Agenda

- Packet Sniffing and Spoofing

Packet Sniffing

the process of capturing live data as they flow across a network.

- Administrator: understand network characteristics and diagnose faulty networks and configurations.
- Intruder: reconnaissance and exploitation.

Promiscuous Mode and Monitor Mode

- Promiscuous Mode: wired network. When in this mode, NIC passes every frame received from the network to the kernel, regardless of whether the destination MAC address matches with the card's own address or not.
- Monitor Mode: wireless network

Packet Spoofing

the process when some critical information in the packet is forged.

- TCP SYN flooding attack: source ip address;
- TCP session hijacking attack: ip addresses, port numbers, sequence number;
- DNS cache poisoning attack: DNS server's ip address.

Reference

A large portion of the material is adapted/copied from:

- Computer Security - A Hands-on Approach by Wenliang Du