ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA CÔNG NGHỆ THÔNG TIN

PBL4: DỰ ÁN HỆ ĐIỀU HÀNH & MẠNG MÁY TÍNH

Đề tài: Tìm hiểu về AWS Cloud, xây dựng một hạ tầng cơ bản để dựng một website và xây dựng cơ chế ngăn chặn các cuộc tấn công.

SINH VIÊN THỰC HIỆN:

Nguyễn Quốc Cường	**LỚP: 20TCLC_KHDL**	**NHÓM: 20.15B**
Lương Thiện	**LỚP: 20TCLC_KHDL**	**NHÓM: 20.15B**
Cao Kiều Văn Mạnh	**LỚP: 20TCLC_KHDL**	**NHÓM: 20.15B**

Giảng Viên Hướng Dẫn: ThS. Nguyễn Thế Xuân Ly

Đà Nẵng, tháng 12/2022

DANH SÁCH HÌNH VẼ

DANH SÁCH BẢNG BIỂU

BẢNG PHÂN CÔNG NHIỆM VỤ

Họ tên	**Nhiệm vụ**
Nguyễn Quốc Cường	- Thiết kế và cài đặt giao diện Web - Front end - Tấn công và phòng thủ XSS - Viết báo cáo và làm slide thuyết trình
Cao Kiều Văn Mạnh	- Thiết kế Web và giao diện - Back end, Front end - Cài đặt và cấu hình Server, Iptables và Snort - Tấn công và phòng thủ DDoS - Phân tích log truy cập và cảnh báo bằng snort
Lương Thiện	- Thiết kế và cài đặt giao diện Web - Back end, Front end - Tấn công và phòng thủ Path Traversal - Tấn công và phòng thủ SQL Injection

Bảng 1: Bảng phân công nhiệm vụ

DANH SÁCH CÁC TỪ VIẾT TẮT

AWS	Amazon Web Service
UFW	Uncomplicated Firewall
VPS	Virtual Private Server
Amazon VPC	Amazon Virtual Private Cloud
SMTP	Simple Mail Transfer Protocol
Network ACLs	Network Access Control List
Amazon EC2	Amazon Elastic Compute Cloud
XSS	Cross Site Scripting
ENI	AWS Elastic Network Interface
DDOS	Distributed Denial of Service

Bảng 2: Danh sách các từ viết tắt

MỞ ĐẦU

Xã hội chúng ta ngày càng phát triển, Internet và Công nghệ thông tin ngày nay đóng một vài trò rất quan trọng trong sự phát triển này cũng như là một phần không thể thiếu đối với từng cá nhân, doanh nghiệp, tổ chức.... Cùng với sự phát triển theo những chiều hướng tốt, các cuộc tấn công và xâm nhập mạng, phá hoại hạ tầng của các dịch vụ trên Internet cũng phát triển theo.

Với các sinh viên ngành Công nghệ Thông tin, cơ sở ngành mạng là một kiến thức chuyên ngành đặc biệt quan trọng. Có thể xem đây là một hướng đi rất rộng mở cho sinh viên. Việc nắm bắt những kỹ thuật cơ bản của chuyên ngành mạng cực kì cần thiết và quan trọng. Mạng máy tính và nguyên lý hệ điều hành là hai trong số rất nhiều những chuyên đề quan trọng, là cơ sở lý thuyết nền tảng của ngành Công nghệ Thông tin nói chung.

Nhằm áp dụng các kiến thức được học vào trong thực tiễn, nhóm chúng em đã thực hiện đề tài **"Tìm hiểu về AWS Cloud, xây dựng một hạ tầng cơ bản để dựng một website và xây dựng tường lửa chặn các cuộc tấn công"**. Báo cáo này là kết quả thực hiện đề tài của nhóm chúng em trong thời gian vừa qua. Mỗi phần trong báo cáo sẽ tiến hành phân tích và giải quyết các vấn đề trong đề tài được giao.

Trong quá trình thực hiện đồ án chắc chắn khó tránh khỏi các sai sót, chúng em rất mong sự góp ý của quý thầy, cô giáo trong Khoa để có thể chỉnh sửa và hoàn thiện hơn. Cuối cùng, chúng em xin gửi lời cảm ơn chân thành nhất đến các thầy, cô giáo trong Khoa, đặc biệt là thầy **Nguyễn Thế Xuân Ly,** đã tận tình hướng dẫn, tạo điều kiện cho chúng em hoàn thành đề tài này.

Chúng em xin chân thành cảm ơn!

Chương 1. CƠ SỞ LÝ THUYẾT

1.1. Giới thiệu đề tài

1.1.1. *Tổng quan đề tài*

- Tìm hiểu về hệ điều hành Linux và Amazon Web Service.
- Tìm hiểu và xây dựng tường lửa trên iptables, ufw.
- Tìm hiểu về các cách thức tấn công phổ biến (XSS, SQL Injection, path Traversal, DDoS).
- Thiết lập giao diện, triển khai cách tấn công và cách phòng thủ.
- Thiết kế hệ thống, môi trường cài đặt.
- Đánh giá kết quả.

1.1.2. *Mục tiêu thực hiện*

- Tìm hiểu được hệ điều hành Linux và xây dựng website trên hệ điều hành này.
- Tìm hiểu cơ chế vận hành, cấu hình, các chức năng của hạ tầng AWS Cloud.
- Xây dựng tường lửa, các quy tắc để chống các cuộc tấn công mạng phổ biến như: XSS, SQL Injection, path Traversal và DDoS.

1.2. Cơ sở lý thuyết

1.2.1. Hệ điều hành Linux

1.2.1.1 Giới thiệu

- Linux là một hệ điều hành mã nguồn mở. Được phát triển bởi Linus Torvalds từ năm 1991 dựa trên hệ điều hành Unix và bằng viết bằng ngôn ngữ C. Đến nay, Linux là một trong những nền tảng phổ biến nhất trên thế giới nhờ sự miễn phí và nhiều ưu điểm vượt trội của nó.
- Sự đa dạng của các bản phân phối chính là điều đã tạo nên tính linh hoạt của hệ điều hành Linux. Một số bản phân phối nổi bật thường gặp như: Ubuntu, Linux Mint, Debian, Centos, Arch Linux, Kali Linux, Fedora, ...

1.2.1.2 Ưu điểm của hệ điều hành Linux

- **Tính linh hoạt, hỗ trợ tốt cho lập trình viên – quản trị mạng**: Người dùng có thể chỉnh sửa hệ điều hành theo nhu cầu sử dụng của mình. Điều

này tạo ra môi trường phát triển lý tưởng cho các lập trình viên cũng như các nhà phát triển.

- **Hoạt động mượt trên các máy tính có cấu hình yếu**: Với Linux, khi nâng cấp lên phiên bản mới, các máy tính có cấu hình yếu vẫn sẽ được nâng cấp và hỗ trợ thường xuyên – tức chất lượng hoạt động vẫn trơn tru và ổn định.
- **Không tốn chi phí mua/bán bản quyền**: Với hệ điều hành này, bạn không cần phải bỏ phí mua bản quyền mà có thể sử dụng đầy đủ các tính năng. Bao gồm các ứng dụng văn phòng OpenOffice và LibreOffice, v.v...
- **Tính bảo mật cao**: tất cả những phần mềm độc hại như virus, mã độc… đều không thể hoạt động trên Linux. Do đó, độ bảo mật của hệ điều hành rất cao.

1.2.2. Iptables và UFW

1.2.2.1 Khái niệm

- **Iptables** là ứng dụng tường lửa miễn phí trong Linux, cho phép thiết lập các quy tắc riêng để kiểm soát truy cập, tăng tính bảo mật. Khi sử dụng máy chủ, Iptables là một trong những công cụ quan trọng giúp bạn ngăn chặn các truy cập không hợp lệ. Đối với các bản phân phối Linux như Ubuntu, Fedora, CentOS… ta có thể tìm thấy công cụ tường lửa tích hợp sẵn Iptables.

1.2.2.2 Thành phần

- Về cơ bản, Iptables chỉ là giao diện dòng lệnh để tương tác với packet filtering của netfilter framework. Cơ chế packet filtering của Iptables hoạt động gồm 3 thành phần là Tables, Chains và Targets.

1.2.2.3 Cấu hình cơ bản của iptables

- Tất cả các dữ liệu trong các gói tin gửi đi được định dạng qua Internet, Linux kernel sẽ lọc các gói tin này bằng cách mang đến một giao diện sử dụng một bảng các bộ lọc. Iptables là ứng dụng dòng lệnh và cũng đồng thời là tường lửa trên Linux cho phép người dùng thiết lập, duy trì và kiểm tra các bảng này.

- Người sử dụng có thể tùy ý thiết lập nhiều bảng với mỗi bảng chứa nhiều chuỗi, mỗi chuỗi là một quy tắc. Mỗi quy tắc sẽ định nghĩa việc phải làm với gói tin khi phù hợp với gói đó.
- Một target (mục tiêu) sẽ được đưa ra khi có một gói tin được xác định. Target có thể là một chuỗi khác để khớp với một trong các giá trị sau:
  - ACCEPT: gói tin được phép đi qua.
  - DROP: gói tin không được phép đi qua.
  - RETURN: bỏ qua chuỗi hiện tại và quay trở lại quy tắc tiếp theo từ chuỗi mà nó được gọi.

1.2.2.4 Cách thiết lập IPtables trên hệ điều hành Linux

- **Bước 1:** Cài đặt IPtables Linux Firewall
  - Cài đặt Iptables:

Hầu hết các phiên bản Linux hiện nay đều được tích hợp sẵn IPtables. Tuy nhiên, nếu chưa có sẵn trên Ubuntu có thể dùng lệnh sau để cài đặt:

```
sudo apt-get update
sudo apt-get install iptables
```

  - Xem trạng thái hiện tại của Iptables:

```
sudo iptables -L –v
```

Trong đó, -L dùng để liệt kê tất cả quy tắc (rule) và –v để liệt kê các danh sách bổ trợ. Chú ý đến ký tự viết hoa và viết thường được phân biệt với nhau.

- **Bước 2:** Định nghĩa các chain rules

Tức là thêm nó vào danh sách chain hiện tại, dưới đây là lệnh IPtables được định dạng với các tùy chọn thông thường.

```
sudo iptables -A -i <interface> -p <protocol (tcp/udp)> -s <source> --dport <port no.> -j <target>
```

Trong đó:

- A là thêm chain rules.
- i<interface> là giao diện mạng cần thực hiện lọc các gói tin.
- p<protocol> là giao thức mang thực hiện lọc (tcp/udp).
- dort<port no.> là cổng muốn đặt bộ lọc.

- **Bước 3:** Lưu giữ các thay đổi. Những IPtables rules được tạo ra đều được lưu trong bộ nhớ, khi reboot máy chủ cần phải tạo lại các rules này. Để lưu giữ các thay đổi vào hệ thống dùng lệnh:

```
sudo /sbin/iptables-save
```

- Để tắt firewall, dùng lệnh:

```
sudo iptables -F
sudo /sbin/iptables-save
```

1.2.2.5 UFW

- **UFW (Uncomplicated Firewall)** là một giao diện sử dụng thao tác với Iptables nhằm hướng tới việc đơn giản hoá quá trình cấu hình tường lửa. Vì Iptables là một công cụ vững chắc và linh hoạt nên người mới sử dụng sẽ thấy rất khó để thiết lập đúng cấu hình tường lửa. Nếu đang tìm kiếm công cụ nhằm nâng cao bảo mật mạng của mình thì UFW sẽ là sự lựa chọn tốt.
- **Bật UFW:** để bật ufw dùng lệnh sau: **sudo ufw enable**
- **Tắt UFW:** dùng lệnh: **sudo ufw disable**

1.2.3. Amazon Web Service (AWS)

1.2.3.1 Giới thiệu

- **Amazon web services** là một nền tảng điện toán đám mây được phát triển và được cung cấp bởi Amazon.com. Dịch vụ Web đôi khi được gọi là dịch vụ đám mây hoặc các dịch vụ điện toán từ xa. Các dịch vụ AWS đầu tiên đã được đưa ra vào năm 2006 để cung cấp các dịch vụ trực tuyến cho các trang web và các ứng dụng phía máy khách.

1.2.3.2 Cơ chế vận hành

- AWS được chia thành các dịch vụ khác nhau, mỗi loại có thể được cấu hình theo những cách khác nhau dựa trên nhu cầu của người dùng. Người dùng sẽ có thể xem các tùy chọn cấu hình và bản đồ máy chủ riêng lẻ cho một dịch vụ AWS.
- Hơn 100 dịch vụ bao gồm các Web Services của Amazon, bao gồm các dịch vụ dành cho máy tính, cơ sở dữ liệu, quản lý cơ sở hạ tầng, phát triển ứng dụng và bảo mật. Các dịch vụ này bao gồm:

- Tính toán
- Cơ sở dữ liệu lưu trữ
- Quản lý dữ liệu
- Kết nối mạng
- Quản lý dữ liệu lớn
- Trí tuệ nhân tạo (AI)
- v.v...

- Amazon Web Services cung cấp dịch vụ từ hàng chục trung tâm dữ liệu trải rộng trên các khu vực khả dụng (AZ) ở các khu vực trên thế giới. AZ là một vị trí chứa nhiều trung tâm dữ liệu vật lý. Một khu vực là một tập hợp các AZ ở gần nhau về mặt địa lý được kết nối bằng các liên kết mạng có độ trễ thấp.

1.2.3.3 Amazon VPC

- **Amazon Virtual Private Cloud (Amazon VPC)** là dịch vụ cho phép khởi chạy các tài nguyên AWS trong mạng ảo đơn theo logic được xác định. Bạn có toàn quyền kiểm soát môi trường mạng ảo của mình, bao gồm lựa chọn dải địa chỉ IP, tạo các mạng con, cấu hình các bảng định tuyến và cổng kết nối mạng. Bạn có thể dùng cả IPv4 và IPv6 cho hầu hết các tài nguyên trong đám mây riêng ảo, giúp bảo mật nghiêm ngặt và truy cập dễ dàng các tài nguyên cũng như ứng dụng.
- **Các thành phần của VPC:**
  - **IPv4 and IPv6 address blocks**: VPC IP address ranges được định nghĩa bằng Classless interdomain routing (CIDR) blocks. Bạn có thể thêm primary và secondary CIDR blocks vào VPC, nếu như secondary CIDR block có cùng address range với primary block.
  - **Subnet**: được hiểu là 1 sub network (mạng con ảo). Sau khi tạo 1 VPC, bạn có thể thêm một hoặc nhiều subnet (mạng con) trong mỗi Availability Zone. Khi bạn tạo 1 subnet, bạn cần chỉ định khối CIDR cho subnet đó. Mỗi subnet phải nằm hoàn toàn trong 1 Availability Zone và không thể kéo dài tới các zone khác. Các Availability Zone là các vị trí riêng biệt được thiết kế để cách ly để tránh bị ảnh hưởng khi các zone khác gặp vấn đề. Có 2 loại subnet:

- **Public Subnet**: là 1 subnet được định tuyến tới một internet gateway. Một instance trong public subnet có thể giao tiếp với internet thông qua địa chỉ IPv4 (public IPv4 address hoặc Elastic IP address).
- **Private Subnet**: Ngược với Public Subnet, Private Subnet là một subnet không được định tuyến tới một internet gateway. Bạn không thể truy cập vào các instance trên một Private Subnet từ internet.

- **Route tables** là bảng định tuyến, bao gồm một tập hợp các rule (được gọi là route), được sử dụng để xác định đường đi, nơi đến của các gói tin từ mạng con hay gateway.
- **Internet connectivity:**
  - **Internet Gateway**: là một thành phần cho phép giao tiếp giữa VPC và Internet. Nói một cách dễ hiểu hơn là một server trong VPC muốn giao tiếp được với Internet thì cần có Internet Gateway.
  - **NAT Gateway**: là một thành phần cho phép server ảo trong mạng private có thể kết nối tới Internet hoặc dịch vụ khác của AWS nhưng lại ngăn không cho Internet kết nối đến server đó.
  - **NAT Instance**: là một server ảo được chúng ta tạo ra và quản lý có chức năng tương tự như NAT Gateway. Bạn có thể tham khảo sự khác nhau giữa NAT Gateway và NAT Instance được mô tả chi tiết tại đây
- **Elastic IP addresses** là một địa chỉ public IPv4, có thể kết nối được từ Internet được sử dụng cho:
  - EC2 instance
  - AWS elastic network interface (ENI)
  - Một số service khác cần public IP address
- **Network/subnet security**: AWS cung cấp hai tính năng mà bạn có thể sử dụng để tăng cường bảo mật trong VPC của bạn: Security Group và Network ACLs.
  - Security Group kiểm soát lưu lượng vào và ra cho các instance
  - Network ACL giúp kiểm soát lưu lượng truy cập vào và ra cho subnet.

- Một số networking services khác như: Virtual Private Networks (VPNs), Direct connectivity between VPCs (VPC peering), Gateways, Mirror sessions

1.2.3.4 Security Group

- **Security Group** là một tường lửa ảo (Virtual Firewall) để điều khiển truy cập giữa các EC Instance. Khi khởi tạo 1 instance, bạn cần chỉ ra 1 hoặc nhiều security group. Và sau khi tạo 1 instance bạn có thể thay đổi Security Group đó.
- Bạn có thể thêm và xóa nhiều luật ở bất cứ thời điểm. Thay đổi sẽ tự động được áp dụng vào các instances mà đã được gắn với Security Group đó.
- **Security Group Rules**
  - Mặc định Security Group cho phép mọi truy cập ra ngoài.
  - Security Group là thường phải cho phép truy cập. Bạn không thể tạo rule với chỉ quyền từ chối truy cập.
  - Security Groups là stateful firewall. Nghĩa là nếu bạn gửi 1 truy vấn từ instance của bạn. Một phản hồi của truy vấn đó sẽ được cho phép lưu chuyển trở lại mà không phụ thuộc vào bất kỳ luật nào của Security Groups (Inbound)
  - Chúng ta có thể thêm và xóa nhiều luật ở bất cứ thời điểm. Thay đổi sẽ tự động được áp dụng vào các instances mà đã được gắn với Security Group đó.
  - Khi bạn gán nhiều security group tới một 1 instance, Các luật từ mỗi security group sẽ được tổng hợp để ra 1 tập hợp các luật phù hợp. AWS sẽ dựa vào đó để xác định là có được phép truy cập không.
- **Default Security Groups**: Mặc định tài khoản AWS của bạn có 1 security group mặc định cho VPC mặc định của mỗi một region (vùng). Nếu bạn không chỉ ra 1 security group khi tạo instance, thì instance của bạn sẽ được gắn với security group mặc định của VPC
- Một security group mặc định có tên là <default-ID> được gán tự động bởi AWS. Một số luật của security group mặc định:
  - Cho phép truy cập giữa các instance cùng được gán vào 1 security group mặc định.
  - Cho phép lưu lượng truy cập từ instance đi ra bên ngoài.
  - Bạn có thể thêm hoặc xóa luật cho bất kỳ security group mặc định nào.

