### **Bài thực hành số 1**

### **Quét và phân tích lưu lượng mạng**

#### **Mục tiêu của bài thực hành**

Nghiên cứu các công cụ quét lưu lượng mạng như **tcpdump** và **Wireshark**.

#### **Nhiệm vụ**

* Làm quen với mục đích và khả năng của các công cụ sau: **tcpdump, Wireshark**;
* Cài đặt các công cụ này trên máy vật lý hoặc máy ảo;
* Thực hiện quét lưu lượng theo các tùy chọn được chỉ định và lưu **dữ liệu trích xuất** (*dump*) của lưu lượng mạng;
* Nghiên cứu cách sử dụng bộ lọc của **Wireshark**;
* Ghi lại kết quả thực hành dưới dạng **báo cáo**.
* **Lưu ý:** Có thể sử dụng **máy ảo** với hệ điều hành **Kali Linux** hoặc bất kỳ bản phân phối **Debian-based Linux** nào khác.

#### **Các tùy chọn thực hành**

1. Xem video trên trang **RuTube**.
2. Gửi tin nhắn trong ứng dụng **VK Messenger**.
3. Tải lên một tệp tin lên **Google Drive**.
4. Thực hiện cuộc gọi qua **Zoom/Skype/WhatsApp/Telegram/TeamSpeak**.

### **Nội dung bài thực hành**

#### **1. Cài đặt công cụ**

Trước tiên, cần cài đặt **tcpdump** và **Wireshark**. **Nhiều bản phân phối Linux đã đi kèm với tcpdump. Bản phân phối Kali Linux cũng được trang bị sẵn Wireshark.**

Để cài đặt **tcpdump** trên hệ điều hành dựa trên Debian, hãy mở terminal và chạy lệnh:

sudo apt install tcpdump

Tương tự, cài đặt **Wireshark** bằng lệnh:

sudo apt install wireshark

#### **2. Quét lưu lượng mạng**

Để quét lưu lượng mạng, mở terminal và nhập lệnh:

sudo tcpdump [tên\_tệp].pcap

(trong đó **tên\_tệp** là tên file chứa dữ liệu trích xuất sau khi quét).

⚠ **Lưu ý!** Chỉ thực hiện các thao tác trong **bước 3** sau khi bắt đầu quét lưu lượng.

#### **3. Thực hiện theo các tùy chọn**

Sau khi bắt đầu quét, thực hiện các hành động theo tùy chọn thực hành của bạn.

📌 **Ghi chú:**

* Kiểm tra với giảng viên về tùy chọn thực hành của bạn.
* Nếu tùy chọn yêu cầu **đăng nhập**, **không thực hiện trước**.
* Nếu tùy chọn yêu cầu **cài đặt phần mềm của bên thứ ba**, hãy chuẩn bị trước.

⚠ **Quan trọng!** Chỉ dừng **tcpdump** sau khi hoàn thành tất cả các hành động trong tùy chọn.

Dừng quá trình **tcpdump** bằng tổ hợp phím:

Ctrl + C

#### **4. Bài tập bổ sung**

Quét lưu lượng mạng theo tùy chọn thực hành bằng **Wireshark**, sau đó **so sánh dữ liệu trích xuất** với dữ liệu thu được từ **tcpdump**.

### **Yêu cầu đối với báo cáo**

Báo cáo phải bao gồm **ảnh chụp màn hình** về quá trình sử dụng từng công cụ và mô tả **toàn bộ trình tự thao tác**, như đã nêu trong phần **"Nội dung bài thực hành"** của tài liệu này.

Ngoài ra, báo cáo cần đính kèm **tệp chứa dữ liệu trích xuất lưu lượng mạng**.

Việc trình bày báo cáo phải tuân thủ **yêu cầu của giảng viên**.

<https://hackware.ru/?p=10246#8>

<https://blog.sedicomm.com/2017/05/30/tcpdump-poleznoe-rukovodstvo-s-primerami/>

<https://omgubuntu.ru/ustanovitie-i-ispolzuitie-wireshark-v-ubuntu-linux/>

<https://hackware.ru/?p=7008>

<https://networkguru.ru/wireshark-filtr-po-ip-portu-protokolu-mac/>