An Analytical Approach to Psychological Behavior of Hackers' Motives

Elie Nasr[1], Elie Kfoury[1], Maya Kfoury[2], and Liliane Karam[1]

[1]American University of Science and Technology, Computer Science Department, Beirut, Lebanon
{enasr, ekfoury}@aust.edu.lb, lkaram@yahoo.com
[2]Lebanese University, Psychology Department, Beirut, Lebanon
mayakfoury97@gmail.com

Abstract. Cyber-attacks have always been a critical concern in the field of information security and personal privacy. Although designing security mitigation against cyber-attacks requires the researcher to adopt the mind of a hacker, we still have a lack of knowledge about the psychology behind the hacker's behavior. Contrary to popular belief, the intentions of a hacker are not always bad and hacking is not necessarily a cyber-crime. This paper has many objectives including: defining hacking and the different types of hackers; investigating the motives that drive a person to become a hacker; and, assessing what major role hacking plays in influencing university students. This research is exploratory and uses a quantitative approach; it relies on the use of a survey questionnaire addressed to a sample of 150 students who have taken hacking courses and/or exposed to hacking activities. This questionnaire is inspired from module A, and module C of the Hacker Profiling Project [1] (HPP) adopted by United Nations Interregional Crime and Justice Research (UNICRI). Findings are to help organizations and institutions understanding the cyber-criminal mind and hackers' motives, and hence, be selective in choosing their potential laborers and their corresponding ranks especially in critical administrative positions.

Keywords: Cyber-attacks, information security, psychology, cyber-crime, hackers, survey, behavior.

1 Introduction

Psychology is the scientific study of human and animal behavior with the object of understanding why living beings behave as they do [2].On the other hand, in the computer security context, a hacker is somebody who looks for and/or misuses vulnerabilities in a computer or a network. The culture that is composed of hackers is usually referred to as the computer underground and is now a known community. There are different communities on the web; each is composed of a number of computer hackers, willing to perform either malicious activities, or research on discovering existing threats in current protocols and systems. Furthermore, threats can be discovered accidentally such as the recent Heartbleed bug [3]. Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. The Heartbleed bug was one of the largest security vulnerabilities of 2014, not only because of the media attention it garnered but also because it affected over half a million web sites on the Internet. Because the bug was in OpenSSL, it affected web sites, VPN concentrators, client applications and mobile devices.

In this paper, we tackle the psychology behind the hacker's mind, starting from how a human being turn from a normal person into a hacker as well as relating each proposed psychological theory to a practical example of a hacker. This is achieved through a questionnaire influenced by two HPP's questionnaire modules: Module A reflects Personal data (gender, age, social status, family context, study/work), and Module C mirrors Technical and criminological data (targets, techniques/tools, motivations, ethics, perception of the illegality of their own activity, crimes committed, deterrence).

In the following section, we discuss the different types of hackers classified by the community of hackers and by different institutes. Afterwards, we demonstrate famous classical psychology theories, and propose a relation of each theory to the mind of the hacker, aiming at understanding the mindset of a hacker from the student perspective.

2 Types of Hackers

"Hacker" is a free term and has diverse implications. Traditionally, hacking was defined as allowing a system to behave in a manner different from what it was intended to. However, the expression "Hacker" is now commonly defined as somebody who breaks into PC systems for the joy he/she gets while performing it or for other goals such as stealing information for cash or political inspirations. Hackers are mainly grouped into three broad categories [4]: White hat hackers, black hat hackers, and grey hat hackers. We briefly discuss each type below:

2.1 White Hat Hackers

The term "white hat" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems [5]. A penetration test, or pen test, is an endeavour to assess the security of an IT organization by securely attempting to detect vulnerabilities. These vulnerabilities may exist in systems' configuration, application's flow, operating systems, end-user activities. Nowadays, we find companies working as penetration testing firms where a group of expert white hat hackers tries to penetrate the network of a certain client, usually a company, for the sake of auditing the security measures.

2.2 Black Hat Hackers

Black hat hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".
A black hat hacker can also be classified as different sub types:

Script Kiddies. A script kiddie is often, but not always, a juvenile hacker; an attacker who uses scripts or programs developed by more sophisticated hackers or crackers. Oftentimes the underlying motivation for a script kiddies attack is simply to garner the attention of peers. Script Kiddies are generally looked down upon by the hacking community for their lack of self-taught skills and reliance upon premade exploit programs and files. It is often thought that script kiddies are destined to become crackers or black hat hackers in that their rush for skill and power generally supersedes their desire to educate themselves fully in the complexities of hacking [6].

State Sponsored. Governments often hire state-sponsored hackers in order to ensure that there are no security holes in their infrastructure. But often, this type of hacking can enter spy territory as well. Those who are skilled at infiltrating systems can be encouraged to poke around the secret files of a government, or gain access to classified materials about the next big weapon being developed in nations identified as threats to our way of life [7].

Spy Hackers. Cyber spying, or cyber espionage, is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware [8]. Hackers that are concerned in cyber spying are called spy hackers.

Cyber Terrorists. Cyber-terrorism is defined by the Technolytics Institute as "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives [9].

