SAND2017-4142C

Dynamic Cybersecurity Training Environments for an Evolving Cyber Workforce

William M.S. Stout

Vincent E. Urias, Brian Van Leeuwen, Han W. Lin

Sandia National Laboratories

Albuquerque, New Mexico

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Outline

- Introduction and Motivation
- Current Methods and the Status Quo
- The Benefits of Live Training
- Use-Case Study and Lessons Learned
- Conclusion

INTRODUCTION AND MOTIVATION

Introduction

- Global shortfall of 378K InfoSec staff, to increase to 1.5M by 2019
- Need: Real-world scenarios to include:
  - Defense techniques
  - Attack-based approaches
  - Adversary understanding/methodology
- Lack of standards exist to streamline training requirements

Introduction

- Secure computing environment training:
  - Testbeds → real hardware
  - Assess impact of breach
  - Eval strategies for new security capabilities
- However,
  - Expensive
  - Difficult to maintain
  - Time consuming to construct/deploy
  - Often single purpose

CURRENT METHODS AND THE STATUS QUO

Current Methods & the Status Quo

- First responders and cybersecurity pros
- Certs not enough, need for immersive training
  - Evaluation against objectives is key
- Comparable to pilots and solders; train like you fight (e.g., CDX)
  - High-pressure, combative situations
  - Need to tie back to the mission and goals
- LVC + CDX

THE BENEFITS OF LIVE TRAINING

Live Training

- Cyber Training Platform Requirements
  - Hosts
  - Network System Architecture
  - System Security Mechanisms/Applications
  - System Load/Traffic Generation
  - Malicious Intrusion/Cyber-attack

Live Training

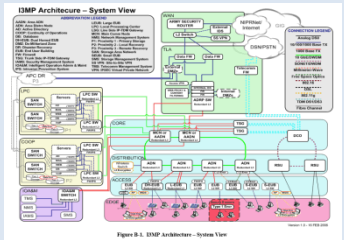
- Perceived Gaps, Limitations and Opportunities
  - Training environments do not adequately represent operations systems.
  - Training environments are often stuck in the contexts they were developed in and stale quickly.
  - System maintenance of a virtual training environment is too much work.

Live Training

- Modularity and modality
  - Appliance training
  - Specific task reinforcement
  - Targeted scenarios
  - Certification/technique training
  - Team studies

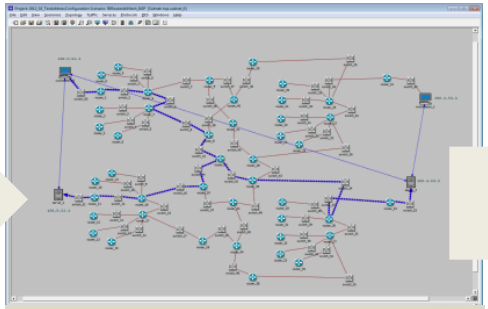
Live Training LVC

Specification information:
- Device configurations
- Network architecture
- Typical architecture

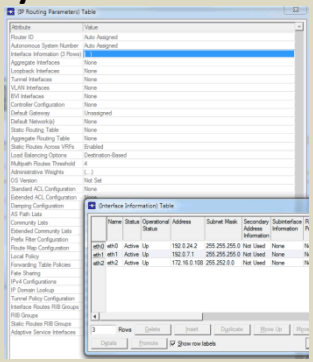


Discovery
- Traceroute
- Third-party tools
- Port mapping / scans
- SNMP
- L2/L3 Discovery
- Operational data (LLDP, CAM Table, ARP)

Design Estimation
- Design tools
- Best Practices
- Mission / Purpose
- Time



Produce model with full complexity of desired system



Identify OS Types

Test operation of specification in simulation
- Reachability
- Routing
- Firewalls

Modify as necessary to meet modeling purpose

Create outputs to compare to emulation model outputs for validation

USE-CASE EXAMPLE AND LESSONS LEARNED

Use-Case Study

- Sandia partnered with customer to create "fight through" training environment
  - Focused on network defense / hunt
  - Comprised of physical/virtual infrastructure; three network enclaves

Use-Case Study

- Three training zones:
  - α-Zone (SNL)
    - Emulated DMZ security stack (IDS, FW,)
    - Enterprise services (DNS, email, web)
  - β-Zone (SNL)
    - Bridged alpha and gamma zones
    - Emulated global internet, ICS, and Enterprise Network
  - γ-Zone (customer)
    - Landing/entry zone on-prem
    - L2TP to SNL zones

Use-Case Study

- High-fidelity & Interactivity
  - Physical/Virtual routers/switches
    - True switching/routing protocols
    - Engineered QoS (latency) on long-haul
  - VM Snapshot / Write-through
  - In-network services (IM, bulletins)
  - Vulnerable endpoints/services
  - VNC Replay / Artificial traffic generation
  - Dynamic “drop-in” VM/Users

Use-Case Study

- Data Collection
  - VM introspection from hypervisor
  - Mouse/keyboard from framebuffer (VNC)
  - Network flow and packet capture
- SNMP capture (e.g., CAM, performance, routes)
- VM agents (e.g., SplunkForwarder)

Lessons Learned

- Granular instrumentation provides “what” – extrapolation to answer other questions is more difficult
  - “Why” actions were done, and what were the residual effects?
    - Event correlation → causality analysis
    - Future effects? Motivations?

Lessons Learned

- Decision branches
  - Within the “cyber cockpit”
    - Student pass/fail at instances
    - State snapshot, scenario replay
    - Start/Stop/Resume
    - Choose-your-own adventure → realtime, automated scenario development
    - Behavioral input & analysis

Lessons Learned

- Measures of Effectiveness (MOE)
  - Training teams must understand their roles, tasks and how actions supported/impeded the overall mission
  - MOEs that determine ‘mission accomplishment’ and the tests/objectives in the scenarios
  - Individual MOEs vs Team MOEs
  - All detrimental to further implementing policy, developing TTPs, analyzing information and feedback to trainers.

CONCLUSIONS

Conclusions

- Need for foundational tools for CPTs to practice/hone/learn new skills is needed.
- “Train as you fight”
- Physical vs LVC
- Not enough to just craft the environment or know the what’s
  - Need for MOE and feedback loops

Dynamic Cybersecurity Training Environments for an Evolving Cyber Workforce

Questions/Comments

William M.S. Stout

wmstout@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP