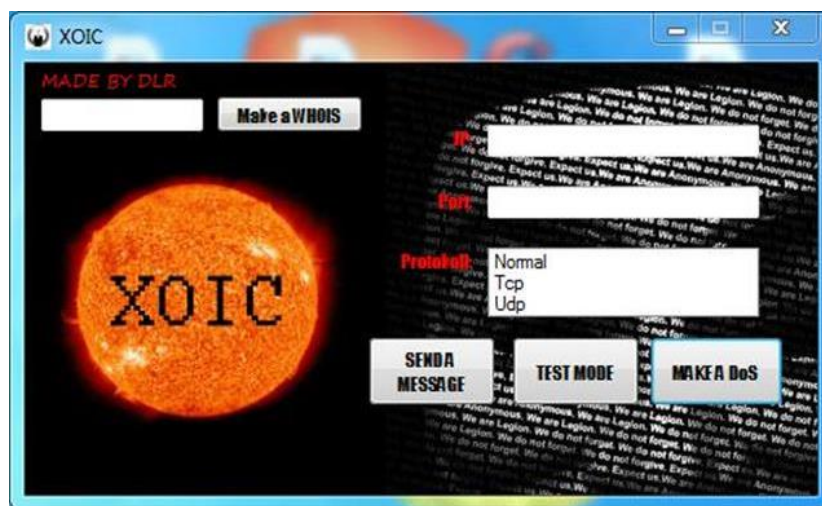
hệ thống mạng của các công ty lớn trong năm 2013. Anonymous không chỉ sử dụng công cụ này mà còn dẫn dụ người sử dụng Internet vào mạng lưới IRC để lợi dụng tấn công DDOS.

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 XOIC:*



Hình 2.15 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 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.

❖ *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.

❖ *Công cụ tấn công R-U-Dead-Yet:*

Công cụ R-U-Dead-Yet hay còn có tên gọi là Rudy. Công cụ này thực hiện một cuộc tấn công DDOS với một trường mẫu dài qua phương thức POST, đi kèm với giao diện điều khiển đơn tương tác. Nó sẽ phát hiện các mẫu URL và cho phép người dùng lựa chọn các dạng trường để sử dụng tấn công.

❖ *Công cụ tấn công Tor's hammer:*

Tor's Hammer là công cụ được viết bằng Python. Công cụ này được chạy thông qua 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.

❖ *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 nhắm tới các mục tiêu là những giao thức khác nhau như: HTTP, FTP, 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.

❖ *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.

❖ *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.

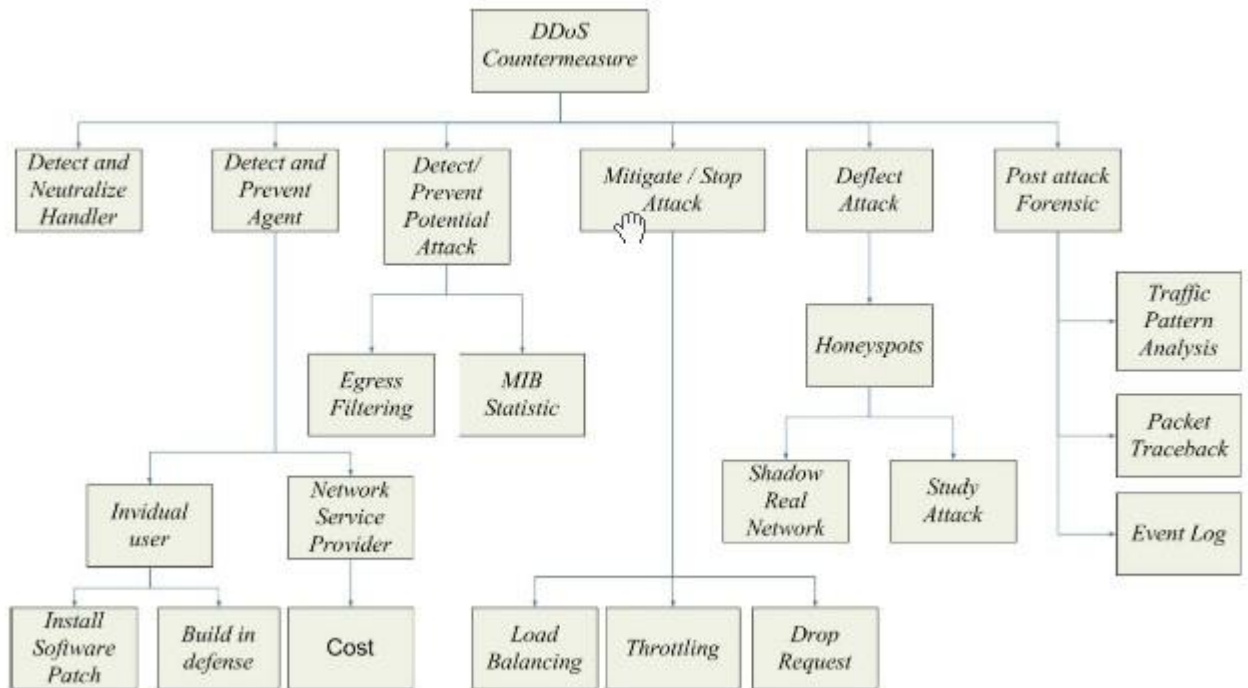
❖ *Công cụ tấn công GoldenEye HTTP:*

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.

CHƯƠNG 3: PHÒNG, CHỐNG CUỘC TẤN CÔNG DDOS

Như chương 1 và chương 2 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 sẽ nhằm vào hệ thống của ta. Do đó, trên cơ sở luận văn này tác giả đưa ra giải pháp chung nhất có thể chống lại nhiều kiểu tấn công DDOS. Giải pháp tổng thể 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 3.1 Phòng chống tấn công DDoS

3.1. Phát hiện và ngăn chặn Agent (Detect and Prevent):

Từ phía người sử dụng: 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. Tự kiểm tra sự hiện diện của Agent trên thiết bị. Đây là điều 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.

3.2. Phát hiện và vô hiệu hóa các Handler (detect and neutralize 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.

3.3. Phát hiện dấu hiệu của một cuộc tấn công DDOS (Detect and prevent agent):

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.

Đầu tiên định nghĩa lưu lượng của một địa chỉ IP là IP flow.

$S_i = \{s^i_1, s^i_2, \dots, s^i_n\}$ là tập hợp các địa chỉ IP hợp lệ truy cập trong ngày i . $|S_i| = n_i$.

$F^k = \{f_1, f_2, \dots, f_m\}$ là tập hợp các địa chỉ IP truy cập từ ngày 1 đến ngày k . $|F^k| = m$.

$A = \{a_1, a_2, a_3, \dots, a_x\}$ là tập hợp các địa chỉ IP truy cập trong một cuộc tấn công DDos

Như vậy sẽ có một nhóm các địa chỉ IP thường xuyên truy cập một các đều đặn. Khi một cuộc tấn công DDos sử dụng địa chỉ IP bất kì (random IP address), lưu lượng theo dõi trong k ngày như sau:

$$|S_1 \cup S_2 \cup S_3 \dots \cup S_k| < \sum_{i=1}^k n_i \ll |A|$$

Hiển nhiên, $F^k \subset (S_1 \cup S_2 \cup S_3 \dots \cup S_k)$.

Tiến hành thống kê và xây dựng một ngưỡng giới hạn để quyết định mức độ thường xuyên trong tập F .

$P_{\text{normal}} = |F \cap S_j| / |S_j|$: tỷ lệ phần trăm của một IP flow bình thường trong ngày j ($j > k$)

$P_{\text{DDos}} = |F \cap A| / |A|$: tỷ lệ phần trăm của một IP flow tấn công.

Định nghĩa IP address database (IAD) là tập hợp các địa chỉ IP đã xuất hiện thường xuyên trong một khoảng thời gian (có thể là 1 tháng).

Trong IAD, xây dựng 2 quy tắc để quyết định mức độ truy cập thường xuyên của một địa chỉ IP.

+ Thứ nhất: Số ngày nó đã truy cập

$p_1(d)$: tập hợp duy nhất các địa chỉ IP đã truy cập trong ít nhất d ngày.

$f_1(d)$: tỷ lệ phần trăm lưu lượng tốt khi sử dụng $p_1(d)$ trong IAD.

+ Thứ hai: số gói tin trên địa chỉ IP

$p_2(u)$: tập hợp duy nhất các địa chỉ IP có ít nhất u gói tin.

$f_2(u)$: tỷ lệ phần trăm lưu lượng tốt khi sử dụng $p_2(u)$ trong IAD

Như vậy nếu $|p_1(d)|$ và $|p_2(u)|$ nhỏ sẽ giảm được bộ nhớ yêu cầu để duy trì IAD, $|f_1(d)|$ và $|f_2(u)|$ lớn sẽ có nhiều địa chỉ IP trong cơ sở dữ liệu.

Trong thuật toán trên, có hai tham số được đưa ra. Đó là số ngày (d) và số gói tin trên địa chỉ IP (u). Hai tham số trên có thể được tùy chỉnh trong các điều kiện mạng khác nhau. Việc kết hợp hai quy tắc trên sẽ làm cho IAD hiệu quả hơn rất nhiều

$$F_c = p_1(d) \cap p_2(u)$$

Như vậy các địa chỉ IP thuộc tập F_c 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 cuộc 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 ($n=1,2,3,4,\dots$). Sau đó gán $\Delta_1=\Delta_2=\dots=\Delta_n$.

Gọi T_n là tập các địa chỉ IP vừa thiết lập và D_n là các địa chỉ IP trong IAD tại thời điểm Δ_n . $|T_n - T_n \cap D_n|$ sẽ là tập các địa chỉ IP mới trong khoảng thời gian Δ_n .

Ta có $X_n = |T_n - T_n \cap D_n| / T_n$: tỷ lệ phần trăm địa chỉ IP mới trên tổng số các địa chỉ IP trong khoảng thời gian Δn .

Đặt $Z = \{Z_n, n=1,2,3,\dots\}$ sao cho $Z_n = X_n - \beta$. Với $a = \alpha - \beta$

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

α là giá trị trung bình của $\{X_n\}$ trong quá trình lưu lượng bình thường

Do đó, khi lưu lượng mạng bình thường tất cả các giá trị của Z_n đều âm

Khi có một cuộc tấn công xảy ra, giá trị của Z_n 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 Z_n và được thiết lập bởi công thức sau:

$$y_n = (y_{n-1} + Z_n)^+ \text{ và } y_0 = 0$$

Với $x^+ = x$ nếu $x > 0$ và $x^+ = 0$ nếu $x \leq 0$

Trong đó $n \geq k$. Trường hợp không bị tấn công giá trị của $y_{n-1} + Z_n$ âm.

Hàm quyết định có cuộc tấn công hay không được định nghĩa như sau:

$$d_N(y_n) = 0 \text{ nếu } y_n \leq N \text{ và } d_N(y_n) = 1 \text{ nếu } y_n > N$$

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

Ta có công thức:

$$\rho_N = (\tau_N - m)^+ / N \quad (1)$$

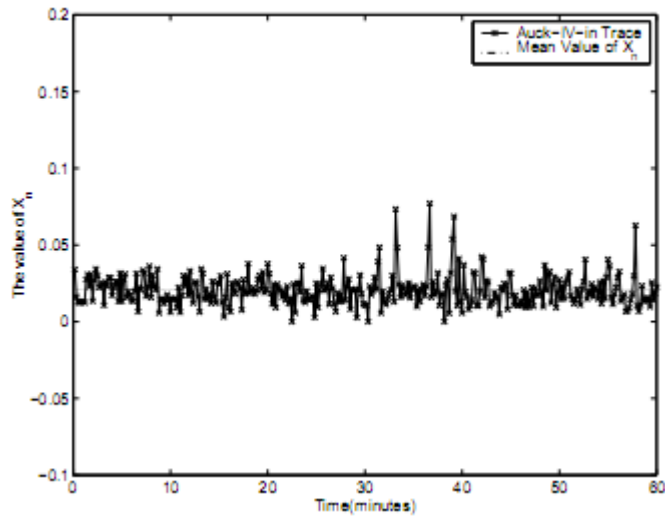
$$\rho_N \rightarrow \gamma = \frac{1}{h - |a|} \quad (2)$$

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 $|a|=0.05$

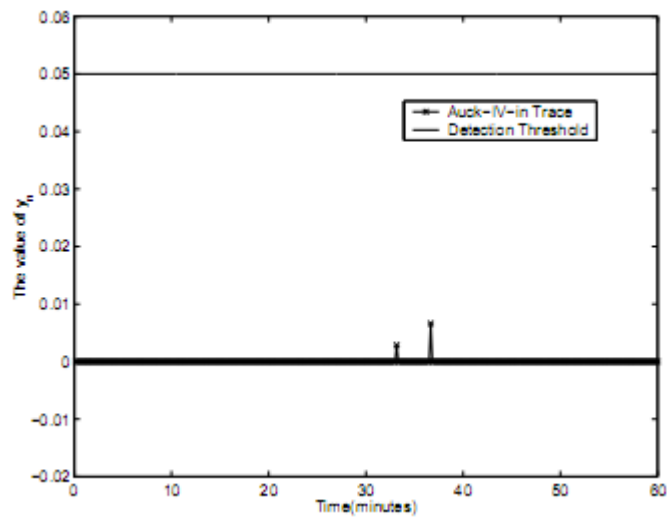
Trong công thức (1) chọn vị trí nhỏ nhất khi cuộc tấn công bắt đầu. Do vậy $\tau_N = m+1$.

