Revelation and Science
Vol. 03, No. 02 (1435H/2013) 30-38

Towards Islamic Ethics in Professional Penetration Testing

Qazi Mamoon Ashraf and Mohamed Hadi Habaebi
Department of Electrical and Computer Engineering
International Islamic University Malaysia

Abstract
The high rate of technological advances in the field of computing has resulted in a rapid increase in the occurrence of new loopholes in systems. To ensure the security of their computing systems, big companies resort to using penetration testing as a solution, whereby an external company is hired to evaluate the security of the computer system or network in question. At various stages in the penetration testing process, the professionals who are hired have access to vital technical information about many companies. It is important for the professionals to appreciate the ethics involved in their work because failure to secure – or misuse of – the information may result in acute leaks of critical data. Many Muslim professionals are involved in many stages of the penetration testing process, and it is crucial for them to be aware not only of the preeminent position given to ethics and ethical conduct in Islam, but also of what they must do to maintain their ethical integrity. This paper highlights the ethical issues inherent in penetration testing operations, discusses their practical implications for Muslim professionals, and sets out the key ethical steps that need to be taken. It also offers a solution based on an Islamic framework of ethical principles and values derived from the Holy *Qur'an* and the *Sunnah*.

Keywords: *Network Security, Penetration Testing, Social Ethics*

Abstrak
Kemajuan teknologi yang saling berubah dalam bidang pengkomputeran telah menyebabkan peningkatan penciptaan kelemahan baru dalam sistem. Bagi menjamin keselamatan sistem perkomputeran, syarikat-syarikat besar mengambil jalan keluar dengan menggunakan ujian penembusan sebagai penyelesaian manakala syarikat luar di bawah perspektif mengupah sistem keselamatan komputer atau rangkaian. Terdapat banyak profesional Islam yang mempunyai peranan penting dalam pelbagai peringkat proses ujian penembusan dan mempunyai akses kepada maklumat teknikal bagi kebanyakan syarikat. Kegagalan untuk merahsiakan maklumat yang kritikal atau penyalahgunaan boleh mengakibatkan kebocoran data akut. Antara sebab profesional harus memahami etika yang terlibat dan melaksanakannya secara mahir adalah kerana etika merupakan aspek yang penting di dalam Islam. Kajian ini membincangkan langkah-langkah etika utama dan membentangkan isu-isu yang timbul berdasarkan ujian penembusan moden. Ia berkaitan prinsip etika tradisional terhadap cubaan penyelesaian bagi menyelesaikan masalah dengan menggunakan kerangka nilai-nilai etika Islam; yang berasal dari al-Quran dan Sunnah dan menyediakan paras etika yang tinggi di semua peringkat bagi umat Islam.

Kata kunci: *Keselamatan Rangkaian, Penembusan Ujian, Etika Sosial*

Introduction

The escalation in interconnection between computers and networks has resulted in cyber-attacks having far reaching implications and repercussions. Central agencies are seeing an increase in cyber threats that have the potential to become as devastating as the Sept. 11, 2001 (Ratnam, 2012). Figure 1 presents an open source collection of statistics by a computer security professional on his website demonstrating the ever increasing prospect of online security threats and cyber-attacks (Passeri, 2012). It can be seen that hactivism and cyber-crime are the most important

**Corresponding author: Qazi Mamoon Ashraf*
Department of Electrical and Computer Engineering,
Kulliyyah of Engineering,
International Islamic University Malaysia
E-mail: mamoonq@gmail.com

constituents of cyber-attacks. Hactivism refers to the practice of behavior using knowledge of computers and networking and system penetration as a means of protest or to promote political behavior and is usually practiced by non-professionals. Reasons for the same may be varied; such attacks may arise from communal circumstances, as a form of societal protest or existence of different political beliefs. Such attacks have the potential to result in massive economic losses, loss of repute, and many legal issues. However, these attacks are justified by the hactivists to be necessary, in order to achieve a greater good. The definition of good is relative, and perhaps all parties may not hold the same view. Eventually, the problem to categorize the purpose and content of such attacks is solved by the legal framework, which defines activities as legal or non-legal.

Penetration testing is a legally permitted scheme whereby an external corporation or an ex-hacker is employed to assess the security of the computer system or network under viewpoint. This is done by lawfully conducting tests and attacks against the system and exhaustive documentation of the loopholes and other weaknesses with detailed permission being given to the penetration testers. The focal motive is to discover weakness in their systems and fix them before a malicious user attempts to exploit. Penetration testing thus acts as a thin-line border between what is considered right and what is considered wrong. As cyber-attacks escalate, so does the demand for information security professionals such as penetration testers; who possess true network penetration testing and ethical hacking skills. These professionals work on the edge of what is legally allowed, and have painstaking detailed knowledge of the legal rules and regulations concerned with their industry.

