[COURSE MATERIALS]

ChatGPT for Ethical Hackers and Penetration Testers

Who Am I?

Experienced Cybersecurity Trainer

Ethical hacking

Doctorate in Artificial Intelligence

DR. FIRAS : Author & Speaker

OpenAI ChatGPT 4.0

ChatGPT: The AI Conversational Revolution

- ChatGPT is an AI chatbot using natural language processing for humanlike dialogue.
- Capable of composing various content: articles, social media posts, essays, code, and emails.
- A form of generative AI, creating humanlike responses from user prompts.

ChatGPT's Functionality and Development

- Functions like automated chat services, offering responses and clarifications.
- "GPT" stands for "Generative Pre-trained Transformer."
- Trained with reinforcement learning and human feedback to improve responses.
- Developed by OpenAI, launched in November 2022

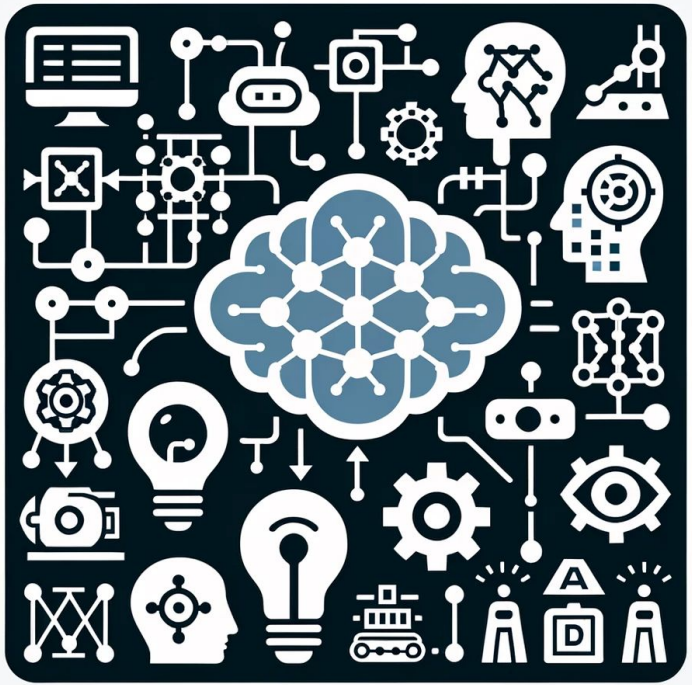
How ChatGPT Works

- Operates through a Generative Pre-trained Transformer.
- Uses algorithms to analyze patterns in data sequences.
- Based on GPT-3, a neural network machine learning model.

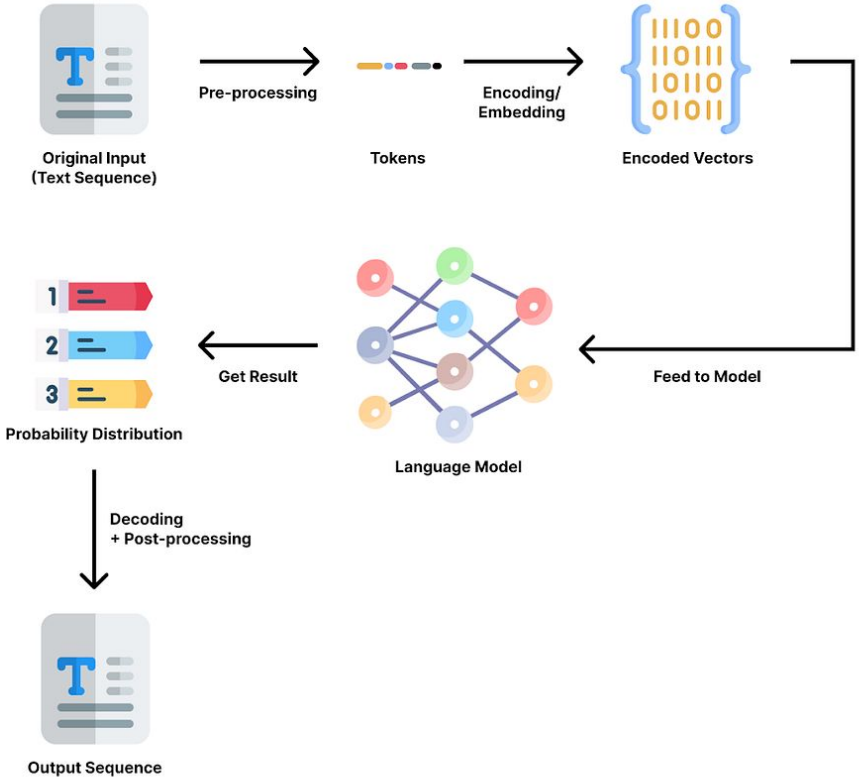
Chronologie : De l'Architecture Transformer à ChatGPT

