Netsec mid1

Mid-Term Exam

- **Due** Oct 4 at 11:59pm
- **Points** 76
- **Questions** 11
- **Available** Oct 4 at 12:01am - Oct 6 at 11:59pm
- **Time Limit** 240 Minutes

Instructions

Welcome to the mid-term! The mid-term is available on Oct 4th starting at 12:01AM and is due by Oct 4th 11:59PM.

- Each question requires a short paragraph response and/or a diagram.
- No references are required.
- 4 hour time limit once you start the quiz.
- Upload any diagrams or figures on Question 10.
- Good luck!

This quiz was locked Oct 6 at 11:59pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	215 minutes	73 out of 76

Correct answers are hidden.

Score for this quiz: **73** out of 76
Submitted Oct 4 at 11:12pm
This attempt took 215 minutes.

Question 1

6 / 6 pts

Please answer the question below (we assume that 2 = 1,000, 2 = 1,000,000,

and 2 = 1,000,000,000 to simply your computation.) You need to show your

calculation procedure in addition to the final result.

An implementation of TCP uses a random number to serve as the initial sequence

number. An attacker wants to guess the sequence number and conduct blind reset

attack. We know that the receiver’s window size is 32K bytes, and the attacker can

send out 4K packets / second. Please calculate: at the worst case, how many

seconds does the attacker need to send out packets to guarantee that at least one

packet falls into the receiver’s window?

Your Answer:

1) Given,

$2^{10} = 1000$

$2^{20} = 1,000,000$

$2^{30} = 1,000,000,000$

Receiver Sequence number possible

Spaces $= 2^{32}$

Receiver's window size = 32k Bytes

$\Rightarrow 2^{15}$ Bytes

$$\Rightarrow \frac{2^{32}}{2^{15}} = 2^{17} \text{ packets}$$

$$\Rightarrow \frac{2^{17} \text{ packets}}{2^{12} \frac{\text{packets}}{\text{seconds}}} \Rightarrow 2^{5} \text{ sec}$$

$\Rightarrow 32$ Seconds.

Question 2

6 / 6 pts

In the ARP protocol, a node can send out a gratuitous ARP request packet: both

the source and destination IP addresses will be the IP address of the sender.

Please answer: (a) In the ARP packet (not the Ethernet header part), what will be

the source and destination Ethernet addresses in the gratuitous packet? (b) how

can this packet be used to detect IP address conflict in the same sub-network that

is connected by a hub? Make sure that you answer both sub-questions.

Your Answer:

(a) In the ARP packet (not the Ethernet header part), the source Ethernet address in the gratuitous packet is the Sender Ethernet address and whereas the destination Ethernet address in the gratuitous packet is the broadcast Ethernet address.

(b) In the scenario where the source and destination IP address having the same IP address of the sender, request packet can be used to detect IP address conflict in the

same sub-network that is connected by the hub by getting acknowledgement from another node having the same IP address. Otherwise, there shouldn’t be any conflict. Hence the the request packets are used to detect IP address conflict in the same sub-network that is connected by a hub

Question 3

12 / 12 pts

ARP poisoning can be used to generate fake ARP cache entries in the node so

that a packet targeting at node A will be delivered to node B, and node B can get

the information.

Please answer:

(a) when we set an Ethernet card to promiscuous mode, we can also eavesdrop

on the traffic on the Ethernet cable. Do you think the ARP poisoning is the same

as setting the card to promiscuous mode? If not, please use an example to

illustrate that ARP poisoning can achieve some malicious goals that the

promiscuous mode cannot.

(b) A company uses a firewall to isolate the Intranet within the company and the

outside Internet. The company's web server is located behind the firewall in the

Intranet. To allow the outside customers to access the company's information, the

firewall uses IP address based authentication: only the packets with the server's IP

address as the source or destination can penetrate the firewall.

Please draw a figure to illustrate how a computer in the Intranet can use ARP poisoning to bypass

the firewall and access the outside Internet, at the same time, the outside

customers can still get the information from the web server. If you draw a figure to

answer the question, you can attach it at Question 10.

Your Answer:

(a) ARP poisoning is not same as setting the card to promiscuous mode. This is because the ARP poisoning is an active(direct) attack and eavesdropping is an passive(indirect) attack. In the ARP poisoning the traffic can be manipulated but in the passive attack or the card in the promiscuous mode, the traffic can only be observed and there shouldn’t be any active attack.

