1. Nội dung và hướng dẫn thực hiện bài thực hành

1.1. Mục đích

- Giúp sinh viên tìm hiểu về DNS và cách để mã hoá truy vấn DNS, tăng cường bảo mật khi duyệt web.

1.2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux, biết sử dụng Wireshark và Firefox.

1.3. Nội dung thực hành

- Khởi động bài lab bằng cách vào terminal và gõ:

startlab secure-dns

(chú ý: sinh viên sử dụng email stu.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)

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, cùng đại diện cho máy **computer**.

- Trên một terminal, sử dụng công cụ dig để truy vấn DNS bằng nhiều máy chủ DNS khác nhau. Xem độ trễ (query time) của các truy vấn và rút ra nhận xét.

dig @1.1.1.1 portal.ptit.edu.vn

dig @8.8.8.8 portal.ptit.edu.vn

dig @94.140.14.14 portal.ptit.edu.vn

dig @76.76.2.0 portal.ptit.edu.vn

- Vẫn trên terminal đó, khởi động Firefox bằng lệnh

firefox

- Trên terminal còn lại, khởi động Wireshark bằng lệnh

sudo wireshark

- Bật chế độ bắt gói tin trong Wireshark trên tất cả interface. Mở lại giao diện Firefox và kết nối tới trang web https://www.wikipedia.org

- Theo dõi trên Wireshark và tìm truy vấn DNS yêu cầu phân giải địa chỉ IP của Wikipedia. Lưu kết quả thu được vào tệp tên là *task2.pcap*, lưu vào thư mục */home/ubuntu*. Lưu ý đuôi tệp là pcap chứ không phải pcapng.
- Mở lại giao diện Firefox và vào Settings (Cài đặt) -> Privacy & Security (Riêng tư & Bảo mật). Kéo xuống để thấy mục DNS over HTTPS, chọn chế độ Max Protection (Bảo vệ tối đa) và chọn máy chủ DNS là Cloudflare.
- Khởi động lại chế độ bắt gói tin của Wireshark. Mở lại giao diện Firefox và truy cập trang web https://www.facebook.com
- Theo dõi trên Wireshark xem có bắt được truy vấn DNS yêu cầu phân giải địa chỉ IP của Facebook hay không.
- Tắt Firefox và khởi động lại chế độ bắt gói tin của Wireshark. Trên terminal chạy lệnh:

  dig google.com
- Theo dõi trên Wireshark xem có bắt được truy vấn DNS yêu cầu phân giải địa chỉ IP của Google hay không, và giải thích tại sao.
- Mở tệp tin /etc/systemd/resolved.conf bằng lệnh

  sudo nano /etc/systemd/resolved.conf
- Sửa các dòng có chứa *DNS*, *DNSSEC*, *DNSOverTLS* thành

  DNS=1.1.1.1 8.8.8.8

  DNSSEC=yes

  DNSOverTLS=yes
- Lưu ý cần xoá dấu # trước các dòng này. Sau đó lưu tệp bằng Ctrl + X.
- Mở tệp tin /etc/resolv.conf bằng lệnh

  sudo nano /etc/resolv.conf
- Sửa mục nameserver từ 127.0.0.11 thành 127.0.0.53. Lưu tệp. Khởi động lại dịch vụ systemd-resolved bằng lệnh

  sudo systemctl restart systemd-resolved
- Khởi động lại chế độ bắt gói tin của Wireshark. Trên terminal còn lại, chạy lệnh

  dig google.com
- Theo dõi trên Wireshark xem có bắt được truy vấn DNS yêu cầu phân giải địa chỉ IP của Google hay không, và giải thích tại sao.