Small-Scale Cyber Security Competitions

Mike O'Leary

Towson University

16th Colloquium for Information Systems Security Education
Orlando, FL
June 11-13, 2012

Regional & National Competitions

- National Collegiate Cyber Defense Competition (NCCDC)
- Regional Collegiate Cyber Defense Competitions
- UCSB Capture the Flag Competition
- Military Academies CDX
- National Cyber League (NCL)
- DC3 Digital Forensic Challenge
- MITRE Cyber Challenge
- Maryland Cyber Challenge
- Utah Cyber Challenge
- CANVAS
- MIT Lincoln Laboratory / CSAIL Capture the Flag Competition

Introduction

Introduction

Source: `http://commons.wikimedia.org/wiki/File:Duke_UNC_Basketball_Game_at_Chapel_Hill.jpg`

Introduction

Introduction

Source: `http://www.arteyfotografia.com.ar/3544/fotos/180721/`

Introduction

Introduction

Introduction

Introduction

Our Experiences

- Long running hands-on capstone course in computer security
- Club level competitions
- Informal competitions with as many as five different schools
- Long time coach of the Towson Cyber Defense team
  - Mid-Atlantic Collegiate Cyber Defense Competition
  - National Collegiate Cyber Defense Competition
  - Maryland Cyber Challenge
  - CSC Cyb3r Battl3ground Competition

Our Environment

- Four tables with six computers per table.
  - Hosts run VMWare Workstation
  - Each computer has 16 GB of memory enabling us to run as many as eight virtual machines comfortably on a single host.
- The computers live on an isolated private network with only a file server containing software and installation discs.
- Students do not have privileged access to the host, and do not have access to the network infrastructure.
  - We can (and do) use the lab for a class at 3:00, run a short 75 minute competition at 5:00, and then use the lab for another class at 7:00.

Our Environment

- A competition can be run by simply developing the necessary virtual machines and deploying them through the classroom.
  - This is well within the capability of a single faculty member.
  - Restricting work solely to virtual machines reduces complexity means students do not experiment with hardware firewalls, routers, and switches.
- Student participants all have a solid background in networking, operating systems, and databases.
- Our competitions are aimed at students of comparable skill levels.

Competition Types

- We have run three types of competitions:
  - Class-based competitions
  - Competitions with pre-built systems
  - Competitions where student teams build their own systems.

Classroom Competitions: Setup

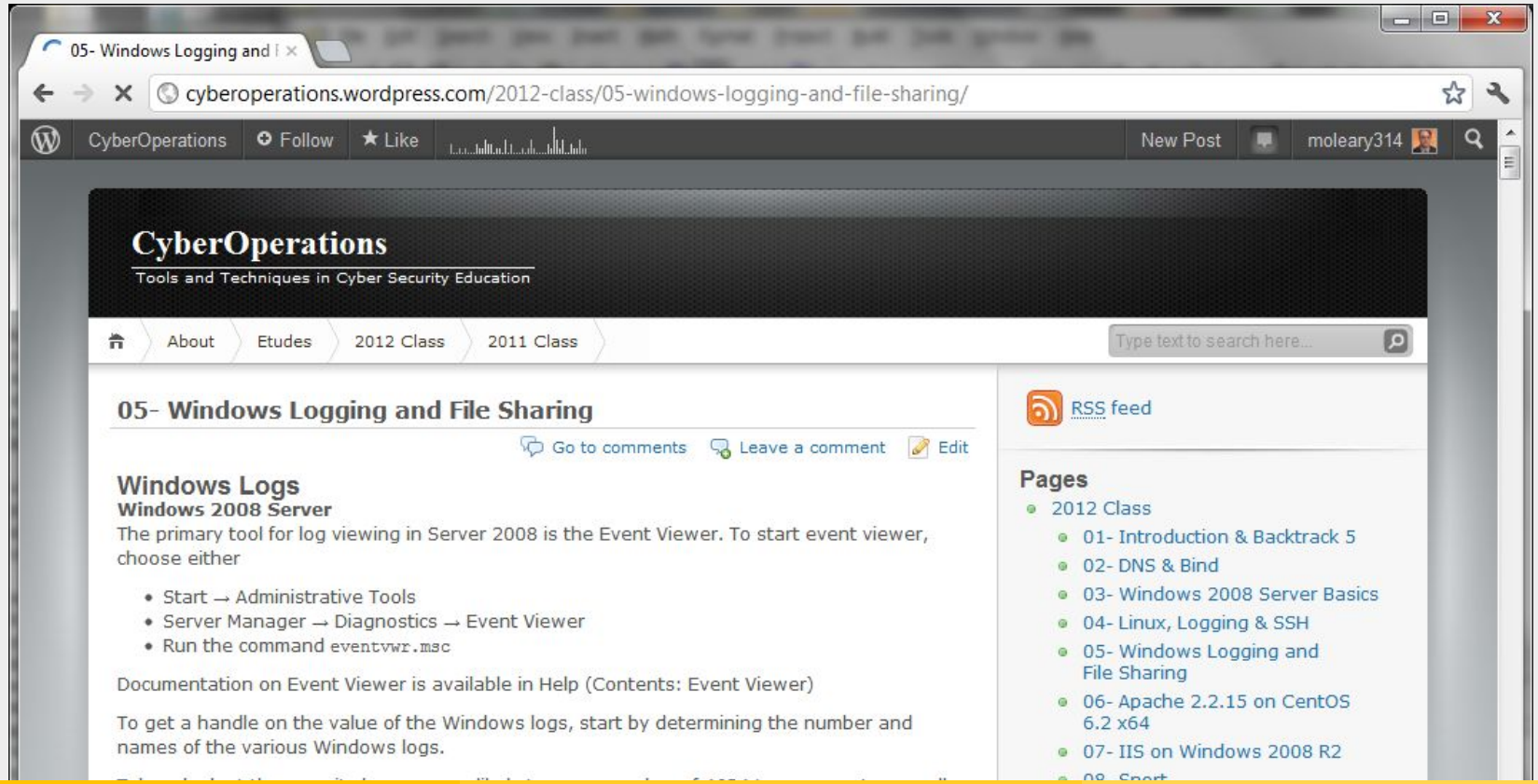
- Four teams of three to six students.
- Students are given functional requirements for a network.
  - Students design, build, and implement their own network.
- Typical exercise tasks require
  - DNS infrastructure
  - Domain controllers
  - File servers
  - Remote access (*e.g.* SSH, RDP)
  - Logging infrastructure
- More complex exercise tasks include
  - Web servers (IIS and/or Apache)
  - Databases
  - Intrusion detection systems (Snort)
  - E-Commerce solutions (*e.g.* Zen Cart)
  - IPFire firewall solutions

