Ethical Dilemmas and Dimensions in Penetration Testing

Shamal Faily[1], John McAlaney[1] and Claudia Iacob[2]

[1]Bournemouth University, UK
[2]University of East London, UK
e-mail: {sfaily,jmcalaney}@bournemouth.ac.uk; c.iacob@uel.ac.uk

Abstract

Penetration testers are required to attack systems to evaluate their security, but without engaging in unethical behaviour while doing so. Despite work on hacker values and studies into security practice, there is little literature devoted to the ethical pressures associated with penetration testing. This paper presents several ethical dilemmas and dimensions associated with penetration testing; these shed light on the ethical positions taken by penetration testers, and help identify potential fallacies and biases associated with each position.

Keywords

Penetration Testing, Ethics, Dilemmas, Fallacies, Biases

1. Introduction

Penetration testers attack systems to evaluate their security in the face of realistic threats. These attacks take the form of authorised *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.

Hacking a system requires technical prowess, creativity, and ingenuity to find unexpected ways of appropriating it (Geer and Harthorne, 2002). Penetration testing requires all of this, with the added constraint that finding and exploiting vulnerabilities should neither harm the system nor encroach on the dignity of those affected by it. Unfortunately, commercial pressures mean that penetration testers face pressure to discover insecurity without themselves engaging in unethical behaviour before, during, and after a penetration test. For example, consider the following scenario: *An investment bank is considering whether to enter a long-term contract for information assurance services with a security consultancy. As a pilot project, the bank commissions the firm to evaluate whether a policy forbidding the plugging in of unauthorised USB devices into workstations is being adhered to. The IT staff at the bank want the firm to adapt a known piece of banking malware that, when installed on a USB stick which is plugged into one of the bank's workstations, will email a selection of spreadsheet files on a shared working directory to an email*

account owned by the firm. This simple test will help the bank evaluate who in the company is violating the policy.

Such a test may be legal if the exfiltrated data was not personal, but this legality may be questionable depending on the legal jurisdiction where the test takes place. There are also question marks about the morality associated with employing malware, and engaging with markets where the malware is acquired might also have ethical implications based on the nature of the exploit or the system under evaluation (Egelman et al., 2013). Finally, is the use of deception and de-anonymisation of employees acceptable, particularly where a policy is intentionally violated to achieve critical productivity goals (Adams and Sasse, 1999)?

Previous work (Chiesa et al., 2009; Holt, 2010) has started to glean an understanding of hacker values, but has focused on hackers trying to compromise systems, rather than 'ethical' hackers trying to protect them. These studies indicate that the morality of many hacker's actions, and whether or not they exceed the ethical parameters of a given situation, varies based on mood or other factors. Although there have been studies of different types of security practitioners (Haber and Bailey, 2007; Werlinger et al., 2009), the social and ethical challenges faced by penetration testers remains an unexplored area. A better understanding of these challenges might provide directions for improving the techniques and tools used to penetration test systems.

In this paper, we present several ethical dilemmas and dimensions faced by penetration testers; these shed light on how penetration testers value the role of ethics, justify ethical decisions, and shape perceptions around their clients and practices. We consider the relationship between ethics and penetration testing in Section 2 before describing our approach in Section 3. We present the ethical dilemmas and dimensions found in Section 4, and illustrate its use in unpacking fallacies and biases, before concluding in Section 5.

2. Ethics and Penetration Testing

Ethics is the study of morality (Tavani, 2006). By providing principles and theories about different viewpoints about what is meant to be 'right', ethics helps classify arguments, defend a position or better understand the position others take and, in doing so, helps determine an appropriate course of action. Penetration testing vivifies ethics, forcing practitioners to think about the consequences of a variety of situations, ranging from agreeing the parameters of a test, to deciding which techniques should or should not be allowed during a test (Bishop, 2007). Unfortunately, as the previous section illustrated, many dilemmas are more sophisticated and fall within a grey area where a response may be legal, but potentially unethical. While the necessity to attend to ethical considerations is broadly accepted, guidance on how to do so is not. For example, the Open Source Security Testing Methodology Manual (OSSTM) states that, when evaluating the security posture of a target, “business and industry ethics policies” that influence

security and privacy requirements should be identified (Hertzog, 2010). However, the objective of undertaking such a review is to scope any testing activity and identify vulnerabilities that might lead to inappropriate disclosure of private information. OSSTM puts emphasis on what should be evaluated rather than the techniques used to carry out an evaluation; it is non-prescriptive about how such policies should be identified and analysed.

