

# WHAT IS CAPTURE THE FLAG?

A Fabulous (and Fun) Way to Learn and Sharpen Cybersecurity Skills!

By Penelope Rozhkova

# AGENDA

01/

**CTF VS HACK-A-THON**

02/

**TYPES OF CTF GAMES**

03/

**WHERE TO START**

04/

**SHARPENING SKILLS**

05/

**UPPING YOUR GAME – PROFESSIONAL DEVELOPMENT**

# CTF VS HACK-A-THON

---

# CTF -- WHAT IT'S NOT

Hack-a-thon

[Hackathon - Wikipedia](#)

[https://en.wikipedia.org › wiki › Hackathon](#)

A **hackathon** (also known as a hack day, hackfest, datathon or codefest; a portmanteau of hacking marathon) is a design sprint-like event; often, in which **computer programmers** and others involved in **software development**, including graphic designers, interface designers, project managers, domain experts, and others ...

CTF stands for Capture the Flag.

- It is ***not*** a playground or paintball game.



<https://www.wikihow.com/Play-Capture-the-Flag>

# CTF -- WHAT IT IS



- A CTF is a set of security challenges.
- When a challenge is solved, you identify a flag and submit it for points.
- You are provided with a scenario or clues to solve the challenge.
- You use cyber security skills to solve the challenges.

# **TYPES OF CTF GAMES**

---

# JEOPARDY STYLE CTF

CTFLEARN



<https://ctflearn.com/>

Learn

Challenges

Scoreboard

Category: All

Difficulty: All

Solved: Unsolved

Order: Most Solves

Reset Filters

Basic Inject

Where Can My Robot Go?

Base 2 2 the 6

POST Practice

Hextroadinary

## Make your teams aware of all types of cyber risks

The challenges proposed by MALICE Events examine all the skills in computer security. They encourage the practice of offensive security techniques so that your teams can better understand how an attack is launched, how much impact it may cause, and how they can protect themselves effectively from such an incident.

We have a catalog of challenge which are immediately available, and if necessary we can also develop new challenge exercises according to the risks specific to your business.

 Web Awareness of all flaws identified by OWASP impacting the websites.	 Exploitation Techniques for operating binary applications.	 Cryptography Low cryptographic algorithms, errors in the use of existing libraries.
 Configuration Exploitation of configuration errors in various frameworks and applications.	 Reverse Analysis of algorithms and applications to understand how they work.	 Forensic Analysis of the traces of an information system to extract data.
 Steganography Techniques for concealing information in a document, an image, or a data flow.	 Scripting Development challenges	

[https://malice.  
fr/en/jeopardy](https://malice.fr/en/jeopardy)

# JEOPARDY STYLE CTF

**MetaCTF** Problems Scoreboard Rules Stats <https://metactf.com/cybergames> Logout Dashboard ↗

With National University's scholarship opportunities, you may be eligible to save 25% on cybersecurity tuition. Start sooner and finish faster with 4-week classes and year-round enrollment at National University. Choose from 75+ programs and 100% online classes. Get started today at NU.edu

**Binary Exploitation** **Cryptography** **Forensics** **Reconnaissance**

**Reverse Engineering** **Web Exploitation** **Other**

Bonus Help UI Settings CyberChef

**Flag Format** (solved by 1055 teams) **50**

All flags should be obvious and a `string_separated_with_underscores`. Most of the flags will be surrounded by `MetaCTF{}` as well, but in the cases where that would make the problem too trivial, we did not include the `MetaCTF{}` part.

If the flag will be in a different format, we will specify that in the problem description. Additionally, all flags are case-insensitive. If you solve this challenge, make sure to tell your teammates about the flag format!

**Submit!**

# SANS TOMAHAWQUE

<https://www.tomahawque.com/>

## Challenges

120X12

# ATTACKER VS DEFENDER CTF



Where do I find  
these things?

- Subscribe to Newsletters
- Security Conferences
- Discord Servers
- Slack Workspaces

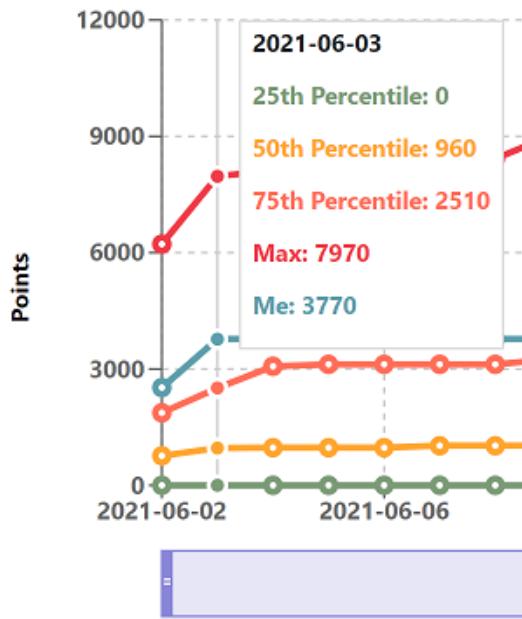
<https://medium.com/@redteamvillage/red-team-vs-blue-team-ctf-c0c0n-2019-44fcb42fbd46>

# RED TEAM

<https://cmdnctrl.net/ranges>

On this Red Team CTF platform, you attempt to compromise web applications to find flags.

## EVENT OVERVIEW



The screenshot shows the "RANGES" section of the cmdnctrl.net platform. At the top right, it displays "PancakesCon2020 Join another event" with a score of 75 and rank 368. Below this, there are two rows of challenge cards:

- Financial Shadow Bank**: A lock icon indicates it's locked. Description: Shadow Bank is the premier bank for people who love cryptocurrencies and hate those pesky minimum password requirements. Transfer money, request a loan, or buy and sell stocks and currencies. Screenshot: A dark-themed mobile app interface. Status: 0 challenges solved, NOT AVAILABLE.
- HR AccountAll**: A lock icon indicates it's locked. Description: AccountAll is the HR portal that turns humans into resources. Employees, managers and HR administrators can log in to manage payroll, timesheets, performance reviews and more. Screenshot: A mobile app interface showing a cloud icon. Status: 0 challenges solved, NOT AVAILABLE.
- Retail Shred**: A lock icon indicates it's locked. Description: Shred is your one-stop shop for skateboards, spray paint, pencils and all the other trappings of hoodlumism. Show off your best work in the graffiti gallery, or buy a gift card for the petty criminal in your life. Screenshot: A mobile app interface showing a portrait of a person. Status: 0 challenges solved, NOT AVAILABLE.
- Social Media InstaFriends**: A lock icon indicates it's locked. Description: InstaFriends is the social networking site that helps you make friends instantly. Well, probably not you in particular. You weirdo. Screenshot: A mobile app interface showing three people. Status: 1 of 52 challenges solved, EVENT NOT RUNNING.
- Mobile/IoT Runstoppable**: A lock icon indicates it's locked. Description: An Android fitness tracker that will turn you into a Runstoppable human being. NOTE: many challenges must be solved through flag submission found on the "Challenger" page under "My Stats". Screenshot: A mobile app interface showing a bird icon. Status: 0 challenges solved, NOT AVAILABLE.
- Financial The Gold Standard**: A lock icon indicates it's locked. Description: Shadow account got hacked? Switch to the Gold Standard for heightened security and a ROOM FULL OF GOLD. Screenshot: A mobile app interface showing gold coins. Status: 0 challenges solved, NOT AVAILABLE.
- Cryptocurrency DigiExchange**: A lock icon indicates it's locked. Description: Go crazy with crypto-currencies! Screenshot: A mobile app interface showing a green digital grid. Status: 0 challenges solved, NOT AVAILABLE.
- Marketplace Letsee**: A lock icon indicates it's locked. Description: Letsee is the hippest place for all the hottest products. We offer chic handmade items we purchased at goodwill, and marked up 500%. Finally, you can buy happiness! Screenshot: A mobile app interface showing a sofa and plants. Status: 0 challenges solved, NOT AVAILABLE.
- Cloud Forensict**: A lock icon indicates it's locked. Description: Welcome to your first day at Forensict! Please create a Portal account to start your journey. Screenshot: A mobile app interface showing a globe icon. Status: 0 challenges solved, NOT AVAILABLE.
- Cloud SecureSafeCrate**: A lock icon indicates it's locked. Description: So Secure. So Safe. So CRATE. Ponder Uniquely Inside Your Crate. Screenshot: A mobile app interface showing a safe icon. Status: 0 challenges solved, NOT AVAILABLE.

