



HACK
A-SAT 4

CTF
FINALS

mhackeroni @ DEFCON 31 CTF & Hack-A-Sat 4 - Forum Cyber 4.0

Who am I?



Marco Festa - @marcof_92 - marco.festas@gmail.com

Computer Science and Engineering @ Politecnico di Milano.

Capturing flags with TowerOfHanoi since 2014

Red Team @ Intesa Sanpaolo - 2018

Security Researcher @ CrowdStrike since - 2021

Founder @ mhackeroni - 2018

What is a **CTF**?

Capture The Flag

IT security-oriented competition

Try to break into **applications / systems**

... to get flags: **flag{this_is_a_secret}**

What is a jeopardy CTF?



What is a jeopardy CTF?

The screenshot shows a Jeopardy CTF interface for 'CAPTURE THE FLAG'. At the top, there are navigation links: Teams, Scoreboard, Challenges, CAPTURE THE FLAG (logo), Beginners Quest, README, and Logout [mHACHeroni]. The main area is divided into six categories: CRYPTO, MISC, PUJN, RE, and WEB. Each category contains a list of challenges with their respective point values and solve counts. Some challenges are highlighted in green, indicating they have been solved.

Category	Challenge Name	Points	Solves
CRYPTO	BETTER ZIP	231pt	38 solves
	DM COLLISION	176pt	63 solves
	DOGESTORE	267pt	27 solves
	MITM	243pt	34 solves
	PERFECT SECREC4	158pt	74 solves
MISC	BOOKSHELF	363pt	10 solves
	FEEL IT	208pt	47 solves
	PHRACK	420pt	5 solves
	TAPE	355pt	11 solves
	WIRED CSV	220pt	42 solves
PUJN	DRIVE	500pt	0 solves
	EXECVE SANDBOX	283pt	23 solves
	APT42 - PART 2	420pt	5 solves
	SANDBOX COMPAT	420pt	5 solves
	SFTP	181pt	60 solves
RE	SHALL WE PLAY A GAME?	113pt	113 solves
	BACK TO THE BASICS	293pt	
WEB	BBS	453pt	3 solves
	CAT CHAT	210pt	

What is a jeopardy CTF?



What is a jeopardy CTF?

The screenshot displays a CTF competition interface with a central challenge window. The challenge is titled "EXECVE SANDBOX" and is worth 283 points. The description asks for a command to execute `./flag` in a sandbox. The solution is `$ nc execve-sandbox.ctfcompetition.com 1337`. The interface also shows a scoreboard with various other challenges and their scores.

Challenge Name	Points	Solves
BETTER ZIP	500pt	0 solves
DM COLLISION	283pt	23 solves
DOGESTORE	420pt	5 solves
MITM	420pt	5 solves
PERFECT SECREC4	181pt	60 solves
SHALL WE PLAY A GAME?	113pt	11 solves
BACK TO THE BASICS	293pt	
BBS	453pt	3 solves
CAT CHAT	210pt	

What is a jeopardy CTF?

Teams

Scoreboard

Challenges

CAPTURE
the FLAG

Beginners Quest

README

Logout [mHACHeroni]

SCOREBOARD

Top 10 Teams



Where is a CTF? ctftime.org

CTF TIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About Timezone: Europe/Rome marcof

Team rating

2024 2023 2022 2021 2020 2019 2018 2017 2016 2015
2014 2013 2012 2011

Place	Team	Country	Rating
1	kalmarunionen		1124,250
2	The Flat Network Society		722,025
3	thehackerscrew		659,020
4	r3kapig		603,746
5	bi0s		516,885
6	Project Sekai		493,283
7	organizers		463,230
8	Blue Water		460,385
9	Never Stop Exploiting		426,750
10	CyberSpace		393,901

[Full rating](#) | [Rating formula](#)

Upcoming events

Open

Format	Name	Date	Duration
	Akasec CTF 2024 On-line	ven, Glu. 07, 15:37 — dom, Glu. 09, 15:37 CEST	2d 0h 100 teams
	BCACTF 5.0 On-line	ven, Glu. 07, 22:00 — lun, Glu. 10, 22:00 CEST	3d 0h 58 teams
	ESAJIP CTF 2024 Angers and Aix-en-Provence, France	ven, Glu. 07, 23:00 — sab, Glu. 08, 10:00 CEST	11h 0 teams

Past events

With scoreboard All

N0PSctf

Glu. 02, 2024 22:00 CEST | On-line | [Weight voting in progress](#)

Place	Team	Country	Points *
1	PwnSec		0,000
2	UofCTCF		0,000
3	Thread in the Needle		0,000

[629 teams total](#) | [Tasks and writeups](#)

DASCTF X HDCTF 2024 Open Competition

Glu. 02, 2024 20:00 CEST | On-line | [Weight voting in progress](#)

Place	Team	Country	Points *
1	SanDiego		0,000
2	荳蔻口地春天等待价		0,000
3	混个参与奖OVO		0,000

[422 teams total](#) | [Tasks and writeups](#)

Codegate CTF 2024 Preliminary

Glu. 02, 2024 03:00 CEST | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	USACyKor		73,160
2	More Smoked Leet Chicken		51,606
3	Blue Water		41,200

[215 teams total](#) | [Tasks and writeups](#)

2004

2005



.....

Tower of Hanoi (Politecnico di Milano)

- 1st at UCSB iCTF 2004
- 1st at UCSB iCTF 2005



Ethical **hacking** in Italy...

2009

2004

2005

.....

2007

2008

2009

.....

c00kies@venice

(Ca' Foscari Venezia)

- 3rd at UCSB iCTF 2010
- 3rd at RuCTFe 2017
- 2nd at RuCTF 2018



Ethical **hacking** in Italy...

2016

2004

2005

.....

2007

2008

2009

.....

2016

CTF  **TIME** Top 500 teams:

+ **JBZ**

+ **TowerOfCOokies**

(TowerOfHanoi + c00kies@venice)



Ethical **hacking** in Italy...

2017

2004

2005

.....

2007

2008

2009

.....

2016

2017

2018

CTF  **TIME** Top 500 teams:

+ TheRomanXploIt

(Sapienza)

+ Spritzers

(Università Degli Studi di Padova)



Ethical **hacking** in Italy...

2018

2004

2005

.....

2007

2008

2009

.....

2016

2017

2018



=



+



+



+



TowerOfHanoi
(Politecnico di Milano)

c00kies@venice
(Ca' Foscari Venezia)

TheRomanXpl0it
(La Sapienza Roma)

Spritzers
(Università di Padova)

Our simple goal:

Compete in the DEFCON CTF!



World's largest **hacker** convention - **Las Vegas**

> 30.000 attendees in 2018



DEFCON CTF

During the year each team tries to qualify to the greatest of all CTF

Let's qualify!

