

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO THỰC HÀNH

**TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG**

**Bài thực hành số 1:**

**DÒ QUÉT LỖ HỔNG VÀ**

**KHAI THÁC MỘT SỐ LỖ HỔNG PHỔ BIẾN**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

**Lớp:** AT17G

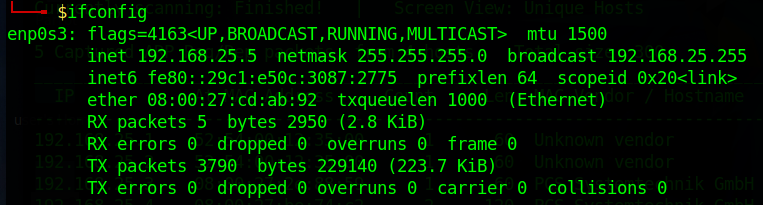
**Thời gian nộp bài:** 29/12/2023

***Giảng viên hướng dẫn****:* Phạm Minh Thuấn

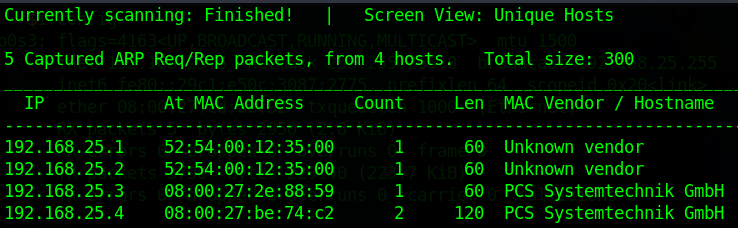
Hà Nội, 29-12-2023

# Khai thác

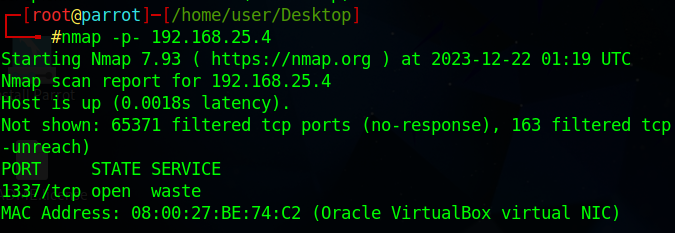
Địa chỉ ip của parrot:



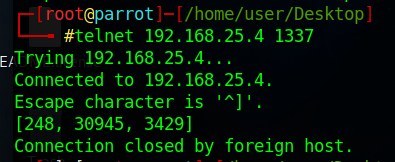
Quét các cổng để tìm máy nạn nhân (KnockKnock):



Nmap ip 192.168.25.4 để xem các dịch vụ , phiên bản, hệ điều hành:

