**Self-Assessment**

My journey into IT started with a genuine curiosity about how technology works and a desire to solve problems. Early experiences tinkering with computers, combined with a stint at Geek Squad, gave me a solid foundation in troubleshooting and customer service. Helping my aunt's company with their IT issues further solidified my interest in pursuing a career in this field. I realized the impact technology has on businesses and how vital it is to keep systems running smoothly and securely. This led me to pursue a BS in Cybersecurity and obtain my CompTIA Security+ certification.

My coursework has been instrumental in developing my technical skills. I’ve delved into SQL exploits, learned Python programming, and gained expertise in developing IDS plans. While I’m confident in my ability to analyze security threats and propose solutions, I recognize the need to further develop my software development skills. My focus and determination are definite strengths. I’m able to immerse myself in complex problems and see them through to resolution. However, I sometimes get so engrossed in the technical aspects that I overlook the bigger picture or the human element. I’m working on improving my communication and collaboration skills to ensure I can effectively convey technical information to non-technical audiences and work seamlessly within a team.

My goal is to become a Security Analyst, leveraging my skills and knowledge to protect organizations from cyber threats. The penetration testing project at Brown & Haley is a perfect opportunity to apply my learning in a real-world setting and gain valuable experience. I’m excited about the challenge and eager to contribute to the company's security posture. I'm confident that my dedication, combined with the guidance of my site supervisor, Dan Fabian, will lead to a successful project outcome. One potential challenge I foresee is balancing the project's technical demands with the need to effectively communicate and collaborate with stakeholders who may not have a deep understanding of cybersecurity. I’m committed to overcoming this challenge by practicing clear and concise communication and actively seeking feedback.

**Lifelong Learning and Professional Development Plan**

The IT field is constantly evolving, making continuous learning essential for staying relevant and competitive. My lifelong learning plan focuses on staying up-to-date with the latest security threats and technologies, deepening my technical expertise, and enhancing my soft skills. Specifically, I plan to:

* **Pursue relevant certifications:** I aim to obtain certifications like the Certified Ethical Hacker (CEH) and the Certified Information Systems Security Professional (CISSP) to demonstrate my expertise and commitment to the field.
* **Engage in continuous learning:** I will stay current with emerging threats and technologies by attending industry conferences, participating in online forums, and subscribing to relevant publications.
* **Develop software development skills:** I will dedicate time to improving my coding proficiency in languages like Python and Javascript to enhance my ability to develop security tools and automate tasks.
* **Cultivate mentorship relationships:** I will seek out mentors in the cybersecurity field to gain insights, guidance, and support throughout my career.
* **Join professional organizations:** I will actively participate in organizations like (ISC)² and SANS to network with other professionals and stay informed about industry best practices.

This continuous learning approach is crucial for adapting to the ever-changing landscape of cybersecurity and ensuring I can effectively contribute to the field.

**Action Learning Summary**

Action learning is a powerful approach to learning by doing. It involves tackling real-world problems, reflecting on experiences, and learning from both successes and failures. As the project leader for the penetration testing project, my role in the action learning process is multifaceted:

* **Communication:** I've used email, phone calls, and video conferencing to communicate with my site supervisor, Dan Fabian, and other stakeholders. I’ve also documented my progress and findings in written reports.
* **Decision Tools:** I’ve used project management software like Trello to organize tasks, track progress, and collaborate with team members. I've also utilized various security tools for the penetration testing itself.
* **Collaboration:** Collaboration with Dan has been essential in shaping the project scope and ensuring its alignment with Brown & Haley's needs. His feedback has been invaluable in refining my approach and ensuring the project's relevance.
* **Reflective Learning:** My coursework at Capella has provided me with a strong theoretical foundation in cybersecurity, which has been crucial in guiding my approach to the penetration testing project. My previous work experience, while not directly related to security, has helped me develop problem-solving and customer service skills that have been beneficial in this project. One lesson learned is the importance of clear and frequent communication with stakeholders to manage expectations and ensure project success.

This action learning experience has not only allowed me to apply my knowledge and skills but also to identify areas for improvement and develop a deeper understanding of the challenges and rewards of working in a real-world environment. I will carry these lessons forward in my future endeavors in the cybersecurity field.