Although some of the ethical implications of hacking are understood (Spafford, 1992), the implications of *ethical* hacking are comparatively ill-explored. Moreover, while the role of ethics is discussed in computing degree courses, there are inconsistent options in what should be taught to students to prepare them for their professional careers (Hall, 2014). Consequently, professional penetration testers inevitably fall back on professional codes to provide advice on their conduct; such codes need to be broad enough to cover ethical conflicts and concerns, yet specific enough to guide decision-making in actual situations (Perlman and Varma, 2002). There have been several examples of the security community drawing up such codes for ethical hackers. For example, the Council of Registered Ethical Security Testers (CREST) provides their members with a code of conduct (CREST, 2014). This code not only stipulates a code of ethics, but is also an aide-memoire for good practice; these include the need to evaluate the impact of new techniques and tools, and requirements to explain project deliverables to clients, and keep up to date with new standards and regulations. However, such codes are often framed as constraints and rules rather than providing specific guidance. Not only do such codes give the false impression that locating and following a directive is both necessary and sufficient to behave ethically, they also fail to provide advice on how to deal with conflicts of ethical significance (Ladd, 1985).

Penetration testers are expected to make informed decisions based on their understanding of the situation at hand, supported by any procedural, ethical, and technical training they may have undertaken (Xynos et al., 2010). Although there is a plethora of books and events that provide technical training, there is little to describe the form that ethical training might take. Moreover, Xynos and his colleagues claim that ambiguity associated with penetration testing practices raise a number of other questions about how penetration testers demonstrate professionalism, how clients can be confident that a penetration testing team can be trusted to complete their assignment, and their work is fit for purpose?

(Pierce et al., 2006) have proposed a conceptual model of penetration testing ethics, which is centered on the role of integrity. It considers the avoidance of conflicts of interest, false positives and negatives, and binding ethical and legal agreements influences professional integrity, which, in turn, helps protect the interests of clients and the security profession in general. This model is grounded in technical literature of penetration testing, and codes of practice, which encompass it. The role of the model purports to provide guidelines for what it means for ethical hackers to behave ethically. The issues at stake are, however, greyer than suggested by this framework. For example, Pierce et al. claim that if penetration testers refuse to engage with criminal hackers then they are using their skills only for commissioned tests and are upholding the profession. However, there are numerous ways that penetration testers

might fail to uphold the profession. Moreover, the framework implies that behaving legally is synonymous with behaving ethically. This fails to recognise scenarios of legal ambiguity; penetration testers must unpack these to determine the right thing to do.

3. Approach

To understand the relationship between penetration testing and ethics, we interviewed eight professional penetration testers. While largely unstructured, the interviews sought responses to some of the questions raised by the related work (Pierce et al., 2006; Xynos et al., 2010; CREST, 2014). These were structured around the following four areas.

- Responsibilities: What are your professional responsibilities, and how do you ensure you that you and your team behave responsibly?

- Practices: How do you assess the legal and ethical import of your everyday practice?

- Ethics: What ethical codes of practice do you rely on, and how do you resolve any ethical dilemmas you might face?

- Assurance: What assurances do you provide of your professionalism, and how can clients be confident that you can be trusted to complete your engagement?

To ensure a consistent level of professional expertise, all interviewees either held qualifications awarded by CREST, or an equivalent qualification recognised by the UK government's CHECK scheme (CESG, 2014). Interviewees either worked for security practices recognised as CREST member companies or, in some cases, UK government teams with a responsibility for penetrating government systems and installations. During the interviews, interviewees were encouraged to talk about their own experiences carrying out penetration tests. Given the broadness of the term `penetration test' these ranged from office-based white and black box evaluations of a client's product, through to open-scope `red team' tests. Client confidentiality and lack of security clearance made it difficult for interviewees to talk precisely about specific examples. In such cases, interviewees were presented with hypothetical ethical dilemmas (similar to that presented in Section 1) and asked to describe how they would address them.

