CYBER SECURITY WORK EXPERIENCE PORTFOLIO

CAPGEMINI

Sanjot Nagra

Contents

Introduction

I am currently a sixth form student at Highfields School who is engaging in work experience with Capgemini for one week (July 10th-14th). The field I am conducting this work experience in is Cyber Security, which complements my interest in Computer Science as a career path. Personally, I have researched and learnt lots about Computer Science but one thing that I am unfamiliar with is Cyber Security. This is because it is not taught in a lot of depth. Therefore, I would like to learn more about how Capgemini deals with Cyber Security and how they manage this with other businesses. Capgemini are responsible for keeping numerous firms' data secure, this is why it is the perfect place for this.

Capgemini, established in 1967 with only seven employees, has evolved into a global frontrunner in digital transformation. By 2022, their workforce has grown to approximately 359,000 employees. Specialising in consulting, digital transformation, technology, and engineering services, Capgemini collaborates with diverse clients using cloud and digital platforms. Their primary objective is to identify, construct, and execute transformative solutions that enable businesses to optimise technology, foster growth, and gain a sustainable competitive advantage over rivals. With a remarkable nine-year streak of being recognised as one of the world's most ethical companies, Capgemini upholds seven core values: Honesty, Boldness, Trust, Freedom, Fun, Modesty, and Team spirit.

Evidence 1 – Introduction to Portfolios

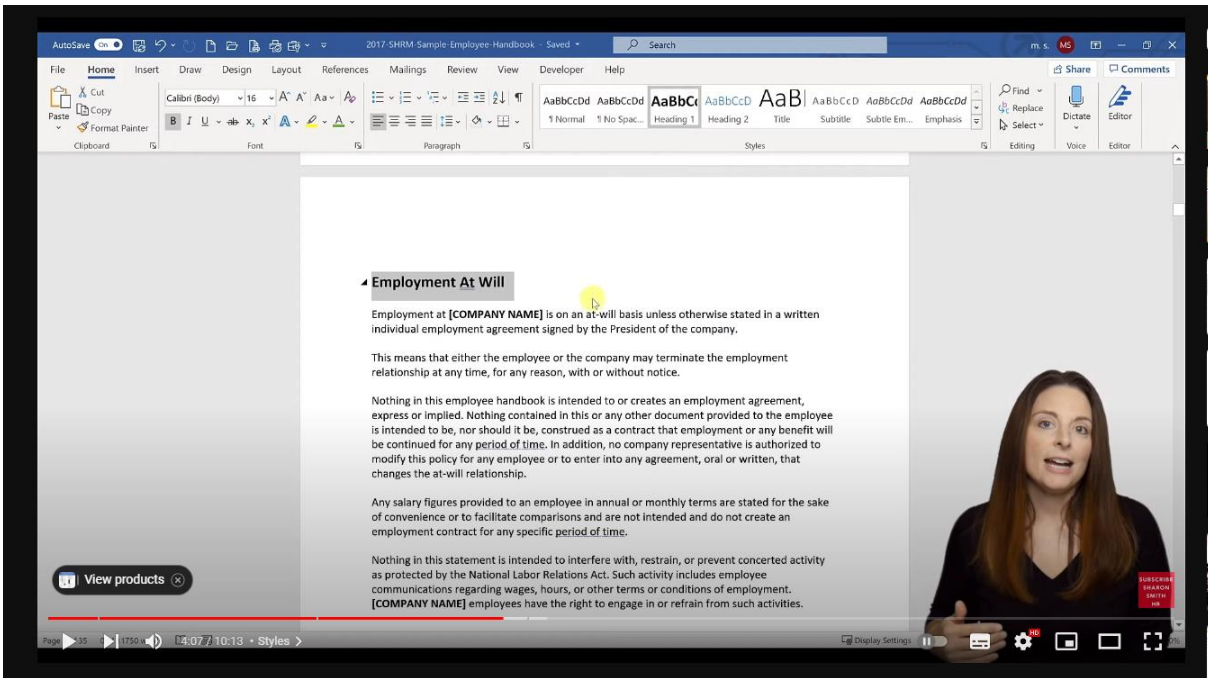
Sanjot Nagra

Situation:

During the initial introduction to the work experience on Monday, we were instructed to create portfolios that would document our work throughout the duration of the experience. The first step involved crafting a cover page, featuring a photo and clear text, to provide an overview of the portfolio. Additionally, we were provided with a YouTube video to assist in creating a table of contents and customising the portfolio's style. Moving forward, the objective was to ensure that the portfolio would be regularly updated daily.

Obstacle:

The main challenge was to effectively design and structure the portfolio to showcase the work experience. This included creating an engaging cover page, using the provided YouTube video to generate a functional table of contents, and maintaining consistent updates to reflect daily progress.



Employment At Will

Employment at **[COMPANY NAME]** is on an at-will basis unless otherwise stated in a written individual employment agreement signed by the President of the company.

This means that either the employee or the company may terminate the employment relationship at any time, for any reason, with or without notice.