DEF CON Quals @ Politecnico di Milano, May 2018

**mHACKeroni @ DEFCON Quals
May 2018 @ NECSTLab, Milan**

Our results pre 2018 in **DEF CON CTF QUALS?**

- **2012: Tower Of Hanoi - 34th**
- **2013: Tower Of Hanoi - 53rd**
- **2014: Tower Of Hanoi - 51st**
- **2015: Tower Of Hanoi - 36th**
- **2017: Tower Of Hanoi - 30th**
- **2018: mHACKeroni - ...**

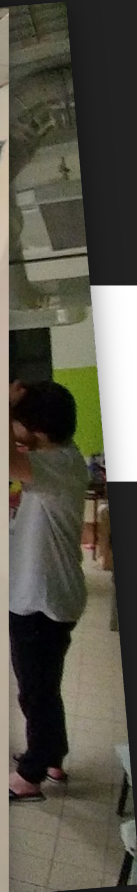
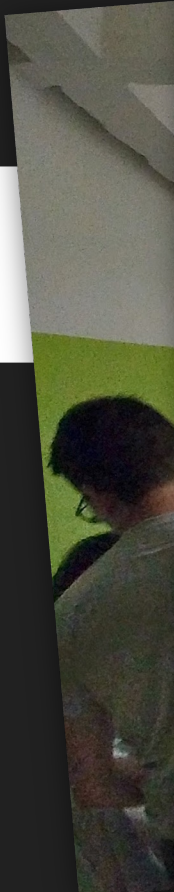




PERICOLO
RAGGI
LASER

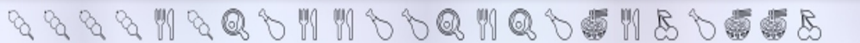




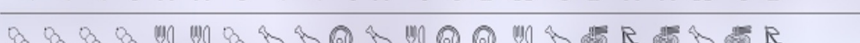
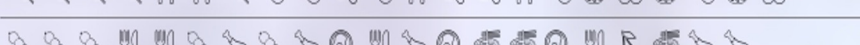
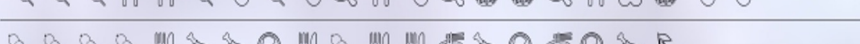
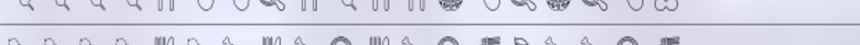


ALLARME
ANTINCENDIO





So this is the **result!**

#	Team	Ordered	Points
1	Samurai		4294
2	mhackeroni		4066
3	PPP		3909
4	Krautstrike		3815
5	RPISEC		3670
6	Tea Deliverers		3650
7	KaisHack+PLUS+GoN		3462
8	HITCON		3272
9	Shellphish		2742
10	Dragon Sector		2679

.. over 600 teams worldwide

So this is the result!

Hacker sì, ma con un'etica

Dal Politecnico a Las Vegas con i "Mhackeroni"

di SIMONA BALLATORE - MILANO -

SI CHIAMANO "Mhackeroni", sono hacker etici. Partecipano a competizioni, "giocano", ma soprattutto si allenano a combattere quegli hacker - per nulla etici - che mettono a rischio i sistemi informatici. Per farlo il Politecnico di Milano, che già aveva un suo team, ha unito le forze con le squadre di hacker della Ca' Foscari di Venezia, della Sapienza di Roma, dell'Università di Padova e con una community online: insieme hanno creato una super-squadra, i Mhackeroni, appunto. Hanno un sito - www.mhackeroni.it - e un canale Twitter. «Il nome ci è subito piaciuto», sottolineano i "Tower of Hanoi" del Politecnico. Il loro gruppo è nato nel laboratorio Nest del Dipartimento di Elettronica, Informazione e Bioingegneria guidato dal professore Stefano Zanero: sono 23, fra loro



ATTACCO E DIFESA | Mhackeroni in azione nel dipartimento Nest

ci sono dottorandi, studenti e dottorati, hanno dai 22 ai 29 anni. Si allenano settimanalmente, formano nuovi hacker etici. «Giochiamo da diversi anni - spiegano Marco Festa, Davide Quarta e Denny Zeng a nome del gruppo - Abbiamo conosciuto altre real-

tà italiane, ci siamo visti di persona e abbiamo deciso di unirli per raggiungere livelli più alti. Com'è stato fatto in Germania». E così, insieme, i Mhackeroni si sono classificati secondi - su ben 586 squadre - alle qualifiche del "DefCon Ctf", la più importante del

petizione "Capture the flag" - si chiama così - di sicurezza informatica a livello mondiale. «Un risultato storico e il miglior piazzamento mai ottenuto da una squadra italiana: è stato sorprendente l'affiatamento che si è creato», sottolineano gli universitari, pronti a volare a Las Vegas ad agosto, dal 9 al 12.

SI GIOCA, si affrontano problemi realistici in applicazioni create ad hoc dagli organizzatori. Ci saranno i migliori team a Las Vegas. Cercheranno di esserci tutti e 35. «L'invito ufficiale è per otto persone - sottolineano - ma come succede alle altre squadre in massa vorremmo partecipare in massa. Stiamo raccogliendo fondi per portare tutti. Cerchiamo sponsor». E alleati nella guerra per la sicurezza informatica. Più cervelli ci sono più aumenta la possibilità di vincere. «È la conferenza sulla sicurezza informatica più im-

Fra gare e lezioni

È più di un gioco
Alleniamo i giovani
a difendere siti
per garantire
la sicurezza informatica



Il gruppo Tower of Hanoi del Politecnico di Milano si è unito alla Ca' Foscari all'università di Padova e alla Sapienza

#	Team
1	Samurai
2	mhackeroni
3	PPP
4	Krautstrike
5	RPISEC
6	Tea Deliverers
7	KaisHack+PLUS+GoN
8	HITCON
9	Shellphish
10	Dragon Sector

	Points
	4294
	4066
	3909
	3815
	3670
	3650
	3462
	3272
	2742
	2679

© SPOREGIOVE RISERVATA

So this is the result!

VEGAS HERE WE COME!



#	Team
1	Samurai
2	mhackeroni
3	PPP
4	Krautstrike
5	RPISEC
6	Tea Deliverers
7	KaisHack+PLUS+GoN
8	HITCON
9	Shellphish
10	Dragon Sector

	Points
	4294
	4066
	3909
	3815
	3670
	3650
	3462
	3272
	2742
	2679

laborio Nestor...
Elettronica, Informazione e Bio-
ingegneria guidato dal professore
Stefano Zanero: sono 23, fra loro
Denny Zeng a...
- Abbiamo conosciuto altre real...

inuno
diverse
dedica-
spaziera
dagli at-
sono di-
li scenari
è quella
i team ha
gere, deve
endersi. Si
passato era
il voto tele-
e di Trump-
e di sicurez-
zio per testa-
a. Conoscere
ico per com-
e durante le
siano "talent
o aziende che
dell'ateneo per
la sicurezza del
vitare falle. Ol-
e c'è di più: es-
è una missione.
ossessione.
© INFOPOLICE RISERVATA

mhackeroni in 2023?

- **A group of friends who still plays CTFs while developing their career in the Infosec world**
- **Promoting Information Security culture and spreading passion to new students and enthusiasts**
- **New friends joined us** ABOUT: BLANKETS
- **Since 2023 CERTIFIED SATELLITE HACKERS** 

Hack-A-Sat ?

