BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 05 (Session 05)**

**Tên chủ đề: Khai thác tường lửa**

**trong Linux**

*GV: Trần Nguyễn Đức Huy*

*Ngày báo cáo: 4/1/2022*

**Nhóm: 05**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT101.N12.ATCL.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Vũ Hoàng Thạch Thiết | 20521957 | 20521957@gm.uit.edu.vn |
| 2 | Nguyễn Hùng Thịnh | 20521963 | 20521963@gm.uit.edu.vn |
| 3 | Dương Đỗ Khoa | 20521465 | 20521465@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Câu 1 | 100% |
| 2 | Câu 2 | 100% |
| 3 | Câu 3 | 0% |
| 4 | Câu 4 | 0% |
| 5 | Câu 1 | 100% |
| 6 | Câu 2 | 100% |
| 7 | Câu 3 | 0% |
|  | Câu 4 | 0% |
|  | Câu 5 | 0% |
|  | Câu 6 | 100% |

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

MỤC LỤC

[A. BÁO CÁO CHI TIẾT 3](#_Toc122620308)

[Câu 1: 3](#_Toc122620309)

[Câu 2: 4](#_Toc122620310)

[Câu 3: 5](#_Toc122620311)

[Câu 4: 5](#_Toc122620312)

[Câu 1: 5](#_Toc122620313)

[Câu 2: 5](#_Toc122620314)

[Câu 3: 6](#_Toc122620315)

[Câu 4: 6](#_Toc122620316)

[Câu 5: 6](#_Toc122620317)

[Câu 6: 6](#_Toc122620318)

[B. TÀI LIỆU THAM KHẢO 6](#_Toc122620319)

[**YÊU CẦU CHUNG** 7](#_Toc122620320)

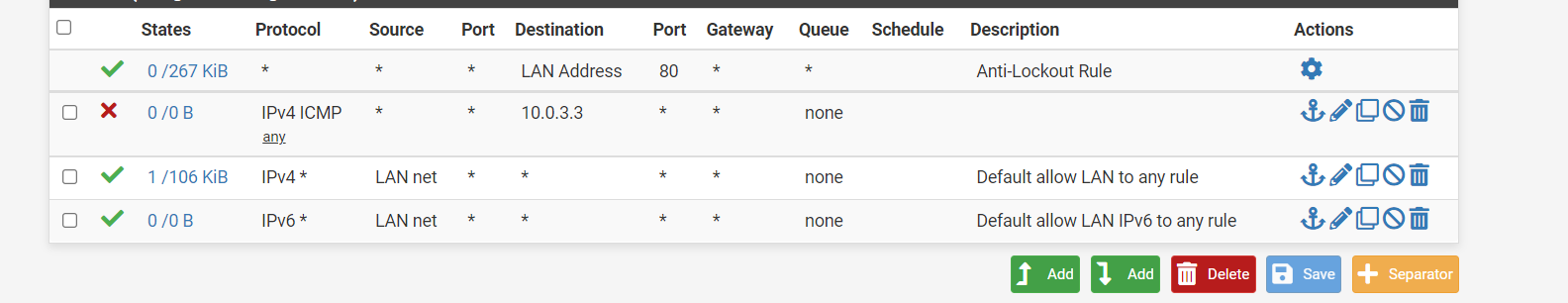
# BÁO CÁO CHI TIẾT

## Câu 1:

#### **Câu hỏi:**

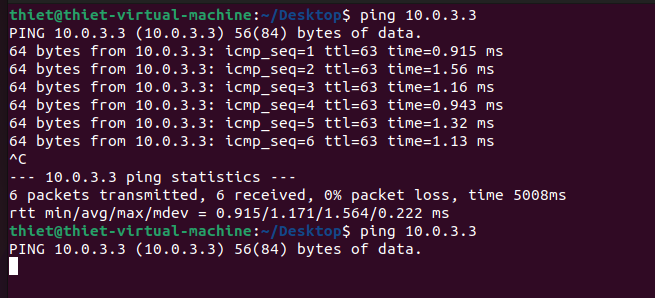
Không cho phép các máy trong mạng nội bộ (192.168.3.0/24) thực hiện ping đến máy VM B.

