



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
Annapolis, 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



- The Cyber Battlefield

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

- 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 Reconnaissance
 - Network Attack
 - Network Attack and Defense

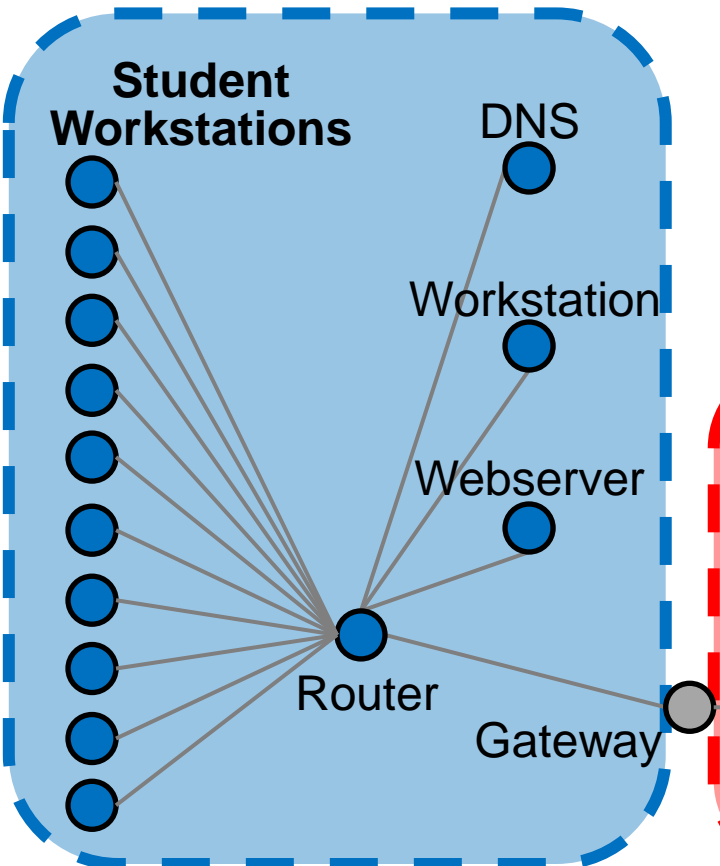




Classroom Cyber Exercise

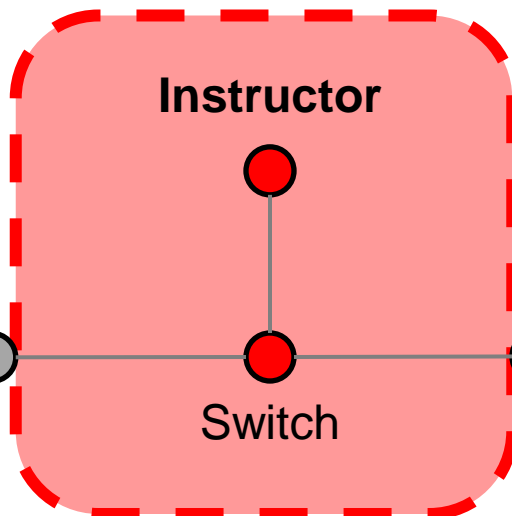
- Each class (20 students) divided into two teams
 - Each team has 10 students, one student leader

