COMP 8670 Problem Set (Winter 2025)
due date: April 4, 2025

1. (10 points) **Printer Discovery Protocol Vulnerability Analysis** - A consortium of printer vendors have come up with a **great new protocol** to help users automatically discover the set of printers on their local network. In this protocol, when the user wants to print something, the user's computer automatically broadcasts a **Printer Discovery packet**. A Printer Discovery packet is a UDP packet whose destination address is the *broadcast address*, and whose source and destination port is **56184**. Because this is a broadcast packet, *every host on the local network will receive it.*

   Printers constantly listen for **Printer Discovery packets**. Any time that they receive one, they immediately respond with a **Printer Announcement packet**. A Printer Announcement packet is a UDP packet whose destination address is the *broadcast address*, and whose source and destination port is **56185**; its payload identifies the *name of the printer*, the *printer's IP address*, and any *special options supported by the printer* (e.g., 2-sided printing, color printing). The Printer Announcement packet is broadcast to the entire network, so that other hosts on the local network can also learn about this printer.

   Whenever a machine receives a **Printer Announcement packet**, it checks that the source address of the packet matches the printer's IP address found in the payload. In case of a mismatch, it *ignores the packet.* Otherwise, it accepts the packet and adds this printer to its list of known printers. If the machine's list of known printers already contains a printer with the same name, the machine *overwrites the previous entry* in its list with the information found in the newly received packet.

   Vicky the Victim is about to connect her laptop to a local switched Ethernet network. Her laptop will use this printer discovery protocol to look for a printer, and then Vicky will connect to one of the printers found in this way and send it a *sensitive corporate document* to be printed. Meanwhile, **Attila the Attacker's** computer is attached to this same network. Attila has the ability to inject packets onto this network and to receive all broadcast packets, but he cannot eavesdrop on other traffic. The printers are in locked rooms that Attila does not have access to, and Attila has not been able to hack or access any of the machines or printers attached to this network, so his only hope is to attack the printer discovery protocol.

   (a) (4 points) Can Attila arrange to learn the contents of Vicky's document without physically accessing any of the printers? If your answer is "yes," describe the attack; if your answer is "no", explain why this kind of attack is not possible. **NOTE: an ARP poison attack is not possible in this network**

   (b) (4 points) Describe two distinct Denial-of-Service (DoS) attacks that Attila could execute against the Printer Discovery Protocol. Explain the mechanisms of each attack. Furthermore, identify which of these two attacks could directly result in financial loss for the affected organization and justify how this financial loss would occur. **NOTE: an ARP poison attack is not possible in this network**

   (c) (2 points) Can Attila modify what is printed on the printer? In other words, Attila wants to replace Vicky's chosen document with something else Attila has chosen, hopefully without Vicky noticing. It's unacceptable if Vicky's original document gets printed in addition to Attila's replacement because then Vicky might notice and get suspicious; Attila is only interested in an attack that causes his document to be printed instead of Vicky's. Can Attila mount such an attack without physically accessing any of the printers? If your answer is "yes," describe the attack; if your answer is "no", explain why this kind of attack is not possible. **NOTE: an ARP poison attack is not possible in this network**

2. At Hilltop Academy, the school's IT department has recently upgraded the network infrastructure to support a seamless virtual classroom environment. As part of the upgrade, the network now heavily relies on internal web services to host educational resources, which are crucial for daily academic activities.

   Eva, an IT intern at Hilltop Academy, is tasked with maintaining the school's network and ensuring its security. She has been studying network protocols and security measures as part of her internship. However, she's new to practical network security and still learning about potential vulnerabilities and their implications.

   Meanwhile, Leo, a student with a keen interest in networking and cybersecurity, discovers the concept of ICMP Redirect attacks during his studies. Intrigued by the theoretical aspects, he decides to test his understanding on the school's network. Leo's intention is not malicious; he merely wants to see if such an attack is feasible and how it would manifest in a real-world scenario. The network structure is as follows:

   - Internal Web Service Server: IP Address 192.168.70.10 `NOTE: Different Subnet`
   - Eva's Workstation: IP Address 192.168.50.20
   - Leo's Laptop: IP Address 192.168.50.30
   - Default Gateway (Router): IP Address 192.168.50.1
   - Teacher's Workstation: IP Address 192.168.50.40
   - Student Workstations: IP Addresses ranging from 192.168.50.50 to 192.168.50.60

