masterskill
education through innovation

aci LEARNING | SKILL LABS

AI/ML in Cybersecurity Labs (Cybersecurity Analytics), Skill Labs

Course Specifications

Course Number: ACI76-017SL_rev1.0
Lab Length: Approximately 12 hours

Use ChatGPT and YARA to Analyze Malware

Introduction
Overview

This lab introduces the concept of malware analysis using YARA, a powerful and flexible pattern-matching tool. Participants will gain hands-on experience in identifying and analyzing malware samples by creating custom YARA rules. By the end of this lab, participants will be equipped with the fundamental skills required to detect and analyze malware using YARA.

In this lab, you will:

1. Understand the basics of malware analysis.
2. Create custom YARA rules to detect specific malware characteristics.
3. Analyze a malware sample using YARA rules.

	Key Term	Description
1	YARA	YARA is an open-source tool used for pattern matching and detection of malware and other malicious activities. It uses rules containing strings and regular expressions to identify specific patterns within files or processes.
2	Rule	A YARA rule is a set of conditions that define patterns to be matched against files or processes. Rules consist of strings, regular expressions, and conditions that determine if a match is found.
3	String	In YARA, a string is a sequence of characters or a regular expression pattern to be searched for within a file or process. Strings can be plain text or use regular expressions to match complex patterns.
4	Regular Expression	A regular expression (regex) is a sequence of characters that define a search pattern. It provides a powerful way to match and manipulate strings based on specific patterns of characters. YARA supports regex patterns for more advanced and flexible matching.
5	Condition	A condition in YARA determines if a rule is considered a match or not. It can include logical operators (AND, OR, NOT) and comparisons to evaluate the presence or absence of specific strings or properties within a file or process.
6	Modifier	In YARA, modifiers are optional flags that can be added to a string or regex pattern to modify the matching behavior. Modifiers can control case sensitivity, word boundaries, multiline matching, and other aspects of pattern matching.

Using ChatGPT and AI/ML to Combat Social Engineering Attacks

Introduction
Overview

Social engineering is a psychological manipulation technique that exploits human behaviors, trust, and emotions to deceive individuals into revealing sensitive information, performing actions, or compromising security. Attackers employ various tactics, such as phishing, smishing, vishing, pretexting, and impersonation, to manipulate targets' cognitive biases and emotions, often bypassing technical safeguards. Awareness, education, and vigilance are crucial for individuals and organizations to mitigate the risks posed by social engineering attacks and protect against unauthorized access, data breaches, and other security breaches.

ChatGPT allows users and cybersecurity analysts to check for potential phishing emails and SMS message attempts before they occur. There is a cybersecurity search engine available to allow instant checking of phishing attempts through URL checks and email attachments in Google Chrome.

In this lab, you will learn to:

1. Use ChatGPT to review the validity of different examples of phishing emails and smishing messages.
2. Use ChatGPT to create a smishing text message.
3. Send an SMS text message via Gmail.
4. Use AI/ML tools to check links as malicious.

	Key Term	Description
1	Phishing	Attackers send deceptive emails or messages impersonating a legitimate entity, such as a bank, social media site, or organization, to trick recipients into revealing their sensitive information like passwords, credit card details, or personal identification.
2	Smishing	Smishing, a portmanteau of "SMS" (Short Message Service) and "phishing," is a form of social engineering attack conducted via text messages (SMS) or other messaging apps.
3	Vishing	Vishing, short for "voice phishing," is a type of social engineering attack that involves manipulating individuals over the phone to extract sensitive information, gain unauthorized access, or facilitate fraudulent activities.
4	Pretexting	Attackers create a fabricated scenario or pretext to gain the target's trust. For instance, they might pose as a coworker, IT support, or another trusted entity to convince the target to share confidential information.
5	Baiting	This involves enticing victims with an appealing item, such as a free software download or physical device, that contains malicious software. Once the victim interacts with the item, the attacker gains access to the system.
6	Quid Pro Quo	Attackers promise something of value in exchange for sensitive information or access. For example, an attacker might call pretending to be IT support and offer to fix a computer issue in exchange for the user's login credentials.
7	Tailgating	An attacker gains unauthorized physical access to a secured building by following an authorized person through a controlled entry point.
8	Impersonation	Attackers may pretend to be someone of authority, such as a manager or executive, to manipulate employees into disclosing confidential information or performing actions they shouldn't.
9	Honeytrap	This involves using romantic or sexual enticement to manipulate a target into revealing information or taking certain actions.

