An toàn mạng (INT1482) - Bài thực hành số 1

1. Mục đích:

- Tìm hiểu về giao thức DNS và hệ thống tên miền
- Luyện thực hành tìm thông tin về các tên miền sử dụng một số công cụ sẵn có

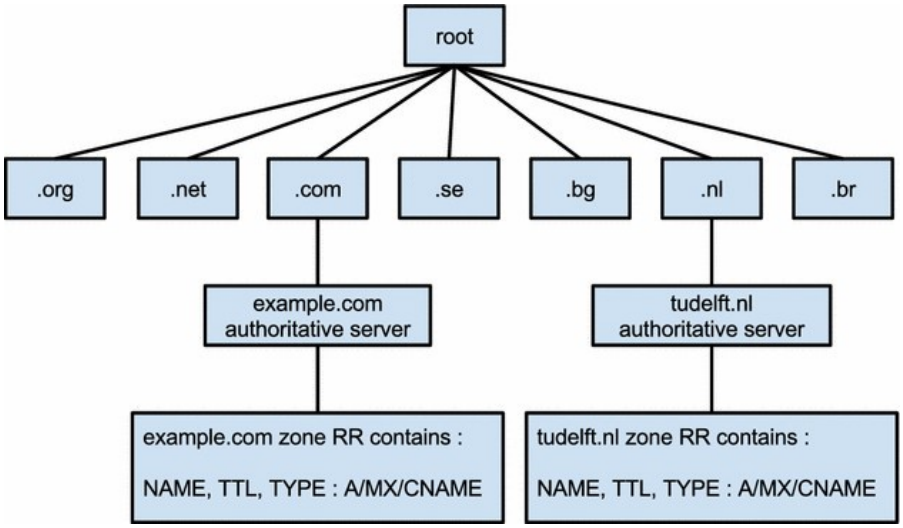
2. Các phần mềm, công cụ cần có

- Kali Linux và các công cụ trích xuất thông tin về các tên miền có sẵn trong Kali Linux:
  - nslookup
  - dig
  - dnsenum
  - dnsrecon
  - nmap

2. Tìm hiểu về giao thức DNS và hệ thống tên miền

DNS (Domain Name System) là giao thức vận hành hệ thống tên miền. Hệ thống tên miền là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ (dạng ký tự, ví dụ www.example.com) sang địa chỉ IP (dạng số, ví dụ 123.11.5.19) tương ứng của tên miền đó. Cổng chuẩn của giao thức DNS là UDP 53. DNS giúp liên kết các tên với các thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

DNS quản lý các tên miền theo mô hình cây (tree), gồm gốc (root) và các mức tên miền theo mô hình cây / phân cấp. Các máy chủ tên miền (DNS server) là thành phần quan trọng trong hệ thống tên miền: máy chủ lưu các thông tin về tên miền và cho phép chuyển đổi tên miền → IP và ngược lại. Thông tin về các tên miền được lưu trong các file gọi là zone (vùng/miền).



3. Nội dung thực hành

3.1 Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux 2023 (nếu chưa cài đặt) trên 1 máy ảo (hoặc máy thực)
  - Bản ISO của Kali Linux có thể tải tại: https://www.kali.org/get-kali/#kali-bare-metal

    - Bản cài sẵn trên máy ảo của Kali Linux có thể tải tại: https://www.kali.org/get-kali/#kali-virtual-machines
    - Đổi tên máy Kali Linux thành dạng Mã SV-Tên-Kali. Ví dụ: Bạn Trần Đức Cường, mã sv B20DCAT018 → tên máy là B20AT018-Cuong-Kali.
- Kiểm tra xem trên Kali Linux đã có sẵn các công cụ nslookup, dig, dnsenum, dnsrecon và nmap chưa bằng cách gõ tên các công cụ này và chạy trong terminal.

