Owen Stewart

Professor Yalpi

CYSE 201S

November 24, 2024

Social Sciences in Penetration Testing

Social science is the scientific study of how people interact with each other in society. Many people in the cybersecurity fields depend on principles from social science to do their jobs properly. One of the careers that rely on these principles is penetration testing. Penetration testing is a practice that simulates attacks on computers and computers networks to identify vulnerabilities within these systems. Penetration testers are usually hired by companies to test their systems and then give a report on their findings.

One of the most important principles that penetration testers depend on is skepticism. When a company says that their network may be secure, it is a penetration testers job to see if this is actually true by attacking their network in the same way a real criminal would. This skepticism is what allows penetration testers to fully test a company's claims so that they can discover as many vulnerabilities as possible. If penetration testers weren't skeptical of a company's claims, they would most likely not find many hidden vulnerabilities in their systems.

Another principle that penetration testers depend on is research. Penetration testing itself can is a type of research. Penetration testing could be considered a field study, since testers make reports of what they find while they are "in the field". Penetration testers also rely on another type of research, archival research. They use archival research to learn about the systems and

software that companies use, to see if there are any vulnerabilities in the versions of these software of systems that the companies use. Without archival research, penetration testers would have to play a guessing game to figure out what versions of software a company is using and how they could exploit them.

Penetration testing could also be considered an experiment. Since the testers are usually given a minimal amount of information before testing a network, they have to experiment to make maps of the network, figure out what systems are being used, and how they can exploit them. While conducting these experiments, testers have to be careful to not do any real harm that could negatively affect the business. This could cost them their job or even more if the company decides to take legal action.

One more principle that penetration testers rely on is parsimony. Parsimony is a principle that says that explanations should be kept simple. Penetration testers need to write reports that are simple enough for the company to understand, but not so complex that they won't be able to figure out what is or is not wrong with their network.

In the field of penetration testing there is not much diversity. There is almost no representation of women, or people of color. However, this also applies to many more field in cybersecurity, and not just penetration testing.

In conclusion, penetration testers rely on multiple principles of social science to do their jobs. They rely on skepticism and parsimony to do their job and write reports. They also rely on different types of research. These types of research are archival, field studies, and experiments.