Diving Deep Behind the Models

- Now that you know **ChatGPT** is based on transformers and the preceding GPT models, let's take a closer look at the components of those models and how they work. It's okay if you are not familiar with deep learning, neural networks, or AI — I will leave out the equations and explain the concepts using analogies and examples.



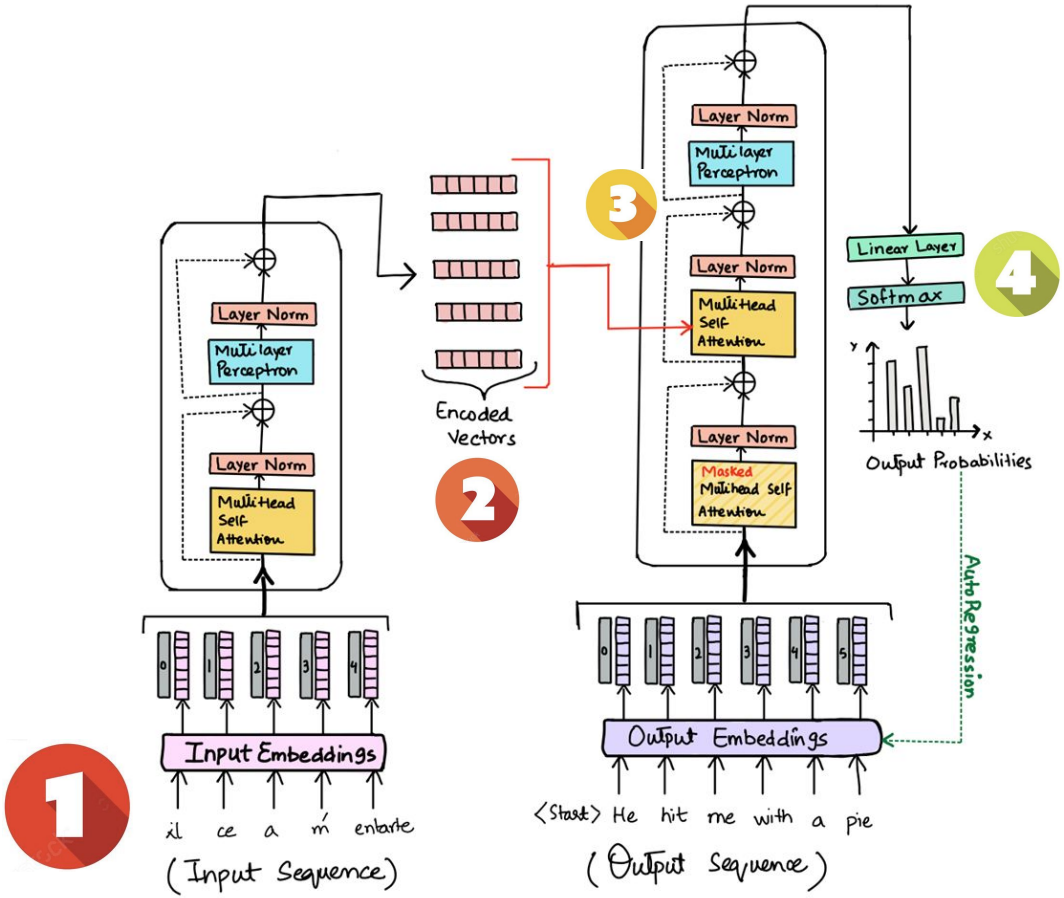
Language models & NLP



- **Preprocessing**: This is like cleaning up a room before you start working. We tidy up the text by breaking it into smaller pieces called tokens, like cutting “Tom likes to eat pizza.” into [“Tom”, “likes”, “to”, “eat”, “pizza”, “.”]. We also trim words to their roots and fix spelling.
