VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

Chapter 2: **Sniffers**

By
Dr. Ravi Verma

Outcome of Session

- **Students will be able to :**
- Explore the concept of Network Trapping through different Sniffing Tools and Techniques .
- Can list the tools used for Sniffing the network traffic as well as monitoring network activities.

Contents To Be Discuss

- Sniffing
- What can be Sniffed?
- How it works?
- Sniffing the Networks
- Types of Sniffing
- Active Sniffing
- Passive Sniffing
- Protocols which are affected
- Hardware Protocols Analyzer
- Lawful Inspections
- Sniffing Tools

Sniffing

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

Sniffing Cont..

- In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

- One can sniff the following sensitive information from a network –
- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

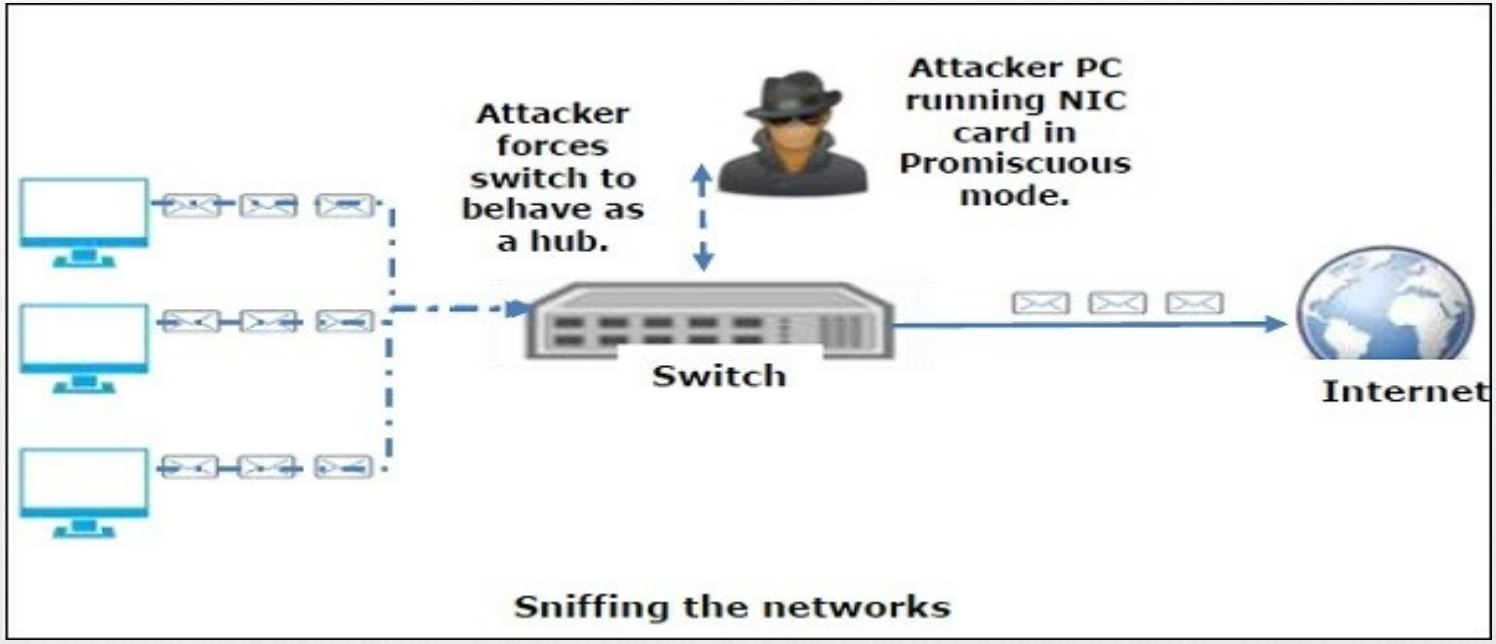
How it works?

- 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.
- Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC.

How it works? Cont..

- By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

Sniffing the Networks



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Types of Sniffing Cont..

- **Active Sniffing**
- In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Active Sniffing

- Following are the Active Sniffing Techniques −
- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected

- Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −
- **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.

Protocols which are affected Cont..

- **NNTP** (Network News Transfer Protocol)− It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- **POP** (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.

Protocols which are affected Cont..

- **IMAP** (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

Hardware Protocol Analysers

Before we go into further details of sniffers, it is important that we discuss about **hardware protocol analyzers**. These devices plug into the network at the hardware level and can monitor traffic without manipulating it.

Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.

Hardware Protocol Analysers

- They capture a data packet, decode it, and analyze its content according to certain rules.
- Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

Lawful Interception

- Lawful Interception (LI) is defined as legally sanctioned access to communications network data such as telephone calls or email messages. LI must always be in pursuance of a lawful authority for the purpose of analysis or evidence. Therefore, LI is a security process in which a network operator or service provider gives law enforcement officials permission to access private communications of individuals or organizations.

Lawful Interception

- Almost all countries have drafted and enacted legislation to regulate lawful interception procedures; standardization groups are creating LI technology specifications. Usually, LI activities are taken for the purpose of infrastructure protection and cyber security. However, operators of private network infrastructures can maintain LI capabilities within their own networks as an inherent right, unless otherwise prohibited.
-

Sniffing Tools

- There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones −
- **BetterCAP** − BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.

Sniffing Tools Cont..

- **Ettercap** − Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
- **Wireshark** − It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.
- **Tcpdump** − It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.

Sniffing Tools

- **WinDump** − A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.
- **OmniPeek** − Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.
- **Dsniff** − A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.

Sniffing Tools

- **EtherApe** − It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.
- **MSN Sniffer** − It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.
- **NetWitness NextGen** − It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.
- A potential hacker can use any of these sniffing tools to analyze traffic on a network and dissect information.

Question Please?

THANK YOU