

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
PHÂN HIỆU TẠI TP. HỒ CHÍ MINH
BỘ MÔN CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP

**ĐỀ TÀI: TÌM HIỂU CÁC PHƯƠNG THỨC TẤN CÔNG TỪ CHỐI DỊCH
VỤ VÀ GIẢI PHÁP NGĂN CHẶN**

Giảng viên hướng dẫn: NGUYỄN XUÂN SÂM

Sinh viên thực hiện: LÊ QUANG VŨ

Lớp : CÔNG NGHỆ THÔNG TIN

Khoá : 58

Tp. Hồ Chí Minh, tháng 8 năm 2021

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
PHÂN HIỆU TẠI TP. HỒ CHÍ MINH
BỘ MÔN CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP

**ĐỀ TÀI: TÌM HIỂU CÁC PHƯƠNG THỨC TẤN CÔNG TỪ CHỐI DỊCH
VỤ VÀ GIẢI PHÁP NGĂN CHẶN**

Giảng viên hướng dẫn: NGUYỄN XUÂN SÂM

Sinh viên thực hiện: LÊ QUANG VŨ

Lớp : CÔNG NGHỆ THÔNG TIN

Khoá : 58

Tp. Hồ Chí Minh, tháng 8 năm 2021

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP
BỘ MÔN: CÔNG NGHỆ THÔNG TIN
-----***-----

Mã sinh viên: 5851071090

Họ tên SV: Lê Quang Vũ

Khóa: 58

Lớp: CQ.58.CNTT

1. Tên đề tài: Tìm hiểu các phương thức tấn công từ chối dịch vụ và giải pháp ngăn chặn

2. Mục đích, yêu cầu

- Mục đích:
 - Tìm hiểu cách thức, phương pháp tấn công từ đó đưa ra giải pháp phù hợp ngăn chặn.
- Yêu cầu:
 - Tìm hiểu về DOS/DDOS.
 - Tìm hiểu về hệ thống phát hiện xâm nhập IDS.
 - Hiểu về cách triển khai CRM
 - Cài đặt 1 hệ thống có thể phát hiện tấn công DOS/DDOS.
 - Sử dụng firewall để ngăn chặn tấn công DOS/DDOS

3. Nội dung và phạm vi đề tài

- Nội dung đề tài:
 - Giới thiệu tổng quan về DOS/DDOS.
 - Giới thiệu về hệ thống phát hiện xâm nhập IDS.
 - Nghiên cứu cách cài đặt hệ thống và các phương thức hoạt động của hệ thống phát hiện xâm nhập.
 - Nghiên cứu cài đặt phương thức phòng thủ để bảo vệ servers trước tấn công DOS/DDOS.
- Phạm vi đề tài:

- Cài đặt hệ thống phát hiện xâm nhập và tìm phương thức phòng thủ của hệ thống.

4. Công nghệ, công cụ và ngôn ngữ lập trình:

- Công cụ hỗ trợ tạo máy ảo: Vmware Workstation.
- Hệ thống phát hiện xâm nhập: Snort.
- Tường lửa bảo vệ: CSF Firewall.

5. Các kết quả chính dự kiến sẽ đạt được và ứng dụng:

- Hoàn chỉnh cuốn báo cáo đề tài.
- Khái quát được tổng quan về tấn công từ chối dịch vụ DOS/DDOS.
- Nắm được cách cài đặt và sử dụng hệ thống phát hiện xâm nhập Snort và tường lửa bảo vệ CSF Firewall.
- Nắm được các ưu, nhược điểm của hệ thống phát hiện xâm nhập Snort và tường lửa bảo vệ CSF firewall.
- Xây dựng được hệ thống bảo vệ servers trước sự tấn công DOS/DDOS.

6. Giáo viên và cán bộ hướng dẫn:

Họ tên: Nguyễn Xuân Sâm

Đơn vị công tác: Trưởng Bộ môn Mạng Máy tính & Mạng Khoa Công nghệ Thông tin
Số 2 Học viện Công nghệ Bưu chính Viễn thông Bộ Thông tin và Truyền thông

Điện thoại: 096-993-8284

Email: samnx@ptithcm.edu.vn

Ngày tháng 07 năm 2021

Trưởng BM Công nghệ Thông tin

Đã giao nhiệm vụ TKTN

Giáo viên hướng dẫn

Nguyễn Xuân Sâm

Đã nhận nhiệm vụ TKTN

Sinh viên: Lê Quang Vũ

Ký tên:

Điện thoại: 0931254428

Email: 5851071090@st.utc2.edu.vn

LỜI CẢM ƠN

Lời nói đầu tiên, em xin gửi tới Quý Thầy Cô Bộ môn Công nghệ Thông tin Trường Đại học Giao thông vận tải phân hiệu tại thành phố Hồ Chí Minh lời chúc sức khỏe và lòng biết ơn sâu sắc.

Em xin chân thành cảm ơn quý thầy cô đã giúp đỡ tạo điều kiện để em hoàn thành đồ án với đề tài “**Tìm hiểu các phương thức tấn công từ chối dịch vụ và giải pháp ngăn chặn**”. Đặc biệt em xin cảm ơn Thầy Nguyễn Xuân Sâm đã nhiệt tình giúp đỡ, hướng dẫn cho em kiến thức, định hướng và kỹ năng để có thể hoàn thành đồ án tốt nghiệp này.

Tuy đã cố gắng trong quá trình nghiên cứu tìm hiểu tuy nhiên do kiến thức còn hạn chế nên vẫn còn tồn tại nhiều thiếu sót. Vì vậy em rất mong nhận được sự đóng góp ý kiến của Quý thầy cô bộ môn để đề tài của em có thể hoàn thiện hơn.

Lời sau cùng, em xin gửi lời chúc tới Quý Thầy Cô Bộ môn Công nghệ thông tin và hơn hết là Thầy Nguyễn Xuân Sâm có thật nhiều sức khỏe, có nhiều thành công trong công việc.

Em xin chân thành cảm ơn!

Tp. Hồ Chí Minh, ngày....tháng.....năm 2021

Sinh viên thực hiện

Lê Quang Vũ

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Tp. Hồ Chí Minh, ngày tháng năm

Giáo viên hướng dẫn

Nguyễn Xuân Sâm

MỤC LỤC

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP	I
LỜI CẢM ƠN.....	III
NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN	IV
MỤC LỤC	V
MỞ ĐẦU	1
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ CÁC PHƯƠNG THỨC TẤN CÔNG	
MẠNG MÁY TÍNH.....	3
1.1 TỔNG QUAN AN TOÀN MẠNG VÀ TẤN CÔNG MẠNG:.....	3
1.1.1 Nguy cơ đe dọa máy tính, an toàn thông tin:	3
1.1.2 Những vấn đề đảm bảo an ninh và an toàn mạng:	3
1.1.3 Đối tượng tấn công mạng:.....	4
1.1.4 Hệ thống CRM xây dựng trong đồ án.....	4
1.1.5 Các lỗ hổng trong bảo mật và phương thức tấn công mạng:	4
1.2 GIỚI THIỆU KỸ THUẬT TẤN CÔNG DOS:	7
1.2.1 Giới thiệu tấn công DoS:.....	7
1.2.2 Lịch sử các cuộc tấn công và phát triển của DoS:	7
1.2.3 Mục đích của tấn công DoS và hiểm họa:	8
1.3 GIỚI THIỆU KỸ THUẬT TẤN CÔNG DDOS:.....	9
1.3.1 Giới thiệu tấn công DdoS:	9
1.3.2 Lịch sử các cuộc tấn công và phát triển của DDoS:	9
1.3.3 Mục đích của tấn công DDoS và hiểm họa:	11
1.4 CÁC SỐ LIỆU TẤN CÔNG DOS/DDoS:	12
1.5 SỰ KHÁC BIỆT CỦA 2 KIỂU TẤN CÔNG DOS VÀ DDOS:.....	17
1.6 KẾT LUẬN CHƯƠNG:.....	18
CHƯƠNG 2. CÁC HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ DDOS	19
2.1 CÁC LOẠI TẤN CÔNG DDOS CƠ BẢN:.....	19
2.2 TẤN CÔNG SLOWLORIS:	19

2.2.1	Khái niệm:	19
2.2.2	Lịch sử xuất hiện:	20
2.2.3	Cơ chế tấn công:	21
2.2.4	Mức độ phá hoại:	21
2.3	TẤN CÔNG UDP FLOOD:	21
2.3.1	Khái niệm:	21
2.3.2	Lịch sử xuất hiện:	22
2.3.3	Cơ chế tấn công:	23
2.3.4	Mức độ phá hoại:	23
2.4	TẤN CÔNG SYN FLOOD:	24
2.4.1	Khái niệm:	24
2.4.2	Lịch sử xuất hiện:	24
2.4.3	Cơ chế tấn công:	25
2.4.4	Mức độ phá hoại:	26
2.5	TẤN CÔNG PING OF DEATH:	27
2.5.1	Khái niệm:	27
2.5.2	Lịch sử xuất hiện:	28
2.5.3	Cơ chế tấn công:	28
2.5.4	Mức độ phá hoại:	29
2.6	TẤN CÔNG NTP AMPLIFICATION:	29
2.6.1	Khái niệm:	29
2.6.2	Lịch sử xuất hiện:	30
2.6.3	Cơ chế tấn công:	30
2.6.4	Mức độ phá hoại:	30
2.7	TẤN CÔNG HTTP FLOOD:	31
2.7.1	Khái niệm:	31
2.7.2	Lịch sử xuất hiện:	31
2.7.3	Cơ chế tấn công:	32
2.7.4	Mức độ phá hoại:	32

2.8 KẾT LUẬN CHƯƠNG:.....	33
CHƯƠNG 3. CÀI ĐẶT PHƯƠNG THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ	34
3.1 GIỚI THIỆU CÁC CÔNG CỤ ĐỂ GIẢ LẬP TẤN CÔNG TỪ CHỐI DỊCH VỤ:	34
3.1.1 VMware Server:	34
3.1.2 Hệ điều hành Kali Linux:.....	34
3.1.3 Hệ điều hành Ubuntu Server:.....	35
3.2 GIẢ LẬP PHÍA BỊ TẤN CÔNG TỪ CHỐI DỊCH VỤ:.....	37
3.3 GIẢ LẬP PHÍA TẤN CÔNG TỪ CHỐI DỊCH VỤ:.....	39
3.4 KẾT LUẬN CHƯƠNG:.....	42
CHƯƠNG 4. GIẢI PHÁP NGĂN CHẶN TẤN CÔNG TỪ CHỐI DỊCH VỤ	43
4.1 GIỚI THIỆU HỆ THỐNG PHÒNG THỦ:	43
4.1.1 Giới thiệu hệ thống phát hiện xâm nhập Snort:	43
4.1.2 Giới thiệu ứng dụng CSF Firewall:.....	44
4.2 GIẢ LẬP NGĂN CHẶN TẤN CÔNG TỪ CHỐI DỊCH VỤ:	45
4.3 KẾT LUẬN CHƯƠNG:.....	56
CHƯƠNG 5. KẾT LUẬN VÀ KIẾN NGHỊ	57
5.1 KẾT QUẢ ĐẠT ĐƯỢC:.....	57
5.2 TỒN TẠI:.....	57
5.3 HƯỚNG PHÁT TRIỂN:	58
PHỤ LỤC	59

DANH MỤC CHỮ VIẾT TẮT

STT	Mô tả	Ý nghĩa	Ghi chú
1	GB	Gigabyte	
2	USD	United States Dollar	
3	OTP	One-time password	
4	IP	Internet Protocol	
5	CRM	Customer relationship management	
6	DoS	Denial-of-service	
7	DDoS	Distributed Denial of Service	
8	CPU	Central Processing Unit	
9	KB	Kilobyte	
10	URL	Uniform Resource Locator	
11	SQL	<i>Structured Query Language</i>	
12	UDP	User Datagram Protocol	
13	TFN	Tax File Number	
14	IOT	Internet Of Things	
15	Gbps	Gigabits per second	
16	DNS	Domain Name System	
17	CNN	Convolutional Neural Network	
18	PC	Personal Computer	
19	ICMP	Internet Control Message Protocol	
20	HTTP	Hypertext Transfer Protocol	

21	HTTPS	Hypertext Transfer Protocol Secure	
22	NTP	Network Time Protocol	
23	CERT	Computer Emergency Response Team	
24	TCP	Transmission Control Protocol	
25	Mpps	Mega packet per second	
26	GRE	Generic Routing Encapsulation	
27	CNTT	Computers And Information Technology	
28	SaaS	Software As a Service	
29	SYN	The Synchronous Idle Character	
30	IETF	Internet Engineering Task Force	
31	ACK	Acknowledge	
32	PoD	Proof Of Delivery	
33	CVE-ID	Common Vulnerabilities and Exposures	
34	VU	Volume unit	
35	OSCP	Offensive Security Certified Professional	
36	OSCE	Organization for Security and Co-operation in Europe	
37	OSWP	Offensive Security Wireless Professional	
38	OSEE	Open System Engineering	

		Environment	
39	IE	Internet Explorer	
40	APT	Advanced Package Tool	
41	CSF	Cerebrospinal Fluid	
42	SID	Session Identification	

DANH MỤC BẢNG BIỂU

Bảng 1. 1: Sự khác biệt của 2 kiểu tấn công DoS và DDoS	17
Bảng 3. 1: Chú thích lệnh tấn công Slowloris	40
Bảng 4. 1: Các thuộc tính Rules của hệ thống phát hiện xâm nhập Snort	50

DANH MỤC HÌNH ẢNH

Hình 1. 1: So sánh số lượng tấn công DDoS, quý 1 và 2 năm 2020 và quý 2 năm 2019 ..	13
Hình 1. 2: Phân bố các tấn công DDoS theo quốc gia trong quý 1 và 2/2020	14
Hình 1. 3: Phân bố các tấn công DDoS riêng biệt theo địa lý trong quý 1 và quý 2/2020	15
Hình 1. 4: Các khuyến nghị để giảm thiểu nguy cơ bị tấn công DoS/DDoS	16
Hình 2. 1: Quá trình tấn công Slowloris.....	20
Hình 2. 2: Lưu đồ quy trình nghiệp vụ của tấn công slowloris	20
Hình 2. 3: Quá trình tấn công UFD Flooding.....	22
Hình 2. 4: Quá trình tấn công UFD Flooding.....	22
Hình 2. 5: Quá trình tấn công SYN Flood.....	26
Hình 2. 6: Quá trình tấn công Ping of Death.....	27
Hình 2. 7: Lưu đồ quy trình nghiệp vụ của tấn công Ping of Death	28
Hình 2. 8: Quá trình tấn công NTP Amplification	30
Hình 2. 9: Quá trình tấn công HTTP Flood.....	31
Hình 3. 1: Lưu đồ quy trình nghiệp vụ phía bị tấn công	37
Hình 3. 2: Lưu đồ quy trình nghiệp vụ phía tấn công	40
Hình 3. 3: Kết quả về việc website bị slow loading page	41
Hình 3. 4: Kết quả về việc website nhận quá nhiều kết nối	41
Hình 4. 1: Cấu trúc của Rules trong hệ thống phát hiện xâm nhập Snort	43
Hình 4. 2: Lưu đồ quy trình nghiệp vụ ngăn chặn tấn công từ chối dịch vụ.....	45
Hình 4. 3: phát hiện lỗi khi cài đặt hệ thống Snort.....	47
Hình 4. 4: Hệ thống Snort yêu cầu cổng truy cập	47
Hình 4. 5: Kết quả kiểm tra cổng truy cập	48
Hình 4. 6: Cài đặt lớp truy cập đến Servers Apache	48
Hình 4. 7: Chú thích về cài đặt cổng nhận	49
Hình 4. 8: Cài đặt cổng nhận cho hệ thống phát hiện xâm nhập Snort	49
Hình 4. 9: Tạo file chứa Rules và cài đặt lệnh Rules	50

Hình 4. 10: Khởi chạy hệ thống chống xâm nhập	52
Hình 4. 11: Hiện thị tất cả các cuộc tấn công Slowloris tới Servers Apache	52
Hình 4. 12: Kiểm tra hệ thống đã được cài vào Server	53
Hình 4. 13: Thống kê tất cả các tấn công Slowloris bị chặn lại	55
Hình 4. 14: Ngừng hoạt động CSF Firewall.....	55
Hình 4. 15: Thống kê tấn công Slowloris khi ngừng hoạt động CSF Firewall	56

MỞ ĐẦU

1. Lý do chọn đề tài

Ngày nay, mạng Internet đang phát triển và mở rộng trên phạm vi toàn thế giới. Các công 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, Attack DNS, UDP/ICMP Flooding, TCP/SYN Flooding,... 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.

Với những lợi ích đã nêu trên em xin chọn đề tài **“Tìm hiểu các phương thức tấn công từ chối dịch vụ và giải pháp ngăn chặn”** làm đề tài đồ án tốt nghiệp.

2. Mục tiêu nghiên cứu

- Đầu tiên, nghiên cứu về tấn công từ chối dịch vụ DOS/DDOS và chọn ra 1 phương thức tấn công để demo.
- Sau đó, nghiên cứu về hệ thống phát hiện xâm nhập Snort và tường lửa CSF firewall.
- Cuối cùng, sử dụng tất cả những gì đã nghiên cứu tạo ra bản demo hoàn chỉnh.

3. Đối tượng và phạm vi nghiên cứu

Lê Quang Vũ – K58

- Đối tượng nghiên cứu: tấn công từ chối dịch vụ DOS/DDOS, hệ thống phát hiện xâm nhập Snort và tường lửa CSF.
- Phạm vi nghiên cứu của đề tài tập trung vào tấn công từ chối dịch vụ DOS/DDOS và giải pháp ngăn chặn.

4. Cấu trúc báo cáo thực tập tốt nghiệp

- 1.4.1 Chương 1: Giới thiệu chung về các phương thức tấn công mạng máy tính.
- 1.4.2 Chương 2: Các hình thức tấn công từ chối dịch vụ.
- 1.4.3 Chương 3: Cài đặt phương thức tấn công từ chối dịch vụ.
- 1.4.4 Chương 4: Giải pháp ngăn chặn tấn công từ chối dịch vụ.
- 1.4.5 Chương 5: Kết luận và kiến nghị.

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ CÁC PHƯƠNG THỨC TẤN CÔNG MẠNG MÁY TÍNH

1.1 Tổng quan an toàn mạng và tấn công mạng:

1.1.1 Nguy cơ đe dọa máy tính, an toàn thông tin:

Do ảnh hưởng của Covid-19, xu hướng làm việc online của các tổ chức, doanh nghiệp trở nên phổ biến hơn. Điều này gián tiếp giúp tin tặc dễ tiếp cận thông tin của người dùng.

Năm 2020, Covid-19 bùng phát khiến hàng loạt tổ chức, doanh nghiệp phải chuyển sang làm việc từ xa. Các phần mềm làm việc trực tuyến được tìm kiếm và sử dụng phổ biến hơn. Nhiều đơn vị buộc phải mở hệ thống internet để nhân viên có thể truy cập và làm việc từ xa. Điều này tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công và đánh cắp thông tin.

Trong năm qua, hàng loạt vụ tấn công mạng quy mô lớn diễn ra trên toàn cầu. Điển hình như sự cố nhà máy của Foxconn bị tin tặc tấn công và đòi 34 triệu USD tiền chuộc dữ liệu. Một sự cố khác là Intel bị tin tặc tấn công, gây rò rỉ 20GB dữ liệu bí mật. Vì vậy, khi làm việc từ xa, các tổ chức, doanh nghiệp cần thiết lập môi trường kết nối an toàn bằng cách trang bị đầy đủ các giải pháp an ninh mạng.

Năm 2020, hàng trăm tỷ đồng đã bị tin tặc chiếm đoạt qua tấn công an ninh mạng liên quan đến ngân hàng, trong đó chủ yếu là các vụ đánh cắp mã OTP giao dịch của người dùng. Cách thức chính của tin tặc là lừa người dùng cài đặt phần mềm gián điệp trên điện thoại để lấy trộm tin nhắn OTP, thực hiện giao dịch bất hợp pháp. Điển hình là vụ việc VN84App, phần mềm thu thập tin nhắn OTP giao dịch ngân hàng, đã lây nhiễm hàng nghìn smartphone tại Việt Nam.

1.1.2 Những vấn đề đảm bảo an ninh và an toàn mạng:

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

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

1.1.3 Đối tượng tấn công mạng:

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

Các đối tượng tấn công mạng bao gồm:

- **Hacker:** Xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của hệ thống.
- **Masquerader:** Giả mạo thông tin, địa chỉ IP, tên miền, định danh người dùng.
- **Eavesdropping:** Là đối tượng nghe trộm thông tin trên mạng để lấy cắp thông tin.

1.1.4 Hệ thống CRM xây dựng trong đồ án.

Đối tượng bị tấn công có thể là cá nhân, doanh nghiệp, tổ chức hoặc nhà nước. Hacker sẽ tiếp cận thông qua mạng nội bộ (gồm máy tính, thiết bị, con người). Trong yếu tố con người, hacker có thể tiếp cận thông qua thiết bị mobile, mạng xã hội, ứng dụng phần mềm.

1.1.5 Các lỗ hổng trong bảo mật và phương thức tấn công mạng:

- Các loại lỗ hổng trong bảo mật:
 - **Lỗ hổng loại C:** Cho phép thực hiện hình thức tấn công theo kiểu DoS (Denial of Services – Từ chối dịch vụ) làm ảnh hưởng tới chất lượng dịch vụ, ngưng trệ, gián đoạn hệ thống, nhưng không phá hỏng dữ liệu hoặc đoạt được quyền truy cập hệ thống.
 - **Lỗ hổng loại B:** Lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến lộ, lọt thông tin.
 - **Lỗ hổng loại A:** Cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống.
- Các hình thức tấn công mạng phổ biến:
 - **Tấn công trực tiếp:** Sử dụng một máy tính để tấn công một máy tính khác với mục đích dò tìm mật mã, tên tài khoản tương ứng, Kẻ tấn công có thể sử dụng một số chương trình giải mã để giải mã các file chứa password

trên hệ thống máy tính của nạn nhân. Do đó, những mật khẩu ngắn và đơn giản thường rất dễ bị phát hiện.