Muslim professionals are significantly active around the computer engineering and information technology industry and a substantial population can be assumed to be involved in penetration testing as well. After completion of a project, these professionals discover loopholes in the client system and thus have potential access to critical data. Not only that, the penetration tester or, for that matter, any staff member of the security firm may have access to all the existing penetration testing reports that document the discovered weaknesses with breathtaking details.

To understand the ethics involved in penetration testing, we have to comprehend the concept of ethics, the concept of penetration testing and then the ethical problems involved. Much work has been done to explore the social issue and penetration tests dealing with ethics in vulnerability testing such as by (Matwyshyn, Cui, Keromytis, & Stolfo, 2010) and the social implication of a penetration process by (Smith, Yurcik, & Doss, 2002). Research also includes work on modeling the code of ethics (Pierce, Jones, & Warren, 2006), and work on the fundamentals of practice against hackers by (Eugune, 2002) & (Furnell & Papadaki, 2008). However, to the authors' knowledge, there is no such work which focusses on the Islamic perspective of ethics and penetration testing.

Generally, penetration testing professionals are bound by a general code of ethics to govern their behavior and to impart a sense of responsibility. Strict adherence to the code is required from their part. Muslim professionals, however, have a greater responsibility for the protection of the data because they are not only limited by professional ethical principles but are also constrained by the collective mindset and principles of Islam.

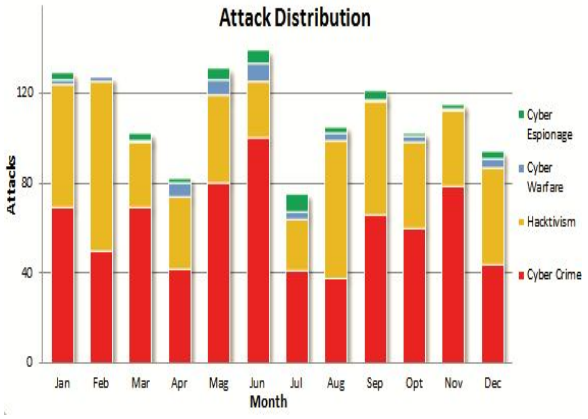

Figure 1: 2012 Cyber Attack Statistics (Passeri, 2012)

The rest of this paper is divided as follows. The second section deals with the background work explaining the traditional steps in penetration testing and moves on to introduce the Islamic concepts which define ethics. The third section unites the two and presents the proposed taxonomy-based model towards realizing Islamic values in professional penetration testing. The fourth section discusses the limitations and advantages of such an approach in the context of the consequence of applying the model. Finally, section five summarizes the contribution of this work.

Contextual Concepts

Traditional Elements of a Penetration Test

The basic elements of information security are confidentiality, integrity and availability (CIA) (Summers & Tickner). Confidentiality ensures that the information is not disclosed to unauthorized persons or processes whereas integrity refers to the inability of modification of information by unauthorized users.

Availability, on the other hand, ensures that the system's authorized users have appropriate uninterrupted access to the information in the system.

Penetration testing is one of the oldest methods for assessing the security of a computer system in terms of confidentiality, integrity as well as availability. In the early 1970's, the Department of Defense in the US used this method to prove the existence of the security weaknesses in computer systems. This was done in order to create more secure systems. Nowadays, penetration testing is increasingly used by organizations to assure the security of information systems and services, so that security weaknesses can be fixed before they get exposed.

Figure 2 summarizes common steps/methodology used in malicious penetration testing (Methodology for Penetration Testing, 2009) & (Krutz & Vines, 2008). The major theme of penetration testing describes how the tests should be conducted based on a collected set of tools at the professional's disposal. This includes five phases of reconnaissance *viz.* scanning, acquiring entrance, maintaining access and finally covering up the tracks.