1.2.3.5 Network ACLs

- **Network ACLs (Network Access Control List)** là một layer tùy chọn cho bảo mật VPC của bạn, hoạt động giống như firewall để điều khiển lưu lượng truy cập ra vào giữa 1 hoặc nhiều subnets. Bạn thiết lập các rule cho Network ACLS giống như cách làm với Security Group để tạo thêm 1 lớp bảo mật bổ sung cho VPC.
- Rule mặc định của Network ACLs cho phép lưu lượng mạng vào (outbound) và ra (inbound) đối với địa chỉ IPv4 và cả IPv6.
- Có thể tạo một Network ACL riêng và gán nó tới một subnet. Nhưng mặc định, mỗi 1 Network ACL tạo ra sẽ từ chối tất cả Inbound và Outbound traffic cho đến khi bạn thêm Rule
- Một số nét cơ bản về Network ACLs:
    - Rule mặc định của Network ACLs cho phép lưu lượng mạng vào (outbound) và ra (inbound) đối với địa chỉ IPv4 và cả IPv6
    - Bạn có thể tạo một Network ACL riêng và gán nó tới một subnet. Nhưng mặc định, mỗi 1 Network ACL tạo ra sẽ từ chối tất cả Inbound và Outbound traffic cho đến khi bạn thêm Rule
    - Mỗi subnet phải được gán với 1 network ACLs. Nếu bạn không chỉ ra 1 Network ACL, thì subnet sẽ tự động được liên kết với 1 network ACL mặc định.
    - Network ACL có thế gán tới nhiều subnet, tuy nhiên 1 subnet chỉ có thể được gán bởi 1 Network ACL ở 1 thời điểm. Khi bạn gán với 1 Network ACL mới, những cái cũ sẽ bị gỡ bỏ.
    - Một network ACL chứa 1 danh sách các quy tắc được đánh số. Bắt đầu bởi rule có số nhỏ nhất, để xác định lưu lượng mạng đươc cho phép ra vào. Số lớn nhất mà bạn có thể sử dụng cho 1 rule là 32766
    - Một network ACL phân chia Rule thành inbound và outbound rule, và mỗi rule thì có thể cho phép hoặc từ chối truy cập
    - Network ACLs là không có trạng thái;
    - Security groups: Hoạt động giống như một tường lửa cho EC2 Instances, điều khiển lưu lượng truy cập ra vào mạng ở mức EC2 instance. Các bạn vui lòng đọc bài viết Tìm hiểu về Security Group để biết thêm chi tiết.
    - Network access control lists (ACLs) – Hoạt động giống như một tường lửa cho subnet, điều khiển lưu lượng truy cập ra vào mạng ở mức subnet.

1.2.3.6 Bảng so sánh giữa Network ACLs và Security Group

Security Group	Network ACL
Quản lý lưu lượng vào ra ở mức Instance	Quản lý lưu lượng vào ra ở mức Subnet
Chỉ hỗ trợ Allow Rule (Cho phép)	Hỗ trợ cả Allow Rule (Cho phép) và Deny Rule (Từ chối)
Là một tường lửa có trạng thái: Lưu lượng phản hồi là được phép, mà không ảnh hưởng bởi bất kỳ 1 luật nào.	Là một tường lửa không trạng thái: Lưu lượng phản hồi phải được cho phép bởi luật.
AWS đánh giá tất cả các rule trước khi quyết định có cho phép lưu lượng truy cập	AWS xử lý các rule theo thứ tự số khi quyết định có cho phép lưu lượng truy cập
Chỉ áp dụng cho 1 instance nếu ai đó chỉ định security group khi khởi chạy	Tự động áp dụng cho tất cả các instance trong subnet được liên kết với (do đó, bạn không phải

Bảng 3: So sánh Network ACLs và Security Group

1.2.3.7 APPLICATION LOAD BALANCER

- **Application Load Balancer** là một tính năng của Elastic Load Balancing cho phép nhà phát triển định cấu hình và định tuyến lưu lượng truy cập của người dùng cuối đến các ứng dụng dựa trên đám mây công cộng AWS.

- Trong môi trường đám mây có nhiều dịch vụ web, load balancer là điều cần thiết. Bằng cách phân phối lưu lượng mạng và luồng thông tin trên nhiều máy chủ, bộ load balancer đảm bảo không có máy chủ đơn lẻ nào chịu quá nhiều nhu cầu. Điều này cải thiện khả năng đáp ứng và tính khả

dụng của ứng dụng, nâng cao trải nghiệm người dùng và có thể bảo vệ khỏi các cuộc tấn công từ chối dịch vụ (DDoS) phân tán.

1.2.3.8 Amazon EC2 Instance

1.2.3.8.1 *Khái niệm*

- **Amazon Elastic Compute Cloud (Amazon EC2)** là một cơ sở hạ tầng điện toán đám mây được cung cấp bởi **Amazon Web Services (AWS)** giúp cung cấp tài nguyên máy tính ảo theo yêu cầu.
- **Amazon EC2** cung cấp các ứng dụng máy tính ảo có thể mở rộng về khả năng xử lý cùng các thành phần phần cứng ảo như bộ nhớ máy tính (ram), vi xử lý, linh hoạt trong việc lựa chọn các phân vùng lưu trữ dữ liệu ở các nền tảng khác nhau và sự an toàn trong quản lý dịch vụ bởi kiến trúc ảo hoá đám mây mạnh mẽ của AWS.
- **Amazon EC2** sẽ cung cấp một hoặc nhiều máy chủ ảo có thể kết hợp với nhau để dễ dàng triển khai ứng dụng nhanh nhất và đảm bảo tính sẵn sàng cao nhất. Thậm chí về mặt thanh toán bạn dễ dàng biết được các mức chi phí cần thanh toán dựa trên thông tin tài nguyên bạn sử dụng.

1.2.3.8.2 *Các đặc tính*

- **Scaling**
  - Scaling Up/Down: Tăng/Giảm capacity(RAM, CPU,...) của Instance.
  - Scaling In/Out: Tăng/Giảm số lượng Instance.
- **Security**
  - Có thể thiết lập rank IP Private dành riêng cho EC2.
  - Sử dụng Security Group và Network ACLS để control inbound/outbound.
  - Có thể thiết lập IPsec VPN giữa Data Center và AWS Clound.
  - Delicated Instance -> Tạo EC2 trên 1 hardware physical dành riêng cho 1 khách hàng duy nhất.

1.2.4. Các cuộc tấn công thường gặp

1.2.4.1 Cross Site Scripting(XSS)

1.2.4.1.1 *Khái niệm*

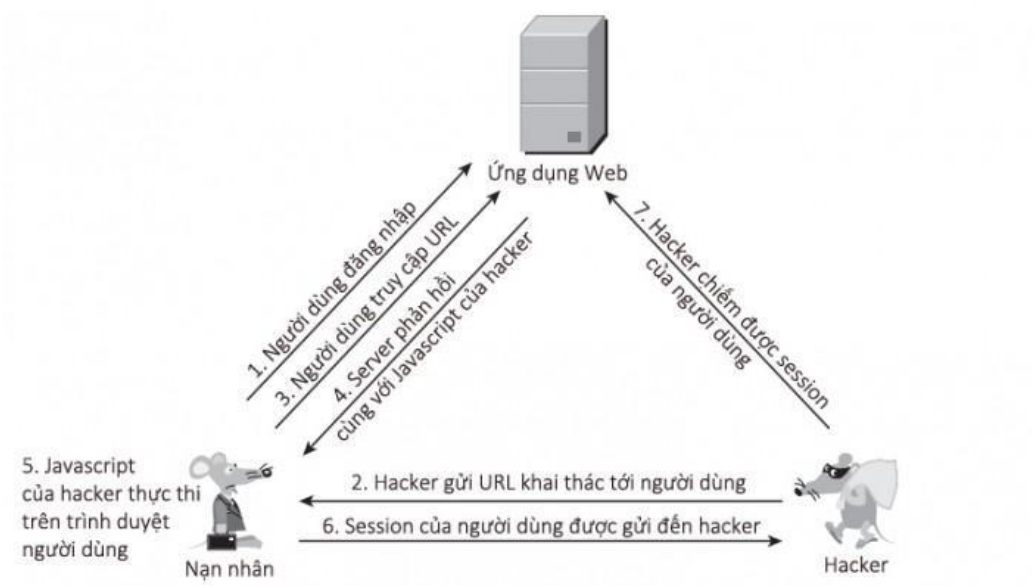
- **Cross Site Scripting (XSS)** là một trong những tấn công phổ biến và dễ bị tấn công nhất mà tất cả các Tester có kinh nghiệm đều biết đến. Nó được coi là một trong những tấn công nguy hiểm nhất đối với các ứng dụng web và có thể mang lại những hậu quả nghiêm trọng. Tấn công XSS là một đoạn mã độc, để khai thác một lỗ hổng XSS, tin tặc sẽ chèn mã độc thông qua các đoạn script để thực thi chúng ở phía Client. Thông thường, các cuộc tấn công XSS được sử dụng để vượt qua truy cập và mạo danh người dùng.

1.2.4.1.2 *Mục đích tấn công*

- Mục đích chính của cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác.
- Trong hầu hết các trường hợp, cuộc tấn công này đang được sử dụng để ăn cắp cookie của người khác. Như chúng ta biết, cookie giúp chúng ta đăng nhập tự động. Do đó với cookie bị đánh cắp, chúng ta có thể đăng nhập bằng các thông tin nhận dạng khác. Và đây là một trong những lý do, tại sao cuộc tấn công này được coi là một trong những cuộc tấn công nguy hiểm nhất, Tấn công XSS đang được thực hiện ở phía client. Nó có thể được thực hiện với các ngôn ngữ lập trình phía client khác nhau. Tuy nhiên, thường xuyên nhất cuộc tấn công này được thực hiện với Javascript và HTML.

1.2.4.1.3 *Các phương thức tấn công*

- **Reflected XSS:** Cách tấn công này chỉ thực thi được ở phía Client mà không lưu vào cơ sở dữ liệu của Website.Nếu muốn khai thác lỗi này, hacker cần tìm lỗ hổng nằm trong ứng dụng web, sau đó tra lien kết trỏ đến trang web chứa lỗ hổng. Một khi người dùng truy cập lien kết,máy chủ sẽ trả về trang web kèm mã độc của hackẻ đã kèm vào nằm trong liên kết.



Hình ảnh 1 :Hình ảnh tấn công XSS

- **Stored XSS**: Khác với Reflected tấn công trực tiếp vào một số nạn nhân mà hacker nhắm đến, Stored XSS hướng đến nhiều nạn nhân hơn. Lỗi này xảy ra khi ứng dụng web không kiểm tra kỹ các dữ liệu đầu vào trước khi lưu vào cơ sở dữ liệu (ở đây tôi dùng khái niệm này để chỉ database, file hay những khu vực khác nhằm lưu trữ dữ liệu của ứng dụng web). Ví dụ như các form góp ý, các comment trên các trang web.
- **DOM Based XSS**: DOM Based XSS là kỹ thuật khai thác XSS dựa trên việc thay đổi cấu trúc DOM của tài liệu, cụ thể là HTML. Chúng ta cùng xem xét một ví dụ cụ thể sau.

1.2.4.2 SQL INJECTION

1.2.4.2.1 *Khái Niệm*

- **SQL Injection** được coi là một loại kỹ thuật khai thác trái phép dữ liệu từ database thông qua việc lợi dụng các lỗ hổng về câu truy vấn.
- Cách thực hiện thông thường sẽ là thêm 1 đoạn SQL vào câu lệnh cũ để làm sai, lỗi truy vấn ban đầu. Những kẻ tấn công có thể xâm nhập và thực hiện các tác vụ tương tự vai trò quản trị web, đồng thời lấy đi các dữ liệu quan trọng.

1.2.4.2.2 *Phân Loại*

- **In-band SQLi**: Đây là một trong những phương thức tấn công phổ biến nhất hiện nay do dễ thực hiện và khá hiệu quả. Những kẻ xâm nhập thường dùng 1 kênh liên lạc để khởi động và truy cập vào dữ liệu bằng 2 hình thức:
    - **Error-based SQLi**: Kẻ xâm nhập sẽ tạo ra các tác động lớn tới cơ sở dữ liệu, kích thích tạo ra thông báo lỗi và lợi dụng để khai thác thông tin.
    - **Union-based SQLi**: Lợi dụng toán tử UNION SQL, hacker sử dụng phối hợp nhiều câu lệnh để nhận HTTP response, thông tin được chứa trong đó và có thể khai thác dễ dàng.
- **Inferential (Blind) SQLi**: Đây là phương thức xâm nhập có tác động chậm hơn nhưng hiệu quả vô cùng tốt. Hacker thường thực hiện bằng cách gửi data payload đến máy chủ và dựa vào đó tính toán cơ chế, cấu trúc của server. Nhờ vậy dễ dàng tìm ra phương thức xâm nhập phù hợp.
- **Out-of-band SQLi**: Khi server không ổn định hoặc quá chậm, hacker sẽ thực hiện hình thức này để tận dụng các nguồn kích hoạt không đồng bộ. Xâm nhập bằng cách nhằm tạo ra DNS hoặc HTTP request kích hoạt server tự động chuyển dữ liệu và hacker có thể tận dụng để lấy cắp thông tin ở khâu này.

1.2.4.2.3 *Hậu quả*

- Hậu quả lớn nhất mà SQL Injection gây ra là: Làm lộ dữ liệu trong database. Tuỳ vào tầm quan trọng của dữ liệu mà hậu quả dao động ở mức nhẹ cho đến vô cùng nghiêm trọng.
- Lộ dữ liệu khách hàng có thể ảnh hưởng rất nghiêm trọng đến công ty. Hình ảnh công ty có thể bị ảnh hưởng, khách hàng chuyển qua sử dụng dịch vụ khác, dẫn đến phá sản v…v...
- Lỗ hỗng này cũng ảnh hưởng lớn đến khách hàng. Do họ thường dùng chung một mật khẩu cho nhiều tài khoản, chỉ cần lộ mật khẩu một tài khoản thì các tài khoản khác cũng sẽ có nguy cơ bị ảnh hưởng theo. Bên cạnh đó, tin tặc có thể sử dụng các thông tin cá nhân của khách hàng mà chúng đã khai thác được cho các việc bất hợp pháp.

- SQL Injection cho phép kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh, ... các dữ liệu có trên cơ sở dữ liệu. Từ đó tin tặc có thể xóa toàn bộ dữ liệu và làm cho hệ thống ngừng hoạt động hoàn toàn.

1.2.4.3 Path Traversal

1.2.4.3.1 *Khái niệm*

- Path traversal hay còn gọi là Directory traversal là một lỗ hổng bảo mật cho phép kẻ tấn công đọc các file tùy ý trên server. Nó dẫn đến việc bị lộ thông tin nhạy cảm của ứng dụng web như thông tin đăng nhập, một số file hoặc thư mục hệ điều hành.

1.2.4.3.2 *Path Traversal có thể xuất hiện ở đâu?*

- Tương tự như OS Command Injection thì Path Traversal có thể xuất hiện ở bất kì đâu nếu không thực hiện các biện pháp như lọc các kí tự mà người dùng nhập vào và ràng buộc hoặc phân quyền rõ ràng cho file và folder được phép truy cập.

1.2.4.3.3 *Nguyên nhân gây ra Path Traversal*

- Do lập trình viên chủ quan, không phân quyền thư mục rõ ràng và không lọc ra kí tự mà người dùng nhập vào có an toàn hay không. Từ đó kẻ tấn công có thể lợi dụng mà truy cập vào bằng các dấu phân cách thư mục mà truy cập và chỉnh sửa các file có trên hệ thống.

1.2.4.4 Distributed Denial of Service (DDoS)

1.2.4.4.1 *Khái niệm*

- **Distributed Denial of Service (DDoS)** là tên gọi khác của tấn công từ chối dịch vụ. Bạn có thể hiểu đơn giản là cuộc tấn công được gây nên bằng việc tạo ra một lượng truy cập ảo ồ ạt vào môt địa chỉ website tại cùng một thời điểm. Điều này nhằm tấn công vào máy chủ lưu trữ khiến hệ thống chạy chậm hoặc không thể chạy được nữa.

1.2.4.4.2 *Cách nhận biết cuộc tấn công*

- Thông thường các server của website đang gặp phải một cuộc tấn công DDoS sẽ có những dấu hiệu như khi mặc dù mạng Internet đang ổn định và truy cập các website khác vẫn diễn ra bình thường nhưng mạng của bạn

hoặc mạng của hệ thống bị chậm một cách bất thường bị truy cập vào website đó.

- Bạn có thể kiểm tra xem email của bản thân có đang phải nhận được nhiều thư rác hay không. Việc không thể truy cập vào một mục của website hay không thể truy cập vào nhiều website cũng là dấu hiệu của một cuộc tấn công DDoS.

1.2.4.4.3 *Các dạng tấn công từ chối dịch vụ DDoS*

Có thể chia tấn công DDoS thành hai loại lớn: Gây nghẽn băng thông và gây cạn tài nguyên. Một số dạng tấn công thường gặp như sau:

- **Gây nghẽn mạng (UDP flood và ping flood)**: gây quá tải hệ thống mạng bằng lượng truy cập lớn từ nhiều nguồn để chặn các lượt truy cập thực của người dùng bằng các gói UDP và ICMP
- **Tấn công chuyển hướng**: gây tốn tài nguyên bằng cách giả mạo IP nguồn để các máy chủ mục tiêu phản hồi về máy chủ nạn nhân, từ đó tạo ra các cuộc tấn công với quy mô lớn, đặc biệt là các hệ thống có khả năng khuếch đại. Được thực hiện bằng cách gửi IP mạo danh đến nhiều máy tính để nhận lại lượng phản hồi về địa chỉ đích giả mạo được định sẵn. Khi đó nạn nhân cũng sẽ không biết được nguồn thực sự tấn công mình.
- **Tấn công SYN flood (TCP):** gây cạn tài nguyên máy chủ và chặn việc nhận các yêu cầu kết nối mới bằng cách lợi dụng quá trình "bắt tay" 3 bước TCP: Gửi đi yêu cầu SYN đến máy chủ và được phản hồi bằng một gói SYN-ACK, tuy nhiên không gửi lại gói ACK khiến cho tài nguyên máy chủ bị sử dụng hết vào việc đợi gói ACK gửi về.
- **Tấn công HTTP flood (Web Spidering):** gây cạn tài nguyên máy chủ bằng cách dùng bộ quét web spider để quét các website.

