From Training to Education: Building Offensive Curriculum from Training Certifications

By: Michael Kranch

CANSec 2018 – October 27-28

Who Am I?

- B.S. / M.S. in Computer Science
- U.S. Army Cyber Officer
- Assistant Professor USMA (West Point)
  - Coach of the Capture the Flag (CTF) Team
  - Coach of the Cyber Defense Team

www.mjkranch.com

Warning: Opinions Follow

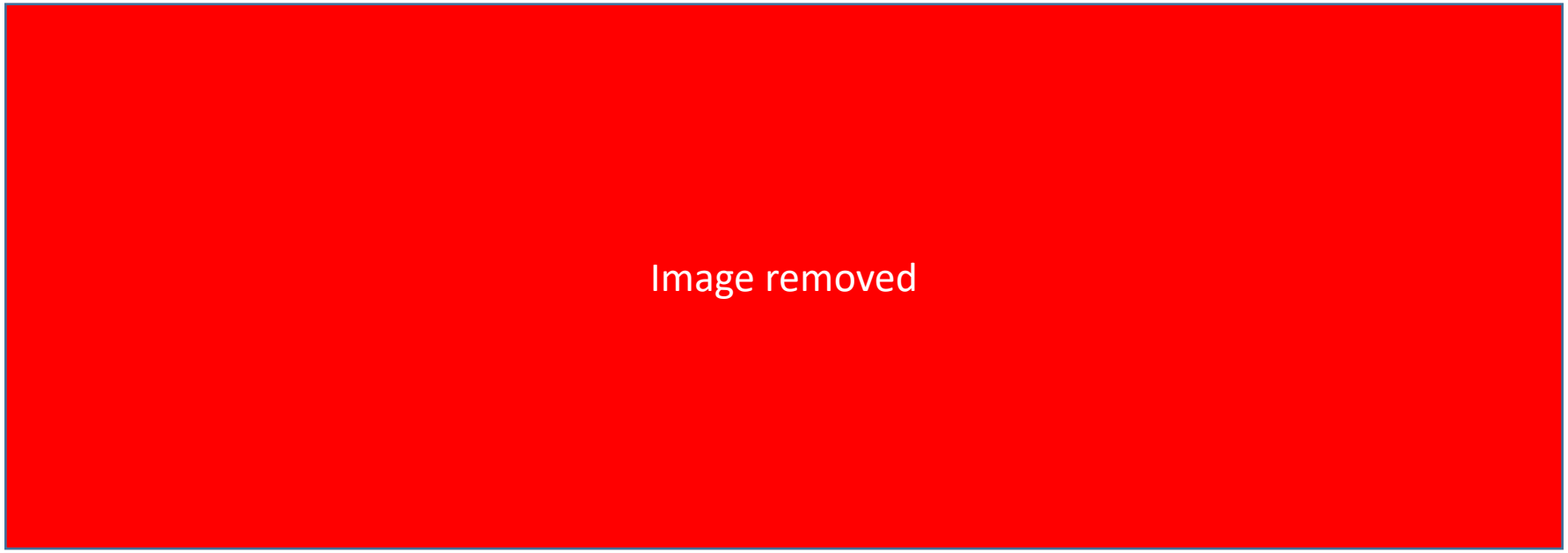
So What?

- Developing offensive courses is hard but important
- Industry security certifications provide a useful blueprint
  - Real-world applicability
  - Tested Framework
  - Motivation (Gamification)
- Incorporating the academic mindset (the why) to the industry training (the what) provides the best hybrid experience for your students.

How did I get here?

Coaching a CDC

Then I Visited the Red Team



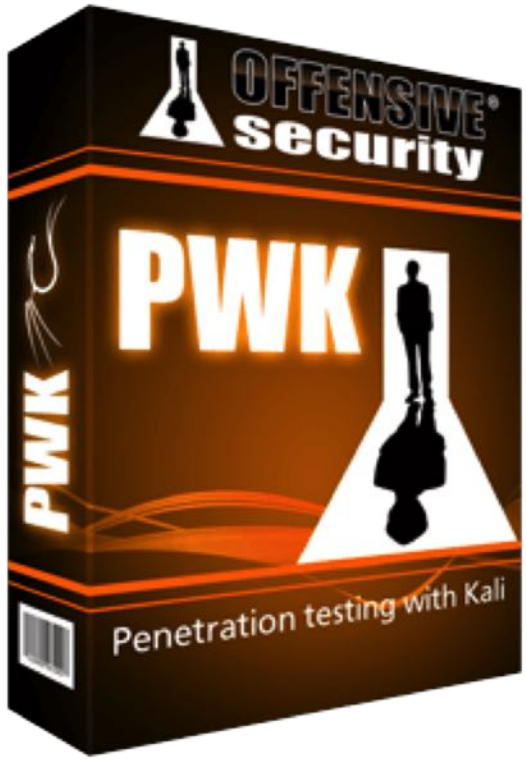
Offensive Curriculum is Hard

- Breadth of Subject Matter
  - Diverse pre-requisites (really skills)
  - IT or CS or both?
  - Troubleshooting is hard
- Large Infrastructure Requirement
  - Maintaining intentionally breakable systems
- Fast Evolution of Material
  - New tools / techniques
  - New exploits (Eternal Blue)

