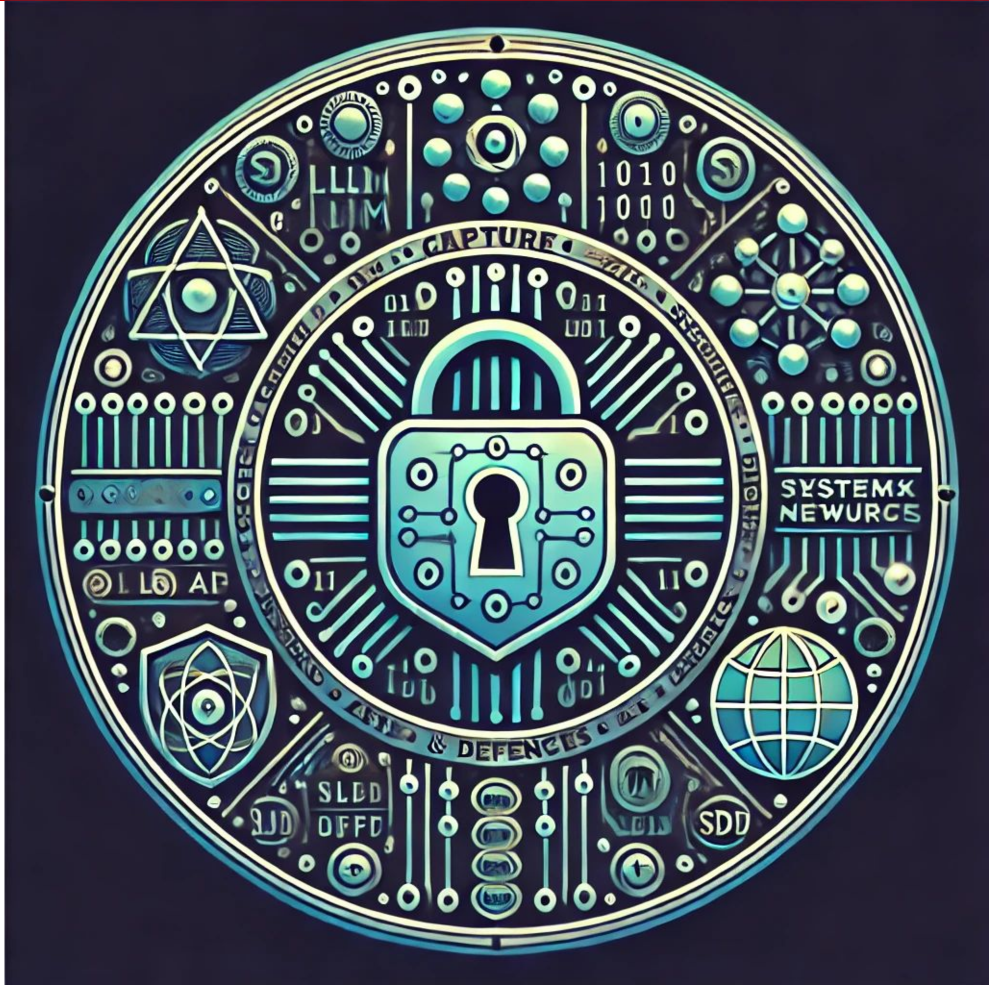
NC STATE UNIVERSITY

CSC-537 Systems Attacks and Defenses

Capture the Flag (CTF) Best Practices for Organizing Security Competitions

Alexandros Kapravelos
akaprav@ncsu.edu



Introduction

Capture the Flag (CTF) competitions are cybersecurity events designed to test and improve security skills in a safe environment.

They help individuals and organizations enhance their security awareness and identify talent.

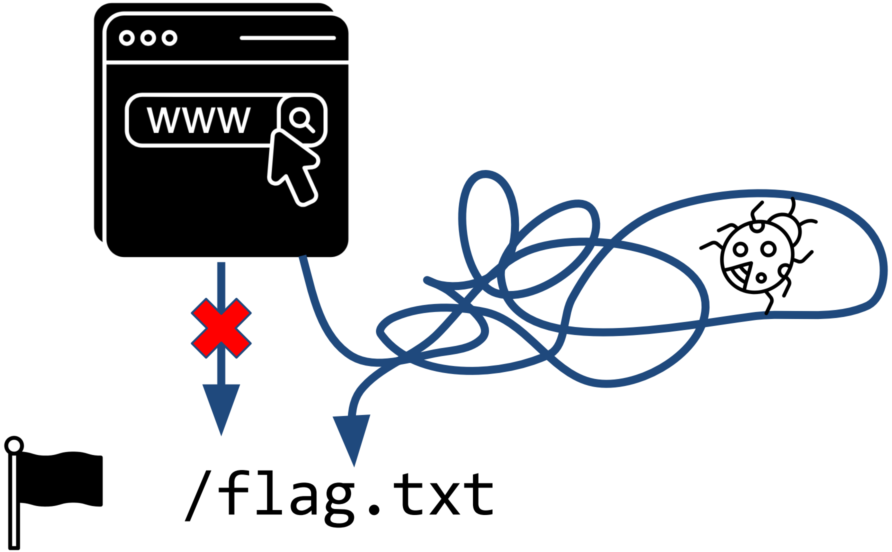
Why play CTFs?

