BUILDING A CTF TEAM
THE BEGINNERS GUIDE

Johnathan Miranda
@niden

PS C:\> GET-CONTENT -PATH C:\ABOUT_ME.TXT

- AD Air Force *Cyber* Warfare Operator
- Endpoint Security Lead @ AFCERT
- PowerShell lover
- Avid CTFer
- Slack troll
- Dad of 2, Husband of 1
- First time speaker

U.S. AIR FORCE

OUTLINE

- Wat is a CTF?
- Why should you play?
- It’s Dangerous to Go Alone
- Standard types of CTF events
- Challenge types
- Setting up your environment
- Communication/Collaboration Tools
- Gathering your squad!
- Don’t be afraid of failure
- Communicate!!
- Practice Practice Practice
- Online Resources

WAT IS A CTF?!

- CTF (Capture the Flag) – A security focused competition where the objective is to obtain the most amount of flags.

WHY SHOULD YOU PLAY?

- Teach yourself a new skill
- Soft skill development
- Objectively measurable success/failure
- It’s just plain fun
- Seriously its fun

IT’S DANGEROUS TO GO ALONE

- Creating/Building a CTF Team is a great way to start collaborating with others
- Ability to specialize in one or two categories
- Learning the basics of managing a team and balancing team dynamics
- Bounce ideas off of each other

Shameless Zelda Reference

STANDARD TYPES OF CTF EVENTS

- Jeopardy Style (Most CTF's)
- Attack & Defense (CCDC, Pro's V Joes @ BSidesLV)
- Hack Quest (SANS Holiday Hack)

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

TYPICAL CHALLENGE TYPES

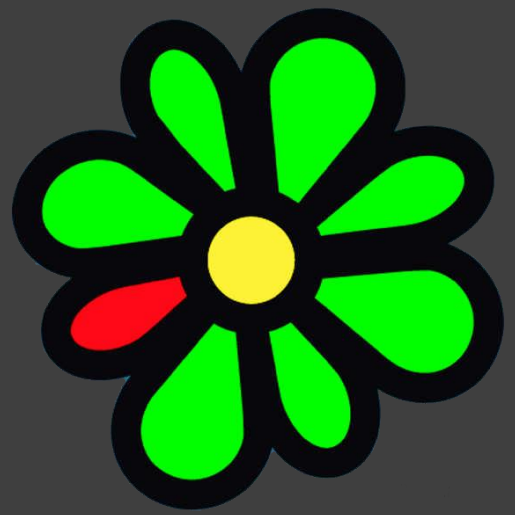
- Binary Exploitation
- Cryptography
- Forensics
- Programming
- Recon (OSINT)
- Reverse Engineering
- Web Exploitation

SETTING UP YOUR ENVIRONMENT

- Virtualize everything
- VMWare Player/Virtual Box are free
- Vagrant (Epic Treasure)
- ESXi if you have a server lying around
- You can start with Kali then customize as needed
- Roll your own OS with tools for a project

COMMUNICATION / COLLABORATION TOOLS

- Chat – Skype, Google Hangouts, Slack, IRC
- Documentation – KeepNote, OneNote, mdwiki, Confluence, Google Docs, GitHub, Notepad