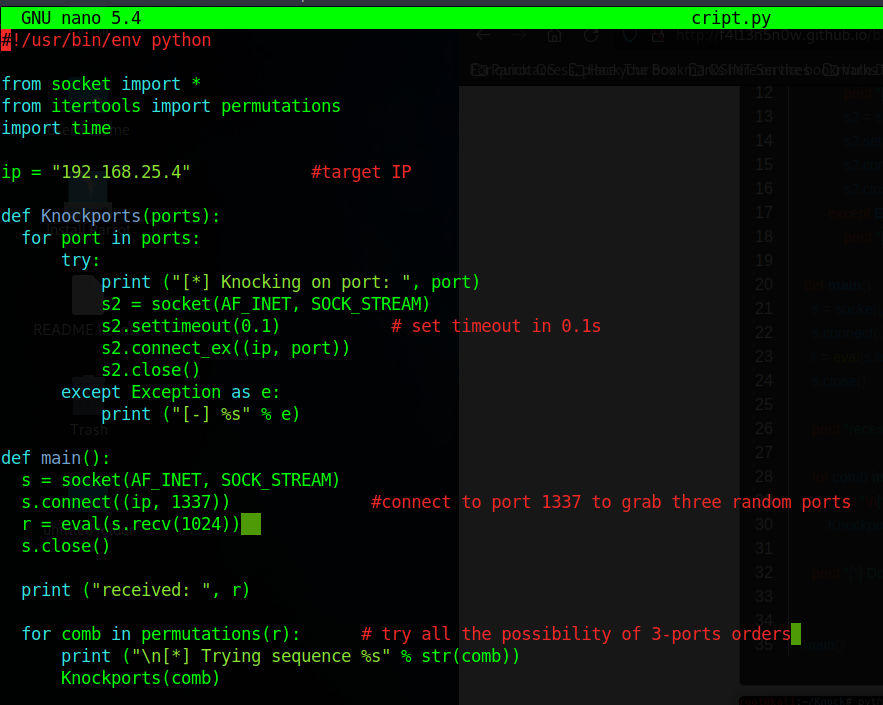


Kết nối với port 1337 không thành công

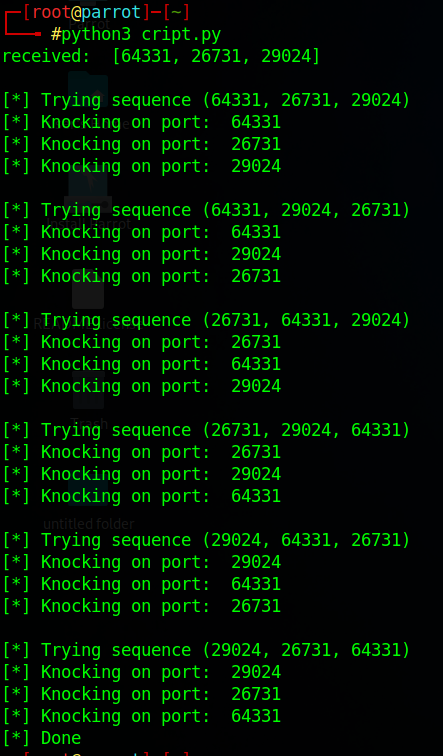


Dùng kỹ thuật port knocking, cho phép giấu đi các port và hầu như phương thức giải đố, phải đúng yêu cầu thì mới có thể mở port thực sự hoạt động

