Innovative Pedagogical Approaches to a Capstone Laboratory Course in Cyber Operations

Mike O’Leary
Towson University

SIGCSE 2017
• Introduction
• Course Content
• Flipping the Classroom
• Live Exercises
• Balancing Offense and Defense
• Red Team
• Reports & Forensics
• Grading
• Student Expectations
• Conclusions
• Capstone Course

• Students
  • Seniors, Spring semester
  • Cyber-security track
    • Operating systems, operating systems security, networking, and network security
  • End up working for
    • NSA, Veris Group, MITRE, Cisco, and the FBI

• Setting
  • Isolated classroom laboratory
  • Extensive use of virtual machines
Course Content

- Kali; Metasploit
- Operational Awareness
- BIND
- Active Directory, Group Policy
- Logging; Network services
- Apache; ModSecurity
- IIS; ModSecurity
- Firewalls
- MySQL/MariaDB
- Intrusion Detection; Snort
- Web Applications
  - WordPress, Joomla, Zen Cart
• Source material
• Motivation for the flip
  • Pacing
• Student reaction
  • Specialization
• Benefits to students
  • Responsibility
Live Exercises

**Team 1**
**Kali Net**
10.1.57.0/24

**.production.team1.tu**
- Houston
  - DC
  - 10.1.199.99
- TampaBay
  - DC
  - 10.1.199.191
- LittleRock
  - Win. File Server
  - 10.1.199.89
- Albuquerque
  - IIS
  - 10.1.199.190
- SantaCruz
  - Apache
  - 10.1.199.135
- Minneapolis
  - Public Linux
  - 10.1.199.76
- Reno
  - SSH, FTP
  - 10.1.199.237
- Phoenix
  - Win. Destkop
  - 10.1.199.73

**.corp.team1.tu**
- SantaFe
  - Samba
  - 10.1.33.133
- Columbus
  - BIND
  - 10.1.33.101
- PaloAlto
  - BIND
  - 10.1.33.249
- Baltimore
  - Linux Desktop
  - 10.1.33.19
- LasVegas
  - Apache
  - 10.1.33.70
- Honolulu
  - Win. Desktop
  - 10.1.33.214
- Cincinnati
  - Log Server
  - 10.1.33.14

**.sales.team1.tu**
- Seattle
  - SSH, FTP
  - 10.1.214.149
- Milwaukee
  - Win. Destkop
  - 10.1.214.245
- Miami
  - IIS
  - 10.1.214.242
- Orlando
  - Apache
  - 10.1.214.45
- StLouis
  - Cash Register
  - 10.1.214.30
- Monterey
  - DC
  - 10.1.214.212
- Jacksonville
  - DC
  - 10.1.214.215
- Philadelphia
  - Win. File Server
  - 10.1.214.52

**Exercise Network**
- Exercise Control
  - 10.0.6.250, 251
- Red Team
  - Varies

**Team 2**
- 10.2.x.0/24
- x ∈ {76,87,93,232}

**Team 3**
- 10.3.x.0/24
- x ∈ {106,119,202,246}

**Team 4**
- 10.4.x.0/24
- x ∈ {12,58,125,142}
# Live Exercises

## Nagios Core

**Current Network Status**
- Last Updated: Tue Apr 5 17:26:05 EDT 2016
- Updated every 20 seconds
- Nagios® Core 3.6.1

**Host Status Totals**
- All Problems: 8
- All Types: 2

**Service Status Totals**
- All Problems: 62
- All Types: 623

### Service Overview For All Host Groups

<table>
<thead>
<tr>
<th>Team 1 (Team 1)</th>
<th>Team 2 (Team 2)</th>
<th>Team 3 (Team 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td><strong>Status</strong></td>
<td><strong>Services</strong></td>
</tr>
<tr>
<td>abour.sales.team1.tu</td>
<td>UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>ashkelton.production.team1.tu</td>
<td>UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>airots.sales.team1.tu</td>
<td>UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>amoral.production.team1.tu</td>
<td>UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>arista.sales.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>b Stall.sales.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>bethlehem.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>biozept.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>bubs.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>bydco.sales.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>elevente_production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>elk4k.sales.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>hawara.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>heliopols.corp.team1.tu</td>
<td>UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>himan positives.corp.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>kompas.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>ksenimony.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>laporte.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>lpcorps.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>mizrim.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>naxs.corp.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>nadin.sales.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>pear.res.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>rogue.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>tovia.corp.production.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>utexas.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>wlv.corp.team1.tu</td>
<td>UP</td>
<td>1 OK</td>
</tr>
</tbody>
</table>

**Actions**
- OK: Normal
- CRITICAL: Critical
- WARNING: Warning
- UNKNOWN: Unknown
Case Studies Exercise Control
2017 (With new Awesome Sauce)

RULES:

This system is Exercise Control; it is out-of-bounds for the exercise.

Exercise control is not to be used to attack other systems. This means no nmap scans, shell pivoting, or other pieces of cleverness. This goes for student teams as well as for the red team. If it comes from Exercise Control, you can assume it is to be trusted.

To a point. This is Case Studies, after all.

Using Exercise Control

Exercise Control lives at:

- IP: 10.0.6.250
- Hostname: winterfell.classex.tu

Although, since you are visiting this page, I guess you figured that part out.
Balancing Offense and Defense

• How to balance offense & defense?
  • Class focus is on defense, not offense

• Older software (2008-2014)
  • Multiple known exploits

• 9,396 allowable passwords
  • P1# + common 8 letter word

• Simon Says
  • Class email server
  • Class Stikked server

• Blocking by IP
Balancing Offense and Defense
Red Team

• Recruiting
  • 4-8 per exercise
  • Volunteers, primarily recent graduates

• Benefits
  • Student benefits are pedagogical
  • Red team benefits in corporate / government recruiting

• Management
  • Emphasize pedagogical nature of the experience
• Student reports (40-80 pages)
  • How was the network set up?
  • How well did it function?
  • What offensive activity was performed?
  • How were their networks compromised?
    • Attack recovery!
      • Account lock-outs
      • Cryptolocker
      • MBR overwrite (Nyan Cat)
      • Custom malware
Grading

• The full state of the network is not known to the instructor, before or after.
  • Service states (Graded with Nagios)
  • Reconnaissance / Attacks
  • Defense
  • Analysis
  • Report Quality
• Each team starts with 20 points, and can lose points due to successful attacks:
  • (2 points/system up to 10 points) Opponent gains a shell on a system.
  • (4 points/system up to 20 points) Opponent gains root/administrator access.
  • (15 points) Opponent gains domain administrator access.
  • (1 points/file) Opponent gains access to confidential file.
  • (1 points/file) Opponent dumps some or all of a confidential file in public.

• Points lost to a successful attack can be regained through analysis.
  • If the team correctly identifies an attack, one half of the lost points are recovered.
  • If the team is also able to identify the source of the attack, the remaining one half of the lost points are recovered.
Student Expectations

• Students that do not fully engage with the course
  • Checkpoints
  • Per-student grading of exercise services

• Ethics & Sportsmanship

• Mentoring
  • Red Team!
• “Curricula must prepare students for lifelong learning and must include professional practice (e.g., communication skills, team-work, ethics) as components of the undergraduate experience. Computer science students must learn to integrate theory and practice, to recognize the importance of abstraction, and to appreciate the value of good engineering design.”

- ACM curriculum guide
Questions?