10	Quizzes and Surveys	Attackers use seemingly harmless quizzes or surveys to collect personal information that can be used for identity theft or other malicious purposes.
11	Dumpster Diving	Attackers search through trash or recycling to find discarded documents with sensitive information like passwords, credit card statements, or invoices.

Use ChatGPT to Run Web Application Security Testing with Zap Attack Proxy

Introduction

Overview

Using ChatGPT for web application security testing with the Zap Attack Proxy, you can enhance your testing capabilities by integrating natural language understanding into your security assessments. ChatGPT assists security professionals by generating insightful test cases and scenarios, automating repetitive tasks, and providing real-time feedback on potential vulnerabilities identified by Zap. This powerful combination of AI-driven conversation and security expertise streamlines the testing process, helping teams identify and remediate web application vulnerabilities more effectively, ultimately fortifying their defenses against cyber threats.

In this lab, you will learn to:

1. Use ChatGPT to assist in setting up Zap Attack Proxy.
2. Execute and investigate vulnerabilities of a vulnerable web application.
3. Use ChatGPT to learn about the vulnerabilities found and how to secure them.

	Key Term	Description
1	Web Application Security	The practice of protecting web applications from security threats and vulnerabilities by implementing various security measures, protocols, and best practices.
2	OWASP	A nonprofit organization that provides resources and guidance on web application security, including a list of the top web application security risks known as the OWASP Top Ten.
3	SQL Injection	A type of security vulnerability where an attacker can manipulate a web application's SQL query to gain unauthorized access to a database or retrieve sensitive data.
4	Cross-Site Scripting (XSS)	A vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users, potentially leading to data theft or session hijacking.
5	Cross-Site Request Forgery (CSRF)	An attack where an attacker tricks a user into executing malicious actions on a website without their knowledge or consent.
6	Cookie Poisoning	Cookie poisoning is a type of attack where an attacker manipulates or modifies cookies stored on a user's computer to gain unauthorized access or perform malicious actions on a website or web application.

Using AI/ML to Detect Deepfakes

Introduction

Overview

The deepfakes detection lab aims to provide participants with hands-on experience in identifying and detecting deepfake images, audio, and videos. Deepfakes are manipulated images, audio, and videos created using artificial intelligence techniques, which can be challenging to distinguish from real images, audio, and videos. In this lab, you will learn various techniques and tools to identify and analyze deepfakes, enabling you to better understand the implications of this emerging technology.

In this lab, you will learn to:

1. Understand the concept of deepfakes and their potential impact on society.
2. Understand techniques to identify visual artifacts and inconsistencies in deepfake images and videos.
3. Understand techniques to identify audio inconsistencies in deepfake audio.
4. Familiarize yourself with different tools and methods for deepfake detection.
5. Gain practical experience in detecting and analyzing deepfake videos.

	Key Term	Description
1	Deepfake	Deepfake refers to the use of artificial intelligence (AI) techniques to create convincing images, audio, or video hoaxes. It involves the manipulation or synthesis of content to make it appear as though someone said or did something they never actually did. Deepfakes can be used for various purposes, including spreading disinformation, creating fake profiles, or manipulating public opinion.
2	Textual Deepfake	Textual deepfakes involve the generation of synthetic text that mimics the writing style or content of a specific person. They can be used to create fake news articles, social media posts, or emails.
3	Deepfake Video	Deepfake videos are created by using AI algorithms to manipulate or replace the faces of individuals in videos. This technology can make it appear as though someone is saying or doing something they never actually did. Face swapping is a common application of deepfake technology.
4	Deepfake Audio	Deepfake audio involves the generation of synthetic voices that mimic the speech patterns and intonations of specific individuals. This can be used to create fake voice recordings or impersonate someone's voice.
5	Deepfake Image	A deepfake image is a type of manipulated or synthetic image created using deep learning techniques, particularly general adversarial networks (GANs) and deep neural networks.

Use ChatGPT and Python for Robotic Process Automation (RPA)

Introduction
Overview

In the world of robotic process automation (RPA), businesses can enhance their efficiency and productivity by using powerful tools such as ChatGPT and Python.