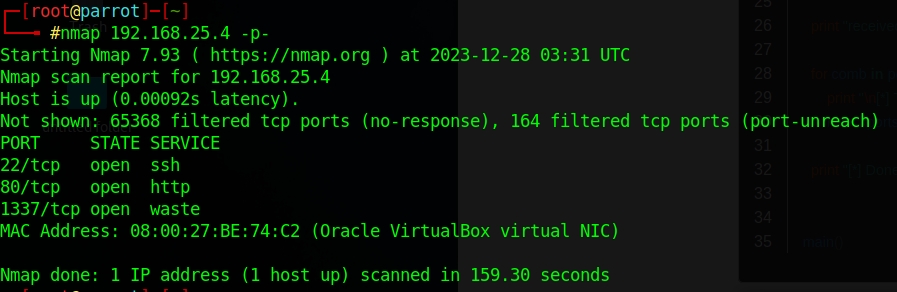
Từ đó ta cần 1 script để làm điều này



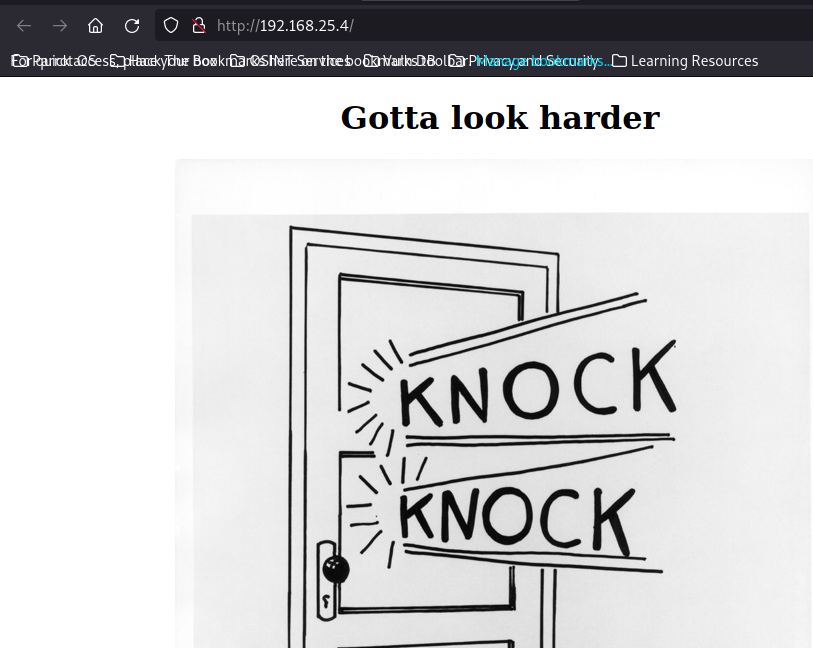
Chạy script



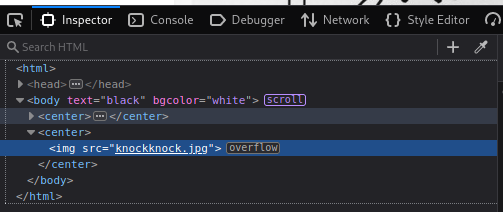
Kiểm tra xem port 1337 mở không



Xem trang knock knock



Xem mã nguồn của trang



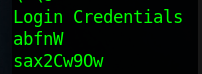
Tải ảnh knockknock về



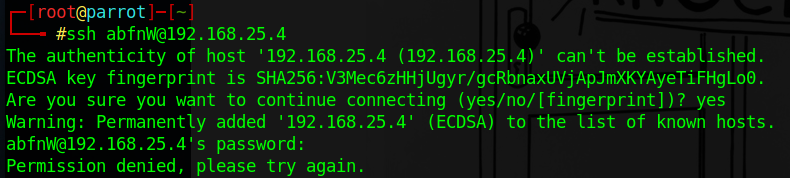
Giải mã ảnh



Có user, password

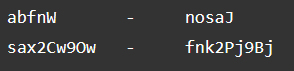


Đăng nhập không thành công

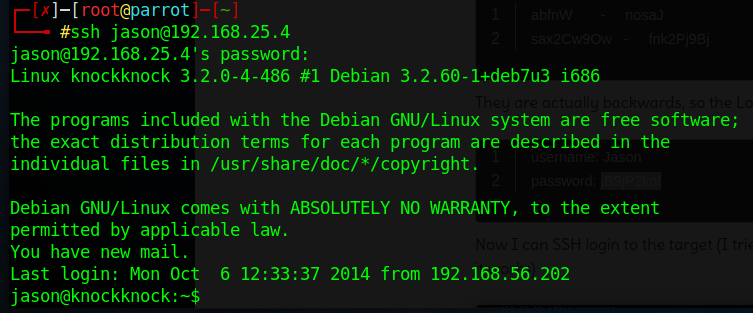


User, password đã bị reverse ta dùng ROT13 để decode và rev nó để có thể sử dụng được

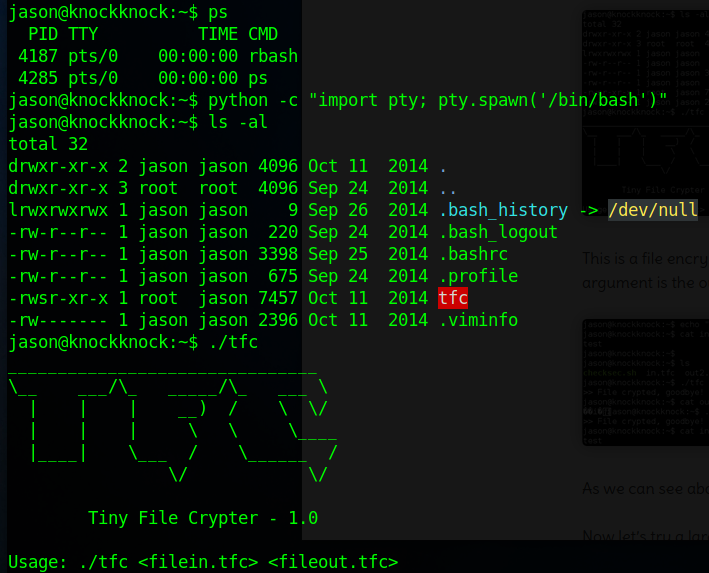
Sau khi giải mã:



