Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):7-14
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

ANALYSIS OF INCREASING HACKING AND CRACKING TECHNIQUES

Bilal Ahmad Kamal

Evergreen Public High school / University of Sargodha

ABSTRACT

In this work, the explanation is about how the computer's containing valuable information is being unsecured and the techniques to make it secure. This technique contains information on the tools and skills a hacker uses to infiltrate computer systems and networks. This work proposes the study of hacking; as the cost of hacking attacks continues to rise, many of the businesses have been forced to increase spending on network security. However, hackers have also developed new skills and techniques that allow them to break more complex systems. Hacking involves compromising the security of networks, breaking the security of application software's or creating malicious program such as viruses, threats, logic bombs, worms, etc[1]. This work describes the various techniques of hacking and cracking, also how they work. I proposed that the term "hacking and cracking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

INTRODUCTION

Hacking tricks can be divided into different categories elaborated below:

1. Trojan programs that share files via instant messenger.
2. Phishing
3. Fake Websites.
4. Spoofing
5. Spyware
6. Electronic Bulletin Boards
7. Information Brokers
8. Internet Public Records
9. Trojan Horses
10. Wormhole Attack Trojan programs that share files via instant messenger instant messaging allows file-sharing on a computer.

All present popular instant messengers have file sharing abilities, or allow users to have the above functionality by installing patches or plug-ins; this is also a major threat to present information security. These communication software also make it difficult for existing hack prevention method to prevent and control information security. Hackers use instant communication capability to plant Trojan program into an unsuspected program; the planted program is a kind of remotely controlled hacking tool that can conceal itself and is unauthorized. The Trojan program is unknowingly executed, controlling the infected computer; it can read, delete, move and execute any file on the computer. The advantages of a hacker replacing remotely installed backdoor Trojan programs with instant messengers to access files are: When the victim gets online, the hacker will be informed. Thus, a hacker can track and access the infected computer, and incessantly steal user information. A hacker need not open a new port to perform transmissions; he can perform his operations through the already opened instant messenger port. Even if a computer uses dynamic IP addresses, its screen name doesn't change.

Hijacking and Impersonation

There are various ways through which a hacker can impersonate other users. The most commonly used method is eavesdropping on unsuspecting users to retrieve user accounts, passwords and other user related information. The theft of user account number and related information is a very serious problem in any instant messenger. For instance, a hacker after stealing a user's information impersonate the user; the user's contacts not knowing that the user's account has been hacked believe that the person they're talking to is the user, and are persuaded to execute certain programs or reveal confidential information. Hence, theft of user identity not only endangers a user but also surrounding users. Guarding against Internet security problems is presently the focus of future research; because without good protection, a computer can be easily attacked, causing major losses. Hackers wishing to obtain user accounts may do so with the help of Trojans designed to steal passwords. If an instant messenger client stores his/her password on his/her computer, then a hacker can send a Trojan program to the unsuspecting user. When the user executes the program, the program shall search for the user's password and send it to the hacker. There are several ways through which a Trojan program can send messages back to the hacker. The methods include instant messenger, IRC, emails, etc. Current four most popular instant messengers are AIM, Yahoo! Messenger, ICQ, and MSN Messenger, none of which encrypts its flow. Therefore, a hacker can use a man-in-the-middle attack to hijack a connection, then impersonate the hijacked user and participate in a chat-session.

An intrusion can be defined as an attempt to break into or to misuse a computer system for personal use. The word misuse; is a broad, and that can mean to something as severe as stealing confidential data to something as minor such as misusing your email system for spam, using your personal profiles, etc [1]. Today, both the Internet and corporate intranets are simply crawling with people from all walks of life that are continuously trying to test the security of various systems and networks for securing their data. Although the term “hacker” is in widespread use, the sense in which it is employed is generally incorrect. Popular media and entertainment providers have used it to describe anyone who tampers with a system, particularly involved in criminal activity. The hacker penetrates asystem remotely across the network. This journalistic misuse of the name upset many “traditional” hackers, who responded to the vilification of their good name by offering a new term for these individuals i.e. “crackers.”

Crackers are vandals and thieves whose sole purpose is unauthorized "cracking" into secure systems for personal gain

2. HACKING

In computer networking, hacking is any technical effort to manipulate the normal behaviour of network connections and connected systems. Hacking is an attitude and practice surrounding the use, consumption, and production of computer related work. Hacking uses Authorized or Unauthorized attempts to bypass the security mechanisms of an information systems or network. In simple words Hacking means finding out weaknesses in a computer or computer networks. The term "hacker" can mean two different things: 1. Someone who is very good at computer programming, networking, or other related computer functions and loves to share his knowledge with other people. 2. Someone who uses their expert computer skills and knowledge to gain unauthorized access to systems, corporations, governments, or networks for his personal use. Hacker seeks to understand computer, phone or other systems strictly for the satisfaction of having that knowledge. Hackers wonder how things work and have an incredible curiosity. Hackers will sometimes do questionable legal things, such as breaking into systems, but they generally will not cause harm once they break in. Contrast a hacker there is a term called cracker. Hacking is the practice of modifying the features of a computer system, in order to accomplish a goal outside of the creator's original purpose. The main goal of hacker is to steal the important or the secrete information or to destroy the enemies computer network. Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as phone hacking, brain hacking, server hacking, email hacking, etc. and it's not limited to either of them.

