**ISS Capstone Project Presentations**

## **Friday, August 12th, 2022**

|  |  |  |
| --- | --- | --- |
| Title | Description | Presentation Time |
| **Containers: Modern Virtual Security** | Containers offer large improvements in software efficiency for large-scale operations such as YouTube, Netflix, and Amazon. Modernizing SaaS infrastructure comes with new risks, including standard web application and database exploitations, brute force attacks, and container escape exploitations.  The greatest threat to containerization systems is the risk of container escapes. If an unauthorized user can escape the isolated container environment, they will be able to access host machine, server, service, etc. to gain further system access.  This project is implementing a containerized web application and database to demonstrate web application attacks and application hardening techniques. It is also implementing a containerized honeypot service to entice potential attackers attempting SSH brute force attacks within a network. | **8:30-9:00 AM** |
| **The Authentication Simulation Station** | Authentication is one of the most important processes in the world of cybersecurity. The typical ‘username and password’ form of authentication leaves many users frustrated between password resets, monthly password changes and leaked or stolen password databases. Biometric authentication aims to alleviate these problems with passwords by using information from the biology of individuals. From smart phones to workstations, biometric authentication is quickly becoming a standard. This project will offer a look at the implementation of 2 forms of biometrics: Facial recognition and voiceprint analysis. it will also offer a comparison of these forms to the commonly established password framework. | **9:00 – 9:30 AM** |
| **Building a Cryptocurrency Token** | In the last decade cryptocurrency has become popularized virtual tender. One of the main cryptocurrency features is the reputation of being safe, in regards that currency that an individual hold cannot be plagiarized or falsified. This project focus on the elements in the construction of a cryptocurrency token as well as its security controls. The coding of smart contracts, how blockchains are appended, and the contents inside a blockchain node are explored. Additionally, theoretical weaknesses within a blockchain with prevention and mitigation techniques are explored. To demonstrate the token, the project is built on a forked private Ethereum block chain. | **9:30 – 10:00 AM** |
| **Securing Legacy Systems** | A legacy system is a technology, system or software program that no longer receives technical support, operating system patches and software upgrades but it is critical to an organization's day-to-day operations. Organizations keep legacy systems because it is challenging, costly and time-consuming to replace. Numerous vulnerabilities are present among older operating systems or applications due to a lack of proper security patches, which attracts adversaries attempting to exploit businesses and puts these systems at risk of being compromised. This project focuses on implementing proactive and reactive security measures to mitigate risks exposed by legacy systems so that organizations can continue using these end-of-life systems essential to managing their business. Boundary defence, firewall, IDS/IPS, system hardening, and continuous monitoring are some of the overall security strategies utilized in this project. | **10:00 – 10:30 AM** |
| **Resource Tracker WebApp** | This project presents a secure web application for resource tracking. This is an industry project which assists our partner, Deloitte, to develop a secure web application to automate their resource tracking process.  This project illustrates the end-to-end software development lifecycle (SDLC) from requirement analysis, design, implementation, and testing. It is also a full stack web development from front-end to backend which various technologies have been applied. ReactJS is chosen for the front-end web site development. MySQL database, Node.js and Express.js are chosen for backend server.  Web application security is one of our key concerns. During the development, various techniques are applied to mitigate potential web application vulnerabilities such as Code Injection, SQL Injection, XSS, and CSRF.  This project demonstrates the abilities of students in full stack web development as well as applying the cyber security knowledges learnt from this program. | **10:30– 11:00 AM** |
| **SIEM implementation on a network using the ELK-stack infrastructure** | A Security Information Event Management or SIEM system is a practical solution that identifies and analyzes activity from various sources on a network. It can then apply analytics to discover reoccurring trends as well as detect threats to alert management. The goal of this project is to fully build, configure and implement a SIEM infrastructure to analyze and log certain security devices and activities within a network. This will be achieved by implementing tools Elastic Search, Logstash and Kibana. Logs captured by various beats and visualization on Kibana will be demonstrated | **11:00– 11:30 AM** |
| **Purple Team**  **Training**  **Grounds** | In this project a network of virtual machines was set up to allow multiple users to practice a range of cybersecurity related skills. Broken into Red Team and Blue Team operations users can attempt to break and protect the virtual network in real time. Red Team tasks and challenges can be found in the form of: Active Directory Attacks and Recon, Network Recon and Exploitation, Privilege Escalation, and more. Blue Team tasks and challenges can be found in the form of: Firewall Configuration, IDS/IPS Configuration, Network Recon, Traffic Analysis, and more. With these challenges a sandbox type environment for participants to practice their cybersecurity skills was set up. | **11:30 – 12:00 PM** |
| **Splunk SIEM Tool** | In security we deal with a lot of information and being able to absorb and react to it quickly can be of great use during an attack. Being able to detect and solve problems quickly can save a company money and reputation. A SIEM tool allows us to have information sent to us and indexed to streamline the response. This project implements a functional SIEM tool, Splunk that will focus on catching signals of machines on the network and relaying the information of a specific attack depending on the symptoms. A playbook is created with a variety of attacks and solutions and/or recommendations on how to mitigate them. | **1:00 – 1:30 PM** |