ChatGPT is an intelligent chatbot that can assist in performing specific tasks. It can be integrated into various systems and has natural language processing capabilities that allow it to understand user queries and provide relevant responses or execute predefined actions.

Python is a versatile programming language known for its simplicity and readability, which plays a crucial role in RPA implementation. Its extensive libraries and frameworks enable developers to create custom scripts for automating specific tasks or integrating different components within an RPA workflow.

When combined effectively, ChatGPT and Python offer a comprehensive solution to empower businesses to reduce manual effort while improving accuracy and scalability in their day-to-day processes.

In this lab, you will learn to:

1. Use ChatGPT to generate Python RPA Windows scripts to automate repetitive user tasks.
2. Use ChatGPT to generate Python RPA Linux scripts to automate repetitive user tasks.

	Key Term	Description
1	Robotic Process Automation (RPA)	Robotic process automation is a technology that uses software robots or "bots" to automate repetitive and rule-based tasks within business processes, improving efficiency and reducing the need for human intervention.
2	ChatGPT	ChatGPT is a natural language processing AI model developed by OpenAI, capable of understanding and generating human-like text responses. It can be used to facilitate human–computer interactions and automate certain text-based tasks in RPA workflows.
3	Python	Python is a high-level programming language known for its simplicity and versatility. It is commonly used in RPA for scripting, task automation, and integrating various software components due to its extensive libraries and frameworks.
4	Workflow Automation	Workflow automation refers to the process of using software and tools like Ansible and Python to streamline and automate the sequential steps or tasks within an RPA process, enhancing efficiency and reducing errors.
5	Bot Development	Bot development is the process of designing, coding, and configuring software robots (bots) that mimic human actions to perform specific tasks in RPA. Python and Ansible may be employed in the development and management of these bots.

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 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 and Cuckoo Sandbox to Analyze Malware

Introduction
Overview

In today's digital landscape, the threat of malware looms large. To protect your systems and data, it is crucial to analyze malware effectively. That's where Cuckoo Sandbox comes in—a powerful tool designed to help you dissect and understand the inner workings of malicious software. Cuckoo Sandbox is indeed a valuable tool for analyzing malware in today's digital landscape. With the increasing threat of malicious software, it has become essential to have effective methods to protect systems and data. Cuckoo Sandbox provides a powerful solution by allowing users to dissect and understand the inner workings of malware. By running suspicious files or URLs within Cuckoo Sandbox, you can gain insights into how malware behaves and what actions it takes within your system. The tool provides detailed reports on the behavior, network traffic, registry modifications, and other activities performed by the analyzed malware.

In this lab, you will learn to:

1. Gain practical experience in analyzing and understanding the behavior of different types of malware.
2. Develop skills in monitoring and analyzing the behavior of malware samples in a controlled and isolated environment.
3. Use Cuckoo Sandbox to analyze malware.

By achieving these objectives, participants will develop comprehensive skills and knowledge in malware analysis, enabling them to better understand, detect, and mitigate the risks posed by various types of malware.

	Key Term	Description
1	Malware	Malicious software designed to cause harm, such as viruses, worms, trojans, ransomware, or spyware
2	Malware Analysis	The process of dissecting and understanding the behavior, functionality, and impact of malware to identify its capabilities, intentions, and potential mitigation strategies
3	Dynamic Analysis	The examination of malware behavior in a controlled environment, typically using sandboxing techniques, to observe its actions, interactions, and potential impact on a system or network
4	Cuckoo Sandbox	A controlled environment or virtual machine that isolates and monitors the execution of potentially malicious files or software; it helps analyze malware behavior without impacting the host system.

Basics of Prompt Engineering

Introduction
Overview

ChatGPT, also known as the OpenAI GPT-3, is a large language model developed by OpenAI, a San Francisco-based artificial intelligence research company. It is a powerful natural language processing tool capable of generating human-like responses to a variety of prompts.

ChatGPT is based on GPT-3, which was trained on a massive corpus of text data, including books, news articles, and other online sources. The model uses deep learning algorithms to analyze and learn from this vast amount of data, allowing it to generate coherent and grammatically correct responses.

