Attacks tools to be implemented

1. ARP cache poisoning
2. HTTP / TCP Session Hijacking
3. DHCP starvation
4. DHCP spoofing
5. TCP SYN flood
6. Ping of Death
7. Port Scanning
8. Known Password attack
9. Dictionary attack
10. ICMP ping spoofing
11. ICMP redirect attack
12. ICMP smurf attack
13. ICMP Blind Connection-Reset
14. ICMP Source-Quench Attacks
15. Ping flood attack
16. TCP reset attack on Telnet / SSH
17. TCP reset attack on video streaming
18. Optimistic TCP ACK attack
19. MAC table flooding attack (of the switch)
20. DoS attack to the DNS server (using spoofed IP address)
21. DNS cache poisoning

Note: You MUST program your OWN attack tool. Each student of a group is responsible of **one attack tool**. Clearly mention this in 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: 27 July by 5:00 pm)**
  a. Definition of the attack with topology diagram
  b. Timing diagram of the original protocol and your attack timing diagram,your attacking 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 submission** (13th and 14th week)
    - a. Steps of attacks, snapshots, victim screen, etc
    - b. Is your attack successful? Why do you think it was successful?
    - c. Observed output in attacker PC, victim PC, and other related PC (server, etc)
    - d. Did you design any countermeasure for such attack? How?

Marks Distribution

1. Design report : 30% (Please meet me with the draft report before submitting design report)
2. Implementation: 50%
3. Final Report: 20%
4. **Bonus:** 10% bonus will be added if any group can design and implement defense mechanism of any attack tools.