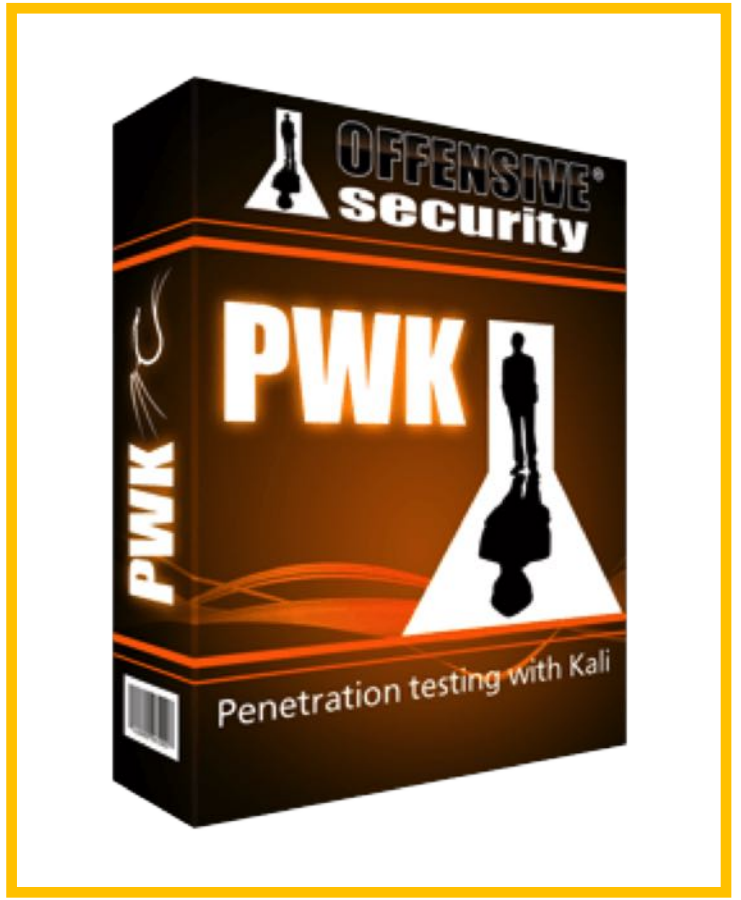
Offensive Curriculum is Hard

- Breadth of Subject Matter
  - Diverse pre-requisites (really skills)
  - IT or CS or both?
  - Troubleshooting is hard
- Large Infrastructure Requirement
  - Maintaining intentional breakable systems
- Fast Evolution of Material
  - New tools / techniques
  - New exploits (Eternal Blue)
- Legal / Network Issues

