Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts

Michael Kranch
www.mjkranch.com

CISSE – June 10th, 2019

How can we best teach future cybersecurity professionals?

So What?

- Offensive and defensive techniques both teach cybersecurity's core competencies
- Cybersecurity requires resilient lifelong learners, and offensive techniques best develop these attributes
- Combining academia's concept focus (the why) with industry's relevant training (the what) through gamification (the how) provides the best hybrid education experience

Motivation

Cyb NSA ATTACKS WEST POINT! RELAX, IT'S A CYBERWAR GAME PX)

Capture the Flag (CTF)

Red Teaming the CDX

Coaching the CDX

Offense vs. Defense

- Do offensive techniques really establish a better mindset?
- Can both offensive and defensive techniques be used to teach the same security skills?

Offense vs. Defense

- Do offensive tech[illegible]lly establish a better mindset?
- Can both offen[illegible]e and [illegible]sive techniques be used to teach [illegible]ecurity skills?

Offense vs. Defense

Offense vs. Defense

- What are cybersecurity's core skills?
- Which skills do offensive and defensive techniques teach?
- Does the technique actually impact the resulting mindset?

What are cybersecurity's core concepts?

Core Concepts Definition

- The concepts expected of any cybersecurity professional entering the workforce
- Equivalent to **fundamental knowledge** or **essential skills**
- Three components:
  - Timeless
  - Not tied to current technology
  - Those ideas that provide the greatest barrier to future mastery (specialization)

Is this a Core Concept?

Digital Forensics?

Programming or Scripting?

Vulnerability Assessment?

Networking?

Reporting?

Enjoying Tasty Beverages?

Command Line Tools?

Malware Analysis?

Cybersecurity Frameworks

- NICE Cybersecurity Workforce Framework
- Cybersecurity Curricula 2017 (CSEC2017)
- Cybersecurity Assessment Tools (CATS) Project

NICE Workforce Framework

Does not establish core skills

CISSE

NICE Workforce Framework

Does not establish core skills

Cybersecurity Curricula 2017

- Establishes the guidelines for post-secondary degree programs in cybersecurity
  - A JTF of 325 contributors from 35 countries
- 8 Knowledge Areas (KAs)
  - Data, Software, Component, Connection, System, Human, Organization, and Societal
- **Defines essential concepts in each KA**

Association for Computing Machinery

IEEE COMPUTER SOCIETY

ASSOCIATION FOR INFORMATION SYSTEMS

ifip

CISSE

CSEC17 Essential Skills Example

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

CSEC17 Essential Skills Example

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

CATS Project

- Collaborative project to build a suite of educational assessment tools
- Topics determined through a Delphi process
- Two tools:
  - Cybersecurity Concept Inventory (CCI)
    - Concepts learned after first cybersecurity course
  - Cybersecurity Curriculum Assessment (CCA)
    - Concepts understood when entering the workforce

Example CATS (CCI) Topics

Topic	Importance	Difficulty
Identify vulnerabilities and failures	9	8
Identify attacks against CIA triad and authentication	9	8
Devise a defense	9	7
Identify the security goals	9	6
Identify potential targets and attackers	9	5
Devise an attack	8	8
Given a breach, explain how to recover from it	8	8
Explain why a failure happened	8	7
Identify risky behaviors	8	7
Identify vulnerabilities based on usability issues	8	7

Which skills do offensive and defensive techniques teach?

Is it Offensive, Defensive or Both?

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

Is it Offensive, Defensive or Both?

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		**Recovery**
		Testing
		Documentation

Is it Offensive, Defensive or Both?

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

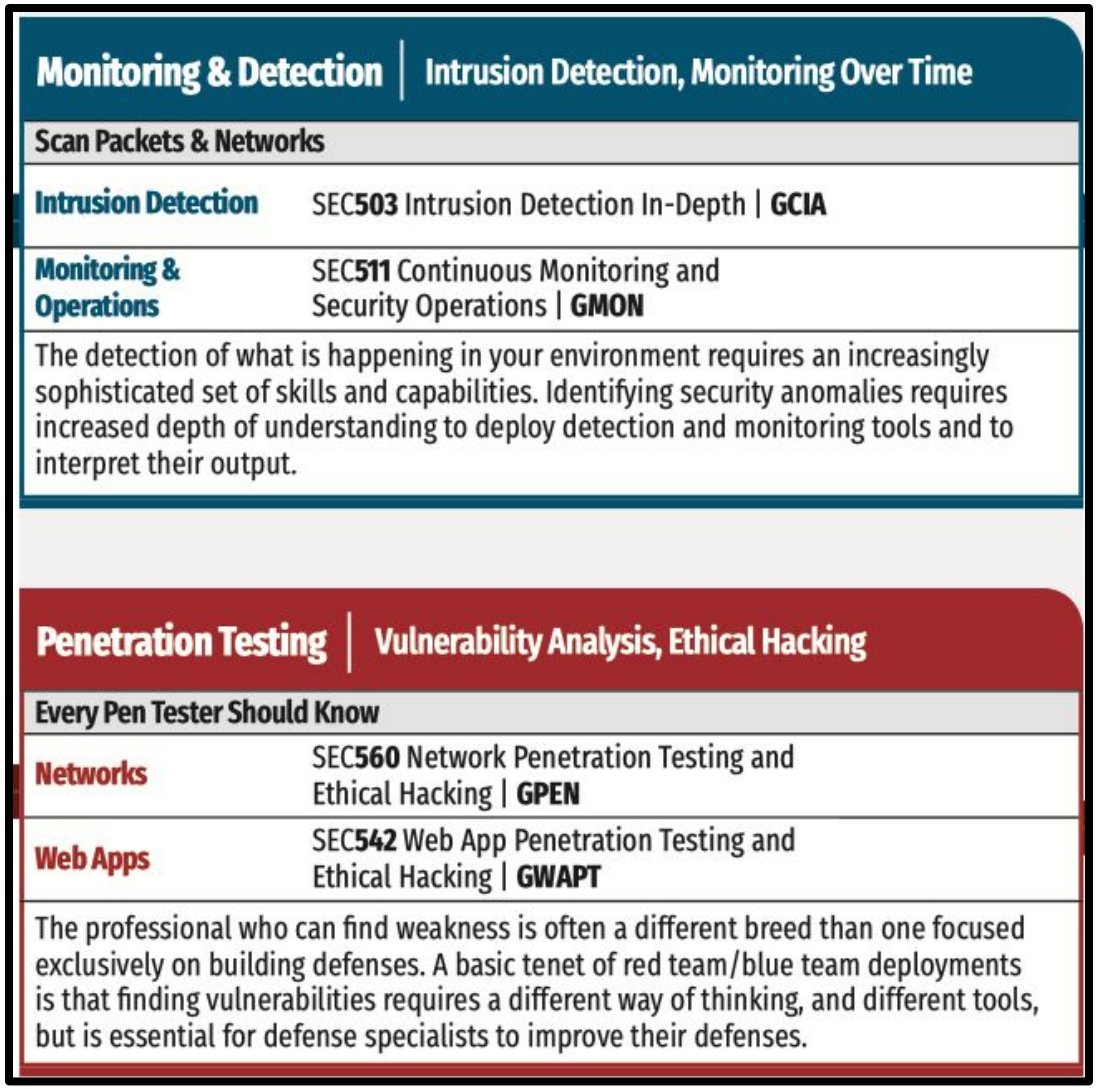
Is it Offensive, Defensive or Both?

