# Essay title: Is Ethical Hacking Truly Ethical?

**Name:** Joseph Cherian

**Student ID number:** 19210222

**Email address:** joseph.cherian2@mail.dcu.ie

**Programme:** MCM1

**Module code:** CA640

**Date of submission:** 15.11.2019

**Word count: ~**2500 (excluding disclaimer, bibliography, citations)

**Disclaimer:**

An essay submitted to Dublin City University, School of Computing for module CA640 Professional and Research Practice, 2018/2019.

I understand that the University regards breaches of academic integrity and plagiarism as grave and serious. I have read and understood the DCU Academic Integrity and Plagiarism Policy. I accept the penalties that may be imposed should I engage in practice or practices that breach this policy.

I have identified and included the source of all facts, ideas, opinions, viewpoints of others in the assignment references. Direct quotations, paraphrasing, discussion of ideas from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the sources cited are identified in the assignment references.

I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

By signing this form or by submitting this material online I confirm that this assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study. By signing this form or by submitting material for assessment online I confirm that I have read and understood DCU Academic Integrity and Plagiarism Policy (available at: http://www.dcu.ie/registry/examinations/index.shtml)

Name: Joseph Cherian

Date: 28-10-2019

1. An introduction to the case

**Ethical hacking** is a term used to describe hacking performed by a company or individual which helps in identifying potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the company to improve the system security, to minimize or eliminate any potential attacks. The main difference between ethical hacking and hacking is the legal implementation of ethical hacking to provide the solution of making unauthorized hacking attacks within an organization to access other systems. The company follows it as it follows some rules and regulations. Due to the indifference in unethical hacking activities, ethical hacking is established. It is becoming more common that many institutions offer courses for ethical hackers nowadays. Unless this hacking process is excluded, many problems will arise in the future, changing the entire data in the company will cause illegal actions to be carried out. The company's reputation is destroyed through it. An ethical hacker changes the actual content of the data in certain cases which is one of the main problems of ethical hacking. (ComputerHope, n.d.) (EssayBot, n.d.)

2. A review of the literature on the subject

Organizations have sensitive information that they protect which can include credit card information, source code for a software program or a password for entering the system of an organization. CEO of the organization is responsible for ensuring that the organization’s sensitive information is kept protected. Consequently, to protect their sensitive information, many CEO’s have attempted to ensure that their organizations follow standards such as ISO27002, King and COBIT as often as possible.

2.1 Methods that are currently used by companies to secure information

It is expected that all communication systems, including applications, infrastructure and networking services, are protected from incidents and abuse which can be achieved through employing a set of safety measures. This will ensure that the communication systems and application are available, reliable, trusted, safe, identifiable and auditable. These measures are vital in economic terms.

Another safety measure that is used by organisations to secure information is risk management. Chichakli (2009) defines risk management as the process of identifying risk, accessing risk and taking steps to reduce the risk to an acceptable level. (Academia, n.d.)It is a process that allows IT managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that protects their organizations mission.

Other measures that businesses used to protect their information include installing and activating software firewalls on all their business systems and patching operating systems and applications.

2.2 The use of ethical hacking to secure the information in a company

According to Graves (2010) ethical hacking is a process in which security professionals use their hacking skills and tools to defend and protect information of a business. The process of testing the security of a network is known as penetration testing (Graves, 2010). The process of penetration testing can be divided into four phases: planning, discovery, exploitation and reporting

* Initially at the planning phase, the assignment scope is defined. Under the guidance of responsible legal departments and lawyers; management approvals, documents and agreements like NDA (Non-Disclosure Agreements) are signed.
* The discovery phase is also known as information gathering phase. During the information gathering process the penetration testing team launches scanning enumeration procedures to gain as much information as possible about the target network and the participating networks and services.
* The third phase of a penetration test is the exploitation phase. Using the discovered vulnerabilities arriving from the previous phase as an input, the penetration testing team revises the matching proof-of-concept exploits that may lead to a system or service security bridge.
* The last phase that completes a penetration process is the reporting phase. A successful report details all the findings and their impact to the company by taking into account both the technical and management aspects in its format.

