Discussion on the Technology of Computer Network Hacker Attack and Defense

Xinliang Zhu[1,2]

[1]School of Optical Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, 200093, China

[2]Information Office, University of Shanghai for Science and Technology, Shanghai, 200093, China

Keywords: Computer network; Hackers; Offensive and defensive technology

Abstract. Along with the rapid development of science and technology, computer network increasingly proficient, and widely used in various industries. But the presence of the hacker network attack formation, serious threat to the computer network security, how to deal with the network hacker attacks become a hot topic in the attention from all walks of life. In this paper, the computer network hacker attack and defense technology carries on the discussion and research, in order to offer the reference for the professional visitors to study.

Introduction

With the development and application of computer network technology, in the process of using computer network hacker attacks also more and more frequent, as a computer programmer when writing code, there will be more or less holes. These holes will be network hackers, hackers to steal, tampering with or steal data and information from a computer, causing immeasurable loss.

Overview of computer hackers

Hackers concept

Hackers is the transliteration of English “Hacker”, usually some computer amateur or professional invaders, and computer skills and levels of Hacker Cracker, or out of invasion of curiosity and a sense of accomplishment, or invasive with poor safety protection system as the other important springboard of the machine, or to apply system resources, theft of confidential information, and malicious attacks. Hackers can use various methods and means of computer network attack.

The main means of hacker attack

The traditional means of hackers attack

1). Social engineering attacks: social engineering attacks are hackers based on the weakness of human nature, social psychology, such as knowledge, through to the target host operator to monitor, access to an important sensitive information, and thus to attack the target host. During the attack, hackers will pass the target which is to send E-mail, wireless communication tools, a variety of ways, such as telephone, SMS to deceive the target, or use other means and strategy, to indirect access to the password, or other important information, and then an analysis of the information obtained through the access control of the target host access, using the network to attacking it.

2). Information collection type attack: information collection type of attack is to point the hacker to attack the target host and other related facilities, and the target host for reconnaissance information management personnel, familiar with and master the target security situation, in order to find a means attacking target vulnerability.

3). Cheat type attack: Cheat type attack is a hacker using network trust relationships between entities to IP spoofing, Web fraud, mail fraud and non-technical deception, such as a means to reach the purpose of attack [1]. IP spoofing is a network hacker through the mutual trust relationship between the host, the action of IP packets forged as the source IP address, pretend to be other systems or the sender's identity, to use a computer to the Internet, and use another machine IP address, pretend to be another machine with the server dealing with the means of attack; Web of deception is a kind of

difficult to detect attack technique. Hackers can make one have the same Web pages and Web link errors, after the attacker click open the browser, hackers will steal an attack skill all information relevant Web; Mail fraud is a hacker from his identity information and forged into the mail server administrator email scams, diddle user account information and other relevant information.

4). Loopholes and defects attacks: Loopholes and defects against refers to hackers using programmers write system loophole attack or deficiencies in a way. Its performance is mainly a buffer overflow attack, denial of service attacks and distributed denial of service attack [2]. Buffer overflow attacks are hackers to fill in data in a computer buffer digits, make its more than buffer capacity itself, causes the failure of the program runs, the system shutdown, restart, etc., hackers use this time to unauthorized instructions, acquisition system privilege, for all kinds of illegal operation; Denial of service attack by sending a large number of PNG useless packets, the hacker to paralyze the part or the entire computer website and network of a kind of technique; Distributed denial of service attack is on traditional Dos attack means a kind of evolution, the single way of one-to-one attack to evolve into a means of distributed denial-of-service attack.

5). Utilize type attack: Utilize type attack is by using the methods of guessing passwords, trojans directly on the host attack, thereby achieve control of the host [5] .

The hacker attacks ways in the new period

1). Hardware attack: Hardware attack is a new means of attack, the hacker directly on the host BLOS chip implanted Trojans, viruses, direct damage to host firewalls, antivirus software, so as to control the host system and various kinds of method permissions.

