

Security Exercises for the Online Classroom with DETER



Peter A. H. Peterson and Dr. Peter L. Reiher
{pahp, [reiher](mailto:reiher@cs.ucla.edu)}@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)

Key Points

1. DETER is an ideal choice for hands-on, online security education.

Key Points

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?

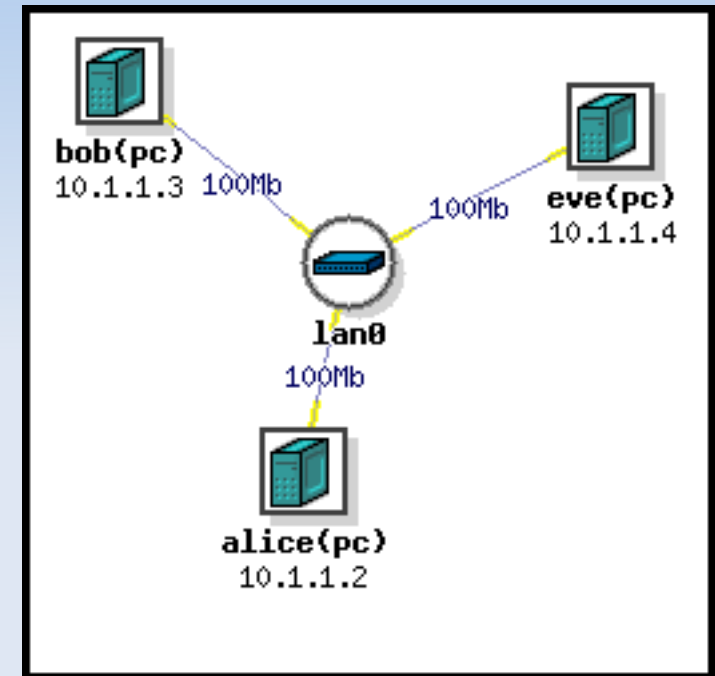
- Theory alone does not provide security
 - Real security is theory **and** practice, together
- The real world is complicated
- “Give a person a fish...”
- Real-world scenarios and tools add relevancy
- Fundamental issues exemplified in real systems

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?

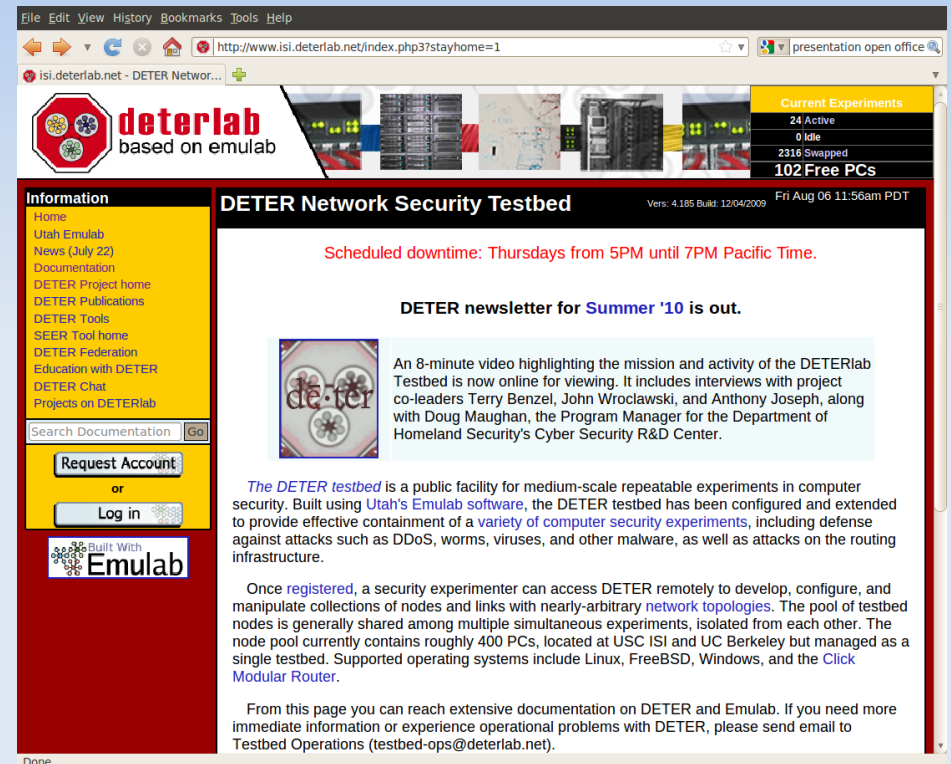
- Remote software support
- Multi-gigabyte download
- Bugfixes
- Virtual networking
- Cheating
- Overhead of multiple hosts