Malicious Insiders. An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems [10].

2.3 Grey Hat Hackers

Grey hat describes a cracker (or, if you prefer, hacker) who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a grey hat acts without malicious intent. The goal of a grey hat is to improve system and network security. However, by publicizing vulnerability, the grey hat may give other crackers the opportunity to exploit it. This differs from the white hat who alerts system owners and vendors of vulnerability without actually exploiting it in public [11].
Having described the different types of hackers, we will explore in the following section the major psychological theories and investigate how a hacker might be related to each theory.

3 Psychological Theories

Each subsection listed below demonstrates a famous psychology theory with its relation to hackers.

3.1 Psychoanalytic Theory

The theory of personality developed by Freud that focuses on repression and unconscious forces and includes the concepts of infantile sexuality, resistance, transference, and division of the psyche into the id, ego, and superego [12].
As Sigmund Freud, founder of psychoanalysis, suggests, our psyche is composed of 3 parts: the id (Latin for "it” [13]) that represents the instinctive and primitive desires, the Super Ego that represents the values and ethics of society taught to the individual by his parents, and the Ego that develops to reconcile between the impractical id desires and the realistic world. In this paper, we are interested in the Super Ego; that is built up by a satisfactory relationship with the parental figure. From a psychoanalytic perspective, the criminal behavior in general is a manifestation of a weak Super Ego, criminals are able to commit crimes without feeling guilty, their conscience –or superego- does not work correctly because they were unable to shape a solid and adoring relationship with their parents or parental figure. This theory can also be applied on cyber criminals, including hackers. Thus the hacker’s behavior is explained by a weak super ego and perhaps an absence of a parental figure. This theory seems suitable for black hat hackers because these hackers have no moral ground to prevent them from doing unethical activities like cracking someone’s system and ravaging their privacy.
Moreover, psychoanalytic theory might investigate the hacker’s personality in a different perspective.
Freud proposed that the criminal’s actions are a way to liberate himself/herself from the guilt caused by the Oedipus complex which is the unresolved desire of a child for sexual gratification through the parent of the opposite sex. This involves, first, identification with and, later, hatred for the parent of the same sex, who is considered by the child as a rival.
This interpretation is also applied on cyber criminals including black hat hackers.

3.2 Theory of Moral Development

Kohlberg suggested that developing children advance through distinct stages of moral development in a way comparable to their development through Piaget's well-known stages of cognitive development [14]. His perceptions and experiments on children and adults, allowed him to hypothesize that people step forward successively from a stage to the next in an invariant order, not skipping any stage or regressing to any preceding stage. These are stages of reflection processing, suggesting diverse methods of considering and critical thinking at every stage. The delay in moral reasoning leads to a criminal behavior in general. In this case, the criminals are hedonist, which means that they fulfil their needs without caring at all about the consequences. This applies on cyber criminals, that include black hat hackers, spy hackers, script kiddies, terrorist and malicious hackers. White hackers on the other hand, have a solid development on the moral reasoning.

3.3 Theory of Inferiority Complex

Inferiority complex is a term used to portray individuals who compensate their feeling of inferiority by acting ways that make them seem predominant. They do this in the light of the fact that controlling others may help them feel less insufficient.

This theory can explain some hackers' behavior, for example a person who feels like he is socially excluded for being a geek [15] might use his abilities to hack in order to feel superior to his victims and control them.

3.4 Theory of Cognitive Behavioral Psychology

The claim to fame of Behavioral and Cognitive Psychology accentuates an experimental-clinical way to deal with the use of behavioral and cognitive sciences to comprehend human conduct and create intercessions that improve the human condition. Behavioral and Cognitive psychologists take part in exploration, instruction, preparing, and clinical practice regarding an extensive variety of issues and populaces. [16]

In this theory, we will talk about two sub theories:

Theory of Operant Conditioning. Operant conditioning (also, "instrumental conditioning") is a learning process in which behavior is sensitive to, or controlled by, its consequences [17]. For example, a child may learn to open a box to get the candy inside, or learn to avoid touching a hot stove. In contrast, classical conditioning causes a stimulus to signal a positive or negative consequence; the resulting behavior does not produce the consequence. For example, the sight of a colorful wrapper comes to signal "candy", causing a child to salivate, or the sound of a door slam comes to signal an angry parent, causing a child to tremble. The study of animal learning in the 20th century was dominated by the analysis of these two sorts of learning, and they are still at the core of behavior analysis.

The black hat hackers in this theory will have positive reinforcement when hacking since they will get what they need: This might be letting other people be afraid from them, or getting paid for example

Regarding the white hat hackers, they could be altruistic people who like to help others, thus helping others would be a positive reinforcement, or they could be getting paid by their employers, which is also a reinforcement

As for the grey hat hackers, they are half altruistic, half egoistic; they get a positive reinforcement from both cases.

