BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Lab 4: Linux Firewall Exploration**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O12.ATCL – Nhóm 03

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Hoàng Trúc Anh | 21521817 | [21521817@gm.uit.edu.vn](mailto:21521817@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520353@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Bài 1 | 100% |
| 2 | Bài 2 | 100% |
| 3 | Bài 3 | 100% |
| 4 | Bài 4 | 100% |
| 5 | Bài 5 | 100% |
| 6 | Bài 6 | 100% |
| 7 | Bài 7 | 100% |
| 8 | Bài 8 | 100% |
| 9 | Bài 9 | 100% |
| 10 | Bài 10 | 100% |
| 11 | Bài 11 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Trình bày ý nghĩa các tham số sử dụng trong 2 lệnh thiết lập tunnel và kết nối telnet ở trên.**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Description automatically generated

* Trong lệnh thiết lập tunnel (ssh -fN -L 8000:localhost:23 penguin@10.0.3.3):

-f: Chạy ssh ở chế độ nền (background).

-N: Không thực hiện lệnh từ xa (no command).

-L 8000:localhost:23: Thiết lập một kênh chuyển tiếp cổng (port forwarding). Ở đây, cổng 8000 trên máy A được chuyển tiếp đến cổng 23 (telnet) trên máy B.

penguin@10.0.3.3: Địa chỉ và tên người dùng của máy B.

* Trong lệnh kết nối telnet (telnet localhost 8000):

localhost: Địa chỉ của máy A.

8000: Cổng được thiết lập để chuyển tiếp thông qua tunnel.

Ý nghĩa chung của quá trình này là thiết lập một tunnel SSH từ máy A đến máy B, và sau đó, sử dụng telnet trên máy A để kết nối đến cổng 8000, nhưng dữ liệu sẽ được chuyển tiếp qua tunnel SSH và đến cổng 23 (telnet) trên máy B.

1. **Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không? Nếu có, nguyên nhân tại sao Firewall không việc sử dụng telnet này? Nếu không, thì kết nối từ máy A đến máy B như thế nào để không đi qua máy Firewall?**

* Các gói tin có này có đi qua firewall, nhưng thay vì đi qua cổng 23 của telnet thì nó đi qua cổng 8000 của SSH tunnel. Do các rule được cài sẵn trên firewall đã chặn cổng 23 của mạng 192.168.3.0/24 nhưng SSH tunnel đã dùng cổng 8000 để thiết lập kết nối nên các gói tin vẫn sẽ đi qua firewall như bình thường mà không bị chặn.
* Các gói tin sau khi đi qua cổng 8000 sẽ được chuyển tiếp đến cổng 23 mà không bị firewall chặn vì kết nối SSH tunnel được mã hóa và không thể bị giám sát hoặc can thiệp bởi Firewall.

1. **Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

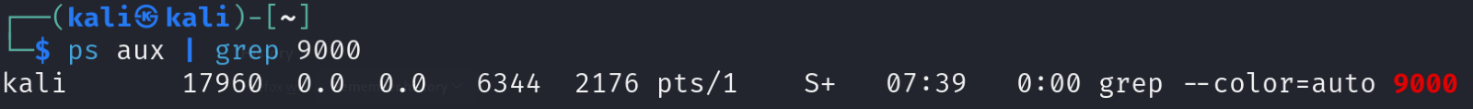
Description automatically generated

Giải thích chi tiết hơn về các cờ được sử dụng trong lệnh:

* “-D 9000”: Cờ này xác định chuyển tiếp cổng cấp ứng "động" cục bộ. Điều này có nghĩa là máy chủ SSH sẽ tự động tạo quy tắc chuyển tiếp cổng mới cho mỗi kết nối được tạo với cổng cục bộ 9000. Sau đó, máy chủ SSH sẽ chuyển tiếp các kết nối này đến máy từ xa có địa chỉ IP là 10.0.3.3. Điều này rất hữu ích cho việc truyền tải lưu lượng không có số cổng cố định, chẳng hạn như lưu lượng HTTP.
* “-C”: Cờ này xác định rằng dữ liệu nên được nén trước khi được truyền qua kết nối SSH. Điều này có thể giúp giảm lượng băng thông được sử dụng, điều này có thể quan trọng đối với các kết nối qua mạng chậm hoặc tốn kém.
* “penguin@10.0.3.3”: Điều này xác định tên máy chủ từ xa và địa chỉ IP để kết nối đến. Trong trường hợp này, tên máy chủ là "penguin" và địa chỉ IP là 10.0.3.3.