For instance, in the man-in-the-middle attack, the packets from source to destination can we tracked(spoofed) by the attacker and the acknowledgement packets can be changed and then resend it to the sender. Here the active attack makes some impact, whereas in the promiscuous mode, the attacker could just watch out on the traffic but couldn’t make any impact by sending the spoofed packets.

(b) The malicious node should poison both the webserver and firewall ARP caches to access the websites. The malicious node do first access the web server and firewall ARP caches. The web server IP address will first be mapped with the malicious code MAC address by poisoning the firewall ARP cache. And then the malicious code will corrupt the ARP cache on the webserver by mapping the firewall IP address to its MAC address. The malicious node will employ IP spoofing to pretend to be the Web server's IP address in order to breach the firewall once both the firewall and web server's ARP caches have been poisoned. Please refer the figure 3(b) for reference

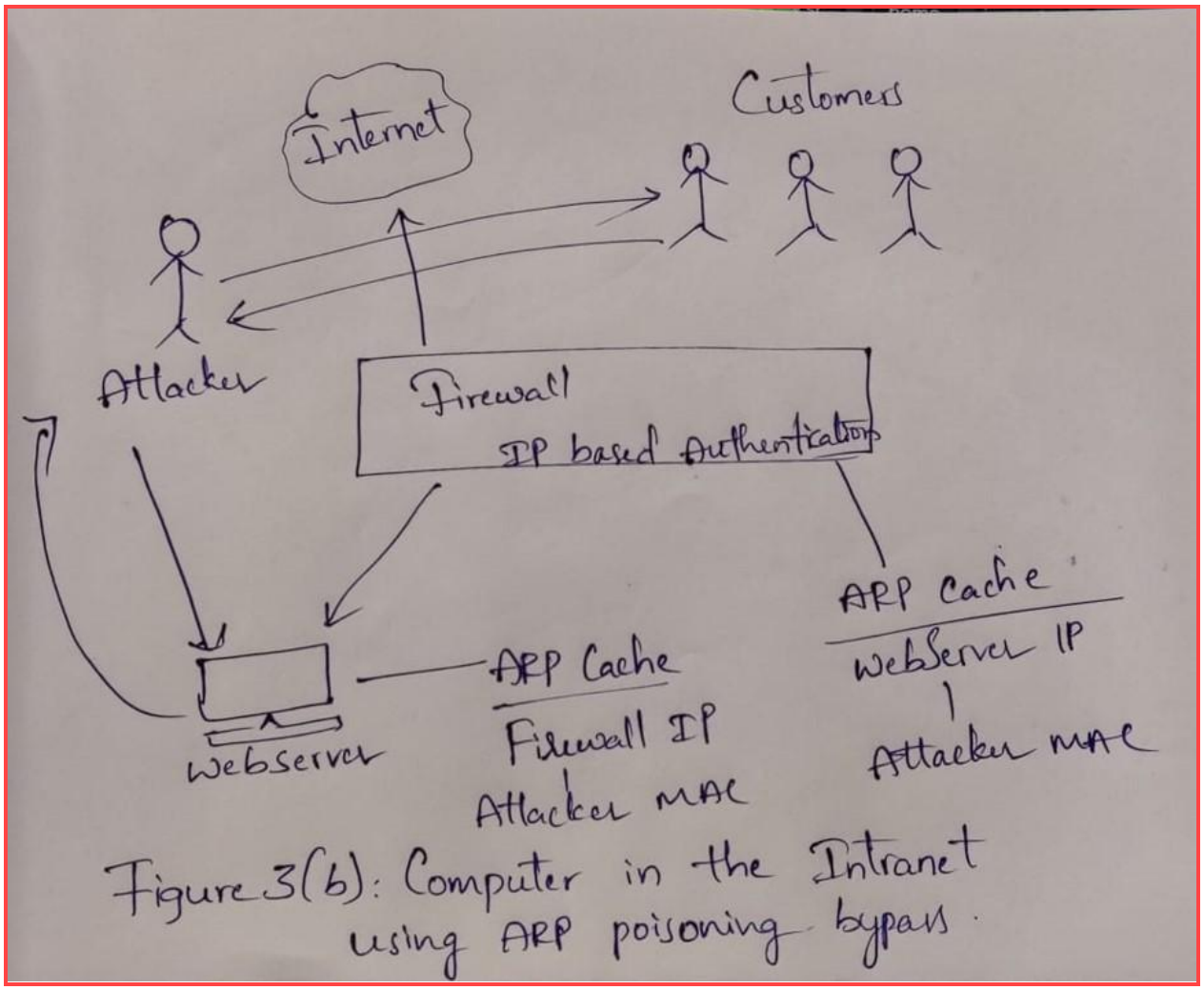


Figure 3(b): Computer in the Intranet using ARP poisoning bypass.

