Here are the code.org projects I completed. Unfortunately, I can't provide all the details for the questions. This is the most I can offer.

## Unit 1 Project: Cyberchef CTF

I learned how to tackle cybersecurity puzzles by following this guide! It breaks down different challenges, like finding hidden info or cracking codes, into steps I can follow. This way I can solve them myself and improve my cybersecurity skills.

**CTF Challenges (Required)**

Use the answer boxes below to document any CTF challenges you completed.  Be sure to include information about **how** you solved the problem – Imagine you’re writing a how-to guide for future cybersecurity students!

**Trivia Challenges**

|  |  |
| --- | --- |
| **👥 Challenge 1:** Honesty is Best Policy | **Solution:  The "Honesty is Best Policy" challenge is a trivia challenge that involves finding information related to a specific cybersecurity concept or principle.** |
| **How to Solve:How to Solve:**  **Read the Challenge Prompt: Carefully read the challenge prompt to understand what information is being sought. In this case, it's likely related to honesty in cybersecurity.**  **Search for Clues: Look for keywords or hints in the challenge prompt that can guide your search. In this challenge, focus on honesty and its relevance in cybersecurity.**  **Use Search Engines: Utilize search engines like Google to look for information related to honesty in cybersecurity. Use keywords such as "honesty in cybersecurity" or "integrity in information security."**  **Check Trusted Sources: Ensure that the information you find is from reputable sources. Government websites, cybersecurity organizations, and well-known experts in the field are good places to verify information.**  **Extract Relevant Information: Once you find information related to honesty in cybersecurity, extract the relevant details that directly answer the challenge. This could include principles, best practices, or examples.**  **Submit the Answer: Enter the extracted information or answer into the platform you are using to complete the challenge.** | |

|  |  |
| --- | --- |
| **👥 Challenge 2:** Lots of Jobs! | **Solution:  Solution: The "Lots of Jobs!" challenge likely involves identifying and understanding various job roles or positions within the cybersecurity field.** |
| **How to Solve: How to Solve:**  **Read the Challenge Prompt: Carefully read the challenge prompt to understand the specific requirements. It may ask for a list of cybersecurity job roles, their responsibilities, or other related information.**  **Brainstorm Initial Ideas: Before searching, brainstorm a list of common cybersecurity job roles you are already familiar with. This can help you start your search with a foundation.**  **Use Online Resources: Utilize online resources such as cybersecurity job boards, industry websites, or career guides to gather information about different job roles in cybersecurity.**  **Explore Specializations: Cybersecurity encompasses various specializations such as penetration testing, incident response, malware analysis, and more. Ensure that you cover a diverse range of roles to provide a comprehensive answer.**  **Check Certifications: Look into cybersecurity certifications as they often correspond to specific job roles. Certification websites or official documentation can provide insights into the skills and responsibilities associated with each certification.**  **Compile Information: Create a list or document summarizing the different cybersecurity job roles, their responsibilities, and any notable skills or qualifications required.**  **Submit the Answer: Enter the compiled information into your platform to complete the challenge.** | |

|  |  |
| --- | --- |
| **👥 Challenge 3:** Hostage | **Solution:  Solution: The "Hostage" challenge likely involves a scenario where you need to rescue or recover a compromised system or data.** |
| **How to Solve:**  **Read the Challenge Prompt: Carefully read the challenge prompt to understand the scenario, the compromised system, and any additional information provided.**  **Identify the Type of Attack: Determine the type of attack or compromise described in the challenge. This could be a ransomware attack, unauthorized access, data breach, etc.**  **Gather Initial Information: Take note of any information provided in the prompt, such as the affected system, the attacker's demands, or any specific details about the compromise.**  **Research the Attack Scenario: Conduct research on the type of attack mentioned in the challenge. Understand common techniques, tools, and mitigation strategies associated with that particular attack.**  **Formulate a Plan: Based on your research, formulate a plan to recover the compromised system or data. This might involve isolating the affected system, restoring from backups, or employing specific security measures.**  **Implement the Plan: Follow through with your plan to recover the compromised system or data. If the challenge involves interacting with a simulated environment, use the provided tools or commands to execute your plan.**  **Verify the Resolution: Ensure that the compromised system is successfully recovered. Check for any lingering vulnerabilities or traces of the attack.**  **Document the Steps Taken: If the CTF platform requires documentation, write a summary of the steps you took to resolve the situation. Include details about the attack, your research, and the actions you performed.**  **Submit the Answer: Enter the necessary information or documentation into your platform to complete the challenge.** | |

