

Forum:[Hack Forums](#)

Thread: [Wireshark Tutorial: Network & Passwords Sniffer](#)

SIM-4086413 - August 3, 2019, 2:11 pm

Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet. Network Sniffers are programs that capture low-level package data that is transmitted over a network. An attacker can analyze this information to discover valuable information such as user ids and passwords.

In this article, we will introduce you to common network sniffing techniques and tools used to sniff networks. We will also look at countermeasures that you can put in place to protect sensitive information been transmitted over a network.

Topics covered in this tutorialWhat is network sniffing?

Active and passive sniffing

Hacking Activity: Sniff Network

What is Media Access Control (MAC) Flooding

What is network sniffing?

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.

Network sniffing is the process of intercepting data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

Capture sensitive data such as login credentials

Eavesdrop on chat messages

Capture files have been transmitted over a network

The following are protocols that are vulnerable to sniffing

Telnet

Rlogin

HTTP

SMTP

NNTP

POP

FTP

IMAP

The above protocols are vulnerable if login details are sent in plain text

Passive and Active Sniffing

Before we look at passive and active sniffing, let's look at two major devices used to network computers; hubs and switches.

A hub works by sending broadcast messages to all output ports on it except the one that has sent

the broadcast. The recipient computer responds to the broadcast message if the IP address matches. This means when using a hub, all the computers on a network can see the broadcast message. It operates at the physical layer (layer 1) of the OSI Model.

The diagram below illustrates how the hub works.

A switch works differently; it maps IP/MAC addresses to physical ports on it. Broadcast messages are sent to the physical ports that match the IP/MAC address configurations for the recipient computer. This means broadcast messages are only seen by the recipient computer. Switches operate at the data link layer (layer 2) and network layer (layer 3).

The diagram below illustrates how the switch works.

Passive sniffing is intercepting packages transmitted over a network that uses a hub. It is called passive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcast messages to all the computers on the network.

Active sniffing is intercepting packages transmitted over a network that uses a switch. There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding.

Hacking Activity: Sniff network traffic

In this practical scenario, we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol. For this example, we will sniff the network using Wireshark, then login to a web application that does not use secure communication. We will login to a web application on <http://www.techpanda.org/>

The login address is admin@google.com , and the password is Password2010.

Note: we will login to the web app for demonstration purposes only. The technique can also sniff data packets from other computers that are on the same network as the one that you are using to sniff. The sniffing is not only limited to techpanda.org, but also sniffs all HTTP and other protocols data packets.

Sniffing the network using Wireshark

The illustration below shows you the steps that you will carry out to complete this exercise without confusion

Download Wireshark from this link <http://www.wireshark.org/download.html>

Open Wireshark

You will get the following screen

Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.

Click on start button as shown above

Open your web browser and type in <http://www.techpanda.org/>

The login email is admin@google.com and the password is Password2010

Click on submit button

A successful logon should give you the following dashboard

Go back to Wireshark and stop the live capture

Filter for HTTP protocol results only using the filter textbox

Locate the Info column and look for entries with the HTTP verb POST and click on it

Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded

You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

What is a MAC Flooding?

MAC flooding is a network sniffing technique that floods the switch MAC table with fake MAC addresses. This leads to overloading the switch memory and makes it act as a hub. Once the switch has been compromised, it sends the broadcast messages to all computers on a network. This makes it possible to sniff data packets as they sent on the network.

Counter Measures against MAC flooding

Some switches have the port security feature. This feature can be used to limit the number of MAC addresses on the ports. It can also be used to maintain a secure MAC address table in addition to the one provided by the switch.

Authentication, Authorization and Accounting servers can be used to filter discovered MAC addresses.

Sniffing Counter Measures

Restriction to network physical media highly reduces the chances of a network sniffer been installed
Encrypting messages as they are transmitted over the network greatly reduces their value as they are difficult to decrypt.

Changing the network to a Secure Shell (SSH) network also reduces the chances of the network been sniffed.

SummaryNetwork sniffing is intercepting packages as they are transmitted over the network

Passive sniffing is done on a network that uses a hub. It is difficult to detect.

Active sniffing is done on a network that uses a switch. It is easy to detect.

MAC flooding works by flooding the MAC table address list with fake MAC addresses. This makes the switch to operate like a HUB

Security measures as outlined above can help protect the network against sniffing.

Credits: www.hacking-tutorial.com

akela4you - August 3, 2019, 2:53 pm

nice post,i will be back to read it again

Bryan - August 4, 2019, 5:31 pm

so basically you could go to starbucks and wait for someone to login to gmail for example? or do large companies have preventative methods?

bonevirus - August 5, 2019, 6:20 pm

This is only for non encrypted / non secure websites.. i think if you were to try and view protected packets youll need to decrypt them right? im trynna see how i can avoid that. (I heard wireshark can decrypt some but not all packets)

destroyer.taker - September 3, 2019, 1:25 pm

nice info there man.. but i think all the websites that someone want to gain other account access are transmitting encrypted data so you wont see the actual data with wireshark i think ?!