07 Sniffing

Topics to be covered

- Hubs and switches and how they distribute traffic
- Flaws in ARP protocol
- MitM attack

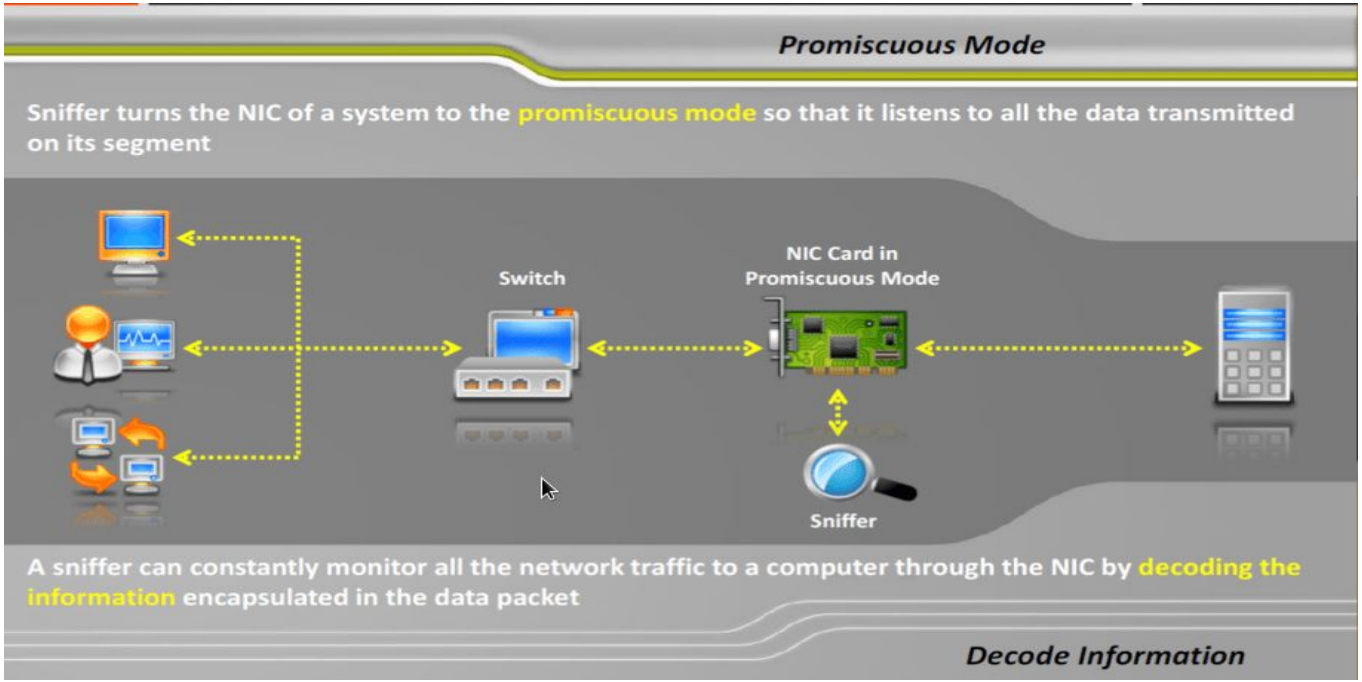
Packet Sniffing

It is the process of monitoring and capturing all data packets passing through a given network using software or hardware device.

It is a form of wiretap applied to computer networks.

Attackers use sniffers to capture data packets containing sensitive information such as passwords, account information etc.

