Capture the Flag

Robert Boedigheimer

@boedie

About Me

- Microsoft MVP – Developer Technologies
- Progress Ninja – Fiddler
- ASPInsiders
- Pluralsight Author
- 3rd Degree Black Belt, Tae Kwon Do

- @boedie
- robert@boedie.dev
- www.boedie.dev

Be Safe!

- Windows Sandbox
- Virtual Machine (*Windows - Native Boot*)

What is Capture The Flag (CTF)?

- Not the outdoor game!

- Computer security competition
- Utilize a variety of different security techniques to find “flags”
- Flag typically follows a pattern, like *Flag{…}*

- Name of the challenge is often a hint
- Document how solved (or attempted) for yourself or a writeup

Types

- **Jeopardy** – list of independent challenges for various points
  - Cryptography (or Encoding)
  - Steganography
  - Web Exploitation
  - Forensics
  - Reverse Engineering
  - Binary Exploitation
- Attack/Defend – teams attempt to take over opponents' server or protect their own

GSCC 2020 – Welcome Challenge

d2VsY29tZS10by1jYXB0dXJlLXRoZS1mbGFnIQ

welcome-to-capture-the-flag!

GSCC 2020 – Key Challenge

Use the key to find the flag

key.jpg

KEY-FLAG-CRANK-BANJO

GSCC 2020 – Image is Everything

Download the file. Can you find the flag?

ImageIsEverything.txt

<GRANITE STATE />
{CODE CAMP}
All Your Base Are Belong To Us

GSCC 2020 – Environmentally Friendly

Clue was just a link to a docker image…

stone-feeder-option

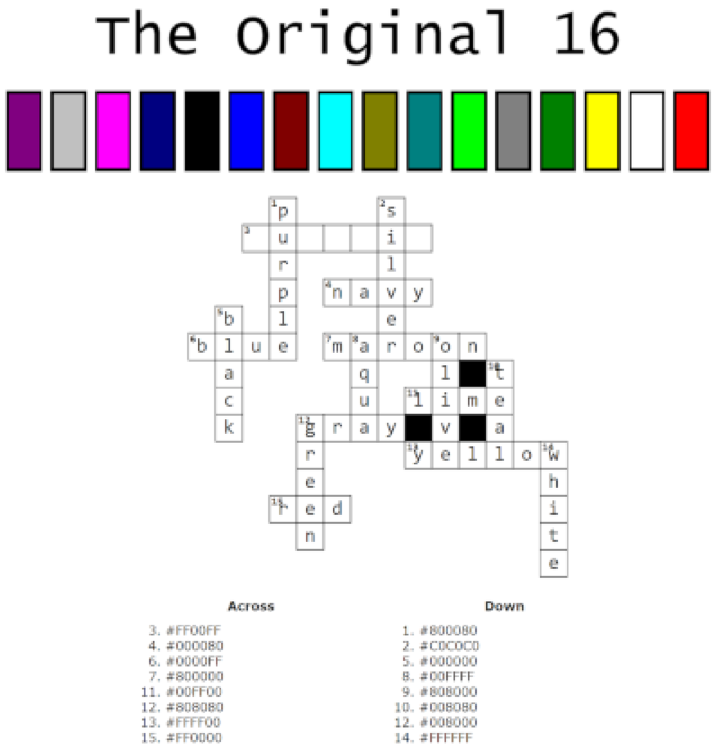
GSCC 2020 – Following Protocol

I'm sure I don't have a key logger uploading what I type, but... can you just check?

capture.pcap file

key=h

GSCC 2021 – Sweet 16



The Original 16

🟪⬜🟪🟦⬛🟦🟥🟦🟨🟦🟩⬜🟩🟨⬜🟥

			1 p				2 s						
		3	u				i						
			r				l						
			p		4 n	a	v	y					
	5 b		l				e						
6 b	l	u	e		7 m	8 a	r	o	9 o	n			
	a					q			l	■	10 t		
	c					u		11 l	i	m	e		
	k			12 g	r	a	y	■	v	■	a		
				r				13 y	e	l	l	o	14 w
				e									h
			15 r	e	d								i
				n									t
													e

