IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, March 2022
Impact Factor: 6.252

Ethical Hacking and Its phases

Miss. Dakhni Rushda Naushad[1], Ms. Ulde Ayman Ajaz[2]
Teacher[1] and Student, TYBSc[2]
Anjuman Islam Janjira, Degree College of Science, Murud-Janjira, Raigad, Maharashtra, India

Abstract: *The state of security on the internet is very poor. Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. As public and private organizations migrate more of their critical functions or applications such as electronic commerce, marketing and database access to the Internet, then criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. Ethical hacking is an identical activity which aims to find and rectify the weakness and vulnerabilities in a system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what is ethical hacking, what are the types of ethical hacking, impact of Hacking on Businesses and Governments. This paper studied the different types of hacking with its phases.*

Keywords: Artificial in Vulnerabilities, Hacker, Cracker, Port and Intrusion

I. INTRODUCTION

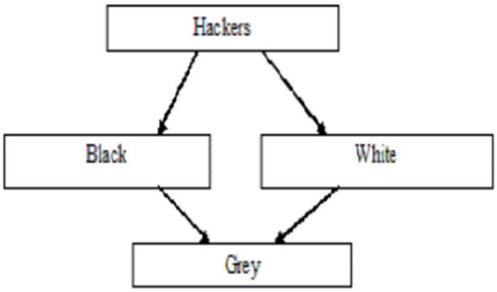
1.1 What is Hacking?

Hacking is the technique in which the persons, what's in a name? Call them hackers, crackers, intruders, or attackers, they are all interlopers who are trying to break into your networks and systems. Some do it for fun, some do it for profit or some simply do it to disrupt your operations and perhaps gain some recognition. Though they all have one thing in common; they are trying to uncover a weakness in your system in order to exploit it.

1.2 What is Ethical Hacking?

Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming".[3] Ethical hacking is defined as the practice of hacking without malicious intent. The Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security .According to Palmer (2004, as quoted by Pashel, 2006): "Ethical hackers employ the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems' security and report back to owners with the vulnerabilities they found and instructions for how to remedy them". [10] The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers.

II. TYPES OF HACKING/HACKERS



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, March 2022
Impact Factor: 6.252

The hacking can be classified in three different categories, according to the shades or colours of the "Hat". The word Hat has its origin from old western movies where the colour of Hero's' cap was "White" and the villains' cap was "Black". It may also be said that the lighter the colour, the less is the intension to harm.

2.1 White Hat Hackers

White Hat Hackers are authorized and paid person by the companies, with good intends and moral standing. They are also known as "IT Technicians". Their job is to safeguard Internet, businesses, computer networks and systems from crackers. Some companies pay IT professionals to attempt to hack their own servers and computers to test their security. They do hacking for the benefit of the company. They break security to test their own security system. The white Hat Hacker is also called as an Ethical Hacker. In contrast to White Hat Hackers.

2.2 Black Hat Hackers

The intension of Black Hat Hackers is to harm the computer systems and network. They break the security and intrude into the network to harm and destroy data in order to make the network unusable. They deface the websites, steal the data, and breach the security. They crack the programs and passwords to gain entry in the unauthorized network or system. They do such things for their own personal interest like money. They are also known as "Crackers" or Malicious Hackers Other than white hats and black hats.

2.3Grey Hat Hackers

Another form of hacking is a Grey Hat. As like in inheritance, some or all properties of the base class/classes are inherited by the derived class, similarly a grey hat hacker inherits the properties of both Black Hat and White Hat. They are the ones who have ethics. A Grey Hat Hacker gathers information and enters into a computer system to breech the security, for the purpose of notifying the administrator that there are loopholes in the security and the system can be hacked. Then they themselves may offer the remedy. They are well aware of what is right and what is wrong but sometimes act in a negative direction. A Gray Hat may breach the organizations' computer security, and may exploit and deface it. But usually they make changes in the existing programs that can be repaired. After sometime, it is themselves who inform the administrator about the company's security loopholes. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations' network. While hacking a system, irrespective of ethical hacking (white hat hacking) or malicious hacking (black hat hacking), the hacker has to follow some steps to enter into a computer system, which can be discussed as follows.

