Applications of CyberSecurity Using ChatGPT, Skill Labs

Course Specifications

Course Number: ACI76-018SL_rev1.0
Lab Length: Approximately 8 hours

Introduction to ChatGPT and Generative AI

Introduction
Overview

Generative AI is a branch of artificial intelligence that utilizes techniques and focused on generating models and algorithms that have the ability to generate new and original content.

ChatGPT is an advanced language model developed by OpenAI. ChatGPT is designed to generate human-like responses to text inputs. It can understand and provide contextually based responses on a wide range of topics.

Outcomes

In this lab, you will learn to:

1. Start-up ChatGPT.
2. Work with ChatGPT chats.
3. Use ChatGPT as a cybersecurity tool for users.
4. Use ChatGPT as a cybersecurity tool for organizations.

	Key Term	Description
1	ChatGPT	ChatGPT is an advanced language model developed by OpenAI.
2	OpenAI	OpenAI, or Open Artificial Intelligence, is an artificial intelligence research organization and company.
3	GPT	GPT stands for "Generative Pretrained Transformer."

Use ChatGPT to Plan and Execute a Phishing Simulation for an Organization

Introduction
Overview

As a part of an organization's security policy, the organization should have an organized training and awareness plan. Part of that plan should be periodic phishing simulations. Phishing is a cyberattack in which an attacker poses as a trustworthy person to deceive individuals and trick them into providing sensitive information. A phishing simulation should resemble a real-life phishing attempt while prioritizing the security and well-being of an organization's employees.

In this lab, you will learn to:

1. Plan a phishing simulation for an organization.
2. Set up the environment to support a phishing simulation.
3. Craft a phishing message.
4. Deliver and execute the phishing message.
5. Follow up and educate users who fell for the phishing attempt.

	Key Term	Description
1	Phishing	Phishing is a form of cyberattack in which an attacker poses as a trustworthy entity or organization to deceive individuals and trick them into providing sensitive information, such as passwords, credit card details, or personal data.
2	Types of Phishing Attacks	Email, spear phishing, whaling, smishing, and vishing
3	Phishing Simulation	A phishing simulation for an organization should closely resemble a real-life phishing attempt while prioritizing the security and well-being of the organization's employees.

Use ChatGPT for Social Media Threat Intelligence

Introduction
Overview

Social media threat intelligence refers to the practice of collecting, analyzing, and utilizing information from social media platforms to identify and mitigate potential threats. It involves monitoring social media networks for security risks, malicious activities, and emerging threats that could impact individuals, organizations, or society at large.

In this lab, you will learn to:

1. Use ChatGPT to detect malicious social media posts on Facebook.
2. Use ChatGPT to detect malicious social media posts on Twitter.

	Key Term	Description
1	Malicious social media intelligence	The practice of collecting and analyzing information from social media platforms to identify and respond to potential threats, risks, and malicious activities.
2	Social media threats	Various risks and dangers that users may encounter on social media platforms, including phishing attacks, account takeovers, malware distribution, social engineering tactics, fake news, online harassment, privacy concerns, scams, and more.
3	Malicious social media posts	Content shared on social media platforms that aim to deceive, spread misinformation, harass individuals, exploit users, or promote malicious activities. Examples include phishing scams, fake news, disinformation campaigns, online harassment, account impersonation, social engineering attacks, fraudulent offers, hate speech, and extremist content.
4	Malware	Malicious software designed to infiltrate, disrupt, damage, or gain unauthorized access to computer systems, networks, or devices. In the context of social media, malware may target platforms or users through techniques such as worms, Trojans, spyware, or ransomware.

Use ChatGPT to Create an Incident Response Policy for an Organization

Introduction
Overview

In today's interconnected and digital landscape, the need for a robust cybersecurity incident response plan is paramount. Cyber threats, such as data breaches, ransomware attacks, and sophisticated malware, pose a constant risk to organizations' sensitive information, financial stability, and reputation. A well-structured incident response plan provides a clear and coordinated framework to detect, assess, and respond promptly to security incidents, minimizing their impact and facilitating swift recovery. By outlining predefined roles, responsibilities, and communication channels, the plan ensures a unified and efficient response from the incident response team. Additionally, the plan is vital to comply with legal requirements, preserve crucial evidence for investigations, and demonstrate due diligence in protecting customer trust. Ultimately, a cybersecurity incident response plan strengthens the organization's resilience, enhances its ability to mitigate cyber threats, and safeguards its future in the face of an ever-evolving threat landscape.

In this lab, you will learn to:

1. Use ChatGPT to create a cybersecurity incident response policy for an organization.
2. Use ChatGPT to generate a PDF report using LaTeX.
3. Use ChatGPT to create a Google Docs.
4. Use ChatGPT and Google Apps Script to create a Google Docs.

	Key Term	Description
1	Incident response	The organized and structured approach taken by individuals or organizations to effectively manage and address cybersecurity incidents, including cyberattacks, data breaches, and other security threats
2	Cybersecurity incident	Any event or occurrence that poses a risk to the confidentiality, integrity, or availability of information systems and data, leading to potential harm or disruption
3	Detection	The process of identifying and recognizing a security incident through various monitoring tools, logs, and security alerts
4	Assessment	The act of evaluating and analyzing a detected incident to understand its nature, severity, and potential impact on the organization
5	Containment	The immediate response action to isolate and restrict the affected systems, preventing the incident from spreading further
6	Eradication	The phase of incident response where the root cause of the incident is identified and eliminated, removing all traces of the attacker's presence from the affected systems
7	Recovery	The process of restoring affected systems, data, and services to their normal functioning state after the incident has been contained and eradicated
8	Post-incident analysis	Also known as a "post-mortem," it involves a comprehensive review of the incident response process to identify strengths, weaknesses, and areas for improvement
9	Incident response plan	A predefined and documented strategy outlining the steps, roles, responsibilities, and communication procedures to be followed in the event of a cybersecurity incident

Use ChatGPT to Detect and Mitigate Security Vulnerabilities in Python Code

Introduction
Overview

ChatGPT is an advanced language model developed by OpenAI. ChatGPT is designed to generate human-like responses to text inputs. It can understand and provide contextually based responses on a wide range of topics.

