Information and Computer Security (2018)

Original Research Article

Computer Network Attack and Defense Technology

Xinyue Yang,Shujun Zhou,Guanghui Ren,Yaling Liu

Computer Engineering, North Sea University of Technology, Guangxi, China

ABSTRACT

In recent years, the Internet as a symbol of the computer network protocols, standards and application technology development is extremely rapid. But the Internet is like a sharp double-edged sword, it is for the convenience of people at the same time, but also for computer viruses and computer crime to provide the soil, for systems, network protocols and databases, whether it is its own design flaws, or due to human factors caused by a variety of security vulnerabilities, may be some of the other attempts to use hackers and attack, so the establishment of an effective network security system is even more urgent. To ensure network security, reliable, you must be familiar with the general process of hacker network attacks. The only way to do before the hacker attack the necessary precautions is to ensure that the network is safe and reliable operation. This article comprehensively analyzes the steps, methods and common attack tools of network attack, and tells the concrete precautionary measures from several aspects, so that readers have a comprehensive network of knowledge, in the treatment of network threats are well prepared.

KEYWORDS: hacker network security attack defense

1. Introduction

With the progress of society, the development of the times, the computer network in people's lives become more and more important, people use the network more and more frequently, this is the trend of the times. Network in the continuous development, updating, progress, some confidential information will become very important, information warfare has started, network security technology research without delay.

2. Computer Network Security

Computer network security refers to the use of network management control and technical measures to ensure that in a network environment, the data confidentiality, integrity and usability can be protected. Computer network security includes two aspects, namely, physical security and logical security. Physical safety means that the system equipment and related facilities are physically protected from damage, loss and so on. Logical security includes information about the integrity, confidentiality and availability.

Computer network security includes not only the hardware of the network, the software that manages the control network, but also the shared resources and the fast network service. Therefore, the definition of network security should consider covering all the contents of the computer network. According to the definition of computer security given by ISO, it is considered that computer network security means that 'the hardware, software and data resources in the computer network system are protected from accidental or malicious reasons, so that the network system is continuous and reliable, the normal operation of the network and the normal network services.

Because of the development of the Internet, the whole world economy is rapidly integrating, and the whole country is like a huge network of machines. Computer network has become the country's economic base and lifeline. The computer network is rapidly gaining popularity in all areas of economy and life, and the whole society is increasingly dependent on the network. A large number of enterprises, organizations, government departments and institutions are in the formation and development of their own network, and connected to the Internet to fully share, the use of network information and resources. The network has become a powerful driving force in social and economic development. Its status is more and more important. With the development of the network, but also produced a variety of problems, including security issues are particularly prominent. Understand the various threats facing the network, prevent and

eliminate these threats, to achieve real network security has become the most important thing in the development of the network.

3. Network security status and hidden dangers

The problem of network security has become a common challenge for human beings in the information age. The domestic network security problem is also becoming more and more prominent. The information system is facing the challenge of network security. The information system has many weak links in forecasting, responding, preventing and restoring ability. The information system is facing the challenge of network security. The information system has many weak links in the prediction, reaction, prevention and recovery ability, and internet political subversive activities frequently.

With the deepening of the information process and the rapid development of the Internet, people's work, study and way of life are undergoing tremendous changes, the efficiency is greatly improved, and the information resources are shared to the greatest extent. But must be seen, followed by the development of information technology network security issues increasingly prominent, if not a good solution to this problem, will hinder the development of information technology.

According to statistics, the current global average every 20 seconds will happen with the Internet host was invaded the incident, the United States 75% to 85% of the site cannot resist hacking, about 75% of corporate online information theft, of which 5% of the enterprise loss more than $ 50,000. And the spread of the virus through the network regardless of its speed of transmission, spread and destructive aspects than the single virus is more discolored. At present the world has found more than 50,000 kinds of viruses, and still more than 10 kinds of growth rate every day. Data show that the virus caused by the loss of network economic losses accounted for 76%.