MITM Topology

DETER

- Dynamic physical networks
- Based on Emulab
- ~300 machines
- Internet-accessible
- Public
- Grouped resources
- Security focused



The screenshot shows the DETER Network Security Testbed homepage. The browser address bar displays <http://www.isi.deterlab.net/index.php3?stayhome=1>. The page features a navigation menu on the left with links to Home, Utah Emulab, News (July 22), Documentation, DETER Project home, DETER Publications, DETER Tools, SEER Tool home, DETER Federation, Education with DETER, DETER Chat, and Projects on DETERlab. Below the menu is a search box for documentation and buttons for 'Request Account' and 'Log in'. The main content area is titled 'DETER Network Security Testbed' and includes a 'Scheduled downtime: Thursdays from 5PM until 7PM Pacific Time.' notice. A section titled 'DETER newsletter for Summer '10 is out.' features an 8-minute video highlighting the mission and activity of the DETERlab Testbed. The page also contains detailed text about the testbed's capabilities, supported operating systems, and contact information for Testbed Operations.

DETER Homepage

DETER Experiments

- Network Topology
- Machines
- Software

The screenshot displays the DETERlab web interface for an experiment titled "Experiment (UCLAClass/alpha-mitm)". The interface includes a navigation menu with "My DETERlab", "Logout", "News", and "Contact Us". A search bar for "Search Documentation" is also present. The main content area shows the experiment's network topology, which consists of four nodes: "bob(pc)" (10.1.1.3), "eve(pc)" (10.1.1.4), "aLice(pc)" (10.1.1.2), and a central "lan0" node. All connections are labeled "100mb". The interface also features a "Settings" tab, a "Visualization" tab, and a "Details" tab. A table below the topology shows the status of 102 free PCs, with 7 currently reloading. The table lists PC IDs and their status:

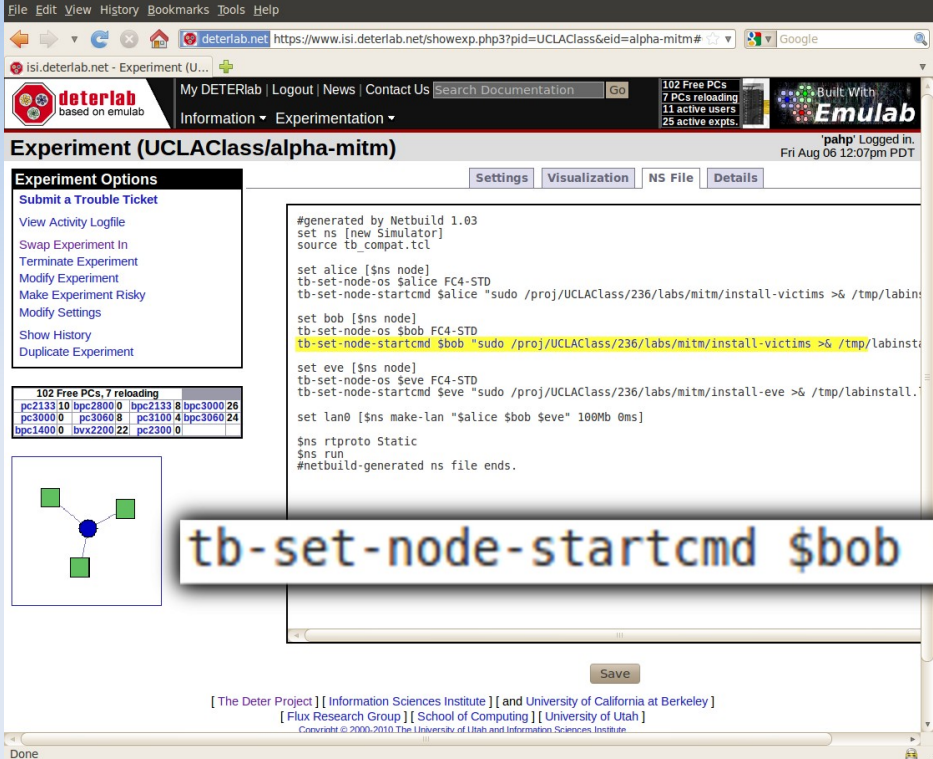
102 Free PCs, 7 reloading			
pc2133	bpc2800	bpc2133	bpc3000
pc3000	pc3060	pc3100	bpc3060
bpc1400	bvx2200	pc2300	

