**Project Status Report 1**

**Please answer the following questions and submit this doc to Blackboard as a PDF (similar to Lab Report submissions). Only ONE member of your team needs to submit, however I would encourage all team members to participate in and review this document prior to submission.**

1. **What project is your team working on?**

**ZEEK**

“Install the latest copy of Zeek and configure the file analysis modules to carve out objects from network traffic. Focus mostly on MS Office Documents (spreadsheets, documents, presentations), PDFs and PE executables. Build your VM such that objects extracted from Zeek will be dumped to a local directory where it can be analyzed by other tools. Write a small script in python that computes a SHA-256 hash of the object, performs mime-type classification (i.e. with filemagic) and performs a querty against VirusTotal to determine if the object is malicious or benign. Package everything into an analysis report and submit the VM. Demo this on a VM in the shared infrastructure.”

1. List your team members, and their GMU email address:
   1. Isaac Moscoso
   2. Manish
   3. Nancy Le
   4. Paul
2. **For each team member, briefly describe the planned role they have on the team, and provide some detail for what tasks they will perform (this can change over time, but please indicate the current state)**
   1. Isaac Moscoso – VM Build and ZEEK configuration
   2. Manish – Python Scripting
   3. **.**
   4. **.**
3. **What tasks has your team accomplished so far? (there is no “correct” answer for this)**
   1. Currently the following tasks have been completed
      1. Install the latest copy of Zeek
      2. Configure the file analysis modules to carve out objects from network traffic. Focus mostly on MS Office Documents (spreadsheets, documents, presentations), PDFs and PE executables.
      3. Build your VM such that objected extracted from Zeek will be dumped to a local directory where it can be analyzed by other tools
4. **What tasks does your team plan to accomplish within the next 2 weeks? (there is no “correct” answer for this)**
   1. Right now, with regards to the Ubuntu Server (Zeek), the next two weeks will involve testing. Zeek is currently configured to capture the necessary network traffic, and dump it into a local directory. It is configured but untested so we will be using a copy of the class Kali instance to download some of the files from a server and attempting to extract and deposit objects into the local zeek directory for further analysis by the python program.
5. **What questions do you have for the professor w.r.t. this project?**
   1. none
6. **Does your team have any concerns about finishing this project on-time? If so, what have you done so far to mitigate these concerns?** 
   1. None – we are amazing.