First International Conference on Cyber Crisis Cooperation: Cyber Exercises

27 June 2012

Cyber Exercises, Small and Large

Commander Mike Bilzor
Computer Science Department
U.S. Naval Academy
Annpolis, Maryland U.S.A.
bilzor@usna.edu

Cyber Exercise - Small

In the Classroom

Intro to Cyber Security

- Freshman (first year) class, ~18-year-old students
- One-semester course, ~600 students per semester
- Taken by all students, regardless of intended major
  - No background knowledge assumed
- First offered in 2011-2012 academic year

Course Outline - Three Sections

Public Site: http://www.usna.edu/cs/si110/

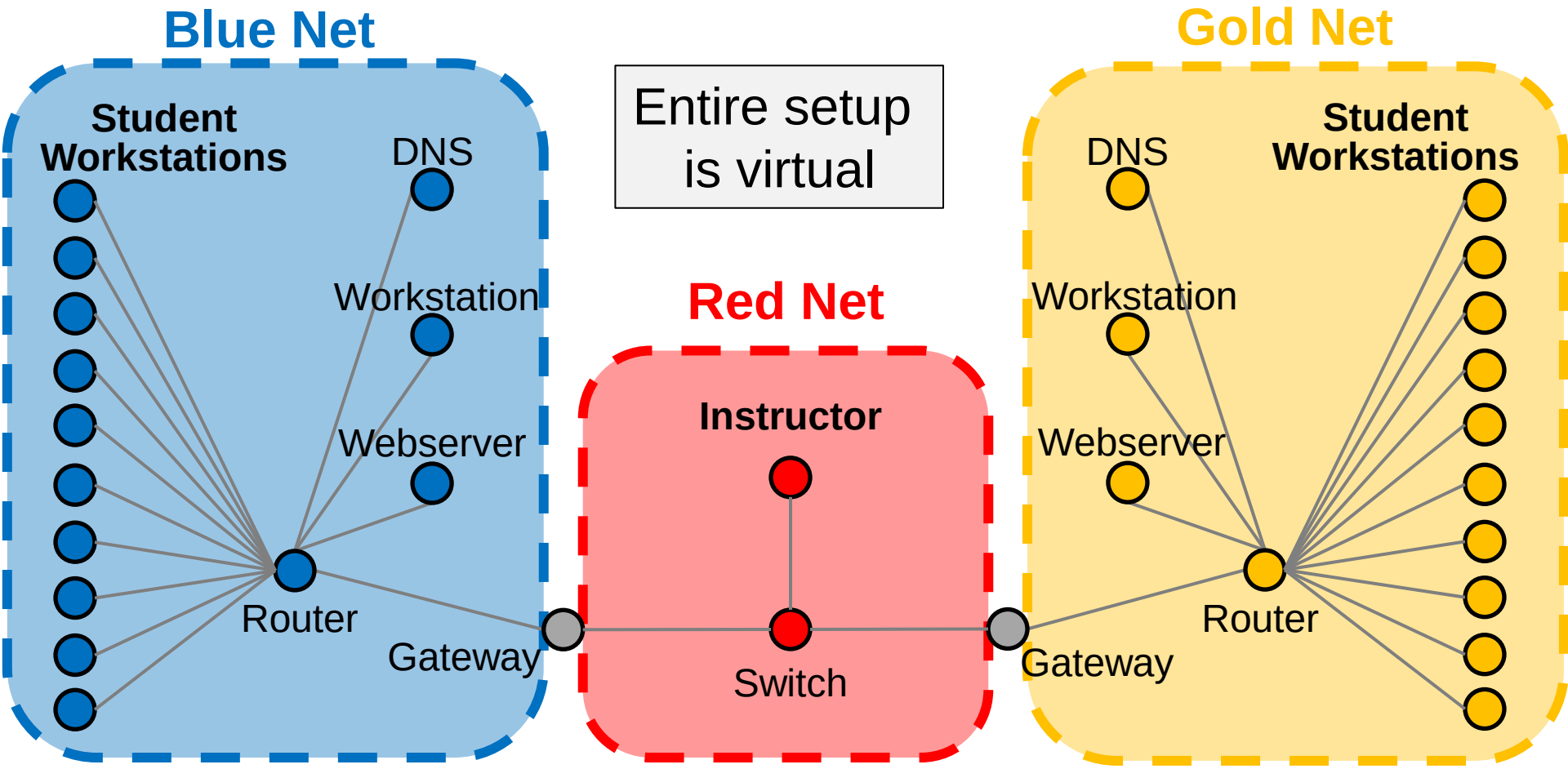
- The Cyber Battlefield
  - Digital data, computer components, operating systems, programs
  - Web: Servers, browsers, HTML, build your own webpage, scripting, injection attacks, cross-site scripting
  - Networks: Protocols, build-a-LAN lab, wireless networks
- Models and Tools
  - Information assurance, firewalls, authentication and cryptography, certificates
- Cyber Operations
  - Forensics, malware, network reconaissance, network attack, network defense

