Research and Design of Multi-level Network Security Active Defense System

Xian Ou(✉)

Department of Information and Communication, Officers College of PAP, Chengdu, China
ouxianer@126.com

Abstract. As the network continues to integrate into our lives, the threat posed by the network is also increasingly serious, our data may be stolen at any time, and the national government network may be invaded by malicious attackers, resulting in network paralysis and irreparable losses. Security is a problem that cannot be ignored. This paper proposes to build a multi-level network security active defense system to improve the network security defense performance.

Keywords: Network security · Active defense · defense system

1 Introduction

In the era of big data, the network security situation and strategy are undergoing great changes. Today's Internet and people's lives have been integrated, the network world and the real world have been deeply connected, and the boundaries between online and offline have disappeared. Any security problem in cyberspace will directly map to the security of the real world, and will profoundly affect the normal and stable operation of society.

2 Threats to Network Security Defense

The traditional network security defense mechanism often takes the exploitation of vulnerabilities as the defense target. It is believed that network attackers often attack in the way of exploitation of vulnerabilities, and security can be ensured by patching the system and deploying the monitoring of the exploitation of vulnerabilities. In the latest network environment, network security defense has the following problems.

2.1 Facing the Means of Network Attack, the Form of Network Security Defense is Relatively Simple

With the application and deployment of new technologies such as cloud computing, mobile Internet and Internet of Things accelerating, network security threats will continue to take new forms. The traditional security defense uses firewalls as the basic equipment for network security protection, and the coordination of various devices is not enough. The attacked host is very easy to become a security "island", and it is difficult to achieve collaborative defense.

N. Akhtar et al. (Eds.): PMIS 2023, AHIS 8, pp. 1158–1164, 2023.
https://doi.org/10.2991/978-94-6463-200-2_122

2.2 Technical Defects of Network Security Defense

The traditional network security defense lacks the analysis of mail, file and download data channel content. The attack code often evades the traditional detection by embedding the document content, or conceals or changes its characteristics by encrypting the malicious code, bypassing the security defense system based on signature and known characteristics.

2.3 Network Advanced Persistent Malicious Attack (APT Attack) Threat

When traditional network security is faced with the advanced sustainability threat (APT) attack that integrates social engineering, the defender can not effectively defend comprehensively. As long as APT attackers achieve a single breakthrough, they can gradually penetrate into the network to achieve the purpose of attack.

Most malicious software will perform fast and destructive attacks, but APT adopts different, more strategic and covert methods. Attackers invade through traditional malware such as Trojan horses or phishing, but after that, they will cover up their tracks, secretly move around the entire network and implant their attack software. After the attackers gain the stronghold, they can achieve their goals, and their goals are almost the same: continuously extracting data for months or even years.

3 Active Defense in Network Security

Active defense strategy is proposed in network security to improve the ability of information system to discover, detect, analyze and migrate threats and vulnerabilities synchronously and in real time. Therefore, when adopting active defense measures, we should pay attention to clarifying the design objectives and functions of the active defense system, build a complete network security active defense system, ensure that with the support of advanced technology, improve the network security management effect, and play the active role of active defense technologies and measures.

3.1 Define the Design Objectives and Functions of Active Defense

First, the design objectives of the system should be clarified. The main purpose of the system design is to adopt active defense technology to solve the problems of current network management software, optimize the relevant active defense technology system, analyze the system vulnerability mechanism through experimental operation, carry out security detection activities, and make relevant security emergency response. Secondly, the functional module of the active defense system should be designed to meet the requirements of detection analysis, protection processing and response processing for the operation of the network system. It can comprehensively detect whether there is an attack during the operation of the network system, display relevant content, and take protective measures. For example, in the application process of the defense module, it is of great significance to carry out relevant network forensics, countermeasures, patch installation, system backup, etc., and to be able to purchase relevant defense tools, installation tools, and make relevant responses.

3.2 Reasonably Design Relevant Systems

In order to ensure the security of the network system operation in practical work, we should reasonably design the active defense system, give full play to the application role and advantages of the active defense technology, and ensure that we can improve the effect of active defense in all aspects.

Customize the application according to the application scenario and environment, reinforce the targeted security policy at the host level (operating system, database, middleware, etc.), and do a good job of the overall security policy construction at the network level and the specific policy configuration and activation of each security device on this basis. For example, for Web systems that can be accessed via the Internet, it is necessary to first enable XSS vulnerability defense, SQL injection vulnerability defense, upload vulnerability defense and other common Web vulnerability defense strategies in the application firewall, configure intrusion prevention strategies appropriate to the application scenario, and set access control policies in the firewall and other devices with access control functions to control users' access to protected resources; Secondly, according to the security characteristics of the Web, implement strict identity authentication technical measures in the source code of the application system (forcibly limit the complexity of the password, provide the function of handling login failure), access control measures (strictly control the access of different users to resources, and avoid unauthorized access between users of the same level and users of different levels) Security audit measures (security audit of user login and important operations, and ensure that the audit log is not modified, deleted or overwritten), communication integrity and confidentiality measures (using encrypted communication protocols, such as https protocol), resource control measures (providing idle session binding function, source code and middleware both limit the maximum number of concurrent session connections, limit the number of users who log on multiple, etc.); Finally, combined with the above measures, the server and database are targeted for security reinforcement to achieve mandatory password restriction, account locking, two-factor authentication, mandatory access control, security audit, malicious code prevention, host intrusion prevention and resource control.