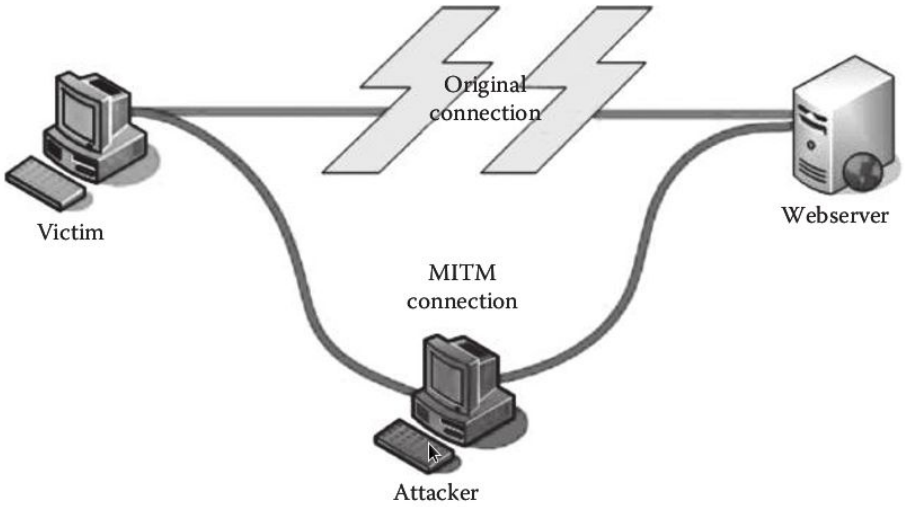
How sniffing works?



Types of Sniffing

- Active sniffing
  - Performed on switched network
  - Active sniffing involves injecting Address Resolution Protocol (ARP) packets into the network to flood the switch's Content Addressable Memory (CAM) Table, that keeps a track of which host is connected to which port
- Passive Sniffing
  - Performed on hubbed network

Man in the Middle (MitM) Attack



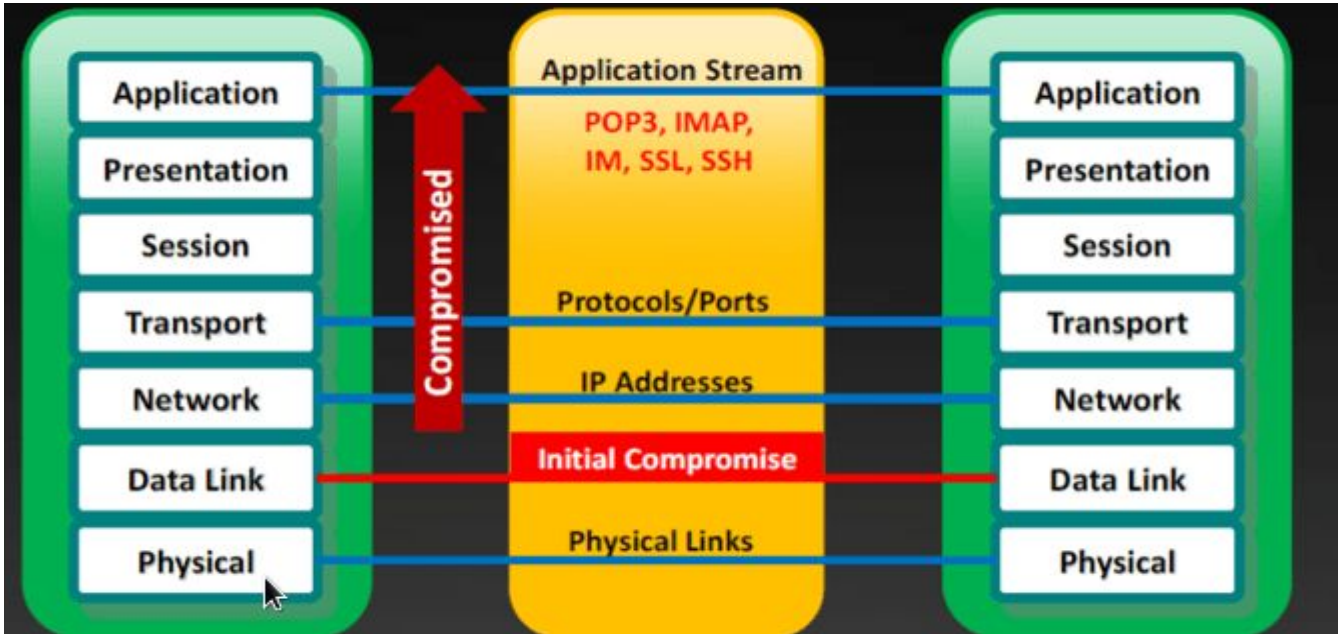
The idea behind a MITM attack is that the attacker places himself in the middle of the communication between a client and a server. Therefore, any communication that is being performed between a client and a server will be captured by the attacker.