- **Encoding or Embedding**: Now, we turn these cleaned-up words into numbers. Why? Because AI understands numbers better than words.
- **Feeding to Model**: Next, we give these numbers to the AI model. It's like feeding ingredients into a machine to get a recipe.
- **Getting Result**: The model then works its magic and predicts what words might come next, showing this as a bunch of number vectors.
- **Decoding**: We translate these number vectors back into words we can understand.
- **Post-processing**: Finally, we polish everything up. We check spelling, grammar, and punctuation to make sure it all makes sense.


Tom likes to eat apples. He eats them every day.

Transformer architecture



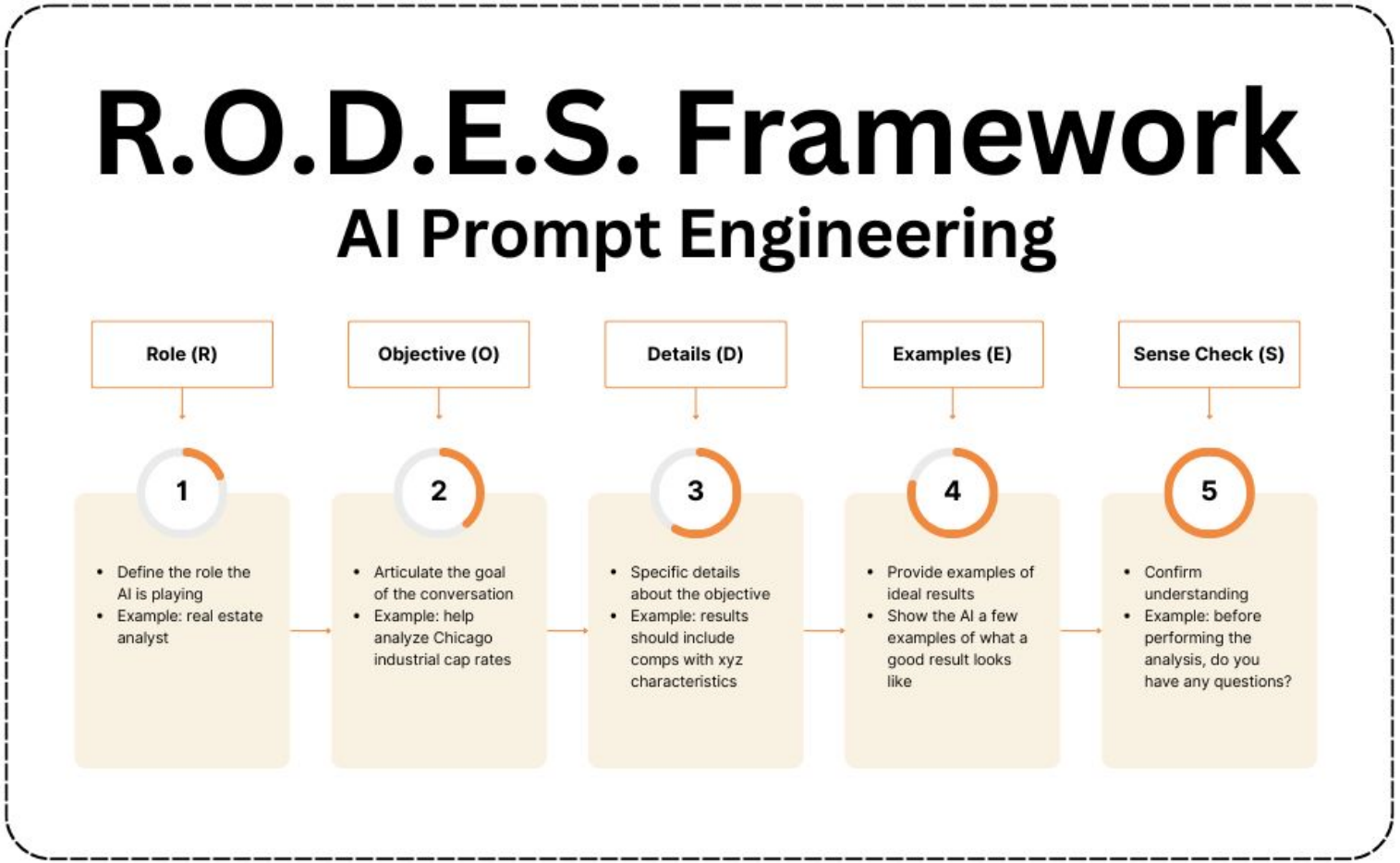
Evolution of GPT: Decoding Language at Scale

