Lab-Project 6: TCP Handshake with scapy

Máy sử dụng: Kali Linux; Ubuntu

**Starting a netcat Listener on the Linux Target Machine**

**\*** Máy Ubuntu:

Tại Terminal thứ nhất, sử dụng lệnh: **nc -l -p 5555**

Tại Terminal thứ 2 sử dụng lệnh**: watch “netstat -an | grep 5555”**

A screenshot of a computer

Description automatically generated

**Finding the Target Linux Machine’s IP Address:**

+ Sử dụng lệnh **ifconfig** để hiển thị IP của máy Linux

**A screenshot of a computer screen

Description automatically generated**

**Blocking RST Packets on the Linux Sender Machine**

\* Máy Kali:

+ Sử dụng các lệnh sau:

**iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP**

**iptables -L**

A screenshot of a computer

Description automatically generated

**=>** Sử dụng lệnh 1: Lệnh này sẽ chặn tất cả các gói tin TCP đi ra có cờ RST, ngăn không cho thiết lập lại kết nối TCP

**=>** Lệnh 2: Lệnh này liệt kê (list) tất cả các luật iptables hiện tại trên hệ thống, bao gồm các luật trong các chuỗi như INPUT, OUTPUT, và FORWARD

**Starting scapy on Linux Sender Machine**

**+** Trên máy Kali, gõ lệnh scapy để sử dụng:

A computer screen shot of a number

Description automatically generated

+ Setup các trường như sau:

A screenshot of a computer

Description automatically generated

**Sending a SYN Packet from the Linux Sender Machine:**

**\*** Máy Kali:

Sử dụng lệnh sr1(i/t); thấy được packet đã được gửi

**A screen shot of a computer code

Description automatically generated**

**\*** Trên máy Ubuntu:

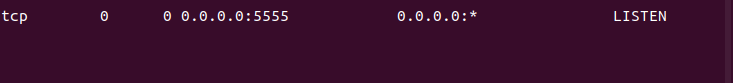
Thấy gói tin đã được gửi

A screenshot of a computer

Description automatically generated

**Observing TCP timeout:**

+ Sau khoảng 1 phút, nhận thấy rằng, kết nối biến mất khỏi danh sách netstat



=> Nguyên nhân: Đây là thiết lập mặc định trong kali Linux, chờ 60 giây trước khi từ bỏ kết nối

=> Không đủ thời gian quan sát

**Lengthening the TCP Timeout on the Linux Target Machine**

**+** Mục tiêu: Kéo dài thời gian lên 10 phút

Sử dụng lệnh**: echo 10 > /proc/sys/net/ipv4/tcp\_synack\_retries**

=> Do trong thiết lập thời gian TCP, tập trung vào phần tcp\_synack\_retries – Là số lần tối đa một phân đoạn SYN/ACK cho kết nối TCP thụ động được truyền lại, cài đặt sẽ mặc định là 5 ⬄ các phiên sẽ hết thời gian sau 60s

A screenshot of a computer

Description automatically generated

**Re-sending a SYN from the Linux Sender Machine**

**\*** Máy Kali:

+ Gửi lại máy Ubuntu bằng lệnh **sr1(i/t)**

**A computer screen with text

Description automatically generated**

**\*** Trên máy Ubuntu:

**Screens screenshot of a computer screen

Description automatically generated**

**Analyzing the SYN/ACK Packet:**

**\*** Máy Kali:

**+** Các phần quan trọng chú ý đến:

* Seq number
* Ack number
* Flags

+ Sửa các trường trên thành như sau:

**t.flags = “A”**

**t.seq = 1**

**t.ack = 1173360089**

**+** Gửi đi bằng lệnh send(i/t)

**A screenshot of a computer

Description automatically generated**

**Observing the Session on the Linux Target Machine:**

+ Trên máy Ubuntu thu được:

**Screens screenshot of a computer screen

Description automatically generated**

=> Thu được ESTABLISHED connection ⬄ Hoàn thành