COUNTER HACK

Building Compelling Cyber Challenges and Range Scenarios

Chris Elgee | @chriselgee

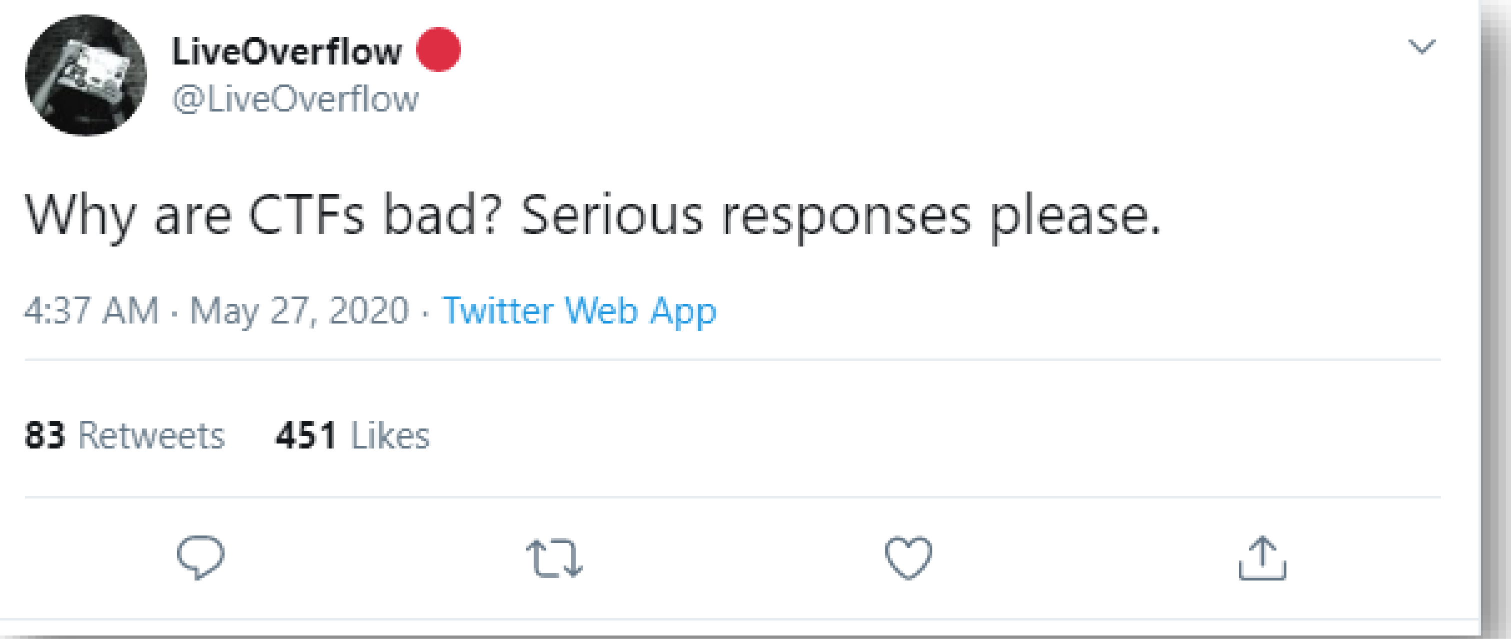
Simon McNamee | @mcnamee_simon

5 June 2020

Agenda

Hit List

- Why?
- Target Audience
- Challenge Shape
- Story?
- Making the Sausage
- Secret Sauce!



LiveOverflow
@LiveOverflow

Why are CTFs bad? Serious responses please.

4:37 AM · May 27, 2020 · Twitter Web App

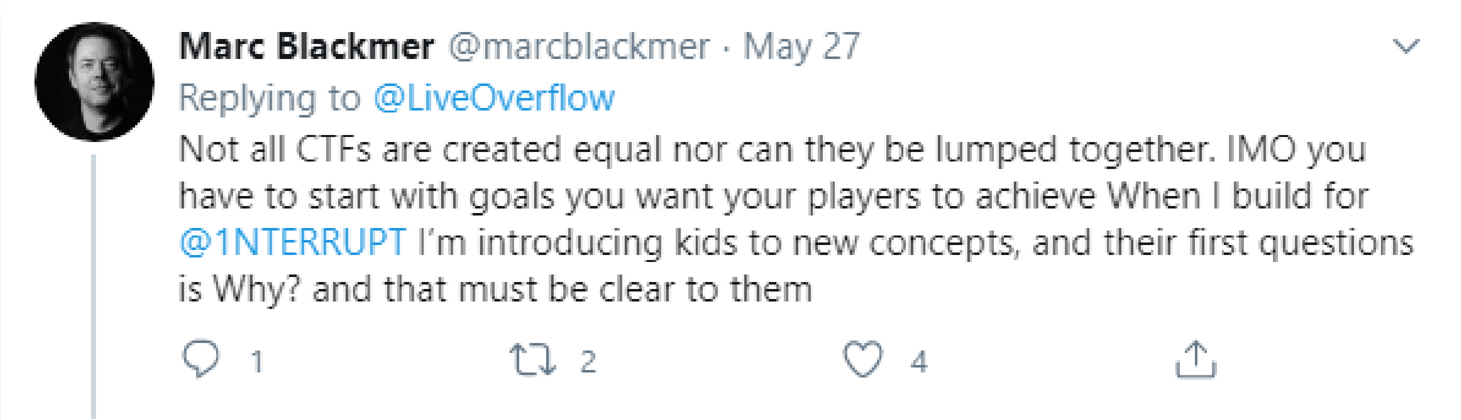
83 Retweets 451 Likes

Why?

Why?

Training Purpose

- Which skills
- Target end state
- Individual or team



Marc Blackmer @marcblackmer · May 27

Replying to @LiveOverflow

Not all CTFs are created equal nor can they be lumped together. IMO you have to start with goals you want your players to achieve When I build for @1NTERRUPT I'm introducing kids to new concepts, and their first questions is Why? and that must be clear to them

rs, Four Months

On-Site Core NetWars Tournament

Miniaturized Physical City

Online DFIR NetWars, Four Months

On-Site DFIR NetWars Tournament

6 Days of Hands-on Learning

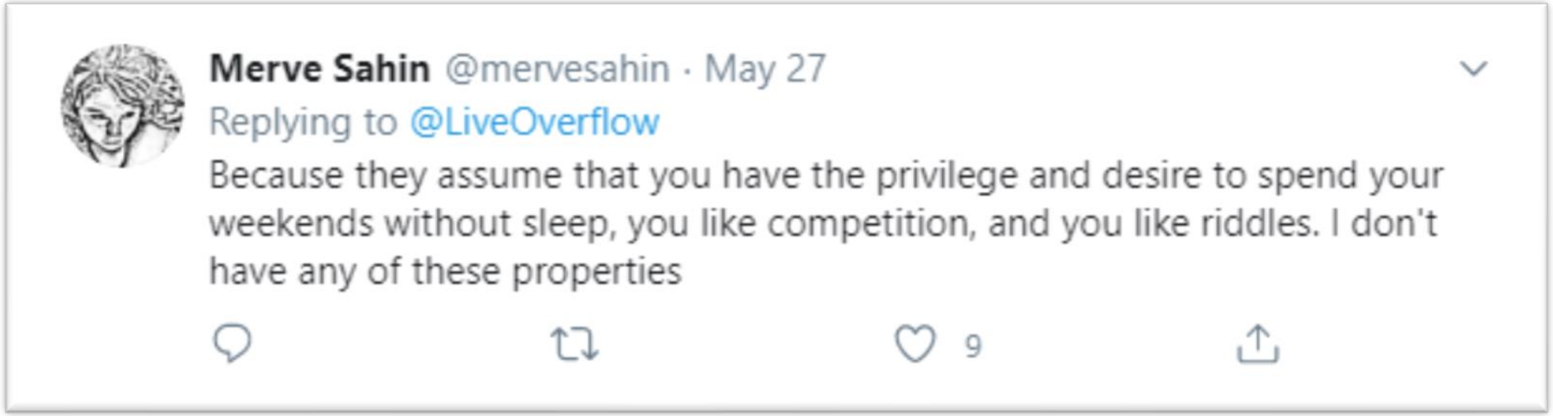
GRID NetWars

ICS NetWars

Cyber Defense NetWars

Target Audience

Target Audience | Competition



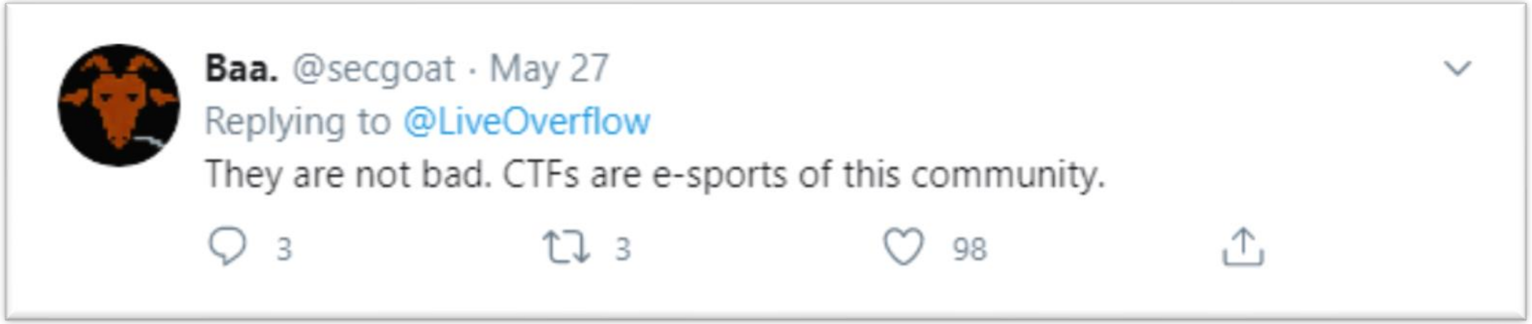
Merve Sahin @mervesahin · May 27

Replying to @LiveOverflow

Because they assume that you have the privilege and desire to spend your weekends without sleep, you like competition, and you like riddles. I don't have any of these properties