Exercise - End of Semester

- Course culmination - three labs, each 2 hours long
  - Network Reconaissance
  - Network Attack
  - Network Attack and Defense

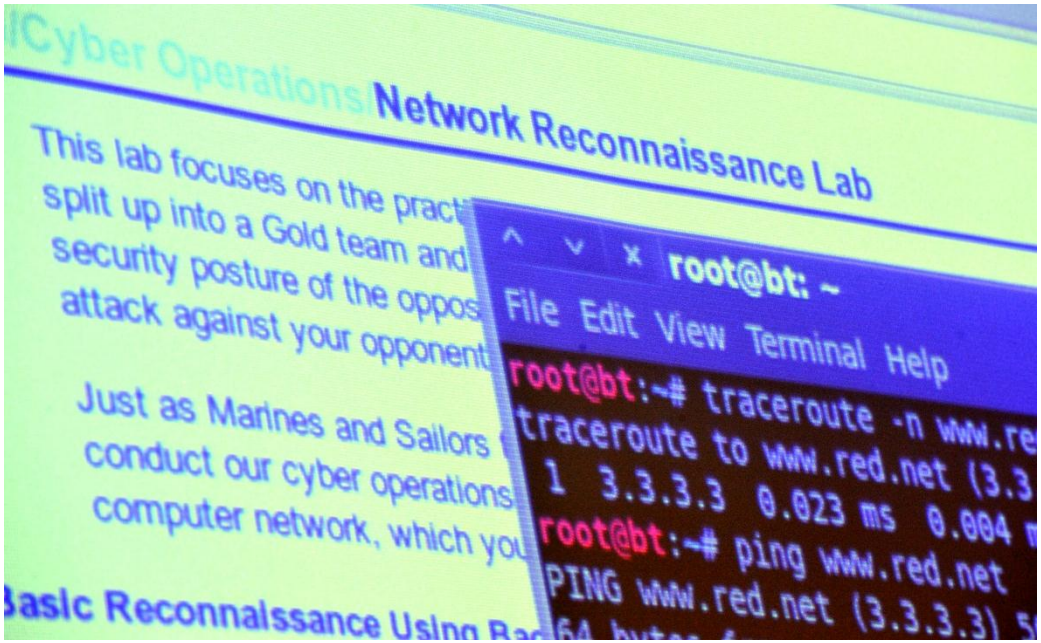
Classroom Cyber Exercise

- Each class (20 students) divided into two teams
  - Each team has 10 students, one student leader



Classroom Cyber Exercises

- Tools
  - Central servers - three VMWare ESX servers
  - Student and Instructor client - VSphere Client
  - Exercise target virtual machines to attack/defend
    - Windows Server 2003
    - Windows XP
    - Ubuntu Linux
  - Student virtual workstations
    - Backtrack 5



Conduct

- Offense: semi-scripted initially, with "hints" on vulnerabilities
  - Metasploit Framework attacks - denial of service, password cracking, etc.
- Defense: strengthen passwords, encrypt valuable information, construct firewall rules, remove/restrict unnecessary accounts, privileges, and services
- Goals:
  - Capture the flag - adversary data token
  - Compromise adversary services: accounts, web site, DNS, etc.