1.2.5. Phương pháp ngăn chặn các cuộc tấn công

1.2.5.1 Phương pháp ngăn chặn XSS

Cuộc tấn công XSS gồm 3 cách tấn công như sau: Reflected XSS, Stored XSS, DOM Based XSS.

- Đối với **Reflected XSS và DOM Based XSS**, chúng ta vô hiệu hoá các thẻ thuộc tính html trong dữ liệu đầu vào được truyền đi qua hai phương pháp post và get, hoặc kiểm tra có xuất hiện các thẻ thuộc tính html, đặc biệt là các thẻ chứa ngôn ngữ lập trình như “<script>”, “<php”,… Nếu có, không cho phép thực hiện các chức năng và đồng thời in ra thông báo.
- Đối với **Stored XSS**, chúng ta mã hoá dữ liệu đầu vào thành dãy mã ASCII, để làm vô hiệu hoá các mã độc tấn công XSS trước khi lưu dữ liệu vào database. Ngoài ra, đối với các dữ liệu truyền đi, là thông số để hệ thống thực thi một chức năng nào đó, có thể kiểm tra dữ liệu đầu vào tương tự với Reflected XSS và DOM Based XSS.
- Không hiển thị lại trực tiếp những thông tin đầu vào được truyền đi thông qua phương thức get và post, nếu có thì phải kiểm tra trước để xem có thẻ html không. Nếu bắt buộc phải in ra dù cho đó là thẻ html, cần mã hoá trước khi hiển thị.

1.2.5.2 Phương pháp ngăn chặn Path Traversal

Người dùng được phép xem các nội dung tệp tin được lưu trữ trên máy chủ thông qua trình duyệt. Tuy nhiên, bằng cách chỉnh sửa nội dụng trên url, người dùng có thể xem những nội dung tệp tin của đáng lẽ không được phép truy cập từ máy khách. Ta có các cách ngăn chặn sau:

- Khi nhận dữ liệu đầu vào là yêu cầu kết xuất thông tin đến một tệp tin trong hệ thống, cần kiểm tra tài khoản người dùng có quyền truy cập nội dung tệp tin không.
- Có thể kiểm tra bằng các câu lệnh truy vấn cơ sở dữ liệu, hoặc sử dụng các tệp tin khác trong máy chủ có dữ liệu chỉ định phân quyền truy cập: gồm cái white list chứa thông tin về cái tệp tin mà tài khoản nào có thể truy cập.
- Sau khi kiểm tra, nếu thấy tài khoản không có quyền truy cập, thông báo cho người dùng, đồng thời chặn.

1.2.5.3 Phương pháp ngăn chặn SQL Injection

Để bảo vệ hệ thống trước nguy cơ SQL Injection, chúng ta có thể thực hiện các biện pháp sau:

- Lọc dữ liệu từ người dùng: Cách phòng chống này tương tự như XSS. Ta sử dụng filter để lọc các kí tự đặc biệt (; ” ‘) hoặc các từ khoá (SELECT, UNION) do người dùng nhập vào. Luôn đảm bảo dữ liệu đã được xác thực trước khi được sử dụng trong các câu lệnh SQL.

- Không cộng chuỗi để tạo SQL: Sử dụng parameter thay vì cộng chuỗi. Nếu dữ liệu truyền vào không hợp pháp, SQL Engine sẽ tự động báo lỗi. Bên cạnh đó, khi sử dụng parameter, chúng ta cũng có thể dễ dàng xác thực dữ liệu hơn.
- Không hiển thị exception, message lỗi: Hacker dựa vào message lỗi để tìm ra cấu trúc database. Khi có lỗi, ta chỉ hiện thông báo lỗi chứ không hiển thị đầy đủ thông tin về lỗi, tránh hacker lợi dụng.
- Phân quyền rõ ràng trong cơ sở dữ liệu: Nếu chỉ truy cập dữ liệu từ một số bảng, chúng ta nên tạo các tài khoản và gán quyền truy cập cho tài khoản đó. Lúc này, dù hacker có inject được SQL cũng không thể đọc dữ liệu từ các bảng chính, sửa hay xoá dữ liệu.
- Backup dữ liệu thường xuyên: các dữ liệu quan trọng trong hệ thống cần phải thường xuyên được backup nhằm đảm bảo khi bị tấn công thì ta vẫn có thể khôi phục được.
- Xoá các stored procedure không dùng như xp_cmdshell, xp_startmail, xp_sendmail, sp_makewebtask trong database master.

Bên cạnh đó, với các thông tin quan trọng như mật khẩu người dùng, chúng ta cần sử dụng các phương thức mã hóa để đảm bảo khi dữ liệu bị rò rỉ thì hacker cũng không thể sử dụng.

1.2.5.4 Phương pháp ngăn chặn DDoS

Với nhiều hình thức tấn công DDoS như đã trình bày ở trên, chúng ta cũng có nhiều cách để phòng chống các cuộc tấn công như sau

- Nếu chúng ta có thể xác định địa chỉ IP của các máy tính thực hiện tấn công: có thể tạo một ACL (danh sách quản lý truy cập) trong tường lửa để chặn những IP này.
- Giám sát lưu lượng truy cập: bằng cách này, chúng ta có thể phát hiện được các vụ tấn công DDoS nhỏ mà tin tặc vẫn thường dùng để kiểm thử năng lực của mạng lưới trước khi tấn công thật sự.

- Tăng băng thông, sử dụng các hệ thống cân bằng tải, chuyển hướng cuộc tấn công, dùng cơ chế chống mạo danh IP hoặc chuyển lượng truy cập sang một nhà cung cấp dịch vụ chống DDoS.
- Thiết lập các quy tắc trong tường lửa của để bảo vệ hệ thống

Trong phạm vi đề tài này, nhóm chúng em tiến hành ngăn chặn các cuộc tấn công DDoS bằng cách thiết lập các quy tắc trên tường lửa (iptables). Quá trình thiết lập iptables để ngăn chặn các cuộc tấn công DDoS như sau:

- Cài đặt và bật iptables trên hệ thống.
- Sử dụng các lệnh trong iptables để thêm các quy tắc vào tường lửa. Những quy tắc này xác định truy cập nào được chấp nhận, từ chối hoặc bỏ qua bởi hệ thống.
- Nếu biết được địa chỉ IP của nguồn tấn công DDoS tới hệ thống. Chúng ta có thể chặn truy cập từ một hoặc một dải địa chỉ IP cụ thể bằng câu lệnh iptables -A INPUT -s a.b.c.d -j DROP.
- Nếu cuộc tấn công chọn mục tiêu là một cổng cụ thể trên hệ thống, chúng ta có thể chặn truy cập trên cổng đó để ngăn chặn cuộc tấn công bằng câu lệnh iptables -A INPUT -p tcp --dport 80 -j DROP. Ta cũng có thể sử dụng cách này để cho phép truy cập vào các port có cung cấp dịch vụ trên hệ thống và chặn các truy cập vào các port không cung cấp dịch vụ.
- Chúng ta cũng có thể giới hạn tốc độ của lưu lượng truy cập vào hệ thống để giúp giảm thiểu tác động của một cuộc tấn công DDoS cũng như đảm bảo các dịch vụ hệ thống đang cung cấp không bị gián đoạn. Ta có thể sử dụng câu lệnh sau: iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT.
- Nếu hệ thống cung cấp dịch vụ cho một địa chỉ hoặc một mạng cụ thể, chúng ta có thể sử dụng câu lệnh “DROP” hoặc “ACCEPT” để ngăn chặn các truy cập bên ngoài vùng cung cấp dịch vụ và chỉ cho phép các địa chỉ hoặc mạng cụ thể sử dụng dịch vụ.

1.2.6. Phân tích log truy cập để phát hiện và cảnh báo xâm nhập bằng Snort

1.2.6.1 Mục đích

- Việc phân tích log truy cập hệ thống cung cấp cho người quản trị hệ thống một công cụ để phát hiện và cảnh báo các cuộc tấn công có thể nhắm vào hệ thống. Từ đó có các biện pháp ngăn chặn và phòng tránh để đảm bảo các dịch vụ của hệ thống không bị ảnh hưởng bởi cách cuộc tấn công. Từ đó đảm bảo sự an toàn về dữ liệu của người dùng cũng như các chức năng của hệ thống.

1.2.6.2 Sử dụng Snort để phân tích log truy cập của Website

- Snort là phần mềm IDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời. Với kiến trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình. Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris …
- Bên cạnh việc có thể hoạt động như một ứng dụng bắt gói tin thông thường, Snort còn được cấu hình để chạy như một NIDS.
- Sau khi cài đặt thành công, Snort có thể hoạt động ở 3 chế độ:
    - Package sniffer: hiển thị thông tin header các gói tin.
    - Package log: ghi lại các thông tin vào file log để xử lý sau này.
    - IDS: phân tích các gói tin hoặc các luồng TCP, thực hiện các chức năng IDS theo cơ chế signature-based.
- Với Snort, ta có thể sử dụng các luật để phát hiện xâm nhập, một luật trong Snort được chia thành hai phần đó là phần header và options. Phần header bao gồm: rule action, protocol, địa chỉ ip nguồn, địa chỉ ip đích, subnetmask, port nguồn, port đích. Phần options bao gồm các thông điệp cảnh báo, thông tin

các phần của gói tin sẽ đ0ược kiểm tra để xác định xem hành động nào sẽ được áp dụng.

- Luật - rules được hình thành từ 02 thành phần chính là rules header và rules options.
- Bên cạnh các luật cộng đồng được Snort hỗ trợ, chúng ta có thể tự cấu hình các luật cần thiết với hệ thống hiện tại.

1.2.6.3 Sử dụng Python để thống kê và trực quan hóa số liệu về log truy cập

- Bên cạnh việc sử dụng Snort để phát hiện và cảnh báo các cuộc tấn công, chúng ta cũng có sử dụng Snort thể lưu lại lịch sử log truy cập vào hệ thống dưới dạng file csv. Từ dữ liệu này, bằng các công cụ phân tích dữ liệu như Python, Excel, người quản trị hệ thống có thể thống kê và trực quan hóa số liệu và rút ra các thông tin quan trọng như cổng thường bị tấn công, giao thức thường được sử dụng để tấn công hệ thống, ... từ đó đưa ra các giải pháp để tối ưu việc bảo vệ hệ thống trong tương lai.

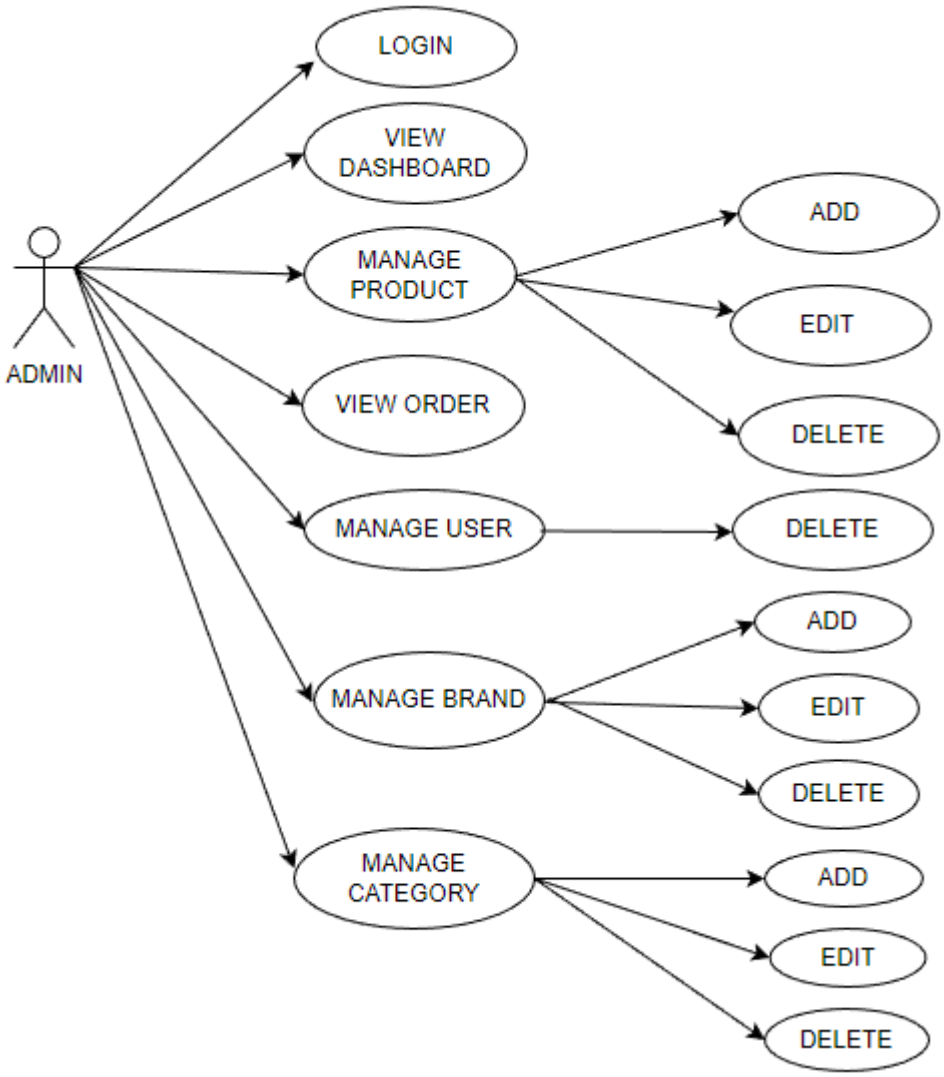
Chương 2. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

2.1. Phân tích yêu cầu hệ thống

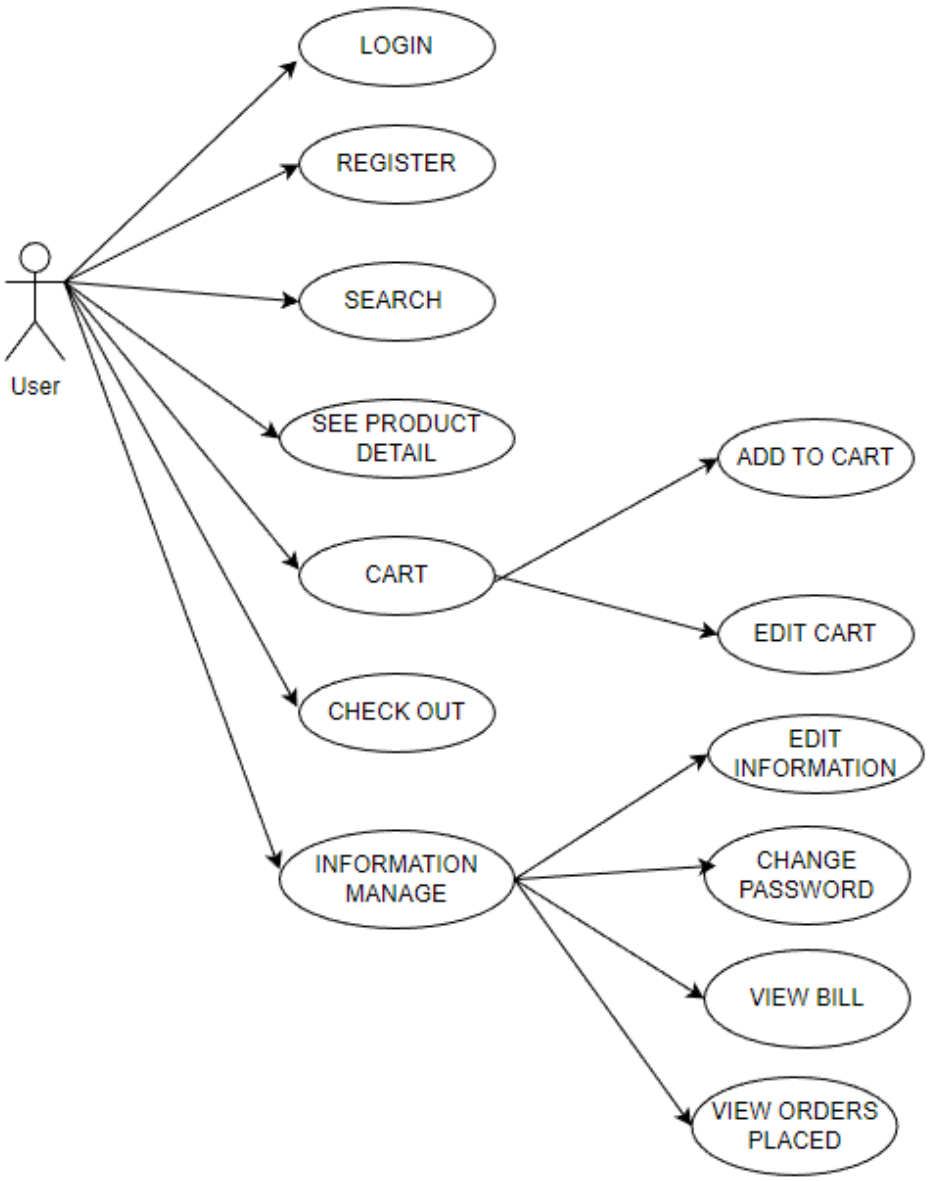
- **Phân tích yêu cầu**: thực hiện xây dựng hệ thống cung cấp dịch vụ website thương mại điện tử cũng như các cơ chế bảo vệ hệ thống trước các cuộc tấn công mạng.
- **Yêu cầu**: hệ thống cung cấp website thương mại điện tử và xây dựng tường lửa cũng như các cơ chế ngăn chặn và phân tích các cuộc tấn công
    - **Đầu vào**:
        - Máy chủ web chứa Website
        - Máy tấn công
        - Website thương mại điện tử có giao diện và các chức năng có thể bị tấn công.
    - **Đầu ra**:
        - Phân tích log truy cập của Website nhằm tìm ra các cuộc tấn công và tiến hành ngăn chặn trên iptables.
        - Phân tích và chống lại được các cuộc tấn công nhắm vào hệ thống của tin tặc như: XSS, SQL Injection, Path traversal, DDoS.