- **Kỹ thuật đánh lừa (Social Engineering):** Đây là thủ thuật được nhiều hacker sử dụng cho các cuộc tấn công thâm nhập vào hệ thống mạng và máy tính bởi tính đơn giản mà hiệu quả của nó. Kỹ thuật này thường được sử dụng để lấy cắp mật khẩu, thông tin, tấn công vào và phá hủy hệ thống. Ví dụ, kỹ thuật đánh lừa Fake Email Login.
- **Kỹ thuật tấn công vào vùng ẩn:** Những phần bị giấu đi trong các website thường chứa những thông tin về phiên làm việc của các client. Các phiên làm việc này thường được ghi lại ở máy khách chứ không tổ chức cơ sở dữ liệu trên máy chủ. Vì vậy, người tấn công có thể sử dụng chiêu thức View Source của trình duyệt để đọc phần đầu đi này và từ đó có thể tìm ra các sơ hở của trang Web mà họ muốn tấn công. Từ đó, có thể tấn công vào hệ thống máy chủ.
- **Tấn công vào các lỗ hổng bảo mật:** Hiện nay, các lỗ hổng bảo mật được phát hiện càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Các hãng sản xuất cũng luôn cập nhật các bản vá lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước. Do đó, người sử dụng phải luôn cập nhật thông tin và nâng cấp phiên bản cũ mà mình đang sử dụng để tránh các hacker lợi dụng điều này tấn công vào hệ thống.
- **Khai thác tình trạng tràn bộ đệm:** Tràn bộ đệm là một tình trạng xảy ra khi dữ liệu được gửi quá nhiều so với khả năng xử lý của hệ thống hay CPU. Nếu hacker khai thác tình trạng tràn bộ đệm này thì họ có thể làm cho hệ thống bị tê liệt hoặc làm cho hệ thống mất khả năng kiểm soát.
- **Nghe trộm:** Các hệ thống trao đổi thông tin qua mạng đôi khi không được bảo mật tốt và lợi dụng điều này, hacker có thể truy cập vào data paths để nghe trộm hoặc đọc trộm luồng dữ liệu truyền qua.
- **Kỹ thuật giả mạo địa chỉ:** Thông thường, các mạng máy tính nối với Internet đều được bảo vệ bằng tường lửa. Tường lửa có thể hiểu là cổng duy nhất mà người đi vào nhà hay đi ra cũng phải qua đó. Tường lửa hạn chế rất nhiều khả năng tấn công từ bên ngoài và gia tăng sự tin tưởng lẫn nhau trong việc sử dụng tài nguyên chia sẻ trong mạng nội bộ.

- **Kỹ thuật chèn mã lệnh:** Một kỹ thuật tấn công căn bản và được sử dụng cho một số kỹ thuật tấn công khác là chèn mã lệnh vào trang web từ một máy khách bất kỳ của người tấn công.
- **Kỹ thuật chèn mã lệnh:** cho phép người tấn công đưa mã lệnh thực thi vào phiên làm việc trên web của một người dùng khác. Khi mã lệnh này chạy, nó sẽ cho phép người tấn công thực hiện nhiều hành vi như giám sát phiên làm việc trên trang web hoặc có thể toàn quyền điều khiển máy tính của nạn nhân. Kỹ thuật tấn công này thành công hay thất bại tùy thuộc vào khả năng và sự linh hoạt của người tấn công.
- **Tấn công vào hệ thống có cấu hình không an toàn:** Cấu hình không an toàn cũng là một lỗ hổng bảo mật của hệ thống. Các lỗ hổng này được tạo ra do các ứng dụng có các thiết lập không an toàn hoặc người quản trị hệ thống định cấu hình không an toàn. Chẳng hạn như cấu hình máy chủ web cho phép ai cũng có quyền duyệt qua hệ thống thư mục. Việc thiết lập như trên có thể làm lộ các thông tin nhạy cảm như mã nguồn, mật khẩu hay các thông tin của khách hàng.
- **Tấn công dùng Cookies:** Cookie là những phần tử dữ liệu nhỏ có cấu trúc được chia sẻ giữa website và trình duyệt của người dùng. Cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (size dưới 4KB). Chúng được các site tạo ra để lưu trữ, truy tìm, nhận biết các thông tin về người dùng đã ghé thăm site và những vùng mà họ đi qua trong site. Những thông tin này có thể bao gồm tên, định danh người dùng, mật khẩu, sở thích, thói quen,
- **Can thiệp vào tham số trên URL:** Đây là cách tấn công đưa tham số trực tiếp vào URL. Việc tấn công có thể dùng các câu lệnh SQL để khai thác cơ sở dữ liệu trên các máy chủ bị lỗi. Điển hình cho kỹ thuật tấn công này là tấn công bằng lỗi “SQL INJECTION”. Kiểu tấn công này gọn nhẹ nhưng hiệu quả bởi người tấn công chỉ cần một công cụ tấn công duy nhất là trình duyệt web và backdoor.
- **Từ chối dịch vụ:** Kiểu tấn công này thông thường làm tê liệt một số dịch vụ, được gọi là DoS (Denial of Service - Tấn công từ chối dịch vụ). Các tấn công này lợi dụng một số lỗi trong phần mềm hay các lỗ hổng bảo mật trên hệ thống, hacker sẽ ra lệnh cho máy tính của chúng gửi yêu cầu đến các máy chủ ứng dụng, thường là các server trên mạng. Các yêu cầu này được

gửi đến liên tục làm cho hệ thống nghẽn mạch và một số dịch vụ sẽ không đáp ứng được cho khách hàng thật sự.

1.2 Giới thiệu kỹ thuật tấn công DoS:

1.2.1 Giới thiệu tấn công DoS:

- Tấn công DoS là một kiểu tấn công mà người làm cho 1 hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.
- Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).
- Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công.

1.2.2 Lịch sử các cuộc tấn công và phát triển của DoS:

- Các tấn công DoS bắt đầu vào khoảng đầu những năm 90. Đầu tiên, chúng hoàn toàn “nguyên thủy”, bao gồm chỉ một kẻ tấn công khai thác băng thông tối đa từ nạn nhân, ngăn những người khác được phục vụ. Điều này được thực hiện chủ yếu bằng đó, các cuộc tấn công trở nên phức tạp hơn, bằng cách giả làm nạn nhân, gửi vài thông điệp và để các máy khác làm ngập máy nạn nhân với các thông điệp trả lời (Smurf attack, IP spoofing,...).
- Các tấn công này phải được đồng bộ hóa một cách thủ công bởi nhiều kẻ tấn công để tạo ra 1 sự phá hủy có hiệu quả. Sự dịch chuyển đến việc tự động hóa sự đồng bộ, kết hợp này và tạo ra một tấn công song song lớn trở nên phổ biến từ 1997, với sự ra đời của công cụ tấn công DDoS đầu tiên được công bố rộng rãi, đó là Trinoo. Nó dựa trên tấn công UDP flood và các giao tiếp master-slave (khiến các máy trung gian tham gia vào trong cuộc tấn công bằng cách đặt lên chúng các chương trình được điều khiển từ xa). Trong những năm tiếp theo, vài công cụ nữa được phổ biến – TFN (tribe flood network), TFN2K, và Stacheldraht.
- Tuy nhiên, chỉ từ cuối năm 1999 mới có những báo cáo về những tấn công như vậy, và đề tài này được công chúng biết đến chỉ sau khi một cuộc tấn công lớn vào các site công cộng tháng 2/2000.
- Từ đó các cuộc tấn công DoS thường xuyên xảy ra. Ví dụ:

- Vào ngày 15 tháng 8 năm 2003, Microsoft đã chịu đợt tấn công DoS cực mạnh và làm gián đoạn website trong vòng 2 giờ.
- Vào lúc 15:09 giờ GMT ngày 27 tháng 3 năm 2003: toàn bộ phiên bản tiếng anh của website Al-Jazeera bị tấn công làm gián đoạn trong nhiều giờ.

1.2.3 Mục đích của tấn công DoS và hiểm họa:

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó.
- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.
- Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó như bị:
 - Disable Network – Tắt mạng
 - Disable Organization – Tổ chức không hoạt động
 - Financial Loss – Tài chính bị mất
- Như chúng ta biết ở bên trên tấn công DoS xảy ra khi kẻ tấn công sử dụng hết tài nguyên của hệ thống và hệ thống không thể đáp ứng cho người dùng bình thường được vậy các tài nguyên chúng thường sử dụng để tấn công là gì:
 - Chúng sẽ tạo ra sự khan hiếm, những giới hạn và không đổi mới tài nguyên.
 - Băng thông của hệ thống mạng (Network Bandwidth), bộ nhớ, ổ đĩa, và CPU Time hay cấu trúc dữ liệu đều là mục tiêu của tấn công DoS.
 - Tấn công vào hệ thống khác phục vụ cho mạng máy tính như: hệ thống điều hòa, hệ thống điện, hệ thống làm mát và nhiều tài nguyên khác của doanh nghiệp. Bạn thử tưởng tượng khi nguồn điện vào máy chủ web bị ngắt thì người dùng có thể truy cập vào máy chủ đó không.
 - Phá hoại hoặc thay đổi các thông tin cấu hình.
 - Phá hoại tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hòa,...

1.3 Giới thiệu kỹ thuật tấn công DDoS:

1.3.1 Giới thiệu tấn công DDoS:

- DDoS là viết tắt của Distributed Denial-of-Service (Tấn công từ chối dịch vụ phân tán). Tấn công DDoS xảy ra khi các server và mạng bị tràn ngập với lưu lượng truy cập nhiều quá mức. Mục đích của DDoS là áp đảo các trang web hoặc server với lượng lớn request, khiến hệ thống không thể hoạt động nữa.
- Thứ hai là khái niệm botnet – là các mạng lưới máy tính rất rộng lớn. Botnet thường được sử dụng để thực hiện các cuộc tấn công DDoS. Chúng thường bao gồm các máy tính bị xâm nhập (thiết bị IOT, server, máy trạm, router...) được điều khiển bởi server trung tâm.
- Các cuộc tấn công DDoS cũng có thể được bắt nguồn từ hàng chục ngàn máy tính được kết nối mạng với nhau. Các máy này không phải botnet, tức là không bị xâm nhập. Thay vào đó, chúng là những máy bị cấu hình sai, hoặc chỉ đơn giản là bị lừa tham gia vào một botnet.

1.3.2 Lịch sử các cuộc tấn công và phát triển của DDoS:

- **Estonia: 27/4/2007**
 - Điềm qua một chút về bối cảnh xã hội lúc bấy giờ ở Estonia. Khi đó đang có một sự phân chia chính trị về một nghĩa trang quân sự ở Estonia. Đối với cộng đồng người Estonia nói tiếng Nga, bức tượng đại diện cho sự giải phóng của Đức quốc xã. Mặt khác, những người dân tộc Estonian lại cho rằng đó là biểu tượng của sự áp bức từ Liên Xô.
 - Vào ngày 27/4 năm 2007, một loạt các cuộc tấn công mạng đã nổ ra. Hầu hết đó là các cuộc tấn công DDoS. Các cá nhân đã sử dụng ping flood và botnet để spam và lật đổ nhiều tổ chức tài chính. Cùng với đó là nhiều cơ quan chính phủ lẫn cửa hàng truyền thông. Các cuộc tấn công này hiện vẫn được coi là một trong những cuộc tấn công tinh vi nhất. Đồng thời, đây cũng là một ví dụ tiêu biểu về tấn công chính trị bằng DDoS.
- **Cộng hòa Georgia: 20/7/2008**
 - Vào năm 2008, Cộng hòa Georgia đã trải qua một đợt tấn công DDoS khổng lồ. Nó diễn ra chỉ vài tuần trước khi bị xâm lược bởi Nga. Cuộc tấn công này dường như nhắm vào tổng thống Georgia, hạ gục các trang web chính phủ. Sau này, các cuộc tấn công được cho rằng là để giảm nỗ lực giao

tiếp với những người ủng hộ Đảng Georgia. Không lâu sau đó, Georgia trở thành nạn nhân trong cuộc xâm lăng của nước Nga.

- Cuộc tấn công này đã được ghi chép lại như một ví dụ về tấn công mạng kết hợp với tấn công vật lý. Cuộc tấn công này được nghiên cứu trên toàn thế giới. Không chỉ bởi các chuyên gia mạng mà còn bởi các nhóm quân sự.

- **Spamhaus: 18/3/2013**

- Spamhaus, hay còn được gọi là “Cuộc tấn công gần như đã phá vỡ cả Internet”. Lúc bấy giờ, đây chính là cuộc tấn công DDoS lớn nhất trong lịch sử internet.
- Cuộc tấn công được thúc đẩy khi một nhóm có tên Cyberpunk bị blacklist bởi Spamhaus. Nhằm trả thù, nhóm đã nhắm vào tổ chức anti-spam đang cố gắng cắt giảm nỗ lực spam với một cuộc tấn công DDoS. Cuối cùng, tổng dữ liệu của đợt tấn công DDoS này lên đến 300 Gbps.
- Lần tấn công này lớn đến nỗi nó đã hạ gục được cả CloudFlare, một công ty bảo mật internet được thiết kế đặc biệt để chống lại các cuộc tấn công này. Và CloudFlare đã gục ngã hoàn toàn chỉ trong một thời gian ngắn ngủi.

- **Occupy Central: Tháng 6/2014**

- Occupy Central – Chiến dịch chiếm lĩnh Trung Hoàn từng nổ ra ở Hong Kong vào năm 2014. Trong giai đoạn này, các cuộc tấn công DDoS được thực hiện với mục đích làm tê liệt các cuộc biểu tình dân chủ đang xảy ra vào lúc đó. Hai trang web tin tức, Apple Daily và PopVote lúc ấy cũng đã phát hành các nội dung nhằm hỗ trợ phe dân chủ.
- Cuộc tấn công này còn lớn hơn nhiều so với Spamhaus, với tổng dữ liệu đạt đến 500 Gbps. Cuộc tấn công này đã phá vỡ khả năng phát hiện bằng cách nguy trang các packet giống như lưu lượng bình thường. Nhiều người cho rằng cuộc tấn công này được triển khai bởi chính phủ Trung Quốc. Với mục đích giảm suy yếu sự ủng hộ dành cho phe dân chủ.

- **Dyn: 21/10/2016**

- Năm 2016, một cuộc tấn công DDoS khổng lồ đã được triển khai để chống lại nhà cung cấp DNS Dyn. Nó nhằm vào các server của công ty bằng botnet Mirai, chiếm lấy hàng ngàn trang web. Cuộc tấn công này đã ảnh hưởng nghiêm trọng đến thị trường chứng khoán. Đồng thời cũng là hồi chuông cảnh tỉnh về các lỗ hổng của thiết bị IOT.

- Botnet Mirai bao gồm một nhóm các thiết bị IOT được kết nối với nhau. Các botnet được tạo bằng cách khai thác thông tin đăng nhập trên các thiết bị tiêu dùng. Các thông tin này hầu như không bao giờ được thay đổi bởi các người dùng. Cuộc tấn công này đã ảnh hưởng đến 69 công ty khác nữa. Trong đó bao gồm cả các nhà sản xuất lớn như Amazon, CNN và Visa.

- **GitHub: 28/8/2018**

- Một trong những cuộc tấn công DDoS lớn nhất lịch sử đã được nhắm vào GitHub. Đây chính là một trong những nền tảng phát triển nổi tiếng nhất thế giới. Vào lúc đó, đây chính là cuộc tấn công lớn nhất từng xuất hiện. Tuy nhiên, nhờ vào các biện pháp phòng chống DDoS hiệu quả, nền tảng chỉ bị offline trong vài phút.
- Các kẻ tấn công đã giả mạo địa chỉ IP của GitHub, lấy được quyền truy cập vào memcached để tăng lượng lưu lượng vào nền tảng. Tuy vậy, tổ chức đã nhanh chóng cảnh báo hỗ trợ. Sau đó, các lưu lượng đã được chuyển qua những trung tâm khác để hạn chế thiệt hại. GitHub đã hoàn tất việc sao lưu và tái hoạt động chỉ trong 10 phút.

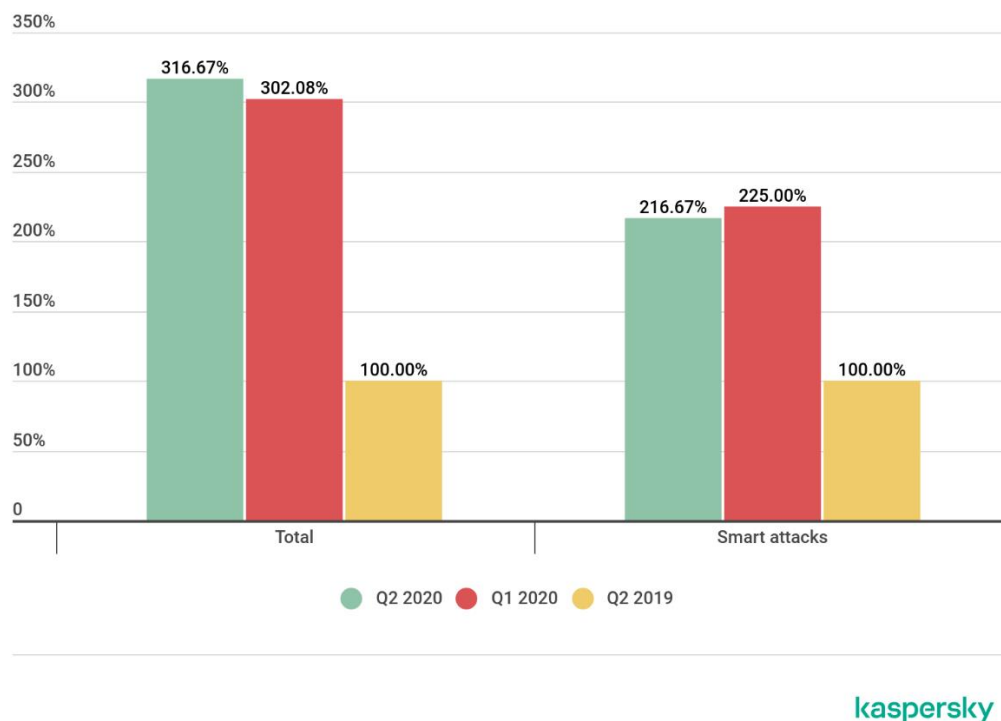
1.3.3 Mục đích của tấn công DDoS và hiểm họa:

- Mục đích của tấn công DDoS:
 - **Tài chính:** Tấn công DDoS thường được kết hợp tấn công ransomware. Những kẻ tấn công thường là một phần của một nhóm tội phạm có tổ chức. Thậm chí, các doanh nghiệp đối thủ cũng có thể thực hiện tấn công DDoS để có được lợi thế cạnh tranh.
 - **Bất đồng về ý thức hệ:** Các cuộc tấn công thường nhắm vào các cơ quan quản lý hay các nhóm biểu tình áp bức trong chính trị. Những cuộc tấn công này thường được tiến hành để hỗ trợ một hệ thống chính trị hay tôn giáo cụ thể.
 - **Chiến thuật:** Trong trường hợp này, tấn công DDoS thường chỉ là một phần trong các chiến dịch lớn. Đôi khi, các chiến dịch còn kết hợp với tấn công vật lý hay tấn công phần mềm.
 - **Thương mại:** Tấn công DDoS có thể thu thập được những thông tin hoặc gây thiệt hại cho các ngành công nghiệp cụ thể. Lấy ví dụ, các cuộc tấn công vào Sony, British Airways...khiến người tiêu dùng mất niềm tin vào cả ngành công nghiệp ấy.

- **Tống tiền:** Các cuộc tấn công có thể được sử dụng cho các lợi ích cá nhân, hoặc thậm chí tống tiền.
- **Tấn công do nhà nước:** Một số cuộc tấn công DDoS được tiến hành nhằm gây rối loạn trong quân sự cũng như người dân.
- **Hiểm họa của tấn công DDoS:**
 - Các threat actor ngày càng tận dụng DDoS để tống tiền bằng cách làm sập hạ tầng mạng nếu không trả tiền. Trong một số trường hợp, nó được sử dụng để làm mất tập trung nạn nhân. Sau đó thực hiện các hành động chính như đánh cắp dữ liệu, tấn công Ransomware.
 - Tất nhiên những điều này chưa đủ, DDoS đã dần trở thành một yếu tố cạnh tranh phi đạo đức. Các doanh nhân xấu sẽ sử dụng nó như một phương thức ngăn cản đối thủ của họ. Bởi vì sử dụng dịch vụ không bị gián đoạn rất quan trọng với doanh nghiệp. Downtime có thể ảnh hưởng trực tiếp đến trải nghiệm của khách hàng. Dẫn đến các vấn đề nghiêm trọng khác, khiến doanh nghiệp tổn thất tài chính.
 - DDoS đang tiến triển mạnh mẽ với những công nghệ tiên tiến trên toàn cầu. Nó đã khiến các tổ chức và chính phủ phải cảnh giác trong hơn hai thập kỷ. Trong quý 1 năm 2020, số lượng cuộc tấn công tăng gấp đôi so với quý 4 năm 2019. Điều đó đồng nghĩa với việc các mối đe dọa đang ngày càng leo thang.

1.4 Các số liệu tấn công DoS/DDoS:

- Các chuyên gia có nhận xét, các tội phạm mạng tiếp tục xu hướng tìm kiếm các lỗ hổng an toàn thông tin mới và dự báo rằng, trong thời gian tới sẽ có thêm nhiều các phương pháp tấn công tinh vi khác góp phần vào khuếch đại tấn công DDoS.
- Báo cáo tấn công DDoS quý 2/2020 từ Kaspersky cho thấy số lượng tấn công DDoS quý 2/2020 cao hơn gần 217% so với cùng kỳ năm 2019. Kết quả này trái ngược với xu hướng hàng năm mà các nhà nghiên cứu của Kaspersky đã ghi nhận được.
- Thông thường, số lượng các cuộc tấn công DDoS sẽ thay đổi theo mùa. Đầu năm thường là thời gian có tổng tấn công DDoS cao hơn, vì đây là mùa cao điểm kinh doanh và số lượng tấn công sẽ giảm dần vào cuối mùa xuân và mùa hè. Ví dụ: số lượng tấn công DDoS quý 2/2019 đã giảm 39% so với quý 1/2019, và của quý 2/2018 thấp hơn 34% so với quý 1/2018.

