

Innovative Pedagogical Approaches to a Capstone Laboratory Course in Cyber Operations

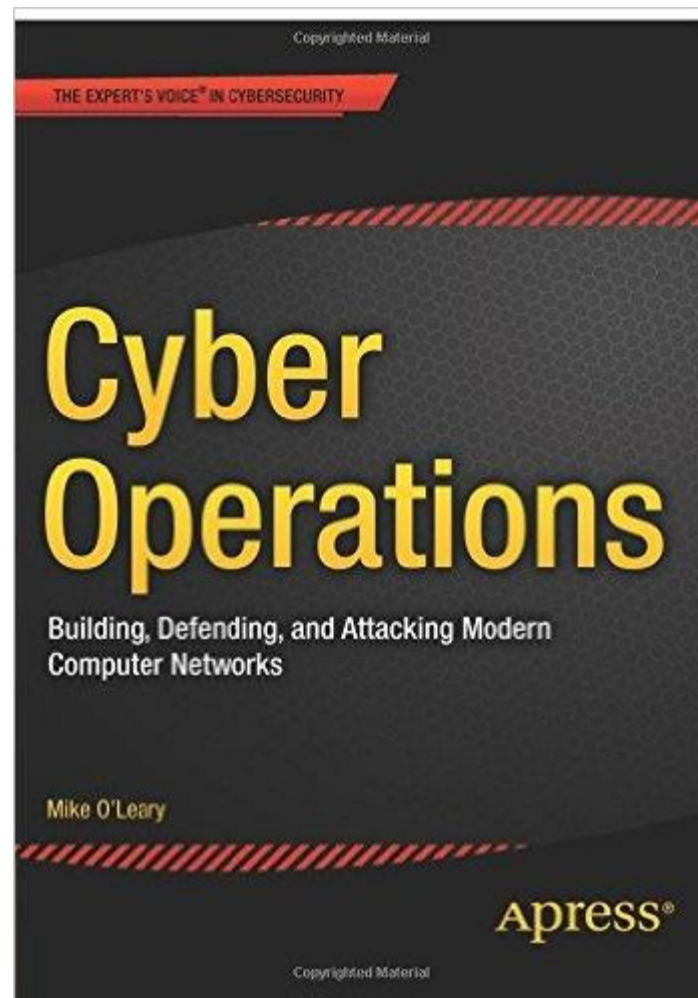
Mike O'Leary
Towson University

SIGCSE 2017

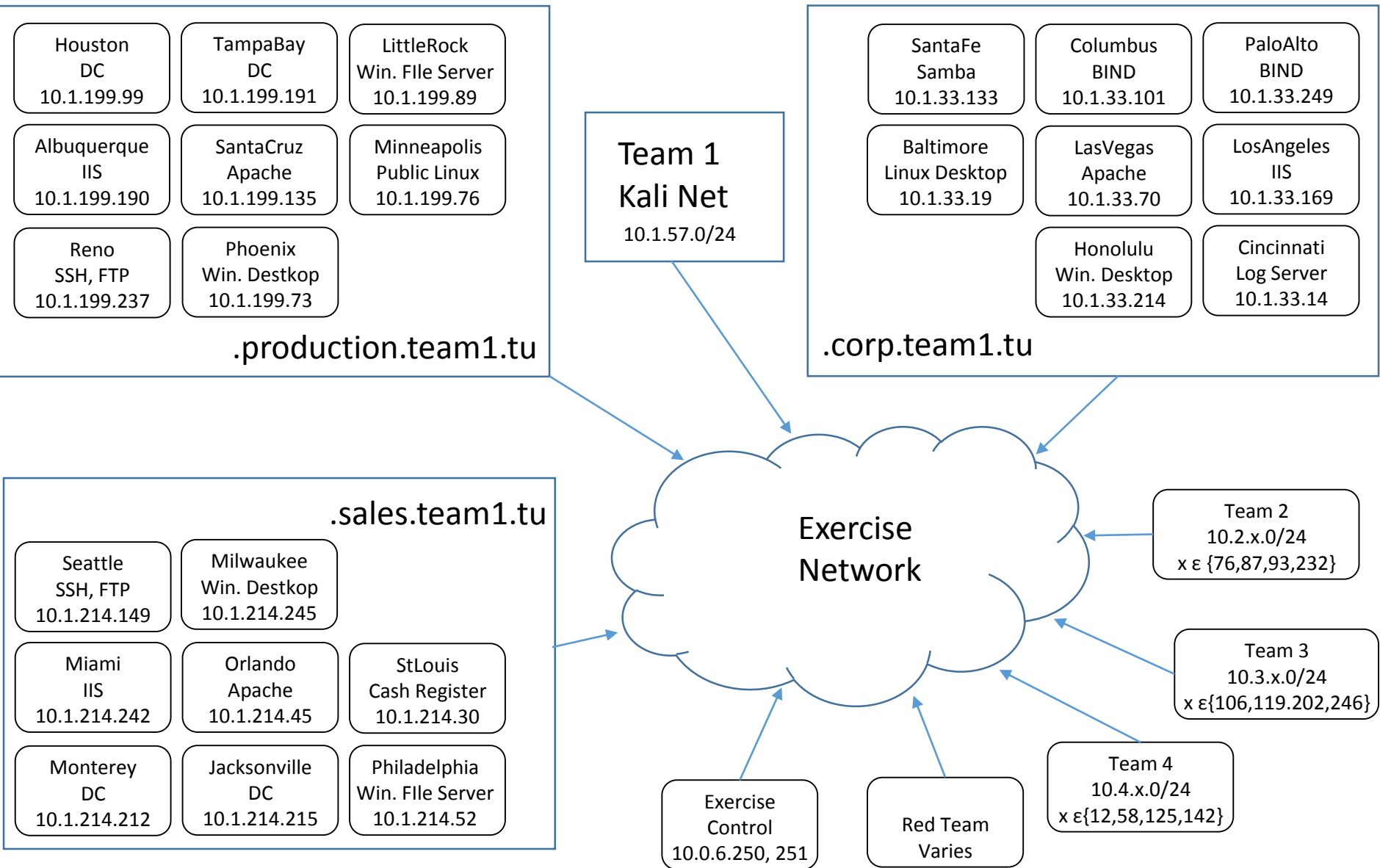
- Introduction
- Course Content
- Flipping the Classroom
- Live Exercises
- Balancing Offense and Defense
- Red Team
- Reports & Forensics
- Grading
- Student Expectations
- Conclusions

- 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

- 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



Nagios Core

file:///C:/Users/moleary/Google%20Drive/COSC%20481%20Spring%202016/Exercises/Exercise%202/Service%20Scoring/Day%201/530.htm

Nagios®

Current Network Status
 Last Updated: Tue Apr 5 17:29:08 EDT 2016
 Updated every 90 seconds
 Nagios® Core™ 3.5.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
90	2	0	0
All Problems All Types			
2	92		

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
570	7	2	53	0
All Problems All Types				
62	632			

General
 Home
 Documentation

Current Status
 Tactical Overview
 Map
 Hosts
 Services
 Host Groups
 Summary
 Grid
 Service Groups
 Summary
 Grid
 Problems
 Services
 (Unhandled)
 Hosts
 (Unhandled)
 Network Outages