Vì vậy, tóm lại, lệnh này đang thiết lập proxy SOCKS trên máy cục bộ tại cổng 9000. Proxy SOCKS này sẽ chuyển tiếp tất cả lưu lượng truy cập đến máy từ xa có địa chỉ IP là 10.0.3.3, thông qua đường hầm SSH được mã hóa dưới dạng người dùng penguin.

1. **Thực hiện ngắt SSH Tunnel, xoá cache của trình duyệt và truy cập lại trang www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?**

Tắt SSH Tunnel và xoá cache của trình duyệt   
  
A screenshot of a computer error

Description automatically generated

Truy cập lại trang web facebook:

A screenshot of a computer

Description automatically generated

Kết quả: sau khi ngắt tunnel và xóa cache thì không đến được trang, do lúc này việc kết nối sẽ trở về là thông qua tường lửa pfsense, và bị filter nên không thể kết nối đến

1. **Nếu trên Firewall, áp dụng rule chặn kết nối SSH (port 22), lúc này có thể thiết lập tunnel này được hay không? Tại sao?**

Tạo 1 rule chặn kết nối ssh ở port 22

A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated

Sau khi tạo rule thì sẽ không thực hiện được kết nối ssh / tunnel nữa, vì lúc nãy việc kết nối ssh là trên port 22, đúng với rule block là chặn ssh trên port 22 của pfSense nên việc ssh là không thể.

1. **Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát của Firewall trong trường hợp trên.**

Có nhiều giải pháp để ngặn chặn việc bypass fw , tuy nhiên nhóm sẽ đề xuất các giải pháp triển khai trên PfSense :  
- Kiểm soát Cổng và Giao Thức SSH:

Hạn chế cổng SSH chỉ cho phép kết nối từ máy A đến máy B.  
Sử dụng một cổng SSH không phổ biến hoặc đặt một cổng khác ngoài cổng mặc định (ví dụ: không sử dụng cổng 22).  
Sử dụng giao thức TCP Wrapper để chỉ cho phép các địa chỉ IP cụ thể kết nối vào cổng SSH.

-Thiết lập Quy tắc Tường lửa Nghiêm ngặt:

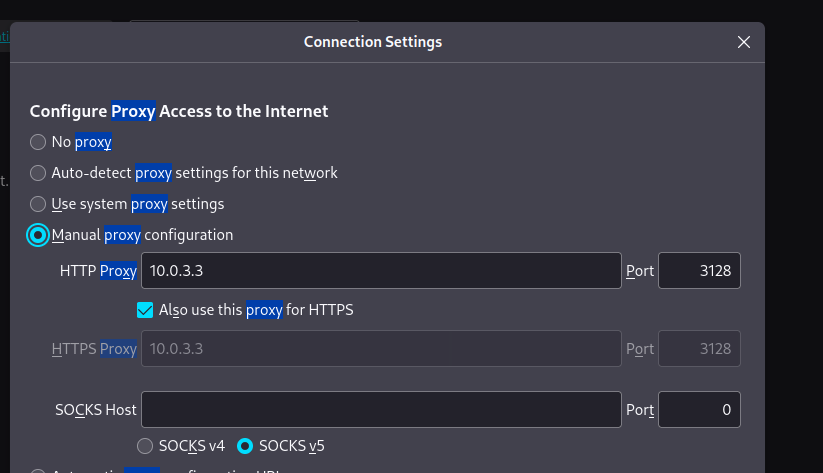
Xây dựng quy tắc tường lửa chặt chẽ để chỉ cho phép lưu lượng cần thiết đi qua.  
Chặn lưu lượng đến và từ các cổng SSH không an toàn hoặc không mong muốn.  
Cấu hình logging để theo dõi những truy cập bị chặn.