Blue Net

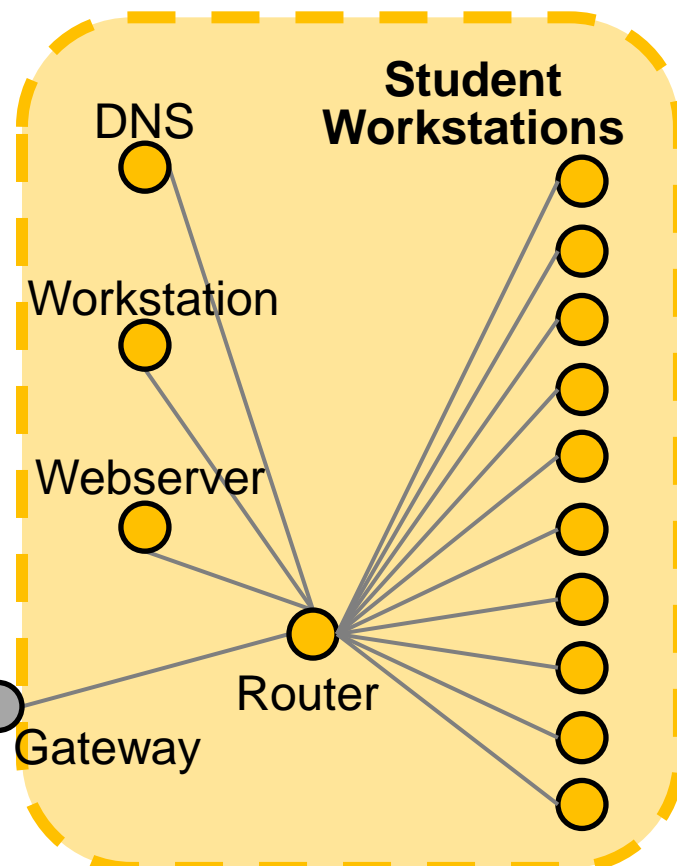


Entire setup
is virtual

Red Net



Gold Net



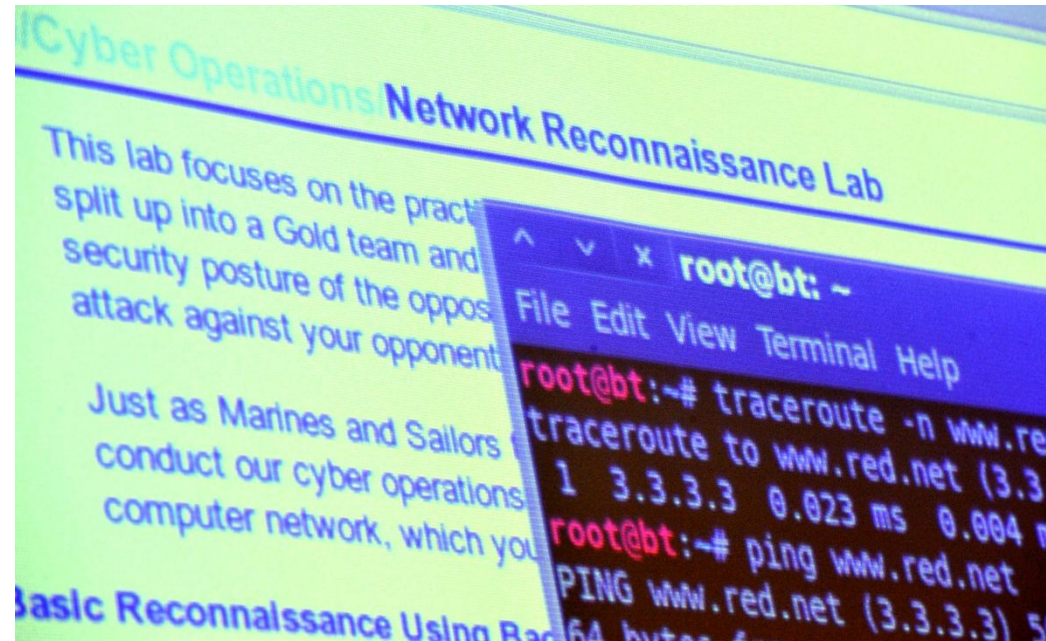


Classroom Cyber Exercises



• 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

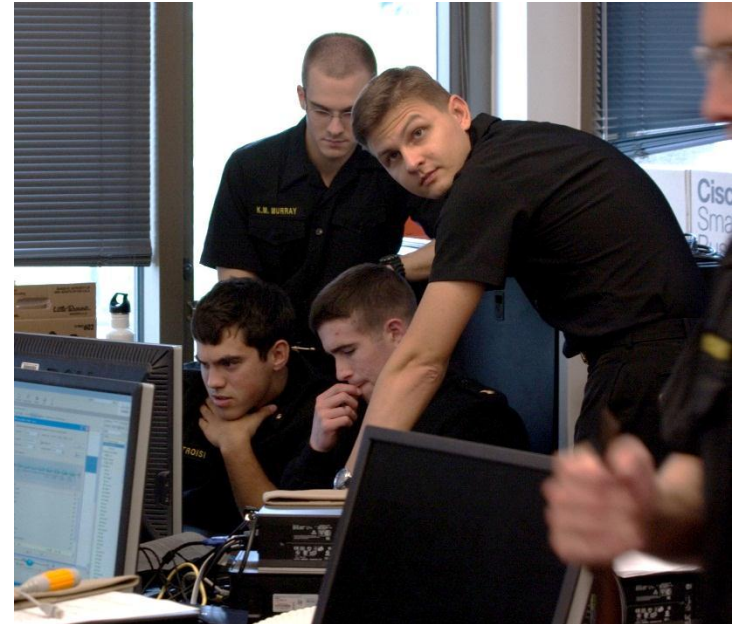
U.S. Naval Academy
U.S. Air Force Academy
U.S. Military Academy
U.S. Coast Guard Academy
U.S. Merchant Marine Academy
U.S. Naval Postgraduate School
Air Force Institute of Technology
Royal Military College of Canada



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 available hacking tools

```
Applications Places System Sun May 1, 1:48 PM
root@bt: ~
File Edit View Terminal Help
CH 6 ][ Elapsed: 9 mins ][ 2011-05-01 13:48 ][ WPA handshake: 1A:91:FB:B0:DF:
BSSID Pwr RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
1A:91:FB:B0:DF:66 -73 80 4172
00:18:E7:CF:81:CC -83 67 2570
00:14:D1:47:28:F6 -85 7 254
00:1C:10:9F:CE:E1 -84 0 27
00:16:B6:2C:CC:F2 -85 0 17
00:18:F8:5B:B7:6A -84 0 8

BSSID STATION Pwr
(not associated) 0C:60:76:57:49:3F -71
(not associated) 00:21:5A:B6:FC:8D -77
(not associated) 78:CA:39:A0:A7:2C -77
(not associated) 24:AB:81:5F:F9:6E -81
(not associated) 00:14:A5:DE:F5:0E -81
1A:91:FB:B0:DF:66 00:27:19:BC:60:24 -77
