CTFs for Fun and Profit:

Playing Games to Build Your Skills

David Tomaschik (@matir)

Obligatory Disclaimer

The views & positions in this presentation are the author’s and do not necessarily reflect those of my employers -- past, present, or future.

Obligatory Bio

- 10+ Years of CTF Experience
  - Played countless CTFs & Wargames
  - Staff, BSidesSF CTF
  - Staff, Pros vs Joes CTF (BSidesLV)
- Senior Security Engineer, Google
  - Tech Lead, Red Team
- Security Blogger (https://systemoverlord.com)
- Twitter (@Matir)

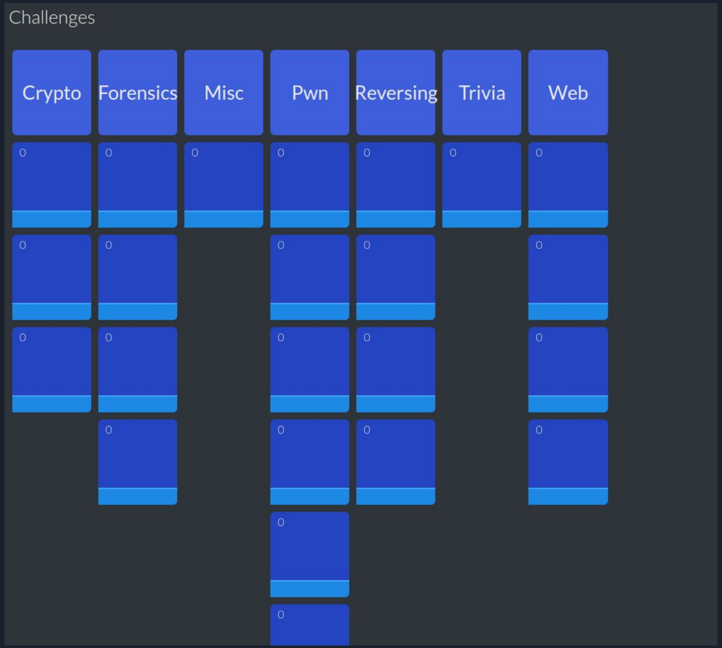
Obligatory Outline

- (Very) Quick CTF Primer
  - Styles of CTFs
  - Playing CTFs
- Skills Used/Learned in CTFs
  - Overlap with security practitioners
  - Improving overlap for players
  - Improving overlap for organizers

CTF Primer

CTF Styles (Typical Categories)

- Jeopardy
  - Panel of problems to be solved
  - Generally in any order
- Attack/Defense
  - Run network services
  - Find & exploit, patch your own
- Misc
  - Defense Only (CCDC)
  - Story-Style



Challenges

Crypto	Forensics	Misc	Pwn	Reversing	Trivia	Web
0	0	0	0	0	0	0
0	0		0	0		0
0	0		0	0		0
	0		0	0		0
			0			
			0			

CTF Styles (Spectrum)

Realistic

Contrived

- Real Services
- Business-Like Environment
- CVEs seen in the Wild

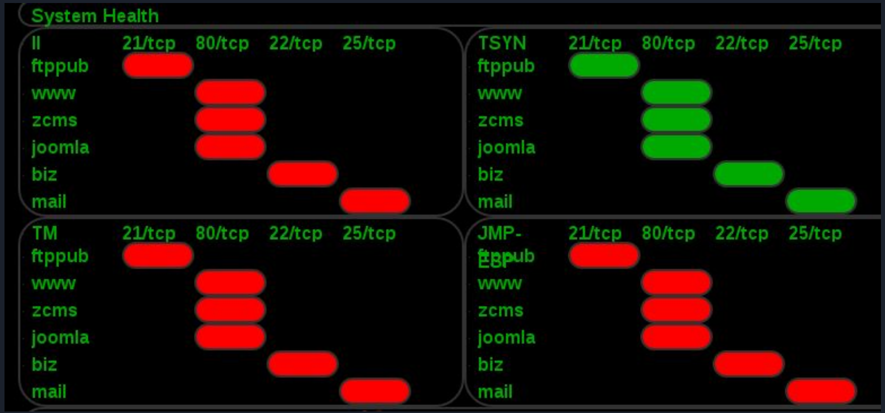
- Fictional Architectures
- Services with no purpose

DEF CON CTF

- Top Tier CTF
- Attack/Defense
- Contrived Challenges to test CTF Skills
  - Middle Endian Architecture Anyone?

