Network Security

- Sniffing programs: programs which can analyze the headers in a packet, for info like sender IP, receiver IP, sequence numbers etc.
  - Active sniffing: Sniffer acquires the packet because it is in the same network. Done only on broadcasted packets.
  - Passive sniffing: Packets are acquired by changing the default gateway of sender so that the packets get routed through the sniffer. Gateway is changed by *ARP spoofing*.
- ARP (Address Resolution Protocol):
  - Process of getting physical/MAC address from logical/IP address.
  - A request is broadcasted like "host with IP of x.x.x.x, send your MAC address". Every host in the network checks if the IP matches with it's own, and if it does, it sends a unicast with it's MAC address.
  - The MAC address is at that moment. It may change with time.
  - IP vs MAC address table is maintained in ARP cache, and it is cleared after some time.
- RARP: Reverse ARP. Gets IP from MAC.
- ARP Spoofing:
  - ARP cache is updated whether an ARP request is sent or not. If a spoofed ARP reply is sent, it will cause hosts to update the cache with wrong entry. This is called cache poisoning.
  - If a host C updates host A's cache so that it's cache contains entry of IP_B,MAC_C, and updates cache of B to contain entry IP_A,MAC_C, all messages that A and B send to eachother will go through C first. C can then alter the messages before forwarding to the meant destination.
  - If a single IP is poisoned from all hosts with some MAC address that does not exist, host with that IP will not receive any messages. This is a type of DoS attack.

war driving:can I find a wireless network? war dialing:can I find a modem to connect to? SQL injection cross site scripting