

Network Security

Class X lab 25









Sniffing



monitoring and capturing all the packets passing through a given network using sniffing tools

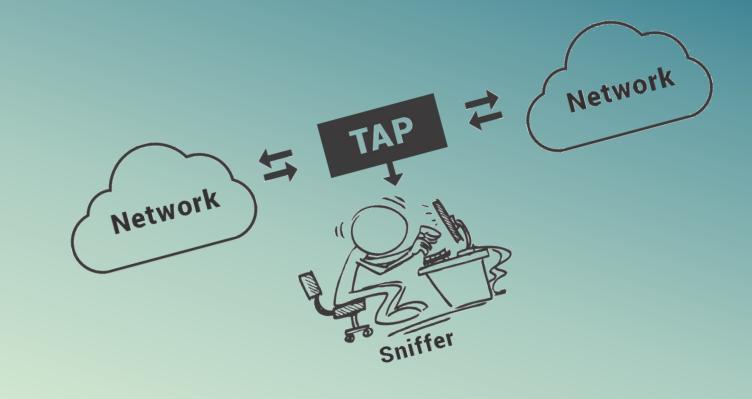






What can be sniffed?

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

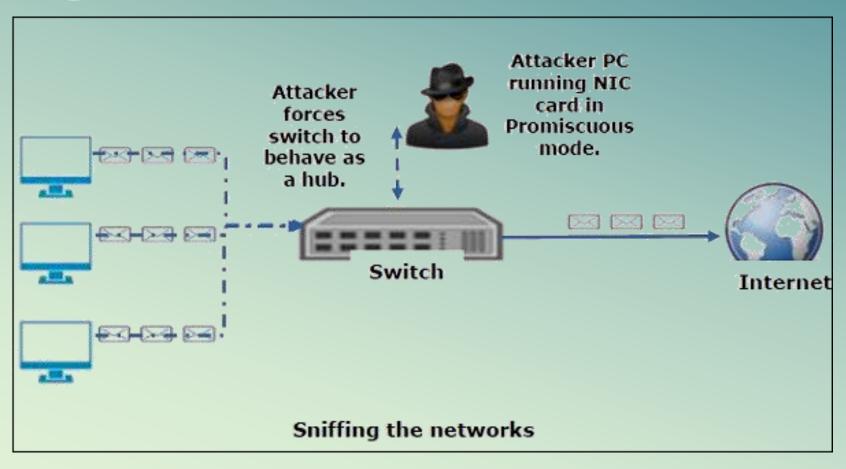








How Sniffing works?



A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment



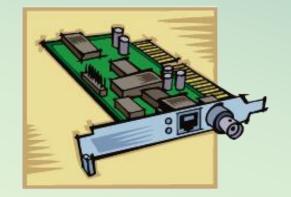




Types of Sniffing

- There are two types of sniffing
 - Passive sniffing
 - Sniffing through a Hub
 - Active sniffing
 - Sniffing through a Switch





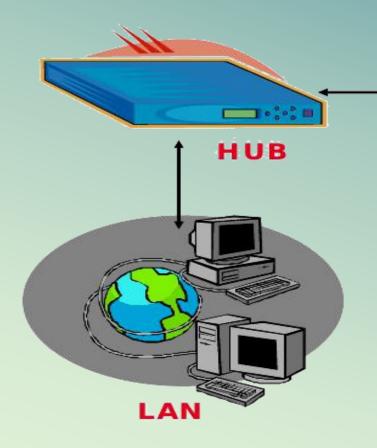








Passive Sniffing







- It is called passive because it is difficult to detect
- "Passive sniffing" means sniffing through a hub
- Attacker simply connects the laptop to the hub and starts sniffing







Active Sniffing