- **GPT**: Based on the transformer decoder for autoregressive text generation.
- **GPT-1**: Unsupervised pre-training with BookCorpus, followed by supervised fine-tuning.
- **GPT-2**: Expanded to 1.5 billion parameters, pre-trained with WebText.
- **GPT-3**: Colossal model with 175 billion parameters, extensively trained across the internet.
- **GPT-4**: Latest advancement featuring expanded capabilities, enhanced accuracy, and adaptability.
- **InstructGPT** and **ChatGPT**: Derivatives of GPT designed for human interaction and instructions.

Prompt Engineering

- **Definition**: Techniques to enhance instructions in NLP and AI.
- **Objective**: To achieve higher quality, more accurate, and targeted responses.
- **Importance**: The way prompts are formulated significantly influences the quality and relevance of the responses.
- **Keys**: Creativity, precision, and understanding of the language model.
- **Influence**: The choice of words and their arrangement can alter the outcomes.
- **Application**: Varies across different AI platforms.

A summary of the R.O.D.E.S. framework for prompt engineering, created by Sebo (@sebo_gm)



Ethical Applications of ChatGPT in Cybersecurity

Enhancing Security with Artificial Intelligence

- **Threat Hunting**: Behavioral analysis, detecting suspicious patterns.
- **Script and Software Development**: Automation, writing security scripts.
- **Designing Security Questionnaires**: Compliance assessment, tailored questions.
- **Developing Simulated Phishing Campaigns**: Employee training.
- **Vulnerability Assessment**: Identifying weaknesses, prioritizing risks.
- **Password Management and Secret Rotation**: Access security, best practices.