**Reconnaissance Challenges**

|  |  |
| --- | --- |
| **👥 Challenge 4:** 11,185,272 | **Solution:   The "11,185,272" challenge likely involves reconnaissance to discover information related to a specific target, such as an IP address, domain, or network.** |
| **How to Solve:**  **Check for Clues in the Prompt: Read the challenge prompt for any hints or clues about the target. Look for keywords that may indicate the type of information you need to discover.**  **Use Network Scanning Tools: Utilize network scanning tools like Nmap to scan the specified target. Perform a comprehensive scan to identify open ports, services running, and potentially vulnerable areas.**  **DNS Enumeration: If the challenge involves a domain, use DNS enumeration tools to gather information about the domain, such as associated subdomains, mail servers, and name servers.**  **WHOIS Lookup: Perform a WHOIS lookup on any provided domain information. This can reveal details about domain ownership, registration date, and contact information.**  **Use Online Databases: Cross-reference any identified IP addresses or domains with online databases that catalog information about websites, services, or known vulnerabilities.**  **Check for Hidden Information: Examine the source code of web pages, if applicable, for hidden comments, metadata, or any information that may lead to additional details about the target.**  **Explore Port-Specific Information: If the numerical value in the challenge title represents a port number, research common services associated with that port and potential vulnerabilities.**  **Document Findings: Keep detailed notes of the information you discover, including IP addresses, domains, open ports, and any other relevant data.**  **Submit the Answer: Enter the identified information into the CTF platform as your solution to the challenge.** | |

|  |  |
| --- | --- |
| **👥 Challenge 5:** Read Me | **Solution:   Solution: The "Read Me" challenge likely involves finding information within a provided file or document.** |
| **How to Solve: How to Solve:**  **Download and Examine the File: If the challenge provides a file to read, download and examine its contents. The file may be a text document, image, or archive.**  **Check for Hidden Information: Look for hidden information within the file. This could include comments, metadata, or any encoded messages.**  **Explore File Properties: Examine the properties of the file, especially if it's an image or document. Some files contain additional details in their metadata.**  **Use Appropriate Tools: Depending on the file type, use appropriate tools to extract information. For text documents, a simple text editor may suffice. For images, tools like exiftool can reveal metadata.**  **Decode Encoded Messages: If there are encoded messages within the file, use decoding techniques or online tools to decipher the information.**  **Look for Patterns or Clues: Analyze the content for patterns, clues, or references that may lead to the solution. Pay attention to any keywords or phrases that stand out.**  **Document Findings: Keep detailed notes of any information you find within the file.**  **Submit the Answer: Enter the discovered information as your solution to the challenge.** | |