Pros vs Joes CTF

- Defense-Focused
- 4 Blue (Purple) Teams, 1 Red Team
- Here at BSidesLV
- Real World Software, Environment



System Health

II	21/tcp	80/tcp	22/tcp	25/tcp
ftppub	🟥			
www		🟥		
zcms		🟥		
joomla		🟥		
biz			🟥	
mail				🟥

TSYN	21/tcp	80/tcp	22/tcp	25/tcp
ftppub	🟩			
www		🟩		
zcms		🟩		
joomla		🟩		
biz			🟩	
mail				🟩

TM	21/tcp	80/tcp	22/tcp	25/tcp
ftppub	🟥			
www		🟥		
zcms		🟥		
joomla		🟥		
biz			🟥	
mail				🟥

JMP- ESP	21/tcp	80/tcp	22/tcp	25/tcp
ftppub	🟥			
www		🟥		
zcms		🟥		
joomla		🟥		
biz			🟥	
mail				🟥

Wargames

- Sets of Challenges to be Solved
- Not time-bound
- Good opportunity to expand skills with little commitment

Educational Value of CTFs

Can You Learn From CTFs?

Can You Learn From CTFs?

Short Answer:

Yes

But What?

- Some Technical Skills
  - Reverse Engineering
  - Exploitation
  - Forensics
  - Scripting
- Thinking Outside the Box

