

# Hands-On Cyber Competitions

Irvin Lemus



[Infosecirvin.info](http://Infosecirvin.info)  
[@infosecirvin](https://twitter.com/infosecirvin)



SkillsUSA®



[Baycyber.net](http://Baycyber.net)

[irvin.lemus@wastc.org](mailto:irvin.lemus@wastc.org)



WESTERN ACADEMY  
SUPPORT & TRAINING CENTER

# Agenda

- Contests
  - Capture The Flag
  - Purple Competition
  - CyberPatriot
- Resources
  - Cloud Infrastructure
  - Teaching Resources
- Getting Started
  - Hosting Digitally
  - Hosting Physically
- Q & A



# Contests: Capture the Flag

Game: <https://ctf.baycyber.net>

RDP to desktop.baycyberctf.net

Username: baccc1 <-pick a number 2-100

Password: baccc123 <-same for all

- Easiest to deploy & understand
  - Solve challenges, get points
- Host Requirements
  - Cloud Desktop
    - Bypass local restrictions
  - Cloud CTF
- Student Requirements
  - Internet connected device with browser & ssh client
    - No client? [No problem!](#)



Ctf created by Jacobs Otto, Jetta Ragsdale, Bradley Bettencourt, Jeremy Woodling, Janelly Servin, Brandon Pimentel, George Nunez of Cabrillo College, including students from the Bay Area Region's Cyber Competitions Program

# Contests: Capture the Flag

## Learning Resources:

- [Terminus](#) (Linux Terminal game)
- [Linux Unhatched](#) (Linux Course)
- [SS64](#) (CLI reference)
- [CTF 101](#) (CTF Intro)
- [SQLBolt](#) (SQL Intro)
- [OvertheWire](#) (Wargames)
- [Reverse Engineering for Beginners](#)

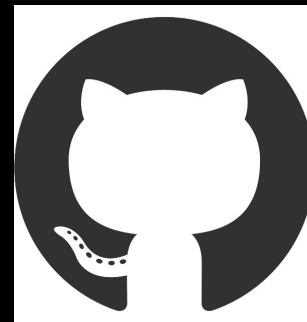
## Games: [ctftime.org](https://ctftime.org)

- Beginners
  - [picoCTF](#)
  - [SANS CyberStart](#)
  - [HSCTF](#) / [PACTF](#)
- Intermediate
  - [CSAW](#) & [CSAW RED](#)
  - [KringleCon](#)
  - [SquareCTF](#)
- Paid
  - [National Cyber League](#) (\$35/person)

# Contests: Capture the Flag

## Technical Resources:

- Host
  - [Digital Ocean](#) is the easiest to get started
    - [AWS](#) and [GCP](#) are other options
  - Student Server w/Tools
    - [Irvin's setup scripts](#)



# Purple Competition

- More complicated to set up
  - Blue VM creation
  - Kali VM
  - SSH access only to all
  - Distribute accounts
- Teams of 6
  - 3 defense, 3 offense per team
- **Blue Team:** Defend your systems from the opposing Red Team
- **Red Team:** turn off opposing Blue Team's systems



# Purple Competition

Learning Resources:

- [Baycyber.net](https://baycyber.net)
- [SecGen](https://secgen.com)
- [Root-Me.org](https://root-me.org)
- [HacktheBox.eu](https://hackthebox.eu)
- [TryHackMe.com](https://tryhackme.com)
- [OWASP Juice Shop](https://owasp-juice.shop)
- [Web Security Academy](https://web-security-academy.com)



# CyberPatriot

- Local VMs
  - VMware supported; Vbox not supported
  - ESXi implementation is possible, but is challenging
- Hardening Systems
  - Windows Desktop/Server
  - Ubuntu/Debian
- Cisco Networking
  - Select chapters from courses
- Support
  - Practice Images
  - Scoring Systems
  - IT Concerns
  - Local Hardware Requirements





# Hosting Digitally

- Set up a cloud account
  - GCP has \$300 credit/account, can use same credit card repeatedly
  - AWS Educate grants \$75/student
  - DO has searchable promo codes
- Create questions/challenges for students
  - Use similar content from other CTFs to start
  - Have students create their own



# Hosting Digitally

## Practice Environments:

- [SecGen](#) (*Purple Competition*)
  - Requires local VM for SecGen
    - [Raw Install Instructions](#)
  - Clouds accept Debian 8/9
- Splunk BOTS 1 & 2
  - [Splunk BOTS 1](#)
  - [Splunk BOTS 2](#)
- [OWASP Juice Shop](#)
- [DVWA Docker](#)

## Suggested VMs

- Metasploitable 1
- Metasploitable 2

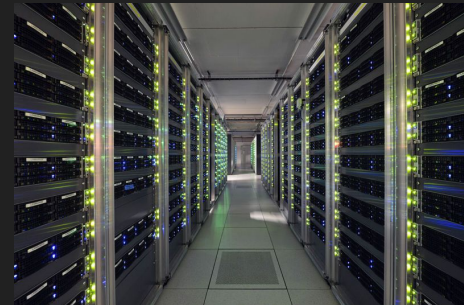
## Suggested Websites:

- [Root-me.org](#) \*no VPN
- [Hackthebox.eu](#)
- [Tryhackme.com](#)



# Hosting Physically

- Server
  - VMware ESXi
  - 2+ NICs
  - 8+ CPU Cores
  - 16+GB RAM
  - 500+GB Storage
- Network
  - Gigabit Network for uploading
- Administration
  - Clients have VMware to create VMs
  - Create student accounts that can access ESXi
  - Updates/upgrades/upkeep
- Human Aspect
  - Community Colleges
    - Getting students to participate in and create contests
    - Connecting with local K-12
  - MS/HS
    - Building a student base to participate and create contests
  - Work with Regional Directors (formerly Deputy Sector Navigators) on funding sources



Q and A



# Hands-On Cyber Competitions

Irvin Lemus



[Infosecirvin.info](http://Infosecirvin.info)  
[@infosecirvin](https://twitter.com/infosecirvin)



SkillsUSA®



[Baycyber.net](http://Baycyber.net)

[irvin.lemus@wastc.org](mailto:irvin.lemus@wastc.org)



WESTERN ACADEMY  
SUPPORT & TRAINING CENTER