NETWARS TOURNAMENT

Jupiter Rockets

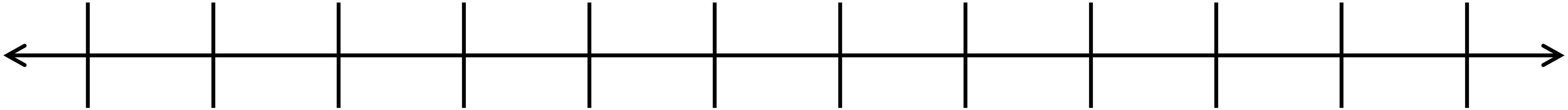


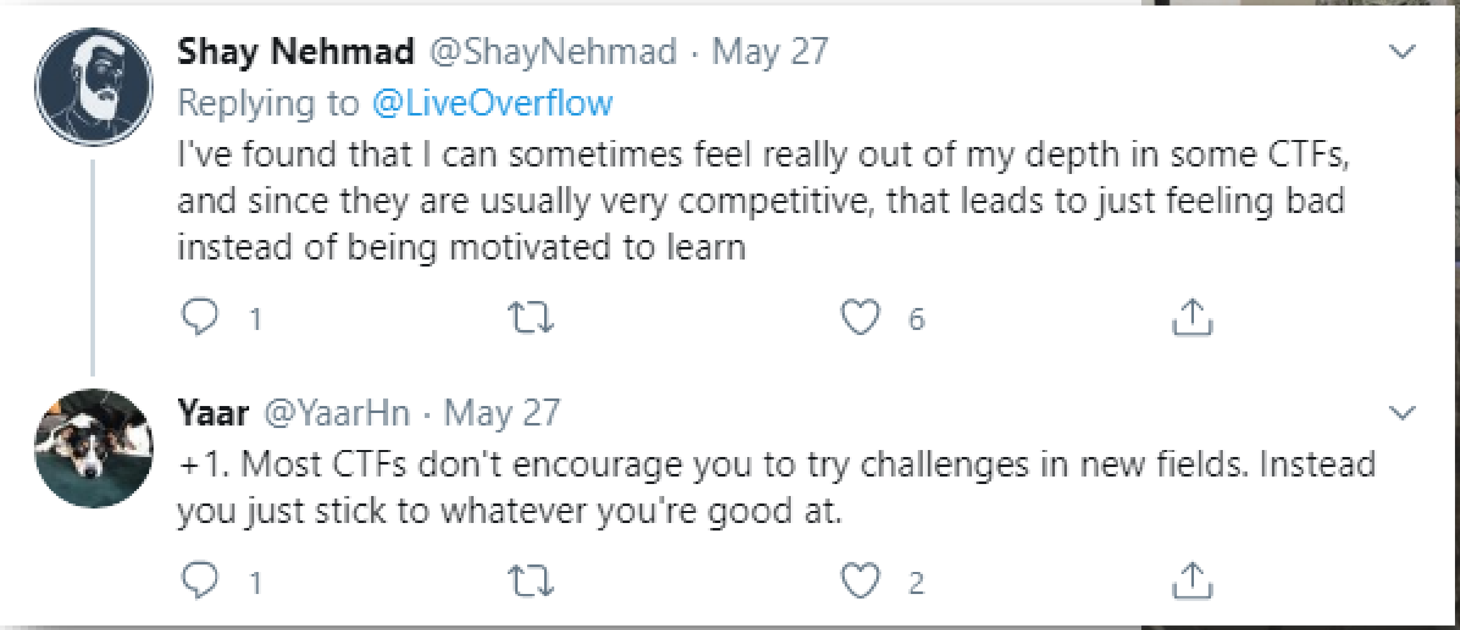
Baa. @secgoat · May 27

Replying to @LiveOverflow

They are not bad. CTFs are e-sports of this community.

Target Audience | Skill Level & Teams



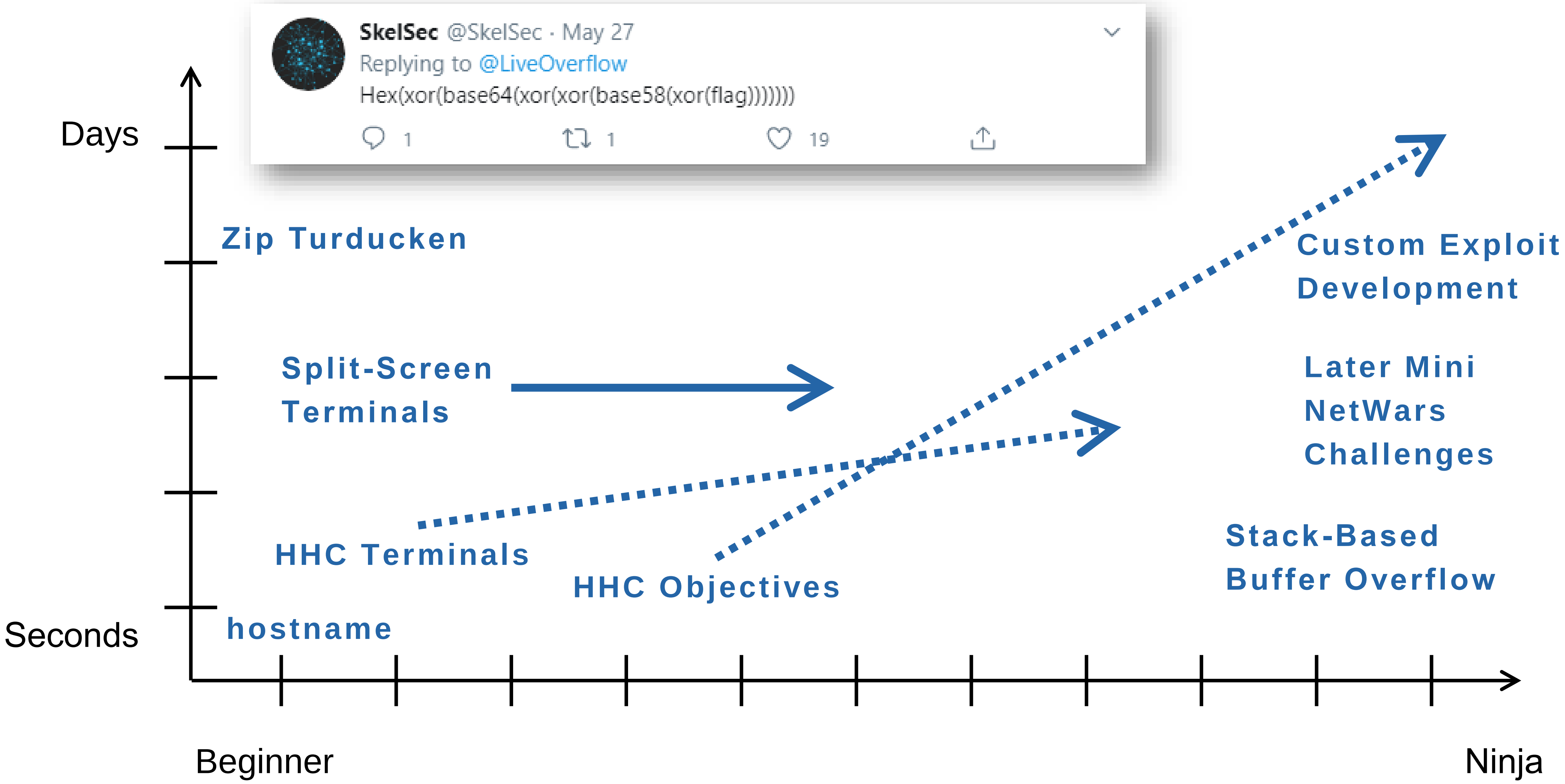


Shay Nehmad @ShayNehmad · May 27
Replying to @LiveOverflow
I've found that I can sometimes feel really out of my depth in some CTFs, and since they are usually very competitive, that leads to just feeling bad instead of being motivated to learn

Yaar @YaarHn · May 27
+1. Most CTFs don't encourage you to try challenges in new fields. Instead you just stick to whatever you're good at.

