Research on hacking

What are the different issues and motivations that arise in a person that he opts for hacking? Is money, thrill or something to break the rules inspires the hacker to indulge into such acts are discussed in this paper. This paper also gives you an insight to consider how important the network security plays to avoid hackers to steal away information that is very confidential. Measures are to be taken in order to remove these possibilities.

In recent years we have seen a drastic change in the field of IT, where electronic commerce, email, online shopping, online banking, information bank of numerous data, software development has improved leaps and bounds. As the technology has increased to new heights the hackers have found a way to get easy money. They find ways to get into government confidential files, personal banking details, steal away their money from the banks, implant a Trojan or virus into different computers to make them vulnerable to work. In this paper I have thrown some light on hackers skills, their perspective, their targets.

Introduction

Hacking according to oxford dictionary means to “gain unauthorized access (to data in a computer)”. Banks defines hacking as “something that boring mainframe computer operators did to improve performance and battle boredom.” [1]. Here a bank focuses on boredom as the reason of hacking. Darlington believes hacking is not limited to accessing data or information but also includes an attack on the privacy of all people [5]. Almost all different opinions agree on the illegality of hacking.

On the other hand the word hacker is the agent of hack or hacking and it was defined as a person who enjoys accessing files whether for fun, imposing power or the interest related to the accessed files or data according to Taylor [8]. While Marotta has a negative view of the hacker as a data lord, a barbarian who takes what he wants [9]. Himanen defines hacker as any person who performs illegal actions whether they were related to computer or not which means the usage of a device apart from its functionality. Seems hacking according to Himanen is related to any illegal or unauthorized action [7].

Clear from the definitions mentioned above that there is a controversy that encounters the judgment and definition of hacking, controversy aroused because it’s hard to decide exactly what the aim is behind hacking or how to know the mentality of the hacker. That’s why the ethics and motivation of hackers should be paid attention and discussed then understanding the hacker will be much easier.

Who is the hacker?

According to Taylor, Hacker can be anyone who has knowledge of things; he can be a graduate or a computer professional working at a multinational company. He can be one amongst us. A is part of the society, a computer professional who wants to use technology for his own benefit [11]. Hackers are experts and professional people who first enjoy the technology and through research and development they gain more interest and you never know when this curiosity of technology changes into crime. People must realise that the technology is good lest it is used for the countries benefit, but it has adverse affect when things turn upside down, that the hackers learn this technique in order to gain profits for themselves through illegal ways. Levy described hackers in regard to the history; she divided the life history of hackers into three generations: the first generation of hacking was made of experts of computer programming who never stopped improving their skills then misuse them, the second generation was made of computer hardware developers who found hacking and accessing data and information for free as an appealing idea while the third generation included developers of games architecture [8]. And I think the fourth generation of developers are those who know about computers and have just enough knowledge about computer programming.

Pipkin classification of hackers depends on the functionality, in other words the classification depends on the way hacker interacts with what is being hacked. Hackers were classified into three different types; the first type is called In-house hacker. An in-house hackers actually works inside the company, who knows the system security, has access to all the features. His motivation to hacking might be because he wasn't recognised as a potential candidate for promotion or because he was betrayed by his fellow colleagues. The second type of hackers is a super hacker who doesn't interact with the system, but remotely monitors all the movements or the data transactions that are going on and depending on the situation and the amount of money that is being transferred he then changes that transaction into his account. And finally, comes the professional hacker, he is very strong and capable of getting any type of data from anywhere, he has the ability to manipulate things and change them to his benefit, programming Trojans and software that get installed on the system through hidden window and then sits on the system[10].

Motivations behind Hacking

Hacker's psychology and the fuel that encourages him/her to perform such illegal activities, also because hackers view about what they are doing is far different from our views as victims Furnell ([6]

Pipkin, in his paper Halting the hacker, says "the challenging part of the hacker's personality as the biggest motivation; this means that the hacker feels the joy and excitement when hacking systems that are provided with the almost perfect security tools" [10]. One of the main reasons for hacking is excitement where hackers find adrenalin rush to break the law, to find an easy access to earn money by hacking crucial information of the customers by creating unreal shopping websites and obtaining payment details, credit card details.

Furnell judged hackers "depending on the harm they cause whatever was their motivation, because hacking is a disease and should be removed so that the effect of hacker attacks will be minimized" [6]. The motivations behind hacking are an issue that is discussed heavily due to the importance of understanding the

An ethical hacker attempts to duplicate the intent and actions of malicious hackers without causing harm. Ethical hackers conduct penetration tests to determine what an attacker can find out about an information system, whether a hacker can gain and maintain access to the system, and whether the hacker's tracks can be successfully covered without being detected. The ethical hacker operates with the permission and knowledge of the organization they are trying to defend and tries to find weaknesses in the information system that can be exploited.