At the bottom right, it shows the user's stats: "ICMP\_Google\_2021 Join another event" with a score of 3,770 and rank 37. The user is identified as "PiranhaMama".

# BLUE TEAM

In a Blue Team CTF platform, you attempt to harden systems to prevent compromises to find flags.



RangeForce

11h ·

...

📣 The Persistence Challenge is officially live!

Login to the Community Edition between now and August 8 to participate in three exclusive cybersecurity challenges:

- Level One: Malicious Remote IPs
- Level Two: Compromised Accounts
- Level Three: Advanced Persistence

Do you have what it takes to defend against these threats? Prove your skills for a chance to earn prizes.

Ready to get started? If you're not yet a member of our Community Edition, sign up for free here: <https://hubs.la/H0R314f0>

Introducing the RangeForce Community SOC

Join the Community Edition today to:

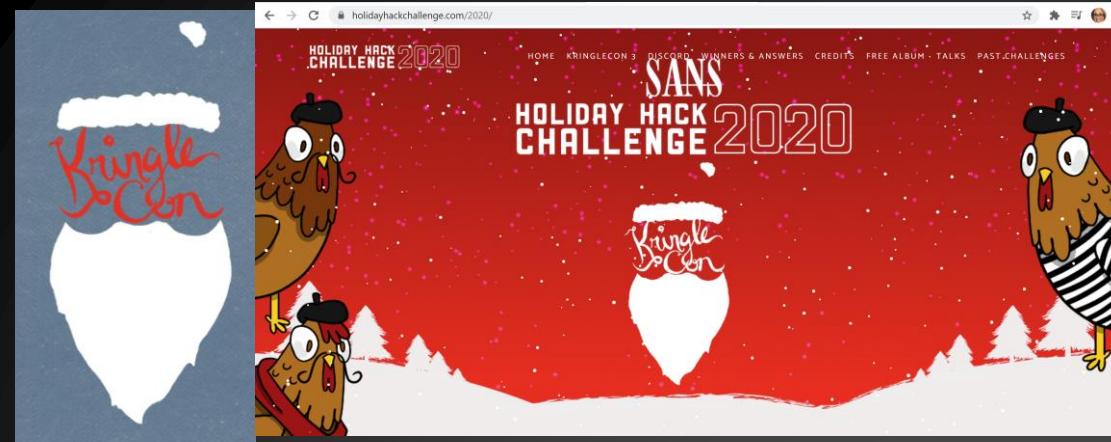
- 🛡️ Hone your skills with red and blue team training
- 🛡️ Take part in regular cybersecurity challenges
- 🛡️ See NMap, Splunk, Wireshark, and more in action
- 🛡️ Claim your first RangeForce Badge when you complete 10 core modules



Participate in the Persistence Challenge by logging in to the RangeForce Community Edition platform between July 21st and August 8th.

# INTERACTIVE

<https://2020.kringlecon.com/>



2020.kringlecon.com

A screenshot of the KringleCon 2020 interactive chat interface. The main area shows a 3D-style castle approach with various characters: Pepper Minstix (green skin, pink pants), Unescape Timux (black mask icon), piranhamama (text only), Santa (red suit), Pierre (chicken), Jewel Loggins (elf), Shiny Upatree (pink pants), and izzyTOG (orange circle). The right side features a sidebar with a question mark icon, volume icon, settings icon, and a discord link. Below that is a scrollable log of messages from participants like gkalsi, amk536, and FatherStalin, dated from January 17th to January 27th. A bottom banner says "Hellooo! Type here to chat." with a speech bubble icon.

ADULTS  
ONLY

# TRACELABS – OSINT FOR GOOD

<https://www.tracelabs.org/initiatives/search-party>

## Search Party

Crowdsourced OSINT to Find Missing Persons

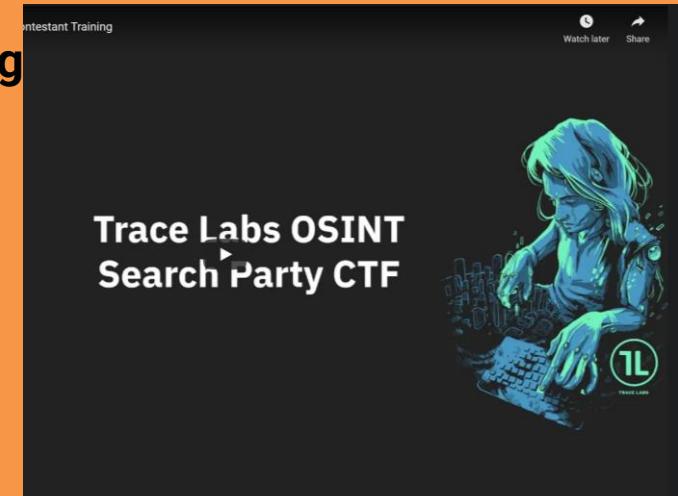
Trace Labs is designed to be a catalyst for improving the state of missing persons location and family reunification. We provide a modern, cost effective and transparent solution to a problem that is destroying families.

[Learn More](#)



## Trace Labs OSINT Search Party CTF Contestant Training

<https://www.youtube.com/watch?v=f526PYm6cqU&t=4s>



<https://www.tracelabs.org/blog/things-youll-wish-youd-known-before-your-first-search-party-ctf>

# WHERE TO START

---



# picoCTF

[https://picoctf.org/get\\_started.html](https://picoctf.org/get_started.html)



<https://www.youtube.com/watch?v=x-qaeuw74WE&list=PL1H1sBF1VAKVTu-v1XcJV9VVdhEEALvkY>

## picoPrimer

Wonder what the shell is and how to use it? Maybe you haven't thought about cryptography in ages and need a refresh? Revisit concepts you are familiar with or read something new to you in the picoPrimer. Authored by the picoCTF education team, the picoPrimer reviews cybersecurity principles used in our competition challenges. You do not need any additional software to read the picoPrimer or solve the challenges at the end of each chapter.

[Start picoPrimer](#)

## picoGym

picoGym is a noncompetitive practice space where you can explore and solve challenges from previously released picoCTF competitions, find fresh never before revealed challenges, and build a knowledge base of cybersecurity skills in a safe environment.

Whether you are a cybersecurity professional, competitive hacker or new to CTFs you will find interesting challenges in the picoGym that you can solve at your own pace. Team picoCTF will regularly update this challenge repository so visit the picoGym often.

[Practice in the picoGym](#)

# GETTING STARTED AT PICO

GET STARTED

## Practice



Practice your skills with challenges from previous competitions in the picoGym. Most problems from each competition will be added to the picoGym when the competition finishes.