#### **Trả lời:**



Hình . Rule chặn mạng nội bộ (192.168.3.0/24) ping đến máy B

* Ban đầu, khi disable rule thì máy A có thể ping đến máy B
* Sau khi enable rule thì máy A không thể ping đến máy B



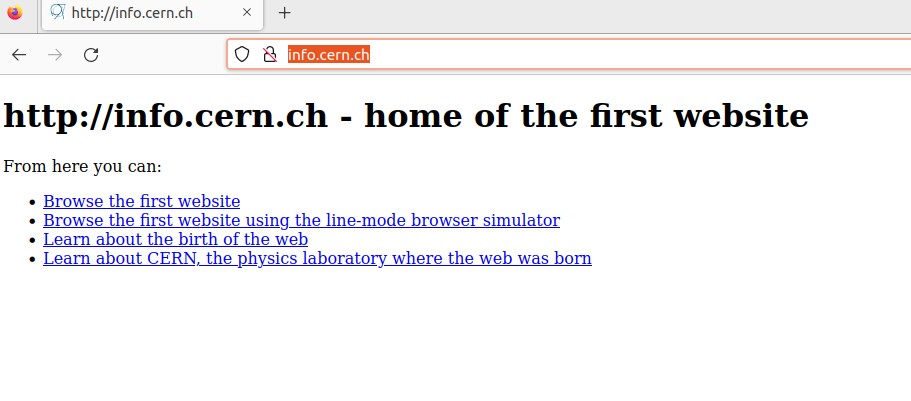
Hình . Khi enable rule thì máy A không thể ping đến máy B

## Câu 2:

#### **Câu hỏi:**

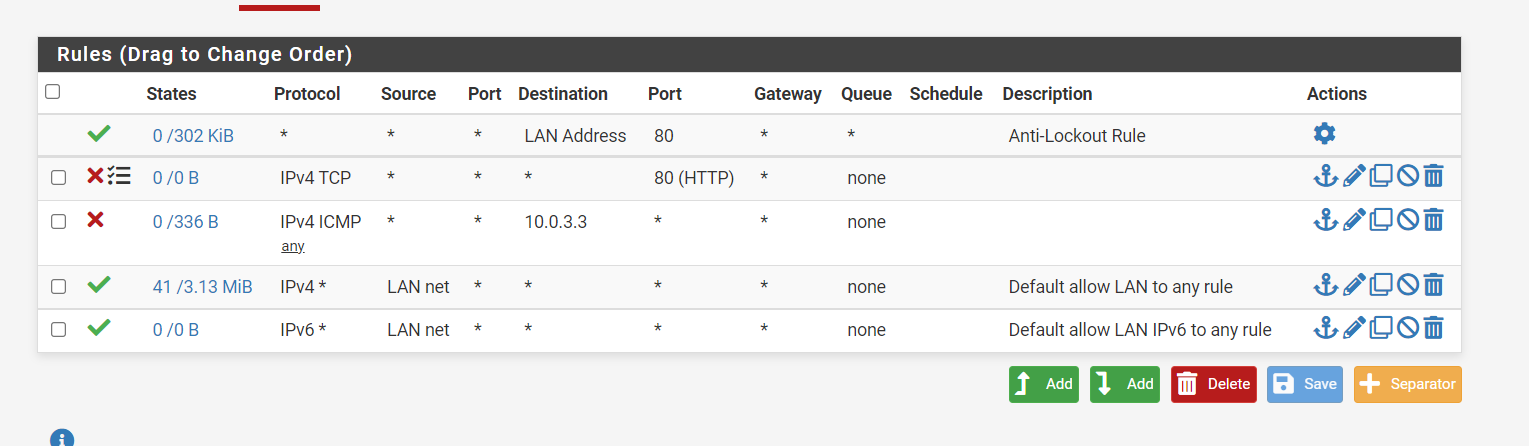
Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao thức http (cổng 80)