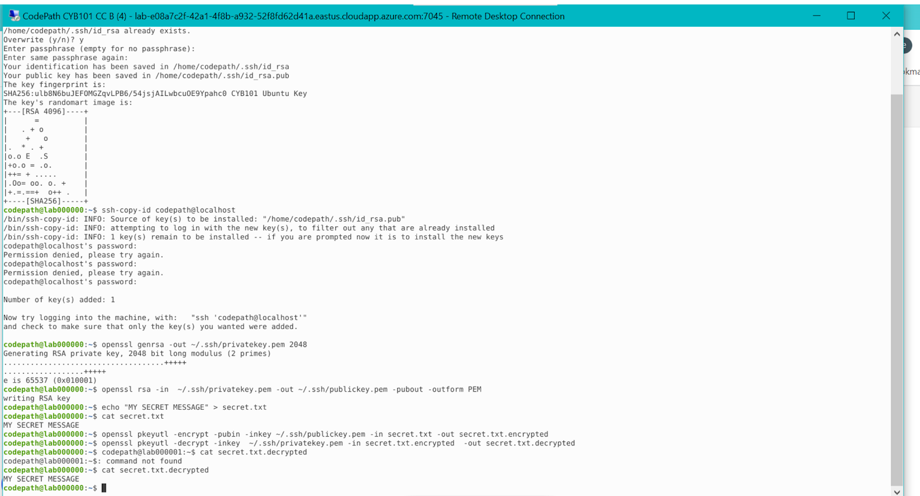
|  |  |
| --- | --- |
| **👥 Challenge 6:** Three Even, Two Odd | **Solution:  The "Three Even, Two Odd" challenge likely involves manipulating or analyzing numerical values to meet a specific condition.** |
| **How to Solve: How to Solve:**  **Understand the Challenge: Read the challenge prompt to understand the condition or requirement. In this case, it likely involves manipulating numbers to have three even and two odd values.**  **Start with Random Values: Begin by trying random sets of numbers and checking if they meet the condition. Adjust the numbers iteratively to reach the desired combination.**  **Consider Constraints: If there are constraints mentioned in the challenge (e.g., numbers within a specific range), make sure to adhere to them while experimenting.**  **Use Simple Math Operations: Experiment with basic mathematical operations (addition, subtraction, multiplication, division) to manipulate the numbers and achieve the required combination.**  **Automate the Process: If possible, write a simple script or use a programming language to automate the process of trying different combinations until the condition is satisfied.**  **Document the Solution: Once you find a set of numbers that meets the condition, document the solution.**  **Submit the Answer: Enter the identified set of numbers as your solution to the challenge.** | |

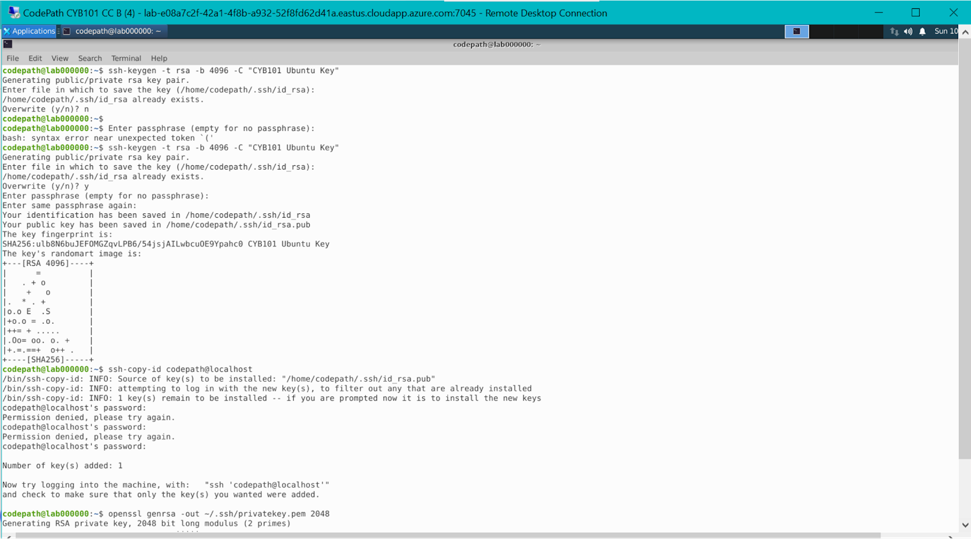
**Cryptography Challenges**

|  |  |
| --- | --- |
| **👥 Challenge 7:** Shifty | **Solution:   Solution: The "Shifty" challenge likely involves a form of encryption or encoding that requires deciphering to reveal hidden information.** |
| **How to Solve: How to Solve:**  **Analyze the Challenge Prompt: Read the challenge prompt for any hints or clues about the type of encryption or encoding used. Look for keywords that may suggest a specific technique.**  **Look for Patterns: Examine the encoded text for any patterns or repetitions. This can provide insights into the encryption method used.**  **Check for Common Algorithms: Consider common cryptographic algorithms or encoding techniques such as Caesar cipher, Base64, XOR, etc. Try decoding the text using these methods.**  **Brute Force Attack: If the encryption method is not immediately clear, consider using a brute force approach. Try applying different algorithms systematically until you find the correct one.**  **Frequency Analysis: If the text appears to be a substitution cipher, use frequency analysis to identify common letters or patterns. This can help decipher the encoding.**  **Use Online Tools: There are various online tools and websites that offer automatic decoding for common encryption methods. Use these tools to quickly test different possibilities.**  **Iterate and Adjust: If your initial attempts do not yield results, iterate and adjust your approach based on the feedback you receive from decoding attempts.**  **Document the Solution: Once you successfully decode the message, document the solution, including the method you used.**  **Submit the Answer: Enter the decoded information as your solution to the challenge.** | |