Across

3. #FF00FF
4. #000080
6. #0000FF
7. #800000
11. #00FF00
12. #808080
13. #FFFF00
15. #FF0000

Down

1. #800080
2. #C0C0C0
5. #000000
8. #00FFFF
9. #808000
10. #008080
12. #008000
14. #FFFFFF

fuchsia

GSCC 2021 – Free Ebook

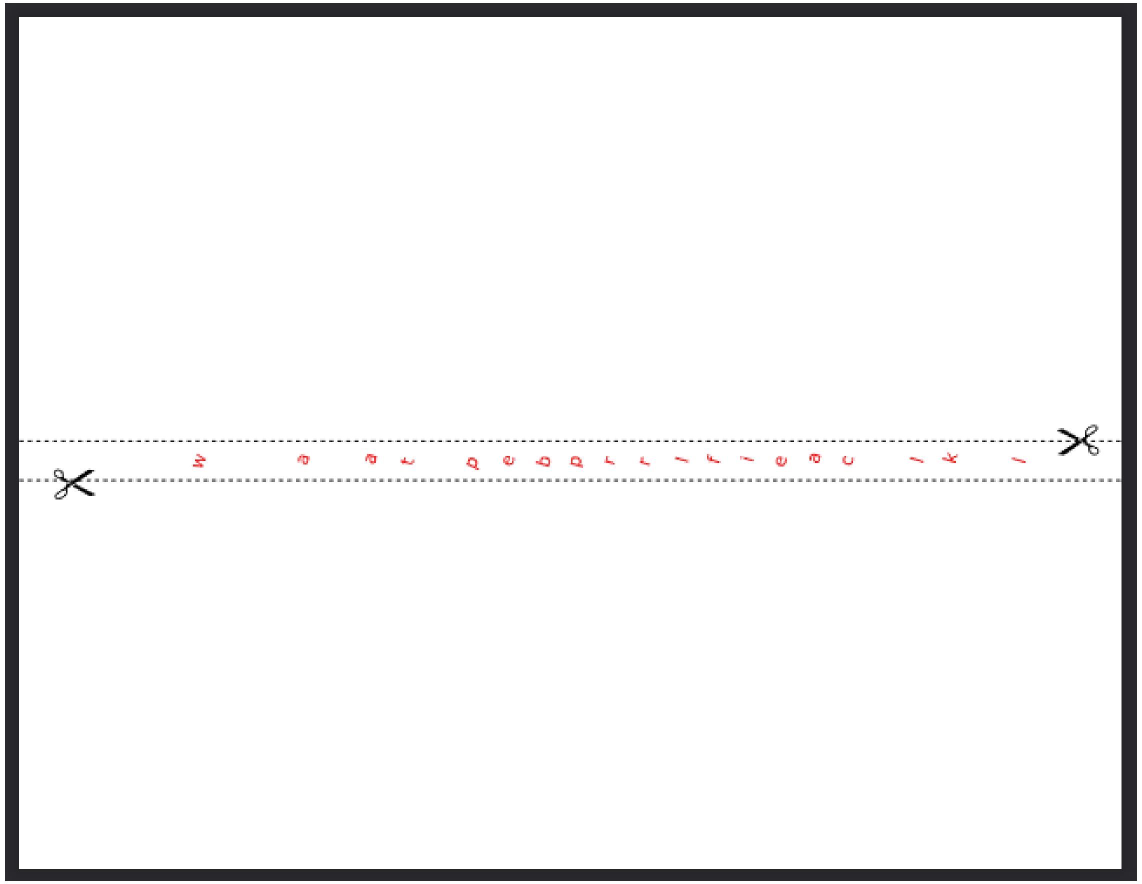
*… for the cost of a monthly subscription

Picture of bookshelf

whale-circuit-coin-claw

GSCC 2021 – All Wound Up

Pencil me in for this challenge!