Theory of Reflex Pavlovien. Classical conditioning occurs when a conditioned stimulus is paired with an unconditioned stimulus. Usually, the conditioned stimulus (CS) is a neutral stimulus (e.g., the sound of a tuning fork), the unconditioned stimulus (US) is biologically potent (e.g., the taste of food) and the unconditioned response (UR) to the unconditioned stimulus is an unlearned reflex response (e.g., salivation). After pairing is repeated (some learning may occur already after only one pairing), the organism exhibits a conditioned response (CR) to the conditioned stimulus when the conditioned stimulus is presented alone. The conditioned response is usually similar to the unconditioned response, but unlike the unconditioned response, it must be acquired through experience and is relatively impermanent. [18]. Hackers apply this methodology of thinking when they discover certain vulnerability in the system. They will keep trying to penetrate the system even though they don't have any profit.

Theory of Social Learning. Social learning theory coordinated behavioral and cognitive theories of learning so as to give a far reaching demonstrate that could represent the extensive variety of learning encounters that happen in this present reality [19].

Since hackers are always participating in a community, they benefit and learn from others. Thus, continual learning will exist in order to benefit from the interaction with the community.

Kleptomania. Kleptomania is the inability to refrain from the urge to steal items and is done for reasons other than personal use or financial gain. First described in 1816, Kleptomania is classified in psychiatry as an impulse control disorder. Alternatively, some of the main characteristics of the disorder, which consist of recurring intrusion feelings, an inability to resist the urge to steal, and a release of pressure following the theft, suggest that kleptomania could be an obsessive-compulsive spectrum disorder, although this is disputed. [20]

The behavior of hackers who steal data just for the pleasure of stealing with no other incentive or benefit, such as a fulfilment of a financial need for example might be explained by kleptomania.

3.5 Theory of Criminal Personality

This theory was one of the most debatable topics in psychology. Some people agreed that this personality exists while others refused this theory. According to different authors the criminal personality is characterized by: egocentrism, aggressiveness, need to dominate, intolerance to frustration, and indifference toward the victims and weakness of the moral sense [21].

We expect that malicious hackers have a criminal personality since they carelessly hurt their victims for their personal benefits

4 Research Questions

Designing security mitigation against cyber-attacks requires the researcher to adopt the mind of a hacker. We still have lack of knowledge about the psychology behind the hacker's behavior. Consequently, the researchers developed the following research questions:

1. **Does having a low or moderate self-esteem influence on the person's motives to perform a hacking activity?**
2. **Is the level of parental authority related to the type of hacking the human identifies with?**
3. **Is there a relationship between breaking a vulnerable system for reward and social economic status?**
4. **Do people involved in hacking communities have the full knowledge regarding hacking and types of hackers?**
5. **Is "Considering the consequences of malicious hacking" related to the type of hacking people identify with?**

5 Methodology

This paper is exploratory in nature and uses quantitative research methodology. The purpose is to understand the motives that drive a person to become a hacker. The quantitative approach is based on using a survey questionnaire distributed to a sample respondents consisted of Computer Science, Information and Communications Technology (ICT), and Computer and Communications Engineering (CCE) students. The researchers located the universities from Beirut region that hold the aforementioned degrees and follow the American system. A list of universities was obtained, and four of them were chosen randomly. The chosen universities were: American University of Science and Technology (AUST), American University of Beirut (AUB), Lebanese American University (LAU), and Haigazian University (HU)

A cluster sample was followed in a sense that 19 questionnaires were given to the administration of Computer Science, ICT, and CCE in order to give it to students to fill them.

6 Results and findings

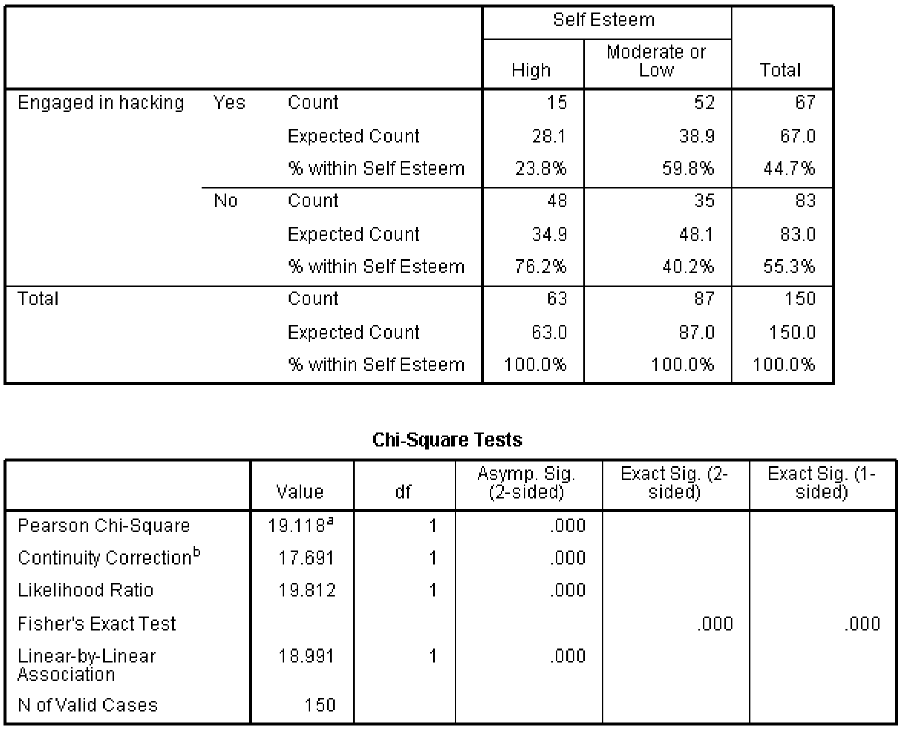
1. **Does having a low or moderate self-esteem influence on the person's motives to perform a hacking activity?**

In inferiority complex theory, we assumed that generally a person who feels like he/she is socially excluded for being a geek, might use his abilities to hack.