GET STARTED

## Compete



You must register for each competition with updated information to play new challenges and be eligible for prizes. Most competitions will have classroom and team features.

GET STARTED

## Webshell



Use our webshell to access various tools to solve challenges in Linux, right from your browser. [Read more about the shell.](#)

picoCTF Webshell

```
Enter your picoCTF username: piranhamama
Enter your picoCTF password (characters will be hidden):
=====
Welcome to the picoCTF webshell!

 The webshell is intended only for solving picoCTF challenges. Any other usage is a violation of our terms and conditions.

 Sessions are monitored and logged to prevent abuse. Please do not enter any sensitive information into the webshell.

 Files stored outside of your home directory will not persist between webshell sessions.

 Network connectivity and resources are limited. Some limits can be checked by typing `usage`.

 Idle sessions will automatically log out after 15 minutes.

 For more information and a beginner's guide, type `less ~/README.txt`
```

piranhamama-picoctf@webshell:~\$ █

# GETTING STARTED AT PICO

picoCTF Learn Practice Compete piranhamama picoGym Practice Challenges picoGym Score: 0

Filters

Hide Solved

Search by Name

Category Filter

All Categories

- Web Exploitation
- Cryptography
- Reverse Engineering
- Forensics
- General Skills
- Binary Exploitation

First Appearance

Any

- picoMini by redpwn
- picoCTF 2021
- picoCTF 2020 Mini-Competition
- picoCTF 2019
- picoCTF 2018

picoGym Practice Challenges

1 2 3 4 5 6 7 > »

General Skills	Cryptography	General Skills
Obedient Cat	Mod 26	Python Wrangling
18,976 solves	17,003 solves	9,832 solves
87%	92%	60%
General Skills	Forensics	General Skills
Wave a flag	information	Nice netcat...
12,215 solves	6,334 solves	10,480 solves
91%	37%	92%
Reverse Engineering	Binary Exploitation	Web Exploitation
Transformation	Stonks	GET aHEAD
3,396 solves	1,701 solves	5,168 solves
56%	63%	76%
Cryptography	General Skills	General Skills
Mind your Ps and Qs	Static ain't always noise	Tab, Tab, Attack
2,378 solves	6,792 solves	6,936 solves
64%	90%	81%

1 2 3 4 5 6 7 > »



<https://www.facebook.com/picoctf.competition>

<https://twitter.com/picoctf>

<https://discord.com/invite/WQGdYaB>

---

# NATIONAL CYBERSECURITY COMPETITIONS

---



The screenshot displays the National Cyber League platform interface. On the left, a sidebar titled "Modules Overview" lists ten modules with their respective icons, challenge counts, question counts, and completion percentages. The modules are:

- Open Source Intelligence**: 10 challenges, 10 questions, 0% completion.
- Cryptography**: 10 challenges, 10 questions, 0% completion.
- Password Cracking**: 10 challenges, 10 questions, 0% completion.
- Log Analysis**: 10 challenges, 10 questions, 0% completion.
- Network Traffic Analysis**: 10 challenges, 10 questions, 0% completion.
- Wireless Access Exploitation**: 10 challenges, 10 questions, 0% completion.
- Forensics**: 10 challenges, 10 questions, 0% completion.
- Scanning**: 10 challenges, 10 questions, 0% completion.
- Web Application Exploitation**: 10 challenges, 10 questions, 0% completion.
- Enumeration & Exploitation**: 10 challenges, 10 questions, 0% completion.

The main area shows a user profile for "PiranhaMania" with a score of 0 points out of 6325, 0% accuracy, and 0% completion. It also features a "Skills Tracker" section with a circular radar chart showing completion levels for each module. The chart has segments for Open Source Intelligence, Cryptography, Password Cracking, Log Analysis, Network Traffic Analysis, Wireless Access Exploitation, Forensics, Scanning, Web Application Exploitation, and Enumeration & Exploitation. The chart is currently at the center, indicating no completion.



## NATIONAL CYBER LEAGUE – INSIDE THE GYMNASIUM



Open Source Intelligence	
Meta (Easy)	0 / 6
Lookup (Easy)	0 / 3
Threat Intel (Easy)	0 / 6
30 ATTEMPTS	
HTTP (Easy)	0 / 3
SSL (Medium)	0 / 3
Barcode (Medium)	0 / 2

Click to Reveal Solution Guide



**CYBER SKYLINE**  
© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.



Meta (Easy) (120 points)

#### Cyber Command

Test your abilities to extract metadata.

7:58:20 pm

Q1 - 20 points

When was the image created? Round down to the nearest minute

Answer...

Q2 - 20 points

What are the dimensions of the image? (ex: 800x600)

Answer...

Q3 - 20 points

What is the make of the camera that took the picture?

Answer...

Q4 - 20 points

What is the model of the camera that took the picture?

Answer...

Q5 - 20 points

What is the exposure time for the picture? (ex: 1/200)

Answer...

NATIONAL CYBER LEAGUE –  
INSIDE THE GYMNASIUM

# NCL SCOUTING REPORT

<https://nationalcyberleague.org/scoutingreport>

 POWERED BY 

The National Cyber League  
Where Cybersecurity is a Passion

Student Player  
student@nationalcyberleague.org

## NCL Scouting Report

What follows is a customized NCL Scouting Report of your performance in the NCL Individual Game. We hope you find it to be valuable in both confirming your skills and identifying areas for improvement. In addition, the NCL Scouting Report can be used as part of any job application, as it provides an external validation of skills as demonstrated in competitive gameplay based on industry-recognized certification exam and framework objectives.

The following definitions apply to your performance across a range of cybersecurity scenarios

- **National Rank:** overall place with respect to all players, across all Brackets
- **Bracket Rank:** overall place within the Bracket
- **Performance Score:** total points earned; the higher the score, the higher the ranking
- **Accuracy:** percentage of flag submissions that were correct (total flag captures divided by total flag attempts).
- **Completion:** percentage of possible flags submitted (total flag captures divided by total possible flags).

The following are the categories of cybersecurity scenarios that you were evaluated against:

1. **Cryptography**  
Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.
2. **Enumeration and Exploitation**  
Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.
3. **Log Analysis**  
Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
4. **Network Traffic Analysis**  
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.
5. **Open Source Intelligence**  
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
6. **Password Cracking**  
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.
7. **Scanning**  
Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
8. **Web Application Exploitation**  
Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
9. **Wireless Access Exploitation**  
Identify the security posture of wireless networks from network captures.

## NCL Preseason

2 <sup>ND</sup> PLACE OUT OF 5379 NATIONAL RANK	1760 POINTS OUT OF 1760 PERFORMANCE SCORE	 96.1% ACCURACY	 100.0% COMPLETION
100 <sup>th</sup> National Percentile	Averages National: 621.6	National: 59.7%	National: 49.0%

Based on Preseason performance, **Student Player** was placed into the **Gold Bracket** for the Individual Game.

2 | Learn more at [nationalcyberleague.org](https://nationalcyberleague.org) | Verify this report at [cyberskyline.com/report/SAMPLE](https://cyberskyline.com/report/SAMPLE)

 POWERED BY 

 POWERED BY 

The National Cyber League  
Where Cybersecurity is a Passion

Student Player  
student@nationalcyberleague.org

## NCL Individual Game

The NCL Individual Game is designed for student players nationwide to compete in realtime in the categories listed below. The Individual Game evaluates the technical cybersecurity skills of the individual, without the assistance of others.