## Project 2: All About SSH Keys

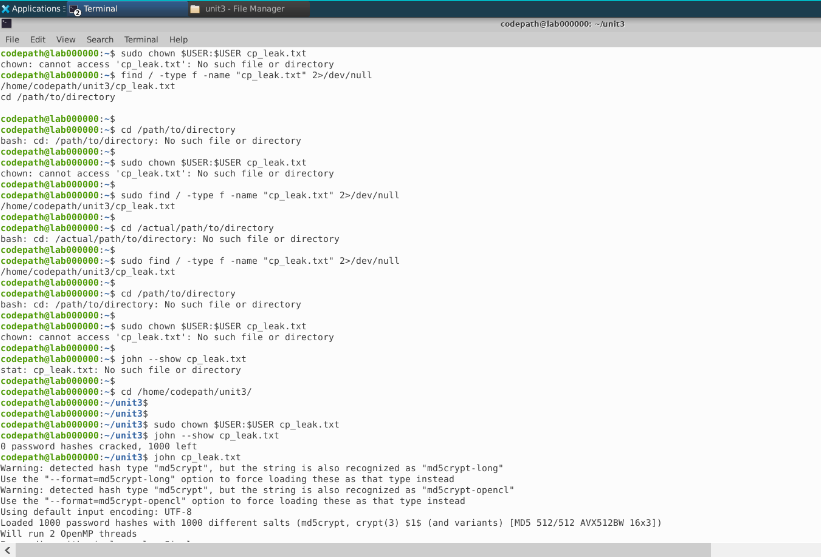
This project teaches how to use special keys to log in securely to computers and scramble messages so only certain people can read them.

