**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 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 năm 2021

TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI **CỘNG HÒA XÃ HỘI CHỦ NGHIÃ VIỆT NAM**

**PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH** Độc lập – Tự do – Hạnh phúc

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

1. **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.

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

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

1. **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 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

1. **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 hơn 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 hiện 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 hiên

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](#_Toc75616338)

[LỜI CẢM ƠN iv](#_Toc75616339)

[NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN v](#_Toc75616340)

[MỤC LỤC vi](#_Toc75616341)

[MỞ ĐẦU 1](#_Toc75616342)

[CHƯƠNG 1 CƠ SỞ LÝ THUYẾN 3](#_Toc75616343)

[1.1 Tổng quan về CRM 3](#_Toc75616344)

[1.1.1 Giới thiệu về CRM 3](#_Toc75616345)

[1.1.2 Thế nào là một hệ thống CRM toàn diện 3](#_Toc75616346)

[1.1.3 Thực tế xây dựng hệ thống CRM ngày nay 3](#_Toc75616347)

[1.1.4 Hệ thống CRM xây dựng trong đồ án. 4](#_Toc75616348)

[1.2 Tổng quan về Idempiere 4](#_Toc75616349)

[1.2.1 Khái niệm về idempiere 4](#_Toc75616350)

[1.2.2 Mối tương quan giữa ERP và CMR 5](#_Toc75616351)

[CHƯƠNG 2 PHÂN TÍCH YÊU CẦU KHÁCH HÀNG 6](#_Toc75616352)

[2.1 Yêu cầu thực tế của công ty xăng dầu 6](#_Toc75616353)

[2.2 Xây dựng tài liêu diễn tả các quy trình nghiệp vụ 14](#_Toc75616354)

[2.2.1 Quy Trình Tạo đơn hàng 15](#_Toc75616355)

[2.2.2 Quy trình xuất hóa đơn (1B) 18](#_Toc75616356)

[2.2.3 Quy trình Điều chỉnh/ Hủy đơn hàng (1C) 22](#_Toc75616357)

[2.2.4 Quy trình Tách phiếu xuất kho hàng gửi (2A) 25](#_Toc75616358)

[2.2.5 Quy trình Tách phiếu xuất kho kiêm vận chuyển nội bộ (2B) 28](#_Toc75616359)

[2.2.6 Quy trình điều chỉnh phiếu xuất kho hàng gửi và phiếu xuất kho kiêm vận chuyển nội bộ (2C) 30](#_Toc75616360)

[2.2.7 Quy trình lập kế hoạch nhận hàng 34](#_Toc75616361)

[2.2.8 Quy trình giao nhận hàng tại kho (4) 35](#_Toc75616362)

[2.2.9 Quy trình giao nhận hàng tại kho/CHXD của khách hàng bán buôn (5A) 38](#_Toc75616363)

[2.2.10 Quy trình giao nhận hàng tại kho của khách hàng công nghiệp 39](#_Toc75616364)

[2.2.11 Quy trình thanh toán 42](#_Toc75616365)

[2.2.12 Quy trình tích hợp chứng từ điện tử 42](#_Toc75616366)

[2.2.13 Quy trình Quản lý Khách hàng 43](#_Toc75616367)

[2.2.14 Quy trình Quản lý hợp đồng 44](#_Toc75616368)

[CHƯƠNG 3 XÂY DỰNG CƠ SỞ DỮ LIỆU 45](#_Toc75616369)

[3.1 Hệ cơ sở dữ liệu chuẩn. 45](#_Toc75616370)

[3.2 Thiết kế cấu trúc dữ liệu 45](#_Toc75616371)

[3.2.1 Sơ đồ quan hệ người dùng 46](#_Toc75616372)

[3.2.2 Sơ đồ quan hệ vai trò (chức năng-role) 50](#_Toc75616373)

[3.2.3 Sơ đồ quan hệ đơn vị kinh doanh 50](#_Toc75616374)

[3.2.4 Sơ đồ quan hệ sản phẩm 51](#_Toc75616375)

[3.2.5 Sơ đồ quan hệ đơn hàng 51](#_Toc75616376)

[3.2.6 Sơ đồ quan hệ giá 52](#_Toc75616377)

[3.2.7 Sơ đồ quan hệ thanh toán 52](#_Toc75616378)

[3.2.8 Sơ đồ quan hệ hóa đơn 53](#_Toc75616379)

[3.2.9 Sơ đồ quan hệ hợp đồng 53](#_Toc75616380)

[3.2.10 Phiếu xuất 54](#_Toc75616381)

[CHƯƠNG 4 THỬ NGHIỆM VÀ ĐÁNH GIÁ 55](#_Toc75616382)

[4.1 Kết quả thử nghiệm 55](#_Toc75616383)

[4.1.1 Chức năng chính của chương trình 55](#_Toc75616384)

[CHƯƠNG 5 KẾT LUẬN VÀ KIẾN NGHỊ 65](#_Toc75616385)

**DANH MỤC CHỮ VIẾT TẮT**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Mô tả** | **Ý nghĩa** | **Ghi chú** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**DANH MỤC BẢNG BIỂU**

**DANH MỤC HÌNH ẢNH**

[*Hình 2.1 Quy trình tạo đơn hàng* 26](#_Toc75616419)

[*Hình 2.2* *Quy trình xuất hóa đơn.* 29](#_Toc75616420)

[*Hình 2.3* *Quy trình điều chỉnh/Hủy đơn hàng* 33](#_Toc75616421)

[*Hình 2.4 Quy trình tách phiếu xuất kho hàng gửi (2A)* 36](#_Toc75616422)

[*Hình 2.5* *Quy trình tách phiếu xuất kho kiêm vận chuyển nội bộ* 38](#_Toc75616423)

[*Hình 2.6 Quy trình điều chỉnh phiếu xuất kho hàng gửi kiêm vận chuyển nội bộ* 40](#_Toc75616424)

[*Hình 2.8 Quy trình giao nhận hàng tại kho* 45](#_Toc75616426)

[*Hình 2.9 Quy trình giao nhận hàng tại kho/CHXD của khách hàng bán buôn.* 48](#_Toc75616427)