At the bottom of the interface, there is a footer with the following text: "[The Deter Project] [Information Sciences Institute] [and University of California at Berkeley] [Flux Research Group] [School of Computing] [University of Utah] Copyright © 2000-2010 The University of Utah and Information Sciences Institute".

DETER Topology designer

DETER Customization

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



The screenshot shows the DETERlab web interface for an experiment titled "Experiment (UCLClass/alpha-mitm)". The interface includes a navigation menu, a status bar showing "102 Free PCs, 7 reloading", and a main content area with a "tb-set-node-startcmd" script. A callout box highlights the command "tb-set-node-startcmd \$bob".

```
#generated by Netbuild 1.03
set ns [new Simulator]
source tb_compat.tcl

set alice [$ns node]
tb-set-node-os $alice FC4-STD
tb-set-node-startcmd $alice "sudo /proj/UCLClass/236/labs/mitm/install-victims >& /tmp/labinst

set bob [$ns node]
tb-set-node-os $bob FC4-STD
tb-set-node-startcmd $bob "sudo /proj/UCLClass/236/labs/mitm/install-victims >& /tmp/labinst

set eve [$ns node]
tb-set-node-os $eve FC4-STD
tb-set-node-startcmd $eve "sudo /proj/UCLClass/236/labs/mitm/install-eve >& /tmp/labinstall.

set lan0 [$ns make-lan "$alice $bob $eve" 100Mb 0ms]

$ns rtproto Static
$ns run
#netbuild-generated ns file ends.
```

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?

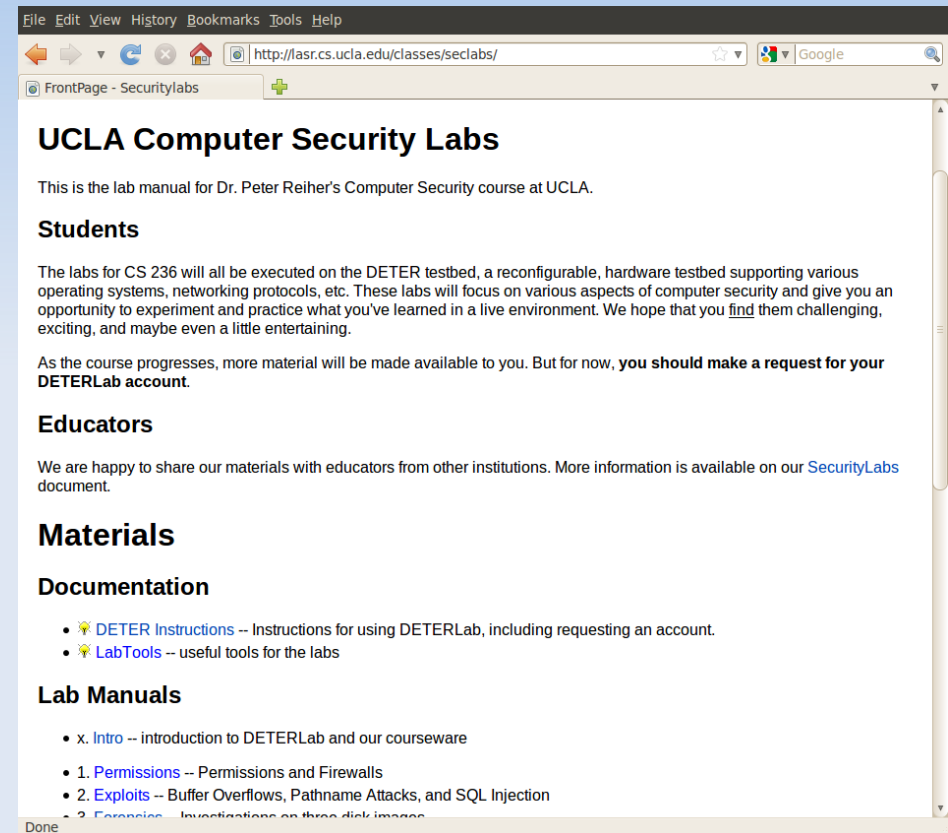
- Shared testbed with finite resources
 - Only a minor inconvenience in practice
- Not local hardware
- Overkill for some uses
- “Installation media” not 100% secure