10 <sup>TH</sup> PLACE OUT OF 5357 NATIONAL RANK	9 <sup>TH</sup> PLACE OUT OF 639 GOLD BRACKET RANK	2810 POINTS OUT OF 3000 PERFORMANCE SCORE	 95.6% ACCURACY	 97.4% COMPLETION
100 <sup>th</sup> National Percentile	99 <sup>th</sup> Gold Bracket Percentile	Averages National: 838.6 Gold Bracket: 1619.5	National: 65.6% Gold Bracket: 77.1%	National: 37.9% Gold Bracket: 66.4%
Cryptography		390 POINTS OUT OF 390	100.0% ACCURACY	COMPLETION:  100.0%
Enumeration and Exploitation		350 POINTS OUT OF 350	92.3% ACCURACY	COMPLETION:  100.0%
Log Analysis		400 POINTS OUT OF 400	100.0% ACCURACY	COMPLETION:  100.0%
Network Traffic Analysis		350 POINTS OUT OF 350	95.8% ACCURACY	COMPLETION:  100.0%
Open Source Intelligence		260 POINTS OUT OF 260	95.5% ACCURACY	COMPLETION:  100.0%
Password Cracking		255 POINTS OUT OF 255	100.0% ACCURACY	COMPLETION:  89.5%
Scanning		200 POINTS OUT OF 250	90.9% ACCURACY	COMPLETION:  90.9%
Web Application Exploitation		350 POINTS OUT OF 350	100.0% ACCURACY	COMPLETION:  100.0%
Wireless Access Exploitation		155 POINTS OUT OF 205	80.0% ACCURACY	COMPLETION:  92.3%

Note: Survey module (100 points) was excluded from this report.

3 | Learn more at [nationalcyberleague.org](https://nationalcyberleague.org) | Verify this report at [cyberskyline.com/report/SAMPLE](https://cyberskyline.com/report/SAMPLE)

 POWERED BY 

<https://static1.squarespace.com/static/5e13a4b584a68c775e362068/t/5f3c5888533a540ce85da2c0/1597790354053/NEW+Spring+2020+Sample+Scouting+Report.pdf>

# WHERE TO FIND OUT MORE ABOUT NCL

**CryptoKait**  
Home of the National Cyber League Player Ambassadors

CRYPTOKAIT · BLOG · INITIATIVES · NATIONAL CYBER LEAGUE · PERSONAL DEVELOPMENT · CYBERSEC CLUBS · CYBERSEC BOOTCAMPS

Welcome

On This Page – Jump to:  
[CryptoKait](#) • [Initiatives](#) • [NCL](#) • [Personal Development](#) • [CS Clubs](#) • [CS Bootcamps](#)

---

**CryptoKait**

[About CryptoKait](#)    [Workshops & Appearances](#)    [Contact](#)

*CryptoKait's Most Recent Blog Posts*

CYBERSECURITY CLUB SURVIVAL GUIDE

BLOG CATEGORY: CYBERSECURITY CLUBS

COLLABORATION TIPS

VORITE NCL PA -



- FOLLOW -

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,680 other followers

Enter your email address

**FOLLOW**

- YOUR FAVORITE AUTHORS -

 **Ox6OODFOOD**

How to Support Student Organizations

Helping Students During the Games

<https://cryptokait.com/>

**Cost:**  
**\$35 per person  
each semester.**

# **UPPING YOUR GAME – PROFESSIONAL DEVELOPMENT**

---

# BLUE TEAM

In a Blue Team CTF platform, you attempt to harden systems to prevent compromises to find flags.



RangeForce

11h ·

...

📣 The Persistence Challenge is officially live!

Login to the Community Edition between now and August 8 to participate in three exclusive cybersecurity challenges:

- Level One: Malicious Remote IPs
- Level Two: Compromised Accounts
- Level Three: Advanced Persistence

Do you have what it takes to defend against these threats? Prove your skills for a chance to earn prizes.

Ready to get started? If you're not yet a member of our Community Edition, sign up for free here: <https://hubs.la/H0R314f0>

Introducing the RangeForce Community SOC

Join the Community Edition today to:

- 🛡️ Hone your skills with red and blue team training
- 🛡️ Take part in regular cybersecurity challenges
- 🛡️ See NMap, Splunk, Wireshark, and more in action
- 🛡️ Claim your first RangeForce Badge when you complete 10 core modules



Participate in the Persistence Challenge by logging in to the RangeForce Community Edition platform between July 21st and August 8th.



SECURE CODE  
WARRIOR



Tournaments



Training ▾



Courses ▾



Assessments



Resources

## Identify Solution

Determine the correct fix from a number of different proposed solutions for the vulnerability listed below. These solutions will be full code repositories, where completely different approaches may have been taken to address the problem.

### Vulnerability Category

Injection Flaws - SQL Injection

This is the vulnerability you are trying to identify the correct solution for.

Continue

VIEW SOLUTIONS

```
form = request.form()
if form.validate():
    sql = "INSERT INTO highscore"
    sql += " (" + ", ".join(form.name.data) + ")"
    sql += " VALUES (" + ", ".join(form.name.data) + ")"

    db.session.execute(sql)
    db.session.commit()

    return redirect(url_for('index'))
```

```
return abort(400)
```

Personalize your content by sharing your preferences

Preferred development language(s) at work?

- C Basic
- C++ Basic
- Objective-C iOS SDK
- PHP Basic
- PHP Symfony
- Java Basic
- Java Spring
- Java Enterprise Edition (JSP)
- Java Enterprise Edition (JSF)
- Java Servlets
- Java Enterprise Edition API
- Java Spring API
- Java Android SDK
- JavaScript Node.js (Express)
- JavaScript Node.js API
- Python Basic
- Python Django
- Python Flask
- Python API
- C# (.NET) Basic
- C# (.NET) Web API
- C# (.NET) MVC
- C# (.NET) Web Forms
- C# (.NET) Core
- Ruby Rails
- Scala Play
- Swift iOS SDK
- Kotlin Android SDK
- Kotlin Spring API
- JavaScript Basic
- JavaScript Angular.io (2+)
- JavaScript React
- JavaScript Vue.js
- JavaScript React Native
- PL/SQL Basic
- COBOL Basic
- GO Basic
- GO API
- Pseudocode Basic
- Pseudocode Mobile
- Terraform Basic
- Ansible Basic
- Docker Basic
- CloudFormation Basic
- Kubernetes Basic
- Rust Basic
- Perl Dancer2
- PowerShell Basic
- Salesforce Apex
- TypeScript Basic
- Bash Basic
- COBOL Mainframe
- RPG Basic

SKIP FOR NOW

SAVE CHANGES

### Active Missions

- Level 1: A cyber-criminal from Botswana is attacking the `Longitude Financial` application
- Level 2: A Hacker from Niger is attacking the `Energy Blue` application
- Level 3: A cyber-criminal from Canada is attacking the `Solar Electric` application
- Level 4: A state-sponsored adversary from Mexico is attacking the `Longitude Financial` application
- Level 5: A state-sponsored adversary from China is attacking the `Energy Blue` application
- Level 6: A Hacker from Germany is attacking the `World Bank` application
- Level 7: A Hacktivist from Italy is attacking the `Hot Deals` application
- Level 8: A Hacker from France is attacking the `World Bank` application

