Cybersecurity Portfolio

Name: Derrick Lamison
Email: Dlam1028@gmail.com
Phone: 909-896-2512
LinkedIn Profile: www.linkedin.com/in/derrick-lamison-b556a888
GitHub Profile: https://github.com/Dlam1028

Introduction

As a cybersecurity professional, I have developed a comprehensive skill set that span both technical and theoretical aspects of cybersecurity. I have applied these skills in a variety of real-world scenarios through hands-on projects, including Python scripting, file handling, incident response, network security, and algorithm development. This portfolio documents my journey and the work I've done throughout the **Google Coursera Cybersecurity Certification Program**.

Skills Acquired

- **Python Programming**: Writing and debugging Python code, file manipulation, parsing data, and algorithm development.
- **Cybersecurity Fundamentals**: Understanding threat landscape, vulnerability management, incident response, and network security concepts.
- **Risk Management**: Identifying risks and implementing controls for data protection and secure access management.
- **Incident Handling**: Documenting and managing security incidents, leveraging both manual and automated tools.
- **File Handling & Data Security**: Using Python to automate file management processes, ensuring data integrity and security.

Portfolio Projects

1. Incident Handler's Journal

Description:
As part of my incident response training, I maintained an incident handler's journal. This journal tracked various incidents, documented the tools and methods used, and reflected on my learning. The entries focused on incident investigation and response strategies, including identifying threats, vulnerabilities, and the steps taken to mitigate risks.

Key Skills Demonstrated:

- Documentation of cybersecurity incidents
- Analysis of risk management techniques
- Use of cybersecurity tools for incident detection and prevention

Sample Entry (Excerpt):

Date: [Insert Date]
Incident Description: A malware outbreak was detected in the company's internal network.
Incident Investigation (The 5 W's):

- **What:** Malware causing unauthorized actions on systems.
- **Where:** Company's internal network and file servers.
- **When:** Incident was detected at 3:00 PM.
- **Who:** Employees with admin privileges were impacted.
- **Why:** Attackers exploited vulnerability in an outdated software version.

Tools Used:

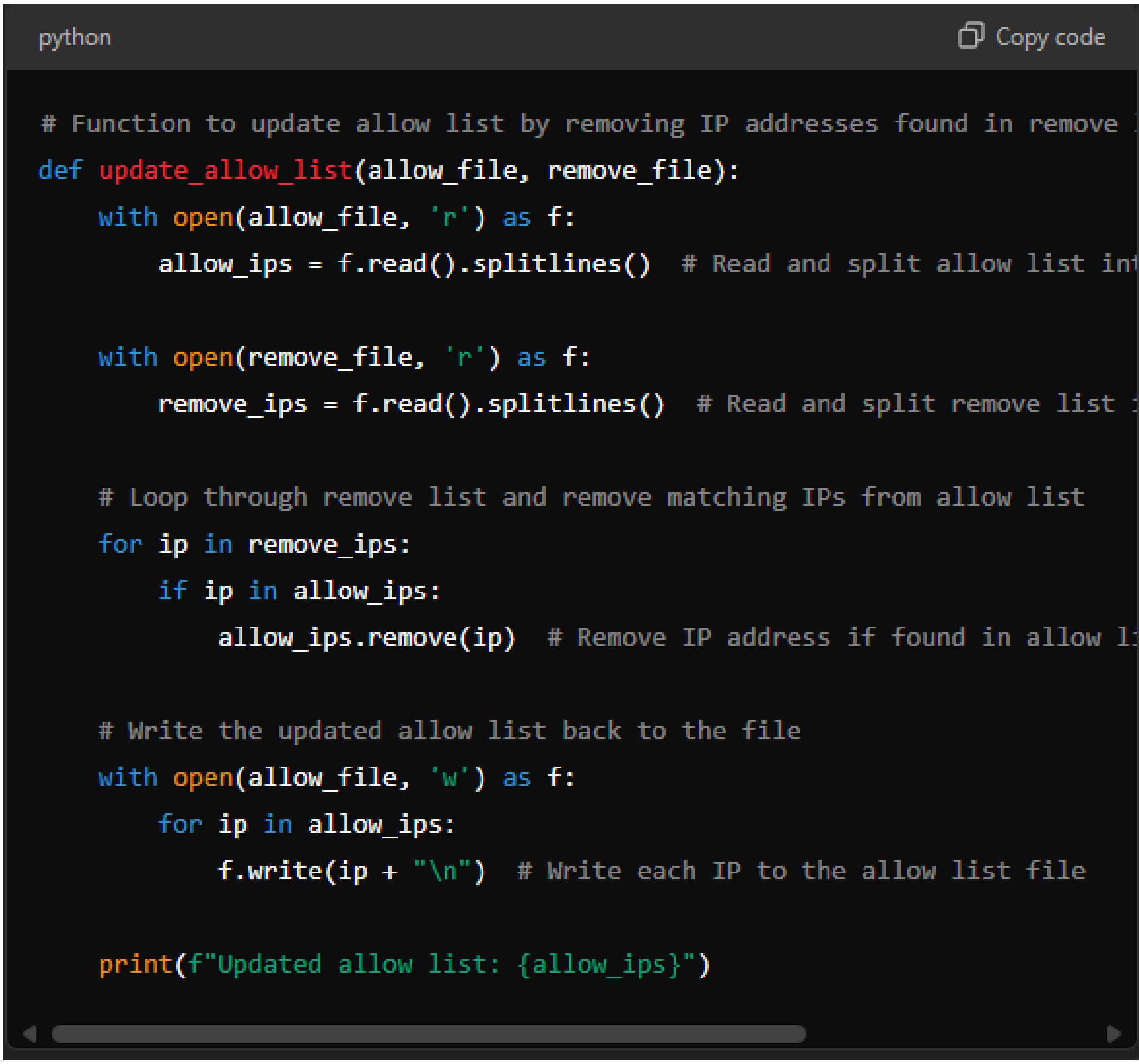
- Antivirus and malware detection software
- Network monitoring tools
- Incident management platform