Ethical hackers simulate how an attacker with no inside knowledge of a network might try to penetrate and believe their activities benefit society by exposing system weaknesses-stressing that if they can break these networks so could terrorists. The result has not only enhanced local security for the ethical hacker but also enhanced overall internet security. (Academia, n.d.)

3.Liffick's analysis of the case

3.1. Main Participants and Actions

3.1.1 Primary Participants

* Ethical Hackers (White hat hackers)
* An ethical hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer network or other computing resource on behalf of its owners (generally organisation) and with their permission to find security vulnerabilities that a malicious hacker could potentially exploit.
* The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in networks. It includes finding any vulnerabilities and to determine whether any unauthorised access is possible or not.
* Ethical hackers use their skills to bypass the organisation’s security. However instead of taking advantage of the vulnerabilities in the IT security, they document them and try to provide solutions so that organizations can try to fix them. (TechTarget, n.d.)
* Organisation (Company)
* Companies especially small companies are becoming targets of computer criminals and these criminals compromise the information of the companies. The information gets stolen or damaged and the current security measures that the companies are using such as firewalls, anti-viruses and password encryption are not adequate. The companies can adopt ethical hacking in order to assist in addressing the current security problems that they are facing. Ethical hacking can provide companies with improved data protection along with productivity thus enabling them to be more competitive. (Academia, n.d.)

**3.1.2 Secondary Participants**

* **Black hat hackers**

Black Hat hackers are criminals who break into computer systems with malicious intent. They may destroy files, hold computers hostage, or steal passwords, credit card numbers, and other personal information by releasing malware. Ethical hackers are hired by organizations to test their security against the black hat hackers. (kaspersky, n.d.)

**3.1.3 Implied Participants**

* General Services Administration(GSA)
* The "penetration test" service has been standardized by the General Services Administration (GSA) as a pre-vetted support service, to rapidly address potential vulnerabilities, and stop adversaries before they impact US federal, state and local governments. These services are referred to as Highly Adaptive Cybersecurity Services (HACS) and are listed at the US GSA Advantage website.
* The key service providers which have been technically reviewed and vetted to provide these advanced penetration services have been identified by this effort. The improvement in the rapid ordering and deployment of these services, reduction in the US government contract duplication, and protection and support of the US infrastructure in a more timely manner have been intended by this GSA service. (wikipedia, n.d.)

#### 3.2 Reduced List of Participants

 Actions are not mentioned as they are already mentioned above.

**3.2.1 Secondary Participants**

* **Black hat hackers**

**3.2.2 Implied Participants**

* General Services Administration(GSA)

3.3 Legal Considerations

The legal risks of ethical hacking include lawsuits due to disclosure of confidential information. Such disclosure can lead to a legal battle involving the company and the ethical hacker. It is very easy for ethical hacking to result in a legal battle if it is not properly performed. It is also possible for the ethical hacker to commit errors to the point that the company’s profitability is negatively affected.

The company could sue the ethical hacker for failing to perform properly, in such a case. The ethical hacker could be at legal risk if proper care and precaution are not taken seriously. To address these legal issues, it is imperative for the ethical hacker to always perform his job defensively to minimize compromising the client’s network. Defensive performance emphasizes extra caution and prevention in ethical hacking. (Ethical Hacking Code of Ethics: Security, Risk & Issues, n.d.)

3.4 Possible Options for Participants

* Ethical Hackers (White hat hackers)
* Try to be sincere and ethical in their work by not trying to steal or damage the information in the organization network.
* Organisation (Company)
* Try to improve the security of their network as much as possible to prevent black hat hackers from invading into their network.
* Monitor the activities of the ethical hackers thoroughly and try to block access to the part of the network they might not require for their activity.

