PROJECT SPECIFICATION AND PLAN

Learning Platform for Cyber Security Professionals

Laura Chudzio - C00253150

Table of Contents

What is the project supposed to be?

The fundamental purpose of this project is to create and establish a comprehensive training program explicitly tailored for security professionals. This training program serves as a dynamic and multifaceted platform designed to equip individuals working within the cybersecurity field with the essential knowledge, skills, and practical expertise they need to thrive in their roles. The learning platform will be hosted on a website.

What will the project deliver?

Core Deliverables:

1. Website features
   - The website will be written in HTML, CSS, PHP, and JavaScript. The website will include a database for user login and passwords. The passwords within the database will be hashed and salted for security measures. The website will allow the user to keep track of their progress on the platform.
   - Hands-on training modules with practical exercises.
   - Assessments and exams to evaluate students' understanding.
   - Certification upon successful program completion.

2. This component of the project encompasses the creation of a structured and flexible curriculum. The curriculum is organized into modules, each dedicated to a crucial aspect of cybersecurity. These modules address vital security areas such as Vulnerability Management, Encryption, Password Management, Antivirus Software, Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Penetration Testing, and Network Security Monitoring. Each module provides in-depth knowledge and practical skills relevant to its respective security domain.

   The content of the learning platform:

   - **Vulnerability Management:** how to identify and address vulnerabilities in systems and applications, enabling them to proactively safeguard digital assets. (Fekete, Hufschmidt, & Kruse, 2014)
   - **Encryption:** encryption methods, algorithms, and their applications, ensuring participants can secure sensitive data through encryption.
   - **Password Management:** Access control, this module teaches best practices for creating, storing, and managing secure passwords, mitigating a common security risk. (humans.txt, n.d.)
   - **Antivirus Software:** functionality and limitations of antivirus solutions, making informed decisions about endpoint security. (Henry, n.d.)
   - **Web Application Firewall (WAF):** Role of WAFs in protecting web applications from threats, covering rule creation, threat detection, and incident response.
   - **Intrusion Detection System (IDS):** Deploy, configure, and monitor IDS solutions to detect and respond to suspicious network activities and security breaches. (Campos, Oliveira, & Roisenberg, 2012)
   - **Intrusion Prevention System (IPS):** Building on IDS knowledge, implementing proactive measures to prevent security incidents, such as blocking malicious traffic and attacks. (Stiawan, Idris, & Abdullah, 2011)
   - **Penetration Testing:** Engage in ethical hacking practices, assessing system vulnerabilities, exploiting them, and providing recommendations for strengthening security.
   - **Network Security Monitoring:** Network security monitoring, encompassing log analysis, anomaly detection, and incident response procedures, ensuring network infrastructure resilience.

Non-Core Deliverables:

1. Online community platform for participants.
2. Course recommendations.
3. A resource library with articles, whitepapers, videos, and tutorials.

Who is going to be using this?

The primary audience for this comprehensive cybersecurity training program is mid-level security professionals looking to advance and enhance their existing skill sets. These individuals typically have a foundational understanding of cybersecurity principles and may have some experience in the field. However, they aspire to take their careers to the next level by acquiring more in-depth knowledge, practical expertise, and specialized skills in various cybersecurity domains.

Metrics

To assess the success of my fourth-year project, I will consider the following aspects:

1. Learning Outcomes – Acquisition of New Tools and Skill Expansion.
2. Certification Completion – Keeping track of necessary deliverables, to ensure that enough of work is put in place.
3. Job placement – The project could be reviewed from previous employer within cyber security.
4. Operational status – Conduction of assessments to verify the proper functioning of all components.

Is there a precedent for this application?

- This project is an inspiration from existing cybersecurity college course and other educational platforms such as TryHackMe, Hackthebox and it incorporates valuable insights gained from past experiences during my internship as a cybersecurity analyst.

How it differs:

- This program offers a unique capability analysis of security tools and techniques, providing practical insights into their use and effectiveness.
- Emphasizes hands-on training and real-world scenarios.
- Offers a community-building component to encourage networking and collaboration.

