

**Đồ án CDIO**

**CMU-CS 447 BIS**

**BÁO CÁO NHÓM**

**Hệ thống mô phỏng tấn công – phòng thủ trên không gian mạng máy tính**

**GIÁO VIÊN HƯỚNG DẪN: Nguyễn Thị Anh Đào**

**NHÓM SINH VIÊN THỰC HIỆN:**

**NGUYỄN VĂN TUẤN - 26211136259**

**NGÔ HẢI LONG - 26211125106**

**NGUYỄN ĐỨC PHÚ - 26211100755**

**NGUYỄN QUANG MINH - 26211135153**

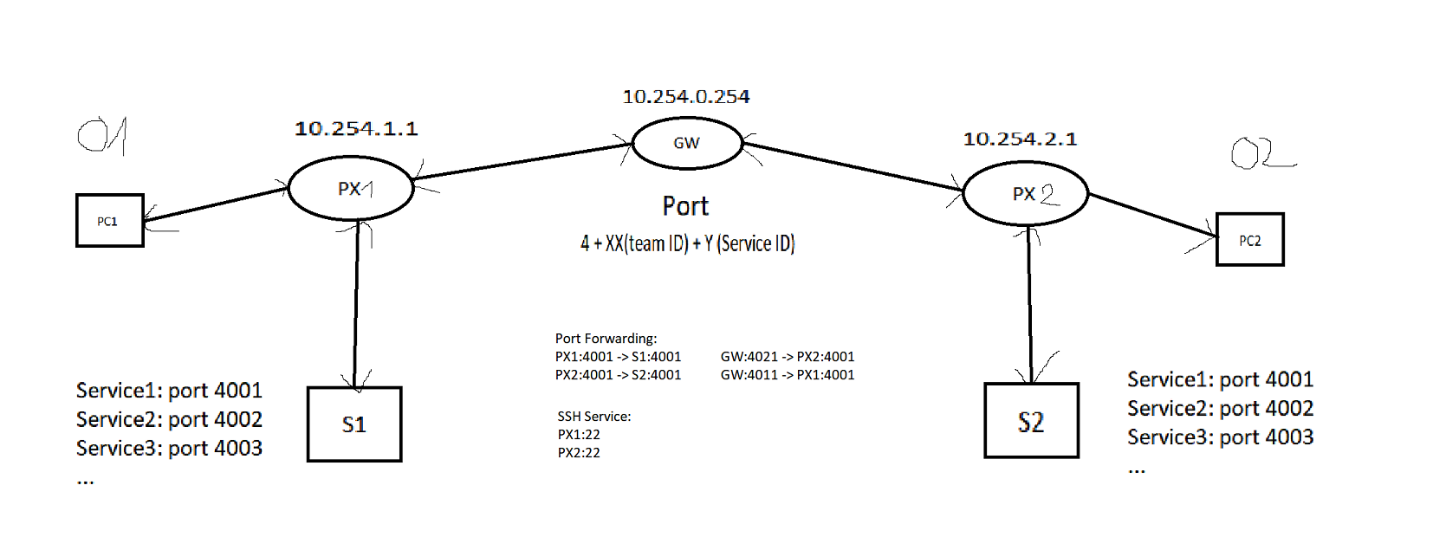
1. **Ý tưởng**

Dựng một hệ thống mô phỏng tấn công phòng thủ phục vụ cho việc diễn tập, luyện tập về an toàn thông tin cho sinh viên và doanh nghiệp.

Quy trình xây dựng hệ thống bao gồm:

* Thiết kế mô hình mạng.
* Xây dựng server với các giao thức kết nối cần thiết.
* Bổ sung các services.
* Xây dựng các kịch bản tấn công – phòng thủ
* Dựng hệ thống demo.

1. **Sơ đồ hệ thống:**



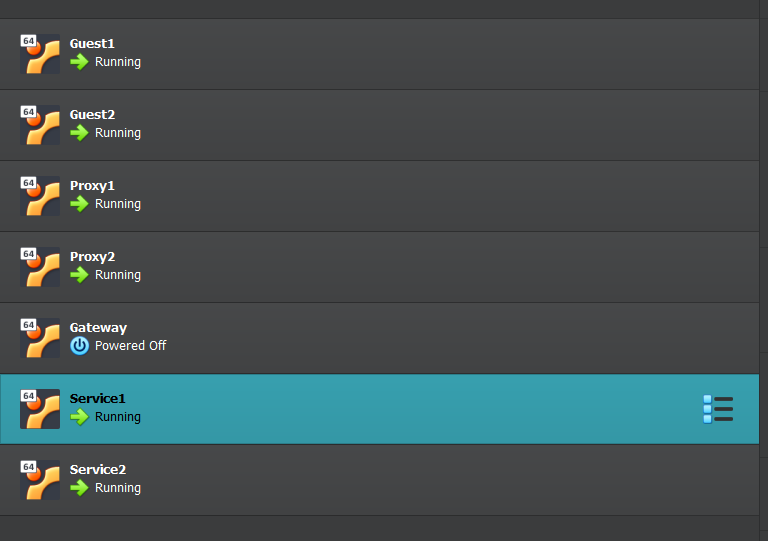
Sơ đồ hệ thống

S1, S2: Server chứa các services, tương ứng các port 4001, 4002, 400x, … cho các services.