---

2. Python Algorithm for File Updates

Project Overview:
Developed a Python script to manage and update a healthcare company's allow list for restricted IP addresses. The algorithm checks for IP addresses from a **remove list** and removes any matching IPs from the **allow list**, automating access control for sensitive healthcare data.

Code Example:



```python
# Function to update allow list by removing IP addresses found in remove
def update_allow_list(allow_file, remove_file):
    with open(allow_file, 'r') as f:
        allow_ips = f.read().splitlines()  # Read and split allow list int

    with open(remove_file, 'r') as f:
        remove_ips = f.read().splitlines()  # Read and split remove list

    # Loop through remove list and remove matching IPs from allow list
    for ip in remove_ips:
        if ip in allow_ips:
            allow_ips.remove(ip)  # Remove IP address if found in allow l

    # Write the updated allow list back to the file
    with open(allow_file, 'w') as f:
        for ip in allow_ips:
            f.write(ip + "\n")  # Write each IP to the allow list file

    print(f"Updated allow list: {allow_ips}")
```

Key Skills Demonstrated:

- Using Python to read, manipulate, and write files.
- Applying list manipulation and control flow (loops) in Python.
- Automating sensitive access control processes.

Detailed Explanation of Functions:

- **with open()**: Safely opens files and ensures they are closed after use.
- **.read() & .splitlines()**: Used for reading files and converting them into a list format for easier manipulation.
- **for loop**: Iterates over the remove list and removes matching IP addresses.
- **.remove()**: Removes an item from a list if it matches a specified condition.
- **File Writing**: The updated allow list is written back to the file.

3. Security Incident Response

Project Overview:
In this project, I simulated a real-world incident response scenario. The project included identifying a security incident, responding to it using appropriate tools, and documenting the response actions taken.

Key Skills Demonstrated:

- Incident identification and classification
- Application of cybersecurity frameworks (NIST)
- Practical use of incident management tools and platforms

---

4. Data Protection and Risk Mitigation Plan

Project Overview:
Developed a comprehensive risk management plan for securing sensitive healthcare data. The plan included vulnerability assessments, threat analysis, and the implementation of access control mechanisms to mitigate risks associated with unauthorized access.

Key Skills Demonstrated:

- Risk management principles
- Identifying vulnerabilities and threats
- Implementing access control and data protection strategies

Reflections

Throughout the **Google Coursera Cybersecurity Certification Program**, I have gained hands-on experience in both theoretical and practical aspects of cybersecurity. The **Python-based file handling** algorithm for updating an allow list, in particular, demonstrated the importance of automation in security processes. By leveraging coding and scripting, I was able to optimize the management of sensitive data access, an essential skill for any cybersecurity professional.

I have also learned the importance of **incident handling** and documenting every step in a security event, which ensures that the response process is both effective and transparent. Additionally, my exposure to risk management, particularly in a healthcare setting, has reinforced the need to always balance security with operational efficiency.

These experiences, combined with the knowledge acquired throughout this certification, have significantly enhanced my abilities as a **cybersecurity professional**, and I am excited to continue applying these skills in real-world scenarios.

Summary of Tools Used

- **Python**: Used for automating file updates and developing algorithms for access control.
- **Incident Management Tools**: Used to detect, analyze, and respond to security incidents.
- **Cybersecurity Frameworks (NIST)**: Applied to structure incident response and risk management activities.