International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 07
July 2022

Ethical Hacking - Comparative Study between Different Countries

Pavan Patil, *Student, Department of Computer Applications, IFIM College, E City, Bangalore*

Naveen Kumar, *Student, Department of Computer Applications, IFIM College, E City, Bangalore*

Ajmal S, *Student, Department of Computer Applications, IFIM College, E City, Bangalore*

Yiga Raymond, *Student, Department of Computer Applications, IFIM College, E City, Bangalore*

Prof. Sunetra Chatterjee, *Assistant Professor, Department of Computer Applications, IFIM College, E City, Bangalore*

Abstract:
Ethical hacking is a technique used by an individual or a company to detect the potential threats on a computer or network. A person who performs these techniques is called an ethical hacker. An ethical hacker acts as hacker but in an ethical way. An ethical hacker analysis the code used in the system and detects the weak points where hacking is possible. Then provides the information to improve the system security. Hacking is the method for figuring out the shortcomings and weaknesses in the framework or PC organization. It is a method for portraying the strategy of hacking in a moral manner for any organization. The moral programmer has a great reason to make it happen. In reality, it has turned into the overall discernment to us for programmers that he will be awful, devotees, criminals, and dishonest. Fundamentally a portion of the programmer has even done severely for certain associations like they have taken vital data of their clients. In a portion of the public authority associations, they have harmed extremely private data like government-managed retirement numbers and other touchy data. That is the explanation programmers are not having generally excellent standing. To keep away from such circumstances numerous associations have recruited numerous moral programmers to keep track of their framework and PC organization. Moral programmers are assuming to test and really look at weaknesses and shortcomings in the current framework. There is each other face of the coin which tells that without programmers the weaknesses and openings of programming would stay unseen [1]. In this paper, I have attempted to make sense of the great and terrible face of programmers and even of moral programmers additionally and the different effects on the various region of our general public. A review shows that practically 90% of assaults occur within which shows how simple it is to attack into the framework or organization for insiders.

Keywords: Ethical Hacking, Hackers, White hat, Black hat, Grey hat, Impact on Society.

INTRODUCTION

Hacking can be defined as obtaining access to a system that you are not supposed to.

Copyright © authors 2022

Example: Login into someone's Email account that is not supposed to be accessed, Obtaining access to a computer that you are not supposed to have access ,extracting information that you are not supposed to extract ,these methods are some examples of hacking. There are lot of ways to hack a system.

In 1960 marked the first hacking event which took place at MIT and at the same time, the term 'HACKER' was Coined.

Hacking is hacking and one who performs hacking is a criminal, no matter whether he performed it in an ethically or not. The one who performs it is referred to as computer criminals or cyber criminals. However, the technique used helped many organizations improving their system security efficiently. Then the revolution started training and employing the ethical hackers. To become an ethical hacker, one needs to work towards a certification to become a Certified Ethical Hacker (CEH).

Any Electrical device like computer, phone, laptop, a network, a router, a website , a server Each device has an operating system, and they have the program installed on these operating systems. We will look at how to gain access to the computers. In this example, we are going to use a computer. We are going to have a Linux device hacker, and we are going to have a window device target. We can apply the same concepts if we are targeting a web server, a laptop or a phone, but we will be considering them all just like a normal computer. We can set up a web server on our computer, we can make it look and act like a website, or even make it act like a TV, or for that matter, anything we want. TVs and all such things are just simple computers with less complicated hardware in them.

Ethical Hacking have various advantages,
These are some examples of those advantages

- Ethical hacking can be used to recover the information's that are lost, examples if you lost or forget a password we can solve the issues with the help of ethical hacking.
- Ethical hacking can be used to perform test's that involve in the penetration testing to increase the security of the data, system or computer and of a network.
- It is also used to test the speed and growth of the Current network security.

There are various disadvantages of hacking:

- It can harm the privacy of someone.
- Hacking is illegal.
- Criminal can use hacking to their advantage.
- Hampering system operations.

Gaining access attack is the second part of the network penetration testing. In this section, we will connect to the network. This will allow us to launch more powerful attacks and get more accurate information. If a network doesn't use encryption, we can just connect to it and sniff out unencrypted data. If a network is wired, we can use a cable and connect to it, perhaps through changing our MAC address.