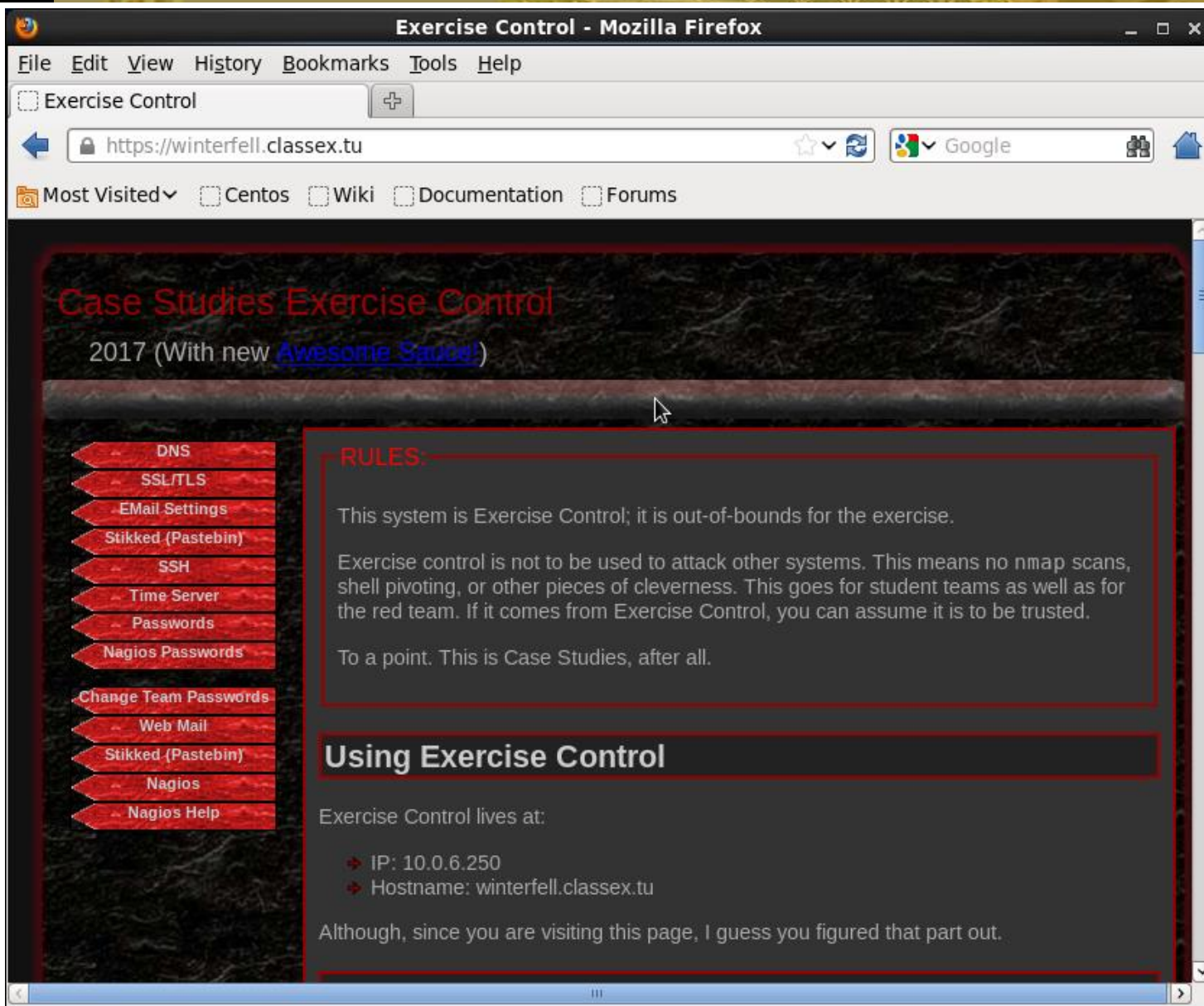
Quick Search:

Reports
 Availability
 Trends
 Alerts
 History
 Summary
 Histogram
 Notifications
 Event Log

System
 Comments
 Downtime
 Process Info
 Performance Info
 Scheduling Queue
 Configuration