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	**Connection attacks**	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

Methodology

- Classify a resource as offensive or defensive
  - Self classification (SANS, Offensive Security)
  - Utilize taxonomy presented in “Cybersecurity Teaching through Gamification” by Gonzalez et al.
- Measure of assessment
  - Direct observation of concepts through performing tasks
  - Analysis of syllabus
- Resources – focused on introductory resources
  - CTFs (PicoCTF & OverTheWire)
  - SANS (SEC503/511/560, FOR508)
  - Offensive Security (PWK)

SANS Classification Example



Monitoring & Detection | **Intrusion Detection, Monitoring Over Time**

Scan Packets & Networks	
Intrusion Detection	SEC**503** Intrusion Detection In-Depth | **GCIA**
Monitoring & Operations	SEC**511** Continuous Monitoring and Security Operations | **GMON**

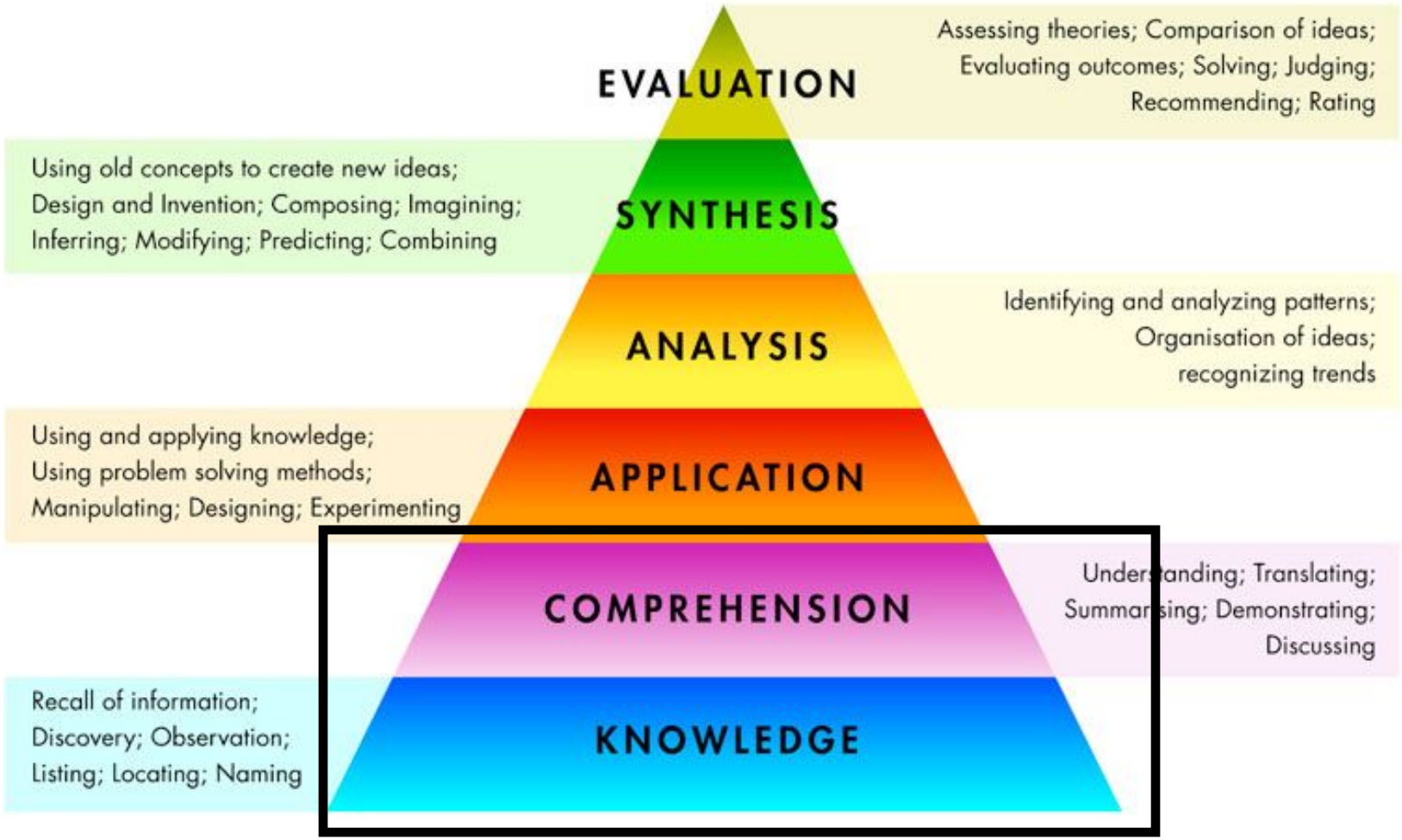
The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing | **Vulnerability Analysis, Ethical Hacking**

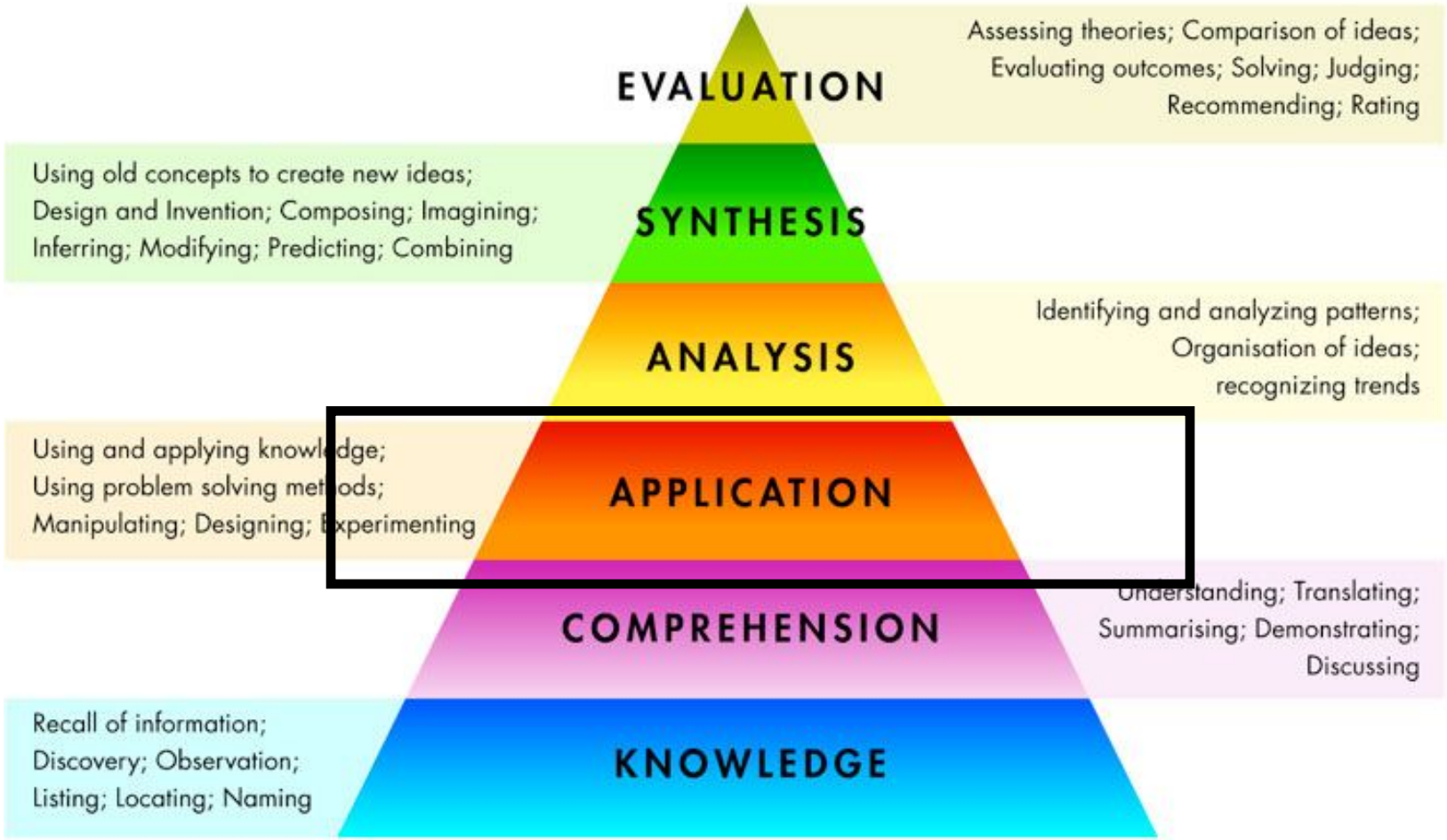
Every Pen Tester Should Know	
Networks	SEC**560** Network Penetration Testing and Ethical Hacking | **GPEN**
Web Apps	SEC**542** Web App Penetration Testing and Ethical Hacking | **GWAPT**

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but is essential for defense specialists to improve their defenses.