Python is a powerful scripting tool that can be very useful for a cybersecurity professional. This lab provides step-by-step instructions on how to use ChatGPT to write secure Python code.

If not programmed correctly, programs typically have security vulnerabilities in them. Recognizing the vulnerabilities makes fixing them easy. This lab purposely introduces the most common Python security vulnerabilities and uses ChatGPT to determine and mitigate the security vulnerabilities.

Outcomes

In this lab, you will learn to:

1. Use ChatGPT to detect security vulnerabilities in Python code.
2. Use ChatGPT to mitigate Python security vulnerabilities.

	Key Term	Description
1	ChatGPT	ChatGPT is an advanced language model developed by OpenAI. ChatGPT is designed to generate human-like responses to text inputs. It can understand and provide contextually based responses on a wide range of topics.
2	Python	Python is a scripting language used by cybersecurity professionals.
3	Vulnerability	A vulnerability refers to a weakness or flaw in a system, software, network, or any other technology that can be exploited by an attacker to compromise its security or violate its intended functionality.

Use ChatGPT to Write Cybersecurity Automation Scripts

Introduction
Overview

Cybersecurity has become a critical aspect of our digital world. With the increasing number of cyber threats, organizations and individuals are constantly seeking ways to protect their sensitive information. In this lab, we will explore the concept of cybersecurity from both a cyber offensive and defensive point of view, delve into the examples of cybersecurity pentesting and cyber defense automation, and examine the different cybersecurity automation scripts for both pentesting and cyber defense.

In this lab, you will learn to:

1. Use ChatGPT to write pentesting automation scripts in Python.
2. Use ChatGPT to write cyber defense automation scripts in Python.

	Key Term	Description
1	Defense in depth	Defense in depth involves implementing multiple layers of security measures to create a strong defense barrier.
2	Security operations center	A Security operations center (SOC) is the nerve center of an organization's cybersecurity defense. It is a team of highly skilled professionals who monitor, analyze, and respond to security incidents in real time.
3	Python	Python is one of the most popular programming languages that serve different purposes in the world of cybersecurity automation.
4	Penetrating testing	Penetration testing, also known as pen testing, is a crucial process in the world of cybersecurity. It involves simulating real-world attacks on computer systems and networks to identify vulnerabilities and assess their potential impact.
5	Cyber defense	Cyber defense involves multiple stages or components to protect computer systems, networks, and data from unauthorized access, attacks, and threats.

Use ChatGPT to Write a Security Policy for an Organization

Introduction

Overview

Organizations in all sectors and industries require a cybersecurity strategy to protect their assets and infrastructure from attacks. Cybersecurity refers to the practice of protecting systems, networks, and data from unauthorized users. Organizations require implementing measures to prevent, detect, and respond to potential threats or attacks from internal and external users. A cybersecurity policy outlines an organization's approach to managing and mitigating risks related to protecting digital assets.

In this lab, you will learn to:

1. Use ChatGPT to understand the cyber threat landscape for an organization
2. Use ChatGPT to outline a cybersecurity policy for an organization using the NIST Cybersecurity Policy Framework
3. Use ChatGPT to create the different sections of a cybersecurity policy for an organization
4. Use ChatGPT to assist in creating a cybersecurity training and awareness policy and plan

	Key Term	Description
1	cybersecurity policy	A cybersecurity policy is a formal document that outlines an organization's approach to managing and mitigating risks related to information security and protecting its digital assets.
2	CIA Triad	The CIA triad is a widely recognized model for information security that consists of three fundamental principles: confidentiality, integrity, and availability.
3	NIST	National Institute of Standards and Technology
4	cyber threat	A cyber threat refers to potential or actual risk or danger posed by individuals, groups, or entities that exploit vulnerabilities in computer systems, networks, or digital infrastructure with malicious intent.

Use ChatGPT to Develop Social Engineering Training

Introduction
Overview

As part of an overall cybersecurity policy, organizations must have a training and awareness plan that includes social engineering training. Social engineering is a tactic used by malicious individuals to manipulate and deceive others to gain unauthorized access to sensitive information or systems. It involves exploiting human psychology, trust, and vulnerabilities to bypass traditional security measures. Awareness, caution, and education are essential in protecting against social engineering attacks.

In this lab, you will learn to:

1. Use ChatGPT to create a social engineering presentation.
2. Use ChatGPT to generate PDF slides using LaTex.
3. Use ChatGPT to generate Google slides.

	Key Term	Description
1	Social engineering	The art of manipulating and deceiving individuals to gain unauthorized access to information, systems, or physical locations.
2	Phishing	A form of social engineering where attackers impersonate legitimate individuals or organizations to trick victims into revealing sensitive information, such as passwords or credit card details, usually via email or fake websites.
3	Pretexting	A technique where an attacker creates a fictional scenario or pretext to manipulate individuals into providing sensitive information or access to secure areas.
4	Baiting	A social engineering tactic that involves leaving physical devices, such as USB drives or CDs, in public places to entice individuals into using them, unknowingly introducing malware or compromising their systems.
5	Impersonation	Pretending to be someone else, such as a trusted colleague, company representative, or service provider, to deceive individuals into divulging sensitive information or performing actions they wouldn't otherwise do.