3.5 Possible Justifications for Actions

* Ethical Hackers (White hat hackers)
* Hired by the organisations to check the security of the network in an organisation and to provide the solutions.
* Organisation (Company)
* It is impossible to prevent black hat hackers from stealing or damaging vital information in their network using security measures such as firewalls, anti-viruses and password encryption
* To check the security of the network in an organisation and to provide solutions a suitable resource is required. Hence ethical hackers are hired by organisations.

3.6 Key Statements

I was addicted to hacking, more for the intellectual challenge, the curiosity, the seduction of adventure; not for stealing, or causing damage or writing computer viruses.

- Kevin Mitnick

But we are HACKERS and hackers have black terminals with green font colors.

- J. Nunemaker

Hackers are actually good, pleasant and extremely intelligent people who could keep computer criminals on the run.

- Ankit Fadia (The Hackorial, n.d.)

3.7 Questions raised

What if the ethical hacker performs unethical actions during the course of the hacking task? (Do Ethical Hackers Need Legal Protection?, n.d.)

What if a solicited hacker may exceed the scope of work and venture into software sections not allowed as per the agreement? (Do Ethical Hackers Need Legal Protection?, n.d.)

What is the importance of securing information in companies?

3.8 Analogies employed

1.Brute Force Attacks

Brute force in computing can consist of a hacker in a short period of time trying to use as many passwords as possible to get in. This method of attack is quite devastating when it’s effective as there are programs that can randomly generate countless passwords in seconds.

2.Social Engineering

Social engineering takes a calculated approach to data theft and hacking. Hackers will take the identity of someone you think you can trust with this information, like an old friend or your elderly grandmother and make personalised attempts to steal your passwords.

3.Security Exploits

Security exploits are weaknesses in software on your computer that allow hackers to access your system and create all kinds of problems. These can range from particular lines of code that create problems for your organization to weaknesses in the way that sensitive information is handled. Ultimately, to allow a hacker into your infrastructure it only takes a single crack in your defences a security exploit.

4.Trojan Horse

Just like the Greek horse of old, a Trojan sneaks onto your network and plants a backdoor, allowing for secret re-entry later. Often times, a Trojan will use a data breach to mask its presence, and then continue to steal information in small doses as time goes on.

5.Two-Factor Authentication

Two-factor authentication can be used to provide this secondary credential to your online accounts or network logins. A secondary code can be sent to an email address or mobile device, which allows employees to access critical information using both these credentials. (caiservice, n.d.)

### 3.9 Codes of Ethics Utilised

Codes of ethics for ethical hacking are focused on the duties, responsibilities and limits of the ethical hacker in doing his job. The ethical hacker must make sure that the client’s system is properly evaluated for security issues and vulnerabilities.

1. Before performing any ethical hacking, ensure that you understand and know the nature and characteristics of the client company’s business, system and network. This will guide you in handling sensitive, confidential or proprietary information you might handle while doing ethical hacking.
2. Before and while doing ethical hacking, determine the sensitivity of the information involved. This should ensure that you do not violate laws, rules and regulations in handling confidential personal, financial or proprietary information.
3. During and after ethical hacking, always maintain transparency with the client. Communicate all pertinent information you found while ethically hacking the client’s network. Transparency ensures that the client knows what is going on while hacking. Transparency enables the client to take necessary actions for security of the network.
4. Do not go beyond the limits set by the client while performing ethical hacking. It is possible for you to have access beyond the target areas that the client signed up for, in ethical hacking. Stay within the target areas of the network specified in the work agreement. Do not go to other areas or components of the network that are not specified in the agreement. Minimize exposure of confidential information. Increase your trustworthiness as an ethical hacker. The ethical hacker must ensure the overall effectiveness of the activity. (Ethical Hacking Code of Ethics: Security, Risk & Issues, n.d.)

## 3.10 Alternative proposals

### Pessimistic

### Organizations could try to improve their network security by using strong password encryption and firewalls. In this way they could avoid having an ethical hacker to test their network security against malicious hackers.