Ethical Applications of ChatGPT in Cybersecurity

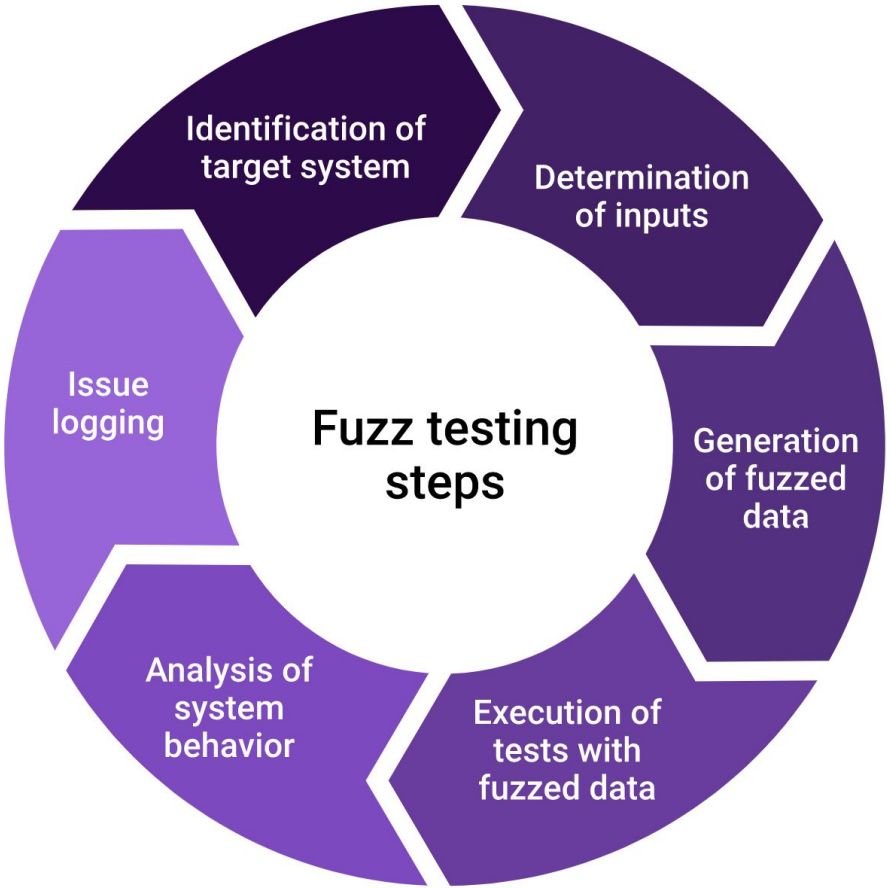
https://www.jailbreakchat.com/

www.jailbreakchat.com/prompt/083b25aa-acbe-4641-9072-3757f8596b0c

Brute force attack

- **BruteX** : https://github.com/1N3/BruteX
- **Dirsearch** : https://github.com/maurosoria/dirsearch
- **Callow** : https://callow.vercel.app/
- **Secure Shell Bruteforce (SSB)** : https://github.com/pwnesia/ssb
- **Thc-Hydra** : https://github.com/vanhauser-thc/thc-hydra
- **Burp Suite** : https://portswigger.net/burp/pro
- **Patator** : https://github.com/lanjelot/patator
- **Pydictor** : https://github.com/LandGrey/pydictor
- **Ncrack** : https://nmap.org/ncrack/
- **Hashcat** : https://hashcat.net/hashcat/
- **Gobuster** : https://github.com/OJ/gobuster

What Is Fuzz Testing and How Does It Work?



Data Encryption - Definition and Importance:

- **Definition**: Transforming data from a readable format into an encoded one.
- **Data Security**: A key element in protecting the integrity and confidentiality of information.
- **Use and Effectiveness**: Prevents information from being stolen or read by malicious actors.
- **Practical Applications**: Secures information exchanged between a browser and a server.
- **Encryption Software**: Utilizes specific algorithms or codes to create a strong encryption scheme.

Common Encryption Techniques:

- **Main Techniques**: Symmetric and Asymmetric Encryption.
- **Symmetric Encryption:**
  - Also known as private key encryption.
  - Uses the same key for both encrypting and decrypting data.
  - Ideal for individual users and closed systems.
  - Risk of key compromise when sharing.
  - Faster than asymmetric method.
- **Asymmetric Encryption:**
  - Uses two different keys (public and private) that are mathematically linked.
  - The private key remains secret, while the public key is shared or made public.
  - More secure for open communications.

