IOWA STATE UNIVERSITY
College of Engineering

Argonne NATIONAL LABORATORY

Luke Tang
Jacob Perin
Collin McElvain
Abdelrahman Baz
Hazem Abdeltawab
Bernard Ang

Benjamin Blakely, Cyber Security Researcher

With help from Dr. Thomas Daniels

Cyber Network Capture Generator

Senior Design Poster Session
April 2019
SD-MAY19-05

Summary

The needs to analyze traffic for hosts, applications, or services is essential in the world of computer security. Traffic is a way of describing how a computer sends information to the internet, and how the computer receives that information back. Traffic analysis is used to detect any malicious or harmful programs that can enter and harms one's computer, like a virus. Thus, preventing any undesired outcomes.

The solution of the problem is to create a program that automatically analyzes traffic data of many types, helping researchers create more innovative ways to combat malwares, and other unsafe softwares. This proposed program will not only serve as a catalyst for researchers to come up with potential solutions, but also provide a simple understanding of Traffic and its effect in computers.

Design Requirements

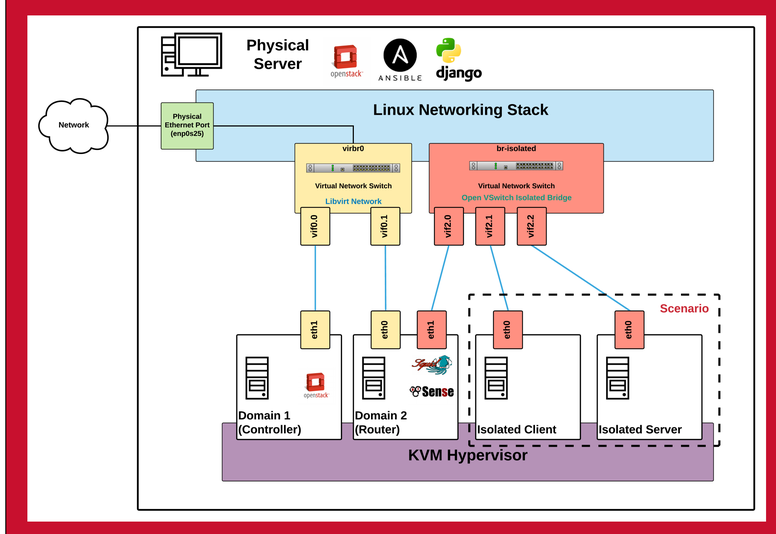
Functional Requirements

- The web application shall allow the user to create network capture from pre-determined combination of client, server, daemon(s), application, and activity
- While the virtual machines are active the server shall store network traffic to database
- The hypervisor software shall be remotely accessible through a web application
- The web application shall provide secure user authentication prior to access

Non-Functional Requirements

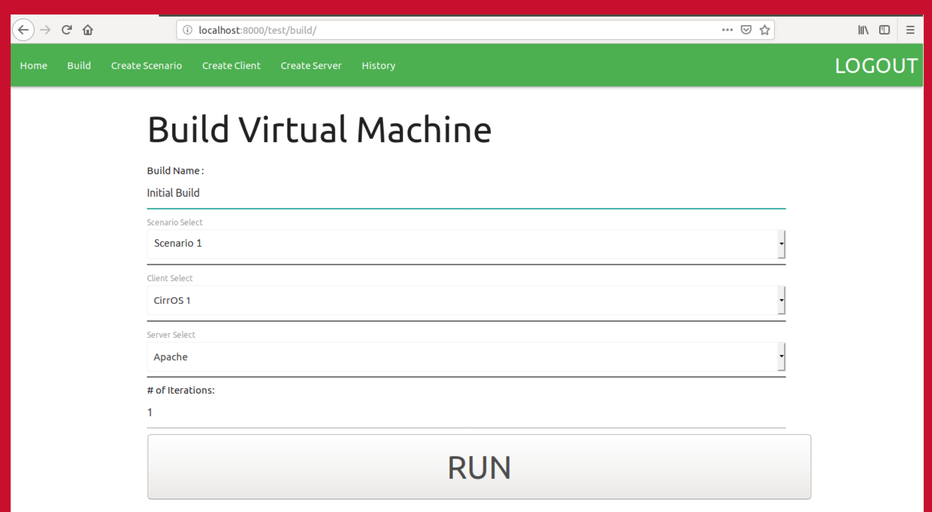
- Usability: All functions will be accessible through a web application
- Cost: No costs associated with software as everything is open source