III. METHODOLOGY

3.1 Hacking Phases

Hacking can be done by following these five phases:

Phase 1: Reconnaissance: can be active or passive: in passive reconnaissance the information is gathered regarding the target without knowledge of targeted company (or individual). It could be done simply by searching information of the target on internet or bribing an employee of targeted company who would reveal and provide useful information to the hacker.

This process is also called as "information gathering". In this approach, hacker does not attack the system or network of the company to gather information. Whereas in active reconnaissance, the hacker enters into the network to discover individual hosts, ip addresses and network services. This process is also called as "rattling the doorknobs". In this method, there is a high risk of being caught as compared to passive reconnaissance.

Phase 2: Scanning: In Scanning Phase, The Information Gathered In Phase 1 Is Used To Examine The Network. Tools LikeDialers', Port Scanners Etc. are being used by the Hacker to Examine the Network So As To Gain Entry in the Company's System and Network.

Phase 3: Owning the System: This Is the Real and Actual Hacking Phase. The Hacker Uses The Information Discovered In Earlier Two Phases To Attack And Enter Into The Local Area Network (LAN, Either Wired Or Wireless), Local Pc Access, Internet Or Offline. This Phase Is Also Called As "Owning The System".

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, March 2022
Impact Factor: 6.252

Phase 4: Zombie System: Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or additional attacks), by making changes in the system in such a way that other hackers or security personals cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as "Zombie System".

Phase 5: Evidence Removal: In this phase, the hacker removes and destroys all the evidences and traces of hacking, such as log files or Intrusion Detection System Alarms, so that he could not be caught and traced. This also saves him from entering into any trial or legality. Now, once the system is hacked by hacker, there are several testing methods available called penetration testing to discover the hackers and crackers

IV. Literature Review

The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. More and more computers get connected to the Internet, wireless devices and networks are booming. As, with most industrial advances, there is also other face: illegal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. There is also a dark side of web and web technological advancements in form of "Criminal Hackers" that are posing a threat to websites and web related services as well as corporate activities. The number of these hackers are increasing while the resources available to law-enforcement agencies are also increasing, but at a much slower rate. So, the hackers are clearly winning the battle with law-enforcement agencies, which are must content themselves with investigating and prosecuting the most spectacular cases. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy.

4.1 Advantages of Ethical Hacking

Following are the advantages of Ethical Hacking as follows.

- This helps to fight against cyber terrorism and to fight against national security breaches.
- This helps to take preventive action against hackers.
- This helps to build a system that prevents any kinds of penetration by hackers.
- This offers security to banking and financial establishments.
- This helps to identify and close the open holes in a computer system or network.

4.2 Disadvantages of Ethical Hacking

Following are the disadvantages of Ethical Hacking as follows.

- This may corrupt the files or data of an organization.
- They might use information gained for malicious use. Subsequently, trustful programmers are expected to have achievement in this framework.
- By hiring such professionals will increase costs to the company.
- This technique can harm someone's privacy.
- This system is illegal.

V. Result and Discussion

Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customers' personal and financial data and often are targeted by their own employees, whether disgruntled or just opportunistic. Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can linger for years after the actual attack. Companies can lose consumer confidence and in many cases are held legally responsible for any loss to their customers. The cost of recovering from an attack can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc. Companies, and more recently, consumers, are investing more and more money into preventing an

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, March 2022
Impact Factor: 6.252

attack before it actually happens. Businesses that hold stores of consumer's personal and financial data are especially taking extra steps to insure the data's safety.

VI. CONCLUSION

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies' their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. Which may allow a malicious hacker to breach their security system. Ethical Hackers help organizations to understand the present hidden problems in their servers and corporate network. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

ACKNOWLEDGEMENT

I hereby declare that all the information provided in the respected paper is authenticated, authorized and hence reliable. I would like to thanks all the viewers and readers of this paper for their precious time.

REFERENCES

[1]. Wikipedia
[2]. Gurpreet K. Juneja,"Ethical hanking :A technique to enhance information security "International journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
[3]. K.BalaChowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
[4]. Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013)
[5]. "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity" August 14 - 16, 2013 Cancun, Mexico. "Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems "Undergraduates Students Aury M. Curbelo, Ph.D,Alfredo Cruz, Ph.D.
[6]. Kumar Utkarsh" System Security and Ethical Hacking"