Project 2025: Attack Tools Implementation

Attack 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
21. IPv6 Router Advertisement (RA) Flooding
22. Slowloris Attack
23. TCP Window Scaling Attack
24. Exploitation of Format String Vulnerability on a C-based logging server
25. ARP DoS via Gratuitous ARP Storm

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

Implement the assigned tool with your group member. Clearly specify in the report which member was responsible for each part.

Lab Reports

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

Design Report (Deadline: 11th 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 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