3.3 Improve the Function of Active Defense System

The corresponding network security attack and defense experimental platform can be built. The construction of the network security attack and defense experimental platform can improve the function of the active defense system, simulate and demonstrate the network attack behavior and defense behavior, truly reflect the actual situation, and within the simulated network environment, demonstrate the process and principle of network attack and defense, and visually present the relevant active defense technology application results. In this process, technicians design attack module and defense module according to the experimental situation of active defense technology. Among them, the attack module is mainly the scanning system, detection system, attack prediction system, etc. on the host side, which can achieve the detection purpose of the target, scan the vulnerabilities, find out the attack behavior in a timely manner, clarify the hidden security problems in the operation of the network system, and propose corresponding security management countermeasures; The defense module can detect, analyze, protect and respond to the operation of the network system. It can comprehensively detect whether there is an attack during the operation of the network system, display relevant content, and take protective measures. For example, in the application process of the defense module, it is of great significance to carry out relevant network forensics, countermeasures, patch installation, system backup, etc., and to purchase relevant defense tools, installation tools, and make relevant responses.

4 Design of Active Defense System for Multi-level Network Security

The multi-level network security active defense system is mainly to reasonably deploy key security devices and related threat awareness systems, so as to effectively prevent various types of factors that threaten network security from causing problems to users. Therefore, this paper designs a multi-level network security active defense system, which is the boundary defense layer, the security detection layer, the traffic monitoring layer, and the terminal protection layer. It covers threat intelligence collection, attack detection capability, vulnerability detection function, abnormal behavior detection, terminal security response and other aspects. The multi-level network security active defense system is shown in Fig. 1.

4.1 Boundary Defense Layer

At the border defense layer, network security devices such as firewalls and intrusion detection systems can be deployed. Firewalls can integrate innovative security technologies such as threat intelligence collection, big data analysis and security visualization. IPS can realize traffic analysis, alarm and blocking of abnormal or attack behaviors of the protection network. IPS can not only detect attacks, but also automatically and real-time implement defense strategies, effectively ensuring the security of the information system. Therefore, the firewall can cooperate with IPS to build a threat defense platform at the network boundary.

The policies among devices can complement each other to achieve multi-dimensional redundancy and multiple protection of policies. For example:

(1) Both firewalls and switches can be configured with access control policies to achieve the redundancy of key access control policies. Even if the firewall fails or the firewall is breached by hackers, the core switch still has access control function, preventing hackers from accessing controlled resources;

(2) Access address restrictions can be restricted by the security device itself, and the switch can also be restricted by ACL. If the security device fails or is broken, the ACL of the switch can still restrict access to unauthorized addresses;

(3) Intrusion prevention strategy: IPS or IDS can configure intrusion prevention strategy, and many firewalls also have basic intrusion prevention function, which can be turned on as a supplement or backup. Because IPS or IDS are generally deployed by bypass, even if IPS fails, the system still has basic intrusion prevention function.