Service Overview For All Host Groups

Team 1 (Team 1)				Team 2 (Team 2)				Team 3 (Team 3)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
abusir.sales.team1.tu	UP	7 OK		avignon.corp.team2.tu	UP	8 OK		anchorage.sales.team3.tu	UP	1 WARNING 8 CRITICAL	
akhetaten.production.team1.tu	UP	8 OK		bayonne.production.team2.tu	UP	8 OK		buffalo.corp.team3.tu	UP	13 OK	
akoris.sales.team1.tu	UP	8 OK		bourges.corp.team2.tu	UP	8 OK		charleston.sales.team3.tu	UP	2 OK	
amara.production.team1.tu	UP	2 OK		brest.sales.team2.tu	UP	8 OK		chicago.production.team3.tu	UP	1 OK	
aniba.sales.team1.tu	UP	1 OK		cannes.sales.team2.tu	UP	13 OK		cincinnati.production.team3.tu	UP	7 OK	
balat.sales.team1.tu	UP	13 OK		carcassonne.sales.team2.tu	UP	7 OK		cleveland.sales.team3.tu	UP	6 OK 1 WARNING 8 CRITICAL	
benihasan.corp.team1.tu	UP	8 OK		chartres.production.team2.tu	UP	6 OK 1 WARNING		columbus.corp.team3.tu	UP	6 OK	
busiris.production.team1.tu	UP	1 OK		dijon.sales.team2.tu	UP	7 OK		hawaii.corp.team3.tu	UP	1 OK	
buto.production.team1.tu	UP	7 OK		larochelle.production.team2.tu	UP	7 OK		houston.production.team3.tu	UP	8 OK	
byblos.sales.team1.tu	UP	7 OK		lemans.corp.team2.tu	UP	7 OK		lebam.sales.team3.tu	UP	7 OK	
elephantine.production.team1.tu	UP	7 OK		lille.corp.team2.tu	UP	12 OK		memphis.sales.team3.tu	UP	8 OK	
elkab.sales.team1.tu	UP	1 OK		limoges.corp.team2.tu	UP	8 OK		miami.corp.team3.tu	UP	12 OK	
hawara.corp.team1.tu	UP	6 OK 2 CRITICAL		lyons.production.team2.tu	UP	2 OK		neworleans.production.team3.tu	UP	1 OK 1 UNKNOWN	
heliopolis.corp.team1.tu	UP	6 OK 8 CRITICAL		marseilles.production.team2.tu	UP	1 OK		olympia.production.team3.tu	UP	7 OK	
hieraconpolis.production.team1.tu	UP	7 OK		nantes.corp.team2.tu	UP	12 OK		omaha.corp.team3.tu	UP	12 OK	
koptos.corp.team1.tu	UP	12 OK		nice.corp.team2.tu	UP	1 OK		philadelphia.sales.team3.tu	UP	7 OK	
merimde.corp.team1.tu	UP	10 OK 3 CRITICAL		nimes.production.team2.tu	UP	7 OK		pittsburgh.corp.team3.tu	UP	8 OK	
negade.production.team1.tu	UP	13 OK		orleans.sales.team2.tu	UP	2 OK		richmond.corp.team3.tu	UP	7 OK	
ombos.corp.team1.tu	DOWN	7 CRITICAL		poitiers.sales.team2.tu	UP	1 OK		saltlakecity.production.team3.tu	UP	1 WARNING 8 CRITICAL	
oryx.sales.team1.tu	UP	7 OK		rennes.sales.team2.tu	UP	1 OK		santamonica.sales.team3.tu	UP	1 OK	
sebennytus.sales.team1.tu	UP	2 OK		rouen.corp.team2.tu	UP	13 OK		spokane.corp.team3.tu	UP	8 OK	
semna.corp.team1.tu	UP	1 OK		strasbourg.sales.team2.tu	UP	7 OK		springfield.production.team3.tu	UP	6 OK 1 WARNING 8 CRITICAL	
thebes.corp.team1.tu	UP	6 OK		tours.production.team2.tu	UP	13 OK		washington.corp.team3.tu	UP	1 OK	



Exercise Control - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Exercise Control

https://winterfell.classex.tu

Most Visited Centos Wiki Documentation Forums

Case Studies Exercise Control

2017 (With new [Awesome Sauce!](#))

- DNS
- SSL/TLS
- EMail Settings
- Stikked (Pastebin)
- SSH
- Time Server
- Passwords
- Nagios Passwords
- Change Team Passwords
- Web Mail
- Stikked (Pastebin)
- Nagios
- Nagios Help

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.

- 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 Sticked server
- Blocking by IP

Team4 Passwords - Exercise Control - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Team4 Passwords - Exercise Co... +

https://winterfell.classex.tu/stikked/view/cc41e243

Most Visited Centos Wiki Documentation Forums

Exercise Control

Create Recent Trending API About


Team4 Passwords

From Mammoth Tern, 4 Days ago, written in Plain Text, viewed 15 times.

