Final IAL Proposal

Leo Newton

IT-FPX4993 – Cybersecurity Capstone

Capella University

Professor Williams

12/15/24

Table of Contents

[Executive Summary 3](#_Toc185177926)

[Project Scope 3](#_Toc185177927)

[Milestones and Deliverables 4](#_Toc185177928)

[Risks and Communication Plan 4](#_Toc185177929)

[Organization and site supervisor selection 5](#_Toc185177930)

[Environmental Scan 6](#_Toc185177931)

[SWOT Analysis 6](#_Toc185177932)

[Process of Developing a Project Charter 7](#_Toc185177933)

[Research on Charter Elements 8](#_Toc185177934)

[Intersection between SWOT Analysis and Project Charter 9](#_Toc185177935)

[Conclusions based on SWOT Analysis 10](#_Toc185177936)

[Literature Review Outline 10](#_Toc185177937)

[Annotated Bibliography 15](#_Toc185177938)

[Self-Assessment 18](#_Toc185177939)

[Lifelong Learning and Professional Development Plan 20](#_Toc185177940)

[Action Learning Summary 20](#_Toc185177941)

[Solutions Analysis 21](#_Toc185177942)

[Proposed Model/Architecture 23](#_Toc185177943)

[Recommended Technology 23](#_Toc185177944)

[Supporting IT Principles 23](#_Toc185177945)

[Key Legal, Ethical, and Policy Issues 24](#_Toc185177946)

[Needs and Risk Analysis 24](#_Toc185177947)

[Risk Matrix 24](#_Toc185177948)

[Barriers and Adjustments 25](#_Toc185177949)

[Insights and Advice 25](#_Toc185177950)

[Legal, Ethical, and Policy Analysis 25](#_Toc185177951)

[Reflection 27](#_Toc185177952)

[References 29](#_Toc185177953)

# Executive Summary

Brown & Haley, a renowned confectionery company based in Tacoma, Washington, faces increasing cybersecurity threats common to the manufacturing and food industries. While the company has a robust IT infrastructure supporting its operations, its cybersecurity practices have not kept pace with the evolving threat landscape. Recognizing this vulnerability, Office Manager Dan Fabian initiated this project to proactively assess and enhance the company's security posture. This project aligns with Brown & Haley's strategic objectives of protecting its intellectual property, maintaining business continuity, and safeguarding its brand reputation (Corvell, 2024).

The primary objective of this project is to identify and assess vulnerabilities in Brown & Haley's IT infrastructure to reduce the risk of cyberattacks and data breaches. Specific objectives include:

* Identify and document all critical vulnerabilities in the company's network, systems, and applications.
* Assess the potential impact of these vulnerabilities on business operations.
* Provide actionable recommendations for remediation to improve the company's security posture.
* Enhance employee cybersecurity awareness and training.
* Comply with industry regulations and best practices for cybersecurity.

# Project Scope

This project will encompass a comprehensive penetration test of Brown & Haley's IT infrastructure, including both the factory and office environments. The scope includes:

* **Network Penetration Testing:** Assessing the security of the company's network perimeter, including firewalls, routers, and other network devices.
* **Web Application Penetration Testing:** Evaluating the security of the company's website and other web applications.
* **Wireless Network Penetration Testing:** Analyzing the security of the company's wireless networks.
* **Social Engineering Testing:** Simulating social engineering attacks to assess employee susceptibility to phishing and other social engineering tactics.

The scope explicitly *excludes* physical security assessments, penetration testing of third-party systems not directly managed by Brown & Haley, and any activities that could disrupt critical business operations.

# Milestones and Deliverables

|  |  |  |
| --- | --- | --- |
| Milestone | Deliverable | Date |
| Project Initiation | Project Charter Approved | 2024-01-15 |
| Planning and Scoping | Penetration Test Plan Document | 2024-01-29 |
| Vulnerability Scanning | Vulnerability Scan Report | 2024-02-12 |
| Penetration Testing | Penetration Test Report | 2024-02-26 |
| Remediation Recommendations | Remediation Plan Document | 2024-03-11 |
| Project Closure | Final Project Report and Presentation | 2024-03-25 |

# Risks and Communication Plan

**Potential Risks**

* **Service Disruption:** Mitigated by conducting testing during off-peak hours and having rollback plans.
* **Undiscovered Vulnerabilities:** Mitigated by using multiple testing tools and techniques, and retesting after remediation.
* **False Positives:** Mitigated by thorough validation of findings.

