RESEARCH ARTICLE | MAY 08 2017

The research of computer network security and protection strategy

Jian He

AIP Conf. Proc. 1839, 020173 (2017)
https://doi.org/10.1063/1.4982538

The Research of Computer Network Security and Protection Strategy

Jian He

Luoding Polytechnic, Luoding, Guangdong, 527200, China

Abstract. With the widespread popularity of computer network applications, its security is also received a high degree of attention. Factors affecting the safety of network is complex, for to do a good job of network security is a systematic work, has the high challenge. For safety and reliability problems of computer network system, this paper combined with practical work experience, from the threat of network security, security technology, network some Suggestions and measures for the system design principle, in order to make the masses of users in computer networks to enhance safety awareness and master certain network security technology.

Key words: Network Security; Technology; Strategies; Principle

INTRODUCTION

Nowadays, the application of computer network has extended to every corner of the world and areas, is an unprecedented impact on people's work and life, as well as electric power, transportation, and has increasingly become an integral part of people's life. At the same time, with the expanding of network size, and the understanding of network knowledge is more and more in-depth, more and more unsafe factors such as the network attack, has been a serious threat to network and information security. Computer network security has become a global concern. Computer network and information security technology is the core issue of the computer and network systems for effective protection. Network security protection involves very wide range, from a technical level, mainly including data encryption, identity authentication, intrusion detection and intrusion protection, virus protection and virtual private networks (VPNS), etc., some of these technologies is active defense, some of them are passive protection, and some are to provide support and platform for the research of security. Computer network security by adopting various technical and management measures, make the normal operation of the network system, to ensure the availability, integrity and privacy of network data. So, to establish the purpose of network security protection is to ensure that the data transmission and exchange through the network, not happen such as add, modify, loss and leak.

THE HIDDEN TROUBLE IN A TYPICAL COMPUTER NETWORK SECURITY

Routing protocol defects

(1) Source routing option using .Source routing in the IP header option is used to the IP packet routing, thus, an IP packet can be specified according to the forecast of routing to arrive at the destination host. But it also created opportunities for the invaders, when a host know in advance that there is a trusted host, you can use the source routing options disguised as a trusted host, so as to attack system, the equivalent of make the host may be under attack from all other hosts.

(2) The forge ARP packet. Forge ARP packet is a kind of very complex technology, involves many aspects of TCP/IP and Ethernet characteristics, in this as ARP security issues is not very appropriate. Fake ARP packet is the main process to the IP address of the destination host and Ethernet address for an ARP packet source address, this can

Materials Science, Energy Technology, and Power Engineering I
AIP Conf. Proc. 1839, 020173-1–020173-5; doi: 10.1063/1.4982538
Published by AIP Publishing. 978-0-7354-1509-6/$30.00

cause another IP spoof. In this attack mainly in switched Ethernet, switched Ethernet, exchange hub in receiving each ARP packet update Cache. Constantly send spoof ARP packet can make both packages sent to the destination host to an intruder, so switched Ethernet can be monitored. The ways to solve the above problems is: will exchange hub set as static binding. A feasible approach is when your host runs abnormally (slow network, IP packets presented .according to higher), reflect to the network administrator.

Windows operating system security flaw

ISAPI buffer overflow Microsoft IIS (Internet Information Server) is the most used Microsoft Windows NT and Windows 2000 Server software. At the time of install IIS, multiple ISAPI (Internet Services Application Programming Interface) is automatically installed. ISAPI allows developers to use a variety of dynamic link library DLLs to extend the IIS server performance. Some dynamic link libraries, for example, idq.dll, a programming error, so they are not correct boundary check. In particular, they don't block the long string. An attacker can take advantage of this to the DLL to send data, result in buffer overflow, and then control the IIS server. Solution to the problem of the above is if it is found that system has this kind of defect, then install the latest Microsoft patches. At the same time, should check and cancel all don't need the ISAPI extension. Regularly check whether these extensions is restored. Least privilege rule to remember is that the system should run the required minimum service system to work normally.

Safety defects existing in the Internet

The Internet use TCP/IP protocol, so the flaws of the TCP/IP protocol itself led to the development of the Internet is not safe. Although the TCP/IP protocol with strong ability, network interconnection technology, support for multiple independent application protocol etc., however, due to the agreement, when they were written without considering safety factors, so a lot of security problems in the agreement. Mainly include: TCP/IP protocol data flow using clear text transmission, especially in the use of HTTP, FTP, Telnet and user account and password in plaintext transmission, so the data information is easy to be online hacking, tampering and forgery.

(1) The Source Address Spoofing (the Source Address Spoofing), TCP/IP protocol in the IP Address as a unique identifier for the network node, the node's IP Address is not completely fixed, so the attacker can directly modify the node's IP Address within a certain scope, pretending to be a trusted node's IP Address.

(2) The Source Routing cheating (Source Routing Spoofing), IP packets for test purposes set up an options - IP Source Routing, this option can indicate to the node routing directly, so that the attacker can use this option to cheat, illegal connection.