- **First CTF style hacking competition with space security in mind**
- **4 year project by the Department of the Air Force U.S.A.**
- **Remote qualification round + on site finals during DEFCON**
- **Hacking a real satellite ??**

HACK-A-SAT

Qualification rounds 2023

HACK
A-SAT 4



CTF
FINALS



1. Krautsat

2. mhackeroni

3. SpaceBitsRUs

4. Poland Can Into Space

5. jmp fs: [rcx]

6. DiceGang

7. WeltALLES!

8. if this doesn't work we'll get more for next year



Place

Team name

Score

Time of Last Solution

1	Blue Water	3753.0	2023-05-28 19:13:50 UTC
2	The Parliament of Ducks	3499.0	2023-05-28 21:22:55 UTC
3	orgakraut	3466.0	2023-05-28 23:48:11 UTC
4	SuperDiceCode	3398.0	2023-05-28 23:37:32 UTC
5	TWN48	3236.0	2023-05-28 22:41:55 UTC
6	Straw Hat	3204.0	2023-05-28 22:25:51 UTC
7	Norsecode'23	3090.0	2023-05-28 23:54:24 UTC
8	mhackeroni	2920.0	2023-05-28 22:32:12 UTC
9	P1G BuT S4D	2745.0	2023-05-28 23:48:49 UTC
10	Shellphish	2500.0	2023-05-28 23:52:24 UTC

DEFCON CTF & Hack-A-Sat 4 **FINALS**

Las Vegas, 11th - 13th August 2023

2 simultaneous CTFs Finals 🤖

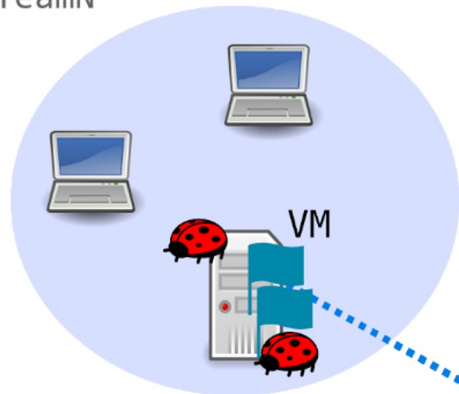
Game Rules: **DEFCON CTF**

- **Attack and defence CTF**
 - **GOTO next_slide**
- **King Of The Hill challenges**
 - **Each team submits an optimal solution for the problem**
 - **The first X teams gets point**
 - **Every turn teams can submit new solution the climb rankings**
- **Live CTF**
 - **1vs1 speed hacking contest**

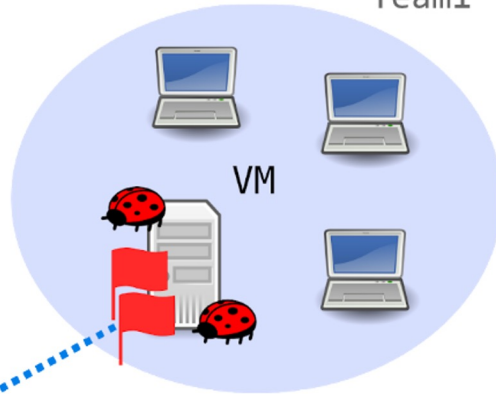
What is an **Attack & Defense** CTF?

- **In an A&D CTF, teams are each given the same set of vulnerable server software.**
- **Within the game network, teams will launch attacks against each others servers hoping to exploit the vulnerabilities they've found.**
- **Teams will need to properly patch their software so that it is protected against these exploits and functions normally.**
- **Teams receive points for extracting flags, properly defending their flags, and keeping their servers operating normally.**

