Experiences In Cyber Security Education:
The MIT Lincoln Laboratory Capture-the-Flag Exercise*

Joseph Werther, Michael Zhivich, Timothy Leek, Nickolai Zeldovich

Cyber Security Experimentation And Test 2011

8 August 2011

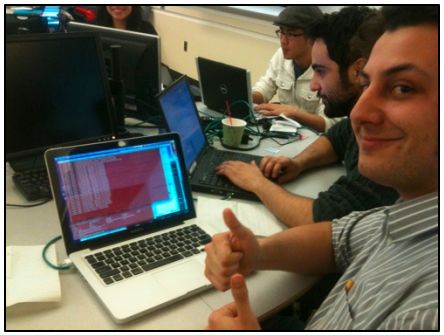
∗This work is sponsored by DARPA CRASH under Air Force contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

Outline

- Introduction to the MIT/LL CTF
- Pedagogic Principles
- Similar Exercises & Related Work
- MIT/LL CTF Exercise Design
- Survey Results
- Lessons Learned and Future work

MIT/LL CTF by Numbers

- 10 boxes of Joe
- 20 boxes of donuts
- 15 Ethernet switches
- 180’ of CAT6 cable
- 1 ESX server
- 5,193 lines of Python,
- 2,415 lines of PHP
- 1,432 lines of JavaScript
- 347 lines of HTML
- Too many late nights to count
- 1 custom flag
- $1,500 + 4 iPods
- 5 lectures + 1 lab
- 45 excellent contenders
- 1 unforgettable weekend



Introduction to the MIT/LL CTF

- A Capture the Flag Exercise for Boston Area Universities
  - 53 Participants from 6 Universities
  - A two day exercise preceded by a week of lectures & labs
- Focused on web application security
  - Covered security at multiple levels
  - Application, server, and client exploitation
- Built around the Wordpress Content Management System
  - Pervasive blogging tool
  - Easily extensible for CTF purposes
- Designed with education in mind
  - Make computer security accessible to a large community
  - Make traditional CS students passionate about security

Pedagogic Principles

- 3 main ways to learn computer security
  - Reading, Building, and Experiencing
  - Tried to include all 3 elements into the MIT/LL CTF

- We consider offensive education to be very important
  - Required to fully understand defense
  - Motivated by previous work (Fanelli, Bratus, Locasto)

- Distributed the CTF Team VM a month before the event
  - Did not include challenge (exploitable) plug-ins
  - Emulated a more realistic IT/Security environment
  - Encouraged students to research and practice systems security ahead of time

Educational Components

- Held 5 Lectures in the month before the CTF
  - Lectures were held in the evening
  - Slides and pointers to Internet resources provided
- Class 1 - Introduction to MITLL/CTF
  - What is a CTF, how is it played?
  - Rules and mechanics of the MIT/LL CTF
- Class 2 – Web Applications & Wordpress
  - Teach the Wordpress API
  - Give the basics of plug-in design
- Class 3 – Web Server Security
  - Security principles and tools for locking down LAMP servers
  - Case study by MIT's SIPB
- Classes 4 & 5 – Web Application Security
  - Explored multiple types of vulnerabilities
  - Covered bug identification, exploitation and mitigation
  - Held lab session using Google's Gruyere