Shape of a Challenge

Shape of a Challenge | Time & Skill Axes



SkelSec @SkelSec · May 27

Replying to @LiveOverflow

Hex(xor(base64(xor(xor(base58(xor(flag)))))))

1 1 19

Days

Seconds

Beginner

Ninja

Zip Turducken

Split-Screen Terminals

HHC Terminals

HHC Objectives

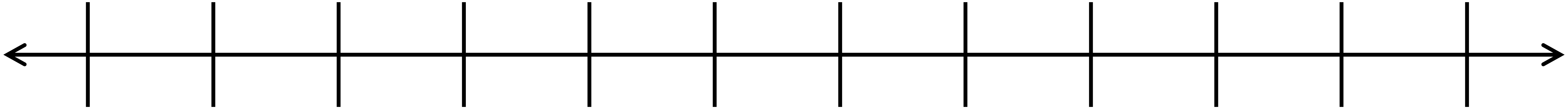
hostname

Custom Exploit Development

Later Mini NetWars Challenges

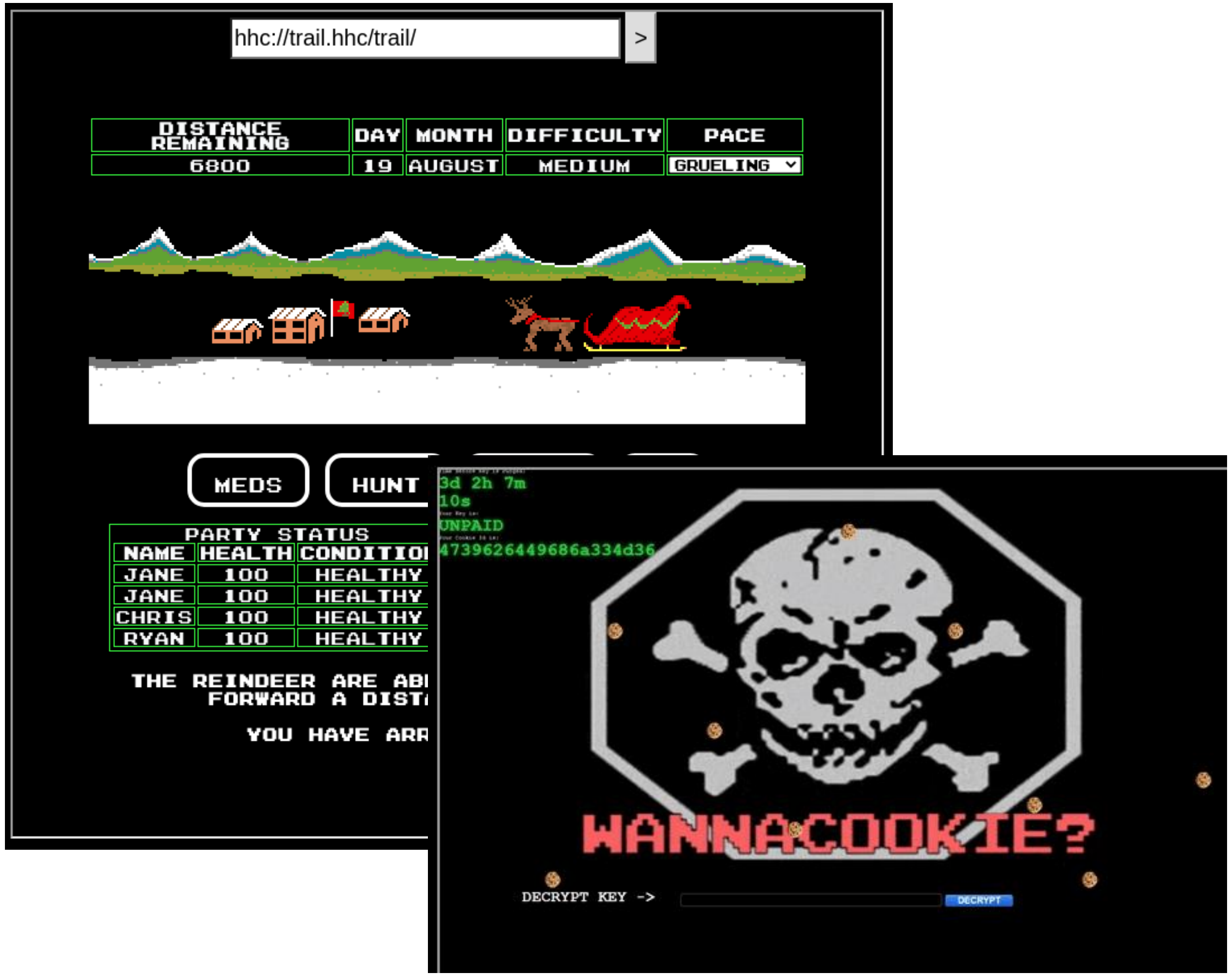
Stack-Based Buffer Overflow

Shape of a Challenge | Direction



Guided

ReadyGo



DISTANCE REMAINING	DAY	MONTH	DIFFICULTY	PACE
6800	19	AUGUST	MEDIUM	GRUELING

PARTY STATUS

NAME	HEALTH	CONDITIOI
JANE	100	HEALTHY
JANE	100	HEALTHY
CHRIS	100	HEALTHY
RYAN	100	HEALTHY

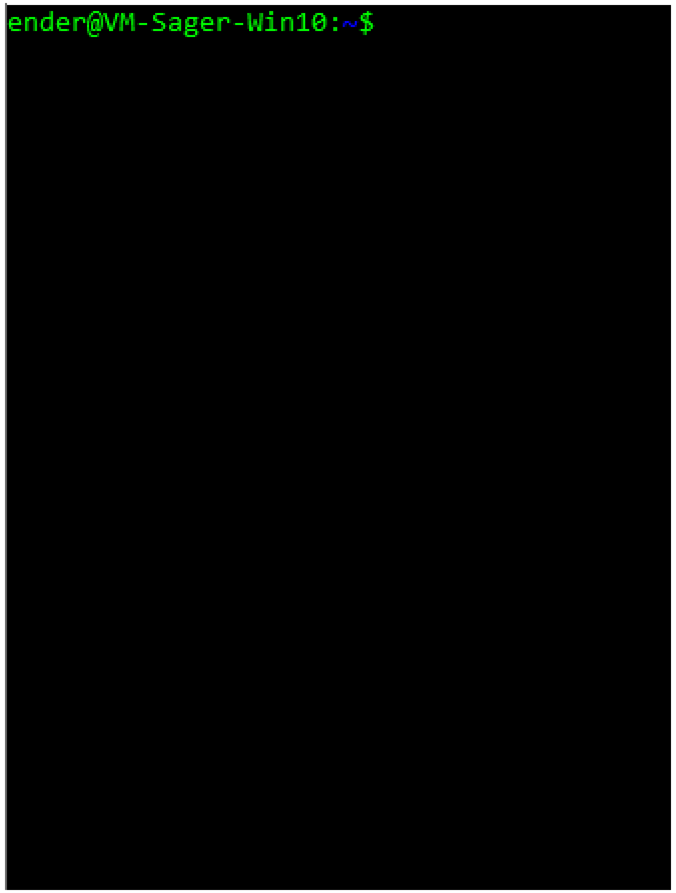
THE REINDEER ARE ABI
FORWARD A DISTA

YOU HAVE ARR

Time Until Key is Purged:
3d 2h 7m
10s
Your Key is:
UNPAID
Your Cookie ID is:
4739626449686a334d36

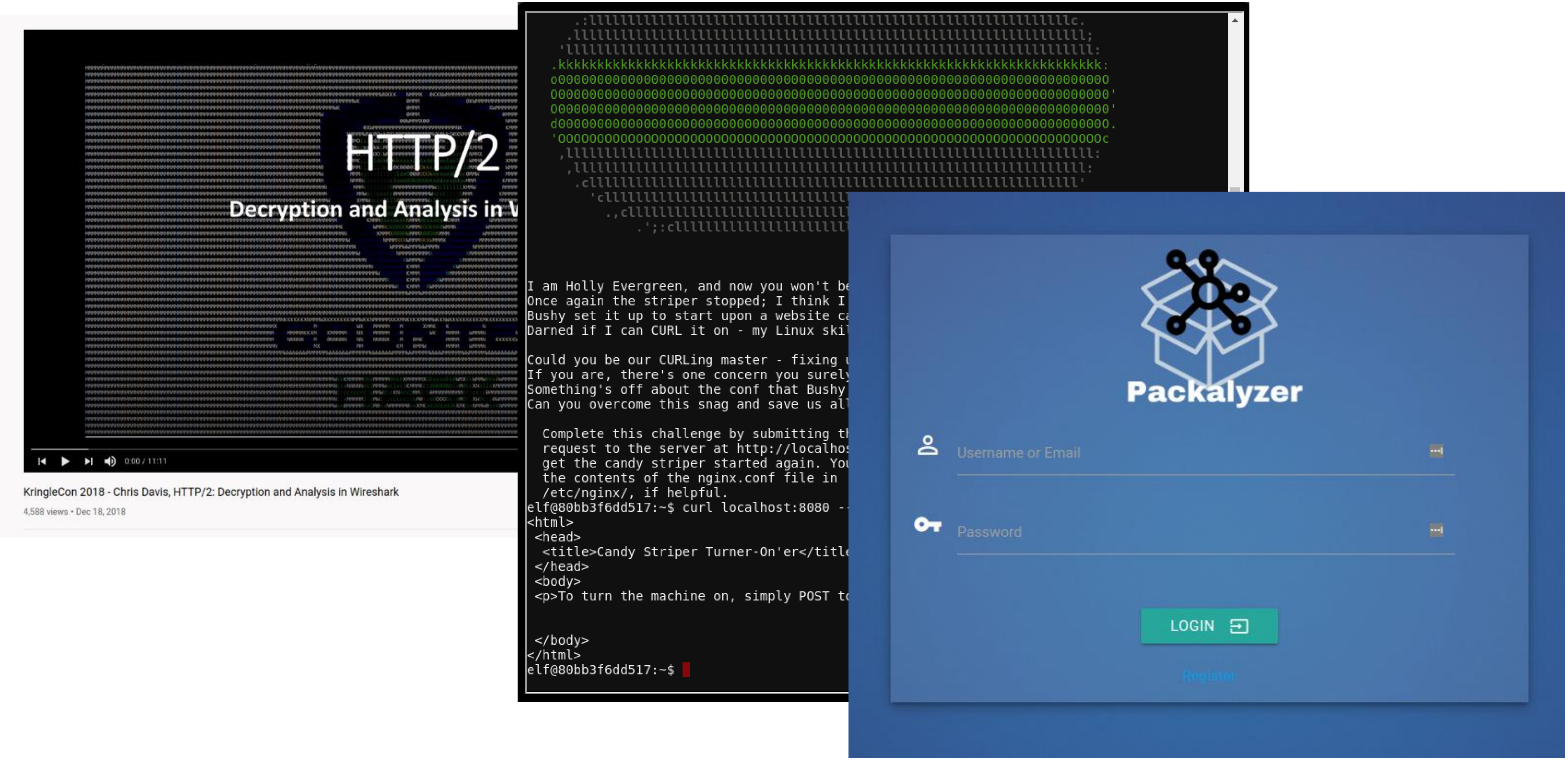
WANNACOOKIE?

