IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016), PP 90-92
www.iosrjournals.org

Overview of Hacking

Sova Pal (Bera)
Department of Computer Science, Y. S. Palpara Mahavidyalaya Palpara, Purba Medinipur, 721458, India

Abstract: *Hacking and hacker are terms that generally tend to have negative effect on people. These days, largely due to popular media most people wrongly think of hackers as computer criminal and the person who doing something mischievous things in other computer, delete data, damage os & steal password and cause harm to system release viruses etc. "Hacker" is not computer criminal. The tech community now distinguishes between hackers, who identify security flaws in order to improve computer systems and crackers, who attempt to exploit those flaws to their own advantage. Now different sides of hacking is discussed.*
Keywords: *Trojan horse, Worm, Firewall.*

I. Introduction

Hacking has been a part of computing for 40 years. Some of the first hackers were members of the Massachusetts Institute of Technology (MIT) Tech Model Railroading Club (TMRC) in 1950s. Security is the condition of being protected against danger or loss. In general sense, security is a concept similar to safety. In the case of networks the security is also called the information security. Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction. The intent of hacking is to discover vulnerabilities so system can be better secured. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment or to evaluate those weaknesses to assist in removing them. Basic purpose of hacker is to know the system internally without any bad intension.

Hacking

Hacking is the process of attempting to gain or successfully gaining, unauthorized access to computer resources. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose.

Types of Hacking

- Website Hacking – Website hacking means taking control from the website owner to a person who hacks the website.
- Network Hacking – Network hacking is generally means gathering information about domain by using tools like Telnet, Netstat, etc. over the network.
- Ethical Hacking – Ethical hacking is where a person hacks to find weakness in a system and then usually patches them.
- Email Hacking – Email hacking is illicit access to an email account or email correspondence.
- Password Hacking – Password hacking or password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- Online Banking Hacking – Online banking hacking is unauthorized accessing bank accounts without knowing the password or without permission of account holder.
- Computer Hacking – Computer hacking is when files on your computer are viewed, created, or edited without your authorization.

Type of Hackers

Hackers can be divided into three groups on the basis of why they are hacking system.

- White hat hacker –A white hat hacker breaks security for non-malicious reasons. Perhaps to test own security system or while working for a security company which makes security software. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC- Council also known as the International Council of Commerce Consultants is one of those organizations that have developed certifications, courseware, classes and online training covering the diverse arena of ethical hacking.
- Black hat hacker – A black hat hacker "violates computer security for little reason beyond maliciousness or for personal gain" (Moore,2005). Black hat hackers break into secure networks to destroy, modify or steal data or to make the network unusable for those who are authorized to use the network. Black hat hackers are also referred to as the "crackers" within the security industry and modern programmers.

- Grey hat hacker– A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect.
  Besides those hackers other different types of hackers are Elite hacker, Script kiddie, Neophyte, Blue hat and Hacktivist.

Tools used by Hackers

- Trojan horses - Trojan horses are malicious programs or legitimate software is to be used set up a back door in a computer system.
- Virus – Virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.
- Worm – Worm is a like virus and also a self-replicating program. The difference between a virus and a worm is that a worm does not attach itself to other code.
- Vulnerability scanner – This tool is used by hackers for quickly check computers on a network for known weakness. Hackers also use port scanners.
- Sniffer – Sniffer is an application that captures password and other data in transit either within the computer or over the network.
- Root Kit – This tool is for hiding the fact that a computer's security has been compromised.

Ways to protect systems from Hacking

Hacking is a serious present day problem and important steps must be taken against it.

- Implement a firewall – It keeps hackers and viruses out of computer networks, allow to pass through only authorized data.
- Develop a corporate security policy – You should choose unique large password that are a combination of letters and numbers and should be changed every 90 days to limit hackers' ability. And immediately delete the user name and password when someone leaves company.
- Install anti-virus software – It should run the most recent version of an anti-virus
- Keep operating systems up to date – It should upgrade os frequently and regularly install the latest versions of software.
- Don't run unnecessary network services – When installing systems, any non-essential features should be disabled.

What should do after hacked?

- shutdown or turn off the system
- Separate the system from network
- Restore the system with the backup or reinstall all programs
- Connect the system to the network

Advantages of Hacking

- "To catch a thief you have to think like a thief"
- Helps in closing the open holes in the system network
- Used to recover lost information where the computer password has been lost
- Teaches you that no technology is 100% secure
- Provides security to banking and financial establishments
- Prevents website defacements
- To test how good security is on your own network

II. Conclusion

Ethical hacking is now a growing profession that is still used by the United States government, as well as technology companies and other corporations. Many large companies employ teams of ethical hackers to help keep their systems secure, such as IBM.

The most important thing, until and unless a ethical hacker thinks like a cracker you can never become a expert ethical hacker because to get most out of any computer system you must understand the mindset of crackers that what they can do and up to what level they can damage. Now when you will identify the vulnerabilities and loopholes, if you fixes them so that in future anyone cannot breach that same vulnerability then you are Hacker or ethical hacker or White Hat hacker and if you utilized that loophole of misdeeds or fun then its cracking or Black hat hacking.

With increases in computer technology, as well as increases in integration of computers into everyday life, it is evident that there is a place for hackers in the future but finding where they will stand is something that only time can tell.

References

[1]. Pragmatic Overview of Hacking & Its Counter Measures by Yogita Negi, 2011
[2]. Unofficial Guide to Ethical Hacking by Ankit Fadia
[3]. What is the difference between Hackers and Intruders by Asmaa Shaker, Prof. Sharad Gore, Int. Journal of Scientific & Engineering Research Vol. 2 Issue 7 July 2011 ISSN 2229-5518
[4]. Hacking: The Basics by Zachary Wilson, April 4, 2001.
[5]. www.wikipedia.org/wiki/Hacking
[6]. www.hackingtruth.com
[7]. https://qualitycrush.wordpress.com/2014/06/24/ethical-hacking-advantages-and-disadvantages/