- *Reconnaissance:* This is an opening activity in which an attacker attempts to gather data about a target. It includes attempts to document information such as the people involved, the computer systems, as well as the software technology being used across the system. It can be classified as either passive or active. Passive reconnaissance is a realized by monitoring the network using sniffer software or other mechanism to acquire information about the system. On the other hand, active reconnaissance scans the network to acquire information about the operating systems being used, available services, open ports, routers as well as hosts.
- *Scanning:* Scanning is an activity that precedes the actual attack and involves collection of more detailed information. This stage enables access to the network and consequential harmful activities. Steps in this stage are based on the data obtained during the first phase. The risk to the organization or business is considered high in the scanning phase.
- *Acquiring Access:* This phase is where the actual attack is implemented, therefore the business risk is at the highest level. During this phase, the attacker can access the operating system, and launch other attacks. Another goal is to obtain system privileges not normally available to the conventional user.
- *Maintaining Access:* Typical activities involved in maintaining access include downloading password files that can be reused to enter the system at a later time. To maintain ownership of the compromised system, an attacker might repair the vulnerability that allowed him to gain access in the first place. This is done to prevent other attackers from entering the system.
- *Covering any Tracks:* This stage contains steps to cover up such that no one should be aware of the attacker's malicious activities on the computer systems.

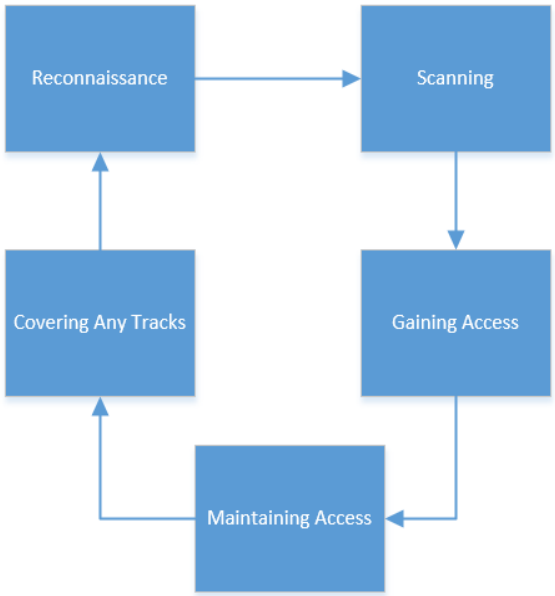

Figure 2: Malicious Penetration Testing Steps (Methodology for Penetration Testing, 2009) (Krutz & Vines, 2008)

Islamic Perspective of Ethics

Islamic ethical values are derived from two highest sources of knowledge which are The Holy Qur'an and Sunnah of Prophet Mohammed (PBUH). Sunnah is mainly defined by Muslim scholars as the recorded sayings and behavior of Prophet Mohammed which is mainly documented in six authenticated resources of Sahih al-Bukhari, Sahih Muslim, Sunan Abi-Daud, Jamea al-Termezhi, Sunan Ibn-Maja, and Sunan al-Nissae (Sahih Bukhari, Sahih Muslim). Islam considers ethics as an essential factor in rebuilding the society based on understanding of the Qur'an and Sunnah. This ethical rebuilding of human behavior will bring benefit, peace, and prosperity to mankind (Beekun, 1996).

The goals of Islam are not primarily materialistic but they are based on concepts of human well-being and good life with socio-economic justice (Chapra, 1992). A very important view to keep in mind is that Islamic ethical principles associate mankind acts with his intention. It is stated in the Holy Qur'an:

> *"Verily this Qur'an Doth guide to that which is most right (or stable)"* [The Qur'an 17:9]

We should also keep in mind the focus of Islam. While traditional ethics keep the society in mind, Islamic ethics lay focus on the individual. Robert Bellah states that Islam emphasized on the equality of all Muslims, and suggests that early Islamic community placed a particular value on individuals, as opposed to collective or group responsibility (McAuliffe, 2005).

Within an Islamic context, the term most closely related to ethics in the Qur'an is *khuluq*. The Qur'an also uses a whole set of terms to describe goodness. These include *khayr* (goodness), *birr* (righteousness), *qist* (equity), '*adl* (equilibrium and justice), *haqq* (truth), *ma'ruf* (known and approved), and *taqwa* (piety) (Fakhry, 1991). We can easily see the importance that Islam keeps on good conduct and ethics by looking at the frequency that related terms are mentioned (Hameed, 2010) as tabulated in Table 1.