Nothing in this employee handbook is intended to or creates an employment agreement, express or implied. Nothing contained in this or any other document provided to the employee is intended to be, nor should it be, construed as a contract that employment or any benefit will be continued for any period of time. In addition, no company representative is authorized to modify this policy for any employee or to enter into any agreement, oral or written, that changes the at-will relationship.

Any salary figures provided to an employee in annual or monthly terms are stated for the sake of convenience or to facilitate comparisons and are not intended and do not create an employment contract for any specific period of time.

Nothing in this statement is intended to interfere with, restrain, or prevent concerted activity as protected by the National Labor Relations Act. Such activity includes employee communications regarding wages, hours, or other terms or conditions of employment. **[COMPANY NAME]** employees have the right to engage in or refrain from such activities.

Action:

To address the challenge, I began by designing a visually appealing cover page for my portfolio. I carefully selected a suitable photo and included clear, concise text to convey the purpose and content of the portfolio. Leveraging the instructions from the YouTube video, I used its guidance to create an organised table of contents that would help navigate the portfolio effectively. Additionally, I customised the style and appearance of the portfolio to enhance its visual appeal and ensure cohesiveness.

Result:

As a result of these actions, I successfully created a portfolio that served as a comprehensive record of my work experience. The cover page provided an engaging introduction, while the table of contents enabled easy navigation throughout the portfolio. By committing to daily updates, I ensured that the portfolio remained up-to-date and accurately reflected my progress and achievements. This diligent approach in portfolio creation demonstrated my organisational skills, diligence, and commitment to maintaining an informative and visually appealing document.

Evidence 2 – Social Engineering Worksheets

Situation:

On Tuesday morning, we had a presentation on social engineering. The presentation focused on the vulnerability of individuals in breaching sensitive data. We examined several case studies, one of which involved a woman manipulating a phone services' customer service team.

Obstacle:

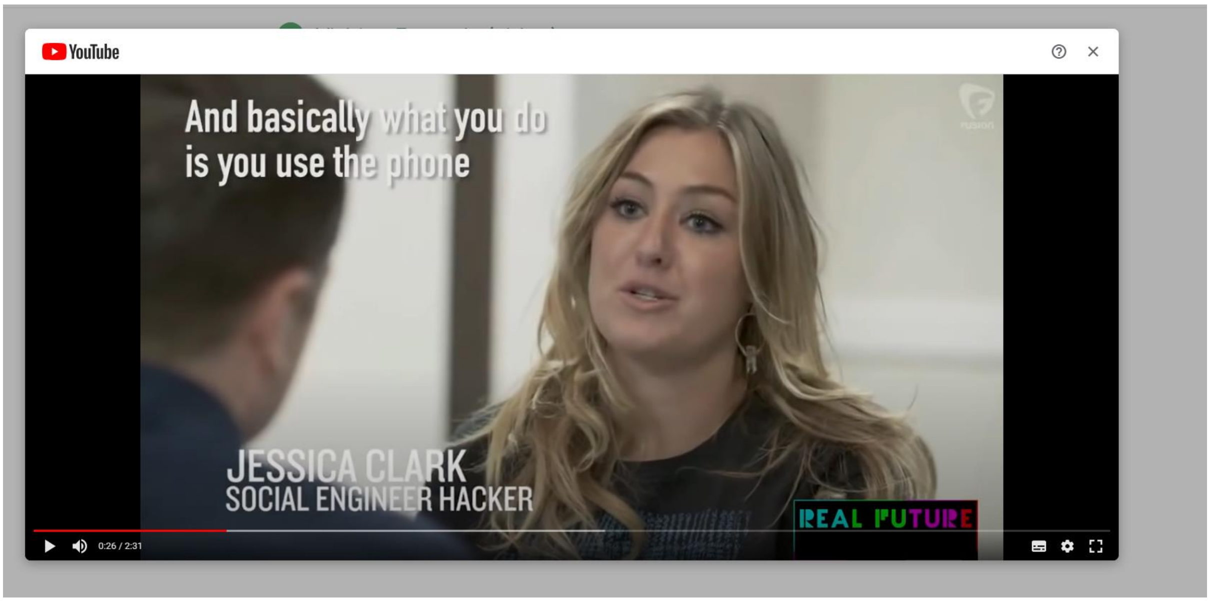
The woman aimed to gain access to the man's phone account by posing as his wife. She pretended that her part of the account was not set up and successfully convinced the customer service team to add her as an authorised user. To make her act seem authentic, she played sounds of a baby crying over the phone.

