EE/CprE/SE 491 SDMAY-19

Weekly Report 3

16/2/2019 - 22/2/2019

Group number: ***5***

Project title: ***Cyber Network Capture Generator***

Client : ***Benjamin Blakely***

Advisor : ***Dr. Thomas Daniels***

Team Members:

Jacob Perin - ***Scribe***

Luke Tang - ***Meeting Facilitator***

Collin McElvain - ***Chief Architect***

Abdelrahman Baz - ***Chief Architect***

Hazem Abdeltawab - ***Test Manager***

Bernard Ang - ***Report Manager***

Weekly Summary

Team is moving towards combining project parts. However, the project has been broken into front end and back end for a long time. This will be a long process. Collin has been tasked with working with front end team. Some developing goals are adding structure to team commits (good GitHub practice), cleaning code (lots of experimentation to clean), and establishing clear-cut routes to back end logic. The back end team has split into necessary parts to establish an isolated network, automation of machines, and capture. However, these parts have all proven to be difficult to combine and each large in scale. Still developing.

Past week accomplishments

- • Bernard :
  - Worked to make sure that the web interface pulls data from the database and testing it with the admin function provided by DJango
- • Jacob :
  - Setup OpenStack environment to allow for control of contained VM from local host machine … (better for client & team)
  - Research into Ansible Modules -- external functionality such as support with openstack, below allows for instantiation of instances via ansible:
    - https://docs.ansible.com/ansible/latest/modules/os_server_module.html#os-server-module
  - Successfully deployed VM's with different OS on configured network.
- • Collin :
  - Working on Apache on our private IP given to us by ISU with Abdul. Also testing Ansible set up by Jacob.
- • Lucas:
  - Creation and modification of web crawling selenium scripts in python
    - Finished successful testing and implementation
  - Initial creation of unencrypted basehttp client/server setup on a localhost environment
  - Initial creation and experimentation of SSH on separate instances on a localhost
  - Created virtual environment with manual parameters in a separate KVM setup to test behavioral scripts
    - Pfsense successful
    - 2 ubuntu boxes successful
  - Initial research and experimentation with networking solutions in the virtual enviorment
- •Abdelrahman:
  - Got Apache working with MySQL and Django (Faced some package related difficulties at first)

- • Hazem :
  - Helped **Bernard** pair the front-end interface with MySQL

Individual contributions

Team member	**Contribution**	**Weekly**	**Cumulative**

		Hours	Hours
Bernard Ang	Made sure the interface pulls data from database	**6**	**15**
Collin Mcelvain	Working with Abdul on IP and researching some Ansible things.	**7**	**15**
Jacob Perin	Successful integration of ansible into OpenStack	**8**	**32**
Lucas Tang	Behavior Scripts and Networking	**8**	**24**
Abdelrahman Baz	Apache connection with the database	**6**	**18**
Hazem Abdeltawab	Pairing MySQL with front-end	**8**	**21**

Plan to accomplish for the next week

- Bernard
  - Make sure the details in the web interface are displayed properly
- Hazem Abdeltawab
  - Configure front-end interface to accept File types from back-end
- Jacob Perin
  - Work on networking problems.
    - WIP: OpenStack blocks suspicious network traffic … This will break application in several ways
      - Problem 1: Lucas Tang configured a PFSense box. Openstack will block traffic from incoming machine via custom firewall rules
      - Problem 2: The whole point of project is deploy and observe malicious network traffic. Firewall setup in OpenStack will break this.
- Collin McElvain
  - Begin making python scripts that will dynamically create the ansible file to configure VM. Also learn Python, should be quick.
- Abdelrahman Baz
  - Start looking into how to make the server routes to send the data between the frontend and the backend
- Lucas Tang
  - Further completion of behavioral scripts

- Further completion of new network enviornment