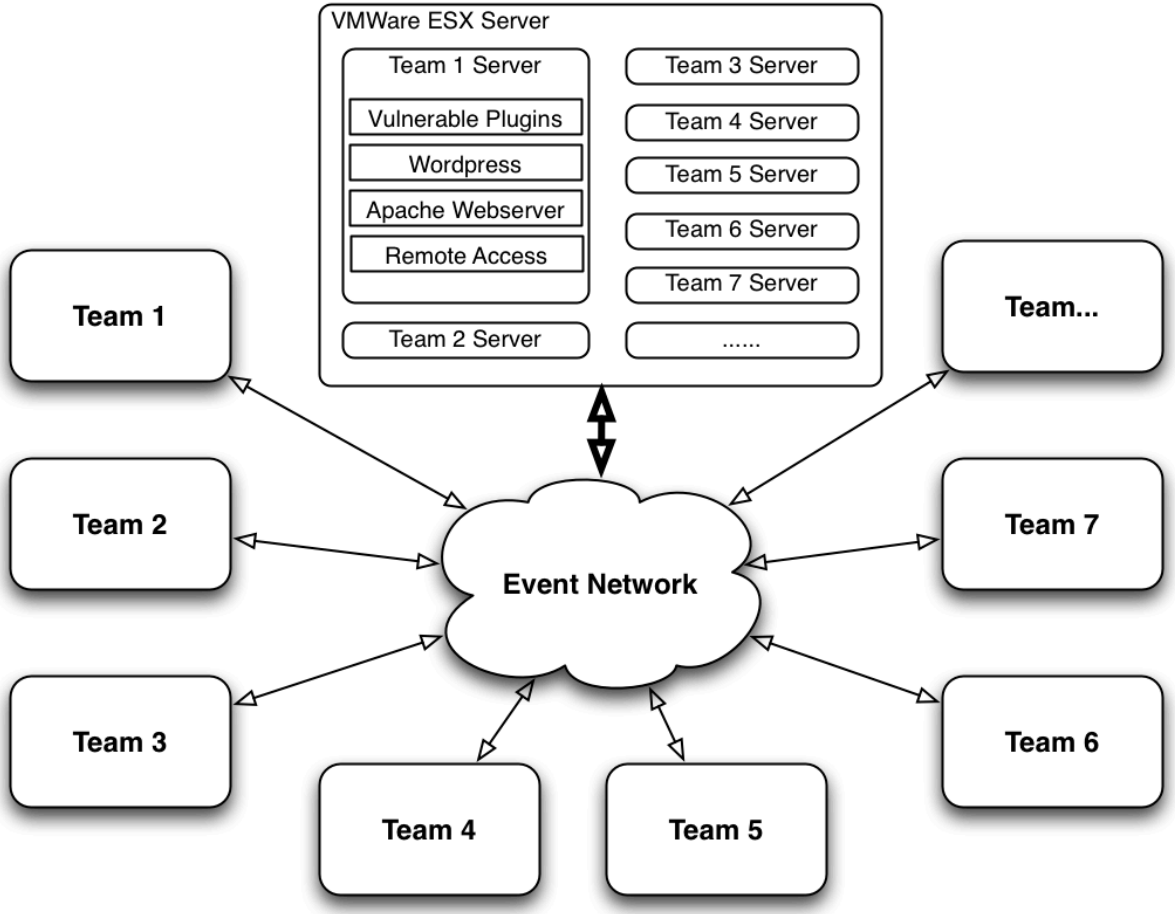
Similar Exercises & Related Work

- DefCon CTF (Team vs. Team)
  - Requires qualification round (very high barrier to entry)
  - Qualification are open to all who wish to participate
- iCTF (previously Team vs. Team, now different)
  - Large intra-university CTF
  - No lecture/lab component
- CCDC (Team Vs. Red Team)
  - Concentrated on Computer Network & System Defense
  - Aimed at giving practical experience in defending commercial networks
- NSA's CDX (Team Vs. Red Team)
  - Restricted to military educational institutions
- Other University CTFs
  - Many based around semester-long courses
  - Majority are limited to only one university

MIT/LL CTF Exercise Landscape

- Each team was provisioned a "Team VM" on ESX server
  - Connected to the VM from laptops for defensive configuration
  - Could conduct offense from laptops or VM
- VM ran a standard LAMP stack
  - Came pre-configured with a set of custom Wordpress plug-ins
- The first 30 minutes were not scored
  - Apply patches, secure server VMs
  - Attacks permitted during this period
- Valuable/sensitive information was represented by flags
  - Flags consisted on long alpha-numeric strings
  - Resided on file system and in database
- Grading bots evaluated each teams VM for functionality
  - Evaluation and flag rotation took place at random points in a 15 minute interval