Case Study

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

Lab Manual

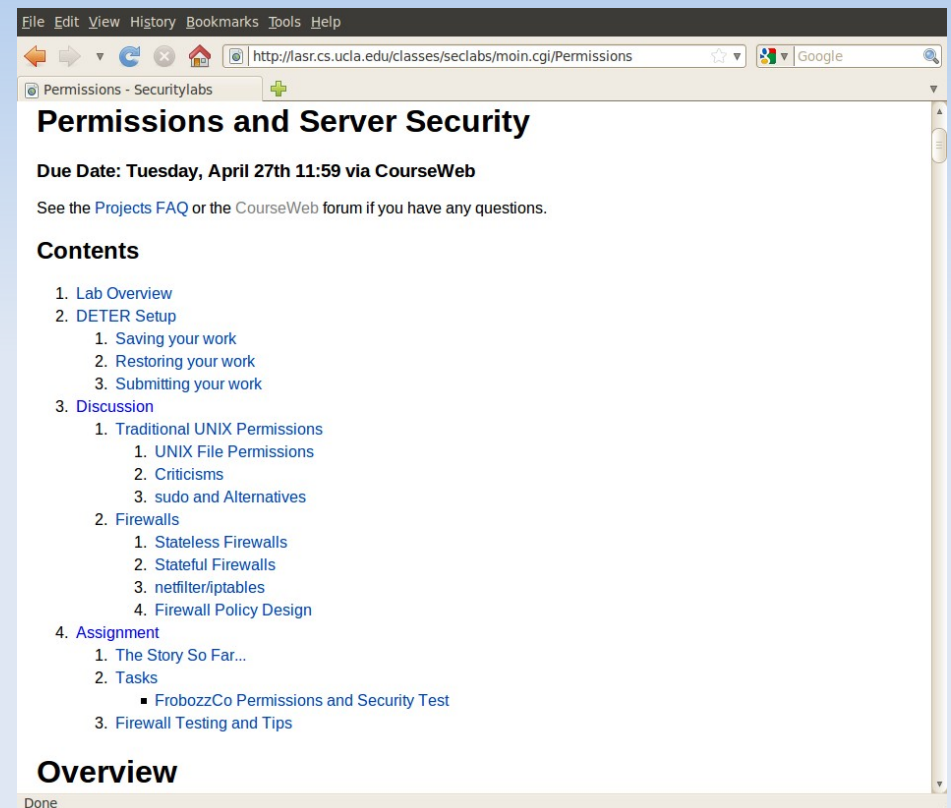
- Wiki for CMS
- Remote Access
- Easy to update
 - Read-only for students
- Internal/External links



