Multiple Choice: choose the best answer

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

A. Link layer
B. Network layer
C. Transport layer
D. Application layer

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

A. 0
B. 10
C. 110
D. 1110

3. If an IP address has a netmask of 255.255.252.0, how many bits are used for denoting the subnet?

A. 20
B. 21
C. 22
D. 23

4. For a subnet 192.168.60.0/24, which of the following IP address is the broadcast IP address?

A. 192.168.60.1
B. 192.168.60.2
C. 192.168.60.255
D. None of the above

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

A. docker ps -a
B. docker ps
C. docker ls -a
D. docker ls

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

A. services
B. containers
C. networks
D. images

. Which of the following is a correct way to use Scapy to create TCP packets for destina
.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)/TCP(dport = (200, 300))

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

A. Link layer
B. Network layer
C. Transport layer
D. Application layer

9. In an Ethernet frame, the following code in the type header indicates an ARP packet?

A. 0x8000
B. 0x8060
C. 0x0800
D. 0x0806

In an IP datagram, which of the following code in the protocol header indicates the payload of the IP gram is a TCP segment?

following is a correct command to use netcat to make a TCP server listening at port

mmand is correct to set aa:bb:cc:dd:ee:ff as the MAC address for 10.0.2.10

f

A. SOCK_DGRAM
B. SOCK_STREAM
C. SOCK_RAW
D. SOCK_PACKET

15. Which of the following is the correct bpf filter to show all TCP packets from host 192.168.1.81, ports 100 to 200?

A. tcp and port 100-200 and host 192.168.1.81
B. tcp and portrange 100-200 and host 192.168.1.81
C. tcp and portrange 100-200 and src host 192.168.1.81
D. tcp and port 100-200 and src host 192.168.1.81

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

A. 02:42:b7:41:b9:8g
B. 00:0c:29:8b:d9:03
C. 02:42:b7:41:b9:8d
D. 02:42:02:e4:80:41

17. Which of the following statement about checksum is not correct?

A. When UDP's checksum field is set to be 0, the receiver will ignore the checksum field
B. TCP's checksum is calculated on both the TCP headers and data
C. IP's checksum is calculated on both the IP headers and data
D. UDP's checksum is calculated on both the UDP headers and data

18. What interface will be used to route packets to destination 10.10.20.10

I: 0.0.0.0/0 dev interface-a
II: 10.10.0.0/16 dev interface-b
III: 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

19. 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 Ethernet header
B. The source MAC is the broadcast address ff:ff:ff:ff:ff:ff in both ARP header and Ethernet header
C. The source and destination IP are both set to the IP of the machine issuing the gratuitous ARP
D. Ordinarily, no reply packet will occur

20. You used Scapy to craft a TCP packet

>>> pkt = IP(dst="153.91.1.10")/TCP()/"Hello"

Which of the following statement(s) is correct to set the TCP's flag to SYN?

A. pkt.flags = 'S'
B. pkt[TCP].flags = 'S'
C. pkt.haslayer(TCP).flags='S'
D. Both B and C

21. Which of the following statement about virtual machine and container is not correct?

A. Each VM has its own OS while all containers share a single OS from the host machine
B. VM requires much more system resources such as memory compared with that of container
C. VM size is larger than container
D. VM is less secure than container

22. Which of the following statement displays the least detailed information about a packet pkt?

A. >>> pkt
B. >>> pkt.summary()
C. >>> pkt.show()
D. >>> ls(pkt)

23. Assume a packet is created as follows

pkt = IP()/TCP()/'Hello'

Which of the following statement is correct to retrieve the data 'Hello'?

A. pkt.payload.payload.payload
B. pkt.payload.payload
C. pkt.payload.load
D. pkt.payload.payload.load

24. Based on the routing table below from a router, which of the following statement is incorrect?

```
$ ip route
default via 10.0.2.2 dev ens33  proto static  metric 100
10.0.2.0/24 dev ens33  proto kernel  scope link  src 10.0.2.128  metric 100
169.254.0.0/16 dev ens33  scope link  metric 1000
192.168.60.0/24 dev ens38  proto kernel  scope link  src 192.168.60.128  metric 200
```

A. To route the packets to the 10.0.2.0/24 network, interface ens33 will be selected and its associated IP is 10.0.2.2
B. To route the packets to the 192.168.60.0/24 network, interface ens38 will be selected and its associated IP is 192.168.60.128
C. The default gateway router is at 10.0.2.2
D. 169.254.0.0/16 are the link local addresses which are not routable