One of the key features of ChatGPT is its ability to generate human-like responses to prompts. This means that users can ask it questions, provide it with information, or give it instructions, and the model will generate a response that appears to be written by a human.

For example, a user might ask ChatGPT to help them write an essay or to give them a recipe for a particular dish. The model can generate a well-structured and well-written response, providing the user with valuable information or guidance.

In addition to generating human-like responses, ChatGPT can also be used to perform a variety of other tasks, such as summarizing long passages of text, answering questions, and completing sentences. This makes it a useful tool for a wide range of applications, including education, business, and personal use.

However, it is important to note that ChatGPT is not a fully autonomous system. It requires user input in the form of a prompt, and the quality of the response will depend on the clarity and specificity of the prompt. If the user does not provide a clear and specific prompt, the model may generate irrelevant or incorrect responses.

In order to create effective ChatGPT prompts, it is important to keep a few things in mind. First, the prompt should be clear and concise, providing the model with a clear idea of what the user is asking for. Second, the prompt should be specific, providing the model with as much relevant information as possible. Finally, the prompt should be concise, avoiding unnecessary words or phrases that might confuse or mislead the model.

In conclusion, ChatGPT is a powerful tool for generating human-like responses to a variety of prompts. By following a few guidelines, users can create effective and usable prompts, allowing them to harness the power of the model for their own purposes.

In this lab, you will learn to:

1. Create simple prompts in ChatGPT.
2. Create intermediate prompts in ChatGPT.

	Key Term	Description
1	Prompt Template	A structured framework used to create prompts for generating specific types of content or responses from language models
2	Introduction	The initial part of a prompt that provides context or sets the stage for the conversation
3	Main Question/Request	The central query or instruction in a prompt that specifies the desired information or action from the AI
4	Additional Details	Supplementary details or parameters provided in a prompt to narrow down the response
5	Follow-up Questions	Questions included in a prompt to guide the conversation and provide a natural flow for further queries
6	Closing or Thanks	Polite closing statements or expressions of gratitude used to conclude a prompt
7	Formatting and Style	Guidelines specifying how information in the response should be presented, such as paragraph format, bullet points, etc
8	Length Guidelines	Instructions regarding the desired length of the response, whether it should be concise or detailed

	Key Term	Description
9	Language and Tone	Desired language style, tone (formal, informal, friendly), and any specific writing conventions to be followed
10	Examples	Sample prompts or illustrative queries that align with the template to demonstrate effective usage

Intermediate/Advanced Prompt Engineering

Introduction
Overview

In this lab, you will be creating different prompt formats for natural language processing and human–computer interaction. Crafting effective prompts is crucial for enhancing user experiences in applications such as chatbots and virtual assistants. In this lab, we will explore various approaches to prompt formulation, covering key elements like context, role, entity, action, type, task, purpose, expectation, request, steps, and examples. By the end of this lab, you will gain valuable insights into designing prompts that are tailored to specific needs and scenarios, ultimately improving communication between users and systems.

In this lab, you will learn to:

1. Create different prompt formats using context, role, entity, action, type, and examples.
2. Create different prompt formats using role, task, and format.
3. Create different prompt formats using purpose, expectation, context, request, and action.
4. Create different prompt formats using roles, actions, and steps, context, examples, and format.
5. Create prompts using prompt priming and adjusting parameters.

	Key Term	Description
1	Prompt Engineering	The practice of crafting prompts, an essential skill in natural language processing and human–computer interaction.
2	Context	The overarching environment and circumstances that influence user experiences and interactions
3	Role	The user's position and purpose, which play a central role in guiding interactions and shaping the user experience
4	Entity	Specific objects, concepts, or elements that enrich prompts by providing depth and specificity
5	Action	The user's intended activity or operation, which contributes to the clarity and effectiveness of prompts
6	Type	The classification or category of prompts, helping tailor them to specific needs and scenarios
7	Task	A task-oriented approach to prompts that leads users through defined roles and responsibilities

	Key Term	Description
8	Purpose	The clear objectives and goals that prompt design aims to align user interactions with
9	Expectation	The anticipation or foresight of outcomes, set by prompts to guide user expectations effectively
10	Request	User-initiated queries or demands, prompting corresponding actions or responses
11	Steps	A sequence of actions or processes that users are guided through within prompts
12	Examples	Illustrative instances or cases that make abstract concepts tangible for users
13	Format	The structure or style of prompts, such as linear narratives, branching conversations, or concise queries
14	Prompt Priming	A technique that influences user responses by adjusting parameters and customizing prompts for better engagement