DECRYPT KEY ->



```
ender@VM-Sager-Win10:~$
```

Shape of a Challenge | Successive Challenges



KringleCon 2018 - Chris Davis, HTTP/2: Decryption and Analysis in Wireshark

4,588 views • Dec 18, 2018

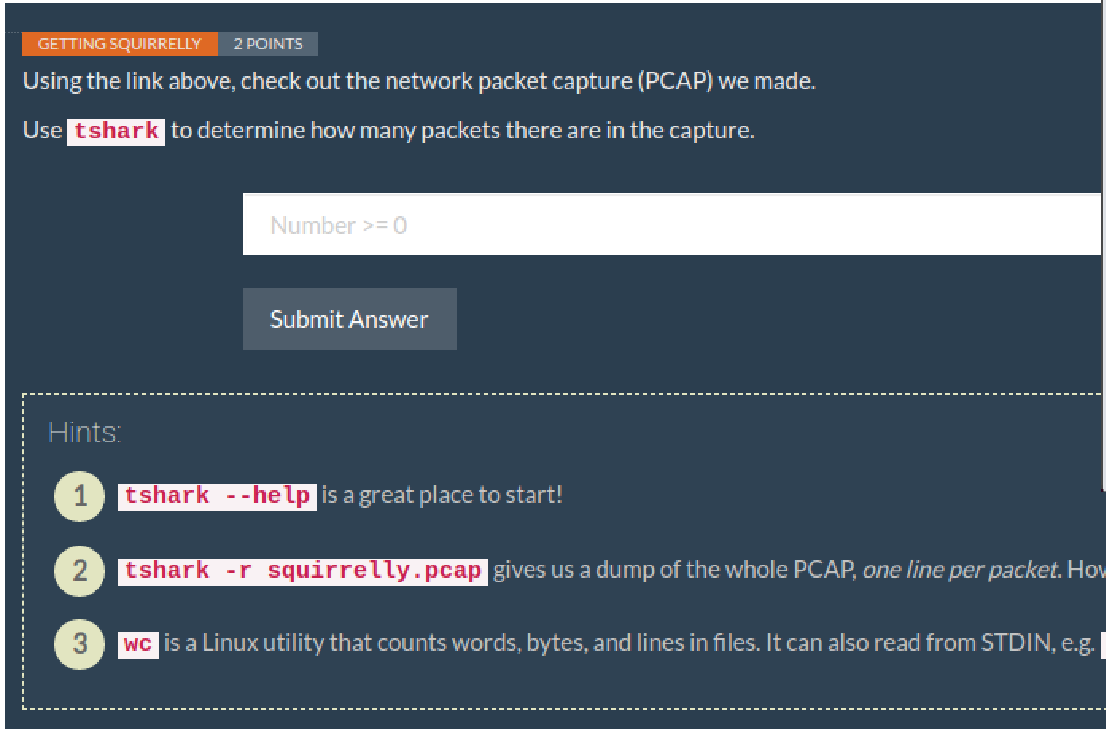
```
I am Holly Evergreen, and now you won't be
Once again the striper stopped; I think I
Bushy set it up to start upon a website ca
Darned if I can CURL it on - my Linux ski

Could you be our CURLing master - fixing u
If you are, there's one concern you surely
Something's off about the conf that Bushy
Can you overcome this snag and save us all

  Complete this challenge by submitting th
  request to the server at http://localhos
  get the candy striper started again. You
  the contents of the nginx.conf file in
  /etc/nginx/, if helpful.
elf@80bb3f6dd517:~$ curl localhost:8080 --
<html>
 <head>
  <title>Candy Striper Turner-On'er</title
 </head>
 <body>
 <p>To turn the machine on, simply POST to


 </body>
</html>
elf@80bb3f6dd517:~$ 
```

Shape of a Challenge | Hints and Split-Screen Terminals



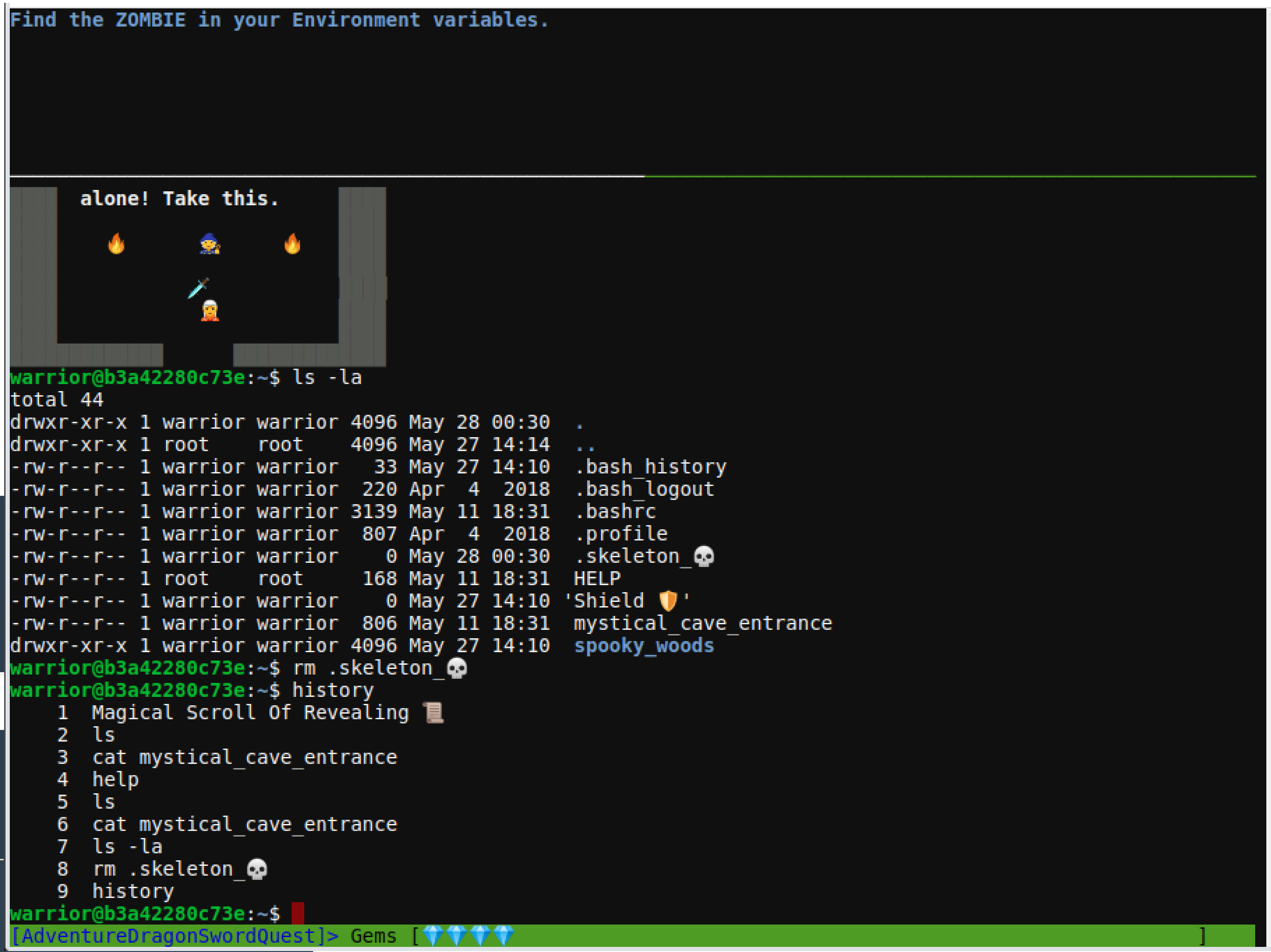
GETTING SQUIRRELLY 2 POINTS

Using the link above, check out the network packet capture (PCAP) we made.

Use `tshark` to determine how many packets there are in the capture.

Hints:

1. `tshark --help` is a great place to start!
2. `tshark -r squirrelly.pcap` gives us a dump of the whole PCAP, *one line per packet*. How can we count those lines?
3. `wc` is a Linux utility that counts words, bytes, and lines in files. It can also read from STDIN, e.g. `cat file.txt | wc -l`

