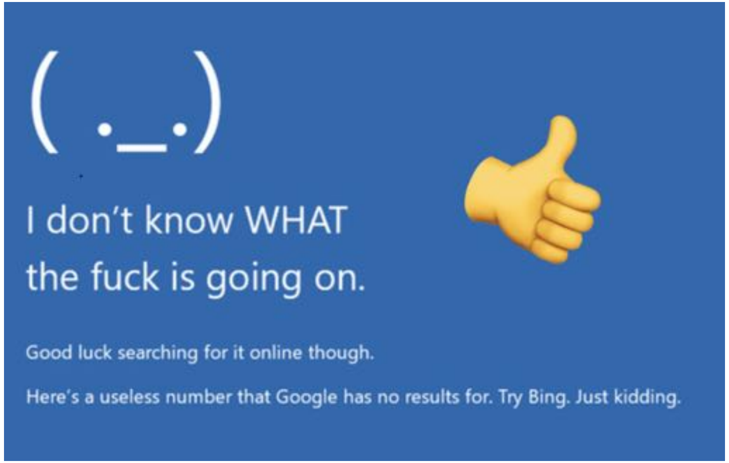
Competing for the Future – Building and Automation InfoSec Competitions

Thoughts and insight into organizing competitions

Who are we?



(._.)

I don’t know WHAT the fuck is going on.

Good luck searching for it online though.

Here’s a useless number that Google has no results for. Try Bing. Just kidding.

Who are we?

(spicey)wasabi

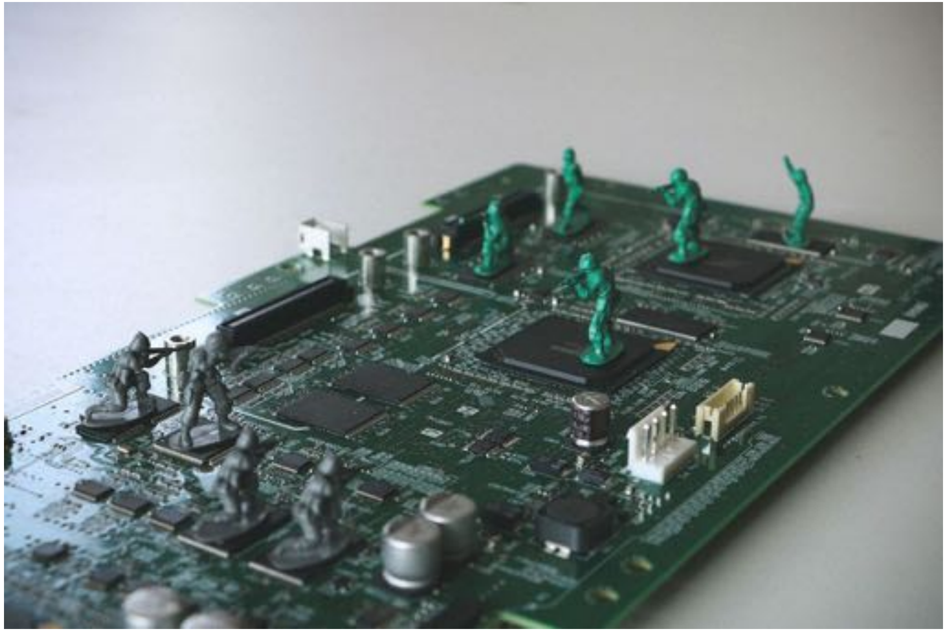
Security researcher who dabbles in the arts of system administration. He has participated CCDC, CPTC, and many CTFs before starting to help organize a cyber defense competition himself.

bluescreenofwin

Windows System Administrator and Windows hacker. He currently employed as a Security Analyst and when he is not at drowning in logs he can be found brewing copious amounts of delicious beer in his garage. Is on track to graduate with his B.S. in Computer Information Systems (eventually, some day).

What happened to WRCCDC

- Lead Changes
- Organizational changes
- Complete loss of infrastructure
- Most volunteers had no means of communicating with each other.



