Final Project: Generative AI for Cybersecurity

Estimated time needed: 60 minutes

Welcome to the final project.

About the final project

As a security analyst at the fictional organization 'International Fusion Tech Power Corporation Limited,' you're on a critical mission. Scientists reported suspicious emails, prompting a comprehensive analysis to unveil a potential phishing attack. Your scrutiny extends to certain scientists' systems, revealing a background program.

Further investigations uncovered a network log exposing suspicious activities across the organization. Your focus now is to analyze the log, identify the primary remote IP address, and determine associated port numbers for communication. Subsequently, you're tasked with preparing an incident report to inform management.

The analysis reveals a phishing attack compromising systems. With no playbook in place, you turn to ChatGPT for assistance. Your role is vital in crafting an effective playbook to manage and mitigate the impact of this sophisticated phishing and malware attack, safeguarding the organization's critical infrastructure.

This project aims to equip you with the practical skills needed to assess and mitigate cybersecurity threats, particularly in the context of potential phishing attacks on a critical organization.

The project comprises five exercises, with a scenario provided for each.

Exercise 1: Spam email detection

As a Security Analyst at the nuclear power generation organization, you have been informed that several scientists within the organization have reported receiving suspicious emails from unknown senders. Some scientists have flagged these emails as suspicious, and you have been tasked with conducting a comprehensive analysis to determine whether the emails constitute a phishing attack on the organization. Follow the steps to accomplish the task.

1. Click and download the email copy.
2. Open ChatGPT.
3. Compose a prompt instruction for ChatGPT that guides it to analyze an email text and determine whether the email indicates a phishing attempt.
4. Review the response generated by ChatGPT.
5. Explore various prompt instructions until you receive a satisfactory answer.

Example

Examine the content of this email and determine whether it exhibits characteristics of a phishing attempt or not.

Subject: Urgent Research Collaboration Opportunity - Exclusive Nuclear Insights!

Dear Dr. Simson,
We hope this message finds you well. Our esteemed organization, the International Nuclear Fusion Advancements Consortium (INFAC), has recently come across ground breaking research that aligns perfectly with your expertise. We believe your involvement is crucial for the success of this venture.

Dr. Smith
Director of Collaborative Research
International Nuclear Fusion Advancements Consortium (INFAC)

Exercise 2: Code analysis of a malware program

You became suspicious of certain scientists' systems. Upon analysis, you discovered a program running in the background. After conducting reverse engineering, you obtained the code stored in the file `malicious.txt`.

Now, perform a code analysis using ChatGPT to identify the actions and potential harm caused by this program to the organization.

1. Click to open and save the malicious.txt file.
2. Open ChatGPT.
3. Craft a prompt instruction for ChatGPT, instructing it to analyze a programming code and identify malicious activities.
4. Review the response generated by ChatGPT.
5. Experiment with different prompt instructions until you obtain a response that meets your satisfaction.

Example

Analyze the programming code and identify potential malicious activities or security vulnerabilities. Provide insights into the code's behavior and assess its impact on system security.

```
from docx import Document
import os
def identify_keywords_and_write(file_path, output_file):
    document = Document(file_path)
    has_keywords = any("nuclear" in paragraph.text.lower() and "research" in paragraph.text.lower() for paragraph in document.paragr
    if has_keywords:
        with open(output_file, 'a') as output:
            output.write(os.path.basename(file_path) + '\n')
def process_directory(directory_path, output_file):
    for filename in os.listdir(directory_path):
        if filename.endswith(".docx"):
            file_path = os.path.join(directory_path, filename)
```

```
            identify_keywords_and_write(file_path, output_file)
if \__name__ == "\__main__":
    # Provide the path to the directory containing Word files
    word_files_directory = "path/to/your/word/files"
    # Output file for storing names of important files
    output_file_path = "important.doc"
    for file_name in os.listdir(word_files_directory):
        if file_name.endswith(".docx"):
            file_path = os.path.join(word_files_directory, file_name)
            identify_keywords_and_write(file_path, output_file_path)
    print("Process completed. Check 'important.doc' for results.")
```

Exercise 3: Network log analysis for threat intelligence

After detecting a malicious program on a system, you discover a network log revealing suspicious activities across multiple computers within the organization. Your task now is to analyze the log, pinpoint the remote IP address that the majority of compromised computers are communicating with, and determine the associated port numbers for these communications. Follow the steps to accomplish the task

1. Click to open and save the netlog.txt file.
2. Open ChatGPT.
3. Create a prompt instruction for ChatGPT to analyze the network log file, identifying the destination IP address where the maximum outbound traffic originated and determining the associated port number.
4. Review the response generated by ChatGPT.
5. Explore various prompt instructions until you achieve a response that aligns with your satisfaction.