2). Virtual machine attack: Virtual machine attack is a hacker attack: the virtual machine virtual machine developed a new type of attack methods, through the virtual machine will attack the host whereabouts hide, and then to attack the target host.

3). Wireless technology attacks: wireless technology is a network hacker using mobile phone; wireless sensor network technology, Bluetooth technology, infrared technology and wireless communication technology such as RFID to hacking and data of the user and the enterprise information intercept method.

Tools that hackers are commonly used.

1). Scanner: scanning device is hacking through to the target host various TCP port scan, access to the target host software version information, to grasp the target host's weakness, to attack the target host.

2). Password attack: password to password cracking or password hacker attack is destruction of a tool, can quickly help hacking into the host.

3). Trojan horse programs: a Trojan horse program is a hacker that using malicious programs to Trojan horse lurk in the user's computer, so as to capture the user and the control system of the remote access.

4). Network sniffer: the network sniffer is a hacker through a network adapter installed on a network sniffer, thereby to steal of effective information and data, and then destroy the whole network system.

Techniques discussed of computer network hacker attack and defense in this paper

1). Data encryption: data encryption is based on the data, information and data encryption, prevent hackers to monitor and attacks, to ensure data security. Commonly used with DES and RSA encryption method [7] .

Short for DES is a Data Encryption Standard, it is a use of secret key Encryption algorithm, through the initial displacement and inverse displacement according to a 64 - bit clear text input block combination transform method called 64 - bit cipher text output block. Initial displacement is the input of a 64 - bit data blocks are divided into each part of the long 32-bit L0, R0 two parts, and then input the 58th to first, 50th to 2nd... And so on, the last one is the original. 7. For example: set in the input values for D1D2D3 before... D64, after the initial displacement results as: L0 = D58D50... The D8. R0 = D57D49... D7. Inverse displacement is after 16 times iteration computation, and the

computing results L16, input and inverse displacement R16. Inverse displacement is the initial displacement on the basis of inverse operation again, it can effectively guarantee the data security, the DES method which has been widely applied in computer network system.

RSA is one of the computer technology of the most influential public key encryption algorithm, it is composed of encryption key and decryption keys, in the RSA algorithm, RSA key length is 500 bits long, at least 1024 is usually used. Only a relatively short RSA key has been compromised, the length longer RSA keys is not easy to be cracked. This requires the use of a longer key to guarantee its safety, the length of the same level of security for RSA key, such as table 1.

Table 1. The length of the same level of security for RSA key

Level of confidentiality	Symmetric key length（bit)	The length of the key for RSA（bit）	The length of the key for ECC（bit）	Secret years
80	80	1024	160	2010
112	112	2048	224	2030
128	128	3072	256	2040
192	192	7680	384	2080
256	256	15360	512	2120

2). Access controls: Access controls is based on user identity information and ownership by a predetermined range, to limit their access to certain information, or to limit its use some kind of control function, general access control is usually a system administrator on the server, directories, files, information, data and network resources access control. Access control mainly includes the subject control, object control and control strategy. The type of access control are discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC). Discretionary access control is through the files, folders, share resources such as unique resources for access control system. The user can free to set access permissions; Wallpaper is access control system for the main body of the wallpaper of access control methods, generally only the system administrator can determine the user's access and security level, and the users themselves cannot free to change its access permissions. MAC commonly used security level is divided into four levels: Top Secret level (Top Secret) levels, Secret (Secret), Confidential (Confidential) and no grade level (Unclas Sified), including T > S > C > U [3]. All users of the system and processes as the main body, documents and data as the object, security label distribution respectively, to identify the safety level. RBAC is the abbreviation of Role-based Access Control. Role - -based Access Control, it is through the study of the Role of the user to Control Access to methods. Its main is according to the needs of different tasks, different roles are defined, and then the resource and operation permissions distribution of the different roles in a reasonable manner, to give a same role to groups of users to specify a role for access control.