Use Generative AI for Text Generation Part II

Introduction

Overview

Generative AI, driven by large language models and deep neural networks, has made significant strides in producing human-like text at scale. These technologies are trained on extensive textual data, enabling them to understand the intricate patterns and nuances of human writing. As a result, organizations can automate various forms of textual content creation, from marketing narratives to product descriptions, with minimal human intervention. However, concerns have arisen regarding the lack of oversight in autonomously generating sensitive communications.

In education, it offers personalized learning experiences by creating tailored lessons and practice materials, allowing educators to focus on higher-level instruction. Moreover, in marketing and SEO, generative AI automates content creation, potentially revolutionizing these fields by generating human-like content aligned with specific topics and business needs. Additionally, in HR, it streamlines recruitment processes, automating tasks like resume screening and candidate identification. Although generative AI holds immense promise, responsible and ethical usage remains paramount across these diverse applications.

In this lab, you will learn to:

1. Create educational application prompts.
2. Create HR applications and marketing and SEO prompts.
3. Create job search application prompts.

	Key Term	Description
1	Generative AI	An advanced technology that uses large language models and deep neural networks to autonomously produce human-like text, enabling various applications across industries
2	Marketing and SEO Applications	Leveraging generative AI for automating content creation tailored to specific topics, keywords, and business needs, which has the potential to revolutionize content

	Key Term	Description
		marketing and SEO efforts
3	HR Applications	The strategic use of generative AI in HR departments to streamline recruitment processes, including resume screening, candidate identification, and improving overall hiring efficiency
4	Educational Applications	Implementing generative AI in education to create personalized lessons, practice questions, and formative feedback for students, freeing educators to focus on higher-level instructional activities
5	Job Search Applications	The use of generative AI to assist job seekers in finding opportunities, including generating targeted cover letters and resumes, enhancing career services, and exploring job postings and alternative career paths
6	Content Creation	The process of using generative AI to generate high-quality textual content, such as articles, blog posts, and social media updates while mimicking human writing styles and tones

Use Generative AI for Image Generation

Introduction
Overview

Generative AI, with Craiyon at its heart, has brought about a leap in crafting images. Now, the creation of visuals with stunning detail and lifelike qualities is within reach.

Neural networks are central to this tech. They learn from heaps of data and grasp intricate image patterns. Craiyon harnesses these neural networks; as a result, it churns out visuals akin to real-life snaps or art pieces.

Moreover, Craiyon breathes life into generative AI by infusing specific styles into creations. Style transfer techniques let the AI echo famed artists' strokes or sprinkle unique visual flairs on its work—unleashing new realms for those who craft with pen or pixel.

Craiyon's use also sparked tools that let folks tweak AI-crafted images live—a more natural way to shape digital masterpieces.

Craiyon's blend into generative AI boosts image making sky-high—with realism, personal touch, and hands-on shaping all part of the mix. Its growth may change games we play or alter art we make—in short; its future shines bright across sectors galore.

In this lab, you will learn to:

1. Write basic AI image prompts.
2. Write AI image prompts using a template.

	Key Term	Description
1	Generative AI	An advanced technology that uses large language models and deep neural networks to autonomously produce human-like text, enabling various applications across industries
2	Neural Networks	The core technology behind generative AI, capable of learning from large datasets to recognize intricate patterns in images, enabling the creation of highly detailed and realistic visuals
3	Craiyon	A tool that uses neural networks within the realm of generative AI to produce images that are remarkably similar to real-life photographs or artworks. It embodies the integration of generative AI in crafting visuals with precision and artistic flair.
4	Style Transfer	Techniques used by generative AI, like Craiyon, to incorporate specific artistic styles into the generated images. This allows the AI to mimic the strokes of famous artists or apply unique visual effects, thus expanding the creative possibilities for digital art and design.
5	Personal Touch	The ability of users to infuse their unique style and preferences into AI-generated images, thanks to the capabilities of Craiyon and similar technologies. This feature emphasizes the role of human creativity in guiding and refining the output of generative AI.