Time to take on CCDC!

- Volunteer experience is great!
- Drew on years of experience playing in competitions
- Tinkered and attended conferences

I mean..

How hard can it be to put on a competition?

“It is easy to just build challenges”

Danger Ahead

- Competitions are serious business for competitors
- Organizing Takes lots of time and volunteers disappear
- Everyone is happy to lead until they have to commit
- Resources cost money

To potential organizers

People are unreliable

People ARE unreliable

People are unreliable

People ARE unreliable

People are unreliable

Competition

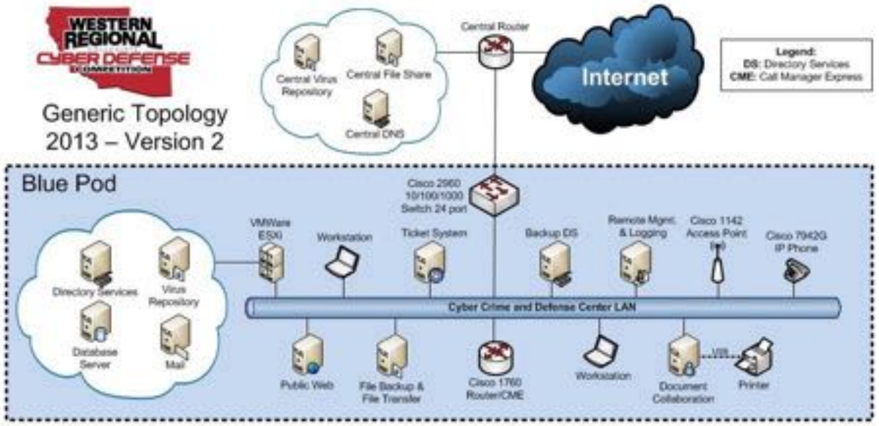
- Provide a safe means for competitors to learn new skills
- Test knowledge in a variety of environments
- Find jobs for the industry

About WRCCDC

- Academic competition in existence since 2008
- CCDC comprises of 6 regions - including Western region
- Teams prepare over the course of a year for a two day competition
- Goal is to simulate a (realistic) corporate environment

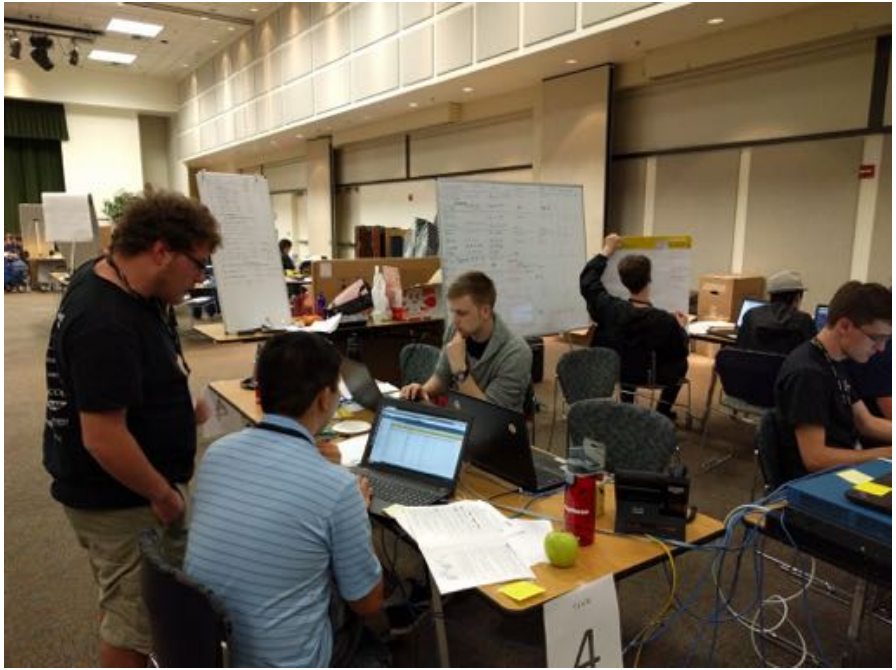
But why?