| **The LoRaWan Protocol**  **Research** | IOT have a major role in people daily life, and the advancement of technology transformation is changing our world, making the future more desirable as well limitless possibilities. IoT provides higher level of data exchange, the ability to have stable communication, stable connectivity, and data analytics. Business, Governments, Banks, and Big Industries uses IoT to enhance the lives of their citizens. The LoRaWan is an open source communication protocol implemented in IoT devices that allows flexible and economical connectivity. It's a long-range wide area Network enabling farmers, smart city's, policing systems to have the benefit of low-cost quality data communication, also using low power. This Project performs a research on LoRaWan protocol, its advantages, disadvantages and security features and issues. A report will be provided with vulnerability’s findings and respective mitigations. | **1:30 – 2:00 PM** |
| **Educational Hacking Game** | This python programming project focuses on helping people become interested in the world of ethical hacking. The game emulates a Linux like filesystem and command line. Many of the commands that are used in the terminal are modeled off the real-world machines. The game is designed to provide a Hollywood style hacking experience while including real-world aspects that teach the player command line usage and machine exploitation. The process of exploiting machines is simplified to provide a mix of both fun and educational content for the player. | **2:00 – 2:30 PM** |
| **TAD**  **(The Active Deponent)**  **Vehicle/Asset Tracker** | This project creates a heatmap overlaid on satellite imagery using cellular and GPS enabled IoT solution that actively collects cell signal strength and location data at defined intervals, stored in the cloud, with a web app to display the data in a heatmap. The Notecard is not an application processor and hosts no customer application code. It can be used as data pump peripheral that is focused on bidirectional, asynchronous, secure data staging and transfer of JSON notes. The Notecard can also be configured as a low powered, autonomous, asset tracking device, in which case it does not require a host processor. Modern services require that the cloud and the device perform bidirectional authentication so that neither can be spoofed. For many applications it's important that over-the-air and over-the-wire data is encrypted. For this reason, this project’s Notecard integrates an STSAFE Secure Element which contains symmetric keys manufactured into the chip. Neither the manufacturer of the Notecard nor the manufacturer of the customer's product has any need to handle or manage secure key material. The keys generated by STMicroelectronics for the Notecard use ECC with the NIST P-384 curve, and the signature algorithm is ECDSA-with-SHA384. | **2:30 – 3:00 PM** |
| **Facial Recognition Security Program with Multi-Factor Authentication** | Facial recognition is contactless technology which allows people to authenticate themselves without interacting with the device. It also is hygienic and convenient as it does not come into contact with the recognition equipment. In this project a facial recognition program was built implementing machine learning technology. A multi-factor authentication system was implemented for enhanced security. A web page was created for authentication, and a database to manage user IDs and passwords. Camera usage detections after face recognition will be recorded on a log file. The log file can be accessed by security system administrators to enhance security. | **3:00 - 3:30 PM** |
| **Deploying a containerize Environment: Docker and Kubernetes Research** | Over the years, Server rooms have become smaller, coupled with the fact that IT administrators continued to seek for a more economical but productive ways to deploy companies' IT resources in a one-fit all system.  Docker and Kubernetes fit this goal. These allow for the cluster of operating systems but extremely light weight that uses only few resources. This report will seek to highlight and demonstrate the benefits of deploying a docker and Kubernetes in a Linux machine as well as some security risks associated with its deployment. The project will explore from docker set-up to its implementation in a production environment. | **3:30 – 4:00 PM** |
| **Fish Tank Monitor and Live Video System** | Fish tanks or aquariums house many living species that need to be in a controlled environment. Many tanks have little to no monitoring of the levels of oxygen, pH, or temperature that the owners can view in real-time. This project focuses on set up a secure fish monitoring system that utilizes multiple Raspberry Pi’s that monitor the water temperature, and the pH of the water and has a camera that overlooks the fish tank. The data is transferred into a secure server that is hosted on a Raspberry Pi. From the server hosted on the second raspberry pi, the end-user will be able to view the sensor readings by a secure web app and view the fish tank in real-time. Because the levels of the water must be accurate and no one other than the account owner should be able to view their fish tank, authentication of the user accounts must be secured, and the values of the monitor readings cannot be altered. | **4:00 – 4:30 PM** |

Topic: Information System Security Capstone Project Presentation

Time: Aug 12, 2022 08:30 AM Edmonton

Join Zoom Meeting

<https://sait-ca.zoom.us/j/85617297627?pwd=TDlVaWd3OUE3am9EZ05MZ3BYQXpzdz09>

Meeting ID: 856 1729 7627

Passcode: 438804

One tap mobile

+16694449171,,85617297627# US

+16699006833,,85617297627# US (San Jose)

Dial by your location

+1 669 444 9171 US

+1 669 900 6833 US (San Jose)

+1 929 436 2866 US (New York)

+1 253 215 8782 US (Tacoma)

+1 301 715 8592 US (Washington DC)

+1 312 626 6799 US (Chicago)

+1 346 248 7799 US (Houston)

+1 646 931 3860 US

Meeting ID: 856 1729 7627

Find your local number: <https://sait-ca.zoom.us/u/kcLpNGQpcu>