[*Hình 2.10 Quy trình giao nhận hàng tại kho của khách hàng công nghiệp*. 50](#_Toc75616428)

[*Hình 2.11 Quy trình thanh toán* 52](#_Toc75616429)

[*Hình 2.12 Quy trình tích hợp chức từ điển tử.* 53](#_Toc75616430)

[*Hình 2.13 Quy trình quản lý khách hàng.* 53](#_Toc75616431)

[*Hình 3.1 Tổng quan các bảng trong hệ cơ sở dữ liệu* 55](#_Toc75616433)

[*Hình 3.2mô hình quan hệ theo chức năng hệ thống* 56](#_Toc75616434)

[*Hình 3.3 Sơ đồ quan hệ người dùng* 56](#_Toc75616435)

[*Hình 3.4 Sơ đồ quan hệ vai trò (chức năng -role)* 59](#_Toc75616436)

[*Hình 3.5 Sơ đồ quan hệ đơn vị kinh doanh* 59](#_Toc75616437)

[*Hình 3.6 Sơ đồ quan hệ sản phẩm* 60](#_Toc75616438)

[*Hình 3.7 Sơ đồ quan hệ đơn hàng* 60](#_Toc75616439)

[*Hình 3.8 Sơ đồ quan hệ giá* 61](#_Toc75616440)

[*Hình 3.9 Sơ đồ quan hệ thanh toán* 61](#_Toc75616441)

[*Hình 3.10 Sơ đồ quan hệ hóa đơn* 62](#_Toc75616442)

[*Hình 3.11 Sơ đồ quan hệ hợp đồng* 62](#_Toc75616443)

[*Hình 3.12 Sơ đồ quan hệ phiếu xuất* 63](#_Toc75616444)

MỞ ĐẦU

* 1. Lý do chọn đề tài

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

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

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

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.

* 1. Mục tiêu nghiên cứu

- Đầu tiên, nghiên cứu về tấn công từ chối dịch 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.

* 1. Đối tượng và phạm vi nghiên cứu

- 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.

* 1. Cấu trúc báo cáo thực tập tốt nghiệp

- Việc cài đặt hệ thống chống tấn công từ chối dịch vụ DOS/DDOS là việc hết sức cần thiết cho hiện tại:

* + Đối với các cá nhân, chúng ta sẽ bảo đảm được việc demo các đồ án hay việc demo cho các khách hàng sẽ ko bị gián đoạn.
  + Đối với các doanh nghiệp, thì sẽ không bị rò rỉ thông tin cho các doanh nghiệp đối địch với mình cũng như các đối thủ.
  + Đối với các tổ chức xã hội, những bảo mật này sẽ giúp cho các tổ chức ko bị vi phạm quyền riêng tư cá nhân và bảo đảm được hệ thống hoạt động tốt. Ví dụ: nếu 1 tổ chức bị rò rỉ thông tin hay hệ thống có vấn đề về việc chậm trễ sẽ có rất nhiều ảnh hưởng đến người dân cũng như người tin tưởng tổ chức đó.

- Kiến thức về servers là một thứ không thể thiếu đối với bất kì 1 doanh nghiệp hay 1 công ty nào. Nhiều người nghĩ rằng kiến thức servers chỉ có thể được áp dụng bởi các công ty lớn với đội ngũ lớn mạnh.

- Trong cuốn báo cáo này, tôi muốn cho thấy việc tự xây dựng các giải pháp bảo mật từ kiến thức servers là cực kì dễ dàng như thế nào và cách thực hiện nó một cách hiệu quả nhất. Các ứng dụng của servers là vô tận và với lượng thông tin xử lý cực lớn.

* 1. Cấu trúc báo cáo thực tập tốt nghiệp
     1. Chương 1: trình bày …
     2. Chương 2: trình bày …
     3. Chương 3: trình bày ....

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

## Tổng quan an toàn mạng và tấn công mạng:

### 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. Trong bài viết này, hãy cùng SecurityBox tìm hiểu giải pháp phòng chống mất an toàn thông tin cho tổ chức, doanh nghiệp.

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 vây, 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.

### 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.

### 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.

### 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.

### 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 liễu hoặc đoạt được quyền truy cập hệ thống.
  + **Lỗ hổng loại B**: Lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến lộ, lọt thông tin.
  + **Lỗ hổng loại A**: Cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống.
* Các hình thức tấn công mạng phổ biến:
  + **Tấn công trực tiếp:** Sử dụng một máy tính để tấn công một máy tính khác với mục đích dò tìm mật mã, tên tài khoản tương ứng, …. Kẻ tấn công có thể sử dụng một số chương trình giải mã để giải mã các file chứa password trên hệ thống máy tính của nạn nhân. Do đó, những mật khẩu ngắn và đơn giản thường rất dễ bị phát hiện.
  + **Kỹ thuật đánh lừa (Social Engineering):** Đây là thủ thuật được nhiều hacker sử dụng cho các cuộc tấn công thâm nhập vào hệ thống mạng và máy tính bởi tính đơn giản mà hiệu quả của nó. Kỹ thuật này thường được sử dụng để lấy cắp mật khẩu, thông tin, tấn công vào và phá hủy hệ thống. Ví dụ, kỹ thuật đánh lừa Fake Email Login.
  + **Kỹ thuật tấn công vào vùng ẩn:** Những phần bị dấu đi trong các website thường chứa những thông tin về phiên làm việc của các client. Các phiên làm việc này thường được ghi lại ở máy khách chứ không tổ chức cơ sở dữ liệu trên máy chủ. Vì vậy, người tấn công có thể sử dụng chiêu thức View Source của trình duyệt để đọc phần đầu đi này và từ đó có thể tìm ra các sơ hở của trang Web mà họ muốn tấn công. Từ đó, có thể tấn công vào hệ thống máy chủ.
  + **Tấn công vào các lỗ hổng bảo mật:** Hiện, nay các lỗ hổng bảo mật được phát hiện càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Các hãng sản xuất cũng luôn cập nhật các bản vá lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước. Do đó, người sử dụng phải luôn cập nhật thông tin và nâng cấp phiên bản cũ mà mình đang sử dụng để tránh các hacker lợi dụng điều này tấn công vào hệ thống.
  + **Khai thác tình trạng tràn bộ đệm:** Tràn bộ đệm là một tình trạng xảy ra khi dữ liệu được gửi quá nhiều so với khả năng xử lý của hệ thống hay CPU. Nếu hacker khai thác tình trạng tràn bộ đệm này thì họ có thể làm cho hệ thống bị tê liệt hoặc làm cho hệ thống mất khả năng kiểm soát.
  + **Nghe trộm:** Các hệ thống trao đổi thông tin qua mạng đôi khi không được bảo mật tốt và lợi dụng điều này, hacker có thể truy cập vào data paths để nghe trộm hoặc đọc trộm luồng dữ liệu truyền qua.
  + **Kỹ thuật giả mạo địa chỉ:** Thông thường, các mạng máy tính nối với Internet đều được bảo vệ bằng tường lửa. Tường lửa có thể hiểu là cổng duy nhất mà người đi vào nhà hay đi ra cũng phải qua đó. Tường lửa hạn chế rất nhiều khả năng tấn công từ bên ngoài và gia tăng sự tin tưởng lẫn nhau trong việc sử dụng tài nguyên chia sẻ trong mạng nội bộ.
  + **Kỹ thuật 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 gởi đến liên tục làm cho hệ thống nghẽn mạch và một số dịch vụ sẽ không đáp ứng được cho khách hàng thật sự.

