Attacks tools to be implemented

1. ARP cache poisoning + Man-in-the-middle attack
2. Packet sniffing attack and sniff http/telnet passwords
3. HTTP / TCP Session Hijacking attack
4. DHCP starvation
5. DHCP spoofing
6. TCP SYN flood + DoS attack
7. Ping of Death + Ping flood attack
8. Port Scanning with OS information / version
9. Dictionary attack and Known Password attack
10. ICMP ping spoofing + ICMP redirect attack
11. ICMP smurf attack
12. ICMP Blind Connection-Reset + Blind throughput reduction attack against TCP
13. IP spoofing attack + DoS attack
14. TCP reset attack on Telnet
15. TCP reset attack on video streaming
16. Optimistic TCP ACK attack (streaming server)
17. MAC table flooding attack (of the switch)
18. DoS attack to the DNS server (using spoofed IP address)
19. DNS cache poisoning + Phishing attack
20. Wi-Fi password cracking attack

Note: You MUST program your OWN attack tool. You **MUST NOT** use any tool available in the Internet. It will be **mostly C/C++ code.** You must craft your own frame / packet / segment using your own code.

Each student of a group is responsible of **one attack tool**. Clearly mention this in the TOP SHEET of the design report and final report (the name and ID of the student who is responsible for specific attack tool)

Lab Reports

You should submit two lab reports. The report should cover the following sections:

- **Design report (Deadline: 13th Week)**
    a. Definition of the attack with topology diagram
    b. Timing diagram of the original protocol and your attack timing diagram with attack strategies
    c. Packet / Frame details for your attack and any modification in the header or so.
    d. Justification: why you think your design should work.

- **Final report & Implementation demo** (14th and 15th week)
    a. Steps of attacks, snapshots, victim screen, etc.
    b. Is your attack successful? Why do you think it was successful? Why not?
    c. Observed output in attacker PC, victim PC, and other related PC (server, client, etc.)
    d. Did you design any countermeasure for such an attack? How?

Marks Distribution

1. Design report : 20%
2. Implementation and successful demo: 60%
3. Final Report: 20%
4. **Bonus:** 10% bonus will be added if any group can design and implement defense mechanism of any attack tools.