URL <https://winterfell.classex.tu/stikked/view/cc41e243>

Embed [Show code](#)

[Download Paste](#) or [View Raw](#) — [Expand Paste](#) to full width of browser



```

1. [445][smb] host: 10.4.233.78 login: nmedina password: P1#nutshell
2. [445][smb] host: 10.4.233.78 login: bnichols password: P1#boldness
3. [445][smb] host: 10.4.233.78 login: nward password: P1#numerals
4. [STATUS] 10396.67 tries/min, 31190 tries in 00:03h, 335293 to do in 00:33h, 1 active
5. [445][smb] host: 10.4.233.78 login: gcarter password: P1#gemstone
6. [445][smb] host: 10.4.233.78 login: bjohnson password: P1#bombings
7. [445][smb] host: 10.4.233.78 login: tmorgan password: P1#targeted
8. [STATUS] 9672.71 tries/min, 67709 tries in 00:07h, 298774 to do in 00:31h, 1 active
9. [445][smb] host: 10.4.233.78 login: dkelley password: P1#dutyfree
10. [445][smb] host: 10.4.233.78 login: gwood password: P1#gestures
11. [445][smb] host: 10.4.233.78 login: rwallace password: P1#reversal
12. [445][smb] host: 10.4.233.78 login: mholmes password: P1#molehill
13. [445][smb] host: 10.4.233.78 login: jarmstrong password: P1#jetplane
14. [445][smb] host: 10.4.233.78 login: chawkins password: P1#charring
15. [STATUS] 9508.60 tries/min, 142629 tries in 00:15h, 223854 to do in 00:24h, 1 active
16. [445][smb] host: 10.4.233.78 login: mharvey password: P1#mahogany
17. [445][smb] host: 10.4.233.78 login: tfuller password: P1#toenails
18. [445][smb] host: 10.4.233.78 login: dtorres password: P1#doctoral
19. [445][smb] host: 10.4.233.78 login: sduncan password: P1#surgical
20. [STATUS] 9185.30 tries/min, 183706 tries in 00:20h, 182777 to do in 00:20h, 1 active
21. [445][smb] host: 10.4.233.78 login: mbrown password: P1#mobsters
22. [445][smb] host: 10.4.233.78 login: cthompson password: P1#cottoned
23. [445][smb] host: 10.4.233.78 login: bjenkins password: P1#benjamin
24. [445][smb] host: 10.4.233.78 login: bjenkins password: P1#benjamin

```

- 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

- 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

- 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

WE FOLLOW INDUSTRY STANDARD PRACTICES	WE'VE ALWAYS DONE IT THIS WAY	WHAT DO YOU HAVE AGAINST US?	[COMPLETE SILENCE]	YOU MUST BE BEING PAID BY OUR COMPETITION
NOTHING IS 100% SECURE	NO ONE WOULD EVER THINK OF THAT	NOBODY'S PERFECT	WHY DO YOU HATE AMERICA?	WE HAVE THOROUGHLY INVESTIGATED AND ARE UNCONCERNED
IT WOULD BE TOO EXPENSIVE TO FIX THAT	THIS IS PROBABLY FIXED IN THE NEXT RELEASE	SECURITY PROBLEM EXCUSE BINGO	NO ONE HAS EVER FOUND ANY PROBLEMS	WE EMPLOY TOP SECURITY EXPERTS
OUR SUCCESS SPEAKS FOR ITSELF	YOU'RE ONLY HELPING THE BAD GUYS	YOU'RE PARANOID	YOU'RE JUST LOOKING FOR ATTENTION	WE MEET ALL INDUSTRY STANDARDS
WE HAVE CISSP CERTIFIED ENGINEERS	LA, LA, LA WE'RE NOT LISTENING	WHAT KIND OF A PERSON LOOKS FOR FLAWS?	YOU'RE PART OF A CONSPIRACY	YOU'RE JUST AN ACADEMIC