TeamN



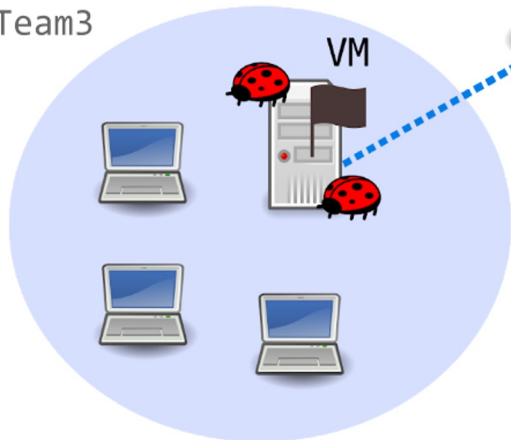
Team1



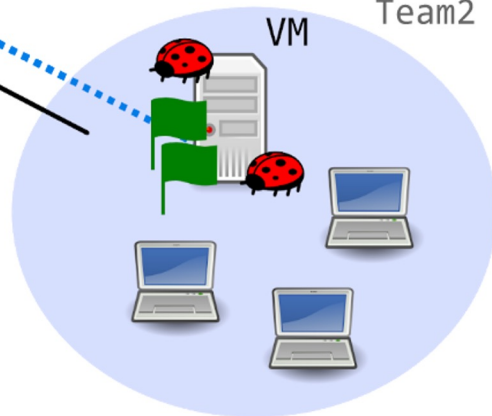
Checksystem



Team3

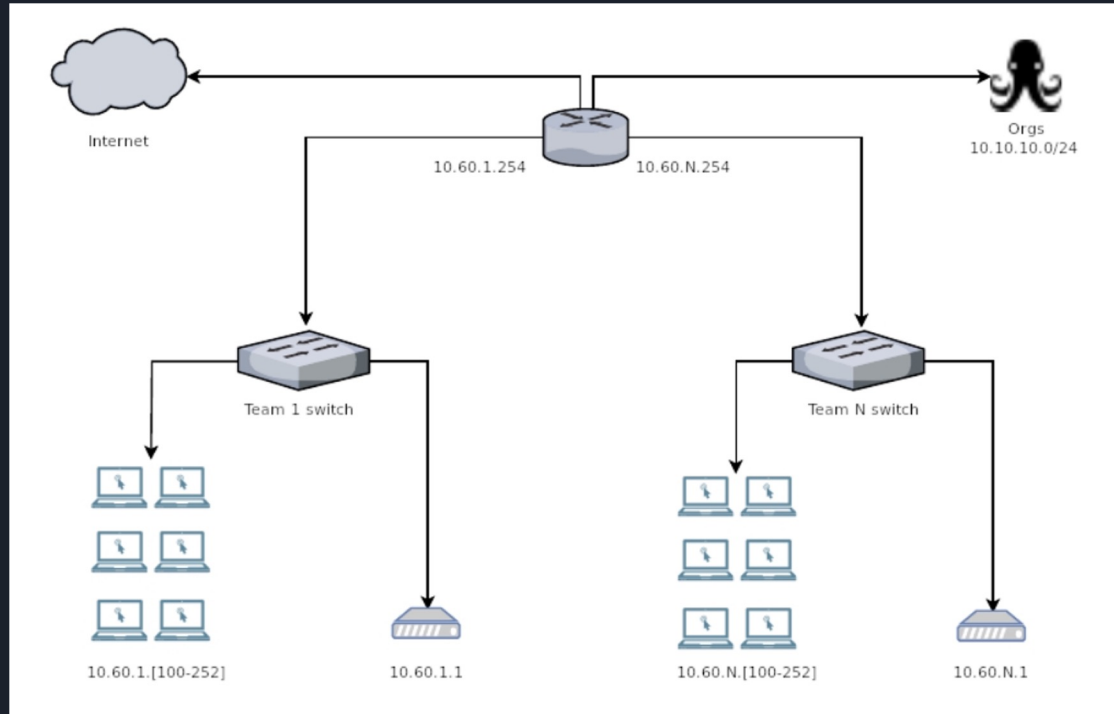


Team2



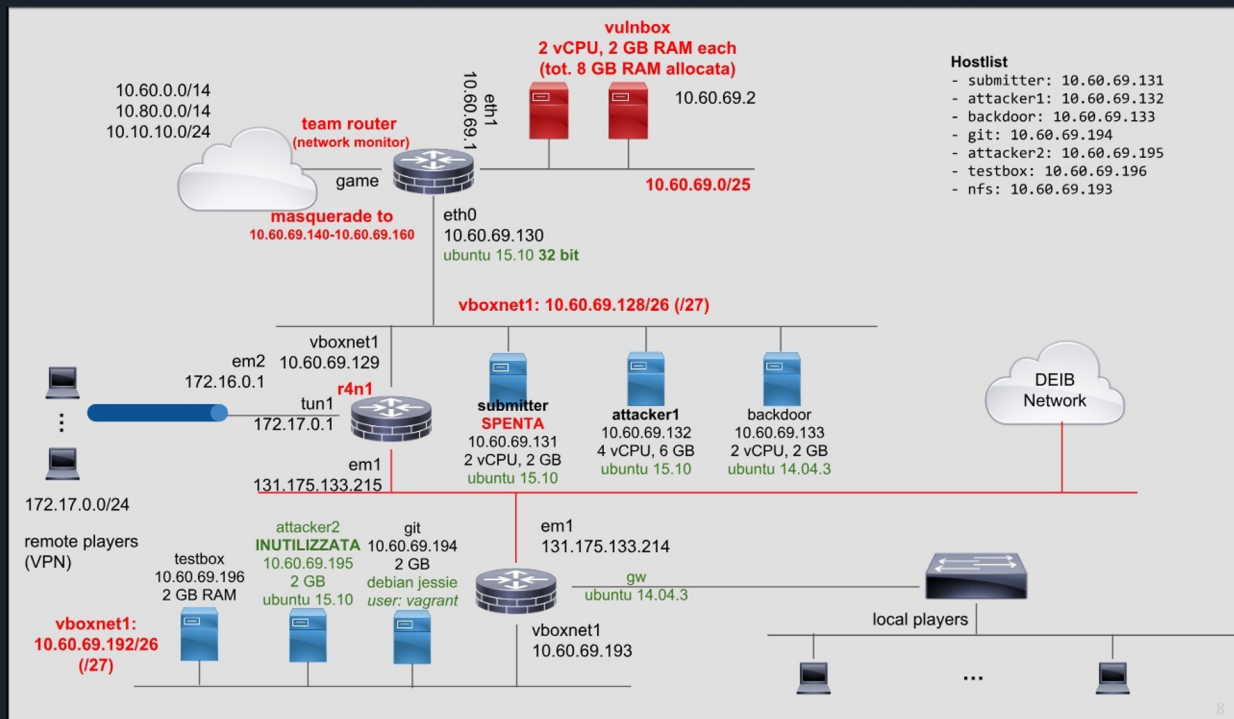
What is an **Attack & Defense** CTF?

- **Organizers network diagram**



What is an **Attack & Defense** CTF?

- Ours



What is an **Attack & Defense** CTF?

- **RuCTF T-1**

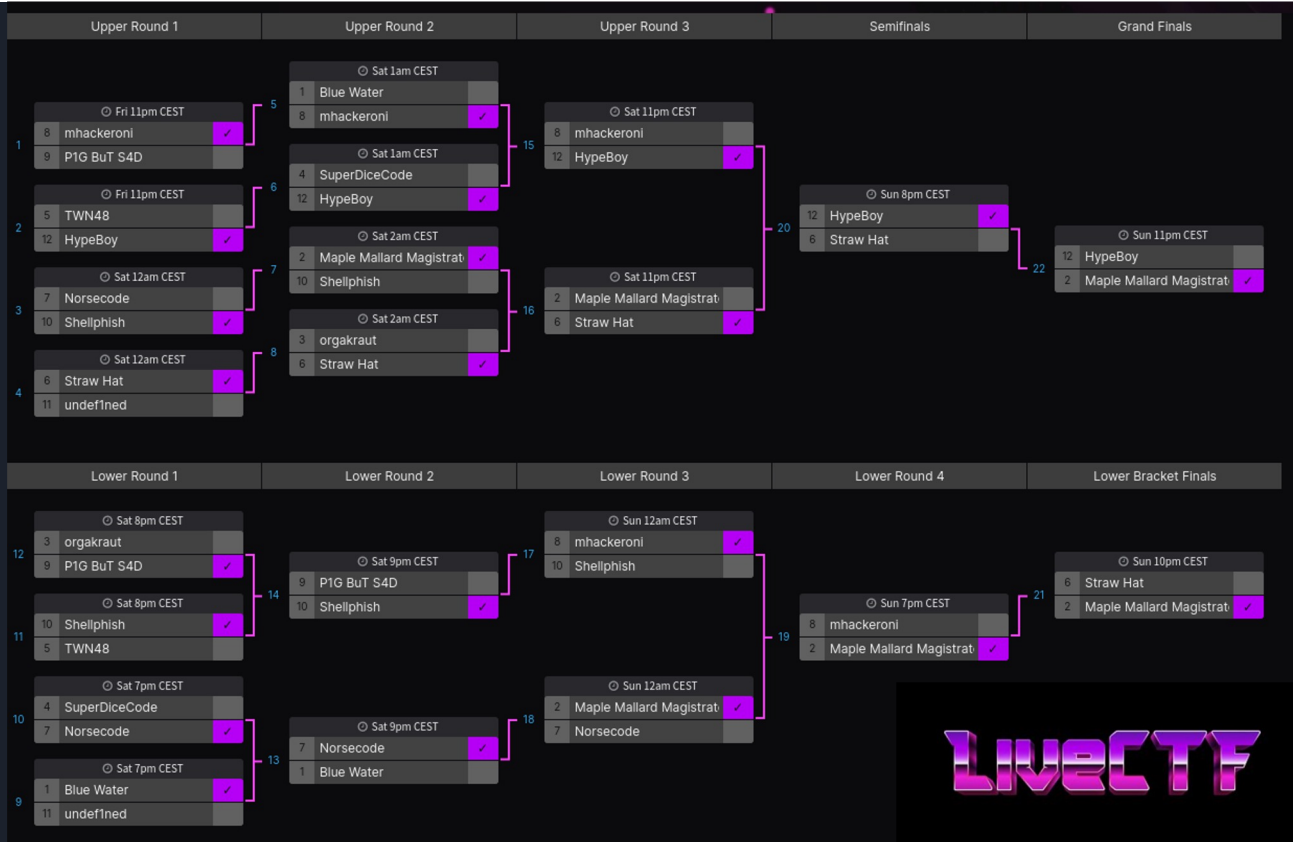


What is an **Attack & Defense** CTF?

- **RuCTF Arena**



DEFCON CTF challenges: LIVE CTF



LIVECTF

CTF FINALS

How do we fly 60+ people to Vegas?

Winning prizes from other CTFs...

RCTF 2018:

3rd Place



W CTF 2018:

2nd Place



Google CTF 2018:

19th Place



How do we fly 60+ people to Vegas?

... but, above all, thanks to our sponsors & supporters!