Question 4

9 / 10 pts

In ICMP protocol, type 11 error is “time exceeded” error.

(a) Please illustrate how we can implement the “traceroute” functionality to find out

the intermediate routers between two nodes A and B?

(b) We assume that every router will send out the ICMP packet back to the source.

If we line up the routers that send back the ICMP packets one after another, can

we be sure to get the complete path between A and B? Please explain the

reason.

Your Answer:

(**a**) Data that transfers from the source to the destination are mapped using the traceroute feature. Therefore, every router involved in the transfer will receive every packet. For instance, if we have two nodes A and B acting as the source and destination, the node A can determine the amount of hops by starting a TTL traceroute. Therefore, the packet will reach node A as the Time to Live decreases to zero for the purpose of tracing the first hop. Once more, Node A is able to determine the traceroute by setting the Time to Live to 2. The Time to Live value will continue to increase in this manner until the packet reaches its destination. From there, we can reach the point at which the packet was unable to move further. Please refer figure 4(a) for reference.

(b)With the assumption that each router would return the ICMP packet to the source, we can determine the full path from the source to the destination. Considering the path between node A and Node B, we cant be sure to get the complete path between the nodes as the path might be broken or intermittently connected.

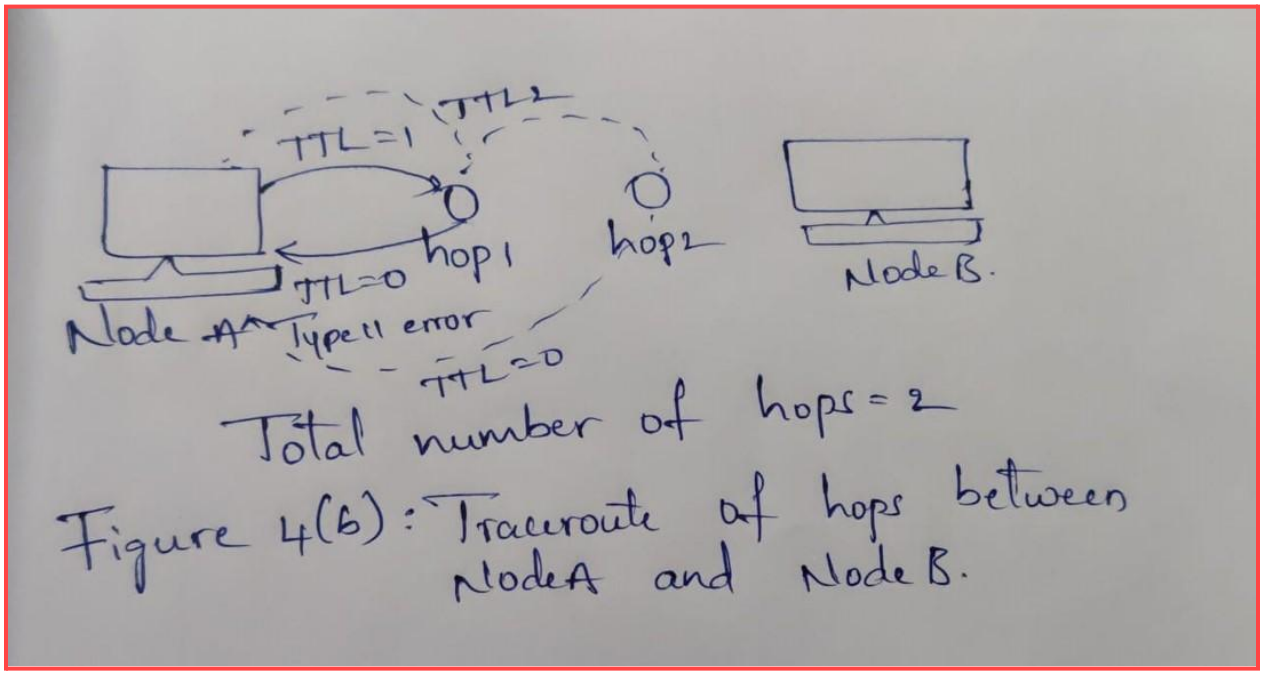


Figure 4(b): Traceroute of hops between Node A and Node B.

