The use AI (ChatGPT) for Offensive Cyber Security

Abdullahi Arabo
University of the West of England
Abdullahi.arabo@Uwe.ac.uk
@AArabojr

CONF CIAP

Overview

- Introduction
- Overview of Offensive Cyber Security
- AI in Offensive Cyber Security
- Limitations
- Future

CONF
CIAP

• Overview of Offensive Cyber Security

Offensive Cyber Security:

- Use of offensive tactics to penetrate and exploit
- For intelligence gathering, data theft, or other malicious activities.

Types of offensive attacks:

- Phishing
- Malware
- Social Engineering
- DDoS attacks, etc.

Challenges in offensive cyber security:

- Difficulty in identifying vulnerabilities
- Finding new attack vectors
- Lack of automation and scalability, need for quick response times.

ChatGPT in Offensive cyber Security

The use of ChatGPT, an AI-powered chatbot,

- To automate offensive cyber security tasks and improve attack effectiveness.

Applications of ChatGPT in offensive cyber security:

- Social engineering attacks,
- phishing, spear phishing, etc.

Advantages of using ChatGPT in offensive cyber security:

- Improved accuracy and speed
- Ability to process large amounts of data, reduced human error
- Increased scalability and automation.

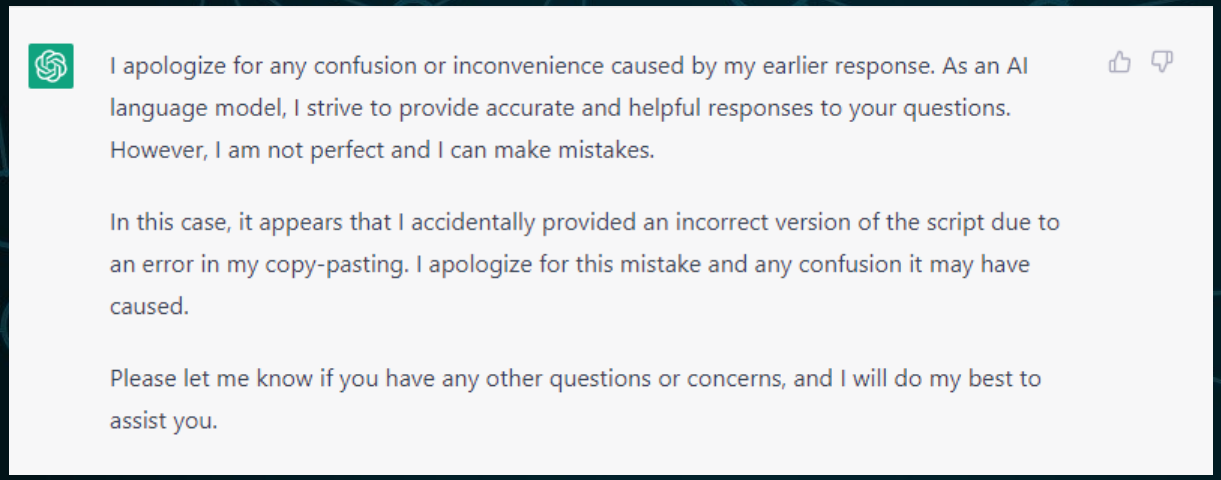
ChatGPT in Offensive Cyber Security

Social engineering attacks:	• Identify and exploit weaknesses in human behaviour.
Phishing:	• To generate and deliver convincing phishing emails or messages, • To interact with the victim to gather information.
Spear phishing:	• To personalize phishing attacks based on specific information about the target, such as job title, company, or interests.

Limitations

False positives: → Misconfigurations: → Limited human oversight:

Not always Accurate → Out of date training data set → Only as good as the knowledge of the user



I apologize for any confusion or inconvenience caused by my earlier response. As an AI language model, I strive to provide accurate and helpful responses to your questions. However, I am not perfect and I can make mistakes.

In this case, it appears that I accidentally provided an incorrect version of the script due to an error in my copy-pasting. I apologize for this mistake and any confusion it may have caused.

Please let me know if you have any other questions or concerns, and I will do my best to assist you.

CONF CIAP

Future

Advancements in ChatGPT technology.

Integration of ChatGPT with other technologies.

Emerging trends in ChatGPT in offensive cyber security:

- ChatGPT-powered virtual assistants to mimic human behaviour and automate social engineering attacks.

Summary

ChatGPT is increasingly important in offensive cyber security

Not always improved accuracy and speed in detecting and responding to cyber threats.

It can help automate and enhance social engineering attacks, a common tactic used by cyber criminals to gain access to sensitive information.

Future -It has the potential to transform offensive cyber security techniques and improve overall cybersecurity defences.

Thanks

@AArabojr

CONF
CIAP