**Communication Plan**

* **Weekly Status Reports:** Provide Dan Fabian with weekly updates on project progress, identified vulnerabilities, and remediation recommendations.
* **Final Report and Presentation:** Present a comprehensive final report and presentation to Dan Fabian and other key stakeholders, outlining the project findings and recommendations.
* **Ad-hoc Communication:** Maintain open communication channels with Dan Fabian and the IT team to address any questions or concerns throughout the project.

Communication with stakeholders, including Dan Fabian, IT staff, and executive management, will be maintained throughout the project lifecycle through regular meetings, email updates, and a final presentation of findings and recommendations. This proactive approach aligns with best practices for risk communication (Hooker & Leask, 2020).

This penetration testing project will significantly enhance Brown & Haley's cybersecurity posture, protect its valuable assets, and strengthen its reputation as a secure and reliable business partner.

# Organization and site supervisor selection

* **Name:** Dan Fabian
* **Organization:** Brown & Halley
* **Contact Information:** [dfabian@brown-haley.com](https://www.google.com/url?sa=E&q=mailto%3Adfabian%40brown-haley.com)
* **Role:** Office Manager
* **Length of Time with Organization:** 15 years
* **Contact Method:** Met through a work agency a couple of years ago.
* **Relevant Information:** Dan oversees the day-to-day operations of the office, including IT infrastructure and cybersecurity practices. He is responsible for implementing new technologies and processes, making him a key stakeholder for this project. He has expressed concerns about the company's current cybersecurity posture and is actively seeking ways to improve it.

# Environmental Scan

**Introduction to Brown & Haley and Current Situation**

Brown & Haley is a well-established chocolate candy factory located in Tacoma, Washington. Known for its Almond Roca and other confections, the company has a significant presence in the region and distributes its products nationally and internationally. While Brown & Haley has embraced technology for manufacturing and sales, its cybersecurity practices have not kept pace with the evolving threat landscape. This presents a significant risk to the company's operations, intellectual property, and reputation.

**Problem/Improvement Area**

Brown & Haley needs a comprehensive penetration test conducted to assess the security of its IT infrastructure, both in the factory and office environments. This assessment will identify vulnerabilities and weaknesses that could be exploited by malicious actors, providing a roadmap for implementing necessary security improvements.

# SWOT Analysis

* **Strengths:**
  + Established brand recognition and market share.
  + Strong local presence and community ties.
  + Experienced workforce in manufacturing and sales.
  + Existing IT infrastructure, albeit with security gaps.
  + Management's willingness to invest in security improvements.
* **Weaknesses:**
  + Outdated cybersecurity practices and infrastructure.
  + Lack of dedicated cybersecurity personnel.
  + Limited employee training on cybersecurity awareness.
  + Potential vulnerabilities in both physical and digital security.
  + No documented incident response plan.
* **Opportunities:**
  + Implementing robust cybersecurity measures to protect sensitive data and intellectual property.
  + Enhancing brand reputation and customer trust by demonstrating a commitment to security.
  + Leveraging technology to improve efficiency and productivity in a secure environment.
  + Meeting increasing industry regulations and compliance requirements.
  + Attracting and retaining talent by fostering a secure and technologically advanced workplace.
* **Threats:**
  + Increasingly sophisticated cyberattacks targeting manufacturing and food industries.
  + Data breaches and ransomware attacks leading to financial losses and reputational damage.
  + Industrial espionage and theft of intellectual property.
  + Disruption of operations due to cybersecurity incidents.
  + Regulatory penalties for non-compliance with security standards.

# Process of Developing a Project Charter

Developing a project charter is a crucial first step in any project, as it formally authorizes the project and provides the project manager with the authority to allocate resources. It serves as a foundational document, outlining the project's purpose, scope, and key stakeholders, and guiding the project team throughout its lifecycle.

1. **Identify the Need:** This usually starts with a business case or a problem statement, outlining the reason for initiating the project.
2. **Define High-Level Scope and Objectives:** What are the project's goals? What are the key deliverables? What's included and excluded?
3. **Identify Key Stakeholders:** Who are the individuals or groups impacted by or who can influence the project?
4. **Assign a Project Manager:** This individual will be responsible for leading and managing the project.
5. **Develop the Project Charter:** This document formally authorizes the project and outlines key information.
6. **Review and Approve the Charter:** Key stakeholders review and approve the charter, signifying their agreement and commitment.