## Giới thiệu kỹ thuật tấn công DoS:

### 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 kể tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).
* Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đính của tấn công DoS.

### 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, vaf 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 tháng 2/2000.
* Từ đó các cuộc tấn công DoS thường xuyên sảy ra. Ví dụ:
  + Vào ngày 15 tháng 8 năm 2003, Microsoft đã chịu đợt tấn công DoS cực mạnh và làm gián đoạn websites trong vòng 2 giờ.
  + Vào lúc 15:09 giờ GMT ngày 27 tháng 3 năm 2003: toàn bộ phiên bản tiếng anh của website Al-Jazeera bị tấn công làm gián đoạn trong nhiều giờ.

### 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, hệt hống 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,…

## Giới thiệu kỹ thuật tấn công DdoS:

### 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 bonet – 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.

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

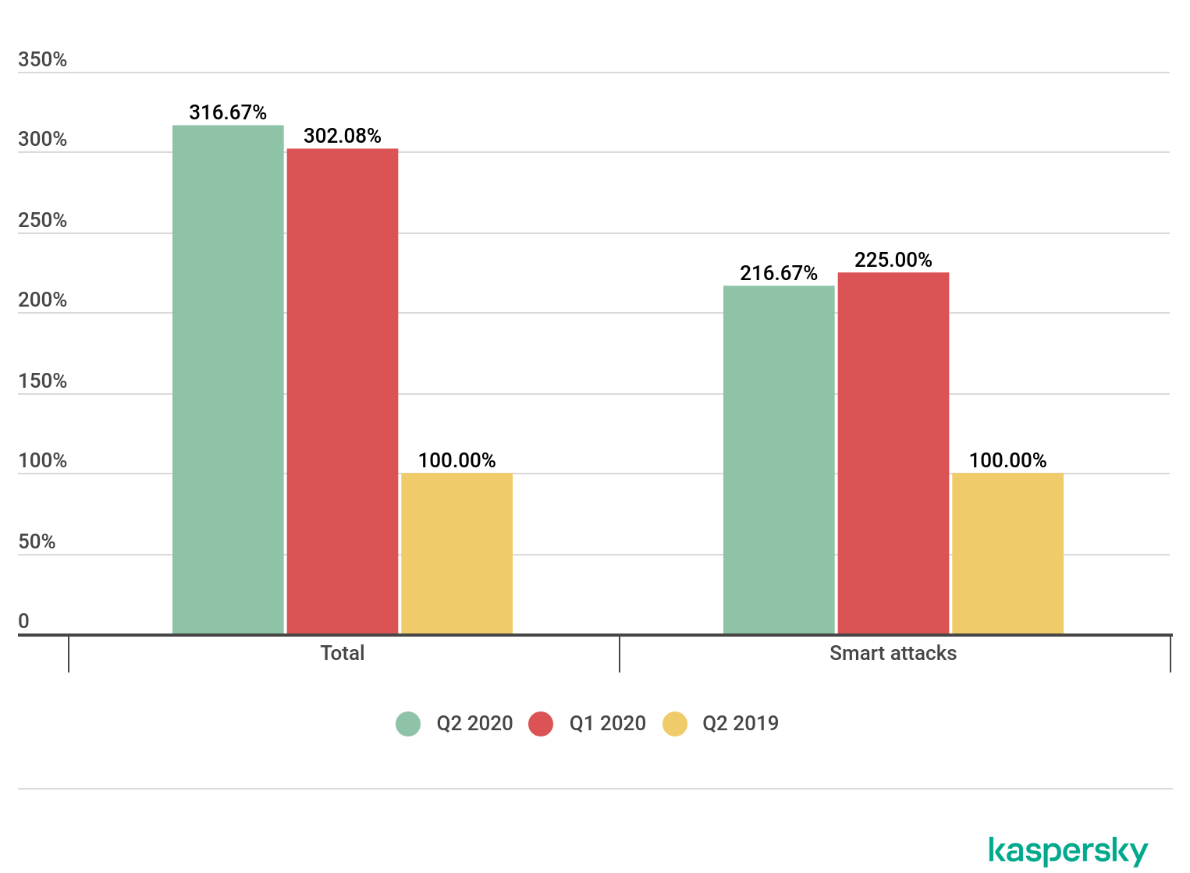
* **Estonia: 27/4/2007**
  + Điểm qua một chút về bối cảnh xã hội lúc bấy giờ ở Estonia. Khi đó đang có một sự phân chia chính trị về một nghĩa trang quân sự ở Estonia. Đối với cộng đồng người Estonia nói tiếng Nga, bức tượng đại diện cho sự giải phóng của Đức quốc xã. Mặt khác, những người dân tộc Estonian 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 – Chiếm 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 ti 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 chị bị offline trong vài phút.
  + Các kẻ tấn công đã giả mạo địa chỉ IP của GitHub, lấy được quyền truy cập vào memcache 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.

