

CCDC: Let's get down to *BUSINESS*

I promise this is important T.T



Weekly Schedule

Date	CPTC (10AM-12PM)	CCDC (1PM-4PM)
Jul 8	Cyber Bootcamp Kickoff!	
Jul 15	Intro to Pen Testing	Business Week
Jul 22	Hacking Web Apps	Introduction to Networking
Jul 29	Hacking Linux	Securing Linux
Aug 5	Hacking Windows	Securing Windows
Aug 12	How to be a Consultant	Review Week
Aug 19-20	CPTC Tryouts (All day)	
Aug 26		CCDC Tryouts (1-5PM)

whoami

- ❖ **jessica leung | @jeSSH**
- ❖ **CCDC business monkey**
 - ex-windwos team
- ❖ **co-head honcho @ SWIFT**
- ❖ **pentest @ Visa**



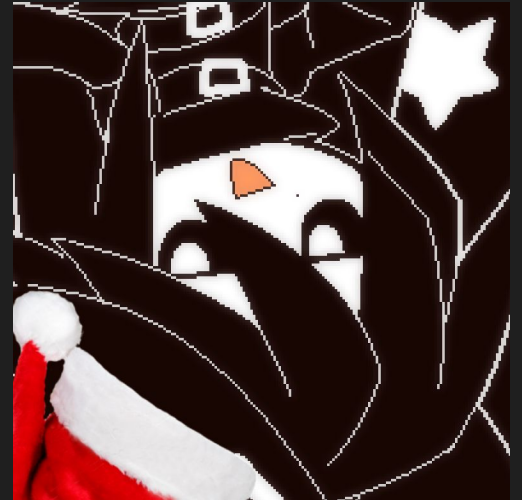
New Inject Came In



Its Compliance

whoami

- ❖ **Marshall Ung | Shadowclaw**
- ❖ **3rd Year CE**
- ❖ **CCDC**
 - Alternate Threat Hunter 2022-2023
 - Threat Hunter 2023
- ❖ **CPTC**
 - Alternate Pentester 2022
 - Pentester 2023



whoami

- ❖ **sydney duong | @sidknee**
- ❖ **CCDC business monkey helper**
- ❖ **external VP for SWIFT**
- ❖ **PMO for ITA @ LA City Hall**

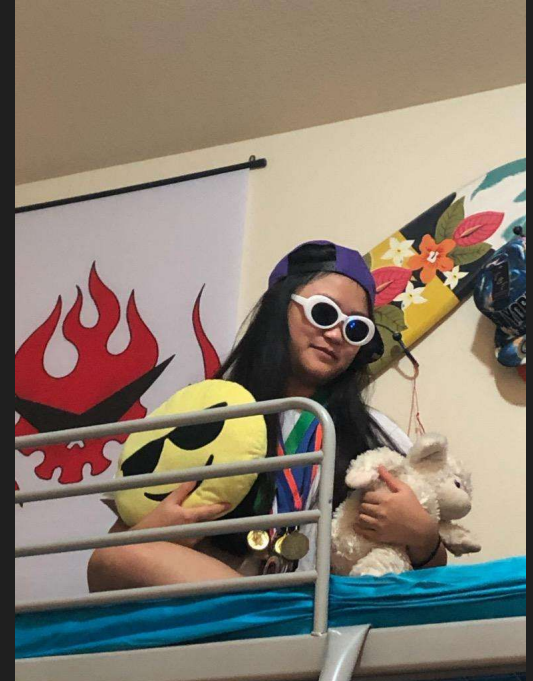


Table of Contents

| 01 Why Business?

| 02 Injects

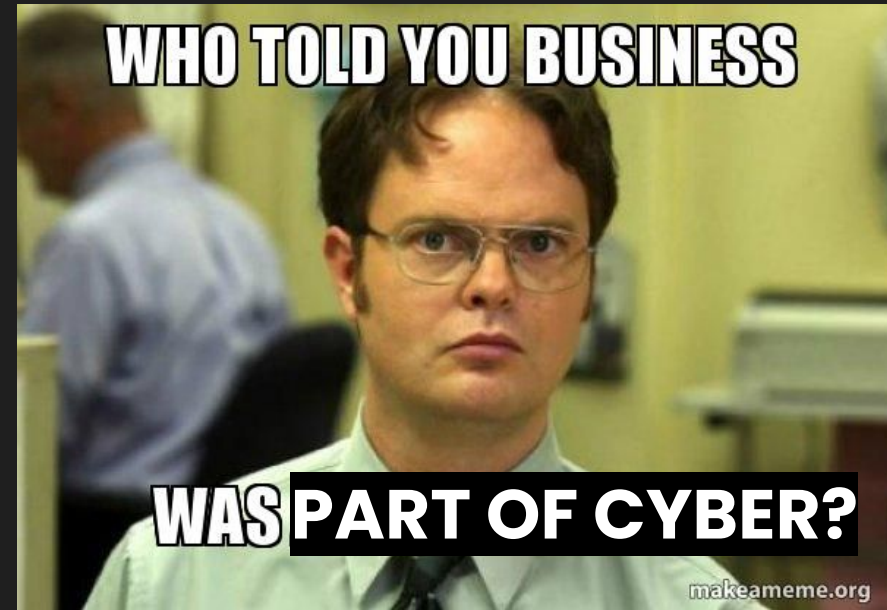
| 03 Forced Vacations

| 04 Report to your boss (us)

01

Business???