They are beneficial for:

- Developers learning about common vulnerabilities
- Practical, contained environment to improve/demonstrate your skills
- Security professionals honing offensive and defensive skills
- Organizations building security-conscious cultures
- Recruiting top talent

What is a CTF?

Capture `flags` to prove you have exploited a vulnerability



CTF types

- Jeopardy-style
- Attack-Defense
- King of the Hill (KoTH)
- Mixed or custom formats

Jeopardy-style CTFs

Participants solve challenges in categories such as:

- Web security (SQLi, XSS, CSRF)
- Cryptography (breaking ciphers, protocols)
- Forensics (analyzing disk images, network traffic)
- Reverse engineering (understanding software behavior)
- Binary exploitation (buffer overflows, format string vulnerabilities)
- Networking (protocol analysis, traffic manipulation)
- Steganography (hidden data in images or audio)
- Programming (scripts, algorithmic challenges)
- Miscellaneous/General (unique puzzles, security trivia)

Each solved challenge awards points based on difficulty

HackPack CTF focus

Mostly these types of challenges:

- Web security
- Binary exploitation
- Cryptography
- LLM security
- Reverse engineering

Attack-Defense CTFs

Teams defend their own vulnerable systems while attacking other teams

- Points for patching vulnerabilities, exploiting weaknesses, and capturing flags
- More complex to organize, requiring isolated infrastructure and continuous monitoring
- Skills needed: system administration, network security, offensive tactics, and incident response

Key component: The Gameserver

- Periodically places and retrieves flags on each team’s system (Vulnbox)
- Uses NAT to obscure attack sources

Strategies:

- Focus on attack
- Focus on defense
- Balanced approach

King of the Hill (KoTH) CTFs

Combines Jeopardy and Attack-Defense elements

- Participants fight for control of a specific system or service
- Must also defend it against others
- Machine resets periodically revert challenges to their initial state

This format requires:

- Offensive skills to exploit and gain initial control
- Defensive tactics to maintain control against incoming attacks

DOOM

DEFCON 27 CTF finals - DOOM

- Each of the 16 teams received an Xbox
- Networked multiplayer deathmatch mode
- Hack the game itself to become the reigning King of the Hill
  - Control special areas of the map to score points

Restrictions:

1) Players cannot use their weapon until they bypass a simple check
2) Players cannot score points until they change their name from "sheep" (default) to their team name

Mixed CTF Format

Merges multiple CTF styles into a single event

- May include Jeopardy-style challenges alongside attack scenarios
- Could feature hardware hacking, physical security, or wargame elements
- Offers a comprehensive test of diverse cybersecurity skills

CTF Gameserver Architecture

Essential for Attack-Defense CTFs

- Centralized Command & Control through a shared database
- Time divided into ticks for flag placement and checks
- Checker Scripts validate service status by placing and retrieving flags
- Flags generated with a secret key and MAC for authentication
- Randomized team numbers help prevent targeted attacks

Best Practices: Defining Objectives and Scope

- Clearly define goals for the competition
- Identify your target audience
- Determine the scope of challenges
- Consider the time frame of the event

Best Practices: Designing Engaging Challenges

- Provide a diverse set of challenges with varying difficulty
- Align challenges with real-world scenarios and industry trends
- Give clear instructions to reduce confusion
- Include hints to prevent participant frustration, avoid having players guessing as much as possible
- Define bot parameters if bots are involved
- Think about unintended solutions and try to prevent them
- It’s an educational competition. What will the players learn in security from your challenge?

