LITERATURE SURVEY

TEAM ID: PNT2022TMID08662
TITLE: WEB PHISHING DETECTION

1.Title: Detection of Phishing Websites by Using Machine Learning-Based URL Analysis.
Author: Mehmet Korkmaz, Ozgur KoraySahingoz, BanuDiri.

Year: 2020

Techniques Used: XGBOOST,RF , LR ,KNN,SVM,DTANN,NB

Description: A machine learning-based phishing detection system by using eight different algorithms to analyze the URLs, and three different datasets to compare the results with other works. The experimental results depict that the proposed models have an outstanding performance with a success rate.

2.Title: A Deep Learning-Based Framework for Phishing Website Detection

Author: Lizhen Tang , Qusay H. Mahmoud

Year: 2021

Techniques Used: RNN-GRU, web browser extension.

Description: The author briefed that they have implemented the framework as a browser plugin capable of determining whether there is a phishing risk in real-time when the user visits a web page and gives a warning message.It combines Temultiple strategies to improve accuracy, reduce false alarm rates, and reduce calculation time, including whitelist filtering, blacklist interception, and machine learning (ML) prediction.

3.Title: Detection of Phishing Websites from URLs by using Classification Techniques on WEKA

Author: BuketGeyik, Kubra Erensoy, EmreKocyigit

Year: 2021

Techniques Used: Machine learning, classification algorithms, phishing detection, cybersecurity

Description: The anti-phishing method has been developed by detecting the attacks made with the technologies used. we combined the websites used by phishing attacks into a dataset, then we obtained some results using 4 classification algorithms with this dataset.

4.Title: Real Time Detection of Phishing Websites

Author: Abdulghani Ali Ahmed, Nurul Amirah Abdullah

Year: 2016

Techniques Used: URL,Yahoo Datasets ,Phishing Detection

Description: A detection technique of phishing websites based on checking Uniform Resources Locators (URLs) of web pages. The proposed solution is able to distinguish between the legitimate web page and fake web page by checking the Uniform Resources Locators (URLs) of suspected web pages. URLs are inspected based on particular characteristics to check the phishing web pages. The detected attacks are reported for prevention. The performance of the proposed solution is evaluated using Phish tank and Yahoo directory datasets.

5.Title: Phishing URL Detection: A Real-Case Scenario Through Login URLs

Author: Manuel sánchez-paniagua , eduardo fidalgo fernández ,enrique alegre ,wesam alnabki, víctor gonzález-castro

Year: 2022

Techniques Used: Machine learning and deep learning approaches , cybercrime , phishing detection, url.

Description: The list provided on that website only contains the domain names, extracted the complete URL. To reach the login page from a website,It used the Selenium web driver and Python, checking buttons or links that could lead to the login form web page.Once we found the presumptive login and inspected if the form had a password field in order to confirm whether it was a login form. Otherwise, it was not added to the dataset. In this, collected reported phishing URLs from Phishtank.

6.Title: A Novel Machine Learning Approach to Detect Phishing Websites

Author: Ishant Tyagi, Jatin Shad, Shubham Sharma, Siddharth Gaur, Gagandeep Kaur

Year: 2018

Techniques Used: Decision Tree, Random Forest, Gradient Boosting , Generalized Linear Model, prediction for a new URL.

Description: In this technique ,they determined most targeted brand names and their legit URL via Google and their real phishing URLs from PhishTank website. Those extracted using python and used for prediction for a new URL. Input URL, Extract 30 features of URL, Use these features for predictive analysis,It checks whether it obtains positive or negative output.if negative it notifies the user that the website is phishing otherwise Notify the user that the website is safe.