Shen Changxiang, academician of the Chinese Academy of Engineering, said: 'Building information and network security line is of great importance, without delay.

In the field of computer crime and network infringement, whether it is the number, means, or nature, size, has come to a staggering point. According to statistics, the United States each year due to network security problems suffered more than 17 billion US dollars of economic losses, Germany, Britain are also more than billions of dollars, France for 10 billion francs, Japan, Singapore is also very serious. In the international criminal law circles listed in the modern society of new crime list, computer crime has been ranked first. In 2003, 56% of the 524 organizations interviewed by the CSI / FBI survey met computer security incidents, of which 38% met 1 to 5 and more than 16% had encountered 11 or more. The number of organizations that have become frequent attacks on the Internet has been increasing for three consecutive years; the denial of service (DoS) has risen from 27% in 2000 to 42% in 2003. According to the survey, 96% of the 521 organizations surveyed had Web sites, 30% of which provided e-commerce services, and 20% of these sites were found to have been unlicensed or misused in 2003. Even more disturbing is that 33% of organizations say they do not know whether their site is damaged. According to statistics, the global average every 20s on an online intrusion, hackers once found the weak part of the system, all users will suffer.

3.1. Potential Threats

There are many factors that make up the insecurity of computer information, including human factors, natural factors and occasional factors. Among them, the human factor means that some criminals use the computer network exists loopholes, or sneak into the computer room, theft of computer system resources, illegal access to important data, tampering with system data, destruction of hardware equipment, the preparation of computer viruses. Human factor is the biggest threat to computer information network security. Computer network insecurity mainly in the following areas:

(1) Five characteristics of network security:

Confidentiality: Information is not disclosed to unauthorized users, entities or processes, or for their use.

Integrity: The characteristics of data that cannot be changed without authorization. That is, the information stored in the storage or transmission process is not modified, not destroyed and lost characteristics.

Availability: Features that can be accessed by authorized entities and used as needed, whether or not to access the required information when needed. Such as denial of service in the network environment, destruction of the network and the normal operation of the system are all on the availability of attacks.

Controllability: the ability to control the dissemination and content of information.

Reviewability: The basis for the security issues that arise

(2) Vulnerability of computer networks:

The Internet is open to the world of the network, any unit or individual can easily transfer and access to a variety of information online, the Internet has this open, shared, international features on the computer network security challenges. Internet insecurity mainly has the following:

(3) The openness of the network

Network technology is fully open, making the network facing attacks from many aspects. Or attacks from physical transmission lines, or attacks from network communication protocols, as well as attacks on computer software and hardware vulnerabilities.

(4) The international nature of the network

It means that the attack on the network is not only from the local network of users, but also other countries on the Internet hackers, so the security of the network is facing the challenges of internationalization.

(5) Freedom of the network

Most of the network on the use of the user without technical constraints, users can freely access, publish and obtain all kinds of information.

Therefore, there are many unpredictable factors in the network, the Internet is open to the world network, security has become a big problem, in order to protect the security of information, we must strengthen the network security construction.

4. Network attack and defense technology

Hacker attacks and network security is closely together, the study of network security does not study hacking technology is simply on paper, research attack technology does not study the network security is behind closed doors. In some sense, there is no security without attack, the system administrator can use the common attack means to detect the system, and the relevant loopholes to take measures.

Cyber-attacks have goodwill and malicious, well-intentioned attacks can help system administrators check system vulnerabilities, malicious attacks can include: for personal grievances and attacks, business or personal purpose to obtain secret information, national hatred, the use of the other side of the system resources to meet their own the demand, to seek excitement, to others to help and some non-purpose attack. Therefore, each of us is likely to face a security threat, it is necessary to understand the network security, and be able to deal with some security issues.

4.1. Network Attack Steps:

Here we look at how those attackers find your computer security vulnerabilities, and to understand their attack techniques.