2.2. Thiết kế hệ thống

2.2.1. Sơ đồ use-case hệ thống

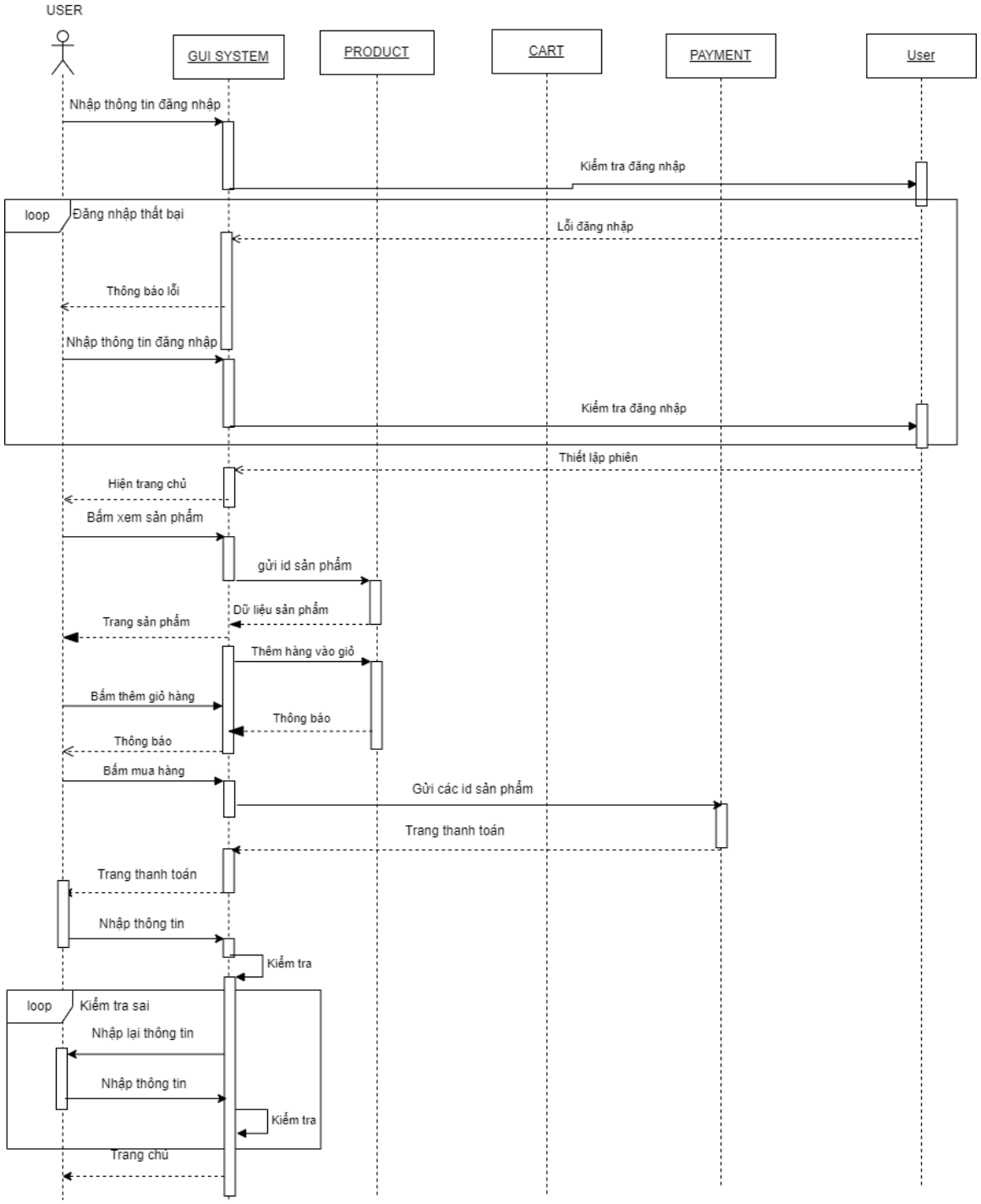


Hình ảnh 2: Sơ đồ Use Case của Admin



Hình ảnh 3: Sơ đồ Use-case User

2.2.2. Thiết kế chức năng hệ thống



Hình ảnh 4: Sơ đồ Sequence các hoạt động của người dùng

2.2.3. Môi trường cài đặt và cấu hình Server

2.2.3.1 Môi trường cài đặt

- Ngôn ngữ lập trình sử dụng: PHP, HTML, CSS, Javascript, Shell, Python.
- Công cụ hỗ trợ: Git, Github, VMWare, Snort,...

- Công cụ lập trình: Visual Studio Code

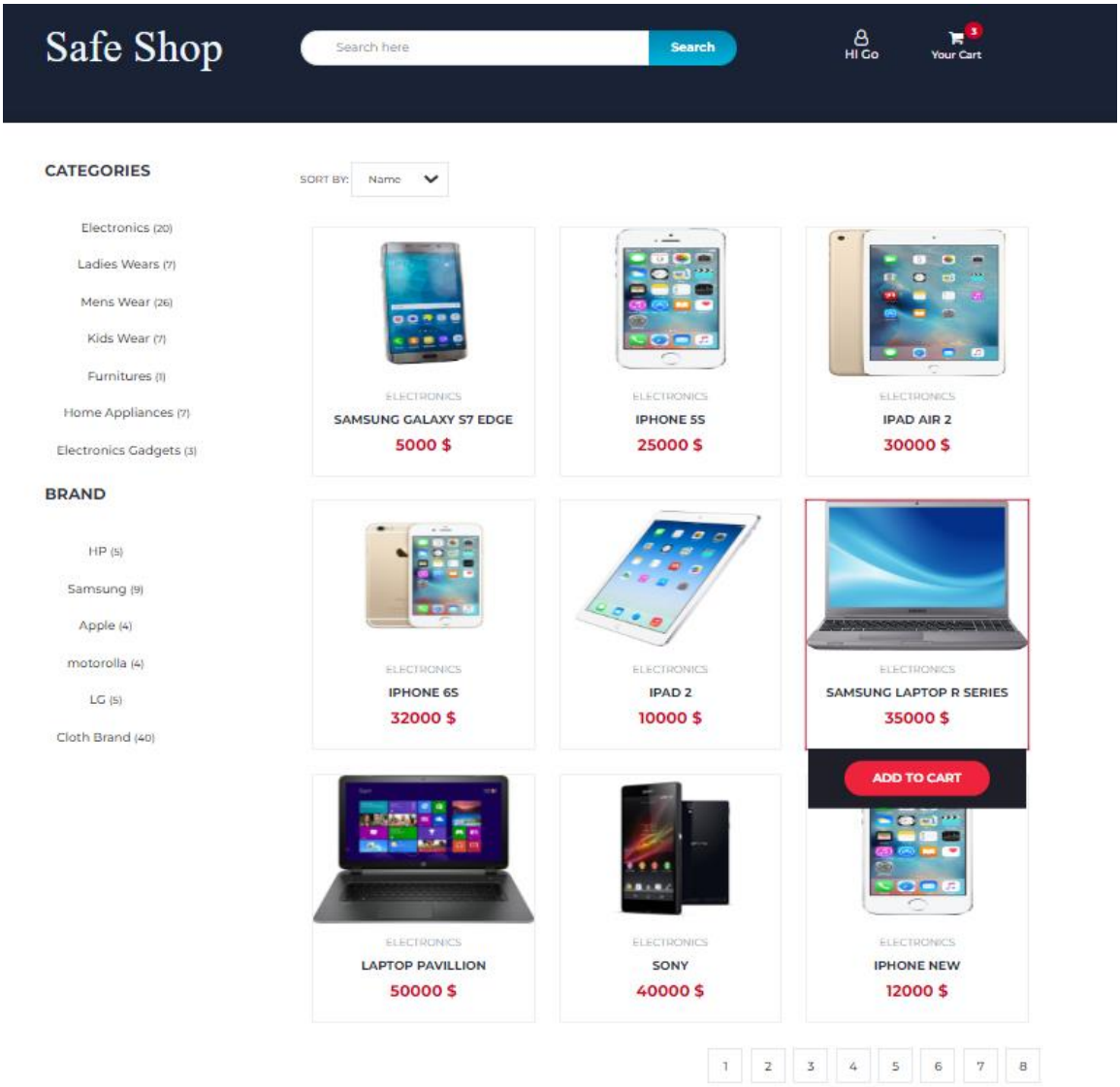
2.2.3.2 Cấu hình Server

- Hệ điều hành: Ubuntu.
- Web server: Apache.
- Cơ sở dữ liệu: MySQL.
- Cấu hình tường lửa sử dụng iptables.
- Phân tích và cảnh báo xâm nhập với Snort.

Chương 3. TRIỂN KHAI VÀ ĐÁNH GIÁ KẾT QUẢ

3.1. Giao diện và chức năng của chương trình

3.1.1. *Giao diện chính*

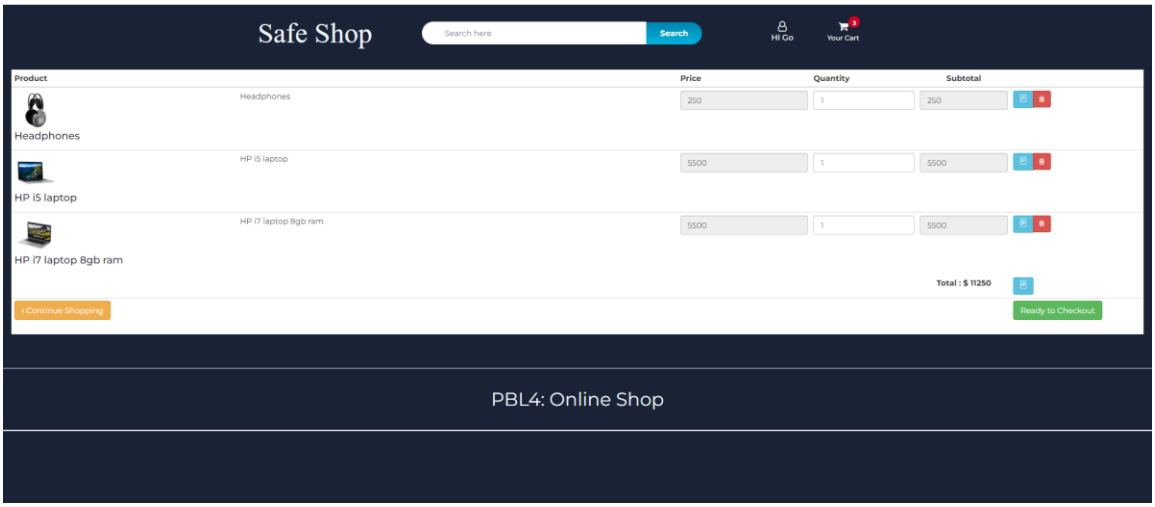


Hình ảnh 5 :Giao diện màn hình chính

Giao diện	Trang chủ Website
Mô tả	Khi người dùng muốn xem sản phẩm
Truy cập	- Truy cập vào trang giao diện chính của trang web - Có thể tìm kiếm sản phẩm theo tên - Có thể chọn theo thể loại hoặc thương hiệu mà user muốn mua - Có thể sắp xếp theo tên hoặc theo giá tiền để dễ dàng tìm kiếm

Bảng 4: Bảng mô tả chức năng trang chủ

3.1.2. *Giao diện giỏ hàng*

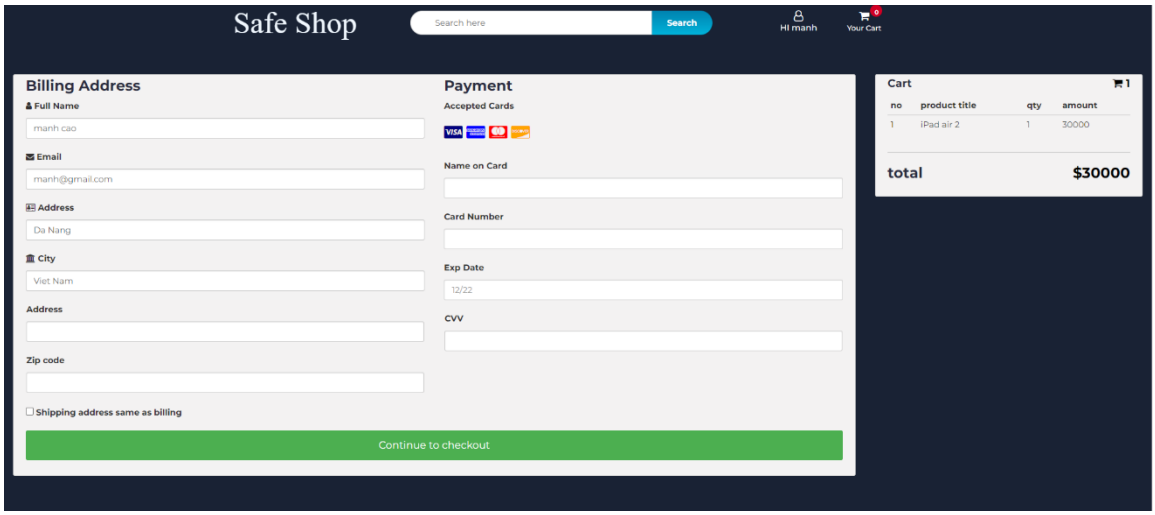


Hình ảnh 6 : Giao diện giỏ hàng

Giao diện	Trang giỏ hàng (Cart)
Mô tả	Khi người dùng muốn mua sản phẩm
Truy cập	- Người dùng sau khi chọn được đồ mình muốn mua, có thể thêm vào giỏ hàng - Có thể xoá hoặc lưu tất cả các món đồ trong giỏ hàng - Có thể chọn được số lượng muốn mua ,và có thể xem được tổng giá trị đơn hàng

Bảng 5: Bảng mô tả chức năng giỏ hàng

3.1.3. *Giao diện thanh toán*

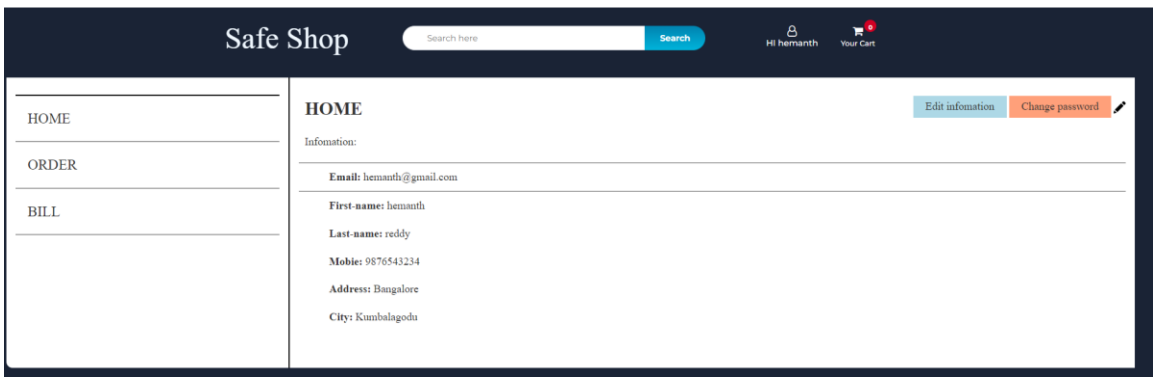


Hình ảnh 7 :Giao diện thanh toán

Giao diện	Trang thanh toán (Payment)
Mô tả	Khi người dùng muốn mua,thanh toán sản phẩm
Truy cập	- Sau khi người dùng muốn mua hàng, sẽ qua trang thanh toán - Nhập đầy đủ các thông tin liên quan,có thể xem được tổng giá tiền mà đơn hàng mình phải trả

Bảng 6: Bảng mô tả chức năng thanh toán

3.1.4. *Giao diện thông tin cá nhân*

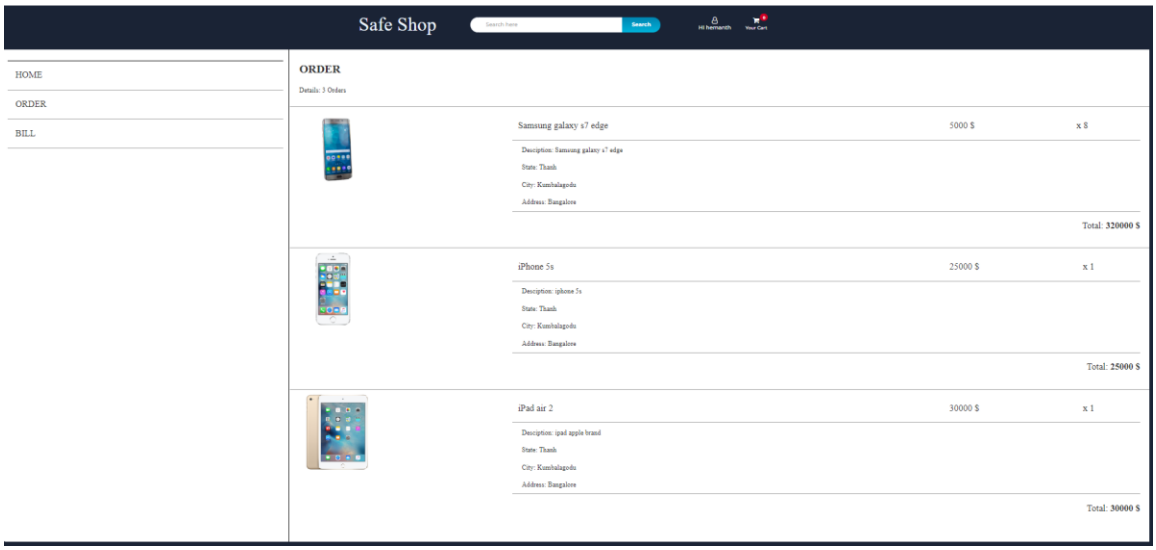


Hình ảnh 8 :Giao diện trang thông tin cá nhân

Giao diện	Trang thông tin cá nhân
Mô tả	- Khi người dùng muốn xem thông tin,sửa,đổi mật khẩu
Truy cập	- Người dùng có thể xem thông tin của bản thân,có thể chỉnh sửa thông tin,đổi mật khẩu

Bảng 7: Bảng mô tả chức năng trang thông tin cá nhân

3.1.5. *Giao diện lịch sử mua hàng trong trang thông tin cá nhân*

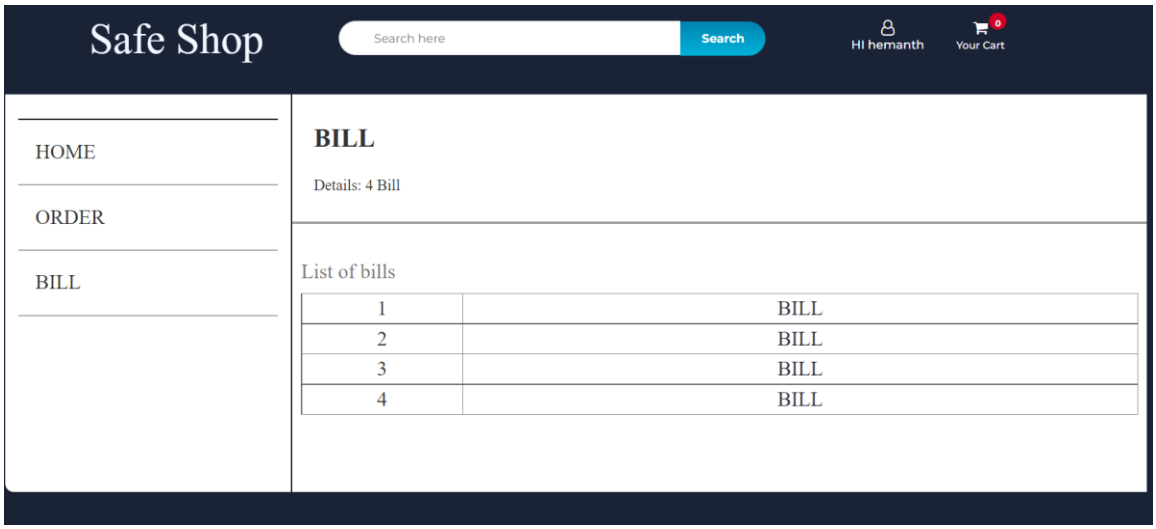


Hình ảnh 9 :giao diện lịch sử mua hàng trong trang cá nhân

Giao diện	Trang thông tin lịch sử mua hàng (Order)
Mô tả	Khi người dùng muốn xem thông tin những đơn hàng mà mình đã đặt
Truy cập	- Có thể xem được mình đã đặt bao nhiêu bill,chi tiết từng bill

