Christopher Uweh

Professor DeAndre Favors

ACCCSMay22-289

31 October 2022

<div align="center">Summative Research Project: Penetration Test Proposal</div>

<u>Executive Summary:</u>

Enterprises and consumers increasingly rely on computing networks because all users expect to exchange information at the speed of thought. With the evolution of technology, there has been a greater focus on ease of use. Routine tasks rely on computers for accessing, providing, or just storing information. Vigilant compliance may seem burdensome; however, the potential fines and reputational damage caused by insufficient security can be fatal. There is a sense of urgency on behalf of organizations such as Green Clothing Company (GCC) to secure these assets from likely threats and vulnerabilities. GCC provided information about its current organizational setup, which is a perfect starting point.

Hackers break into systems for various reasons. Understanding how and why malicious hackers attack and exploit systems is essential. Security professionals must guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seek(s) to use the same infrastructure for illegal activities (Ethical Hacking Essentials). This assessment responsibly mimics real-world attack scenarios using gray box testing to provide GCC with data-driven insights.

<u>Information Gathering And Client Expectations:</u>

Popular depictions of hacking provide a false image of the true nature of the Enterprise Information Theft paradigm: Typically, a man in a hoodie furiously types code on a laptop,