A successful attack, can be summarized into the basic five steps, but according to the actual situation can be adjusted at any time, summed up is the 'hacker attacks Penta.'

(1) The first step: hidden IP

This step must be done, because if the traces of their own invasion were found, when the FBI to find the door when everything is late. There are usually two ways to achieve your own IP hidden:

The first method is to first invade a computer on the Internet (commonly known as 'broiler'), the use of this computer to attack, so even if found, but also 'broiler' IP address.

The second way is to do multi-pole springboard 'Sock agent', so that the invasion of the computer is left behind the proxy computer's IP address, such as attacking A country's site, the general choice from the A country far from the B country computer as 'broiler' or 'agent', so cross-country attacks, generally difficult to be detected.

(2) The second step: check out the location of the scan

Check out the location is the way to attack the target through a variety of ways to understand (including any available clues, but to ensure that the information is accurate), determine the attack time and place.

The purpose of the scan is to use a variety of tools in the attack target IP address or address on the host to find loopholes. Scanning is divided into two strategies: passive and active.

(3) Step 3: Obtain system or administrator privileges

Get the authority of the administrator is to connect to the remote computer, to control, to achieve their own attack purposes. Access to system and administrator privileges are: through the system vulnerabilities to obtain system

privileges; through the management of vulnerabilities to obtain administrator privileges; through software vulnerabilities to get the system permissions; by listening to obtain sensitive information to obtain the appropriate permissions; through the weak password to obtain the remote administrator's User password; through the exhaustion method to obtain the remote administrator's user password; by breaking the target machine has a relationship with another machine to get the target machine control; by deceiving access to authority and other effective methods.

(4) The fourth step: planting the back door

In order to maintain long-term access to their own fruit, in the already broken computer to plant some of the back door for their own visit.

(5) The fifth step: in the network stealth

After a successful invasion, generally in the other side of the computer has been stored on the relevant log, so easy to be found by the administrator, after the invasion needs to clear the login log has other relevant log.

4.2. Attackers commonly used attack tools:

D.O.S attack tool:

Such as WinNuke by sending OOB loopholes lead to the system blue screen; Bonk by sending a large number of forged UDP packets lead to system reboot; TearDrop by overlapping IP fragments caused by the system's TCP / IP stack collapse; WinArp by sending special packets on the other machine FluShot causes the system to solidify by sending a specific IP packet; Bloo causes the system to slow down or even solidify by sending a large number of ICMP packets; PIMP passes through the IGMP Loopholes lead to the system blue screen or even restart; Jolt through a large number of forged ICMP and UDP system has become very slow or even restart.

Trojan horse program:

(1) BO2000 (BackOrifice): It is the most powerful TCP / IP framework of the attack tool, you can collect information, execute system commands, reset the machine, redirect the network client / server application. BO2000 supports multiple network protocols, which can be transmitted using TCP or UDP, and can be encrypted with XOR encryption algorithms or more advanced 3DES encryption algorithms. BO2000 after the machine is completely under the control of others, hackers become super users, all of your operations can be BO2000 comes with the 'secret camera' recorded as 'video'.

(2) 'Glacier': Glacier is a domestic Trojan program, with a simple Chinese use interface, and only a few popular anti-virus, the firewall can be found in the existence of glaciers. Glacier function than the foreign Trojans to no less. It can automatically track the target machine screen changes, you can completely simulate the keyboard and mouse input, that is, while the host side of the screen changes and monitor the synchronization occurs at the same time, the monitoring side of all keyboard and mouse operation will be reflected in the control side of the screen. It can record a variety of password information, including the boot password, screen saver password, a variety of shared resource passwords and the vast majority of the dialog box appeared in the password information; it can get system information; it can also carry out registry operations, including the main key to browse, add or delete, copy, rename and read and write keys and all other registry operations.

