For my paper I will be looking at how penetration testers use social science in their jobs. There are multiple types of penetration testing like network, cloud, and social engineering testing. Each of these methods use some concepts of social sciences. This is shown in how they can go about their testing. First, they have time to prepare for what they need to do. Secondly, they perform reconnaissance which could be scanning for obvious holes in their network security or asking questions of the employees to gather data. Next, they initiate the attack using the information they gather. Lastly, they give a analyze the problems and give a report to the hirers (Penetration testing. (n.d.)).

Network penetrations testers jobs are to "[simulate] the processes hackers would use to attack your business network, network applications, business website, and attached devices" (Sca. (2020, November 09)). This also creates a scenario that "show organizations how effectively their current security defenses [and staff] would act when facing full-scale cyberattacks" (Sca. (2020, November 09)). To do their jobs well they need to get in the mindset of someone who is actually attacking their systems. One way they can more easily do this is by becoming a part of the hacker community/subculture and talking with them and picking up tricks and methods. Another way of analyzing how hackers do things are to directly observe how they do it by setting a honeypot trap to observe them.

Cloud penetration testers make sure that the companies are safe regarding their use of cloud technology. Although, cloud penetration testing is very similar to network penetration testing there are a few differences. It is harder to do because the computer they are attacking they might have zero information on except for the connection the company uses.

Social engineering penetration testers use many different forms of social sciences to complete their job well. They use their ability to use people or persuade them. One of the ways a social engineering penetration tester might try to get to the target system is by tailgating someone into restricted areas like the server room or another room with access. They also might use peoples naiveness and leave a flash drive laying around that an employee might pick up and plug into the system, without thinking of the potential consequences, to check the contents of the flash drive. These penetrations testers also frequently use phishing or vishing to see if “an employee unwittingly gives away key information” (Penetration testers. (2021, March 16)). To do this phishing they may try to gain their trust or impersonate a higher-up or a co-worker to make the employee willingly give them information, like passwords or valuable information on the system. They might also send normal phishing emails to the employee’s personal emails, because even though people are not supposed to do it many do. Both methods might allow the tester to gain access to the system or to the account of the employee that was phished, which could be counted as a success depending on the goal.

Penetration testing. (n.d.). Retrieved December 01, 2021, from https://www.coresecurity.com/penetration-testing

Penetration testers. (2021, March 16). Retrieved December 01, 2021, from https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/

Sca. (2020, November 09). Network penetration testing and how does it detect security threats? Retrieved December 01, 2021, from https://www.scasecurity.com/network-penetration-testing/

Cloud Penetration Testing. (n.d.). Retrieved December 01, 2021, from https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/

Notes and PowerPoints from class