Demystifying Capture The Flags (CTF)

PRESENTER
Barrett Darnell
March 5, 2020

Overview

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