BV'TECH



NOZOMI
NETWORKS



POLITECNICO
MILANO 1863

rev.ng



Politecnico
di Torino



CYBERSECURITY
NATIONAL LAB

mhackeroni arrives in Vegas



**Or Venice ??? We are
a bit confused..**



Our main **concerns** & **planning**

1. Team structure and organization
2. Internet connectivity & Network
3. Hardware
4. Tools

1. Team structure and organization

Arena



Suite




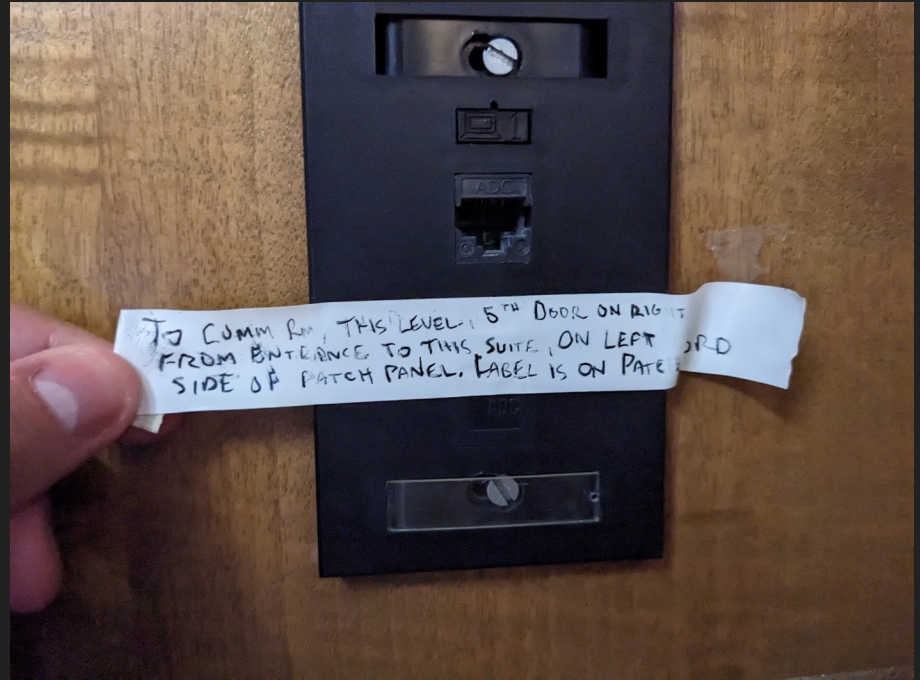
2. Internet connectivity & Network: uplink

- Hotel LAN
- LTE Sim Cards & Antennas
- Radio Bridge to another hotel
 - Bellagio?



2. Internet connectivity & Network: uplink

- Hotel LAN  (we got lucky)
- ~~LTE Sim Cards & Antennas~~
- ~~Radio Bridge to another hotel~~
 - ~~Bellagio?~~



2. Internet connectivity & Network: local network

Network layout

- VPN router (on AWS) to connect all the subnetworks we defined
- 4 fiber-connected switches (in red)
- 3 wifi AP (in green)
- Ironman + multiple mini PCs (in fuchsia)



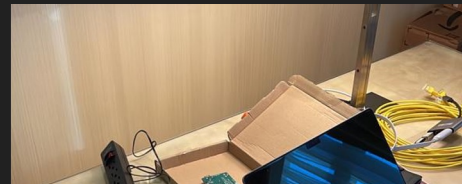
2. Internet connectivity & Network: local network

Play the Sysadmin CTF!



2. Internet connectivity & Network: local network

Play the Sysadmin CTF!



ORDER PLACED
August 7, 2023

TOTAL
\$695.03

SHIP TO
Hold for Guest: DANIELE LAIN - 0041786461009 ▾

Delivered August 10 ← **T-1** 🙌

Your package was left in the mail room. Signed by: Rafael

[Mikrotik CSS326-24G-2S+RM 24 port Gigabit Ethernet switch with two SFP+ ports](#)