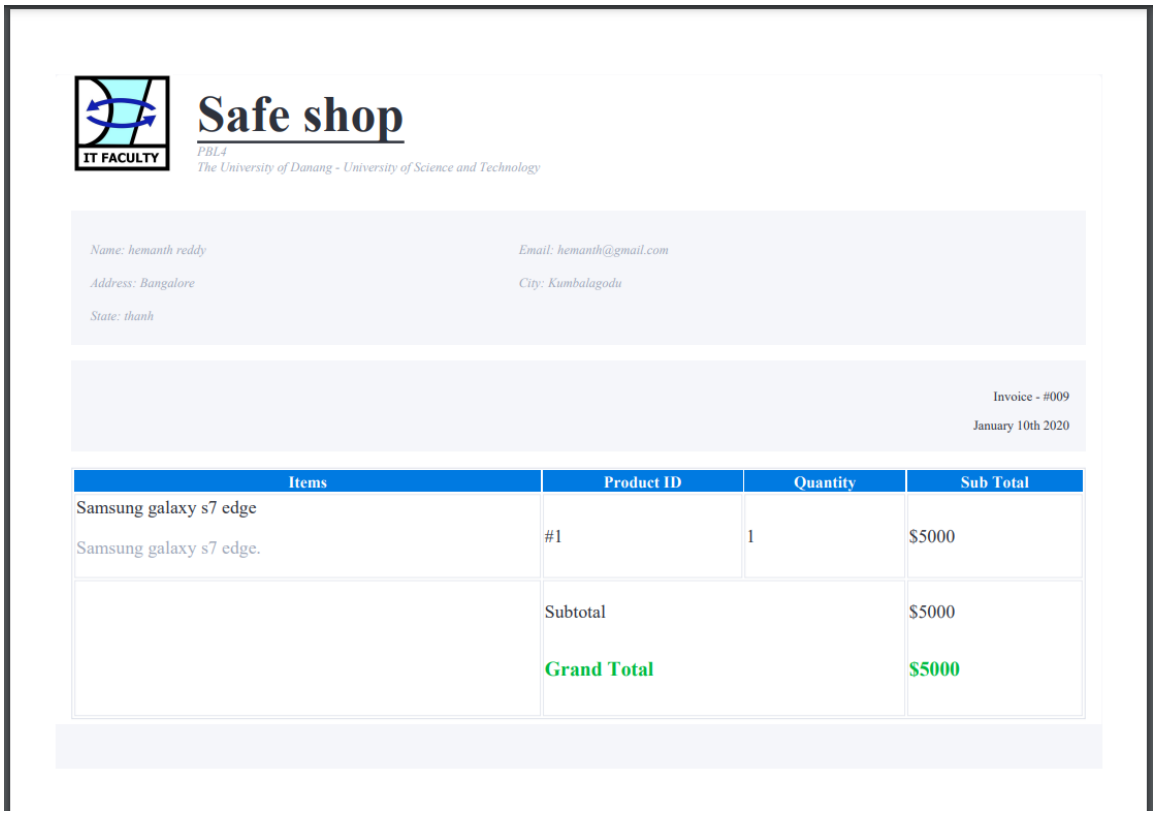
Bảng 8: Bảng mô tả chức năng xem lịch sử mua hàng

3.1.6. *Giao diện hoá đơn trong trang thông tin cá nhân*



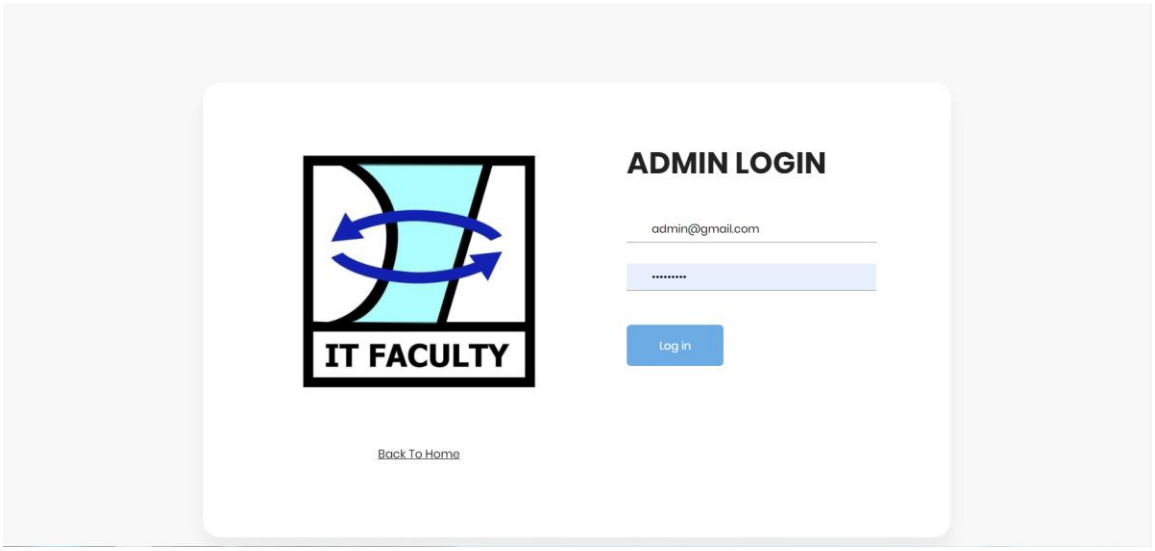
Hình ảnh 10 :Giao diện hoá đơn trong trang cá nhân

Xuất ra pdf :



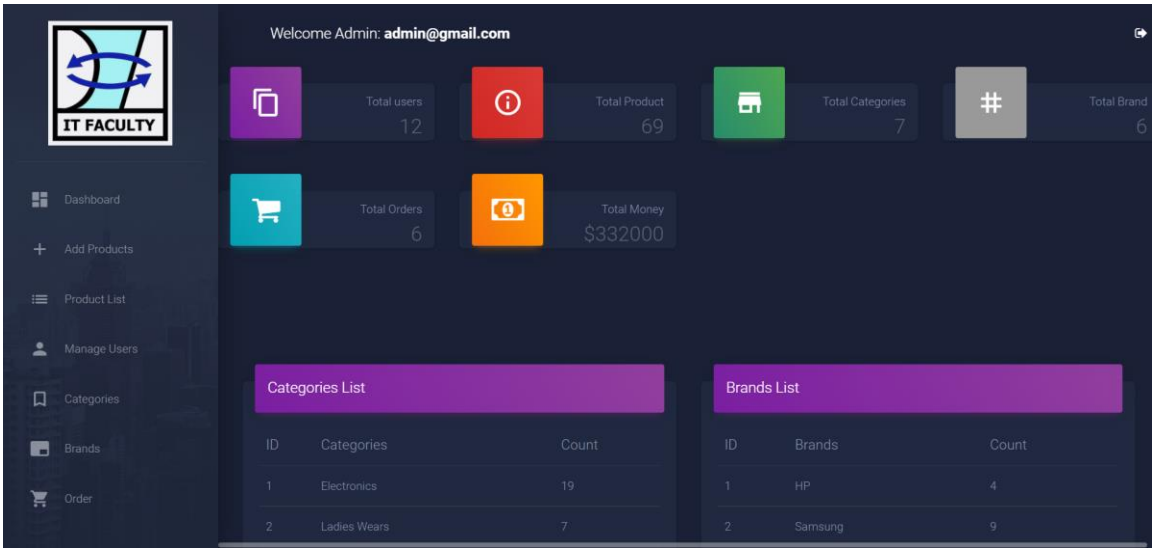
Hình ảnh 11 : Giao diện file pdf xuất hoá đơn

3.1.7. *Giao diện trang đăng nhập admin*



Hình ảnh 12 :Giao diện đăng nhập admin

3.1.8. *Giao diện trang chủ admin*

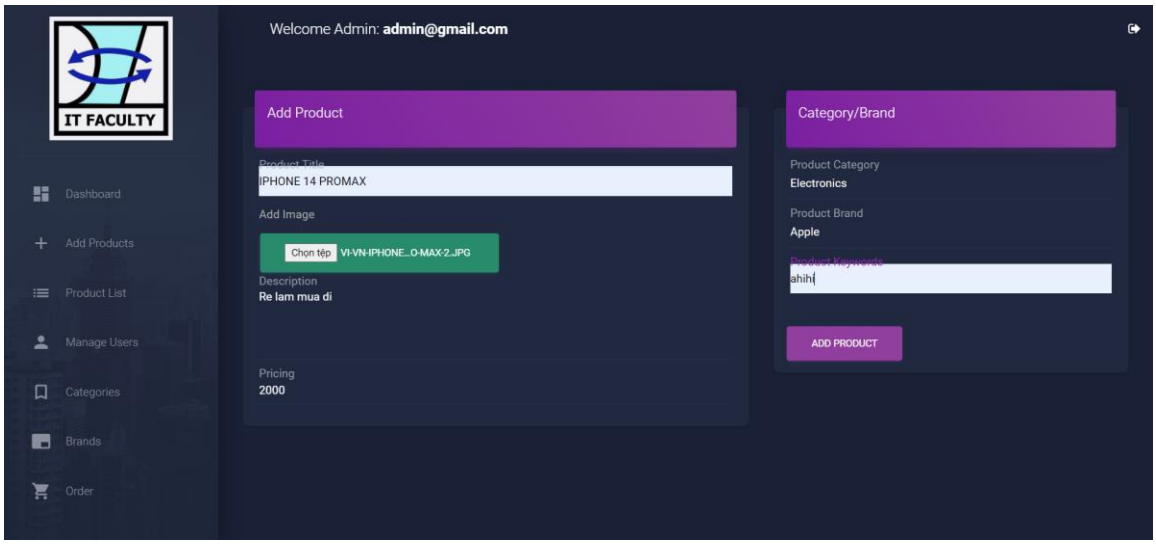


Hình ảnh 13 :Giao diện trang chủ admin

Giao diện	Trang chủ admin
Mô tả	Khi admin muốn xem thông tin (tổng người dùng,tổng sản phẩm,..)
Truy cập	- Admin có thể thêm sản phẩm,xem sản phẩm,chỉnh sửa sản phẩm,thể loại,…

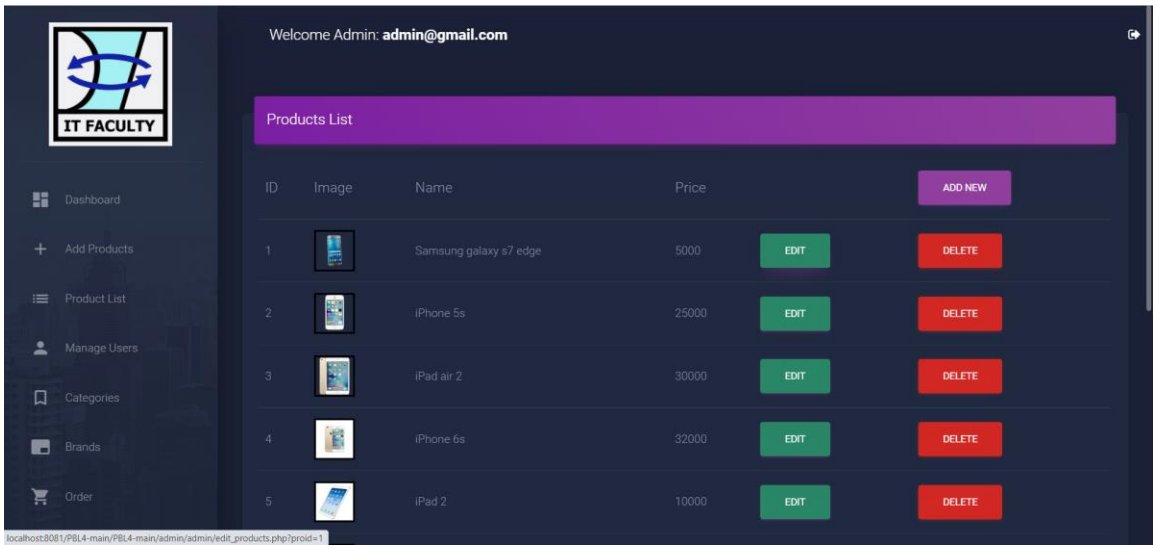
Bảng 9: Bảng mô tả chức năng trang chủ admin

3.1.9. *Giao diện chức năng thêm sản phẩm*



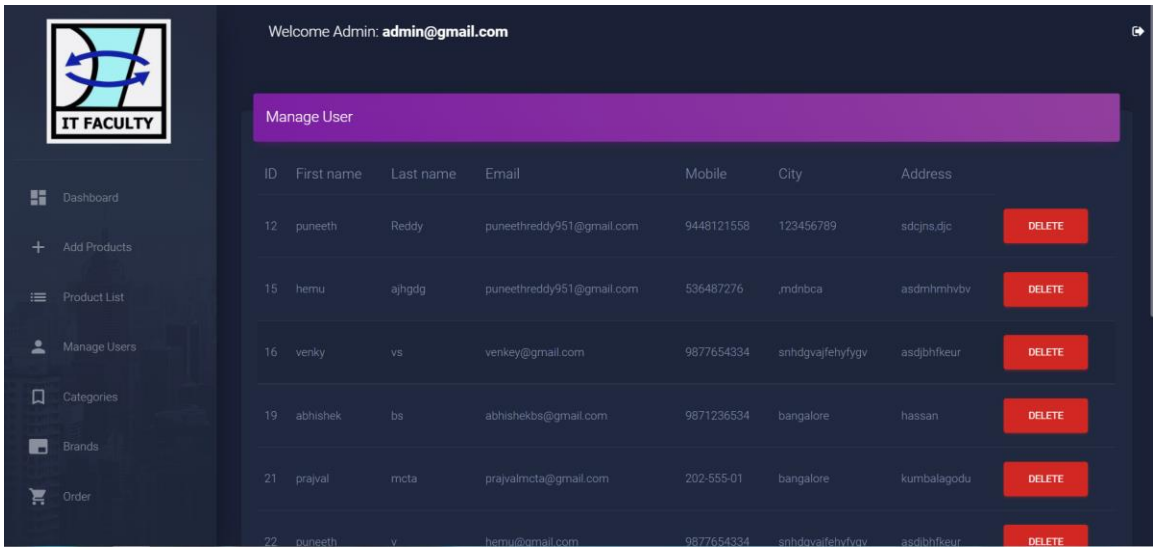
Hình ảnh 14 :Giao diện chức năng thêm sản phẩm

3.1.10. *Giao diện chức năng quản lý sản phẩm*



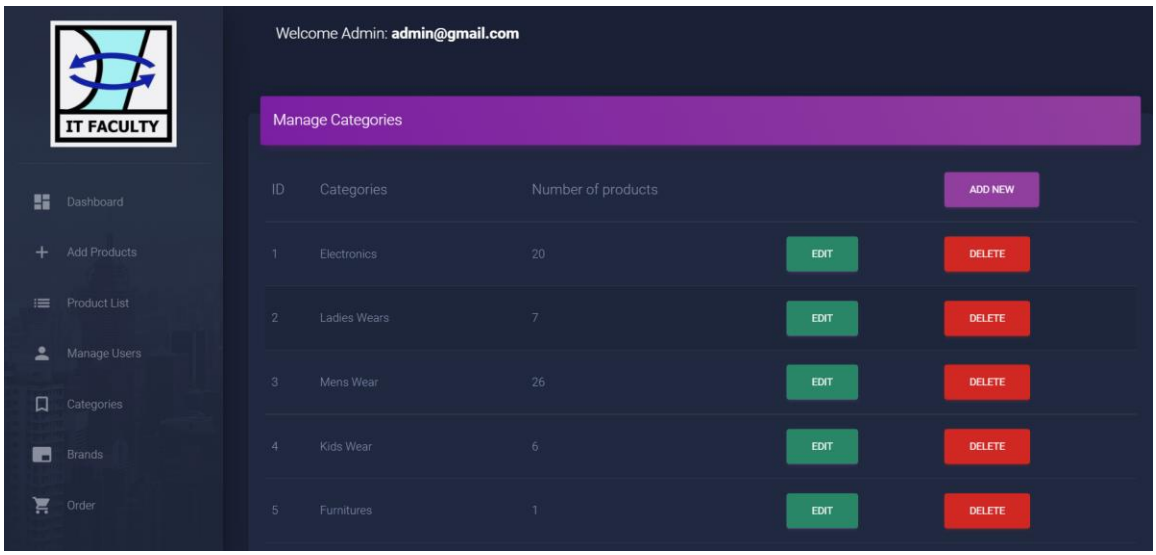
Hình ảnh 15 :Giao diện chức năng quản lý sản phẩm