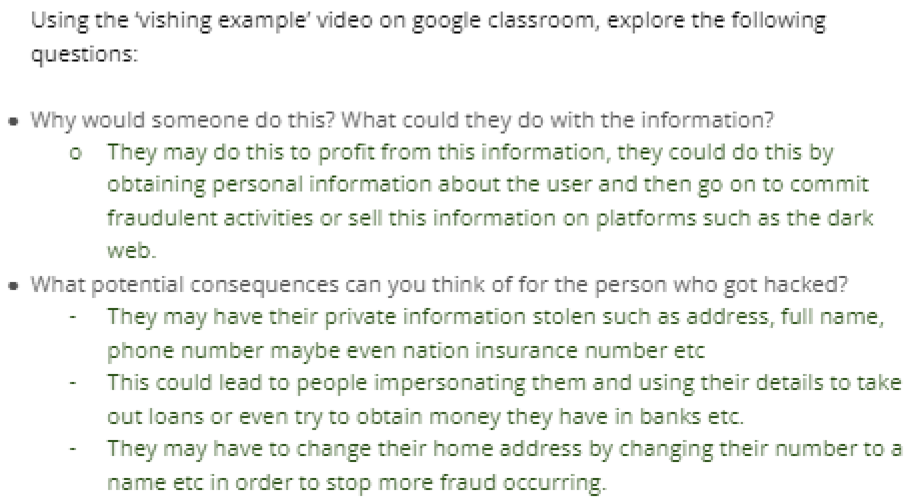
Action:

After watching the video, I was given a worksheet to complete. The worksheet contained various questions related to the case study. I carefully read each question and then reviewed the video to locate the relevant information needed to answer them. I made sure to pay attention to details and took notes to ensure accuracy.

Result:

By thoroughly analysing the video and employing attentive viewing, I successfully answered the questions on the worksheet with an elevated level of detail. This exercise enhanced my understanding of social engineering techniques and how individuals can exploit human vulnerabilities to breach sensitive data to us, a women manipulated a phone services' customer service team by making it appear she was the man's wife, and her part of their phone account was not setup. She was able to convince them to make her an added person onto the account by claiming she was this man's wife and playing sounds of a baby crying to convey an authentic act.




Using the 'vishing example' video on google classroom, explore the following questions:

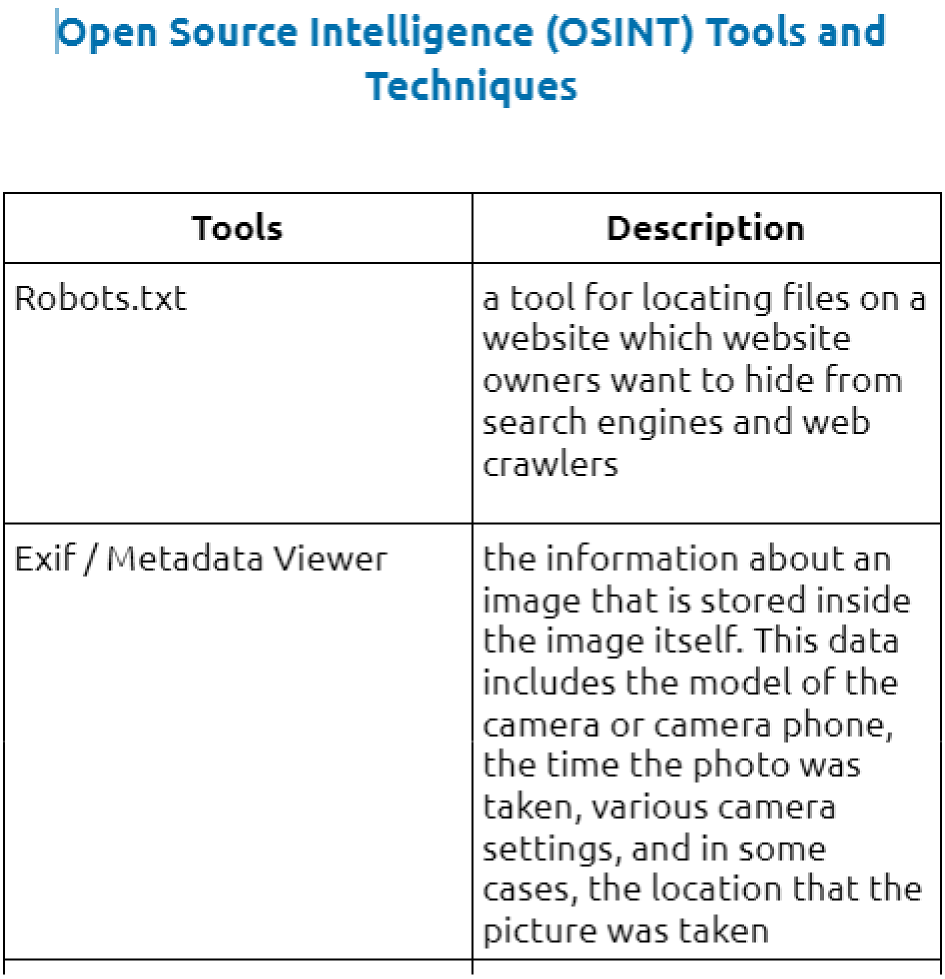
- Why would someone do this? What could they do with the information?
  - They may do this to profit from this information, they could do this by obtaining personal information about the user and then go on to commit fraudulent activities or sell this information on platforms such as the dark web.
- What potential consequences can you think of for the person who got hacked?
  - They may have their private information stolen such as address, full name, phone number maybe even nation insurance number etc
  - This could lead to people impersonating them and using their details to take out loans or even try to obtain money they have in banks etc.
  - They may have to change their home address by changing their number to a name etc in order to stop more fraud occurring.

