"Argue for or against the use of hacking as a means of identifying weaknesses in computer security."

January 8, 2014

There is much ambiguity and controversy surrounding the terms *'hacker'* and *'hacking'*. Traditionally, a hacker can be defined as "A person who enjoys exploring the details of programmable systems and stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary" [8, pg. 339-340]. This was intended as a complementary term for gifted computer programmers. However the term has since come to describe those who break into computer systems for malicious purposes. Advocates of the former definition insist that the term 'cracker' be used to describe such an individual [8, pg. 400][10, pg. 1][6, pg. 1-2]. However in this essay I use the term 'hacker', and its verbal extension 'hacking', with the latter definition in mind. This essay discusses the merits and issues of using hacking as a means of identifying weaknesses in computer security.

The terms 'Ethical Hacking' or 'White Hat Hacking' are used to describe hacking for positive purposes. Ethical hackers attempt to find weaknesses in a client's system, with the client's full consent and within the bounds of the law, in order to expose any holes in security found to the client so they may take steps to fix them[7, pg. 1]. Notably, they do this by utilising the same techniques that would be used by malicious hackers (referred to as 'Black Hat' hackers[7, pg. 1-2]). As much as they can, they will attempt to break the system in question over a period of days, weeks or longer. However, where a Black Hat would take advantage of a security flaw and cause damage, the ethical hacker can provide the client with insight on how to fix it. This process is commonly called penetration testing.

It must be stressed that the main advantage of this approach is that an ethical hacker thinks and acts as a black hat hacker. Palmer, to whom the term 'ethical hacker' is often attributed, summarises this stance nicely: "Just as in sports or warfare, knowledge of the skills and techniques of your opponent is vital to your success" [6]. Though there may be other useful techniques to test system security, what penetration testing can provide is the most real world test. It can be likened to crash testing a car. It is difficult to find many examples of the successful use of ethical hacking in companies since, as we will see, there are many reasons not to make this information publicly available. However an early example is the US Air Force's security evaluation of the MULTICS operating

system[3].

However, there are some criticisms of ethical hacking as a practice. These can be summarised under three headings: education, hacker corruption and the intrinsic risks of performing an ethical hack. I will outline and address each of these in turn.

With penetration testing increasing in popularity, many universities are now offering courses in ethical hacking. Naturally there are some concerns over this; an ethical hacker must know the skills of a black hat hacker, so it follows that an effective course on ethical hacking is equally an effective education in malicious hacking. The main concern then is that students will use the skills they acquire from such a course to engage in black hat activities. This is a valid concern indeed, however there are convincing counter-arguments. Firstly, it can be argued that many computer scientists already possess the skills of a hacker[7, pg. 3] or could learn these skills from existing resources [1, pg. 2]. However providing a formal education on the subject opens an important opportunity: students can be educated in the legal and ethical implications of their actions [7, pg. 3]. Furthermore, it is possible to conduct criminal background checks on students with the hope of quickly weeding out those who are harbouring malicious intentions [4, pg. 2].

Assuming we already have a fully trained and vetted ethical hacker, the next issue we must consider is corruption. That is, that a hacker may abuse their position by, for example, exposing security weaknesses to criminal groups or black hat groups for financial gain or as the result of being coerced. Obviously this is a very hard, perhaps even impossible, risk to eliminate completely. After all regardless of any countermeasure taken to ensure the hacker is trustworthy, there is always a chance that they may turn corrupt. Despite this, I feel the risk is still worth taking. We take similar risks in many other fields: for example when training a police officer, it could be argued that they could use their understanding of the legal process to engage in criminal activities and cover their tracks. But we still recognise that there is a need for police and so deem this an acceptable risk. Likewise, we must do the same with ethical hacking.

The previous two points are related in that they question whether the motives of an ethical hacker will always remain pure. Though we can never guarentee this, there are countermeasures available to minimise the risk of such occurences. We have already mentioned criminal background checks. A further step is security vetting, which involves a full assessment of the individuals background and character to assess whether they are 'trustworthy' [9].