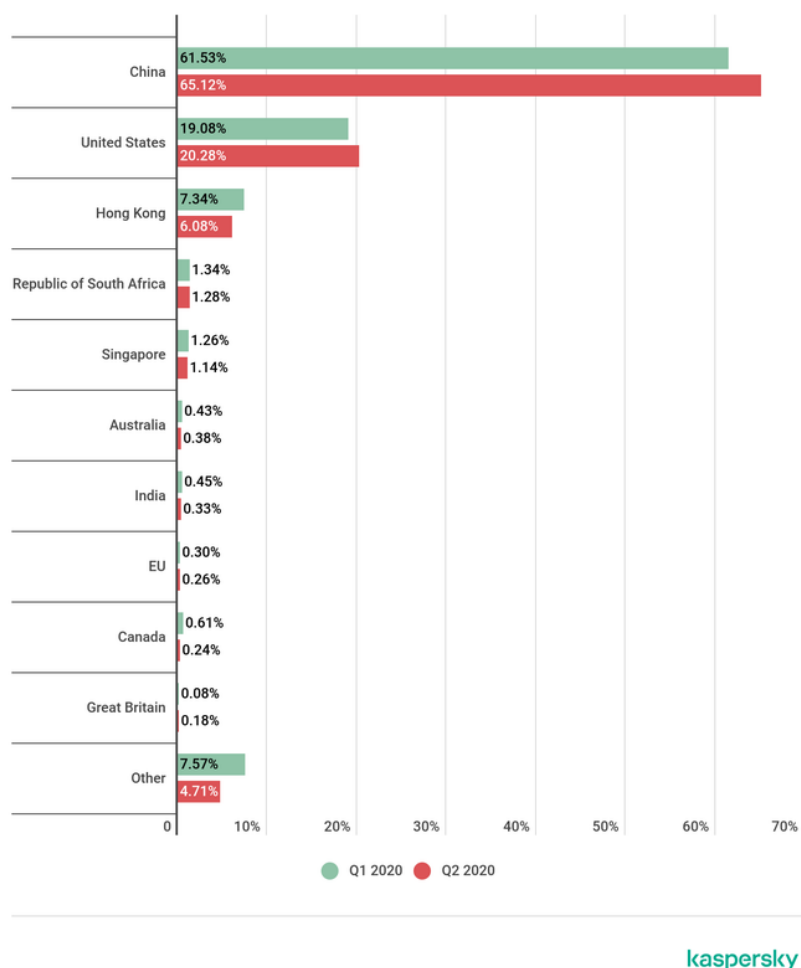


Hình 1. 1: So sánh số lượng tấn công DDoS, quý 1 và 2 năm 2020 và quý 2 năm 2019

- Ta có thể thấy số lượng cuộc tấn công trung bình mỗi ngày trong quý 2/2020 đã tăng gần 30% so với quý 1/2020 và số lượng cuộc tấn công nhiều nhất trong 1 ngày được ghi nhận là gần 300 tấn công trong quý 2(diễn ra vào ngày 9/4), trong khi kỷ lục của quý 1/2020 là 242 tấn công.
- Ông Alexey Kiselev, Giám đốc phát triển kinh doanh của nhóm Kaspersky DDoS Protection cho biết: “Năm nay, mọi người không thể tận hưởng một kỳ nghỉ hè như thường lệ vì nhiều khu vực đã áp dụng biện pháp ngăn chặn COVID-19. Điều này khiến nhiều người phải dành nhiều thời gian online hơn cho cả hoạt động cá nhân và công việc. Kết quả là, chúng ta đã chứng kiến sự gia tăng chưa từng có đối với tấn công DDoS. Cho đến nay, chưa có dấu hiệu cho thấy tấn công sẽ sụt giảm.”
- Phân bố địa lý của các cuộc tấn công:
 - Dẫn đầu về số lượng các cuộc tấn công DDoS trong quý 2 là Trung Quốc, với tỷ lệ thay đổi không đáng kể (65,12% so với 61,53% trong quý 1).
 - Đứng ở vị trí thứ 2 là Mỹ (20,28%). Hồng Kông vẫn nằm trong vào Top 3 (6,08%). Xuất hiện trong top 10 bảng xếp hạng tấn công DDoS của quý 2/2020 còn có Cộng hòa Nam Phi (1,28%, đứng vị trí thứ 4), Singapore (1,14%, đứng vị trí thứ 5), Australia (0,38%, đứng vị trí thứ 6), Ấn Độ

(0,33%, đứng vị trí thứ 7), châu Âu (0,26%, đứng vị trí thứ 8), Canada (0,24%, đứng vị trí thứ 9) và Anh (0,18%, đứng vị trí thứ 10).

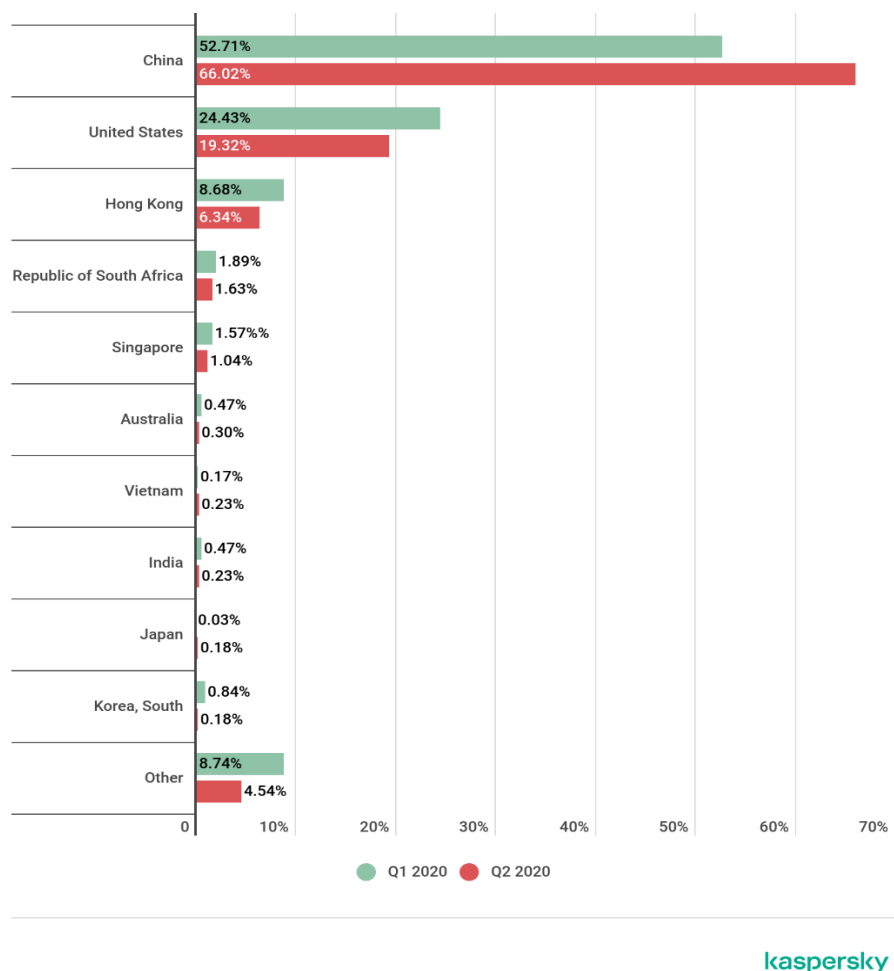
- Điều đáng chú ý là Anh mới xuất hiện trong bảng xếp hạng, thay vị trí của Hàn Quốc trong quý trước. Romania, đã trượt từ vị trí thứ 4 xuống vị trí 17, rời khỏi top 10.



Hình 1. 2: Phân bố các tấn công DDoS theo quốc gia trong quý 1 và 2/2020

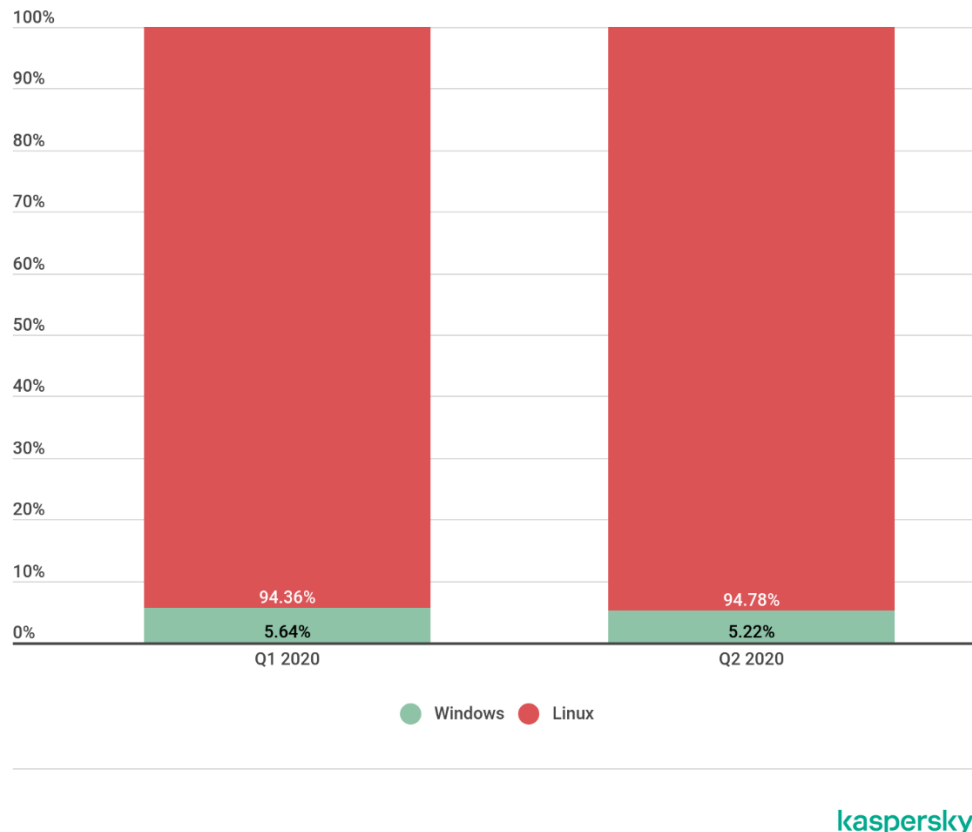
- Phân bố các mục tiêu riêng biệt theo lãnh thổ tương tự với sự phân bố số lượng các cuộc tấn công: Trung Quốc có tỷ trọng lớn nhất (66,02%). Vị trí thứ 2 thuộc về Mỹ (19,32%) và thứ 3 là Hồng Kông (6,34%), thứ 4 là Nam Phi (1,63%) và thứ 5 là Singapore (1,04%). Như vậy, chỉ có Trung Quốc tăng tỷ trọng mục tiêu so với kỳ báo cáo trước đó, tăng 13,31% trong khi các quốc gia còn lại đều giảm nhẹ.
- Vị trí thứ 6 thuộc về Úc (0,3%), nhảy từ vị trí thứ 9 trong quý đầu tiên. Ngoài ra, Việt Nam đã trở lại top 10 sau một thời gian ngắn vắng mặt: với sự gia tăng nhỏ về tỷ trọng mục tiêu trên lãnh thổ của mình (tăng 0,06 %, lên 0,23%), Việt Nam chiếm vị trí 7, thay cho Hàn Quốc quý trước (hiện đứng vị trí thứ 10). Hai quốc gia

còn lại bảng xếp hạng top 10 quý này là Ấn Độ (0,23%) và Nhật Bản (0,18%), lần lượt vị trí thứ 8 và 9.



Hình 1. 3: Phân bố các tấn công DDoS riêng biệt theo địa lý trong quý 1 và quý 2/2020

- Phân bố tấn công DDoS theo loại:
 - Tấn công botnet dựa trên Linux chiếm tỷ lệ nhiều hơn hẳn với 94,78%, tấn công botnet dựa trên Windows giảm, chiếm 5,22% (quý 1 là 4,81%).



Hình 1. 4: Các khuyến nghị để giảm thiểu nguy cơ bị tấn công DoS/DDoS

- Các chuyên gia của Kaspersky khuyến nghị các doanh nghiệp nên duy trì hoạt động của tài nguyên web bằng cách tham khảo ý kiến từ các chuyên gia am hiểu biện pháp ứng phó với tấn công DDoS. Các doanh nghiệp cũng cần luôn sẵn sàng để đáp ứng công việc ngoài giờ, kể cả vào buổi tối và cuối tuần.
- Xác thực các thỏa thuận và thông tin liên hệ của bên thứ ba - bao gồm những thỏa thuận được thực hiện với nhà cung cấp dịch vụ Internet - là cần thiết.
- Những điều này sẽ giúp chúng ta nhanh chóng truy cập các thỏa thuận trong trường hợp bị tấn công DoS/DDoS.

1.5 Sự khác biệt của 2 kiểu tấn công DoS và DDoS:

Bảng 1. 1: Sự khác biệt của 2 kiểu tấn công DoS và DDoS

DoS	DDoS
DoS là viết tắt của Denial of service	DDoS là viết tắt của Distributed Denial of service
Trong cuộc tấn công DoS, chỉ một hệ thống nhắm mục tiêu vào hệ thống nạn nhân.	Trong DDoS, nhiều hệ thống tấn công hệ thống nạn nhân.
PC bị nhắm mục tiêu được load từ gói dữ liệu gửi từ một vị trí duy nhất.	PC bị nhắm mục tiêu được load từ gói dữ liệu gửi từ nhiều vị trí.
Tấn công DoS chậm hơn so với DDoS.	Tấn công DDoS nhanh hơn tấn công DoS.
Có thể bị chặn dễ dàng vì chỉ sử dụng một hệ thống.	Rất khó để ngăn chặn cuộc tấn công này vì nhiều thiết bị đang gửi gói tin và tấn công từ nhiều vị trí.
Trong cuộc tấn công DoS, chỉ một thiết bị duy nhất được sử dụng với các công cụ tấn công DoS.	Trong cuộc tấn công DDoS, nhiều bot được sử dụng để tấn công cùng một lúc.
Các cuộc tấn công DoS rất dễ theo dõi.	Các cuộc tấn công DDoS rất khó theo dõi.
Lưu lượng truy cập trong cuộc tấn công DoS ít hơn so với DDoS.	Các cuộc tấn công DDoS cho phép kẻ tấn công gửi một lượng lớn lưu lượng truy cập đến mạng nạn nhân.
Các loại tấn công DoS là: 1. Tấn công tràn bộ đệm 2. Tấn công Ping of Death hoặc ICMP flood 3. Tấn công Teardrop Attack	Các loại tấn công DDoS là: 1. Tấn công Volumetric (tấn công băng thông) 2. Tấn công Fragmentation Attack (phân mảnh dữ liệu) 3. Application Layer Attack (khai thác lỗ hổng trong các ứng dụng)

1.6 Kết luận chương:

- Trong chương này, em đã giới thiệu về tổng quan của tấn công mạng máy tính cũng như tấn công từ chối dịch vụ, giới thiệu về nguy hiểm và lịch sử cũng như trình bày các mục đích của tấn công từ chối dịch vụ.
- Ngoài ra, em còn giới thiệu về sự khác biệt của 2 loại tấn công từ chối dịch vụ DoS/DDoS và các số liệu của các cuộc tấn công được cập nhật gần nhất. Em cũng giới thiệu về tấn công mạng cũng như các vấn đề để đảm bảo an ninh mạng cho các doanh nghiệp và cá nhân có thể đảm bảo an toàn. Theo như ở trên đã phân tích em thấy được hình thức tấn công từ chối dịch vụ DDoS mạnh hơn DoS rất nhiều nên em sẽ phân tích 1 số tấn công phổ biến của tấn công từ chối dịch vụ DDoS ở chương 2 tiếp theo.

CHƯƠNG 2. CÁC HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ DDOS

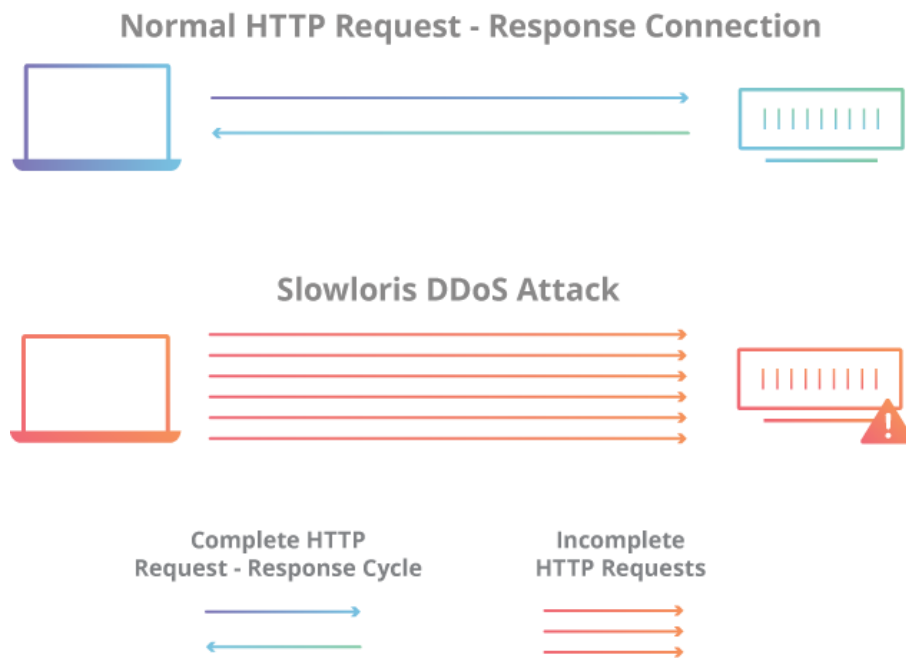
2.1 Các loại tấn công DDoS cơ bản:

- Mặc dù DDoS có những chế độ tấn công ít phức tạp hơn những hình thức tấn công mạng khác, nhưng chúng ta phải cẩn thận vì chúng càng ngày càng trở nên tinh vi và mạnh hơn. Có 3 loại tấn công DDoS cơ bản như sau:
- **Volume-based attacks:** Loại tấn công sử dụng lưu lượng truy cập cao để làm ngập băng thông mạng.
- **Protocol attacks:** Loại tấn công tập trung vào việc khai thác nguồn tài nguyên máy chủ.
- **Application attacks:** Tấn công nhắm vào các ứng dụng web và được coi là một loại tấn công tinh vi và nghiêm trọng nhất.

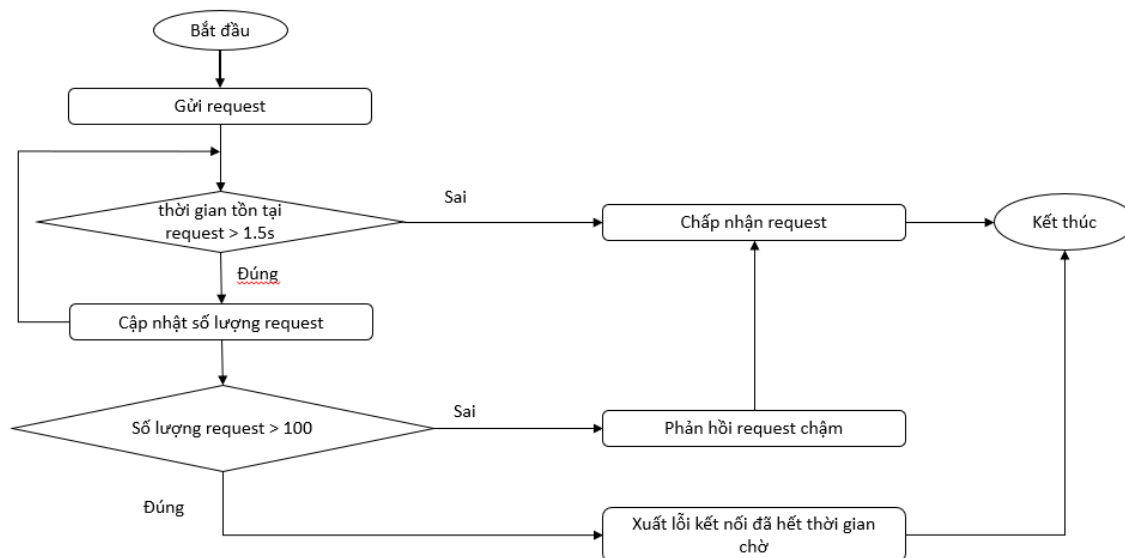
2.2 Tấn công Slowloris:

2.2.1 Khái niệm:

- Slowloris là một cuộc tấn công lớp ứng dụng hoạt động bằng cách sử dụng các yêu cầu HTTP một phần. Các chức năng tấn công bằng cách mở các kết nối đến một máy chủ Web được nhắm mục tiêu và sau đó giữ cho các kết nối đó mở miễn là có thể.
- Là một công cụ tấn công cụ thể được thiết kế để cho phép một máy duy nhất hạ gục máy chủ mà không cần sử dụng nhiều băng thông.
- Không giống như các cuộc tấn công DDoS dựa trên phản xạ tiêu thụ băng thông như khuếch đại NTP, kiểu tấn công này sử dụng lượng băng thông thấp và thay vào đó nhằm mục đích sử dụng hết tài nguyên máy chủ với các yêu cầu có vẻ chậm hơn bình thường nhưng lại bắt buộc lưu lượng thông thường.
- Nó nằm trong danh mục các cuộc tấn công được gọi là các cuộc tấn công thấp và chậm. Máy chủ được nhắm mục tiêu sẽ chỉ có rất nhiều luồng có sẵn để xử lý các kết nối đồng thời. Mỗi luồng máy chủ sẽ cố gắng duy trì sự sống trong khi chờ yêu cầu chậm hoàn thành, điều này không bao giờ xảy ra. Khi vượt quá các kết nối tối đa có thể của máy chủ, mỗi kết nối bổ sung sẽ không được trả lời và từ chối dịch vụ sẽ xảy ra.



Hình 2. 1: Quá trình tấn công Slowloris



Hình 2. 2: Lưu đồ quy trình nghiệp vụ của tấn công slowloris

2.2.2 Lịch sử xuất hiện:

- Amit Klein đã chỉ cho em một bài đăng của Adrian Ilarion Ciobanu được viết vào đầu năm 2007 mô tả hoàn hảo về cuộc tấn công từ chối dịch vụ slowloris. Nó cũng được mô tả vào năm 2005 trong phần "Các cuộc tấn công theo mô hình lập trình" của Apache Security.

2.2.3 Cơ chế tấn công:

- Slowloris được tiếp hành theo các bước sau:
 - **Bước 1:** Kẻ tấn công trước tiên mở nhiều kết nối đến máy chủ được nhắm mục tiêu bằng cách gửi nhiều yêu cầu HTTP một phần.
 - **Bước 2:** Mục tiêu mở một luồng cho mỗi yêu cầu đến, với mục đích đóng luồng sau khi kết nối hoàn tất. Để có hiệu quả, nếu kết nối mất quá nhiều thời gian, máy chủ sẽ hết thời gian kết nối quá dài, giải phóng chuỗi cho yêu cầu tiếp theo.
 - **Bước 3:** Để ngăn chặn mục tiêu hết thời gian kết nối, kẻ tấn công định kỳ gửi các tiêu đề yêu cầu một phần đến mục tiêu để giữ cho yêu cầu tồn tại.
 - **Bước 4:** Máy chủ được nhắm mục tiêu không bao giờ có thể phát hành bất kỳ kết nối một phần mở nào trong khi chờ kết thúc yêu cầu. Khi tất cả các luồng có sẵn đang được sử dụng, máy chủ sẽ không thể đáp ứng các yêu cầu bổ sung được thực hiện từ lưu lượng truy cập thông thường, dẫn đến từ chối dịch vụ.

2.2.4 Mức độ phá hoại:

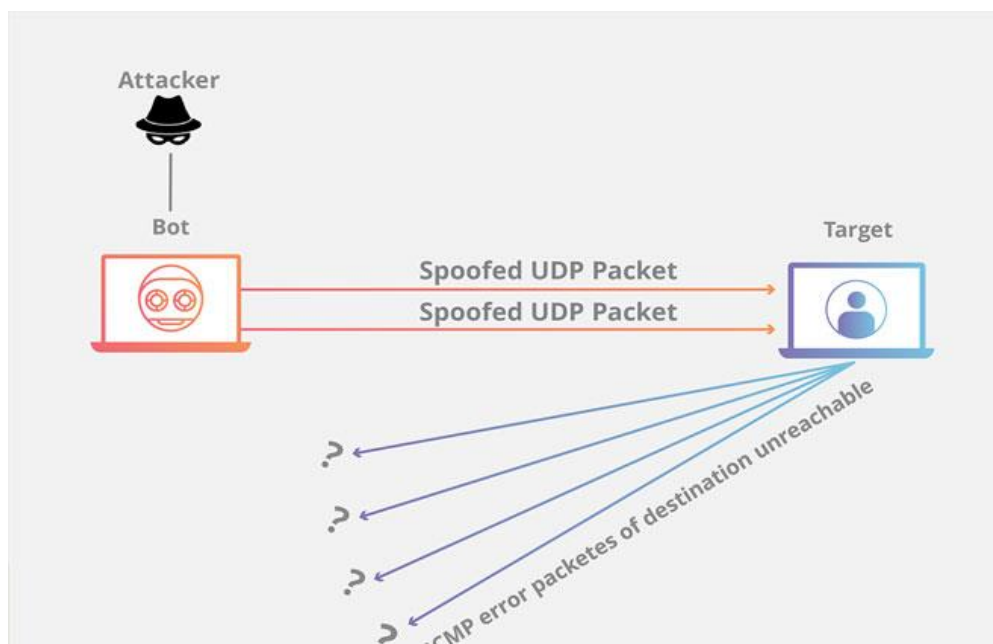
- Máy chủ được nhắm mục tiêu sẽ bị lấp đầy bởi các gói tin và các nỗ lực kết nối bổ sung (hợp pháp) sẽ bị từ chối. Khi máy chủ bị quá nhiều gói tin cũng có thể dẫn đến sập server và không khởi động lại trong khoảng thời gian tấn công.