# Research on Charter Elements

* **Clear Project Objectives:** Instead of vague statements, use SMART (Specific, Measurable, Achievable, Relevant, Time-bound) objectives. For example, instead of "Improve cybersecurity," a SMART objective would be "Reduce the number of critical vulnerabilities identified in a penetration test by 50% within six months." This aligns with research emphasizing the importance of clear goals for project success (Locke & Latham, 2002).
* **Well-Defined Scope:** Clearly delineate what is included and, importantly, what is *excluded* from the project scope. This prevents scope creep and ensures the project team focuses on the agreed-upon deliverables. For example, a penetration test charter might explicitly exclude physical security assessments. This is supported by research showing that clearly defined scope reduces project failure rates (PMI, 2021).
* **Stakeholder Analysis:** Go beyond just listing stakeholders. Analyze their influence and interest levels using a power/interest grid. This helps prioritize communication and engagement strategies. Research by Mitchell, Agle, and Wood (Mitchell et. al., 1997) highlights the importance of stakeholder salience in project management.
* **Risk Assessment:** Include a preliminary risk assessment in the charter, identifying potential risks and outlining mitigation strategies. This proactive approach helps avoid surprises and delays later in the project. This aligns with research on risk management best practices (Kaplan et. al., 2024).
* **Communication Plan:** Outline how communication will be managed throughout the project. Specify communication frequency, methods, and responsible parties. Research by Pinto and Slevin (Pinto et. al., 1988) emphasizes the crucial role of effective communication in project success.
* **Defined Success Criteria:** Clearly define what constitutes project success. These criteria should be measurable and tied to the project objectives. For example, "Successful completion of the penetration test and delivery of a comprehensive vulnerability report within the allocated budget and timeframe."
* **Explicit Authorization:** The charter must include a clear statement of authorization from the project sponsor, granting the project manager the authority to proceed and allocate resources.
* **Version Control:** Implement version control for the charter to track changes and ensure everyone is working with the most up-to-date document.

By incorporating these research-backed recommendations, project charters become more effective tools for guiding projects towards successful completion. They provide clarity, alignment, and a solid foundation for decision-making throughout the project lifecycle.

# Intersection between SWOT Analysis and Project Charter

The SWOT analysis directly informs the project charter by providing a clear understanding of the context in which the penetration testing project will take place. The identified weaknesses (e.g., outdated cybersecurity practices) become the drivers for the project objectives. The opportunities highlighted in the SWOT analysis contribute to the project's business case, justifying the investment in security improvements. Threats underscore the urgency and importance of the project. Finally, the strengths can be leveraged to support project execution. For example, management's willingness to invest in security improvements facilitates securing necessary budget and resources within the project charter.

# Conclusions based on SWOT Analysis

The SWOT analysis reveals a clear need for improved cybersecurity measures at Brown & Haley. The penetration testing project is crucial to identify and address vulnerabilities before they are exploited by malicious actors. By investing in this project, Brown & Haley can mitigate the identified threats, capitalize on the opportunities, and strengthen its overall security posture. This will not only protect the company's assets but also enhance its reputation and ensure its long-term sustainability. This project will allow me to utilize my cybersecurity knowledge and skills to make a significant contribution to the organization and gain valuable real-world experience. My role will be to plan, execute, and document the penetration test, working closely with Dan Fabian to ensure the project aligns with the company's needs and objectives.

# Literature Review Outline

**I. Introduction**

* **The Importance of Penetration Testing:** Penetration testing is a simulated cyberattack against a computer system, network, or web application to identify security vulnerabilities. It is a crucial aspect of proactive cybersecurity, allowing organizations to discover and mitigate weaknesses before malicious actors can exploit them. In today's interconnected world, where organizations rely heavily on technology and cyber threats are becoming increasingly sophisticated, penetration testing is no longer optional but essential for maintaining a strong security posture.
* **Focus and Scope of the Review:** This literature review examines existing methodologies, tools, and emerging trends in penetration testing, with a specific focus on its application to manufacturing environments. It explores the unique challenges and security considerations relevant to industrial control systems (ICS) and operational technology (OT) environments, providing context for the penetration testing project at Brown & Haley.
* **Context of Brown & Haley:** Brown & Haley, a confectionery manufacturer, relies heavily on technology for its operations, from production and inventory management to sales and distribution. This reliance increases their exposure to cyber threats, making robust cybersecurity crucial. A penetration test is necessary to identify vulnerabilities in their systems and networks, protecting sensitive data, preventing disruptions to operations, and maintaining the company's reputation. Potential risks include data breaches, ransomware attacks, and disruption of critical manufacturing processes.

