EE/CprE/SE 491 SDMAY-19

Weekly Report 4

23/2/2019 - 1/3/2019

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

Team continued working with their own parts. We met with the Dr. Blakely to discuss the future of the project and lowered the expected deliverables for the project. The front end worked on trying to make sure that the frontend can be combined with the backend whenever needed to produce a VM and getting a PCAP file from it. Progress has been slowed down due to minor issues with some of the softwares needed for the project for particular parts. All in all, the project has been shrank in some way to achieve the given deadlines and expectations.

Past week accomplishments

- • Bernard :
  - Changed the way the tests are displayed and made sure that the details tab was displaying every details of the test.

- • Jacob :
  - WIP (continued): OpenStack Network Configuration
    - Security: Disabling security features in OpenStack has proven to be a multi-step nightmare. It is difficult to configure custom setup features in OpenStack as it often stems across several services (neutron) to configure correctly.
    - https://docs.openstack.org/neutron/queens/configuration/index.html
    - There are two main options to disable (as found so far)
      - Security Groups (OpenStack firewall on network)
        - Blocks network traffic
      - Port Security (OpenStack port filtering on hosts)
        - Blocks undefined ip pairs
    - Initial testing shows success on this
      - (1) Machines can ping each other
      - (2) Can exhibit behavior not defined in security group (ARP, ICMP , etc.)
  - WIP(continued): Ansible Integration
    - Ansible playbooks ssh into machines to perform setup … However, Openstack network must allow for network traffic
      - Creates a dependency on first task functionality
  - WIP(continued): Local host network bridge configuration
    - Openstack connects machines to a defined bridge (must manually create an interface) that it can then connect vNics to …
      - LinuxBridge -- Network driver for deploying instances
      - Level 2 Routing? Hard to understand … Machines can ping gateway within network but are isolated from network traffic.
  - Until network is successfully setup Collin will not be able to test configuration of Ansible boxes. Further, Lucas cannot connect PFSense into network until successfully configured. This is a hindering dependence on future progress of project.

- • Collin :
  - Begin creation of Python scripts:
    - Create initial console gui to demo to client over how the scripts will dynamically create the machine based on options.
    - Create initial ansible file that can be reproduced and ran.
  - Finish up IP for website.
    - Helping Abdul get site up on our static IP, working right now, just need

database.

- • Lucas:
  - ➢ Further development of behavioral scripts
    - ■ Selenium fully functional
    - ■ Basehttp unencrypted functional on localhost, observable traffic on wireshark
    - ■ SSH non-functional
  - ➢ Further attempts at finalizing network configuration (connecting openstack initialization to the pfsense box with internet access)
    - ■ Patching attempts so far have been unsuccesful
- •Abdelrahman:
  - ➢ Didn't do much with the server routes (Collin took care of that)
  - ➢ Started looking into how to bind Apache to a static IP address, to access our web app from other machines.

- • Hazem :
  - ➢ Configured interface to accept File types from backend

Individual contributions

Team member	Contribution	Weekly Hours	Cumulative Hours
Bernard Ang	Changed the way tests are displayed	**8**	**23**
Collin Mcelvain	Creating dynamic Python scripts for ansible	**8**	**23**
Jacob Perin	WIP: Developing initial network structure for Ansible & PFsense with OpenStack VMs	**8**	**40**
Lucas Tang	Behavior scripts and Networking	**8**	**32**
Abdelrahman Baz	Research how to bind an IP address to Apache	**8**	**26**
Hazem Abdeltawab	Accept file types from backend	**8**	**29**

Plan to accomplish for the next week

- Bernard Ang
  - WIP :Fix the ways every page interact with database
- Hazem Abdeltawab
  - Prototype a first test scenario after backend successfully finishes
- Jacob Perin
  - WIP: OpenStack Networking
    - LinuxBridge is very simple. However, that is proving to add difficulty. No way to control the network flow outside of OpenStack is proving to create a problem for attaching network to own router (PFSense.)
    - Looking into more advanced alternative: OpenVSwitch … This will slow down development with research.
    - This is due to repeated failures with LinuxBridge … Requires reconfiguration of OpenStack
- Collin McElvain
  - Begin creating scripts to automate installation of application on target VM
- Abdelrahman Baz
  - Get the static IP binding to Apache step done (as I have been stuck for some time)
- Lucas Tang
  - Make the network function properly
  - Finalize behavioral scripts