2.3 Tấn công UDP Flood:

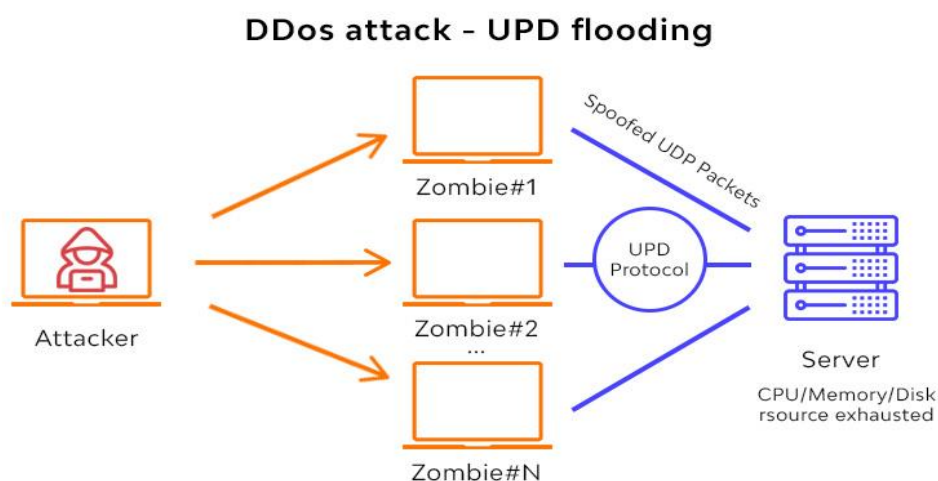
2.3.1 Khái niệm:

- UDP (User Datagram Protocol) là một giao thức kết nối không tin cậy. Một cuộc tấn công gây ngập lụt UDP có thể được bắt đầu bằng cách gửi một số lượng lớn các gói tin UDP tới cổng ngẫu nhiên trên một máy chủ từ xa và kết quả là các máy chủ ở xa sẽ:
 - Kiểm tra các ứng dụng với cổng.
 - Thấy rằng không có ứng dụng nghe ở cổng.
 - Trả lời với một ICMP Destination Unreachable gói.
- Hệ thống nạn nhân sẽ bị buộc nhận nhiều gói tin ICMP, dẫn đến mất khả năng xử lý các yêu cầu của các khách hàng thông thường. Những kẻ tấn công cũng có thể giả mạo địa chỉ IP của gói tin UDP, đảm bảo rằng ICMP gói trở lại quá mức không tiếp cận họ, và nặc danh hóa vị trí mạng của họ. Hầu hết các hệ điều hành sẽ giảm

nhẹ một phần của cuộc tấn công bằng cách hạn chế tốc độ phản ứng ICMP được gửi đi.



Hình 2. 3: Quá trình tấn công UFD Flooding



Hình 2. 4: Quá trình tấn công UFD Flooding

2.3.2 Lịch sử xuất hiện:

- Ngày 8 tháng 2 năm 1996, Trung tâm Điều phối CERT đã nhận được báo cáo về các chương trình khởi động các cuộc tấn công từ chối dịch vụ bằng cách tạo ra một "con bão gói UDP" trên một hệ thống hoặc giữa hai hệ thống. Một cuộc tấn công vào một máy chủ làm cho máy chủ đó hoạt động kém. Một cuộc tấn công giữa hai

máy chủ có thể gây ra tắc nghẽn mạng cực kỳ nghiêm trọng và ảnh hưởng xấu đến hiệu suất máy chủ.

2.3.3 Cơ chế tấn công:

- Trong điều kiện bình thường server nhận packet UDP tại 1 port cụ thể, phản hồi qua 2 bước như sau:
 - **Bước 1:** Trước tiên, server kiểm tra xem có các chương trình nào đang chạy hay không, hiện tại đang lắng nghe các port nào được chỉ định của chương trình.
 - **Bước 2:** Nếu không có chương trình nào nhận packet tại port, thì server sẽ phản hồi với packet ICMP (ping) để thông báo cho người gửi rằng đích không thể truy cập được.
- Còn đối với tấn công UDP Flood trả về kết quả là các máy chủ sẽ:
 - Kiểm tra các ứng dụng với cổng.
 - Thấy rằng không có ứng dụng nghe ở cổng.
 - Trả lời với một ICMP Destination Unreachable gói.
 - Khi số lượng request vượt ngưỡng này sẽ dẫn đến mất khả năng xử lý các yêu cầu của khách hàng thông thường dẫn đến tình trạng từ chối dịch vụ.

2.3.4 Mức độ phá hoại:

- Tấn công ngập lụt (Flood Attacks) bằng UDP chiếm 49% tổng số vụ tấn công DDoS trong quý vừa qua. Đây là thông tin được đưa ra từ Báo cáo Xu hướng Tấn công DDoS Quý 3 năm 2016 được Verisign công bố mới đây.
- Theo đó, Verisign cho biết: Các vụ tấn công ngập lụt sử dụng Giao thức gói dữ liệu người dùng (User Datagram Protocol – UDP) tiếp tục chiếm ưu thế trong Quý 3 năm 2016, chiếm 49% tổng số vụ tấn công trong quý này.
- Những vụ tấn công ngập lụt bằng UDP phổ biến nhất đã được giảm thiểu là các vụ tấn công phản hồi qua Hệ thống tên miền (Domain Name System – DNS), tiếp đến là qua Giao thức đồng bộ thời gian mạng (Network Time Protocol – NTP).
- Đợt tấn công ngập lụt cường độ cao nhất trong Quý 3 năm 2016 là TCP SYN flood đạt đỉnh điểm khoảng 60 Gigabit mỗi giây (Gbps) và 150 triệu gói tin mỗi giây (Mpps). Vụ tấn công ngập lụt này là một trong những vụ tấn công có lượng gói tin truyền đi mỗi giây cao nhất mà Verisign từng quan sát được, vượt qua cả vụ tấn công trước đạt 125 Mpps đã được giảm thiểu bởi Verisign trong Quý 4 năm 2015.

- Vụ tấn công lớn nhất trong Quý 3 năm 2016 đã tận dụng giao thức (IP protocol 47) Mã hóa Định tuyến (Generic Routing Encapsulation – GRE) và đạt đỉnh điểm lên đến 250+ Gbps và 50+ Mpps. Đây là lần đầu tiên Verisign quan sát được loại hình tấn công này trên cơ sở dữ liệu khách hàng của hãng.
- Bên cạnh đó, Báo cáo Xu hướng Tấn công DDoS Quý 3 năm 2016 của Verisign cũng cho thấy một số thông tin quan trọng khác. Cụ thể là:
 - Mức tấn công đỉnh điểm trung bình trong năm 2016 tiếp tục có xu hướng gia tăng so với những năm trước. Mức tấn công đỉnh điểm trung bình trong Quý 3 năm 2016 đạt 12,78 Gbps, tăng 82% so với cùng kỳ năm ngoái.
 - 41% các vụ tấn công DDoS tận dụng 3 hoặc nhiều loại hình tấn công khác nhau.
 - Dịch vụ CNTT/Đám mây/SaaS, chiếm 37% trong tổng số hoạt động giảm thiểu, vẫn là các lĩnh vực bị nhắm đến thường xuyên nhất trong vòng 8 quý vừa qua, theo sau là lĩnh vực tài chính, chiếm 29%.

2.4 Tấn công SYN Flood:

2.4.1 Khái niệm:

- SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (DDoS), tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Bằng việc gửi liên tục gửi các packet tin yêu cầu kết nối ban đầu (SYN).
- Người tấn công có thể áp đảo tất cả các cổng có sẵn trên Server được chọn mục tiêu, làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp hoặc không đáp ứng kịp thời.
- SYN Flood attack sẽ khai thác từ lỗ hổng bên trong TCP/ IP bắt tay nhau trong việc tấn công phá vỡ một dịch vụ web.

2.4.2 Lịch sử xuất hiện:

- Điểm yếu ngập lụt TCP SYN được phát hiện sớm nhất bởi Bill Cheswick và Steve Bellovin vào năm 1994. Họ đã đưa vào và sau đó loại bỏ một đoạn về cuộc tấn công trong cuốn sách "Tường lửa và Bảo mật Internet: Đầy lùi Wily Hacker". Thật không may, không có biện pháp đối phó nào được phát triển trong vòng hai năm tới.
- Cuộc tấn công tràn ngập SYN lần đầu tiên được công bố vào năm 1996, với việc phát hành một công cụ mô tả và khai thác trên Tạp chí Phrack. Ngoài một số điểm

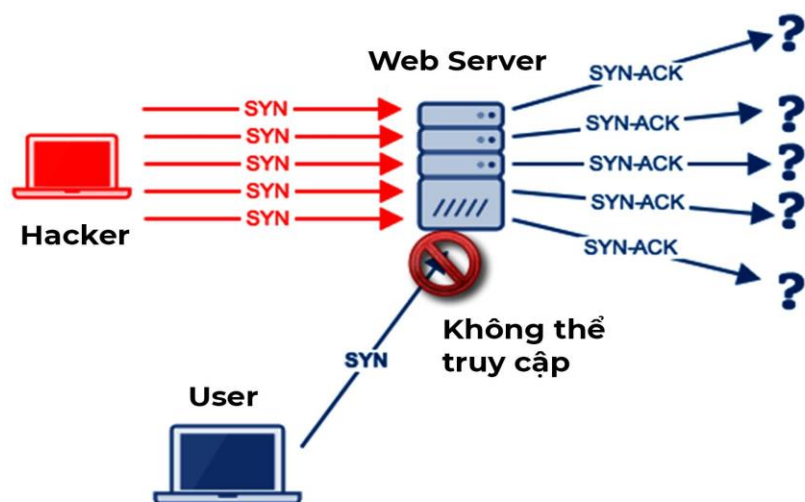
không chính xác nhỏ, bài viết này có chất lượng đủ cao để hữu ích và mã từ bài báo đã được phân phối và sử dụng rộng rãi.

- Vào tháng 9 năm 1996, các cuộc tấn công lũ lụt SYN đã được quan sát thấy trong tự nhiên. Đặc biệt, một cuộc tấn công chống lại một máy chủ thư của ISP đã gây ra tình trạng ngừng hoạt động được công bố rộng rãi. CERT nhanh chóng đưa ra lời khuyên về cuộc tấn công. Lũ lụt SYN đặc biệt nghiêm trọng so với các cuộc tấn công từ chối dịch vụ khác đã biết vào thời điểm đó. Thay vì dựa vào chiến thuật brute-force thông thường là làm cạn kiệt tài nguyên của mạng, SYN lũ lụt nhắm vào các tài nguyên của máy chủ lưu trữ cuối, vốn yêu cầu ít gói tin hơn để cạn kiệt.
- Cộng đồng nhanh chóng phát triển nhiều kỹ thuật khác nhau rộng rãi để ngăn chặn hoặc hạn chế tác động của các cuộc tấn công lũ lụt SYN. Nhiều trong số này đã được triển khai ở các mức độ khác nhau trên Internet, ở cả máy chủ cuối và bộ định tuyến can thiệp. Một số kỹ thuật này đã trở thành phần quan trọng của việc triển khai TCP trong một số hệ điều hành nhất định, mặc dù một số khác biệt đáng kể so với đặc tả TCP và không có kỹ thuật nào trong số này chưa được quy trình IETF chuẩn hóa hoặc chấp nhận.

2.4.3 Cơ chế tấn công:

- Bình thường, một kết nối TCP được thể hiện quy trình 3 bước riêng biệt để tạo được sự kết nối như sau:
 - **Bước 1:** Máy Client gửi 1 packet tin SYN đến Server để yêu cầu kết nối.
 - **Bước 2:** Sau khi tiếp nhận packet SYN, Server phản hồi lại Client bằng một packet SYN/ACK để xác nhận.
 - **Bước 3:** Client nhận được packet tin SYN/ACK thì sẽ trả lời Server bằng packet tin ACK, từ đây kết nối đã được thiết lập và sẵn sàng trao đổi dữ liệu.
- Nhưng với kỹ thuật tấn công SYN Flood thì Client lại tạo ra một số lượng lớn các kết nối TCP nhưng sẽ không hoàn thành các kết nối này. Cụ thể sẽ như sau:
 - **Bước 1:** Kẻ tấn công sẽ gửi một khối lượng lớn các packet tin SYN đến Server được nhắm là mục tiêu và thường là các địa chỉ IP giả mạo.
 - **Bước 2:** Sau đó, Server sẽ phản hồi lại từng yêu cầu kết nối, để lại 1 cổng mở sẵn sàng tiếp nhận và phản hồi.
 - **Bước 3:** Trong khi Server chờ nhận packet ACK từ Client (packet mà không bao giờ đến), kẻ tấn công tiếp tục gửi thêm các packet SYN mới. Sự

xuất hiện các packet SYN này khiến Server tạm thời duy trì kết nối cổng mở trong một thời gian nhất định cho đến khi timeout.



Hình 2. 5: Quá trình tấn công SYN Flood

2.4.4 Mức độ phá hoại:

- **Tăng hàng đợi backlog:** Mỗi hệ điều hành trên thiết bị mục tiêu có một số kết nối nhất định half-open được cho phép. Một phản hồi đối với khối lượng lớn các gói SYN là tăng số lượng kết nối half-open tối đa có thể mà hệ điều hành sẽ cho phép. Để tăng thành công tối đa backlog, hệ thống phải dự trữ thêm tài nguyên bộ nhớ để xử lý tất cả các yêu cầu mới. Nếu hệ thống không có đủ bộ nhớ để xử lý kích thước backlog tồn đọng tăng lên, hiệu suất hệ thống bị ảnh hưởng một cách tiêu cực, nhưng điều đó vẫn tốt hơn bị tấn công DDoS.
- **Lặp lại sự kết nối half-open TCP cũ:** Một cách giảm thiểu liên quan đến việc ghi đè lên các kết nối half-open cũ sau khi backlog đã được lấp đầy. Cách này yêu cầu các kết nối hợp pháp đầy đủ trong thời gian ngắn so với các backlog bằng các packets SYN độc hại. Cách bảo vệ đặc biệt này thất bại khi số lượng tấn công tăng lên hoặc kích thước backlog quá nhỏ thì không thích hợp.
- **SYN cookies:** Cách này liên quan đến việc tạo ra 1 cookie của server. Để tránh nguy cơ mất các kết nối khi backlog đã được lấp đầy. Server phản hồi từng yêu cầu kết nối từ packet SYN/ACK, sau đó loại bỏ phản hồi SYN khỏi backlog, xóa yêu cầu khỏi bộ nhớ và để port mở và sẵn sàng tạo kết nối mới. Nếu kết nối là một yêu cầu hợp pháp và packet ACK cuối cùng được gửi từ client đến server, sau đó server sẽ xây dựng lại (với 1 số hạn chế) tiếp nhận SYN backlog. Mặc dù sự cố

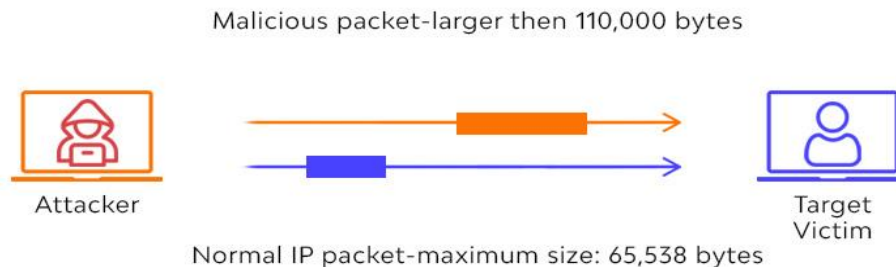
gắng giảm thiểu này mất một số thông tin về kết nối TCP, nhưng nó là tốt hơn so với bị Ddos tấn công.

2.5 Tấn công Ping of Death:

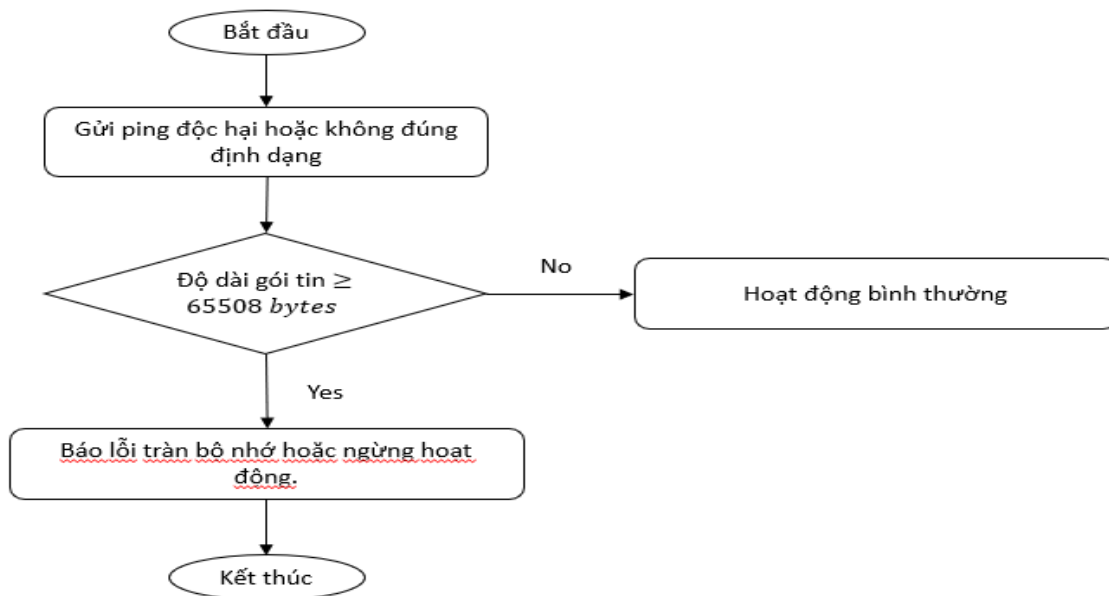
2.5.1 Khái niệm:

- Ping of Death (còn gọi là PoD) là một loại tấn công từ chối dịch vụ (DoS), trong đó kẻ tấn công cố gắng làm sập, mất ổn định hoặc đóng băng máy tính hoặc dịch vụ được nhắm mục tiêu, bằng cách gửi các gói tin có định dạng sai hoặc quá lớn bằng lệnh ping đơn giản.
- Các cuộc tấn công PoD khai thác những điểm yếu cũ có thể đã được vá trong những hệ thống mục tiêu. Tuy nhiên, trong một hệ thống chưa được vá lỗi, cuộc tấn công vẫn có thể diễn ra và trở nên rất nguy hiểm. Gần đây, một kiểu tấn công PoD mới đã trở nên phổ biến.
- Trong cuộc tấn công này, thường được gọi là Ping flood, hệ thống được nhắm mục tiêu bị tấn công với các gói ICMP được gửi nhanh chóng qua ping mà không cần chờ trả lời.

Ping of Death attack



Hình 2. 6: Quá trình tấn công Ping of Death



Hình 2. 7: Lưu đồ quy trình nghiệp vụ của tấn công Ping of Death

2.5.2 Lịch sử xuất hiện:

- Vào ngày 22/01/1997, Mike Bremford người đã cập nhật về vụ tấn công của Ping of Death, ở đây ông đã ghi Ping of death có thể làm sập, khởi động lại hoặc giết một số lượng lớn hệ thống bằng cách gửi một ping có kích thước nhất định từ một máy từ xa. Đây là một vấn đề nghiêm trọng, chủ yếu là vì điều này có thể được sao chép rất dễ dàng và từ một máy ở xa đó là lúc Trong quá trình kiểm tra, máy của ông ở London, Anh đã bị chết từ một máy ở Berkeley, California.
- Vào năm 2013, một phiên bản IPv6 của lỗ hổng bảo mật ping đã được phát hiện trong Microsoft Windows. Ngăn xếp TCP / IP của Windows không xử lý cấp phát bộ nhớ một cách chính xác khi xử lý các gói ICMPv6 không đúng định dạng đến, điều này có thể gây ra từ chối dịch vụ từ xa. Lỗ hổng này đã được sửa trong MS13-065 vào tháng 8 năm 2013. CVE-ID cho lỗ hổng này là CVE-2013-3183.
- Vào năm 2020, một lỗi khác (CVE-2020-16898) trong ICMPv6 đã được tìm thấy xung quanh Quảng cáo bộ định tuyến, thậm chí có thể dẫn đến việc thực thi mã từ xa.

2.5.3 Cơ chế tấn công:

- Kích thước của một gói IPv4 được định dạng chính xác bao gồm tiêu đề IP là 65.535 byte, bao gồm tổng dung lượng payload là 84 byte. Nhiều hệ thống máy

tính trong quá khứ chỉ đơn giản là không thể xử lý các gói lớn và sẽ gặp sự cố nếu nhận được chúng.

- Lỗi này dễ dàng bị khai thác trong các quá trình triển khai TCP/IP ban đầu trong một loạt các hệ điều hành, bao gồm Windows, Mac, Unix, Linux, cũng như các thiết bị mạng, như máy in và router.
- Việc gửi một gói ping lớn hơn 65.535byte vi phạm Internet Protocol, những kẻ tấn công nói chung sẽ gửi các gói không đúng định dạng trong những fragment. Khi hệ thống đích cố gắng tập hợp lại các fragment và kết thúc bằng một gói quá lớn, lỗi tràn bộ nhớ có thể xảy ra và dẫn đến nhiều sự cố hệ thống khác nhau bao gồm cả ngừng hoạt động.

