CS974-Final

● Graded

Student

Sivachandran P

Total Points

40 / 50 pts

Question 1

TCP/IP Laters

3 / 3 pts

✓ **+ 3 pts** Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 2

Protocol Units in TCP/IP

3 / 3 pts

✓ **+ 3 pts** Correct

+ 2 pts Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 3

Connectionless vs. Connection-Oriented

3 / 3 pts

✓ **+ 3 pts** Correct

+ 2 pts Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 4

Preventing Infinite Loops

3 / 3 pts

✓ **+ 3 pts** Correct

+ 2 pts Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 5

Authenticated Source

2 / 3 pts

+ 3 pts Correct

✓ **+ 2 pts** Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

AH and ESP are specifically designed for securing IP packets, making them more efficient and directly relevant for IP-level authentication and encryption

Question 6

TCP Handshake

3 / 3 pts

✓ **+ 3 pts** Correct

+ 2 pts Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 7

TCP Sequence Numbers

3 / 3 pts

✓ **+ 3 pts** Correct

+ 2 pts Almost Correct

+ 1.5 pts Partially Correct

+ 0 pts Wrong or Copy from AI tools

Question 8

ARP Poisoning

1 / 5 pts

+ 5 pts Correct

+ 3 pts Partial Correct

✓ **+ 0 pts** Incorrect / Copy and pasted from AI tools

+ 1 pt Ip forwarding role is not explained. Also, The association of IP and MAC at device level is not clearly explained.

Question 9

BGP Vulnerabilities

4 / 5 pts

✓ **+ 5 pts** Correct

+ 3 pts Partial Correct

+ 0 pts Incorrect / Copy and pasted from AI tools

− 1 pt BGP hijacking - do you mean prefix hijacking?

Question 10

OSPF problem

2 / 4 pts

+ 4 pts Correct

✓ **+ 2 pts** Partial Correct

+ 0 pts Incorrect or copy & pasted from AI tools

💬 OSPF uses message integrity checks like MD5 or SHA-1, which are outdated and vulnerable to attacks : collision attack etc.

Question 11

DNS Protocol

5 / 5 pts

✓ **+ 5 pts** Correct

+ 3 pts Partial Correct

+ 0 pts Incorrect / Copy and pasted from AI tools

Question 12

DNS rebinding attack

1 / 3 pts

+ 3 pts Correct

✓ **+ 0 pts** Incorrect or copy & pasted from AI tools

💬 **+ 1 pt** Given marks for the attempt. Answer is not clearly explained.

Question 13

Public Wifi and DNS

5 / 5 pts

✓ **+ 5 pts** Correct

+ 3 pts Partial Correct

+ 0 pts Incorrect / Copy and pasted from AI tools

Question 14

DNS Source Port Randomization

2 / 2 pts

✓ **+ 2 pts** Correct

+ 0 pts Incorrect

Q1 TCP/IP Laters

3 Points

TCP/IP Protocol architecture shows 4 layers at the end-host, but 3 layers in the network intermediary nodes. Explain in 1-2 sentences -- what are these layers and why is there a difference in number of layers between the two types of nodes?

TCP/IP protocol layers: Application, Transport, Internet and Network access (contains link and physical)
Network intermediary nodes are: Network access, Internet and Transport

The main reason for this difference is because it needs to forward packets, and not necessary to consider application part.

Q2 Protocol Units in TCP/IP

3 Points

The protocol units at the Datalink layer are called frames, at the IP layer, are called packets, at the TCP layer are called segments. Write down the relationship between the sizes of each of these units? Your answer should not be more than 3 equations/inequalities.

1) Datalink layer frame encapsulates the IP packet, so the Frame size should be greater than or equal to Packet size

2) IP packet encapsulates the TCP segment, so Packet size should be greater than or equal to Segment size

3) The Frame should always be greater than or equal to TCP segment

Q3 Connectionless vs. Connection-Oriented

3 Points

Write 1-2 sentences explanation of why TCP is called connection-oriented whereas IP is called connection-less?

TCP connection-oriented, establishes two way channel between sender & receiver before data transfer is initiated, which is reliable.

IP connection-less, not used to establish dedicated path before sending data.