Table 1: Good Ethical Terms in The Qur'an and Sunnah [19]

Statistics		
Good Ethical Characteristics	***No. of Verses***	***No. of Hadith***
Morality, Husn alkhulug walmuamalah (Good Ethics and Dealing)	61	250
Ikhlas (Sincerity)	23	34
Istighfar and Tawba (Repentance and Forgiveness)	202	100
Iswa Hasana, Irshad Islah (Good model and Guidance)	67	82
Wafaa Ahd, Ketmas Ser (Keep promise and Secrecy)	31	50
Alhamd, Alshukr, Althanaa (Thankfulness)	235	142
Sabr, Musabara, Kathm ghaid (Patience and Suppressing Anger)	108	64
Adl, Insaf (Fairness)	23	62
Ilm, Amal (Science, Work)	530	139
Hikmah and Hulum (Wisdom and Tolerance)	129	31
Ihsan (Beneficence)	66	29
Eman and Taqwa (Belief and Piety)	595	145
Tafakr, Tadabrm Taaml (Thinking, contemplating and dealing)	83	48
Amr Maarof Nahi Munkar (Enjoining goodness and forbidding badness)	13	33

In addition to that, a total of 10 verses have been identified to represent the fullest statement of code of behavior every Muslim must follow (A, 2004). These principles were kept in mind while constructing the ethical model for penetration tests. While all do not apply directly to our case: as can be seen below, number 4 states not to engage in 'mercy killings' for fear of starvation and number 5 instructs not to commit adultery. However these underlying principles of thought help establish some ground rules:

1. [The Qur'an 17:22]- Worship only God**:** "*Take not with Allah another object of worship; or thou (O man!) wilt sit in disgrace and destitution"*
2. [The Qur'an 17:23]- Be kind, honorable and humble to one's parents: "*Thy Lord hath decreed that ye worship none but Him, and that ye be kind to parents. Whether one or both of them attain old age in thy life, say not to them a word of contempt, nor repel them, but address them in terms of honor."*
3. [The Qur'an 17:26]- Be neither miserly nor wasteful in one's expenditure: *"And render to the kindred their due rights, as (also) to those in want, and to the wayfarer: But squander not (your wealth) in the manner of a spendthrift."*
4. [The Qur'an 17:31]- Do not engage in 'mercy killings' for fear of starvation*: "Kill not your children for fear of want: We shall provide sustenance for them as well as for you. Verily the killing of them is a great sin."*
5. [The Qur'an 17:32]- Do not commit adultery: "*Nor come nigh to adultery: for it is a shameful (deed) and an evil, opening the road (to other evils)."*
6. [The Qur'an 17:33]- Do not kill unjustly: *"Nor take life – which Allah has made sacred – except for just cause. And if anyone is slain wrongfully, we have given his heir authority but let him not exceed bounds in the matter of taking life; for he is helped (by the Law)."*
7. [The Qur'an 17:34]- Care for orphaned children: "*Come not nigh to the orphan's property except to improve it, until he attains the age of full strength…"*
8. [The Qur'an 17:34]- Keep one's promises: . *"..fulfill (every) engagement [i.e. promise/covenant], for (every) engagement will be enquired into (on the Day of Reckoning)."*
9. [The Qur'an 17:35]- Be honest and fair in one's interactions: "*Give full measure when ye measure, and weigh with a balance that is straight: that is the most fitting and the most advantageous in the final determination."*

10. [The Qur'an 17:36]- Do not be arrogant in one's claims or beliefs: "*And pursue not that of which thou hast no knowledge; for every act of hearing, or of seeing or of (feeling in) the heart will be enquired into (on the Day of Reckoning).*"

Model

The traditional process discussed in the second section does not embrace the ethics of penetration testing clearly and the scope is limited to outlining a methodology for penetration testing. To solve the ethical related problems for Muslim professionals and to help Muslims to implement the Islamic ethics in their workplace we propose this taxonomy-based framework model, taking care of the special aspects that are involved in a penetration testing backdrop. The elements of the ethical conceptual model presented in this paper are summarized in Figure 3. These are based on a hierarchy and include guidelines to always keep the organization in mind, to protect the customer, to uphold the security profession, to avoid conflict of interest, and to avoid conflict with legality. Detailed explanation has been presented in the sub-sections.

The proposed model stands centrally on value and integrity, progressively building on the various concepts that have been presented. The Muslim penetration tester should act with integrity at all times, and try to maintain a distance from crossing the thin line to become a cyber-criminal. To achieve value and integrity in the work habit, the professional would require consistency of actions to achieve a specific set of outcomes. Beyond the purpose of the model elements, there exists a sense of awareness of Islamic principles, and that of an Ultimate Entity of justice. Working ethically just for the sake of it is not applicable, but to exert with Al-Ihsan is recommended; that is to do work aiming for perfection. This can be only achieved by keeping the Creator in mind at all times and have the sense in one's mind that one is answerable to a higher power, instead of a colleague. This model is functionally based on the taxonomy suggested by (Pierce, Jones, & Warren, 2006) and few fragments have been recognized and adapted in the design of the proposed model.