For analyzing the data, the following hypothesis is set:

H0: Engagement in hacking and low (or moderate) self-esteem are independent.
H1: Engagement in hacking and low (or moderate) self-esteem are dependent.

For testing this hypothesis using chi-square test, SPSS tool is used to create the cross tabulation. From this table, we get all observed and expected values, as shown in Figure1



			Self Esteem		
			High	Moderate or Low	Total
Engaged in hacking	Yes	Count	15	52	67
		Expected Count	28.1	38.9	67.0
		% within Self Esteem	23.8%	59.8%	44.7%
	No	Count	48	35	83
		Expected Count	34.9	48.1	83.0
		% within Self Esteem	76.2%	40.2%	55.3%
Total		Count	63	87	150
		Expected Count	63.0	87.0	150.0
		% within Self Esteem	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	19.118[a]	1	.000		
Continuity Correction[b]	17.691	1	.000		
Likelihood Ratio	19.812	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	18.991	1	.000		
N of Valid Cases	150				

Fig. 1. The Chi-Square test of Independence between “Involved in hacking” and “self-esteem”

From the top row of the table, Pearson Chi-Square statistic, $\chi^2 = 19.118a$, and $p < 0.001$; i.e., a very small probability of the observed data under the null hypothesis of no relationship. The null hypothesis is rejected, since $p < 0.05$.

Conclusion: Engagement in hacking seems to be related to self-esteem ($p < 0.001$). Going back to the tabulation (Figure 1), note that people with high self-esteem are less involved in hacking (23.8%) than people with moderate/low self-esteem (59.8%). This proves the complex inferiority theory proposed earlier.

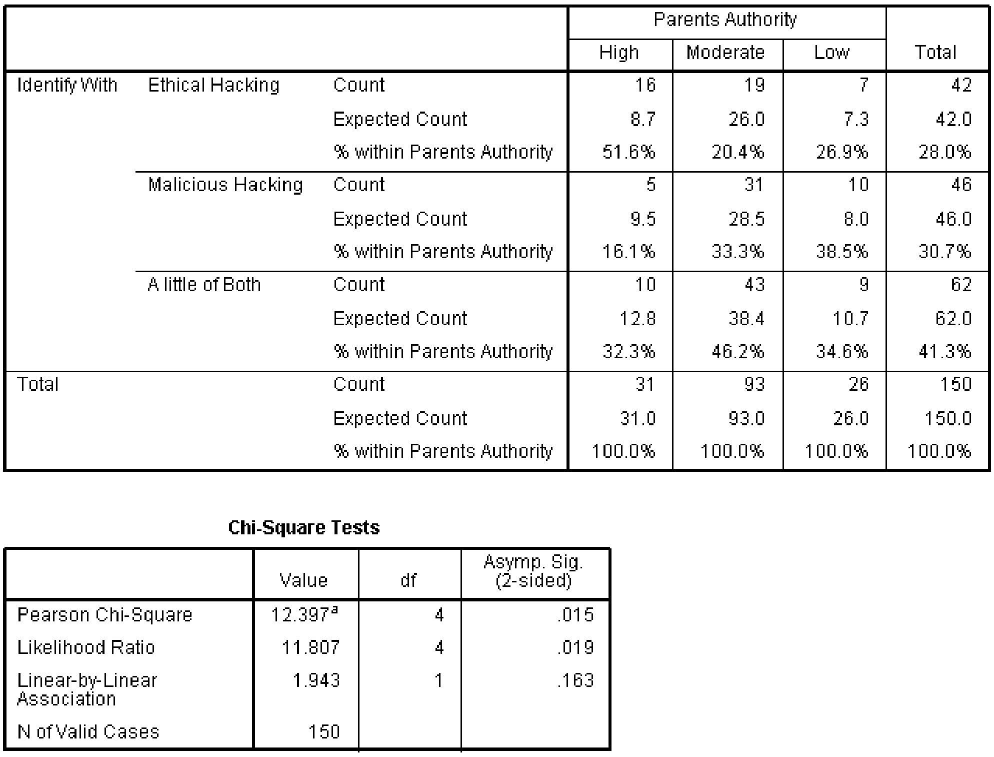
2. Is the level of parental authority related to the type of hacking the human identifies with?

In psychoanalytic theory, we assumed that a person who has a weak super ego, an absence of a parental figure, or a low parental authority tends to perform malicious hacking since there is no moral ground to prevent them.

