ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

Impact and History of Computer Hacking

R.Veerandra kumar[1], II CSE

S. Indhurekha[2], AP/CSE

P.Surya[3], II CSE

SNS College of Technology, Coimbatore

Abstract:

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. In the computer security, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. 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. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word hacker exist that are related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. In the Literature review, different types of hackers and in related work, techniques used in hacking, types of key loggers, dos and don'ts are discussed.

History of hacking

Hacking has been around for more than a century. In the 1870s, several teenagers were flung off the country's brand new phone system by enraged authorities. Here's a peek at how busy hackers have been in the past 35 years.

Early 1960s

University facilities with huge mainframe computers, like MIT's Artificial Intelligence Lab, become staging grounds for hackers. At first, "hacker" was a positive term for a person with a mastery of computers who could push programs beyond what they were designed to do.

Early 1970s

John Draper makes a long-distance call for free by blowing a precise tone into a telephone that tells the phone system to open a line. Draper discovered the whistle as a give-away in a box of children's cereal.

Early 1980s

Author William Gibson coins the term "cyberspace" in a science fiction novel called Neuromancer. Comprehensive Crime Control Act gives Secret Service jurisdiction over credit card and computer fraud. Two hacker groups form, the Legion of Doomin the United States and the Chaos Computer Club in Germany.

Late 1980s

The Computer Fraud and Abuse Act gives more clout to federal authorities. Computer Emergency Response Team is formed by U.S. defense agencies.

In 1998

Hackers break into United Nation's Children Fund Web site, threatening a "holocaust". Hackers claim to have broken into a Pentagon network and stolen software for a military satellite system. They threaten to sell the software to terrorists.

Literature Survey:

The following topics are discussed in the literature review are,

Types of hackers:

- White hat
- Black hat
- Grey hat
- Elite hacker
- Script kiddie
- Neophyte
- Blue hat
- Hacktivist
- Nation state
- Organized criminal gangs
- Bots

White hat:

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker.

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hacker use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them.

Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them.

Black hat:

A black hat hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain.A black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons. This differs from white hat hackers, which are security specialists employed to use hacking methods to find security flaws that black hat hackers may exploit.

Black hat hackers can inflict major damage on both individual computer users and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks.

Grey hat:

A grey hat hacker is a combination of a black hat and a white hat hacker. In Internet slang, the term "grey hat" or "gray hat" refers to a computer hacker or computer security expert whose ethical standards fall somewhere between purely bit of specifics and clarification. Newbie go on to become hackers, a process that goes on constantly, altruistic and purely malicious.

The term began to be used in the late 1990s, derived from the concepts of "white hat" and "black hat" hackers. When a white hat hacker discovers vulnerability, they will exploit it only with permission and not divulge its existence until it has been fixed, whereas the black hat will illegally exploit it and/or tell others how to do so. The grey hat will neither illegally exploit it, nor tell others how to do so.

Neophyte:

A neophyte is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Newbies/Neophytes:

A newbie or neophyte is a person new to the hacking scene, who has already understood some of the ethics aspects involved. Newbie try to absorb information from tutorials. They rarely ask questions except when really stuck on a concept and in need of requirement.

Blue hat:

A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue Hat to represent a series of security briefing events. An event that is intended to open communication between Microsoft engineers and hackers is called Blue Hat Microsoft Hacker Conference. The event has led to both mutual understanding as well as the occasional confrontation. Microsoft developers were visibly uncomfortable when Metasploit was demonstrated.

Hacktivist:

A Hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message.

Hacktivism:

Hacktivism is the act of hacking a website or computer network in an effort to convey a social or political message. The person who carries out the act of hacktivism is known as a Hacktivist.

In contrast to a malicious hacker who hacks a computer with the intent to steal private information or cause other harm, hacktivists engage in similar forms of disruptive activities to highlight political or social causes. For the hacktivist, hacktivism is an Internet-enabled strategy to exercise civil disobedience. Acts of hacktivism may include website defacement, denial-of-service attacks (Do's), redirects, website parodies, information theft, virtual sabotage and virtual sit-ins.

Nation state: Intelligence agencies and cyber warfare operatives of nation states.

Nation-State Cyber threats:

Why They Hack All nations are not created equal and, like individual hackers, each has a different motivation and capability. This is the first in a series exploring the motivations that drive nation-states to participate in nefarious cyber activity. We know that hackers hack for a variety of reasons. Some hack because they are greedy or have criminal motives. Some hack to satisfy their egos or gain peer recognition. Some hack alone, and some hack in groups. But many hackers, or more accurately "hacktivists," join groups like Anonymous in order to demonstrate their dissatisfaction with powerful organizations such as corporations and governments who fail to share their world views.

Organized criminal gangs:

Groups of hackers that carry out organized criminal activities for profit.

Organized crime in cyberspace:

Organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organizations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged.

The structure of these criminal organizations is different from traditional organized crime organizations. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on “stand alone” basis, as members rarely meet each other in person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organized cybercrime groups from being detected and infiltrated by law enforcement.