(3) NetSpy: can run on Windows95 / 98 / NT / 2000 and other platforms, it is a TCP / IP based on a simple file transfer software, but in fact you can see it as a no authority to control the enhanced Type FTP server. Through it, the attacker can unknowingly download and upload any file on the target machine, and can perform some special operations.

(4) Glacier: the program can automatically track the target computer's screen changes, access to the target computer login password and a variety of password class information, access to the target computer system information, limit the target computer system functions, any target computer files and directories, remote shutdown, send information and other monitoring functions, similar to BO2000.

(5) KeyboardGhost: Windows system is a message loop (MessageLoop) based on the operating system. The core area of the system retains a certain byte as the buffer for the keyboard input, and its data structure is a queue. Keyboard ghost is directly through the visit to the queue, so that the keyboard to enter your e-mail, proxy account, password (displayed on the screen is the asterisk) to be recorded, all involved in the form of an asterisk to display the password window all the symbols will be recorded, and in the system root directory to generate a file called KG.DAT implicit file.

(6) ExeBind: This program can be specified in the attack program bundled to any widely popular software, so that the host program execution, parasitic procedures are also implemented in the background, and support multiple bundles. In fact, by dividing the file several times and many times from the parent process to call the child process to achieve.

4.2.3 Several types of attacks and defense practices introduced

Attack Type Service Denies Attack

Defining a Service Denies an Attack by attempting to crash your service or crush it to prevent you from providing a service that denies an attack is the easiest way to attack,

Method Overview Defense

Since the early stage of the router, the maximum size of the router is limited, many operating systems on the TCP / IP stack implementation in the ICMP package is specified 64KB, and in the header of the package header after reading, the buffer is generated for the payload based on the information contained in the head of the header. When a packet that generates a deformed body that claims to exceed the ICMP upper limit is loaded with a size exceeding 64K, the memory and allocation error caused the TCP / IP stack to crash, causing the receiver to crash. Now all standard TCP / IP implementations have been implemented to deal with oversized packages, and most firewalls can automatically filter these attacks, including Windows, NT (after service pack 3), linux, Solaris, and Mac OS Have the ability to resist the general ping of death attacks. In addition, the firewall configuration, blocking ICMP and any unknown protocol, are to prevent such attacks.

Teardrop The teardrop attack uses the information contained in the header of the packet in the TCP / IP stack implementation that trusts the IP fragment to implement its own attack. The IP segment contains information indicating which segment of the original package is included, and some TCP / IP (including NT before service pack 4) will crash when it receives a fake segment containing an overlapping offset. The server applies the latest service packs, or reorganizes the segments when setting up the firewall, rather than forwarding them.

UDP floods A variety of fake attacks use simple TCP / IP services, such as Chargen and Echo, to deliver useless bandwidth-rich data. By forging a UDP connection with a host's Chargen service, the reply address points to a host that runs the Echo service, which generates enough unwanted data streams between the two hosts, if enough Data flow will lead to bandwidth service attacks. Turn off unnecessary TCP / IP services, or configure the firewall to block UDP requests from these services from the Internet.

SYN floods Some TCP / IP stack implementations can only wait for ACK messages from a limited number of computers because they have only a limited memory buffer used to create a connection if the buffer is filled with a false connection Initial information, the server will stop responding to the next connection until the connection in the buffer attempts to time out. In some implementations that create unrestricted connections, SYN floods have a similar effect. Filter the subsequent connections from the same host on the firewall. The future SYN flood is worrying, because the release of the flood does not seek response, it cannot be from a simple high-capacity transmission identified.

Land attack In a Land attack, a specially crafted SYN packet has its original address and destination address set to a server address, which will cause the receiving server to send a SYN-ACK message to its own address. As a result, the address Send back an ACK message and create an empty connection. Each such connection will remain until the timeout occurs. Unlike the Land attack, many UNIX implementations will crash and NT becomes extremely slow (for about five minutes). Playing the latest patch, or in the firewall configuration, those in the external interface on the station contains the internal source address filter out. (Including 10 domain, 127 domain, 192.168 domain, 172.16 to 172.31 domain).