Protocols vulnerable to sniffing

- HTTP
- Telnet
- POP
- IMAP
- SMTP
- NTP
- FTP

or any other protocol which doesn’t use ”s”, i.e. encryption in transit

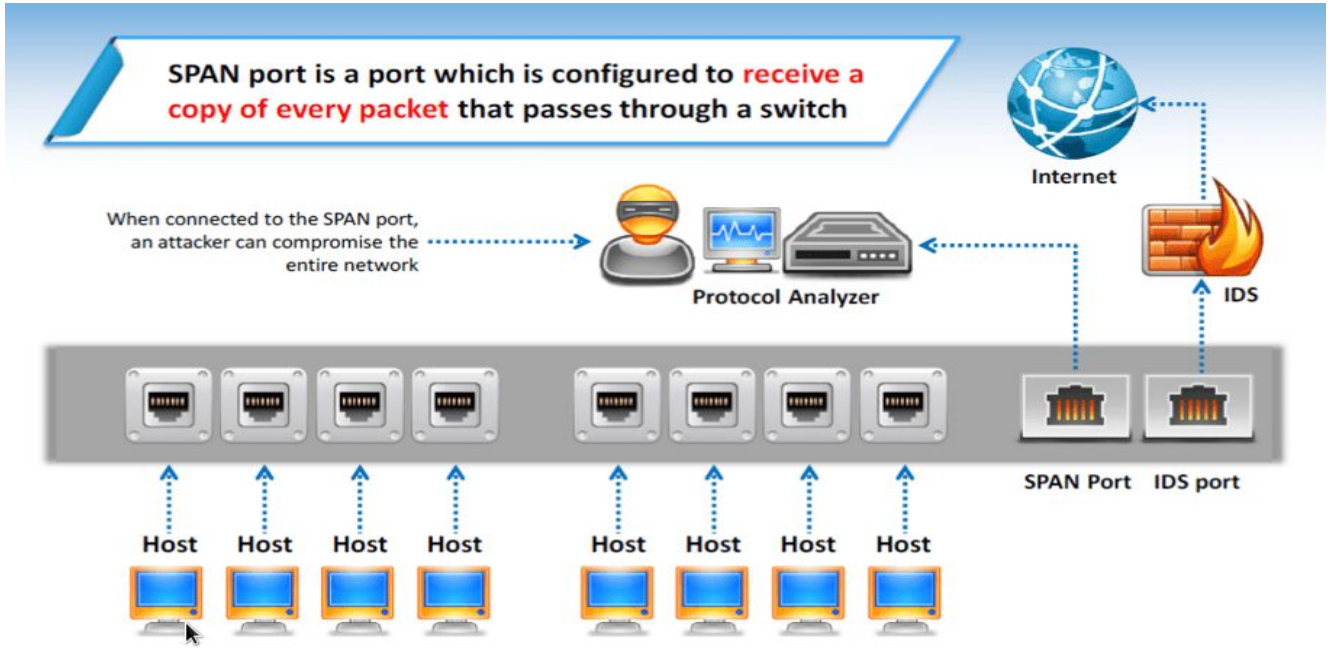
Sniffers working on Data Link Layer



SPAN port

SPAN stands for Switched Port ANalyzer by Cisco. It is a port which is configured to receive copy of every packet that passes through switch.

It does port mirroring. With port mirroring enabled, the switch sends a copy of all network packets seen on one port to another port, where the packet can be analyzed


SPAN port is a port which is configured to receive a copy of every packet that passes through a switch
Internet
When connected to the SPAN port, an attacker can compromise the entire network
Protocol Analyzer
IDS
SPAN Port
IDS port
Host
Host
Host
Host
Host
Host
Host
Host

Some Hardware protocol analyzers

- Colasoft Packet Analyzer
- Aligent packet analyzer
- Radcom Prismlite packet analyzer

Sniffing Methods

- MAC Flooding
- ARP Poisoning
- DNS Poisoning

Sniffing detection methods

- Observing the network traffic
- Observing ARP Table to detect ARP poisoning
- XARP Advanced ARP Poisoning detection tool