DEMYSTIFYING CAPTURE THE FLAGS (CTF)

BARRETT DARNELL

OUR AGENDA

01 WHAT IS A CTF?

02 CTF STYLES

03 CHALLENGE TYPES

04 TECHNICAL SKILLS

05 NON-TECHNICAL SKILLS

06 POST CTF ANALYSIS

WHOAMI

- Security Associate at Bishop Fox
- Managed Security Services, Continuous Attack Surface Testing (CAST)
- SANS Instructor in Training, SEC660
- Previously:
  - Offensive Cyber Operator, US Air Force
  - Certified Operator Trainer
  - Military Instructor
- Notable Wins

CTF STYLES

- Jeopardy
- Attack and Defense
- King of the Hill
- Story/Scenario Driven

TYPES OF CHALLENGES

- Cryptography
- Computer Exploitation
- Forensics
- Programming
- Reverse Engineering
- Trivia/Puzzle
- Web
- Misc.

TECHNICAL SKILLS, TOOLS AND TECHNIQUES

- Windows
- Linux
- Infrastructure
- Networking
- Scripting

TECHNICAL VIGNETTES

IOT CTF by Independent Security Evaluators (ISE)

- Developed tools, cross compiled binaries, learned about IOT
- Used those skills on assessments to pivot into internal networks

Malware RE

- Rudimentary RE skills gained through various CTFs
- Used on assessments to examine unknown binaries

NON-TECHNICAL SKILLS

- Creativity
- Persistence
- Resiliency
- Note Taking, Logging, Analysis
- Preparation and Practice
- Attention to Detail

NON-TECHNICAL VIGNETTE

- Geocaching/Escape rooms
  - Common techniques, recognizing patterns
  - Scratch near a puzzle, timestamp of binaries
- Note taking is critical!
  - Terminal screens
  - Web requests
  - Network traffic
  - Proxy logs

SOCIALIZING & TEAMWORK

- Know your team
- Learn as a team
- Leverage the expertise of others
- Bonding
- Communicating effectively
- Knowledge sharing

POST CTF

- Writeups
- Video walk throughs
- Tooling
- Testing
- Analysis and self-improvement

CONCLUSION & QUESTIONS

- What is a CTF?
- CTF Styles
- Challenge Types
- Technical Skills
- Non-Technical Skills
- Post CTF Analysis