There are many nuances to the ethical problems that are present when penetration testing and many of the have been addressed by certain frameworks and strategies, but these differ from organization to organization. A brief description of penetration testing is the ethical and authorized hacking of a system or network to gauge its security. Since the practice is inherently linked with hacking, ethical issues are abundant.

In a book written by Nathan Clarke, Shamal Faily, a researcher in one of the studies, describes a penetration testers role in depth as “attacking systems to evaluate their security in the face of realistic threats. These attacks take the form of authorized penetration tests that probe a system's defenses; these defenses are then breached to evaluate the impact of any weaknesses; the results of these tests are used to improve a system's security, making them resilient to further attacks (Clarke, 2015).” This is a very common and almost essential practice to ensure that the security of a system is at its best, which is why penetration testing is used all over the world.

“While conducting penetration tests, often called pentests, professionals face many ethical dilemmas. Pentesters face ethical challenges throughout the penetration testing process, from agreeing to the rules of the test and deciding which tools, tactics, and procedures to use all the way through writing the penetration test report (Faily, McAlaney, & Iacob, 2015). Some of the ethical dilemmas confronted at the beginning of the penetration testing cycle are deciding on the rules of engagement for the test. For example, there are many ethical questions that must be answered, such as will social engineering techniques be used to dupe employees and will policy adherence tests that could de-anonymize offending employees be conducted. Ethical issues also arise when conducting the actual penetration test. When penetration testing, evaluating a security feature of a computer system may result in the disclosure of personal or confidential information to the pentester and organization management (Faily, McAlaney, & Iacob, 2015). For example,

when testing the security of an organization's upper-level management, a pentester may find information or files that conflict with the information sharing policy of the organization. Therefore, the pentester faces the moral dilemma of disclosing this information to the organization and possibly causing the manager to face disciplinary actions or just report on the security flaw that allowed access to the computer (Faily, McAlaney, & Iacob, 2015). To strengthen the ethics of pentesters, many industry organizations have developed ethical codes of conduct such as Systems Security Certification Consortium's ethics guidelines and The Information Systems Audit and Control Association's ethical rulebook (Faily, McAlaney, & Iacob, 2015). Clearly, ethical hackers are confronted with many ethical dilemmas when performing penetration tests (Corley, n.d.)."

The benefits and costs of using penetration testing are numerous. Daniel Brecht defines the pros as "helping with data leaks, showing the vulnerabilities of hardware, practices and software that need strengthening, and being the closest security test to a real-world attack (Brecht, 2016)". Brecht also defines the cons as "It being highly unlikely that a pen-tester will find all the security issues or will solve all problems when scanning for vulnerabilities, It takes a pen-tester more time to inspect a given system to identify attack vectors than doing a vulnerability assessment, It is high-labor intensive and can therefore represent an increased cost and some organizations might not be able to allocate a budget to do this, and It might give a false sense of security because being able to withstand most penetration testing attacks might give the sense that systems are 100% safe, but because penetration testing is planned and real attacks occur at random this is not necessarily true (Brecht, 2016)". Questions about the trust put into these penetration testers are raised because they are not government sanctioned employees in most cases. If done incorrectly, private data can be breached, which is an offense

punishable by law due to the right of privacy being violated. This would include but not limited to financial, social security, hospital records, etc.

In conclusion, being a penetration tester comes with its fair share of ethical problems, such as being required to test for breaks in security ethically when the hackers will not do the same, the legal classification of the data that is being tested, the geographical location of where the testing is transpiring, and many others. With these factors in mind, companies and organizations do their best to use frameworks and guidelines to define how penetration testing should be done for their specific data and location to avoid legal action or financial lose. The ethics of practicing penetration testing in murky at best.

Work Cited

Brecht, D. (2016, November 30). Pros and Cons in Penetration Testing Services: The Debate Continues. Infosec Resources. https://resources.infosecinstitute.com/topic/pros-and-cons-in-penetration-testing-services-the-debate-continues/

Clarke, N., & Furnell, S. (2015). Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015). In Google Books. Lulu.com. https://books.google.com/books?hl=en&lr=&id=NQJqCwAAQBAJ&oi=fnd&pg=PA233&dq=ethical+penetration+testing&ots=bpIQuMD3oO&sig=8d4amWKglJd7dDgaIlov_CGbRYg#v=onepage&q=ethical%20penetration%20testing&f=false

Corley, J. (n.d.). CTF Academy : Cybersecurity Ethics. Ctfacademy.github.io. https://ctfacademy.github.io/other/ethics.htm