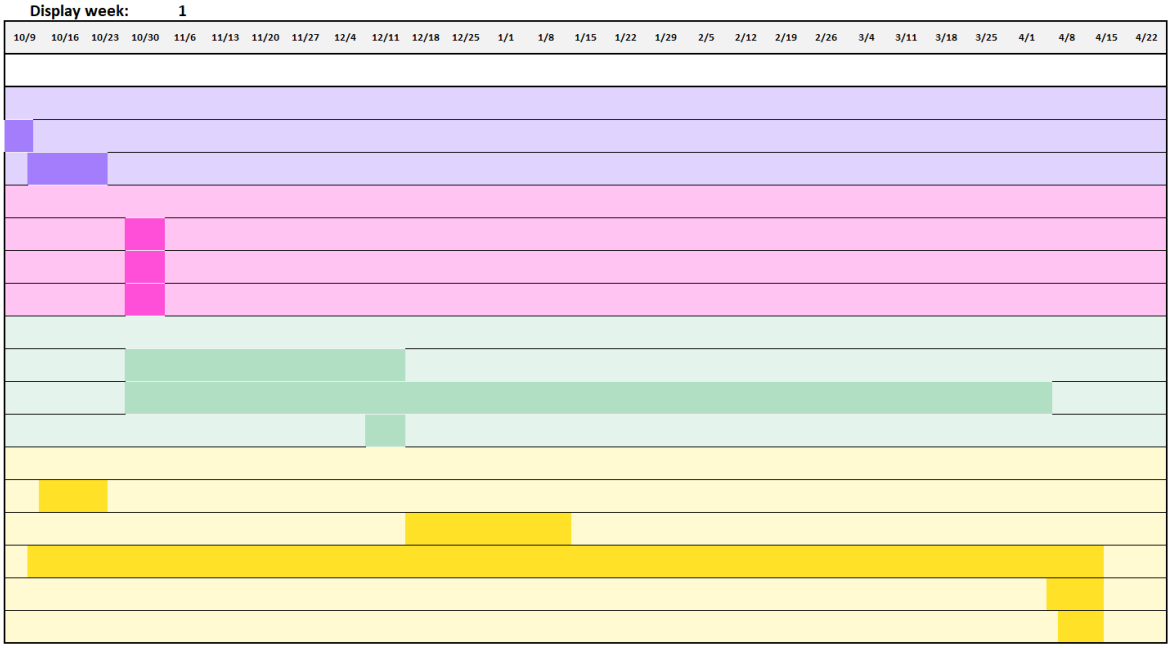
Plan - Timeline

The Gannt Chart below shows a timeline for each task that needs to be completed in this project. (Chakraborty, 2016)

Gannt Chart for Learning platform for cyber security professionals

Display week: 1

Project Start	09/10/2023
TASK	START
Initiation	
Project Idea	09/10/2023
Define goals	13/10/2023
Planning and design	
Website Skelaton	30/10/2023
Research document Skelaton	30/10/2023
Website content plan	30/10/2023
Execution	
Website Work	30/10/2023
Research	30/10/2023
Final Checks for website	11/12/2023
Documentation	
Project Spec	15/10/2023
Presentation	18/12/2023
Final Report	13/10/2023
Proof Read	08/04/2024
Upload final work	10/04/2024



Bibliography

Campos, L. M., Oliveira, R. C., & Roisenberg, M. (2012). *Network Intrusion Detection System Using Data Mining*. Retrieved 10 27, 2023, from https://link.springer.com/chapter/10.1007/978-3-642-32909-8_11

Chakraborty, M. (2016). *Library Guides: SOWK 410 Practice III: GANNT Chart*. Retrieved 10 27, 2023, from http://libraryguides.salisbury.edu/c.php?g=460163&p=4394929

Fekete, A., Hufschmidt, G., & Kruse, S. (2014). Benefits and challenges of resilience and vulnerability for disaster risk management. *International Journal of Disaster Risk Science, 5*(1), 3-20. Retrieved 10 27, 2023, from https://link.springer.com/article/10.1007/s13753-014-0008-3

Henry, A. (n.d.). *The Difference Between Antivirus and Anti-Malware (and Which to Use)*. Retrieved 10 27, 2023, from http://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277

humans.txt. (n.d.). *Enterprise Password Management - Self Service Password Reset - Password Reset - Password Station - Avatier*. Retrieved 10 27, 2023, from https://www.avatier.com/products/identity-management/password-management/password-station/

Stiawan, D., Idris, M. Y., & Abdullah, A. H. (2011). Characterizing Network Intrusion Prevention System. *International Journal of Computer Applications, 14*(1), 11-18. Retrieved 10 27, 2023, from https://ijcaonline.org/archives/volume14/number1/1811-2439

Takemura, T., & 竹村, 司. (2002). *Schedule development method, program, and task schedule development device*. Retrieved 10 27, 2023, from https://patents.google.com/patent/jp2004157805a/en