25. Based on the routing table below from a host, if a student created a packet pkt = IP(dst='192.168.60.3') and sent it out from the host using Scapy, what will be the output for print(pkt[IP].src)?

```
$ ip route
default via 10.0.2.2 dev ens33  proto static  metric 100
10.0.2.0/24 dev ens33  proto kernel  scope link  src 10.0.2.128  metric 100
169.254.0.0/16 dev ens33  scope link  metric 1000
192.168.60.0/24 dev ens38  proto kernel  scope link  src 192.168.60.128  metric 200
```

A. 127.0.0.1
B. 10.0.2.2
C. 192.168.60.128
D. 10.0.2.128

26. Which of the following statement about TCP and UDP is incorrect?

A. TCP is a connection-oriented protocol while UDP is a connection-less protocol
B. UDP's speed is faster than TCP
C. TCP maintains the order of the packets while UDP does not
D. Both TCP and UDP can be used for broadcast

27. Which of the following attack used the IP directed broadcast?

A. Smurf attack
B. Ping of the death attack
C. Teardrop attack
D. ICMP re-direct attack

Jason is a student in the CYBR 5800 class. He is working on the packet sniffing and spoofing lab to spoof an ICMP echo reply packet. Please help him to fill the eight blanks in the following Python script.

```
#!/usr/bin/python3

from scapy.all import *

def spoof_pkt(pkt):
   if ICMP in pkt and pkt[ICMP].type == __1__:
      ip = IP(src=__2__, dst=__3__)
      icmp = ICMP(type=__4__, id=__5__, seq=__6__)

      if pkt.haslayer(Raw):
         data = pkt[Raw].load
         newpkt = __7__
      else:
         newpkt = __8__

      send(newpkt)

pkt = sniff(filter='icmp and src host 10.0.2.128', prn=spoof_pkt)
```

28. What are values in blanks 1 and 4, respectively?

A. 1, 2
B. 8, 0
C. 0, 8
D. 5, 8

9. What are values in blanks 2 and 3, respectively?

A. pkt.dst, pkt.src
B. pkt.src, pkt.dst
C. pkt[IP].dst, pkt[IP].src
D. pkt[IP].src, pkt[IP].dst

10. What are values in blanks 3 and 4, respectively?

A. pkt.id, pkt.seq
B. pkt[IP].id, pkt[IP].seq
C. pkt[ICMP].id, pkt[ICMP].seq
D. pkt.id, pkt[ICMP].seq

11. What are values in blanks 7 and 8, respectively?

A. ip/icmp/data, ip/icmp
B. ip/icmp/load, ip/icmp
C. ip/icmp/payload, ip/icmp/data
D. ip/icmp/data, ip/icmp/payload

Visual is a student in the CYBR 3800 class. He is working on the ARP cache poisoning lab to poison 10.0.2.129's ARP cache using the gratuitous ARP request. His goal is to put the following fake information to 10.0.2.129's cache:

10.0.2.128 - aa:bb:cc:dd:ee:ff

Please help him to fill the seven blanks in the following Python script:

```
#!/usr/bin/python3

from scapy.all import *

VM_A_IP = '10.0.2.129'
VM_A_MAC = '08:0c:29:9d:ed:9c'
VICTIM_IP = '10.0.2.128'
FAKE_MAC = 'aa:bb:cc:dd:ee:ff'

ether = Ether(src=__1__, dst=__2__)
arp = ARP(hwsrc=__3__, hwdst=__4__, psrc=__5__, pdst=__6__, op=__7__)

pkt = ether/arp
sendp(pkt)
```

12. What are values in blanks 1 and 3, respectively?

A. VM_A_MAC, FAKE_MAC
B. VM_A_MAC, VM_A_MAC
C. FAKE_MAC, FAKE_MAC
D. FAKE_MAC, VM_A_MAC

13. What are values in blanks 3 and 4, respectively?

A. VM_A_MAC, VM_A_MAC
B. [illegible]
C. VARP_MAC, VARP_MAC
D. [illegible], VM_A_MAC

14. What are values in blanks 5 and 6, respectively?

A. VM_A_IP, VICTIM_IP
B. VM_A_IP, VM_A_IP
C. VICTIM_IP, VICTIM_IP
D. VICTIM_IP, VM_A_IP

15. What is the value in blank 7?

A. 0
B. 1
C. 2
D. 3