Each interview took place at the workplace of the interviewees, and each interview lasted between 45 minutes to an hour. Transcripts from the interviews were subject to open and axial coding (Corbin and Strauss, 2008). From this coding exercise, 34 refined thematic concepts were identified, together with 34 relationships between these concepts. From this emerging model, a set of propositions was written that summarised each of the 34 conceptual relationships. These propositions were

written on post-it notes, and subject to affinity diagramming to identify themed groupings of categories.

4. Results

4.1. Dilemmas

While the interviewees claimed they rarely faced moral dilemmas, we found evidence of two forms of dilemma faced by penetration testers. The first dilemma concerned managing penetration testing clients, and the tension between doing the right thing for the client company (the whole), and the right thing for its staff (the individual). While it was generally accepted that any form of activity that involved deception risks breaking the trust between the company and its staff, some interviewees believed that a company's security policy justified the use of human testing, irrespective of the legality or morality of the policy itself. The second dilemma concerned managing testing practices, and the tension between choosing a structured and carefully considered strategy (structured), over a strategy that was unstructured and contingent (unstructured). The former approach entails structuring an engagement such that ethical concerns are designed out. However, if the scope of a test expands or emergent technology is evaluated, there is a need to be more creative, and less bound by convention.

Based on the affinity diagramming exercise, we found two clusters of thematic concepts. One cluster corresponded with penetration testing behaviour that resolved these dilemmas by taking an individual/unstructured position (IU); the other cluster corresponded with a whole/structured position (WS). Both positions are not mutually exclusive, and we do not consider any position more virtuous than the other.

4.2. Dimensions

On considering the themes associated with the IU and WS positions, we found the following four additional groupings of category; these groupings provide insight into how penetration testers holding each position reflect on different concerns of ethical import. We consider these issues as ethical dimensions (Figure 1), and define these as follows:

- Value of ethics: the value penetration testers see in ethics.
- Ethical appeal: the means used by penetration testers to establish the credibility of their ethical position.
- Client focus: the emphasis placed on responsibly managing clients.
- Practice focus: the emphasis placed on providing assurance about penetration testing practices.

Dimension	Dilemma Positions	
	Individual / Unstructured (IU)	Whole / Structured (WS)
Value of ethics	Interpersonal skills	Legal sense
Ethical appeal	Common sense	Contingency
Client focus	Individual	Collective
Practice focus	Data and tool assurance	Information management

Figure 1: Perspectives adopted by dilemma positions for each dimension

4.2.1. Value of Ethics

For most interviewees, being ethical marked them out as professionals. For example, one interviewee (I4) observed: *"We all have to adhere to the CREST code of ethics, so we all rigorously adhere to that. I think I always go with the mentality that if the client is happy with what you're doing then you're along the right lines. Whenever I try and make a decision, you need to justify whether or not it's going to be beneficial for the client."* For this reason, some interviewees stated that either they or their companies would avoid testing activities, such as social engineering, for fear that these might be easily construed as unethical. Such activities not only jeopardise the well being of deceived clients, but also their career should problems occurred during testing. In some cases, however, such testing was deemed acceptable when undertaken as part of a `red team' test that evaluates a client's broader security posture.

In considering the more specific value of ethics taken by each position, we noted that the IU position considered ethics as a learned, interpersonal skill. When faced with a dilemma, juniors may defer responsibility for tackling ethical hazards to seniors or even their client. However, it is unclear who would be in the best position to tackle the dilemma. While the less senior tester has the most contextual knowledge, they may not necessarily know who is best placed to deal with it. The WS position of ethics is that of a vehicle for legality, and a means for honing legal senses. This standpoint claims that legal and moral issues are treated as one and the same, and that debate takes place in teams when moral issues are found. Testers subscribing to this perspective eschew anything morally ambiguous because it is understood that legal nuances are difficult to unpack.

4.2.2. Ethical appeal

Most interviewees claimed that the appeal used to resolve ethical issues was situational in some way, or – as characterized by I2 – *"The more you test, the more you get a sense of what is risky to do."*

The justification taken by those adopting an IU position is that being ethical is 'common sense'. One interviewee claimed that the ease with which the law can be broken, and the implications to their career of breaking the law keeps testers honest. Junior penetration testers hone their penetration testing 'common sense' by shadowing more senior testers to understand how adopting an adversarial perspective can identify what would be hitherto ignored vulnerabilities. While the primary purpose of such shadowing is to glean an understanding of the technical detail of penetration testing, junior testers develop their understanding of professional penetration testing in the process. The justification taken by those taking a WS position is that being ethical means appealing to contingency and putting any ethical dilemma in context. By placing any prospective ethical issue in context, the risks associated with it become obvious when the right questions are asked at the right time; this ability to identify and address risks in context is developed as testers become more experienced.