For analyzing the data, the following hypothesis is set:

H0: “Level of parental authority” and “Type of hacking the human identify with” are independent.
H1: “Level of parental authority” and “Type of hacking the human identify with” are dependent.

For testing this hypothesis using chi-square test, SPSS tool is used to create the cross tabulation. From this table, we get all observed and expected values, as shown in Figure 2



			Parents Authority			Total
			High	Moderate	Low	
Identify With	Ethical Hacking	Count	16	19	7	42
		Expected Count	8.7	26.0	7.3	42.0
		% within Parents Authority	51.6%	20.4%	26.9%	28.0%
	Malicious Hacking	Count	5	31	10	46
		Expected Count	9.5	28.5	8.0	46.0
		% within Parents Authority	16.1%	33.3%	38.5%	30.7%
	A little of Both	Count	10	43	9	62
		Expected Count	12.8	38.4	10.7	62.0
		% within Parents Authority	32.3%	46.2%	34.6%	41.3%
Total		Count	31	93	26	150
		Expected Count	31.0	93.0	26.0	150.0
		% within Parents Authority	100.0%	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.397[a]	4	.015
Likelihood Ratio	11.807	4	.019
Linear-by-Linear Association	1.943	1	.163
N of Valid Cases	150		

Fig. 2. The Chi-Square test of Independence between “Level of parental authority” and “Type of hacking the human identify with”

From the top row of the table, Pearson Chi-Square statistic, χ^2 = 12.397a, and p = 0.015; i.e., a very small probability of the observed data under the null hypothesis of no relationship. The null hypothesis is rejected, since p < 0.05.

Conclusion: “Level of parental authority” seems to be related to “Type of hacking the human identify with” (p = 0.015). Going back to the tabulation (Figure 2), we note that people with high parental authority identify primarily with ethical hacking (51.6%). People with low parental authority identify mostly with malicious hacking. This proves the psychoanalytic theory proposed earlier.

3. Is there a relationship between breaking a vulnerable system for reward and social economic status?

For analyzing the data, two variables were chosen:

1) Income Bracket

2) If vulnerable system discovered would you break it.

Below is a barchart showing the percentage of people with below and above average along with their actions (break or not).

