University of Texas Rio Grande Valley

Department of Informatics and Engineering Systems

Past Capstone Project Abstracts

Bachelor of Science in Cybersecurity

Spring 2024

Malicious Network Traffic Analysis with Machine Learning

Team: Isaiah Ramirez

Advisor: Dr. Quweider

Abstract:

With the proliferation of network capable devices from host systems to servers, sensors, IoT, and cellular phones, there is a huge amount of data that is being transported in flight in the form of network traffic. Such traffic will likely carry malicious data among its benign traffic. To distinguish between malicious traffic and non-malicious traffic researchers have been using Machin Learning algorithms to train and automate the process. The goal of our capstone project is to take network traffic data and create a machine learning algorithm. The result should be a working program that can easily predict and classify traffic into two categories: non-malicious and malicious network traffic.

NetBox: A Networking Toolbox, An All-in-One Networking Tool Designed for Industry Novices

Team: Cody Bravo, Javier Cardenas, Christopher Enriquez

Advisor: Lucas Hall

Abstract:

One of the most important topics related to the field of cyber security is that of computer networks. When it comes to industry novices who are looking to gather information or troubleshoot a network, there is a plethora of different tools and options to use in a command-line interface which could be difficult for some users to navigate and interact with. This project aims to combine a number of different networking tools into a single graphical user interface (GUI) application as a way to make working with networks easier for those who may just be getting their careers started in the information technology industry or for those who are seasoned professionals and may want

Cybersecurity Training Platform with Gamification

Team: Alicia Dominquez, Jasmine Olivarez

Advisor: Lucas Hall

Abstract:

Social engineering is a method used by cybercriminals to take advantage of well-intentioned, or naïve, employees to gain unauthorized access to important, and often confidential, information from a target organization. Training and awareness are the most effective deterrents of common social engineering attacks. By building a cybersecurity training platform with gamification, the goal is to promote awareness of the signs of social engineering while also reinforcing their new knowledge through gameplay.

Comparative Analysis of Honeypot Types for Enhanced Cybersecurity

Team: Daniel Sanchez, Benito Juarez, Homero Ramirez

Advisor: Lucas Hall

Abstract:

Objectives:

1. Categorization and Classification: Systematically categorize different types of honeypots based on their purpose, deployment, level of interaction, design, location, and deployment stage.

2. Performance Metrics: Define and establish performance metrics to evaluate the efficacy of each honeypot type, considering factors such as detection rates, false positives, resource utilization, and ease of deployment.

3. Simulation Environment: Create a controlled and realistic simulation environment for deploying different honeypot types, ensuring a representative and comparable evaluation platform.

4. Data Collection and Analysis: Implement a systematic data collection process to capture and analyze the activities of potential attackers across various honeypot deployments. This includes studying attack patterns, tactics, and techniques employed.

5. Security Implications: Assess the security implications of deploying different honeypot types, considering both the protection they offer and any potential risks they may introduce to the network.

6. Practical Deployment Considerations: Investigate practical considerations for deploying and maintaining each type of honeypot in real-world scenarios, including scalability, ease of integration, and adaptability to evolving threats.

Expected Outcomes:

1. Comparative Effectiveness: Provide insights into the comparative effectiveness of different honeypot types in detecting and mitigating cyber threats.

2. Best Practices: Identify best practices and recommendations for deploying specific honeypot types based on the organization's security objectives and requirements.

3. Threat Intelligence: Contribute to the generation of valuable threat intelligence by understanding and documenting the tactics, techniques, and procedures (TTPs) employed by potential attackers across diverse honeypot environments.

4. Decision Support: Offer decision support for organizations looking to enhance their cybersecurity defenses through the strategic deployment of honeypots, considering the trade-offs and benefits associated with each type.

By undertaking this comparative analysis, the project aims to empower cybersecurity professionals and organizations with actionable insights to bolster their defenses and proactively address emerging cyber threats.

Serial Communication-based Device Identification

Team: Ramon Garcia

Advisor: Dr. Jorge Castillo

Abstract:

Serial communication protocols, i.e., USART, I2C or SPI, serve as a set of rules and conventions that govern the exchange of data between devices, one bit at a time, over a communication link. These protocols play a crucial role in ensuring reliable and efficient communication between electronic devices. In adversarial scenarios, where malicious actors may attempt to compromise systems via communicating devices, the ability to accurately identify infected devices becomes a fundamental aspect of maintaining a secure and resilient communication ecosystem. We aim to categorize devices by analyzing the distinct semiconductor properties exhibited, i.e., minimal changes in voltage, via serial communication protocols.