   Given the above network setup, Leo has successfully executed an ICMP Redirect attack. Using the script in Listing 1.

```
from scapy.all import *

# Configuration of IP addresses based on the Hilltop Academy scenario
# TODO: Assign the correct IP addresses based on the given scenario
gateway_ip =  " __GATEWAY_IP__ "
attacker_ip = "__ATTACKER_IP__"
victim_ip = "__VICTIM_IP__"
target_ip = "__TARGET_IP__"

# Constructing the ICMP redirect packet
# Type 5 is Redirect, code 1 is for host redirect
icmp = ICMP(type=5, code=1)

# The new gateway the victim should use
# TODO: Specify the gateway IP the victim should use (hint: it's the attacker's IP)
icmp.gw = "__NEW_GATEWAY_IP__"

# The IP layer for the ICMP redirect
```

```
19 # TODO: Set the source of the redirect (gateway's IP) and destination (victim's IP)
20 ip = IP(src="__GATEWAY_IP__", dst="__VICTIM_IP__")
21
22 # The IP layer of the original packet that triggered the redirect
23 # Typically, this would be a packet sent from the victim to an outside IP
24 # TODO: Mimic an original packet that the victim might send to the target
25 original_packet_ip = IP(src="__VICTIM_IP__", dst="__TARGET_IP__")
26
27 # Constructing the full packet (ICMP redirect + original IP header)
28 # The original packet is typically represented just by its header
29 # TODO: Combine the IP, ICMP, and original packet layers correctly
30
31 # Sending the packet
32 # TODO: Use the correct function from Scapy to send the crafted packet
33
34 #DONE!
```

Listing 1: Leo's script to implement the ICMP Redirect

(a) (2 points) What would be the source IP address and the MAC address in the ICMP Redirect message sent by Leo's Laptop to the Teacher's Workstation?

(b) (2 points) After receiving the ICMP Redirect message, what changes occur in the routing table of the Teacher's Workstation?

(c) (2 points) Indicate the new route (including the next-hop IP address) that the Teacher's Workstation will use to send packets intended for the Internal Web Service Server after the ICMP Redirect attack is successful.

(d) (2 points) What should be the content of the ICMP Redirect message to make sure the Teacher's Workstation routes the traffic as intended by Leo?

(e) (2 points) If Eva notices unusual network activity and investigates the traffic coming to and from the Teacher's Workstation, identify the signs that would indicate an ICMP Redirect attack is taking place.

3. Using the Python code in listing 1 answer the following

(a) (1.5 points) Replace the placeholders (`__ATTACKER_IP__`, `__VICTIM_IP__`, `__TARGET_IP__`, `__NEW_GATEWAY_IP__`, `__GATEWAY_IP__`) with the correct IP addresses based on the scenario provided.

(b) (1.5 points) Combine the `ip`, `icmp`, and `original_packet_ip` layers to construct the full ICMP redirect packet. On-Line 30

(c) (2 points) Use the appropriate Scapy function to send the crafted packet. On-Line 33

4. (12 points) Based on your understanding of Link-State and Distance-Vector routing protocols, answer the following questions:

(a) (3 points) Assume we are using Link-State routing for the network in figure 1 ”Network Topology A”. Is it possible to for oscillation problem to occur. Explain your answer by stating which router(s) and link(s) would be affected. (you may only assume the cost of existing links changed or a link failure)