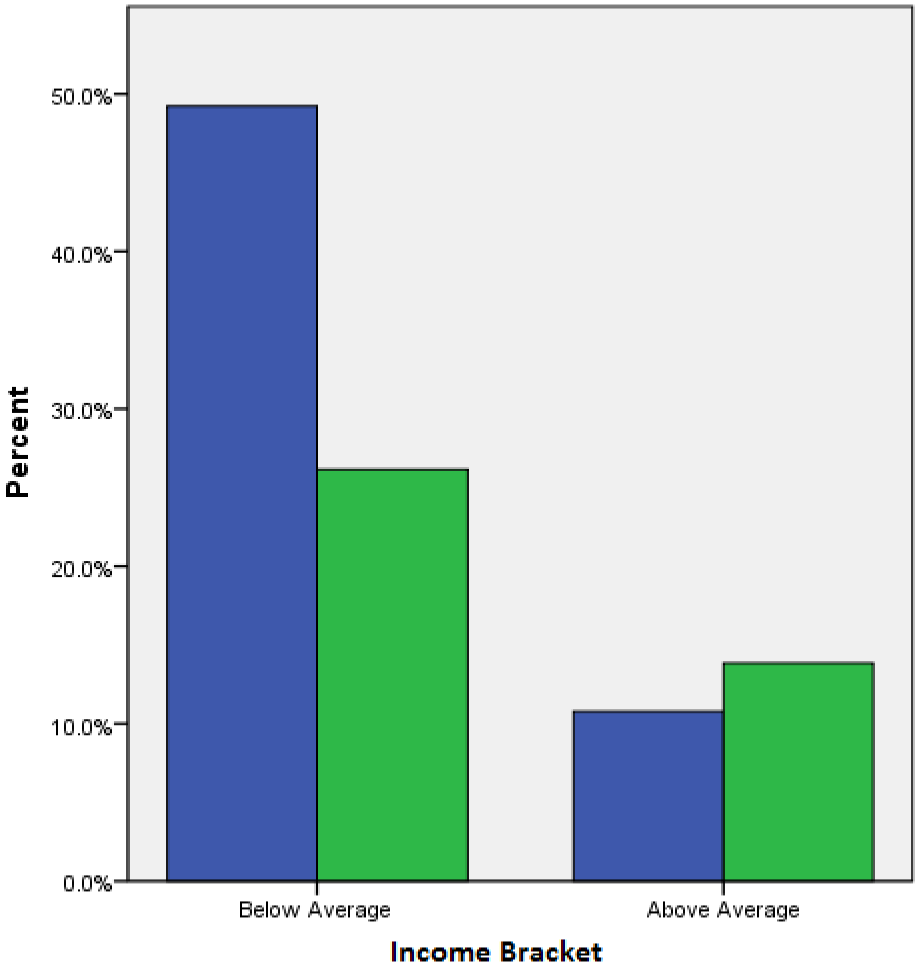


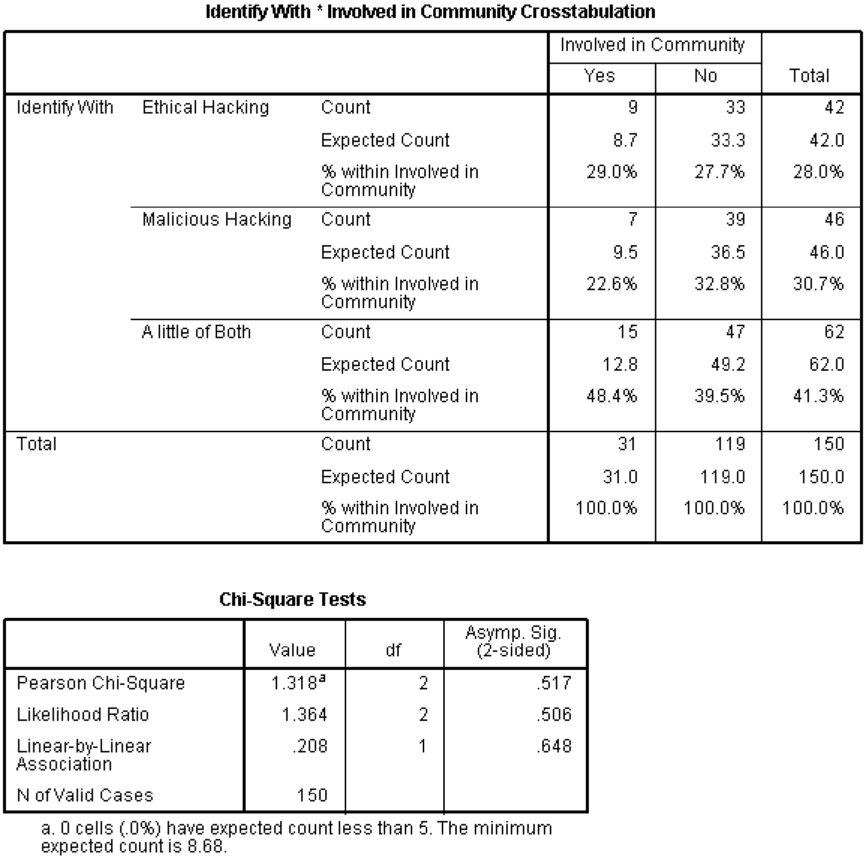
Fig. 3. Barchart showing the percentage of income bracket and performing malicious hacking

From the barchart we can see that people with low income bracket tend to break vulnerable systems more than people with high income bracket. Hence, the economic status plays an important role in determining whether a person might become a malicious hacker or not.

4. Is there an association between people involved in hacking communities and the type of hacking they identify with?

In social learning theory, we assumed that hackers, who are involved in hacking community, tend to learn from each other for good purposes.
For analyzing the data, the following hypothesis is set:

H0: There is no association between people involved in hacking communities and the type of hacking they identify with.
H1: There is an association between people involved in hacking communities and the type of hacking they identify with.
For testing this hypothesis using chi-square test, SPSS tool is used to create the cross tabulation. From this table, we get all observed and expected values, as shown in Figure 4



Identify With * Involved in Community Crosstabulation

			Involved in Community		Total
			Yes	No	
Identify With	Ethical Hacking	Count	9	33	42
		Expected Count	8.7	33.3	42.0
		% within Involved in Community	29.0%	27.7%	28.0%
	Malicious Hacking	Count	7	39	46
		Expected Count	9.5	36.5	46.0
		% within Involved in Community	22.6%	32.8%	30.7%
	A little of Both	Count	15	47	62
		Expected Count	12.8	49.2	62.0
		% within Involved in Community	48.4%	39.5%	41.3%
Total		Count	31	119	150
		Expected Count	31.0	119.0	150.0
		% within Involved in Community	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.318[a]	2	.517
Likelihood Ratio	1.364	2	.506
Linear-by-Linear Association	.208	1	.648
N of Valid Cases	150		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8.68.

