**Bài thực hành:**

**Phát hiện các lỗ hổng bảo mật sử dụng công cụ rà quét**

1. **Mục đích:**

* Giúp sinh viên hiểu về khái niệm về lỗ hổng bảo mật và cách phát hiện các lỗ hổng bảo mật sử dụng các công cụ rà quét nmap.

1. **Yêu cầu đối với sinh viên:**

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.

1. Nội dung thực hành

* Khởi động bài lab:
  + Vào terminal, gõ:

*labtainer -r nmap-discovery*

*(chú ý: sinh viên sử dụng <TÊN\_TÀI\_KHOẢN> của mình để nhập thông tin người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm.)*

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: ***mycomputer***, một cái là đại diện cho máy chủ: ***friedshrimp.***Biết rằng 2 máy nằm cùng mạng LAN.

* Trên terminal ***mycomputer*** sử dụng lệnh “ifconfig”, xác định địa chỉ IP và địa chỉ mạng LAN.

Trên máy khách ***mycomputer*** sử dung nmap để tìm ra địa chỉ IP của máy ***friedshrimp*** vì chúng cùng nằm trong mạng LAN

*nmap –sP <IP mạng LAN>*

ví dụ IP máy: 172.25.0.2 à IP mạng LAN cần điền 172.25.0.0/24

          Tiếp tục sử dụng nmap để tìm cổng dịch vụ đang mở trên máy ***friedshrimp***biết rằng cổng (port) nằm từ 2000-3000.

*nmap –p 2000-3000 <IP friedshrimp>*

* + - * Sau khi xác định được cổng ssh đang mở. Sử dụng ssh để truy cập vào máy chủ. Tên máy chủ và mật khẩu là: ubuntu.

*ssh –p <port> <IP friedshrimp>*

* + - * Sau khi truy cập được vào máy chủ ***friedshrimp*** đi tìm file friedshrimp.txt. Mở và đọc file.
      * Đóng kết nối từ máy ***mycomputer*** đến ***friedshrimp.***
* Kết thúc bài lab:
  + Trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

*stoplab nmap-discovery*

* + Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab. Sinh viên cần nộp file .lab để chấm điểm
* Khởi động lại bài lab:
  + Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer -r nmap-discovery*

* Kiểm tra kết quả trong quá trình làm bài: *checkwork <tên bài lab>*