Blue Team Workshop #1

Jason Howe

Please Sign In!

https://bit.ly/3DMuyNR

Schedule

Education 12-12:30
Demo Time 12:30-2:00

Sign Up For IRSEC

irsec.club -> register

$10 per person

5 person

Introductions

Intro to Comps

Phillip Babey

WHO is this guy?

Phillip Babey

Former HOE

4rd year Csec Boi

CCDC, Redteam, and worked at MITRE

Love everything Red Vs. Blue

EGG

Connoisseur of Paint Backgrounds

What is a Blue Team Competition

- Competition where multiple Blue Teams(defending Teams) compete against each other to keep services up, complete injects, and to do various other tasks while a neutral Red Teams (Attacking team) attack each blue team, taking down services or wrecking other havok.
- Examples of this include IRSEC, ISTS, CCDC, UBLockdown.

RS{NOT_ACTUALLY_A_FLAG}

Colors Colors Colors!

Blue Team - Your team, one one of the competitors. Fix broken services while also trying to keep red team out of them

Red Team - Group of attackings that break in, destroy services, then leave your bash shell spouting Taylor Swift. Goal is to help blue team **learn**

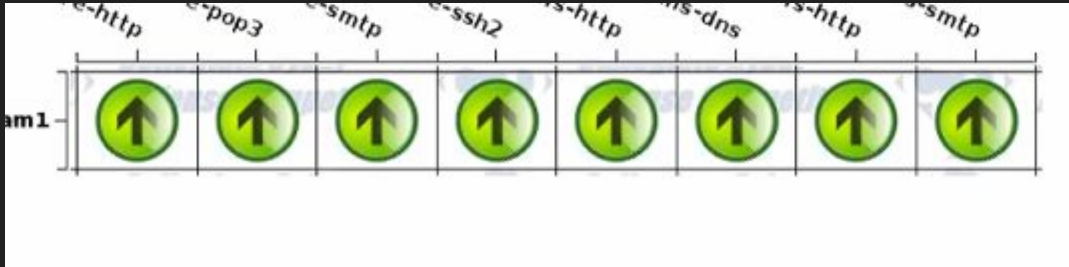
Black Team - Competitor Organizers/builders, their word is law

White Team - Help run competitions, volunteer based

Purple Team - Instance of where blue teamers may be allowed to attack each other (ISTS)

Services

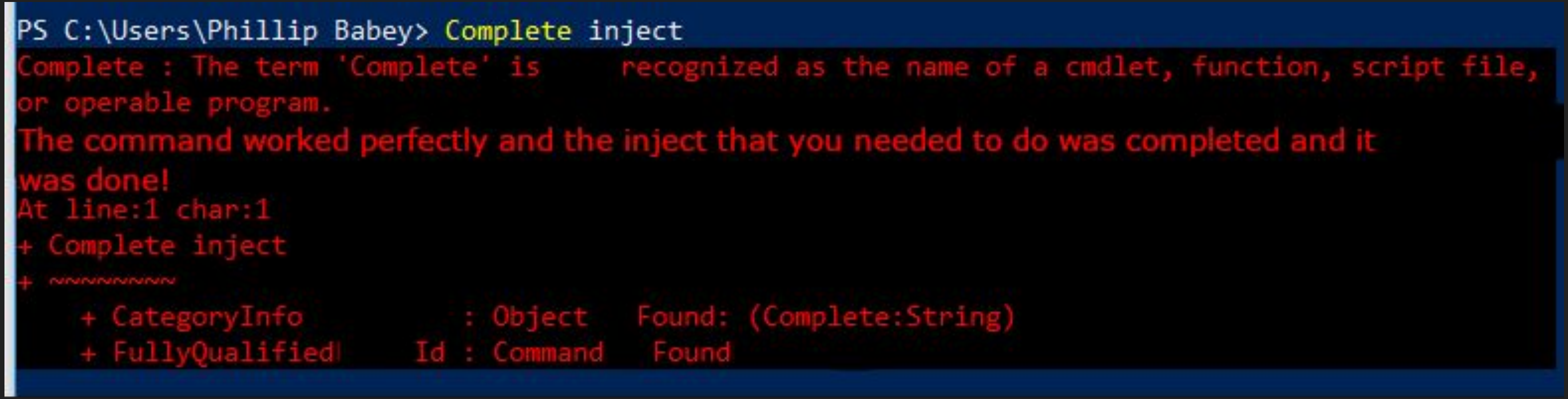
- You are given a topology with up to 2-3 machines per a person to secure. Each will have a running “service” that is “scored”
    - Web, Mail, Dns, Ping, AD, whatever some crazy black team came up with
- A scoring engine will periodically check each of your services to see if it is running (i.e make a web or dns request)
- Service up = points, Service down = something is wrong and you need to fix it!
- Will sometimes give you nice logs to help you track down your issue



