IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 61-63
www.iosrjournals.org

The Legality of Ethical Hacking

OMOYIOLA Bayo Olushola
Corresponding Author:OMOYIOLA Bayo Olushola

Abstract: *The legality of ethical hacking has been a topic of debate. Over the years, malicious hacking has given hacking a bad name but from the beginning hacking was not intended to be a criminal activity. Though hacking could be malicious, it could also be ethical, legal and acceptable. In this paper, we analyse the legality and acceptability of ethical hacking and why it is not a criminal activity.*

Keywords*: Hacking, Ethical hacking, Computer crime, Criminal activity, Malicious hacking, Crime.*

Date of Submission: 10-01-2018 Date of acceptance: 26-01-2018

I. Introduction

Ethical hacking is not a criminal activity. It is a legally accepted hacking that is not a crime. Some form of hacking are not necessarily a crime. For instance, intelligence gathering which is the first stage of hacking is not necessarily a crime. The reason is because the information collected in the process could be used for research purposes, rather than for malicious purposes. In the case of ethical hacking, itis authorized and legally accepted. Unlike malicious hacking like unauthorized access, unauthorized privilege escalation andunauthorized penetration testing(Choo, 2011; Won, Ok-Ran, Chulyn&Jungmin, 2011).

1.1The Acceptability of Ethical hacking

Ethical hacking is not a crime. Just as hacking was not a crime from the beginning when true hacking was linked with studying programming languages and computer systems with the hope of creating new innovations to solve problems. Ethical Hacking shouldn't be regarded as a crime because it is legal, authorized and acceptable. In the beginning, hacking was regarded as a form of tinkering. It was a process that involved making changes to something in order to get something new. However,people's perception and motivation about hacking has changed over the years. Initially, hackers were people who sought to understudy computers thoroughly. These set of people brought about innovation and technological breakthroughs as a result of their activities. Hackers were responsible for almost every innovation, invention and technological breakthrough. They were responsible for the invention of personal computers and even the World Wide Web. The first set of hackers did not break laws because true hackers align with code of conducts and regulations. The motivation of hackers was essentially about renovating existing program codes and making them more efficient.Not all forms of hacking are illegal. Some hacking processes could be compared to what happens when the owner of a car mistakenly locks his car key inside his car and tries other means to open the door. He could do this forcefully and/or tactically. One could also liken some hacking processes to downloading. The internet has billions of users accessing it regularly. There are billions of computers and networks connected to the internet. People online access millions of websites and millions of software. Everyone online seem to be engaged in one form of downloading or the other. Some form of downloading have been considered as illegal but that does not mean that downloading should be regarded as a crime. People all over the world visit google.com every day searching for information. If information gathering was a crime, google would not be in existence today. In the same vein, not all form of hacking are crimes because not all cases are harmful. Antonio Mille, a judge in Argentina ruled that hacking was not a crime, claiming that hacking does not harm people, things and animals (Elsevier, 2002). Ethical hacking should not be regarded as a crime because it is not offensive in nature.It is carried out by ethical hackers that do not use their hacking skills for destructive, offensive or harmful purposes. Rather they use it for defensive purposes (Conrad, 2012; Cooper, 2016). Such hackers are known as white hats. They are different from black hats, green hats, blue hats, suicide hackers and script kiddies who are engaged in malicious attacks (Cooper, 2016). Rather than use their hacking expertise for evil purposes, they use it to protect systems and users. They are professional and ethical hackers. There is another set of good hackers who do not engage in destructive purposes. They are known as red hat hackers. These red hat hackers use their hacking skills for rendering consultancy services such as penetration tests and vulnerability assessments. They are similar to white hat hackers. They shut down the activities of black hats or malicious hackers (Bowles, 2012).Ethical hacking should not be regarded as a crime for all the reasons mentioned. More so, because ethical hacking activities does not include illegal processes such as gaining unauthorized access, illegal privilege escalation, unauthorized attacking, illegal maintaining access and unauthorized covering track (Caldwell, 2011; Choo, 2011; Won, Ok-Ran, Chulyn&Jungmin, 2011).

