SNIFFERS

Encryption At The Firewall

Internal LAN

Firewall encryption

Firewall decryption

Bad guy with snooping equipment
Table of Contents

- Introduction
- Sniffer Capabilities
- How Sniffer Works?
- Types of Sniffing
- Preventing Sniffing
- AntiSniff

Dr. Ajay Nagne
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.

Dr. Ajay Nagne
There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network.

Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.
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.
Sniffing is a process of monitoring and capturing all data packets passing through given network.

Sniffers are used by network/system administrator to monitor and troubleshoot network traffic.

Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.
Sniffers can be hardware or software installed in the system.

By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.
Packet sniffing: act of capturing data packets flowing across network.

The sniffer is a program/device that monitor data travelling over a network.

- **legitimate uses** to monitor network performance or troubleshoot problems: network audit, demonstrate insecurity of plaintext network protocols

- Also used by **hackers and crackers** to gather information illegally about networks they intend to break into: passwords, IP addresses, credit card numbers, protocols being used on the network and other information (binary data into something intelligible) that will help the attacker infiltrate the network.
Sniffers are almost as old as the Internet itself.
They are one of the first tools that allowed system administrators to analyze their network and pinpoint where a problem is occurring.
Unfortunately, crackers also run sniffers to spy on your network and steal various kinds of data.
A popular tool called **Antisniff**, which allows you to automatically detect sniffers running on your network.

Dr. Ajay Nagne
What are Sniffers?

- In a non-switched network, Ethernet frames broadcast to all machines on the network, but only the computer that the packets are destined for will respond.

- All of the other machines on that network still see the packet, but if they are not the intended receiver, they will disregard it.

- When a computer is running sniffer software and it’s network interface is in promiscuous mode (where it listens for ALL traffic), then the computer has the ability to view all of the packets crossing the network.
Sniffing motives:

- Getting username and passwords
- Stealing bank related/transaction related information
-Spying on email and chat messages
- Identity theft

Dr. Ajay Nagne
Sniffer Capabilities

- **Watch all network traffic** over any Network Interface Card (NIC) connected to the host machine: TCP, IP, UDP, ICMP, ARP, RARP. Also port specific traffic: http, ftp, telnet, ...

- **Forging ARP** replies: intercept packets from target host(s) on the LAN intended for another host on the LAN: effective way of sniffing traffic on a switch

- **Passive sniffing**: determine the local gateway of an unknown network – Data link layer (Hub)

- **Sniffing HTTP traffic**: output all requested URLs and do offline log analysis
Sniffer Capabilities

- **Active Sniffing**: Flood local network with random MAC addresses: switches will fail open in repeating mode, facilitating sniffing. This is no longer passive sniffing *(Switch)*

- **Password sniffing**: minimally parsing each application protocol, and saving the "interesting" pieces

- **Capture URLs** from a client to local web browser for display URL, updated in real-time: when the target surfs, the local browser surfs

Dr. Ajay Nagne
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

Dr. Ajay Nagne
How Does a Sniffer Work?

- Packet sniffer must be on the same network as the originating or intended destination machine.
- Remote sniffing: install some Trojan or backdoor program on one of the computers on either the sending or receiving networks they may be able to do the packet sniffing remotely.
- Trojan: malicious program disguised as a normal application (perform a desirable function for the user prior to run or install but steals information or harms the system).
- Backdoor: secret or undocumented means of getting into a computer system (is a method of bypassing normal authentication).

Dr. Ajay Nagne
How Sniffer Works?

- Most common way of networking computers – Ethernet

- Computer connected to LAN has two addresses – MAC Address (uniquely identifies each node in a network & stored on Network card), MAC is used by Ethernet protocol while building frames to transfer data to an from a system

- IP Address – used by applications.

- **Data Link Layer** uses an **Ethernet header** with the **MAC address of the destination machine** rather than IP address. The Network Layer is responsible for mapping IP network address to the MAC address as required by Data Link protocol.

- It initially looks for the MAC addresses of the destination machine in a table - called as ARP cache.
If no entry is found for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-network.

The machine with that particular address responds to the source machine with its MAC address. This MAC address then gets added to the source machine ARP cache.

The source machine, in all its communication with the destination machine, uses this MAC.
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. 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.
Attacker forces switch to behave as a hub.

Attacker PC running NIC card in Promiscuous mode.

Sniffing the networks
Packet sniffing is a technique of monitoring every packet that crosses the network.
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 the attacker is just hiding dormant and getting the information.

- **Active Sniffing**
  - As the name suggests, active involves some activity or interaction by the attacker in order to gain information.
1) 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.
2) 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 Techniques

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning
Protocols which are affected

- **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.

- **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.

Dr. Ajay Nagne
Protocols which are affected

- **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.

- **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.

Dr. Ajay Nagne
Preventing Sniffing

- Prevention: which network services send data in the **plain text**? default /old POP, SMTP, FTP, Telnet, News clients, ICQ, MSN and AOL Instant messengers send passwords in clear text

- When logging into e-mail services check if **encrypted login is supported**.