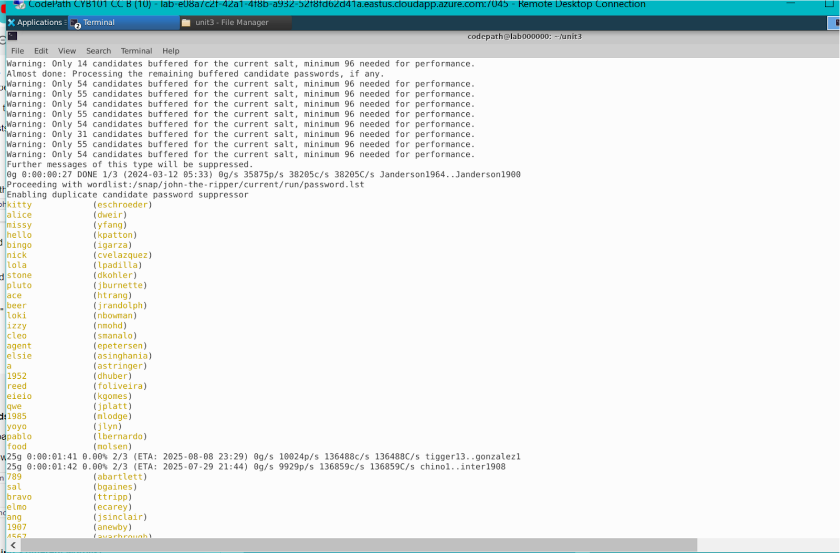


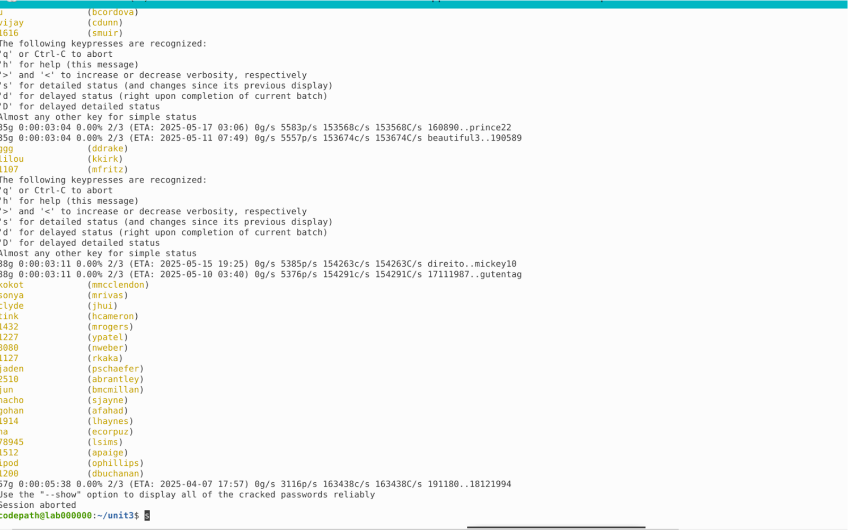
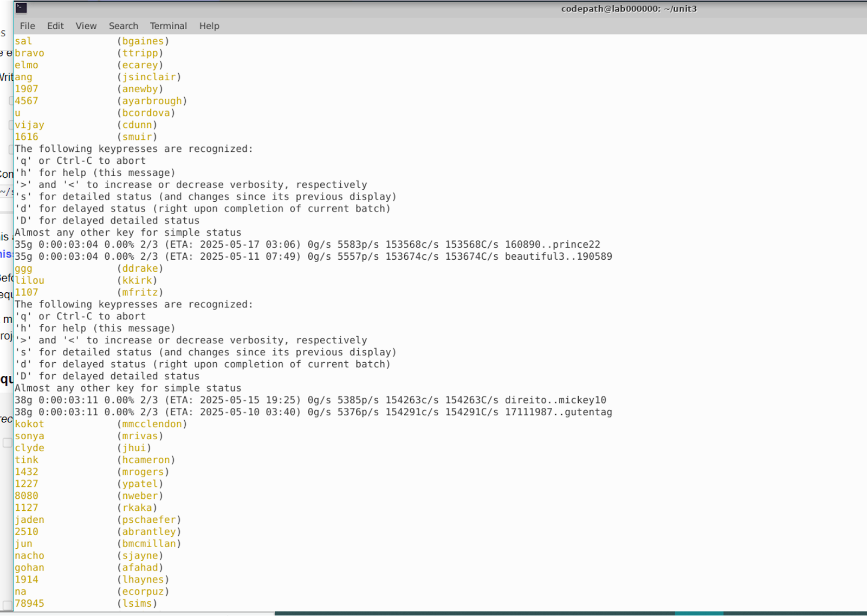


## Project #3: Password Crack-a-thon

Project 3: I tested password strength. This helps me understand why complex passwords are important and how weak passwords can be easily cracked.