View

View

View

View

View

View

View

View

View





New to infosec?  
**START HERE**

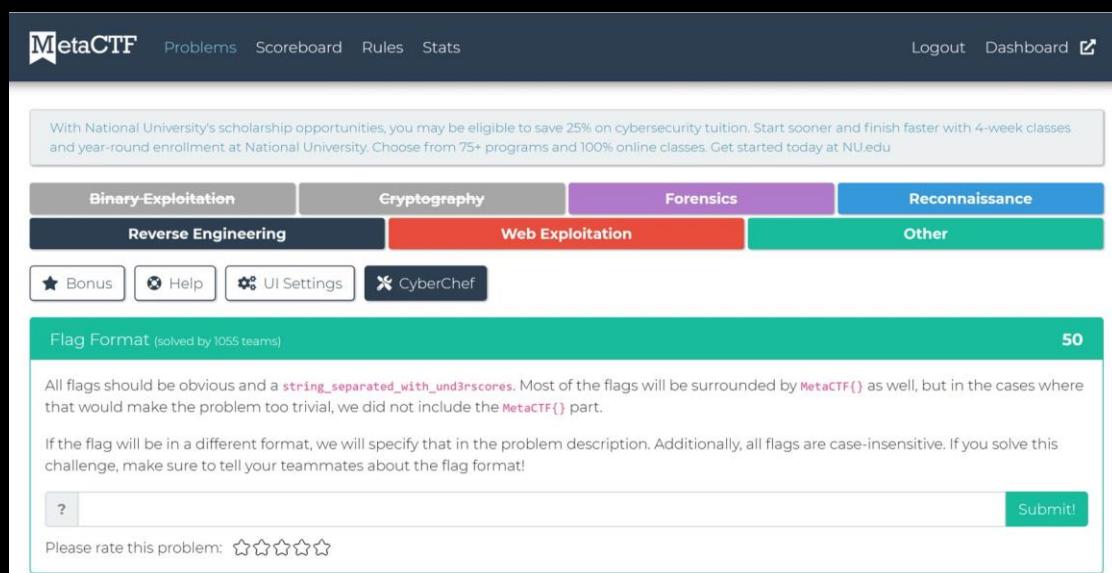


## Getting Started with Base64 Encoding and Decoding



[https://www.youtube.com/watch?v=TzG\\_ifIiig](https://www.youtube.com/watch?v=TzG_ifIiig)

# BHIS ANTISYPHON CYBER RANGE



With National University's scholarship opportunities, you may be eligible to save 25% on cybersecurity tuition. Start sooner and finish faster with 4-week classes and year-round enrollment at National University. Choose from 75+ programs and 100% online classes. Get started today at NU.edu

**Binary Exploitation**   **Cryptography**   **Forensics**   **Reconnaissance**  
**Reverse Engineering**   **Web Exploitation**   **Other**

**Bonus**   **Help**   **UI Settings**   **CyberChef**

**Flag Format** (solved by 1055 teams) **50**

All flags should be obvious and a `string_separated_with_underscores`. Most of the flags will be surrounded by `MetaCTF{}` as well, but in the cases where that would make the problem too trivial, we did not include the `MetaCTF{}` part.

If the flag will be in a different format, we will specify that in the problem description. Additionally, all flags are case-insensitive. If you solve this challenge, make sure to tell your teammates about the flag format!

Please rate this problem: 

**Submit!**

In the BHIS Antisyphon range, every question either has a very heavy hint or a direct link to a short training video, blog or webcast covering the technique needed to solve the challenge.

\$30/month

Because we have built-in tutorials and hints, many can start with little to no experience.

Currently, there are over 127 questions covering topics like Web, Recon, Pentesting, Forensics, Crypto, Reverse Engineering, and Threat Hunting. <https://www.blackhillsinfosec.com/services/cyber-range/>



## King of the Hill Beta

Be the first to hack into a machine, and then retain your presence by patching vulnerabilities to stop your foes from taking your position!

Attack then defend!

<https://tryhackme.com/games/koth>



## About

King of the Hill (KoTH) is a competitive hacking game, where you play against 10 other hackers to compromise a machine and then patch its vulnerabilities to stop other players from also gaining access. The longer you maintain your access, the more points you get.

King of the Hill is now free to play!

HACKER BUSINESS UNIVERSITY

HACKTHEBOX

Products

Resources

Company

<https://www.hackthebox.eu/>

NEW HTB Business CTF: A hacking competition for companies | £20,000 worth of prizes! >



# A Massive Hacking Playground

Cyber Training  
Gamified

Training needs to be fun. Points, badges, first blood, multiplayer battles, progress bars, "Hall of Fame" scoreboards, ranks, teams, and more!

# Hack The Box OSCP-like VMs

Curated by: TJnull at Netsec Focus

## Linux Boxes:

Lame  
brainfuck  
shocker  
bashed  
nibbles  
beep  
cronos  
nineveh  
sense  
solidstate  
kotarak  
node  
valentine  
poison  
sunday  
tartarsauce  
Irked  
Friendzone

## Windows Boxes:

legacy  
Blue  
Devel  
Optimum  
Bastard  
granny  
Arctic  
grandpa  
silo  
bounty  
jerry  
conceal

## More challenging than OSCP, but good practice:

Jeeves [Windows]  
Bart [Windows]  
Tally [Windows]  
Active [Windows]  
Jail [Linux]  
falafel [Linux]  
Devops [Linux]  
Hawk [Linux]  
Netmon [Windows]  
Lightweight [Linux]  
La Casa De Papel [Linux]



<https://pbs.twimg.com/media/ECG-gPnW4AMs32A.jpg:large>

# Vulnhub/Hackthebox OSWE-like VMs

Curated by: TJnull at Netsec Focus

## Hackthebox

### Linux Boxes:

Vault  
popcorn  
Celestial  
Blocky (Good to practice with JD-GUI)  
Falafel  
Zipper  
Unattended  
Help  
Mango [Focus on creating your own Boolean Script]

### Windows Boxes:

JSON

### More challenging than OSWE, but good practice:

Arkham  
Hackback  
Holiday

## Vulnhub

Silky-CTF: 0x02: <https://www.vulnhub.com/entry/silky-ctf-0x02,307/>  
bwapp: <https://www.vulnhub.com/series/bwapp,34/>  
Homeless 1: <https://www.vulnhub.com/entry/homeless-1,215/>  
Seattle 0.3 <https://www.vulnhub.com/entry/seattle-v03,145/>  
Ted 1: <https://www.vulnhub.com/entry/ted-1,327/>  
Raven 2: <https://www.vulnhub.com/entry/raven-2,269/>  
Potato: <https://www.vulnhub.com/entry/potato-1,529/>  
Secure Code 1: <https://www.vulnhub.com/entry/securecode-1,651/>

Flick 2: <https://www.vulnhub.com/entry/flick-2,122/>

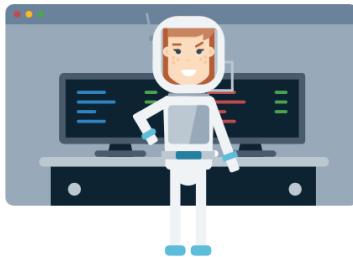


Welcome to **CyberStart Go**, your chance to experience life as a cyber security professional! You have 60 minutes to play through as many of the challenges as you can. Good luck!

Begin >

<https://go.cyberstart.com/>

# Train as you play in our immersive cyber security learning experience



## Non-traditional learning

No textbooks or lectures, just fun, online challenges that build towards highly respected academic outcomes.



## Beginner-friendly

A carefully curated syllabus, designed to gently onboard and progressively challenge you.



## Transferrable skills

We help you build a portfolio of transferrable skills recognised and desired by employers.