In some cases, to test the effectiveness of their information system security team, an organization will not inform their team of the ethical hacker's activities. This situation is referred to as operating in a double blind environment. To operate effectively, the ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support the ethical hacker's efforts.

Hacker and Ethical Hacker Characteristics and Operation

Research on hacking

Hackers can be categorized into the three general classes of black hats, gray hats, and white hats. A black hat hacker or cracker has the necessary computing expertise to carry out harmful attacks on information systems. A gray hat is a hacker with a split personality. At times, this individual will not break the law and, in fact, might help to defend a network. At other times, the gray hat hacker reverts to black hat activities. The white hat individual usually has exceptional computer skills and uses his or her abilities to increase the security posture of information systems and defend them from malicious attacks. This individual might be an information security consultant or security analyst.

Entities that perform ethical hacking functions for organizations usually fall into one of three categories: white hats, former black hats, and independent consulting organizations. The white hat ethical hacker has the appropriate computer skills and understanding of the black hat hacker mentality and methods. This person might be an independent consultant hired to perform ethical hacking activities. The former black hat hacker is, we might hope, reformed and brings actual black hat experience to his or her work. There is a concern about this individual in that you can never be certain that he or she will not revert to their former malicious activities. The third category of ethical hacker is taken by consulting companies that perform a variety of services for organizations including accounting, auditing, and information system security.

Related Types of Computer Crime and attack

Different kind of hacking attacks are considered as computer crimes. The following is the list of crimes which are committed frequently:

Password Hacking

Hackers find a way to illegally hack into the passwords of users of federal bureau, banks in order to gain benefits from them.

Network intrusions

Malicious Trojan, worms and viruses to gain access into the information systems.

Cheat

Illegal use of people identities such as credit card details.

Software piracy

Illegal copying and use of software

Viruses

Viruses, Trojan horses and worm cause the computers to become more vulnerable and susceptible to hardware damage.

IP address spoofing

Disguising the IP address and using that to gain illegal access into countries most confidential files.

Money Laundering

Illegally acquiring funds through the manipulation and falsification of financial statements and illegal transactions.

Data-modification

The modifying all the data.

Smuggling of files

Gain illegal access of confidential files including bodies like military/government networks, communication systems, power grids, and the financial community

Pipkin lists a number of hacking attacks that are most commonly used in breaking system and causing disruption and damage for services. These attacks can be summarized as following [10]:

Software piracy is a criminal offense. Many hackers have indulged in making copies of software and selling them to gain profits on their own. The companies who develop these software will have to bare all the losses only because of someone who is illegally misusing software. Stealing confidential files through illegal access of the companies most confidential files. Hackers have many such motives, few of them like denial of services to the user and to make hardware conflict, making unwanted popup, causing trouble, terrorism.

Taylor listed the main characteristics of hacking attacks in three points [8]:

- Simplicity: means that the attack should be simple in appearance but the effects are impressive and the results will be as pleasing to the hacker as what he planned for. It means that do your job in a smart and easy way.
- Mastery: the methods used in hacking contain sophisticated knowledge which is difficult for anyone to understand. The reason behind mastery is to make sure that the hacker is the only one who can solve the problem being caused.
- Illicitness: means that the act is against all rules and laws.

Conclusion

Earlier hackers were considered to be genius because they helped in many ways in the development of computers and internet technology as such, but in this modern world where personal benefit has played a major importance in one’s life, people are often attracted to things they can do and gain through illegal entry into people privacy and using for their own benefits.

Different motivations and opinions have been discussed in this paper, but if we consider them as a person they are a live example of genius because of their abilities of doing the unbelievable and unachievable by getting more involved into the programming and understanding the loop holes in the security systems. I think because of these, scientists and researchers have spent lots of technology to improve the systems security and make them more secure so that no illegal access can be gained.

In my own view understanding the different perspective of a hacker, we can develop a much more secure and much more sophisticated environment and provide a safer world for transactions and online shopping. The bad things of them should be taken into good only to benefit our country and its progress

Notorious Hacking Groups of all times.

- **Anonymous**
- **The level seven screw**
- **Lizard Squad**
- **Chaos Computer club**
- **LulzSec**
- **Syrian Electronic army**
- **Globalhell**
- **Network crack program Hacker group**
- **TeaMpOison**

Research on hacking

Ethical Advice

- As you are online, so are the bad guys
- Gain visibility into your organization’s cyber risk
- Security is not just computer science – it’s a mindset
- The only firewall that protects against cyber criminals is your brain
- How do you protect our country from cyber-attacks? Start by protecting your own network
- Watch out for cybercriminals
- Think before you click