Bloom's Taxonomy



Bloom's Taxonomy



Results

Results

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	38	-	53	-	44	-	135	-
Assessed Concepts	38	100%	44	83%	34	77%	116	86%
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	35	92%	37	84%	31	91%	103	89%
Defensive Total	33	87%	43	98%	34	100%	110	95%
Primarily Offensive	16	42%	6	14%	10	29%	32	28%
Primarily Defensive	6	16%	2	5%	5	15%	13	11%

Results

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	**38**	**-**	**53**	**-**	**44**	**-**	**135**	**-**
Assessed Concepts	38	100%	44	83%	34	77%	116	86%
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	35	92%	37	84%	31	91%	103	89%
Defensive Total	33	87%	43	98%	34	100%	110	95%
Primarily Offensive	16	42%	6	14%	10	29%	32	28%
Primarily Defensive	6	16%	2	5%	5	15%	13	11%

Results

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	38	-	53	-	44	-	135	-
Assessed Concepts	**38**	**100%**	**44**	**83%**	**34**	**77%**	**116**	**86%**
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	35	92%	37	84%	31	91%	103	89%
Defensive Total	33	87%	43	98%	34	100%	110	95%
Primarily Offensive	16	42%	6	14%	10	29%	32	28%
Primarily Defensive	6	16%	2	5%	5	15%	13	11%

Results

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	38	-	53	-	44	-	135	-
Assessed Concepts	38	100%	44	83%	34	77%	116	86%
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	**35**	**92%**	**37**	**84%**	**31**	**91%**	**103**	**89%**
Defensive Total	**33**	**87%**	**43**	**98%**	**34**	**100%**	**110**	**95%**
Primarily Offensive	16	42%	6	14%	10	29%	32	28%
Primarily Defensive	6	16%	2	5%	5	15%	13	11%

Results

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	38	-	53	-	44	-	135	-
Assessed Concepts	38	100%	44	83%	34	77%	116	86%
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	35	92%	37	84%	31	91%	103	89%
~~Defensive Total~~	~~33~~	~~87%~~	~~43~~	~~98%~~	~~34~~	~~100%~~	~~110~~	~~95%~~
Primarily Offensive	**16**	**42%**	**6**	**14%**	**10**	**29%**	**32**	**28%**
Primarily Defensive	**6**	**16%**	**2**	**5%**	**5**	**15%**	**13**	**11%**

Results

- Both offensive (89%) and defensive (95%) cover the majority of the concepts and are relatively comparable
  - Defensive techniques cover 6% more of the concepts than offensive
  - Offensive techniques cover 17% of the concepts in greater details than defensive
- **Either technique can be used to teach the majority of the concepts, and both are needed to teach all**

Results

- Both offensive (89%) and defensive (95%) cover the majority of the concepts and are relatively comparable
  - Defensive techniques cover 6% more of the concepts than offensive
  - Offensive techniques cover 17% of the concepts in greater details than defensive

- **Either technique can be used to teach the majority of the concepts, and both are needed to teach all**

Does the technique actually impact the resulting mindset?

Important Psychological Outcomes

- Lifelong Learning
  - The independent pursuit of learning without formal institutional support or affiliation
  - In ACM, IEEE, AITP, and numerous other codes
  - Growth mindset (Carol Dweck)
- Intrinsic Motivation
  - Passion
  - Community
- Resilience
  - Built by facing, failing, then overcoming moderate challenges

Important Psychological Outcomes

- Lifelong Learning
  - The independent pursuit of learning without formal institutional support or affiliation
  - In ACM, IEEE, AITP, and numerous other codes
  - **Growth mindset (Carol Dweck)**
- Intrinsic Motivation
  - Passion
  - Community
- Resilience
  - Built by facing, failing, then overcoming moderate challenges

Important Psychological Outcomes

- Lifelong Learning
  - The independent pursuit of learning without formal institutional support or affiliation
  - In ACM, IEEE, AITP, and numerous other codes
  - Growth mindset (Carol Dweck)
- Intrinsic Motivation
  - Passion
  - Community
- Resilience
  - **Built by facing, failing, then overcoming moderate challenges**

Positive Impact of the Offense

- Security Mindset
  - "Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail" – Bruce Schneier
  - Harmless Failures - Ed Felten
- Expectation to fail often and repeatedly
- Repeatedly have "small victories"
- Interesting and enjoyable

Negative Impact of the Defense

- Assets (checklists) vs. graphs (relationships) mentality
- Limited ability to face and overcome challenges
  - Inherently always lose
  - "Defense-only exercises can be very demotivational, as students feel like they've been bullied by the red team and that they aren't capable" – Dr. Carlisle
- Not as impactful for building intrinsic motivation
  - Not as exciting or engaging
  - Not active (involves waiting and can be boring at times)

Psychological Conclusions

- Developing intrinsic motivation is more difficult with purely defensive techniques
- Defensive techniques can be de-motivational
- Offensive techniques are best for building resiliency and intrinsic motivation, required attributes of lifelong learners

Psychological Conclusions

- Developing intrinsic motivation is more difficult with purely defensive techniques
- Defensive techniques can be de-motivational
- **Offensive techniques are best for building resiliency and intrinsic motivation, required attributes of lifelong learners**

So What?

- Offensive and defensive techniques both teach cybersecurity's core competencies
- Cybersecurity requires resilient lifelong learners, and offensive techniques best develop these attributes
- Combining academia's concept focus (the why) with industry's relevant training (the what) through gamification (the how) provides the best hybrid education experience

Questions

How do I build effective offensive training?

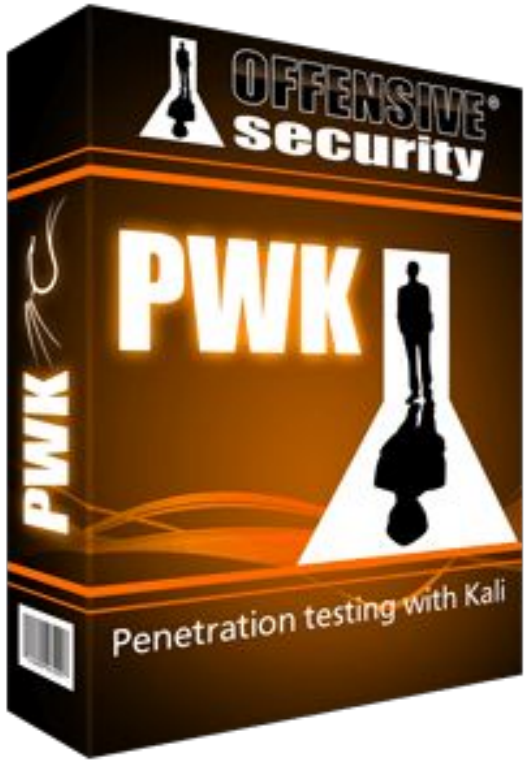
Offensive Curriculum is Hard

- Large Infrastructure Requirement
  - Maintaining intentionally breakable systems
- Fast Evolution of Material
  - New tools / techniques
  - New exploits (Eternal Blue)
- Breadth of Subject Matter
  - Diverse pre-requisites
  - Troubleshooting is hard
- Legal / Network Issues