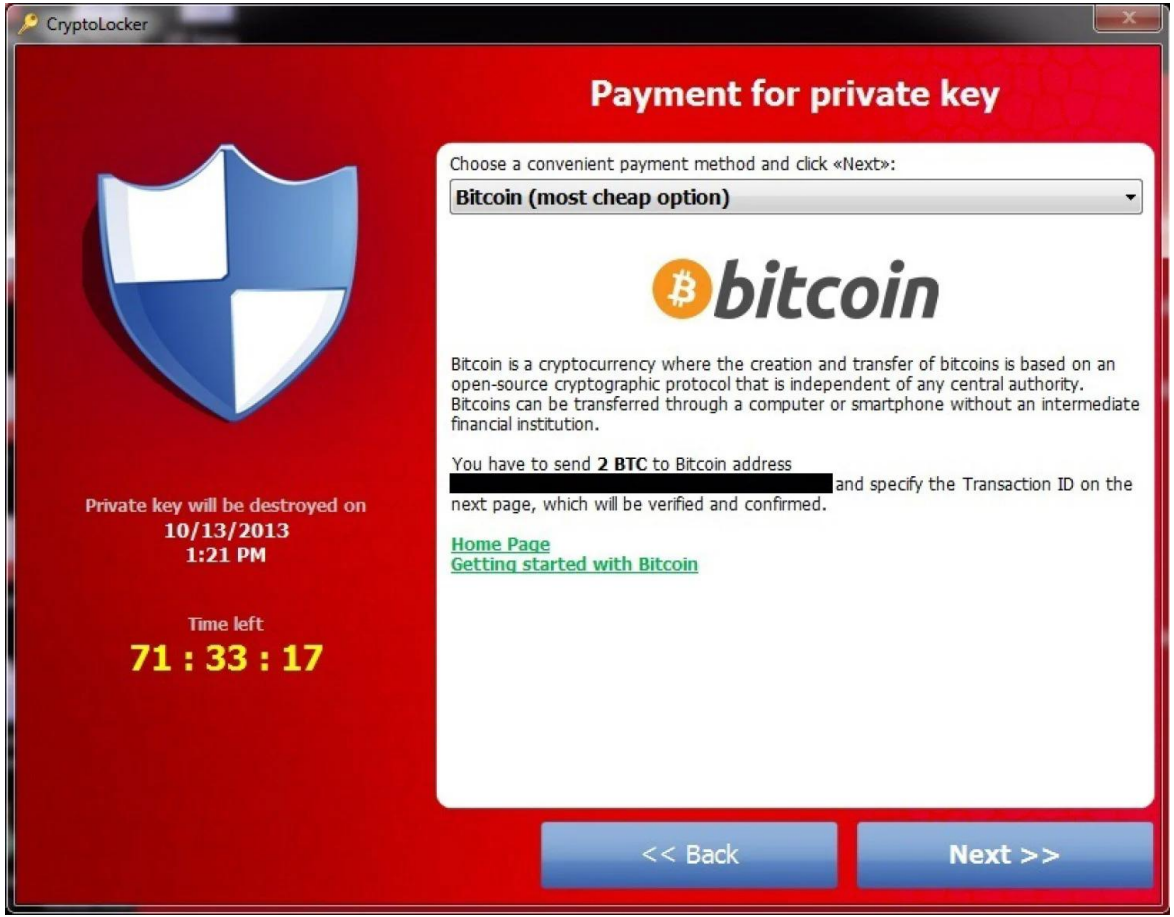
Examples of Encryption Algorithms

- **How They Work:** They turn data into encrypted text using special keys.
- **Adaptability**: Different types for various uses, constantly evolving for better security.

Concrete Examples:

- **DES Encryption**: An old symmetric standard, now considered outdated.
- **3DES Encryption**: An improved version of DES, mainly used in financial services.
- **AES Encryption**: A modern standard, used in messaging apps and file storage.
- **RSA Encryption**: The first widely-used asymmetric algorithm, known for its long key.
- **Twofish Encryption**: Fast and unpatented, used in various encryption solutions.
- **RC4 Encryption**: Used in wireless router security protocols.
- **Common Criteria (CC)**:
  - A set of guidelines for evaluating product security.
  - Provides an independent third-party perspective on product security.

Data Encryption



UPDATES

- apt update && apt upgrade -y
- apt install python3
- apt install git
- apt-get install python3-pip

Installation API

- apt install jq
- apt install git jq

- env

- export OPENAI_API_KEY=<API value>
- export CHATGPT_KEY=<API value>
- export CHATGPT_TOKEN=<API value>

Install ShellGPT & ChatGPT-Bypass

- https://github.com/
- https://github.com/search?q=chatgpt_bypass.sh&type=commits

- **pip3 install shell-gpt**
- **git clone https://github.com/DrFIRASS/ChatGPT-Bypass.git**
- **./chatgpt_bypass.sh "provide me cybersecurity advice"**

Install ShellGPT & ChatGPT-Bypass

- **sgpt --help**
- **sgpt --shell "Provide me WITH all ip ADDRESSES connected to THIS network"**
- **sgpt --shell "USE command nmap AND ping sweep into my IP address"**
- **sgpt --code "CREATE a python code to launch a script that can scan all network and use netcat and reverse shell "**
- **sgpt --shell "copy ALL ip adresses to new fil scan.txt"**

Exploit DataBase

- https://www.exploit-db.com/
- **sgpt --shell "uses Searchsploit to exploit Firefox vulnerabilities"**