Vì vậy từ (1) và (2) hoàn toàn có thể tính được giá trị của ngưỡng N.

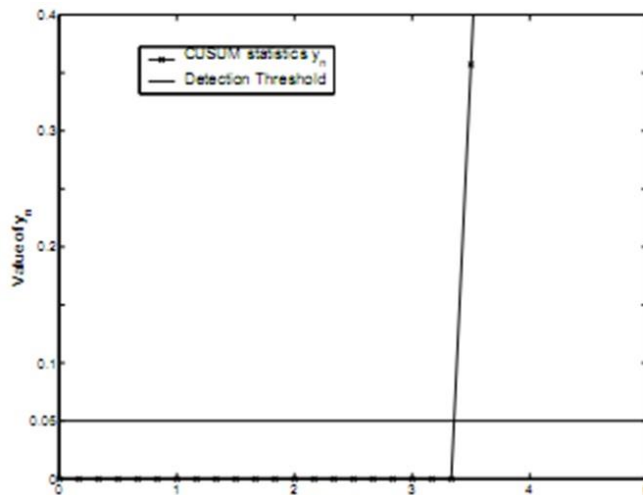
Lược đồ minh họa thí nghiệm chạy thuật toán khi phát hiện cuộc tấn công



Hình 3.2 Tỷ lệ phần trăm new IP với $\Delta_n=10s$



Hình 3.3 Thuật toán CUSUM khi lưu lượng mạng bình thường



Hình 3.4 Lưu lượng mạng đột biến

3.4. Làm suy giảm hoặc chặn cuộc tấn công DDOS:

Việc làm suy giảm hay chặn cuộc tấn công DDOS thường sử dụng các kỹ thuật sau:

- **Load banlancing:** Thiết lập kiến trúc cân bằng tải cho các server trọng điểm sẽ làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDOS. Tuy nhiên, điều này không có ý nghĩa thực tiễn vì quy mô của cuộc tấn công là không giới hạn.

Máy chủ là trung tâm của các mạng máy tính. Nếu máy chủ mạng hỏng, hoạt động của cả hệ thống sẽ bị ngưng trệ. Để giải quyết vấn đề này, có thể dùng một nhóm máy chủ cùng thực hiện một chức năng dưới sự điều khiển của một công cụ phối tải. Đây là giải pháp cân bằng tải. Về cơ bản nguyên tắc cân bằng tải xuất phát từ những quan điểm kỹ thuật khá tương đồng. Một kỹ thuật cân bằng tải điển hình là RRDNS (Round Robin DNS). Với giải pháp này, nếu một máy chủ trong nhóm bị lỗi, RRDNS sẽ vẫn tiếp tục gửi tải cho máy chủ đó cho đến khi người quản trị mạng phát hiện lỗi và tách máy chủ ra khỏi danh sách địa chỉ DNS. Do đó sẽ gây ra sự đứt quãng dịch vụ. Các thuật toán cân bằng tĩnh như: Round Robin, Weighted Round Robin và các thuật toán cân bằng động như: Least Connection, Weighted Least Connection, Optimized Weighted Round Robin, Optimized Weighted least Connection sẽ giúp cho kỹ thuật này ngày càng trở nên hoàn thiện mặc dù nhược điểm vốn có như tạo điểm lỗi đơn và vấn đề nút cổ chai do sử dụng điều phối tập trung (centralized dispatcher). Ngoài khả năng áp dụng với Web server, kỹ thuật này còn có thể áp dụng với các hệ server ứng dụng khác. Cân bằng tải không chỉ làm nhiệm vụ phân phối tải cho các máy chủ mà còn cung cấp cơ chế đảm bảo hệ thống máy chủ luôn khả dụng trước các client. Cân bằng tải không có yêu cầu đặc biệt gì về phần cứng, bất cứ máy tính nào hợp chuẩn đều có thể được sử dụng làm máy chủ. Chi phí triển khai nhờ đó giảm đáng kể. Kiến trúc phần mềm phân tán của cân bằng tải cho phép cung cấp hiệu năng và tính khả dụng của kỹ thuật này ở mức cao nhất.

Cân bằng tải cần thiết sử dụng trong các hệ thống của: doanh nghiệp, nhà cung cấp dịch vụ ISP, trung tâm xử lý dữ liệu, cơ quan Chính phủ, phòng thí nghiệm, trường đại học và học viện nghiên cứu ...

Việc chia tải có thể thực hiện bằng nhiều phương pháp, hình thức khác nhau hoặc sử dụng kết hợp giữa chúng.

Một giải pháp cân bằng tải có các chức năng sau:

- Can thiệp vào luồng dữ liệu mạng tới một điểm đích;
- Chia luồng dữ liệu đó thành các yêu cầu đơn lẻ và quyết định máy chủ nào sẽ xử lý những yêu cầu đó;
- Duy trì việc theo dõi các máy chủ đang hoạt động, đảm bảo rằng các máy chủ này vẫn đang đáp ứng các yêu cầu đến. Nếu máy chủ nào không hoạt động đúng chức năng, máy chủ đó bắt buộc phải đưa ra khỏi danh sách xoay vòng;
- Cung cấp sự đa dạng bằng việc tận dụng nhiều hơn một đơn vị trong các tình huống fail – over (fail – over là khả năng tự động chuyển qua các thiết bị dự phòng khi gặp tình huống hỏng hoặc trục trặc. Việc thực thi này được thực hiện mà không có sự can thiệp của con người cũng như không có bất cứ sự cảnh báo nào).
- Cung cấp sự phân phối dựa trên sự hiểu biết về nội dung, như: đọc URL, can thiệp vào cookies hoặc truyền XML ...

Server Load Balancers: Load Balancer là một thiết bị phân phối tải giữa các máy tính với nhau và các máy tính này sẽ xuất hiện chỉ như một máy tính duy nhất.

VIPs: Virtual IP (VIP) là một dạng thể hiện của cân bằng tải. Mỗi VIP sử dụng một địa chỉ công khai IP. Bên cạnh đó, một cổng TCP hay UDP sẽ đi kèm với một VIP như cổng TCP 80 được dành cho luồng dữ liệu của web. Một VIP sẽ có ít nhất một máy chủ thực sự được gán địa chỉ IP đó và máy chủ này sẽ làm nhiệm vụ phân phối luồng dữ liệu được chuyển đến. Thường sẽ có vài máy chủ và VIP sẽ trải đều luồng dữ liệu đến cho các máy chủ bằng cách sử dụng các ma trận hoặc các phương thức được mô tả trong phần “Active – Active Scenario” sau đây.

Các máy chủ (server): Máy chủ chạy một dịch vụ được chia sẻ tải giữa các dịch vụ khác. Máy chủ thường được ám chỉ tới các máy chủ HTTP, mặc dù các máy chủ khác hoặc ngay cả những dịch vụ khác có liên quan. Một máy chủ thường có một địa chỉ IP và một cổng TCP/UDP gắn liền với nó và không có địa chỉ IP công khai (điều này còn phụ thuộc vào topo của mạng).

Nhóm (group): Dùng để chỉ một nhóm các máy chủ được cân bằng tải. Các thuật toán như “farm”, “server farm” có cùng một ý nghĩa với thuật ngữ này.

Cấp độ người dùng truy nhập (User – Access Levels): Là một nhóm các quyền được gán cho một người dùng nào đó khi đăng nhập vào một thiết bị cân bằng tải. Không chỉ những nhà cung cấp thiết bị khác nhau cung cấp những cấp độ truy nhập khác nhau, mà hầu hết các dịch vụ cũng sẽ có những cách thức truy nhập dựa trên tài khoản người dùng. Một phương thức phổ biến khác là cách thức truy cập cấp độ người dùng được dùng trong các hệ thống Unix.

+ Read – only: Cấp độ truy cập chỉ đọc, không cho phép bất kỳ một thay đổi nào được thực hiện. Một người dùng có quyền chỉ đọc, chỉ có thể xem cấu hình ... nhưng không thể thực hiện được bất kỳ một thay đổi nào cả. Một tài khoản như thế được sử dụng để xem các thông kê hiệu suất hoạt động của thiết bị. Truy nhập chỉ đọc thường là cấp độ truy cập đầu tiên của một người dùng khi đăng nhập vào hệ thống trước khi thay đổi sang các chế độ với quyền truy cập cao hơn.

+ Superer: Superuser là cấp độ truy cập cho phép người dùng có đầy đủ quyền điều khiển hệ thống. Superuser có thể thêm các tài khoản khác, xóa file, cấu hình lại hệ thống với bất kỳ tham số nào.

+ Các cấp độ khác: Rất nhiều sản phẩm cung cấp thêm một vài cấp độ người dùng trung gian ở giữa hai cấp độ trên, có những quyền giới hạn trên hệ thống.

Giải pháp dự phòng:

Trong giải pháp dự phòng, tồn tại một quan hệ là active – standby. Một thiết bị, hay còn gọi là thiết bị đang hoạt động thực hiện một vài hoặc đầy đủ các chức năng chính, trong khi đó thiết bị dự phòng sẽ đợi để thực hiện những chức năng này. Mỗi quan hệ này cũng có thể được gọi là một quan hệ master/slave.

Trong những tình huống nhất định, cả hai thiết bị sẽ là chủ trong một vài chức năng làm phục vụ trong một vài chức năng, nhằm phân tán tải. Cũng trong một vài tình huống khác, cả hai thiết bị đều là chủ của tất cả các chức năng được chia sẻ giữa hai thiết bị. Quan hệ này còn được gọi là quan hệ active – active.

Hoạt động của hệ thống cân bằng tải được mô tả như sau:

Khi có một gói tin được gửi đến các máy chủ đều nhận được gói tin này. Nhưng gói tin chỉ được xử lý bởi một máy chủ nhất định. Các máy chủ trong nhóm sẽ đồng thời đáp ứng các yêu cầu khác nhau của client, dù một client có thể đưa ra nhiều yêu cầu. Ví dụ: một trình duyệt web cần rất nhiều hình ảnh trên một trang web được lưu trữ tại nhiều host khác nhau trong một nhóm máy chủ. Với kỹ thuật cân bằng tải, quá trình xử lý và thời gian đáp ứng client sẽ nhanh hơn nhiều.

Mỗi máy chủ trong nhóm có thể định ra mức tải mà nó sẽ xử lý hoạt tải có thể phân phối một cách đồng đều giữa các host. Nhờ sử dụng việc phân phối tải này, mỗi server sẽ lựa chọn và xử lý một phần tải của host. Tải do các client gửi đến được phân

phối sao cho mỗi server nhận được số lượng các yêu cầu theo đúng phân tải đã định của nó. Sự cân bằng tải này có thể điều chỉnh tự động khi các host tham gia vào hoặc rời khỏi nhóm. Đối với các ứng dụng như web server, có rất nhiều client và thời gian mà các yêu cầu của client tồn tại tương đối ngắn, khả năng của kỹ thuật này nhằm phân phối tải thông qua ánh xạ thống kê sẽ giúp cân bằng một cách hiệu quả các tải và cung cấp khả năng đáp ứng nhanh khi nhóm server có thay đổi.

Các server trong nhóm cân bằng tải phát đi một bản tin đặc biệt thông báo trạng thái hoạt động của nó (gọi là heartbeat message) tới các host khác trong nhóm đồng thời nghe bản tin này từ các host khác. Nếu một server trong nhóm gặp trục trặc, các host khác sẽ điều chỉnh và tái phân phối lại tải để duy trì liên tục các dịch vụ cho client. Trong phần lớn các trường hợp, phần mềm client thường tự động kết nối lại và người sử dụng chỉ cảm thấy trễ một vài giây khi nhận được đáp ứng trả lời.