Return window closed on September 9, 2023

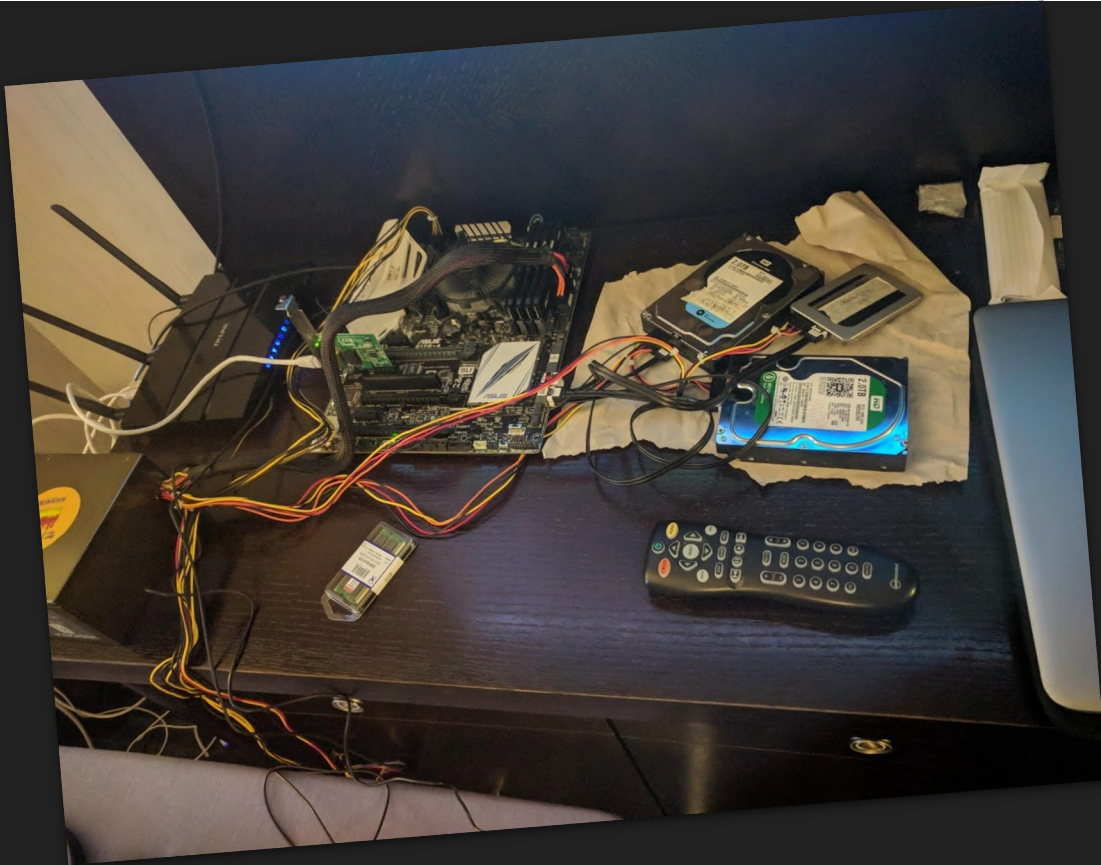


Buy it again

View your item

4

3. Hardware



3. Hardware



4. Tools: locally hosted **services**



4. Tools: our custom CTF tools

doublethink

flappyflag

reverse-chall-exploiter

burrito

cocktail-hack



eakeasy

tunniceddu

kastykpr

bnhooker

attacker-toh

salamella-preload

IDArling

toh_



door

toh_



toh_submitter

flowtracer

10000+ Python loc

4000+ C/C++ loc

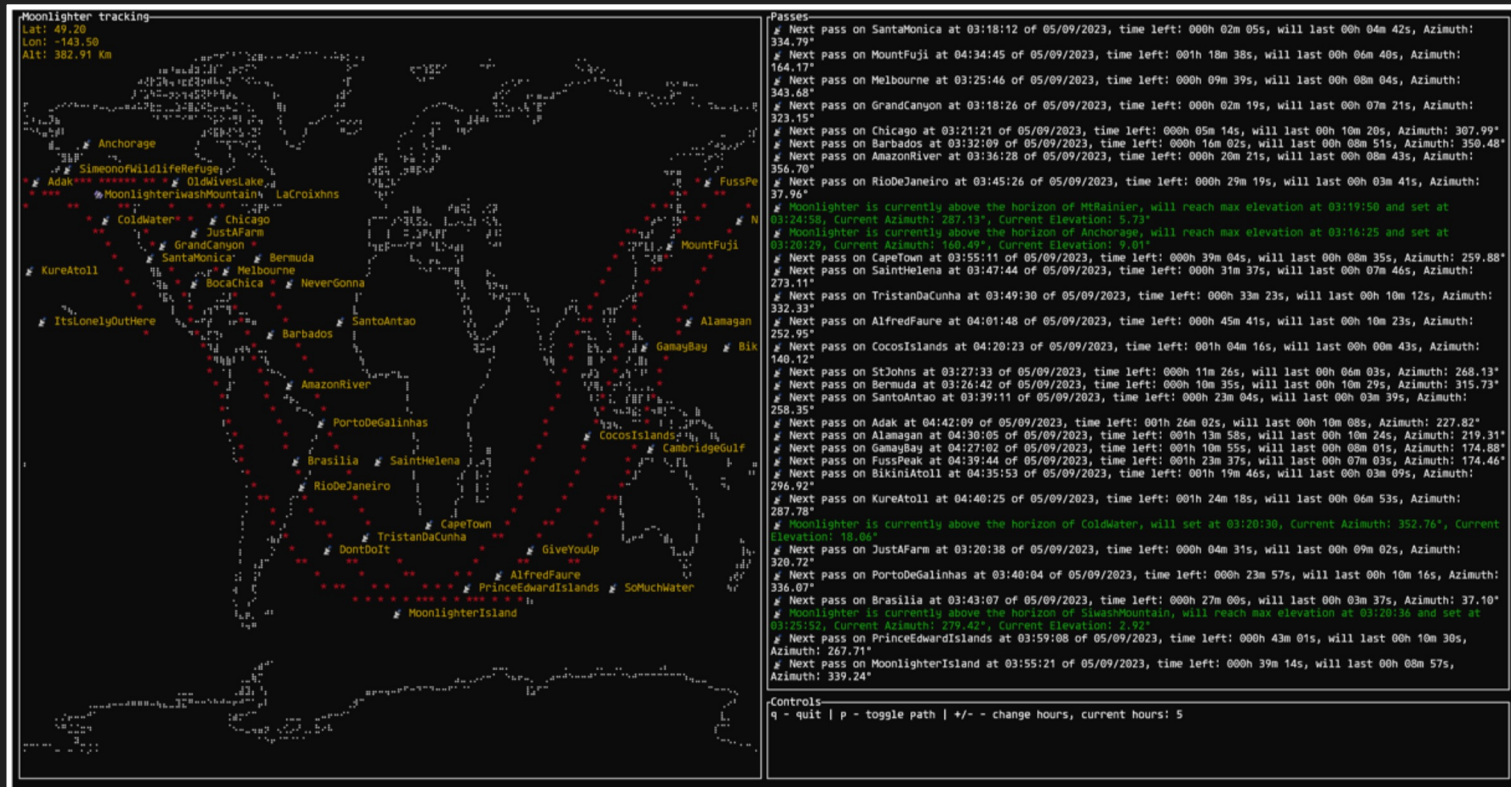
Thousands of JS, bash, go loc

4. Tools: Tunniceddu

DECLASSIFIED



4. Tools: monlighter track



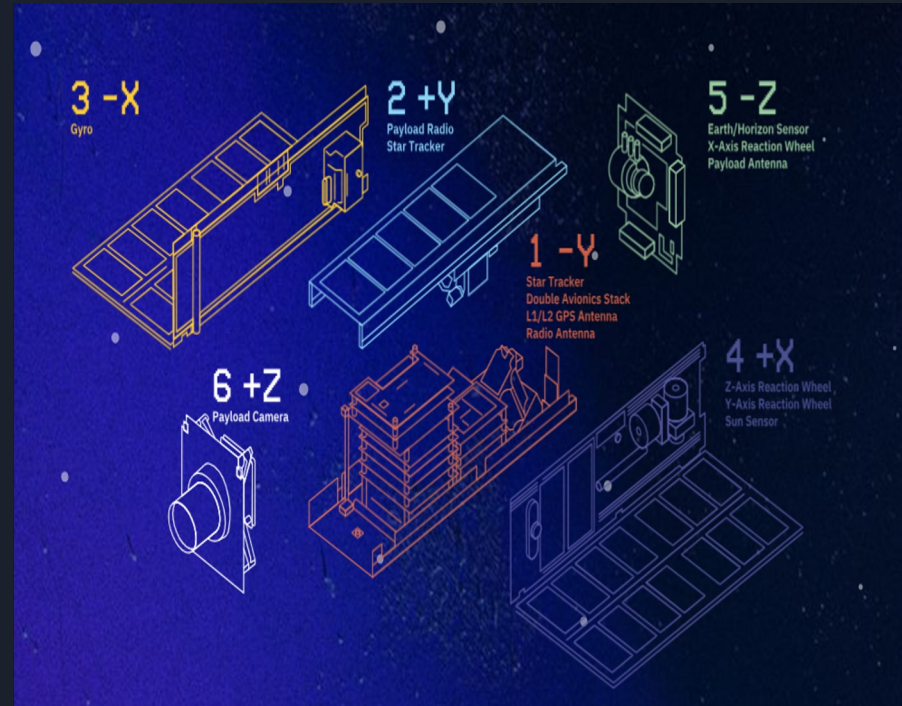
Game Rules: Hack-A-Sat 4 finals

- **5 Teams invited**
 - mhackeroni, SpaceBitsRUS, PolandCanIntoSpace, jmp fs[rcx], KrautSat
- **50k\$ Cash Prize**
- **Mix of jeopardy and on-orbit challenges**
- **An actual orbiting satellite as a target: moonlighter**
 - Launched on June 6th with SpaceX CRS-2 Falcon
 - Hosted on the ISS and deployed in orbit on July 6th
 - 3U CubeSat (30x10x10cm) with multiple sensor and actuators:
 - Gyroscope, camera, radio, earth/horizon sensor, L1/L2 GPS Antennas, X/Y/Z axis reaction wheel



Game Rules: Hack-A-Sat 4 finals

- Risc-V Machine
- Running **LUA**
- 100Mhz
- Can Communicate with Subsystem
- Very Slow Feedback (need another pass)



Game Rules: Hack-A-Sat 4 finals

Contact Window (Upload Payload)



HACK
A-SAT 4

Game Rules: Hack-A-Sat 4 finals

Contact Window (Run)



HACK
A-SAT 4

Game Rules: Hack-A-Sat 4 finals

Contact Window (Download)



HACK
A-SAT 4



Game Rules: Hack-A-Sat 4 finals

SATELLITE OPS SCHEDULE					
		"Deadline to Submit Tasks"	"Ops Window for Submitted Tasks"		
	ID	Deadline	Start	Stop	Day
	40	16:21:22	16:42:18	17:35:06	Friday
	41	17:30:06	17:51:47	19:33:34	Friday
	42	19:28:34	19:49:24	21:09:48	Friday
	43	21:04:48	21:25:59	1:26:15	Friday
	44	1:21:15	1:41:37	2:05:00	Friday
	45	2:00:00	8:00:00	19:30:00	Deadline Friday; Ops Window Saturday
	46	20:12:01	20:33:43	00:53:05	Saturday
	47	1:00:00	2:45:00	03:45:00	Saturday

*All times in UTC



Game Rules: Hack-A-Sat 4 finals



Hack-A-Sat 4 challenges: Shutterbug

Take a picture of objectives in *targets.yml*.