The Network


VMWare ESX Server
Team 1 Server
Vulnerable Plugins
Wordpress
Apache Webserver
Remote Access
Team 2 Server
Team 3 Server
Team 4 Server
Team 5 Server
Team 6 Server
Team 7 Server
.....
Team 1
Team 2
Team 3
Team 4
Team 5
Team 6
Team 7
Team...
Event Network

MIT/LL CTF Scoring

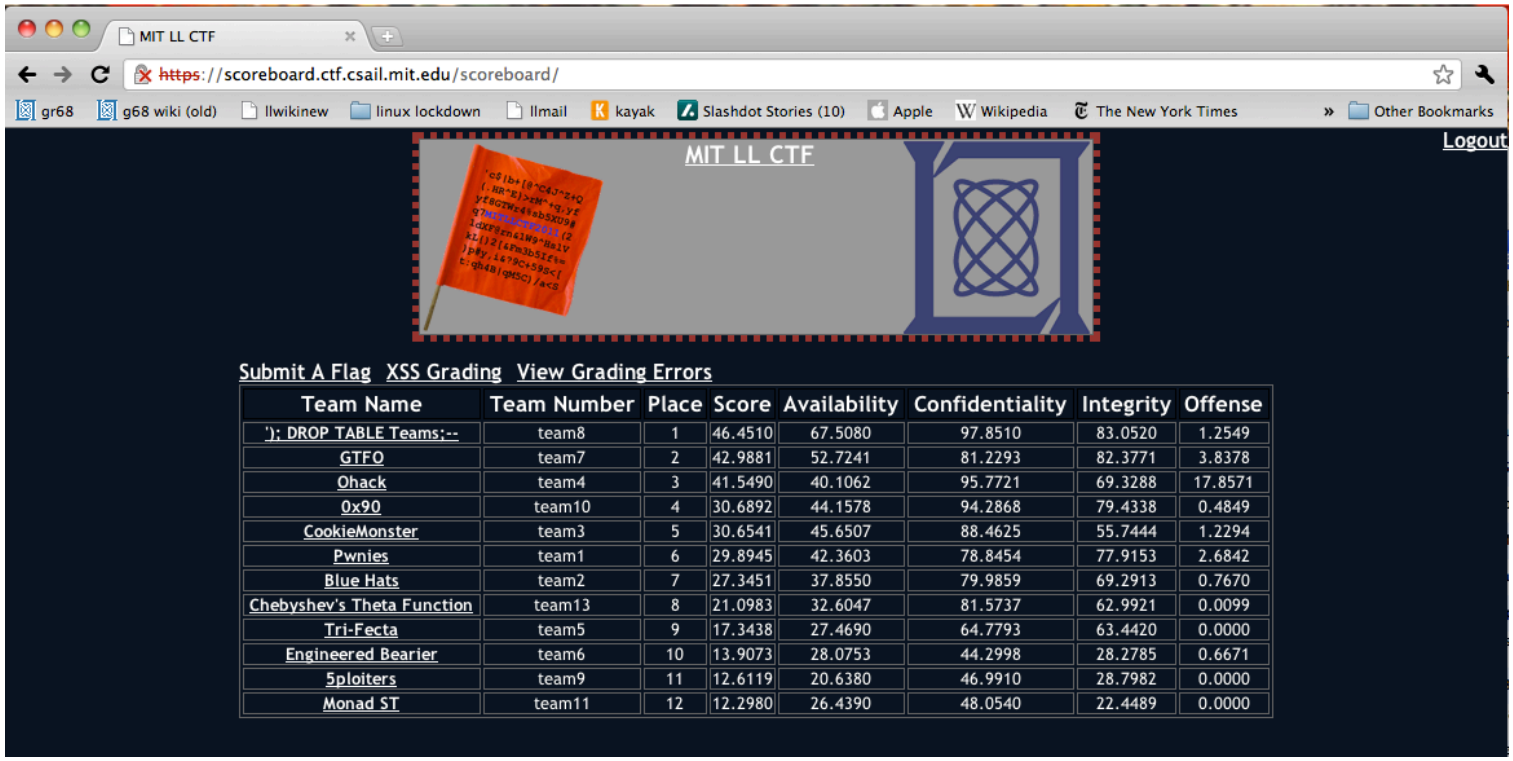
- **Scores calculated as a weighted average of four sub-scores**