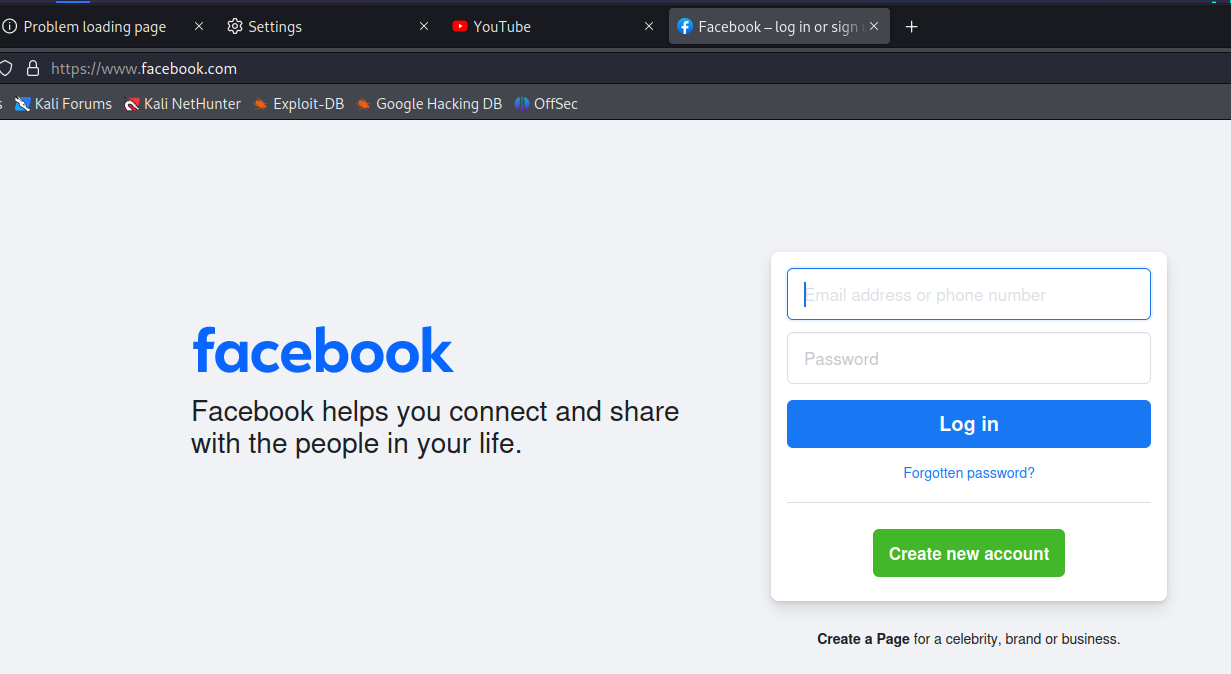
-Sử dụng Hệ Thống IDS/IPS:

Cài đặt và cấu hình một hệ thống IDS/IPS trên pfSense để theo dõi các mô hình hoạt động đáng ngờ.  
Tích hợp các luật chặn hoặc cảnh báo để ngăn chặn hoặc báo cáo về việc sử dụng SSH tunneling.  
Đảm bảo rằng cơ sở dữ liệu luật IDS/IPS được cập nhật đều đặn để nhận biết các mô hình tấn công mới.

1. **Đoạn chương trình script.pl trên hoạt động như thế nào?**

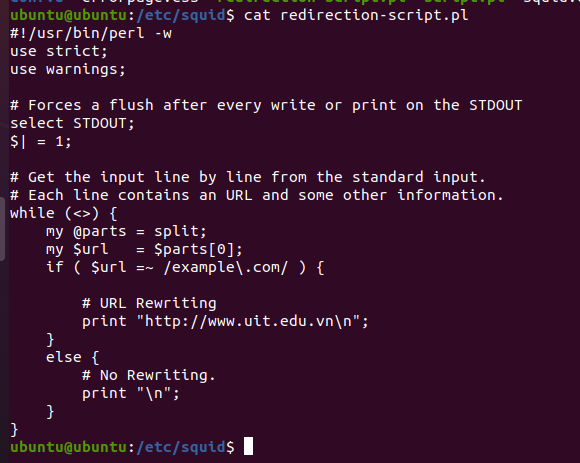
Chuẩn bị:





Lí do mà sau khi dùng proxy thì vma có thể truy cập vào facebook.com bởi vì dataflow lúc này chuyển hướng trực tiếp từ vma->proxy->vmb , không có qua fw pfsense nên không bị chặn

Code



+) Sử dụng strict và warnings để áp dụng các quy tắc nghiêm ngặt và cảnh báo trong mã. select STDOUT; $| = 1; để bật chế độ tự động xóa đệm và làm cho đầu ra (STDOUT) ngay lập tức hiển thị trên màn hình.