### Mục đích của tấn công DDoS và hiểm họa:

* Mục đích của tấn công DDoS:
  + **Tài chính:** Tấn công DDoS thường được kết hợp với tấn công ransomeware. 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 bực 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. Đều đó đồng nghĩa với việc các mối đe dọa đang ngày càng leo thang.

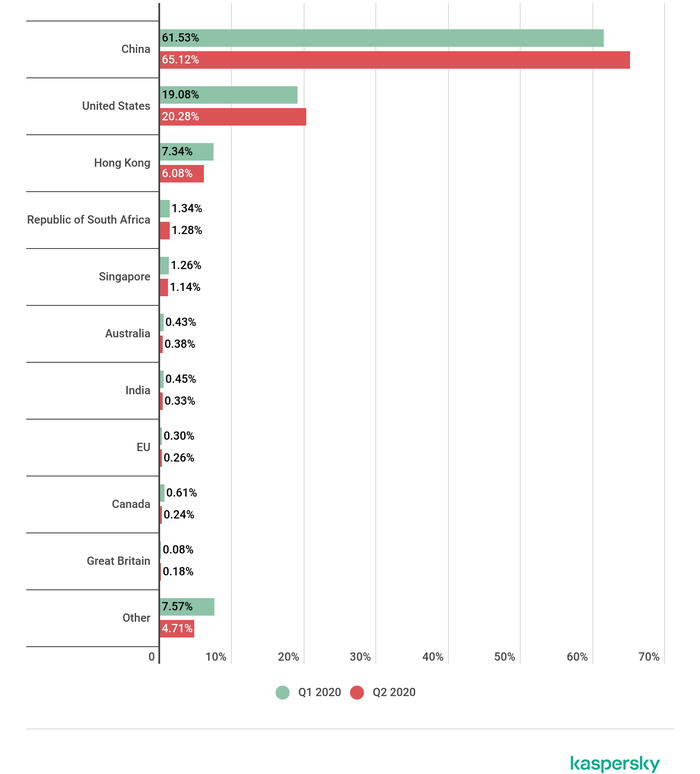
## Các số liệu tấn công DoS/DDoS:

* 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.



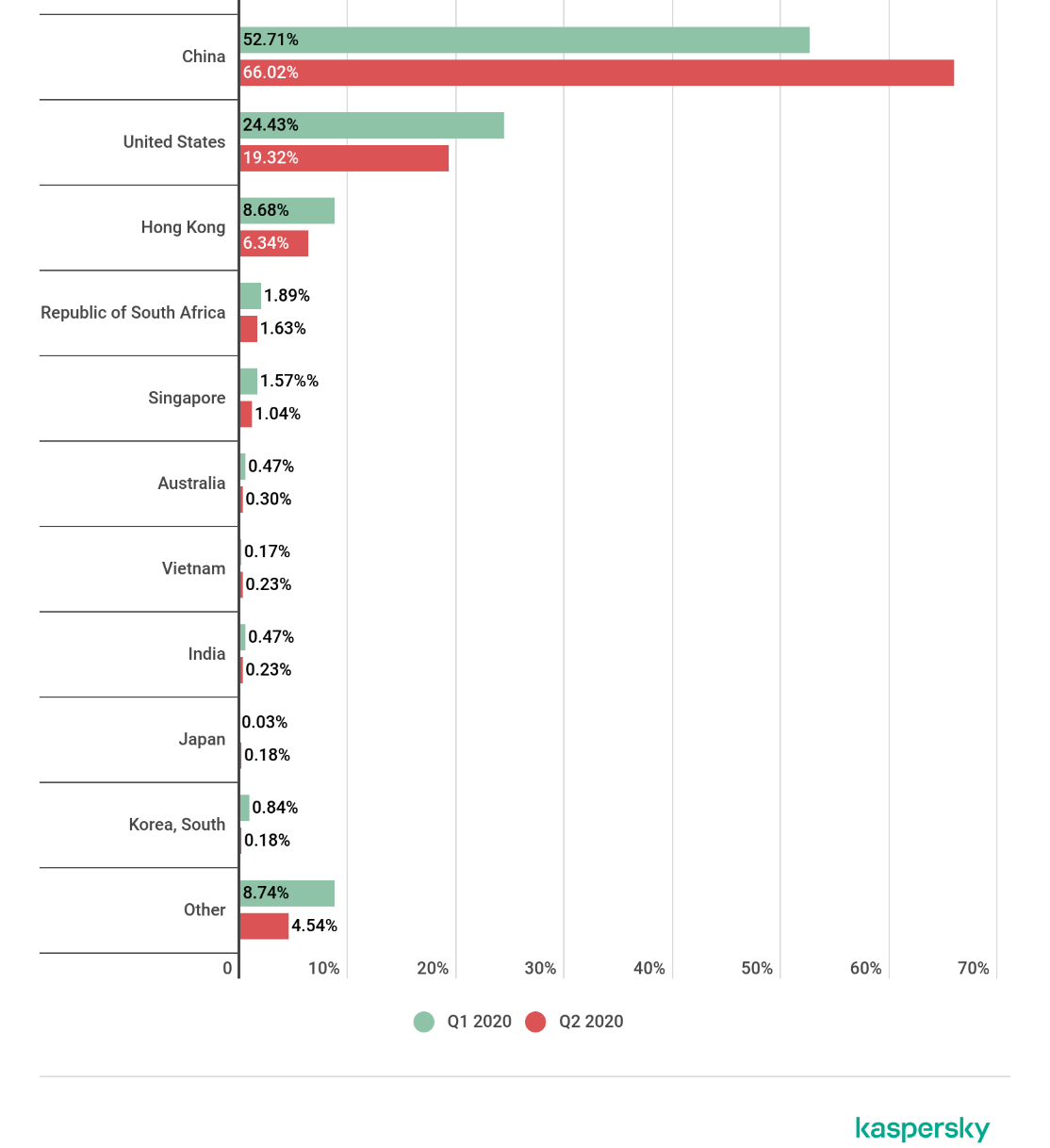
Hình: So sánh số lượng các cuộc tấn công DDoS, quý 1 và quý 2 năm 2020 và quý 2 năm 2019

* 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 lệ thường vì nhiều khu vực đã áp dụng biện phát 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 tôi 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, rơi khỏi top 10.