Hackers can be of three types i.e. 1. White hat hackers 2. Gray hat hackers 3. Black hat hackers 1. White hat hackers White hat hackers are the good guys who identify the security weakness of the system or network and inform the owner about them 2. Gray hat hackers A grey hat, in the hacking community, refers to a skilled hacker who is somewhere in between white and black hat hackers 3. Black hat hackers A black hat hacker is the villain or bad guy, who crash into victim's security to steal information and destroy the victims security network

3.TECHNIQUES OF HACKING

These techniques comprises of either taking control over terminal or server to make it useless or to crash it. Following are the techniques used for hacking purpose explained as, 3.1 Denial of Service DoS attacks give hackers a way to bring down a network without gaining internal access. DoS attacks work by flooding the access routers with bogus traffic which can affect e-mail, TCP, packets. 3.2 Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister which modifies the packets. 3.3 Spoofing means pretending to be something you are not. In Internet terms it means pretending to be a different Internet address from the one you really have in order to gain something. 3.4 Viruses and Worms Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms affect the networks by flooding them with huge amounts of bogus traffic, usually through e-mail. 3.5 Key loggers suppose, everything you type in the system is mailed to the hacker..!! It would be easy to track your password from that. Key loggers perform similar functionalities. So next time you type anything. Beware..!! 3.6 Social Engineering This was one of the oldest tricks for hacking. If the hacker try to convince user that you are a legitimate person from the system and needs your password for the continuation of the service or some maintenance. But it won’t work because it is an old technique. 3.7 Fake Messengers In this hacking technique, attacker send the fake messages so that the user can fill his own information like login id, password , etc[4],[5].

4. CRACKING

Cracker is the common term used to describe a malicious hacker. Crackers get into all kinds of mischief, including breaking or "cracking" copy protection on software programs, breaking into systems and causing harm, changing data, or stealing. Hackers regard crackers as a less educated group of individuals that cannot truly create their own work, and simply steal other people's work to cause mischief, or for personal gain. Crackers break into or crack systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal secret information, often making other people miserable

5 TECHINIQUES OF CRACKING

There are three basic types of password cracking techniques that can be explained below,

1. Dictionary Cracker can run a file of words against user accounts, and if the password is found to be simple word, it can be found pretty quickly.
2. Hybrid We know that the user utilize common method to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.
3. Brute force This technique of hacking is complex one and time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broke.
4. PROPOSED IDEA There are a few variations on the types of attacks that successfully employ hacking. Although some are relatively dated, others are very pertinent to current security concerns. Hacking consists of several steps, which I will briefly outline here, then explain in detail

5. First, the target host is chosen. Next, a pattern of trust is discovered, along with a trusted host. The trusted host is then disabled, and the target's TCP sequence numbers are sampled. The trusted host is impersonated, the sequence numbers guessed, and a connection attempt is made to

a service that only requires address-based authentication. If successful, the attacker executes a simple command to leave a backdoor. Details of an Attack Hacking in brief consists of several steps; 1. Selecting a target host (or victim). 2. The trust relationships are reviewed to identity a host that has a “trust” relationship with the target host 3. The trusted host is then disabled and the target’s TCP sequence number are sampled. 4. The trusted host is then impersonated, the sequence number forged (after being calculated). 5. A connection attempt is made to a service that only requires address-based Authentication (no user id or password).
6.IF a successful connection is made, the attacker executes a simple command to leave a backdoor.

7. DIFFERENCE BETWEEN HACKING AND CRACKING

The main difference between these two techniques is “Hacking builds things” and “Cracking breaks them”. Hacking and cracking are the two different forms of Internet and computer related privacy, usually hazardous. In this article, I’ll be discussing the differences between hacking, and cracking[8]. They are two completely different things, but people usually get confused between the two, they both end with a similar sound ‘Hacking’ and they’re both malicious forms of cyber activity. In this article, I’ll be talking about the difference between hacking, and cracking. A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multiple of reasons, such as profit, protest, or challenge. Malicious attacks on computer networks are officially known as cracking, while hacking truly applies only to activities having good intentions. Most non-technical people fail to make this distinction. Besides all these, it’s extremely common to see the term "hack" misused and be applied to cracks as well

8. CONCLUSION

In this work, at last I want to conclude that, how the attacker affects the security which tremendously affect our growing environment. Many security experts are predicting a shift for hacking in which hackers can exploit a weakness in a particular service to send and receive information under false identities. As Security professionals, we must remain current with the Operating Systems that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks. Understanding how and why attacks are used, combined with a few simple prevention techniques, can help protect your network from hacking.

Our main goal in this paper is to show how these two techniques i.e. hacking and cracking are performed in various ways and how the attacker can easily attack the users system using these two techniques.