Da heck I thought this was a
cyber defense competition??!!!!



Whoa!

Before you roll your eyes...
Cybersecurity serves as a
function of business



CCDC score breakdown

20%

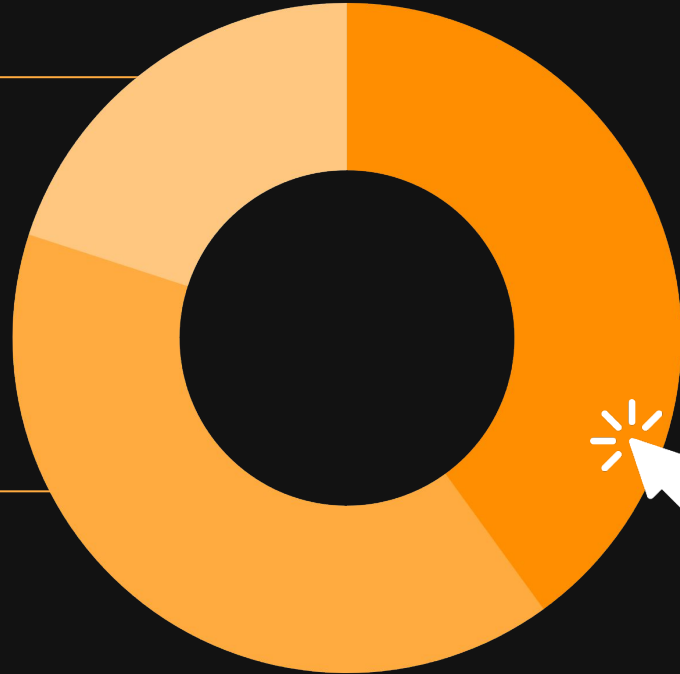
Orange team

40%

Services

40%

Business injects



Fundamental principles of cybersecurity



Integrity



Confidentiality



Availability

Fundamental principles of cybersecurity *(in the context of a business)*



Fundamental principles of cybersecurity (in the context of a business)

**The risk of an interruption
to business is why we are
hired...**

reputational damage



Confidentiality

integrity



Availability

interruption of
business functions

As a result...

**we also have an obligation
to support the business**



It's more
challenging
than you
think...



Infinite curveballs

They took gsuite from me

Technical tasks

Why do we need three firewalls??

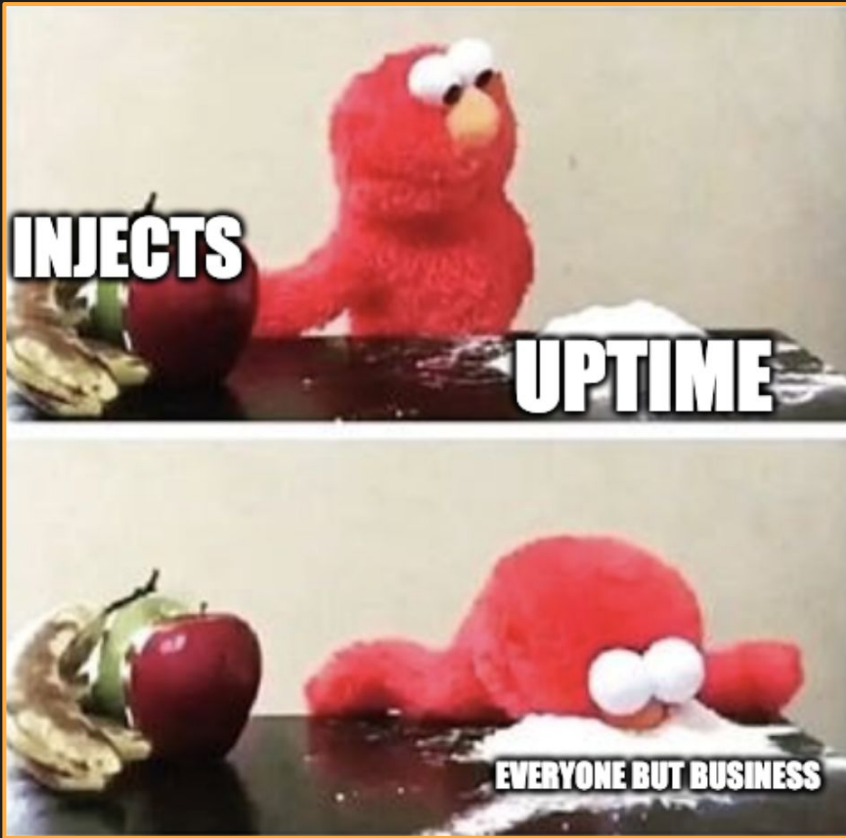
Broad understanding

What even is a cloud and why does it migrate???