The final issue to be addressed is the risk associated with performing penetration testing, assuming that the hacker(s) are trustworthy and are not intentionally causing problems. Palmer outlines many of these potential issues, including unintentional system crashes, denial of service, degraded network performance, etc [6]. Basically, anything that could be the result of a real threat may become manifest during an penetration test. Naturally this can be rather serious; though the ethical hacker is not out to cause damage, disruption of service to company networks or websites may cause a severe loss of revenue if

allowed to continue. Whilst this is a concern, it must be emphasised that the entire point of performing such security tests is to prevent such attacks in the future by parties who do intend to cause damage. The company can choose when these tests are performed and can of course limit the scope of the testing as required to avoid major disruption [6, pg. 9].

A second branch of risk stems from malicious hackers gaining access to the data used or produced by the ethical hacker. For example, if a corrupt employee were to gain access to the ethical hackers report on the system's security weaknesses, they would be in a position to exploit them. Even worse, their actions may be masked by the penetration testing being conducted. Though again this is naturally a cause for concern, countermeasures can be taken, including conducting the ethical hack from a highly secured location, changing the origin of the security test often, etc [6, pg. 9].

Finally, it is worth discussing a third form of hacking dubbed 'Grey Hat'. As the name suggests, this falls somewhere between white and black hat activities. Exactly what constitutes grey hat hacking is somewhat vague; the term is largely a catch-all for the grey area between white and black hat. However one possible explanation is engaging in black hat activities with the intention of exposing security flaws to the system owner. While this sounds identical to white hat hacking, grey hat hacking is not necessarily conducted in a controlled environment or with the system owner's consent. As such, all of the aforementioned risk is present with none of the preventative countermeasures in place. Despite good intentions, this form of hacking can be seriously harmful.

I believe it is pivotal that a hacker have the system owner's consent. Not only can hacking without consent be considered a legal offence under the Computer Misuse Act 1990, but it does not give the system owner any opportunity to address the risks of penetration testing. A valid compromise can be found in the 'Bug Bounties' scheme deployed by Microsoft [5] and Facebook [2]. This gives hackers a chance to be rewarded for their efforts whilst defining acceptable guidelines intended to protect all parties.

To summarise, there are a number of potential risks in using ethical hacking, the primary being that it is impossible to assert that the hacker in question will never use the skills and information they have obtained to cause the very problems they are employed to prevent. However as mentioned, this is pervasive of human culture in general; whenever someone is taught potentially dangerous skills, there is always the possibility they will use them for evil rather than good. Despite this, ethical hacking offers the ability to test systems in the realest way possible: by exposing them to the attacks that a malicious hacker would attempt. I believe that the benefits of this outweigh the inevitable risks. The key is that hacking be conducted with the appropriate cautions outlined in this essay and with the full consent of the system owner.

References

[1] Patricia Y. Logan & Allen Clarkson. Teaching Students to Hack: Curriculum Issues in Information Security. *SIGCSE*, 2005.

[2] Facebook. Facebook Bug Bounty. https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766. Accessed 16/11/2013.

[3] P.A. Karger and R.R. Schell. Multics security evaluation:vulnerability analysis. *ESD-TR-74-193*, 2:1974, June.

[4] Danish Jamil & Muhammad Numan Ali Khan. Is Ethical Hacking Ethical? *International Journal of Engineering Science and Technology (IJEST)*, 40(3):769–780, April 2001.

[5] Microsoft. Microsoft Bug Bounty. http://technet.microsoft.com/en-us/security/dn425036. Accessed 16/11/2013.

[6] C.C. Palmer. Ethical Hacking. *IBM Systems Journal*, 3(5):3758–3763, May 2011.

[7] Brian A. Pashel. Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level. In *Proceedings of the 3rd annual conference on information security curriculum development*, pages 197–200. InfoSecSD, September 2006.

[8] Eric S. Raymond. The New Hacker's Dictionary v.4.3.3 (Jargon File). http://www.proselex.net/documents/the%20new%20hacker%27s%20dictionary.pdf, 2002. This is the jargon file provided free as a supplement to the full book 'The New Hacker's Dictionary'. This file should be used when looking up references, not the book.

[9] SJC. Security Vetting Overview. http://www.securityvetting.org.uk/. Accessed: 16/11/2013.

[10] Nataliya B. Sukhai. Hacking And Cybercrime. In *InfoSecCD Conference'04*. InfoSecSD, October 2004.