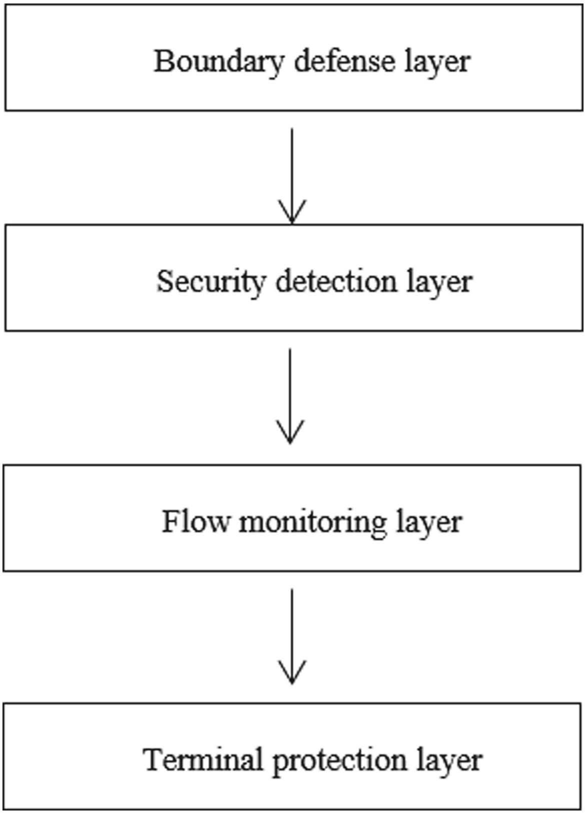

Fig. 1. Multi-level network security active defense system

4.2 Security Detection Layer

In order to fully grasp the IT assets on the Internet, including application systems, domain names, ports, application services, ip, etc., so as not to cause blind spots in the organization's defense boundaries, an asset discovery system should be configured. The core function of the system is asset and application discovery, which actively discovers the host, server, security equipment, network equipment, industrial control equipment, web applications, middleware, databases, etc. in the system, And generate asset and application lists. In addition, deploy the operation and maintenance security management and audit system, whose core functions are identity authentication, account management, access control, etc., which can carry out unified operation and maintenance management and audit on the network equipment, database, security equipment, host system and other resources of the IT center.

4.3 Flow Monitoring Layer

The behavior characteristics of the network can be reflected by the dynamic characteristics of the traffic it carries. Therefore, various parameters of the traffic in the network (such as the size of received and sent datagrams, packet loss rate, datagram delay and other information) can be targeted monitored, and the operation status of the network can be analyzed from these parameters. By analyzing and studying the traffic characteristics carried on the network, it is possible to provide an effective way to explore the internal operation mechanism of the network.

In addition, network traffic reflects the operation status of the network and is the key to judge whether the network is running normally. If the traffic received by the network exceeds its actual carrying capacity, the network performance will be reduced. The traffic measurement can not only reflect whether the network equipment (such as routers, switches, etc.) works normally, but also reflect the resource bottleneck of the entire network operation. Therefore, the health of the network traffic in the enterprise network is as important as the blood in the human body.

In the traffic monitoring layer, a traffic threat awareness system can be deployed. Based on network traffic and terminal EDR logs, the system uses threat intelligence, rule engine, file virtual execution, machine learning and other technologies to accurately detect the intrusion behaviors of known advanced network attacks and unknown new network attacks against hosts and servers in the network. Its core functions include advanced threat detection, abnormal behavior detection Alarm response processing and attack backtracking analysis.

4.4 Terminal Protection Layer

Deployment of terminal response system at user terminals is an extension and supplement of traditional terminal security products in advanced threat detection and response. It assesses unknown risks in the network from the dimensions of host, network, user, file, etc. through threat intelligence, machine learning, etc. Core functions of equipment:

(1) Provide comprehensive monitoring and data collection of user behavior, including IP access, terminal process, DNS access, file operation, etc.

(2) Provide deep automatic anomaly detection capability to detect common penetration tools.

(3) Carry out traceback analysis to completely trace the attack link of suspicious process behavior.

(4) You can create custom abnormal behavior detection conditions to trigger alarms according to business requirements.

(5) Support threat tracking and sign data search, such as the search of mail logs, operating system information, IP access audit, driver information and other sign data.

5 Application and Result Analysis

In the network security attack and defense experimental platform, we design the defense module according to the detection mechanism, protection mechanism and response mechanism of the active defense technology according to the active defense system studied above. During the application process of the defense module, we can carry out the relevant network forensics, confrontation processing, patch installation, system backup, etc. The attack module mainly includes the scanning system, detection system, attack prediction system and so on.

After the application of the active defense system, all levels and equipment strategies are configured and enabled according to the application scenario. We use the client of the attack module to perform scanning and detection work, and find 0 security vulnerabilities at the host/application level: 0 operating system vulnerability, 0 middleware vulnerability, 0 database vulnerability, and 0 high-risk security vulnerabilities that can be exploited at the application level. The experimental results show that the active defense system proposed in this paper can effectively improve the level of Internet security defense.

6 Summarize

The network security active defense system is a multi-level system, including a variety of technical components and active security strategies that can realize the network security active defense function, including the deployment of network security equipment, data collection and analysis, defense response, and so on. With active defense measures, we can solve the security problems that may exist in the current network system operation process, and improve the security level and security performance of the overall network system operation.

References

1. Zhao Shan. An analysis of the active defense system of network security [J] Network Security Technology and Application, 2022 (4): 2.
2. Gu Liqiang. Analysis of active defense technology system and its application in network security [J] Communication World, 2017 (14): 2.
3. Zhang Wei Exploration of attack and defense strategies and active defense ideas in network security [J] Network Security Technology and Application, 2020 (9): 2.
4. Zhang Shiqi Discussion on attack and defense strategies and active defense in network security [J] Mobile information, 2020 (3): 00106-00107.
5. Li Yanhua. Research on Big Data Security Technology [J]. Cyberspace Security, 2020 (2): 15-23.