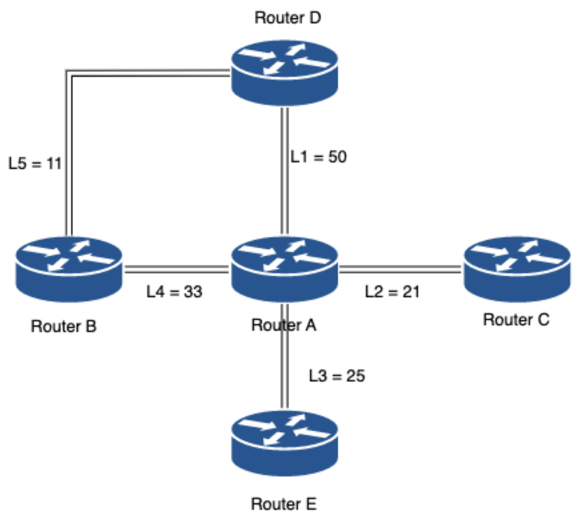

Figure 1: Network Topology A

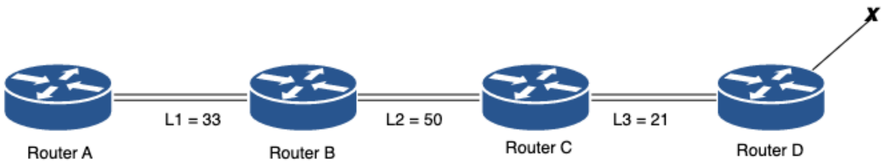

Figure 2: Network Topology B

(b) (3 points) Assume we are using Distance-Vector routing for the network in figure 1 "Network Topology A". Is it possible to for a routing loop problem to occur. Explain your answer by stating which router(s) and link(s) would be affected. (you may only assume the cost of existing links changed or a link failure)

(c) (3 points) Assume we are using Link-State routing for the network in figure 2 "Network Topology B". Is it possible to for oscillation problem to occur. Explain your answer by stating which router(s) and link(s) would be affected. (you may only assume the cost of existing links change or a link failure)

(d) (3 points) Assume we are using Distance-Vector routing for the network in figure 2 "Network Topology B". Is it possible to for a routing loop problem to occur. Explain your answer by stating which router(s) and link(s) would be affected. (you may only assume the cost of existing links change or a link failure)

5. (13 points) Consider we implemented a simple congestion control algorithm, where the window size is doubled as long as no congestion occurs and decreases by half when congestion is detected. Assume we do not have a slow start in our algorithm, and the algorithm uses a Selective Repeat approach for pipelining. Suppose we have zero transmission delay and infinite bandwidth. The algorithm works in units of packets rather than bytes and starts each connection with a congestion window equal to one packet. The Window size change when each packet in the pipeline has been acknowledged or timeout

   (a) (8 points) Show for sending 15 different packets (duplicate packets do not count), how the window size will change, and the packets sent in each window, assume that packet number 5 and 9 were lost the first time they were sent. You may use the following table to show your answer

Window Size	Packet Sent

Table 1: Question 2.a Section 3

   (b) (5 points) Assume that we set the initial estimated RTT to 20 ms and we measured the actual RTT for packets 2, 5, 9, 13 as shown in table 2. Calculate the estimated RTT for packet number 14.

Packet #	2	5	9	13
RTT	21 ms	19 ms	24 ms	22 ms

Table 2: Question 2.b Section 3

6. (15 points) Imagine you are tasked with designing a TimeSync protocol (a text-based application layer protocol) for time synchronization between multiple devices and a time server over a local area network (LAN). TimeSync uses the UDP as the transport layer protocol. Your objective is to create a protocol that ensures devices receive the correct time from the server and can tolerate a time drift of up to ± 30 seconds. A client device should be able to ask the time server for the current time and update its clock accordingly based on the server's response. Your design should consider the UDP communication characteristics and provide error-handling mechanisms. (**hint: delays might affect the time drift between server and client**)

   (a) (7 points) Define the message format for both time synchronization requests and responses in your protocol.

(b) (8 points) Sketch a timeline for the operation of your protocol in case of a simple time synchronization request and response with no error, and in case there is one error (e.g. time drift greater than 30 seconds)

7. (20 points) The RDT version 3.0 can handle crush failure (packet corruption and packet loss) but not time failure (long delay), as discussed in the lecture.. RDT version 3.0 operates on a stop-and-wait mechanism. It sends a single packet, then patiently awaits acknowledgment or times out before transmitting the next packet or retransmitting any lost packets. Moreover, RDT version 3.0 follows an alternating bit protocol (ABP), utilizing only two possible values for the sequence number: 0 and 1." Consider two hosts, A and B, communicating over RDT v3.0. Host A sends the message "CAT" to host B. Assume that each data packet can carry 1 byte (character), the sequence number and checksum.

   (a) (8 points) Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets exchanged between A and B. When B received the message "CAT" correctly, there was no crash or time failure.

   (b) (6 points) Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets between A and B. When B only receives the message "CA" and not "CAT" due to time failure. A and B will fail to detect that the message was sent incorrectly and terminate the connection.

   (c) (6 points) Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets between A and B. B only receives the message "CATC" and not "CAT" due to time failure. A and B will fail to detect that the message was sent incorrectly and terminate the connection.