**Bài thực hành 1: Sử dụng nmap nâng cao**

**TÊN\_BÀI\_LAB: nmap-ssh**

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

1. ***Mục đích***

* Bài thực hành này sử dụng nmap và các kỹ năng đã thực hiện trong các bài lab trước để xác định và khai thác điểm yếu trong hệ thống.
* Bạn thực hiện kiểm tra bảo mật đặc biệt cho một khách hàng tin rằng máy chủ SSH nội bộ của họ tương đối an toàn, nhưng lại muốn xác nhận tính hợp lệ của việc này. Mục tiêu của bạn là cố gắng truy cập từ xa vào máy chủ SSH đó và xem nội dung của một tệp đã chọn.

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

* Tìm hiểu về nmap, tshark, tcpdump
  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***

* Khởi động lab
  + Chạy lệnh: *labtainer nmap-ssh* trong terminal của Labtainer
  + Kết quả có một thiết bị ảo bao gồm một bash shell trên một máy tính có tên “MyComputer”. Tiện ích nmap được cài đặt sẵn trên máy tính đó. Bạn cũng sẽ có một thiết bị ảo được kết nối với “bộ định tuyến/router” và một bash shell ở đó. Bạn đã được thông báo rằng bộ định tuyến nằm giữa máy client của tổ chức và máy chủ.
* Tình huống và yêu cầu:
  + Bạn đã biết địa chỉ IP máy chủ SSH mục tiêu là 172.25.0.2 và số cổng SSH thường xuyên thay đổi trong phạm vi 2000-3000. Bạn đã được cấp một tài khoản, "analysis" trên máy client và trên bộ định tuyến.

client <===> [Router] <===> server

* + Mục tiêu của bạn là SSH thành công từ “MyComputer” vào tài khoản “ubuntu” trên máy chủ SSH.
  + Gợi ý:
    - nmap được cài đặt trên máy tính của tôi.
    - tshark và tcpdump được cài đặt trên bộ định tuyến
    - Những dịch vụ mạng được bảo vệ bằng mật khẩu nào khác đang được sử dụng trên mạng? Và bởi ai?
* Chạy bài lab và thực hiện các yêu cầu trên. Mô tả, phân tích 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