In the backdrop of the model, it is helpful to know that penetration testing professionals rarely work as individuals, except in rare cases. Generally, they work as part of a larger information security corporations or organizations, comprising of different departments. These departments, may include research, legal, human resources, as well as managed infrastructure services.

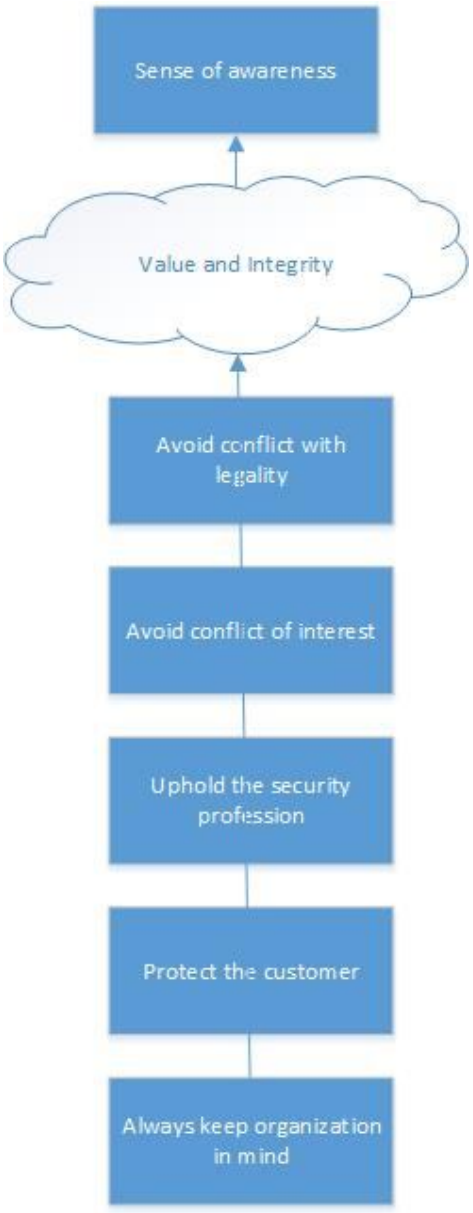

Figure 3: A conceptual model of Islamic Penetration Ethics

Avoid conflict with legality

It is indispensably important that the organization and the penetration tester have an identical understanding of what is authorized to be done and what not. Furthermore, the organization commonly arranges for an exhaustive legal contract stating the scope as well as all the terms and conditions of the penetration test. The scope includes the technical areas which are to be covered, and which areas to be stayed away from. The penetration test and a malicious attempt towards hacking, is just separated by a thin line; a line set up by the legal contract. As has been seen, in the event of a successful penetration test, a penetration tester can be open to dismissal and prosecution unless contract

terms are included to protect the individuals conducting the test.

For a Muslim professional, the laws could be made more compatible by introducing a Shariah compliant contract, which not only deals with elements of the penetration test but also mentions how a Muslim professional is constrained by his value and his integrity. Shariah based legal principles would also cover how the actions of a Muslim are covered, and may provide a much deeper definition of the scope of the penetration test. Consequently, such a legal contract should enforce strict adherence on the part of the Muslim professional. The Qur'an states:

> *"...fulfill (every) engagement [i.e. promise/covenant], for (every) engagement will be enquired into (on the Day of Reckoning)."*
>
> [The Qur'an 17:34]

This particular verse motivates the individual to strictly lay down the rules of conduct and follow them, as the individual is now not just answerable to the client, but also to Allah. It is common to notice that Muslim professionals in technical IT based jobs tend to relate less to what their religion talks, as compared to sciences of humanities such as related to medical, social or political knowledge. The concept is limited to the western definition of ethics, which only lays down the rules of conduct, but no solid motivation. Islam, however, provides a strong motivation for a penetration testing professional to honor his job, and protect his client.

Conditions of ethics need to be included legally into the contract. The professional can avoid any potential conflicts with legality, if the existing information security laws are modified suitably according to Shariah. If the laws are not modified accordingly, then the incompatibility may give rise a situation where the traditional legal laws conflict with the some minor yet fundamental principles of Islam. The professional will most probably adhere to the traditional laws, and ignore the teachings of Islam, considering the impact to be low as compared to potentially losing his source of income. Eventually, a Shariah compatible or a Shariah based legal ruling on defining the scope will help the individual avoid the conflict with legality.