+) Sử dụng vòng lặp vô hạn “while (<>)” để đọc từng dòng từ đầu vào chuẩn.

+) Sử dụng split để chia dòng thành các phần, lưu vào mảng @parts.

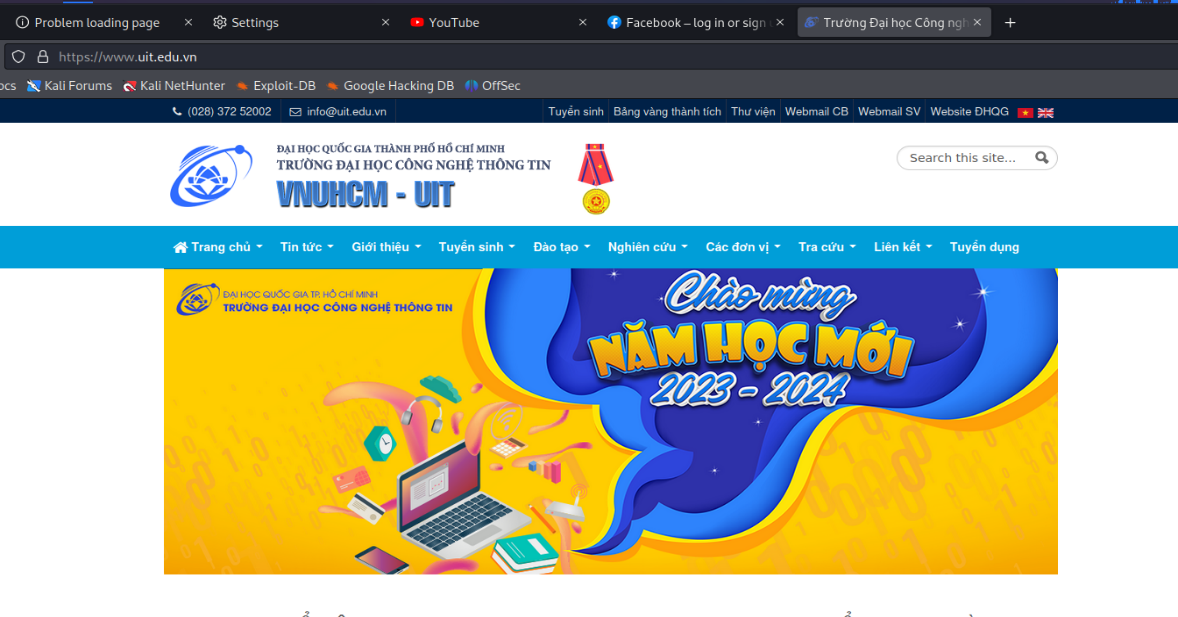
+) Lấy URL từ phần tử đầu tiên của mảng @parts.

+) Kiểm tra xem URL có chứa chuỗi "example.com" hay không. Nếu URL chứa "example.com", chương trình in ra URL mới "<http://www.uit.edu.vn>".

Nếu không, in ra một dòng trống.

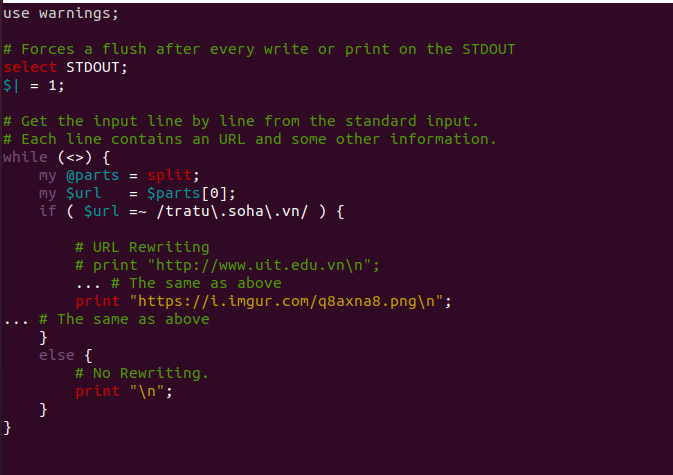
à Khi ta truy cập vào một trang web, vòng lặp while này sẽ chia nhỏ từng phần của request và viết lại url “example.com” để chuyển hướng tới trang “uit.edu.vn”, nếu không phải url “example” thì vẫn tới trang web gốc

