Collegiate Cyber Defense Competition

Ben Actis

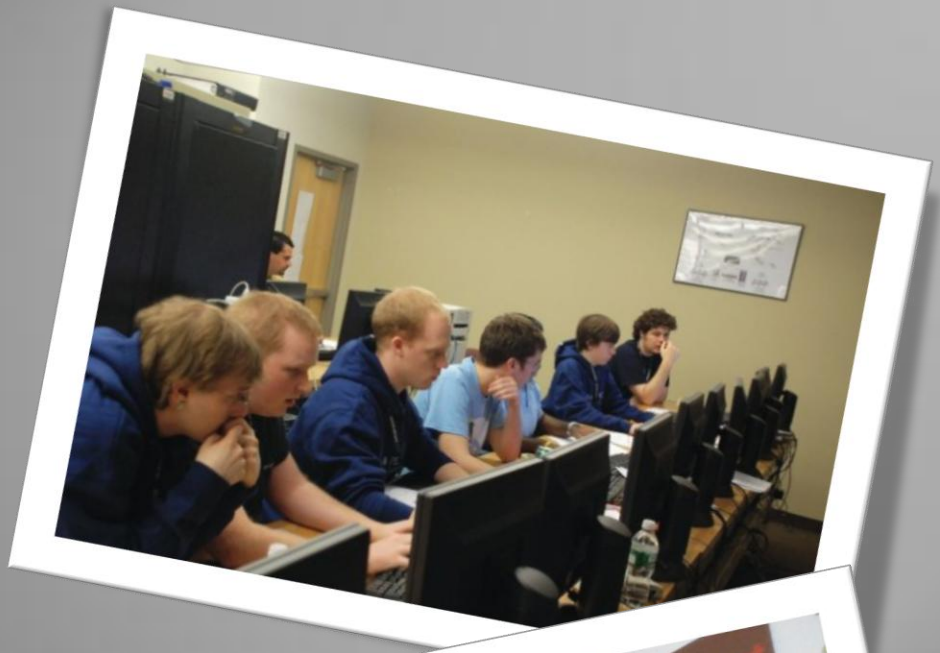
Readers digest version

- NECCDC
- Layout
- Prep
- Actual game day

NECCDC Background

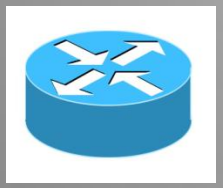
Rules

- Defensive only
- Rewarded for
  - Data Preservation
  - Services
  - Injects
- Penalized for
  - Successful breaches