Avoid conflict of interest

Muslims are scattered over the face of the earth, and are linked to different cultures and traditions. The only thing that binds them is Islam, and its teachings. Muslims originating from particular places or all Muslims as such, tend to have emotional feelings attached with certain individuals, groups or tribes. Imagine a scenario where a particular company belonging to a particular group hires the penetration testing company for its services, and the Muslim professional as one of the testers. The Muslim penetration tester faces a conflict of interest as there would be not sufficient motivation for him to do the test ethically. The tester may find it a chance to legally find about the clients vulnerabilities and may sell it to third parties without actually reporting it.

The Islamic ethical principles which associate mankind acts with his intention can be effectively used in such a case to solve the conflict. It was narrated on the authority of Umar ibn al-Khattab who said: I heard the Messenger of Allah say:

> *"All actions are judged by motives, and each person will be rewarded according to their intention. Thus, he whose migration was to God and His Messenger, his migration is to God and His Messenger; but he whose migration was for some worldly thing he might gain, or for a wife he might marry, his migration is to that for which he migrated."*
>
> [Hadith 1, Hadith An-Nawawi: Al-Bukhari & Muslim]

Therefore it is required that a Muslim tester needs to check on his intention before accepting the contract. If there arises any sort of a thought, even though minor, that the individual may not be fair during the test, then it will be best for him to avoid the contract all together. This may be done by informing the parent organization of conflict of interest that may arise in his part. If the individual feels that he will be fair, then he may go ahead and agree to conduct the test. But the individual has to be very careful while handling the client's data. The power at his hands can result in beneficial acts but on the other hand, it can significantly damage the reputation of the company, and the reputation of Islam. It can even result in legal action by the company against the penetration tester. Thus a Muslim penetration tester should never lose sight of this fact and always keep the client company's data secure, and wherever possible avoid situations leading to conflict of interest.

Uphold the security profession

Promotion of unrestricted hacking contests can be considered unethical as it greatly suggests a false security guarantee. Many public hacking contests for security assurance are being organized throughout the world to imply a false security assurance as well as publicizing penetration testing companies. One event being held in Malaysia is even being organized by a public university and a private penetration testing

company (I Hack 2013, 2013). In an opinion published in (Pierce, Jones, & Warren, 2006)

> *"..Such contests draw unnecessary attention to the client network as a perception of a 'fair game' target will endure in the hacking community far longer than the expiration of the testing contract."*

An incorrect security guarantee amounts to falsehood and Islam is strict about principles of honesty and truthfulness. The Qur'an reminds us about the benefits of being honest and fair in one's interactions:

> *"Give full measure when ye measure, and weigh with a balance that is straight: that is the most fitting and the most advantageous in the final determination."* [The Qur'an 17:35]

Protect the customer

The Muslim penetration tester is required to protect the customer and the customer's interests. (Pierce, Jones, & Warren, 2006) supports this by stating that:

> *"This holds true even if it is in the best interest of the customer to engage a different testing company. In that event, the tester should not recommend any particular company so as to avoid the possibility of a conflict of interest or the perception of one."*

In the event of a conflict, such as those resulting from personal, communal or different political beliefs, the priority should be to protect the customer. No matter what, the customer has to be protected from economic losses, loss of repute, and legal actions. The economic losses may result from leaking of sensitive information online, such as the status of security of the company's computer systems. This may result in lessened trust towards the company and eventually harm the financial stability as shares prices may drop. Loss of reputation may be caused by unnecessary advertising the critical system vulnerabilities, such as in a casual conversation with a family member where the penetration tester talks about his findings.

Thus, to operate effectively, the penetration tester must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support the tester's efforts. The penetration tester, at all times, may not discuss what has been discovered, and should not even lightheartedly refer to the weaknesses in any client company.

Organisational point of view

Organizations need to be very sure about who they are bringing in, and look for suitable certifications or qualifications that can indicate a professional capability. The staff should be able to test for vulnerabilities and proficient in recording whatever results they obtain.

A Muslim penetration tester must have an exhaustive sense of traditional ethics supplemented by the teaching of The Qur'an and Sunnah. Undeniably the idea of penetration testing is worrying as typically it is the ex-hackers who are employed by the organization and offer their services to test and secure systems. As ex-hackers, these professionals are highly knowledgeable in the technical aspects but it can be assumed to some extent that these professionals may lack in the field of ethics. We need to be fairly sure that anyone being taught the techniques has a properly mindset, not destructive by nature, to prevent misuse of the knowledge by such an individual.