## Welcome message

[Read again >](#)





## Fun scenarios

You will become an agent for the virtual Cyber Protection Agency and investigate criminal gangs who are using their cyber skills to do damage online. You'll have to use various defensive tactics to thwart these cyber criminals' attempts.



## Four distinct bases

Tackle cyber-criminal gangs in HQ by solving puzzles and using cyber security skills like binary reversing, SQL Injection and XSS.

[More about the bases](#)



## Agent profile and badges

All users get their own agent profile, complete with dozens of badges to collect and share with your friends as you work your way through the challenges.



## Progressive difficulty

CyberStart features over 200 interactive security challenges ranging from simple through to extreme. The huge breadth of topics covered and easy to follow platform, helps get beginners started and fast-track those with a hidden talent.



## Progress tracking

Track your progress through CyberStart with points and badges. With over 200 hours of cyber security training material and games, it is important to visualise your learning journey.



## Helpful Field Manual

For those looking for more traditional learning support when completing the challenges, CyberStart also features an extensive 'field manual', with write-ups, video demos and interactive quizzes.

**From:** Agent J

Hello agent, I am thrilled to welcome you to the Cyber Protection Agency (CPA) – the number one place to sharpen and develop your cyber security knowledge!

At the CPA our job is to stop fearsome gangs of cyber criminals and prevent organisations from being attacked. As your mentor, it is my job to perfect your skills in a variety of security disciplines and help you progress through the agency.

As a junior agent you have access to 4 bases: the Headquarters Base, the Moon Base, the Forensics Base and the Volcano Base.

The HQ Base will see you tackle various cyber criminal gangs – gathering information about them, cracking codes, finding security flaws and dissecting their digital trail. On the Moon Base is where you'll learn to program in Python, using your own code editor to execute and run code, gradually picking up all the skills you will need to write your own programs. At the Forensics Base, you'll be working under Agent S to help tackle a variety of interesting forensics cases from all over the world. Finally, in the Volcano Base, it's time to put your training to the test. Agent J has a collection of missions for you in real environments where you can find flaws for organisations to fix and report them before the bad guys!

As you complete the challenges in each base more levels will unlock, earning you points, badges and promotions.

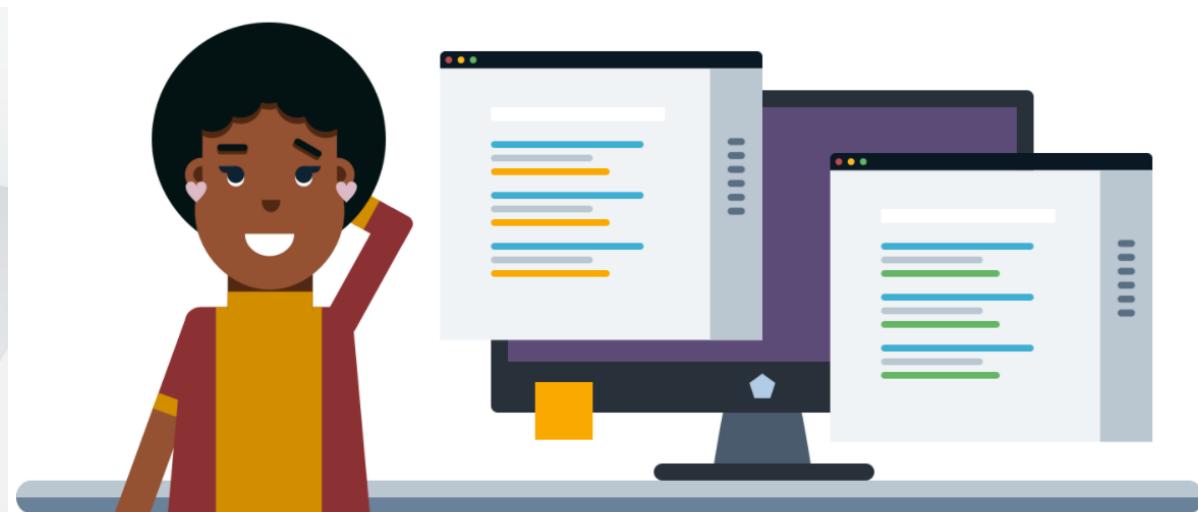
Before we let you dive in, there are a few important things that will help you to progress:

**Briefing** - When you approach each challenge take time to read the briefing; they will often help you to understand the process you should follow on a challenge.

**Flags** - When you tackle each challenge you're looking for something called a 'flag'. This is simply a code which you need to put into the box on the top left of the Toolbox on the challenge page and hit enter. If you get it right, you'll see a 'success' message and you'll be able to move on to the next challenge.

**Field manual** - On the bases page you will find a field manual. This is packed full of tips and tricks that will help with challenges. The manual covers all the basics that you need to know during your time at the CPA. Topics include Linux, programming, web attacks, cryptography and forensics.

**Hints** - At the bottom left of each challenge you'll see a link that says, 'See a hint'. If you're stuck, make sure to use these, they're a great way to keep moving.

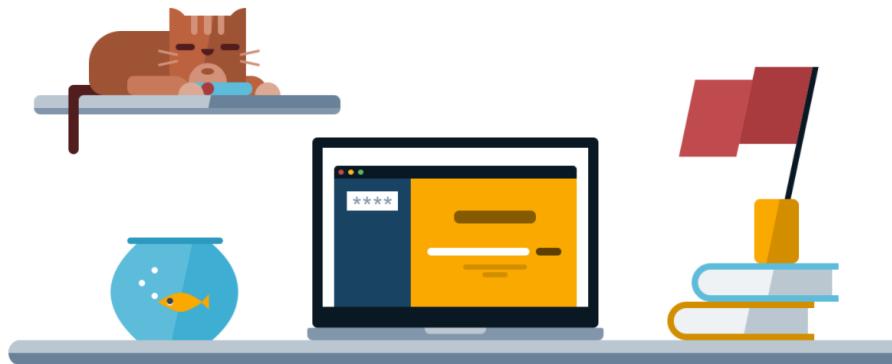


**Search engines** - It is absolutely not cheating to jump on to a search engine and try to find more information about a tool or technique. In fact, that is simply being a great security practitioner!

**Ethics** - It is important, as you develop your security skills, that you use your skills ethically and only hack the targets the game instructs you to. You should ensure you are following local laws and have written consent from the owner of a target. Just because you can hack something doesn't mean you have permission to do so! If you are unsure at any point please contact [support@joincyberstart.com](mailto:support@joincyberstart.com).

**Virtual machine** - The first five levels of CyberStart Game can be run on a modern web browser e.g the latest version of Chrome or Firefox. However, when you reach level six of the HQ, many of the challenges require you to play the game from inside a virtual machine (VM) provided by CyberStart. You can [view instructions on how to set up your VM here](#).

**Badges** - Whilst completing challenges you can also collect badges. These include the 'speedster' badge, awarded if you complete a challenge in under 30 seconds, and 'shell surfer', awarded if you can complete a challenge which uses SSH. Your badge collection can be found [on your profile page](#).



