Anthony Shawn Bandy
Engineering 350
Monday 2:00PM
Writing Assignment 3
02/24/2013

Ethical Hacking

Ethical hacking is typically defined as penetrating one's own computer systems to discover vulnerabilities. In the process of doing so, an ethical hacker employs many of the same techniques and software tools that a criminal hacker would use. Businesses and organizations employ ethical hackers as a means of buttressing enterprise networks and computer systems, particularly as the growth of commerce over the Internet has become a standard business practice.[1]

Ethical, or white-hat, hacking began in the 1970s when the United States Air Force evaluated the Multics operating system's security features. The security team performed their evaluation using real-world techniques in order to simulate realistic security conditions in the field. These techniques festered in the dark corners of government organizations, universities and businesses until, in 1992, two researchers, Farmer and Venema formalized the ideas that would become the backbone of ethical hacking in a public Usenet post. Because they realized the time required to learn and use their techniques would be beyond most system administrators they packaged a set of tools together and called it the *Systems Administrator's Tools for Analyzing Networks.* Perhaps more important than their technical contribution, was simply that the brought into public discussion a topic that was as important as it was taboo.

[1] This paper primarily relies on "Ethical hacking" by C.C. Palmer downloaded from http://pdf.textfiles.com/security/palmer.pdf on 21 Feb. 2013.

According to IBM, an ethical hacker tries to determine what an attacker can access on the target system, what can be done with that access, and whether that access would be noticed by the security regime in place. At the heart of those three questions are the specific assets at risk so it is also important that the hacker's client is able to assign a value to those assets. Before the work begins, it is critical that the ethical hacker work closely with the client to document in writing the number and nature of the tests that are to be conducted and the specific systems that are to be tested as the activities would often be illegal in most jurisdictions.

There is some debate about the legitimacy of the phrase "ethical hacker."[2] Olson uses a different definition for hacker than Palmer:

> *The term "hacker" has two connotations: someone that has been convicted of a computer related criminal activity, or someone who thinks a certain way about technology.*[3]

According to Olson, from this definition either a hacker is a criminal – or one who engages in criminal activities – or someone who is interested in the inner workings of computer systems. In either case, she argues, the term "ethical" is either a contradiction or has little meaning. As an analogy she suggests that we do not hire "ethical locksmiths" but simply locksmiths.[4] Ultimately Olson's point is that we should not use "ethical" to legitimize an illegitimate practice but should instead choose another word or phrase.

---

[2] Olson, Parmy. "Exploding the Myth of the Ethical Hacker." Forbes.com, 31 Jul. 2012. Web. 22 Feb 2013. http://www.forbes.com/sites/parmyolson/2012/07/31/exploding-the-myth-of-the-ethical-hacker/

[3] Ibid.

[4] Although I agree with most of what Olson writes, I think she is off the mark here as locksmiths must be certified in most legal jurisdictions and have strict codes of conduct to which they must adhere.