- CCDC is special to us (volunteers)
- Unique
- Challenges both competitors and organizers



Establishing Precedent

- Taking over people have expectations and excuses are not an option EVER
- “95%” Attrition Rate of Competitors and Volunteers
- What do competitors truly value?
- What is fun? It’s relative….

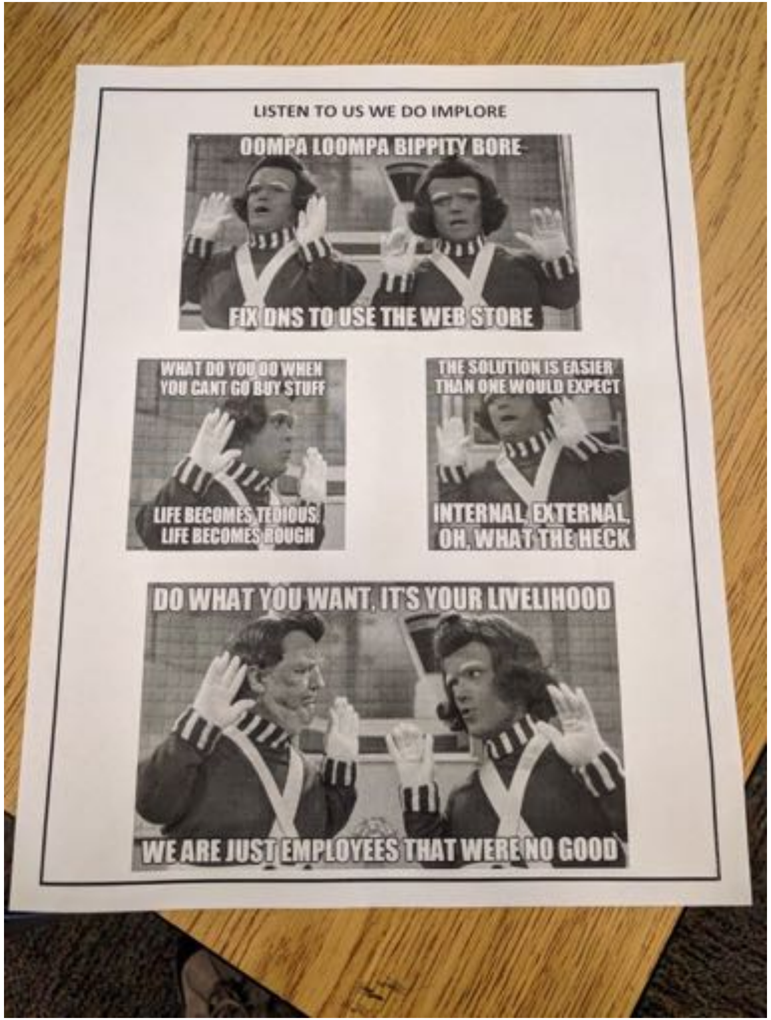


The Old Guard

- Point breakdowns not made clear to competitors
- Not much exposure to competition architecture prior to regionals (final competition for region)
- Rainbow team (team bleed over)
- Lack of hosted training

Keeping the Customers Happy

- Define the rules
- Explain in detail all parts of the competition
- Tell people what you expect
- Give people insight into what they will be doing
- And post hints 😉



LISTEN TO US WE DO IMPLORE

OOMPA LOOMPA BIPPITY BORE
FIX DNS TO USE THE WEB STORE

WHAT DO YOU DO WHEN
YOU CANT GO BUY STUFF
LIFE BECOMES TEDIOUS,
LIFE BECOMES ROUGH

THE SOLUTION IS EASIER
THAN ONE WOULD EXPECT
INTERNAL, EXTERNAL,
OH, WHAT THE HECK

DO WHAT YOU WANT, IT'S YOUR LIVELIHOOD
WE ARE JUST EMPLOYEES THAT WERE NO GOOD

Modern World, Modern Competition

- How do you make learning information security and defense fun and interesting for students (or anyone really)
- What makes sense today? (CCDC in the past has been very traditional infrastructure design)

You and You and You get learning!

