www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11466-11468

Ethical Hacking

Deepak Kumar[1], Ankit Agarwal[2], Abhishek Bhardwaj[3]

[1] *IP University, Sirifort College of Computer Technology and Management*
8, Institutional Area, Rohini Sector-25, New Delhi
deepakkumar2294@yahoo.com
[2] *IP University, Sirifort College of Computer Technology and Management*
8, Institutional Area, Rohini Sector-25, New Delhi
ankit96505@gmail.com
[3] *IP University, Sirifort College of Computer Technology and Management*
8, Institutional Area, Rohini Sector-25, New Delhi
abhi14.amity@gmail.com

Abstract: ***Today, security is the main problem. Almost all the work is done over the internet crucial data are sent over the web and other information is placed over internet. While all the data is available online, there are many type of users who interact with data some of them for their need and others for gaining knowledge that how to destroy the data without the knowledge of the owner. There are various techniques used for protection of data but the hacker (or cracker) is more intelligent to hack the security, basically there are two categories of hackers that are different from each other on the basis of their intensions. The one who has good intensions are known as ethical hackers because they ethics to use their skill and techniques of hacking to provide security to the sensitive data of the organization. To understand this concept fully we describe introduction about the hacking, types of hackers, a survey of IC3, rules of ethical hacking and the advantages of the ethical hacking.***

Keywords: Ethical hackers, White hats, malicious hackers, Grey hats.

Introduction

Security is the major fact in today's era where internet use is very vast and fast growing. Every organization has issues related to security about their sensitive and confidential data. This is only because of hacking, Hacking is done by a person who has wrong intensions. Basically there are two types of hackers, one who has rights of securing data while using hacking techniques and the other who uses his knowledge to break security to harm the organization. These hackers are categorized into two categories [2]

1. Ethical Hackers
2. Malicious Hackers

Hacking is a process of controlling the system of an organization without the knowledge of the organization members. In contrast it is called breaking the security to steal the sensitive and confidential information such as credit card numbers, telephone numbers, home addresses, bank account numbers etc that are available on network. This illustrates that security is a discipline which protects the confidentiality, integrity & availability of resources. It refers this era as a "Security Era" not because we are very much concerned about security but due to the maximum need of security [3].It also explains that the explosive growth of internet has brought many good things such as electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail and new avenues of advertising and information distribution etc. but there is also a dark side such as criminal hackers. The government, companies and private citizens around the world are anxious to be a part of this revolution, but they are very much afraid that some hackers will break into their Web Server and replaces their information with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization information to the open internet. Cyber Security is the most talked about topic and the most concerned area in today's online world.

Survey on Cyber Security

I noticed on a report from government website that is actually "Internet Crime Current Report". The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NWC3).

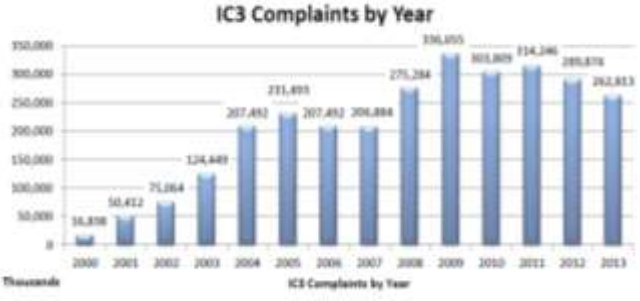

Figure 1: Complaint Graph of IC3 [7]

The graph (Fig. 1) shows that till year 2009 numbers of complaint were increased at an exponential rate. But after 2009 it is little down in 2010 but increased in 2011 and is almost the same in the remaining years. This shows that how much important the security is in this era of computer world.

The following data (Fig. 2) illustrates that how the IC3 dealt with the cyber security till their last report.

Figure 2: Complaint Reported to the IC3 [7]

ABOUT HACKING:-

Before knowing about the ethical hacking first we have to know about hacking which is a brainchild of curiosity, As a result of curiosity, the hacker always wants to know more about information, depending upon his taste.

Several definitions of hackers are

- Hackers are capable individuals with extreme computer knowledge about software as well as hardware.
- A hacker is a person who enjoys learning the details of computer systems and enhances his capabilities. He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks.

Popularly, hackers are referred to someone who penetrates into computer network security systems. Originally, the term hacking was defined as - "A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers."
Ethical hacking: Ethical hacking is a process in which the hacker has clear intensions to break computer security to save the organization from intrusion attacks. They never reveal the facts and information about the organizations. Ethical hackers are also known as "Red Teams", "Penetration Testing" or "Intrusion Testing". Malicious hacking [2]: This is the unauthorized use of computer and network resources. Malicious hackers use software programs such as Trojans, malware and spyware, to gain entry into an organization's network for stealing vital information. It may result to identity theft, loss of confidential data, loss of productivity, use of network resources such as bandwidth abuser and mail flooding, unauthorized transactions using credit or debit card numbers, selling of user's personal details such as phone numbers, addresses, account numbers etc.