**II. Penetration Testing Methodologies and Frameworks**

* **Overview of the Penetration Testing Lifecycle:**
  + Royce (2020): Detailed explanation of each stage in the penetration testing lifecycle: planning and scoping, reconnaissance, vulnerability scanning, exploitation, post-exploitation, and reporting. Highlight the importance of understanding the attacker's mindset and the value of a comprehensive penetration testing report.
  + Mandal (2022): Discussion of common penetration testing methodologies, such as black-box, white-box, and grey-box testing. Explanation of different types of penetration tests (e.g., network, web application, mobile, wireless). Overview of the skills and knowledge required for a career in penetration testing.
* **Essential Penetration Testing Tools:**
  + Rahalkar (2019): In-depth analysis of essential penetration testing tools:
    - NMAP: Network scanning capabilities, including host discovery, port scanning, service and version detection, and operating system identification.
    - OpenVAS: Vulnerability scanning functionalities, including automated vulnerability assessments, detailed vulnerability reports, and remediation guidance.
    - Metasploit Framework: Exploitation framework for developing and executing exploits against identified vulnerabilities. Explanation of Metasploit modules, payloads, and auxiliary tools.

**III. Advanced Penetration Testing Techniques and Emerging Technologies**

* **Bypassing Machine Learning-Based Security:**
  + Chebbi (2018): Examination of the increasing use of machine learning in security systems (e.g., intrusion detection systems, antivirus software) and how penetration testers adapt their techniques to bypass these defenses. Discussion of adversarial machine learning and its implications for penetration testing. Focus on Python scripting and its role in developing custom attack tools.
* **Vulnerability Assessment and Penetration Testing (VAPT):**
  + Vegesna (2023): Detailed explanation of the VAPT lifecycle and its importance in proactive cybersecurity. Discussion of different vulnerability assessment techniques, such as static analysis, dynamic analysis, and software composition analysis. Explanation of how VAPT complements penetration testing to provide a comprehensive security assessment.

**IV. Wireless Network Security and Penetration Testing**

* **Wireless Attack Methods using Kali Linux:**
  + Asaad (2021): Comprehensive analysis of wireless network attack methods using Kali Linux. Detailed explanation of different attack vectors, such as:
    - Password cracking techniques (brute-force, dictionary attacks, offline hash cracking).
    - Wireless sniffing and monitoring.
    - Exploiting vulnerabilities in wireless protocols (e.g., WPA2).
* **Vulnerabilities of Wireless Networks:**
  + Discuss the inherent vulnerabilities of wireless networks compared to wired networks, such as signal interception and unauthorized access. Emphasize the need for strong encryption, access controls, and regular security assessments.

**V. Social Engineering as a Critical Component of Penetration Testing**

* **Methodologies and Techniques:**
  + Watson, Mason, & Ackroyd (2014): Comprehensive overview of social engineering methodologies and techniques used in penetration testing. Detailed explanation of different attack vectors, including:
    - Phishing: Deceptive emails and websites designed to steal credentials.
    - Pretexting: Creating a false scenario to gain sensitive information.
    - Baiting: Offering something enticing to lure victims.
    - Quid pro quo: Offering a service in exchange for information.
    - Tailgating: Gaining unauthorized physical access to restricted areas.
* **Effectiveness of Security Awareness Training:**
  + Junger, Montoya, & Overink (2017): Analysis of research findings regarding the effectiveness of priming and warnings in preventing social engineering attacks. Discussion of the limitations of traditional security awareness training and the need for more interactive and engaging approaches.
* **Social Engineering in a Broader Context:**
  + Erbschloe (2019): Exploration of social engineering beyond the technical realm, emphasizing its application in various societal sectors and its potential for manipulation and fraud. Discussion of the psychological aspects of social engineering and how organizations can develop a security culture to mitigate these risks.
* **Practical Applications of Social Engineering Tools:**
  + Serapiglia (2022): Focus on the use of tools like "Rubber Ducky" USB devices to simulate real-world social engineering attacks in a controlled environment. Emphasis on the ethical considerations and the importance of obtaining proper authorization before conducting social engineering tests.