Q4 Preventing Infinite Loops

3 Points

How does the TTL field in the IP packets help prevent the packets from getting into infinite loops through the Internet? (Your answer should not exceed 2 sentences)

TTL (Time To Live) value will get reduced whenever packet passes via router, and at the time when this count reaches zero, will start to discard the packets and sends ICMP message to sender.

Q5 Authenticated Source

3 Points

Why is the source IP not authenticated in the IP protocol? What would have been required to authenticate it? (Your answer should not exceed more than 3 sentences altogether).

At the time of early design of Internet security was not major focus, and simply designed to transfer packets efficient and easily.

In order to authenticate, we may need the following methods:
Digital signature, IP security and etc.

Q6 TCP Handshake

3 Points

What can go wrong if the 3rd acknowledgement in the 3-way TCP handshake is not sent from the client to the server? (only 1-2 sentence answer will be acceptable)

When connection could not establish in the TCP three way handshake is not shared from Client, below mentioned type of issues might occur:
Could not establish connection or improper connection, Data transmission failure, Could not utilize the resources efficiently and etc.

Q7 TCP Sequence Numbers

3 Points

Why is that the initial sequence number while initiating a TCP handshake is chosen at random rather than from 0 or a fixed number? (1-2 sentence answer is required).

In order to give less chances for attacker to predict and intervene, initial sequence numbers are chosen randomly.
Still it will not prevent from attackers, but reduce the chances to attack.

Q8 ARP Poisoning

5 Points

Suppose your lab has 5 workstations connected to an Ethernet switch. You want to use ARP poisoning to hijack the traffic meant for your lab-mate's workstation. write down the steps required to achieve this? (your answer must be a few short bullet points and not a narrative)

Sharing below the simple steps required to perform Address Resolution Protocol (APR) poisoning:
Step - 1: Identify the target
Step - 2: Enable IP forwarding
Step - 3: Send spoofed ARP replies (arpspoof)
Step - 4: Intercept Traffic and continuously send spoofed ARP replies to get and keep ARP tables poisoned

Q9 BGP Vulnerabilities

5 Points

BGP Path Attestation in the original BGP protocol is not authenticated. This means this lack of authentication can be exploited by miscreants in various ways. List a set of different attacks on BGP infrastructure/protocol that is done exploiting this property. (your answer should be a short 2-4 item list of names of attacks).

Border Gateway Protocol (BGP) lack of authentication makes it vulnerable to various attacks mentioned below:
BGP hijacking, Prefix spoofing, MITM attacks, DDOS bal

Q10 OSPF problem

4 Points

OSPF protocol requires nodes to exchange LSAs and they use message integrity code for this unlike BGP protocol. But this integrity algorithm is not secure - why? (Your answer should not exceed 2 sentences).

In order to ensure authenticity and integrity of LSA (Link State Advertisements) Open Shortest Path First (OSPF) is using Message Integrity Check, and this mechanism is not secure due to the following reasons:
1) Does not Encrypts and plain texts are used
2) Lack of robust key management practices

BGP (Border Gateway Protocol) relies on TCP signature verifications.

Q11 DNS Protocol

5 Points

(i) DNS responses are cached locally -- but for how long are they cached?

Duration depends on the TTL value specified at DNS record,

(ii) What kind of exploits can happen because of this caching of response? (Your answer should list 2-4 bullet points max).

1) DNS cache poisoning (spoofing)
2) DNS rebinding
3) DDos attacks
4) Man-In-The-Middle attack etc.

Q12 DNS rebinding attack

3 Points

Explain in 1-2 sentences how the DNS rebinding attack uses the duration setting of the DNS Caching?

DNS rebinding attack exploits the TimeToLive setting of DNS caching to bypass browser security mechanism.

Q13 Public Wifi and DNS

5 Points

Explain in 1-2 short sentences why public wifi may lead to a DNS resolver-based misdirection and hence it is very insecure to use public wifi?

In general public Wifi are insecure to use, since anyone can access and intercept the connection between browser and server due to unencrypted communication, Rough DNS resolvers, lack of authentication, DNS hijacking and etc.

Q14 DNS Source Port Randomization

2 Points

What is DNS source port randomization used for?

To reduce the predictability
The combination of random transaction ID and random source port makes more difficult for an attacker by increasing the entropies