Ethical Hacking Techniques with Penetration Testing

Shahab Ghalib [1], Namit Gupta [2]

[1] *Student, College of Computing Science & Information Technology*

[2] *Asst. Professors, College of Computing Science & Information Technology*

[1]shahabghalib222@gmail.com

[2]namit.k.gupta@gmail.com

Abstract— **Hacking is an act or activity in which, a person exploits the weakness in a system for self-profit. Ethical hacking is an identical activity which aims to find and rectify the weakness in a system. In the growing era of internet computer security is utmost concern for the organization and government. These organizations are using internet in their wide variety of applications such as E-commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. This paper attempts to discuss the overview of hacking and how ethical hacking disturb and damage the security. Also the Ethical Hackers and malicious Hackers are different from each other and playing their important roles in security. This paper studied the different types of hacking with its phases. The hacking can also be categorized majorly in three categories such as white hat, black hat and grey hat hacking. This paper also present a comparison of the hacking categories with different methods of penetration testing.**

Keywords— **Ethical Hacking, Hackers, Hacking Phases**

I. INTRODUCTION

The increasingly growth of internet has given an entrance passage to many things: e-commerce, email, social networking, and online shopping & information distribution. As the technology advances it has its dark side; hackers. Govt. organization, private citizen & many companies of the world wants to be the part of this revolution. Being afraid of hackers as they could break into the web-server. To counter attack them ethical hackers are used in the Govt. organization, companies etc. This paper describes the skills, attitude & how they helps the customer with the increasingly growth rate of internet network security has been a measure concern of Govt.& private organization. As different organization wants to take advantage of the internet but fail to do so, because of the possibility of being hacked. To minimize the risk of being hacked by the hackers the organizations realized the best possible ways to introduced the independent computer security professionals to

make their way out. In computer security the ethical hackers employ's some tools & techniques that would neither damaged the system nor still information from it. Instead they would evaluate ways to secure then system & report back the owner with the threat they had found & how to cure them.

Fig: 1. HACKING

A. A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. “Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access”. Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber-crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

II. TYPES OF HACKING/HACKERS

Hacking can be classified into three different categories which are as follows:

A. White hat hackers

White Hat Hackers[5] are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out the weaknesses in a computer or a network system as a part of "Penetration Testing" and "Vulnerability Assessments". Ethical hacking is not illegal and it is one of the demanding jobs available in IT industries.

B. Black hat hackers

Black hat hackers[6] also knows as "crackers" are those who hacks the system in order to gain unauthorized access and harm its operations and steal sensitive information. Black hat hacking is always illegal because if its bad intent which include stealing corporate data, violating privacy, damaging the system or block network communication.

C. Grey hat hackers

Grey hat hackers are a blend [6] (mix) of both (black hat and white hat) hackers. They act without malicious intent but for their fun they exploit a security weakness in a computer system or network with the owner's permission.

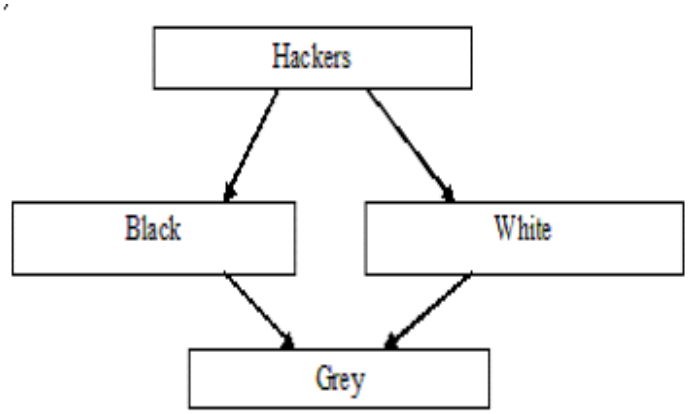

Fig: 2. Types of Hackers

III. HACKING PHASES

Hacking Can Be Done By Following These Five Phases:

Phase 1: Reconnaissance

Reconnaissance Can Be Active Or Passive: In passive reconnaissance [1]. The information is gathered regarding the target without knowledge of targeted company. 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 like diallers, 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.

In this process an attacker begins to actively probe a target machine or network for vulnerability that can be exploited.

Phase 3: Gaining Access/ 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), Local Pc access, Internet or offline. This phase is also called as "Owning the System".

Phase 4: Zombie System

Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or individual 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 (IDS) 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 call penetration testing to discover the hackers and crackers [6].

