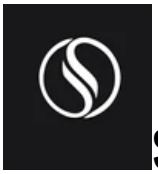
Project Proposal


Sniffer

Software Development Lab III (CSE-336)

Prepared By,

Name : Md. Mahamudul Hasan Roky

ID : 191311075

Semester : 9th

Batch No. : 20

Dept. of CSE, VU

Prepared To,

Md. Nour Nabi

Lecturer,

Dept. of CSE, VU

Introduction

The security of information in technology is increasing very rapidly where the most of the it lies between the transmission control sector of the TCP & UDP. To avoid the compromisation, there exist various kinds of capturing tool to ensure the exact transmission of packets. For instance, wireshark, netcat ensures the payload security and remote-control execution (RCE). Sniffer is one of the most advanced packets capturing tool among the other existing packets capturing tools with a specialized feature.

About Sniffer

Sniffer is designed with a dedicated framework in python programming language where it ensures 90% of packet capturing rate which lies in the cache or cookies of any kinds of clients and servers. It has the ability to analyze the protocol along with source and destination addresses of the payloads. It has also captured the encrypted (extensive markup language injection (XMLI) payloads.

Mission

Sniffer is committed to capture the exact data which lies between clients and servers with a satisfactory number of capturing rate. It has the ability to capture the manipulated protocol and encrypted data along with various kinds of injections where it ensures the protocol and payload security in the transmission control section of open system interconnection (OSI) and Transmission control Protocol (TCP) models. The main mission of ‘Sniffer’ is the figure out the deleted data in the server (cache/cookie).

Vision

Sniffer provides a simple vision with a long-term security of packets and protocols in clients and servers. It will be developed further with the help of cryptography and quantum computing to break the encrypted XML data in which it’s capturing now. Sniffer provides a simple vision called ‘no more manipulations’.

The Problem

Though sniffer provides a great layer of security. There exists some problems which are given below:

1. Linux OS is only recommended to run the script.
2. Only security professionals can run the script.
3. It has no ability of decrypt the XMLI data which you have to decrypt using another decryption tools.
4. Permission is highly recommended to run against any clients or servers.
5. Military servers are not allowed (for now).

Solution

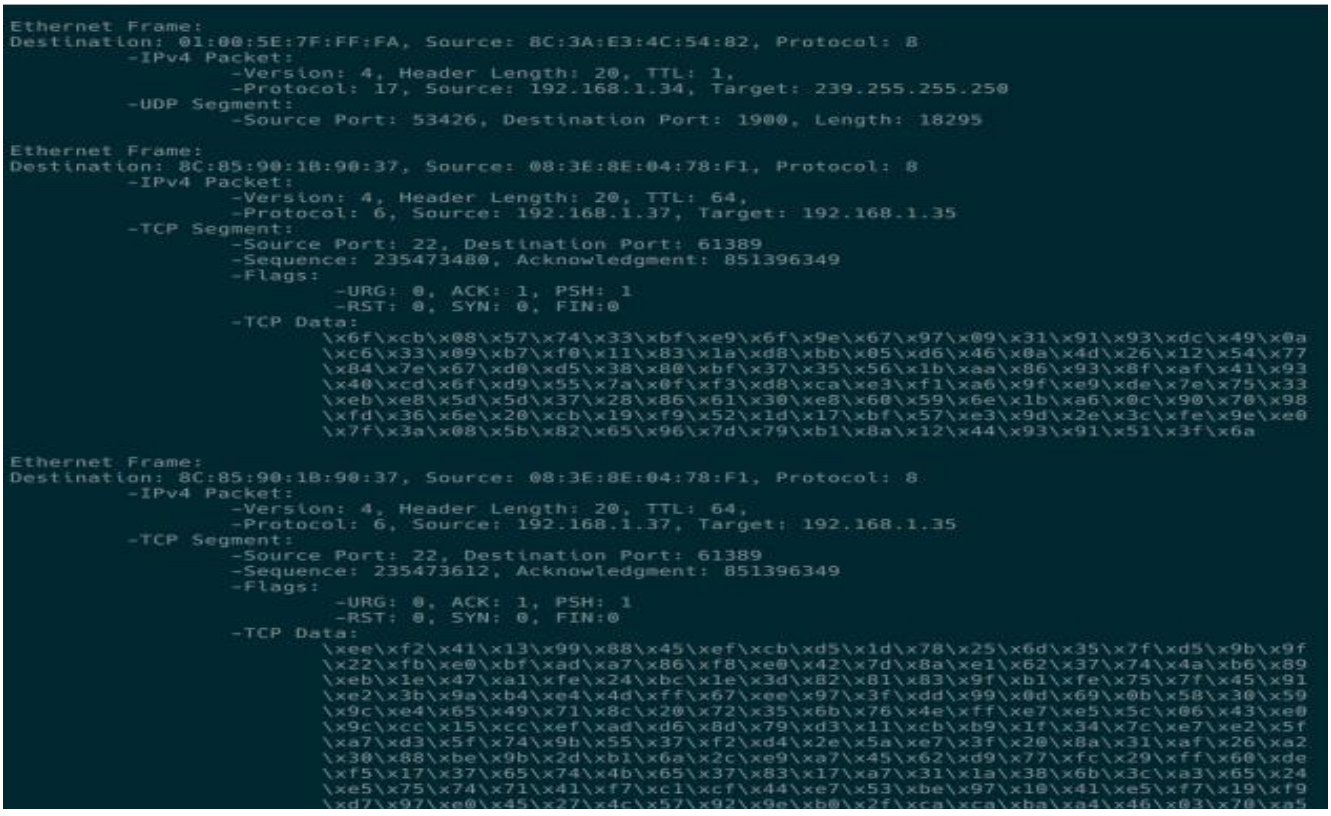
Sniffer has some minor problems compared to its advantages. It has a simple solution which is given below:

1. Customizable script.
2. Virtual Private Networks (VPN) are allowed.
3. Virtual boxes & VMware's are allowed on the same OS.
4. Sudo & Administrator's permission are not needed to run.
5. Promiscuous mode not mandatory for beginners.

Project Description

Phases	Title	Description
Project Name	Sniffer	The whole project has been developed by a scheduled manner to provide a tremendous layer of security named 'Sniffer'
Operating System	Linux	The project has been developed on Linux Operating system because most of the servers are managed by Linux which provides a flexibility of the project to run.
Programming Languages	Python	As python is a great high-level programming language. It's socket framework has been used to develop the project to manage simplicity.
Cost	N/A	The cost of the project will be mentioned by the developer at his/her own need.

Project Interface



References

1. **Instructor (Md. Nour Nabi):** The main part of the project provided the whole guidance of developing, presenting & played a great role in each part of the project.

2. **IBM Developer community** (additional): The community provided a great understanding of the corporate level project along with presentation tactics about the project through their webinar.

3. **PortSwigger Community** (additional) =: The community provided a great understanding of the projects background and contents presented in the proposal and final presentation.