Bots:

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks.

A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source. The botnet may refer to a legitimate network of several computers that share program processing amongst them.

Usually though, when people talk about botnets, they are talking about a group of computers infected with the malicious kind of robot software, the bots, which present a security threat to the computer owner. Once the robot software (also known as malicious software or malware) has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander.

Types of Attacks:

- Network enumeration:

Discovering information about the intended target.

- Vulnerability analysis:

Identifying potential ways of attack.

- Exploitation:

Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

RELATED WORK:

Techniques used in Hacking:

A typical hacker attack is not a simple, one-step procedure. It is rare that a hacker can get online or dial up on a remote computer and use only one method to gain full access. It is more likely that the attacker will need several techniques used in combination to bypass the many layers of protection standing between them and root administrative access. Therefore, as a security consultant or network administrator, you should be well versed in these occult techniques in order to thwart them. This chapter, which will be a review for advanced users, will introduce the main types of hacker attacks.

The following techniques are not specific to wireless networks. Each of these attacks can take multiple forms, and many can be targeted against both wired and wireless networks. When viewed holistically, your wireless network is just another potential hole for a hacker. Therefore, this chapter will review hacking techniques from a generic perspective.

Diverse Hacker Attack Methods:

The stereotyped image conjured up by most people when they hear the term "hacker" is that of a pallid, atrophied recluse cloistered in a dank bedroom, whose spotted complexion is revealed only by the unearthly glare of a Linux box used for port scanning with Perl. This mirage might be set off by other imagined features, such as dusty stacks of Dungeons and Dragons lore from the 1980s, empty Jolt Cola cans, and Japanese techno music streaming from the Net.

However, although computer skill is central to a hacker's profession, there are many additional facets that he must master. In fact, if all you can do is point and click, you are a script kiddie, not a hacker. A real hacker must also rely on physical and interpersonal skills such as social engineering and other "wet work" that involves human interaction. However, because most people have a false stereotype of hackers, they fail to realize that the person they are chatting with or talking to on the phone might in fact be a hacker in disguise. In fact, this common misunderstanding is one of the hackers' greatest assets.

Social Engineering:

Social engineering is not unique to hacking. In fact, many people use this type of trickery every day, both criminally and professionally. Whether it be haggling for a lower price on a lawn mower at a garage sale, or convincing your spouse you really need that new toy or outfit, you are manipulating the "target." Although your motives might be benign, you are guilty of socially engineering the other party.

Lost Password:

One of the most common goals of a hacker is to obtain a valid user account and password. In fact, sometimes this is the only way a hacker can bypass security measures. If a company uses firewalls, intrusion detection systems, and more, a hacker will need to borrow a real account until he can obtain root access and set up a new account for himself. However, how can a hacker get this information? One of the easiest ways is to trick someone into giving it to them.

Phishing:

It is an old and evergreen attacking method to steal confidential information like passwords and credit card numbers etc....An attempt to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

List of phishing types:

- **Spear phishing:**

Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

- **Clone phishing:**

A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Key logger:

It is a many hackers and script kiddie's favorite tool. It is software which records each and every keystroke you enter, including mouse clicks. Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Key logging can also be used to study human–computer interaction. Numerous key logging methods exist. They range from hardware and software-based approaches to acoustic analysis.

TYPES OF KEY LOGGERS:

- Hardware key loggers
- Software key loggers
- **Remote key loggers**

DO'S:

A password must be a combination of small letters, capital letters, numbers and symbols with a minimum character...

(e.g.) rvk19:'sNsCt...2016,,@alg

- Use a strong, unique password
- Turn on two-factor authentication
- Install the browser extension HTTPS everywhere
- Keep your browsing history secret
- Use a password manager
- Update your computer's software and firmware

Take these steps to protect your computer from hackers right away:

- Use a 2 way firewall
- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Web sites
- Practice safe email protocol
- Don't open messages from unknown senders
- Immediately delete messages you suspect to be spam
- Make sure that you have the best security software products installed on your PC
- Use antivirus protection
- Get antispyware software protection

Don'ts:

- A password should not be your personal information like your name, family members, friends, God etc...
- It should not contain such common numbers like 123456 and abc123 etc....

PROPOSED WORK:

How to detect key logger and remove it from your computer:

Key logger is a malicious program that installs on the PC in order to record every your keystrokes, that you type in messages to your friends, all the passwords and logins of your internet accounts, bank accounts, or credit card numbers. Key loggers save your personal information, everything that you can enter, using your keyboard, and send it to the third party. Some key loggers are able to make screenshots of users' activity in order to trace their internet activity. Some of the key loggers can be legitimate, they are used as a parental or employer controls in order to know what your children or employees do in the time when you cannot see it. In such cases all the information is send to the e-mails of the parents or employer, who installed this program. But if you did not install any key logger on your PC and you suspect that someone monitors your internet activity or e-mail correspondence, then you should learn how to detect key logger and remove it from your computer. In most cases it is better to use automatic key logger removal tool in order to remove key logger from your computer.