## Headquarters Base

[Play now >](#)



## Forensics Base

[Play now >](#)



## Moon Base

[Play now >](#)



## Field Manual

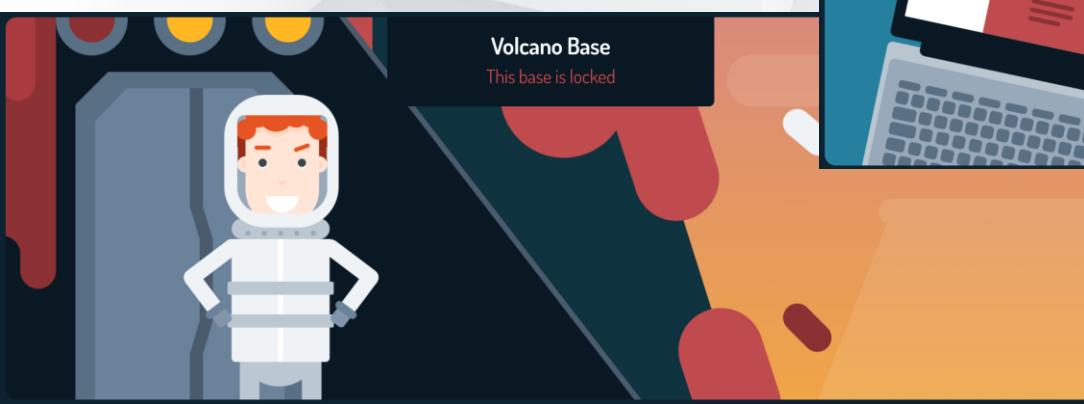
[Explore >](#)



```
100101010010100101  
1001100101010010100  
1010011001001010101  
01010001000100010111  
10011001010100101011  
101001100100101010101
```

## Volcano Base

This base is locked



Remember, the best cyber security professionals are impatient enough to try lots of things at once, patient enough to diligently figure out problems and creative enough to find new approaches to solve challenges!

Good luck agent.

Agent J

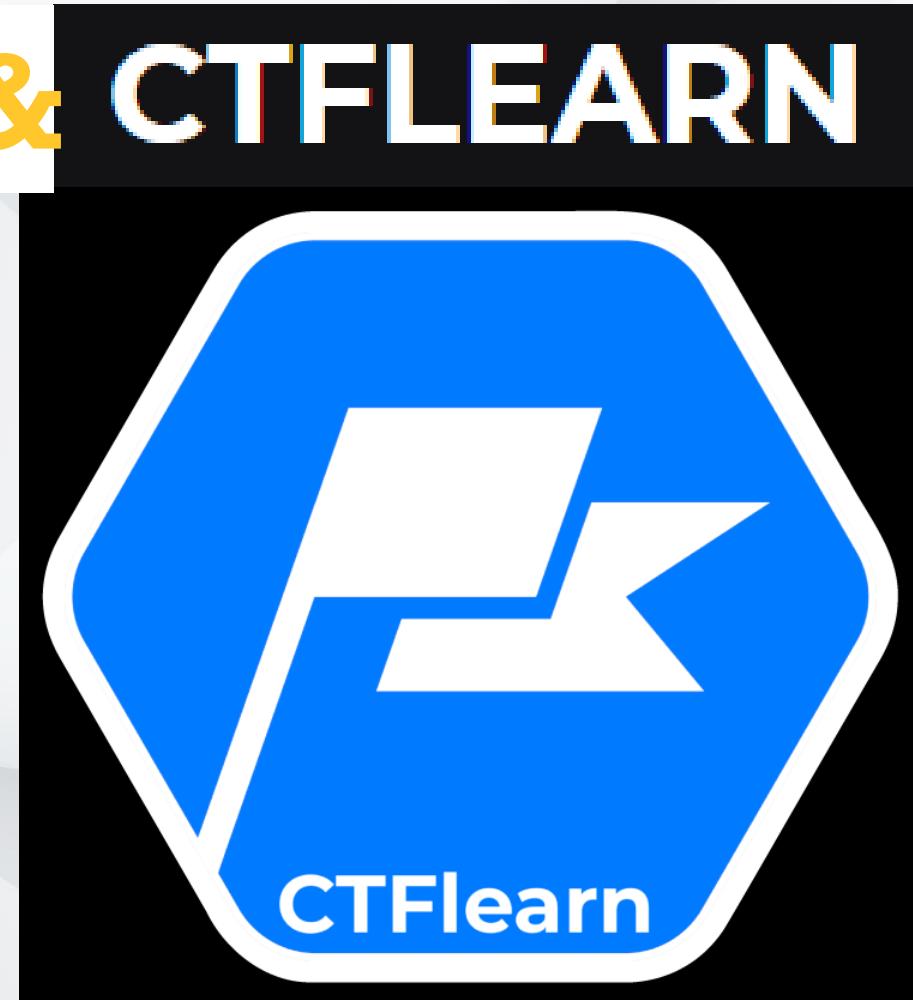
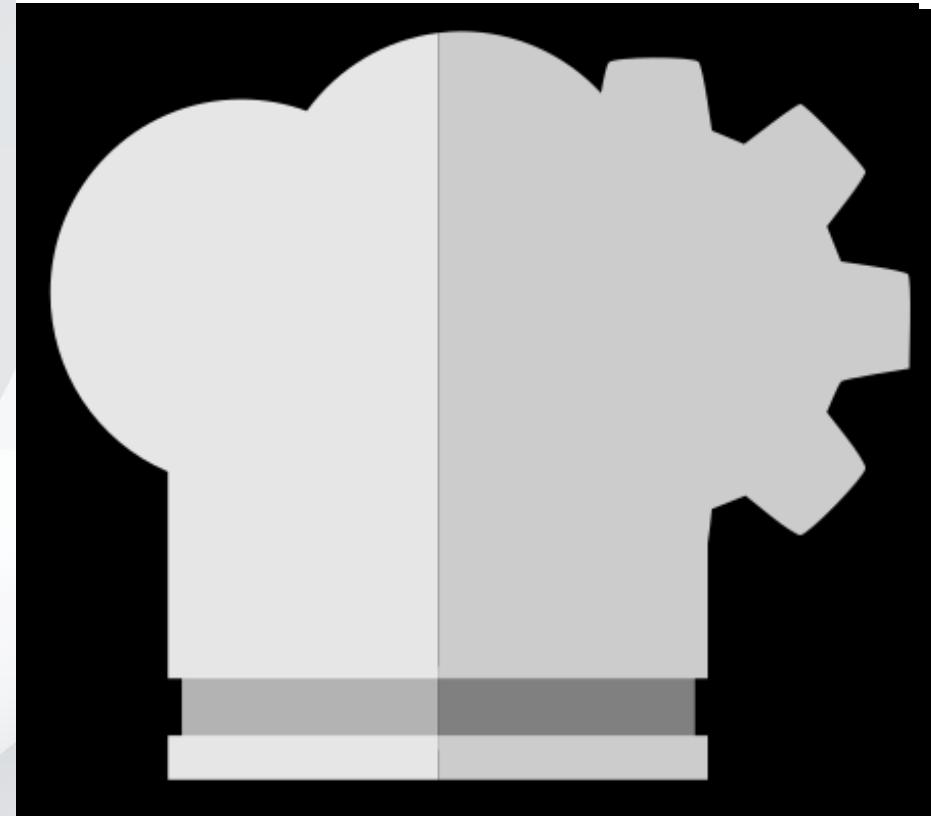
**Tokens should be valid  
for 90 days from  
activation.**



**WALK-THROUGH**

*with*

# CyberChef & CTFLEARN



# CYBERCHEF THE CYBER SWISS ARMY KNIFE

The screenshot shows the CyberChef web application interface. On the left, there is a sidebar titled "Operations" with a search bar and a "Favourites" section containing a star icon. Below this are various categories: Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking, Language, Utils, Date / Time, Extractors, Compression, Hashing, Code tidy, Forensics, and Multimedia. At the bottom of the sidebar are "STEP" and "BAKE!" buttons, along with an "Auto Bake" checkbox. The main area is divided into "Recipe" (top), "Input" (middle), and "Output" (bottom) sections. The "Input" section has file selection icons and a length/lines counter (length: 0, lines: 1). The "Output" section has a time/length counter (time: 0ms, length: 42, lines: 1) and file selection icons. The top right of the interface includes "Options", "About / Support", and a question mark icon.

