SNIFFING

WHAT IS SNIFFING?

You can think of sniffing as an illegal bridge. A method that captures, records, filters between you and your inbound data (packets). It is often used to capture passwords.

WHAT IS THE PURPOSE OF SNIFFING?

- Capture passwords (email, web, SMB, ftp, telnet, SQL),
- Email text,
- Transferred files (e-mail, ftp, SMB).

TYPES OF SNIFFING ATTACKS

1. Passive Sniffing

It is valid for systems with hubs, packets are transmitted to all computers in networks with hubs.

It is easy to sniff as the data in the network is sent to all computers over the LAN.

2. Active Sniffing

Applies to systems with switches.

The switch looks at the MAC addresses and sends the data only to the person who needs it.

The attacker tries to poison the switch, sending thousands of mac addresses, causing the switch to act as a hub and allowing data to exit all ports.

SOME OF THE PROTOCOLS THAT ARE VULNERABLE TO SNIFFING ATTACKS

1. HTML: Hypertext Transfer Protocol
2. TelNet: Client-Server Protocol
3. FTP: Used to transfer files between client and server.
4. POP Post Office Protocol
5. SNMP: Simple Network Management Protocol

TOP SNIFFING TOOLS

1. Wireshark
2. dSniff
3. Debookee

HOW CAN WE PROTECT FROM SNIFFING?

The best way to be protected is to encrypt network traffic. These packets do not prevent them from being captured but are a major obstacle to being read after capture. However, some applications such as AntiSniff can provide information about the presence of a sniffer on the network.

There are more than one tool to check whether there is a sniffer in the network, some of them are;

– Harp Watch

– Promiscan

– Prodetect