(3) The routing information protocol (RIP) Attacks attack. RIP protocol used to publish dynamic routing information in the local area network (LAN), it is to provide consistent routing for the nodes in the local area network (LAN) designed and accessibility of information, but the node to receive the information authenticity checks, so an attacker could issue incorrect routing information online, take advantage of a router or host ICMG redirection information, realize the network attack.

(4) Identify attack (Authentication Attacks), the current firewall system only to identify the IP address, protocol port, to identify the effectiveness of the login user identity.

Computer Virus

Computer viruses can be stored, executable and can be hidden in the executable programs and data files without being found that trigger the access control system after an executable program, it is contagious, latent, triggers and destructive sexual characteristics. A computer virus is mainly transmitted by copying files, files, and run the program operation. In the course of everyday use, floppy disk, hard disk, CD and network is the main way of spreading the virus. Computer virus after running light could reduce the system efficiency, or may damage files, delete files, even make the data loss, destruction of the system hardware, all kinds of unpredictable consequences. In recent years, the emergence of a variety of malignant viruses are based on the spread of the network, the computer network virus damage is very big.

Artificial malicious attacks

This is the biggest threat to the computer network attack. Malicious attacks and can be divided into active attack and passive attack. Attack in various ways to selectively destroy the validity of the information and integrity; Passive attack is in normal working conditions, does not affect the network to intercept, and steals, deciphering to obtain important confidential information. These two kinds of attacks can cause great harm to computer networks, and lead to a leakage of important data. Now use the network software is more or less exist some shortcomings and vulnerabilities, network hackers often use intrusion into important means of information system, eavesdropping, obtain and attack into important information about the sensitivity, modify, and destroy the normal use of the information network, data loss or system paralysis, have significant political influence and economic losses to the country.

The natural environment

Computer network through wired links or radio waves to connect different areas of computer or terminal, often is information transmission in line, so the natural environment and social environment of computer network will produce a great impact. Bad for nature, such as temperature, humidity, dust conditions, such as earthquake, cyclone, fire and accident can cause serious damage to the network and influence; Heavy current, magnetic field would spoil transmission of data information. Computer network is also easy to lightning strike, lightning can easily through the cable and damage to the computer in the net, make computer network paralysis. There's not a good social atmosphere will increase to the network man-made destruction, bring devastating blow to system.

THE APPLICATION OF THE STRATEGY FOR NETWORK SECURITY TECHNOLOGY

Security is the security of the network to survive, only safe and secure, network can realize its own value. The development of network security technology as people network practice and development, it involves technical is very wide, the main techniques such as authentication, encryption, firewall and intrusion detection is an important defense of network security.

VPN Technology

VPN is the latest to solve the problem of information security, one of the most successful technology subject, a virtual private network (VPN) technology is on the public network to establish dedicated network, make the data through the security of encryption "pipe" in the public network. To build on the public communication network VPN there are two kinds of mainstream mechanism, these two mechanisms for routing filtration technology and tunnel technology. The current VPN mainly adopts the following four technology to ensure safe: tunnel technology, encryption technology, key management technology and user identity authentication technology and equipment. Among them, several popular techniques for the PPTP, L2TP tunnel and IPsec VPN tunnel mechanism should be able to have different levels of technology security services, the security services including different intensity of source identification, data encryption, etc. VPN have several classification methods, such as the access into the shuttle VPN and dial-up VPN; According to the tunnel protocol can be divided into the second and third layer; According to a way can be divided into sponsored by the client and the server.

Firewall technology

Firewall is a network access control devices, to refuse in addition to explicitly allow through all communication data, it is different from simple router will determine the direction of network information transmission, but access to the site in the network transmission through relevant to the implementation of a set of one or a set of system access strategy. Most firewalls are the combination of several functions to protect themselves, in the form of transmission network from malicious attacks, one of the most popular technology with static state of packet filtering, dynamic packet filtering, filtering, and the proxy server technology, increase their level of security, but in the concrete practice of the system should not only be considered cost performance, and to consider security network connectivity. In

addition, today's good also adopted the VPN and viewing of a firewall and intrusion detection technology. The firewall security control is mainly based on IP address, it is difficult to provide a consistent, both inside and outside the firewall security strategy for the user; And the firewall only coarse-grained access control, also can't and enterprise internal use other security mechanisms (such as access control) integrated use; In addition, difficult to manage and configure firewall by multiple systems (router, filters, proxy server, gateway, forts host) of firewall, management to avoid negligence.

Intrusion detection technology

Intrusion Detection technology is a hotspot in the research of the network security, is a kind of active safety protection technology, provides the invasions of internal, external and real-time protection misoperation, intercept corresponding Intrusion before network System compromised. Along with the development of the era, Intrusion Detection technology will develop in the direction of the three: distributed Intrusion Detection, intelligent Intrusion Detection and comprehensive security defense solutions. Intrusion Detection System (Intrusion Detection System, IDS for short) is a combination of software and hardware for Intrusion Detection, its main function is to detect, in addition to detecting part prevent invasion; Intrusion detection of precursors, thus processing, such as stop, closed, etc.; Invasion of the archive, providing legal basis; Network intrusion events under threat level assessment and recovery, and other functions.