<https://gchq.github.io/CyberChef/>

# CTF TOOLS

- <https://gchq.github.io/CyberChef/>
- <https://cryptii.com/>
- <http://rumkin.com/tools/cipher/>
- <https://www.dcode.fr/cipher-identifiery>
- <https://futureboy.us/stegano/decinput.html>
- <https://stylesuxx.github.io/steganography/>
- <http://diit.sourceforge.net/Hash Analyzer>
- <https://www.tunnelsup.com/hash-analyzer/ketnalysis>
- <https://www.wireshark.org/>

# CTF TOOLS

- <https://gchq.github.io/CyberChef/>
- <https://cryptii.com/>
- <http://rumkin.com/tools/cipher/>
- <https://www.dcode.fr/cipher-identifiery>
- <https://futureboy.us/stegano/decinput.html>
- <https://stylesuxx.github.io/steganography/>
- <http://diit.sourceforge.net/Hash Analyzer>
- <https://www.tunnelsup.com/hash-analyzer/ketnalysis>
- <https://www.wireshark.org/>

## Bio

- Independent Contractor
- MUTC CyberAcademy Grad
- WiCyS Mentor
- CyberPatriot Coach
- BHIS Nerd Herder
- GenCyber Instructor



piranhamama



piranhamama#8888



peneloperozhkovacsia



@RozhkovaCSIA

#codehedgehogs



# REFERENCES & RESOURCES

## Upcoming CTF Events

<https://ctftime.org/event/list/upcoming>

## picoCTF: Carnegie Mellon University Cybersecurity Competition

### Getting Started with PICO CTF

[https://picoctf.org/get\\_started.html](https://picoctf.org/get_started.html)

John Hammond video - <https://www.youtube.com/watch?v=x-qaeuw74WE&list=PL1H1sBF1VAKVTu-v1XcJV9VVdhEEALvkY>

### PICO CTF social media accounts

<https://www.facebook.com/picoctf.competition>

<https://twitter.com/picoctf>

<https://discord.com/invite/WQGdYaB>

# REFERENCES & RESOURCES

## CTFLEARN

<https://ctflearn.com>

Write-up -- <https://deskel.github.io/ctflearn/>

## SANS CyberStart

CyberStart (paid cyber range) --

<https://hub.joincyberstart.com/entry/sign-up>

CyberStartGo - Free 60-minute instance --

<https://go.cyberstart.com/>

CyberStartAmerica - Free for High School Students --

<https://www.cyberstartamerica.org/>

CTF Unplugged: Offline Competition -

<https://dl.acm.org/doi/10.1145/3017680.3017783>

# REFERENCES & RESOURCES

**Hackathon Definition --**

<https://en.wikipedia.org/wiki/Hackathon>

**What's a CTF videos --**

[https://www.youtube.com/watch?v=c92Cnb9\\_RSc&t=66s](https://www.youtube.com/watch?v=c92Cnb9_RSc&t=66s)

<https://www.youtube.com/watch?v=bxt-JidP3bU>

**Jeopardy Style CTFs**

Malice - <https://malice.fr/en/jeopardy>

MetaCTF - <https://metactf.com/cybergames>

**SANS interactive holiday CTF**

<https://2020.kringlecon.com/>

**Red vs Blue**

**Blog Post --**

<https://medium.com/@redteamvillage/red-team-vs-blue-team-ctf-c0c0n-2019-44fc42fb46>

# REFERENCES & RESOURCES

## Red Team

Red Team Village -- <https://redteamvillage.org/>

Web App Exploitation -- <https://cmdnctrl.net/ranges>

TryHackMe -- <https://tryhackme.com/>

Hack the Box -- <https://ctf.hackthebox.eu/>

<https://alternativeto.net/software/tryhackme/>

## Blue Team

SOC cyber range -- <https://go.rangeforce.com/community-soc-challenge-ce>

Twitch channel --

<https://www.twitch.tv/blueteamvillage>

## Hack-a-thons

<https://www.rasmussen.edu/degrees/technology/blog/what-is-a-hackathon/>

<https://www.hackerearth.com/challenges/?filters=competitive%2Chiring>

# REFERENCES & RESOURCES

## National Cyber League/CyberSkyline

<https://nationalcyberleague.org/>

<https://cyberskyline.com/>

Sample Scouting Report -

<https://static1.squarespace.com/static/5e13a4b584a68c775e362068/t/5f3c5888533a540ce85da2c0/1597790354053/N/EW+Spring+2020+Sample+Scouting+Report.pdf>

NCL Ambassadors' Blog Posts - <https://cryptokait.com/>

## Hack-a-thons:

<https://www.rasmussen.edu/degrees/technology/blog/what-is-a-hackathon/>

<https://www.hackerearth.com/challenges/?filters=competitive%2Chiring>

# REFERENCES & RESOURCES

## CTF TOOLS:

Beginner's Guide -- <https://code.likeagirl.io/ctf-beginner-guide-by-a-beginner-3c86e4959fcc>

CTF Field Guide -- <https://trailofbits.github.io/ctf/>

Beginner CTF Training --

<https://sites.google.com/view/beginnercapturetheflagctf/home?authuser=0>

List of Tools -- <https://int0x33.medium.com/day-18-essential-ctf-tools-1f9af1552214>

CyberChef -- <https://gchq.github.io/CyberChef/>

Hash Analyzer -- <https://www.tunnelsup.com/hash-analyzer/>

Packet Analysis -- <https://www.wireshark.org/>

## Setting up a Virtual Machine:

Blog -- <https://hurricanelabs.com/blog/setting-up-a-virtual-machine-for-your-ctf-toolbox/>

# REFERENCES & RESOURCES

## Cryptography Tools:

[https://www.simonsingh.net/The Black Chamber/index.html](https://www.simonsingh.net/The%20Black%20Chamber/index.html)

<https://cryptii.com/>

<http://rumkin.com/tools/cipher/>

<https://www.dcode.fr/cipher-identifier>

<https://www.cryptogram.org/resource-area/cipher-types/>

<https://www.instructables.com/Best-Codes/>

<https://www.instructables.com/Best-Codes-2/>

## Steganography Tools:

<https://futureboy.us/stegano/decinput.html>

<https://stylesuxx.github.io/steganography/>

<http://diit.sourceforge.net/>

# REFERENCES & RESOURCES

## OSCP Boxes:

Blog-

[https://www.netsecfocus.com/oscsp/2021/05/06/The\\_Journey\\_to\\_Try\\_Harder- TJnull-s\\_Preparation\\_Guide\\_for\\_PEN-200\\_PWK\\_OSCP\\_2.0.html#vulnerable-machines](https://www.netsecfocus.com/oscsp/2021/05/06/The_Journey_to_Try_Harder- TJnull-s_Preparation_Guide_for_PEN-200_PWK_OSCP_2.0.html#vulnerable-machines)

Spreadsheet OSCP and OSWE-

<https://docs.google.com/spreadsheets/d/1dwSMIAPlam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=0>

OSCP List-

<https://pbs.twimg.com/media/ECG-gPnW4AMs32A.jpg:large>