EE/CprE/SE 491 SDMAY-19

Weekly Report 6

8/3/2019 - 14/3/2019

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

This week, we continued the work from the previous week. We met with the client in a meeting and discussed on the timeline we had and the final product expected. The frontend team managed to set up the static IP but ran into multiple issues. The backend team worked on the creation of the VMs and scenario building

Past week accomplishments

- ❖ • Bernard :
  - ➢ Attempted to run the web interface on the static IP
    - ■ Ran into issues trying to access the website due to "permissions" of the database. Tried to search on ways to fix it but was unsuccessful.
    - ■ Researched more on the problem at hand.

- ❖ • Jacob :
  - ➢ Integration of Ansible to set up Ubuntu Virtual Machines
    - ■ Created a script to create a ubuntu virtual machine
    - ■ Wait until machine is set up and ready to be configured
    - ■ SSH into machine and install sample applications
      - ● Successful connection to internet
  - ➢ Cloned machine
    - ■ Backup and research into clonezilla to create "recovery iso" for passing machine to client for easy setup on custom box
      - ● Note: Box will still need to have 1 TB HDD and > 16 GB RAM due to LVM and VM Resource requirements.
- ❖ • Collin :
  - ➢ Begin implementation of Luke's scripts to complete MVP.
  - ➢ Working on usability of app.
- ❖ • Lucas:
  - ➢ Retained full functionality of 4 testing scenario scripts on real host machine configured from openstack:
    - ■ Client/Server transfer GET dummy.html
    - ■ Selenium successfully crawls at "human" pace
    - ■ Portscan successfully hits server and other VM
    - ■ SSH initial functionality retained
    - ■ Capture traffic on host with ovs-tcpdump -i tapb04af4a9-a6
      - ● Can view live or save to file
- ❖ •Abdelrahman:
  - ➢ Solved the DB permissions issue and was able to write data to the DB running on Apache.
  - ➢ Got the static IP to run smoothly with help from Collin

- ❖ • Hazem :
  - ➢ Created a test for connecting backend to frontend successfully

Individual contributions

Team member	Contribution	Weekly Hours	Cumulative Hours
Bernard Ang	Tried to fix issues of server with	**10**	**42**

	database but failed		
Collin Mcelvain	MVP work with Luke's scripts	**10**	**41**
Jacob Perin	Integration between Ansible, Openstack, and PFSense	**8**	**64**
Lucas Tang	PCAP capture to file from host and script migration and testing on host machine	**8**	**48**
Abdelrahman Baz	DB permissions and static IP	**10**	**48**
Hazem Abdeltawab	Prototype test	**8**	**45**

Plan to accomplish for the next week

- ❖ Bernard
    - ➢ Fix issues with the static IP
- ❖ Hazem Abdeltawab
    - ➢ Receive data from backend to display in frontend
- ❖ Jacob Perin
    - ➢ Documentation of OpenStack, Box Configuration, Libvirt + Open VSwitch Networking.
- ❖ Collin McElvain
    - ➢ Finish MVP work and have workable demo by presentation
- ❖ Abdelrahman Baz
    - ➢ Run some tests and fix bugs if found (server side)
- ❖ Lucas Tang
    - ➢ Hand off to Collin for automation process
    - ➢ Further develop SSH scenario to create, compile, and execute C code at regular human pace
    - ➢ Adapt scripts to accept parameters for proper automation handling