apple-brick-waterfall

GSCC 2021 – Clueless

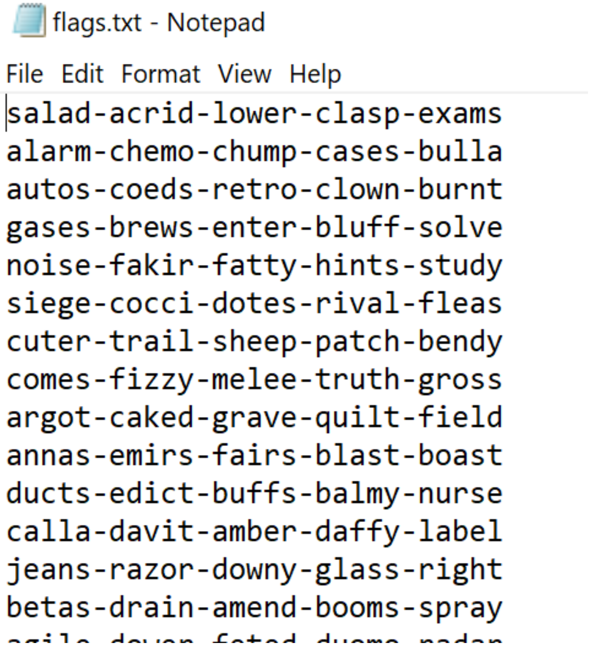
This is an undocumented flag. Can you find it?

Link to web site

anchor-baseball-snowman-unicorn

GSCC 2021 – Choose Wisely

ae443db25650783b78c8f3bd67969062adabe6dd7390b53bbed9f47335fd8db7



```
salad-acrid-lower-clasp-exams
alarm-chemo-chump-cases-bulla
autos-coeds-retro-clown-burnt
gases-brews-enter-bluff-solve
noise-fakir-fatty-hints-study
siege-cocci-dotes-rival-fleas
cuter-trail-sheep-patch-bendy
comes-fizzy-melee-truth-gross
argot-caked-grave-quilt-field
annas-emirs-fairs-blast-boast
ducts-edict-buffs-balmy-nurse
calla-davit-amber-daffy-label
jeans-razor-downy-glass-right
betas-drain-amend-booms-spray
agile-dower-feted-duomo-radar
```

shelf-fixed-start-chins-steak

GSCC 2022 – Physical Challenge

Must be in-person (or very lucky/intuitive) to get this one. On the day of the event, find the **book** that contains the solution to: 53.20.3 284.6.8 25.9.6

where-big-plant

PicoCTF - Insp3ct0r

Kishor Balan tipped us off that the following code may need inspection:

Link to web site

picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2e7b23e3}

CTFLearn - Where Can My Robot Go?

Where do robots find what pages are on a website?

Hint:

What does disallow tell a robot?

CTFlearn{r0b0ts_4r3_th3_futur3}

Useful Tools

- https://www.telerik.com/fiddler
- Browser DevTools
- https://gchq.github.io/CyberChef/
- *https://www.dcode.fr/en*
- https://www.wireshark.org/

- Linux distributions (bunch of useful hacking tools built in)
  - https://www.kali.org/
  - https://www.parrotsec.org/

Learn More

- https://ctf101.org/
- https://picoctf.org/resources.html
- https://primer.picoctf.org/