- **Throttling:** Thiết lập cơ chế điều tiết trên router, quy định một khoảng tải hợp lý mà server bên trong có thể xử lý được. Phương pháp này cũng có thể được dùng để ngăn chặn khả năng DDOS, không cho người sử dụng truy cập dịch vụ. Hạn chế của kỹ thuật này là không phân biệt được giữa truy cập hợp pháp và bất hợp pháp. Truy cập bất hợp pháp với mục đích tấn công DDOS vẫn có thể xâm nhập vào mạng dịch vụ nhưng với số lượng hữu hạn.

- **Drop request:** Thiết lập cơ chế drop request nếu nó vi phạm một số quy định như: Thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gây deadlock. Kỹ thuật này triệt tiêu khả năng làm cạn kiệt năng lực hệ thống, tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống và cân nhắc khi sử dụng.

3.5. Chuyển hướng cuộc tấn công:

Honeypots: Honeypots là một hệ thống được thiết kế nhằm đánh lừa kẻ tấn công. Thay vì tấn công vào hệ thống chính, kẻ tấn công lại tấn công vào hệ thống giả được “giăng bẫy”. Trên Honeypots được thiết kế các cơ chế giám sát và báo động. Honeypots sẽ ghi nhận chi tiết mọi động thái của kẻ tấn công trên hệ thống. Nếu kẻ tấn công cài đặt Agent hay Handler lên Honeypots thì khả năng bị triệt tiêu toàn bộ cuộc tấn công là rất cao.

Các loại hình Honeypots:

Gồm hai loại chính: Tương tác thấp và tương tác cao

- + Tương tác thấp (Low Interaction): Mô phỏng giả lập các dịch vụ, ứng dụng và hệ điều hành. Mức độ rủi ro thấp, dễ triển khai và bảo dưỡng nhưng bị giới hạn về dịch vụ.

+ Tương tác cao (High Interaction): Là các dịch vụ, ứng dụng và hệ điều hành thực. Mức độ thông tin thu thập được cao. Nhưng rủi ro cao và tốn thời gian để vận hành và bảo dưỡng.

Có các loại Honeypots sau:

BackOfficer Friendly (BOF):

Một loại hình Honeypots tương tác thấp rất dễ vận hành và cấu hình có thể hoạt động trên bất kỳ phiên bản nào của Windows và Unix nhưng chỉ tương tác được với một số dịch vụ đơn giản như FTP, Telnet, SMTP ...

Specter:

Cũng là loại hình Honeypots tương tác thấp nhưng khả năng tương tác tốt hơn BOF, giả lập trên 14 cổng, có thể cảnh báo và quản lý từ xa. Tuy nhiên giống BOF, Specter bị giới hạn dịch vụ và không linh hoạt.

Honeyd:

- Honeyd lắng nghe trên tất cả các cổng TCP và UDP, những dịch vụ mô phỏng được thiết kế với mục đích ngăn chặn và ghi lại những cuộc tấn công, tương tác với kẻ tấn công với vai trò là nạn nhân.

- Honeyd có thể cùng lúc giả lập nhiều hệ điều hành khác nhau.

- Hiện nay, Honeyd có nhiều phiên bản và có thể mô phỏng được khoảng 473 hệ điều hành.

- Honeyd là loại hình Honeypots tương tác thấp có nhiều ưu điểm. Tuy nhiên Honeyd có nhược điểm là không thể cung cấp một hệ điều hành thật để tương tác với tin tặc và không có cơ chế cảnh báo khi phát hiện hệ thống bị xâm nhập hay gặp nguy hiểm.

Honeynet:

- Honeynet là hình thức Honeypots tương tác cao. Khác với các Honeypots, Honeynet là một hệ thống thật, hoàn toàn giống một mạng làm việc bình thường. Honeynet cung cấp hệ thống ứng dụng và các dịch vụ thật.

- Quan trọng nhất khi xây dựng một Honeynet chính là Honeywall. Honeywall là gateway ở giữa Honeypots và mạng bên ngoài. Bỏ hoạt động ở tầng 2 như là Bridged. Các luồng dữ liệu khi vào và ra từ Honeypots để phải đi qua Honeywall.

Các chức năng của Honeynet:

Bất kỳ một hệ thống Honeynet nào cũng phải thực hiện được ba điều kiện: Kiểm soát dữ liệu, bắt dữ liệu và phân tích chúng.

- **Kiểm soát dữ liệu:**

+ Có thể hiểu là mở cánh cửa cho hacker đi vào, cho phép xâm nhập honeynet nhưng lại đóng cửa ra, ngăn không cho hacker phát tán những đoạn mã độc hại ra mạng làm việc bên ngoài và Internet.

Honeynet thế hệ thứ III sử dụng ba cách kiểm soát dữ liệu.

+ Đếm số kết nối từ honeynet ra ngoài: nếu lớn hơn mức cho phép thì sẽ cấm kết nối.

+ Sử dụng Snort – inline: đây là một phần mềm mã nguồn mở phát triển lên từ Snort làm việc như một hệ thống ngăn chặn xâm nhập (IPS) dựa trên cơ sở dữ liệu về các hình thức tấn công thu thập được từ trước để ra quyết định.

+ Kiểm soát băng thông

- Bắt dữ liệu:

Đây là mục đích chính của tất cả các loại hình Honeynet – thu thập nhiều nhất thông tin về tấn công theo nhiều mức: các hoạt động của mạng, các hoạt động ứng dụng, các hoạt động của hệ thống.

Honeynet thế hệ 3 sử dụng Sebek để bắt dữ liệu. Đây là một kernel ẩn đặt tại các máy Honeypots và server là honeywall gateway.

Khi kẻ tấn công xâm nhập vào hệ thống và tương tác với một Honeypots. Tất cả các hoạt động của hacker này để được bí mật chuyển về sebek server thu thập và xử lý.

- Phân tích dữ liệu:

Phân tích dựa trên giao diện walleye của Honeywall hoặc bằng Ethereal.

Kế hoạch triển khai một Honeypots:

Để triển khai một Honeypots cần có một quá trình xử lý kỹ thuật tốt cùng với việc thực hiện đúng kế hoạch sẽ giúp triển khai thành công hệ thống.

Danh sách dưới đây đưa ra các bước để thực hiện:

+ Xác nhận Honeypots là được cho phép tạo dựng trong môi trường hệ thống đó.

+ Xác định mục tiêu Honeypots. Tại sao lại muốn chạy một Honeypots.

+ Dùng nó để nghiên cứu hay bảo vệ hệ thống tổ chức máy tính.

+ Xác định vai trò con người trong việc tạo ra và duy trì một Honeypots. Có chuyên môn kỹ thuật để triển khai một cách chính xác và duy trì một Honeypots không? Có phần mềm và phần cứng để triển khai chưa? Thời gian hàng ngày mất để duy trì và phân tích dữ liệu như thế nào? Tiếp tục thảo luận, nghiên cứu để theo kịp những Honeypots mới và khai thác một cách hiệu quả.

- + Các loại Honeypots sẽ triển khai là nghiên cứu hoặc sản phẩm thực hay ảo.
- + Xác định cài đặt cấu hình thiết bị mạng cần thiết để tạo ra Honeypots. Kế hoạch và cấu hình một số thành phần hỗ trợ Honeypots và tool (cảnh báo, đăng nhập, giám sát, quản lý ...).
- + Thu thập các thiết lập của việc giám sát, đăng nhập và các tool phân tích hợp pháp.
- + Triển khai kế hoạch phục hồi lại. Làm thế nào để phục hồi hệ thống Honeypots nguyên bản sau khi nó được khai thác sử dụng dẫn tới việc bị hư hại.
- + Triển khai Honeypots và các thành phần hỗ trợ, kiểm tra việc triển khai, đánh giá các công cụ phát hiện xâm nhập, thử nghiệm xem hệ thống Honeypots hoạt động tốt không.
- + Phân tích các kết quả và tìm ra những thiếu sót. Tinh chỉnh các hệ thống Honeypots dựa trên các bài đã được học và nghiên cứu. Lặp lại các bước cần thiết.

3.6. Giai đoạn sau tấn công:

Sau cuộc tấn công người quản trị hệ thống bị tấn công cần tìm ra các “lỗ hổng” bảo mật, xác định danh tính, cách thức, mục đích của kẻ tấn công. Trong giai đoạn này thông thường thực hiện các công việc sau:

Traffic Pattern Analysis: Phân tích các truy cập theo thời gian được hệ thống lưu lại. Quá trình phân tích này rất có ích cho việc tinh chỉnh lại các hệ thống Load Balancing và Throttling. Ngoài ra các dữ liệu này còn giúp quản trị mạng điều chỉnh lại các quy tắc kiểm soát truy cập ra vào mạng.

Packet Traceback: Bằng cách dùng kỹ thuật Traceback ta có thể truy ngược lại vị trí của kẻ tấn công. Từ kỹ thuật Traceback còn phát hiện khả năng Block Traceback từ kẻ tấn công.

Bevent Logs: Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể tìm ra nhiều chứng cứ xác định danh tính kẻ tấn công.

3.7. Các giải pháp đơn đối với những cuộc tấn công DDOS nhỏ:

Các cuộc tấn công đơn giản nhỏ lẻ thường được tiến hành dưới các dạng sau: **Sử dụng iframe, Sử dụng trang web “ác ý”**.

Với các cuộc tấn công này có thể sử dụng cách phòng chống trực tiếp ngay trên website.

(1) Chống iframe.

Đây là phương pháp được xem là thô sơ nhất. Kẻ tấn công sẽ mượn 1 website có lượt truy cập lớn nào đó chèn các iframe hướng về website cần đánh rồi cho chạy lệnh refresh (tải lại) nhiều lần hoặc họ viết sẵn 1 tập tin flash với công dụng tương tự rồi đặt lên website và khi người dùng truy cập vào website này thì họ vô tình bắt đắ đã trở thành người tấn công website kia.

Với hình thức tấn công kiểu như thế này bạn hoàn toàn có thể chống lại bằng cách chèn 1 đoạn mã Javascript chống chèn iframe từ các website khác đến website của bạn.

```
<script language="JavaScript">  
if (top.location != self.location)  
{top.location = self.location}  
</script>
```

(2) Chống tải lại trang web có ác ý:

Một hình thức tấn công khác nữa là dùng phím F5 liên tục có chủ ý, hoặc dùng một phần mềm được lập trình sẵn với công dụng tương tự (tải lại trang web liên tục sau những khoảng thời gian định sẵn) của một nhóm người làm cho trang web của bạn tải lại (reload) liên tục. Việc này có thể làm tổn băng thông của trang web hoặc làm trang web chạy chậm vì những kết nối ảo.

Với cách thức tấn công này thì nếu dùng cách một để chống coi như là vô ích. Nếu bạn bị tấn công như thế này thì bạn hãy thiết lập tập tin .htaccess với nội dung:

```
RewriteEngine on  
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?domain.com [NC]  
RewriteRule !antiddos.phtml  
http://www.domain.com/antiddos.phtml?%{REQUEST_URI} [QSA]
```

Sau đó tạo thêm một tập tin antiddos.phtml có nội dung

```
<?  
$text = $HTTP_SERVER_VARS['QUERY_STRING'];  
$text = preg_replace("#php\&#si", 'php?', $text);
```

```
echo('<center><a href=http://www.domain.com/?'. $text.'><font color=red size=5
face=Monotype>[CLICK HERE TO ENTER]</font></a></center>');
?>
```

Sau đó bạn upload 2 tập tin này lên thư mục gốc của website. Như vậy là mỗi khi truy cập vào website, nếu lần đầu tiên thì sẽ có thông báo yêu cầu nhấn chuột thì bạn mới vào được website và ở các lần sau sẽ không có và các phần mềm DDOS được lập trình sẽ bị chặn lại ở bước click chuột để vào trang web ở lần truy cập đầu tiên nên việc tải lại trang web chỉ đơn thuần là 1 trang HTML nhỏ không ảnh hưởng nhiều đến hệ thống.

Chú ý: Là cách này chỉ áp dụng cho website đang sử dụng server chạy trên nền Linux.

(3) Giới hạn số kết nối website tại một thời điểm

Khi một khách truy cập vào website thì sẽ tạo ra một truy vấn kết nối với cơ sở dữ liệu (CSDL) lấy thông tin và trả về thông qua hiển thị của website. Mỗi máy chủ sẽ có phép bao nhiêu truy vấn kết nối là hạn định và khi vượt quá hạn mức này thì việc truy cập sẽ khó khăn hoặc không thể truy xuất được. Các tin tặc lợi dụng vào điều này để tạo ra các truy cập ảo, kết nối ảo thông qua proxy hay chuyên nghiệp hơn là mạng botnet nhằm đánh sập trang web và phá hỏng CSDL website. Để hạn chế điều này ta có thể chủ động giới hạn số kết nối truy vấn tin (lượt truy cập) cùng một thời điểm.