Leverage Industry



Leverage Industry



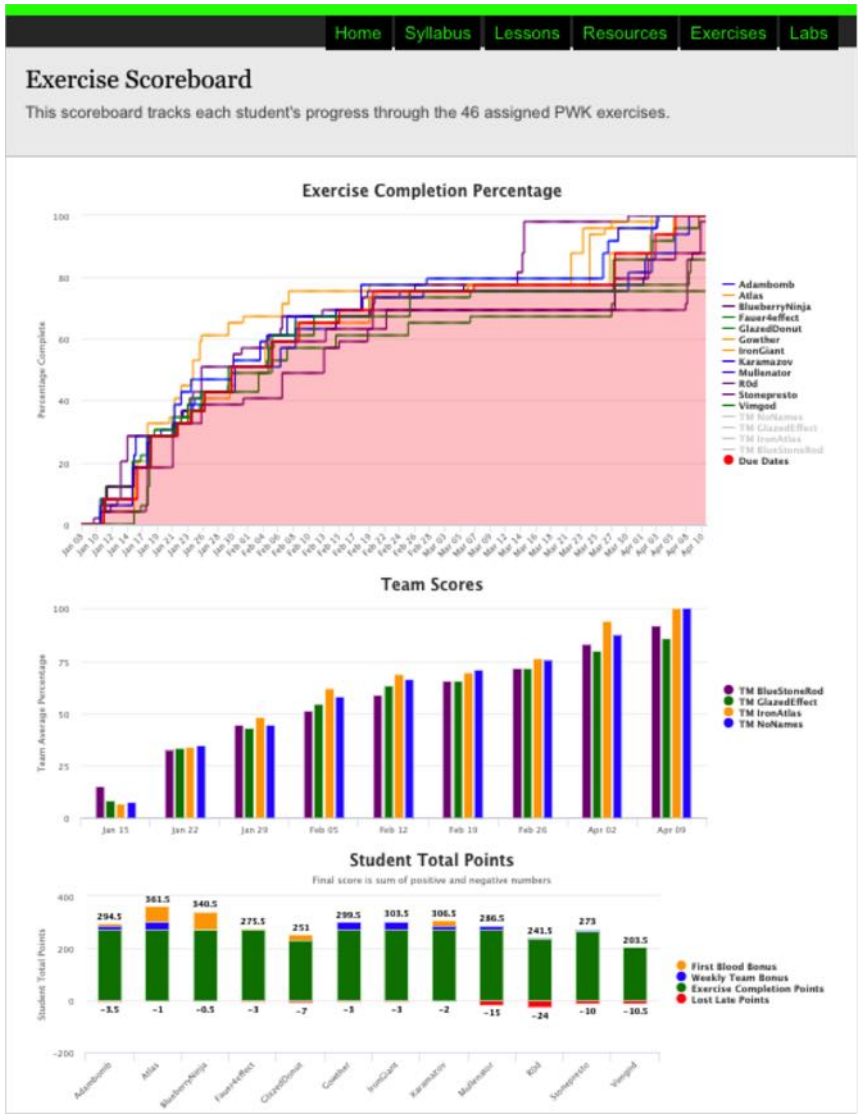
Penetration Testing With Kali

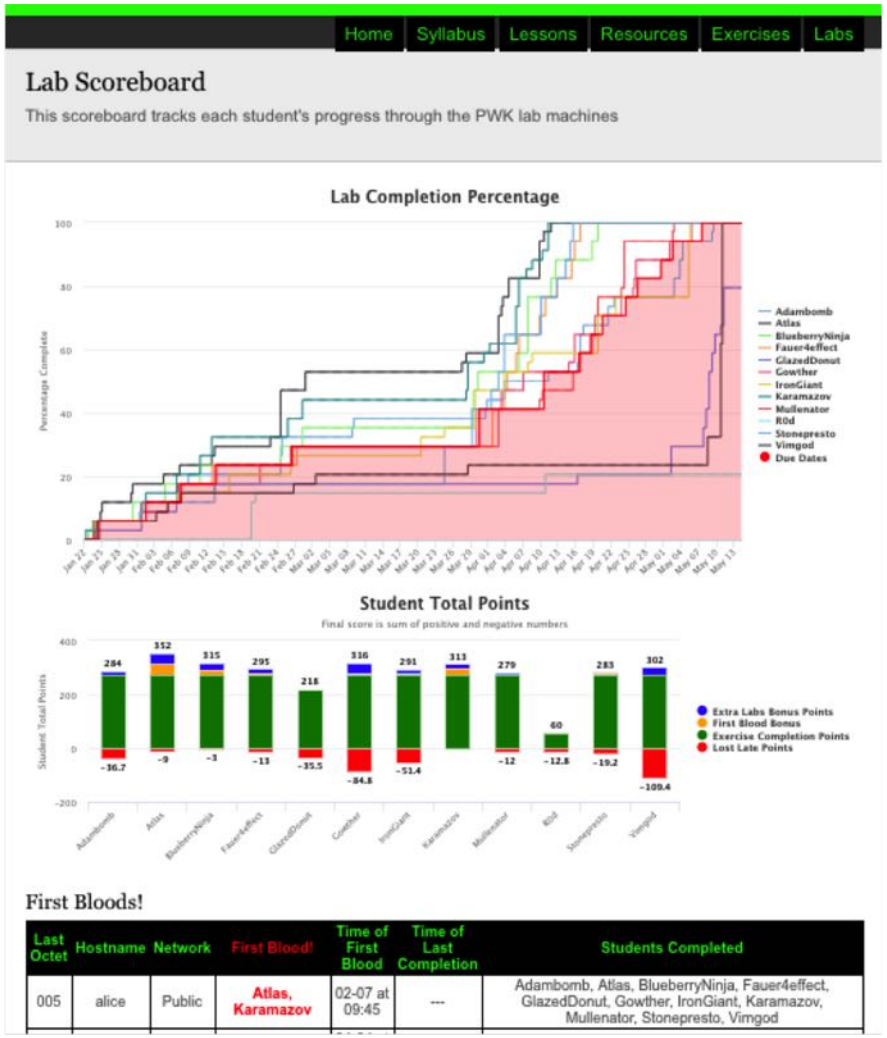
- Course by Offensive Security (Kali Linux)
- Introduces students to ethical hacking tools and techniques
  - Initial Exercises
    - 7 hours of provided videos
    - 350+ page pdf lab guide
    - Local Kali VM / Private Windows 7 Lab Machine
    - Accessed via private VPN
  - Interactive Lab
    - 40 Public Machines
    - ~15 Additional Machines on 3 additional subnets
- Certification (OSCP) - a unique 24-hour performance based exam
  - Very low pass rate

CS485: Ethical Hacking Pilot

- Teaching Methodology
  - All requirements issued at start of semester
  - Lessons simply deeper discussion of course material
  - Extensive use of Gamification
    - Progress tracked live via course website
    - Culminating live performance based final exam
- Students
  - 2017 - 6 Students
    - 4 Seniors, 1 Junior, 1 Sophomore
    - All CS
  - 2018 – 12 Students
    - 6 Seniors, 5 Juniors, 1 Sophomore
    - 8 CS, 2 IT, 1 EE, 1 Math