Dùng 1 trang web http khác thay cho <http://example.com> => <http://tracuu.soha.vn>



1. **Thay đổi nội dung đoạn chương trình trên để khi truy cập vào website example.com, một hình ảnh cảnh báo dừng lại xuất hiện (như hình dưới).**

Code

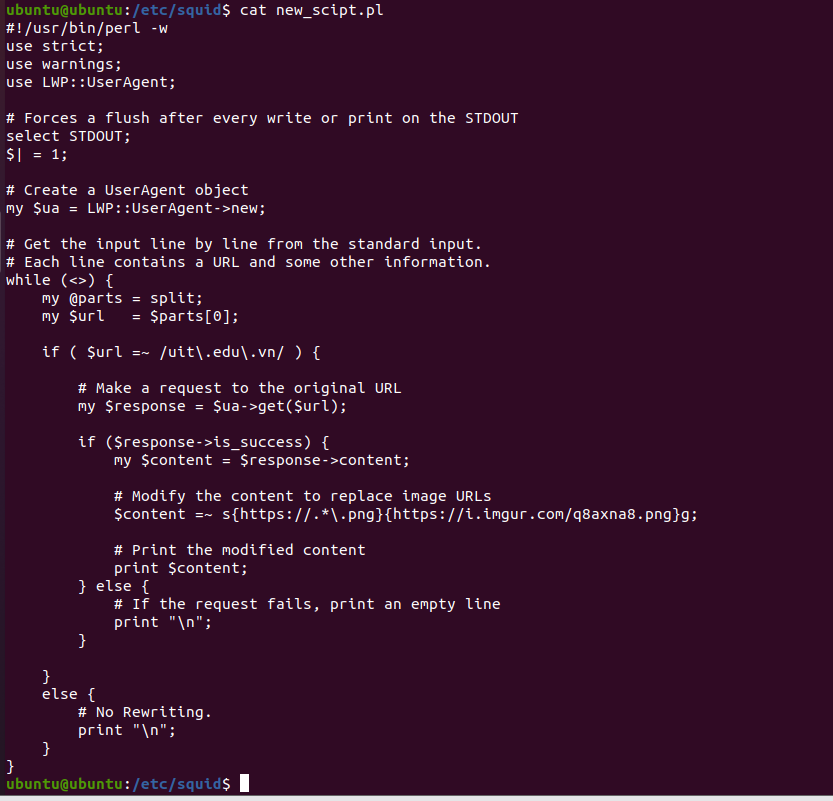


Kết quả

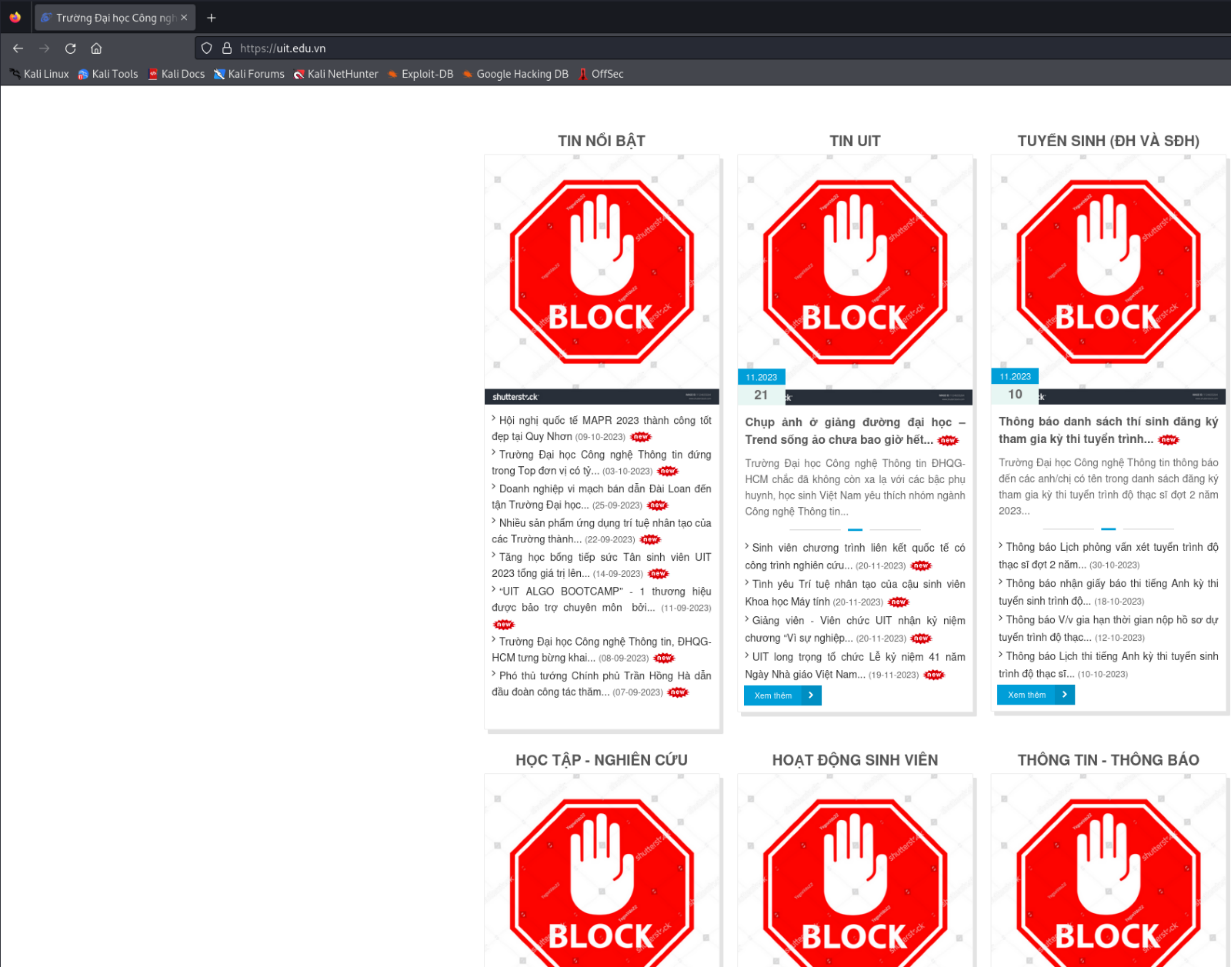


1. **Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh bạn thích (như hình minh hoạ dưới).**

**Code**



Kết quả



1. **Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức này có đặc điểm gì khác nhau?**

pfSense là một hệ thống tường lửa mã nguồn mở được thiết kế để chạy trên máy tính chủ thông dụng hoặc thiết bị nhúng để cung cấp các tính năng tường lửa và VPN. pfSense hỗ trợ một số giao thức thiết lập kết nối VPN phổ biến, bao gồm:

* OpenVPN: Đây là một giao thức VPN mã nguồn mở và linh hoạt. Nó sử dụng một giao thức SSL/TLS cho việc mã hóa và chứng thực. OpenVPN có thể chạy trên nhiều cổng và có thể sử dụng TCP hoặc UDP.
* IPsec: IPsec là một giao thức VPN tiêu chuẩn được sử dụng rộng rãi trong việc xây dựng các kết nối VPN site-to-site và remote access. Nó cung cấp một cơ chế mạnh mẽ cho việc bảo vệ dữ liệu truyền qua mạng.
* L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec): Kết hợp giữa L2TP và IPsec để tạo ra một kết nối VPN an toàn. L2TP tạo ra một kênh truyền dữ liệu, trong khi IPsec đảm bảo tính bảo mật của thông tin truyền qua kênh đó.
* PPTP (Point-to-Point Tunneling Protocol): Mặc dù không được khuyến khích sử dụng do những vấn đề liên quan đến bảo mật, nhưng pfSense vẫn hỗ trợ PPTP. PPTP cung cấp một cách đơn giản để thiết lập kết nối VPN.