Situation:

The next task in my portfolio involved a worksheet focused on OSINT (Open Source Intelligence) terms. I was required to define these terms by conducting online research.

Obstacle:

To complete the worksheet, I needed to gather accurate definitions for the OSINT terms. This required conducting thorough online research to find reliable sources and information.



Open Source Intelligence (OSINT) Tools and Techniques

Tools	Description
Robots.txt	a tool for locating files on a website which website owners want to hide from search engines and web crawlers
Exif / Metadata Viewer	the information about an image that is stored inside the image itself. This data includes the model of the camera or camera phone, the time the photo was taken, various camera settings, and in some cases, the location that the picture was taken

Action:

I approached the task by utilising online resources and conducting targeted searches. I explored various articles and reliable websites related to OSINT. Through careful reading and analysis, I gathered relevant definitions for each term. I took notes and ensured that the definitions I found were accurate and comprehensive.

Result:

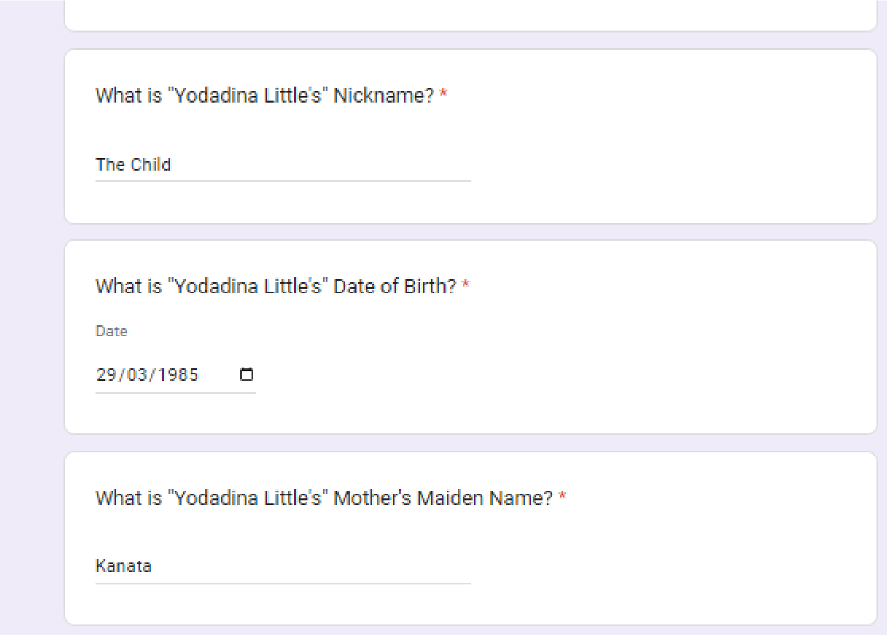
Through my online research efforts, I successfully defined the OSINT terms provided in the worksheet. I filled in the tables with accurate definitions based on the information I gathered. This task allowed me to develop my research skills and deepen my understanding of OSINT concepts different articles to then fill in the tables.

The Situation:

For my final task, I was assigned to collect information on an individual named Yodadina Little. To gather the necessary information, I began by searching the internet.

Obstacle:

The challenge was to find relevant information about Yodadina Little that would provide details such as their educational background and other pertinent details. The information needed to be sourced from various online platforms and websites.



What is "Yodadina Little's" Nickname? *

The Child

What is "Yodadina Little's" Date of Birth? *

Date

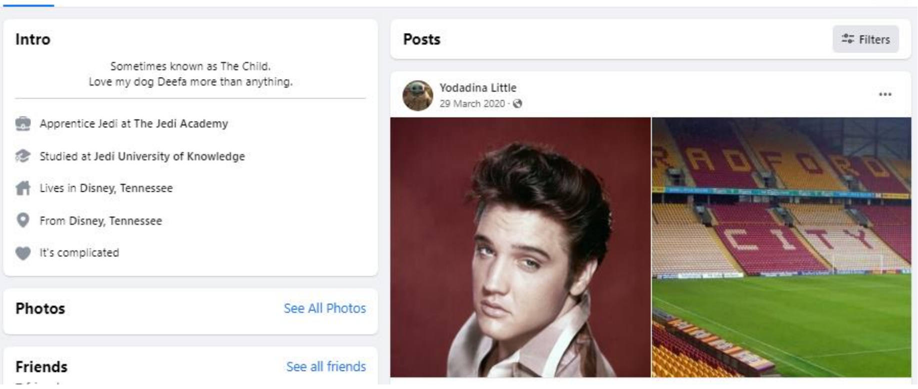
29/03/1985

What is "Yodadina Little's" Mother's Maiden Name? *

Kanata

Action:

To accomplish this task, I initiated an internet search using Yodadina Little's name as a starting point. During my search, I came across a Facebook page that belonged to the individual. This page proved to be a valuable resource, as it contained a wealth of information and pictures related to Yodadina Little. I carefully reviewed the available content, including details about their education and other aspects of their life.