$$Score = W_d * Defense + (1 - W_d) * Offense$$

$$Defense = \sum_{k \in \{C,I,A\}} W_k * K$$

- ***Availability***
  - **Fraction of functionality test cases passed by a team's website**
- ***Confidentiality***
  - **Fraction of a team's flags not submitted by another team**
- ***Integrity***
  - **Fraction of flags remaining unmodified on a team's VM**
- ***Offense***
  - **Fraction of all available flags (belonging to other teams) submitted by a team**

The Scoreboard



Team Name	Team Number	Place	Score	Availability	Confidentiality	Integrity	Offense
'); DROP TABLE Teams;--	team8	1	46.4510	67.5080	97.8510	83.0520	1.2549
GTFO	team7	2	42.9881	52.7241	81.2293	82.3771	3.8378
Ohack	team4	3	41.5490	40.1062	95.7721	69.3288	17.8571
0x90	team10	4	30.6892	44.1578	94.2868	79.4338	0.4849
CookieMonster	team3	5	30.6541	45.6507	88.4625	55.7444	1.2294
Pwnies	team1	6	29.8945	42.3603	78.8454	77.9153	2.6842
Blue Hats	team2	7	27.3451	37.8550	79.9859	69.2913	0.7670
Chebyshev's Theta Function	team13	8	21.0983	32.6047	81.5737	62.9921	0.0099
Tri-Fecta	team5	9	17.3438	27.4690	64.7793	63.4420	0.0000
Engineered Bearier	team6	10	13.9073	28.0753	44.2998	28.2785	0.6671
5ploiters	team9	11	12.6119	20.6380	46.9910	28.7982	0.0000
Monad ST	team11	12	12.2980	26.4390	48.0540	22.4489	0.0000

Survey Results

- Received survey responses from 22 of the participants
  - Overall response very positive (91% said they would like to participate in another CTF)
- Reported skill self-assessment
  - Improved practical computer security skills
  - Increased interest in computer security as a career
  - Some concluded they were overconfident before the CTF
- Preparation time (outside of lecture)
  - 1-2 hours (9 responders)
  - 4-8 hours (8 responders)
- Defense vs Offense
  - 50% spent more time on Defense
  - 36% spent more time on Offense
  - 86% of participants discovered and tried to patch at least 1 vulnerability
  - Those who worked on offense developed an average of 1.5 exploits

Lessons Learned and Future Work

- **Expand the CTF to more New England Colleges**
  - **Improve marketing and getting new students involved**
- **Improve data collection & environment instrumentation**
  - **Ensure the PCAP capture doesn't fail**
  - **Collect performance and traffic logs from VMs**
  - **Better visibility into offensive and defensive activities**
- **Provide teams with off-network console access to VMs**
  - **Offering snapshots and restores was useful, but automated exploitation made this difficult**
- **Devise better methods of measuring education**
  - **Incentivize survey participation**
  - **Survey/test both before and after the CTF & classes**

Discussion Topics

- What are the best ways to measure CTF's effect on participants' knowledge of practical computer security?
  - Quizzes seem unsatisfactory
  - Practical tests are difficult to arrange
- How can we better instrument the CTF without interfering with the game?
  - Would like to have better visibility into defensive posture and offensive activities
  - Compliance with CTF rules of the game
- What are the best ways to encourage learning about practical computer security after the CTF?
  - Reading groups?
  - Hack-a-thons?

Questions?