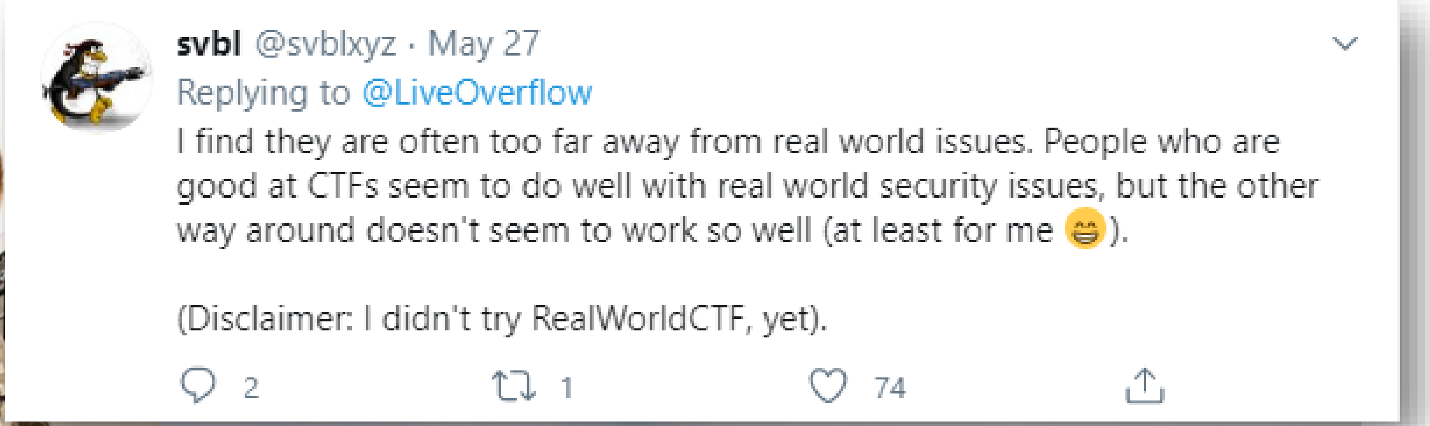


```
Find the ZOMBIE in your Environment variables.
```

```
alone! Take this.
```

```
warrior@b3a42280c73e:~$ ls -la
total 44
drwxr-xr-x 1 warrior warrior 4096 May 28 00:30  .
drwxr-xr-x 1 root    root    4096 May 27 14:14  ..
-rw-r--r-- 1 warrior warrior   33 May 27 14:10  .bash_history
-rw-r--r-- 1 warrior warrior  220 Apr  4  2018  .bash_logout
-rw-r--r-- 1 warrior warrior 3139 May 11 18:31  .bashrc
-rw-r--r-- 1 warrior warrior  807 Apr  4  2018  .profile
-rw-r--r-- 1 warrior warrior    0 May 28 00:30  .skeleton_💀
-rw-r--r-- 1 root    root     168 May 11 18:31  HELP
-rw-r--r-- 1 warrior warrior    0 May 27 14:10 'Shield 🛡'
-rw-r--r-- 1 warrior warrior  806 May 11 18:31  mystical_cave_entrance
drwxr-xr-x 1 warrior warrior 4096 May 27 14:10  spooky_woods
warrior@b3a42280c73e:~$ rm .skeleton_💀
warrior@b3a42280c73e:~$ history
    1  Magical Scroll Of Revealing 📜
    2  ls
    3  cat mystical_cave_entrance
    4  help
    5  ls
    6  cat mystical_cave_entrance
    7  ls -la
    8  rm .skeleton_💀
    9  history
warrior@b3a42280c73e:~$
[AdventureDragonSwordQuest]> Gems [💎💎💎💎                                        ]
```

Shape of a Challenge | Realism vs Range-ism



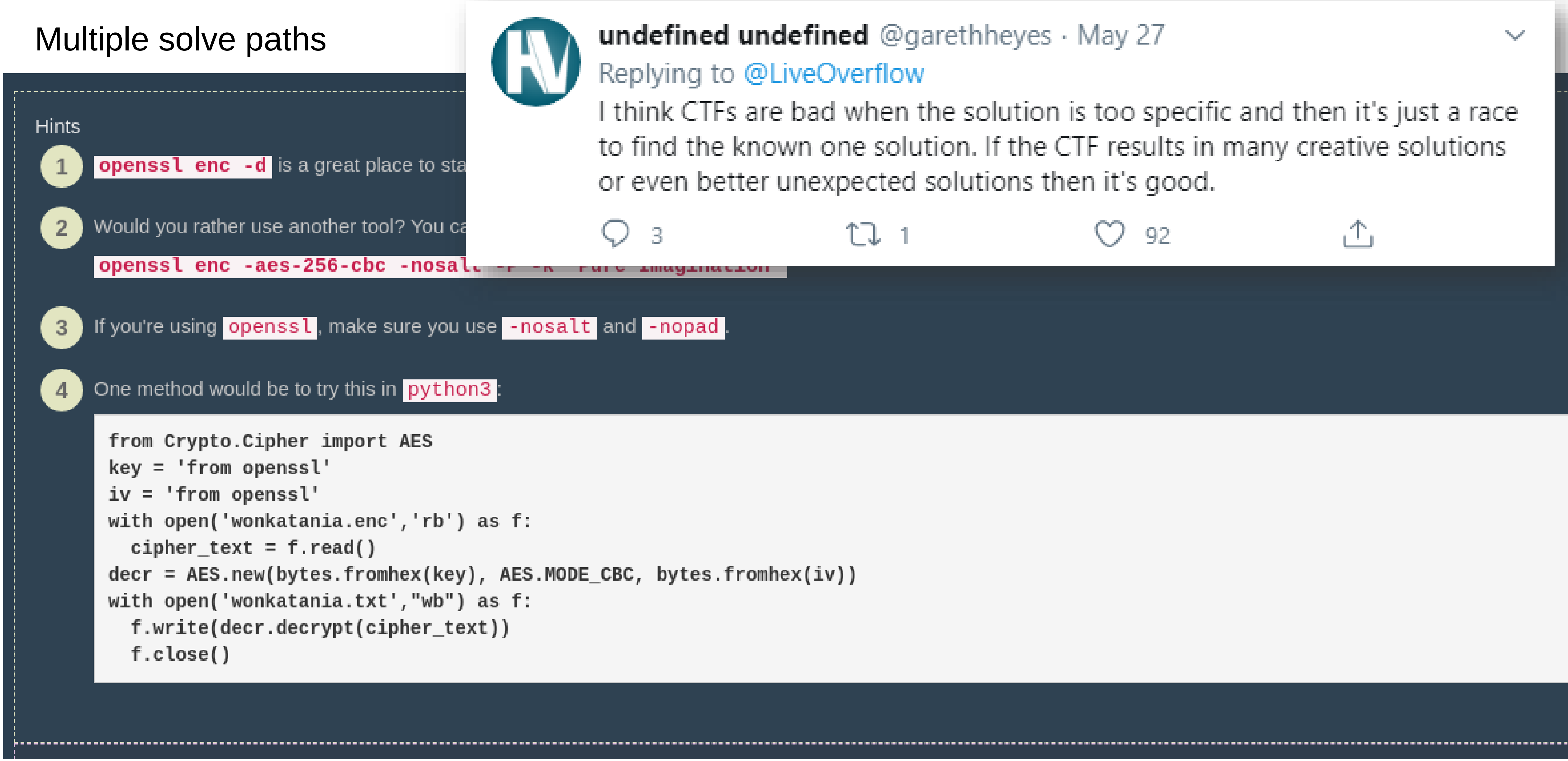
svbl @svblxyz · May 27

Replying to @LiveOverflow

I find they are often too far away from real world issues. People who are good at CTFs seem to do well with real world security issues, but the other way around doesn't seem to work so well (at least for me 😁).

(Disclaimer: I didn't try RealWorldCTF, yet).

Multiple solve paths



undefined undefined @garethheyes · May 27

Replying to @LiveOverflow

I think CTFs are bad when the solution is too specific and then it's just a race to find the known one solution. If the CTF results in many creative solutions or even better unexpected solutions then it's good.

Hints

1 `openssl enc -d` is a great place to sta

2 Would you rather use another tool? You ca

`openssl enc -aes-256-cbc -nosalt -P -k Pure Imagination`

3 If you're using `openssl`, make sure you use `-nosalt` and `-nopad`.

4 One method would be to try this in `python3`:

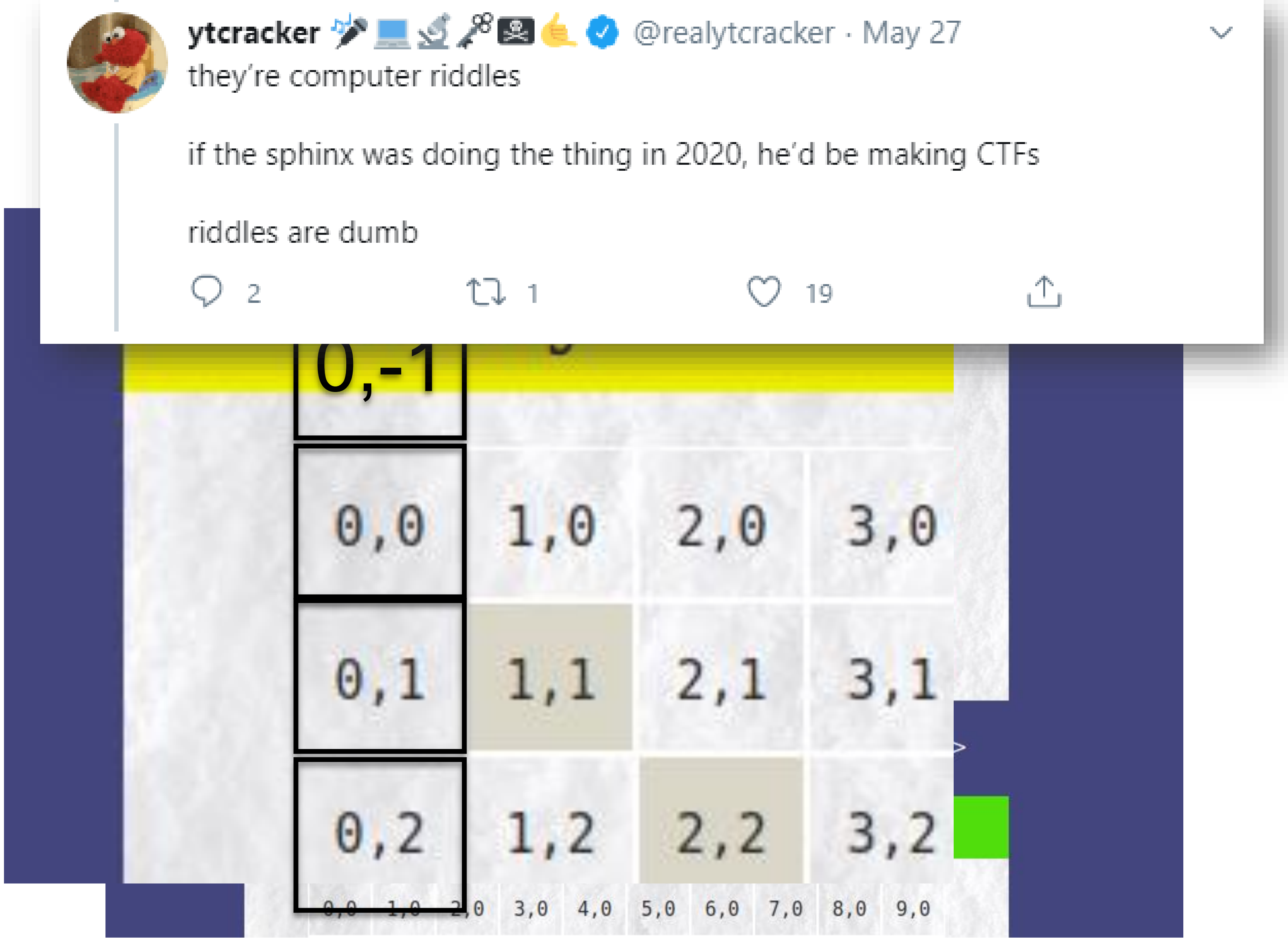
```
from Crypto.Cipher import AES
key = 'from openssl'
iv = 'from openssl'
with open('wonkatania.enc','rb') as f:
  cipher_text = f.read()
decr = AES.new(bytes.fromhex(key), AES.MODE_CBC, bytes.fromhex(iv))
with open('wonkatania.txt',"wb") as f:
  f.write(decr.decrypt(cipher_text))
  f.close()
```