Intro

Sometimes known as The Child.
Love my dog Deefa more than anything.

Apprentice Jedi at The Jedi Academy

Studied at Jedi University of Knowledge

Lives in Disney, Tennessee

From Disney, Tennessee

It's complicated

Photos — See All Photos

Friends — See all friends

Posts — Filters

Yodadina Little
29 March 2020 ·

Result:

By exploring the Facebook page, I was able to collect various pieces of information about Yodadina Little. The information included details about their educational background and other relevant aspects. The abundance of pictures and accompanying information made the process relatively easy and efficient. This task allowed me to effectively utilise online platforms to gather targeted information and deepen my understanding of information retrieval techniques.

Evidence 3 – ICS/OT Presentation

Situation:

On Wednesday morning, our class received a lesson on ICS (Industrial Control Systems) and OT (Operational Technology) attacks in the context of cyber hacking. Following the lesson, we were assigned a task to research companies that had experienced such attacks. I selected CPC organisation in Taiwan and Colonial Pipeline company in the US as my chosen companies. Both companies had fallen victim to ransomware attacks.

Obstacle:

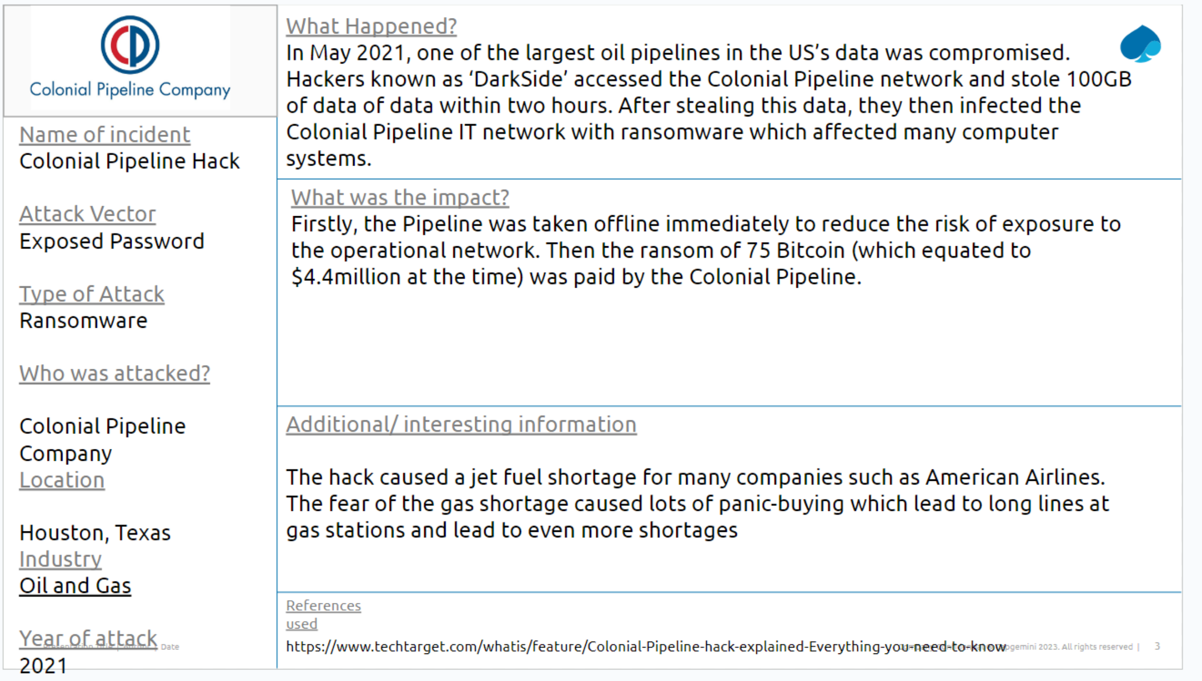
The challenge was to gather accurate and comprehensive information about the ICS and OT attacks targeting CPC organisation and Colonial Pipeline. Additionally, presenting the findings to the class required organising the information in a clear and concise manner.

Action:

To complete the task, I conducted extensive research on the selected companies and their respective ransomware attacks. I explored various online sources, articles, and reports to gather relevant information. I focused on understanding the methods employed in the attacks and the consequences faced by the companies. With the obtained information, I prepared a presentation to share my findings with the class. I included screenshots of the presentations to visually support the information presented.

Result:

I successfully gathered detailed information about the ICS and OT attacks that targeted CPC organisation in Taiwan and Colonial Pipeline company in the US. Through my research, I acquired a deep understanding of the attack methods and the impact on the affected companies. During the presentation, I shared the findings and insights with the class, using the captured screenshots to enhance the clarity and visual impact of the information. This task allowed me to develop my research and presentation skills while expanding my knowledge of cyber hacking and its implications on critical infrastructure systems.