HERE'S
THE WEB
FIND A FLAG

Best Practices: Setting Up Infrastructure

- Select a suitable CTF platform (e.g., CTFd, kCTF, rCTF)
- Ensure reliable, secure infrastructure with sufficient resources
- Use hardened Docker images
- Implement least privilege access controls
- Employ load balancing for high availability
- Monitor and log events for fairness and issue resolution
- Plan for crowd control if hosting a large in-person event

Scoring Systems and Fairness

- Static or dynamic scoring
  - Static scoring assigns fixed points
  - Dynamic scoring reduces point value as more players solve
- Have tie-breakers (time of flag submission, bonus for first blood)
- Enforce rules to prevent cheating or flag sharing
- Address LLM usage to ensure fairness
- Clearly communicate guidelines and expectations

Resources for Creating CTF Challenges

- OWASP:
  - Juice Shop (common web vulnerabilities)
  - Secure Coding Dojo (lessons based on MITRE’s top software errors)
  - WrongSecrets CTF (secrets management vulnerabilities)
- HackTheBox (wide variety of categories, difficulty levels)
- CTFtime.org (list of ongoing events and writeups)
- GitHub (open-source CTF projects and frameworks)
- VirtualBox for local testing
- Popular frameworks:
  - CTFd
  - kCTF
  - rCTF

Examples of great CTF Competitions

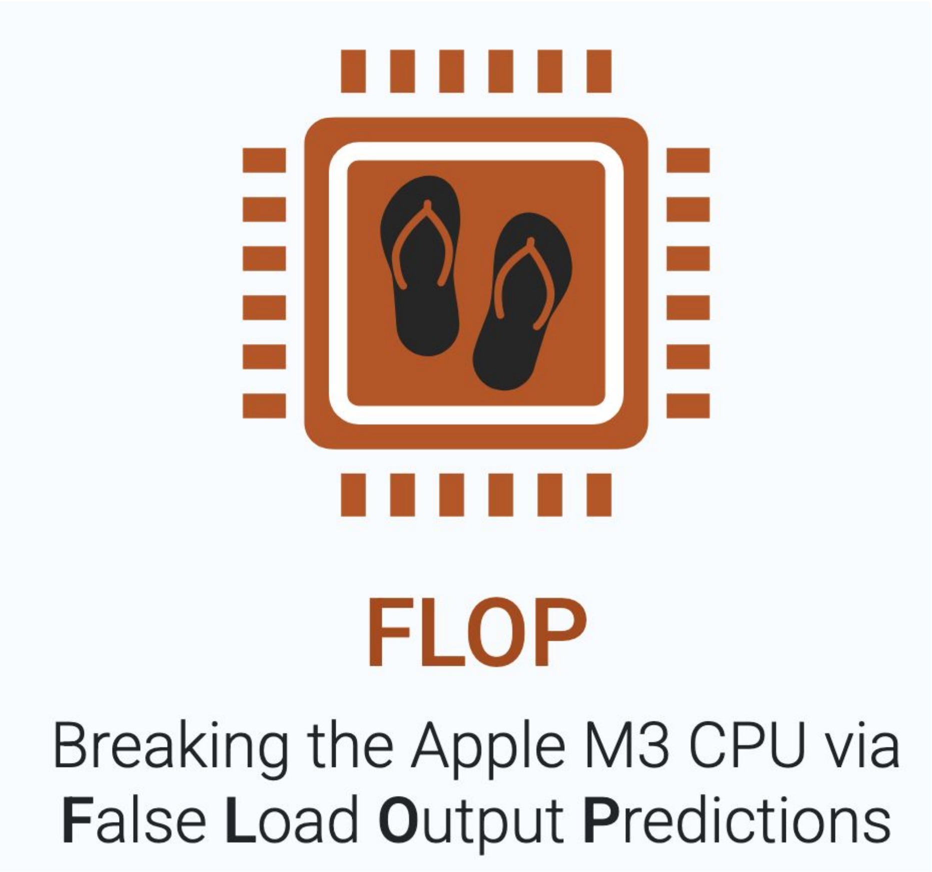
- DEF CON CTF
  - Attack-Defense format
  - World-renowned for advanced challenges
- CSAW CTF
  - Large-scale event for students and professionals
  - Real-world cybersecurity scenarios
- PlaidCTF
  - jeopardy-style, organized by PPP
- PicoCTF
  - year-round learning, entry-level
- iCTF
  - oldest CTF, usually attack-defense, run by UCSB

Summary and Takeaway Points

- CTFs are powerful tools for learning and teaching cybersecurity
- Diverse formats (Jeopardy, Attack-Defense, KoTH, Mixed) cater to various skill sets
- Proper infrastructure, clear objectives, and engaging challenges lead to successful events
- Leveraging available resources and frameworks simplifies organization and challenge creation
- By focusing on best practices and innovation, you can host impactful competitions that benefit participants at all levels

SLAP

Data **S**peculation Attacks via **L**oad **A**ddress **P**rediction on Apple Silicon



FLOP

Breaking the Apple M3 CPU via **F**alse **L**oad **O**utput **P**redictions

https://predictors.fail/