Hacking with Linux networking CLI tools

Bob

2024-06-30

# Packet analysis

sudo tcpdump -ilo -nnvvvxXKS -s0 port 3333

Upon running the above command, the following packet is captured:

08:34:10.790666 IP (tos 0x0, ttl 64, id 12824, offset 0, flags [DF],  
proto TCP (6), length 64)  
  
127.0.0.1.46668 > 127.0.0.1.3333: Flags [P.], seq 2400005725:2400005737,  
ack 373279396, win 512, options [nop,nop,...], length 12  
  
 0x0000: 4500 0040 3218 4000 4006 0a9e 7f00 0001 E..@2.@.@.......  
 0x0010: 7f00 0001 b64c 0d05 8f0d 2e5d 163f caa4 .....L.....].?..  
 0x0020: 8018 0200 fe34 0000 0101 080a c24e e2d7 .....4.......N..  
 0x0030: c24e 1217 6865 6c6c 6f20 776f 726c 640a .N..hello.world.

1. Tell me the meaning of each option used in the previous command.
   * **-i**:
   * **-nn**:
   * **-vvv**:
   * **-x**:
   * **-X**:
   * **-S**:
   * **-K**:
   * **-s0**:
2. Please analyze this captured packet and explain it to me as detailed as you can.
   * **Answer:**

# HTTP

1. Write a simple script showing how HTTP works (you need curl).

#!/bin/bash

1. Record your HTTP demo session with ttyrec.

# Socket programming

## TCP

/\* A simple TCP server written in C \*/  
  
 // Your code

/\* A simple TCP client written in C \*/  
  
 // Your code

## UDP

/\* A simple UDP server written in C \*/  
  
 // Your code

/\* A simple UDP client written in C \*/  
  
 // Your code

# Questions

List at least 5 problems you’ve met while doing this work. When listing your problems, you have to tell me:

1. Description of this problem. For example,
   * What were you trying to do before seeing this problem?
2. How did you try solving this problem? For example,
   * Did you google? web links?
   * Did you read the man page?
   * Did you ask others for hints?

## Problem 1

## Problem 2

## Problem 3

## Problem 4

## Problem 5