Offensive Curriculum is Hard

- Large Infrastructure Requirement
  - Maintaining intentionally breakable systems
- Fast Evolution of Material
  - New tools / techniques
  - New exploits (Eternal Blue)
- Breadth of Subject Matter
  - Diverse prerequisites
  - Troubleshooting is hard
- **Legal / Network Issues**

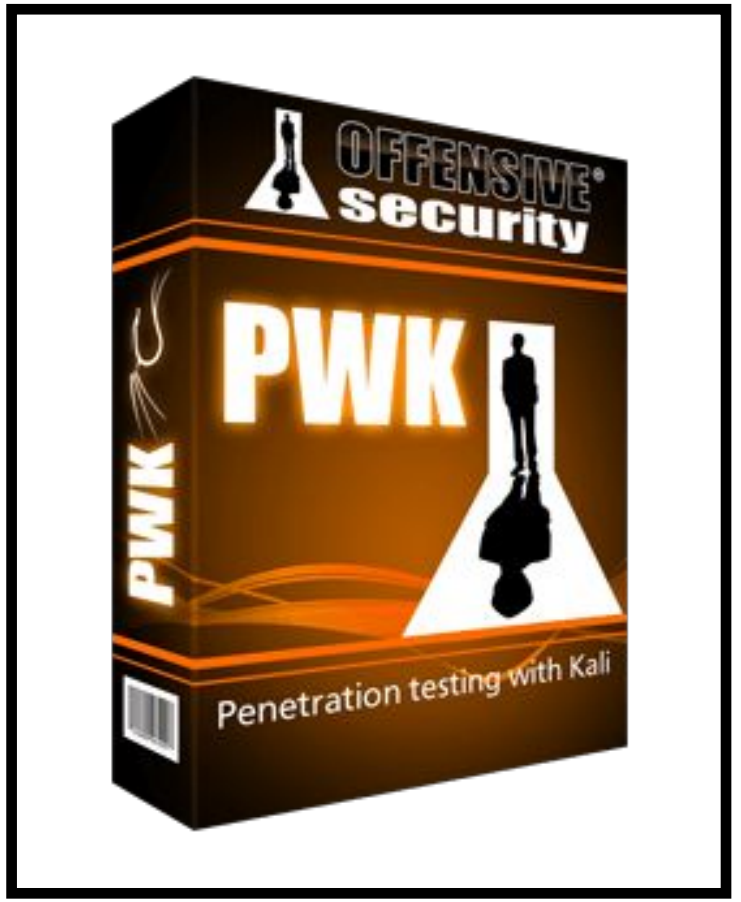
Leverage Industry



Leverage Industry

SANS

C|EH
CERTIFIED ETHICAL HACKER



CISSE

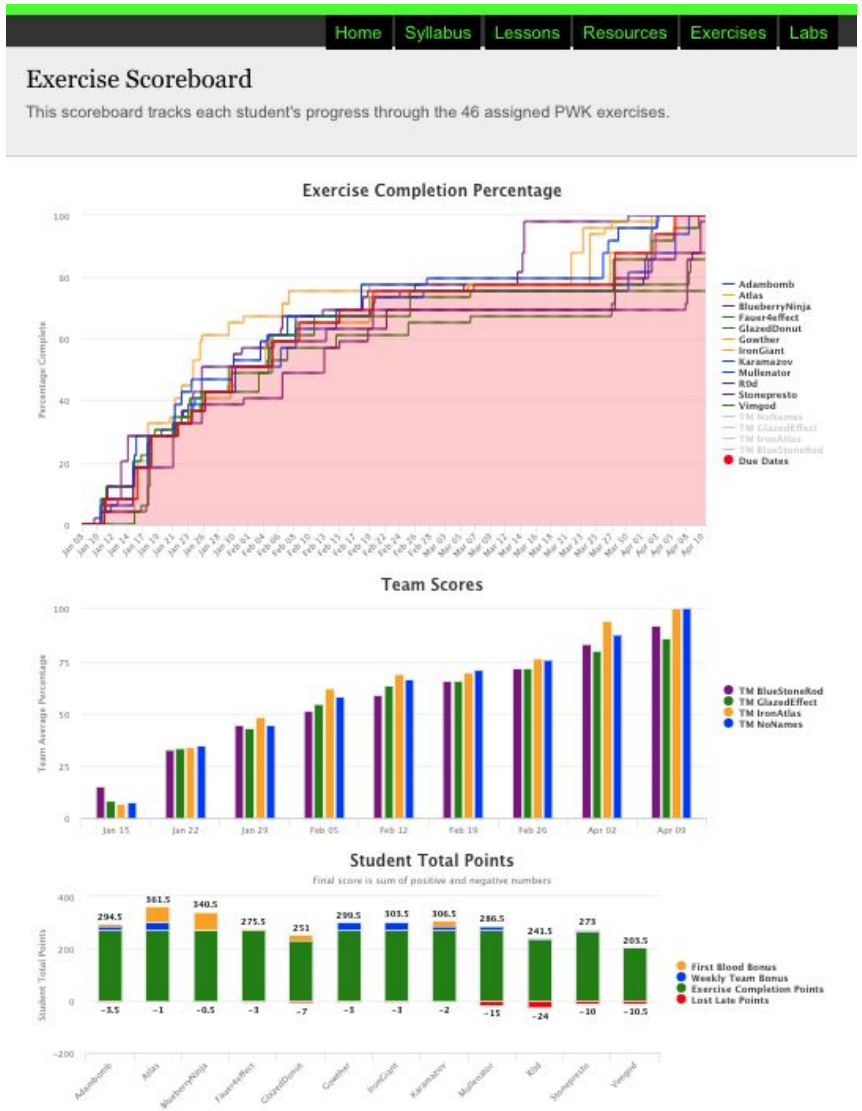
Penetration Testing With Kali

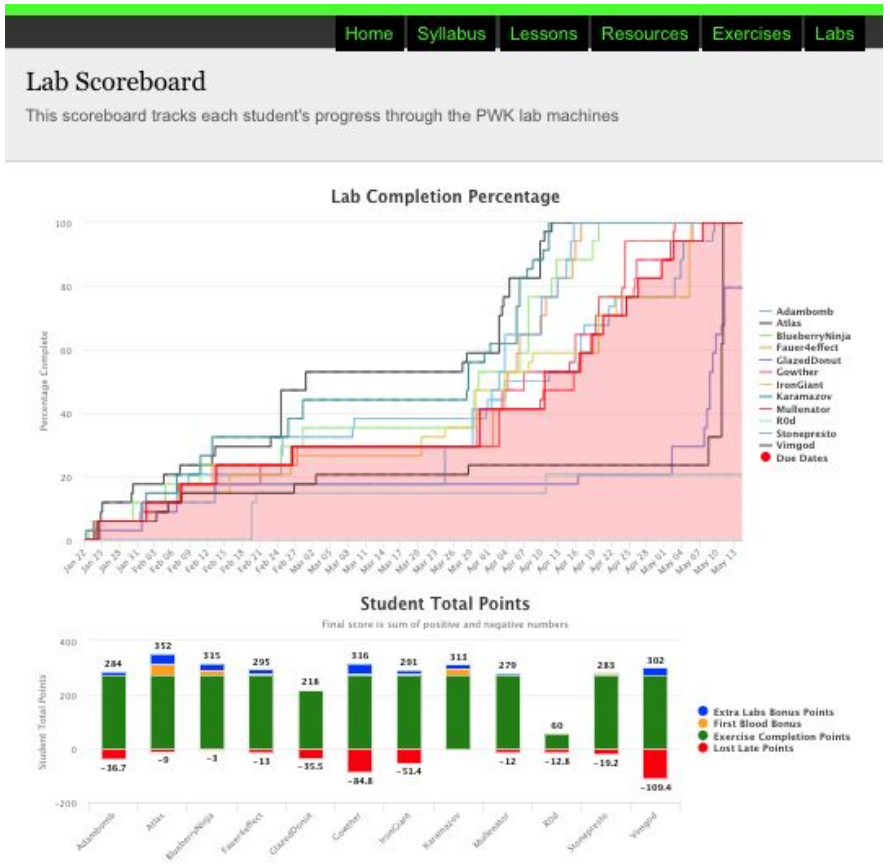
- Course by Offensive Security (Kali Linux)
- Introduces students to ethical hacking tools and techniques
  - Initial Exercises
    - 7 hours of provided videos
    - 350+ page pdf lab guide
    - Local Kali VM / Private Windows 7 Lab Machine
    - Accessed via private VPN
  - Interactive Lab
    - 40 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