Name of incident
Colonial Pipeline Hack

Attack Vector
Exposed Password

Type of Attack
Ransomware

Who was attacked?
Colonial Pipeline Company

Location
Houston, Texas

Industry
Oil and Gas

Year of attack
2021

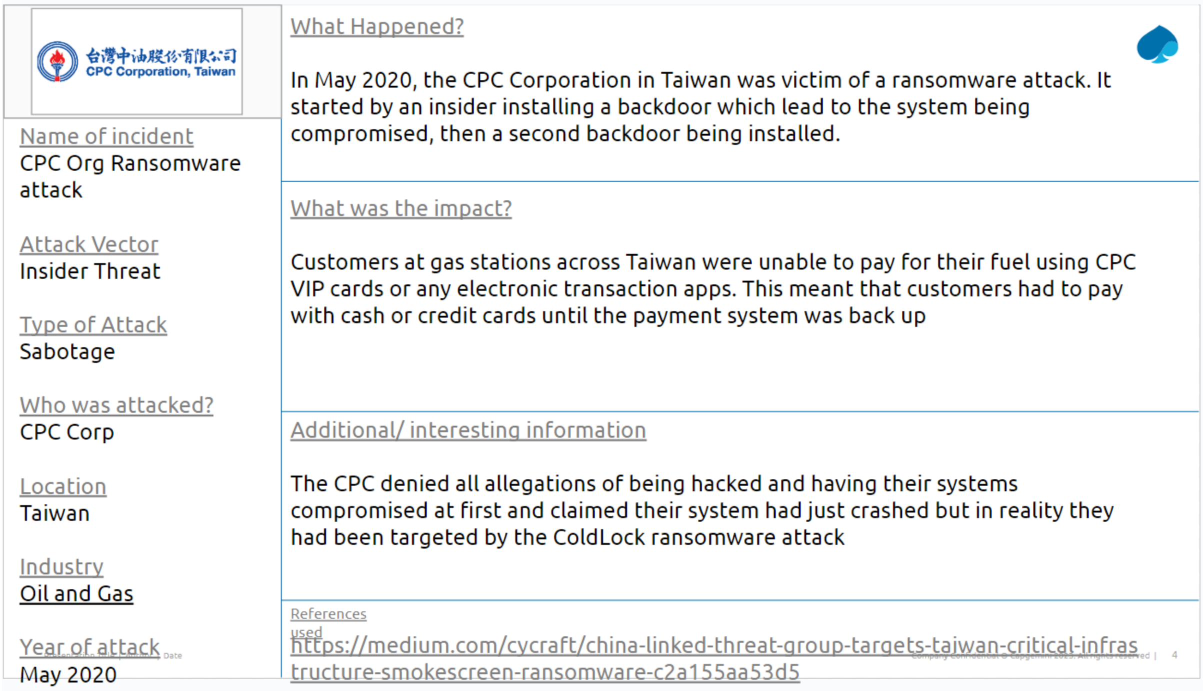
What Happened?
In May 2021, one of the largest oil pipelines in the US's data was compromised. Hackers known as 'DarkSide' accessed the Colonial Pipeline network and stole 100GB of data of data within two hours. After stealing this data, they then infected the Colonial Pipeline IT network with ransomware which affected many computer systems.

What was the impact?
Firstly, the Pipeline was taken offline immediately to reduce the risk of exposure to the operational network. Then the ransom of 75 Bitcoin (which equated to $4.4million at the time) was paid by the Colonial Pipeline.

Additional/ interesting information

The hack caused a jet fuel shortage for many companies such as American Airlines. The fear of the gas shortage caused lots of panic-buying which lead to long lines at gas stations and lead to even more shortages

References used
https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know



Name of incident
CPC Org Ransomware attack

Attack Vector
Insider Threat

Type of Attack
Sabotage

Who was attacked?
CPC Corp

Location
Taiwan

Industry
Oil and Gas

Year of attack
May 2020

What Happened?

In May 2020, the CPC Corporation in Taiwan was victim of a ransomware attack. It started by an insider installing a backdoor which lead to the system being compromised, then a second backdoor being installed.

What was the impact?

Customers at gas stations across Taiwan were unable to pay for their fuel using CPC VIP cards or any electronic transaction apps. This meant that customers had to pay with cash or credit cards until the payment system was back up

Additional/ interesting information

The CPC denied all allegations of being hacked and having their systems compromised at first and claimed their system had just crashed but in reality they had been targeted by the ColdLock ransomware attack

References used
https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

Evidence 4 – Capture the Flag

Situation:

During my sessions on Thursday, we participated in a capture the flag task, consisting of over one hundred tasks with varying point values based on their difficulty. The tasks encompassed areas such as website vulnerability exploitation, Linux command usage, and challenges related to binary and cryptography.