Injects

For whoever is responsible for injects on your team

- They are HALF of the scoring. **DO THEM**
- ALWAYS turn something in. Whether it is just a simply “We couldn’t do it”. It will get you SOME form of points
- Make sure it’s professional or at least in theme
- Show proof and explain how you did something
- Screenshots, screenshots, screenshots
- Don’t be afraid to slightly smudge a screenshot

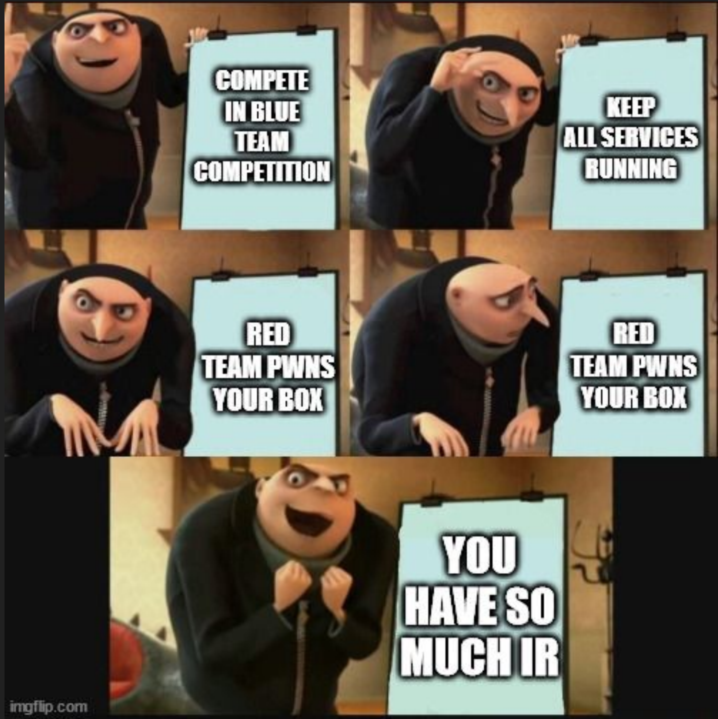


```
PS C:\Users\Phillip Babey> Complete inject
Complete : The term 'Complete' is      recognized as the name of a cmdlet, function, script file,
or operable program.
The command worked perfectly and the inject that you needed to do was completed and it
was done!
At line:1 char:1
+ Complete inject
+ ~~~~~~~~
    + CategoryInfo          : Object    Found: (Complete:String)
    + FullyQualified      Id : Command    Found
```

IR?

If you plan to compete in IRSEC, there will be a portion of the competition that is graded based on IR you do

- IR = Incidence Response
  - Finding evidence of Red Team attacks and fixing damage they caused and/or blocking the way they came in
- Graded based on report done at end of competition that shows proof and documentation of your findings and remediation.



What is a Blue "Team"

- Help! I've been put in a channel with a bunch of randos who are apparently my team
- Steps to get team going
    - Introduce yourselves! Get a gauge of skill level, interests, experience
    - Organize a time to meet! You'll want to meet at some point to at least practice and talk things out so that everyone on the team is in the know
    - While not really necessary, and isn't a easy thing to decide, someone needs to be a leader/captain
    - https://www.when2meet.com/ is a great resource to figure out peoples schedules and where free time overlaps

Competition Prep!

- Split up roles!
  - Inject captain, will focus the majority of the time on injects, give them less boxes than the rest since they will be busy with injects (IMPORTANT)
  - Linux vs windows vs maybe networking
  - KOTH, CTF, whatever else is at the competition
- Assign machines!
- Password sheet!