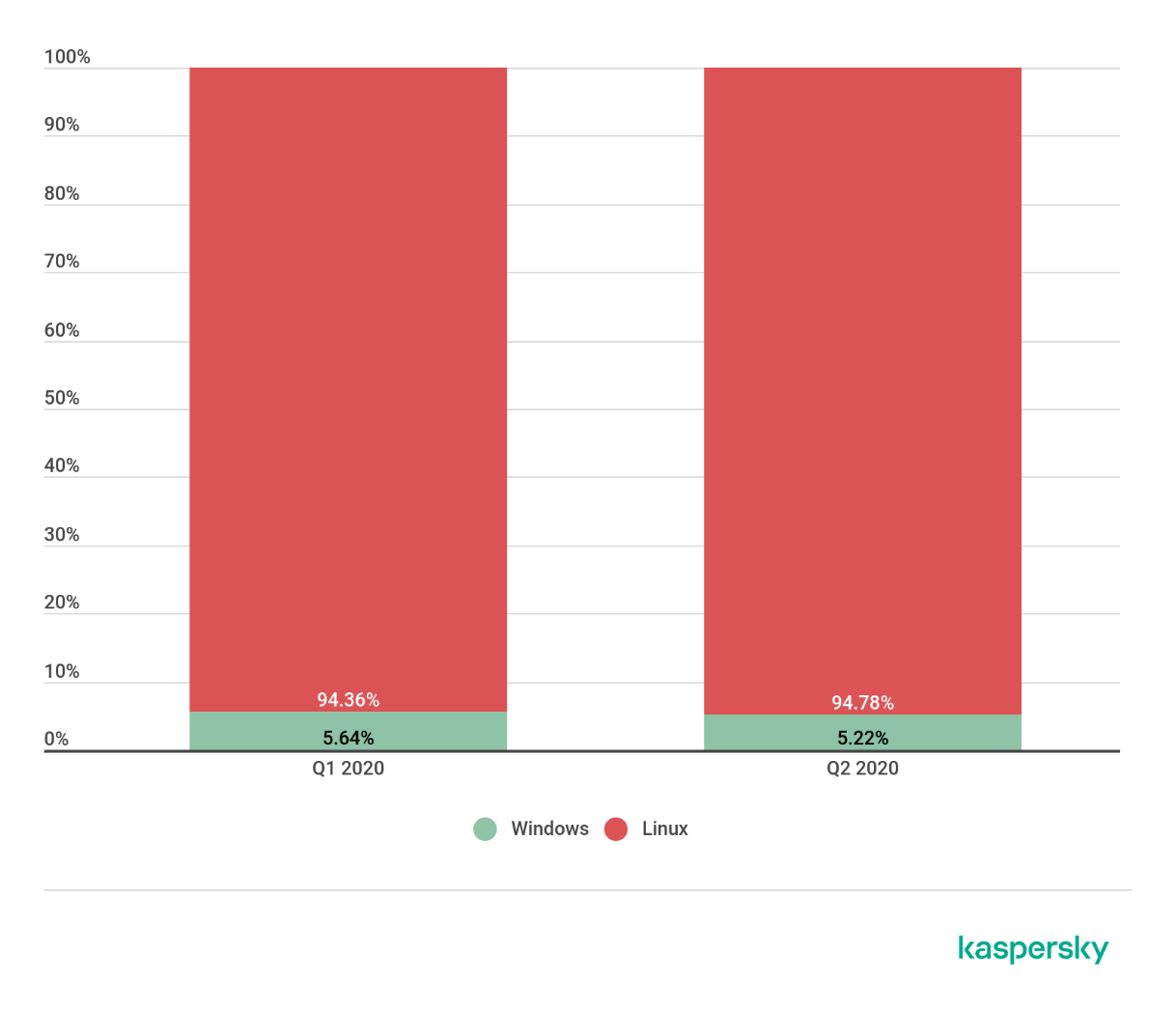
Hình: Phân bố các cuộc tấn công DDoS theo quốc gia trong quý 1 và quý 2/2020

* 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: Phân bố các mục tiêu tấn công DDoS riêng biệt theo địa lý trong quý 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: Tỷ lệ các cuộc tấn công botnet Windows và Linux, quý 1 và quý 2/2020

* 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.

## 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) |

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

## 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.

# CÁC HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ DDOS

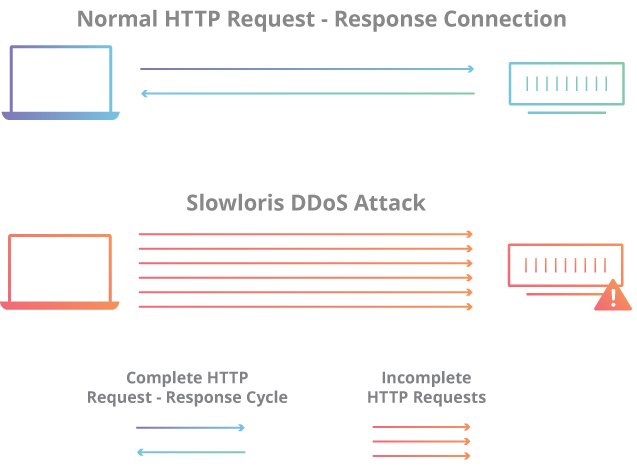
## Các loại tấn công DDOS cơ bản:

* Măc 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.

## Tấn công Slowloris:

### 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 chước 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

### Lịch sử xuất hiện:

* Amit Klein đã chỉ cho tôi 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.

