**AIML Tool to Detect Phishing Domains**

The "AIML Tool to Detect Phishing Domains" project is a comprehensive cybersecurity initiative aimed at enhancing online security by leveraging Artificial Intelligence and Machine Learning (AIML) techniques to identify and mitigate phishing threats. Phishing attacks continue to be a significant cyber threat, exploiting unsuspecting users through deceptive websites that mimic legitimate domains to steal sensitive information.

Describe : Phishing attack is the most prevalent attack technique to compromise users worldwide. Phishing links/websites are shared through number of mediums like email, SMS etc. to target users. These domains are at times host user login page that imitates the genuine target websites. Login attempts on such pages can lead to compromise of user credentials and may also download malicious payload in user computers. The objective of the problem is to identify such phishing domains from the newly registered websites based on open source databases (Example WHOIS Database). Such databases provide list of newly registered domains. The tool should be automated and harness power of AI/ML to identify phishing domains from genuine domains. It may use the following techniques: (a) Backend code / content similarity in web pages. (b) Web page image analysis (i.e. analysis between genuine and phishing site web page images; more the similarity better is the probability score of being a lookalike phishing site). The evaluation would be based on the toolÃƒÂ¢Ã¢â€šÂ¬Ã¢â€žÂ¢s ability with regard to the following: (e) Probability scores of phishing domains on how close they are to the genuine domain. (f) Ability to detect new phishing domains in reasonable time. (g) Ease of use and flexibility in output formats.

**The primary objectives of this project include:**

Advanced AIML Algorithm Development:

Develop and implement cutting-edge AIML algorithms to analyze and detect patterns associated with phishing domains. This involves training the model on a diverse dataset of known phishing websites and legitimate domains to enhance accuracy and reduce false positives.

Feature Extraction and Analysis:

Identify and extract relevant features from URLs and webpage content that are indicative of phishing activities. This may include analyzing domain registration information, URL structure, SSL certificates, and content characteristics to create a robust feature set for the machine learning model.

Real-time Monitoring and Detection:

Implement a real-time monitoring system that continuously assesses incoming URLs and web content for potential phishing indicators. The AIML tool will act as a proactive defense mechanism, swiftly identifying and flagging suspicious domains to prevent users from falling victim to phishing attacks.

User-Friendly Interface:

Design an intuitive and user-friendly interface that allows both cybersecurity professionals and end-users to interact with the tool effortlessly. The interface should provide insights into detected phishing threats, allowing for quick response and remediation.

Integration with Existing Security Infrastructure:

Ensure seamless integration with existing cybersecurity frameworks and tools. This includes compatibility with popular web browsers, email clients, and other security solutions to provide a comprehensive defense against phishing attacks.

Continuous Learning and Adaptation:

Implement mechanisms for the AIML model to continuously learn and adapt to evolving phishing techniques. Regular updates and retraining of the model will be crucial to maintaining its effectiveness against emerging threats.

Performance Metrics and Reporting:

Define and measure key performance metrics to evaluate the effectiveness of the AIML tool. Generate detailed reports that highlight the number of detected phishing domains, false positives, and other relevant statistics to facilitate continuous improvement.

By developing an AIML-based tool to detect phishing domains, this project aims to significantly enhance cybersecurity measures, providing a proactive defense against one of the most prevalent and harmful forms of cyber threats in today's digital landscape.

**S/W Requirements :**

The software stack will encompass a range of tools and technologies essential for the development and deployment of the AI/ML phishing detection tool:

Machine Learning Frameworks: Utilize popular frameworks such as TensorFlow or PyTorch for the development of the phishing domain detection model.

Data Preprocessing Tools: Employ tools for cleaning, normalizing, and preparing datasets for effective machine learning model training.

Real-time Analysis Tools: Implement streaming analytics tools to enable real-time monitoring and analysis of web traffic for potential phishing indicators.

User Interface Development Tools: Use frameworks and libraries for developing a responsive and user-friendly interface for security professionals.

Integration APIs: Develop APIs for seamless integration with existing cybersecurity tools and platforms

**H/W Requirements :**

The project will leverage powerful hardware to support the intensive computational demands of AI/ML algorithms. The hardware requirements include:

Device Equipped with multi-core processors and sufficient RAM to handle large-scale data processing and analysis.

Dedicated GPU Acceleration: Utilize GPUs to accelerate the training and inference processes of the machine learning model, optimizing overall system performance.

Storage Solutions: Implement high-capacity, fast-access storage solutions to manage and store extensive datasets for training and ongoing analysis.