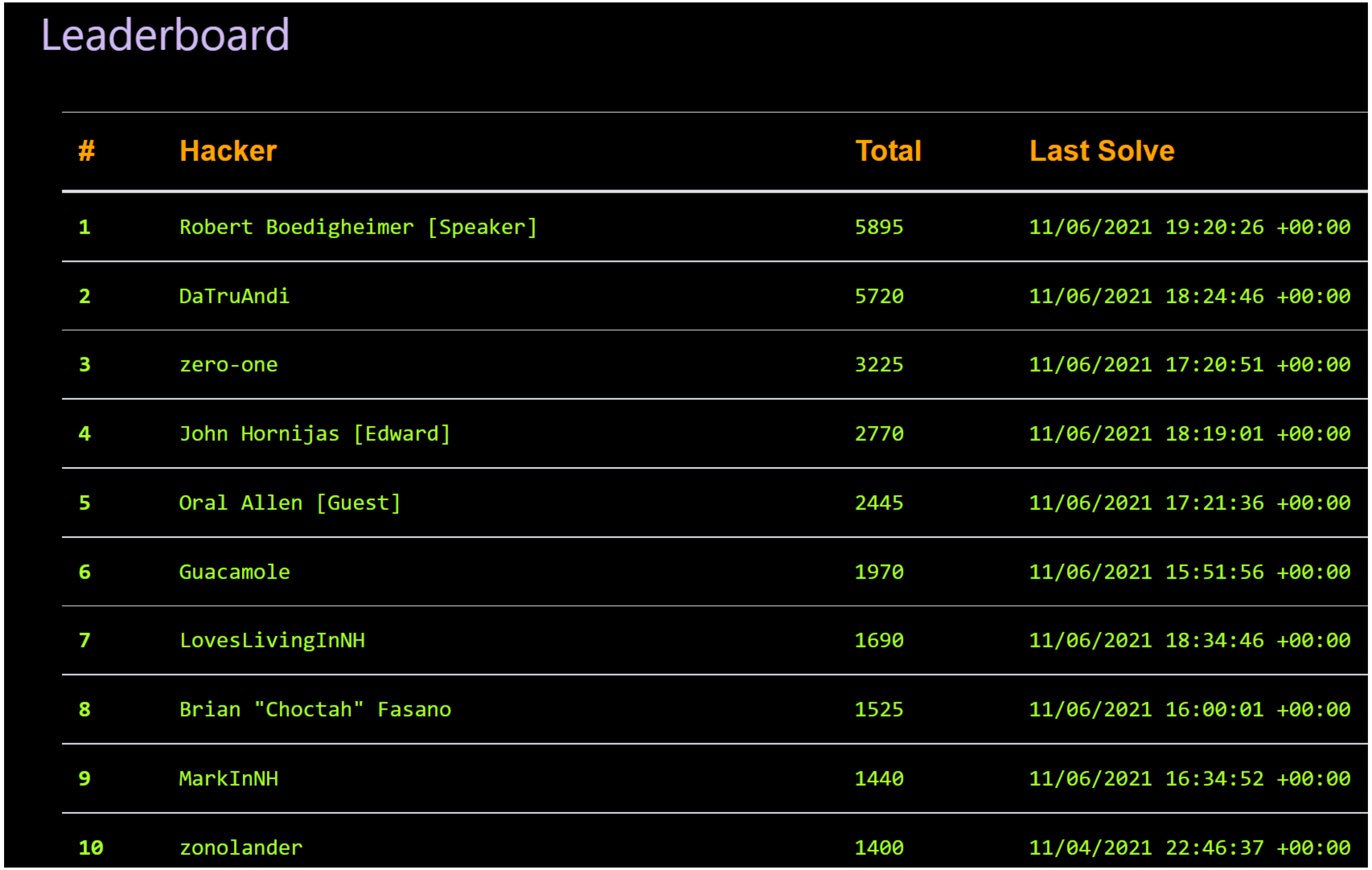
Competitions/Challenges

- https://www.granitestatecodecamp.org/ctf – 12/2/2023
  - Bob Crowley @contrivedex
- https://play.picoctf.org/practice
- https://www.tryhackme.com/christmas - 12/1/2023

- https://ctflearn.com/
- https://ctf.hackthebox.com/
- https://huntress.ctf.games/

- *Major Hacker Conferences (DefCon, Black Hat)*

GSCC 2021



Leaderboard

#	Hacker	Total	Last Solve
1	Robert Boedigheimer [Speaker]	5895	11/06/2021 19:20:26 +00:00
2	DaTruAndi	5720	11/06/2021 18:24:46 +00:00
3	zero-one	3225	11/06/2021 17:20:51 +00:00
4	John Hornijas [Edward]	2770	11/06/2021 18:19:01 +00:00
5	Oral Allen [Guest]	2445	11/06/2021 17:21:36 +00:00
6	Guacamole	1970	11/06/2021 15:51:56 +00:00
7	LovesLivingInNH	1690	11/06/2021 18:34:46 +00:00
8	Brian "Choctah" Fasano	1525	11/06/2021 16:00:01 +00:00
9	MarkInNH	1440	11/06/2021 16:34:52 +00:00
10	zonolander	1400	11/04/2021 22:46:37 +00:00

CAPTURE THE
FLAG 2021
<GRANITE STATE />
{CODE CAMP}

Bob Won
(I didn't help)

Write Ups

- https://github.com/crowleysoftware/GSCC2022_CTF_Solutions
- https://github.com/crowleysoftware/GSCCCTF2021
- https://github.com/crowcoder/GSCCCTF_WriteUp
- tinyurl.com/picoCTF2022

Resources

- https://www.pluralsight.com/authors/robert-boedigheimer
  - Introduction to Cryptography in .NET
  - Fiddler
  - Debugging Your Website with Fiddler and Chrome DevTools

- Sites to safely practice techniques (non-CTF)
  - OWASP Juice Shop
  - Damn Vulnerable Web App (DVWA)

Questions

- @boedie
- robert@boedie.dev
- www.boedie.dev