### 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.

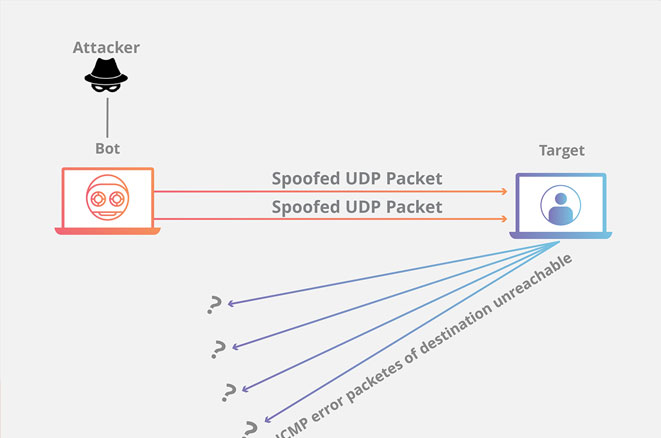
### Mức độ phá hoại:

* 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.

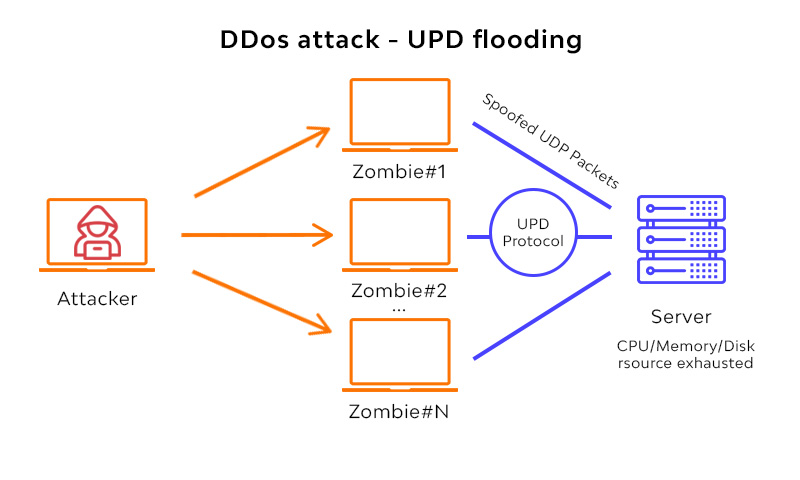
## Tấn công UDP Flood:

### 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](https://www.semtek.com.vn/khai-niem-khach-hang/#Khai_niem_khach_hang_la_gi) 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](https://www.semtek.com.vn/he-dieu-hanh-la-gi/) sẽ giảm nhẹ một phần của cuộc tấn công bằng cách hạn chế tốc độ phản ứng ICMP được gửi đi.



Hình



Hình

### Lịch sử xuất hiện:

* Ngày 8 tháng 2 năm1996, 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 "cơn 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.

### 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 đẫn đến mất khả năng sử lý các yêu cầu của khách hàng thông thường đẫn đến tình trạng từ chối dịch vụ.

### 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%.

## Tấn công SYN Flood:

### Khái niệm:

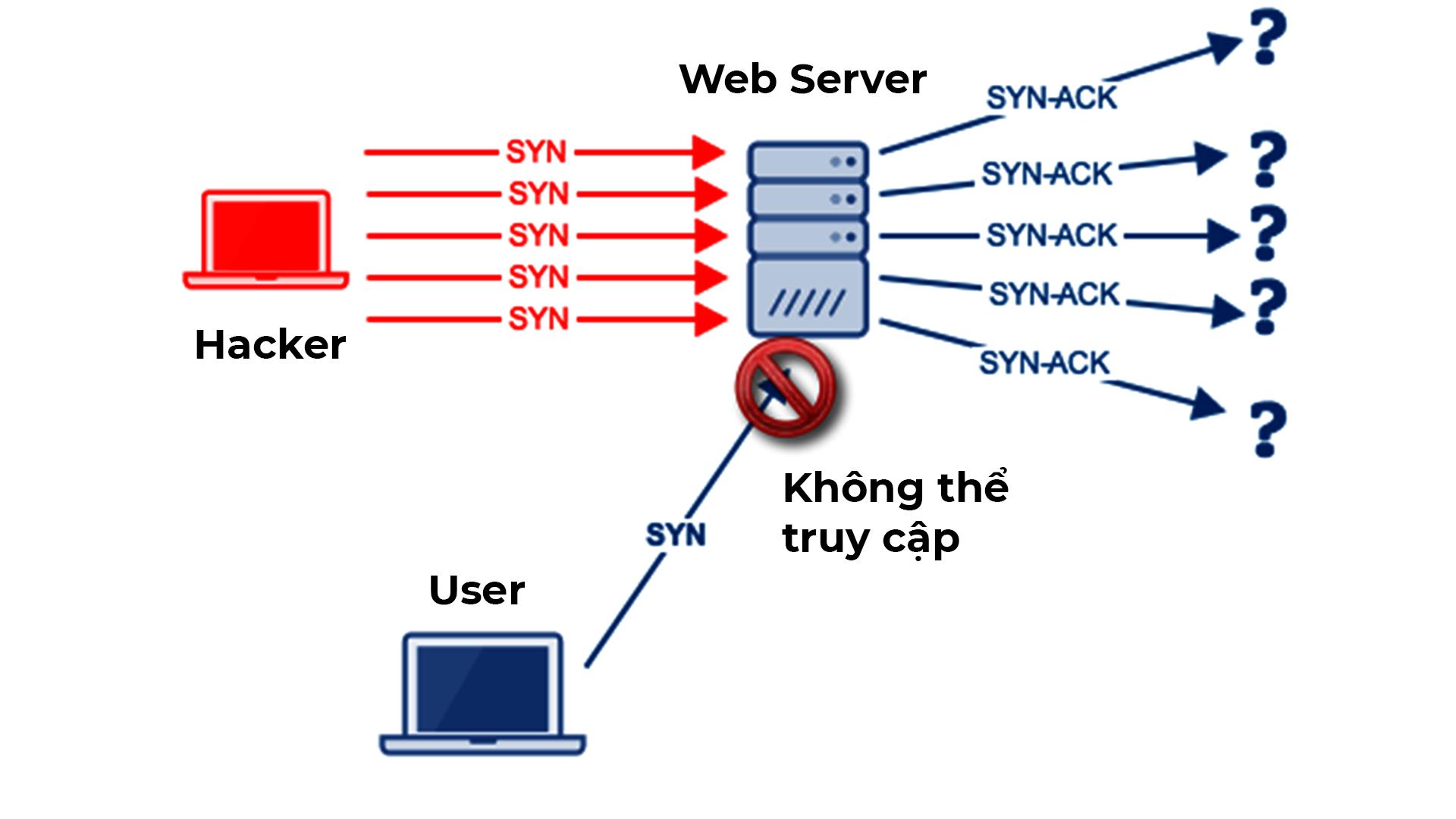
* SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (DDos), tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Bằng việc gửi liên tục gửi các packet tin yêu cầu kết nối ban đầu (SYN).
* Người tấn công có thể áp đảo tất cả các cổng có sẵn trên Server được chọn muc 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.