3). Access controls: Access control is after confirm the identity of visitors' information, giving visitors identity information to different access control, and restrict user access to system resources, or data. The UNIX and Windows NT system USES is with access mechanism is similar; including firewall system and USES this mechanism. Unix and Windows NT system first with the identification of key to request access to users, when the user's real identity confirms, given different access permissions to users; Firewall according to different source address, source port, aim for a variety of software, information, such as testing, decide whether to let the packet pass.

4). Identity authentication: Identity authentication is through to the user, the network host, file, data testing to confirm the visitor identity authenticity, after confirm the user identity, it will give different users access accordingly. Due to the computer network of the world, all information is represented by a specific set of data or code. The computer system can to digital authentication of user identity, including the user access to accept. It is to distinguish by Numbers. The identity authentication technology is the first hurdle that users enter the network resources, when other operations before entering the network system. Identity authentication is through the secret information, had commonly objects and features three ways [4]. Among them, the secret information authentication has two kinds of password authentication and encryption authentication. Password authentication identity information is a common method of encryption authentication is to confirm

the data owner's identity information, such as: IC card for identity authentication should be based on user information such as sound or fingerprints on the user for confirmation.

5). Security audit: Security audit is through professional auditors and property owners commissioned according to the relevant laws and regulations and the administration of authorization, the computer network environment related activities and behavior of the system of independent checks, and the test process and safety information about data record and analysis, finally it makes a safety assessment. The network system security and reliability have certain difference. For example, when a hacker attacks on computer network system, the number of its registered failure will effectively reflect in the system, source and various user identity information will be recorded, as an effective evidence investigation hackers. Related to network security personnel according to the information and data to track of hackers, or analyze hacker, way of preventing hacker attacks. WTMP in the UNIX system files automatically to historical records, user registration and login Windows NT system will use Event Viewer to must examine every major record in the system, discover the unsafe factors in system.

6). Safety monitoring: safety monitoring is a computer network or a host of various activities for the whole real-time monitoring, and analyze the user behavior and system, it makes system vulnerabilities or unsafe problems of configuration that is effectively monitoring, data integrity protection system, and carries on the track record of abnormal behavior, hackers will effectively report all kinds of violation of the network safety regulations. For example, when hackers masquerading as user identity to continuous monitoring system or network login, and register failure, it will monitoring system to detect of hacking, at the same time, the security system will be via E-mail, call a pager or safety warning sound to contact the system administrator. The safety system realized the plot of hacking situation is more serious when, also it will automatically stop a service system, and even stop the entire system, to minimize the damage. In addition, the safety system can be known by the hacker attack characteristics, to analyze the hacker intrusion behavior, and try to tracking the hackers' whereabouts.

7). Security scanning: Security scanning is the use of the known samples, for the various backdoor virus or malicious code such as scanning system. In the scanning process, the user need to update, known samples of antivirus software to update the virus in the code, it make the scanner found in time all kinds of malicious code, avoid virus invasion.

Conclusion

In conclusion, the encrypted data information, the user is the identity authentication and access control, and scanning and monitoring, timely to a computer system, all these can effectively reduce the computer network hacker attacks. Computer network hacker attacks by people from all walks of life concerns, it needs every use of personnel computer networks have higher awareness and at the same time, the computer network researchers and programming staff are more to delve into the computer network technology, reduce the computer network vulnerability, prevent hacker intrusion.

References

[1] Lu Fengjun. Ethics research of network hacker. *Science advisory (management science and technology)*, 2014(07) .

[2] Kong Qingwei, The dangers and reply of hacking. *Industrial and technology BBS*, 2013(05).

[3] Xu Rongsheng. Discuss of new hacking techniques. *Journal of information security and communication security*, 2011(01).

[4] Yang Minghua. Prevent hacking attacks computer main method. *Journal of software Tribune*, 2012(02).

[5] Chen Haihong, Yan Yanlihua. Hackers technology research. *Journal of Chi Feng institute (natural science edition)*, 2010(01) .