Competition organizers always learn new things

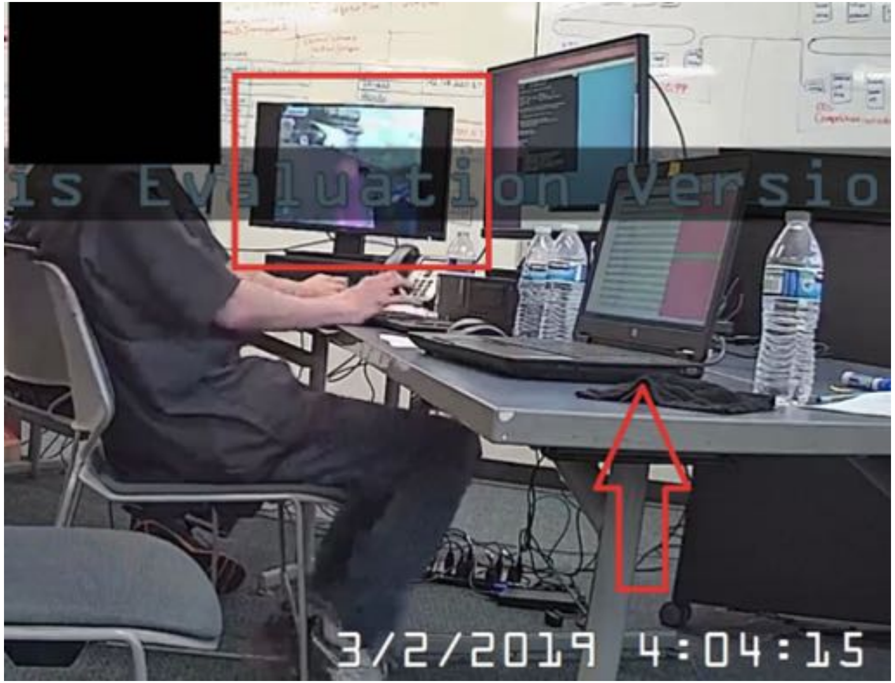
Sometimes we learn new things for competition

But we all learn

Competitions

- Variety of cyber competitions exist:
  - CTF(s)
  - CCDC
  - CPTC
  - Hack the Box
- Goal of competitions: To learn new skills and test skills

  (in humble opinion)



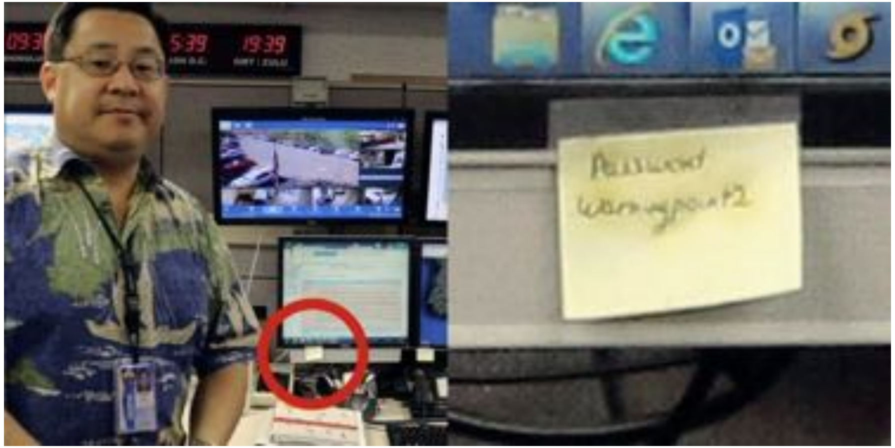
[redacted]

MR. ROBOT

The Mr. Robot Dilemma

- Hacking looks cool - most students only want to be a “hacker”
  - No real development of underlying skills
  - No effort to understand how internal components of software, hardware, and operating systems truly work (System Internals anyone?)
- Information Security Celebrities and TV give a false reality around the industry
- Being a good system administrator makes you much better at many other things - even red teaming

Because the reality is..