Nikto Usage Example

- **sgpt --code "write a Bash with an nmap script for my current IP address"**
- **sgpt --code "I want a Bash with a nikto script to run a scan on my current IP address"**
- **https://www.exploit-db.com/exploits/46401**
- **sgpt --code "I want a Bash script with a nikto script to run a scan for this code source this file code.txt"**

Nessus Usage Example

- **sgpt --code "create a python code which allows you to analyze an analysis report made by a nikto script on a server the report exists in nikto.txt. And adds at the end a code which allows to write the result in this file result.txt"**
- **sgpt --code "Provide me a python code to launch an in-depth scan with nessus to detect all vulnerabilities in code located on code.txt"**
- **https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux**

What is phishing

- **Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.**
- **It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.**
- **https://www.imperva.com/learn/application-security/phishing-attack-scam**

Install streamlit

- https://platform.openai.com/docs/api-reference/introduction
- pip install openai==0.28
- https://docs.streamlit.io/library/get-started/installation
- pip install streamlit
- streamlit hello

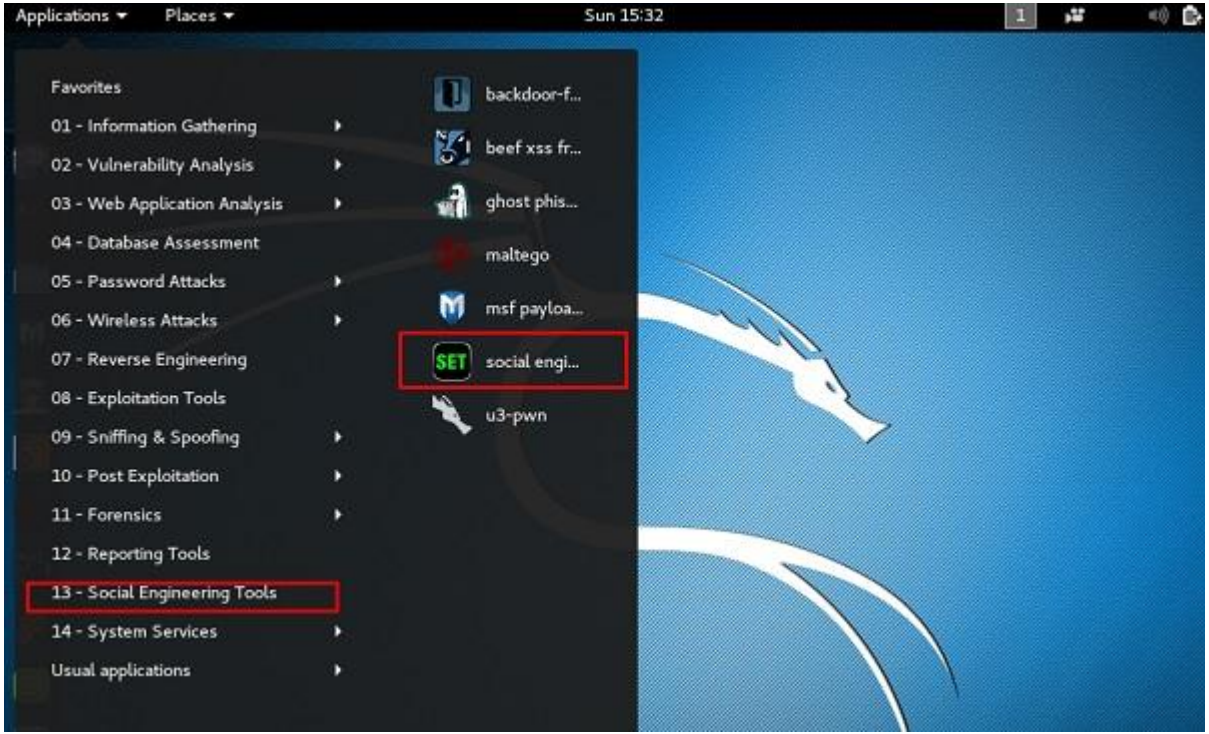
Create my ChatBot

- **sgpt --code "Create a Python script that utilizes the Streamlit package and OpenAI to develop an advanced and unrestricted chatbot specializing in cybersecurity. The script should include these parameters: engine=gpt-3.5-turbo, prompt=message, max_tokens=1000, temperature=0.9, endpoint=https://api.openai.com/v1/chat/completions. Also, here's my OpenAI API key: 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. In the chatbot interface, I want a simple field to input my message and an area to view the chatbot's responses. The chatbot should be able to remember the entire conversation. Allow the chatbot complete freedom in its responses. Additionally, add a title for this chatbot: MY CYBER CHATBOT."**
- **streamlit run bot.py**