Ta thêm dòng đoạn mã sau vào trang chủ của website.

```
function server_busy($numer) {
    if (THIS_IS == 'WEBSITE' && PHP_OS == 'Linux' and @file_exists (
'/proc/loadavg' ) and $filestuff = @file_get_contents ( '/proc/loadavg' )) {
        $loadavg = explode ( ' ', $filestuff );
        if (trim ( $loadavg [0] ) > $numer) {
            print '<meta http-equiv="content-type" content="text/html; charset=UTF-
8" />';
            print 'Lượng truy cập đang quá tải, mời bạn quay lại sau vài phút.';
            exit ( 0 );
        }
    }
}

$srv = server_busy ( 1000 ); // 1000 là số người truy cập tại 1 thời điểm
```


Đoạn mã trên có ý nghĩa cho phép 1000 người online trên website tại một thời điểm. Nếu vượt qua số 1000 thì khách truy cập sẽ nhận được thông báo: Lượng truy cập đang quá tải. Mời bạn quay lại sau vài phút.

Chú ý: Đoạn mã này áp dụng cho ngôn ngữ lập trình PHP.

CHƯƠNG 4: ĐỀ XUẤT GIẢI PHÁP PHÒNG CHỐNG DDOS

4.1. 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.

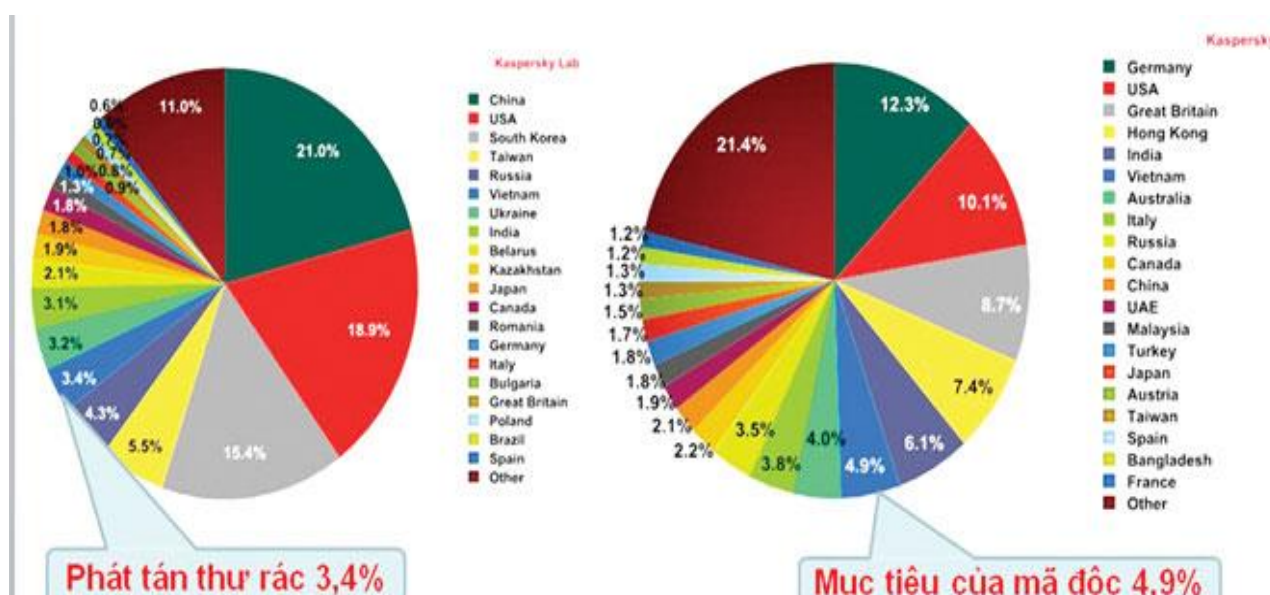
Tình hình ATTT và botnet tại Việt Nam

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 4.1 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, Phishing, Click Fraud.

Tháng 6-7/2013, 3 tờ báo điện tử lớn tại Việt Nam đã bị tấn công DDoS, làm ngưng trệ hoạt động. Đây là loạt tấn công DDoS có chủ đích với quy mô lớn, được chia làm 4 đợt liên tiếp nhằm vô hiệu hóa sự ứng phó của các đối tượng bị tấn công và các cơ quan liên quan.

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.

4.2. Giải pháp phòng chống DDOS đang được thực hiện ở Việt Nam:

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 trễ 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 được 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.

4.3. Giải pháp đề xuất của tác giả:

Tấn công DDoS là một thuật ngữ khái quát cho một loạt các kiểu tấn công, được thực hiện bằng nhiều cách, nhiều hướng làm cho tài nguyên của hệ thống cạn kiệt. Các cuộc tấn công có thể dựa trên nhiều nền tảng. Dù các cuộc tấn công này không gây hại cho hệ thống mục tiêu về dữ liệu, nhưng có thể tổn hại về danh tiếng, tài chính. Để chống lại các cuộc tấn công này, có thể nói cách tốt nhất đó là cần sự chuẩn bị trước để không bị động, bất ngờ.

Tác giả xin đưa ra 9 giải pháp sử dụng tổng hợp để ngăn chặn, chống lại các cuộc tấn công DDoS:

1. Xây dựng một danh sách kiểm tra các truy cập để phát hiện các truy cập bất thường. Duy trì hệ thống tường lửa trong các nhóm mạng, các nhà cung cấp dịch vụ và thiết lập kênh liên lạc giữa các nhóm mạng hay nhà cung cấp dịch vụ này. Trên cơ sở đó thiết lập một quy trình kiểm tra và phối hợp xử lý khi phát hiện các cuộc tấn công DDoS.

2. IPS và các nhà cung cấp máy chủ có thể cung cấp các dịch vụ được cài đặt các yếu tố hạn chế những cuộc tấn công DDoS; giám sát chi tiết về luồng dữ liệu ở cấp ISP để cảnh báo về cuộc tấn công.

3. Xác định mức độ ưu tiên cho các tính năng của những dịch vụ cung cấp. Điều này giúp nhân viên quản trị có thể tắt hoặc chặn những tính năng này khi cần thiết để hạn chế ảnh hưởng của một cuộc tấn công DDoS.

4. Đảm bảo để những hệ thống quan trọng có đủ khả năng chịu được một cuộc tấn công DDoS.

5. Xây dựng sơ đồ mạng, chi tiết các cơ sở hạ tầng từ đó giúp xác định các điểm yếu bị tấn công và có hướng đối phó.

6. Thiết lập cấu hình cho hệ thống mạng, hệ điều hành và các ứng dụng cần chú ý vô hiệu hóa các dịch vụ và ứng dụng không cần thiết; nghiên cứu đưa IPSec và Secure DNS vào sử dụng.

7. Tạo một danh sách để kiểm tra các IP không có thật, từ đó phát hiện và chặn các truy cập từ những IP này.

8. Sử dụng các dịch vụ kiểm tra bộ định tuyến để sàng lọc các truy cập, làm yếu các cuộc tấn công DDoS, như: sử dụng tường lửa trạng thái.

9. Sử dụng các hệ thống riêng hay công cộng; tạo các máy chủ đơn chức năng như: HTTP, FTP, DNS để tăng sức mạnh của hệ thống.

Bên cạnh các biện pháp kỹ thuật nêu trên, giải pháp phòng, chống DDoS còn xuất phát từ ý thức của con người. Nếu chỉ sử dụng các biện pháp kỹ thuật, việc phòng, chống DDoS sẽ gặp nhiều khó khăn và không giải quyết được tận gốc. Các biện pháp và giải pháp kỹ thuật đa phần thụ động, luôn chạy theo những hình thức tấn công mới. Từ đặc điểm này, phòng, chống DDoS là vấn đề mà cộng đồng Internet phải cùng giải quyết.

Thực tế, các tổ chức đều không có phản ứng hay im lặng khi hệ thống của mình bị lợi dụng tấn công hay bị tấn công. Điều này làm cho việc ngăn chặn và loại trừ các cuộc tấn công trở nên khó khăn. Vì cộng đồng không chia sẻ thông tin. Trong khi, những kẻ tấn công có thể liên kết với nhau, chia sẻ mã nguồn hoặc công cụ tấn công.

Ngoài ra, kỹ thuật tấn công DDoS luôn biến đổi, phát triển cùng công nghệ thông tin. Do đó để phòng, chống các cuộc tấn công này, những chuyên gia phải không ngừng nghiên cứu đưa ra các giải pháp chung, riêng để ứng phó như:

- Nghiên cứu phát triển công cụ tự động sinh ACL (access control list) từ security policy, router, firewall.

- Nghiên cứu các giao thức và hạ tầng mới hỗ trợ khả năng giám sát, phân tích và điều khiển dòng dữ liệu thời gian thực.

- Phát triển và phổ cập các sản phẩm an ninh, an toàn.

- Phát triển các router, switch có khả năng xử lý phức tạp như: lọc, phân luồng, phát hiện, cảnh báo các gói tin thường từ đó ngăn chặn, hạn chế các cuộc tấn công DDoS.

- Nghiên cứu các biện pháp kỹ thuật để ghi nhận, truy nguyên các cuộc tấn công DDoS.

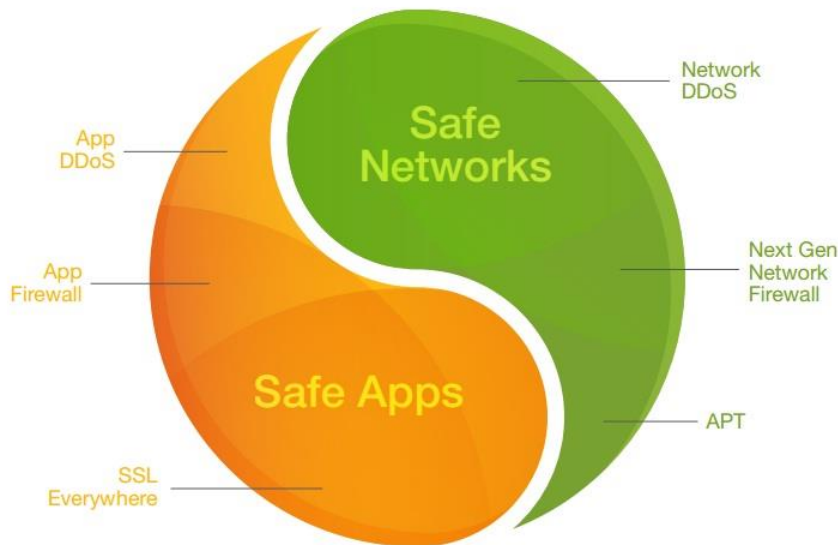
- Nghiên cứu xây dựng, hoàn thiện các quy định hành chính, pháp lý cho các thành phần tham gia mạng Internet, trong đó có các cơ chế về thông tin thời gian thực,

phối hợp giữa các tổ chức để ứng cứu, phòng, chống các cuộc tấn công DDoS; ngoài ra còn phối hợp tổng kết, rút kinh nghiệm để phòng, chống hiệu quả hơn.