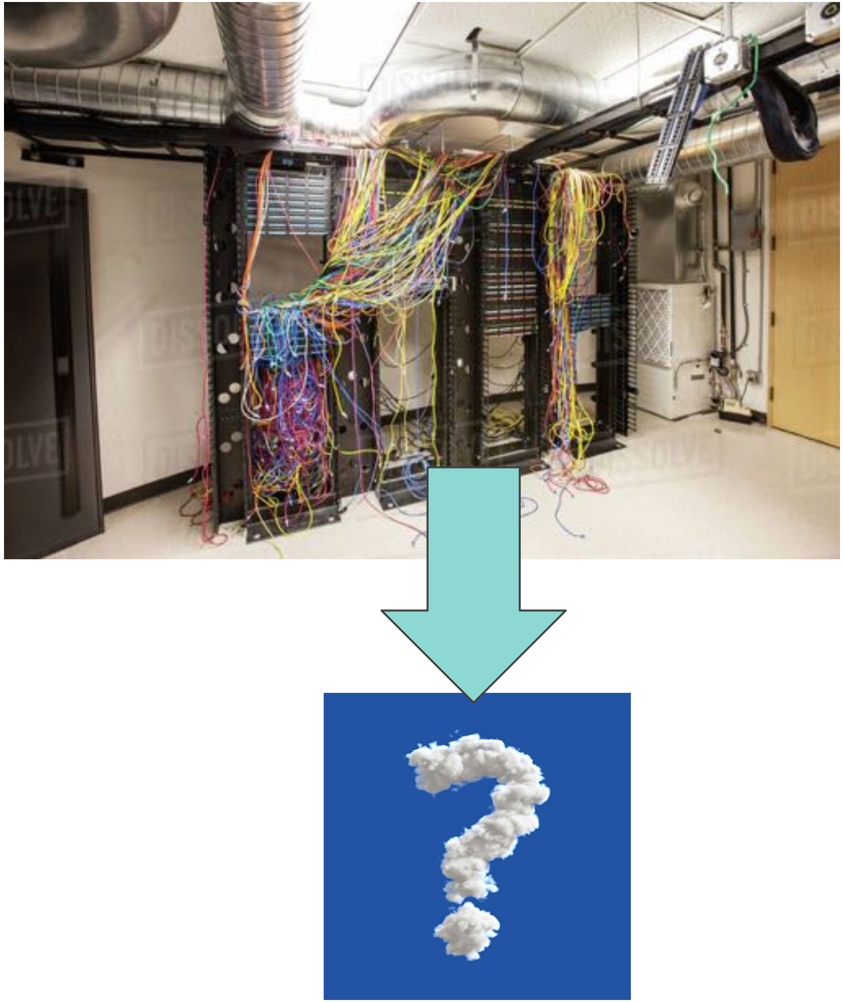


And...

Getting started!

- Competition organizers and competitors are their own distinct bubbles
- Organizers think a scenario is a great idea because its funny or interesting, or challenging
- Competitors want clear, realistic, reasonable scenarios.
- Scenario / Challenge creators prefer obscure to mundane - but mundane most common
- It is easy to get pulled into asking “Why not?” instead of “Should we?”
- **Harsh Reality:** We learned the fine art of encourage learning and skill development and not just develop skids’

It’s Building Time



- Both small and large companies are moving away from traditional client/server infrastructure
- Nothing is in its own boxes anymore - many shared resources
- Many new attack vectors - S3, Cloud Keys, Git (credentials)

