Interview Memorandum

To: Dr. Jaime Acosta, Mr. Christian Murga, Mr. Caesar Zapata

From: Team 5

Subject: Interview Questions for Network Traffic Proxy System

Date: 10/02/2018

CC: Elsa Tai Ramirez, Jose Cabrera Maynez

We are Team 5, consisting of Julio De La Cruz, Oscar Galindo, Kevin Gonzalez, Isai Gonzalez, and Alan Caldelas, from CS4310 Software Engineering. The purpose of this memorandum is to request answers for Dr. Jaime Acosta, Mr. Christian Murga, and Mr. Cesar Zapata, so that we can have a further understanding of the Network Traffic Proxy System (NTPS) project. Our team understands you are the leading expert in the project and would like to clear up certain topics.

All information you share about yourself or the project will be kept confidential. Only with your written permission will the information provided by you be released to anyone outside of Team 5 and our instructors, except as required by law. We ask for permission to transcribe the answers you provide to our inquiry into a document that would act as an appendix to our documentation of the project requirements.

Our inquiry is composed of the following questions, please provided as detailed of an answer as possible.

* **Does the client desire to activate a hook as soon as it is loaded does it prefer the hook be loaded and then, if desired, activated?**
* **From the principal uses of the system, which are to intercept packets, to manage hooks, to configure proxy settings, and to modify packets, along with its possibilities of modification, for example to fuzz a packet is there any principal use for the system that the client deems as relevant and is being ignored? If so, please provide a detailed description of this main use of the system.**
* **When the client refers to interception does the client mean that the packets flowing in the network are directed to the computer system that is “intercepting” or does it mean that every packet going through the network is being copied into our system?**
* **Is the preference of the client that system converts all intercepted packages into PCAP files and build a queue out of the PCAP files, or that it creates a queue of just packets and then allow the creation of a PCAP file?**
* **In the context of the vocabulary used to describe the system is intercepting equivalent to capturing?**
* **With the new functionalities that some network sniffers offer should we consider an integrated solution, or still develop in separate the interceptor and the sniffer?**
* **Of the three original chains included in the iptables tool (I.e. forward, input, and output) which will the system use? Is the system required to provide access to a command line functionality to allow more intricate rules to be set?**
* **Having as a point of reference any generic network configuration please describe the role of the system in the context of how packets are traveling through our network. (To add a little more context, we are interested in a general description of what the system is really doing in regards to packet communication from the perspective of the network as an entity.)**
* **Does the visibility of packets in our system imply capture or capturing is the visibility of packets independent or capture?**
* **Should packets be represented as an editable file, or what kind of entity are packets formatted in terminals?**
* **Please provide an explanation about the role of NFQUEUE or similar tools in our system.**
* **Will the analyst have to be working with other software at the same time the analyst is using our system? If so, will the analyst also have to be using the command prompt or a terminal as well in order to set iptables, or use NFQUEUE?**
* **Please confirm if dropping packets is equivalent to a classical erasing operation or, else, describe in detail what the process involves.**
* **Should the system allow single packets to be saved as PCAP files?**
* **Should the analyst be able to save generated fuzzed packets?**
* **Should the analyst be able to forward single individual packets as well as PCAP files using the packet replayer?**
* **Should the system create a hook collection when a hook is imported into the system or should the system be able to load hooks directly as individual entities?**