Guess what the challenge developer is thinking.

“**Defeat the Enemy with one shot and submit the flag.**”

“Trying to hit the enemy? What are *his* coordinates? Once you figure that out, try `wscat` or just the Developer Console in your browser to make the shot.”

“Can you figure out how? Where would you shoot to defeat the Enemy in a single shot?”



ytcracker @realytcracker · May 27

they're computer riddles

if the sphinx was doing the thing in 2020, he'd be making CTFs

riddles are dumb

2 1 19

0,-1			
0,0	1,0	2,0	3,0
0,1	1,1	2,1	3,1
0,2	1,2	2,2	3,2

0,0 1,0 2,0 3,0 4,0 5,0 6,0 7,0 8,0 9,0

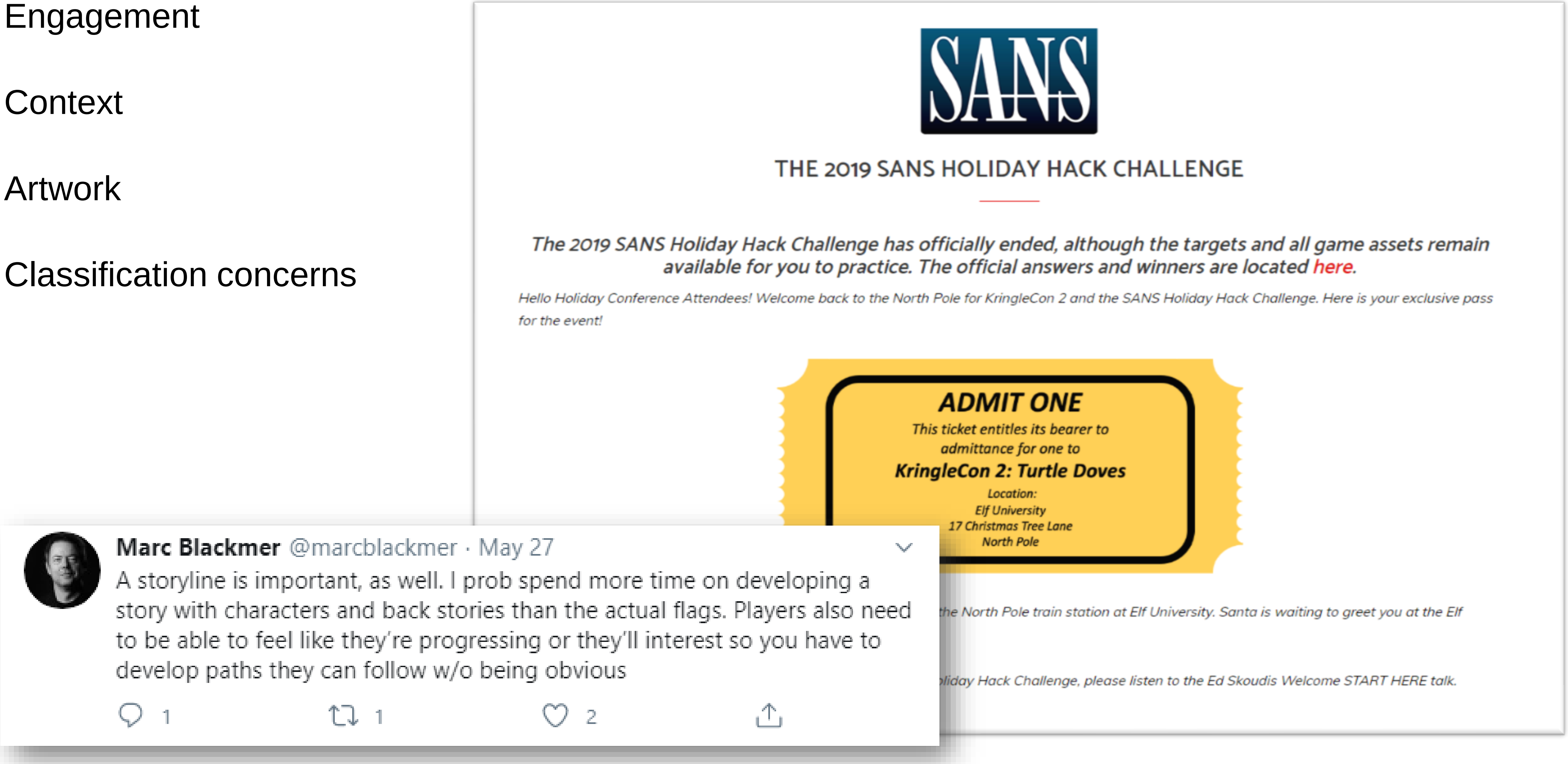
Shape of a Challenge | Storyline

Engagement

Context

Artwork

Classification concerns



SANS

THE 2019 SANS HOLIDAY HACK CHALLENGE

The 2019 SANS Holiday Hack Challenge has officially ended, although the targets and all game assets remain available for you to practice. The official answers and winners are located here.

Hello Holiday Conference Attendees! Welcome back to the North Pole for KringleCon 2 and the SANS Holiday Hack Challenge. Here is your exclusive pass for the event!

ADMIT ONE

This ticket entitles its bearer to admittance for one to

KringleCon 2: Turtle Doves

Location:
Elf University
17 Christmas Tree Lane
North Pole

the North Pole train station at Elf University. Santa is waiting to greet you at the Elf

liday Hack Challenge, please listen to the Ed Skoudis Welcome START HERE talk.

Marc Blackmer @marcblackmer · May 27

A storyline is important, as well. I prob spend more time on developing a story with characters and back stories than the actual flags. Players also need to be able to feel like they're progressing or they'll interest so you have to develop paths they can follow w/o being obvious