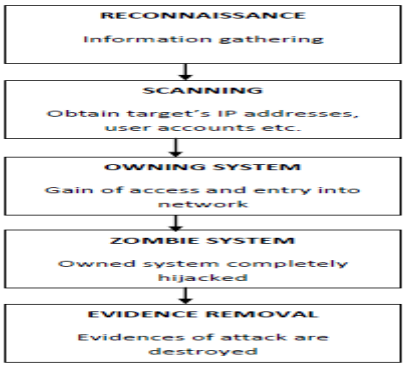

Fig: 3. Hacking Phases

IV. FOOT PRINTING

Foot printing[7] is a part of Reconnaissance process which is used for gathering information gathering possible information about a target computer system or network. Foot printing could be both passive and active. Reviewing a company's website is an example of Passive foot printing, whereas attempting to gain access to sensitive information through social engineering is an example of Active information gathering.

Foot printing is basically the first step where hackers gather as much information as possible to find ways to intrude into a target system or at least decide what type of attack will be most suitable for the target. During this phase it a hacker can collect the following information:

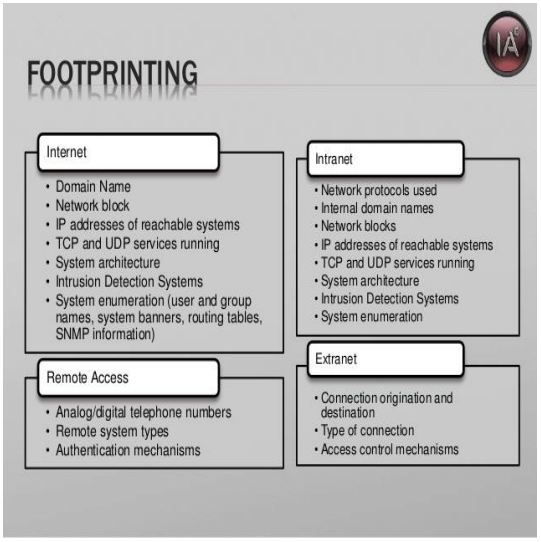

Fig. 1: Foot Printing

- Domain Name
- IP Address
- Employee information
- Phone Number
- Emails
- Job Information

V. TYPES OF SCANNING

A. Port Scanning: In this process the hacker identifies available and open ports and understand what services are running. Port number can be in these 3 range:
Well known ports (0 to 1023)
Registered ports (1024 to 49151)
Dynamic ports (49152 to 65535).

In window system well known ports available in following path: -
C:\windows\system32\drivers\etc\services

VI. PENETRATION TESTING

Penetration testing [8] is a type of security testing that is used to the insecurity of an application. It conducted to find the security risk which might be present the system. If a system is not secured then an attacker can take authorized access to that system.

Why Penetration Testing Is Required

- It identifies a simulation environment that is how an intruder may attack the system through white hat attack.
- It helps to find weak area where an intruder can attack to gain access to computer's features and data.
- It supports to avoid 'black hat attack and protect original data.
- It provides evidence to suggest by it is important to increase investment in security aspects of technology.

When to Perform Penetration Testing

- Security system discovers the new threats by attackers.
- Edit a new network infrastructure.
- Update the system and install new software.
- Relocate the office.

VII. CONCLUSIONS

Hacking has both its Pros and Cons (Benefits and Risks)[2]. Hackers are very diverse. They may bankrupt an industry/company or may protect the data, increasing the revenues for the organization/company. The battle between the Ethical (white hat) hackers and the Malicious (black hat) is long war, which has no end. While Ethical hackers help to understand the company's their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. An Ethical hacking is significant in network security, in order to ensure that the company's critical information is well protected and secure. At the same time it allows the company to identify, and in turn, to take remedial measures to rectify the loopholes that exists in the security system, which may allow a malicious hacker to breach their security system.

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 securing 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 the gap between ethical and malicious[3] as human mind cannot be conquered, but security, but security measures can be tighten.

REFERENCES

[1] EC-Council (n.d.). Ethical Hacking and Countermeasures, online http://www.eccouncil.org/ ipdf/EthicalHacker.pdf (visited on May 2012)
[2] Agarwal, Ankit Kumar, Hacking : Research paper, online http://ankitkumaragarwal.com /hacking-a-research-paper/ (visited on may 2012).
[3] Ethical Hacking Basics Class part, online http://www.go4expert.com/forums/showthread.php?t=11925(visited on May 2012)
[4] Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 978-1-59345-303-9
[5] Kumar Utkarsh" SYSTEM SECURITY AND ETHICAL HACKING".
[6] K.Bala chowdappa et al, /(IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5(3), 2014, 3389-3393.
[7] Wikipedia.
[8] Tutorials point.