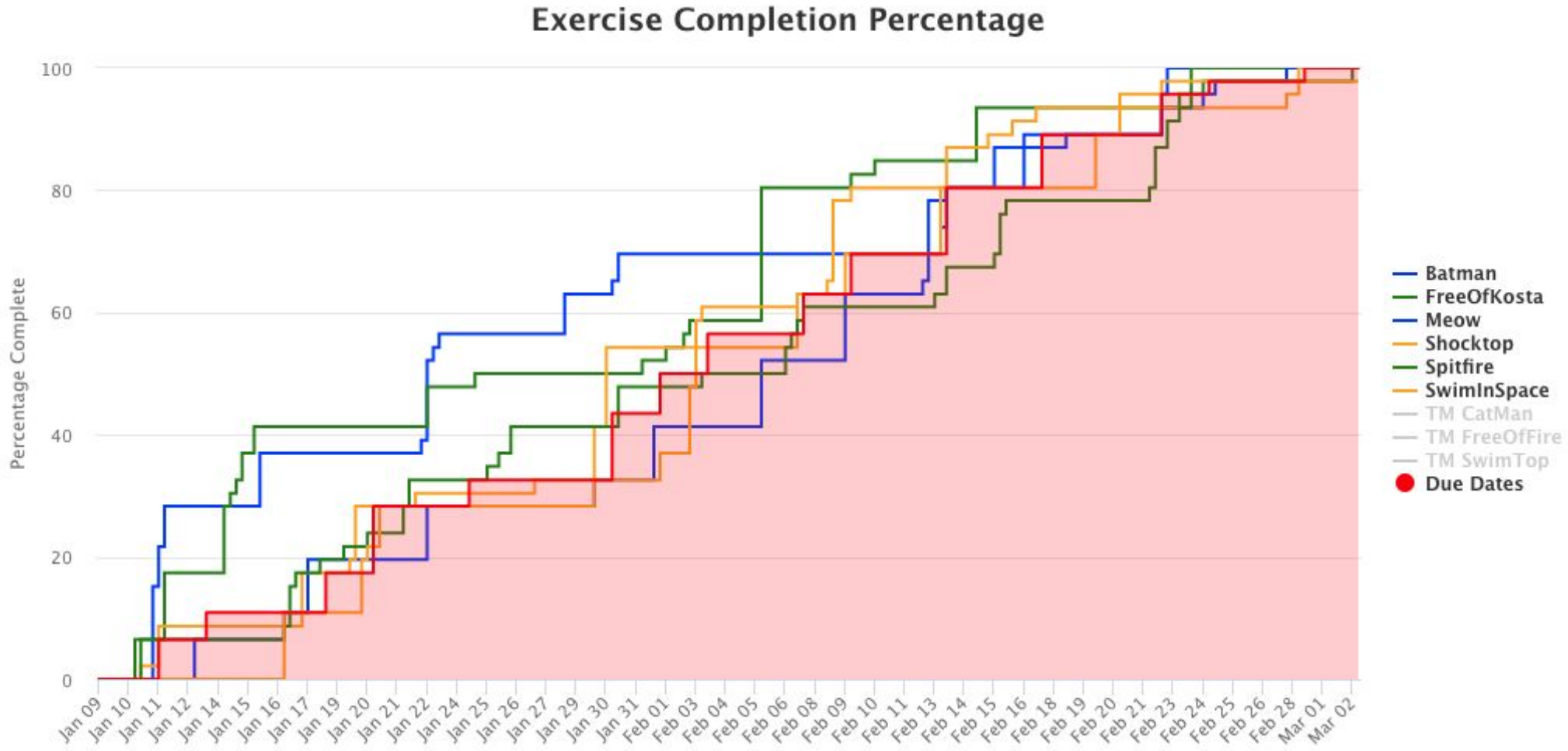


First Bloods!

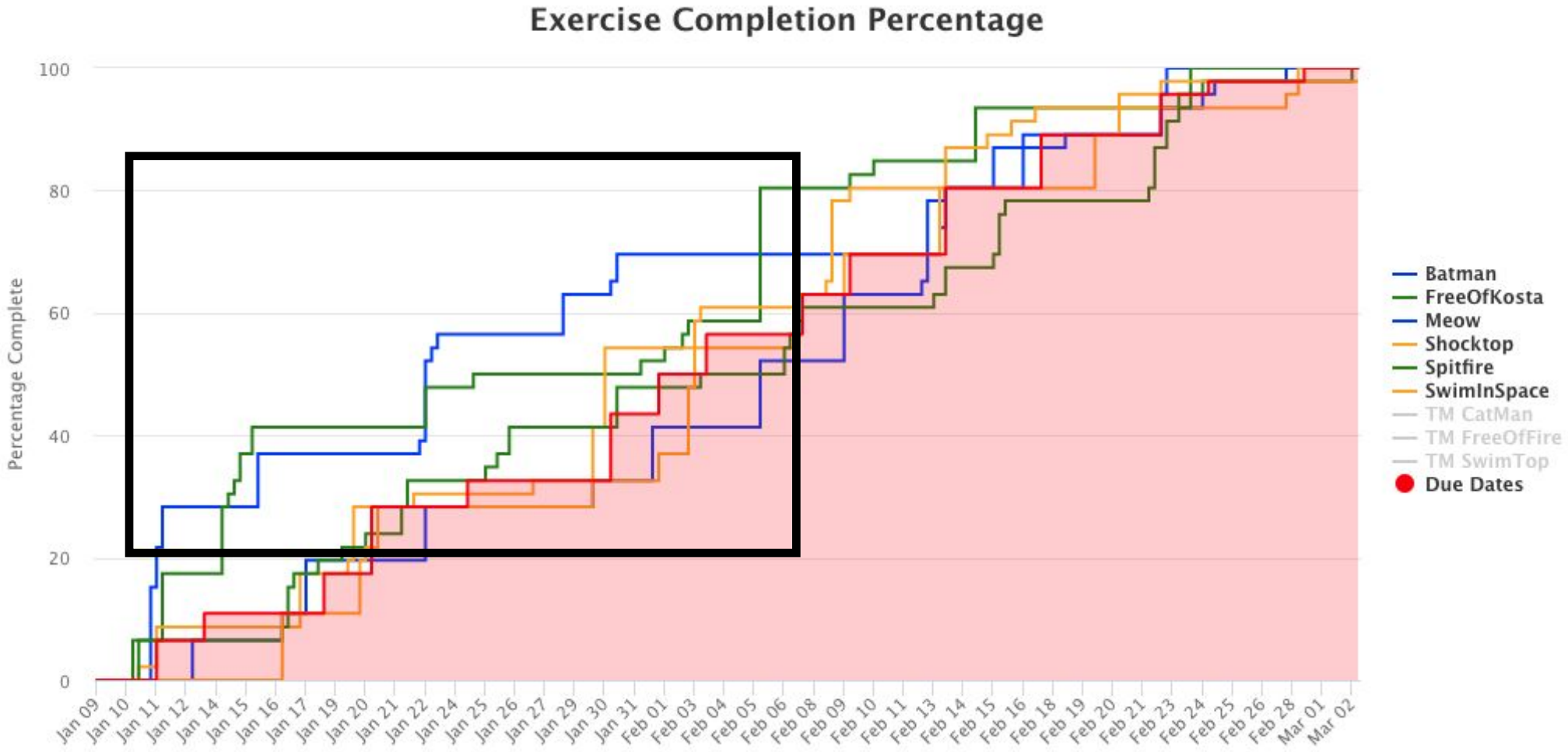
Last Octet	Hostname	Network	First Blood!	Time of First Blood	Time of Last Completion	Students Completed
005	alice	Public	Atlas, Karamazov	02-07 at 09:45	---	Adambomb, Atlas, BlueberryNinja, Fauer4effect, GlazedDonut, Gowther, IronGiant, Karamazov, Mullenator, Stonepresto, Vimgod