It has been stated that:

> *"The principle objective of penetration testing is to test security measures in a company: there is little point to testing systems known to be highly vulnerable. Testing should not commence until appropriate security has been applied to the system. Testing should not be performed without the expressed written permission of the client. Whereas in the hacking community attacks occur non-consensually, contractual arrangements must be in place to provide a degree of separation between hackers and security professionals."* (Pierce, Jones, & Warren, 2006)

Now consider the following verse from The Qur'an:

> *"And render to the kindred their due rights, as (also) to those in want, and to the wayfarer: But squander not (your wealth) in the manner of a spendthrift."* [The Qur'an 17:26]

It is also to be kept in mind to make the penetration test as efficient and as cheap as possible for the client company. This deals directly with Islamic principles which oppose wastage. The trick is to be neither miserly nor wasteful in one's expenditure.

Sense of awareness

Ultimately, the tester's sense of awareness towards the Creator and the feeling of a responsibility should compel them to serve and protect the client while behaving ethically to preserve the integrity of the profession. As seen in Figure 3, avoiding conflicts of interest and avoiding conflicts with legality are

foremost requirements for awareness and responsibility. Islamic term Amanah (Trust) is viewed as an important value that enforces the concept of responsibility towards one's work.

Furthermore, the sense of awareness is a requirement for upholding the profession and for serving and protecting the client. Thus, all together, the principles of upholding the profession and serving and protecting the client, avoiding conflicts of interest, and avoiding legal conflicts build a solid ethical framework. The Qur'an states:

> *"Take not with Allah another object of worship; or thou (O man!) wilt sit in disgrace and destitution."* [The Qur'an 17:22]

Discussion

A Muslim penetration tester must profess in-depth skills of the five phases of penetration testing. However, as was seen these phases are based on technical knowledge and do not include ethical issues in their domain. Few companies have made an effort to link the two by introducing various courses and certifications in an attempt to standardize the knowledge base. Penetration testers are frequently educated of the methods to incorporate best practices followed by experienced experts in the field (EC-Council). These form the foundation to important steps towards bringing an ethical sense into the penetration testing professionals.

In addition to the technical ability, Islamic penetration testing would also require knowledge and understanding of Islamic legal system, and computer-related laws, particularly corresponding to information security. Traditional legal issues are complex because the Internet crosses international boundaries and is accessed from many jurisdictions with different laws and definitions of computer crime. Shariah can thus become the common denominator for cyber laws, and could set the standard for others to follow. Countries following Islamic law can setup work groups to come up with cyber laws spanning the whole world. This will lead to the formation of a standard, global cyber law with roots in Islamic principles and put us on the technological map of the Future Internet.

Any norms regarding ethical behavior are subject to interpretation of local customs, backgrounds, religion, and other environmental influences. Islam, again is the solution, by providing fundamental principles that exceed the constraints put forward by such frivolities. It has to be remembered that all the work should lead to Al-Ihsan, the highest degree of perfection in work and reporting. Thus, just because the client customers have a different religion, or belong to some parts of the world, should not sufficient motivation to tamper with the results. Furthermore, the Muslim penetration professional is required to take full responsibility and fairness and working with Hikmah and make use of this wisdom to settle any arising problems

Many people in Muslim majority countries have been seen to practice hacking for nefarious purposes. These malicious users, who may be Muslims, have a variety of motivations and justifications for their activities. Some of these individuals believe that information should be free and transparent, while some others practice in opposition to standing governments or certain regulations. People who conduct such activities for a cause are said to be practicing Hactivism. Recently, at least 6196 various websites have been defaced by an Indonesian group (Statistics Indonesian Hacker) which may be regarded as Hactivism and the number continues to grow each day. The activities associated were found regarding political causes as of writing of this paper. The reader is reminded that Indonesia is a Muslim majority, and the probability of the participants to be Muslim is very high. It has to be made clear, that no matter what the justification, breaking into computers and networks is illegal based on current laws and regulations and same applies to Muslims as well.

Due to the lack of comprehensive nature of cyber-laws today, there is a possibility of lack of justice in new and unique scenarios across different countries. There is a need for a proper and exhaustive model which encompasses the technical, social as well as the ethical aspects of penetration testing as well as data leak. The concepts introduced in this paper can be used as a starting framework for that. There is also a need to introduce and research on Shariah based legal principles which take care of the legal contract between a company and a Muslim penetration tester. If the laws are not adapted, it would result in a condition of conflict between Islamic teaching and traditional rulings of law.

