Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015

Jelena Mirkovic*, Aimee Tabor+, Simon Woo*, Portia Pusey★
*USC/ISI, +UC Berkeley, ★National CyberWatch Center

Competitions as Recruitment Tools

- Cyber offense, defense or both

+ Fun
+ Engaging
+ Group activity

- Difficult
- Detail-oriented
- Adversarial

ACM Tapia 2015

- ACM Richard Tapia Conferences
  - Celebrate diversity in computing
  - Bring together undergrads, grads, faculty, researchers and professionals
  - After-conference activities: university tours, industry visits, workshops
- Security workshop
  - Includes a hands-on activity like Capture-The-Flag
  - Organized by UC Berkeley TRUST center since 2014
  - No prerequisites to attend, required pre-registration

Novices and Competitions

- Challenging
  - Require background in networking and/or OS
  - Require strong coding skills (scripting)
  - Details matter
  - Many strategies possible for attack/defense
  - Teamwork is crucial
  - Easy to get left behind
- Not ideal as a recruitment tool
  - But fun, engaging, appeal to young people

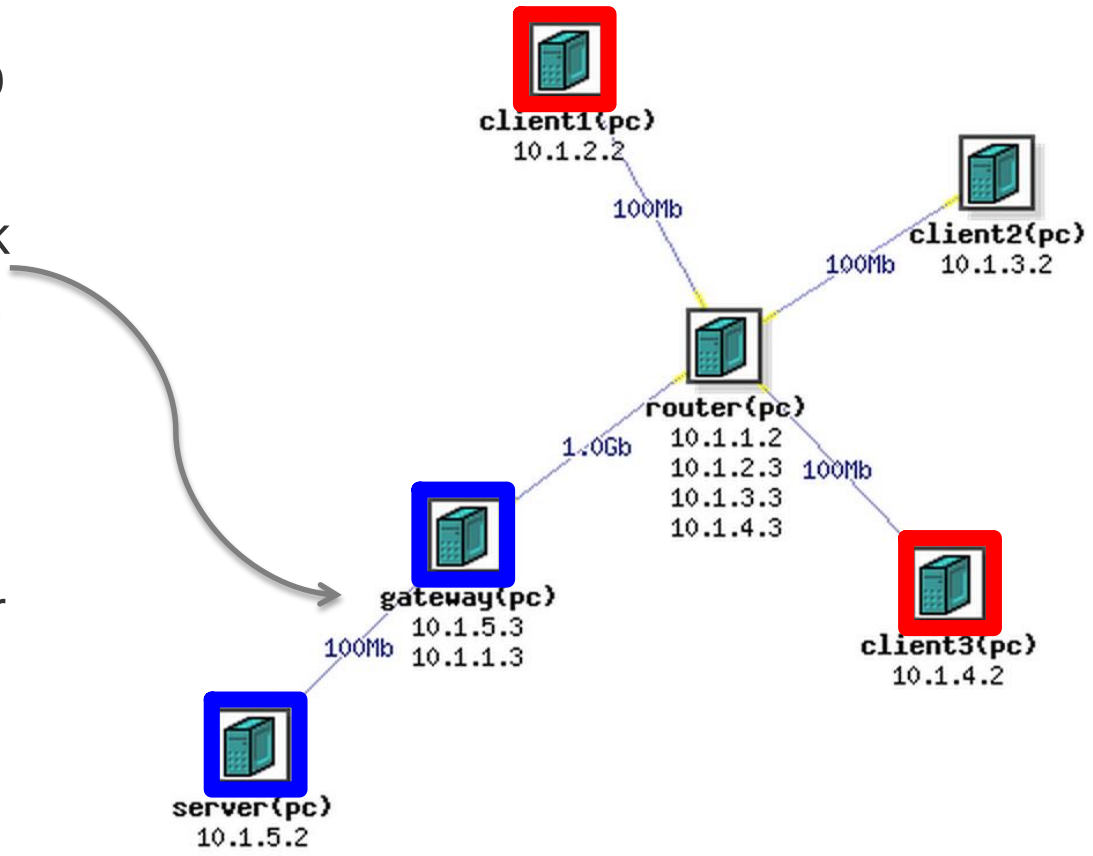
Class Capture-The-Flag

- Integrated with DeterLab http://www.deterlab.net
- Done after lectures and hands-on homeworks
  - Experience adversarial thinking, internalize knowledge

Feature	CCTF
Preparation	A few weeks
Duration	2 h
Topic	Intrusions, DDoS, DNS, BGP, crypto…
Team roles	Both Blue and Red
Occurrence	2-3 times per semester
Difficulty	Intermediate

Resilient Server CCTF

- Red team floods the server node from two clients
  - Targets the bottleneck link or the application, may spoof
- Blue team protects the server
  - Filters at the server or at the gateway
  - Doesn't know which one is the good client