Obstacle:

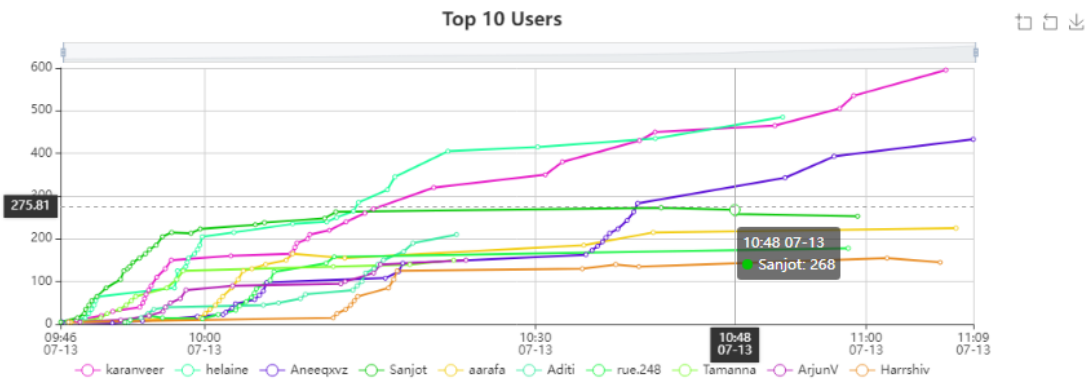
The challenge was to successfully navigate through the capture the flag tasks, conducting research, and leveraging developer tools within the provided websites. Additionally, it required enhancing my understanding of Linux commands and applying knowledge of binary and cryptography to decode messages using ciphers like substitution and Caesar.

Action:

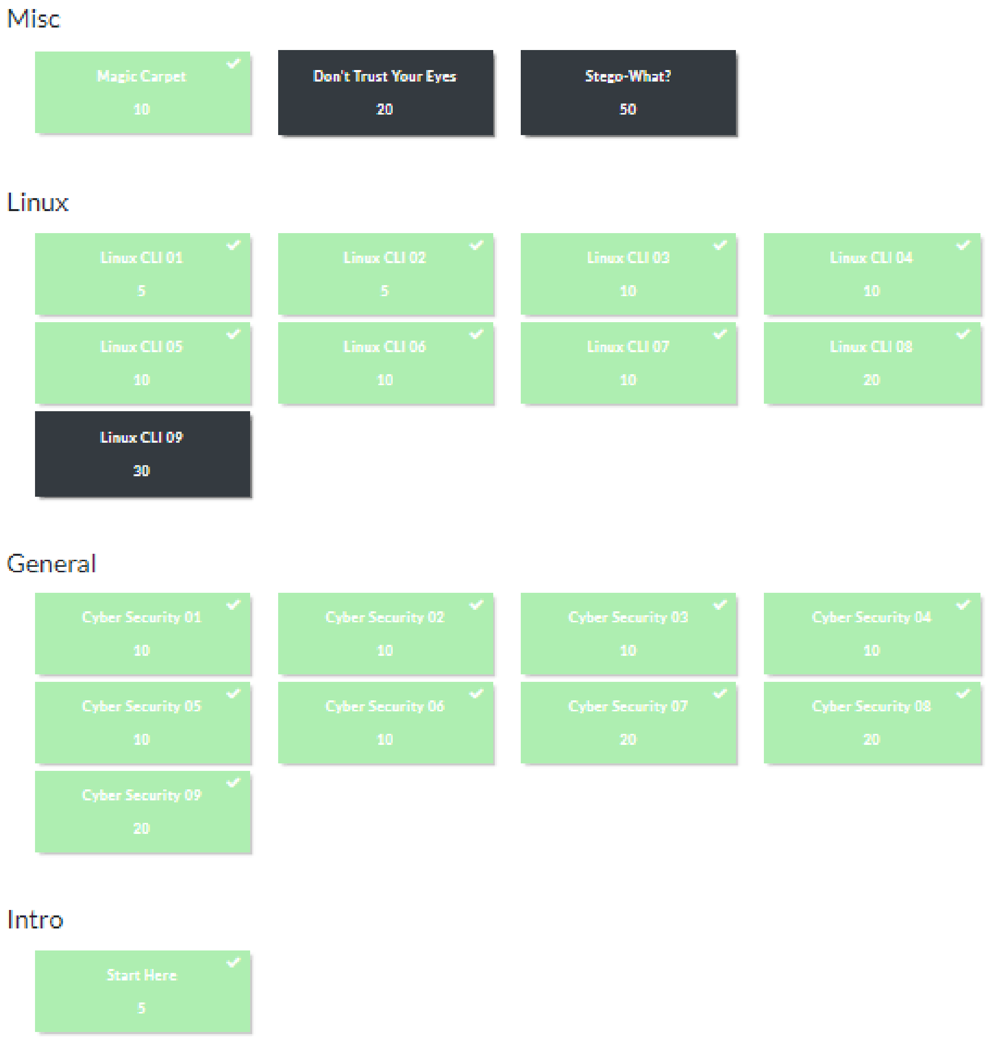
To overcome these challenges, I engaged in extensive research within the provided websites using developer tools. This allowed me to uncover sensitive information and exploit vulnerabilities within the systems. Furthermore, I dedicated time to researching different Linux commands, which improved my proficiency in using the terminal effectively. Additionally, I tackled numerous tasks centred around binary and cryptography, employing decryption techniques to decode messages encrypted with ciphers such as substitution and Caesar.