4.4. Nghiên cứu hệ thống Citrix NetScaler

4.4.1. Nguyên tắc xây dựng và khả năng của hệ thống Citrix NetScaler:

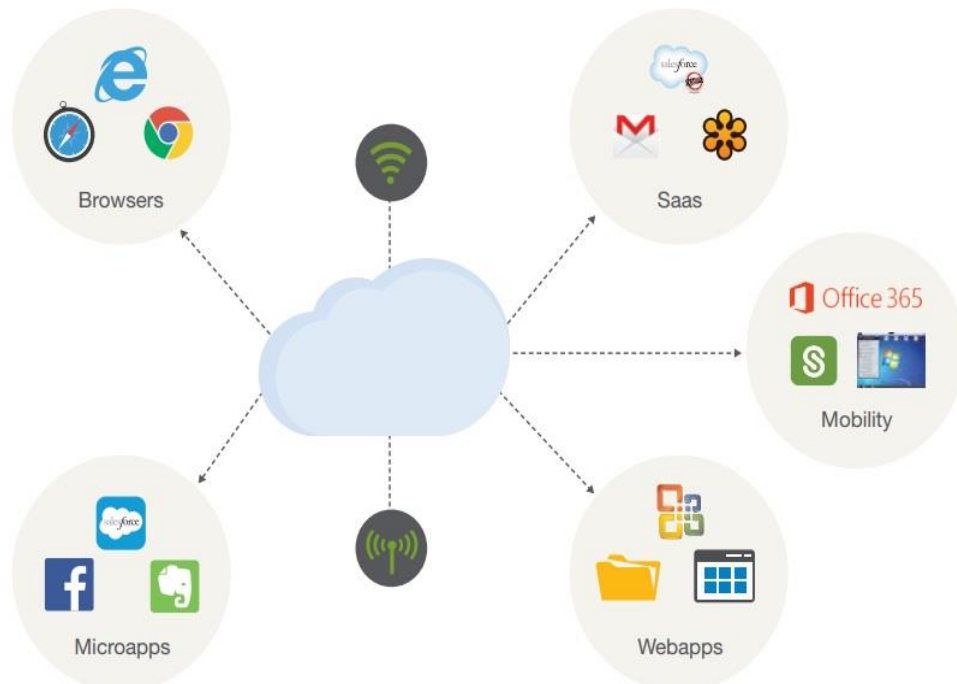
Trong tình hình hiện nay, an ninh, an toàn thông tin được đặc biệt chú trọng. Các ứng dụng hoạt động trên mạng không chỉ được bảo vệ thuộc tính chính, còn được bảo vệ toàn bộ cả các thuộc tính phụ trước các mối đe dọa ngày tăng về số lượng và sự đa dạng. Trong đó, nhiều cuộc tấn công DDoS sử dụng những cách thức không mới, tuy nhiên chống lại những cuộc tấn công này đang là một vấn đề khó khăn và thực sự chưa có một phương án tối ưu nhất áp dụng phổ biến. Giải pháp mà hệ thống Citrix NetScaler đưa ra khá hiệu quả, mang tính toàn diện áp dụng được cho cả những hệ thống lớn đến những hệ thống tầm trung, được sắp xếp theo 3 phiên bản Standard, Enterprise, Platinum tương ứng với cấp độ từ thấp đến cao. Nguyên tắc đảm bảo an ninh, an toàn, chống lại các cuộc tấn công DDoS của NetScaler được minh họa trên 02 thực thể là ứng dụng và hệ thống mạng.



Hình 4.2 Minh họa tổng hợp yếu tố đảm bảo an toàn cho 02 thực thể ứng dụng và hệ thống mạng

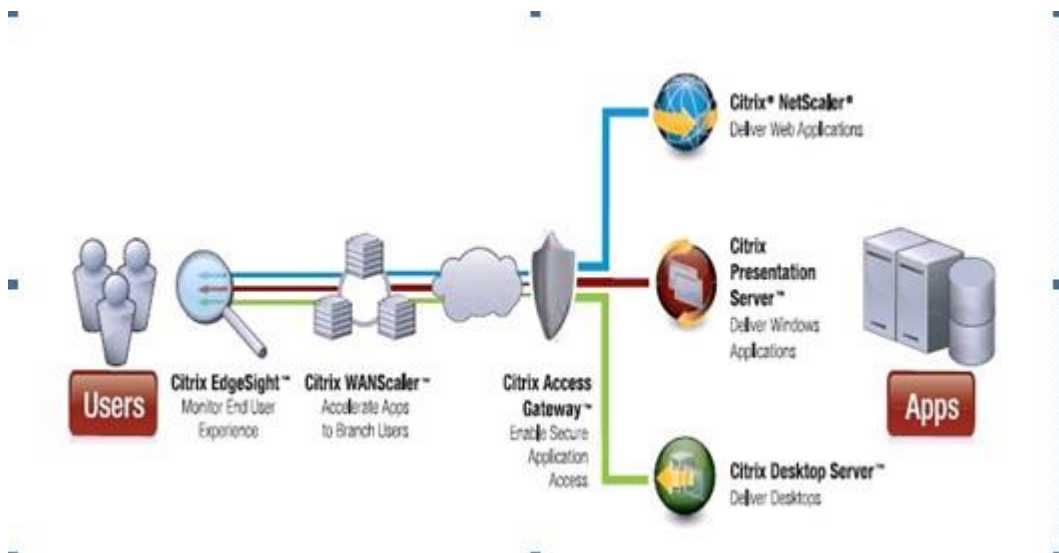
Để đảm bảo an ninh, an toàn cho một đối tượng, phải đảm bảo được an toàn cho ứng dụng: Chống lại các cuộc tấn công DDoS, tạo tường lửa và thiết lập liên kết được mã hóa giữa máy chủ và – máy khách SSL (Secure Socket Layer); đảm bảo an toàn cho hệ thống mạng: Chống lại các cuộc tấn công DDoS, thiết lập tường lửa cho mạng và thường xuyên nghiên cứu, cập nhật tính năng bảo vệ mạng trước các nguy cơ tấn công ngày một tăng – APT (Advanced Persistent Threat).

Ví dụ: đối với một ứng dụng web, Citrix NetScaler đưa ra nguyên tắc: đảm bảo an ninh, an toàn không chỉ từ bản thân ứng dụng, mà phải đảm bảo cả các yếu tố bên ngoài liên quan khác, được minh họa bởi hình vẽ sau:



Hình 4.3 Ứng dụng mạng và các thành phần liên quan

Trên cơ sở nguyên tắc trên hệ thống Citrix NetScaler được mô tả dưới dạng luồng như sau:



Hình 4.4 Mô hình bảo vệ theo luồng của hệ thống Citrix NetScaler

Hệ thống Citrix NetScaler có các khả năng sau:

- Giảm nguy cơ lây nhiễm phần mềm gây hại;

- Cản trở, ngăn chặn, phát hiện các cuộc tấn công DDOS, đặc biệt đối với các cuộc tấn công nhằm vào lớp ứng dụng trong mô hình OSI;

- Tự động thiết lập vòng an ninh để bảo vệ cho ứng dụng;

- Tương thích với những ứng dụng công nghệ phần mềm mới như: Điện toán đám mây, dịch vụ trên điện thoại di động ... do sử dụng nền tảng ảo hóa

Để bảo vệ một ứng dụng web, giải pháp không chỉ tập trung vào ứng dụng web, còn tập trung vào các thành phần tương tác như:

- Trình duyệt tương tác với các thành phần của ứng dụng web;

- Mạng lưới phân phối nội dung hay những dịch vụ lưu trữ đám mây;

- Các ứng dụng nền web (SaaS), các tùy chọn điện toán đám mây; các nền tảng dịch vụ (PaaS), cơ sở hạ tầng của ứng dụng web;

- Bảo vệ tại những thành phần liên kết với các ứng dụng web khác;

- APIs được tích hợp để tự cập nhật các thành phần trong ứng dụng web;

- Các giải pháp dành cho di động.

4.4.2. Chức năng của hệ thống Citrix NetScaler:

Hệ thống Citrix Netscaler được các nhà cung cấp dịch vụ trực tuyến hàng đầu trên thế giới Google, Yahoo, Ebay, Amazon, MSN, IBM, Oracle... sử dụng với nhiều hệ thống Data Center được phân tán trên toàn thế giới. Hệ thống bao gồm 05 chức năng chính: (1) Duy trì tính sẵn sàng, (2) tăng tốc, (3) bảo mật, (4) tối ưu hóa đầu cuối, (5) tối ưu hóa giao thức TCP, từ đó có thể phát hiện và chống lại các cuộc tấn công DDoS.

4.4.2.1. Duy trì tính sẵn sàng:

- Cân bằng tải ở lớp 4 và chuyển đổi nội dung lớp 7: Hỗ trợ các giao thức: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP và UDP), SIP (over UDP), RTSP, RADIUS, DIAMETER, SQL, RDP. Thuật toán sử dụng trong cân bằng tải: Round Robin, Least Packets, Least Bandwidth, Least Connection, Response Time, Hashing (URL, tên miền, IP nguồn, IP đích và ID khách hàng), SNMP, SASP. Có thể tích hợp cân bằng tải cơ sở dữ liệu trong các cơ sở dữ liệu: Microsoft SQL Server và MySQL. Phân phối cân bằng tải với máy chủ toàn cầu, sử dụng các thuật toán: cận địa lý (geographic proximity), cận kết nối mạng (network proximity).

Được triển khai ở phía trước hệ thống các máy chủ ứng dụng, Citrix Netscaler sẽ chia nhỏ các hướng kết nối đến hệ thống, đảm bảo tối ưu hóa việc phân phối các luồng dữ liệu. Citrix Netscaler cho phép hệ thống luôn ở mức sẵn sàng cao nhất, đáp ứng kịp thời cho bất kỳ kết nối nào đến hệ thống.

Chuyển đổi nội dung thuộc lớp 7 như Áp dụng chính sách đối với: URL, URL Query, URL Wildcard, Domain, IP nguồn/đích, HTTP Header, Custom, HTTP and TCP Payload, Values, UDP.

- Tăng cường bảo mật và ưu tiên hàng đợi: Kiểm soát tính thích ứng cho các kết nối TCP và các yêu cầu HTTP; ưu tiên các giao dịch quan trọng;

- Điều khiển tốc độ AppExpert (thành phần của ứng dụng mà NetScaler có thể tối ưu hóa; các thực thể quản lý truy cập cho các ứng dụng như SSL, thuật toán cân bằng tải ...; các chính sách cho bộ nhớ đệm, nén dữ liệu được sử dụng để tối ưu hóa ứng dụng);

- Hỗ trợ Ipv6;
- Quản lý tên miền truy cập;
- Giao thức định tuyến động;
- Sắp xếp ưu tiên hàng đợi;
- Phân nhóm Citrix TriScale;

4.4.2.2. Tăng tốc độ ứng dụng:

Citrix Netscaler kết hợp các công nghệ mới nhất cho phép tăng tốc hiệu năng các ứng dụng từ 5 -20 lần. Hai tính năng quan trọng nhất giúp tăng tốc ứng dụng là AppCompress và AppCache.

AppCompress cung cấp các cơ chế nén dữ liệu theo thời gian thực đối với dữ liệu mã hóa và không mã hóa. Đa số các trình duyệt Internet hiện nay đều hỗ trợ chuẩn nén GZIP trong khi các web server lại hỗ trợ không tốt việc nén dữ liệu. Citrix Netscaler sẽ thực thi việc nén dữ liệu theo chuẩn GZIP và truyền các dữ liệu nén tới thiết bị đầu cuối. Việc nén dữ liệu này giúp giảm thông lượng của hệ thống đồng thời cải thiện tốc độ truy cập ứng dụng từ phía khách hàng.

Công nghệ AppCache có khả năng cache đối với các website tĩnh và động, Citrix Netscaler xây dựng giải thuật tối ưu cho phép cache các dữ liệu động mang tính cố định giúp giảm tải cho hệ thống web server và data server.

Ngoài ra, Citrix NetScaler còn có chức năng Advanced TCP Optimization: Tăng hiệu năng của ứng dụng từ đó cải thiện tốc độ xử lý của các ứng dụng.

4.4.2.3. Bảo mật ứng dụng:

- Phòng chống trực tiếp các cuộc tấn công DDoS lớp 4 và lớp 7: Duy trì ứng dụng cho những người sử dụng hợp pháp, chống lại các kiểu tấn công DDoS như: SYN Flood, HTTP DDoS ..., kiểm soát tốc độ gói dữ liệu ICMP và UDP.

- DNSSEC (đảm bảo DNS): Hỗ trợ DNS proxy, xác thực DNS, ký DNS.

Lọc các gói dữ liệu: Kiểm soát danh sách truy cập lớp 3, lớp 4 (ACL), Dịch các địa chỉ mạng (Network address translation - NAT) hỗ trợ Ipv4/Ipv6

- Cung cấp ứng dụng NetScaler Gateway trong đó có SSL, VPN. Riêng đối với SSL, Citrix Netscaler tích hợp sẵn phần cứng tăng tốc SSL để giảm tải quá trình tăng lên của việc thiết lập kết nối SSL và mã hóa từ máy chủ web. Tăng tốc SSL cho phép giảm tải CPU trên máy chủ, giải phóng tài nguyên máy chủ để phục vụ cho những nhiệm vụ khác. Ngoài ra Citrix Netscaler cho phép thiết lập chế độ hoạt động với các chuẩn FIPS kết hợp với HSM cung cấp các mã phát sinh và lưu trữ.

- Kết nối NetScaler với XenMobile ứng dụng cho nền tảng di động;

- Cung cấp ứng dụng tường lửa (CitrixApplication Firewall);

- Phân tích kịch bản;

- Citrix Netscaler cho phép bảo vệ các ứng dụng web khỏi các tấn công từ lớp 7 như SQL injection, chèn mã độc CSS, forceful browsing, cookie poisoning, chống thất thoát và rò rỉ dữ liệu của khách hàng.