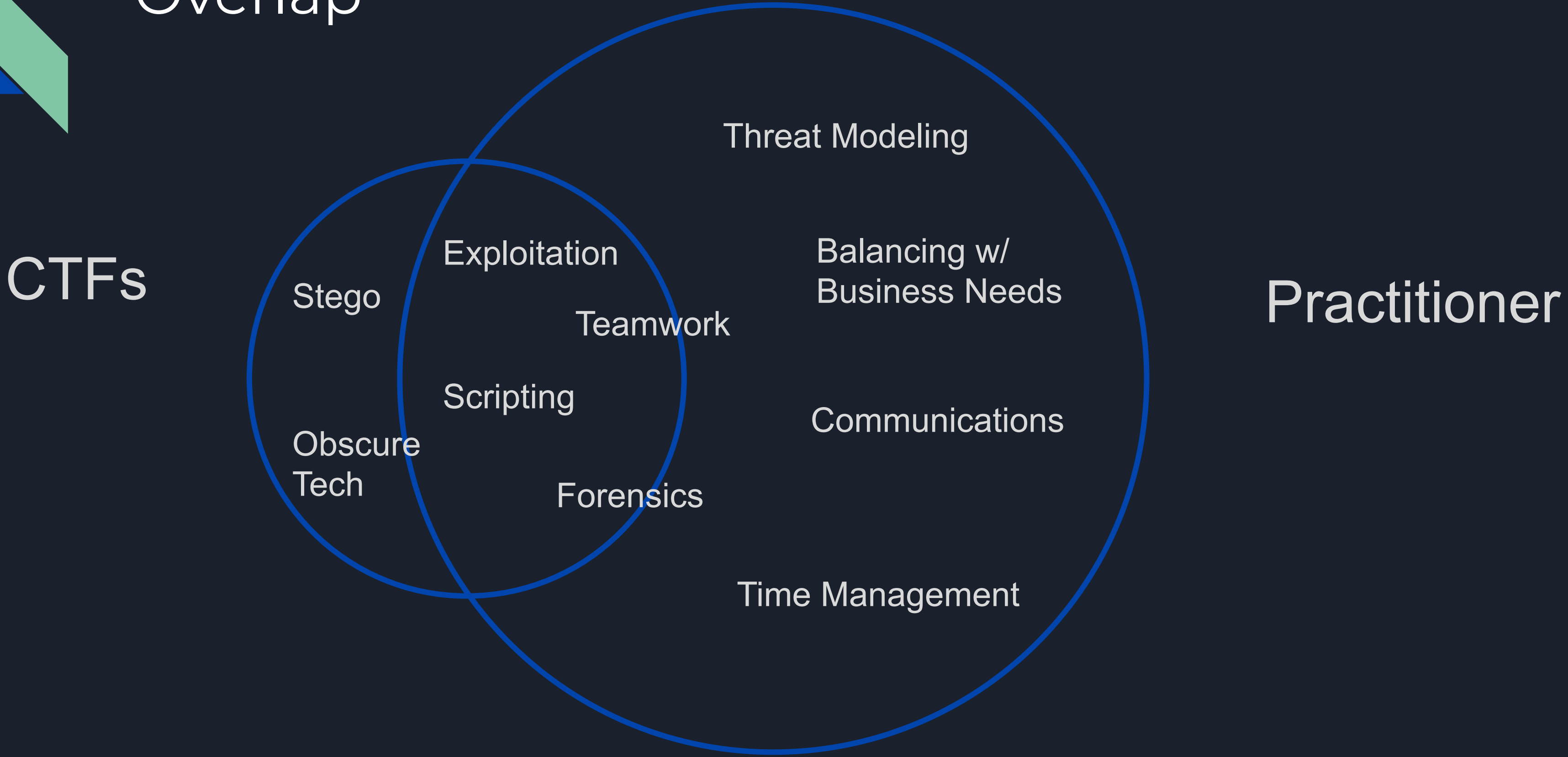
Practitioner Skills

- Technical
  - Reverse Engineering
  - Exploitation
  - Forensics
  - Threat Modeling
  - Triaging
  - Programming

Practitioner Skills (Cont’d)

- Attacker Mindset
  - Goals/Objectives
  - Multiple Approaches
- Communication
  - Report writing
  - Communicating to non-technical individuals
- Teamwork
  - Collaboration
  - Splitting Effort
  - Mentorship