#### **Trả lời:**

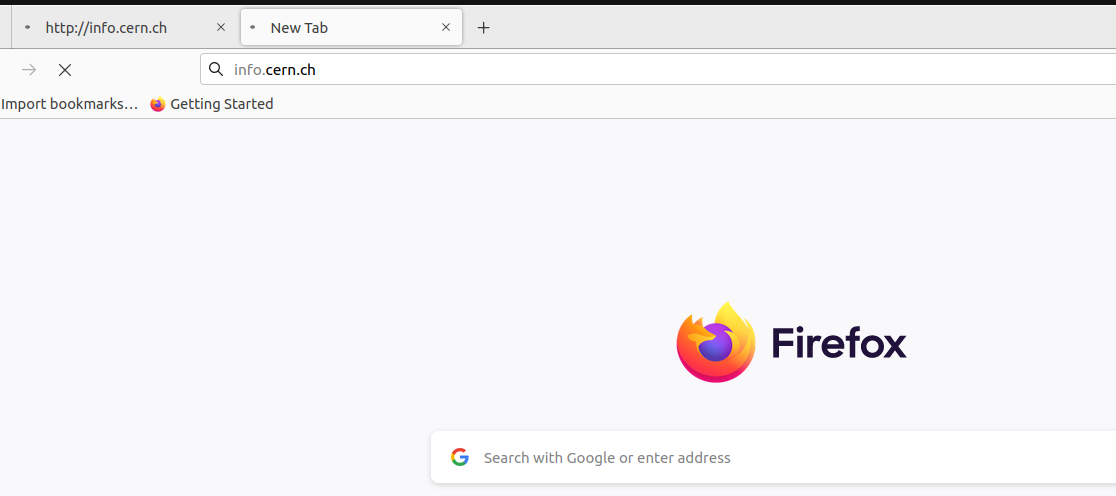
* Ban đầu ta truy cập thành công vào trang http://info.cern.ch

Hình . Truy cập thành công vào web http://info.cern.ch

* Sau khi bật rule chặn port 80, thì không thể truy cập vào các trang http nữa.



Hình . Thiết lập rule chặn truy cập web http port 80



Hình . Không thể truy cập vào trang http

## Câu 3:

#### **Câu hỏi:**

Chặn kết nối telnet từ mạng nội bộ ra bên ngoài.

#### **Trả lời:**

## Câu 4:

#### **Câu hỏi:**

Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và

youtube.com.

#### **Trả lời:**

## Câu 1:

#### **Câu hỏi:**

Trình bày ý nghĩa các tham số sử dụng trong 2 lệnh thiết lập tunnel và kết nối

telnet ở trên

#### **Trả lời:**

- Chuyển tiếp cổng 23 trên máy VMB về cổng 8000 trên máy VMA

## Câu 2:

#### **Câu hỏi:**

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 chặn 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?

#### **Trả lời:**

- Khi sử dụng telnet thực chất các gói tin này không đi qua firewall. Máy A kết nối đến máy B thông qua SSH tunnel lúc này mọi kết nối đến máy local host đều sẽ tương đương với máy B với port 23.

## Câu 3:

#### **Câu hỏi:**

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

#### **Trả lời:**

## Câu 4:

#### **Câu hỏi:**

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?

#### **Trả lời:**

## Câu 5:

#### **Câu hỏi:**

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?

#### **Trả lời:**

## Câu 6:

#### **Câu hỏi:**

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

#### **Trả lời:**

- Giám sát, kiểm soát và kiểm tra các kết nối SSH được mã hóa.

- Cấu hình phù hợp và tăng cường bảo mật hệ điều hành

# TÀI LIỆU THAM KHẢO

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo 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 báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*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-1)