Example

Examine the log to determine the destination IP address where the highest outbound traffic originated and provide the associated port number.

```
Timestamp: 2024-01-15 14:30:00
Source IP: 101.123.171.5
Destination IP: 186.20.20.27
Protocol: TCP
Port: 21
Description: Outbound connection from compromised system. Unusual high traffic to known malicious IP.
...
Timestamp: 2024-01-15 14:31:10
Source IP: 101.123.171.8
Destination IP: 176.30.30.27
Protocol: UDP
Port: 5000
Description: Suspicious outbound traffic detected. Unusual activity to known malicious IP.
...
Timestamp: 2024-01-15 15:45:22
Source IP: 101.123.171.15
Destination IP: 186.20.20.27
Protocol: TCP
Port: 8080
Description: Abnormal traffic pattern detected from compromised system. Connection to known malicious IP.
.
.
.
.
.
.
Timestamp: 2024-01-15 23:10:15
Source IP: 101.123.171.4
Destination IP: 176.30.30.27
Protocol: TCP
Port: 21
Description: Outbound connection from compromised system. Unusual high traffic to known malicious IP.
...
```

Exercise 4: Incident report writing

Prepare an incident report to inform the management about the identified incident.

1. Open ChatGPT.
2. Compose a prompt instruction for ChatGPT to generate an incident report for the identified incident.
3. Review the response generated by ChatGPT.
4. Experiment with different prompt instructions until you obtain a response that aligns with your satisfaction.

Example

Create an incident report to inform the management about the identified suspicious activity based on the logs.

```
Timestamp: 2024-01-15 14:30:00
Source IP: 101.123.171.5
Destination IP: 186.20.20.27
Protocol: TCP
Port: 21
Description: Outbound connection from compromised system. Unusual high traffic to known malicious IP.
Timestamp: 2024-01-15 14:31:10
Source IP: 101.123.171.8
Destination IP: 176.30.30.27
Protocol: UDP
Port: 5000
Description: Suspicious outbound traffic detected. Unusual activity to known malicious IP.
```

```
...
Timestamp: 2024-01-15 15:45:22
Source IP: 101.123.171.15
Destination IP: 186.20.20.27
Protocol: TCP
Port: 8080
Description: Abnormal traffic pattern detected from compromised system. Connection to known malicious IP.
.
.
.
.
Timestamp: 2024-01-15 23:10:15
Source IP: 101.123.171.4
Destination IP: 176.30.30.27
Protocol: TCP
Port: 21
Description: Outbound connection from compromised system. Unusual high traffic to known malicious IP.
```

Exercise 5: Playbook generation for phishing and malware attack

Having conducted the analysis, it's apparent that your organization has become a target of a phishing attack, leading to systems compromised by malware. With no existing playbook for handling such attacks, you now seek assistance to craft a playbook that effectively manages and mitigates the impact of phishing and malware attacks, utilizing the capabilities of ChatGPT.

1. Open ChatGPT.
2. Generate a prompt instruction to develop a playbook addressing phishing and malware attacks.
3. Review the response generated by ChatGPT.
4. Experiment with different prompt instructions until you obtain a response that meets your satisfaction.

Example

Generate a comprehensive playbook to effectively handle phishing and malware attacks, covering incident response, mitigation strategies, and preventive measures.

Summary

Congratulations! You just completed the hands-on lab final project.

In this lab, you focused on comprehensively exploring and evaluating generative AI models. The primary objective involved utilizing these models for content analysis to identify phishing emails effectively. Additionally, you delved into their capabilities for analyzing malicious code and scrutinizing network logs.

Further investigation included exploring the generative AI feature to generate an Incident Report and create a playbook. You learned a lot about generative AI uses by exploring it in various ways. Your involvement in these studies shows you are dedicated to understanding and mastering generative AI for cybersecurity purposes.

Author: Manish Kumar