- Even if you login securely any e-mail you send is still in clear text, anyone on the path that the e-mail travels through can technically read it

- Use Encryption to encrypt the message so that no one on the path to the destination can read: **Pretty Good Privacy** ([http://www.pgpi.org](http://www.pgpi.org))
Preventing Sniffing

- **When shopping on-line** make sure the store has a "secure" connection for submitting credit card details:
  - standard SSL 128bit encryption
    - [http://wp.netscape.com/eng/ssl3/draft302.txt](http://wp.netscape.com/eng/ssl3/draft302.txt) and TLS RFC 2246 and previous lecture and lab)
- Telnet sends password and normal data in plain text:
  - **SSH encrypts connection** (RFC 4251 to RFC 4254 and previous lecture and lab)
- If possible use a Switch rather than a HUB on a LAN: efficient protection in practice (more work required to successfully sniff)
Indication/Detection of Sniffing

- **Difficult to detect that a packet sniffer is sniffing** a connection: passive act (the data is "logged" but unaltered). *Would* require physically checking all your Ethernet connections by walking around, and observing the output of `ifconfig -a` !!!

- A major clue: many DNS lookup are taking place **could** mean the sniffer is attempting to convert IP addresses to host names.
A stronger method of detecting packet sniffing: send an ARP request to the device in question to determine For promiscuous mode: in most cases assumption that it is the network card of the computer running the sniffer.

Defence against sniffing is not really prevention but rather providing security solutions so that even if large amounts of data is sniffed, not much use can be made out of it.

This is the major reason behind one-time passwords and encryption.
The DNS Test

Detection tool itself is in promiscuous mode. Create numerous fake TCP connections on same network segment, expecting a poorly written sniffer picks up on those connections and resolve the IP addresses of the nonexistent hosts.

Packet sniffers can perform reverse DNS lookups for the captured packets. When reverse DNS lookup occurs, a detection tool sniffs (promiscuous mode) the lookup request to see if the target is the one requesting resolution of that nonexistent host.
Indication/Detection of Sniffing

The Ping Test

- Construct an ICMP echo request with: IP @ of the suspected sniffing machine + mismatched MAC @.
- Most systems **should** disregard this packet because bad MAC @. Some Linux, NetBSD and NT systems, when the NIC is in promiscuous, the sniffer collects as a legitimate packet and respond.
- **Clever attackers** make that sniffer does not answer such packets.

Dr. Ajay Nagne
The ICMP Ping Latency Test

Ping the target and note the Round Trip Time (RTT) + create hundreds of fake TCP connections on our network segment at a lightning rate. Then observe if the target machine's network latency increases.

The ARP Test

Send an ARP request to target with a bogus destination MAC @. A machine in promiscuous mode would reply...
Sniffing Tools

- Wireshark
- dSniff
- Debookee
- BetterCAP
- Ettercap
- Tcpdump
- Windump
Wireshark

- An **opensource** packet capturer and analyzer.
- It **supports Windows, Linux** etc. and is a **GUI based tool** (alternate to Tcpdump).
- It used **pcap** to monitor and capture the packets from the **network interface**. The packets can be **filtered basis IP, protocol** and many other parameters.
- The packets can be **grouped or marked** basis relevance. **Each packet can be selected and dissected as per need.**

Dr. Ajay Nagne
It is used for **network analysis and password sniffing from various network protocols**. It can analyze a variety of protocols (FTP, Telnet, POP, rLogin, Microsoft SMB, SNMP, IMAP etc) for getting the information.

Microsoft network monitor: As the name suggests it is used for capturing and analyzing the network. It is used for troubleshooting the network. Some of the features of the software are Grouping, a Large pool of protocol support(300+), Wireless monitor mode, reassembly of fragmented messages etc.
It is a paid tool that can be used to monitor and analyze the network. It is able to intercept and analyze the traffic from devices that are in that subnet, irrespective of the device type (Laptop, devices, TV etc). It offers various modules:

- **Network analysis module**: scan for connected devices, Intercept traffic in a subnet, TCP port scanner, Network analysis and monitoring of HTTP, DNS, TCP, DHCP protocols, Analyse VoIP calls etc.

- **WiFi monitoring module**: Details of access points in radio range, wireless client details, wifi statistics etc.

- **SSL/TLS decryption module**: Support for monitoring and analyzing secured protocols.
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.

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.
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.

WinDump – A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.
A **sniffer** is a software or hardware tool that allows the user to “**sniff**” or monitor your internet traffic in real time, capturing all the data flowing to and from your computer.
In 1999, Antisniff was released. This product attempts to scan your network and determine if a computer is running in promiscuous mode. This is a helpful tool because if a sniffer is detected on your network, then 9 times out of 10, the system has been compromised. With Antisniff, administrators and security teams can finally get a handle on who is watching network traffic at their site. Antisniff was designed to detect compromised machines with IP stacks that a remote attacker could utilize to sniff network traffic.

Dr. Ajay Nagne
This happened to the Computer Science Department at California State University – Stanislaus.

Sniffer programs are used to capture passwords.

In order to protect yourself please change your password.
AntiSniff

Antisniff also helps you find those system administrators who run a sniffer to find out what is wrong with their local network, but forget to ask for authorization beforehand.

If you need to run a sniffer, then you should get permission in writing.

If your Security Administrator is running Antisniff, then there is a good chance they will find it and you will have to explain why you are running a sniffer without authorization.

Hopefully your security policy has a section on sniffers and will provide some guidance if you need to run a sniffer.
Antisniff can also be used by blackhats to find intrusion detection systems. If they know where your intrusion detection systems are, then they can become stealth attackers, causing you much pain because you just spend $150,000 on a new intrusion detection system and they found a way to bypass it.

Dr. Ajay Nagne
Thank You .....!