1A:91:FB:B0:DF:66 00:22:5F:EA:95 -77
00:16:B6:2C:CC:F2 00:10:4F:DF:39:C9 -63

root@bt: ~
File Edit View Terminal Help
No source MAC (-h) specified. Using the device MAC (00:21:29:E2:DE:14)
Read 3147 packets...

Size: 207, FromDS: 1, ToDS: 0 (WEP)

BSSID = 00:18:F8:5B:B7:6A
Dest. MAC = 33:33:00:00:00:0C
Source MAC = B4:82:FE:27:CF:11

0x0000: 0862 0000 3333 0000 000c 0018 f85b b76a .b..33.....[.j
0x0010: b482 fe27 cf11 0017 463e 1e00 38fd 4e05 .....F>..8.N.
0x0020: 5db1 3fb2 be8c 5c2e 4275 d525 e5f2 e620 ].?..Bu.%...
0x0030: bc5f 61b2 8574 c58e 933f 22fc 7240 90ac [.a.t...?.r.o..
0x0040: 7c9f 20d8 72fa 6b5b aa80 297b 0e51 dbad [.r.k[...]{.1..
0x0050: e48e 008c 7e1d ff54 0415 f26c 9fd0 d6e5 .....T..l...
0x0060: b76c 4e81 da44 cd95 4107 c13d 213c facd .LN..D..A..!<.
0x0070: 1372 a8b2 cb51 528e 1f24 2a36 84b4 7955 .r...QR..$*6..yU
0x0080: e67b 260f de6c 1f32 b8bc 83fa 7e66 71d5 .{&.l.2...-fq.
0x0090: 01a2 160b 4349 b500 fd41 9bdf 3576 29d1 .....CI...A..5v).
0x00a0: c34d e14a b0c7 8a05 98a4 061b 76f8 313d .M.J.....v.1=
0x00b0: dcee 5f4f 5876 4853 a626 04eb 2383 da36 ..OXVHS.&.#..6
0x00c0: b652 8ef5 0c7d 6b8f 51e9 8a65 5845 fb .R...}k.Q..eXE.

Use this packet ?
```



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?