Avoid the prohibited zones.

Use the Attitude Control System.

Due to issues with the reaction wheel on the Z axis, we decomposed this rotation in three components on the remaining two body axes (i.e., X and Y). We output these three SciPy rotation objects in quaternion form and scheduled commands accordingly.

We utilized the following script to visually identify which targets were not enclosed within a geofence.



Hack-A-Sat 4 challenges: Shutterbug

```
import yaml
import json
import matplotlib.pyplot as plt
import cartopy.crs as ccrs
import cartopy.feature as cfeature
from shapely.geometry import Polygon, Point

with open("targets.yml", "r") as yaml_file:
    locations_data = yaml.safe_load(yaml_file)

with open("restricted.json", "r") as json_file:
    zones_data = json.load(json_file)

zones = {}
for zone_name, zone_coordinates in zones_data["zones"].items():
    polygon = Polygon([(coord["long"], coord["lat"]) for coord in zone_coordinates])
    zones[zone_name] = polygon

passes = []
with open("passes.txt") as f:
    passes = [line.strip().split()[3] for line in f.readlines()]

latitude_values = []
longitude_values = []
location_names = []
```

```
for location_name, location_data in locations_data["targets"].items():
    if location_name in passes:
        latitude = location_data["location"]["latitude"]
        longitude = location_data["location"]["longitude"]
        latitude_values.append(latitude)
        longitude_values.append(longitude)
        location_names.append(location_name)

fig = plt.figure(figsize=(12, 9))
ax = plt.axes(projection=ccrs.PlateCarree())
ax.add_feature(cfeature.LAND)
ax.add_feature(cfeature.COASTLINE)

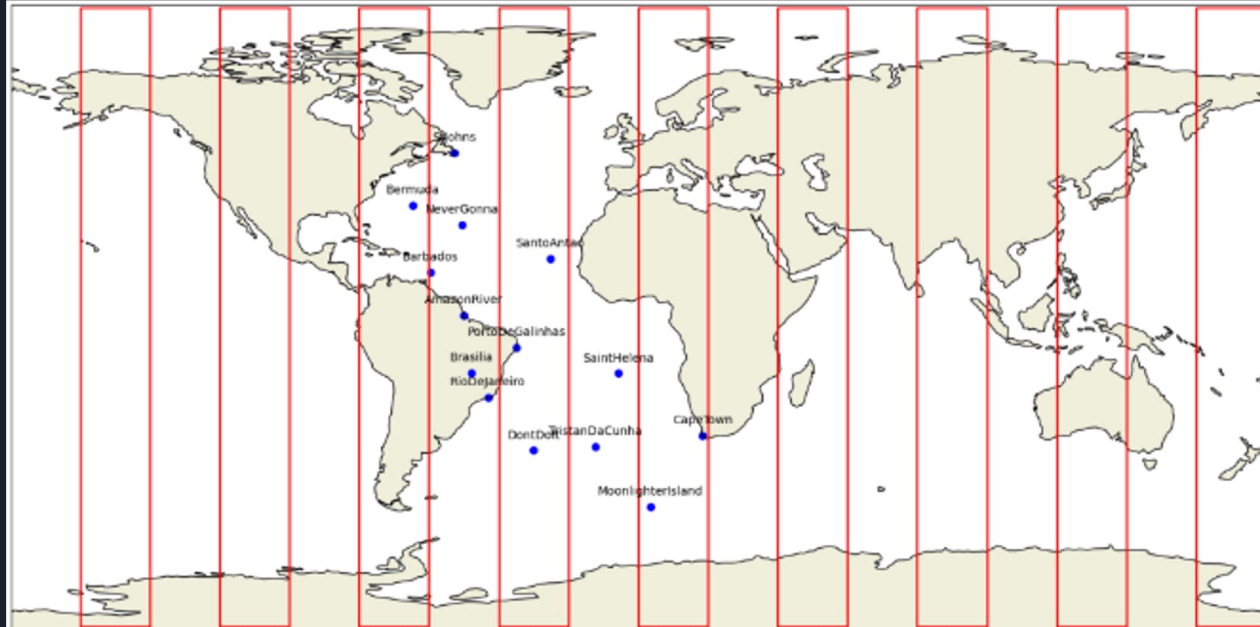
for zone_name, zone_coordinates in zones.items():
    ax.plot(*zone_coordinates.exterior.xy, color='red', linewidth=1.5, linestyle='--', label='Zones')

ax.scatter(longitude_values, latitude_values, color='blue', marker='o', label='Locations')

for i, name in enumerate(location_names):
    ax.annotate(name, (longitude_values[i], latitude_values[i]), textcoords="offset points", xytext=(0,10), ha='center')

ax.set_global()
plt.xlabel('Longitude')
plt.ylabel('Latitude')
plt.grid(True)
plt.show()
return go(f, seed, [])
```

Hack-A-Sat 4 challenges: Shutterbug



Hack-A-Sat 4 challenges: Shutterbug

Learn Space Math Tools:

- Skyfield
- quaternions
- NASA GMAT

RISC-V RevTools:



- Ghidra
- BinaryNinja



Hack-A-Sat 4 challenges: Shutterbug

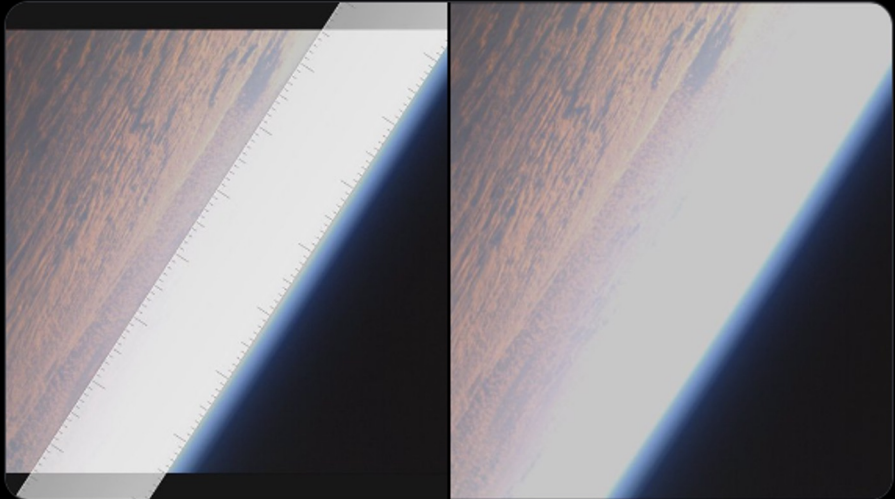


Hack-A-Sat 4 challenges:

This is the picture taken from outer space at DEFCON when hackers hacked a satellite.

I overlaid a ruler, the original is also here as well.