**VI. Penetration Testing in Manufacturing Environments (Industrial Control Systems)**

* **Unique Challenges and Security Considerations:** Discuss the specific challenges and vulnerabilities associated with industrial control systems (ICS) in manufacturing environments. Explain the convergence of IT and OT networks and the increased attack surface it creates. Highlight the potential impact of cyberattacks on physical processes and safety.
* **Relevant Industry Standards and Best Practices:** Explore industry-specific security standards and frameworks, such as NIST SP 800-82 (Guide to Industrial Control Systems Security) and IEC 62443 (Security for industrial automation and control systems). Discuss the importance of adhering to these standards for robust ICS security.
* **Penetration Testing Methodologies for ICS:** Explain the specific methodologies and tools used for penetration testing in ICS environments. Discuss the importance of careful planning and execution to minimize disruption to critical operations. Highlight the need for specialized expertise in ICS security.

**VII. Conclusion**

* **Summary of Key Findings:** This literature review has explored the essential aspects of penetration testing, from established methodologies and tools to emerging trends like bypassing machine learning-based security and addressing the unique challenges of ICS environments. The review has highlighted the importance of a comprehensive approach to penetration testing, encompassing technical assessments, social engineering evaluations, and a focus on continuous improvement.
* **Implications for Brown & Haley:** The findings of this review directly inform the penetration testing project at Brown & Haley. By applying the methodologies and tools discussed, such as the penetration testing lifecycle outlined by Royce (2020) and the tools introduced by Rahalkar (2019), a thorough assessment of Brown & Haley's security posture can be conducted. Furthermore, the research on social engineering highlights the need to include social engineering testing as part of the overall penetration testing engagement.
* **Importance of Ongoing Security Assessments:** Penetration testing is not a one-time event but an ongoing process. Brown & Haley should implement a regular penetration testing schedule, combined with continuous monitoring, vulnerability management, and security awareness training, to maintain a strong and adaptable cybersecurity posture in the face of evolving threats.

# Annotated Bibliography

Royce, D. (2020). *The Art of Network Penetration Testing: How to Take over Any Company in the World*. Manning.

Royce guides readers through a simulated penetration test, taking on the attacker's role to expose network vulnerabilities. It covers all stages of a penetration test, from initial reconnaissance to ultimately controlling the network. Practical exercises involve password cracking, exploiting system weaknesses, and escalating privileges, culminating in a detailed engagement report.

Rahalkar, S. (2019). *Quick Start Guide to Penetration Testing : With NMAP, OpenVAS and Metasploit* (1st ed. 2019.). Apress. <https://doi.org/10.1007/978-1-4842-4270-4>

Rahalker provides a concise introduction to network penetration testing tools NMAP, OpenVAS, and Metasploit, focusing on their integration for increased effectiveness. Readers will learn to perform network scans, vulnerability assessments, and exploit vulnerabilities using these tools, starting with basic usage and progressing to more advanced techniques like scripting and Meterpreter. The book culminates in a real-world penetration testing scenario to apply learned skills.

Mandal, D. (2022). *Penetration Testing for Jobseekers.* (1st ed.). BPB Publications.

Mandal offers practical guidance on various penetration testing techniques covering web, network, mobile, and wireless security, utilizing tools like Kali Linux, Burp Suite, and Metasploit. It aims to prepare readers for a career in penetration testing by covering testing methodologies, report writing, and common interview questions. The book caters to aspiring penetration testers and security analysts, providing a roadmap for career development in cybersecurity.

Chebbi, C. (2018). *Mastering machine learning for penetration testing: develop an extensive skill set to break self-learning systems using Python* (1st edition). Packt.

Chebbi teaches penetration testers how to bypass machine learning-based security systems. It covers fundamental machine learning concepts, then delves into practical attack techniques against systems like intrusion detection and antivirus software. The book is geared towards security professionals with basic Python knowledge, aiming to equip them with the skills to identify and exploit vulnerabilities in intelligent security systems.

Watson, G., Mason, A., & Ackroyd, R. (2014). *Social engineering penetration testing: executing social engineering pen tests, assessments and defense* (1st edition). Syngress.

Watson, Mason and Ackroyd provides a practical methodology for planning and executing social engineering penetration tests, focusing on techniques like phishing, pretexting, and physical breaches. The book offers real-world examples and utilizes open-source tools to demonstrate how to conduct these tests and interpret the results. It ultimately aims to help organizations strengthen their defenses against social engineering attacks by understanding attacker tactics and implementing effective countermeasures.