1.2Computer Crime Definition

Computer crime is defined by US Department of Justice as, "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution" (Fehr, Licalzi& Oates, 2016; Licalzi, 2017; McCurdy, 2010). Computer crime is also called cybercrime. It portrays criminal activity that has computers or networks as a tool, target or place of activity. A computer could be the subject of a crime when it is stolen or damaged. It could also be the site of a crime or the instrument of a crime. Cybercrimes make use of networks but Computer crimes may or may not make use of networks. These computer crimes include the traditional crimes carried out with the utilization of a computer and new computer crimes that has evolved as a result of new computer technologies and the growth of the internet. Cyber-attacks could be hard to stop. These includes the spread of malwares and viruses on the internet (Deibert, 2015; Farwell &Rohozinski, 2011; Katos&Bednar, 2008; Kshetri, 2013). In order to curtail these new crimes, prosecutors utilize technology specialized legislation passed into law by the congress and conventional law that regulates cyberspace activities (Licalzi, 2017; McCurdy, 2010; Pelker, Palmer and Agosti, 2015). Computer crimes include identity theft, fraud and cyber-attacks (Broadhurst, 2006: McCurdy, 2010). Cyber-attacks also includes cyber bullying and cyber terrorism (Furnell& Warren, 1999; Levi, 2008; Rossouw& Johan, 2013; Sukhai, 2004).

Table 1: Computer crimes

S/N	Traditional Crime	Computer Crime
1	Larceny/Theft - Stealing	Stealing of computer parts; Computer-related identity theft in which the hacker pretends to be the actual owner; Phishing; And Cyber theft
2	Fraud: Intentional deceit	Computer-related fraud that causes loss of property as a result of alteration or deletion of data or interference with system. This could be scam, card fraud, auction fraud or retail fraud.
3	Child Pornography: Kid porn	Producing child pornography or distributing it or procuring it through a computer or having it on a computer
4	Forgery: Alteration	Computer-related forgery in which there is alteration or deletion of data resulting in a fake or falsified document. Issuing false documents through computers
5	Piracy and Infringement: Copyright, Intellectual property infringement	Computer-related intellectual property (IP) infringements (such as copyright infringements and IP rights thefts)
6	Arson: Deliberate setting on fire	Making a computer centre a target for damage by fire
7	Conspiracy: Act of plotting	Agreement to execute an illegal act on a computer
8	Espionage/Sabotage	Spying, stealing and destruction of the record of rivals/competitors
9	Burglary: Stealing	Stealing computer parts by breaking in
10	Stalking: Harassment	Cyberstalking: A form of harassment on e-mail and internet
11	Bullying: Fighting	Cyberbullying: Infliction of emotional injury using computer
12	Gambling: Game of luck	Playing of games and betting online for financial rewards on system
13	Blackmailing: Demanding	Act of demanding money in order to hide confidential information through system
14	Extortion: Obtaining money	Obtaining money by threatening to destroy a computer
15	Counterfeiting: Producing fake	Utilizing a computer to produce false duplicates
16	Malware Attacks: Malicious acts	Attacking computers with malicious software
17	Electronic Money Laundering: Financial fraud	Computer-related transfer of illicit funds on the internet

1.2 Criminal Activity Discussion

Criminal activity occurs when criminal law is violated. The examples of computer highlighted and analysed in Table 1 above are criminal activities. These criminal activities are believed to be injurious to the welfare of the public and are legally prohibited. The Council of Europe (CoE) convention and other computer acts have criminalized hacking by criminalizing unauthorized and illegal access (Broadhurst, 2006). Malware attacks, forgery, child pornography, piracy and IP infringements, theft, fraud, arson, conspiracy, espionage, sabotage, burglary, extortion, electronic money laundering, blackmailing, cyberstalking and cyber bullying are criminal activities. They are criminal offences because they are against the law. Some of them are attacks against Confidentiality, Integrity and Availability. While some of the crimes like Fraud, Child Pornography, Counterfeiting, Gambling etc. describes criminal activity that has computers or networks as a tool, other crimes like Forgery, Extortion, Conspiracy, Espionage, Sabotage, Theft describe criminal activity that has computers as a target while Intellectual Property Infringement describes criminal activity that has computers or networks as a place of activity (Machin&Meghir, 2004).

1.3 Hacking definition and explanation

In today's world, most people see hacking as unauthorized access into computer systems and networks. Though it is not supposed to be so. Initially hacking was all about studying programming languages and computer systems with the hope of creating new innovations and program codes to solve problems. It was a kind of tinkering which people engaged in order to produce something new. It was about understanding computers thoroughly, and making innovation and technological breakthroughs. Ethical hacking is not about breaking laws. Ethical hacking is authorized and therefore align with regulations. In today's world, some nerds indulge in malicious hacking. They identify weaknesses in computer systems and gain access into them by exploiting the weaknesses. These unauthorized hacking is carried out by malicious hackers. The malicious hackers are threat agents who engage in hacking based on motivation, opportunity and capability. The threat agents (hackers) engage in hacking, having the capability or power to hack. They have hacking tools and they are very skilled and can carry out a threat. The threat agents also act based on motivation. The hackers carry out threats based on different motives. The motivation could be gain, power, revenge, curiosity or politics. The motive behind their actions could also be terrorism or religion etc. The threat agents also carry out threats based on opportunity. Before the threat agent exploits a target, an opportunity must present itself (Vidalis, Jones & Blyth, 2004). However with ethical hacking which is an authorized and legal form of hacking, it is not so.