3.2 Tìm thông tin về tên miền sử dụng nslookup

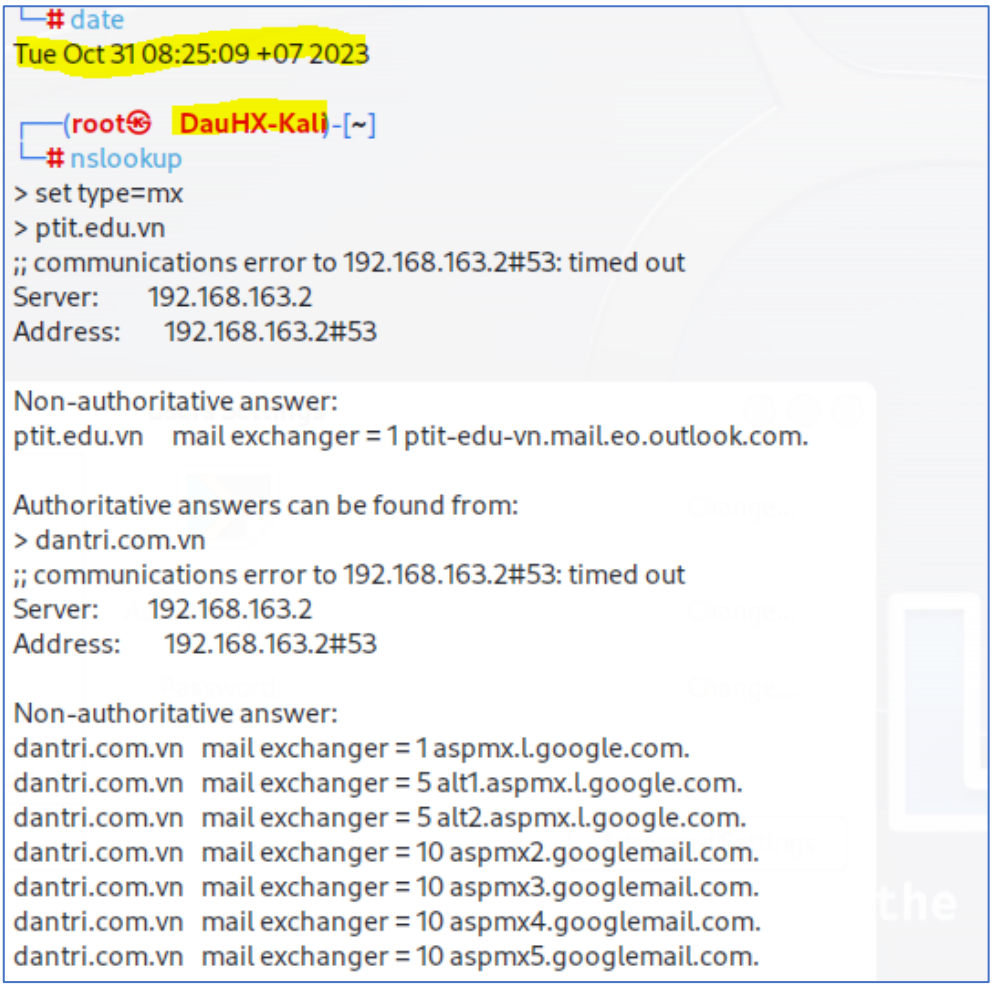
- Khởi động *nslookup* trong cửa sổ terminal
- Tìm địa chỉ IP của các tên miền (thực hiện với 3 tên miền)
  >set type = a
  >ptit.edu.vn
  >(ma_sv).ptit.edu.vn
- Tìm máy chủ DNS của các tên miền (thực hiện với 3 tên miền)
  > set type = ns
  >ptit.edu.vn
- Tìm máy chủ email của các tên miền (thực hiện với 3 tên miền)
  >set type = mx
  >ptit.edu.vn
- Tìm tên miền tương ứng với địa chỉ IP (thực hiện với 3 địa chỉ IP)
  >set type = ptr
  >64.233.187.26
- Gõ lệnh exit để kết thúc

3.3 Tìm thông tin về tên miền sử dụng các công cụ dig, dnsenum, dnsrecon và nmap

- Sử dụng dig (thực hiện với 3 tên miền)
  #dig ptit.edu.vn
- Sử dụng dnsenum (thực hiện với 3 tên miền)
  #dnsenum –thread 15 -s ptit.edu.vn
- Sử dụng dnsrecon (thực hiện với 3 tên miền)
  #dnsrecon -d ptit.edu.vn
- Sử dụng nmap (thực hiện với 3 tên miền)
  #nmap -p53 -T4 --script dns-brute www.ptit.edu.vn

4. Yêu cầu cần đạt

1. Máy Kali hoặc Linux khác phải được đặt tên theo đúng qui định ở mục 3.1
2. Chụp ảnh màn hình kết quả lưu vào file (hoặc giữ nguyên cửa sổ màn hình thực hiện):
    a. Tất cả các màn hình chạy các lệnh (có thể gộp nhiều lệnh vào 1 màn hình)
    b. Có hiển thị ngày giờ thực hiện trong **từng** ảnh chụp màn hình
    c. Màn hình chụp phải gồm đầy đủ tên máy, tên người dùng (như sau)
    d. Với các kết quả dài có thể chụp nhiều trang màn hình và ghép lại.


date
Tue Oct 31 08:25:09 +07 2023
root DauHX-Kali -[~]
nslookup
> set type=mx
> ptit.edu.vn
;; communications error to 192.168.163.2#53: timed out
Server: 192.168.163.2
Address: 192.168.163.2#53
Non-authoritative answer:
ptit.edu.vn mail exchanger = 1 ptit-edu-vn.mail.eo.outlook.com.
Authoritative answers can be found from:
> dantri.com.vn
;; communications error to 192.168.163.2#53: timed out
Server: 192.168.163.2
Address: 192.168.163.2#53
Non-authoritative answer:
dantri.com.vn mail exchanger = 1 aspmx.l.google.com.
dantri.com.vn mail exchanger = 5 alt1.aspmx.l.google.com.
dantri.com.vn mail exchanger = 5 alt2.aspmx.l.google.com.
dantri.com.vn mail exchanger = 10 aspmx2.googlemail.com.
dantri.com.vn mail exchanger = 10 aspmx3.googlemail.com.
dantri.com.vn mail exchanger = 10 aspmx4.googlemail.com.
dantri.com.vn mail exchanger = 10 aspmx5.googlemail.com.