Vegesna, V. V. (2023). Utilizing VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks. *International Journal of Management, Technology and Engineering*, *12*.

Vegesna argues for Vulnerability Assessment and Penetration Testing (VAPT) as a crucial cybersecurity method. It emphasizes the increasing complexity of systems and the rise in vulnerabilities exploited by attackers. The paper details the VAPT lifecycle, various testing techniques, and available tools, advocating for its proactive use to prevent cyberattacks and enhance system security.

Asaad, R. R. (2021). Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, *10*(1), 7-12.

Asaad explores wireless network attack methods using Kali Linux. It focuses on password cracking techniques, including brute-force (dictionary) attacks and offline attacks utilizing hash algorithms like MD5 and SHA-512. The paper also discusses the increasing prevalence of wireless networks and their inherent security vulnerabilities compared to wired connections, emphasizing the need for stronger security measures. Finally, it covers tools and methods available within Kali Linux for exploiting these vulnerabilities.

Serapiglia, A. (2022). Rubber Duckies in the Wild: Proof of Concept Lab for USB Pen Testing Tool. *CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL*.

Serapiglia in this teaching case outlines how to incorporate building a "Rubber Ducky" USB penetration testing tool into a cybersecurity course. Rubber Duckies, disguised as ordinary flash drives, inject keystrokes into computers to create remote access shells for penetration testers. The case emphasizes the importance of ethical hacking and controlled testing environments, providing step-by-step instructions for creating and deploying these tools for educational purposes.

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. doi:10.1016/j.chb.2016.09.012

Junger, Moontoya, and Overink investigated whether priming or warnings could prevent social engineering attacks. Researchers surveyed shoppers in the Netherlands, asking for personal information like email addresses and bank details. The results showed high disclosure rates, with neither priming questions about cybercrime nor explicit warnings significantly reducing the sharing of information, even suggesting a potential adverse effect from warnings in some cases.

Erbschloe, M. (2019). Educating People to Prevent Social Engineering Attacks. In *Social Engineering : Hacking Systems, Nations, and Societies.* (pp. 179–209). CRC Press LLC,. <https://doi.org/10.1201/9780429322143-8>

Erbschole examines social engineering as a hacking tool, exploring its use against both random and targeted systems across various societal sectors. It emphasizes that social engineering extends beyond computer hacking and demonstrates how organizations and individuals can proactively shape their culture to mitigate manipulation and fraud. Readers will learn to analyze organizational security needs and develop countermeasures against social engineering threats.

# 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.

# Solutions Analysis

**Proposed Solution**

Conduct a comprehensive penetration test of Brown & Haley's IT infrastructure, encompassing both the factory and office environments. This will involve a combination of automated vulnerability scanning and manual penetration testing techniques to simulate real-world cyberattacks. The proposed project will be executed in four phases: Planning and Scoping (defining the scope and establishing Rules of Engagement), Vulnerability Discovery (conducting the penetration test using various techniques), Vulnerability Analysis and Reporting (analyzing and prioritizing vulnerabilities, providing remediation recommendations), and Remediation and Post-Assessment (supporting remediation efforts and verifying their effectiveness through a post-assessment test).

**Organizational Problems and Stakeholder Concerns**

This solution directly addresses the identified weakness of outdated cybersecurity practices. It provides a detailed assessment of vulnerabilities, enabling the company to proactively address security gaps and reduce the risk of cyberattacks. This aligns with Dan Fabian’s concerns and management's willingness to invest in security improvements. Upper management is worried that industrial sabotage could cause order delays and cost the company thousands of dollars per hour. Other stakeholders are concerned with potential costs of securing industrial equipment.

**Connection to IT Trends**

Penetration testing is a widely recognized and recommended security practice aligned with industry best practices and frameworks like NIST Cybersecurity Framework and ISO 27001(NIST, 2024: ISO, 2022). The increasing prevalence of cyberattacks, particularly targeting manufacturing and supply chains, makes this solution highly relevant in the current global IT landscape.

**Industry Alignment**

This project keeps Brown & Haley in line with industry standards by proactively addressing cybersecurity risks, which is crucial for maintaining competitiveness and customer trust in today's business environment.