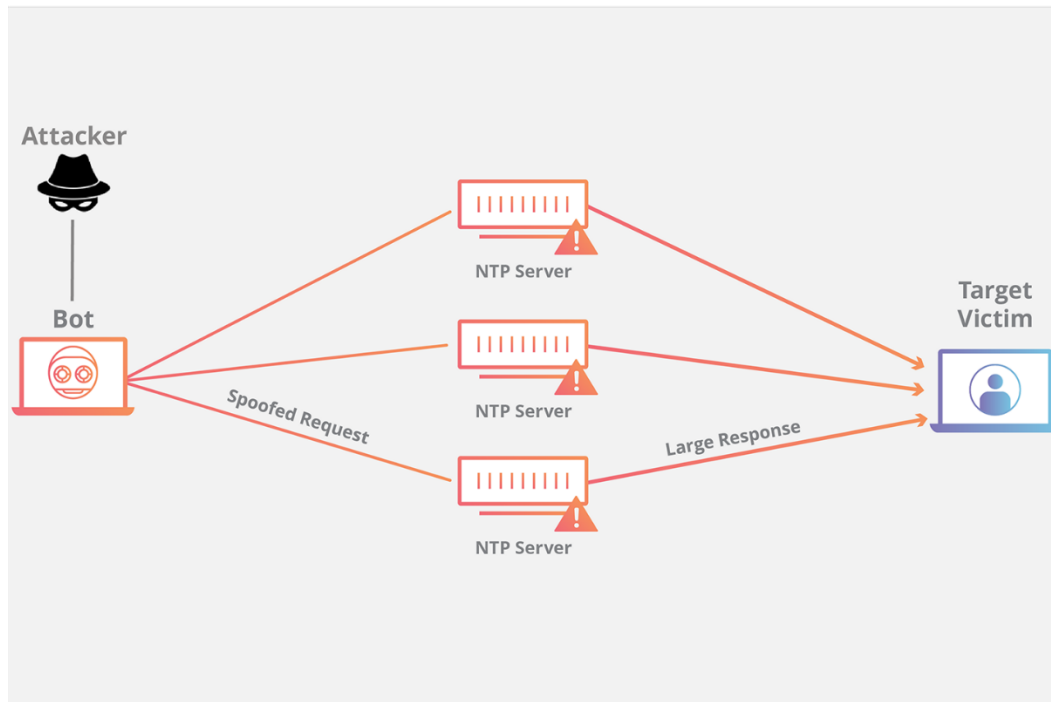
2.5.4 Mức độ phá hoại:

- Máy tính sẽ bị ngừng hoạt động, Reboot hoặc bị crash khi nhận những gói tin lớn.

2.6 Tấn công NTP Amplification:

2.6.1 Khái niệm:

- Là tấn công DDoS dựa trên một lượng lớn các gói tin mà kẻ tấn công khai thác máy chủ Network Time Protocol (NTP) đang hoạt động và cố gắng làm cho hệ thống mạng hay server của nạn nhân quá tải với lượng lớn các gói tin UDP được khuếch đại.
- Các cuộc tấn công DNS flood attacks khác với DNS amplification attacks. Khác với DNS floods, DNS amplification gửi các request nhỏ đến DNS Máy Chủ không bảo mật với cách giả mạo IP của nạn nhân, DNS server này gửi các phản hồi lớn đến nạn nhân từ đó kẻ tấn công không bị phát hiện và tăng tính hiệu quả.



Hình 2. 8: Quá trình tấn công NTP Amplification

2.6.2 Lịch sử xuất hiện:

- NTP là 1 giao thức thuộc loại lâu đời nhất trên thế giới cho đến nay vẫn hoạt động (từ 1982). NTP Amplification đã có lỗi hổng, lỗi hổng này được ghi nhận có mã là CVE-2013-5211 hoặc VU#348126.

2.6.3 Cơ chế tấn công:

- Tấn công khuếch đại NTP có thể được mô tả với 4 bước:
 - **Bước 1:** Kẻ tấn công sử dụng mạng lưới botnet gửi các gói tin UDP với IP giả mạo đến máy chủ NTP bật lệnh monlist. IP giả mạo này là IP của nạn nhân.
 - **Bước 2:** Mỗi gói tin UDP gửi đến máy chủ NTP bằng cách sử dụng lệnh monlist sẽ trả về lượng lớn các phản hồi.
 - **Bước 3:** Máy chủ NTP gửi phản hồi đến IP được giả mạo trong gói tin yêu cầu với lượng lớn dữ liệu.
 - **Bước 4:** IP nhận được quá nhiều phản hồi mà mình không yêu cầu dẫn đến quá tải và từ chối dịch vụ.

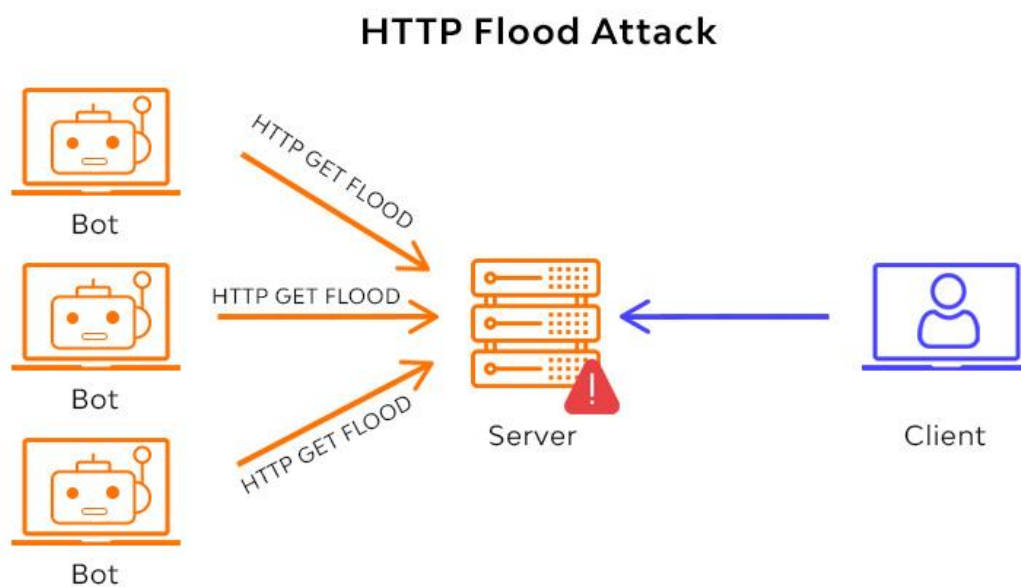
2.6.4 Mức độ phá hoại:

- Khiến hệ thống mạng và webserver bị quá tải.

2.7 Tấn công HTTP Flood:

2.7.1 Khái niệm:

- HTTP flood là một kiểu tấn công Distributed Denial of Service (DDoS - từ chối dịch vụ phân tán), trong đó kẻ tấn công khai thác các yêu cầu HTTP GET hoặc POST có vẻ hợp pháp để tấn công máy chủ web hoặc ứng dụng.
- Tấn công HTTP flood là những cuộc tấn công thường sử dụng một đội quân “zombie” botnet, một nhóm máy tính có kết nối Internet, mỗi máy tính đã bị chiếm quyền kiểm soát, thường là với sự hỗ trợ của phần mềm độc hại như Trojan Horse.
- Là một cuộc tấn công Lớp 7 tinh vi, HTTP flood không sử dụng các gói có định dạng kỳ lạ, các kỹ thuật spoofing (giả mạo) hoặc reflection (ánh xạ sang bên thứ ba) và yêu cầu ít băng thông hơn các cuộc tấn công khác, để “hạ bệ” trang web hoặc máy chủ được nhắm mục tiêu.



Hình 2. 9: Quá trình tấn công HTTP Flood

2.7.2 Lịch sử xuất hiện:

- Một báo cáo bảo mật quý II do Kaspersky thực hiện chỉ ra rằng nguồn tấn công DDoS bắt nguồn từ 86 quốc gia với thời gian tấn công lên đến 122 giờ. Báo cáo đã minh họa sự gia tăng trong cuộc tấn công DDoS HTTP từ 8,43% lên 9,38%.

- Johnson Singh và cộng sự tuyên bố rằng cuộc tấn công DDoS 540 Gbps đã xảy ra vào ngày 31 tháng 8 năm 2016 nhằm vào trang web chính thức của chính phủ liên bang về Olympic Rio 2016 và Bộ Thể thao Brazil.
- Dựa trên báo cáo được thực hiện bởi Arbor Networks (Báo cáo An ninh Cơ sở hạ tầng Toàn cầu (Số XII), 2017) được xuất bản vào Quý 1 năm 2017, các cuộc tấn công xảy ra ở lớp ứng dụng là mục tiêu được nhắm mục tiêu nhiều nhất, trong đó 80% mục tiêu đã tấn công HTTP và 81% nhắm mục tiêu vào Hệ thống tên miền (DNS).

2.7.3 Cơ chế tấn công:

- Khi một client HTTP như trình duyệt web “giao tiếp” với ứng dụng hoặc máy chủ, nó sẽ gửi một yêu cầu HTTP - thường là một trong hai loại yêu cầu: GET hoặc POST. Yêu cầu GET được sử dụng để truy xuất nội dung tĩnh, tiêu chuẩn như hình ảnh, trong khi yêu cầu POST được sử dụng để truy cập các tài nguyên tạo động.
- Cuộc tấn công có hiệu quả nhất khi nó buộc máy chủ hoặc ứng dụng cấp phát tài nguyên tối đa có thể để đáp ứng từng yêu cầu. Do đó, tin tặc nói chung sẽ nhắm tới mục đích làm “ngập” máy chủ hoặc ứng dụng với rất nhiều yêu cầu, mỗi yêu cầu càng dùng nhiều tài nguyên để xử lý càng tốt.
- Vì lý do này, các cuộc tấn công HTTP flood sử dụng những yêu cầu POST có xu hướng “hiệu quả” nhất về tài nguyên theo quan điểm của kẻ tấn công; vì các yêu cầu POST có thể bao gồm những tham số kích hoạt xử lý phía máy chủ phức tạp. Mặt khác, các cuộc tấn công dựa trên HTTP GET có thể được tạo đơn giản và mở rộng hiệu quả hơn trong kịch bản botnet.

2.7.4 Mức độ phá hoại:

- Mức độ của nó được chia làm 2 loại như sau:
 - **Tấn công HTTP GET:** trong hình thức tấn công này, nhiều máy tính hoặc thiết bị khác được điều phối để gửi nhiều yêu cầu về hình ảnh, tệp hoặc một số nội dung khác từ một máy chủ được nhắm mục tiêu. Khi mục tiêu ngập tràn các yêu cầu và phản hồi đến, việc từ chối dịch vụ sẽ xảy ra đối với các yêu cầu bổ sung từ các nguồn lưu lượng truy cập hợp pháp.
 - **Tấn công HTTP POST:** thường khi một biểu mẫu được gửi trên một trang web, máy chủ phải xử lý yêu cầu gửi đến và đẩy dữ liệu vào một lớp liên tục, thường là cơ sở dữ liệu. Quá trình xử lý dữ liệu biểu mẫu và chạy các lệnh cơ sở dữ liệu cần thiết là tương đối chuyên sâu so với lượng công suất

xử lý và bằng thông cần thiết để gửi yêu cầu POST. Cuộc tấn công này sử dụng sự chênh lệch về mức tiêu thụ tài nguyên tương đối, bằng cách gửi nhiều yêu cầu đăng trực tiếp đến một máy chủ được nhắm mục tiêu cho đến khi dung lượng của nó bão hòa và xảy ra từ chối dịch vụ.

2.8 Kết luận chương:

- Trong chương này, em đã giới thiệu và phân tích về các cuộc tấn công từ chối dịch vụ. Từ đó, em lựa chọn hình thức tấn công slowloris để tìm hiểu và triển khai cơ chế tấn công và đưa ra giải pháp ngăn chặn trong chương tiếp theo.

CHƯƠNG 3 . CÀI ĐẶT PHƯƠNG THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ

3.1 Giới thiệu các công cụ để giả lập tấn công từ chối dịch vụ:

3.1.1 VMware Server:

- VMware Server là một sản phẩm ảo hóa miễn phí dành cho Máy chủ Windows và Linux có hỗ trợ cấp doanh nghiệp. VMware® Server cho phép các công ty phân vùng máy chủ vật lý thành nhiều máy ảo, trải nghiệm tất cả những lợi ích của ảo hóa.
- VMware Server hoạt động mạnh mẽ, nhưng vẫn dễ dàng kể cả với những người dùng mới. Công nghệ ảo hóa của VMware đã được hàng nghìn khách hàng tin dùng trong suốt hơn sáu năm qua. Cùng Bizfly Cloud tìm hiểu thông tin chi tiết qua bài viết dưới đây.
- Một virtual machine giống như một máy chủ và là phần mềm. Virtual machine chạy các hệ điều hành và ứng dụng giống như một máy chủ vật lý. Tuy nhiên, máy ảo cung cấp nhiều lợi ích hơn cho người dùng so với máy chủ vật lý. Ví dụ như:
 - Là phần cứng độc lập và chạy trên bất kỳ máy chủ vật lý x86 nào.
 - Có thể truy cập tất cả các tài nguyên phần cứng máy chủ vật lý như CPU, bộ nhớ, đĩa, mạng và thiết bị ngoại vi.
 - Được lưu dưới dạng tệp và có thể được cấp phép và di chuyển nhanh chóng.
 - Hoàn toàn bị cô lập và an toàn.
 - Có thể chạy đồng thời và an toàn trên cùng một máy chủ vật lý.
 - Là thiết bị di động, vì vậy toàn bộ hệ thống bao gồm virtual hardware, operating systems và các ứng dụng được cấu hình đầy đủ có thể dễ dàng di chuyển từ một máy chủ vật lý này đến một máy chủ khác, ngay cả khi đang hoạt động.
 - Có thể được xây dựng và phân phối dưới dạng các thiết bị ảo plug-and-play chứa toàn bộ phần cứng ảo, operating system và các ứng dụng phần mềm được cấu hình đầy đủ.

3.1.2 Hệ điều hành Kali Linux:

- Kali Linux là một bản phân phối Linux được phát triển và duy trì bởi Offensive Security khi được tổ chức này phát hành vào tháng 3 năm 2013, là sự thay thế phát triển cho hệ điều hành BackTrack.

- Offensive Security là một tổ chức nổi tiếng và đáng tin cậy trong thế giới bảo mật, thậm chí chứng nhận các chuyên gia bảo mật với một số chứng chỉ được xem trọng nhất hiện có như: OSCP, OSCE, OSWP, OSEE.
- **Ưu điểm:**
 - Do phát triển trên hệ điều hành Debian, nên Kali có thể sử dụng các repository của Debian hỗ trợ việc cài đặt được nhiều phần mềm và cập nhật phần mềm nhanh chóng.
 - Kali Linux liên tục cải tiến khả năng tương thích với thiết bị phần cứng của rất nhiều loại như điện thoại, raspberry, laptop, server, cloud,... đảm bảo bạn có thể cài đặt trên bất kỳ thiết bị nào.
 - Hỗ trợ mạng wifi (không dây) cực kì tốt với Kali Linux, điều này giúp các chuyên gia bảo mật có thể thực hiện tấn công và kiểm thử khả năng bảo mật của Wifi.
- **Nhược điểm:**
 - Kali không dành cho tất cả mọi người. Đây không phải là bản phân phối Linux thông thường để chạy trên máy tính xách tay của bạn. Có thể bạn tự nghĩ rằng bạn thật tuyệt, thật “nguy hiểm” khi chạy “hệ điều hành hacker”.
 - Nếu bạn làm như vậy, bạn đang chạy một hệ thống có khả năng không an toàn. Kali được thiết kế để chạy dưới quyền root. Nó không được bảo mật và được cấu hình giống an toàn như một bản phân phối Linux thông thường (trường hợp bạn không rành về tối ưu an toàn Linux). Kali Linux là một công cụ tấn công, không phải là một công cụ phòng thủ.

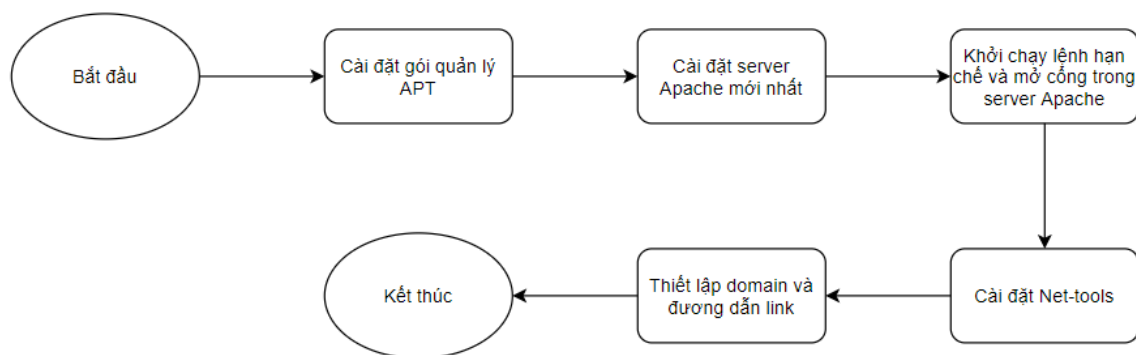
3.1.3 Hệ điều hành Ubuntu Server:

- Ubuntu bắt nguồn từ tiếng châu Phi cổ, có nghĩa là “tình người”. Ubuntu là hệ điều hành mở do người dùng phát triển, với ý nghĩa đó, hệ điều hành Ubuntu ra đời nhằm mục đích chia sẻ và tạo ra những đóng góp lớn cho thế giới công nghệ hiện nay.
- Ubuntu có rất nhiều các bản phân phối khác nhau và phiên bản mới Ubuntu Server thực sự đang mang lại cho người dùng một trải nghiệm tuyệt vời.
- Phiên bản hệ điều hành mới khác hẳn so với các phiên bản Ubuntu tiêu chuẩn bạn từng biết, được ra đời nhằm hỗ trợ cho việc hoạt động của mạng lưới (network) và dịch vụ (service).

- Hệ điều hành được sử dụng để chạy trên các file server đơn giản vì nó đang hoạt động trong 5000 node cloud. Khác với phiên bản Desktop, phiên bản Ubuntu Server không bao gồm việc giao diện đồ họa đối với người dùng. (Graphical User Interface). Bạn có thể tìm hiểu và thấy được sự khác nhau về giao diện giữa 2 phiên bản này.
- **Ưu điểm:**
 - Hoàn toàn miễn phí: Đây là một ưu điểm vượt trội khi sử dụng Ubuntu Server người dùng hoàn toàn không phải trả phí. Trong khi một số hệ điều hành như Window bạn phải mất một chi phí nhất định cho nó mới có thể được sử dụng.
 - Tính bảo mật cao: Độ bảo mật của Ubuntu được nghiên cứu từ các chuyên gia công nghệ. Chúng được đánh giá cao hơn rất nhiều so với Window. Bởi vì Ubuntu sử dụng mã nguồn mở và được sử dụng rộng rãi tại nhiều quốc gia.
 - Tương thích với mọi ứng dụng: Ubuntu Server vẫn hỗ trợ người dùng sử dụng một số ứng dụng, phần mềm, game... trên hệ điều hành Windows. Về tính năng này vẫn được Ubuntu phát triển và mở rộng thêm nhằm đem lại sự tiện lợi tuyệt đối và hỗ trợ tối đa những thói quen sử dụng trên Window khi muốn đổi qua dùng Ubuntu server.
 - Dễ dàng sử dụng: File cài đặt hầu như đã cung cấp đầy đủ toàn bộ các driver có sẵn cần thiết để thiết bị có thể hoạt động bình thường và ổn định. Bên cạnh đó, Ubuntu server cũng sở hữu một kho ứng dụng khổng lồ và hỗ trợ đa dạng và hầu hết nhu cầu của người sử dụng.
- **Nhược điểm:**
 - Khó làm quen và sử dụng.
 - Đối với hệ điều hành ubuntu bạn cần khoảng từ 4-6 tuần để thích nghi và nắm được cách sử dụng. Vì là hệ điều hành mã nguồn mở, bạn phải nhớ tương đối nhiều câu lệnh, điều này khó khăn hơn khi bạn đã quen với những click chuột trên windows.
 - Một số phần mềm không được hỗ trợ: Microsoft office, Phần mềm chụp ảnh, quay video màn hình, IE, skype, webcam, những trình nghe nhạc, xem phim, đồ họa đều rất hạn chế.
 - Ít phổ biến.
 - Khó khăn trong việc cài đặt, nâng cấp và quản lý các ứng dụng.

3.2 Giả lập phía bị tấn công từ chối dịch vụ:

- Ở phần này, em sử dụng Ubuntu Server để giả lập phía bị tấn công qua quá trình như sau:



Hình 3. 1: Lưu đồ quy trình nghiệp vụ phía bị tấn công

- Bước 1: Cài đặt gói quản lý APT:
 - Bước này, em sẽ cài đặt gói APT để hỗ trợ ubuntu cài đặt các gói thư viện

Lệnh 1: `sudo apt update`
Lệnh 2: `sudo apt upgrade`

- Bước 2: Cài đặt server Apache mới nhất
 - Sau khi em cài đặt gói hỗ trợ, em sẽ tiến hành cài đặt server apache nhằm cài đặt giả lập phía bị tấn công:

Lệnh 1: `sudo apt install apache2`

- Em sẽ tiến hành kích hoạt cấu hình khởi động cùng máy chủ bằng lệnh sau:

Lệnh 2: `sudo systemctl is-enabled apache2.service`

❖ Lưu ý: nếu nó không enabled thì dùng lệnh sau:

Lệnh 2.1: `sudo systemctl enable apache2.service`

- Khởi chạy Server Apache 2:

```
Lệnh 3: sudo systemctl start apache2.service
```

- Bước 3: Khởi chạy lệnh hạn chế và mở cổng trong Server Apache
 - Tiếp theo đây là một bước rất quan trọng, em sẽ kích hoạt cấu hình hạn chế để đảm bảo vừa cho phép lưu lượng truy cập mà bạn đã cấu hình vừa đảm bảo vấn đề bảo mật. Thông thường đối với dịch vụ web các bạn chỉ cần mở port 80 cho giao thức HTTP và port 443 cho giao thức HTTPS:

```
Lệnh 1: sudo ufw allow 80/tcp comment 'accept Apache'
```

```
Lệnh 2: sudo ufw allow 443/tcp comment 'accept HTTPS connections'
```

- Bước 4: Cài đặt Net-tools
 - Em sẽ giới thiệu Net-tools là gì và tại sao em lại dùng nó. Net Tools là bộ công cụ nối mạng hỗ trợ tính năng quản lý tập tin, cấu hình toàn bộ các entry trình đơn cũng như lấy IP nội bộ hay quét địa chỉ IP.
 - Ngoài ra, Net Tools còn trang bị rất nhiều tính năng thú vị khác như ghép tập tin hay cài đặt mật khẩu bảo vệ tập tin, cho phép xóa hoàn toàn các tính năng không cần dùng, hay mã hóa tập tin, Nó là 1 tiện ích cung cấp rất nhiều công cụ IP hỗ trợ người dùng mạng thông thường và là một trong những bộ sưu tập tiện ích mạng hoàn chỉnh nhất trên thị trường công nghệ thông tin. Đối với Ubuntu Server chúng ta cài đặt bằng cách dùng lệnh sau:

```
Lệnh 1: sudo apt install net-tools
```

```
Lệnh 2: sudo apt install curl
```

- Bước 5: Thiết lập domain và đường dẫn link:
 - Bước này rất quan trọng vì nó quyết định website của bạn sẽ hoạt động như thế nào và đặt dưới sự quản lý của server nên cần chú trọng. Ở bước này ta cần chú ý dù là nhỏ nhất để tránh ảnh hưởng đến sử dụng website với các khách hàng.

```
Lệnh 1: sudo nano /etc/apache2/sites-available/(tên domain của bạn).conf
```