Gamification Examples

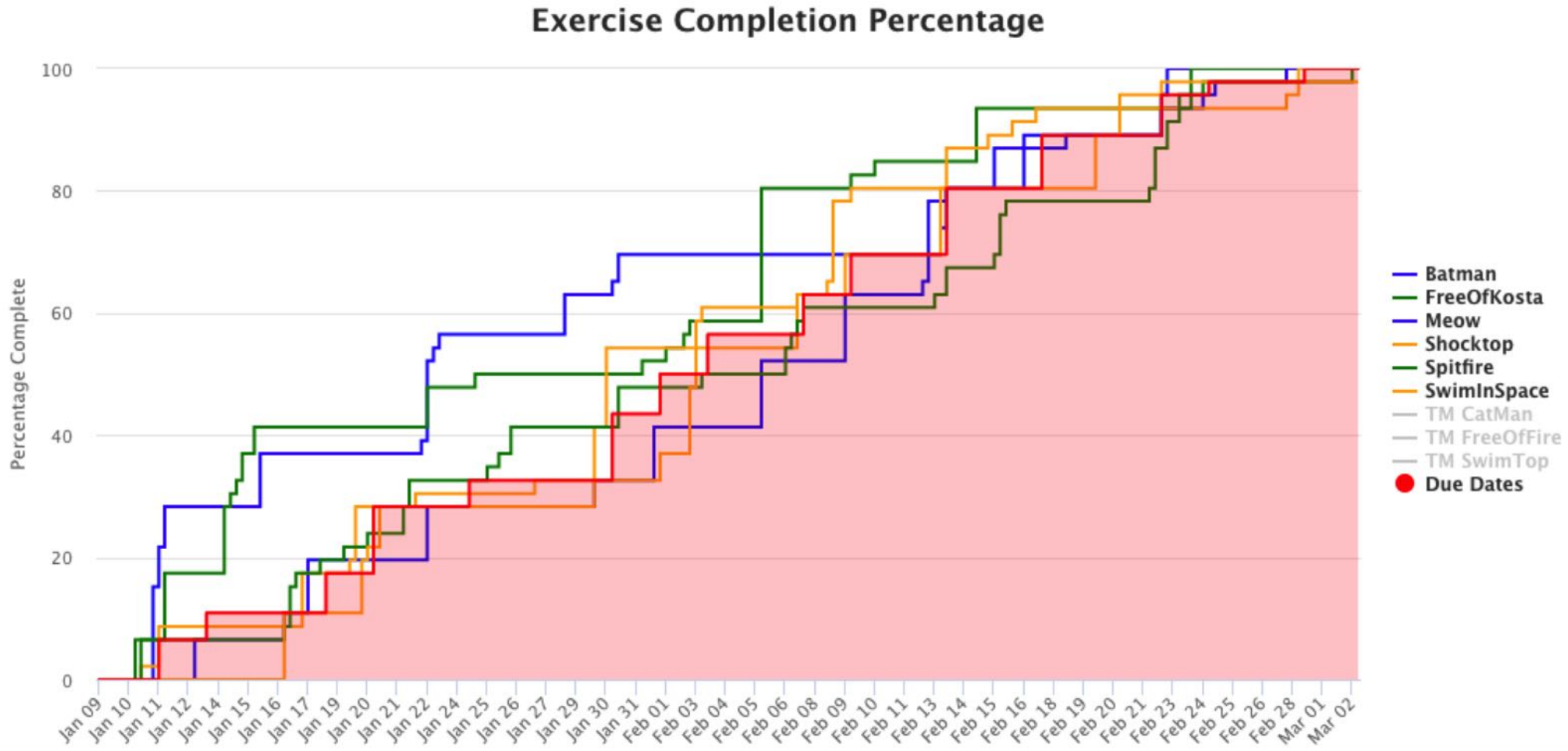




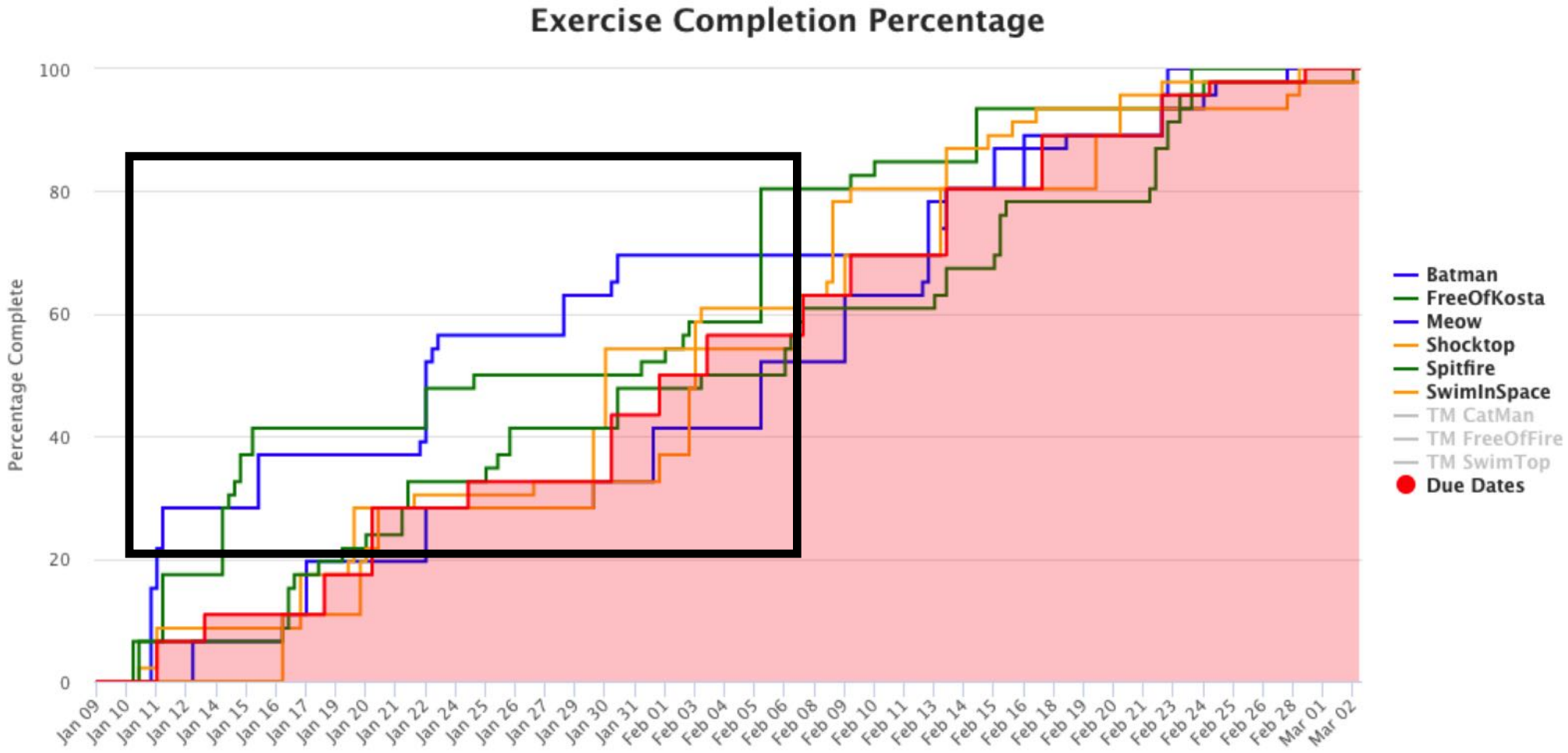
First Bloods!

Last Octet	Hostname	Network	First Blood!	Time of First Blood	Time of Last Completion	Students Completed
005	alice	Public	Atlas, Karamazov	02-07 at 09:45	---	Adambomb, Atlas, BlueberryNinja, Fauer4effect, GlazedDonut, Gowther, IronGiant, Karamazov, Mullenator, Stonepresto, Vimgod

