Security Exercises for the Online Classroom with DETER

Peter A. H. Peterson and Dr. Peter L. Reiher
{pahp, reiher}@cs.ucla.edu

Laboratory for Advanced Systems Research (LASR)
University of California Los Angeles

The 3rd Workshop on Cyber Security Experimentation and Test (CSET’10)
1. DETER is an ideal choice for hands-on, online security education.
2. Realistic, hands-on, exercises are a powerful addition to our security curriculum.
Outline

- Project motivation
- DETER as an educational platform
- Our labs as a case study
- Lessons Learned
- Conclusion
Project Motivation

- Homework for the online classroom

- Requirements
  - Same value as traditional homework
  - Easy to use without much “face time”

- Possibilities
  - Research Projects
  - Pen and paper coursework
  - Hands-on labs
Why Hands-on?

- Theory alone does not provide security
  - Real security is theory and practice, together
- The real world is complicated
- “Give a person a fish...”
- Real-world scenarios and tools add relevancy
- Fundamental issues exemplified in real systems
Hands-on Approaches

- Applications
  - OWASP WebGoat, custom demonstrations, etc.
  - We wanted to use real software systems
  - Some topics hard to put in “application form”

- Virtualization
  - QEMU, VirtualBox, VMware

- Testbeds
  - In-house, Emulab, DETER
Why Not Virtualization?

- Remote software support
- Multi-gigabyte download
- Bugfixes
- Virtual networking
- Cheating
- Overhead of multiple hosts

MITM Topology
- Dynamic physical networks
- Based on Emulab
- ~300 machines
- Internet-accessible
- Public
- Grouped resources
- Security focused
- Network Topology
- Machines
- Software
DETER Customization

- Boot-time customization
- Packages install from course archive on DETER
- Single repository
- Stable platform and interface

DETER customization scripts
DETER for Students

- Individual, private logins
- Simple web control panel
- Requires only a web browser and SSH
- Built-in redundancy
- Backups
- Testbed support
Any DETERrents?

- Shared testbed with finite resources
  - Only a minor inconvenience in practice
- Not local hardware
- Overkill for some uses
- “Installation media” not 100% secure
Case Study

- Hands-on, practical online exercises
- Courseware components
  - DETER
  - Lab Manual
  - Lab software
- Five labs
- Supporting a class on DETER
Lab Manual

- Wiki for CMS
- Remote Access
- Easy to update
  - Read-only for students
- Internal/External links

Lab manual homepage
Lab Template

- Self-contained unit:
  - Overview
  - Technical discussion
  - External reading
  - “The Story So Far…”
  - Assignment

Permissions Lab Table of Contents
Lab Descriptions

- Topics
  - Permissions and Firewalls
  - Exploits
  - Computer Forensics
  - Man-in-the-middle
  - Network intrusion detection systems
- All freely available open-source software
- Most are standard security/networking tools
Permissions & Firewalls

- POSIX file system permissions
  - Including special permissions and sudo
- Stateful firewalls with iptables
- Principle of Least Privilege
- Deny by Default Design
- Emphasis on unexpected interactions
Exploits

- Buffer overflows
- Pathname attacks
- SQL Injection
- Find, Exploit, Patch, Debrief
- No Security in Obscurity
- Failure or Works As Designed?

/`etc/shadow` is not a memo!
Computer Forensics

- Security involves detective work
- Three scenarios and disk images
- Data recovery
- Log analysis
- Analysis and written report
- Talk about exploratory learning!
- Two sides to every story
Man-in-the-middle

- ARP poisoning
- Eavesdropping
- Replay
- Injection
- Canonical MITM
- Nonce design
- The liability of abstraction

The scene of the crime
NIDS

- Intrusion Detection
- Craft signatures
- Real data
- Security tuning
- Highly context sensitive task
- TCP trace analysis

BASE interface
(http://base.secureideas.net/)
Supporting DETER Classes

- Email is the #1 support tool, by far
- Live office hours with
  - Instant messaging
  - SSH tunneling
  - GNU screen
- Low-tech and works like a charm!
We feel DETER superior to VMs for our needs

Especially:

- For online courses
- For multi-node scenarios
- When physical networks are important
- For security-oriented projects

Also great for “brick and mortar” classes
Hands-on Lessons

- Excellent interest and response
- Unexpected and creative answers
- Exploration reaps rewards
- Novices and experts both succeed
- Theory illuminated by practice
Future Work

- Flexibility and Repeatability issues
- Reducing development cost
  - Forensic Image Creator
- New labs
- DETER-specific issues
1. DETER is great for educational use

2. Hands-on, exploratory labs are a powerful (and fun!) way to reinforce theory
Labs available at:
http://lasr.cs.ucla.edu/classes/seclabs/
{pahp, reiher}@cs.ucla.edu

Contact us for more information.