Project Preview (1-2 pages)

Team # & Name: 4ortified

Project Manager (PM): Nicolas Rossi

Team members: Kahlamb Lewis, Eleon Annoor, Ghardesh Dolcharran

Deleted: Team members:

First Topic: Detecting and Preventing Phishing Attacks Using Machine Learning

Descriptions of your 1st topic: This topic aims to build and test a phishing detection system using machine learning techniques. We'll collect phishing datasets from PhishTank API, train a model, and evaluate it's accuracy. We'll use tools like Python, Scikit-learn, Pandas, and PhishTank Dataset.

- What are the research problems?

Phishing attacks remain as one of the most common cybersecurity threats, often bypassing traditional email filters. How can we improve phishing detection accuracy using open-source machine learning tools?

- What are the expected results?

A trained model that is capable of identifying phishing URLS or emails at a higher accuracy than standard filters.

- 1-2 References

- Verma, R., & Dyer, K. (2015). *On the Character of Phishing URLs: Accurate and Robust Statistical Learning Classifiers.* (Link)
- PhishTank (Link)

Second Topic: Testing for IP and DNS leaks while using a VPN

Descriptions of your 2nd topic: In this topic we will test several VPNs for IP address and DNS activity leaks. The IP leak test involves going to an IP detection site whilst connected to the VPN, to determine whether or not it will hide the IP. The DNS leak involves similar steps with the use of a DNS testing site instead

- What are the research problems?
Despite VPNs being designed to hide IP and DNS information, studies have found that several VPNs are still leaking information. This could be due to weak configurations, improper routing, or unencrypted DNS queries

- What are the expected results?
The only IP address visible after the test should VPN server's. The DNS server IPs should match the VPN server as well.

- 1-2 References
  - Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables(USENIX Security 2023)
  - VPNalyzer: Systematic Investigation of the VPN Ecosystem (pdf file)

Third Topic: Network Security Dashboard

Descriptions of your 3rd topic: A real-time monitoring tool that visualizes network activity, detects unusual traffic patterns, and alerts users of potential intrusions. It can simulate basic IDS (Intrusion Detection System) functionality for small networks like campus labs or student organizations.

- What are the research problems?

The main problem this project addresses is the **lack of cybersecurity awareness among college students**. Many students unknowingly fall victim to phishing scams, weak passwords, and unsafe online behavior. This research explores how **interactive learning and gamification** can improve cybersecurity habits and reduce human error, which is the leading cause of cyber incidents.

- What are the expected results?

Cybersecurity education is often technical and inaccessible to non-IT students. By developing an engaging web app like **CampusShield**, the project aims to make security education more approachable and practical. This contributes to building a **security-aware culture** on campus and helps reduce risks of data leaks, account breaches, and social engineering attacks.

- 1-2 References

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

https://pmc.ncbi.nlm.nih.gov/articles/PMC5501883/