Overlap



CTFs

Stego

Obscure Tech

Exploitation

Teamwork

Scripting

Forensics

Threat Modeling

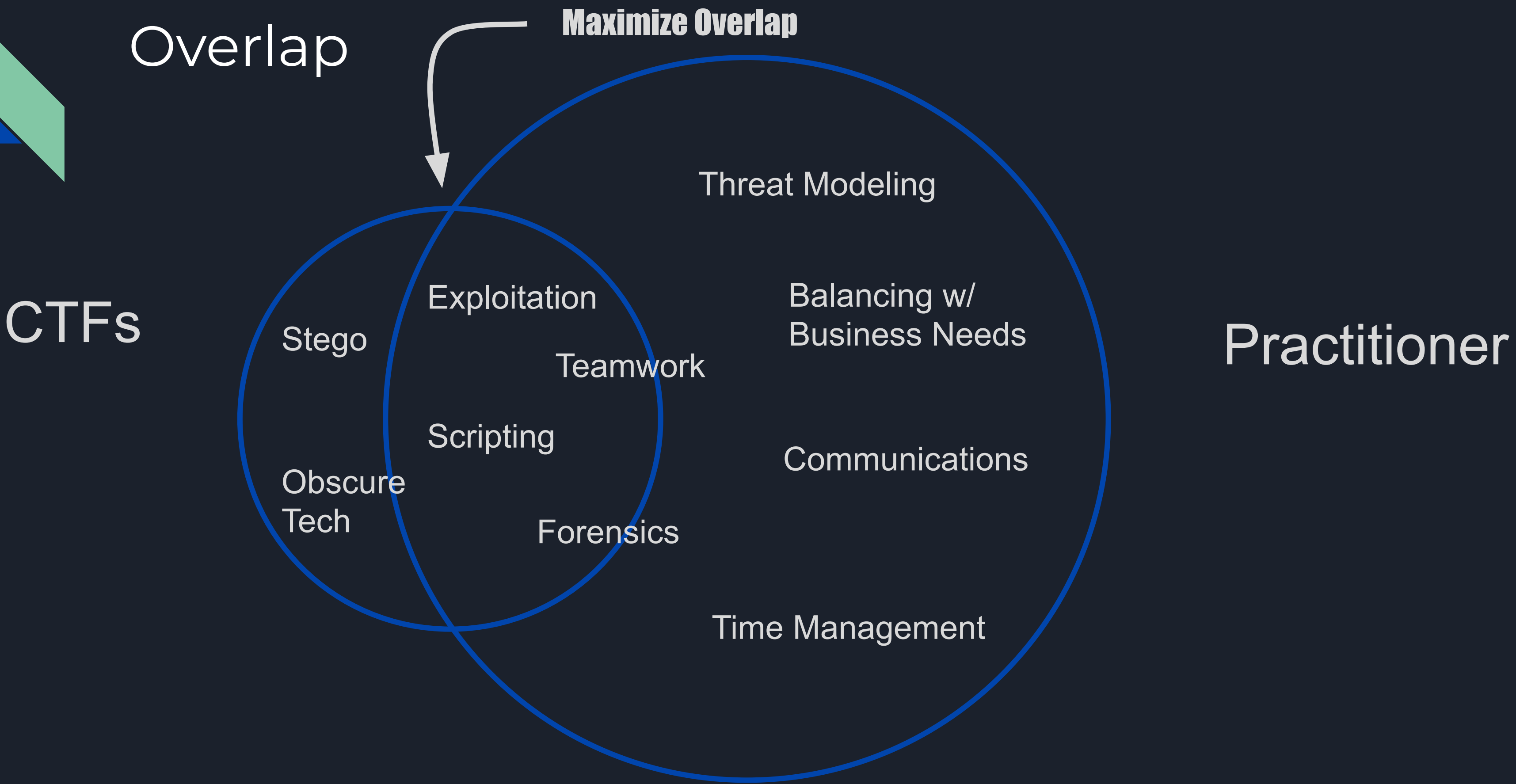
Balancing w/ Business Needs

Communications

Time Management

Practitioner

Overlap


Maximize Overlap
CTFs
Stego
Obscure Tech
Exploitation
Teamwork
Scripting
Forensics
Threat Modeling
Balancing w/ Business Needs
Communications
Time Management
Practitioner

Expanding the Intersection: Communications

- Consider doing “Write-Ups”
    - What the problem was
    - What approach you took
    - Dead-ends
    - What your ultimate solution was
    - How the vulnerability would translate into real-world impact

Expanding the Intersection: Teamwork & Leadership

- Play as part of a team
  - Work challenges together
  - Offer to be a sounding board
  - Experience with other personalities/backgrounds
- Mentor Others
  - Introduce them to CTF
  - Walk through challenges

Other Ways to Get More Out of It

- Step Outside Comfort Zone
  - May reduce scoring, but will have benefits later
  - Don’t give up because it’s hard -- hard is how you learn
- Revisit Challenges
  - After the CTF, you can revisit challenges and read write-ups to understand areas you may not have grasped the first time
  - CTFTime has links to writeups
  - YouTube Channels like LiveOverflow, Gynvael Coldwind

For CTF Designers

Running a CTF With Education in Mind

- Public CTF (Conference, Hackerspace, etc.)
  - Diverse backgrounds/skill levels
  - Various interests
  - Various learning objectives
- Private CTF (In house, Class, etc.)
  - More similar background
  - Usually focused on one area

Gamification

- Multiple studies have shown gamification of education to improve learning performance and skill progression
- Studies have also shown that gamification reduces the perceived effort of students

Source: Hamari, et. al

Case Study: Practitioner Skills in PvJ

- Pros v Joes has education as a core goal
  - Here at BSidesLV!
- Environment is “realistic”
  - Windows domain, servers
  - Linux Servers
  - Varying Versions
  - Real Services: Mail, DNS, etc.

Case Study: Practitioner Skills in PvJ

- Red Cell Pros as Sparring Partner for Blue Joes
- Also 2 Pros on each Blue Cell
  - Serve as mentors and leaders
  - Even as Pro, learn new things
- How often do you get to compare notes with your OpFor?

Building Educational Challenges

- Progressive Challenges
  - Series of challenges introducing new concepts or complexity
  - Build up skills rather than requiring a giant leap
- Challenges with Real World Applicability
  - Based on real CVEs, Forensics Situations, etc.

Challenge Examples

- Based on real vulnerabilities/forensic cases
  - Android app with SQL Injection via Intents
- Realistic Environments
  - Forensics of Real Systems
  - Fully functional apps

Progressive Challenges

- Build several challenges in a series
  - Introduce Concept
  - Add Complexity
  - Force Edge Case/Challenge Growth
- Benefits
  - Challenges for range of players
  - Boost player confidence
  - Build up skills

Progressive Challenge Examples

Encrypted Filesystem Challenge

1. Obvious filesystem with known partial password
2. Filesystem without known password
3. Encrypted filesystem with deleted files needing recovery

SQL Injection Challenge

1. Obvious SQLi (query in error message)
2. SQLi with limited feedback
3. Blind SQLi
4. Blind SQLi with encoding/non-obvious input

Student/Player Motivation

- Competitiveness/scoring
- Progression/storyline
- Skill Building -- particular skills

Questions?

Resources

- This deck: https://1337.fyi/
- CTFTime: https://ctftime.org/
-

References

- Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification. *2014 47th Hawaii International Conference on System Sciences*. doi:10.1109/hicss.2014.377