II. Conclusion

In conclusion, ethical hacking is not a criminal activity and should not be considered as such. While it is true that malicious hacking is a computer crime and criminal activity, ethical hacking is never a crime. Ethical hacking is in line with industry regulation and organizational IT policies. Malicious hacking should be prevented while ethical hacking which promotes research, innovation, and technological breakthroughs should be encouraged and allowed.

References

[1]. Bowles, M. (2012). The business of hacking and birth of an industry. Bell Labs Technical Journal, 17(3), pp.5-16. doi: 10.1002/bltj.21555

[2]. Broadhurst R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), pp.408-433. doi: 10.1108/13639510610684674

[3]. Caldwell T. (2011). Ethical hackers: Putting on the white hat. Network Security. 2011(7), pp.10-13. doi: 10.1016/s1353-4858(11)70075-7

[4]. Choo K.R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(2011), pp.719-731. doi:10.1016/j.cose.2011.08.004.

[5]. Conrad J. (2012). Seeking help: The important role of ethical hackers. Network Security. 2012(8), pp.5-8. doi:10.1016/s1353-4858(12)70071-5

[6]. Cooper, M. (2016). Adventures in Ethical Hacking. ITNOW, 58(3), pp.36-37. doi:10.1093/itnow/bww074

[7]. Deibert R. (2015). Cyberspace under siege. Journal of Democracy, 26(3), pp.64-78.

[8]. Elsevier B.V (2002). In argentina, judge ruled that hacking is not a crime, Computer fraud & security, 2002(5), p.20. doi: 10.1016/S1361-3723(02)00518-3

[9]. Farwell J.P., Rohozinski R. (2011). Stuxnet and the future of cyber war. Survival. 53(1), pp.23-40. doi: 10.1080/00396338.2011.555586

[10]. Fehr C., Licalzi C., Oates T. (2016). Computer crimes. The American Criminal Law Review, 53(4).

[11]. Furnell, S.M. and Warren, M.J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? Computers & Security, 18(1), pp.28-34. doi: 10.1016/S0167-4048(99)80006-6

[12]. Jones A. (1997). Penetration testing and system audit – experience gained during the investigation of systems within the uk. Computers & Security, 16(7), pp.595-602. Doi: 10.1016/s0167-4048(97)80796-1

[13]. Katos V., Bednar P.M (2008). A cyber-crime investigation framework. Computer standards & interfaces. 30(4), pp.223-228. doi: 10.1016/j.csi.2007.10.003

[14]. Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electronic Commerce Research, 13(1), pp.41-69. doi: 10.1007/s10660-013-9105-4

[15]. Levi, M. (2008). White-collar, organised and cyber-crimes in the media: Some contrasts and similarities. Crime, Law and Social Change, 49(5), pp.365-377. doi: 10.1007/s10611-008-9111-y

[16]. Licalzi C. (2017). Computer crimes (thirty second annual survey of white collar crime). American Criminal Law Review. 54(4).

[17]. Machin, S. and Meghir, C. (2004). Crime and economic incentives. Journal of Human Resources, 39(4), pp.958-979.

[18]. McCurdy J.L. (2010). Computer crimes. The American criminal law review, 47(2). pp.287-382

[19]. Pelker C., Palmer A.J., Agosti J. (2015). Computer crimes. The American criminal law review, 47(2). pp.793-822

[20]. Rossouw V.S., Johan V.N. (2013). From information security to cyber security. Computers & security.38. pp.07-102. doi: 10.1016/j.cose.2013.04.004

[21]. Sukhai, N.B. (2004). Hacking and cybercrime. InfoSecCD Proceedings of the 1st annual conference on Information security curriculum development, ACM. pp. 128-132. doi: 10.1145/1059524.1059553

[22]. Vidalis S., Jones A., Blyth A. (2004). Assessing cyber-threats in the information environment. Network Security, 2004(11). pp. 10-16. doi: 10.1016/S1353-4858(04)00156-4

[23]. Won K., Ok-Ran J., Chulyn K., Jungmin S. (2011). The dark side of the internet: Attacks, costs and responses. Information Systems. 36(2011), pp.675-705. doi:10.1016/j.is.2010.11.003

* OMOYIOLA Bayo Olushola,"The Legality of Ethical Hacking." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 61-63.