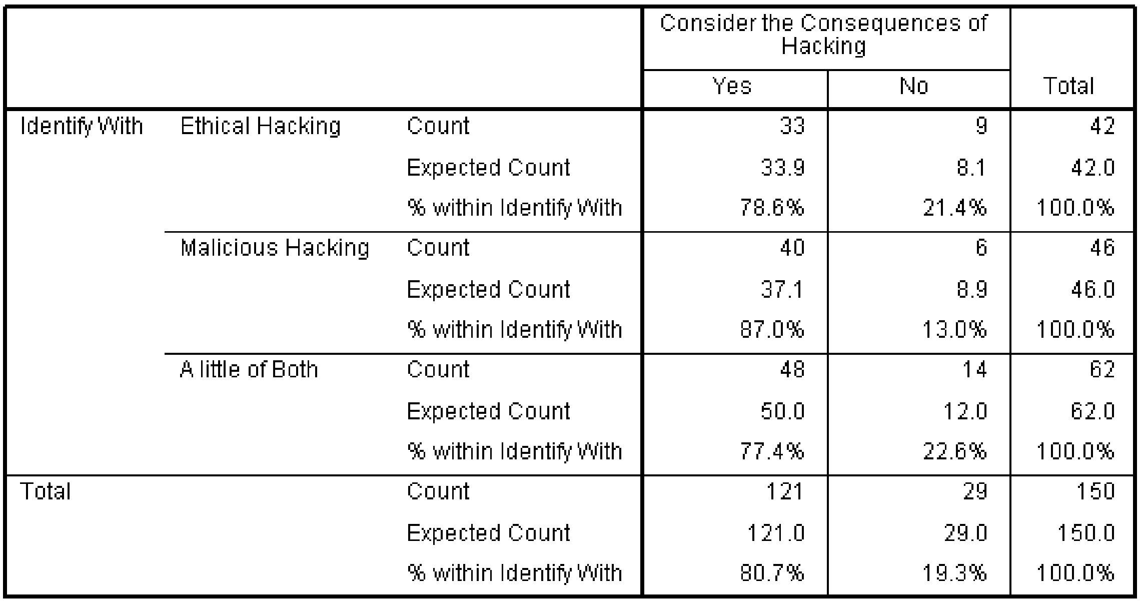
Fig. 4. The Chi-Square test of Independence between “Involved in a community” and “Type of hacking the human identify with”

From the top row of the table, Pearson Chi-Square statistic, χ^2 = 1.318a, and p = 0.517; i.e., a probability greater than 05%. Hence, the null hypothesis is not rejected, since $p > 0.05$.

Conclusion: “Involved in a community” seems not to be related to “Type of hacking the human identify with”. Back to the tabulation (Figure 4), we note that, of the respondents who answered yes on the “Involvement in community” question, we see that 29.0% are involved in hacking for ethical purposes and, 22.6% are involved in hacking for malicious purposes. Hence, the aforementioned Social Learning Theory has been satisfied. As a matter of fact, hackers in a learning community use their skills for the betterment of the society.

5. Is “Considering the consequences of malicious hacking” related to the type of hacking people identify with?

In moral development theory, we assumed that unlike black hat hackers, white hat hackers understand well the consequences and penalties evolved after committing malicious activities.



			Consider the Consequences of Hacking		
			Yes	No	Total
Identify With	Ethical Hacking	Count	33	9	42
		Expected Count	33.9	8.1	42.0
		% within Identify With	78.6%	21.4%	100.0%
	Malicious Hacking	Count	40	6	46
		Expected Count	37.1	8.9	46.0
		% within Identify With	87.0%	13.0%	100.0%
	A little of Both	Count	48	14	62
		Expected Count	50.0	12.0	62.0
		% within Identify With	77.4%	22.6%	100.0%
Total		Count	121	29	150
		Expected Count	121.0	29.0	150.0
		% within Identify With	80.7%	19.3%	100.0%

Fig. 5. Cross tabulation between “Considering the consequences” and “Type of hacking the human identify with”

Interpretation: The above table shows that 1) Of the people who identify with ethical hacking, 78.6% are aware of the consequences, and hence, the result proves the moral development theory. However, 21.4% of ethical hackers still don’t know the consequences. 2) Of the people who identify with malicious hacking, 87.0% are aware of the consequences, yet, still identifying with malicious hacking. This would contradict the moral development theory. Hence, our research shows that this theory has been partially proven.

7 Conclusions

The purpose of the paper is to investigate and assess a sample of 150 respondents’ opinions toward the research questions rewritten herein:

1) Does having a low or moderate self-esteem influence on the person’s motives to perform a hacking activity?
2) Is the level of parental authority related to the type of hacking the human identifies with?
3) Is there a relationship between breaking a vulnerable system for reward and social economic status?
4) Is there an association between people involved in hacking communities and the type of hacking they identify with?
5) Is “Considering the consequences of malicious hacking” related to the type of hacking people identify with?

Results from the descriptive statistics generated from the sample’s responses reveal a mixture of findings with regard to hackers’ psychology. As for the first question, Engagement in hacking seems to be related to self-esteem ($p < 0.001$). Back to the tabulation (Figure 1), note that people with high self-esteem are less involved in hacking (23.8%) than people with moderate/low self-esteem (59.8%). This proves the complex inferiority theory which states that individuals who compensate their feeling of inferiority act in a way that makes them seem predominant.

Regarding the second question, “Level of parental authority” seems to be related to “Type of hacking the human identify with” ($p = 0.015$). Back to the tabulation (Figure 2), we note that people with high parental authority identify primarily with ethical hacking (51.6%). People with low parental authority identify mostly with malicious hacking. This proves the psychoanalytic theory which states that from a psychoanalytic perspective, the criminal behavior in general is a manifestation of a weak Super Ego, criminals are able to commit crimes without feeling guilty, their conscience –or superego- does not work correctly because they were unable to shape a solid and adoring relationship with their parents or parental figure.

For the third question, from the barchart we can see that people with low income bracket tend to break vulnerable systems more than people with average income bracket and above. Hence, the income bracket which is one of the variables of ordering social class plays an important role in determining whether a person might become a malicious hacker or not.

