**CS311: Data Communication**

**Assignment 1**

**Network Sniffing: Watch Your Friends' Network Activity**

Ashutosh Jatav (B16CS004) | Chinmay Garg (B16CS041)

**Introduction**

This report documents the steps to be followed to observe the network packets being sent and received by your friend’s device and to prevent yourself from such sniffing attacks.

We have used **THREE METHODS**  to carry out the sniff attack.

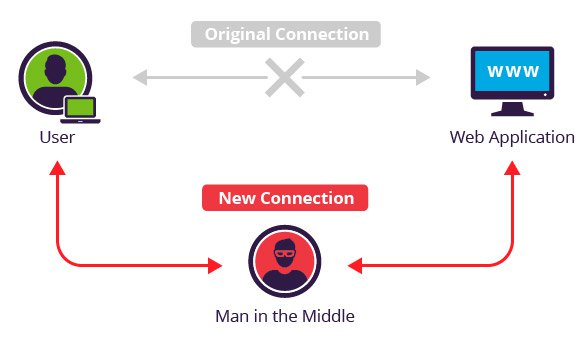
The first method utilizes the man-in-the-middle attack analogy and the others do not.

* Method I uses Arpspoof and Urlsnarf/Wireshark
* Method II uses packet sniffer written in python
* Method III uses TCPdump

**Method I**

**Man-in-the-Middle Attack**

A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. An MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.



In this method we used the following software:

1. Wireshark

Wireshark is a free opensource network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis.

1. Nmap

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

1. Arpspoof

This app redirects traffic on the local network by **forging ARP** replies and sending them to either a specific target or all the hosts on the **local network paths**. Arpspoof is a command line utility that allows you to intercept packets on a switched LAN. It redirects too packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

1. SSLstrip

Sslstrip is a tool that transparently hijacks HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial.

1. URLsnarf

Urlsnarf outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing with your favorite web log analysis tool.

**Procedure**

<https://ourcodeworld.com/articles/read/422/how-to-perform-a-man-in-the-middle-mitm-attack-with-kali-linux> The following steps were followed on Kali Linux referring the article given on above website:

1. Enable packet forwarding

The first thing you need to do is to forward all the IPv4 network packages. In this way your machine will act as a router. Execute the following command in a new terminal:



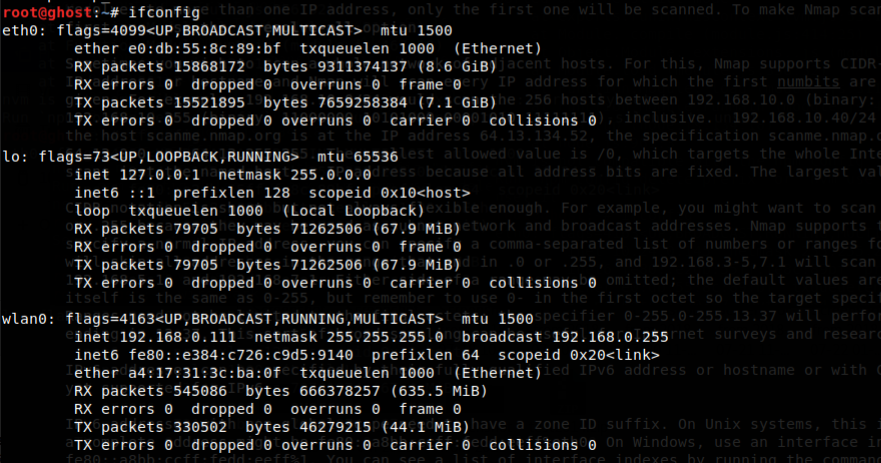
1. Get IP address of gateway

Execute the following command in the terminal:



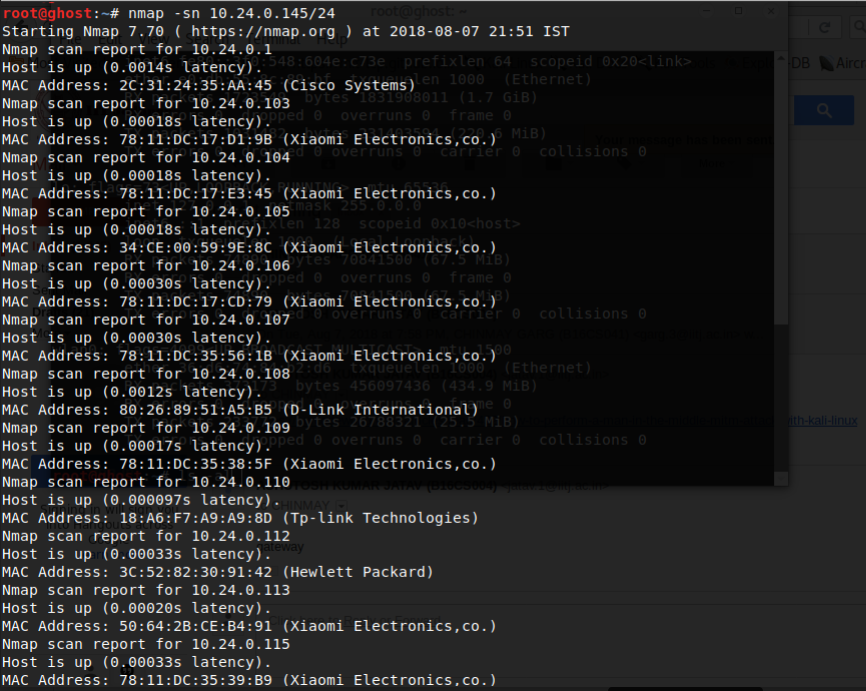
1. Get IP address of your system

Execute the following command in the terminal:



1. Get IP address of the victim

Identify the IP address of the target using Nmap. Execute the following command in the terminal:



1. Intercept packages from victim with arpspoof

The structure of the command to start intercepting packets from the victim to the router is the following:

arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]



1. Intercept packets from router with arpspoof

Now that you're intercepting packets from the victim to the router (running on a terminal), you need now to intercept the packets from the victim to the router with arpspoof. The structure of the command to start intercepting packets from the router to the victim is the following:

arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP]

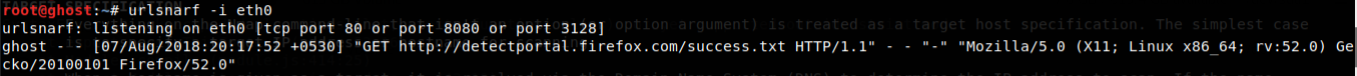


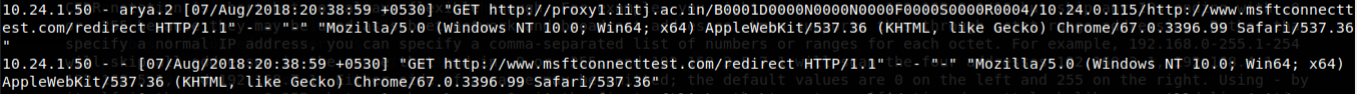
As you can see, it's the same command of the previous step but we switched the position of the arguments. Till this point you're already infiltrated to the connection between your victim and the router. Now you just need to learn how to read those packets using driftnet and urlsnarf.

1. Sniff URLs information from victim navigation

To get information about the websites that our victim visits, you can use urlsnarf for it. The structure of the command to sniff the URLs that your victim visits, is the following:

urlsnarf -i [Network interface name]