www.mjkranch.com

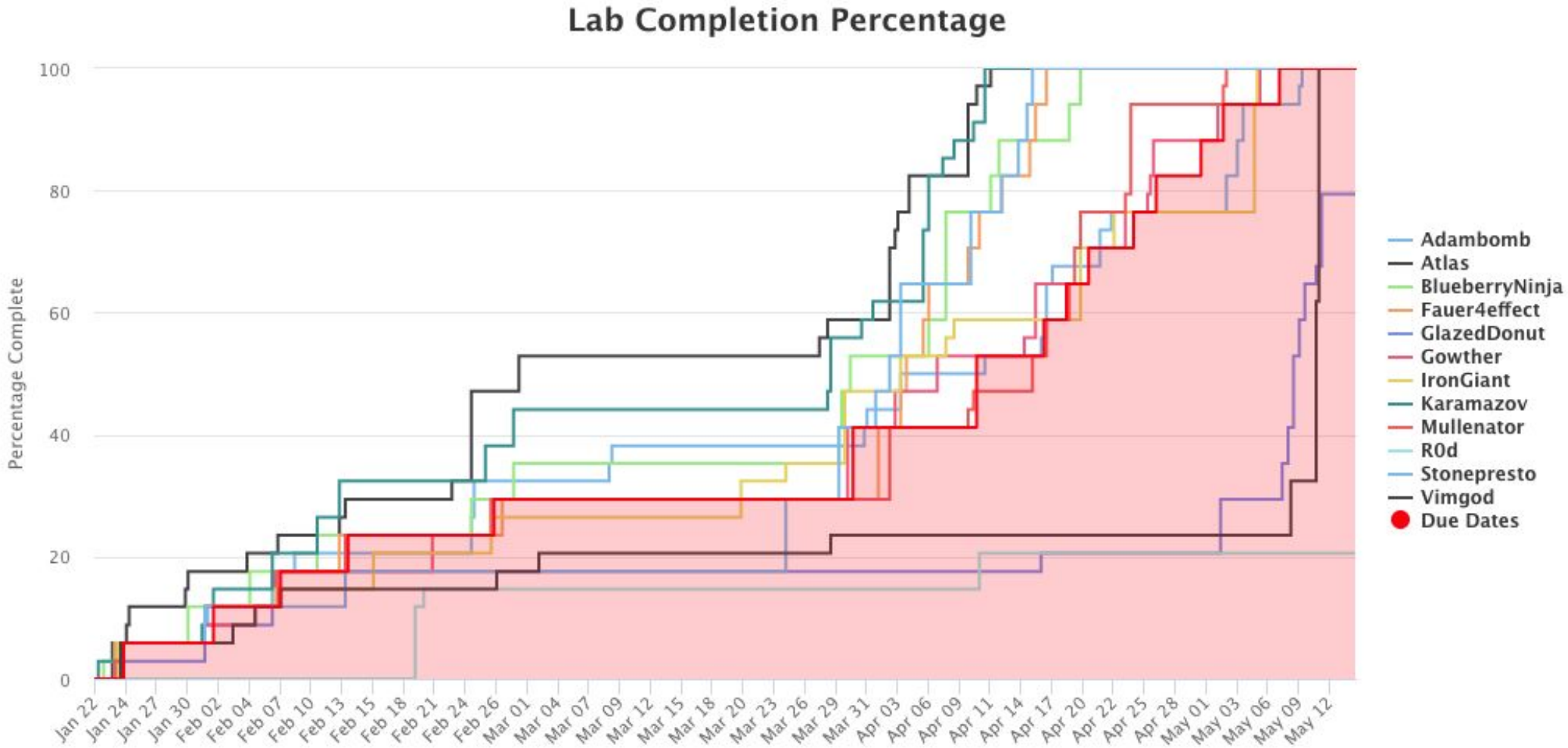
Gamification Examples



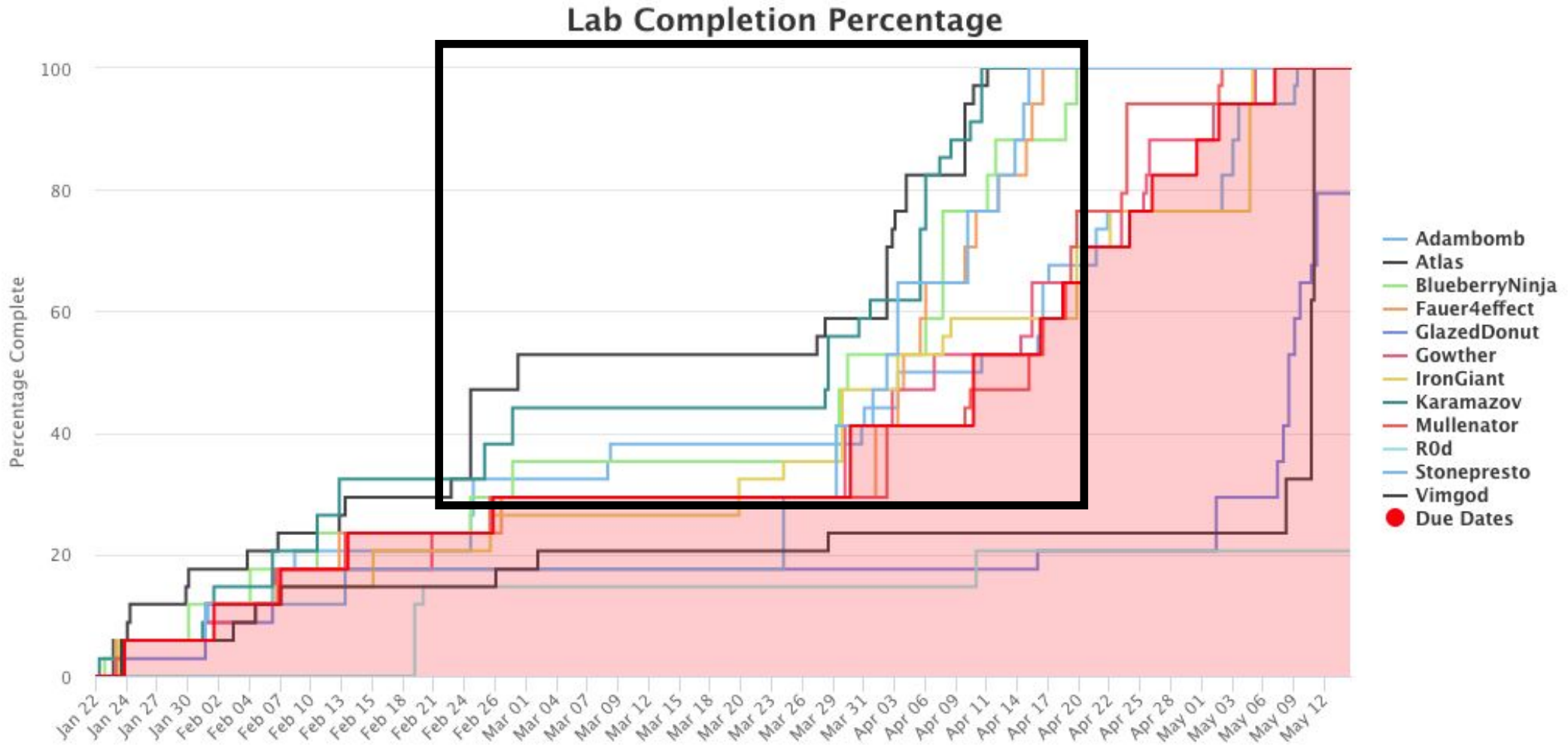
Gamification Examples



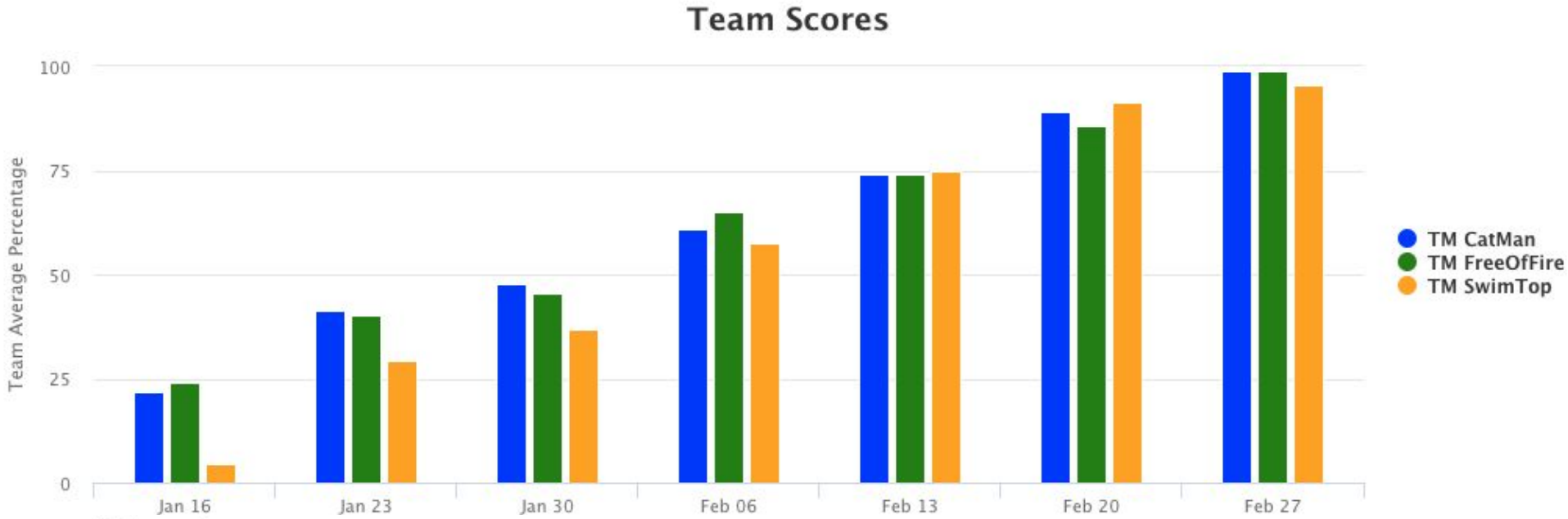
Gamification Examples



Gamification Examples



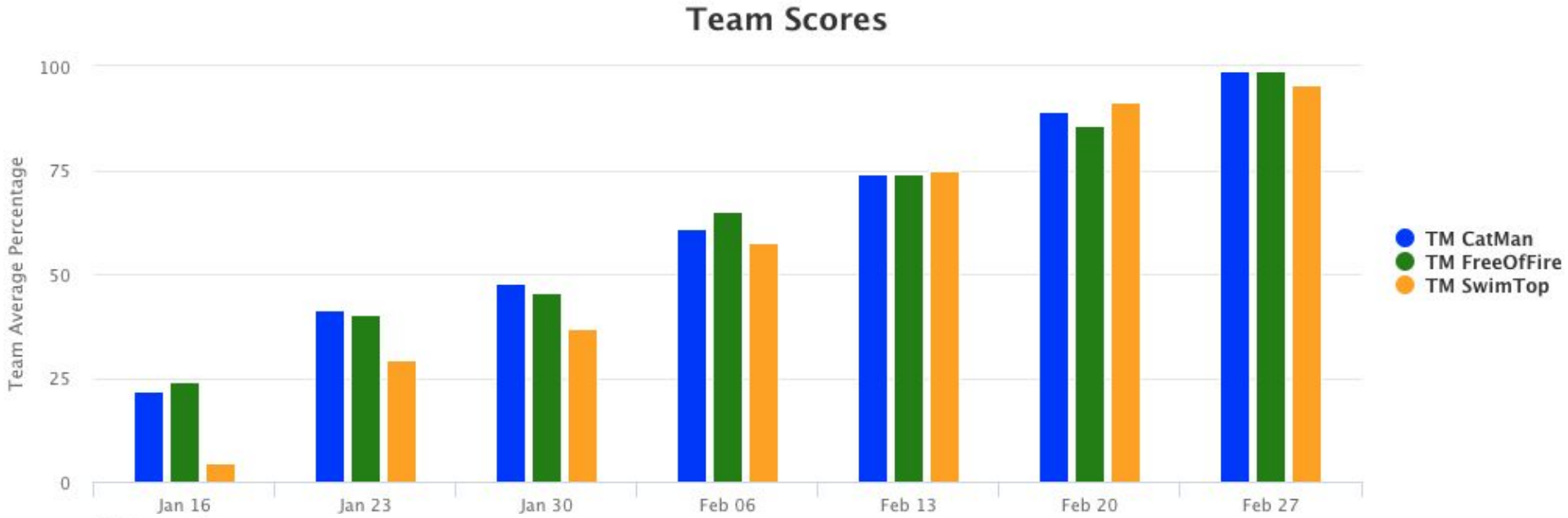
Gamification Examples



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

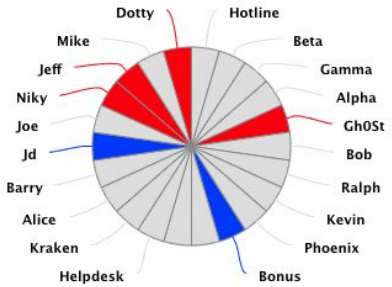


Weekly Winners

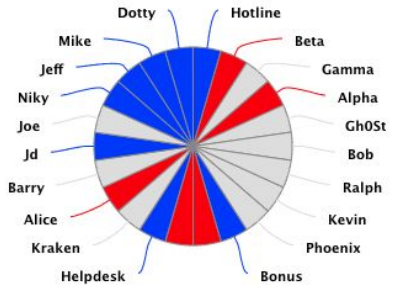
Week #	Date	Winning Team
1	Monday, January 16 at 00:00	TM FreeOfFire
2	Monday, January 23 at 00:00	TM CatMan
3	Monday, January 30 at 00:00	TM CatMan
4	Monday, February 06 at 00:00	TM FreeOfFire
5	Monday, February 13 at 00:00	TM SwimTop
6	Monday, February 20 at 00:00	TM SwimTop
7	Monday, February 27 at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

Live Performance Based Exam

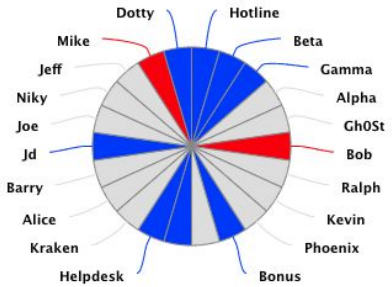
Solves for Batman



Solves for FreeOfKosta



Solves for Meow



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 as much "how"
  - Only possible with smaller class size
- Students **internalized the security mindset**
  - 8/18 earned OSCP

Can I Do This Myself?