Problem: COST

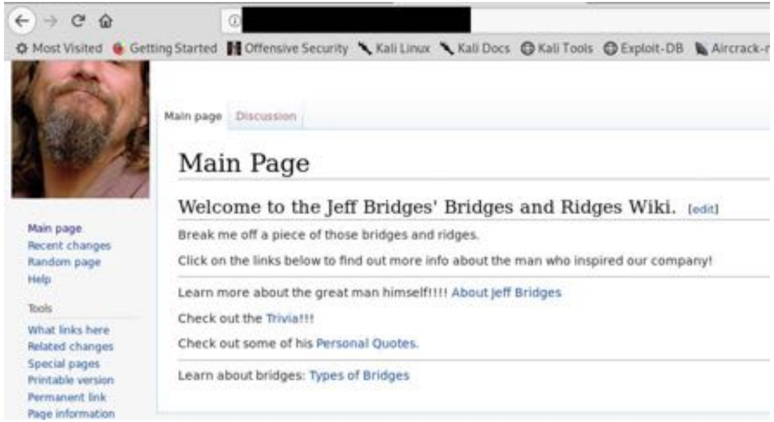
Step 1: Determine Type Of Competition

- Target Audience
  - Students - Should try to provide training
  - Professionals - Make it fun, challenging
  - Mixed
- Number of competitors
  - Small
  - Large
  - Teams
- Strategy Rules for Competitors - How you make the competition fair
- Cost(s) - What type of competition and how costs can be managed dramatically changes how an event is organized.

Step 2: Determine Scenario

- Scenarios can provide a structure around which challenges are built
- Can make a competition more fun
- Not always applicable
- Can be more fun for organizers
- May be step 2 but usually step 1 for organizers (hype machine)

We put a ton of content in…



Main Page

Welcome to the Jeff Bridges' Bridges and Ridges Wiki. [edit]

Break me off a piece of those bridges and ridges.

Click on the links below to find out more info about the man who inspired our company!

Learn more about the great man himself!!!! About Jeff Bridges

Check out the Trivia!!!

Check out some of his Personal Quotes.

Learn about bridges: Types of Bridges

Step 3: Resources

- Containers work well for shared challenges
- VM/VPS/EC2 per team to distribute challenges among teams
- Unique challenges per team/competitor require either a lot of work or automation.
- Provision physical systems? Or just clone..
- Rent Servers!

How do you build?

What does it actually take?

- Pod Design
- On-Site
- Hybrid
- Cloud

What do you use?

- AWS
- Google Cloud
- Azure
- Custom Servers
- Dedicated Hosting

Common Challenges

- Downtime - The OVH Challenge
  Depending on remote providers makes quick fixes nearly impossible
  - Maintenance Windows
  - Recovering requires time - especially during live competitions - how do you plan for this?
- Cost - AWS with Dev Time
  - AWS and Providers are cheap but the cost isn’t low when you factor in development hosts.
- Automation Slowdown
  - Certain tasks - host building and similar become slower compared to when you can simply clone

Step 4: Getting Everything Working

- Sometimes the best challenge is one that is broken… very very… broken
- Providing a load test to see where major issues occur - because they will!
- Have a backup plan and make each part realistic

Step 5: Work it out and run it!

Future Work

- Incorporating current trends
  - Code Review and Hardening
    - For CCDC this was a new one, for CTFs it's pretty much standard
- ICS(s)
  - Also known as the “crusher of dreams”
  - Found a fantastic sponsor at DefCon but real life constraints required them to pull out 3 weeks before competition with almost no deliverables
  - An attempt was made to finish ourselves but shelved for another day
- SIEM
  - Always suggested, never implemented
  - We would love competitors to focus on this but not enough time in the competition
  - Do we offer it to them as a “managed solution”?

Continuing Automation

- Deployable services
  - Vulnerable services, remote administration tools, etc
  - Legitimate services for scoring
  - Mid-competition additions

- Layers of abstraction
  - No real standard for system or service building
  - Windows (lol)
  - Building tools to homogenize disparate systems

Conclusion

Goals:

Make competitions open for everyone and keep improving

Help build everyone's skill!

Questions?

Twitter:

@spiceywasabi
@bluescreenofwin

Competition:

WRCCDC.org