### 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: Đẩy 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.

### 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

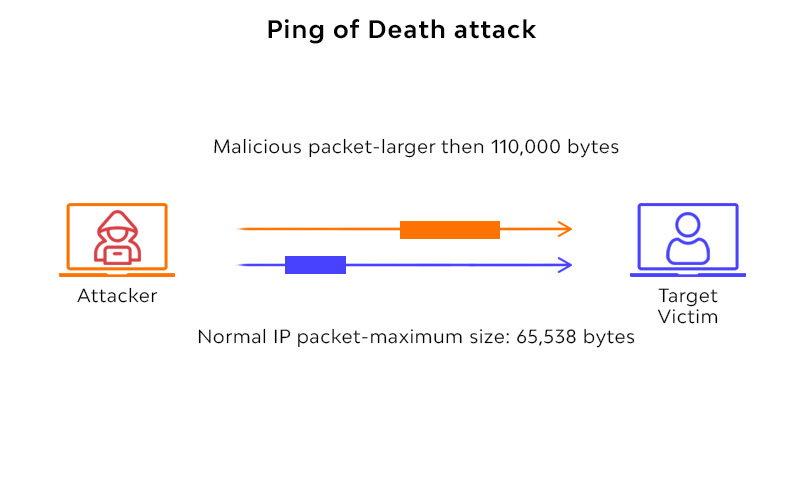
### Mức độ phá hoại:

* **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 dữ trữ thêm tài nguyễn 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 xuất 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 lien 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 SNY/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 môt yêu cầu hợp pháp và packet ACKcuối 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 găng giảm thiểu này mất một số thông tin về kết nối TCP, nhưng nó là tốt hơn so với bị Ddos tấn công.

## Tấn công ****Ping of Death****:

### 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.



Hình

### Lịch sử xuất hiện:

* Vào ngày 22/01/19997, 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.

### 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.

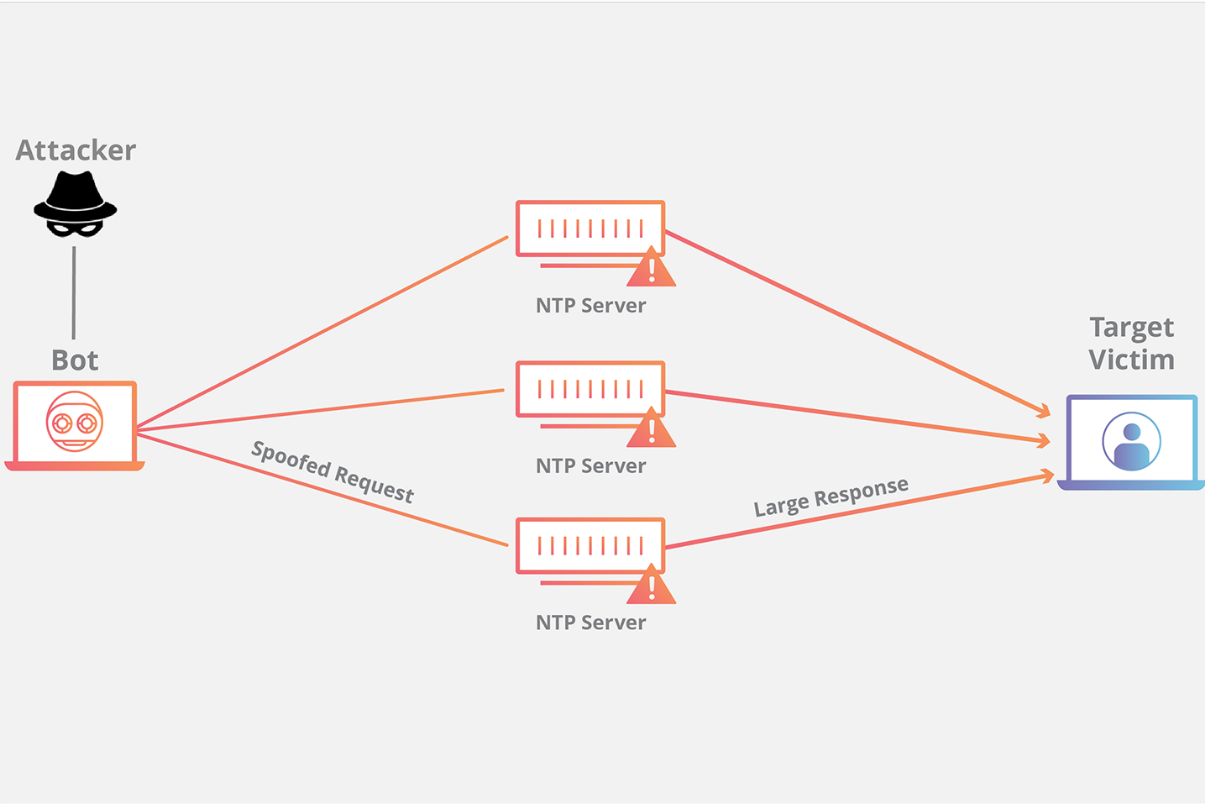
### Mức độ phá hoại:

* Máy tính sẽ bị ngưng họat động, Reboot hoặc bị crash khi nhận những gói tin lớn.