Copyright © authors 2022

If the network uses encryption, we can't get anywhere unless we decrypt it. In this section, we will discuss that how to break that encryption and how to gain access to the networks whether they use WEP/WPA/WPA2.
Once we get access to the target computer, we will see what we can do after we gain access to this computer. This could involve a client-side exploit, server-side exploit, or even just physical access, where the victim leaves their desk, and we get in. In this section, we are going to look at what we can do once we have access to the target. We will also see how we can further exploit that target and increase our privileges, or target other computers in the same place. Ethical hacking can be classified into three categories based on the purpose they serve. Each type of hacker hacks for a different purpose. The different types of hackers are:

Black hat hacker:
One who hacks with malicious intention is the black hat hacker which is the bad guy. To steal money or data or even to destroy the data this type of hacker uses his or her skills. For the purpose of fame, few of them target big organizations stealing their data. Black hats try to break into computer system to steal credit card information and possibly steal valuable information to sell on the black market. They may even lock the computer and the system from the owners and hold them for ransom.
White hat hacker:
The white hat hacker is one who is an ethical hacker. This type of hacker, hacks for a company or organization for security purpose. The white hat is given special authorization with limits on what the hacker can and cannot do on their customer's computer and network system. This special authorization is usually given in a legal document so-called license signed by both the white hat and the company.
Grey hat hacker:
The grey hat hacker is who may violate ethical standards or principles, but without having malicious intention ascribed to black hat hackers. Grey hat hackers may engage in practises that seem less than completely above the board but are often operating for the common good. Grey hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and Black hackers who act maliciously to exploit vulnerabilities in system.
Many people see the world of IT security as a black and white world. However, grey hat hacking plays an important role in the security environment. One of the most common examples given of a grey hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exist. In this case, experts might say that the difference between a white and a grey hat hacker is that the grey hat hacker exploits the vulnerability publicly, which allows other black hat hackers to take advantage of it. By contrast a white hat hacker may do it privately in order to alert the company, without making the results public.

Most of the advantages are obvious. The advantages range from simply preventing malicious hacking for preventing national security breaches. The advantages are
Fighting against national security breaches and terrorism.
Having a secured system that is protected from malicious hackers from gaining access.
As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. The possible drawbacks or disadvantages of ethical hacking are:

Copyright © authors 2022

The ethical hacker using the skills and knowledge they gain to do malicious hacking activities. Allowing the company's financial and banking details to be seen.

OBJECTIVES

- To understand the difference between hacking and ethical hacking
- To understand legal frame of ethical hacking
- To conduct a comparative analysis of ethical hacking among different countries

As soon as people hear hacking, the first thing they relate it to some malicious cyber practices. In contrary, hacking is referred to as legal or illegal practices of accessing information stored in systems by experts. These experts are called as hackers. Hackers have all the knowledge related to programming and its concepts. (Ames,2018) The weak points where programmers failed to develop while working on a software are picked up by hackers to encroach the security framework of the software.

Ethical hacking is performed by hackers as well but their intention behind hacking is not for malicious purposes. Their responsibility is to check and build on software security and thus help to develop a protected software for a business or organization to prevent potential threats. Hacking and ethical hacking can be differentiated based on the purpose they serve. Ethical hackers are referred to as white hats and unethical hackers as black hats. (Jaquet-Chiffelle)

Ethical hackers bring value to organisations by finding security loopholes before someone hacks with malicious intentions. Things are not as they seem, though it looks simple. Ethical hackers can be subject to legal actions, even though they hack systems with good intentions.

Ethical hacking is deemed acceptable if it is asked for by organizations.(Shimonski R) But even then, it doesn't make such hacking immune to legal action. Most dangerous is the position of the hackers who hack systems not asked by organizations but with good intentions. Current laws governing ethical hacking are inadequate and indefinite. The issue of legal protection for ethical hackers needs serious focus. The scope of work and other legal provisions need to be determined.

Hackers have very measurable impact on the society.(Lee M) They are attracting more and younger generations. Though ethical hacking is not bad, but it is also vital to understand what exactly ethical hackers are doing for the interest of society. If we treat hacker is the person who pushes technology beyond perceived norms, there are several fields in computing where ethical hacking or ethical hackers made a measurable impact. Today internet has become the way for any computer to connect to the entire world, which also makes it vulnerable to attacks from the hackers across the world.