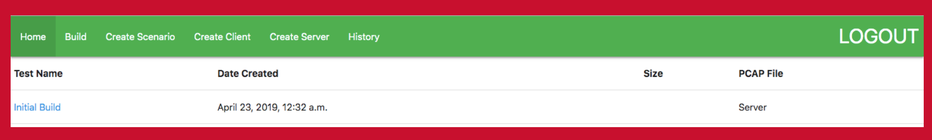
System Architecture and Design



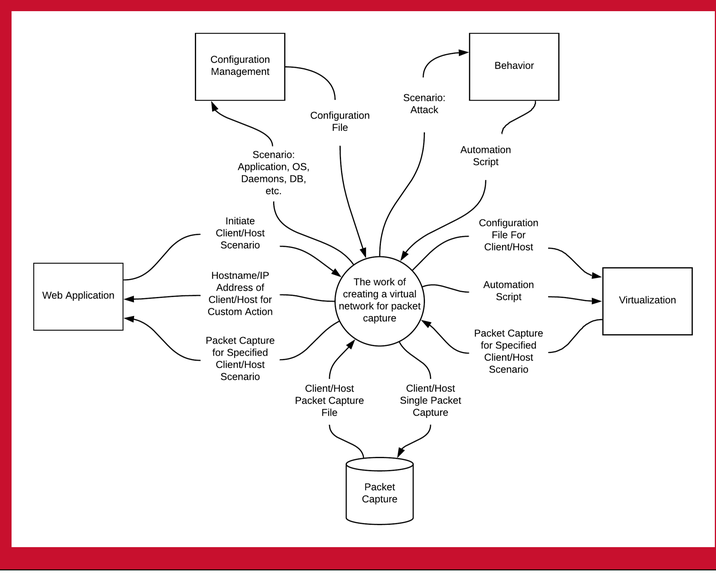
System Architecture Diagram

Web Application for front end user client





Context Diagram



Testing and Evaluation

Frontend

- User selects scenario,server, client and number of iterations and build's the VM
- User selects applications and updates the MySQL Scenario database
- User selects operating system for server and client and updates the MySQL database

Backend:

- PCAP capture on HTTP client/server requests between two virtual machines
- PCAP capture on nmap portscan from one virtual machine to another
- PCAP capture on SSH requests between two virtual machines
- PCAP capture on Selenium Weblcrawler impersonating human traffic

System Implementation

- Ansible
- MySQL
- Openstack
- PFsense/Squid
- Python 3
- Django
- Selenium
- KVM Hypervisor

Applicable Standards and Best Practices

PEP8
- Code styling standard for all python code

CAPEC
- Active catalog of attack vectors
- Tasks executed in our application for any given attack scenario should correlate directly to the matching vector described in cataloged attack scenario

IEEE Standard for Local and metropolitan area networks - Bridges and Bridged Networks
- Background: Network developed must contain malicious traffic to specific host and client. Accomplished by bridging the traffic generated by each host through a proxy.

Conclusions

This project required several iterations of functional testing before arriving with a working prototype. Free opensource contraints on all technology left us limited with a trial and error process to find compatibilities between differing technologies. Our team was forced to abandon Chef, Apache, Xenserver and many other options after extensive research and development. In the end our entire team learned extensively about Networking, Web Applications, and Virtualization.

Special Thanks to: Dr. Joseph Zambreo, Dr. Thomas Daniels, Dr. Manimaran Govindarasu