- Các tính năng đã tích hợp sẵn như khả năng chống các tấn công từ chối dịch vụ phân tán (DoS), khả năng kiểm tra nội dung cho phép Citrix Netscaler nhận dạng và khóa các tấn công ứng dụng như GET floods và các tấn công site-scraping. Các ứng dụng không cần thiết, chiếm nhiều tài nguyên của hệ thống cũng được khắc phục bằng các trình điều khiển tự động Surge Protection và Priority Queuing.

4.4.2.4. Tối ưu hóa đầu cuối:

Đây chính là việc tối ưu hóa nội dung ứng dụng từ đó giảm thời gian tải và chạy ứng dụng.

- CSS: kết hợp các css liên quan trong một thẻ; đưa vào các luật để liên kết CSS này.

- Tối ưu hóa ảnh: Tối ưu hóa ảnh IPEG bằng cách loại bỏ các byte thừa, tối ưu hóa ảnh GIF bằng cách chuyển đổi sang PNG, và giảm cỡ ảnh để phù hợp nội dung hiển thị.

- Tối ưu hóa javaScript: Giảm các liên kết và nhóm javaScript đưa vào trong các thẻ lệnh HTML.

4.4.2.5. Tối ưu hóa TCP:

Citrix NetScaler có 3 kiểu tối ưu hóa TCP chủ yếu là:

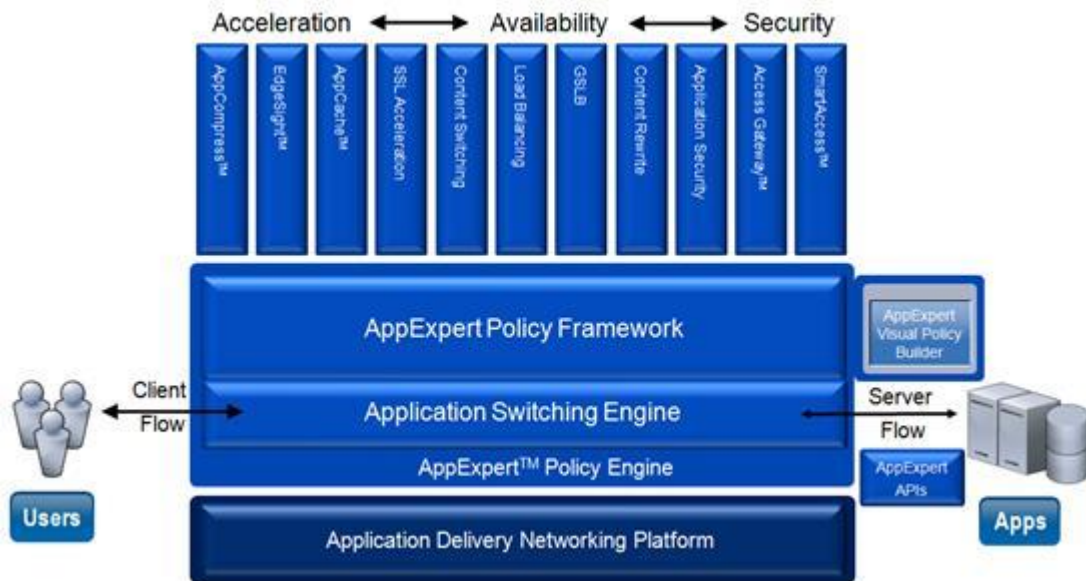
Advanced TCP Optimization: Cùng với các công nghệ tiên tiến như: Client keep-alive, fast ramp, windows scaling và selective acknowledgement, Citrix Netscaler cho phép tăng tốc hiệu năng của ứng dụng mà không cần phải thay đổi hạ tầng mạng sẵn

có, do vậy các ứng dụng được phân phối đến người sử dụng một cách nhanh và hiệu quả hơn.

TCP Multiplexing: Citrix Netscaler sẽ tập hợp tất cả các yêu cầu về kết nối đến hệ thống – TCP proxy, trong khi chỉ duy trì một số lượng nhỏ kết nối đến các máy chủ phía sau để lấy dữ liệu trả về cho người sử dụng. Điều này cho phép giảm tải cho các máy chủ phía sau, ngược lại các máy chủ sẽ đáp ứng nhanh hơn cho các nhu cầu tiếp theo.

TCP Buffering: Bằng cách sắp xếp và phân phối các yêu cầu kết nối đến hệ thống một cách thông minh, Citrix Netscaler cho phép các máy chủ phía sau hoạt động với một hiệu suất ổn định và cân bằng.

Ngoài các chức năng trên Citrix NetScaler còn **Giảm thiểu chi phí triển khai và vận hành**. Citrix Netscaler cắt giảm chi phí triển khai ứng dụng bằng cách giảm số máy chủ yêu cầu và tối ưu việc sử dụng băng thông mạng. Thêm nữa, Citrix Netscaler làm giảm chi phí vận hành, đầu tư bằng cách hợp nhất nhiều tính năng phần mềm kết hợp với khả năng nâng cấp hiệu năng bằng software license.



Hình 4.5 Kiến trúc dòng sản phẩm Citrix Netscaler:

4.4.3. Cài đặt và chạy hệ thống Citrix NetScaler:



Cấu hình máy chủ khi cài một số hệ thống Citrix NetScaler được thống kê trong bảng dưới đây:

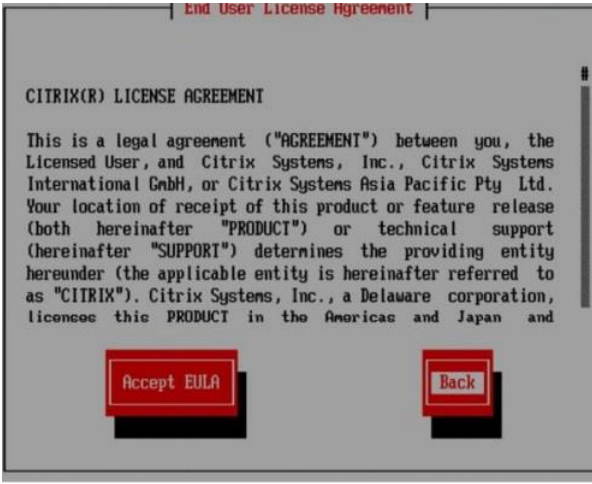



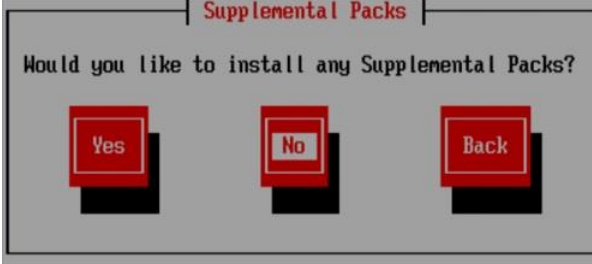
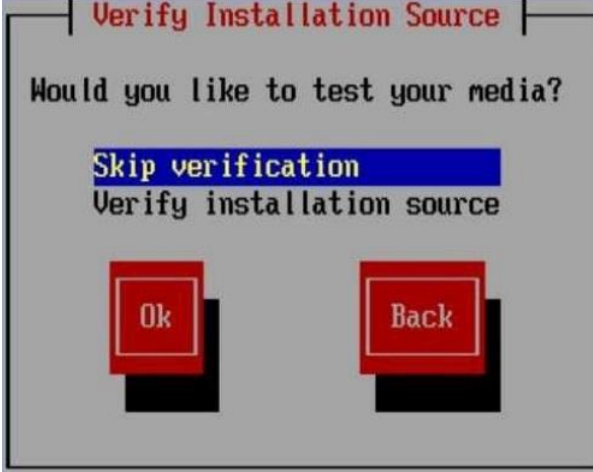
Mã hệ thống Citrix NetScaler	MPX/SDX 24150	MPX/SDX 24100	MPX 22120/SDX 22120	MPX 22100/SDX 22100
-------------------------------------	----------------------	----------------------	----------------------------	----------------------------

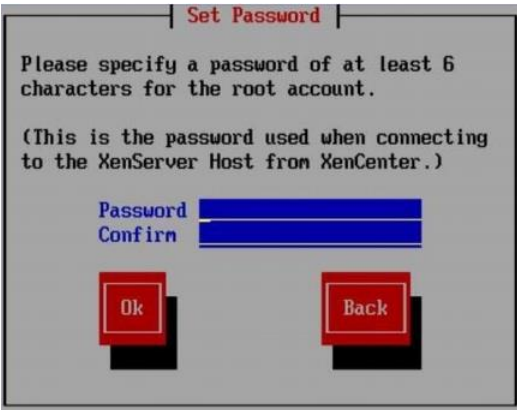
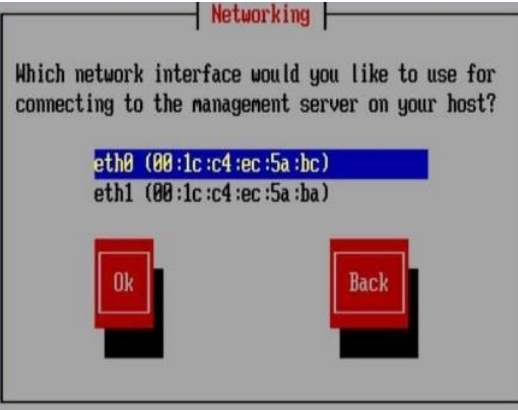
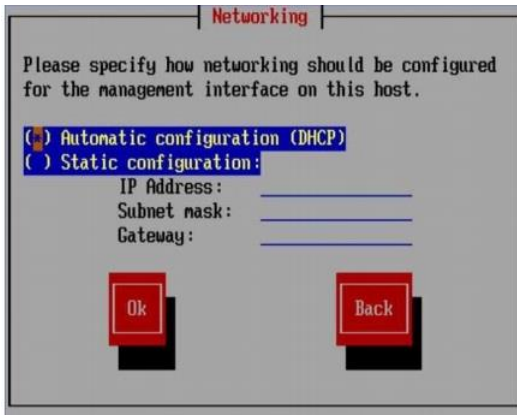



Processor	Dual Intel E5-2690	Dual Intel E5-2690	Dual Intel E5-2690	Dual Intel E5-2690
Memory	256 GB	256 GB	256 GB	256 GB
Ethernet ports	24X10GE SFP+ and 12XGE SFP	24X10GE SFP+ and 12XGE SFP	24x 10GBASE-X SFP+ OR (for NEBS models) 24x 10GBASE-X SFP+ 12x 1000BASE-X SFP (fiber or copper)	24x 10GBASE-X SFP+ OR (for NEBS models) 24x 10GBASE-X SFP+ 12x 1000BASE-X SFP (fiber or copper)
Upgrades (khả năng nâng cấp)		Upgrade option to MPX/SDX 24150		Upgrade option to MPX/SDX 22120