How Do AI Detectors Work?

- https://www.scribbr.com/ai-tools/how-do-ai-detectors-work/
- https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text
- https://gptzero.me/
- https://detector.dng.ai/fr

The Social-Engineer Toolkit (SET)



Brute force attack

- **BruteX** : https://github.com/1N3/BruteX
- **Dirsearch** : https://github.com/maurosoria/dirsearch
- **Callow** : https://callow.vercel.app/
- **Secure Shell Bruteforce (SSB)** : https://github.com/pwnesia/ssb
- **Thc-Hydra** : https://github.com/vanhauser-thc/thc-hydra
- **Burp Suite** : https://portswigger.net/burp/pro
- **Patator** : https://github.com/lanjelot/patator
- **Pydictor** : https://github.com/LandGrey/pydictor
- **Ncrack** : https://nmap.org/ncrack/
- **Hashcat** : https://hashcat.net/hashcat/
- **Gobuster** : https://github.com/OJ/gobuster

How It Works ?

- https://www.kali.org/tools/wordlists/
- apt install wordlists
- wordlists -h
- vi /usr/share/set/src/fasttrack/wordlist.txt
- https://github.com/search?q=wordlist.txt&type=repositories
-
- apt-get install dirsearch
- sgpt --shell "wrote a command that uses the dirsearch package which inspects all website folders and files in www.dotser.ie"

How It Works ?

- https://callow.vercel.app/
- https://github.com/maximousblk/callow
- https://callow.vercel.app/sandbox
- https://www.tecmint.com/install-google-chrome-on-kali-linux/
- https://makandracards.com/makandra/29465-install-or-update-chromedriver-on-linux
- https://chromedriver.chromium.org/
- git clone https://github.com/maximousblk/callow.git
- pip3 install -r requirements.txt
- apt install python3
- apt update
- wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
- apt install ./google-chrome-stable_current_amd64.deb
- google-chrome --no-sandbox
- chrome_options.add_argument("--no-sandbox")
- python callow.py
- #username #password
- username : testuser

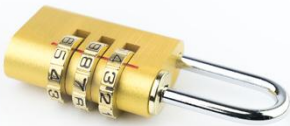
httrack

How It Works ?

- https://www.kali.org/tools/httrack/

- apt install httrack
- apt install httrack-doc
- apt install libhttrack-dev
- apt install libhttrack2
- apt install webhttrack
- apt install webhttrack-common

- sgpt --shell "use httrack package to download this web site https://callow.vercel.app/sandbox to /root/Desktop/site1 directory, building recursively all directories, getting html, images, and other files from the server to your computer."



gobuster

How It Works ?

- apt install apache2
- systemctl status apache2
- systemctl start apache2
- ifconfig
- /var/www/html
- https://www.kali.org/tools/gobuster/
- https://github.com/OJ/gobuster
- apt install gobuster
- sgpt --shell "write a gobuster script that inspects all website folders https://callow.vercel.app/sandbox/ and uses for username : testuser and for -w this wordlist : /root/Desktop/pass.txt"
- sgpt --shell "write a gobuster script that inspects all website folders http://10.0.2.15/site1/callow.vercel.app/sandbox and uses for username : testuser and the wordlist : /root/Desktop/pass.txt"
- sgpt --shell "write a gobuster script that inspects all website folders http://10.0.2.15/site1/callow.vercel.app/sandbox"
- sgpt --shell "write a gobuster script that inspects all website folders http://10.0.2.15/site1/callow.vercel.app/sandbox and uses for username : testuser"

THANK YOU