

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

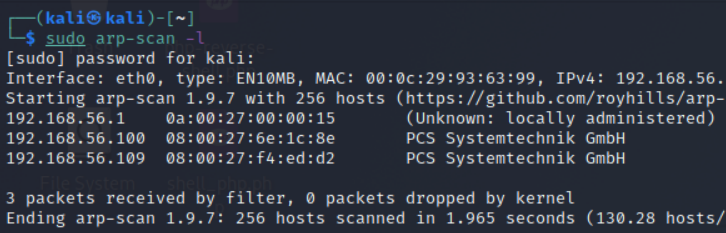
***Giảng viên hướng dẫn****:* Phạm Minh Thuấn

Hà Nội, 29-12-2023

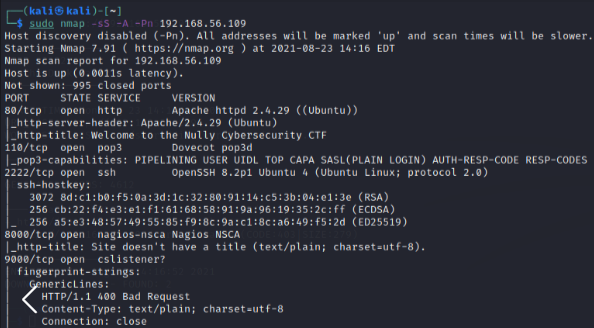
# Khai thác

Địa chỉ IP kali: 192.168.56.102

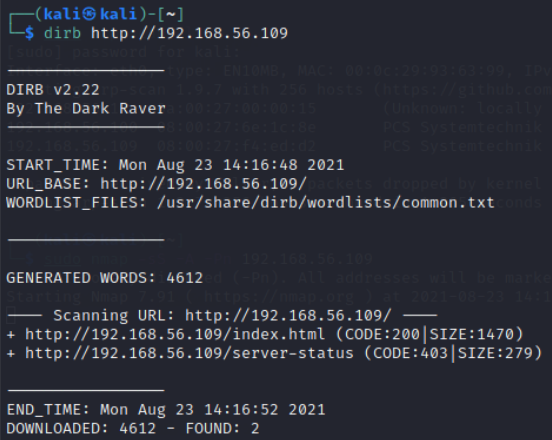
Quét cổng mạng:



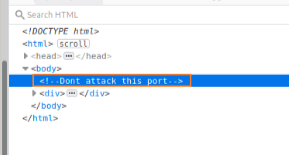
Quét ip 192.168.56.109 thấy 5 cổng mở: 80, 110, 2222, 8000, 9000