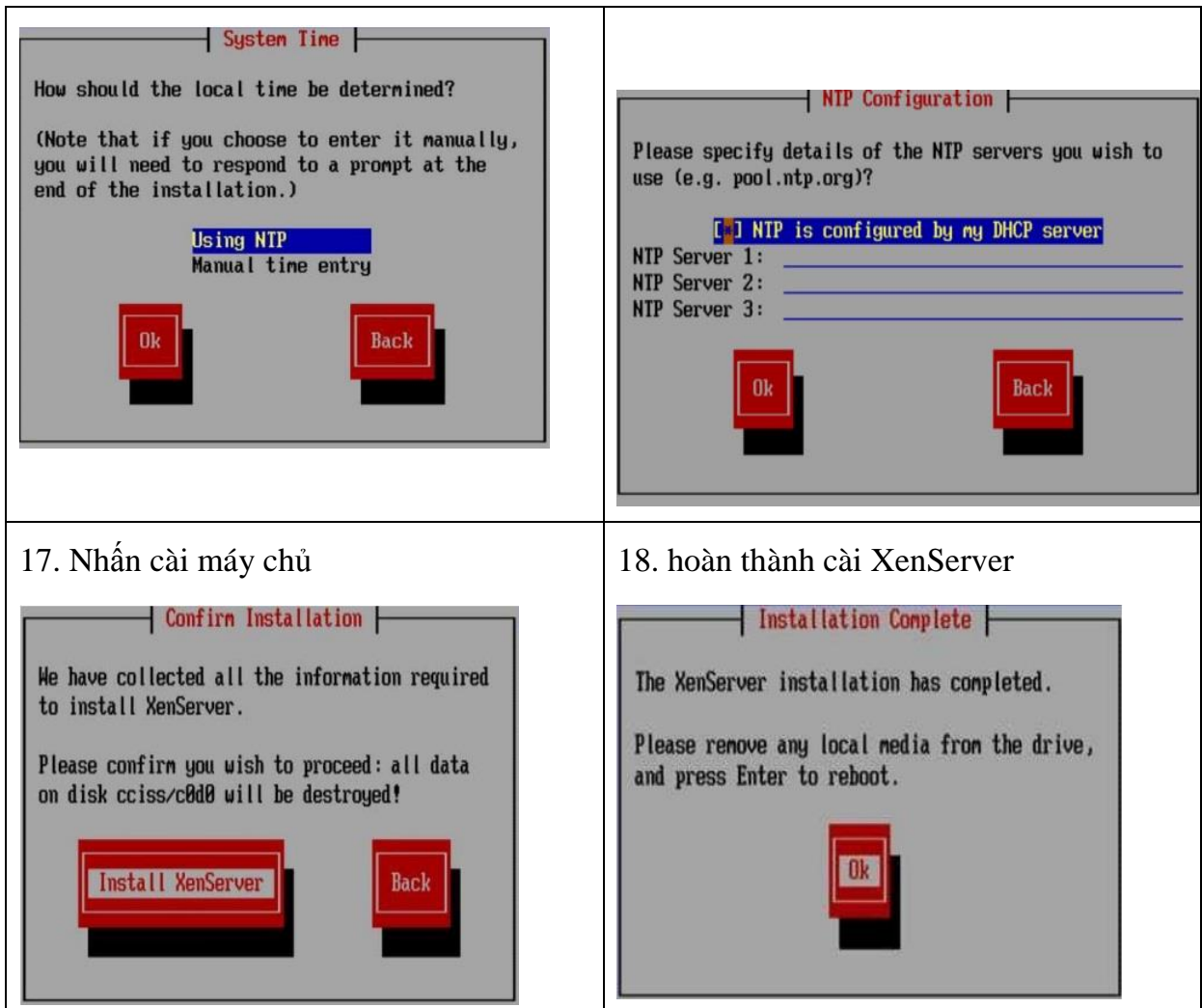
Bảng cấu hình máy chủ khi cài một số hệ thống Citrix NetScaler

Bước 1: Cài đặt Xenserver

<p>1. Chạy file cài, chọn kiểu bàn phím</p> 	<p>2. Bắt đầu tiến hành cài đặt (chọn ok)</p> 
<p>3. Đọc và chấp nhận các điều khoản khi cài đặt.</p>	<p>4. Chọn ok để bắt đầu cài</p>

	
<p>5. Chọn ổ cứng đủ lớn để cài đặt.</p> 	<p>6. Chọn nguồn để cài.</p> 
<p>7. Cài các gói bổ sung, chọn No để tiếp tục.</p> 	<p>8. Chọn bỏ qua xác nhận để tiếp tục.</p> 
<p>9. Cài đặt mật khẩu cho XenServer</p>	<p>10. Chọn loại card mạng</p>

	
<p>11. Chọn cấu hình tự động và ok</p> 	<p>12. Chọn Manually specify và automatically set via</p> 
<p>13. Chọn múi giờ theo quốc gia</p> 	<p>14. Chọn khu vực giờ cụ thể</p> 
<p>15. Chọn thời gian cho mạng (chọn NTP)</p>	<p>16. Nhập NTP để thiết lập thời gian</p>

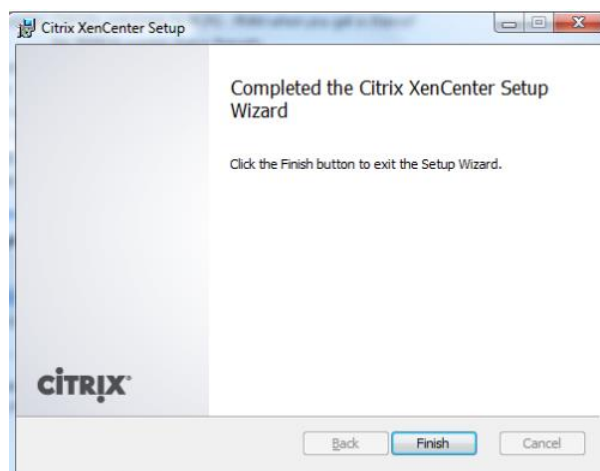


17. Nhấn cài máy chủ

18. hoàn thành cài XenServer

Bước 2: Cài XenCenter

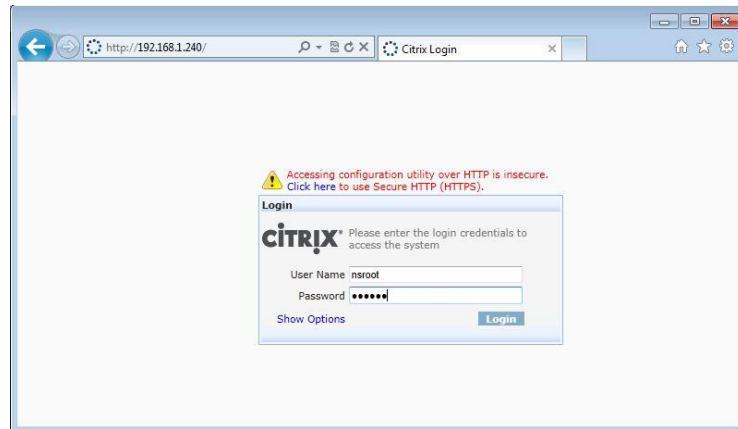
Chạy file XenCenter.msi, sau đó chọn next để chương trình chạy, chú ý chọn all user. Sau khi cài xong, màn hình báo:



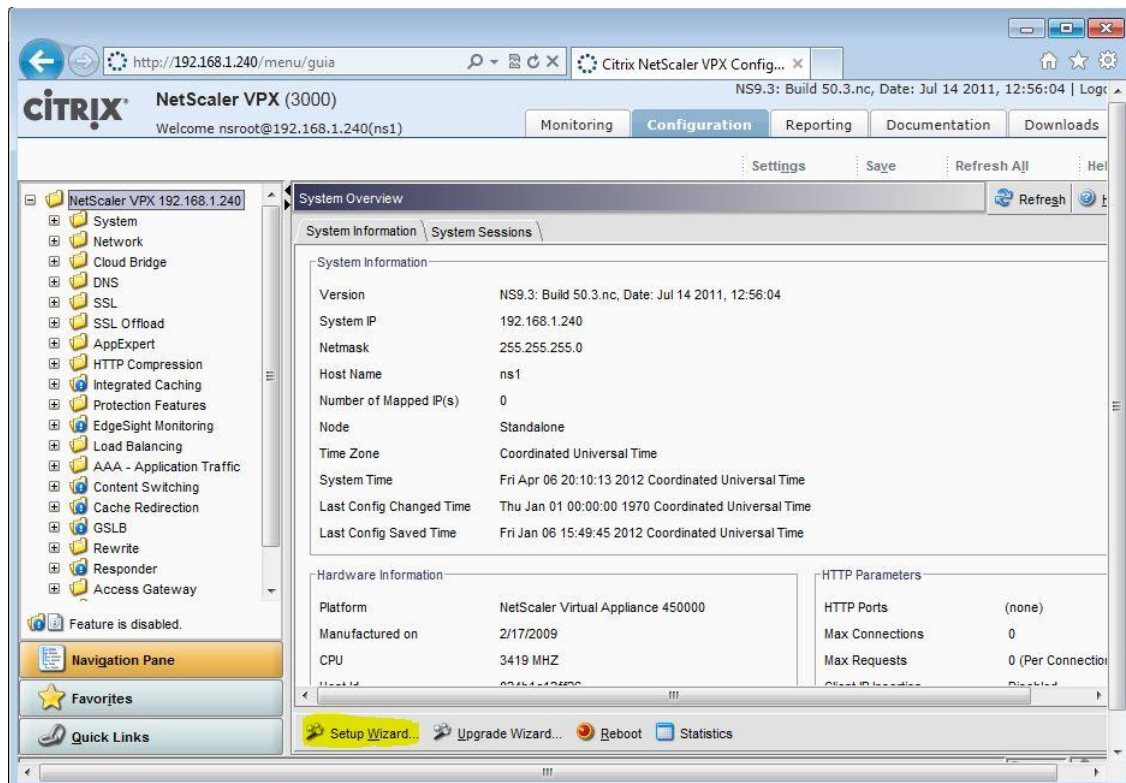
Hình 4.6 Cài XenCenter

Bước 3: Tiếp tục cài đặt các thành phần “NetScaler VPX on VMware”, “VPX on Hyper-V”, “NetScaler VPX on KVM”.

Hệ thống đã cài đặt xong, bắt đầu chạy:



Hình 4.7 Màn hình đăng nhập hệ thống



Hình 4.8 Màn hình hệ thống

4.4.4. Đánh giá hệ thống:

Hệ thống NetScaler hoạt động ổn định, hiệu quả, khả năng phòng chống DDoS khá tương đồng với 9 giải pháp trong Chương 4 do tác giả đưa ra. Tuy nhiên, do đây là hệ thống lớn, tích hợp nhiều tính năng. Vì vậy, quản trị viên phải có kinh nghiệm mới có thể vận hành tốt hệ thống chống lại các cuộc tấn công DDoS.

4.5. Xây dựng kịch bản phòng, chống Ddos:

Kịch bản phòng, chống DDos dựa trên sử dụng giải pháp của hệ thống Citrix NetScaler để bảo vệ một dịch vụ web sử dụng cơ sở dữ liệu SQL Server.

4.5.1. Giai đoạn chuẩn bị:

Sử dụng chức năng tối ưu hóa của Citrix NetScaler để tăng tốc độ ứng dụng từ đó tăng băng thông. Dịch vụ web sẽ đáp ứng cùng lúc một lượng truy cập lớn, nâng cao khả năng chống lại các cuộc tấn công DDos.

Chức năng tối ưu hóa của NetScaler gồm có:

- Tối ưu hóa đầu cuối:

Đây chính là việc tối ưu hóa nội dung ứng dụng từ đó giảm thời gian tải và chạy ứng dụng.

- Tối ưu hóa CSS: kết hợp các css liên quan trong một thẻ; đưa vào các luật để liên kết CSS này.

- Tối ưu hóa ảnh: Tối ưu hóa ảnh IPEG bằng cách loại bỏ các byte thừa, tối ưu hóa ảnh GIF bằng cách chuyển đổi sang PNG, và giảm cỡ ảnh để phù hợp nội dung hiển thị.

- Tối ưu hóa javaScript: Giảm các liên kết và nhóm javaScript đưa vào trong các thẻ lệnh HTML.

- Tối ưu hóa TCP:

Citrix NetScaler có 3 kiểu tối ưu hóa TCP chủ yếu là:

Advanced TCP Optimization: Cùng với các công nghệ tiên tiến như: Client keep-alive, fast ramp, windows scaling và selective acknowledgement, Citrix Netscaler cho phép tăng tốc hiệu năng của ứng dụng mà không cần phải thay đổi hạ tầng mạng sẵn có, do vậy các ứng dụng được phân phối đến người sử dụng một cách nhanh và hiệu quả hơn.

TCP Multiplexing: Citrix Netscaler sẽ tập hợp tất cả các yêu cầu về kết nối đến hệ thống – TCP proxy, trong khi chỉ duy trì một số lượng nhỏ kết nối đến các máy chủ phía sau để lấy dữ liệu trả về cho người sử dụng. Điều này cho phép giảm tải cho các máy chủ phía sau, ngược lại các máy chủ sẽ đáp ứng nhanh hơn cho các nhu cầu tiếp theo.

TCP Buffering: Bằng cách sắp xếp và phân phối các yêu cầu kết nối đến hệ thống một cách thông minh, Citrix Netscaler cho phép các máy chủ phía sau hoạt động với một hiệu suất ổn định và cân bằng.

