实验成绩	
批阅教师	
日　　期	2024/7/8

西南林業大學
SOUTHWEST FORESTRY UNIVERSITY

大数据与智能工程学院
实践（实习）报告

课程名称 综合实习二

专业班级 计科 2023 级专升本 2 班

学　　号 20231159xxx

学生姓名 张三

指导教师 王晓林

2024 年 6 月 30 日

实习时间	2024/6/28 - 2024/6/30	实习天数	3
实习地点	经管楼 219	实习班级	计科 2023 级专升本 2 班
实习人数	74	分组情况	不分组

实习目的

掌握 Linux 平台上常用网络工具的使用，并理解基本的网络编程过程。

1. 掌握用 tcpdump 捕获并分析数据包
2. 掌握用 netcat 完成简单的网络会话
3. 掌握基本的网络编程

实习要求

1. 在 Linux 平台完成所有实验
2. 在 Linux 平台完成实验报告
3. 努力尝试用英文撰写实验报告
4. 将实验作业及报告以 tgz 格式打包，并上传到指定教学网站
5. 迟交报告将被扣分

实习内容

详见《实验指导书》。

课程实习安排

（本栏须填写清楚实习的日期及该天实习的具体内容）

2024/6/28: 学习使用 tmux，ttyrec 等实验所需的命令行工具。学习使用 ip, tcpdump, netcat, curl, ss, nmap 等网络工具。

2024/6/29: 完成用 tcpdump 捕获、分析数据包，用 netcat 实现网络协议会话，以及网络编程等规定实验项目。

2024/6/30: 完成所有实验，并撰写实验报告。

1 Packet analysis

Upon running the following command:

```
sudo tcpdump -ilo -nnvvvxXKS -s0 port 3333
```

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,TS val 3259949783 ecr 3259896343], 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: Specify the network interface card to listen from.
   -nn: Don't print addresses.
   -vvv: Verbose output.
   -x: When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex.
   -X: When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols. In the current implementation this flag may have the same effect as -XX if the packet is truncated.
   -S: Print absolute, rather than relative, TCP sequence numbers.
   -K: Don't attempt to verify IP, TCP, or UDP checksums. This is useful for interfaces that perform some or all of those checksum calcula- tion in hardware; otherwise, all outgoing TCP checksums will be flagged as bad.
   -s0: Setting snaplen to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of tcpdump.
2. Please analyze this captured packet and explain it to me as detailed as you can.
   Answer: 4means ipv4; 5is the header length in word; The 00 following 45 are the ToS bits; 0040 is the total length of this IPv4 packet; 3218 is the identification field; 4000 are the 2 flag bits plus the fragment offset field; 4006 means TTL is 0x40, 0x06 means TCP; 0a9e is the header checksum; 7f00 0001 is the IPv4 address of the loopback interface; b64c is the source port number; 0d05 is the destination port number, 3333 in decimal;

2 HTTP

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

```
#!/bin/bash

echo 'Hello, world!'
```

2. Record your HTTP demo session with `ttyrec`.

3 Socket programming

3.1 TCP

```
/* A simple TCP server written in C */

/* Your code */
```

```
/* A simple TCP client written in C */

// Your code
```

3.2 UDP

```
/* A simple UDP server written in C */

// Your code
```

```
/* A simple UDP client written in C */

// Your code
```

4 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?

4.1 Problems

1.
2.

3.
4.
5.