Observations and Lessons

- Need most/all of one semester of instruction for freshmen (1st year) to develop necessary skills, even for introductory/semi-scripted cyber exercise

- Can't overstate the value of:
  - VMWare ESX Server and VSphere Client
  - Administration of setup using Windows Powershell
  - These tools allow for changing exercise configuration in hours, and clean restart of all virtual machines in minutes (e.g., between consecutive class periods)

Cyber Exercise - Large

Multiple Universities: CDX

CDX: Cyber Defense Exercise

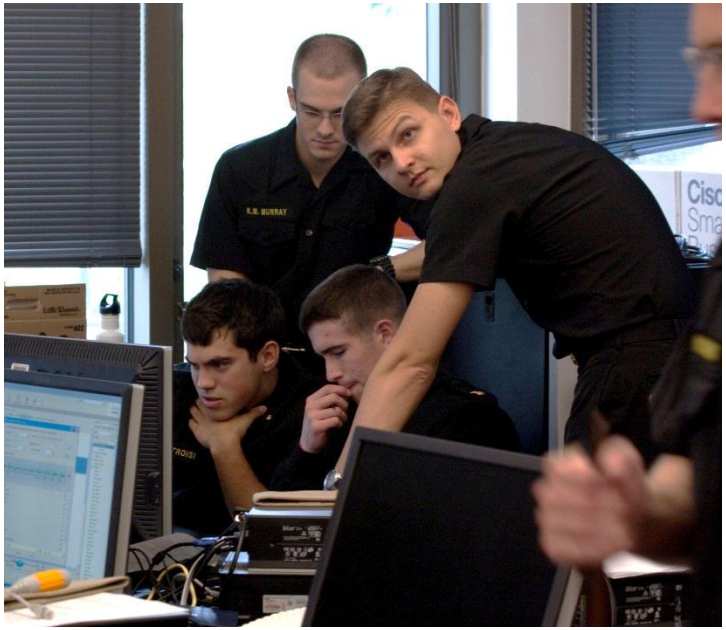
- Designed for military school students
  - Faculty coach, but students perform all exercise tasks
- Currently defense only (no attack)
- Sponsored by NSA
- Exercise occurs annually, over three days in April

Regular Participants

U.S. Naval Academy
U.S. Air Force Academy
U.S. Military Academy
U.S. Coast Guard Academy
U.S. Merchant Marine Academy
U.S. Naval Postgraduate School
Air Force Institute of Technology
Royal Military College of Canada

CDX: Conduct

- NSA
  - Publishes annual directive, network specification
  - Establishes VPN tunnel with each participating school
  - Serves as "red team" attacker
  - Keeps score
- Scoring basis:
  - Service availability
  - Data confidentiality
  - Data/System integrity