Layout

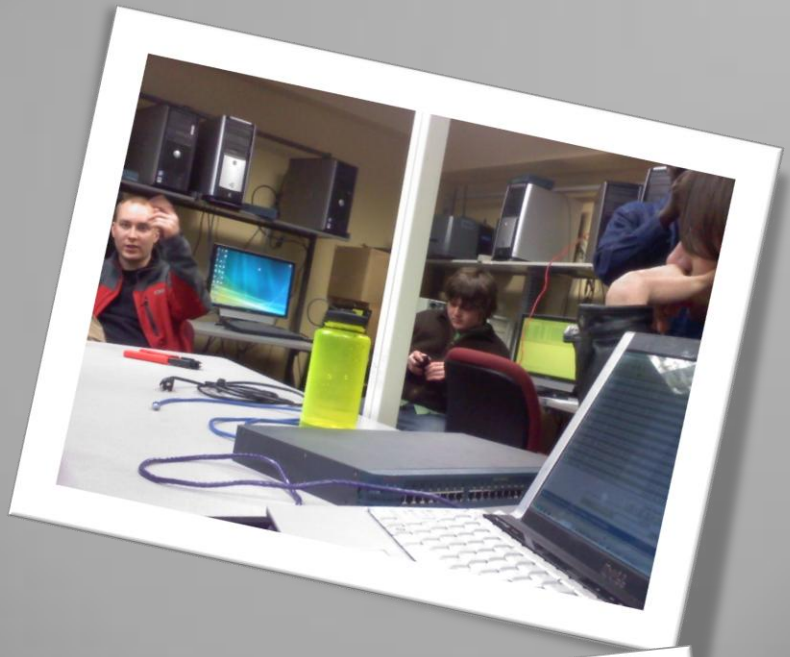
Cisco Router 1841



Cisco Catalyst Switch

Prep

- Perimeter Approach
- Lockdown guides
- Detection

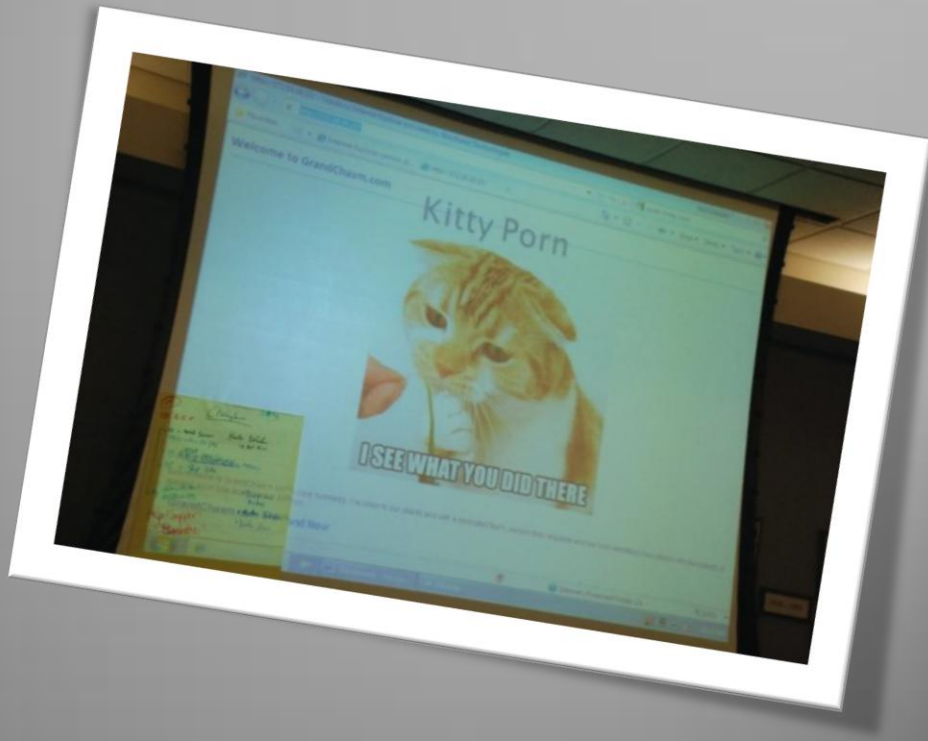


Day 1 11am –7pm

- Passwords
  - Screen saver exploit
- OS Switch
- Compromised router
  - Keylogger
  - SNMP
- Wireless Printer
- Windows 2008 down
- DNS poisoning
- Security websites

Day 1 continued

- Windows 2000 domain
  - IPsec firewall on 2000*
- Unix Based
  - IP tables
  - tripwire
- Windows 2000 hit
  - RPC hit on port 135
  - Similar to blaster, NT authority shutdown
  - Refined IPsec
- Internal vulnerability scans

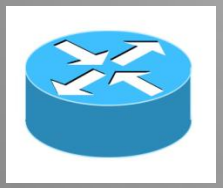


Day 2 8am-7pm

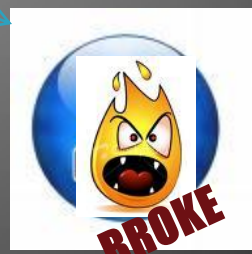
- Windows 2008 issues
  - Compromised?
  - Image issues
  - AD replication failed
  - Hypervisor exploit
- RE3 to Cent OS 3.0
- Win XP reinstall
- Wireless fiasco
- Slackware
- HTTPS

Day 2 Layout

Cisco Router 1841



Cisco Catalyst Switch



Prep for next year & ranking

- Windows 2008 server core
- Host Based IDS
- Consolidated logging
- Placement