You failed to answer B sufficiently, the primary question was can we be sure to get the complete path. The answer is no we cannot.

Question 5

12 / 12 pts

A packet sent by node A has to penetrate three networks to reach node B. The

three networks have the MTU of 1500 byte, 820 byte, and 380 byte, respectively.

(Here the MTU will cover both the IP header and the IP data part, but not the

Ethernet packet part. For example, the 1500 byte MTU can contain a 20-byte IP

header and 1480 Byte data.) Now node A sends out an IP packet with 20-byte IP

header and 1440 byte of data to node B. The “Do not fragment” bit is NOT set.

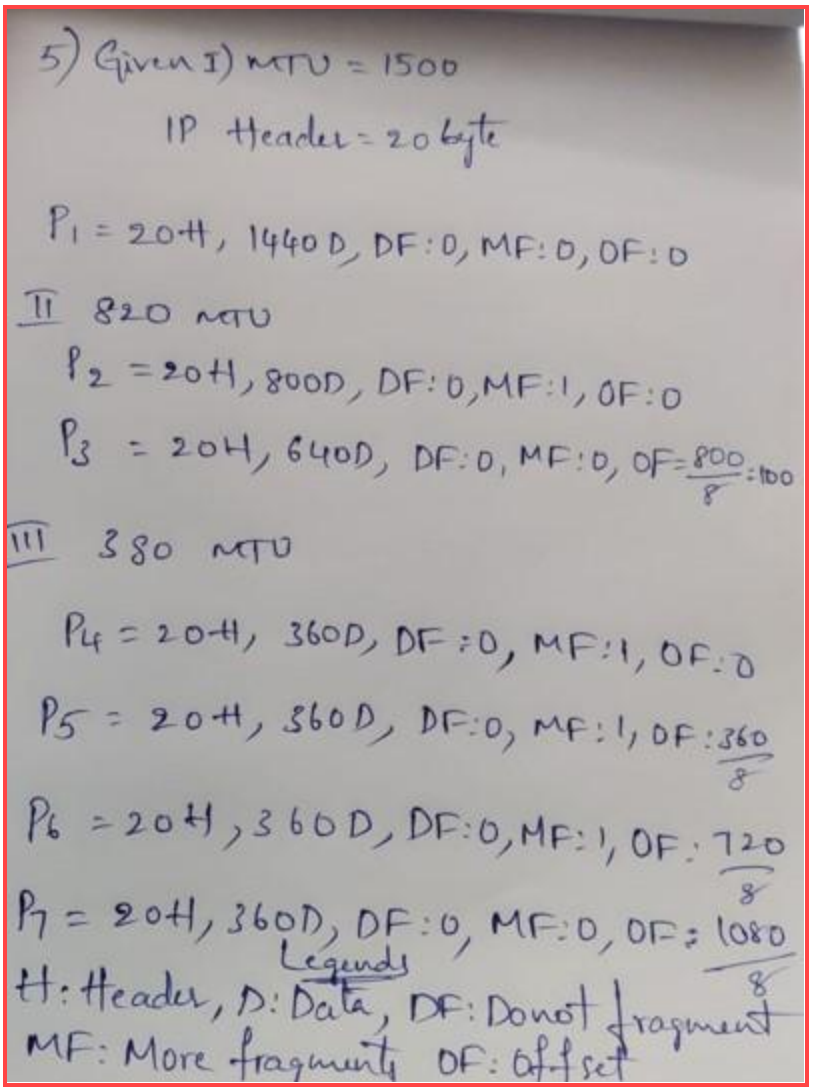
Please illustrate: the number of fragment packets in each network, the values of

the flag bits (both "Do not fragment" and "More fragment") for fragmentation in

each fragment, and the value of fragment offset in each IP fragment. Note that the

fragment offset value needs to fit in the 13 bits field.

Your Answer:



Question 6

5 / 6 pts

Please answer: Do we conduct the reassemble of the IP fragments at the

intermediate routers or at the final destination? Please also explain the reasons.