Lưu Ý: Sao chép các dòng lệnh code dưới và đổi my-domain-name-here thành domain của bạn.

```
<VirtualHost *:80>
    ServerAdmin webmaster@my-domain-name-here
    ServerName my-domain-name-here
    ServerAlias www.my-domain-name-here
    DocumentRoot /home/my-domain-name-here/html
    DirectoryIndex index.html
    ErrorLog ${APACHE_LOG_DIR}/my-domain-name-here-error.log
    CustomLog ${APACHE_LOG_DIR}/my-domain-name-here-access.log
    combined
</VirtualHost>
<Directory /home/my-domain-name-here/html>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

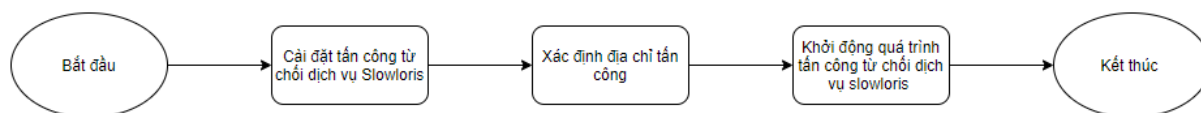
- Sau khi hoàn tất việc cài đặt chúng ta có thể cài đặt thêm về giao diện của website của bạn bằng lệnh sau.

Lệnh 2: `sudo -H gedit /var/www/html/index.html`

Lưu ý: Điền các html bạn muốn vào đây có thể dùng 1 template bất kì

3.3 Giả lập phía tấn công từ chối dịch vụ:

- Về phía bị tấn công em sẽ sử dụng Kali Linux làm hệ điều hành để giả lập phía tấn công theo quy trình sau:



Hình 3. 2: Lưu đồ quy trình nghiệp vụ phía tấn công

- Bước 1: Cài đặt tấn công từ chối dịch vụ Slowloris
 - Em sẽ lấy bản sao kịch bản của Slowloris bằng cách dùng lệnh clone code python của Mattiasgeniar về máy Kali Linux.

Lệnh 1: `Git clone https://github.com/mattiasgeniar/slowloris.git`

- Bước 2: Xác định địa chỉ tấn công
 - Đây là một bước rất quan trọng chúng ta cần phải xác định được địa chỉ URL mà mình muốn tấn công. Sau khi xác định được địa chỉ mà mình muốn tấn công em sẽ bắt đầu các bước để xâm nhập tấn công Servers bằng cách mở và duy trì nhiều kết nối HTTP.
- Bước 3: Khởi động quá trình tấn công từ chối dịch vụ Slowloris
 - Ở đây, em sẽ dùng lệnh sau để đưa nhiều kết nối tới server bằng lệnh sau:

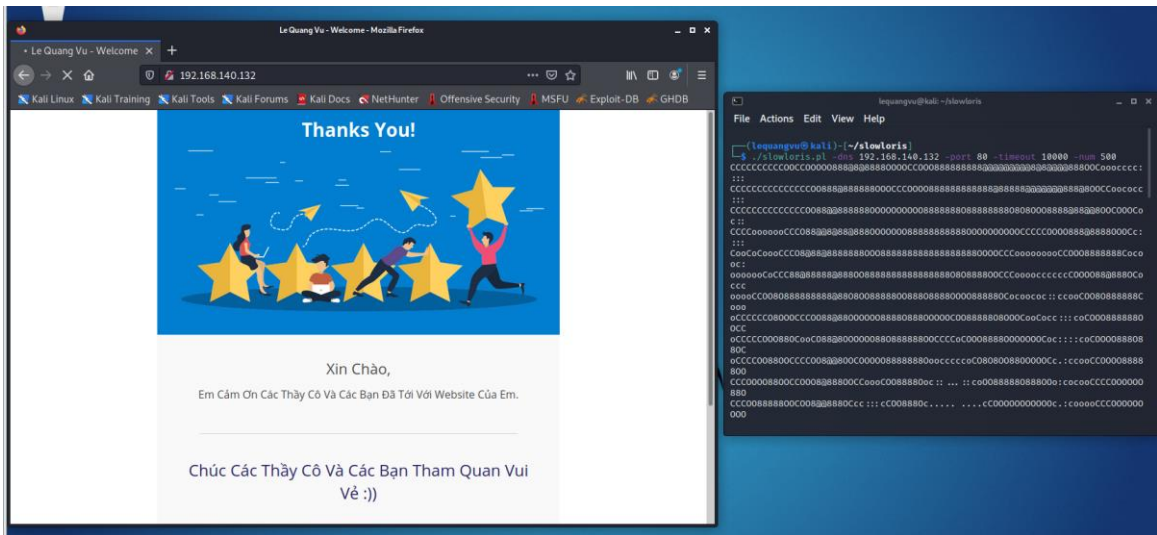
Lệnh 2: `./slowloris.pl -dns (địa chỉ IP bạn muốn tấn công) -port 80 -timeout 2000 -num 750`

Bảng 3. 1: Chú thích lệnh tấn công Slowloris

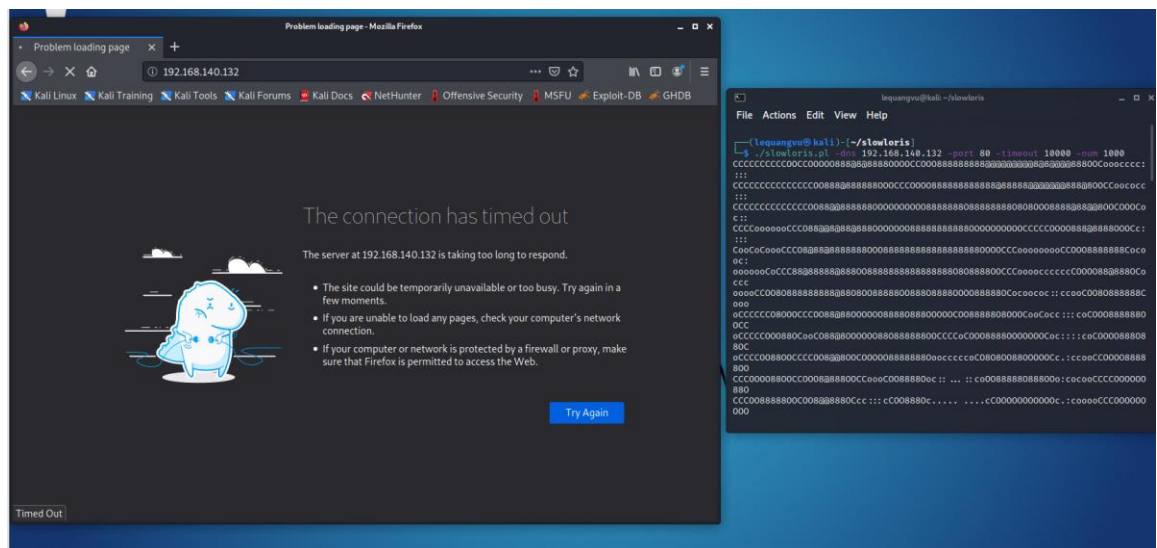
Các lệnh trong tấn công Slowloris	
-dns	Nơi bạn sẽ ghi các địa chỉ IP mà mình tấn công
-port hay có thể ghi là -p	Đây là chỗ bạn phải điền các port mà địa chỉ đó hiện tại đang sử dụng ví dụ HTTP sẽ

	là port 80, còn HTTPS nó sẽ là 443.
-timeout	Là khoảng thời gian mà 1 request truy cập vào Servers Apache trong bao lâu
-num	Là số lượng request truy cập vào Servers

- Kết quả: chúng ta sẽ thấy website hiện tại của chúng ta sẽ bị slow loading page nhưng khi quá nhiều lượt kết nối sẽ dẫn tới việc



Hình 3. 3: Kết quả về việc website bị slow loading page



Hình 3. 4: Kết quả về việc website nhận quá nhiều kết nối

3.4 Kết luận chương:

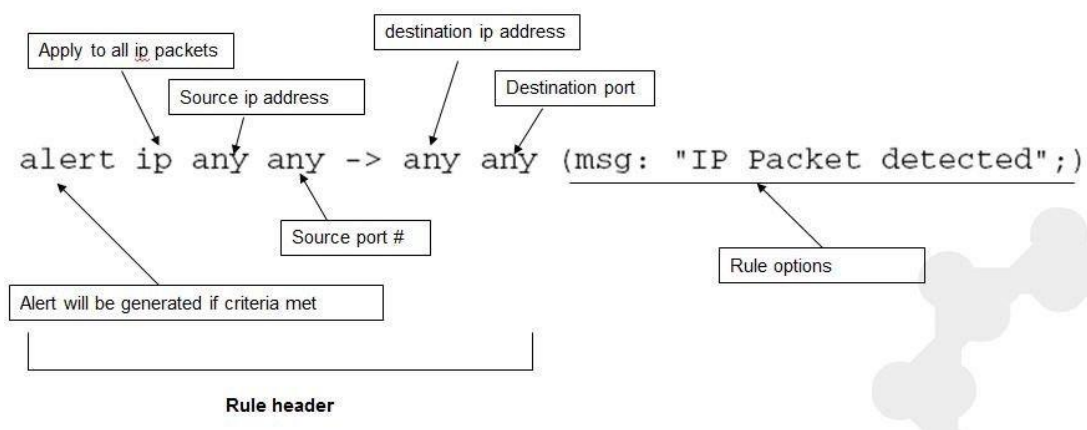
- Sau khi đã tìm hiểu và nắm rõ quy trình của cuộc tấn công slowloris. Từ đó em đưa ra biện pháp phòng thủ thích hợp và làm rõ trong chương tiếp theo.
- Sau quá trình tìm hiểu và thực hiện em đạt được kết quả. Với một máy chủ điều khiển, một máy trạm dùng để tấn công, Attacker có thể tạo ra rất nhiều các địa chỉ giả mạo để tấn công đến máy trạm làm cho website mà server chúng ta quản lý bị chậm hoặc thậm chí là bị quá thời gian kết nối. Nó sẽ làm cho trải nghiệm của người dùng trở nên tệ hơn nên vì vậy để có thể nào phát hiện và ngăn chặn nó, em đã có nghiên cứu qua các loại phòng thủ và đề xuất các loại phòng thủ cần thiết. Em sẽ trình bày chi tiết về nó ở chương tiếp theo.

CHƯƠNG 4. GIẢI PHÁP NGĂN CHẶN TẤN CÔNG TỪ CHỐI DỊCH VỤ

4.1 Giới thiệu hệ thống phòng thủ:

4.1.1 Giới thiệu hệ thống phát hiện xâm nhập Snort:

- Snort là một hệ thống phát hiện và ngăn chặn xâm nhập mạng miễn phí và nguồn mở. Nó sử dụng ngôn ngữ dựa trên quy tắc, thực hiện phân tích giao thức, tìm kiếm kết hợp nội dung và có thể được sử dụng để phát hiện nhiều loại tấn công và thăm dò khác nhau, chẳng hạn như buffer overflows, stealth port scans, CGI Group Inc. attacks, Server Message Block probes, Operating system fingerprinting attempts ...
- Còn về cài đặt luật em sẽ dùng Snort Rules. Nó cung cấp phát hiện các cuộc tấn công và các hoạt động độc hại. Bạn có thể viết các quy tắc cụ thể như cảnh báo, log, ngắt kết nối, v.v ... Các Rule có cú pháp đơn giản. Ngoài ra, bạn có thể viết tất cả các rule trong một tệp cấu hình.
- Snort có 3 chế độ khác nhau bao gồm:
 - Packet Sniffer
 - Packet Logger
 - Neural Information Processing Systems (Hệ thống phát hiện ngăn chặn và xâm nhập mạng)
- Còn về cấu trúc của Rules được cấu hình như sau:



Hình 4. 1: Cấu trúc của Rules trong hệ thống phát hiện xâm nhập Snort

- alert - Rule action. Snort sẽ tạo ra một cảnh báo khi điều kiện thiết lập được đáp ứng.
 - any - Source IP (Nếu bạn sử dụng “any” Snort sẽ xem xét tất cả các source)
 - any - Source port (Nếu bạn sử dụng “any” Snort sẽ xem xét tất cả các ports)
 - any - Destination IP: Snort sẽ xem xét tất cả các destination trên mạng được bảo vệ.
 - any - Destination port: Snort sẽ xem xét tất cả các ports trên mạng được bảo vệ.
- Đối với cấu hình Rule Options:
- msg: “ICMP test” - Snort sẽ gắn thông điệp này với alert.
 - rev:1 - Revision number: Tùy chọn này cho phép bảo trì rule dễ dàng hơn.
 - classtype: icmp-event - Phân loại rule như một “icmp-event”, một trong những loại Snort được xác định trước.

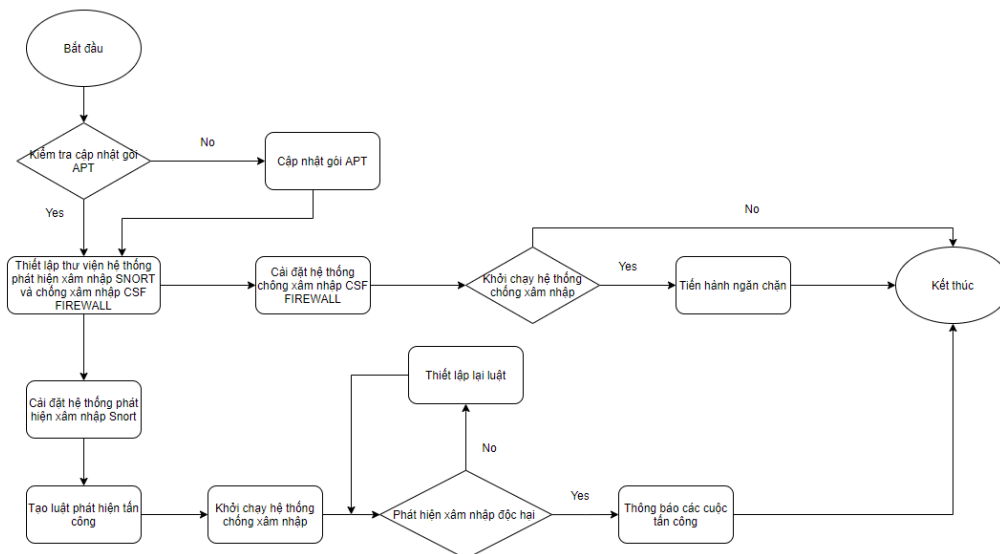
4.1.2 Giới thiệu ứng dụng CSF Firewall:

- CSF (ConfigServer & Firewall) là 1 gói ứng dụng hoạt động trên Linux như 1 Firewall được phát hành miễn phí để tăng tính bảo mật cho server (VPS và Dedicated). CSF hoạt động dựa trên iptables và tiến trình lfd để quét các file log để phát hiện các dấu hiệu tấn công bất thường.
- Lợi ích của việc sử dụng ứng dụng CSF Firewall:
 - Chống DoS các loại.
 - Chống Scan Port.
 - Đưa ra các lời khuyên về việc cấu hình server (VD: Nên nâng cấp Relational Database Management System lên bản mới hơn).
 - Chống BruteForce Attack vào ftp server, web server, mail server, directadmin, cPanel...
 - Chống Syn Flood.
 - Chống Ping Flood.

- Cho phép ngăn chặn truy cập từ 1 quốc gia nào đó bằng cách chỉ định Country Code chuẩn International Organization for Standardization.
- Hỗ trợ IPv6 và IPv4.
- Cho phép khóa IP tạm thời và vĩnh viễn ở tầng mạng (An toàn hơn ở tầng ứng dụng) nên webserver ko phải mệt nhọc xử lý yêu cầu từ các IP bị cấm nữa.
- Cho phép bạn chuyển hướng yêu cầu từ các IP bị khóa sang 1 file html để thông báo cho người dùng biết IP của họ bị khóa.

4.2 Giả lập ngăn chặn tấn công từ chối dịch vụ:

- Ở đây, em sẽ đề cập về hoạt động của những phần mềm trên khi bị tấn công từ chối dịch vụ Slowloris từ attacker.
- Quy trình cài đặt và hoạt động của 2 phần mềm trên được thể hiện như sau:



Hình 4. 2: Lưu đồ quy trình nghiệp vụ ngăn chặn tấn công từ chối dịch vụ

- Bước 1: Kiểm tra cập nhật gói APT:
 - Ở bước này em sẽ cập nhật gói hỗ trợ này vì nó sẽ giúp chúng ta thiết lập các thư viện cần thiết để sử dụng 2 hệ thống trên.

Lệnh 1: Sudo apt-get update -y
 Lệnh 2: Sudo apt-get upgrade -y

- Còn đối với chưa cài đặt gói thì chúng ta cần cài đặt gói bằng những lệnh sau:

Lệnh 3: `sudo apt update`
Lệnh 4: `sudo apt upgrade`

- Bước 2: Thiết lập thư viện hệ thống phát hiện xâm nhập SNORT và chống xâm nhập CSF FIREWALL
 - Em sẽ thiết lập 2 thư viện để có thể cài đặt được các hệ thống phần mềm trên theo quy định hướng dẫn của các phần mềm. Em sẽ dùng 2 lệnh lần lượt như sau:

Lệnh 1: `sudo apt-get install openssh-server ethtool build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev`
Lệnh 2: `Sudo apt-get install sendmail dnsutils giải nén git perl iptables libio-socket-ssl-perl libcrypt-ssleay-perl libnet-libidn-perl libio-socket-inet6-perl libsocket6-perl -y`

- Bước 3: Cài đặt hệ thống phát hiện xâm nhập Snort:
 - Cài đặt hệ thống sẽ làm theo quy trình các lệnh sau:

Lệnh 1: `Sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz`
Lệnh 2: `Sudo wget https://www.snort.org/downloads/snort/snort-2.9.17.1.tar.gz`
Lệnh 3: `tar xvzf daq-2.0.7.tar.gz`
Lệnh 4: `tar xvzf snort-2.9.17.1.tar.gz`
Lệnh 5: `cd daq-2.0.7`
Lệnh 6: `./configure && make && sudo make install`
Lệnh 7: `cd snort-2.9.17.1`
Lệnh 8: `./configure --enable-sourcefire && make && sudo make install`

- Những lệnh trên là việc cần thiết để cài đặt hệ thống phát hiện xâm nhập Snort. Nhưng cần lưu ý trong quá trình cài đặt sẽ có thể phát sinh lỗi như sau em kiến nghị nên dùng lệnh này để khắc phục để hệ thống được cài đặt 1 cách hoàn thiện.

Lệnh 9: `./configure --disable-open-appid`

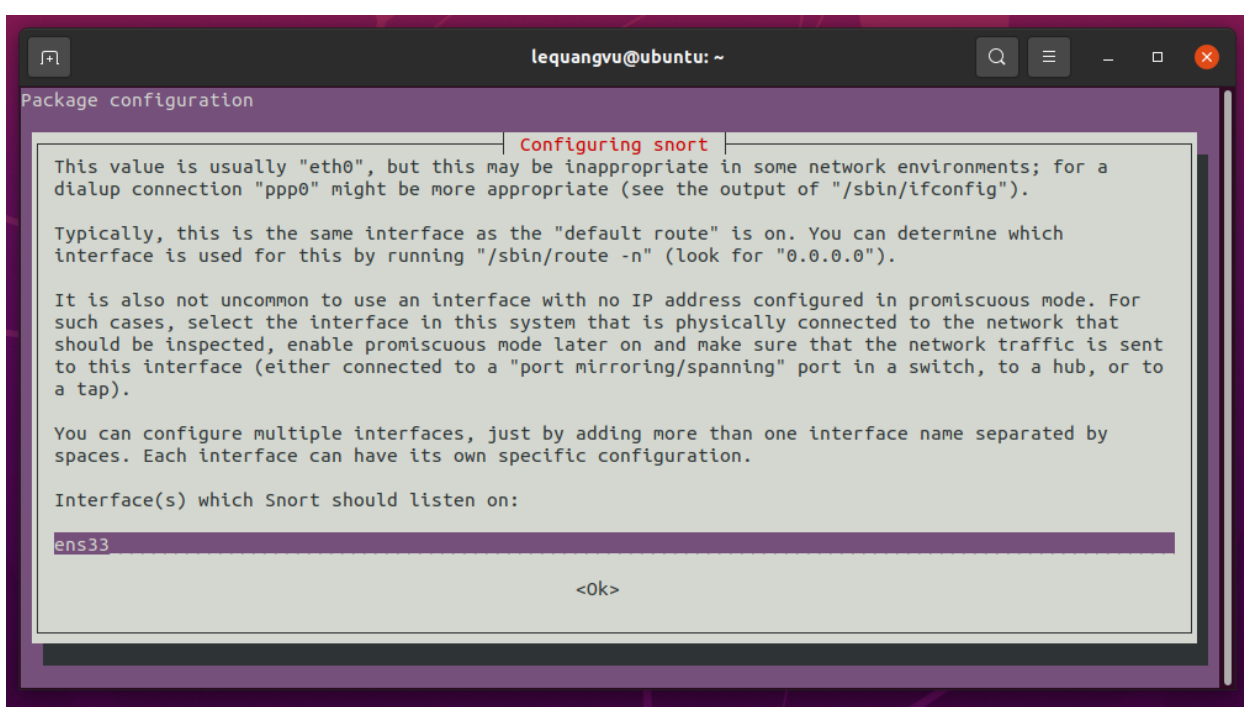
```
ERROR! LuaJIT library not found. Go get it from http://www.luajit.org/ (or)
Try compiling without openAppid using '--disable-open-appid'
configure: error: "Fatal!"
```

Hình 4. 3: phát hiện lỗi khi cài đặt hệ thống Snort

- Quá trình cài đặt hoàn tất chúng ta cần cập nhật thư viện dùng chung với lệnh sau:

Lệnh 10: Sudo ldconfig

- Tiếp theo chúng ta cần cấu hình hệ thống để phát hiện các cuộc tấn công Slowloris:



Hình 4. 4: Hệ thống Snort yêu cầu cổng truy cập

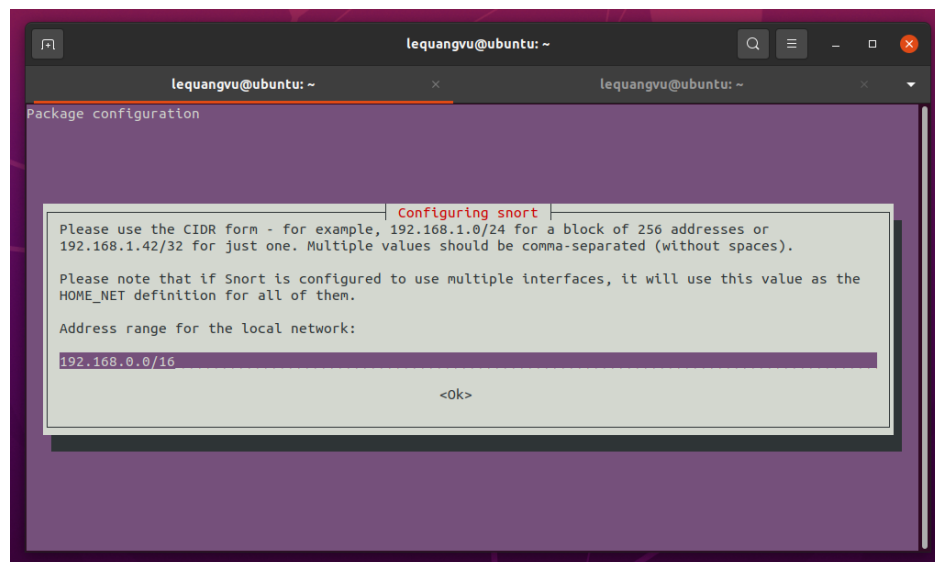
- Khi hệ thống yêu cầu cổng truy cập thì chúng ta phải dùng lệnh sau để xem cổng truy cập của chúng ta như thế nào ở đây của em là ens33 và em thấy được nó khi sử dụng lệnh sau:

Lệnh 11: ifconfig