# Proposed Model/Architecture

1. **Planning and Scoping:** Define the scope of the test, including target systems and testing methodologies.
2. **Vulnerability Scanning:** Automated tools will scan for known vulnerabilities in systems and applications.
3. **Penetration Testing:** Manual techniques will attempt to exploit identified vulnerabilities to simulate real-world attacks.
4. **Reporting and Remediation:** A detailed report will be generated, outlining identified vulnerabilities and recommendations for remediation.

# Recommended Technology

Tools like Nessus, Nmap, and Metasploit will be utilized for vulnerability scanning and penetration testing. NMAP is an industry standard software for scanning networks for open ports and generates details about possible OS versions and other details about possible services running on each port (NMAP, 2024). Metasploit is versatile, terminal based software that is useful for finding vulnerabilities and exploiting them via scripts (Rapid7, 2024). Nessus is an industry leading vulnerability scanner implementing multiple tools all in one (Tenable, 2024).

# Supporting IT Principles

The solution is grounded in principles of confidentiality, integrity, and availability (CIA triad), which are fundamental to information security (NIST, 2020). It also adheres to the principle of least privilege, ensuring that access to systems and data is restricted to authorized personnel only.

# Key Legal, Ethical, and Policy Issues

Obtaining written authorization for the penetration test is crucial. All testing activities must be conducted ethically and within legal boundaries. The findings of the penetration test must be handled confidentially and shared only with authorized personnel. Potential risks include accidental disruption of services during testing and the possibility of undiscovered vulnerabilities. These can be minimized by careful planning, thorough testing in a controlled environment, and close communication with the IT team.

# Needs and Risk Analysis

**Meeting Organizational and Stakeholder Needs**

This solution directly addresses Brown & Haley's need for improved cybersecurity by providing a comprehensive assessment of its IT infrastructure's vulnerabilities. It empowers the organization to make informed decisions about security investments and prioritize remediation efforts. This aligns with Dan Fabian’s goal of strengthening the company's security posture and fulfills management's commitment to protecting company assets and reputation.

# Risk Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Likelihood | Impact | Mitigation Strategy |
| Service Disruption | Low | Medium | Conduct testing during off-peak hours, have rollback plans |
| Undiscovered Vulnerabilities | Medium | High | Utilize multiple testing tools and techniques, retest after remediation |
| Data Breach during Testing | Low | High | Strict data handling procedures, anonymize sensitive data |
| False Positives | Medium | Low | Thoroughly validate findings before reporting |
| Legal/Ethical Issues | Low | High | Obtain written authorization, adhere to ethical guidelines |

# Barriers and Adjustments

A potential barrier is limited budget or time allocated for the project. To address this, the scope of the penetration test can be adjusted to focus on the most critical systems and applications. Another barrier could be resistance from IT staff concerned about potential disruptions. This can be mitigated through clear communication, collaboration, and demonstrating the value of the testing.

# Insights and Advice

For someone working in this area for the first time, it's crucial to thoroughly research and understand the organization's IT infrastructure, business processes, and regulatory requirements. Start with a comprehensive risk assessment to identify potential threats and vulnerabilities. Collaborate closely with stakeholders to understand their concerns and ensure the project meets their needs. Document all testing activities meticulously and communicate findings clearly and concisely.

# Legal, Ethical, and Policy Analysis

**Legal Issues**

 The primary legal consideration is obtaining written authorization from Brown & Haley to conduct the penetration test. This protects both the organization and the penetration tester from any legal repercussions. Compliance with data privacy regulations, such as GDPR or CCPA, if applicable, is also essential (GDPR, 2016: Bukaty, 2019). These regulations would apply to customers in the EU and California, respectively.

**Ethical Implications**

Ethical considerations include respecting the confidentiality of sensitive data discovered during the test and refraining from exploiting vulnerabilities beyond the agreed-upon scope. Transparency and open communication with Brown & Haley throughout the process are crucial for maintaining trust.

**Policies**

Brown & Haley's internal IT policies regarding security testing and data handling must be reviewed and adhered to. Any potential conflicts between the proposed project and existing policies must be addressed and resolved before commencing the penetration test. For example, if there's a policy prohibiting external access to internal systems, an exception must be granted for the penetration test to proceed legally and ethically. The results of the penetration test should be used to improve existing policies and develop new ones where necessary.

**Rules of Engagement**

Lack of clear Rules of Engagement (ROEs) could lead to legal issues, reputational damage, or unintentional access to sensitive data. Develop and agree upon comprehensive ROEs before commencing the test, outlining the scope, permissible testing activities, and data handling procedures. Ensure the ROEs are reviewed and approved by legal counsel.