Your Answer:

There are several reasons to implement the IP fragments reassembling in this way. The main reason is that all the fragments may not flow in the same path while transferring from source to destination. Even this can be achieved by reassembling all the fragments at the particular router, but if we have multiple routers, the reassembling should happens at each and every router which takes long time to reach the destination. This delays the routing speed of the packet. Hence if we conduct the reassemble of the IP fragments at the intermediate routers or at the final destination the routing speed of the packet delays.

A better answer for your final sentence would have been "reassembly of IP fragments are done at the final destination".

Question 7

7 / 8 pts

In UDP protocol, port 13 is the “daytime” service. A time server that receives a packet

to its UDP port 13 will always return a packet to the requester’s IP and UDP port

and tells it the daytime of the server. If the server does not check the requester’s

port number, please illustrate how an attacker can send out one packet to a

daytime server and cause the ping-pong effect between two daytime servers.

Your Answer:

Assume there are two time servers, A and B, that operate similarly to how they do in the current case. The attacker sends a fake UDP packet with the source address of time server B and the source port set to port 13 to the time server A. In this instance, time server A returns the packet to time server B after assuming that the request originated from time server B. The packet will likewise be returned to time server A because time server B operates in the same way as time server A. Between time servers A and B, this series never ends. Time servers' bandwidth and processing power are used in this.

An illustration would have greatly assisted in this answer.

Question 8

6 / 6 pts

ICMP protocol error type 3 code 4 is “destination unreachable” caused by

“fragment needed but DF (do not fragment) bit set”. It will also report the MTU

supported by the network. Please illustrate: how can we use this kind of error to

identify the PATH MTU between a pair of nodes A and B?

Your Answer:

Each network has a maximum transmission unit (MTU) that determines how big a packet can be delivered (MTU). A larger packet is dropped if sent. Therefore, routers or other Layer 3 devices handle those and break them up into smaller pieces to ensure transparent end-to-end communication. As a result, a packet must be identified by its path MTU for effective transmission as it goes through numerous networks on its way from source to destination. Additionally, some packets have the Do not Fragment (DF) flag set, preventing further fragmentation. This could involve audio and video calls as well as packets of encrypted data. As a result, in this scenario, when DF is enabled and the packet is larger

Question 9

8 / 8 pts

In TCP, to improve the safety of the protocol, a node usually needs to select the

port number and the start of the sequence number randomly. Now we assume that

a popular operating system with the name of “Doors 2022” uses a random number

generator that is flawed. If two random numbers are generated very close in time,

the difference between them has 30% probability to be multiple of 265729 (which

is a prime number). Please explain how this flaw will impact the safety of TCP.

Your Answer:

The index in a packet/IP fragment counter that tracks each byte a host sends outside of its system. The sequence number will be raised by 1400 once a TCP packet is transmitted if it has 1400 bytes of data.

An attacker can spoof the TCP handshake if they can estimate the sequence number.

1. The attacker can bombard host A with packets by having host B send them to host A. There is a chance that this will result in a DoS attack.
2. The attacker can connect to B while pretending to be A, and B will attempt to send a reply, but it will never reach A due to the Denial of Service.
3. The attacker can go on communicating with B while pretending to be A if they can predict how B would increment its sequence number during the connection. The size of the data that B transmits is typically the increment. If the application protocol requests relatively fixed-sized answers from B for certain input, this can be inferred.
4. Service denial Attacks can be carried out by bombarding a server with bogus SYN packets or by sending SYN packets through a botnet (without spoofing). Due to the attacker never responding, A stores the connection information and sends SYN/ACK, which could cause the table entries to run out.

Question 10

1 / 1 pts

This question is intentionally left blank. If for Q1 to Q9 you need to draw some

figures, you can upload them here. Please note that you can upload only one file,

so please add all the figures into the single file and label clearly which question the

figures are for.

Sireesha_Midterm_NetworkSecurity.pdf

Question 11

1 / 1 pts

Bonus Question:

In your own words describe network security and why it is important.

Your Answer:

The art of preventing and guarding against unwanted access to corporate networks is known as network security. Network security is a mindset that contrasts with endpoint security, which is concerned with the security of specific devices. Network security is concerned with the connections and interactions between the various devices.

In order to keep the network connection stable, network security is crucial. If your network system is not protected for an extended period of time, your network will be open to various external cyber-attacks.

If your network's traffic volume increases significantly, it may put your network in an unstable state and make it more open to cyberattacks. So, defend yourself from cyber dangers by securing your network infrastructure.

Quiz Score: **73** out of 76

n