Making the Sausage

Making the Sausage | Dev

Challenge concepts

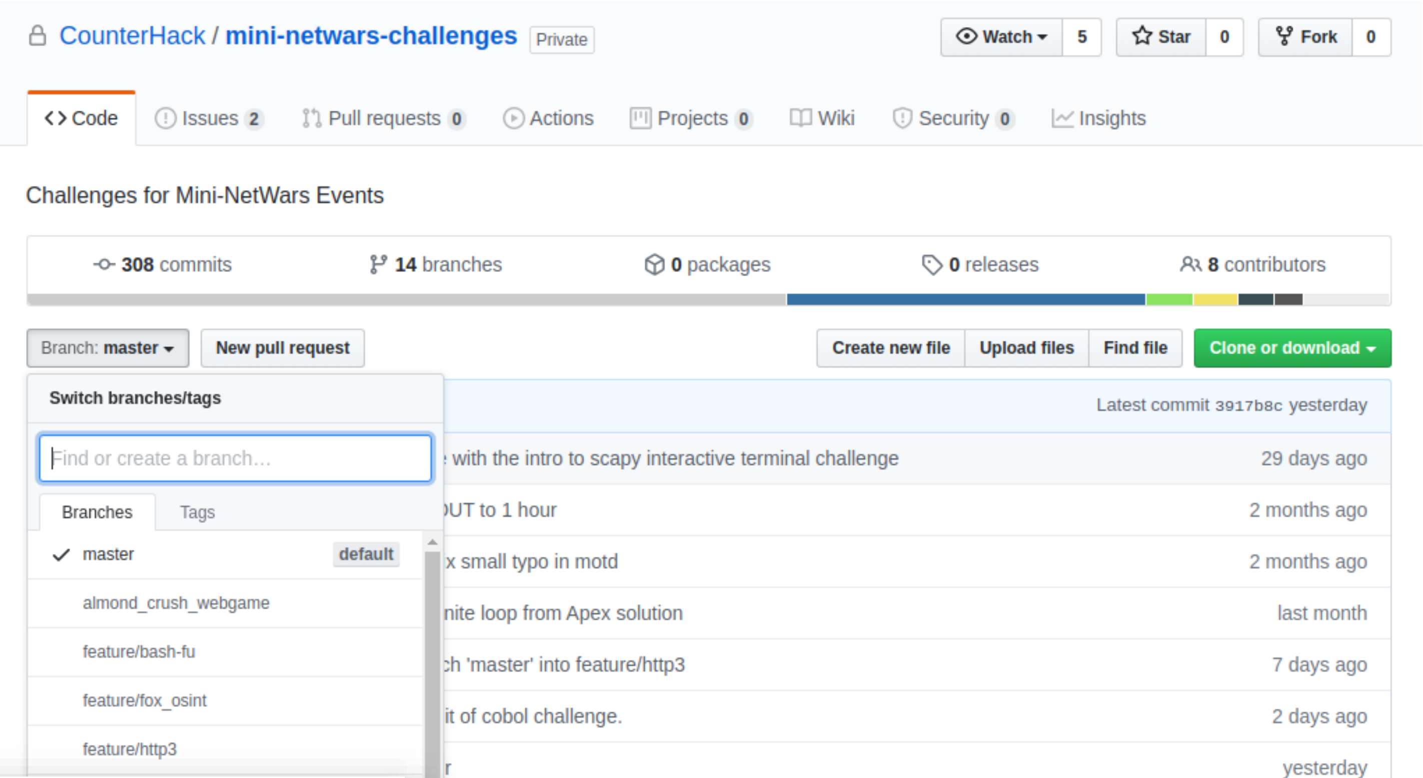
SDLC

Targets as code

QA

Solver scripts

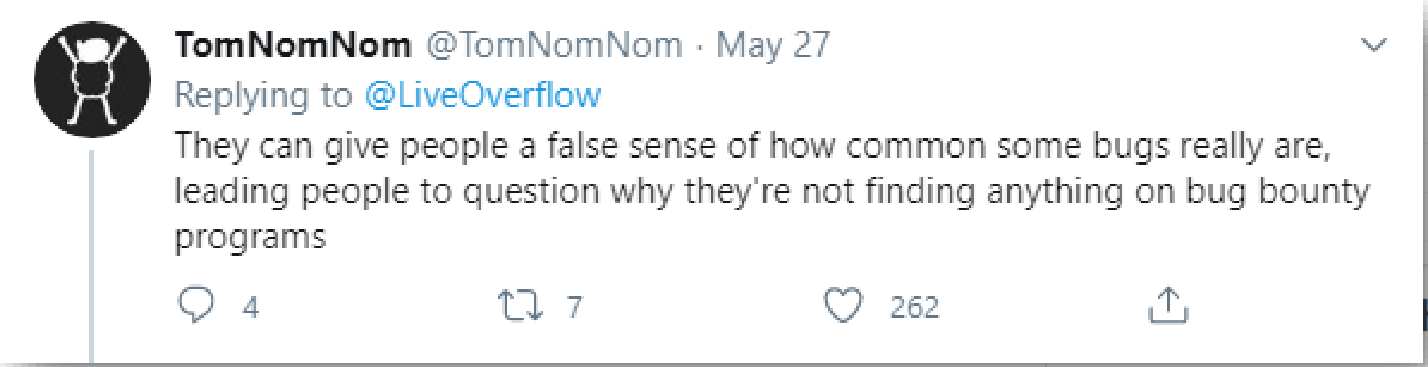
Feedback - peers and players



Challenges for Mini-NetWars Events

Latest commit 3917b8c yesterday

with the intro to scapy interactive terminal challenge	29 days ago
UT to 1 hour	2 months ago
x small typo in motd	2 months ago
nite loop from Apex solution	last month
ch 'master' into feature/http3	7 days ago
it of cobol challenge.	2 days ago
r	yesterday
OUT to 1 hour for all challenges	2 months ago
nsday device UI	2 months ago
Dockerfile	2 months ago



TomNomNom @TomNomNom · May 27

Replying to @LiveOverflow

They can give people a false sense of how common some bugs really are, leading people to question why they're not finding anything on bug bounty programs

hallenges

Use this repo for Mini-NetWars challenges. Create a top-level directory for each quest. Add the challenges in sub-directories, organized by quest.

Making the Sausage | Flags

NetWars{SomeFlagHere} or **192.168.24.19** or **Apache httpd 2.6.8** ?

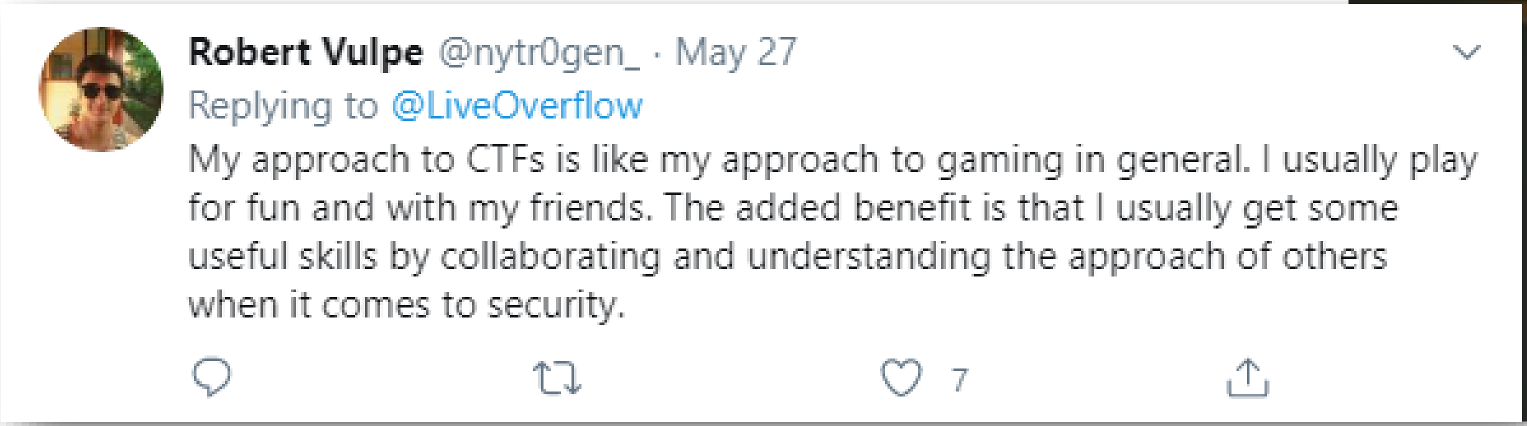
Automatic completion detection

Hiding strings

Penalties?

Individuals

1	M0neyT4lks	Level 3	212
2	dmfr	Level 3	181
3	m0n0plova	Level 3	172
4	Hacks4Beer	Level 2	153
5	Frichetten	Level 2	140
6	badfish907	Level 2	139
7	badgerttl	Level 2	133
8	TheForce	Level 2	131
9	Unkn0wn1	Level 2	127
10	pmgeahan	Level 2	127



Robert Vulpe @nytr0gen_ · May 27

Replying to @LiveOverflow

My approach to CTFs is like my approach to gaming in general. I usually play for fun and with my friends. The added benefit is that I usually get some useful skills by collaborating and understanding the approach of others when it comes to security.