02 Injects

No doctors were involved in the making of these slides





Da heck is an inject?

- Tasks from business execs
- Complete within 1 hour
- Write-ups, infographics, *presentations*

- Examples
 - Conduct a security assessment
 - Recommend a cloud solution
 - Write a Disaster Recovery Policy
 - Create an infographic to promote security awareness

Secret sauce to good injects



Be thorough



Use
professional
language



Provide
supporting
evidence



Being thorough



Swiss Bank XChange

Hello Team!

I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good!
Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann



Being thorough



Swiss Bank XChange

Hello Team!

I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good! Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann

Requirements:

1. Perform an **audit of unnecessary software and services**
 - a. Including **everything** removed prior to this inject
2. List the software and services removed
 - a. Make note of **ports that were closed**
3. **Organize findings by host**

Tips:

- **ALWAYS** take notes on what you are doing
- Anticipate inject prompts



Using professional language



Address the recipient



**Take into account who
your audience is**



**Write with intention, get to
the point**



**DON'T use colloquial
language**



DON'T neglect formatting



**DON'T guess about
information – always
check with the team**



Provide supporting evidence

**YOU ARE TRYING TO
CONVINCE YOUR "BOSS"
THAT **YOUR SOLUTION IS
THE BEST SOLUTION****





Provide supporting evidence

- Give **background** about the issue.
 - Would there be fines if we fail to fix it? Potential loss?
- **WHY** did you choose that solution?
 - What other solutions were there?
- **HOW MUCH** does your solution cost?
 - How does that compare to other solutions?
- **WHO** is going to implement your solution?
 - Who is going to maintain it?



Provide supporting evidence – MUST DOs

SHOW YOUR WORK!!

- Screenshots
- Logs
- Examples of config
- Scripts that were run

NEATLY

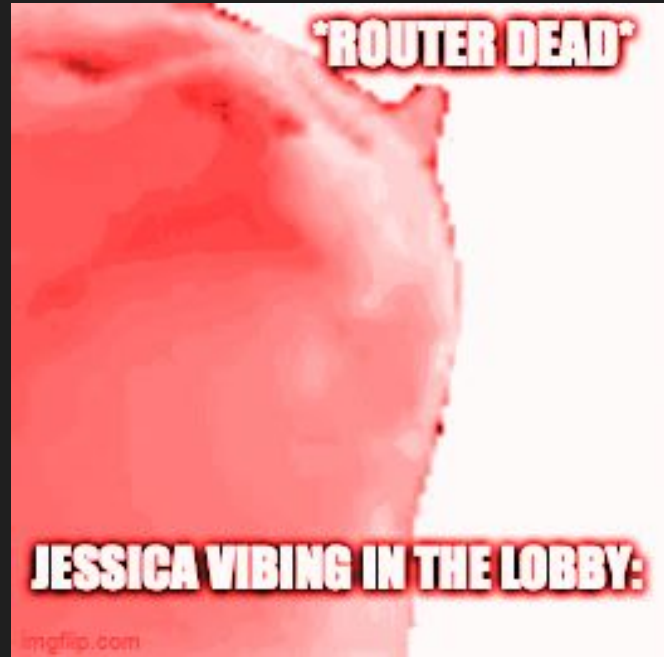
- Categorize your evidence
 - Host
 - OS



03

Forced vacations!

Ayo? :0



Hold up...

VACATION?????

Hold up...

VACATION

**IT'S NOT WHAT
YOU THINK**



1 HOUR

TO CREATE YOUR SLIDES

1 OBJECTIVE

TO PRESENT YOUR BEST PROPOSAL

1 ~~BIG WASTE~~ GOOD USE OF TIME

...where you sit in the lobby and wait your turn while your team cries T.T



How to impress the judges :D (slides edition)



Organized

Declutter your slides!! No long sentences!



Graphics

Use graphs, icons, screenshots...



Sources

USE STATISTICS
AND CITE
SOURCES!

How to impress the judges :D (presentation edition)



Loud

Speak with confidence and rizz them up



Fidgeting

Don't make the judges want to chuck their pens at you



Eye contact

Use open body language and maintain eye contact with the judges

04

Report to your boss!

Bussin Business Bresentation





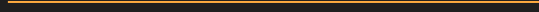
Lab time!

Practice Submitting Injects

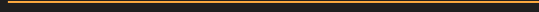
- Injects will be sent through bootcamp discord server in #ccdc-announcements
- Submit your injects to canvas under Assignments > Labs
- Practice submitting on time, but all of them are due as part of this week's hw as completion credit

Tips

- Use the submission template (located in canvas under Assignments > Labs)
- Use professional language and neat formatting
- Be thorough and concise









Surprise! Presentation inject

- Everyone is going to give an individual presentation on a cyber-related topic with **5 minutes prep time**
- Pre-made presentations to choose from (2 people max per topic):
 - Phishing
 - MFA (multi-factor authentication)
 - Types of Malware
- **Edit the slides however you see fit**
- Option to choose your own topic and make your own presentation
- 3 minutes max per presentation
- Camera on optional (but preferred!)
- Won't count towards tryout grade, just practice and do your best!