3.1.11. *Giao diện chức năng quản lý người dùng*



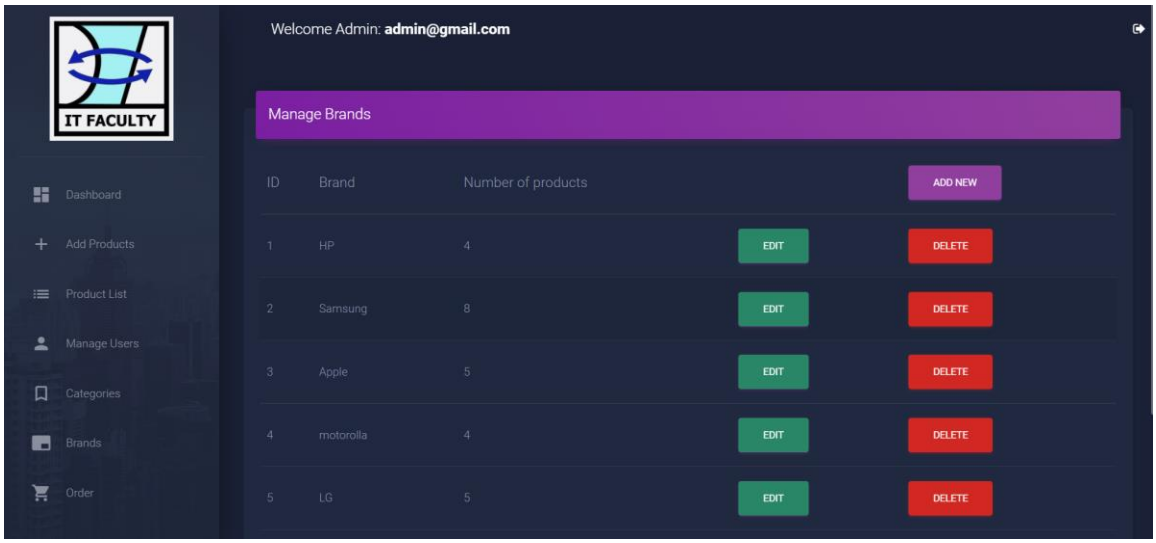
Hình ảnh 16: Giao diện chức năng quản lý người dùng

3.1.12. *Giao diện quản lý danh mục sản phẩm*



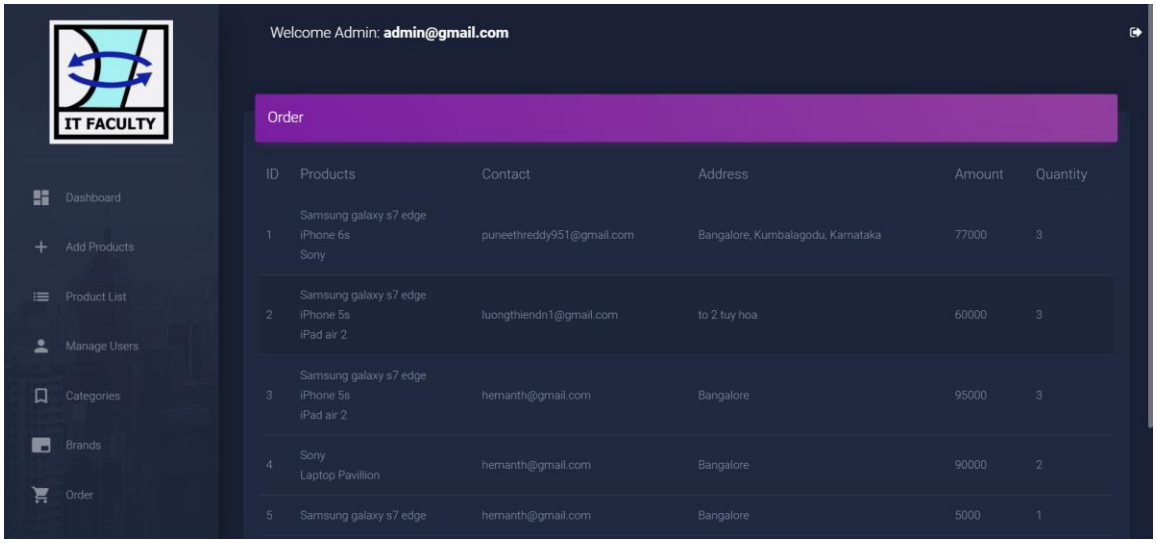
Hình ảnh 17: Giao diện chức năng quản lý danh mục

3.1.13. *Giao diện quản lý thương hiệu sản phẩm*



Hình ảnh 18 : Giao diện quản lý thương hiệu sản phẩm

3.1.14. *Giao diện chức năng quản lý đơn hàng*



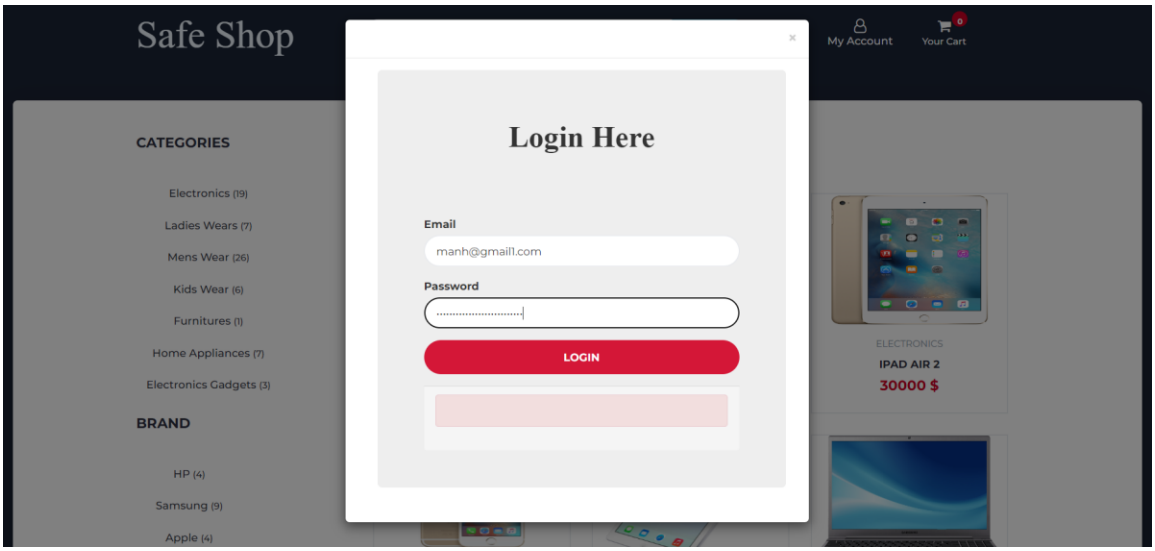
Hình ảnh 19 : Giao diện chức năng quản lý đơn hàng

3.2. Tấn công để kiểm tra hệ thống

3.2.1. *Tấn công SQLi và kết quả*

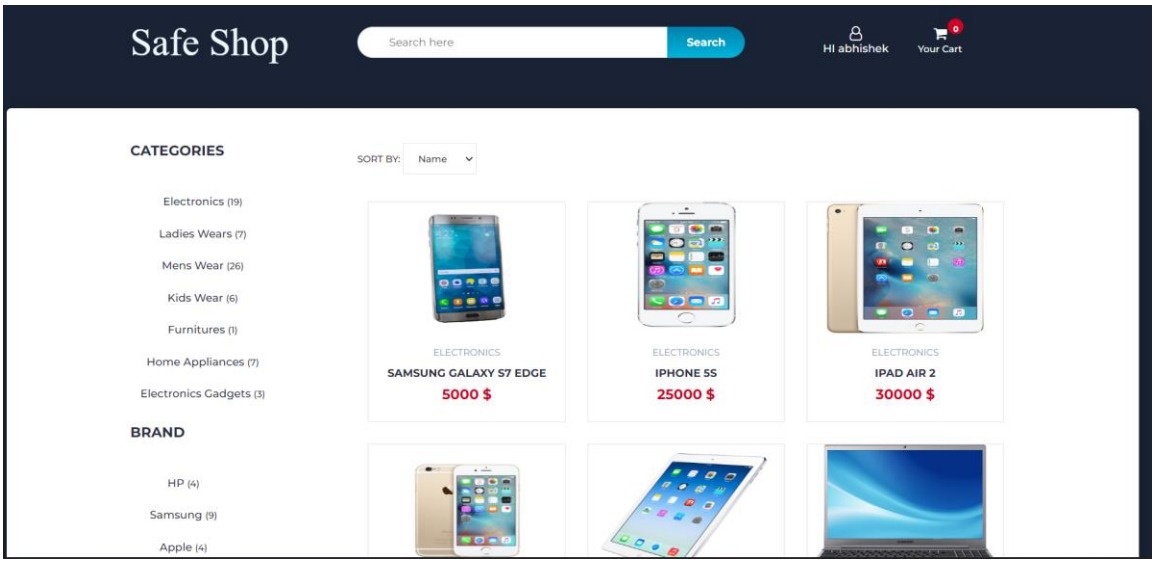
3.2.1.1 Tấn công: đăng nhập website sử dụng từ khoá “or”

- Sử dụng một tài khoản email và password không tồn tại trong hệ thống, với trường password, nhập: fkf' or 1='1' limit 3,1 --



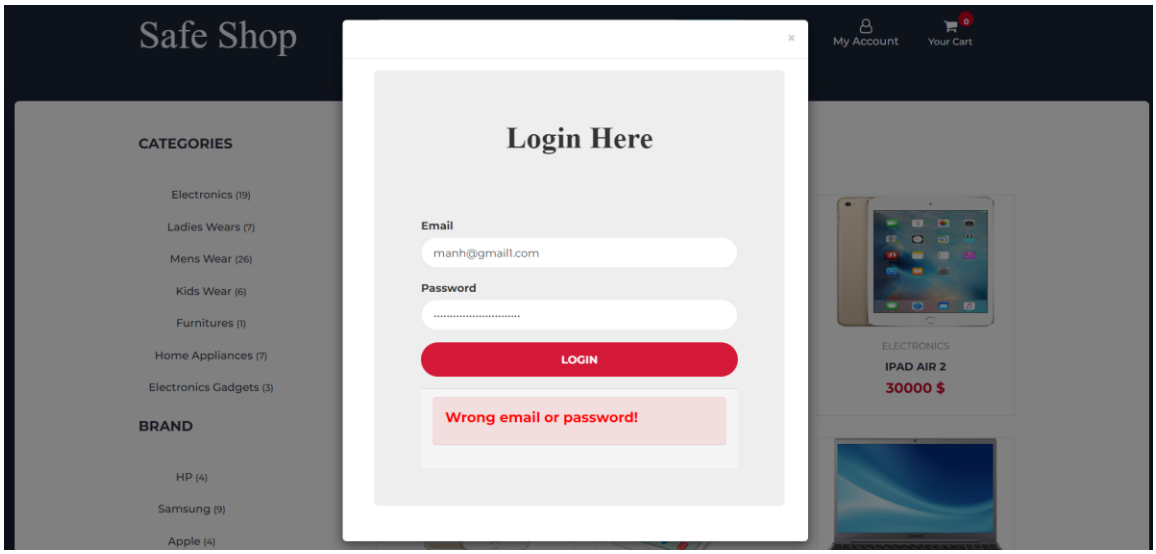
Hình ảnh 20 : Tấn công trang đăng nhập SQL Injection

- Đăng nhập thành công



Hình ảnh 21 : Tấn công đăng nhập bằng SQL Injection thành công

3.2.1.2 Ngăn chặn tấn công

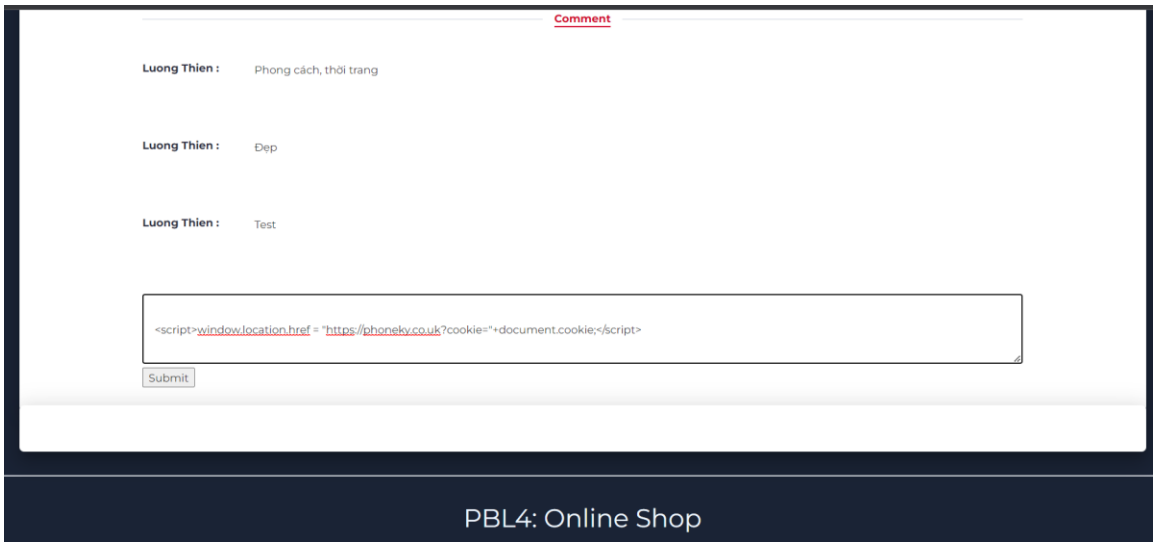


Hình ảnh 22 : Ngăn chặn tấn công SQL Injection thành công

3.2.2. *Tấn công XSS và kết quả*

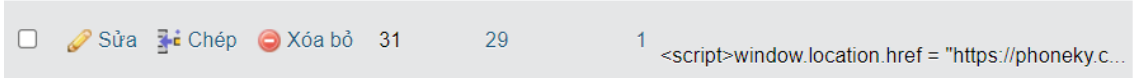
3.2.2.1 Tấn công: Lấy cookie của người dùng.

- Lấy cookie của nạn nhân bằng chức năng comment của trang có URL: http://localhost:8081/PBL4Raw/product.php?p=1#!

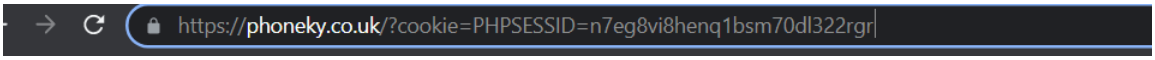


Hình ảnh 23 : Tấn công chức năng bình luận bằng XSS

- Câu lệnh javascript được lưu vào trong cơ sở dữ liệu phpMyAdmin.



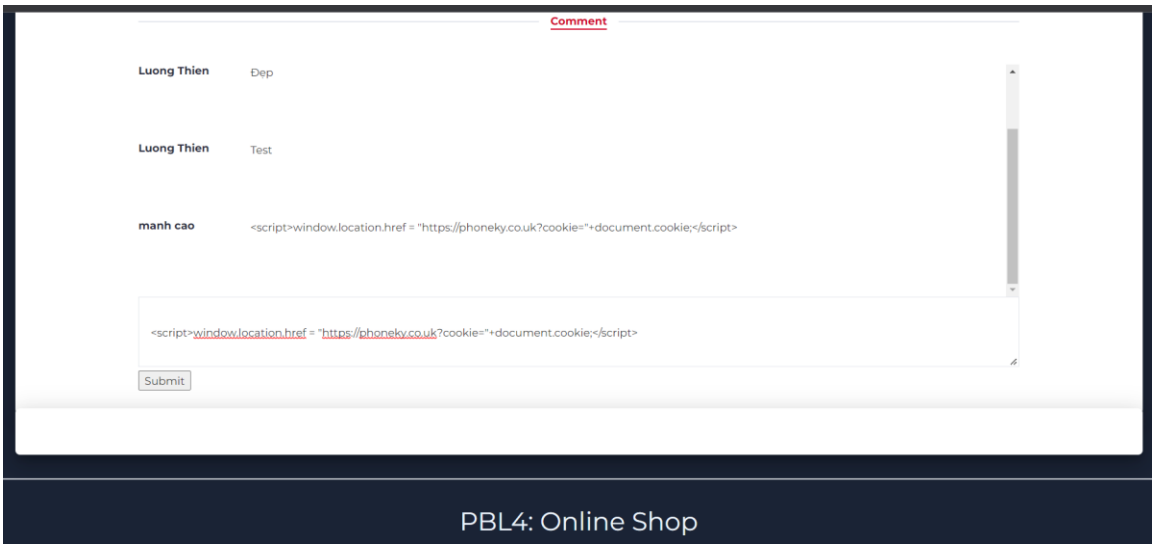
- Một người dùng truy cập vào URL: http://localhost:8081/PBL4Raw/product.php?p=1#! . Nhưng ngay lập tức bị chuyển sang một website khác, trong url còn có thông tin cookie của người dùng.