Classroom Competitions: Structure

- Students provide the instructor with credentials for their network.
- Some credentials are secretly provided to other teams, who verify that the required services are running.
- Student teams without credentials are free to attack using any available tools.
- Student teams with credentials are free to attempt to escalate privileges.
- Student teams cannot know in advance if connections are legitimate (service verifications) or attacks.
- Some attacks are prohibited for pedagogical reasons- *e.g.* resource exhaustion DoS or log deletions.
- Students are graded on the basis of a written report
- Example: `http://pages.towson.edu/moleary/docs/Classes/Cosc481-S12/Exercise3.pdf`

Classroom Competitions: Lessons

- The instructor does not need to build all of the machines for the network.
- The instructor does not know the true state of the network.
- Course material is now available at `cyberoperations.wordpress.com`



Prebuilt Competitions: Environment

- Local competition used to prepare student teams for regional and national competitions.
- Two to four teams of four to eight students.
- Organizer provides each team with 6-10 prebuilt machines
  - These are identical, save for names and addresses.
  - They cover a range of services and operating systems.
- The systems are deliberately misconfigured to contain security holes.
  - Students can play offense by playing defense.
- Students are awarded points for
  - Detecting and remediating holes in their own network
  - Successfully attacking other teams
  - Style
    - Why style?

Student Cyber Defense Teams

Source: http://lolcats.icanhascheezburger.com/2012/06/06/funny-cat-pictures-there-was-a-fly-the-point-is-i-got-it/

Prebuilt Competitions: Holes

- What kinds of holes can be put on systems?
  - Pre-shared SSH keys
  - Trojaning Metasploit
  - Configuring VNC to silently start on boot
  - Modifying path variables to allow other programs (*e.g.* netstat) to be trojaned
  - Misconfiguring FTP servers- allowing anonymous read/write, or running as root
  - Putting tools like PHPShell on the web server
  - Adding privileged users to the system
    - This is particularly fun via cron jobs or at tasks to occur later
  - Using xinetd to bind a root shell
  - Changing permissions on key system files
  - Trojaning startup documentation

Prebuilt Competitions: Lessons

- Setup time is formidable
  - 4 teams $\times$ 6-10 systems $\times$ 2-3 hours per system = a long week.
- Systems are less recyclable than might be expected
- Student interaction with the systems is limited to competition time
- Students enjoy the puzzle nature of the event

Build-A-Net Competitions: Design

- Student teams are provided with precise network specifications, which they then build on their own as virtual machines.
  - Windows 2003 Server (Not R2), DC, DNS, RDP
  - Windows 2008 Server (Not R2), DC, RDP, Exchange
  - Fedora Core 4, DNS, SSH, MySQL (4.1.1)
  - Ubuntu 8.04, SSH, Apache, PHP, MySQL, Joomla 1.5.12
  - Fedora 6, SSH, vsftpd 2.0.5
  - Windows XP (No SP) joined to the domain
  - Windows Vista SP1, joined to the domain
- Precise required version numbers of other software (browsers, mail clients, .pdf readers, Adobe Flash) are provided.
  - Version numbers are selected with known vulnerabilities in mind
- Software can be found at MSDNAA or at various open source repositories.
  - The site `http://oldapps.com` is quite valuable for older Windows software.

Build-A-Net Competition: Timing & Lessons

- The amount of lead time provided to the students depends on their ability level.
  - For newer students, one to two weeks.
  - For advanced students or multi-school competitions, 48-72 hours.
- Students mis-estimate (badly) the amount of work necessary to set up such a network.
- Students learn much in this format.
- Significantly less work for the organizer.

Red Team

- All of these competitions have been run both with and without an external Red Team.
- Recruiting Red Team has been much simpler than expected.
  - Approaching Red Team from the regional CCDC led to many volunteers, and to many recommendations.
  - After running these competitions for many years, graduating seniors and other former students regularly volunteer to serve.

Questions?

Mike O'Leary
School of Emerging Technologies
Towson University
moleary@towson.edu