```
lequangvu@ubuntu: ~  
lequangvu@ubuntu: ~  
lequangvu@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.140.132  netmask 255.255.255.0  broadcast 192.168.140.255  
    inet6 fe80::e2e0:b371:7d44:9594  prefixlen 64  scopeid 0x20<link>  
    ether 00:0c:29:55:7e:a7  txqueuelen 1000  (Ethernet)  
    RX packets 38875  bytes 51753505 (51.7 MB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 17108  bytes 1061193 (1.0 MB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 300  bytes 26137 (26.1 KB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 300  bytes 26137 (26.1 KB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lequangvu@ubuntu:~$
```

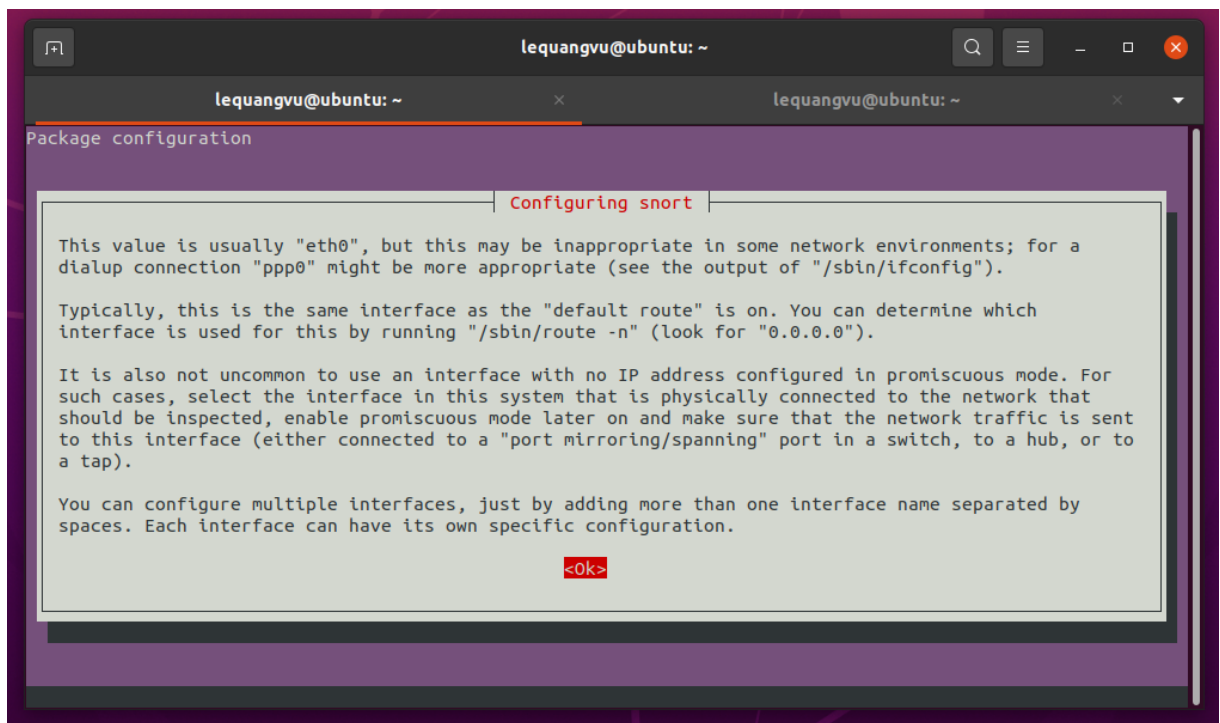
Hình 4. 5: Kết quả kiểm tra cổng truy cập

- Sau đó hệ thống sẽ kêu chúng ta phải cài đặt cổng ở đây em cài đặt cổng bắt toàn bộ địa chỉ truy cập qua lớp C và lớp D:
- Sau đó hệ thống sẽ kêu chúng ta phải cài đặt cổng ở đây em cài đặt cổng bắt toàn bộ địa chỉ truy cập qua lớp C và lớp D:

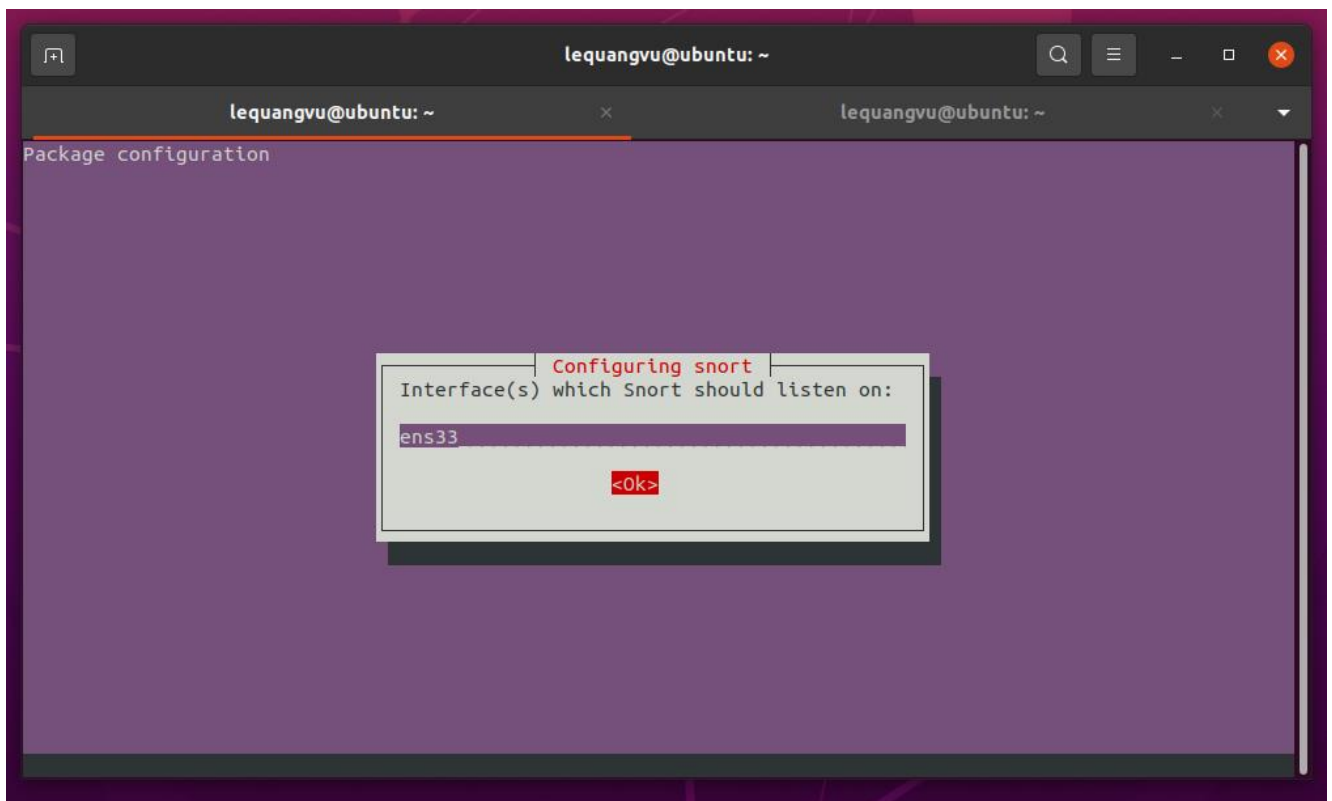


Hình 4. 6: Cài đặt lớp truy cập đến Servers Apache

- Sau Khi bấm OK chúng ta tiếp tục phần kết nối (ở đây em dùng ens33)



Hình 4. 7: Chú thích về cài đặt cổng nhận



Hình 4. 8: Cài đặt cổng nhận cho hệ thống phát hiện xâm nhập Snort

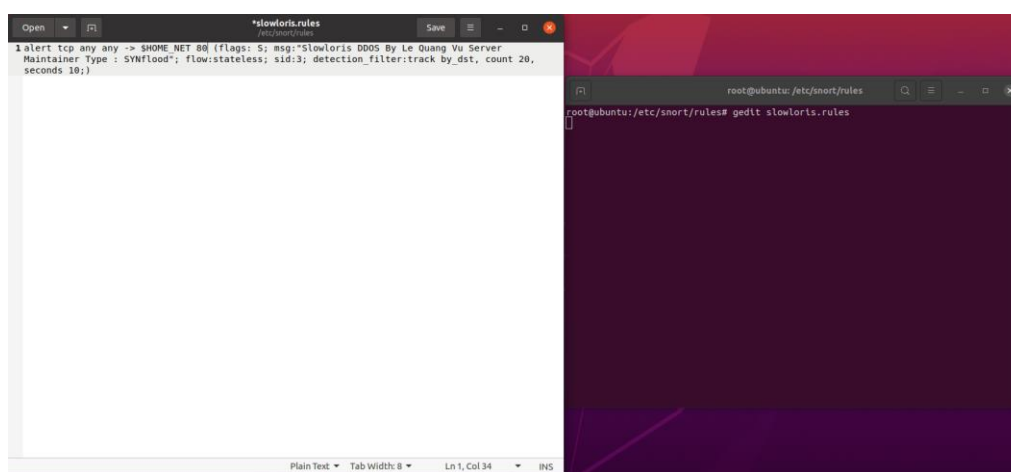
- Bước 4: Tạo luật phát hiện tấn công

- Ở đây ta sẽ tạo 1 rules mới bằng lệnh Gedit tenfile.rules (ở đây em tạo file slowloris.rules)

Lệnh 1: gedit tenfile.rules

- Copy luật sau vào để tạo trình phát hiện tấn công snort

Luật rules: alert tcp any any -> \$HOME_NET 80 (flags: S; msg:"Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYNflood"; flow: stateless; sid: 3; detection_filter: track by_dst, count 20, seconds 10;)



Hình 4. 9: Tạo file chứa Rules và cài đặt lệnh Rules

Bảng 4. 1: Các thuộc tính Rules của hệ thống phát hiện xâm nhập Snort

Thuộc tính các luật	
alert	Xuất ra màn hình
tcp	Giao thức điều khiển truyền vận.
Any any -> \$HOME_NET 80	
any	- any: Toàn bộ IP từ ngoài đi vào.
any	- any: Toàn bộ cổng của tất cả các IP bên ngoài.
\$HOME_NET	- \$HOME_NET: Địa chỉ ta cài đặt tại file snort.conf.
80	- 80: Cổng HTTP.

flags	Từ khóa này dùng để phát hiện xem những bit cờ flag nào được bật trong phần TCP header của gói tin.
msg	Câu lệnh thiết lập thông báo của hệ thống.
flow	Từ khóa flow được sử dụng để áp dụng một luật lên các gói tin di chuyển theo một hướng cụ thể.
sid	Sử dụng Session Identification, các công cụ như Atomicity Consistency Isolation Durability có thể biểu diễn luật thật sự tạo ra một cảnh báo cụ thể.
Detection_filter	Detection_filter định nghĩa 1 mức được thực thi bởi địa chỉ nguồn hoặc địa chỉ đích trước khi một luật phát sinh một sự kiện. Nó thường sử dụng để quy định 1 giới hạn nào đó mà các luật của snort đưa ra cảnh báo. Track by_dst và track by_src: Tỷ lệ được theo dõi bằng địa chỉ IP nguồn hoặc địa chỉ IP đích. Điều này có nghĩa là số lượng được duy trì cho mỗi địa chỉ IP nguồn duy nhất hoặc mỗi địa chỉ IP đích duy nhất.
Count c	Số lượng quy tắc phù hợp tối đa tính bằng giây được phép trước khi vượt quá giới hạn bộ lọc phát hiện. C phải khác không.
Seconds s	Khoảng thời gian mà số lượng được tích lũy. Giá trị phải khác không.

- Sau đó chúng ta cần phải thiết lập rules trên hệ thống Snort qua snort.conf. Chúng ta sẽ kéo xuống dưới và cài đặt đường dẫn đến luật chúng ta đã cài và sau khi xong chúng ta lưu lại.

Cài đường dẫn Rules: include \$RULE_PATH/(tên file tạo ở lệnh 1).rules

- Bước 5: Khởi chạy hệ thống chống xâm nhập

- Chúng ta dùng lệnh để khởi động Snort để xem quá trình bị tấn công như thế nào:

Lệnh 1: `sudo snort -A console -I ens33 -c /etc/snort/snort.conf`

```

lequangvu@ubuntu: ~
lequangvu@ubuntu: /etc/snort
lequangvu@ubuntu: ~$ sudo snort -A console -I ens33 -c /etc/snort/snort.conf
[sudo] password for lequangvu:
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugin!
Initializing Preprocessors!
Initializing Plug-Ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8080 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 13443:13444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8080 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 13443:13444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-optimizations = enabled
  Maximum pattern length = 20
  Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libs_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...

```

Hình 4. 10: Khởi chạy hệ thống chống xâm nhập

- Nếu chúng ta có thể phát hiện khi tấn công thì nó sẽ xuất ra các thông báo nhưng nếu không có thì bạn cài đặt luật trong hệ thống đã sai cần phải chỉnh sửa lại:

```

lequangvu@ubuntu: ~
lequangvu@ubuntu: /etc/snort
lequangvu@ubuntu: ~$ sudo snort -A console -I ens33 -c /etc/snort/snort.conf
06/12-21:46:14.740965 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35118 -> 192.168.140.132:80
06/12-21:46:14.741246 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35120 -> 192.168.140.132:80
06/12-21:46:14.747828 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35122 -> 192.168.140.132:80
06/12-21:46:14.748434 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35124 -> 192.168.140.132:80
06/12-21:46:14.749665 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35126 -> 192.168.140.132:80
06/12-21:46:14.750057 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35128 -> 192.168.140.132:80
06/12-21:46:14.751321 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35130 -> 192.168.140.132:80
06/12-21:46:14.751563 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35132 -> 192.168.140.132:80
06/12-21:46:14.752825 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35134 -> 192.168.140.132:80
06/12-21:46:14.753220 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35136 -> 192.168.140.132:80
06/12-21:46:14.754362 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35138 -> 192.168.140.132:80
06/12-21:46:14.761475 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35140 -> 192.168.140.132:80
06/12-21:46:14.764862 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35142 -> 192.168.140.132:80
06/12-21:46:14.769477 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35144 -> 192.168.140.132:80
06/12-21:46:14.772527 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35146 -> 192.168.140.132:80
06/12-21:46:14.777691 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35148 -> 192.168.140.132:80
06/12-21:46:14.782238 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35150 -> 192.168.140.132:80
06/12-21:46:14.787590 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35152 -> 192.168.140.132:80
06/12-21:46:14.796416 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35154 -> 192.168.140.132:80
06/12-21:46:14.797712 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35156 -> 192.168.140.132:80
06/12-21:46:14.798928 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35158 -> 192.168.140.132:80
06/12-21:46:14.800046 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35160 -> 192.168.140.132:80
06/12-21:46:14.800748 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35162 -> 192.168.140.132:80
06/12-21:46:14.808355 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35164 -> 192.168.140.132:80
06/12-21:46:14.809208 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35166 -> 192.168.140.132:80
06/12-21:46:14.810013 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35168 -> 192.168.140.132:80
06/12-21:46:14.810882 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35170 -> 192.168.140.132:80
06/12-21:46:14.815640 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35172 -> 192.168.140.132:80
06/12-21:46:14.816792 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35174 -> 192.168.140.132:80
06/12-21:46:14.817547 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35176 -> 192.168.140.132:80
06/12-21:46:14.818479 [**] [1:3:0] Slowloris DDOS By Le Quang Vu Server Maintainer Type: SYN Flood [**] [Priority: 0] [TCP] 192.168.140.130:35178 -> 192.168.140.132:80

```

Hình 4. 11: Hiện thị tất cả các cuộc tấn công Slowloris tới Servers Apache

- Sau khi, chúng ta đã phát hiện các cuộc tấn công rồi chúng ta tiếp tục với việc phòng thủ nó bằng phần mềm CSF Firewall qua các bước sau:
- Bước 1: Cài đặt hệ thống chống xâm nhập CSF FIREWALL

- Chúng ta dùng lệnh để cài đặt hệ thống chống tấn công csf firewall lần lượt theo thứ tự:

Lệnh 1: wget <http://download.configserver.com/csf.tgz>

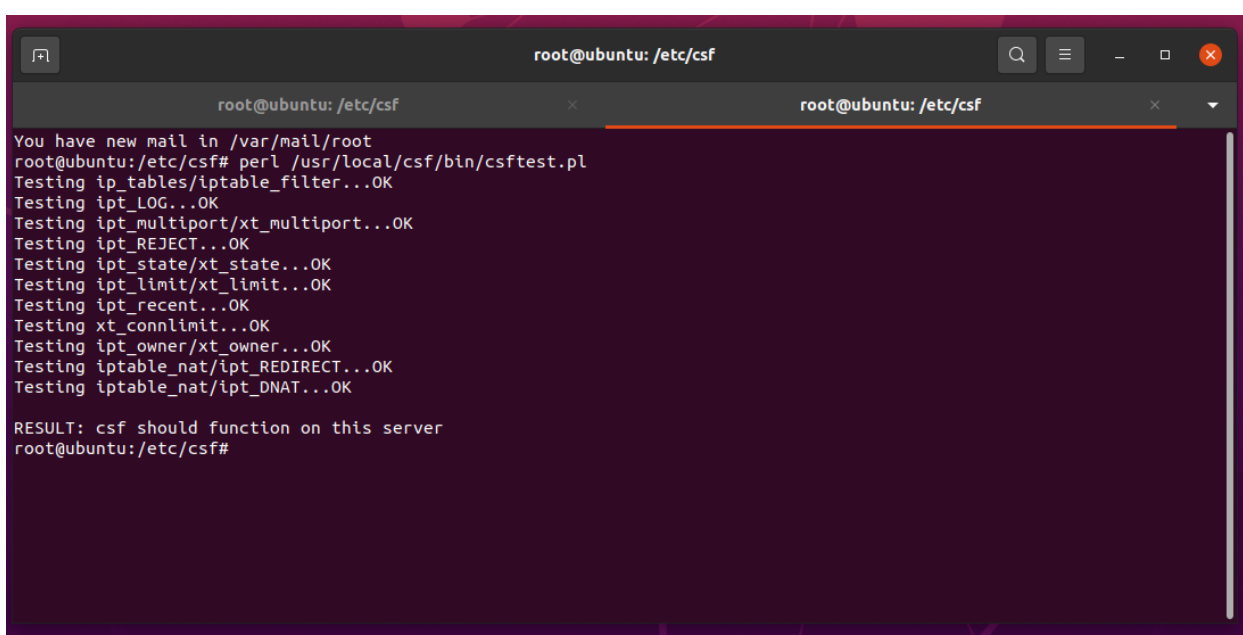
Lệnh 2: tar -xvzf csf.tgz

Lệnh 3: cd csf

Lệnh 4: ls

- Chúng ta cần kiểm tra lại hệ thống đã được cài đặt chưa bằng lệnh sau:

Lệnh 12: perl /usr/local/csf/bin/csfctest.pl



```
root@ubuntu: /etc/csf
You have new mail in /var/mail/root
root@ubuntu:/etc/csf# perl /usr/local/csf/bin/csfctest.pl
Testing ip_tables/iptables_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/iptables_REDIRECT...OK
Testing iptable_nat/iptables_DNAT...OK

RESULT: csf should function on this server
root@ubuntu:/etc/csf#
```

Hình 4. 12: Kiểm tra hệ thống đã được cài vào Server

- Sau khi cài đặt hệ thống thành công chúng ta tiếp tục đến với cài đặt thông số nhằm phòng chống xâm nhập các cuộc tấn công Slowloris. Chỉnh sửa các thông số phòng chống trong file csf.conf:
- Tìm kiếm và cài đặt theo thông số sau:
- Thiết Lập Hoạt Động csf firewall
 - TESTING = "0"
 - RESTRICT_SYSLOG = "3"
- Thiết lập mở cổng và đóng cổng:
 - TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"
 - TCP_OUT = "20,21,22,25,53,80,110,113,443,587,993,995"

- UDP_IN = "20,21,53,80,443"
- UDP_OUT = "20,21,53,113,123"
- Cho phép server truy vấn DNS bên ngoài
 - ICMP_IN = "1"
- Bảo vệ khỏi tấn công DDOS:
 - CONNLIMIT = "80;100,12;100"
 - Hàm này có nghĩa là cổng 80 (http) cho phép 100 kết nối với 1 IP và nếu tạo quá số 100 đó sẽ bị block
 - PORTFLOOD = "80;tcp;100;5"
 - Hàm này có nghĩa là 1 IP nào đó kết nối với cổng 80 bằng giao thức TCP, trong vòng 5s mà tạo ra 100 kết nối thì sẽ bị block
 - SYNFLOOD = "1"
 - SYNFLOOD_RATE = "75/s"
 - SYNFLOOD_BURST = "25"
 - Lệnh SYNFLOOD = "1" dùng để kích hoạt SYN FLOOD
 - SYNFLOOD_RATE dùng để thiết lập gói SYN gửi tới 1 IP/1s. Số lần mà 1 IP có thể chạm tới SYNFLOOD_RATE trước khi bị block
- Sau khi xong chúng ta cần restart hệ thống.
- Bước 2: Khởi chạy hệ thống chống xâm nhập
 - Sau khi thấy hệ thống đã bật chúng ta phải tiếp tục bật 2 loại csf và lfd của hệ thống nhằm ngăn chặn ddos bằng lệnh sau:
 - Csfc: hệ thống tường lửa CSF Firewall
 - LFD là ghi nhận thấy 1 tiến trình đang sử dụng nhiều hơn mức tài nguyên được giám sát.

Lệnh 1: `systemctl start csf`
 Lệnh 2: `systemctl start lfd`

- Sau khi xong chúng ta bắt đầu tấn công bằng ddos và kết quả như sau:

- Sau khi tấn công lại chúng ta thấy vẫn tấn công bình thường

The screenshot shows a terminal window titled 'lequangvu@kali: ~/slowloris'. The window contains the following text:

```

File Actions Edit View Help
Current stats: Slowloris has now sent 1394 packets successfully.
This thread now sleeping for 10000 seconds ...

    Sending data.
Current stats: Slowloris has now sent 1564 packets successfully.
This thread now sleeping for 10000 seconds ...

    Building sockets.
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 1873 packets successfully.
This thread now sleeping for 10000 seconds ...

    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 2088 packets successfully.
This thread now sleeping for 10000 seconds ...

    Sending data.
Current stats: Slowloris has now sent 2354 packets successfully.
This thread now sleeping for 10000 seconds ...

