The Center for Cyber Defenders

Expanding Computer Security Knowledge

SAND2015-5780C

Technology Testing with Emulytics

Project Mentor: Melissa Tucker, 9526

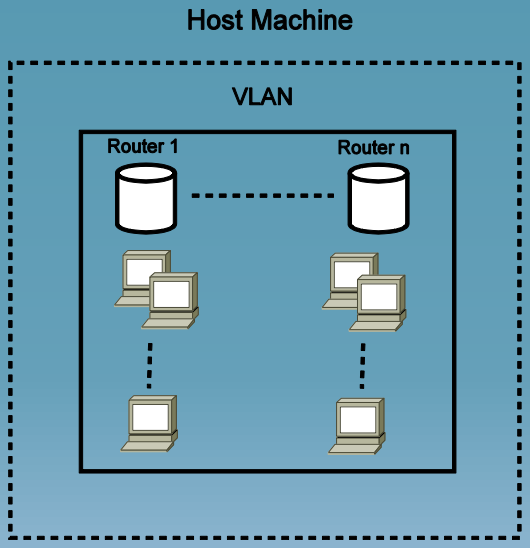
Justin Cox, Utah State University; Rain Dartt, Rose-Hulman Institute of Technology;
John McCloud, New Mexico Institute of Mining and Technology

Problem Statement:

Many technologies are built to deal with the ever-changing needs of digital security; however, they must be tested for performance and efficacy in several environments. Such testing is done as part of The Technology to Practice (TTP) Project.

Minimega:

Minimega is an advanced emulytics platform developed at Sandia National Laboratories by David Fritz. It allows for sharing actual resources of a single host amongst thousands of virtualized machines. It is particularly useful for determining the reliability of software in high-availability, large-scale networks.



Objective and Approach:

- Develop Testing Framework:
  - Multiple Network Types
  - Diverse Mix of Operating Systems
- Testing the Various Technologies
  - Anonymization
  - Encryption
  - Analytics
  - Performance

Results:

- Documentation and Guidelines
- Visualization of Test Results
- Develop Best Practices for Technology Providers

Impact and Benefits:

- Testing with multiple virtual machines without endangering live devices or exhausting resources.
- Help bring cutting-edge solutions to the evolving security landscape.