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

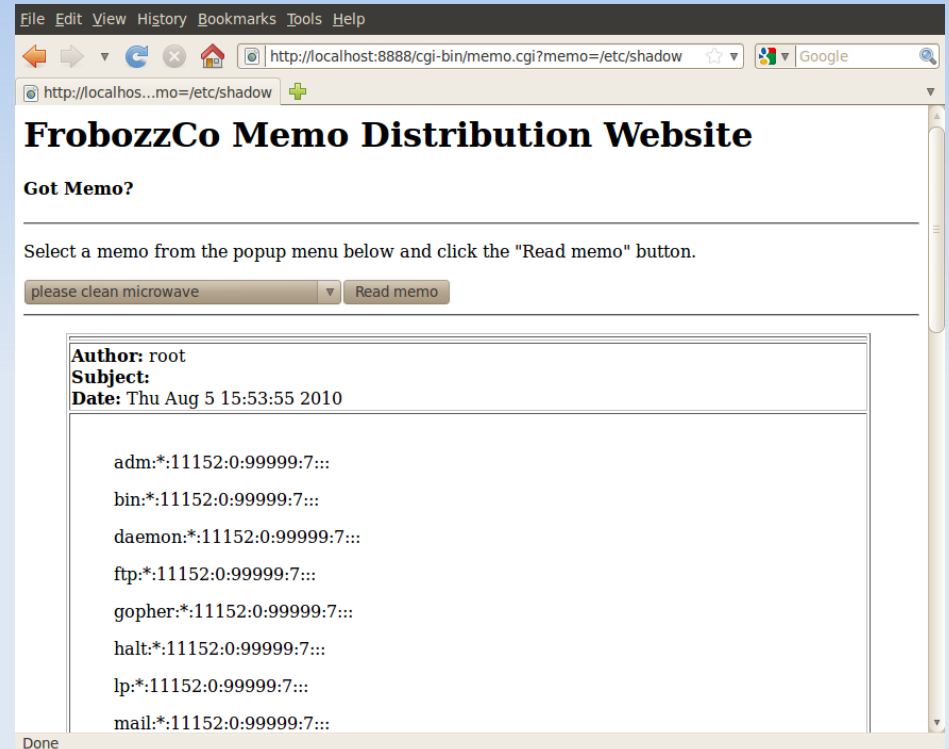
- Topics
 - Permissions and Firewalls
 - Exploits
 - Computer Forensics
 - Man-in-the-middle
 - Network intrusion detection systems
- All freely available open-source software
- Most are standard security/networking tools

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?



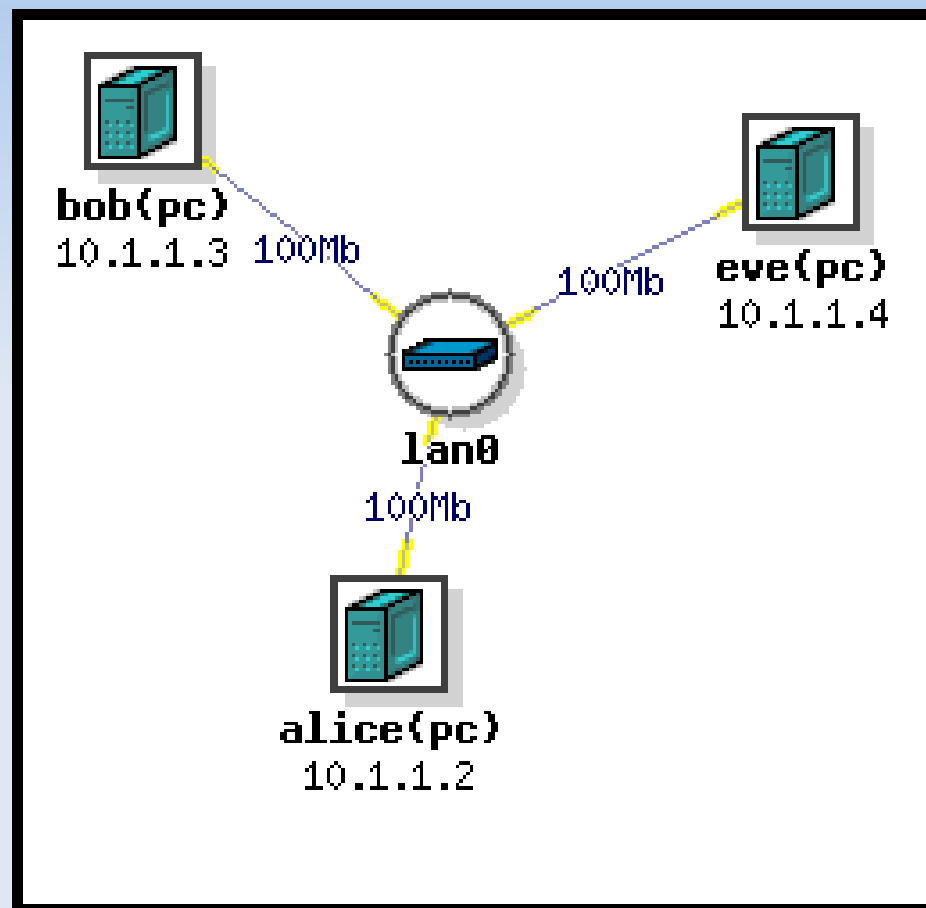
`/etc/shadow` is not a memo!