    Sending data.
Current stats: Slowloris has now sent 2500 packets successfully.
This thread now sleeping for 10000 seconds ...
  
```

Hình 4. 15: Thống kê tấn công Slowloris khi ngừng hoạt động CSF Firewall

4.3 Kết luận chương:

- Em đã phân tích và thiết kế ra phương thức phòng thủ đơn giản mà hiệu quả đối với các cuộc tấn công Slowloris nhưng vẫn còn một vài hạn chế. Sau đây, em sẽ nêu các ưu điểm và nhược điểm của các phần mềm em đã sử dụng và rút ra các kết luận ở chương tiếp theo.

CHƯƠNG 5. KẾT LUẬN VÀ KIẾN NGHỊ

5.1 Kết quả đạt được:

Trong quá trình nghiên cứu và hoàn thành đồ án tốt nghiệp với đề tài “Tìm hiểu các phương thức tấn công từ chối dịch vụ và giải pháp ngăn chặn” em đã đạt được các kết quả như sau:

Về mặt kiến thức

- Hiểu được cơ bản về an ninh mạng và tấn công mạng là gì, hiện trạng thực tế mà thế giới phải gánh chịu các cuộc tấn công.
- Hiểu được quy trình tấn công từ chối dịch vụ để từ đó đưa ra các biện pháp ngăn chặn cũng như giảm thiểu chúng.
- Có được kiến thức về hệ điều hành, hiểu được các quy trình mà 1 hệ điều hành giả lập hoạt động như thế nào.

Về mặt ứng dụng

- Từ những kết quả gặt hái được em đã có thể cài đặt 1 server không phải chịu các cuộc tấn công từ các attacker để từ đó có được biện pháp cũng như tìm hiểu để cài đặt các phần mềm phòng thủ tránh việc xâm nhập của các attacker.

Về mặt kiến thức

- Quá trình làm đồ án tuy thời gian không nhiều nhưng em đã học hỏi, rèn luyện cho bản thân khả năng tìm kiếm, nghiên cứu các cách để giải quyết vấn đề, tài liệu, nhìn nhận và xử lý vấn đề, khả năng xây dựng tài liệu cũng như học được cách thức bảo vệ server, rèn luyện tính kiên nhẫn và tăng khả năng trình bày văn bản, ... đó là những kỹ năng vô cùng cần thiết giúp cho bản thân em có thêm hành trang cho tương lai làm việc phía trước.
- Từ những điều trên, bản thân em đã hoàn thành cơ bản những mục tiêu mà thầy cô và bản thân đã đề ra ban đầu so với đề tài hiện tại.

5.2 Tồn tại:

Bên cạnh những mặt tích cực thì trong đề tài còn nhiều bất cập như:

- Các tài liệu về phân tích hệ thống không còn được cập nhật thường xuyên và đa phần các phần mềm vẫn còn chưa được hoàn hảo dẫn đến các thiếu sót trong quá trình bảo vệ.

- Tài liệu về các việc phòng thủ hiện đã được bảo mật nên việc tìm kiếm trở nên rất khó khăn.
- Vì thời gian và kiến thức còn hạn chế nên việc triển khai các hoạt động của phần mềm chưa được hoàn hảo, chưa triển khai được hết các chức năng luồng chức năng.

5.3 Hướng phát triển:

Trong tương lai nếu có điều kiện đồ án của em sẽ phát triển theo các hướng sau:

- Thiết lập cài đặt 1 phần mềm hoàn hảo có thể tránh các cuộc xâm nhập.
- Nghiên cứu nhiều hơn để xây dựng được tài liệu về các cách thức phòng thủ để cho mọi người đều biết để tránh khỏi các cuộc tấn công của attacker.
- Vì kiến thức còn nhiều hạn chế, thời gian tìm hiểu, nghiên cứu và triển khai còn có hạn vì vậy đồ án của em còn nhiều sai sót, mong quý Thầy Cô sẽ có nhiều nhận xét đánh giá để đồ án của em có thể hoàn thiện và phát triển hơn.

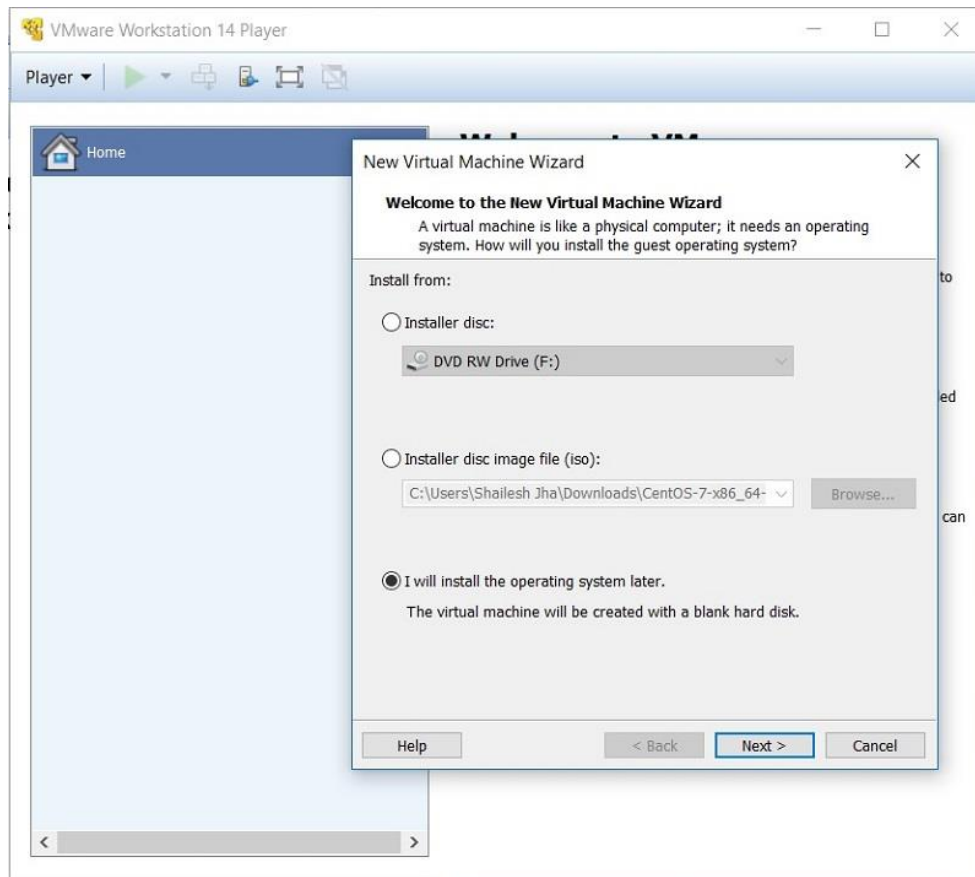
PHỤ LỤC

Phụ lục 1: Hướng dẫn cài đặt

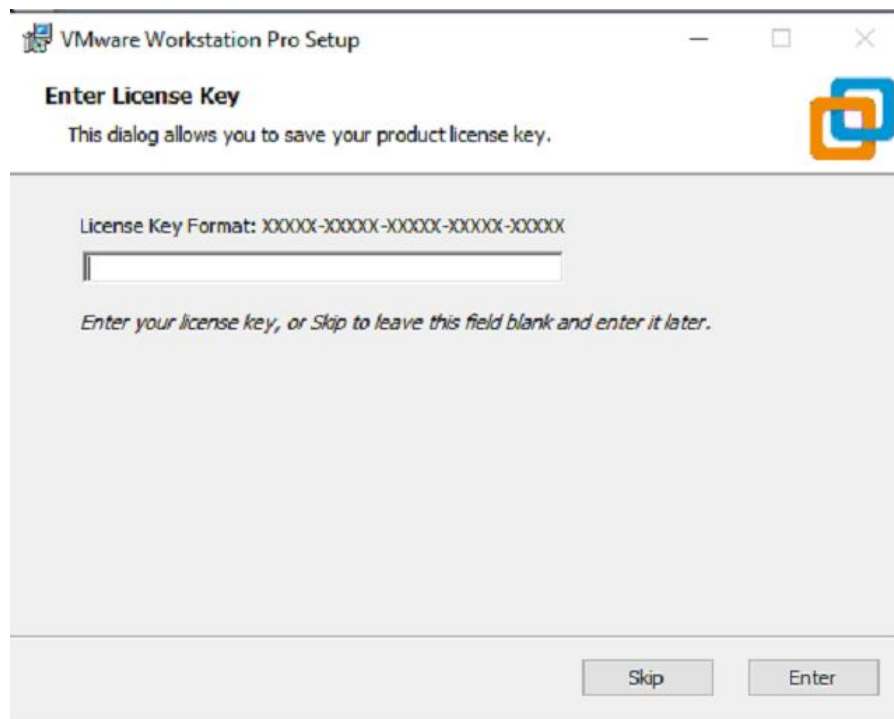
- **Bước 1: Tải phần mềm**



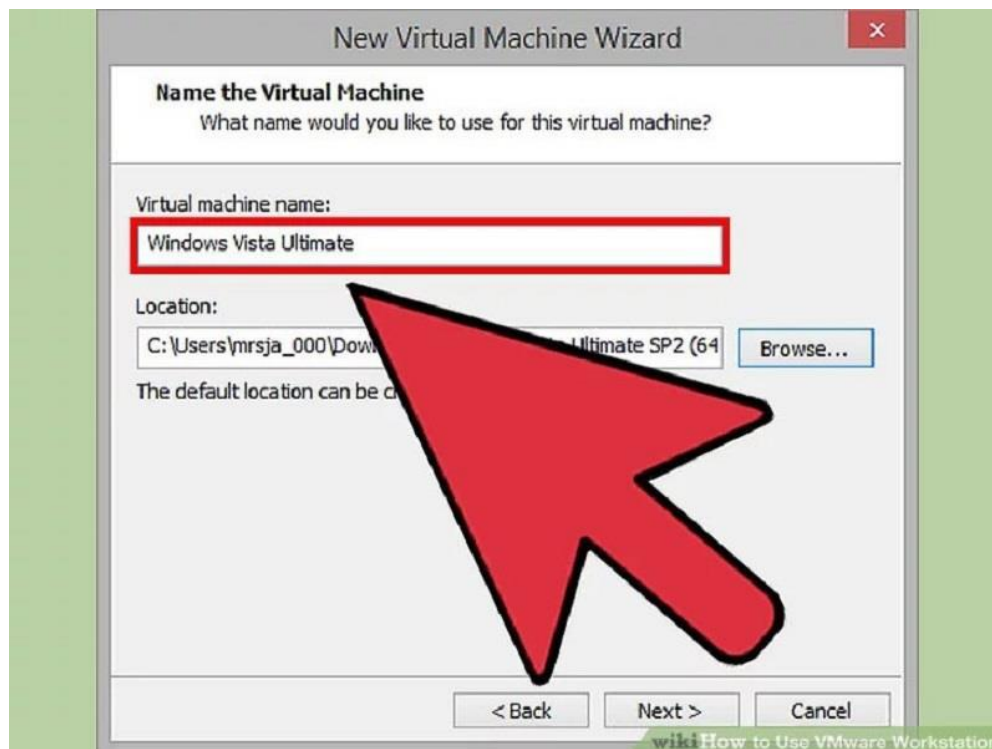
- Hãy bấm vào đây để tải phần mềm VMware Workstation về máy và tiến hành cài đặt. Khi cài đặt, bạn chỉ cần click chuột vào Agree và Next đến khi máy tính hiện thêm lệnh Finish thì click vào đó là bạn đã hoàn thành bước thiết lập cài đặt.
 - Lưu ý: Nếu bạn sử dụng phiên bản Pro hoặc muốn nâng cấp bản Pro thì vẫn có thể tham khảo hướng dẫn này. Vì chung quy thì cách sử dụng và giao diện của Pro mà bản thường giống nhau.
- **Bước 2: Khởi động chương trình**



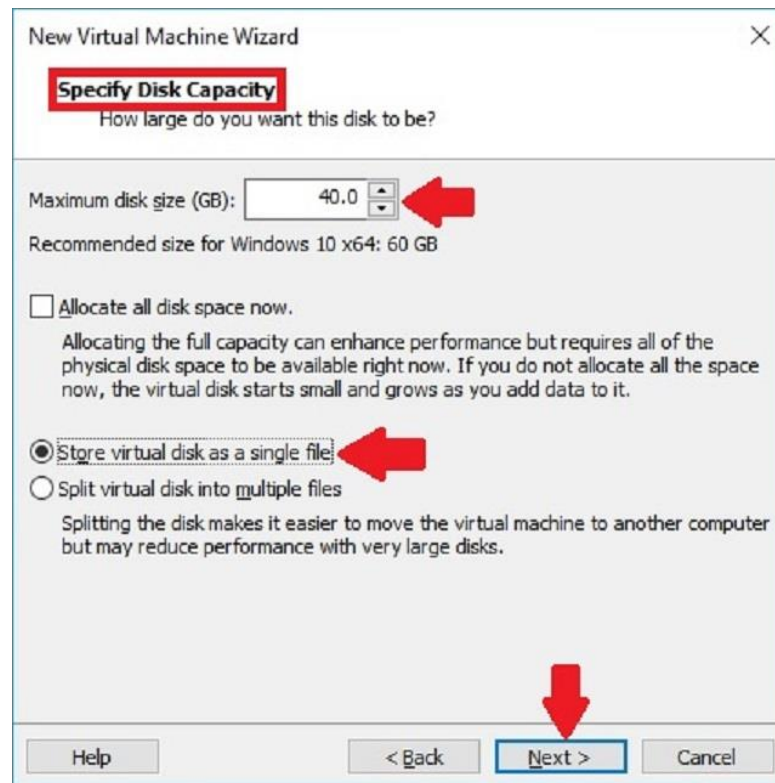
- Click chuột vào biểu tượng Run as administrator để tiến hành khởi động chương trình của phần mềm máy ảo.
- Sau đó, chọn New Virtual Machine và click vào Typical. Tiếp theo là lựa chọn phương tiện cài đặt sau khi nhận được thông báo của VMware. Nếu VMware hỗ trợ cài đặt hệ điều hành hiện tại thì bạn sẽ thấy tùy chọn Easy Installation hiển thị ngay trên màn hình.
- **Bước 3: Product key**



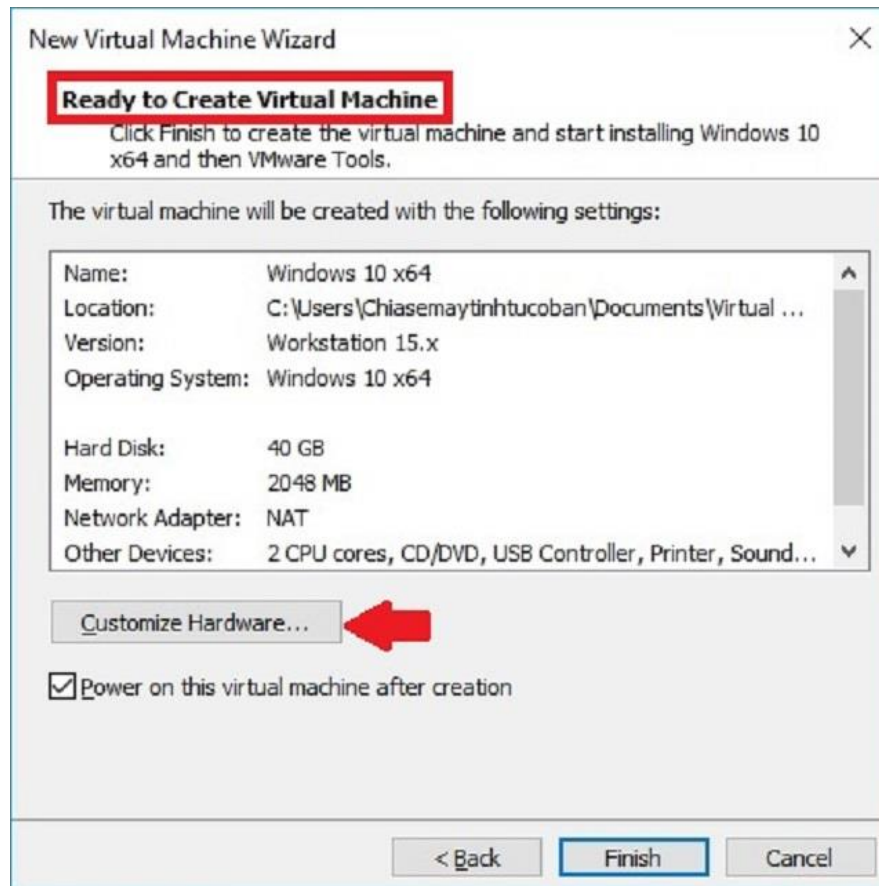
- Nhập product key của Window được sử dụng trên máy ảo, bạn cũng có thể sử dụng key của Window máy tính chủ.
- Tiếp đến là bước bảo mật thông tin và bảo vệ máy ảo, bạn chỉ cần dùng thiết lập mật khẩu là xong.
- **Bước 4: Tên và vị trí lưu máy ảo**



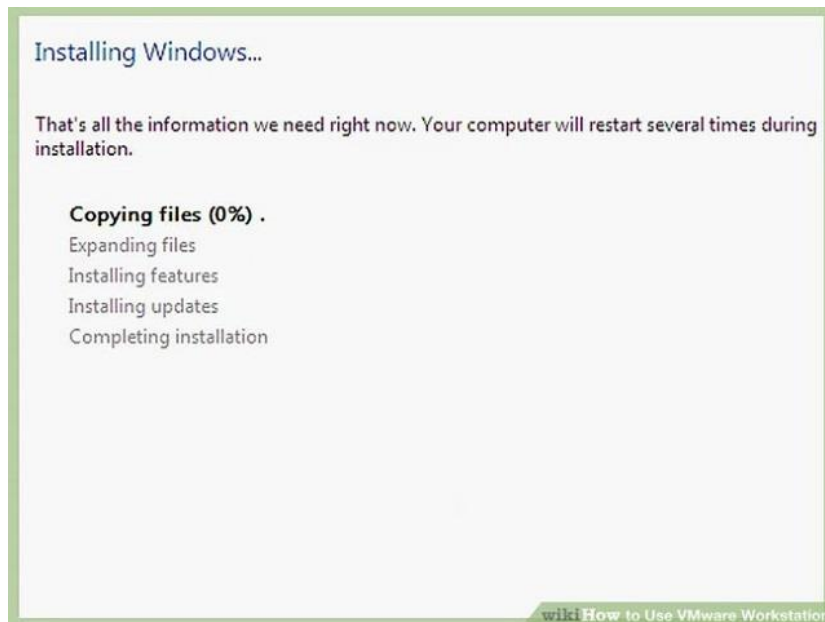
- Tên và vị trí của máy ảo VMware Workstation sẽ giúp bạn phân biệt dễ dàng khi máy tính của bạn có quá nhiều máy ảo khác nhau.
- **Bước 5: Thiết lập Disk Size**



- Đây là thao tác khó nhất và quyết định bạn có cài đặt VMware Workstation thành công hay không. Bạn phải tính toán được dung lượng cần phải sử dụng trên Win cũng như các chương trình cần lưu trữ trên máy ảo.
- Tuy nhiên một điều đáng mừng là VMware có tính năng Recommend để giúp bạn tính toán dung lượng cần thiết trên Windows. Tuy nhiên, bạn vẫn có thể mở rộng thêm để thoải mái sử dụng, nhưng mức mở rộng tối thiểu là 20GB.
- **Bước 6: Xây dựng cấu hình trên máy ảo**



- Hãy chọn Customize Hardware, sau đó bạn có thể thiết lập cấu hình và các phương thức kết nối theo mong muốn của bạn. Tất nhiên cấu hình trên máy ảo thì không thể nào mạnh bằng cấu hình của máy thật.
- Một tips nho nhỏ đó là nếu bạn chỉ cần các tác vụ cơ bản thì chỉ cần từ 1 đến 2GB là đã đảm bảo đủ sử dụng. Vậy thì Network Adapter bạn nên chọn NAT để đảm bảo đường truyền tốt nhất.
- **Bước 7: Cài win và kiểm tra kết quả**
- Nếu tất cả những thông tin bạn cung cấp đã đầy đủ và chính xác thì máy sẽ thao tác tự động giúp bạn. Sau khi cài đặt thành công thì VMware Workstation sẽ hiển thị thêm mục Install VMware Tools.



- Sau khi cài đặt thành công, đừng quên tìm hiểu về cách sử dụng VMware Workstation như thế nào cho đúng cách để mang lại hiệu quả cao nhé.
- Sau khi cài đặt cần phải cài đặt 2 môi trường giả lập sau bao gồm:
 - Hướng dẫn cài đặt KaliLinux: <https://quantrimang.com/cach-cai-dat-va-su-dung-kali-linux-126114>
 - Hướng dẫn cài đặt Ubuntu Server: <https://news.cloud365.vn/huong-dan-cai-dat-ubuntu-20-04/>

Phụ lục 2: Hướng dẫn sử dụng:

- Khởi động 2 thiết bị và thiết lập theo quy trình cài đặt tấn công phòng thủ như đã nói ở Chương 3 và 4.

TÀI LIỆU THAM KHẢO

- [1] B. Gupta, An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook, Germany: Academic Publishing, 2011.
- [2] Eric Chou And Rich Groves, Distributed Denial of Service DDoS Practical Detection and Defense, Highway North, Sebastopol: O'Reilly Media, 2018.
- [3] Allot, "DDoS Attack Handbook Service Providers," Allot, 2018. [Online]. Available: <https://www.allot.com/docs/ddos-attack-handbook.pdf>. [Accessed 14 07 2021].
- [4] Vinicius da Silva Faria, SDToW: A Slowloris Detecting Tool for WMNs, Brazil, 2020.
- [5] Nguyễn Trang, "Tìm hiểu về máy ảo," VMWare, 18 06 2021. [Online]. Available: <https://quantrimang.com/tim-hieu-ve-may-ao-88905>. [Accessed 16 07 2021].
- [6] Nguyễn Thoại, "UBUNTU SERVER CHUYÊN NGHIỆP CHO HỆ THỐNG SERVER," Debian, 08 02 2020. [Online]. Available: <https://www.semtek.com.vn/ubuntu-server-la-gi/>. [Accessed 16 07 2021].
- [7] Quách Chí Cường, "Kali Linux là gì? Giới thiệu Hệ Điều Hành Kali Linux," Debian, 27 08 2018. [Online]. Available: <https://cuongquach.com/kali-linux-la-gi-gioi-thieu-he-dieu-hanh-kali-linux.html>. [Accessed 16 07 2021].
- [8] Đức Trí, "Snort là gì?," Cisco Systems, Sourcefire, 12 10 2019. [Online]. Available: <https://huudoanh.com/snort-la-gi/>. [Accessed 17 07 2021].
- [9] Hưng Nguyễn, "Hướng dẫn cài đặt và cấu hình CSF Firewall chi tiết nhất 2021," 30 03 2021. [Online]. Available: <https://vietnix.vn/csf-firewall/>. [Accessed 19 07 2021].
- [10] Shima Sabri, Noraini Ismail and Amir Hazzim, Slowloris DoS Attack Based Simulation, IOP Publishing Ltd, 2021.
- [11] Chad L. Calvert & Taghi M. Khoshgoftaar, "Slowloris.py," gkbrk, 08 03 2019. [Online]. Available: <https://github.com/gkbrk/slowloris>. [Accessed 19 07 2021].