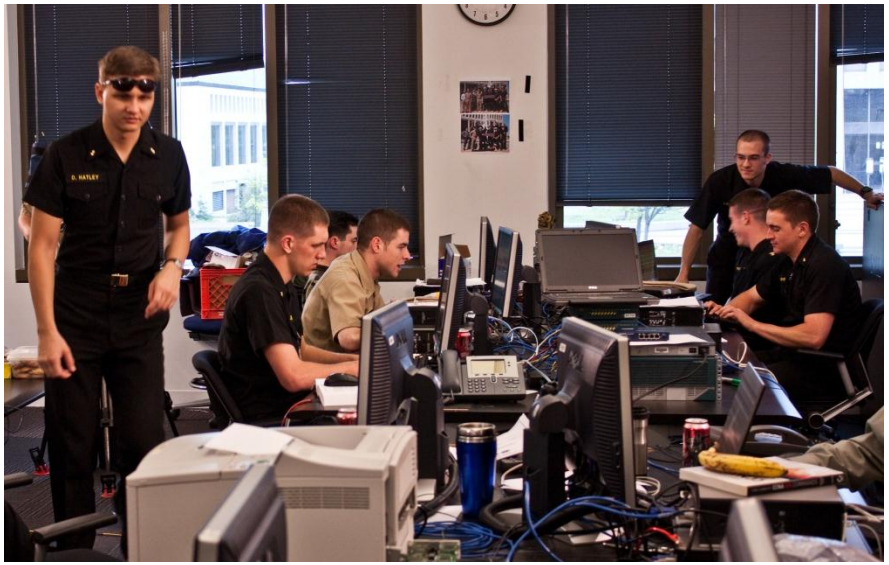


CDX: Services to Defend

- DNS
- Active Directory
- Network Time Protocol
- E-Mail: SMTP, IMAP
- FTP
- IPv4 and IPv6
- VoIP

- User workstations
  - Web server
- Remote access
  - SSH or RDP

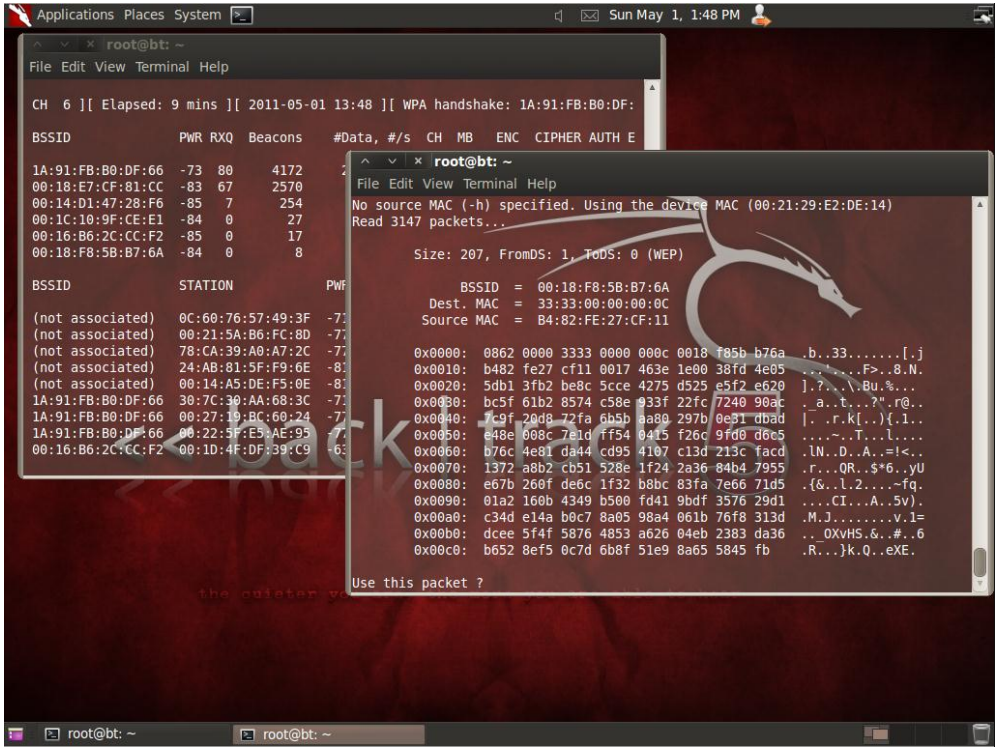
Attack/Defend Window
0900-2200 each day, for 3 days



CDX: Attacks

- Red Cell attacks are unclassified, but representative of common real-world threats

- May use Metasploit Framework or other publicly avavailable hacking tools



CDX Philosophy

- Current focus: students build network systems from scratch, to be as secure as possible
  - Must provide services (e-mail, chat, DNS, SSL, etc.), but students choose the configuration and the software

- Possible future alternative: each school receives identical pre-built network virtual images
  - NSA pre-builds the networks and services
  - Images contain some hidden vulnerabilities
  - Students first examine and secure the networks (patch, update, restrict services, etc.), then defend them

Observations and Lessons

- Systems are 100% virtual - VSphere, ESX
- Commercial classes are expensive, but valuable
  - SANS, etc.
- During the exercise, students run the show
- Using many different geographic locations is okay
- Scoring is automated, but there are always debates regarding points
  - After all, it's a competition

Questions?