**Liability and Insurance**

The penetration testing team could face legal liability for unintended damage or data breaches if they do not have adequate liability insurance. Ensure the penetration testing team has appropriate professional liability insurance and that the contract clearly defines responsibilities and liabilities for both parties.

# Reflection

My initial project idea focused broadly on "improving cybersecurity" at Brown & Haley. However, through research and discussions with my site supervisor, Dan Fabian, the project evolved significantly into a focused penetration testing project. This shift represents the biggest change from my initial concept to the final proposal.

Several key pieces of information drove this change. Firstly, Dan's insights into the company's existing IT infrastructure and security practices revealed a lack of recent updates to main office computers. He expressed specific concerns about potential vulnerabilities in Windows 10 and its lack of future security updates soon. Secondly, my research on cybersecurity best practices highlighted the importance of penetration testing as a crucial tool for identifying and mitigating security risks. Finally, learning about the increasing cyber threats targeting the manufacturing and food industries emphasized the urgency of this project.

Creating the final project proposal taught me several valuable lessons. First, the importance of clearly defining the project scope. Initially, I envisioned a broader project encompassing various cybersecurity improvements. However, I learned that a more focused approach allows for more manageable objectives and deliverables. Second, I learned the value of stakeholder engagement. Regular communication with Dan was crucial for refining the project scope, ensuring its alignment with Brown & Haley's needs, and gaining his support. Third, I gained practical experience in developing a project charter, defining milestones, and creating a realistic timeline.

The most important takeaway from this integrated action learning project is the iterative nature of project development. My initial ideas evolved significantly based on new information and stakeholder feedback. This reinforces the importance of flexibility and adaptability in project management, a principle I will undoubtedly apply to future projects in my field.

I hope to leverage the knowledge and skills developed in this class and my BS IT program to pursue a career in cybersecurity. Specifically, I am interested in specializing in penetration testing and vulnerability management. This project has provided a solid foundation for pursuing this career path, giving me practical experience and a deeper understanding of the challenges and opportunities in this field.

My advice to someone starting this course or the BS IT program is to embrace the hands-on learning opportunities in the labs. Also, be prepared to adapt and refine your project ideas based on new information and stakeholder input. The learning process is iterative, and the ability to adapt is essential for success in the IT field. Finally, don’t underestimate the value of networking and building relationships with professionals in your field. These connections can provide valuable insights, mentorship, and career opportunities.

# References

Bukaty, P. (2019). *The California Consumer Privacy Act (CCPA): An implementation guide*. IT Governance Publishing. <https://doi.org/10.2307/j.ctvjghvnn>

Covell, J. (2024). Brown & Haley. In *International Directory of Company Histories*. <https://www.encyclopedia.com/books/politics-and-business-magazines/brown-haley>

European Parliament, & Council of the European Union. GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved 13 April 2023, from <https://data.europa.eu/eli/reg/2016/679/oj>

*Detecting and Responding to Ransomware and Other Destructive Events.* <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>

Hooker, C., & Leask, J. (2020). *Risk Communication Should be Explicit About Values. A Perspective on Early Communication During COVID-19*. *Journal of bioethical inquiry*, *17*(4), 581–589. <https://doi.org/10.1007/s11673-020-10057-0>

ISO. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022).* <https://www.iso.org/standard/27001>

NIST. (2020). *NIST SPECIAL PUBLICATION 1800-26A****:*** *Data Integrity:*

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

NMAP. (2024). Nmap: Discover your network. <https://nmap.org>

Rapid7. (2024). *Metasploit Documentation*. <https://docs.metasploit.com>

Tenable. (2024). *Tenable Nessus®.* <https://www.tenable.com/products/nessus>

Kaplan, R. S., & Mikes, A. (2024). *Managing risks: A new framework*. Harvard Business Review. https://hbr.org/2012/06/managing-risks-a-new-framework

Locke, E. A., & Latham, G. P. (2002). *Building a practically useful theory of goal setting and task motivation*. American Psychologist, *57*(9), 705.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of management review*, *22*(4), 853-886.

Pinto, J. K., & Slevin, D. P. (1988). Project success: Definitions and measurement techniques. *Project Management Journal*, *19*(1), 67-72.

Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK guide)* (7th ed.).