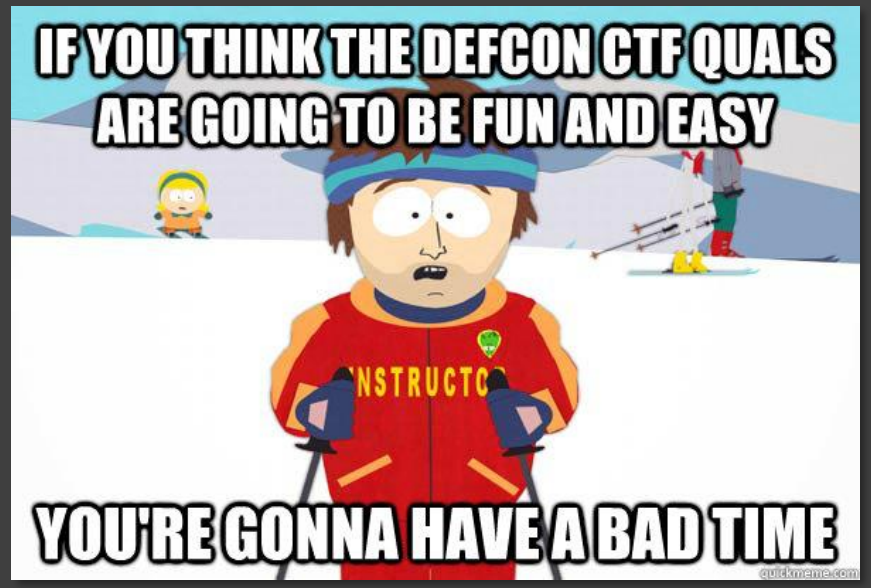



GATHERING YOUR SQUAD!

- Check your school
- Look online r/securityCTF (Open To All)
- Check out CTFTime
- Drag your friends/family into it
- Visit SAHA! and bug them there
  - Seriously do it

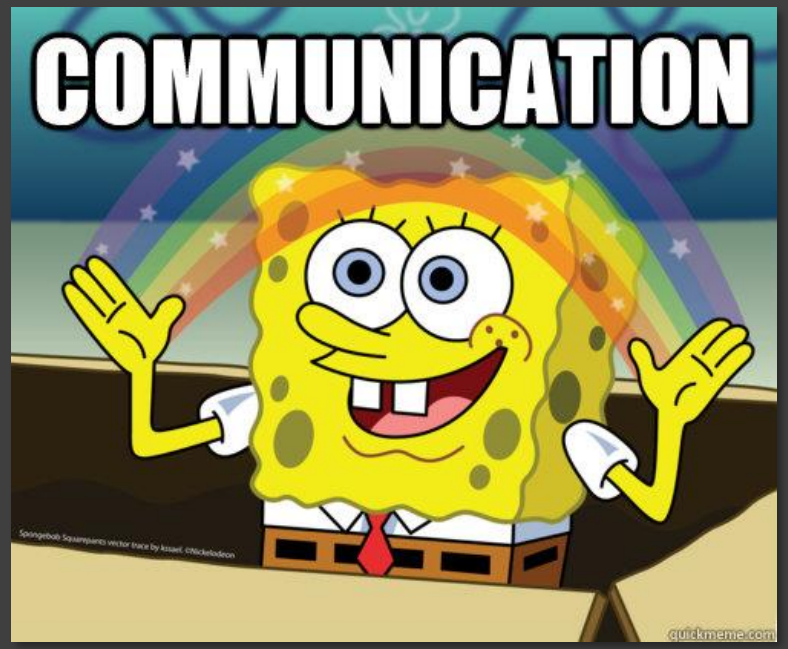
DON’T BE AFRAID OF FAILURE

- You will get stumped
- You may get frustrated
- Your team may come in the bottom 50
- Difficulty level of challenges scale dramatically
- Focus on CTF’s that are created for beginners (as discussed earlier)
- Remember you’re doing this for fun (hopefully)



COMMUNICATE!!

- Use your tools to keep in touch with your team
- Establish a challenge tagging system
- If your teammates are friends, don’t just talk about CTF stuff.
- Take notes on what you’re doing when you’re doing it and back them up
- Talk out challenges with your team



PRACTICE PRACTICE PRACTICE

- Keep at it, always run to come out of a CTF learning at least one new thing
  - Experience with challenges really help
- Write-ups! – *Always* create writeups.
- You will improve, the challenges aren't going to get any easier but you will get better
- Research topics when you're not CTFin

ONLINE RESOURCES

- CTF Field Guide - https://trailofbits.github.io/ctf/
- Awesome CTF - https://github.com/apsdehal/awesome-ctf
- CTF Tools - https://github.com/zardus/ctf-tools
- CTF Time - https://ctftime.org/
- CTF Writeups - https://github.com/ctfs
- CTFHacker’s Blog - http://ctfhacker.com/
- Capture the Swag Blog - https://ctf.rip/
- LiveOverflow - http://liveoverflow.com/
- Netsec Focus – http://netsecfocus.com

THANKS FOR COMING TO MY TALK!

Check these awesome folks out!

MCPA
SAN ANTONIO
DEVELOPING CYBER PROFESSIONALS

Additional questions after BSides?

@niden

niden.sh@gmail.com