## Tấn công ****NTP Amplification****:

### 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

### 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 lỗ hổng, lỗ hổng này được ghi nhận có mã là CVE-2013-5211 hoặc VU#348126.

### 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.

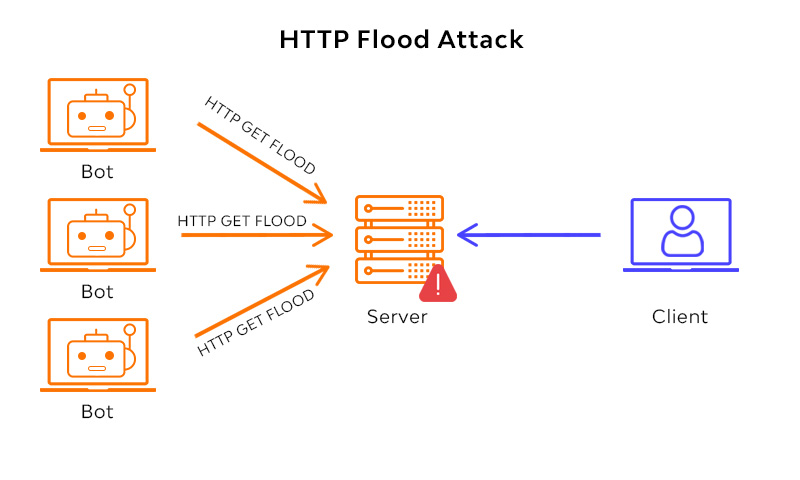
### Mức độ phá hoại:

* Khiến hệ thống mạng và webserver bị quá tải.

## Tấn công ****HTTP Flood****:

### 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

### 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).

### 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 nhằm 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.

### 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 băng 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.

## 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.

# CÀI ĐẶT PHƯƠNG THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ

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

### 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.

### 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 kì 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.

### 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 Ubun 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 nhac, xem phim, đồ họa đều rất hạn chế.
  + Ít phổ biến.
  + Khó khăn trong việc cài đặt, nâng cấp và quản lí các ứng dụng.

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

## Giả lập phía tấn công từ chối dịch vụ:

## Kết luận chương:

# GIẢI PHÁP NGĂN CHẶN TẤN CÔNG TỪ CHỐI DỊCH VỤ

## Giới thiệu hệ thống phòng thủ:

### Giới thiệu hệ thống phát hiện xâm nhập Snort:

## Cách thức hoạt động:

# KẾT LUẬN VÀ KIẾN NGHỊ

1. Kết quả đạt được

Trong quá trình nghiên cứu và hoàn thành đồ án tốt nghiệp với đề tài “” em đã đạt được các kết quả như sau:

**Về mặt kiến thức**

- Hiểu được cơ bản CRM là gì, hiện trạng thực tế mà các công ty bên ngoài thực tế đang xây dựng và sử dụng

- Hiểu được các bước để xây dựng một hệ thống CRM từ phân tích yêu cầu của khách hàng, cũng như xây dựng cơ sở dữ liệu cho các quy trình, triển khai bằng idempiere

- Có kiến thức về java nói chung cũng như cách sử dụng idempiere nói riêng.

**Về mặt ứng dụng.**

Từ những kết quả có được ở mặt kiến thức em đã xây dựng được các tài liệu để có thể xây dựng các tài liệu cần thiết để triển khai một hệ thống CRM. Từ những yêu cầu mà khách hàng đưa ra, đã xây dựng thành công các quy trình, các luồng xử lý trong các quy trình. Xây dựng được nền tảng cơ sở dữ liệu cho các quy trình để từ đó có thể dựa trên nền tảng dữ liệu triển khai hệ thống bằng idempiere.

Về mặt con người

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 tài quy trình, tài liệu, nhịn nhận và xử lý vấn đề, khả năng xây dựng tài liệu cũng như lập trình, rèn luyện tính kiên nhẫn và tăng khả năng trình bày văn bản,… đó là những kĩ năng vô cùng cần thiết giúp cho bản thân em có thêm hành trang cho tương lai làm việc phiá 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.

1. Tồn tại

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

- Các tài liệu về phân tích chức năng theo yêu cầu khách hàng chưa có cơ hội tương tác trao đổi với khách hàng, nên còn nhiều quy trình chưa đúng hoàn toàn với yêu thực mà khách hàng cần.

- Tài liệu cơ sở dữ liệu cho các quy trình còn nhiều thiếu sót

- Vì thời gian và kiến thức còn hạn chế nên việc triển khai các quy trình bằng idempiere chỉ mới ở mức độ tổng quát (master data), chưa triển khai được hết các quy trình, các chức năng luồng chức năng như tài liệu đã mô tả trước đó.

3. Hướng phát triển

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

- Khảo sát ý kiến khách hàng để xây dựng các quy trình luồng chức năng của các quy trình chính xác hơn, phù hợp với mong muốn của khách hàng

- Nghiên cứu nhiều hơn để xây dựng được tài liệu cơ sở dữ liệu phù hợp hơn cho tất cả các quy trình

- Triển khai tất cả các quy trình bằng idempiere, xử lý các chức năng , luồng đi của dữ liệu và luồng công việc chặt chẽ ràng buộc hơn.

Vì kiến thức còn nhiều hạn chế, thời gian tìm hiểu, nghiên cứ 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 đò án của em có thể hoàn thiện và phát triển hơn.

**PHỤ LỤC**

Phụ lục 1: hướng dẫn cài đặt

Phụ lục 2: hướng dẫn sử dụng

**TÀI LIỆU THAM KHẢO**

1. T.S Lê Phan Thị Diệu Thảo, Nguyễn Thảo Phương, *Nợ công và những vấn đề cần bàn thêm*, Nhà xuất bản Kinh Tế.
2. Boulding, K.E. (1995), *Economics analysis*, Hamish Hamilton, London.
3. <Http://dantri.com.vn/c76/s76-402058/nhung-moc-chinh-cua-khung-hoang-no-chau-au.htm>, “Những mốc chính của khủng hoảng nợ châu Âu”