At the time of conflict between traditional values and teaching of Islam, Islamic ethics should be given the highest priority, and thus traditional ethics be overridden. A sense of awareness towards the Creator has to be exist, and the fact that we have been sent on the Earth not to earn money, but for a greater cause.

Conclusion

Penetration testing is an ever-evolving process and a Muslim penetration tester has to persistently endeavor to duplicate the intent and actions of malicious users without causing harm. At the same time, keeping Islamic ethical values as the foremost guide is essential to give full justice to the profession. This

paper proposed an ethical model using the framework of Islamic moral values. It highlighted the key ethical issues in a modern penetration testing background and discussed principles to be used.

The Muslim penetration tester has to operate with the permission and knowledge of the organization and put all effort to find weaknesses in the information system that can be exploited; all while keeping the sense of responsibility towards the Creator. Strictly adherence to the Islamic code of conduct will not only supplement traditional penetration ethics but also raise the quality level of the overall process significantly.

REFERENCES

The Nobel Qur'an, English Translation of the meaning and commentary. (1417 H). (King Fahd Complex for the Printing of the Holy Qur'an) Retrieved from Surah Al-Isra, 17:9.

Methodology for Penetration Testing. 2009, June. International Journal of of Grid and Distributed Computing, 2(2).

I Hack 2013. 2013. (I Hack Competition 2013) Retrieved from http://www.uitm ihack.edu.my/2013/ A, N. S. (2004). Islam. Indian University Press.

Beekun, R. I. 1996. *Islamic Business Ethics*. Virigina: IIIT institution.

Chapra, M. U. 1992. *Islam and the Economics Challenge*. International Institute of Islamic Thought. Virginia.

EC-Council. (n.d.). Certified Ethical Hacker. Retrieved March 20, 2013, from EC-Council: http://www.eccouncil.org/courses/certified_ethical_ hacker.aspx

EC-Council. (n.d.). Licensed Penetration Tester. Retrieved March 20, 2013, from EC-Council: http://www.eccouncil.org/courses/licensed_penetrati on_tester.aspx

Eugune, S. E. 2002,) 10 Jan . Taking a stand on hackers. Computers & Security, 21(5), 382-384.

Fakhry, M. 1991. Ethical Theories in Islam. Leiden: E. J. Brill,. 12-13.

Furnell, S., & Papadaki, M. 2008, 5 May . Testing our defences or defending our tests: the obstacles to performing security assessment references. Computer Fraud & Security, (5), 8-12.

Hameed, S. A. 2010. Software Engineer Islamic Ethics: An interactive web-based model. International Conference on Computer and Communication Engineering, (. 1-7).

Krutz, R. L., & Vines, R. D. 2008. The CEH Prep Guide: The comprehensive guide to Certified Ethical Hacking. Wiley Publishing.

Matwyshyn, A. M., Cui, A., Keromytis, A. D., & Stolfo, S. J. 2010. Ethics in security vulnerability research. Security & Privacy, IEEE, 8(2), 67-72.

McAuliffe, J. D. 2005. Social Sciences and the Qur'an. In Encyclopedia of the Qur'an (. 5, . 66-76). Leiden: Brill.

Passeri, P. 2012, December. 2012 Cyber Attacks Statistics. Retrieved March 14, 2013, from Hackmageddon.com: http://hackmageddon.com/2012-cyber-attacksstatistics-master-index/

Pierce, J., Jones, A., & Warren, M. 2006. Penetration Testing Professional Ethics: a conceptual model and taxonomy. *Australasian Journal of Information Systems*, 13.

Ratnam, G. 2012, October 12. Cyberattacks Could Become as Destructive as 9/11: Panetta. Retrieved March 6, 2013, from BloombergBusinessWeek: http://www.businessweek.com

Sahih Bukhari, Sahih Muslim. (n.d.). Retrieved March 18, 2013, from QuranUrdu: http://www.quranurdu.com/ahadith/ Smith, B., Yurcik, W., & Doss, D. (2002). Ethical hacking: the security justification redux. Social Implications of Information and Communication Technology. *Proceedings IEEE 2002 International Symposium on Technology and Society*, (pp. 374 379).

Statistics Indonesian Hacker. (n.d.). Retrieved August 5, 2013, from http://defaceart.indonesianhacker.or.id/

Summers, A., & Tickner, C. (n.d.). What is Security Analysis? Retrieved March 15, 2013, from Introduction to Security Analysis: http://www.doc.ic.ac.uk/~ajs300/security/index.html

Article history

Received : 13/05/2013

Accepted : 11/12/2013