What is a Sniffing attack and How can you defend it?

**Introduction**

In this article, we will be discussing what is a sniffing attack and how you can save yourself or an organization from a sniffing attack. We will also cover some tools that can be used to perform sniffing and recover information. Sniffing in general terms refers to investigate something covertly in order to find confidential information. From an information security perspective, sniffing refers to tapping the traffic or routing the traffic to a target where it can be captured, analyzed and monitored. Sniffing is usually performed to analyze the network usage, troubleshooting network issues, monitoring the session for development and testing purpose. Since we have understood what basically sniffing is, let’s move on to know how it can be used to perform attacks.

**Define a Sniffing Attack**

Remember back in some movies, law agencies, and criminals used to bug the telephone lines in order to hear the calls that a person receives in order to get some information. This is a perfect example of sniffing attacks (Here's a resource that will navigate you through [cyber security attacks](https://www.greycampus.com/cyber-security)). This technology can be used to test the telephone lines and determine the quality of the call but criminals used it for their own illegitimate purpose. In the world of internet, sniffing can be performed using an application, hardware devices at both the network and host level. Any network packet having information in plain text can be intercepted and read by the attackers. This information can be usernames, passwords, secret codes, banking details or any information which is of value to the attacker. This attack is just the technical equivalent of a physical spy.

**Sniffing motives:**

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

**Types of Sniffing**

There are two types of sniffing- active and passive. As the name suggests, active involves some activity or interaction by the attacker in order to gain information. In passive the attacker is just hiding dormant and getting the information. Let’s discuss passive sniffing first.

**Passive Sniffing:**

This kind of sniffing occurs at the hub. A hub is a device that received the traffic on one port and then retransmits that traffic on all other ports. It does not take into account that the traffic is not meant for other destinations. In this case, if a sniffer device is placed at the hub then all the network traffic can be directly captured by the sniffer. The sniffer can sit there undetected for a long time and spy on the network. Since hubs are not used these days much, this kind of attack will be an old-school trick to perform. Hubs are being replaced by switches and that is where active sniffing comes into the picture.

**Active Sniffing:**

In a nutshell, a switch learns a CAM table that has the mac addresses of the destinations. Basis this table the switch is able to decide what network packet is to be sent where. In active sniffing, the sniffer will flood the switch with bogus requests so that the CAM table gets full. Once the CAM is full the switch will act as a switch and send the network traffic to all ports. Now, this is legitimate traffic that gets distributed to all the ports. This way the attacker can sniff the traffic from the switch.

***Let’s discuss some of the attack implementations in the network***

**MAC flooding:**

Flooding the switch with MAC addresses so that the CAM table is overflowed and sniffing can be done.

**DNS cache poisoning:**

Altering the DNS cache records so that it redirects the request to a malicious website where the attacker can capture the traffic. The malicious website may be a genuine looking website which has been set up by the attacker so that the victims trust the website. The user may enter the login details and they are sniffed right away.

**Evil Twin attack:**

The attacker uses malicious software to change the DNS of the victim. The attacker has a twin DNS set up already (evil twin), which will respond to the requests. This can be easily used to sniff the traffic and reroute it to the website that the attacker wishes.

**MAC spoofing:**

The attacker can gather the MAC address(s) that are being connected to the switch. The sniffing device is set with the same MAC address so that the messages that are intended for the original machine are delivered to the sniffer machine since it has the same MAC address set.

**How do you identify a Sniffer?**

Identifying the type of sniffer can depend on how sophisticated the attack is. It is possible that the sniffer may go undetected for a large amount of time hiding in the network. There is some anti-sniffer software available in the market to catch the intruders but it may be possible that the sniffers get away with it creating a false sense of security. A sniffer can be software installed onto your system, a hardware device plugged in, sniffer at a DNS level or other network nodes etc. Practical networks are complex and so it becomes difficult to identify sniffers. Since identification is tough, we will be discussing ways to render the sniffed information useless to the attacker.