Hình ảnh 24 Tấn công chức năng bình luận bằng XSS thành công

3.2.2.2 Ngăn chặn tấn công

- Mã hoá dữ liệu đầu vào:

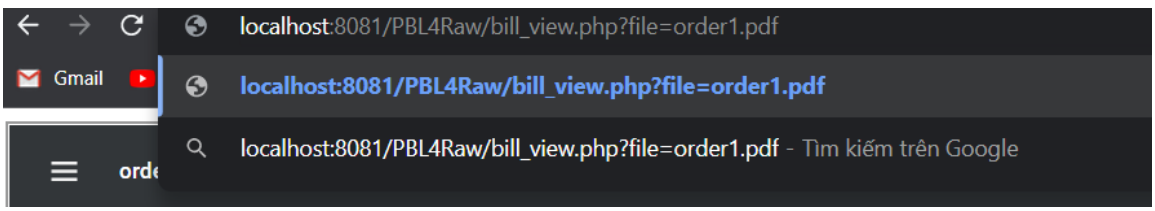


Hình ảnh 25: Ngăn chặn tấn công XSS thành công

3.2.3. Tấn công Path Traversal và kết quả

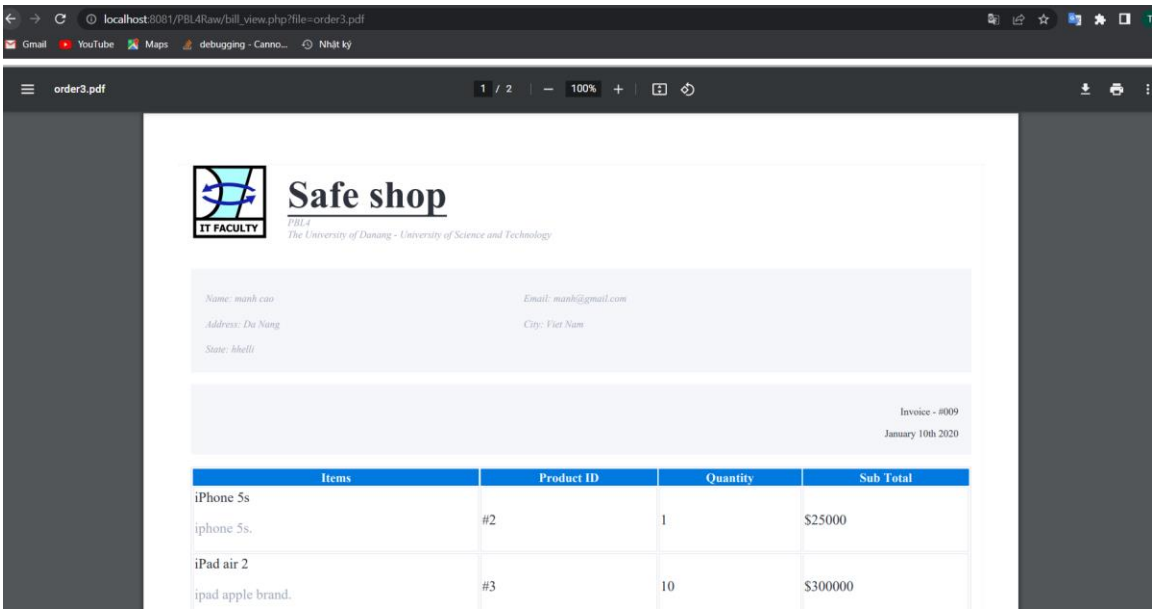
3.2.3.1 Tấn công: Truy cập vào tệp tin khác

- Vào trang cá nhân và xem các hoá đơn của bản thân
- Xem hoá đơn thứ nhất, website sẽ dẫn đến trang có địa chỉ: http://localhost:8081/PBL4Raw/bill_view.php?file=order3.pdf
- Tấn công bằng cách thay đổi URL:



Hình ảnh 26: Tấn công chức năng xem hoá đơn bằng Path Traversal

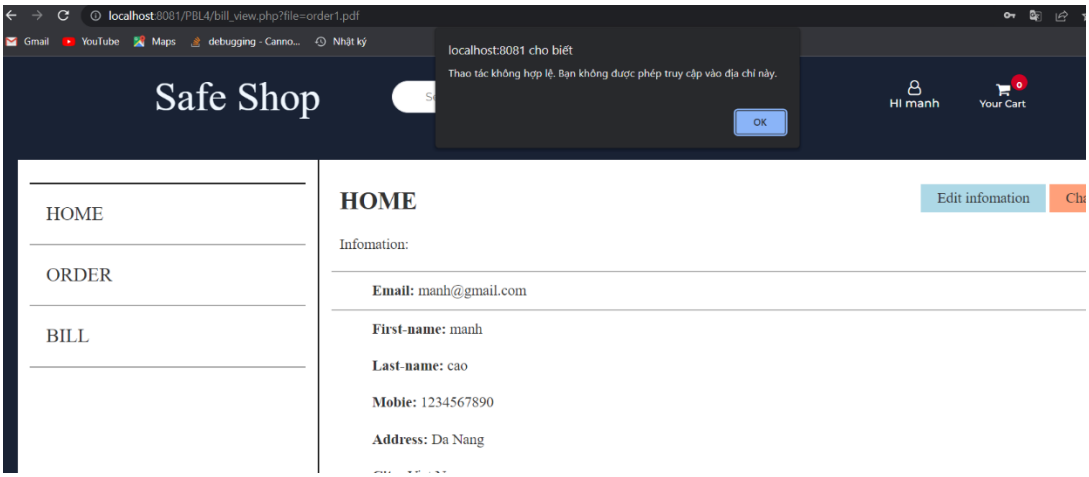
- Đã xem được hoá đơn của người dùng tên Puneeth. Biết được thời gian và các sản phẩm mà tài khoản Puneeth đã đặt mua trên website.



Hình ảnh 27 : Tấn công xem hoá đơn bằng Path Traversal thành công

3.2.3.2 Ngăn chặn tấn công

- Phát hiện truy cập trái phép và cảnh báo người dùng, đồng thời, quay trở lại trang cá nhân của người dùng.

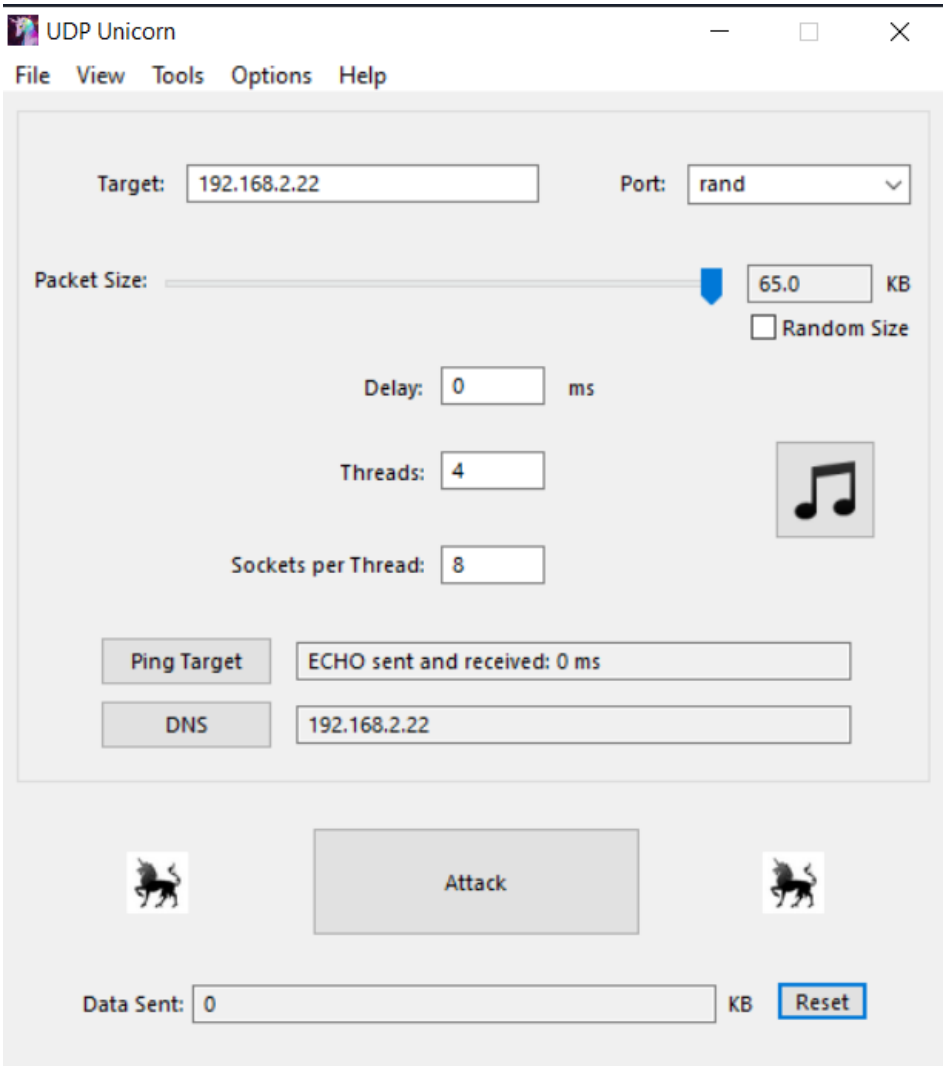


Hình ảnh 28: Ngăn chặn tấn công Path Traversal thành công

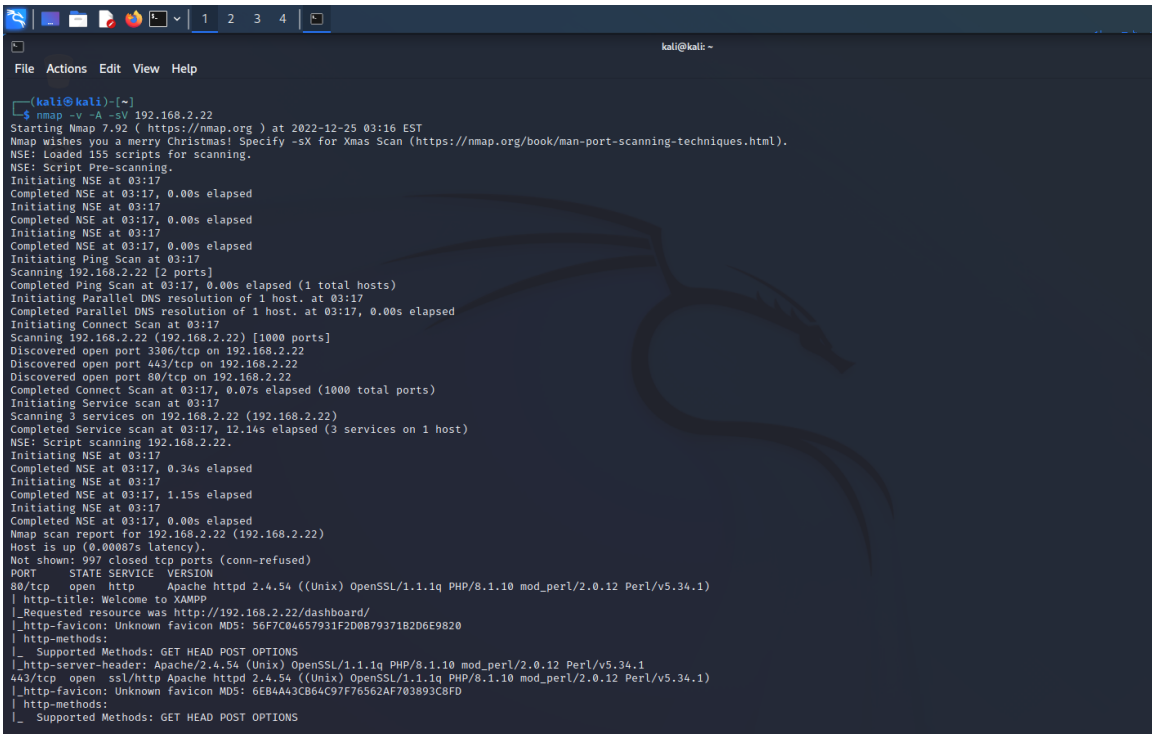
3.2.4. Tấn công DdoS và kết quả

3.2.4.1 Thực hiện tấn công DDos lên server

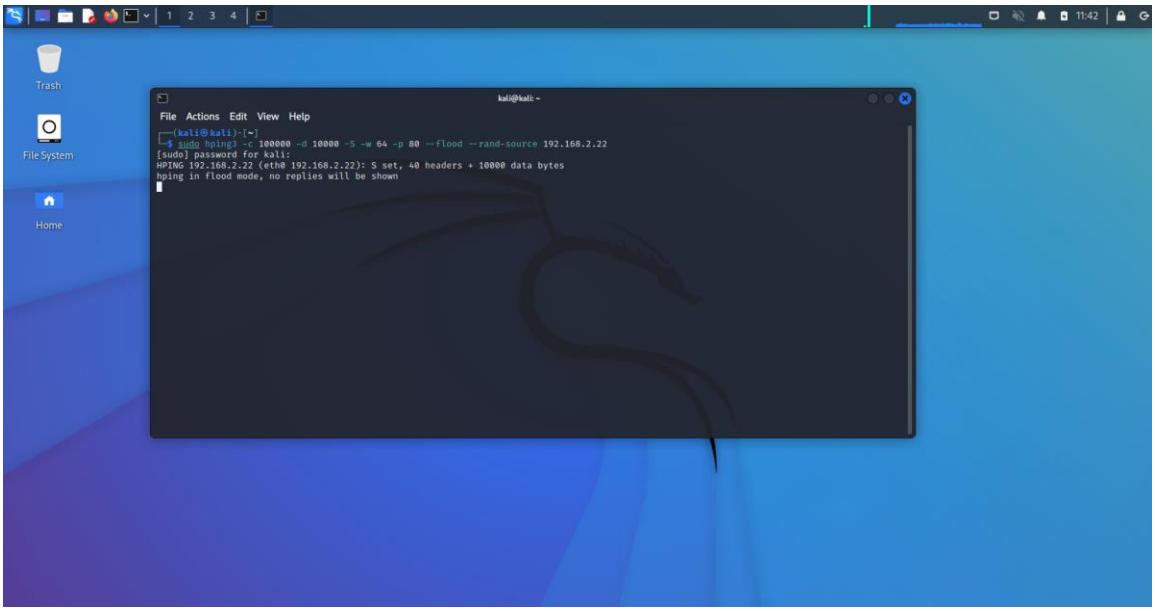
Sử dụng 2 công cụ để tấn công DDos lên hệ thống khi đã biết địa chỉ IP là Unicorn (trên Windows) và hping3 (trên Kali Linux).Ở đây, ta thực hiện tấn công lên Server Ubuntu có địa chỉ IP là 192.168.2.22



Hình ảnh 29: Tấn công bằng công cụ Unicorn

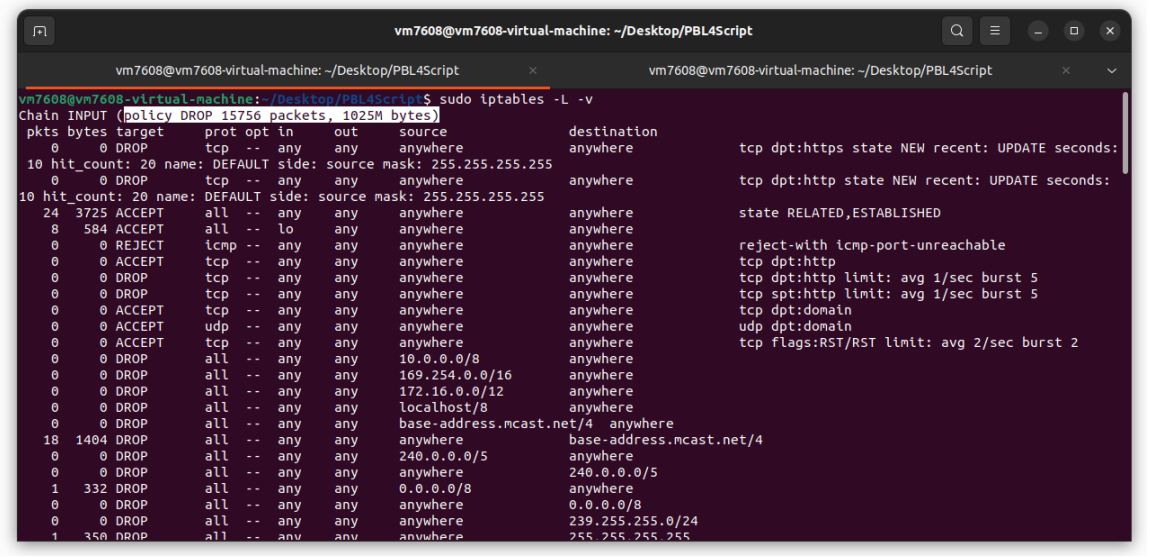


Hình ảnh 30 Quét cổng dịch vụ bằng nmap trên Kali Linux



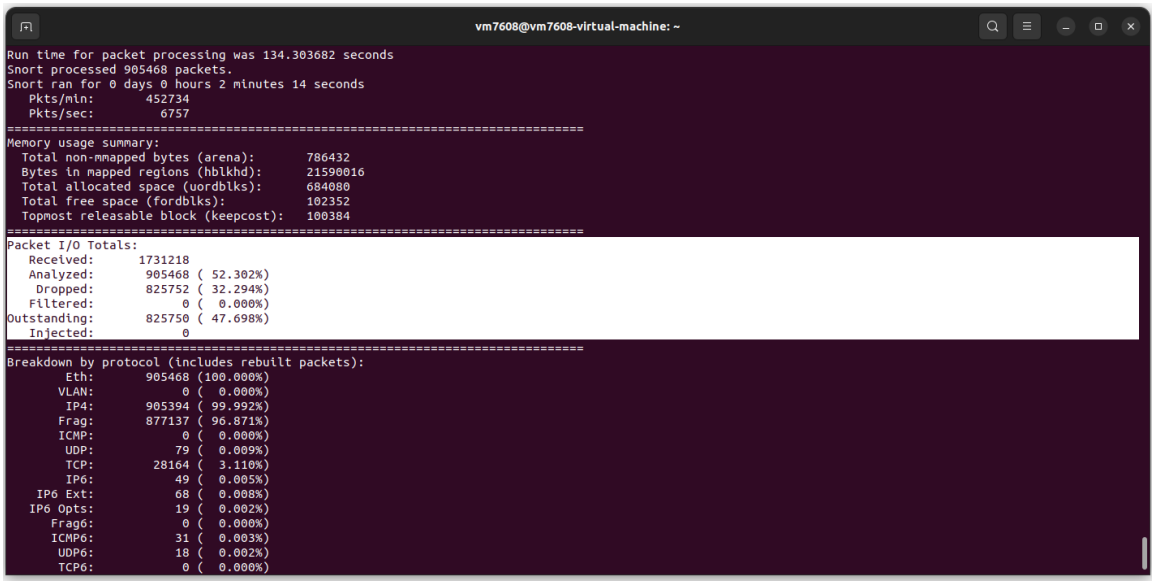
Hình ảnh 31: Tấn công sử dụng hping3 trên hệ điều hành Kali Linux