4.2.3. Client focus

While no interviewees were asked to carry out activities that breached the UK Computer Misuse Act, some interviewees had been asked to consider engaging in activities that might have been in breach of Article 8 of the Human Rights Act. As such, interviewees were mindful of the need to do the right thing for the client with respect to their own legal and moral obligations. For example, I3 notes: *"the major thing for us is to always remember why you're there, and keep within that scope so not to go and explore the network for the sake of exploring the network. We're not there to read people's emails and that kind of thing."*

The IU position is shaped by the need to reactively manage individual contacts within the client organisation. While few interviewees reported active hostility towards them, conflict between penetration testing "red" teams and client infrastructure "blue" teams was not uncommon, particularly in companies where the managerial contact was inexperienced or lack credibility within their organisation. For example, one interviewee stated that, when testing web apps at a client site, any unavailability of the web app would typically be blamed on the testers. In other cases, conflict arose as a response to some form of criticism, be this in the design of software or the infrastructure. The WS position is shaped by the duty to provide value to the client organisation as a whole. This includes keeping the organisation appraised throughout a penetration test, implicitly educating clients about the value of penetration tests, and collaborating in such a way that clients are well placed to fix any problems identified once a final report is delivered. In some cases, this obligation is so strong that some testers addressed dilemmas by focusing initially on the impact to the client, rather than by starting to consider the social and technical implications of the dilemma first. Some interviewees felt obliged to proactively address potential conflict. For example, one interviewee described how he would engage client staff by encouraging them to raise problems with him in such a way that, when highlighted in the final report, recommendations could be stated that address them.

4.2.4. Practice focus

The interviewees unanimously cared about their security practices, and the perceptions people hold about penetration testers. They believed that their association with a professional body, such as CREST, provided some assurance that their work practices are trustworthy. For example, I4 expressed concern that bad practice or low standards potentially undermine their entire industry: *"you have to adhere to all of your ethical guidance and you need to ... if you find those vulnerabilities you need to tell them about them immediately. As security experts, we have to do that otherwise the security industry as a whole... there wouldn't be any faith in it, or any trust."*

The responsibility to penetration testing practice is manifest by the IU and WS positions in different ways. The IU position is concerned with providing assurance about both the tools used, and any findings resulting from tool usage. Several interviewees noted that research into a potential tool's provenance was strongly encouraged by their firms, and internal training courses and seminars are used to share knowledge team members had discovered about new tools. Although some interviewees noted that job interview questions touched upon ethical practice, it was acknowledged that little staff development time was spent on what was described as 'soft consultancy stuff' like ethics. The WS position is shaped by the need to provide assurance about how information is managed. This position focuses on the integrity of information managed and delivered to the client. While this integrity is a product of the tools used to provide input into the report, referring to raw data and logs was considered as something only required as a last resort. Those adopting this position believe that factual information should always be defended, and evidence from different sources is sanitised before use. This level of assurance allays any apprehension that clients might have about what a penetration testing team has been doing.

4.3. Using the model to unpack fallacies and biases

By creating a model of ethical dilemmas and dimensions, it becomes possible to spot fallacies resulting from each position. For example, within the IU position, it is acknowledged that adopting an adversarial perspective, and shadowing more senior colleagues can hone the senses of more junior penetration testers. However, it is a fallacy to assume that ethical behaviour will always follow in such a situation. If the more senior colleague's behaviour is morally ambiguous then a junior tester may not appreciate that practices gleaned are equally ambiguous. Moreover, when adopting an adversarial and unstructured position then there is also a danger that behaviour that seems common sense may become legally ambiguous as well.

Potential biases are also evident when considering tensions between concepts. Within the WS position, educating the client about penetration testing is important, as is the need for clients to accept responsibility for remedying any problems found. When a report has been delivered to the client, positive feedback and the lack of further correspondence may indicate that the report has been accepted and its

recommendations actioned. It is, however, equally possible that the client may have sought the test only to obtain some form of accreditation, and may action few of the recommendations made. Should testers believe the report is being actioned then they may be subject to the fundamental attribution bias; this refers to the tendency of people to ignore possible external causes of the behaviour of others and to assume that their behaviour is a reflection of internal dispositions (Gilbert and Malone, 1995). As such, testers may underestimate how the role of external constraints and requirements shape the behaviour of those around them, and in turn overestimate how much their actions are determined by their personality, values and beliefs. This bias is also evident by the tendency of testers to assume that they are in fact better at understanding the importance of external factors in the behaviour of others than their peers (van Boven et al., 2003).