Caldwell (2011) studied ethical hacking: putting on the white hat. Nowadays ethical hacking has become the vital part of enterprise's network security. Differentiating white hat from malicious black hats hackers are fulfilling a role beyond penetration testing. The skills of white hats are increasing too as the threat's changes. Ethical hacking is becoming a mainstream career option for learners and practitioners who have the knowledge and experience of network security.

Palmer (2001) studied Ethical hacking. Access to computers was usually restricted because of their increasing popularity and continued high cost. Users would challenge access controls when refused access to the computers. They would steal passwords or account numbers. Then

Copyright © authors 2022

explore the system for bugs that might get them past the rules, or even take control of the whole system. In order to run the programs of their choice, or to change the limitations under which their programs were running this was done. The idea of checking a system security by trying to break into it is not new. Crash-testing cars by an automobile company or testing his or her skill at martial arts by sparring with a partner is accepted as prudent.
Smith (2002) studied Ethical hacking: the security justification redux. The state of security on the Internet is bad and becoming worse. Previous research has proved ethical hacking as an altruistic behaviour, but we find ethical hackers act rationally to secure systems that are within their own community. Hacking has entered the era of mass production. Current and future Internet attacks are a technologically enabled crime. Security used to be a private matter until information security was handed over to a few specially trained professionals. Since the law often lags technological advance, social behaviour goes beyond merely adhering to the law. Until a social framework is developed to recognise the good guys (white hats) from the bad guys (black hats), we should be slow to codify into law or disapprove ethical hacking.

DISCUSSION

When individuals hear hacking, the principal thing they relate it to some malevolent digital practices. In opposite, hacking is alluded to as lawful or unlawful acts of getting to data put away in frameworks by specialists. The individual who can hack or acquire unapproved access in a framework and organization without the client's information could be useful for making the better world and furthermore they could obliterate the world, it depends upon the programmer's intension which differentiates them into great programmer called white cap programmers and terrible or malevolent programmer called dark cap programmers. The conflict between these two programmers won't ever end. The learn about additionally uncovers that the authentic clients are the ethical programmers, till their intensions are clear in some other case they are a superb danger, as they have the get right of section to every single piece of measurements of the organization.

This also infers that hacking is a fundamental issue of specialized world. It offers with every feature of being exact and awful. Moral hacking assumes a basic part in maintaining and saving a great deal of mystery data, though malicious hacking can wreck everything. What all depends on is the intension of the programmer. It is al-generally unrealistic to fill an opening among moral and noxious hacking as human thought can't be vanquished, yet security measures can be fix.

CONCLUSION

Ethical hacking has tremendous positive potential, if appropriately utilized. Presumably quite possible challenge is it faces is subjective interpretation. In this way, having a goal, exhaustive and downright legitimate structure in place is vital. The structure ought should have balance between powers to hackers and organizations. An excessive power can be tragic, as it can either unleash destruction with the frameworks or with the certainty or expectations of the hackers. Simultaneously, the ethical hackers' community may likewise contemplate carrying out a deliberate set of rules not withstanding the legal framework.

Various inspirations and suppositions have been examined in this paper, yet on the off chance that we consider them as an individual, they are a live illustration of virtuosos due to their

Copyright © authors 2022

capacities of doing the unimaginable and unattainable by getting more required into the programming and understanding the provisos in the security frameworks. I consider in light of the fact that these, researchers and analysts have spent bunches of innovation to further develop the framework's security and make them safer so no unlawful access can be acquired.

REFERENCES

1) Ames, M. G. (2018). Hackers, computers, and cooperation: A critical history of logo and constructionist learning. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-19.
2) Caldwell T. Ethical hackers: putting on the white hat. Network Security. 2011 Jul 1;2011(7):10-3.
3) Jaquet-Chiffelle DO, Loi M. Ethical and unethical hacking. in The ethics of cybersecurity 2020 (pp. 179-204). Springer, Cham.
4) Palmer CC. Ethical hacking. IBM Systems Journal. 2001;40(3):769-80.
5) Smith B, Yurcik W, Doss D. Ethical hacking: The security justification redux. In IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293) 2002 Jun 6 (pp. 374-379). IEEE.
6) Shimonski R. CEH v9: Certified Ethical Hacker Version 9 Study Guide. John Wiley & Sons; 2016 May 2.
7) Lee M, Lee J. The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers. 2012 Apr;14(2):375-93.

Copyright © authors 2022