**Bài thực hành 1: Sử dụng nmap**

**TÊN\_BÀI\_LAB: nmap-discovery**

***Bài thực hành này dựa trên lab nmap-discovery trong Labtainer framework của trung tâm Cybersecurity and Cyber Operations, Naval Postgraduate School.***

1. ***Mục đích***

* Sử dụng nmap để hiểu cách sử dụng công cụ này trong việc phát hiện các máy tính và dịch vụ trên mạng.

1. ***Chuẩn bị thực hành***
   1. *Tìm hiểu lý thuyết*

* Tìm hiểu về nmap theo tài liệu đã học
  1. *Tài liệu tham khảo*
  2. *Chuẩn bị môi trường*
* Phần mềm ảo hóa: VMWare Workstation.
* Môi trường Labtainer:
  + Download file ova: <https://nps.box.com/shared/static/2chwo31xgxm2hs4hewp2n4nblroyagwz.ova>
  + Chạy VMWare, rồi: File / Open / LabtainerVM-VMWare.ova
* Khởi động bài lab:
  + Vào terminal, gõ:

*cd ~/labtainer/trunk/scripts/labtainer-student*

*labtainer TÊN\_BÀI\_LAB*

*(chú ý: sinh viên sử dụng email ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

* Dừng bài lab:
  + Vào terminal, tại thư mục:

*~/labtainer/trunk/scripts/labtainer-student*

Gõ:

*stoplab*

* File kết quả bài lab dùng để nộp cùng với file báo cáo nằm trong thư mục:

*/home/student/labtainer\_xfer/TÊN\_BÀI\_LAB*

* Trong trường hợp lỗi máy giữa chừng và cần thực hiện lại bài lab, gõ lệnh:

*labtainer -r TÊN\_BÀI\_LAB*

Nếu có lỗi khác, có thể thử khởi động lại máy ảo và chạy lại.

1. ***Nội dung thực hành***

* Sếp muốn bạn chuẩn bị cho một cuộc họp về một dự án mà bạn đã không thực hiện trong nhiều tháng. Bạn có một tệp tóm tắt trên máy chủ “Friedshrimp” mà trước đây bạn đã truy cập qua ssh; tuy nhiên, bạn không thể nhớ địa chỉ IP của “Friedshrimp”, và bạn cũng quên cổng nào mà quản trị mạng đã chỉ định cho ssh trên máy chủ đó. Bạn biết nó ở đâu đó trong khoảng từ 2000 đến 3000. Một điều chắc chắn nhất là tên người dùng và mật khẩu của bạn đều là “ubuntu”. Bạn chỉ còn một tùy chọn: sử dụng lệnh nmap để tìm địa chỉ IP và số cổng được sử dụng bởi dịch vụ ssh. Sau khi tìm thấy thông tin đó, hãy xem lại nội dung của tệp “Friedshrimp.txt” từ một phiên ssh.
* Nếu bạn cần bất kỳ trợ giúp nào với các lệnh nmap, bạn có thể sử dụng “man nmap” để xem hướng dẫn. Lưu ý rằng để chuyển ssh tới máy chủ thông qua cổng khác với cổng mặc định, hãy sử dụng “ssh -p <port> <host>”
* Chạy bài lab *nmap-discovery* trong labtainer và thực hiện yêu cầu trên. Mô tả các bước trong file báo cáo.

1. ***Kết quả cần đạt được***

* Vẽ sơ đồ mạng sử dụng trong bài lab
* Chạy được tất cả các bước như yêu cầu, giải thích/phân tích ngắn gọn các bước và kết quả

1. ***Yêu cầu nộp file kết quả***

* Cần nộp 2 file:
  + 1 file trong thư mục: /home/student/labtainer\_xfer/TÊN\_BÀI\_LAB (tên file dạng *email ptit của sinh viên đã nhập.TÊN\_BÀI\_LAB.lab*)
  + 1 file báo cáo của sinh viên ở dạng pdf, tên file dạng: *Bài thực hành 1\_Họ tên\_Mã sinh viên.pdf (số thứ tự theo đúng thứ tự bài lab)*
    - Trang bìa (ghi rõ môn học, bài thực hành, mã sv và họ và tên)
    - Nội dung mô tả các bước và phân tích sơ bộ + minh chứng kết quả dạng ảnh