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

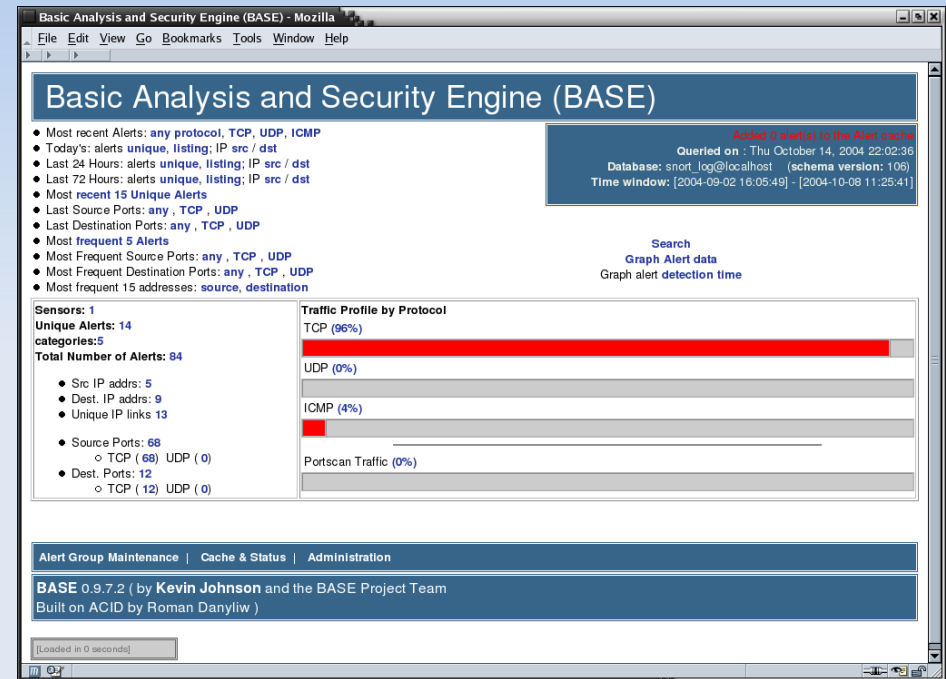
- ARP poisoning
- Eavesdropping
- Replay
- Injection
- Canonical MITM
- Nonce design
- The liability of abstraction



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!

DETER Lessons

- 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

Conclusion

1. DETER is great for educational use
2. Hands-on, exploratory labs are a powerful (and fun!) way to reinforce theory

Q&A

Labs available at:

<http://lasr.cs.ucla.edu/classes/seclabs/>
{pahp, reihher}@cs.ucla.edu

Contact us for more information.