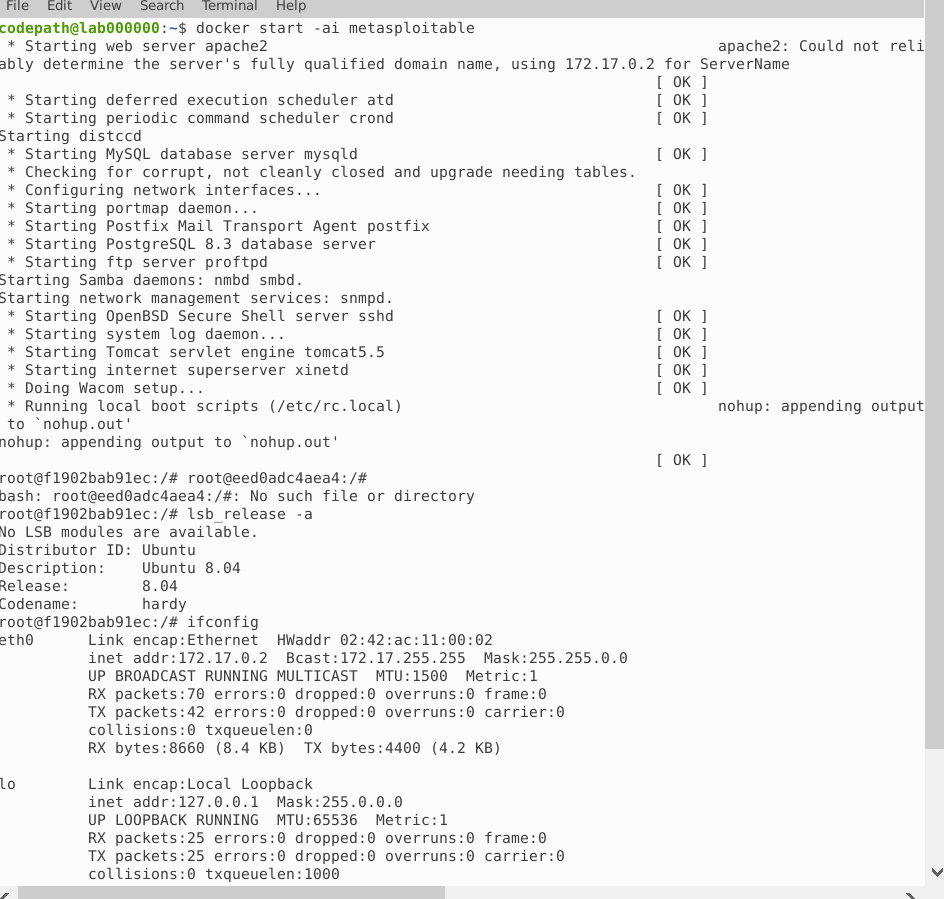


****

****

## Project #4: Exploits!

I explored software vulnerabilities. This shows how important it is to keep software up-to-date and why software companies release security patches.