You can try to use Spy hunter in order to detect and remove key logger.

If you want to perform manual key logger removal instructions, then you are welcome to follow these items in order to fulfill keystroke logger detection:

1. You should trace the behavior of you PC in order to find the common virus symptoms because the key logger symptoms have much in common with the symptoms of other computer infections. We can refer slow computer performance, new icons on your desktop or in tray, network activity and unexpected pop-ups to these symptoms. Also you can notice that the text that you type can appear with little delay – this is the direct symptom that will help you in keystroke logger detection.

2. Open Task Manager in order to end the process of the installed key logger. You should know that not every key logger can be found in Task Manager. Many of them hide their traces. But you should still check the possibility to end its process:

a) Press CTRL+ALT+DELETE and then select Task Manager in the menu.
b) Select Processes tab, scroll the list. Find the process that is called winlogon.exe. One process with such a name is a normal thing, but if you have 2 processes with the same name, then you have a key logger.
c) Highlight the second winlogon.exe and click End process (you should end only the second process with such a name).

If there is just one process with such a name, then you should check all other processes, using the special services that contain information about most of the processes to detect the malicious one.

You can use Liutilities, Neuber or any other service that you know. If you are an experienced user, then it will be much easier for you to check the processes, because you will not miss the system process with any malicious.

If you end the process that belongs to key logger, then the program is deactivated till the next reboot and the third party will not get your personal information.

3. You should also look through the list of the installed programs. So, click Start menu, then All programs, try to find there the program that you did not install. Uninstall such programs.

4. How to detect key logger? You can also detect this malicious program with the help of Startup list. So, you should follow the instructions:

a) Press Windows + R buttons, then type msconfig in the line and press Enter
b) Select Startup tab and disable all the unknown programs
c) Then restart your computer.

There are all the manual instructions that will help you to find key logger on your computer and deactivate it. But you should know that in order to remove key logger you should use any special keylogger finder or keylogger remover. Only special keylogger removal tools know for sure how to detect keylogger, perform keylogger scan and remove this malicious program.

The most effective method to get rid of a keylogger is to perform the manual keylogger removal instructions and then use any automatic tool. The manual method will weaken the malicious program and the program will remove it.

CONCLUSION:

This report looked at them, good and bad things about ethical hacking where you have white hat hackers, they are known as ethical hackers. Then you have black hat hackers, who are the criminal s of the internet. You also have the hacktivist, who break into websites and deface them by changing the content of the website. I also discussed the advantages of ethical hacking, where they protect company's data, and some of the disadvantages where ethical hackers have ended up in jail for hacking into Face book. With the future of technology changing so fast, the ethical hacker has to keep up with the criminals.

REFERENCES:

http://www.symantec.com/specprog/threatreport/entwhitepaper_symantec_internet_security_threat_report_Symantec Internet Security Threat Report, Trends for January 06–June 06, Volume X. Sep. 2006.

http://mitnicksecurity.com/media/2005%20FBI%20Computer%20Crime%20Survey%20Report.pdf2005 FBI Computer Crime Survey Report

http://www.usdoj.gov/criminal/cybercrime/cclaws.html Computer Crime & Intellectual PropertySection, United States Department of Justice

http://www.wired.com/news/politics/0,1283,44007,00.html A 'White Hat' Goes to Jail. MichelleDelio. Wired News. May 22, 2001.

http://www.eweek.com/article2/0,1895,1999070,00.asp Microsoft Takes LSD to Test VistaSecurity. eWeek.com. Ryan Nairaine. Aug. 4, 2006.

http://www.eweek.com/article2/0,1895,1998034,00.asp FBI: Hackers Must Help Fight Web Mob.eWeek.com. Ryan Nairaine. Aug. 2, 2006.

http://www.time.com/time/digital/digital50/10.html John Carmack in Time Digital Archive.

http://www.theregister.co.uk/2001/07/05/max_vision_begins_18month_term/ Max Vision begins18-month term, Joins growing hacker population in stir. Kevin Poulson. The Register. July 5, 2001.

http://en.wikipedia.org/wiki/Social_engineering_(computer_security) Social Engineering.Wikipedia.org.

http://en.wikipedia.org/wiki/DMCA DMCA. Wikipedia.org

http://jargon-file.org/archive/ The Jargon File Archive

http://www.mithral.com/~beberg/manifesto.html The Hacker Manifesto http://www.infragard.net/

http://www.us-cert.gov/

http://en.wikipedia.org/wiki/Convention_on_Cybercrime

http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html A convictedhacker debunks some myths. CNN.com. October 13, 2005

http://web.lexisnexis.com/universe/document?_m=7aac67aa4fca66a2be06b803c9bfecef&_docnum=2&wchp=SURVEY - CORPORATE SECURITY: The black arts of 'white hat' hackers.

http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index.jsp?&pName=WhyAttacking Systems Is a Good Idea. IvánArce, Gary McGraw. IEEE Security &Privacy.July/August 2004.