TYPE OF HACKERS:-

The hackers are categorized above

Figure 3: Types of Hackers

Black Hat Hackers: Their deeds results into destructive activities. They are also known as crackers.

White Hat Hackers: They are professional hackers. They use their skill for defensive purpose in purely an ethical way.

Gray Hat Hackers: They are the hackers who are mixture of both white hat and black hat hackers i.e. work both offensively and defensively.

RULE OF ETHICAL HACKING:-

- The hacker must obey the ethical hacking rules. If they don't follow the rules then it would be dangerous for the organization.
- Execute plan: For the ethical hacker time and patience is more important [2].
- Ethical hacker must have clear intensions to help the organization not to harm them.
- Privacy is the major concern from the organization point of view, thus the ethical hacker must be kept it private because their misuse can be dangerous or illegal.

HACKING PHASES:-

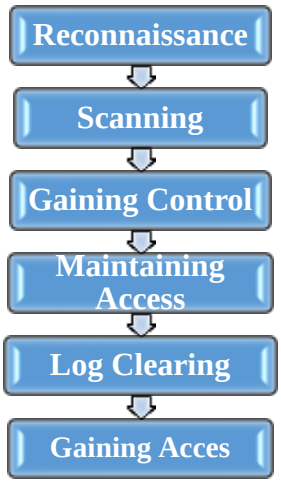

Figure 4: Ethical hacking phases

Reconnaissance: It refers to gather as more information as we can about target in prior to perform an attack. The information is gathered regarding the target without knowledge of targeted company (or Individual).It could be done simply by searching information of target on internet or bribing an employee of the targeted company who would reveal and provide useful information to the hacker. This process is also called as "information gathering" [2]. It can be Active or Passive.
Scanning: It refers to scan for all the open as well as closed ports and even for the known vulnerabilities on the target machine.
Gaining control: It can be gained at OS level, system level or even network level. From normal access hacker can even proceed with privilege escalation. It often includes password cracking, buffer overflows, DoS attack etc.
Maintaining Access: It is where hacker strives to retain it control over target with backdoors, root kits or Trojans. Compromised machines can even be used as Bots and Zombies for further attacks.

Log clearing: It is also known as Daisy Chaining. To avoid being exposed or caught, a good hacker will leave no impressions of his presence. So he attempts to overwrite the system and application logs.

>>Working of an Ethical Hacker:-

The working of an ethical hacker involves the under mentioned steps:

1. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time, these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous.

2. Working ethically: The word ethical can be defined as working with high professional morals and principles.
Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.

3. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords — must be kept private.

4. Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques. You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

5. Executing the plan: In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests.

MAIN BENEFITS OF ETHICAL HACKING:-
As ethical hacking plays an important role in this security era where the network users are increasing frequently and also the hackers who are taking advantages of network while sitting at their home. The ethical hacking has following advantages [6].

- The fight against terrorism and security issues.
- Preventing malicious hackers to gain access of crucial data.
- Ethical hackers believe one can best protect systems by probing them while causing no damage and subsequently fixing the vulnerabilities found.
- Ethical hackers use their knowledge as risk management techniques.

Conclusion
As the use of internet increases, everyone becomes dependent over it and saves their crucial and important data over the internet. Basically this is an invitation to the "crackers" to gain access of information. Thus security is the major problem for the organization. This illustrates the importance of ethical hackers. For this purpose the organization hires ethical hackers who are well knowledge and experienced person.

References

[1] Need of Ethical Hacking in online World (A research paper by Monika Pangaria&VivekShrivastav), www.ijsr.net/archive/v2i4/IJSRON2013859.**pdf**
[2] Ethical Hacking Techniques with Penetration Testing www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.**pdf**(by KB Chowdappa)
[3] System Security and Ethical Hackingwww.ijreat.org/**Papers**%202013/Volume1/IJREATV1I1018.**pdf**
[4] Ethical Hacking by C. C. Palmar, IBM research division
[5] Ethical Hacking by R. Hartley
[6] Compressive Study on Ethical Hackingwww.ermt.net/docs/**papers**/Volume_4/1_January2015/V4N1-117.**pdf**
[7] Internet Crime Complaint Centre link: www.ic3.gov

Author Profile

Deepak Kumar Perusing BCA (Final) from Sirifort College of computer technology and management, Rohini, Delhi, India.

Abhishek Bhardwaj received the B-tech Degree from M.D University, and Degree of M-Tech from Amity University, Noida in the year 2011 and 2013 respectively. From the year 2013 he is working as an Assistant Professor in Sirifort College of computer technology and management, Rohini, Delhi, India, till date. He has completed his thesis of M-tech in the topic "IMAGE PROCESSING" and has already published more than 7 papers in international journals.

Ankit Agarwal Perusing BCA (Final) from Sirifort College of computer technology and management, Rohini, Delhi, India