EE/CprE/SE 491 SDMAY-19

Weekly Report 9

11/21/2018 – 11/26/2018

Group number: ***5***

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

Client : ***Argonne National Laboratory***

Advisor : ***Benjamin Blakely***

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, the team communicated mostly via slack to conclude the research and work to be done for this semester. The frontend team worked more on researching which webserver that will be suitable for our application while the front end team looked for more alternatives to the technologies that should be used in the project.

Past week accomplishments

As a team, we communicated through slack to finish up on the research that has been made in the past weeks. The frontend team worked on researching the advantages of apache and running tests using Django and Apache together. Collin, Jacob, and Lucas have diverged. Collin has taken time to re-orient frontend developers to make sure project is able to come back together in a logical manner. Jacob has continued work into finding a logical alternative to Vagrant technology, with some success.

- • Bernard :
  - Further research into Apache and how it would work well with the Django Framework.
  - Mostly tried to understand the documentation here and to get familiar with it: https://docs.djangoproject.com/en/2.1/howto/deployment/wsgi/modwsgi/
- • Jacob :
  - Further research into OpenStack. OpenStack documents ability to support work with Xen. Refer here: https://docs.openstack.org/ocata/config-reference/compute/hypervisor-xen-libvirt.html
  - This is hopeful. More importantly this has to eventually tie into Chef Provisioning. Since that is the goal. However, this also looks pretty good by documentation on Fog Driver for Chef, here: https://docs.chef.io/provisioning.html
  - More research needs to be done into proper packages on Ubuntu. In addition, alot of configuration is necessary to make sure this actually works as intended.
- • Collin :
  - Created simple mockups that may need updated later. Still a lot of confusion on the Scenario creation page.
  - Looking into selenium for scenario page.
- • Lucas:
  - Looked into further network features: Wireshark, PeStudio, RegShot, TotalCommander, ProcessExplorer, ProcessMonitor, Fakenet, ApadeDNS, Hexinator, Resource Hacker as tools to provide more insight beyond raw PCAP data.
- •Abdelrahman:
  - We decided, for now, to use Apache server with our project
  - Researched how to connect Django app to apache server and followed some tutorials
- • Hazem :
  - Created *mock* connections between the front-end (Apache + Django framework) against a fake back-end. Tests were successful. No problems occured with the connection.

Individual contributions

Team member	Contribution	Weekly Hours	Cumulative Hours
Bernard Ang	Researched on using Apache and Django	**7**	**54+ 7 = 61**
Collin Mcelvain	Researched on Selenium and created mockups	**7**	**48+7=55**
Jacob Perin	Hopeful progress with OpenStack Configuration. Documentation found for relevant parts. In addition, supports automated deployment.	**8**	**60 + 8 = 68**
Lucas Tang	Research potential enhancement technologies relevant to our project	**7**	**55 + 7 = 62**
Abdelrahman Baz	Apache with Django experiments	**7**	**54 + 7 = 61**
Hazem Abdeltawab	Mock connections between front and back end.	**7**	**67 + 7 = 74**

Plan to accomplish for the next week

- Bernard
  - Run tests to make sure Django works with Apache in my machine
- • Jacob :
  - Research into Ubuntu packages for proposed design.
  - Research into Configuration for proposed design
- • Collin :
  - Finishing the Selenium research
  - Finishing the Scenario Mockup page.
- • Lucas:
  - Research hypervisor vulnerabilities with malware detonation
- •Abdelrahman:
  - Try to connect our Django app to Apache server.
- • Hazem :
  - Make final tests to ensure the ability of the server to handle requests from the back-end, making sure that the server is in a good shape for the project.