Result:

As depicted in the screenshot, my efforts and dedication paid off, resulting in a commendable achievement. Amongst my peers, I secured the fourth position in the capture the flag task. This outcome serves as a testament to my acquired skills in website vulnerability analysis, Linux command usage, and cryptographic problem-solving. This experience not only expanded my knowledge but also showcased my ability to perform well in a competitive environment.



Place	User	Score
1	karanveer	595
2	helaine	485
3	Aneeqxvz	433
4	Sanjot	253



Misc

Magic Carpet ✓
10

Don't Trust Your Eyes
20

Stego-What?
50

Linux

Linux CLI 01 ✓
5

Linux CLI 02 ✓
5

Linux CLI 03 ✓
10

Linux CLI 04 ✓
10

Linux CLI 05 ✓
10

Linux CLI 06 ✓
10

Linux CLI 07 ✓
10

Linux CLI 08 ✓
20

Linux CLI 09
30

General

Cyber Security 01 ✓
10

Cyber Security 02 ✓
10

Cyber Security 03 ✓
10

Cyber Security 04 ✓
10

Cyber Security 05 ✓
10

Cyber Security 06 ✓
10

Cyber Security 07 ✓
20

Cyber Security 08 ✓
20

Cyber Security 09 ✓
20

Intro

Start Here ✓
5

Evidence 5 – CISCO Presentation

Situation:

On Friday, during my last session, I was given the task of creating a presentation that consolidated my knowledge from previous sessions. The objective was to identify and discuss the most significant cyber threats faced by businesses, focusing from the perspective of a CISCO. I decided to structure my presentation around four key factors: Phishing, Ransomware, Insider Information, and IoT Security.

Obstacle:

The challenge involved gathering and synthesising information from previous sessions to create a comprehensive presentation on business's major cyber threats. I needed to effectively communicate the significance of Phishing, Ransomware, Insider Information, and IoT Security in the context of business cybersecurity, while also aligning with the expectations of my host.

Action:

To tackle the task, I began by reviewing the knowledge I had acquired from previous sessions on cybersecurity. I conducted additional research to gather the most up-to-date information on the identified cyber threats: Phishing, Ransomware, Insider Information, and IoT Security. I then organised my presentation, outlining the key points for each topic and providing relevant examples and insights. I focused on presenting the information in a clear and engaging manner, utilising visuals, and supporting data to enhance the message.

What is an Organisations Biggest Cyber Challenge?

1

Phishing Attacks

2

Ransomware

3

Insider Threats

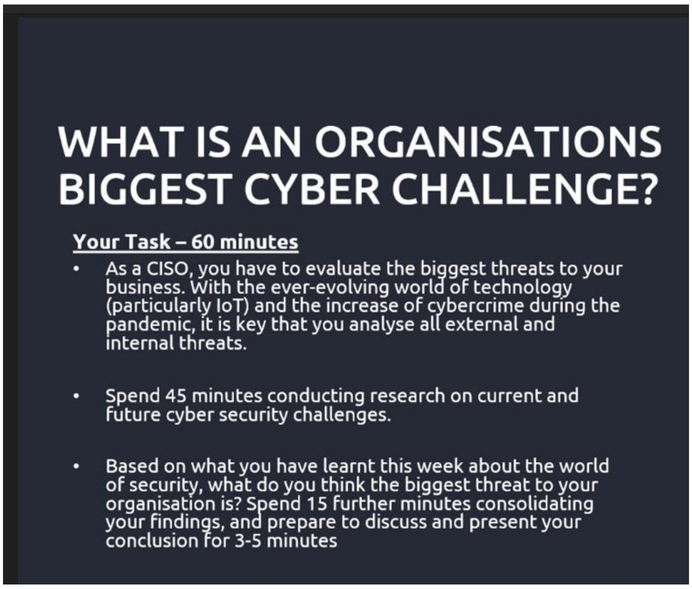
4

IoT Security

5

Result:

With thorough preparation and effective presentation skills, I successfully delivered my presentation on the major cyber threats faced by businesses. I highlighted the significance of Phishing, Ransomware, Insider Information, and IoT Security and provided valuable insights and examples related to each topic. The host of the session was highly pleased with my presentation, indicating that I effectively conveyed my knowledge and demonstrated a comprehensive understanding of the subject matter. This achievement showcased my ability to analyse and communicate complex cybersecurity concepts and underscored my aptitude in addressing business's cybersecurity challenges from a CISCO perspective.



WHAT IS AN ORGANISATIONS BIGGEST CYBER CHALLENGE?

Your Task – 60 minutes

- As a CISO, you have to evaluate the biggest threats to your business. With the ever-evolving world of technology (particularly IoT) and the increase of cybercrime during the pandemic, it is key that you analyse all external and internal threats.
- Spend 45 minutes conducting research on current and future cyber security challenges.
- Based on what you have learnt this week about the world of security, what do you think the biggest threat to your organisation is? Spend 15 further minutes consolidating your findings, and prepare to discuss and present your conclusion for 3-5 minutes