Hình ảnh 32: Hệ thống đang bị tấn công DDoS

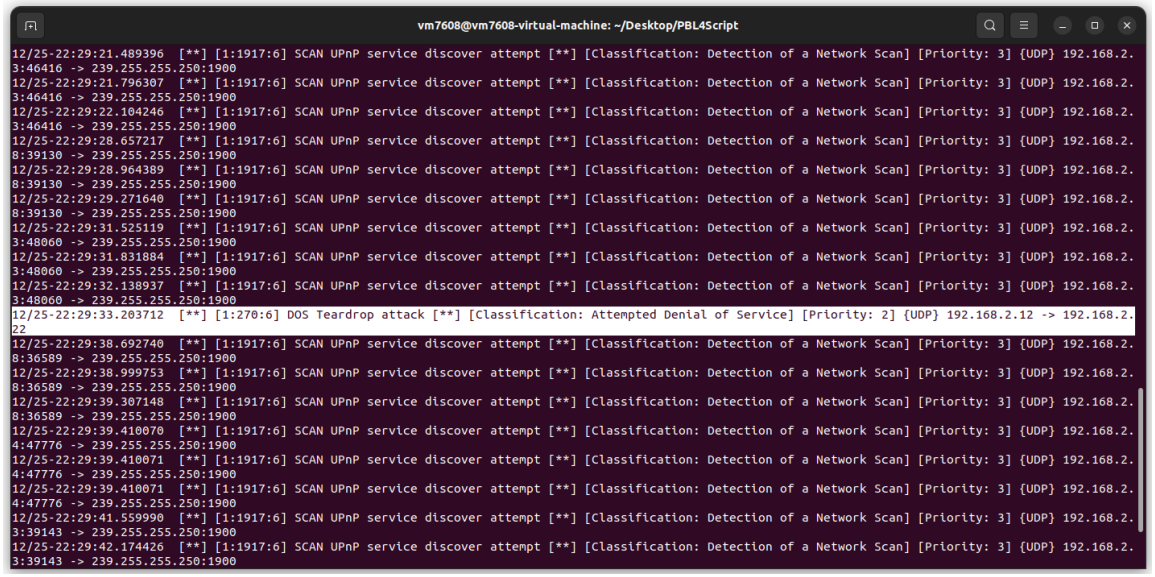


Hình ảnh 33: Kết quả tường lửa ngăn chặn cuộc tấn công DDoS

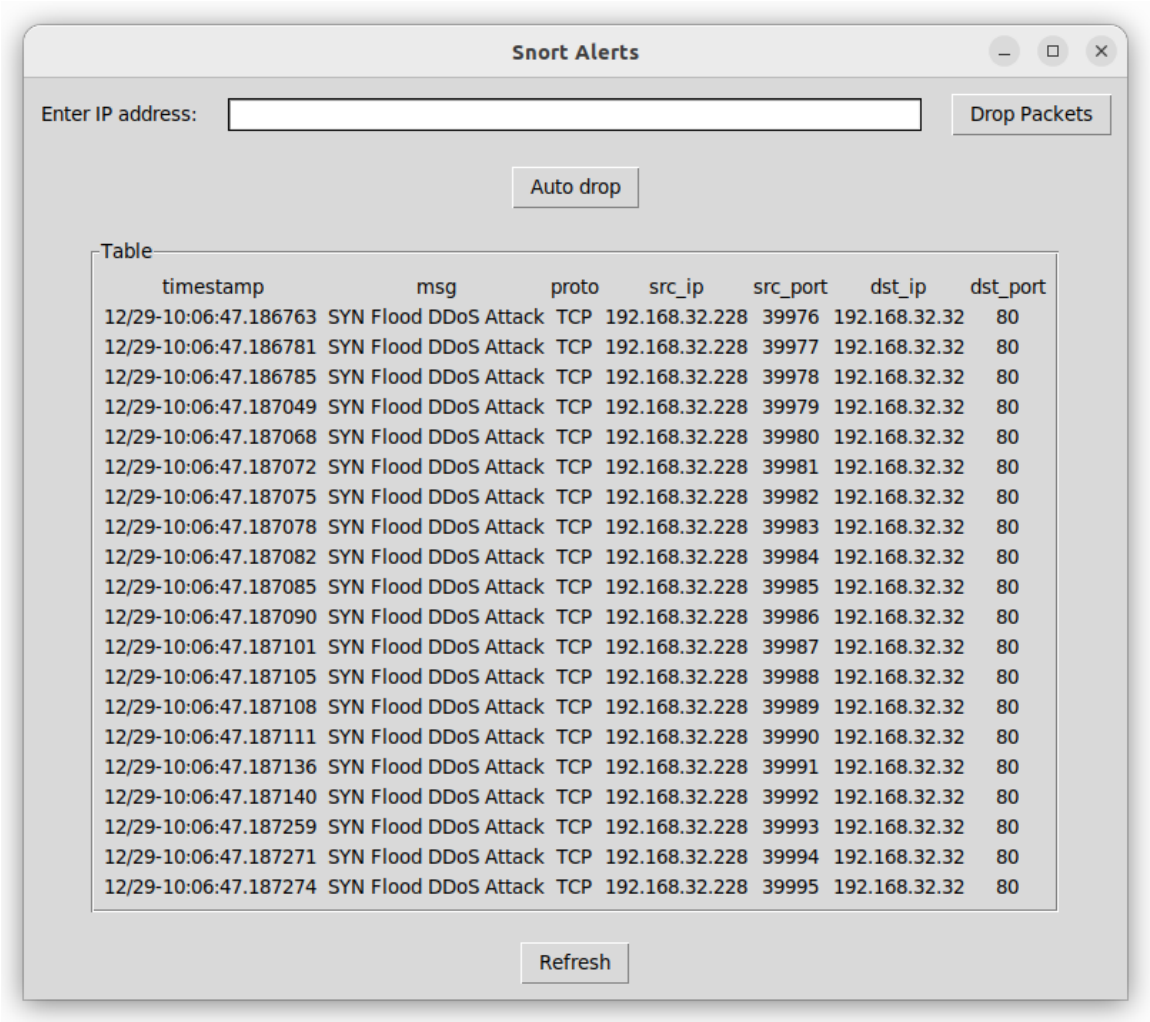
3.3. Kết quả phân tích log và cảnh báo bằng Snort



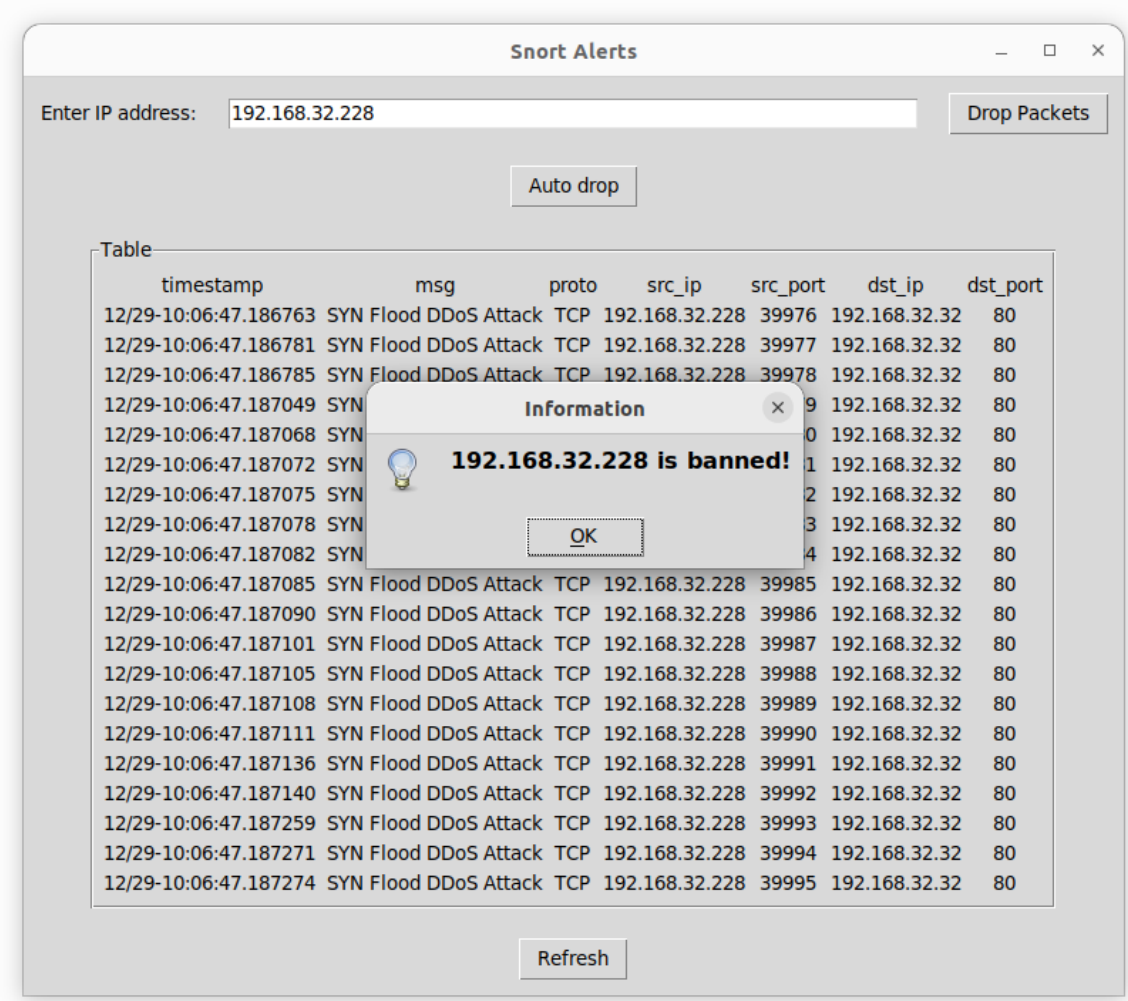
Hình ảnh 34: Thông tin về số packet được Snort phân tích



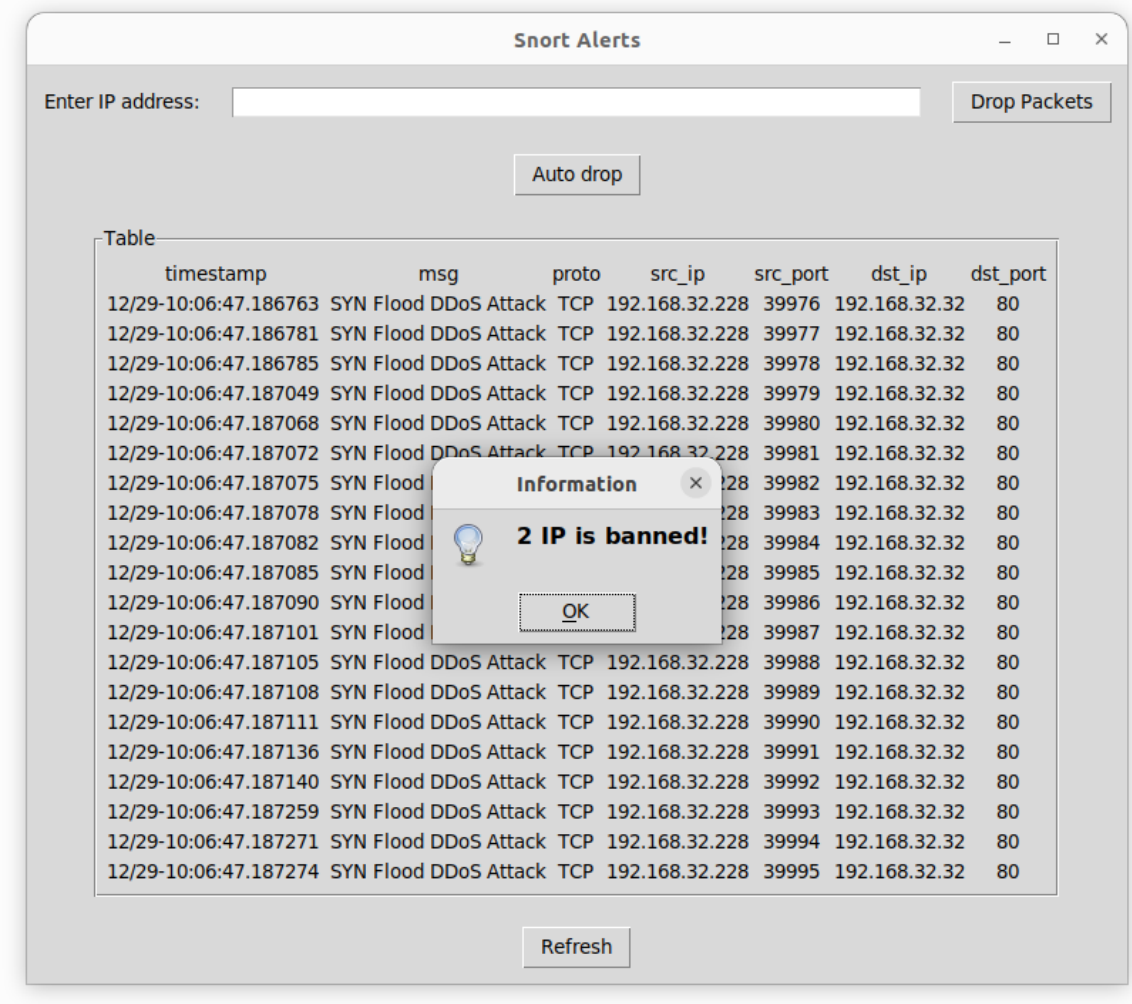
Hình ảnh 35: Snort phát hiện và cảnh báo cuộc tấn công



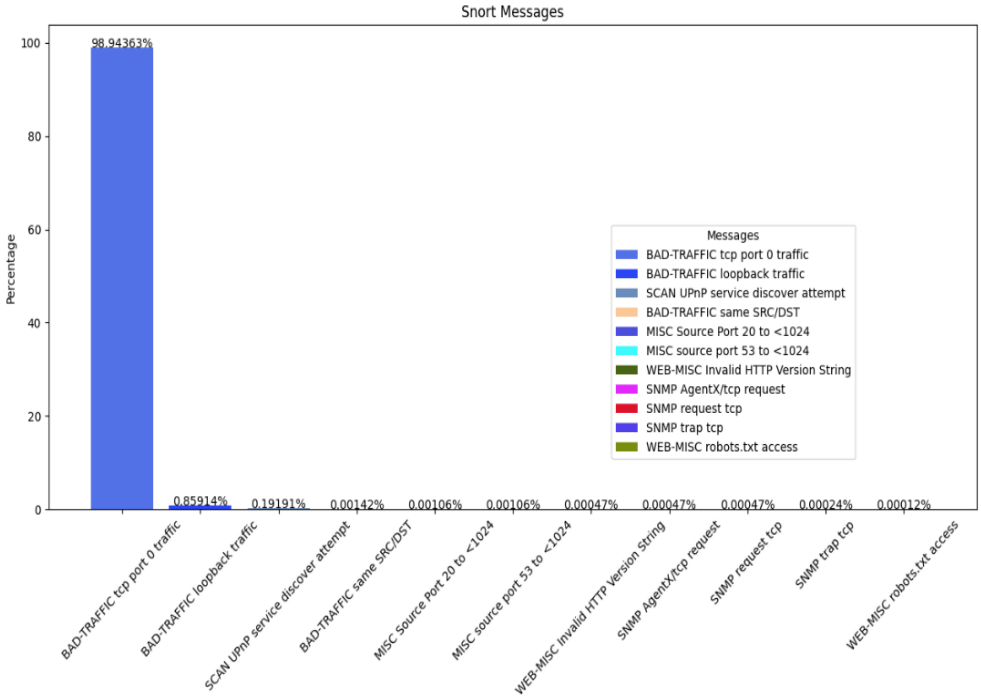
Hình ảnh 36: Xây dựng giao diện để theo dõi cảnh báo từ Snort



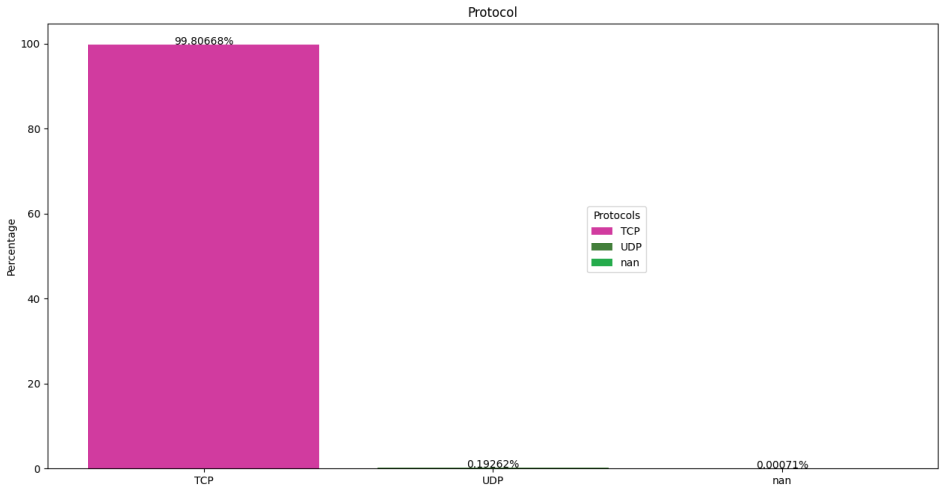
Hình ảnh 37: Chặn một IP nguy hiểm



Hình ảnh 38: Tự động ngăn chặn các IP nguy hiểm



Hình ảnh 39: Thống kê cảnh báo trong file log bằng Python



Hình ảnh 40: Thống kê về thành phần giao thức trong file log bằng Python

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kết luận

- Nhóm đã thành công đáp ứng được mục tiêu đã đề ra, thành công xây dựng, cài đặt website thương mại điện tử với đầy đủ các chức năng cơ bản trên hệ điều hành Linux.
- Nhóm đã tìm hiểu và nắm được các cơ chế, công cụ xây dựng hạ tầng website trên AWS Cloud.
- Nhóm đã phát triển các quy tắc, cách thức phòng chống một số cuộc tấn công thường gặp như XSS, SQL Injection, Path Traversal, DDoS.
- Nhóm đã xây dựng hệ thống phân tích và cảnh báo các cuộc tấn công bằng Snort.
- Tuy các chức năng cơ bản của chương trình hoạt động tốt, nhưng đôi lúc vẫn chưa ổn định và có thể gây ra một vài ngoại lệ.

Hướng phát triển

- Xây dựng hệ thống và website hoàn chỉnh, tối ưu hóa giao diện, độ trễ, khả năng đáp ứng của server và trải nghiệm người dùng.
- Xây dựng tường lửa và các quy tắc một cách tốt hơn để ngăn chặn những cuộc tấn công khác có thể nhắm vào hệ thống trong tương lai.
- Xây dựng hệ thống IPS/IDS, sử dụng các framework và các công cụ khác để bảo vệ hệ thống tốt hơn.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Vĩnh Huế, *Xây dựng hệ thống giám sát và cảnh báo nguy cơ xâm nhập mạng tại trung tâm dữ liệu điện tử tỉnh Quảng Bình*, Luận văn Thạc sĩ – Đại học Bách Khoa – Đại học Đà Nẵng, 2018.

[2] Thạc sĩ Mai Văn Hà, *Bài giảng Công nghệ Web*, tài liệu lưu hành nội bộ, 2017.

[3] Khoa Công nghệ Thông tin – Đại học Bách Khoa – Đại học Đà Nẵng, *Bài giảng Lập Trình Mạng*, tài liệu lưu hành nội bộ, 2022.

[4] Phạm Huy Hoàng, *Bảo mật nhập môn*, toidicodedao.com, 2016.

[5] InterviewBit, *SQL Injection Cheat Sheet*, https://www.interviewbit.com/sql-injection-cheat-sheet/#bypassing-md5-hash-check-login, 18/10/2022.

[6] CheatSheets Series Team, *Cross Site Scripting Prevention Cheat Sheet*, https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html, 05/11/2022.

[7] JavaPipe, *DDoS Protection With Iptables*, https://javapipe.com/blog/iptables-ddos-protection/, 10/11/2022.

[8] Phuong Duong Thi, *Kỹ thuật tấn công XSS và cách ngăn chặn*, https://viblo.asia/p/ky-thuat-tan-cong-xss-va-cach-ngan-chan-YWOZr0Py5Q0, 10/11/2022.

[9] Vũ Tiến Hòa, *Tấn công Path traversal và cách thức phòng thủ*, https://viblo.asia/p/tan-cong-path-traversal-va-cach-thuc-phong-thu-bJzKmO7wl9N, 13/11/2022.

[10] Raj Chandel's Blog, *Detect SQL Injection Attack using Snort IDS*, https://www.hackingarticles.in/detect-sql-injection-attack-using-snort-ids/, 15/11/2022.

PHỤ LỤC