- PWK is best but costly ($1000 per student)
- Cheaper (~$250 per student)
  - VirtualHackingLabs.com
    - Comes recommended but I have not personally tested
- Cheapest (~$40 per student)
  - Textbook
    - Penetration Testing: A Hands-On Introduction to Hacking
    - Rtfm – Red Team Field Manual
  - Lab
    - HacktheBox.eu (free for last 5, 1 new machine each week, $30 a month)
    - Vulnhub.com (free but need to host yourself and writeups exist)

So What?

- Offensive and defensive techniques both teach cybersecurity's core competencies
- Cybersecurity requires resilient lifelong learners, and offensive techniques best develop these attributes
- Combining academia's concept focus (the why) with industry's relevant training (the what) through gamification (the how) provides the best hybrid education experience

Thank you!

Questions?

www.mjkranch.com

CISSE

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.

Example CCA Topics

Topic	Importance	Difficulty
Privacy	10	7
Ethics	10	5
Authentication	10	4
Integrity	10	4
Confidentiality	10	3
Secure coding	9	8
Assess vulnerabilities	9	7
Analyze threats	9	7
Manage risks	9	7
Operating system security	9	7

Offensive or Defensive?

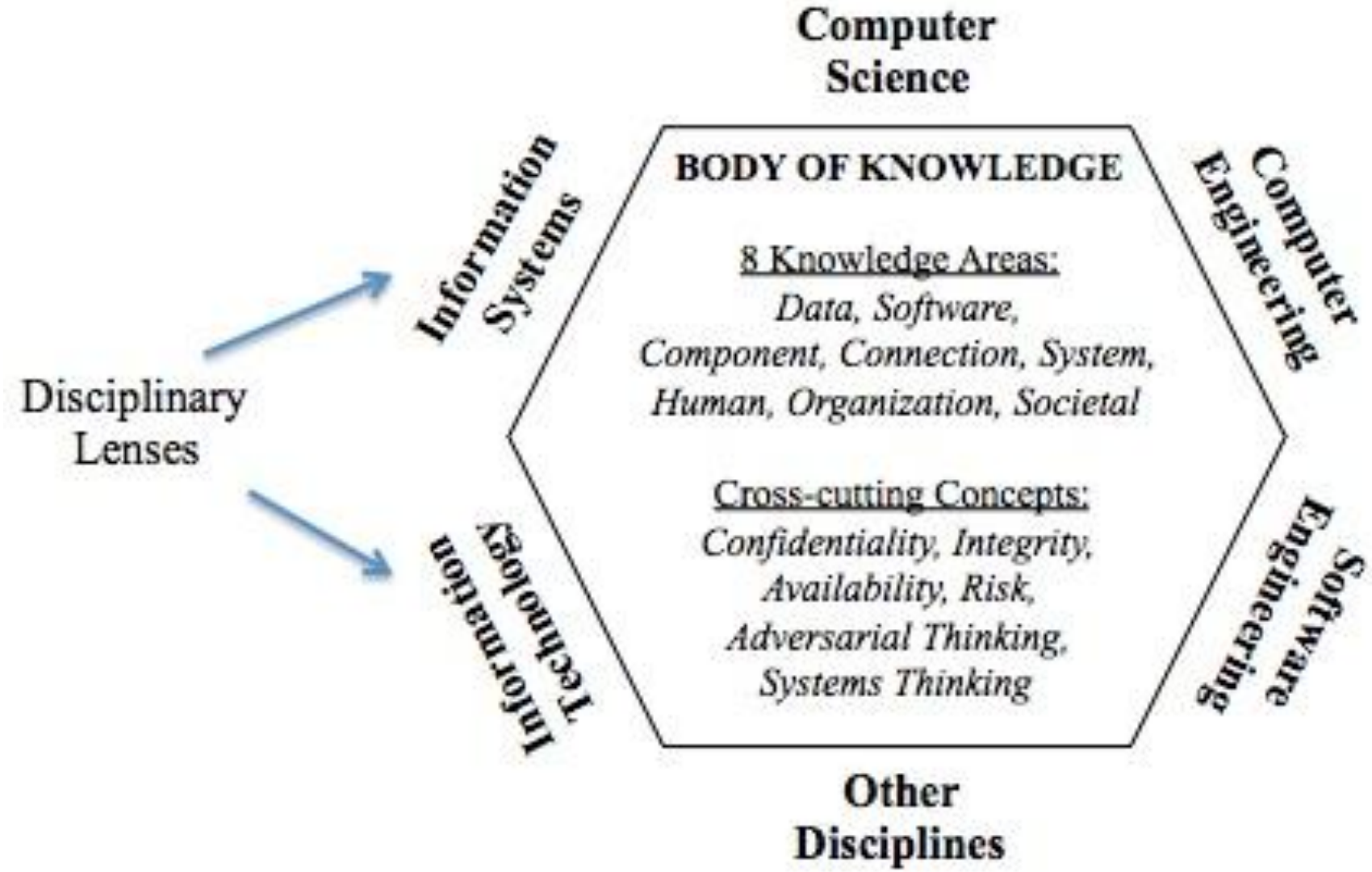
- Network models + protocols
  - http, smb, ftp, ssh, dns.
- Command line proficiency
  - grep, find, chmod, net sh.
- Vulnerability scanning
  - nmap, nessus, google hacking, whois, dig
- Network captures and parsing
  - tcpdump, wireshark, pcaps.
- Programming / Scripting
  - bash, python, PowerShell
- Cryptographic foundations
  - encryption, hashes.
- Binary Analysis / Reversing
  - C, assembly, the stack, insecure functions, gdb, immunity
- Forensics
  - logs, recovering deleted files, important system data

Offensive or Defensive?

- Network models + protocols
- Network captures and parsing
- Command line proficiency
- Vulnerability scanning

- Programming / Scripting
- Cryptographic foundations
- Binary Analysis / Reversing
- Forensics

Cybersecurity Curricula 2017



Who Am I?

- I am an academic
- 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

Penetration & Vulnerability Tester

AVERAGE SALARY

$102,000

COMMON JOB TITLES

- Penetration Tester
- Application Security Architect
- Application Security Analyst
- Senior Penetration Tester
- Security Analyst III

REQUESTED EDUCATION (%)

TOP SKILLS REQUESTED

1. Information Security
2. Penetration Testing
3. Linux
4. Vulnerability assessment
5. Python
6. Information Systems
7. Java
8. Open Web Application Security Project (OWASP)
9. Project Management

TOTAL JOB OPENINGS

9,826

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Analyze
- Protect and Defend

TOP CERTIFICATIONS REQUESTED

- GIAC
- CISA
- CISM
- GIAC Web Application Penetration Tester (GWAPT)
- Security+

Red Team Jobs account for only ~15% of the cybersecurity job openings