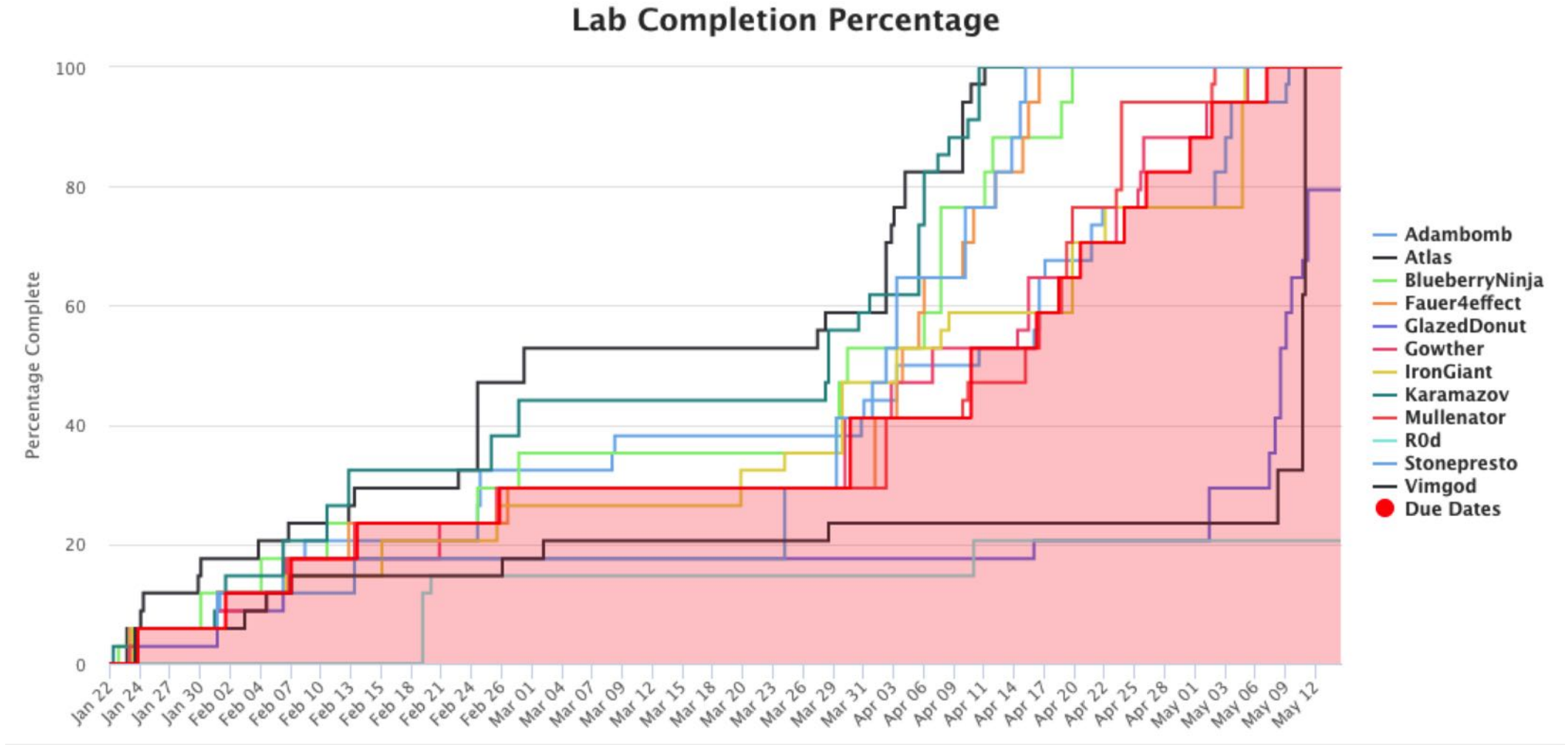
Gamification Examples



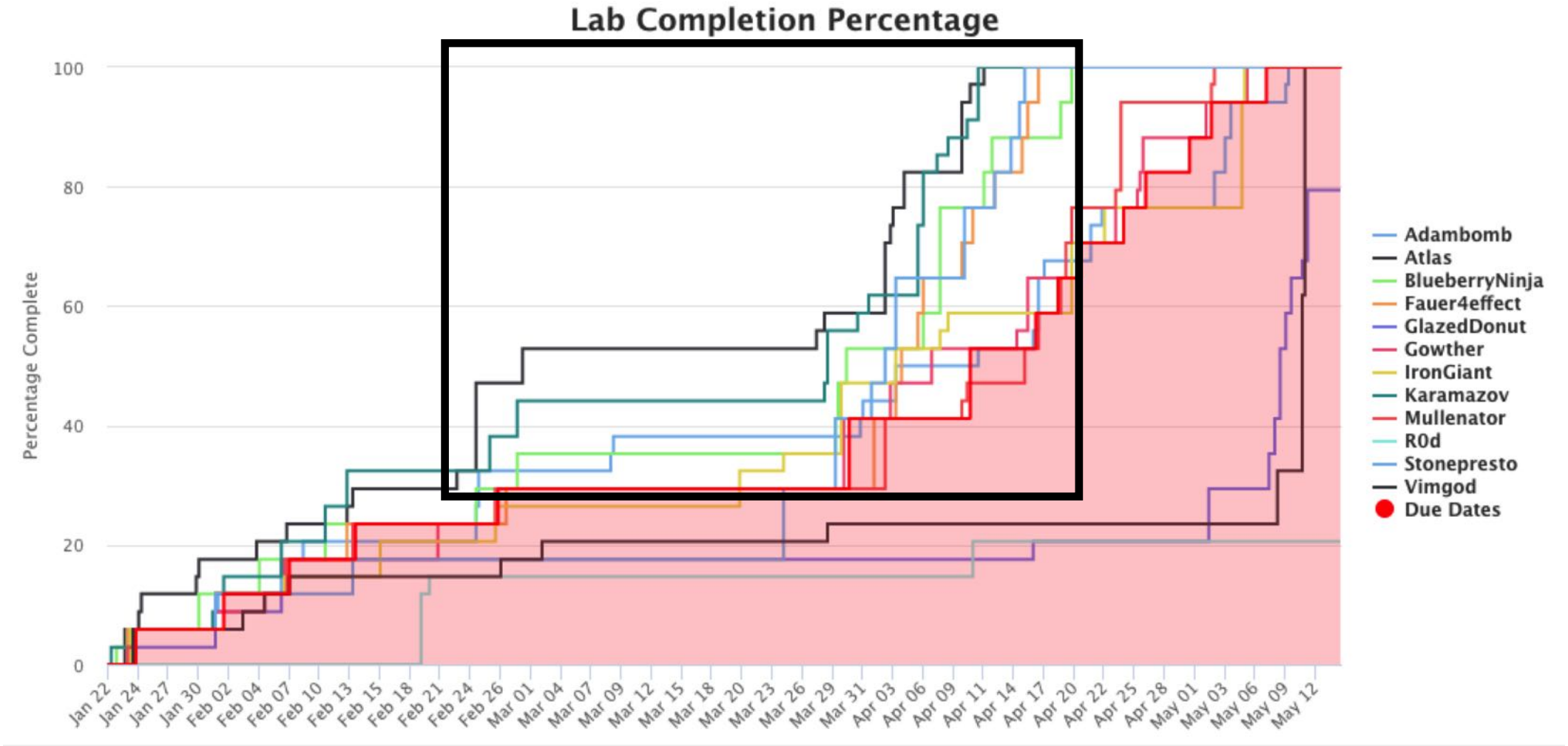
Gamification Examples



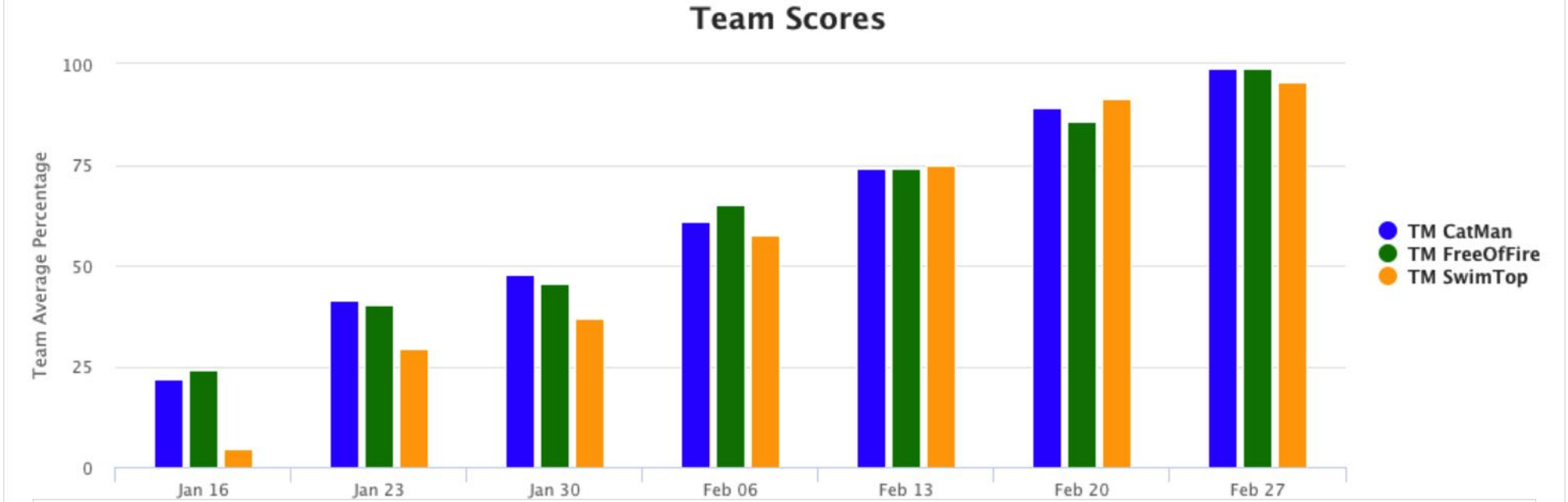
Gamification Examples



Gamification Examples



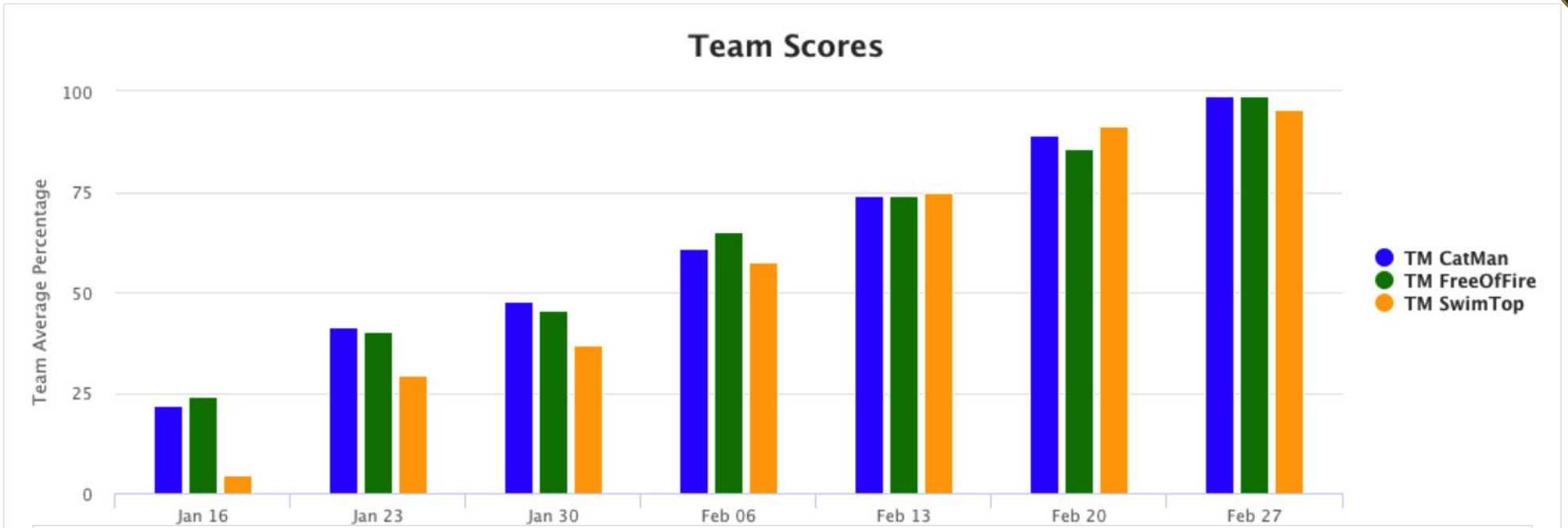
Gamification Examples



Weekly Winners

Week #	Date	Winning Team
1	Monday, January 16 at 00:00	TM FreeOfFire
2	Monday, January 23 at 00:00	TM CatMan
3	Monday, January 30 at 00:00	TM CatMan
4	Monday, February 06 at 00:00	TM FreeOfFire
5	Monday, February 13 at 00:00	TM SwimTop
6	Monday, February 20 at 00:00	TM SwimTop
7	Monday, February 27 at 00:00	TM CatMan, TM FreeOfFire