Resilient Server CCTF

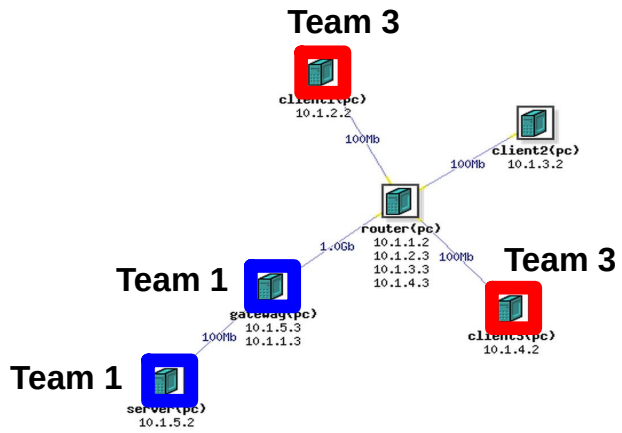
- Score by legitimate client's experience
  - Slow or no response – red team's point
  - Fast response – blue team's point
- Why choose this exercise for the workshop?
  - Easy phenomena to explain to novices
  - Easy to perform the attack, just send lots of traffic
  - Many options for attack/defense

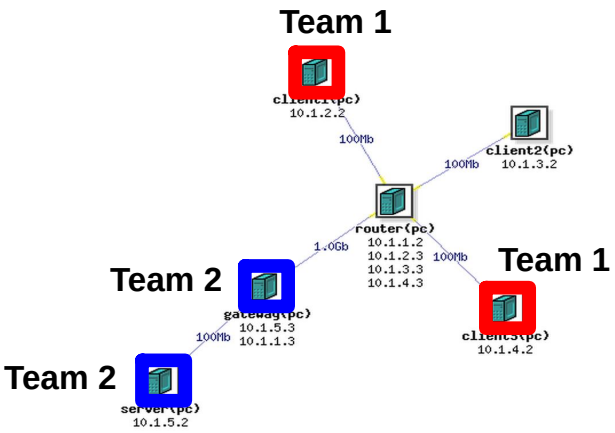
Adjustments for the Workshop

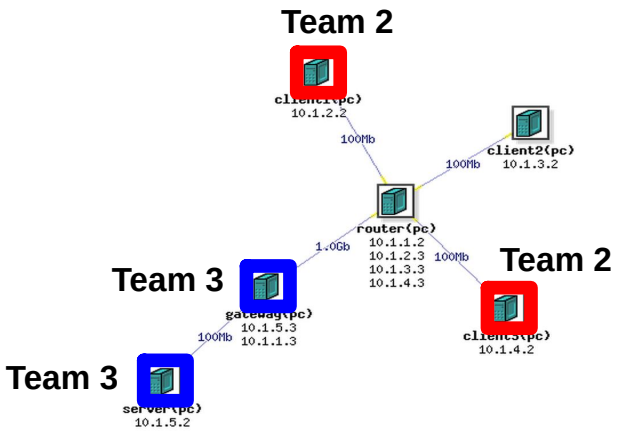
Factor	Adjustment	Outcome
Short prep	Flooder and Slowloris tools provided	Helped by introducing structure
Short prep	Mandatory Linux and DeterLab BoF	Helped by instructional scaffolding
Varied skills	Balanced teams	Helped somewhat (bias and low turnout)
No background	Background materials given before the workshop	Helped somewhat (low adoption)
No background	Mentors with each team	Helped by instructional scaffolding

Competition Setup

- 3 teams
  - Each sub-divided into Blue group and Red group
- 3 parallel competitions







Organizational Challenges

- Team rebalancing
  - Some pre-registered students did not show up
  - Students did not self-evaluate correctly
  - One strong team, two weaker ones
- Background materials are useless
  - A few students read them, missed details
  - Assume self-learning but novices not good at it
  - Mentors helped
- Mixed population
  - Undergrads had harder time than grads

Evaluating Learning/Engagement

- Pre- and post- questionnaire
  - Using a modified UTRECHT-9
  - Measured engagement (feeling happy, inspired, enthusiastic)
  - Measured learning for specific tasks
    (e.g., “I am confident I can develop monitoring software on the gateway machine that will let me automatically check if server is getting slow.”)
- Only 5 matched pairs (out of 18 participants)
  - Show increase in learning and engagement

Roadmap

- Gamification!
- Balance teams by skills and seniority
  - Experience matters
- Advance collection of demographic/competence info
  - Use objective measures like quizzes
- Team building
  - Ice-breaker activities, mentors
- Event logistics
  - Reach all participants; bring new ones to speed
- Additional scaffolding and community building
  - Share knowledge with all teams, demo key activities

Gamification

- A game with clear, easy rules
  - Red team: launch or stop an attack
    - Flooding: UDP/TCP/ICMP, port 80 or random, spoof or not
    - Application: Slowloris
  - Blue team: place or remove a filter
    - At gateway: By protocol, port or IP
    - At application: By conn. duration
- Tools for situational awareness
  - Amount of attack and legitimate traffic reaching the server, breakdown by protocol, port and IP
  - What is dropped by filter

Thank You!

- sunshine@isi.edu
- Stay tuned for competition games!
  - And may the odds be ever in your favor
- If you are interested in hands-on materials for teaching cybersecurity
  - Visit DeterLab – free, easy to use, lots of support

  http://www.deterlab.net