Protocols vulnerable to sniffing attacks

As we are aware that the network follows a layered approach, each layer has a dedicated task that the next layer adds up to it. Till now we have not discussed that on what layer sniffing attacks happen. Sniffing attacks work on various layers depending on the motive of the attack. Sniffers can capture the PDU’s from various layers but layer 3 (Network) and 7 (Application) are of key importance. Out of all the protocols, some are susceptible to sniffing attacks. Secured version of protocols are also available but if some systems are still using the unsecured versions then the risk of information leakage becomes considerable. Let’s discuss some of the protocols that are vulnerable to sniffing attacks.

**1) HTTP:**

Hypertext transfer protocol is used at layer 7 of the OSI model. This is an application layer protocol that transmits the information in plain text. This was fine, when there were static websites or websites that did not required any input from the user. Anyone can set up a MITM proxy in between and listen to all the traffic or modify that traffic for personal gains. Now when we have entered into the web 2.O world, we need to ensure that the user’s interaction is secured. This is ensured by using the secured version of HTTP i.e. HTTPS. Using https, the traffic is encrypted as soon as it leaves layer 7.

**2) TELNET:**

Telnet is a client-server protocol that provides communication facility through virtual terminal. Telnet does not encrypt the traffic by default. Anyone having access to a switch or hub that connects the client and the server can sniff the telnet traffic for username and password. SSH is used as an alternate to the unsecured telnet. SSH uses cryptography to encrypt the traffic and provides confidentiality and integrity to the traffic.

**3) FTP:**

FTP is used to transfer files between client and server. For authentication FTP used plain text username and password mechanism. Like telnet, an attacker can sniff the traffic to gain credentials and access all the files on the server. FTP can be secured by sung SSL/TLS or can be replaced by a more secured version called SFTP (SSH file transfer protocol).

**4) POP:**

It stands for Post office protocol and is used by email clients to download the emails form the mail server. It also used plain text mechanism for communication hence it is also vulnerable to sniffing attacks. POP is followed by POP2 and POP3 which are little bit more secure than the original version.

**5) SNMP:**

Simple network management protocol is used for communication with managed network devices on the network. SNMP uses various messages for communication and community strings for performing client authentication. Community strings in effect are just like password that is transmitted in clear text. SNMP has been superseded by SNMPV2 and V3, v3 being the latest and most secure.

**Top Sniffing tools**

**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 (also consider checking this perfect guide for [cyber security certification](https://www.greycampus.com/cyber-security)).

**dSniff:**

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.

**Debookee:**

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.

**Precautionary measures against Sniffing attacks**

1. Connect to trusted networks: Do you trust a free Wi-Fi offered by the coffee shop next door? Connecting to any public network will have a risk that the traffic might be sniffed. Attackers choose these public places exploiting the user’s lack of knowledge. Public networks are setup and then may or may not be monitored for any intrusions or bugs. Attackers can either sniff that network or create a new network of their own with similar names so that the users get tricked into joining that network. An attacker sitting at an airport can create a Wi-Fi with the name of “Free Airport Wi-Fi” and the nearby users may connect to it sending all the data through the attackers’ sniffer node. The word of caution here is that you should only connect to the network you trust – home network, office network etc.
2. Encrypt! Encrypt! Encrypt! : Encrypt all the traffic that leaves your system. This will ensure that even if the traffic is being sniffed, the attacker will not be able to make sense of it. One thing here to be noted is that security work on defense in depth principle. Encrypting he data does not mean that now everything is safe. The attacker might be able to capture a lot of data and run crypto attacks to get something out of it. Use of secured protocols ensures that the traffic is encrypted and renders security for the traffic. Websites using https protocol are more secure than the ones that use HTTP – how is that achieved? Encryption.
3. Network scanning and monitoring: Networks must be scanned for any kind of intrusion attempt or rogue devices that may be setup in span mode to capture traffic. Network admins must monitor the network as well so as to ensure the device hygiene. IT team can use various techniques to determine the presence of sniffers in the network. Bandwidth monitoring is one, an audit of devices which are set to promiscuous mode etc.

Hope you enjoyed reading this article, feel free to post your questions in the comment section below.