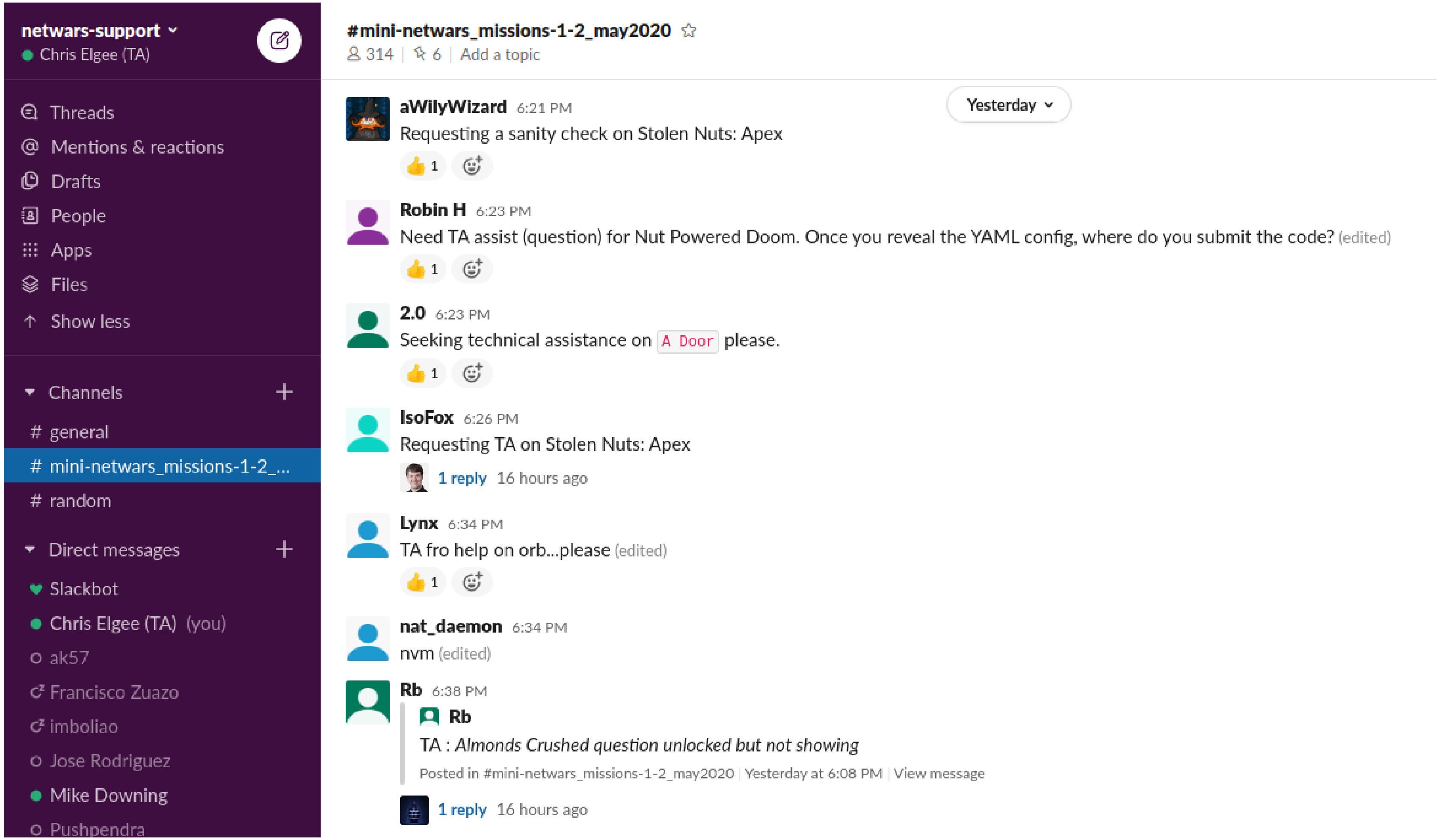
Making the Sausage | Support

Live/Virtual TAs

Email

Reverts

chattr +i



aWilyWizard 6:21 PM
Requesting a sanity check on Stolen Nuts: Apex
👍 1

Robin H 6:23 PM
Need TA assist (question) for Nut Powered Doom. Once you reveal the YAML config, where do you submit the code? (edited)
👍 1

2.0 6:23 PM
Seeking technical assistance on `A Door` please.
👍 1

IsoFox 6:26 PM
Requesting TA on Stolen Nuts: Apex
1 reply 16 hours ago

Lynx 6:34 PM
TA fro help on orb...please (edited)
👍 1

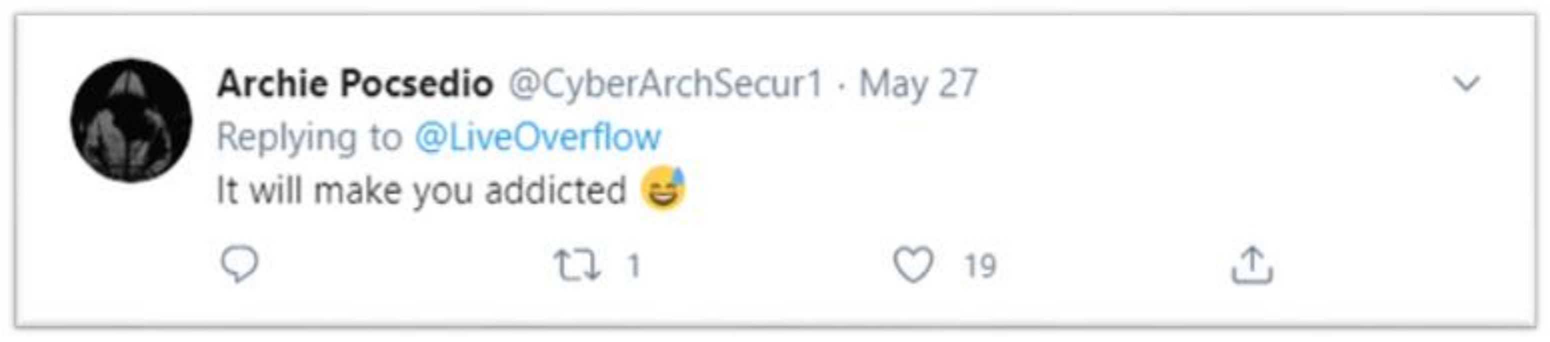
nat_daemon 6:34 PM
nvm (edited)

Rb 6:38 PM
> **Rb**
> TA : *Almonds Crushed question unlocked but not showing*
> Posted in #mini-netwars_missions-1-2_may2020 | Yesterday at 6:08 PM | View message

1 reply 16 hours ago

Secret Sauce

Teamwork



Archie Pocsedio @CyberArchSecur1 · May 27

Replying to @LiveOverflow

It will make you addicted 😅

Parting Shots

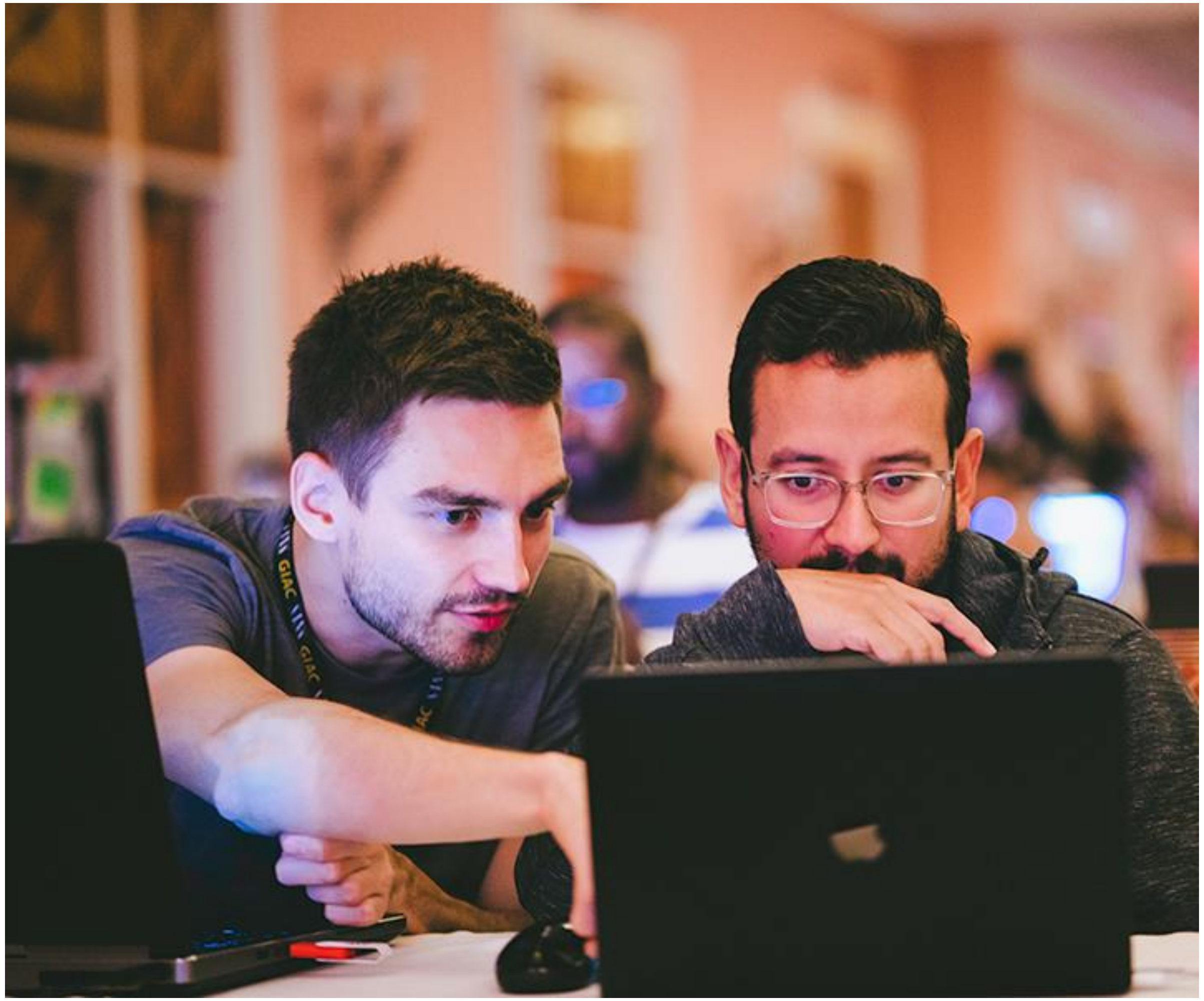
Play CTFs

Compete or don’t

Partner up

Try new things - do something that’s hard for you!

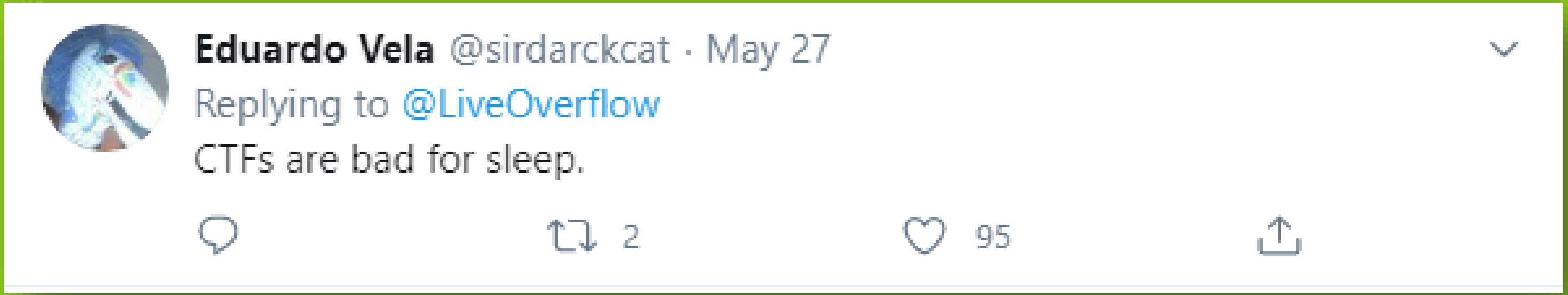
Give honest feedback



THANK YOU!

elgee@counterhack.com

SMcNamee@sans.org



Eduardo Vela @sirdarckcat · May 27

Replying to @LiveOverflow

CTFs are bad for sleep.

COUNTER
HACK