Smurf Attack A simple smurf attack is made by flooding the victim host by using an ICMP reply request packet that sets the reply address to the broadcast address of the victim network, eventually causing all hosts on the network to make a request for this ICMP response Reply, causing the network to block, one or two orders of magnitude higher than the traffic of the pingof death flood. The more complex smurf will change the source address to a third party victim, eventually leading to a third party avalanche. Defense: To prevent hackers from using your network to attack others, turn off the external router or the firewall's broadcast address feature. To prevent the attack, set the rules on the firewall, discard the ICMP package.

Fraggle attack Fraggle attack on the Smurf attack made a simple change, using the UDP response message instead of ICMP. Filter out UDP reply messages on the firewall.

E-mail Bombs E-mail Bombs are one of the oldest anonymous attacks, by setting up a machine that constantly sends a large number of e-mails to the same address, and an attacker can drain the bandwidth of the recipient's network. Configure the e-mail address to automatically delete excess or duplicate messages from the same host.

Malicious messages attack many of the services on a variety of operating systems that have such problems, and since these services do not properly correct the error before processing the information, the information that receives the deformity may collapse. Hit the latest service patch.

Attack type exploits attack

Defining a exploit attack is an attack that attempts to control your machine directly,

Password guessing Once a hacker has identified a host and has discovered an available user account based on NetBIOS, Telnet, or NFS services, successful password guessing can provide machine control. The password which is difficult to guess can be used, such as the combination of words and punctuation. Ensure that services such as NFS, NetBIOS, and Telnet are not exposed to the public domain. If the service supports locking policies, it is locked.

Trojan horse Trojan is a program that is either installed directly by a hacker, or through an unquestionable user secretly to the target system. Once the installation is successful and the administrator privileges are available, the person who installed the program can remotely control the target system remotely. The most effective one called the backdoor program, malicious programs include: NetBus, BackOrifice and BO2k, for the control system benign procedures such as: netcat, VNC, pcAnywhere. The ideal backdoor program runs transparently. Avoid downloading suspicious programs and refuse to perform, and use network scanning software to regularly monitor TCP services on the internal host.

Buffer Overflow as a result of the fact that programmers use a function that does not perform a valid bit check like strcpy (), strcat () in a lot of service programs, it may eventually cause a malicious user to write a short process to further open the security gap and then the code is appended to the end of the buffer payload so that when a buffer overflow occurs, the return pointer points to the malicious code so that the control of the system is captured. Use SafeLib, tripwire to protect the system, or browse the latest security bulletin to update the operating system.

Attack type information collection type attack

Defining an information-gathering attack does not pose a hazard to the target itself, and such attacks are used to provide useful information for further intrusion. Mainly include: scanning technology, architecture spying, and the use of information services.

Scanning technology

The address scan uses ping to detect the destination address, and it responds to its presence. Defense: Filter the ICMP reply message on the firewall. Many firewalls can detect whether they are scanned and automatically block scanning attempts.

Port scanning often uses some software to connect a series of TCP ports to a wide range of hosts, and the scan software reports that it successfully establishes a port for the connected host.

The response maps hackers to send false messages to the host, and then judges which hosts are present based on the message ‘back to’ hostunreachable ‘. At present, due to the normal scanning activity is easily detected by the firewall, hackers instead use the firewall rules do not trigger the common message types, these types include: RESET message, SYN-ACK message, DNS response package. NAT and non-routing proxy servers can automatically resist such attacks, or you can filter ‘hostunreachable’ ICMP responses on the firewall.

Slow Scanning Since the implementation of a general scan detector is determined by monitoring the number of connections initiated by a particular host in a time frame (for example, 10 times per second) to determine whether the hacker can be scanned by using a slow scan Some of the scanning software scans through the lure service to detect slow scans.