SOLUTIONS

Social responses One strategy for combating phishing is to train people to recognise phishing attempts and to deal with them . Education can be promising, especially where training provides direct feedback. People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the email apparently originates to check that the email is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message. Technical responses Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem. Helping to identify legitimate sites Since phishing is based on impersonation, preventing it depend on some reliable way to determine a website's real identity. For example, some anti-phishing toolbars display the domain name for the visited website. The pet-name extension for Fire-fox lets users type in their own labels for websites, so they can later recognize when they have returned to the site. If the site is suspect, then the software may either warn the user or block the site outright. Fake Web sites Fake bank websites stealing account numbers and passwords have become increasingly common with the growth of online financial transactions. Hence, when using online banking, we should take precautions like using a secure encrypted customer's certificate, surf the net following the correct procedure, etc. First, the scammers create a similar website homepage; then they send out e-mails with enticing messages to attract visitors. They may also use fake links to link internet surfers to their website. Next, the fake website tricks the visitors into entering their personal information, credit card information or online banking account number and passwords. After obtaining a user's information, the scammers can use the information to drain the bank accounts, shop online or create fake credit cards and other similar crimes. Usually, there will be a quick search option on these fake websites, luring users to enter their account number and password. When a user enters their account number and password, the website will respond with a message stating that the server is under maintenance. Hence, we must observe the following when using online banking: Observe the correct procedure for entering a banking website. Do not use links resulting from searches or links on other websites. Online banking certifications are currently the most effective security safeguard measure. Do not easily trust e-mails, phone calls, and short messages, etc. that asks for your account number and passwords.
Solutions Internet Explorer 7 and Fire-fox 2 both have sophisticated filters that can detect most fake websites. Here are some other clues that might give away a fake: • Look for evidence of a real-world presence: an address, a phone number, an email contact. If in doubt, send an email, make a phone call or write a letter to establish whether they really exist. • The website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers. • Right-clicking on a hyperlink and selecting "Properties" should reveal a link's true destination - beware if this is different from what is displayed in the email. • Even though you are asked to enter private information there is NO padlock in the browser window or 'https://' at the beginning of the web address to signify

that it is using a secure link and that the site is what it says it is. • A request for personal information such as user name, password or other security details IN FULL, when you are normally only asked for SOME of 49 them. • Although rare, it is possible for your computer to be corrupted by viruses in such a way that you can type a legitimate website address into your browser and still end up at a fake site. This problem is known as 'pharming'. Check the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed. Subtle changes ('eebay' instead of 'ebay' for example) may indicate that your computer is a victim of a pharming attack. Pharming Similar in nature to phishing, Pharming (pronounced farming) is a Hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses - they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years pharming has been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Spoofing A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. A closely interconnected and often confused term with phishing and pharming is spoofing. A "spoofer", in Internet terms, is defined generally as the "cracker" who alters, or "forges", an e-mail address, pretending to originate a message from a different source address than that which he or she truly has. There are many ways an attacker may do this, and there are many types of attacks. The attacker may do this to gain access to a secured site that would accept the "hijacked" address as one of few permissible addresses, or more maliciously, the reason may be to hide the source of any type of attack. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). Spoofing Attacks Techniques Spoofing attacks can be divided into different categories, some of which are elaborated below: Man-in-the-middle attack and internet protocol spoofing An example from cryptography is the man-in-the-middle attack, in which an attacker spoofs Alice into believing they're Bob, and spoofs Bob into believing they're Alice, thus gaining access to all messages in both directions without the trouble of any.

REFERENCES

1. Hacking: The Basics,Zachary WilsonApril 4, 2001Updated by Martin Poulin, GSEC, GCWN, GCIH, CISSPJune 27, 2006
2. The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue: The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE’13], San Francisco State University, CA, U.S.A., March 2013 Doi: 10.7321/jscse.v3.n3.74 e-ISSN: 2251-7545

3. Analysis of Increasing Malwares and Cyber Crimes Using Economic Approach
4. 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 10,Ethical Hacking Procedure Certified Ethical Hacking Ethical Hacking : Future
5. All Types Of Hacking Techniques, http://hackerhubz.blogspot.in/2009/10/all-types-of-hacking-techniques.html
6. Stevens, W. Richard. TCP/IP Illustrated Volume I: The Protocols. Boston, Mass. : Addison-Wesley, 2004.
7. Wright G.R., Stevens, W. R. TCP/IP Illustrated Volume II: The Implementation. Boston, Mass. : Addison-Wesley, 1995.
8. Comer, Douglas E. Internetworking with TCP/IP Volume I: Principles, Protocols and Architecture. Upper Saddle River, New Jersey. : Prentice Hall, 1995
9. Practical Hacking Techniques and Countermeasures by Mark D. Spivey, CISSP
10. Is Ethical Hacking Ethical?,Danish Jamil et al. / International Journal of Engineering Science and Technology (IJEST)
11. Teaching ethical hacking in information security curriculum: A case study,Global Engineering Education Conference (EDUCON), 2013 IEEE,13-15 March 2013.