Thực hiện những challenges liên quan đến network trong trang web:

<https://www.root-me.org/en/Challenges/Network/>

**FTP – authentication**

Khi nhấn start, thì ta sẽ có 1 file ch1.pcap, sử dụng Wireshark để mở

Chọn “Follow TCP Stream”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ta có thể thấy username và password. Nhập password vô là hoàn thành challenge.

**TELNET – authentication**

Khi nhấn start, thì ta sẽ có 1 file ch2.pcap, sử dụng Wireshark để mở

Nhấn chuột phải vào packet sử dụng protocol là TELNET, rồi chọn “Follow TCP stream”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ta có thể thấy thông tin đăng nhập. Nhập password vô là hoàn thành challenge.

A screenshot of a computer

Description automatically generated

**Twitter – authentication**

Khi nhấn start, thì ta sẽ có 1 file ch3.pcap, sử dụng Wireshark để mở.

Ta thấy nó chỉ có 1 HTTP Request

A screenshot of a computer

Description automatically generated

Ta sẽ xem qua thông tin phần HTTP kĩ hơn bằng cách nhấn vô mục Hypertext Transfer Protocol.

A screenshot of a computer

Description automatically generated

Trong phần Authorization có chứa username và password. Ta nhập password vô là hoàn thành challenge.

**ETHERNET frame**

Khi nhấn start thì sẽ hiện ra trang sau, là file text ch12.txt

A screenshot of a computer

Description automatically generated

Giải mã file text

A screenshot of a computer

Description automatically generated

Giải mã phần thông điệp của Authorization thì ta sẽ có được password

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**IP Time to live (Find the TTL used to reach the targeted host in this ICMP exchange.)**

Khi nhấn start thì ta sẽ có file ch7.pcap, sử dụng wireshark để mở.

A screenshot of a computer

Description automatically generated

Thử thách không cung cấp IP máy chủ nguồn/đích, vì vậy phải suy ra nó từ log. Ngay từ đầu, ta giả định nguồn là 24.6.126.218 trong khi máy chủ từ xa là 192.173.244.32. Ta cũng thấy một loạt các phản hồi vượt quá TTL bắt đầu từ 12.244.25.161 cho gói TTL=2, 12.244.72.210 đến 204.2.121.162 cho TTL= 12.

Traceroute bắt đầu mà không biết máy chủ ở khoảng cách bao xa với TTL=1. Mỗi lần vượt quá mức TTL cho mỗi gói ICMP, ta sẽ nhận được gói trả lời cho biết đã vượt quá mức TTL. Đây chính xác là những gì chúng ta thấy trong log. Source của các gói “vượt quá TTL” này khác nhau nhưng đích đến luôn là 24.6.126.218, suy ra là máy chủ nguồn của ta. Thứ hai, lưu ý rằng 24.6.126.218 luôn hiện diện ở nguồn/đích. Điều này cho thấy rõ ràng ứng dụng Wireshark đã được cài đặt trên máy chủ này vì nó ghi lại tất cả các gói gửi đi hoặc gửi đến trên giao diện này.

Ta đã xác định được máy chủ nguồn và đích. Bây giờ khoảng cách đến máy chủ đích là bao nhiêu? Lưu ý rằng ta sẽ tiếp tục nhận được thông báo “TTL exceeded” cho đến khi TTL của gói gốc tăng đến mức ngừng nhận. Cuộn xuống ta thấy điều này dừng ở TTL=13.

A screenshot of a computer

Description automatically generated

Vì vậy, máy chủ đích cách 13 hop. Phản hồi ICMP từ máy chủ từ xa xuất hiện ngay sau gói TTL=13 gửi đi. Nó mang TTL là 51. Từ trang này, chúng tôi biết nhìn chung có 3 giá trị TTL mặc định bao gồm hầu hết tất cả các hệ thống: 64, 128 và 254. Nếu TTL của gói trả lời là 51 thì TTL ban đầu của nó phải là 64. Vì 64- 51=13, điều này có nghĩa là có 13 bước nhảy từ đích đến nguồn, điều này khẳng định rằng máy chủ cách đó 13 bước nhảy.

Vậy nhập 13 vô là ta hoàn thành thử thách.