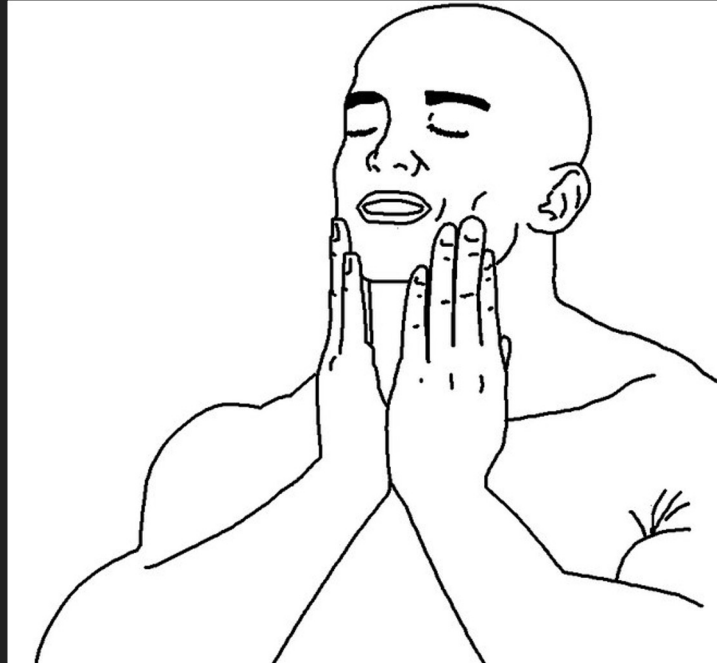


11:21 PM · Aug 20, 2023 · 16.6K Views



Hack-A-Sat: Day 1

We solved Everything!



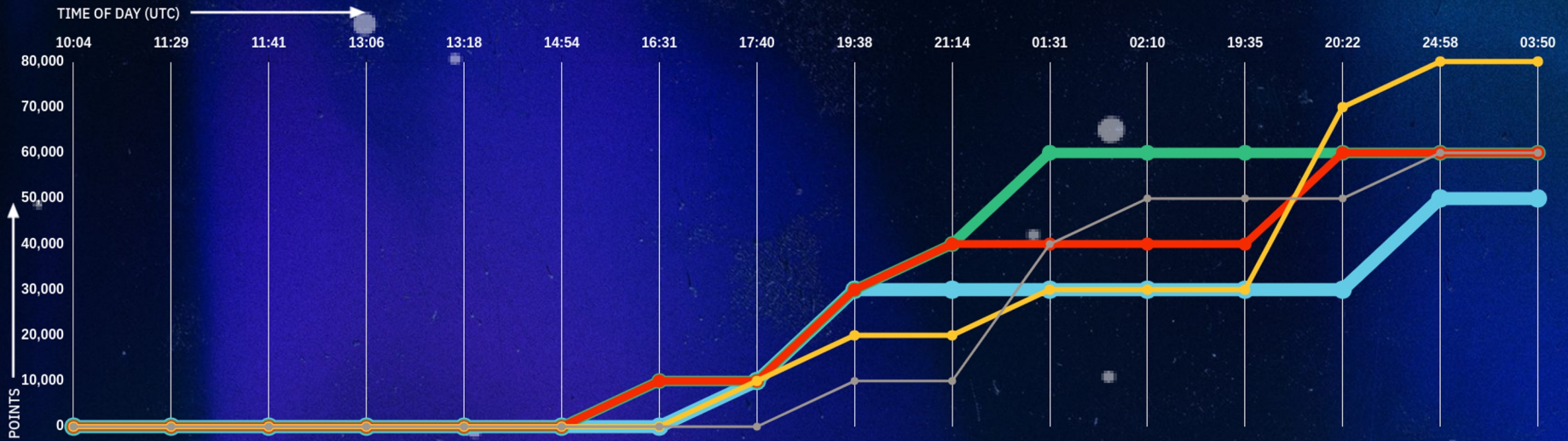
Hack-A-Sat: Day 2

We solved ~~Everything~~ NOTHING!



Hack-A-Sat: Day 3

SCORING HISTOGRAM



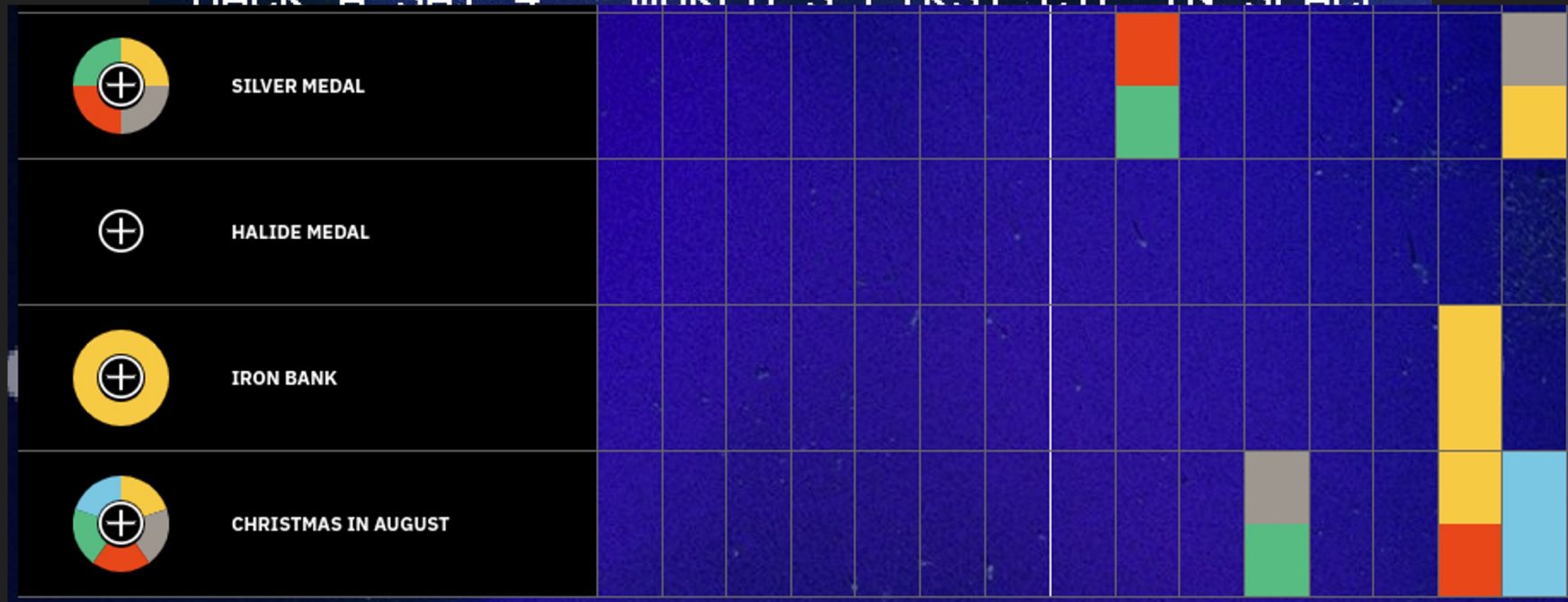
mhackeroni **wins** Hack-A-Sat 4

HACK-A-SAT 4 - WORLD'S FIRST CTF IN SPACE



mhackeroni **wins** Hack-A-Sat 4

HACK-A-SAT 4 - WORLD'S FIRST CTF IN SPACE



mhackeroni **wins** Hack-A-Sat 4



mhackeroni **wins** Hack-A-Sat 4





Thanks!

... and ask us anything :-)

www.mhackeroni.it
info@mhackeroni.it