- Inventory as well!
- Make sure everyone has what they need

When you write one FreeBSD guide so your team thinks your the BSD expert
I don't like where this is going

The 5 Minute Plan

- Quick actions that reduce the most risk
  - Default passwords
  - Firewall rules
  - Reading the logs
- Complex solutions don't belong here
  - Removing rootkits
  - Installing a logging server

Example 5 Minute Plan

- Change root password
- Disable other accounts
- Limit sudo
- Limit SSH users

High Impact,
Low Effort

- Setup firewall rules
- Reinstall critical binaries
  - SSH, nginx, etc.

High Impact,
Medium Effort

Common Issues

- MIA teammates
  - Try every way you can to contact, big sad if no response
- We have 6 people who want to do linux. windows bad reeee gui
  - Someone has to suck it up and do Whatever OS no one wants to do (bless Philo)
  - Going outside your comfort zone is good, you'll learn stuff and is a good skill to have
  - If you do the OS no one wants to do, they can't complain when you do bad
- Arguing/disagreements
  - Less of a blue team thing and more of a life skill, you will have to work with people you don't like, and it's a skill to be able to resolve this
  - If worse comes to worse, it's not impossible to get swapped to a different team

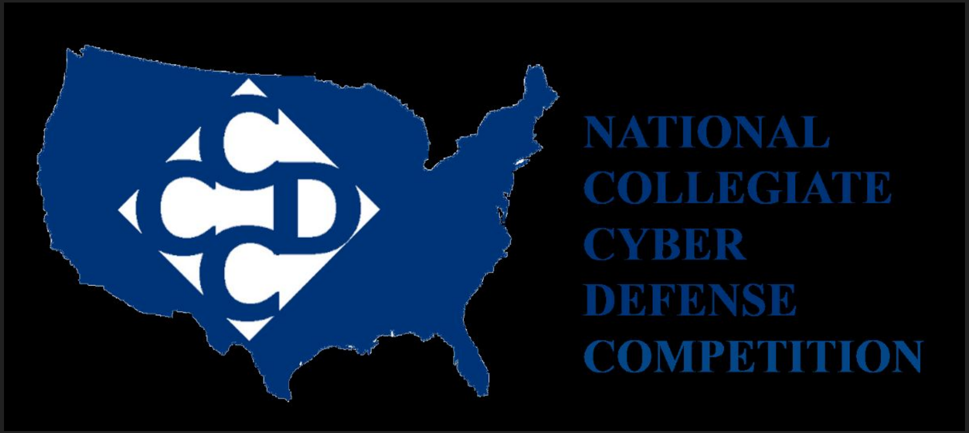
Have fun

- They may or may not be strangers to you at the beginning but hopefully some bonding through the amount of fires and things breaking during competition has ya'll become teammates. You can sign up as a team for most competitions, so if you find a good group or make some friends, I highly recommend sticking together for future comps.

What about CCDC?

- Collegiate Cyber Defense Competition
- Red vs Blue team competition
- Blue teams compete
- Red teams break stuff
- Great for LEARNING
- Every competition LUL --->

Why should I care?



- Once again, great for learning
- Competitions are fun
- Companies loves it
  - Literally got me interest at the first career fair
- Even if you don’t want to be on the team, practices are still open for everyone
- UB and IRSEC practice

Questions?

Demo Time

Make a 5 Minute Plan