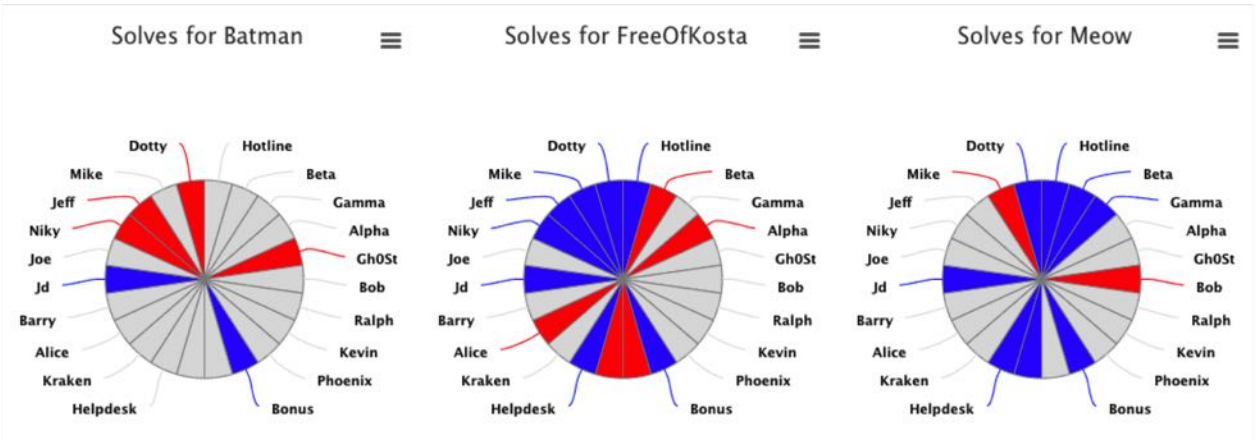
Gamification Examples



Weekly Winners

Week #	Date	Winning Team
1	Monday, January 16 at 00:00	TM FreeOfFire
2	Monday, January 23 at 00:00	TM CatMan
3	Monday, January 30 at 00:00	TM CatMan
4	Monday, February 06 at 00:00	TM FreeOfFire
5	Monday, February 13 at 00:00	TM SwimTop
6	Monday, February 20 at 00:00	TM SwimTop
7	Monday, February 27 at 00:00	TM CatMan, TM FreeOfFire

Live Performance Based Exam



Results

- **Gamification** provided extra motivation (passion)
  - Individual Competition
  - Team Cooperation
  - Incentive to work ahead of deadlines
  - Perseverance through frustrating troubleshooting
- Class format provided **deeper understanding**
  - Answer questions / issues from material
  - Focus on "why" and did not have to discuss much "how"
  - Only possible with smaller class size
- Students **internalized the hacker mindset**
  - 8/18 earned OSCP

So What?

- Developing offensive courses is hard but important
- Industry security certifications provide a useful blueprint
  - Real-world applicability
  - Tested Framework
  - Motivation (Gamification)
- Incorporating the academic mindset (the why) to the industry training (the what) provides the best hybrid experience for your students.

Thank you!

Questions?

www.mjkranch.com