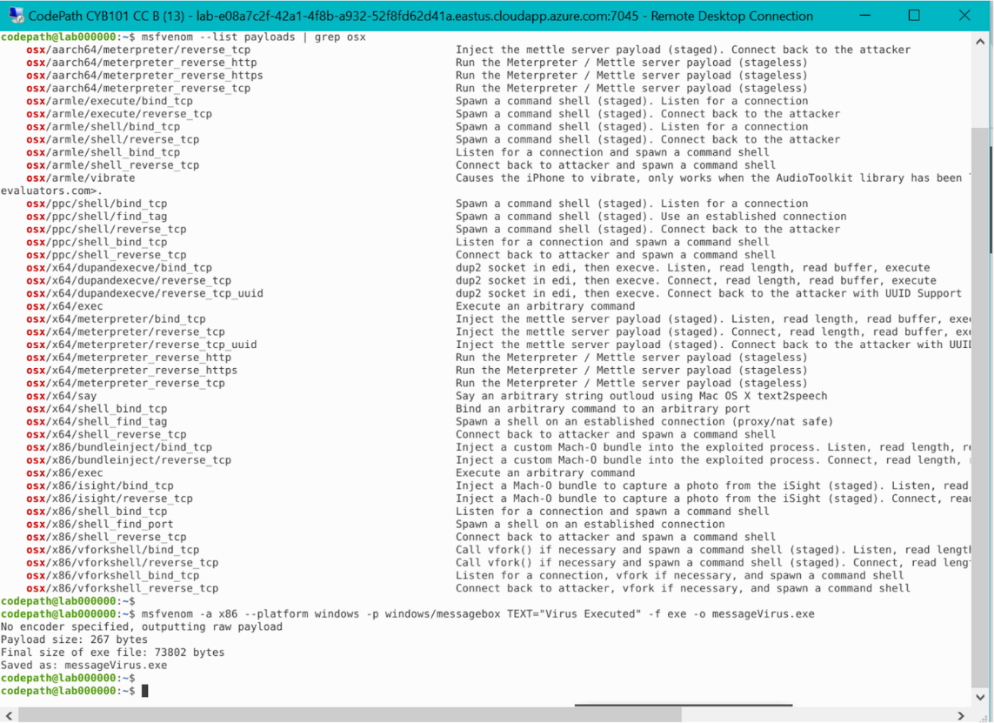
****

****

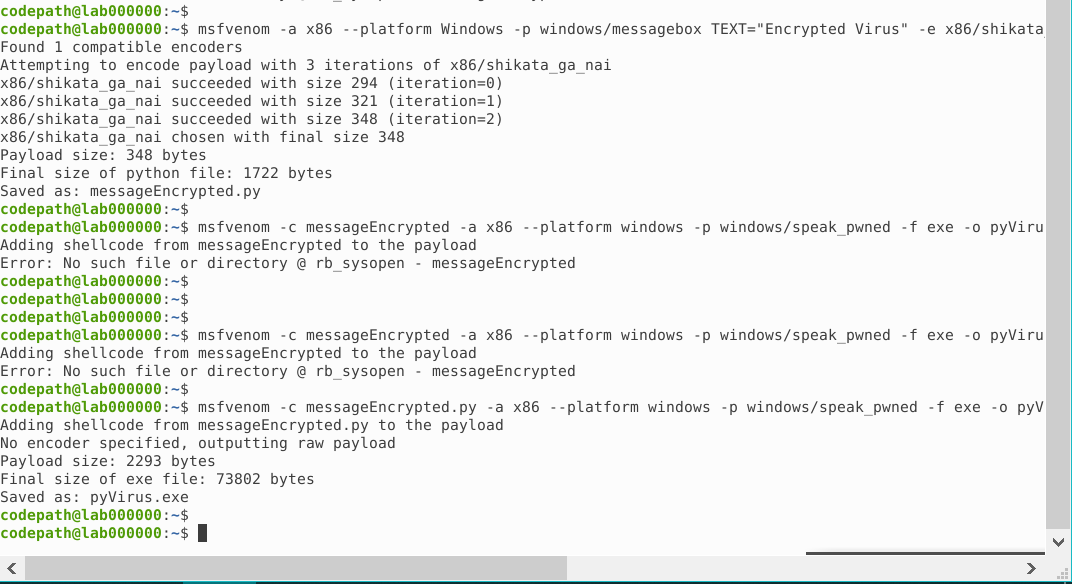
****

## Project 5: DIY Malware

Project 5 I explored how viruses are built using MS Venom, but in a safe environment.