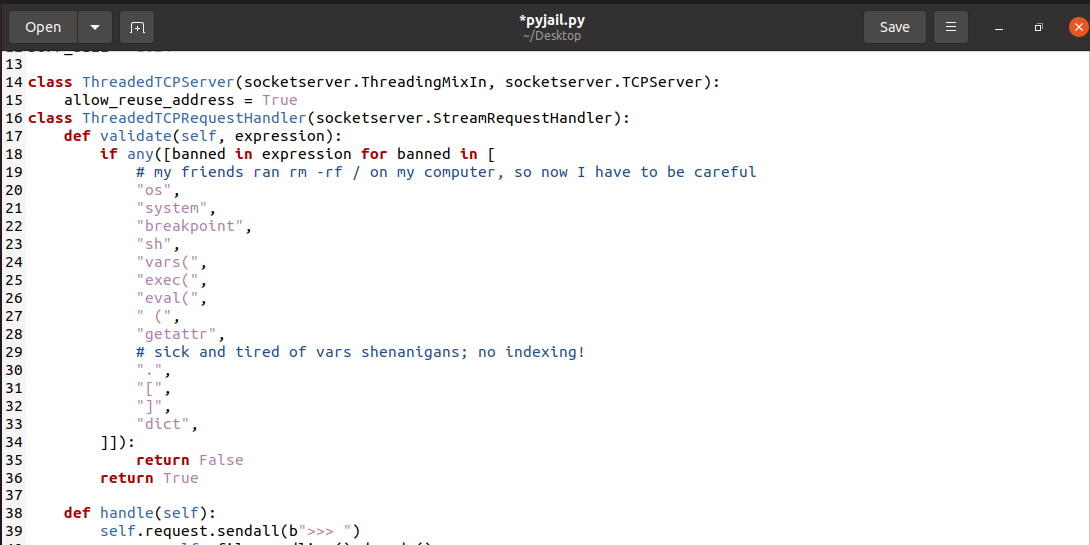
PX1, PX2: 2 máy Proxy dùng để kết nối đến các service.

PC1, PC2: máy của người chơi 2 bên.

GW: Gateway nơi các luồng thông tin được điều phối



1. **Các services**
2. Pyjail

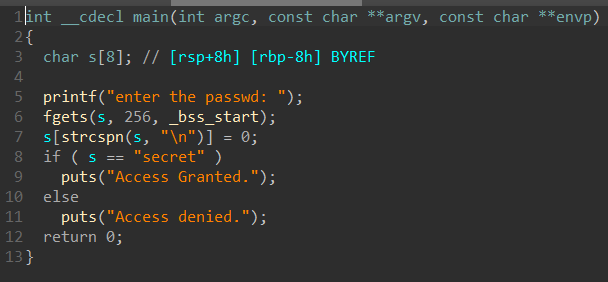


Service này là một máy tính (calculator) viết bằng python, có các filter để tránh bị hacker lợi dụng thực thi lệnh hệ thống.

Port 4001.

1. Buffer 1

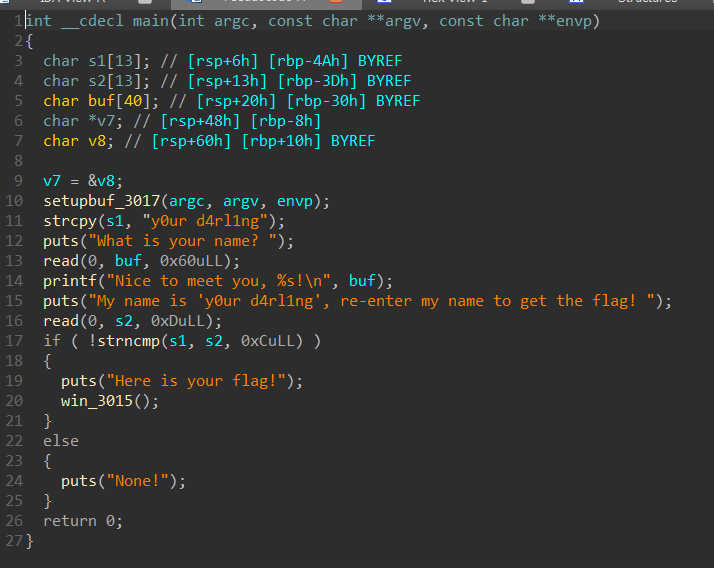
Service kiểm tra password, có lỗ hổng buffer over flow.



Port 4002

1. Buffer 2

Service yêu cầu nhập tên



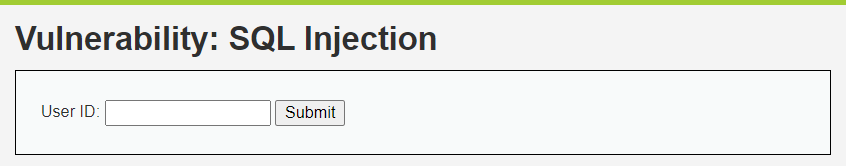
Port 4003

1. Vulnerable web application – DVWA

Web service

Port 80

API: vulnerabilities/sqli/ security level=low



Exploit query: 'union select user, password from users# -> sẽ dump toàn bộ username, password ở table users ()

Các API khác và cách khai thác từng lỗ hổng được viết ở

https://past-smelt-d6d.notion.site/LAB-DVWA-0083a1e20b5d447ea3e9245739c636b7

1. **Quá trình thực hiện**

Tuần 1: bàn bạc và đưa ra được mô hình phù hợp, từ đó viết các requirements.

Tuần 2: Dựng các máy gateway và proxy, thiết lập ssh

Tuần 3: Tiếp tục thiết lập ssh và port forwading, build các vulnerable services, config rule cho Network

Tuần 4: Hoàn thiện port forwarding + ssh tunneling, đưa các service lên VM, dựng các kịch bản, test cases.

Tuần 5: Hoàn thiện trên toàn bộ hệ thống.

1. **Chức năng còn thiếu**

Supervisor, scoreboard