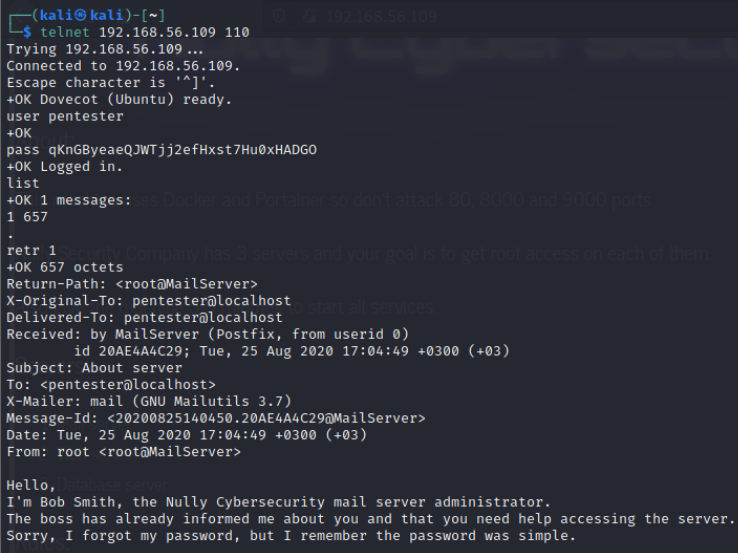
Xem thư mục web cổng 80



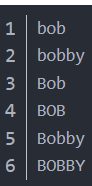
Xem source web



Đăng nhập bằng cổng pop3 mail server



Tạo danh sách người dùng user.txt

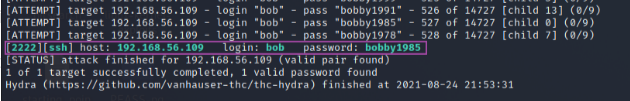


Tạo danh sách mật khẩu

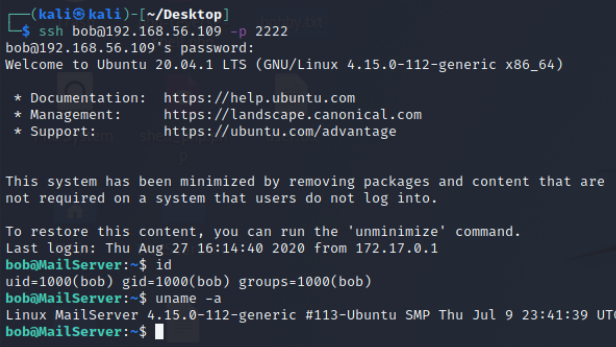


Sử dụng hydra để lấy tên người dùng và mật khẩu

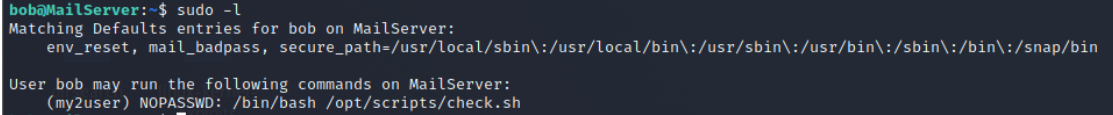




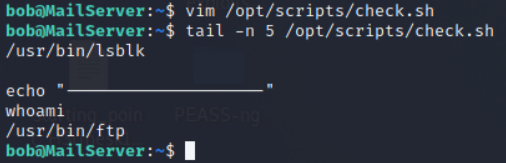
Kết nối ssh và lấy shell thành công



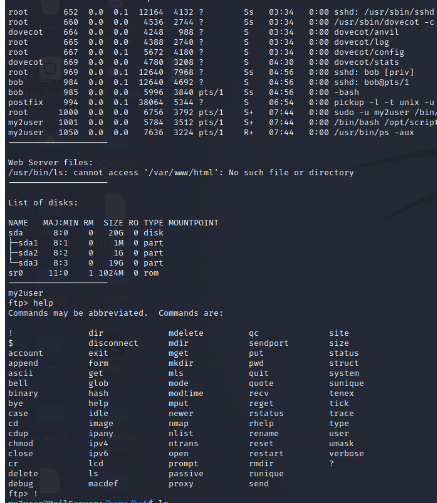
Thực hiện lệnh và thấy người dùng có thể chạy để chuyển đổi sang sudo -l my2user check.sh



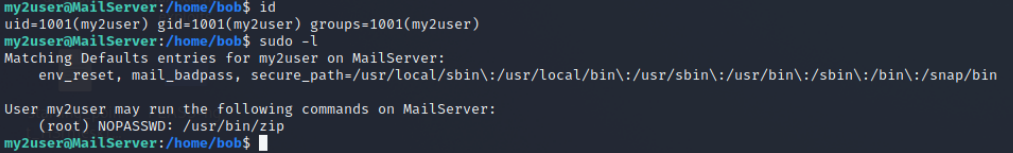
Thêm lệnh vào check.sh whoami /user/bin/ftp



Chạy tập lệnh để thực hiện thành công lệnh đã chèn check.sh



Thực hiện lệnh, người ta phát hiện ra rằng người dùng có thể chạy zip dưới dạng root mà không cần mật khẩu



Thông qua <https://gtfobíns.githup.io> để tìm các lệnh liên quan đến nâng cao đặc quyền thông qua zip