Mỗi giao thức có những đặc điểm khác nhau:

* OpenVPN: Linh hoạt, mã nguồn mở, hỗ trợ nhiều cổng và có thể chạy trên cả TCP và UDP. Thường được coi là lựa chọn ưu tiên trong môi trường doanh nghiệp.
* IPsec: Mạnh mẽ, được sử dụng rộng rãi trong các kịch bản kết nối site-to-site. Thích hợp cho môi trường doanh nghiệp với nhu cầu bảo mật cao.
* L2TP/IPsec: Kết hợp tính năng của cả L2TP và IPsec, tạo ra một kết nối VPN an toàn, phù hợp cho nhiều ứng dụng.
* PPTP: Dễ cấu hình, nhưng ít được ưa chuộng do vấn đề bảo mật. Không nên sử dụng trong các môi trường đòi hỏi tính an toàn cao.

1. **Tìm hiểu và thực hiện cấu hình trên pfSense, sao cho từ máy VM B có thể mở kết nối VPN đến pfSense server để truy cập được máy VM A.**

Đăng nhập Pfsense, tìm đến mục System và chọn Certificate -> chọn Authorities -> nhấn vào Add. Đặt tên và chọn Key type là ECDSA, rồi nhấn Save.

A screenshot of a computer

Description automatically generated

Trong mục System, chọn Certificate -> chọn Certificates -> nhấn vào Add/Sign. Đặt tên, chọn Key type là ECDSA, và đặt Common Name rồi nhấn Save

A screenshot of a computer

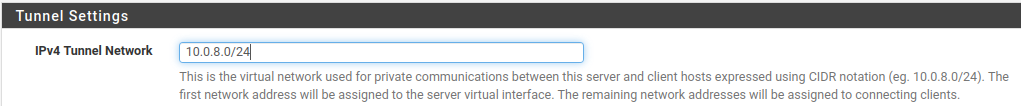
Description automatically generated

Chọn mục VPN -> chọn OpenVPN ->Chọn Wizard thì sẽ hiện ra hình bên dưới. Để cấu hình mặc định và bấm Next cho tới khi hiện “Step 9 of 11”.

A screenshot of a computer

Description automatically generated

Tìm mục Tunnel Settings và chọn mạng 10.0.8.0/24, rồi bấm Next



Chọn cả 2 mục Firewall Rule và OpenVPN rule, rồi nhấn Next -> nhấn Finish

A screenshot of a computer

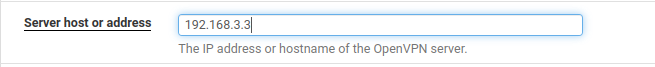
Description automatically generated

Chọn mục VPN -> chọn OpenVPN -> chọn Clients -> nhấn Add

A screenshot of a computer

Description automatically generated

Cấu hình theo địa chỉ IP tương ứng



Chọn Username và Password

A screenshot of a computer

Description automatically generated

Chọn mục System -> chọn Package Manager -> chọn Available Package -> chọn Install -> Chọn Confirm

A screenshot of a computer

Description automatically generated

Chọn System -> chọn User Manager -> chọn Users -> chọn Add. Chọn Username, Password và tên của người dung, rồi chọn ô Click to create a user certificate.

A screenshot of a computer

Description automatically generated

Chọn tên certificate, chọn Key type là ECDSA, rồi nhấn Save

A screenshot of a computer

Description automatically generated

Tải OpenVPN:

*sudo apt install openvpn*

*sudo systemctl restart openvpn*

Kết nối VPN:

*sudo openvpn --auth-user-pass --config Desktop/pfSense-UDP4-1194-vpn-config.ovpn*

Nhập username và password.

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên nộp bài theo thời gian quy định trên course.

**Báo cáo:**

* File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
* Đặt tên theo định dạng: **[Mã lớp]-AssignmentX\_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

*Ví dụ: [NT521.O11.ATCL]-Assignment01\_Nhom03.pdf.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)