5. Conclusion

This paper has presented several ethical dilemmas and dimensions faced by penetration testers. In doing so, we have made two contributions. First, we have shown how the differences associated with the dilemmas identified are manifest across different ethical dilemmas. Second, we have briefly illustrated how both these differences and the model can be used to unpack possible fallacies and biases that affect ethical decision making before, during, or after a penetration test. A limitation of this work is that only UK practitioners were interviewed. However, given the experience level of the testers, there is little reason to assume these results do not scale when considering other testers with an equivalent level of professional experience, particularly those that engage with other professional bodies.

6. Acknowledgements

The research described in this paper was funded by the Bournemouth University FIF project Bournemouth European Network in Cyber Security.

7. References

Adams, A. and Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42:41–46.

Bishop, M. (2007). About penetration testing. Security & Privacy, IEEE, 5(6):84– 87.

van Boven, L., White, K., Kamada, A., and Gilovich, T. (2003). Intuitions about situational correction in self and others. Journal of Personality and Social Psychology, 85(2):249–258.

CESG (2014). What is CHECK? Available from http://www.cesg.gov.uk

Chiesa, R., Ducci, S., and Ciappi, S. (2009). Profiling hackers: the science of criminal profiling as applied to the world of hacking. Auerbach Publications.

Corbin, J. M. and Strauss, A. L. (2008). Basics of qualitative research: techniques and procedures for developing grounded theory. Sage Publications, Inc., 3rd edition.

CREST (2014). Code of Conduct for CREST Qualified Individuals. Available from http://www.crest-approved.org

Egelman, S., Herley, C., and van Oorschot, P. C. (2013). Markets for zero-day exploits: Ethics and implications. In Proceedings of the 2013 Workshop on New Security Paradigms Workshop, NSPW '13, pages 41–46. ACM.

Geer, D. and Harthorne, J. (2002). Penetration testing: a duet. In Computer Security Applications Conference, 2002. Proceedings. 18th Annual, pages 185– 195.

Gilbert, D. T. and Malone, P. S. (1995). The correspondence bias. Psychological Bulletin, 117(1):21–38.

Haber, E. M. and Bailey, J. (2007). Design guidelines for system administration tools developed through ethnographic field studies. In Proceedings of the 2007 symposium on Computer human interaction for the management of information technology, CHIMIT '07. ACM.

Hall, B. R. (2014). A synthesized definition of computer ethics. SIGCAS Comput. Soc., 44(3):21–35.

Hertzog, P. (2010). OSSTMM 3 - The Open Source Security Testing Methodology Manual. ISECOM.

Holt, T. (2010). Examining the role of technology in the formation of deviant subcultures. Social Science Computer Review, 28(4):466–481.

Ladd, J. (1985). The quest for a code of professional ethics: An intellectual and moral confusion. In Johnson, D. G. and Snapper, J. W., editors, Ethical Issues in the Use of Computers, pages 8–13. Wadsworth Publ. Co.

Perlman, B. and Varma, R. (2002). Improving ethical engineering practice. Technology and Society Magazine, IEEE, 21(1):40–47.

Pierce, J., Jones, A., and Warren, M. (2006). Penetration testing professional ethics: a conceptual model and taxonomy. Australasian Journal of Information Systems, 13(2):193–200.

Spafford, E. H. (1992). Are computer hacker break-ins ethical? Journal of Systems and Software, 17(1):41–47.

Tavani, H. T. (2006). Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology. John Wiley & Sons, Inc., New York, NY, USA.

Werlinger, R., Hawkey, K., Botta, D., and Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. International Journal of Human Computer Studies, 67(7):584–606.

Xynos, K., Sutherland, I., Read, H., Everitt, E., and Blyth, A. J. C. (2010). Penetration Testing and Vulnerability Assessments: A Professional Approach. In Proceedings of the 1st International Cyber Resilience Conference, pages 126–132.