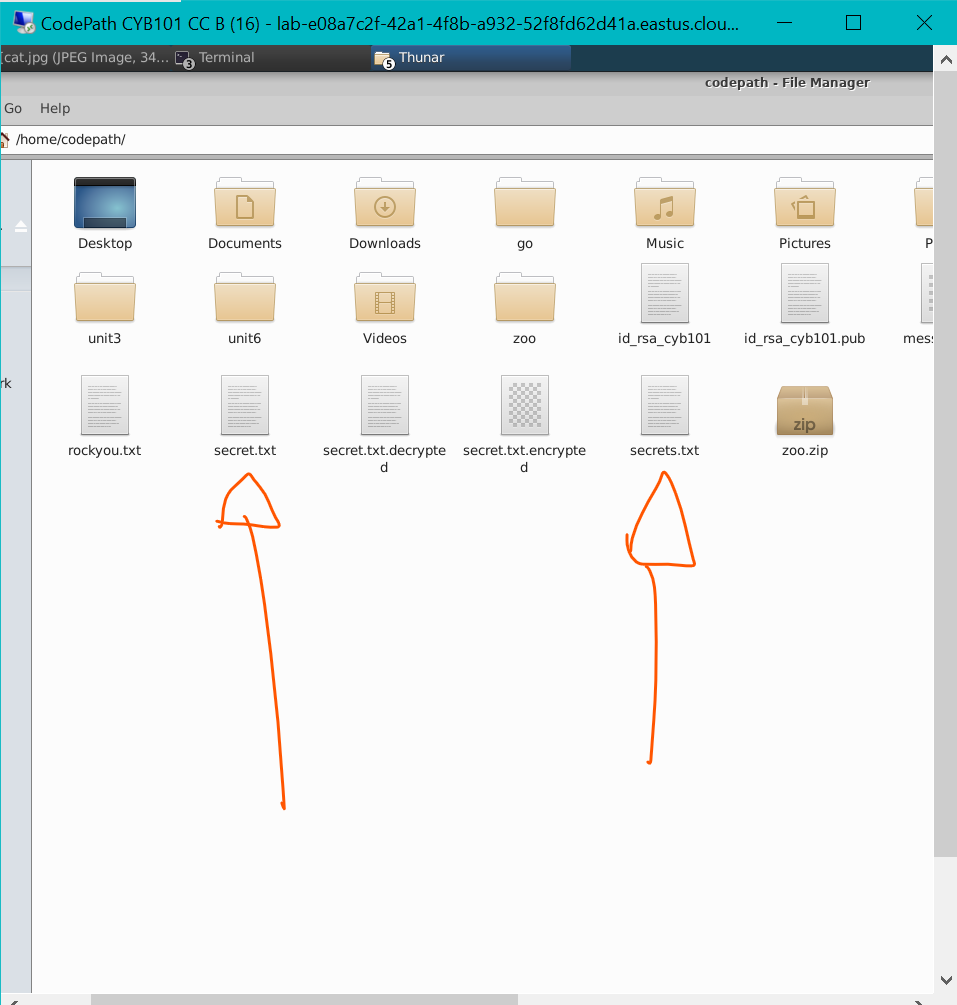
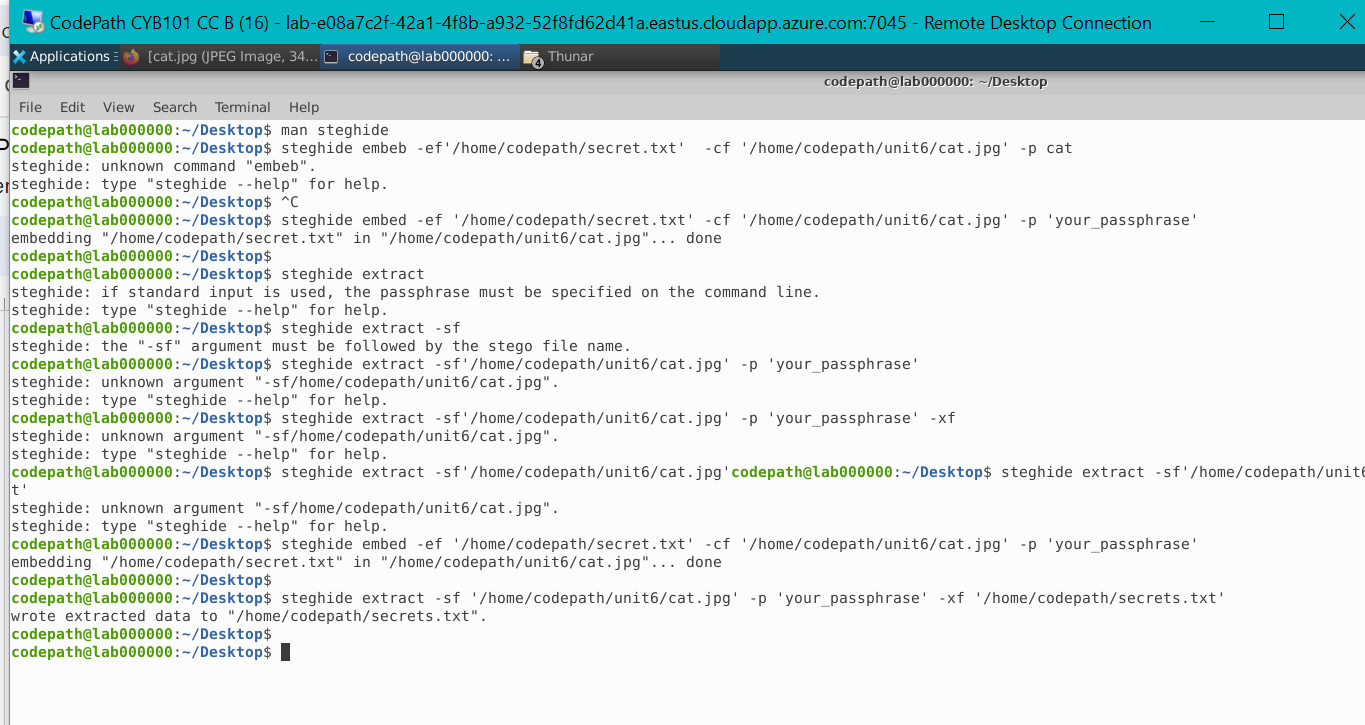
****

****

****

## Project #6: Steghide and Seek

Project 6 let me hide messages inside pictures using Steghide! I learn how to do this by creating messages in a picture through Linux.

.****