EE/CprE/SE 491 SDMAY-19

Weekly Report 5

1/3/2019 - 7/3/2019

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, the team worked individually on parts that are assigned to them. In general, the frontend team was still in the process of getting the web interface to work as it is supposed to. The backend team ran more research and tests on the virtualization of the VM

Past week accomplishments

- • Bernard :
  - Changed the web interface and made sure that every values of the project was pulled from the database.
    - Made sure the pages pushed creation of server,client and scenario into the database.
- • Jacob :

- OpenStack
  - Disable Port Security
    - extension_drivers = port_security
    - **omit**
  - Disable Security Groups
    - firewall_driver = NoopFirewallDriver
    - **add**
  - https://docs.openstack.org/neutron/queens/configuration/ml2-conf.html
  - https://docs.openstack.org/neutron/queens/configuration/index.html
  - *Note: These options are both set for Neutron Networking in default configuration. However, since the goal of this project is to allow for malicious traffic we do not want it in our private network.
- Openvswitch bridge setup complete
  - This took a lot of testing (visual & manual wireshark observation)
  - br-int connects to br-isolated
    - br-int part of openstack
    - br-isolated routed to by br-int (through ovs logic)
  - configured br-isolated with private ip network 172.16.101.0 (Class C Block)
    - OpenStack DHCP boxes (Range 172.16.101.128-254)
  - *Note: This setup is fairly simple. However, it required knowledge of how openvswitch “peer-ports” work and how to set proper gateway & configure bridge in openstack.
- Router Configuration
  - Configure gateway on private network to outside web.
  - Lucas has done research into manual setup with PFSense, but I will do the initial setup on bridged network.
  - PFsense box (Gateway at 172.16.101.1)
    - *Note: On bridged network described above
  - Create 2 NICS:
    - LAN: 172.16.101.1
      - Attatched to br-isolated
      - http://docs.openvswitch.org/en/latest/howto/libvirt/
    - WAN: DHCP 172.16.99.X
      - Attach to Libvirt Network Created earlier in semester.
  - Successfully manually set up machines via openstack that route traffic through bridge and gateway on pfsense box.
- *Note: This will finalize my work on virtualization automation and isolated network configuration. From this point Lucas Tang will configure PFSense

Firewall rules & Squid proxy on PFSense. Also, Lucas will be manually testing behavior automation.

- • Collin :
  - ➢ Worked with Abdul and Hazem to fix DB issue on our static IP address
  - ➢ Working on backend routing and with Bernard on getting data.
- • Lucas:
  - ➢ Configure and test behavioral scripts on host VMs
    - ■ Lost functionality of server/client and ssh scripts
    - ■ Selenium and port scan functionality retained
  - ➢ Added and configured Squid to PFSense
  - ➢ Able to capture pcap on PFSense and monitor traffic in wireshark but need to capture a tcpdump using openvswitch
- •Abdelrahman:
  - ➢ Worked on Solving the permissions issue that prevents writing to the database. But still getting some errors
  - ➢ Worked with Collin on binding a static IP to our Apache server

- • Hazem :
  - ➢ Added some fixes for issues faced when connecting from backend to frontend

Individual contributions

Team member	Contribution	Weekly Hours	Cumulative Hours
Bernard Ang	Changed the interface and made sure of proper database interaction	**9**	**32**
Collin Mcelvain	Static IP fixes and backend connection to frontend	**8**	**31**
Jacob Perin	Configured openvswitch isolated bridge (LAN Network), Initial Setup of PFSense Router, & Successfully connected traffic to outside web through router	**16**	**56**
Lucas Tang	Migration to host VM	**8**	**40**
Abdelrahman Baz	DB permissions and static IP	**12**	**38**

Hazem Abdeltawab	Bug fixes	**8**	**37**

Plan to accomplish for the next week

- Bernard
  - Have static IP working with the web interface
- Hazem Abdeltawab
  - Prototype/ Testing
- Jacob Perin
  - Further develop Ansible Script to off-load work from Collin McElvain on machine creation.
- Collin McElvain
  - Working on finishing routes from frontend data to backend Ansible scripts.
- Abdelrahman Baz
  - Completely solve the DB permissions issue
  - Fix the IP and configure it to the newly provided one
- Lucas Tang
  - Capture PCAP using openvswitch and try to fix client/server and openSSH functionality