### Optimistic

* Ethical hackers try to improve the security of an Organisation’s network and provide solutions by using some tools.
* Hence the ethical hackers must follow certain ethics by not misusing or stealing the information in the organisation network and the organisation must ensure they monitor the activities of the ethical hacker.
* The organisation must provide only the necessary access to the ethical hackers.
* The organisation must take necessary action if any unethical activities are noticed from an ethical hacker

### Compromise

* Ethical hackers must find the loopholes in the organisation’s network and provide solutions to fix the loopholes. They should ensure they are not misusing or stealing the information in the organisation’s network.
* The organisation must provide only the access required by the ethical hacker and monitor the activities of the ethical hacker.

### 3.11 The Ethical Theory That Had Most Influence Over Your Conclusions

Falk (2014) examined ethical objections to grey hat hacking using the ethical theories: utilitarianism, Kant’s maxims and categorical imperative, and Aristotle’s virtue ethics.

The ethical theory that had most influence on my conclusions is utilitarianism.

Utilitarianism considers the outcomes of an action and asks whether it optimizes pleasure while minimizing pain. Because only black hat hacking seeks to increase the pain inflicted on other parties (typically technological or political), it is the only variant of hacking considered unethical in terms of utilitarianism. (pdf\_ethical\_theories, n.d.)

3.12 Conclusion

Companies hire ethical hackers as they need to test their security against black hat hackers, whose evil activities serve their own ends ranging from financial gain to simply causing chaos. By granting them permission to the penetration test, they effectively cover their organisation eyes and ears while these tests are carried out. And at the end of the penetration test, the ethical hacker presents a nicely polished report pointing out the weaknesses and associated recommendations. What the organisation has no idea about is how many laws they have enticed the ethical hacker to break to get to this point. The ethical hacker more importantly, may not care about the laws that have been broken or may not know the laws that have been broken. (IAN SUTHERLAND, n.d.)

# Bibliography

1.(n.d.). Retrieved from EssayBot: https://www.essaybot.com/sample/essays/detail?id=136664&query=Computer%20Ethics

2.(n.d.). Retrieved from ComputerHope: https://www.computerhope.com/jargon/e/ethihack.htm

3.(n.d.). Retrieved from IAN SUTHERLAND: https://ianhsutherland.com/ethical-hacking/

4.(n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Penetration\_test#cite\_note-20

5.(n.d.). Retrieved from kaspersky: https://www.kaspersky.com/resource-center/threats/black-hat-hacker

6.(n.d.). Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/ethical-hacker

7.(n.d.). Retrieved from The Hackorial: http://hackorial.blogspot.com/2014/12/top-10-hacking-quotes.html

8.(n.d.). Retrieved from caiservice: https://www.caiservice.com/blog/5-security-analogies-to-help-you-better-understand-hacking

9.(n.d.). Retrieved from pdf\_ethical\_theories: https://arxiv.org/ftp/arxiv/papers/1512/1512.02707.pdf

*10.Do Ethical Hackers Need Legal Protection?* (n.d.). Retrieved from techopedia: https://www.techopedia.com/do-ethical-hackers-need-legal-protection/2/33135

*11.Ethical Hacking Code of Ethics: Security, Risk & Issues*. (n.d.). Retrieved from panmore: http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

*12.THE ADOPTION AND USE OF ETHICAL HACKING TO SECURE INFORMATION IN SMALL COMPANIES*. (n.d.). Retrieved from Academia: https://www.academia.edu/29496652/THE\_ADOPTION\_AND\_USE\_OF\_ETHICAL\_HACKING\_TO\_SECURE\_INFORMATION\_IN\_SMALL\_COMPANIES

13. <https://www.lawteacher.net/free-law-essays/business-law/netscape-microsoft-antitrust-lawsuit-2927.php>

e vs Microsoft Antitrust Lawsuit,

# d