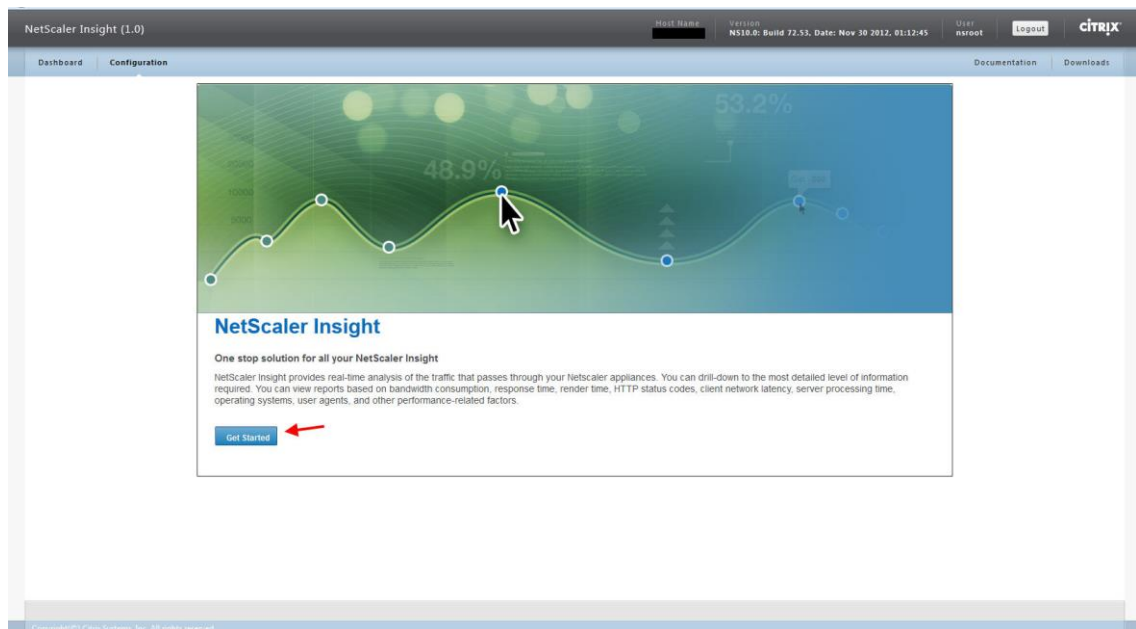
- Tăng tốc ứng dụng:

Sử dụng tính năng AppCompress cung cấp các cơ chế nén dữ liệu theo thời gian thực đối với dữ liệu mã hóa và không mã hóa. Đa số các trình duyệt Internet hiện nay đều hỗ trợ chuẩn nén GZIP trong khi các web server lại hỗ trợ không tốt việc nén dữ liệu. Citrix Netscaler sẽ thực thi việc nén dữ liệu theo chuẩn GZIP và truyền các dữ liệu nén tới thiết bị đầu cuối. Việc nén dữ liệu này giúp giảm thông lượng của hệ thống đồng thời cải thiện tốc độ truy cập ứng dụng web.

- Cài đặt cân bằng tải cho web server:

4.5.2. Giai đoạn phát hiện, chống một cuộc tấn công DDos:

- Sử dụng công cụ AAA Application Traffic để kiểm tra dung lượng truy cập, nếu dung lượng truy cập ở mức cao hoặc đột ngột cao bất thường chứng tỏ có cuộc tấn công DDos. Bảng NetScaler Insight giúp ta phân tích được trực quan:

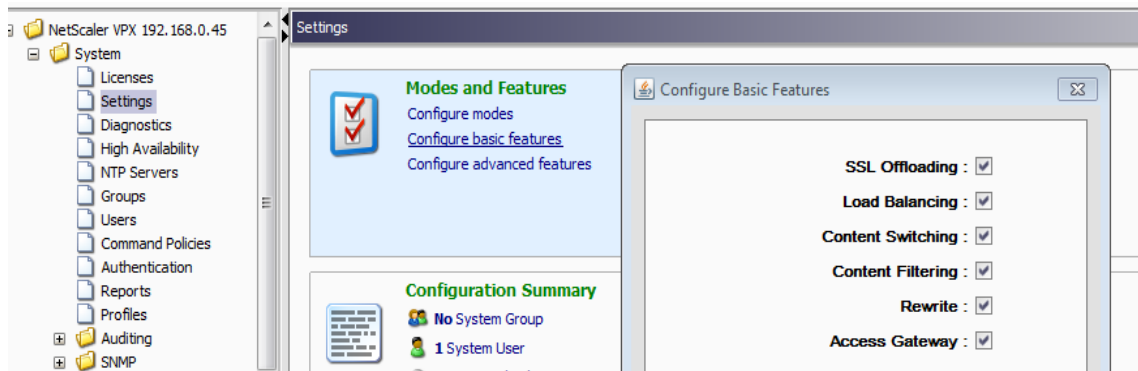


Hình 4.9 Công cụ AAA Application Traffic



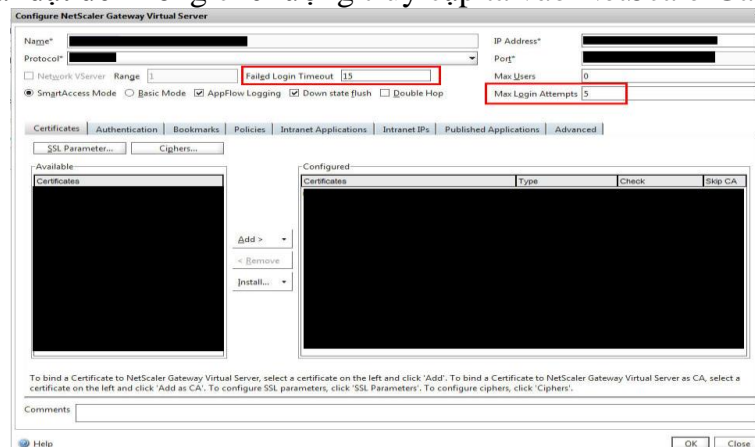
Hình 4.10 Công cụ Monitoring

- Sau khi phát hiện cuộc tấn công ta kích hoạt các tính năng tự động chống DDos của hệ thống Citrix NetScaler. Bằng cách vào System -> Setting, hộp thoại “The Configure Advanced Features” chọn các tính năng Http DDos Protection, Priority queue, Surge Protection. Đồng thời bật tính năng cân bằng tải để tăng băng thông cho hệ thống.

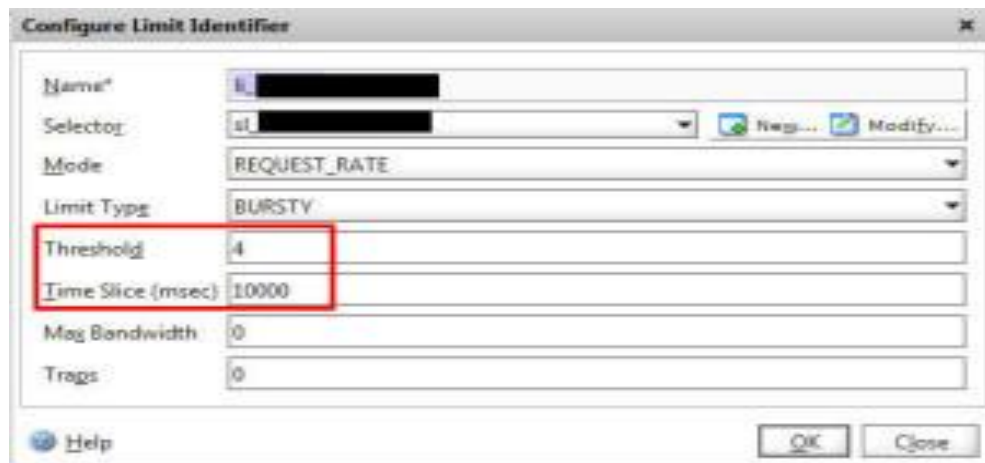


Hình 4.11 Hệ thống Citrix NetScaler

- Theo dõi và cài đặt để không chế lượng truy cập ta vào NetScalerGateway



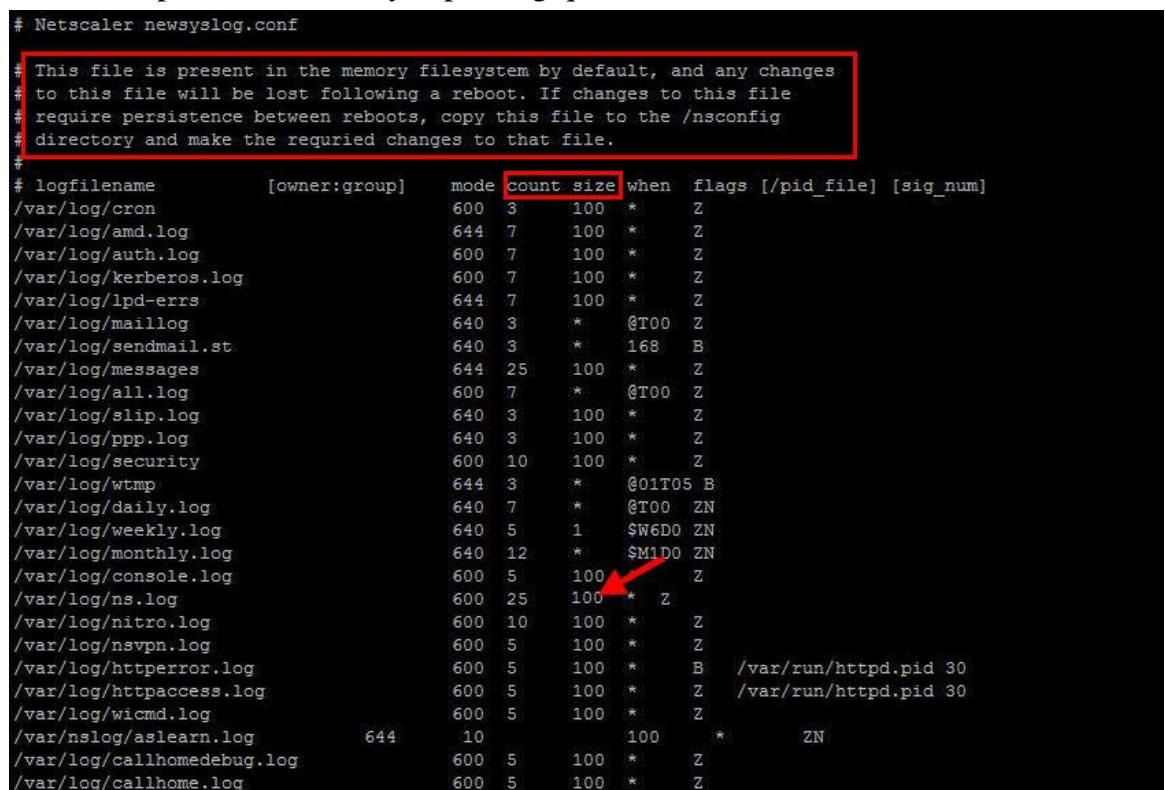
Hình 4.12 Theo dõi và cài đặt



Hình 4.12 Cài đặt giới hạn tốc độ trong AppExpert

4.5.3 Giai đoạn sau tấn công:

Tiến hành phân tích các truy cập thông qua các file SYSLOG và NSLOG.



Hình 4.13 Phân tích các truy cập

KẾT LUẬN

Luận văn đã đạt được những kết quả sau:

- Đưa ra khái niệm và lý thuyết cơ bản về tấn công DDOS.
- Phân loại và phân tích về các kiểu tấn công DDOS.
- Thiết kế mô hình hệ thống phòng chống DDOS, các thành phần trong mô hình.
- Tình hình liên quan tới DDoS và giải pháp phòng, chống DDoS đang triển khai thực hiện ở Việt Nam.
- Đề xuất giải pháp phòng chống DDoS.
- Nghiên cứu về hệ thống an ninh, an toàn có khả năng phòng, chống các cuộc tấn công DDoS.

Định hướng công việc trong tương lai:

Đối với công việc trong tương lai, tôi sẽ nghiên cứu sâu hơn các nội dung liên quan tới việc truy nguyên nguồn tấn công DDoS, một kiểu tấn công DDoS chậm và cách phát hiện. Đồng thời hiện thực hóa mô hình Honey net ở Việt Nam.

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

Tiếng Việt:

- [1] PGS.TS Trịnh Nhật Tiến, 2013. Bài giảng “Phát hiện và diệt Virus máy tính”. Hà Nội: Đại học Công nghệ - Đại học Quốc gia Hà Nội.
- [2] Nguy cơ lộ lọt thông tin trong các cơ quan Đảng, Chính phủ - Đề tài khoa học cấp nhà nước của Ban cơ yếu chính phủ.
- [3] <http://securitydaily.net/chong-botnet-va-ddos-tai-viet-nam/>
- [4] <http://www.hvaonline.net/hvaonline/forums/ddos>

Tiếng Anh:

- [5] M. Li. An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition. *Computers & Security*, 23(7): 549-558, 2004.
- [6] Incapsula’s research team has been tracking trends in the DDoS landscape and has seen a rapid surge in attacks 2014.
- [7] Protecting Against Application DDoS Attacks with BIG-IP ASM: A Three-Step Solution **By Or Katz** Principal Security Engineer
- [8] <http://citrix.com>
- [9] <http://en.wikipedia.org>
- [10] <http://www.cert.org/ddos>
- [11] <https://www.honeynet.org/>