**Career Paper**

**Easton Jarboe**

**ODU**

**CYSE 201s**

**Professor Yalpi**

**4/24/24**

When thinking about jobs and how they relate to social sciences one cyber security job stood out the most. Penetration testing relates to how vulnerable a company is and the penetration testers usually use social science to manipulate a way into the company and find vulnerabilities. It relates to social science on quite a few principles. One of the biggest ones is behavioral analysis (M. Bishop, 2024). Social engineering techniques use psychological principles to assess human behavior and how they can be exploited. They also follow certain ethical hacking frameworks (Hatfield, 2019). They always use legal and ethical considerations informed by social science to see if what they are doing is morally ok. One of the most interesting points that can be used in penetration testing is cultural and socio economic factors. They can be used to either make the job easier or harder depending on things like cultural norms or language barriers. These factors can also influence the way a penetration tester approaches their job. They may need to adjust their approach or their testing criteria,to fit the situation. There are factors that can be used to help a penetration tester identify potential security risks that might not be immediately obvious and they can do it in many different ways. A penetration tester should also take into account what vulnerabilities theft are targeting of the system they are testing. Like when a penetration tester may need to use different testing techniques when testing a banking system or an ecommerce website (H. M. Z. A. Shebli and B. D. Beheshti). These relate to social science because a new approach is needed every time. Analyzing social factors can provide additional information that can help a penetration tester better understand a system's security posture. Additionally, a penetration tester should consider the psychological aspects of human behavior when testing a system. For example a penetration tester should consider how a user might respond to certain types of attacks. This can sometimes cause disparity in the way of how ethical a penetration tester is acting. A penetration tester should also take into account how

a user might respond to certain types of attacks. A penetration tester might choose to avoid attacking a user who is elderly or disabled. There is a certain moral code to this kind of exploitation. If the person is elderly it may be easier to get information out of them, but at the same time it is more difficult because the results of the penetration test could get the person fired and if they are elderly it would mean they probably won't get another job and in the economy today that could lead to serious implications. Overall, a penetration tester should be aware of the potential consequences of their actions and think twice before testing certain individuals. It is ultimately up to the individual to decide, but it is important to consider the ethical implications of their actions. Social science plays a key role in how all fields work but especially cyber security. It is important to understand the implications of the person's work and how they go about doing it. It is always important to consider others when a job is taken.

References

M. Bishop, "About Penetration Testing," in *IEEE Security & Privacy*, vol. 5, no. 6, pp. 84-87, Nov.-Dec. 2007, doi: 10.1109/MSP.2007.159. keywords: {System testing;Permission;Information security;Computer crime;Vehicles;Degradation;Protection;Privacy;education;penetration testing;hacking;ethical hacking;red teams},

H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018, pp. 1-7, doi: 10.1109/LISAT.2018.8378035. keywords: {Penetration testing;Organizations;Tools;Standards organizations;Testing;Software;IT security;penetration test;IT governance;vulnerability assessment;ethics for professional hacking},

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security*, *83*, 354–366. https://doi.org/10.1016/j.cose.2019.02.012