Technically, there are two kinds of invasive monitoring detection model: (1) anomaly detection model, detection and acceptable behavior, the deviation between the every item if it is possible to define acceptable behavior, then each unacceptable behavior is invasion. The test model of non-response rates low, but higher rate of false positives. (2) Feature detection model; Detection and the degree of match between known unacceptable behavior, if it is possible to define all the unacceptable behavior, and each can match behavior will cause alarm. It will be all known system vulnerabilities and attack characteristics of composition an attack to the formal methods, such as libraries, and then will capture the packets with mode matching method and the features of library detailed comparison, to determine whether to attack or malicious invasion, low rate of false positives, this model but non-response rates higher. With the development of network technology, this method of testing the shortcomings and the insufficiency of gradually apparent: need to match the amount of data is too big, can only detect known attacks, such as easy to be deceived.

Data encryption technology

Is the purpose of information encryption protection network data, files, password, and control information, and protect the online transmission of data. The commonly used methods are link encryption, the endpoint encryption and encryption three nodes, the purpose of link encryption is to protect the network node link between information security; The end-to-end encryption is the purpose of the source end user to end user's data protection; Node is the purpose of encryption between the source node and destination node transmission link to provide protection.

Information encryption process is a concrete implementation by a variety of encryption algorithm, to provide high security and protection at the expense of the smaller. In most cases, information encryption is the only way to ensure information confidentiality. If according to the classification and the key is the same to the encryption algorithm can be divided into conventional cryptographic algorithms and public key cipher algorithm? In conventional password, use the same key, the receiver and the sender is the encryption and decryption keys are the same or equivalent. In public key cryptography, the receiver and the sender use keys are the same, and it is almost impossible from decryption key encryption key is derived in this paper. In practice, of course, people usually use the conventional password and public key cryptography together, such as: using DES or IDEA to encrypt information, and RSA is used to transmit the session key.

Authentication technology

Certification is an important technology to prevent malicious attacks, it is important to all kinds of information system security in open environment, the main purpose of the certification, there are two: 1) authentication information of the sender is legal; (2) to verify the integrity of the information to ensure that the information has not been tampered with in the process of transmission, replay or delay, etc. The relevant certification main techniques are: message authentication, identity authentication and digital signature. Message authentication and identity authentication has solved the communication parties interested in conditions to prevent the damage of a third party and camouflage.

Digital signature can prevent others impersonate sending and receiving of information, and prevent I later denied that I have been sending and receiving activities.

Access control technology

Access control is the main strategy of network security and protection, the main task is to ensure that not be illegal use of network resources and access to very much, also is the maintenance of network system security, to protect the important means of network resources, is one of the most important core strategies of network security. Access control technology including network access control, network access control, security control, property safety control directory, the web server security control, network monitoring and locking control, network port and node security control and so on. According to the level of network security, network space environment is different, can be flexibly set the amount and type of access control.

DESIGN PRINCIPLE:

The design principle of network security protection system from the perspective of the network security of network safe protection system design and implementation should be according to the following principles:

(1) The least privilege principle: any object should only have the privilege of the object need to complete their assigned tasks, avoid exposure under attack, and reduce losses caused by invasion.

(2) The principle of defense in depth: network security protection system is a multi-layer safety system, avoid become "single failure point" in the network.

(3) The blocking point principle: the ideal network security protection system should be the safety control points in interconnection network, called it "choke points" here, it simplifies the network security management, easy to monitor network communication and audit.

(4) Principle: the weakest link chain of security protection is the basic principle of the strength of its weakest links, the solution is to keep the balance of strength.

(5) Failure to protect state principle: the network security protection system failure modes should be "fail - safe" type, namely, once the failure, restart the firewall or collapse will block the internal network safety and the rest of the world.

(6) The default declined to state principle: from a security point of view, the default declined to state is failure protection state.

CONCLUSION

The network information security is a fast changing, update the field. This means that simply using a certain protective measures is no guarantee that the network information security, we must comprehensive use of various protection strategy, integrating the advantages, cooperate with each other, so as to set up the network information security protection system. Based on many years' network security work practice of the author to the common network security hidden danger has made the detailed elaboration, summarizes some use of network security strategy, and the design of network security protection system elaborated the basic principle, practice shows that still has a certain reference value. Network security work, is still a need in daily work point guard and will largely reduce network security hidden danger, to protect the normal use of the network.

REFERENCES

1. Anderson J P. Computer Security Threat Monitoring and Surveillance [P]. PA15034, USA. 2015.8.
2. B. Endicott .Active Defense to Cyber Attacks. Information Assurance and Security [J].2014.9.