Kết nối thành công



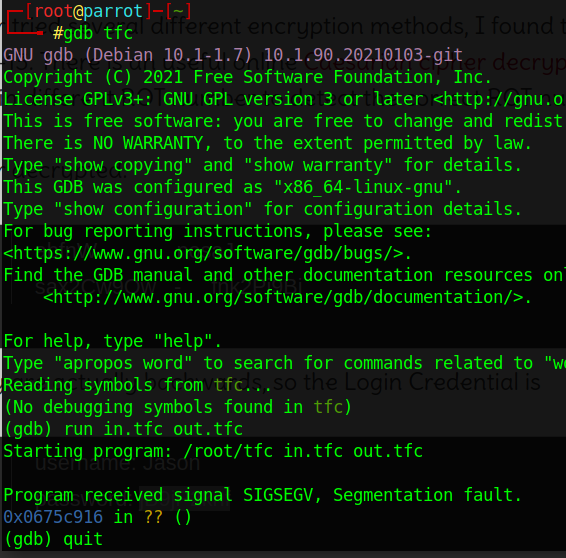
Xem file có trong máy knockknock



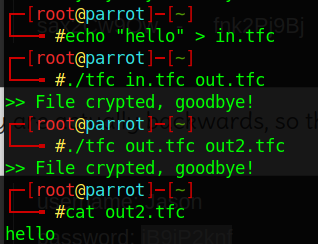
Chuyển file tfc về máy attack



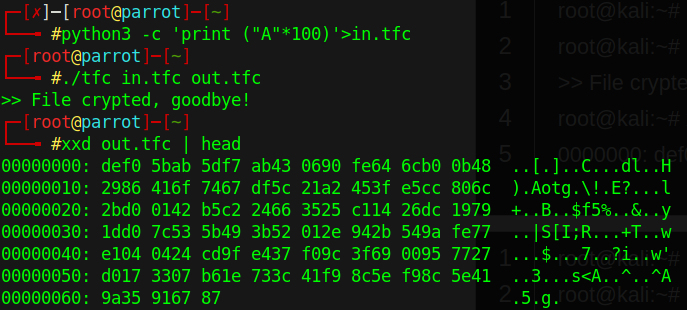
Biên dịch file tfc => Có thể thấy dữ liệu 0x0675c916 khả nghi



Việc đưa 1 input ban đầu sau khi mã hóa và mã hóa thêm 1 lần thì trở về input ban đầu => Thuật toán khóa không bị xáo trộn và trở về ban đầu khi encrypt chính mã hóa ban đầu

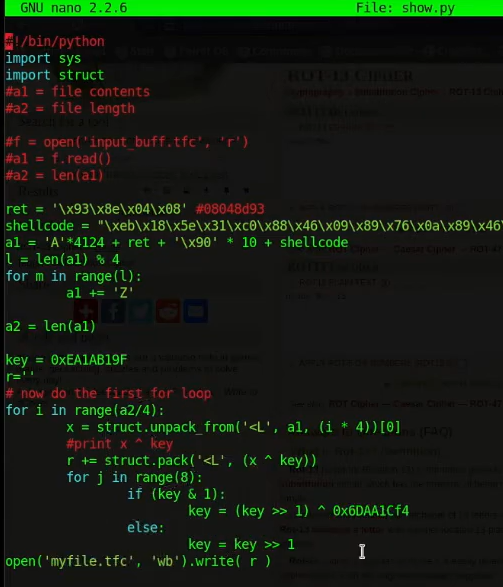


Thử hạ độ dài xem có mã hóa được không

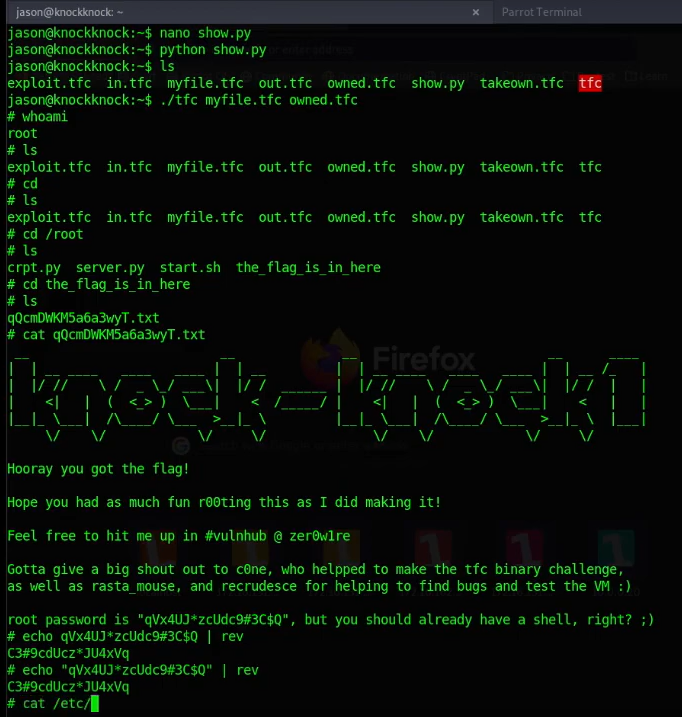


Ta cần 1 shwll để tạo ra nó





Ta có thể chiểm quyền root



Tạo backdoor bằng việc add key ssh vào để lần sau login vào root