The fourth question reveals that the involvement in a community is not related to the type of hacking human identifies with. Back to the tabulation (Figure 4), we note that, of the respondents who answered yes on the "Involvement in community" question, we see that 29.0% are involved in hacking for ethical purposes and, 22.6% are involved in hacking for malicious purposes. Hence, the aforementioned Social Learning Theory has been satisfied. As a matter of fact, hackers in a learning community use their skills for the betterment of the society.

Results from question five shows that 1) Of the people who identify with ethical hacking, 78.6% are aware of the consequences, and hence, the result proves the moral development theory. However, 21.4% of ethical hackers still don't know the consequences. 2) Of the people who identify with malicious hacking, 87.0% are aware of the consequences, yet, still identifying with malicious hacking. This would contradict the moral development theory.

8 Recommendation

In an attempt to explore the hackers' mindset, its motives, and the psychological drives that stimulate the act of hacking, this study focuses on analysing various theories from the field of psychology to correlate them to different types of hackers. It also investigates the relationship between hacking and self-esteem, high parental authority, low income bracket, social learning, and consequences of hacking. A significant amount of the sample responses with high self-esteem seems to be less engaged with hacking compared to those respondents who have low self-esteem. Moreover, those respondents who have low parental authority tend to commit cyber-crimes without feeling guilty since their conscience does not work properly due to a weak Super Ego as they were unable to shape a solid and adoring relationship with their parental figures. Furthermore, low income bracket respondents have a tendency to break a computer system more than people with average income bracket and above. Likewise, hackers in a learning community appear to use their skills for the benefit of the society. And although malicious hackers are aware of the hacking consequences, yet they are still practicing it.

This leads us to recommend that organizations and institutions should be carefully selective when hiring fresh graduates as potential employees. We assume that they have to assign them professional tests designed by psychologists to assess their motives and drives. Their self- esteem has to be measured, their parental authority has to be questioned, their involvement in a community has to be identified, and the awareness of the consequences of malicious hacking carefully estimated.

Other implications from the current research stress that the evaluation process is complicated and the evaluation survey differs from samples selected from academy to industry. Therefore the challenge for future research is to continue with the study of the effectiveness and validity of the current research by using further classifications and clustering analysis.

References

1. Hackers Profiling. UNICRI. [online] Available at: http://www.unicri.it/special_topics/securing_cyberspace/current_activities/hackers_profiling/
2. Stonebridge.uk.com. Stonebridge - Centre Site. [online] Available at: https://www.stonebridge.uk.com/category/psychology (2016)
3. Sans.org. The Role of Static Analysis in Heartbleed. [online] Available at: https://www.sans.org/reading-room/whitepapers/threats/role-static-analysis-heartbleed-35752 (2016).
4. Venue, C.. A guide to computer hacking including vulnerabilities, hacking tools, cybercrime, hacker ethics such as White Hat, Black Hat, Grey Hat, and more. [United States]: [Webster's Digital Services]. (2012)
5. SearchSecurity. What is white hat? - Definition from WhatIs.com. [online] Available at: http://searchsecurity.techtarget.com/definition/white-hat
6. Niharika1 & Ranjeet Kaur2. Honeypots For Network Surveillance. International Journal of Research in Engineering & Technology ISSN(E): 2321-8843; ISSN(P): 2347-4599 (2014)
7. Tim Tech Support. State Sponsored Hacking and Cyber Security Policy. [online] Available at: http://timourrashed.com/state-sponsored-hacking-and-cyber-security-policy (2012)
8. A. Kiyuna, L. Conyers. Cyberwarfare Sourcebook (2015)
9. Kaushik, A. Sailing safe in cyberspace. (2013)
10. Trier, T. Intelligence-based security in private industry. (2015)
11. SearchSecurity. What is gray hat (or grey hat)? - Definition from WhatIs.com. [online] Available at: http://searchsecurity.techtarget.com/definition/gray-hat (2016)
12. Webster's new college dictionary. Boston: Houghton Mifflin Harcourt. (2008)
13. Wiktionary. id. [online] Available at: https://en.wiktionary.org/wiki/id
14. Lapsley, D. and Narváez, D. Moral development, self, and identity. Mahwah, N.J.: Lawrence Erlbaum Associates. (2004)
15. Wiktionary. geek. [online] Available at: https://en.wiktionary.org/wiki/geek
16. Kennedy, F., Kennerley, H. and Pearson, D. (n.d.). Cognitive behavioural approaches to the understanding and treatment of dissociation.
17. Blackman, D.. Operant Conditioning: An experimental analysis of behaviour. London: Methuen. (1974)
18. Ercetin, S. (n.d.). Chaos, complexity and leadership 2014.
19. Sellers, C., Winfree, L. and Akers, R. Social learning theories of crime. Farnham, Surrey, England: Ashgate. (2012)
20. Goldman, M. Kleptomania. Far Hills, N.J.: New Horizon Press. (1998)
21. Yochelson, S. and Samenow, S. (n.d.). The criminal personality. Northvale, N.J.: Jason Aronson.