The architecture detects that the hacker uses an automated tool with a database of known response types to check the response to bad packets from the target host. Because each operating system has its own unique response method (for example, NT and Solaris TCP / IP stack implementation is different), by comparing this unique response with the known response in the database, hackers are often able to determine the target host is running the operating system. Remove or modify a variety of BANNer, including the operating system and a variety of application services, blocking the port used to identify each other’s attack plan.

Use information service

DNS Domain Translation, DNS protocol does not authenticate the conversion or informational updates, which makes the protocol exploited in a number of different ways. If you maintain a public DNS server, hackers only need to implement a domain conversion operation will be able to get all your host name and internal IP address. Filter the domain conversion request at the firewall.

Finger service hackers use the finger command to spy a finger server to get information about the user of the system. Close the finger service and record the IP address of the peer to which the service is trying to connect, or filter it on the firewall.

LDAP service hackers use the LDAP protocol to snoop information about the systems and their users within the network. To block and record the LDAP of the internal network, if the LDAP service is provided on the public machine, the LDAP server should be placed in the DMZ.

Attack type false message attack

Define messages that are used to attack target configurations incorrectly, including: DNS cache corruption, forged e-mail.

DNS cache pollution Because DNS servers exchange information with other name servers without authentication, this allows hackers to incorporate incorrect information and direct users to hackers' own hosts. Filtering inbound DNS updates on the firewall, the external DNS server should not be able to change your internal server's awareness of the internal machine.

Forged e-mail Since SMTP does not authenticate the identity of the sender of the message, the hacker can forge an e-mail to your internal customer, claiming to be from someone who knows and believes, and comes with an installable Trojan horse program, Or a connection to a malicious Web site. Use security tools such as PGP and install e-mail certificates.

6. Conclusions

Network attacks are increasingly rampant, causing a great threat to network security. For any hacker's malicious attacks, there are ways to defense, as long as they understand the means of attack, with a wealth of network knowledge, you can resist hackers crazy attack. Some beginners network friends do not have to worry about, because the market has also launched a number of network security programs, as well as various types of firewall, I believe in the near future, the network will be a safe information transmission media. In particular, it is important to emphasize that cyber security education should be at the top of the security system at all times and that efforts to improve the security awareness and basic prevention of all network users are of great importance to improving the security of the entire network.

The future war is an information war, and cyber warfare is an important part of information warfare. Network confrontation, in fact, is the confrontation between people, it is embodied in the security strategy and attack strategy on the battle. In order to continuously enhance the security capability of information systems, we must fully understand the realization of the system kernel and network protocols, and truly understand the 'minutiae' of the other network system, and should be familiar with the preventive measures for various attack methods. 'Know thyself, ever-victorious'.

This paper discusses the attack methods and precautions of the network in many aspects, mainly to let everyone understand the problems of network security and the matters needing attention in order to maintain the network security. The best defense is the attack, only to understand the hacker's means of attack, we can take an accurate response to these people. The only way to do before the hacker attacks the necessary precautions is ensuring that the network is safe and reliable operation.

References

1. Mu Yong, Li Peixin. Defense! Network attack insider analysis. People's Posts and Telecommunications Press.
2. Feng Qianjin. Computer network attack and prevention. China University of Political Science and Law Press.
3. Shi Zhiguo. Computer Network Security Course. Tsinghua University Press, Beijing Jiaotong University Press.
4. Feng Yuan, Lan Shaohua, Yang Yuwang. Computer network security foundation. Science Press.
5. Jiang Jianchun, Feng Dengguo. Network intrusion detection principle and technology. National Defense Industry Press.
6. Chang Hong. Network complete technology and anti-hackers. Changchun Metallurgical Industry Press.
7. Xian Ming, Bao Weidong, Wang Yongjie. Introduction to the assessment of network attack effectiveness. National Defense University of Science and Technology Press.