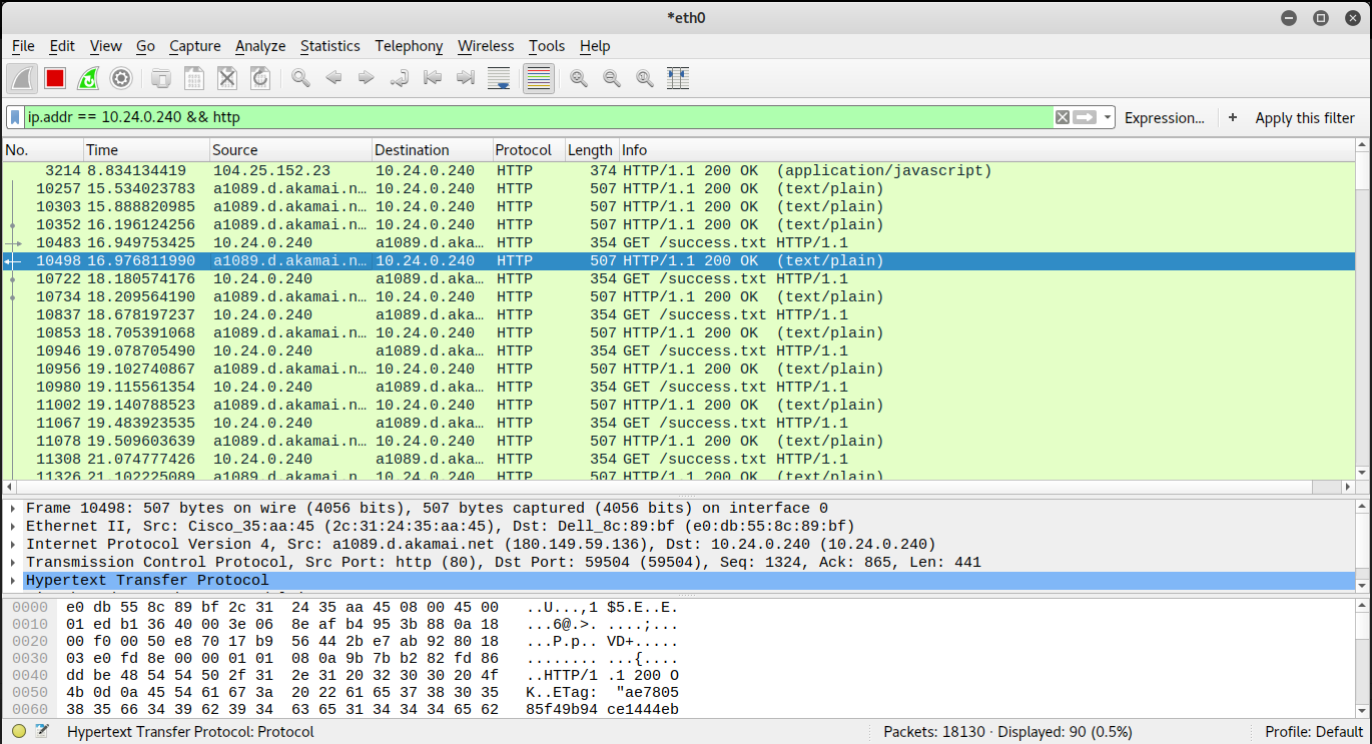


1. Using Wireshark

Open Wireshark and select the network interface you are using and start capturing the packets.

Apply the display filter:

ip.addr == [Victim IP] && http



1. Disable packet forwarding

Once you are done with your attack (you don't want to sniff anymore), remember to disable the packet forwarding in the system again executing the following command on a terminal:

sysctl -w net.ipv4.ip\_forward=0

**Method II**

Sniffers are programs that can capture/sniff/detect network traffic packet by packet and analyze them for various reasons. Packet sniffers can be written in python too. In this article we are going to write a few very simple sniffers in python for the Linux platform. Linux because, although python is a portable, the programs won’t run or give similar results on windows for example. This is due to difference in the implementation of the socket api.

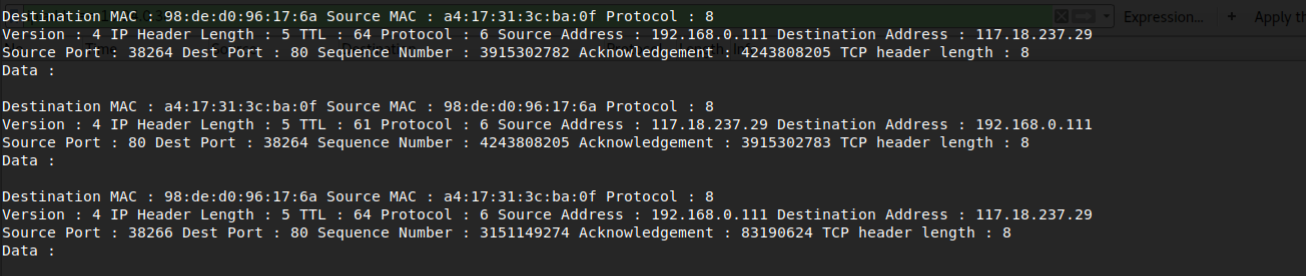
We used the script available on:

<https://www.binarytides.com/python-packet-sniffer-code-linux/>

The code file is also attached along with the assignment. The code breaks down the packet into IP Header + TCP Header + Data.

Write the following command to execute the python script:

$ sudo python tcp\_sniffer.py



**Method III**

In this method we have used tcpdump.

Tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

Tcpdump prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. tcpdump can write packets to standard output or a file. It is also possible to use tcpdump for the specific purpose of intercepting and displaying the communications of another user or computer.

Referring the article given on the website:

<https://danielmiessler.com/study/tcpdump/>

it is easy to see that this method is very simple. It can also be carried out along with an mitm attack.

