Security Snort Early Warning Assessment Program of Hazardous Sources

Shuhua ZHANG
Jilin Agricultural Science and Technology University, Jilin, China

ABSTRACT: This dissertation discusses network security of campus network, and summarizes safety risks and threats faced by campus network at present, meanwhile, it focuses on analyzing attack & defense strategy on DOS network layer, puts forward a campus network security plan using firewall which combines network security intrusion detection system snort, analyzes functional advantages of this plan, and describes installation deployment and configuration method of network security invasion detection system based on snort in campus network environment, as well as summarizes its application effects.
KEYWORD: Network Security, Invasion Detection System, Campus Network, DOS

1 INTRODUCTION

With the popularization of computer network, issue faced by today's campus network is not only to make various network devices interconnected, realize load balancing, support their application, but to consider network security. Hackers outside campus network, hostile attacks inside campus network are all potential dangerous sources. Without network security, those people will ruin campus network devices, ruin campus application servers, and obtain campus private data etc. by all means. So, network security takes the first priority in campus network planning. This chapter introduces contents mainly involving the construction of campus network security system, analyzes security risks and threats faced by campus network, analyzes attack theory of DOS and DDOS, puts forward a campus network security plan using firewall which combines network security invasion detection system snort, analyzes functional advantages of this plan, and summarizes installation deployment and configuration method of snort network security invasion detection system based on open-source code in campus network environment.

2 DOS ATTACK THEORY

The Chinese significance of DoS (Denial of Service) is to refuse service security attack, and such security attack behavior makes network server filled with lots of useless information requiring a reply, which consumes network bandwidth or system resource, causing network or system to become overloaded, which leads to a breakdown and stops providing normal security network service. Hackers incorrectly adopt standard security protocol or security connection method, and send a large amount of security information to server being attacked, which occupies and exceeds the ability of the server being attacked to handle security, making it down or unable to work for user security normally.

Via normal network connection wire, user's transmitting security data information needs confirmation of the server. Then the server replies security data to user. Once the user is determined, he or she could login security data server. Attach method of "refuse service" is: User transmits numerous information to be confirmed to security data server, to make security data server filled with such useless information.

All information has a false address needing replay, thus when server tries to send back, the user could not be found. Then the server will wait temporarily, sometimes it will exceed 1 min, and then cut of the connection. After cutting server connection, hackers will send a new batch of information to be confirmed, and this process will go round and begin again, till cause server unable to function, becoming collapsed.

These DoS attacking methods could also be classified into the following types: TCP SYN Flooding security attack, Smurf security attack and Fraggle security attack etc.

2.1 TCP Syn Flooding security attack

For the need of TCP protocol's continuous three handshake data, at the establishing of each TCP data

connection, a grouping data package with SYN data mark will be sent, after an acknowledge package data is sent by server, client would not send out confirmation data, and server will wait till data overtime, if large quantities of grouping data packages with SYN data label do not acknowledge data after being sent to server, it will make TCP data source at server become exhausted quickly, causing normal connection unable to perform, or even causing system collapse of data server. This is the process of TCP SYN Flooding security attack.

TCP Syn security attack is that large quantities of customers under control send out TCP data but do not reply, making data server resource occupied, and unable to provide user security service normally. Server needs to wait for timeout so as to disconnect the distributed data resource.

2.2 Smurf security attack

Hackers adopt ICMP technology to carry out attack. ICMP commands used frequently include PING.. First, hackers find which routers on network would respond to ICMP data request. Then a false IP source address sends out data information to router's broadcasting address, while router will broadcast such data information to each data device connected to data network. These data devices will respond immediately, which will produce large amounts of data information flow, thus to occupy resource and data network bandwidth of all data devices, while the responded address is the target data being attacked. i.e. Broadcast 100 devices using an ICMP echo (PING) grouping data package, which produces 100 PING grouping acknowledge data packages, thus to produce 500M bit/sec data flow. Such data flow will move to the data server being attacked, making these data servers collapse.

The attack of ICMP Smurf security attack deepens the flooding degree of ICMP data, causing the generation of hundreds of ICMP grouping data packages in one grouping data package, sending security attack into a host which does not need them, while data server transmitting multiple data information packages is used as the amplifier of Smurf security attack.

2.3 Fraggle security attack

Basic concept and methods are like Smurf security attack, but it adopts UDP echo data information. Common method to block the attack of "refuse service" is: Establish a data filter or data sniffer on data network, and block information before data information reaching network data server. Data filter will detect doubtful data security attacking behaviors. If a certain doubtful behavior appears frequently, data filter will be able to receive instruction, block information including security attack, and maintain a smooth external wiring route of website data server.

3 THE STRATEGY OF PREVENTING DOS ATTACK OF CAMPUS INTRANET

Although network security experts are engaged in developing methods to deal with DoS attack, the effect is small, for DoS attack has utilizes TCP protocol's weakness. Carry out configuration on exchanger, and install a special DoS identification and precaution tool specially, to reduce losses caused by DoS attack to the greatest extent.

Use three-layer exchange to establish a complete network security system, and its basis is an intelligent network regarding three-layer exchanger and router as its core, which is a security strategy management tool above layer three.

3.1 LAN layer

On LAN layer, multiple precautions could be adopted. i.e. although the complete elimination of IP grouping faking is almost not possible, network administrator could construct a filter, if data has signal address of intranet, the inner fake IP attacks could be lowered effectively via limiting data input flow. Filter could also limit external IP grouping flows, and prevent DoS attacks with fake IPs from being used as an intermediate system. Other methods include: Closing or limiting specific services, i.e. limiting UDP service to be only used for network diagnosis in intranet. However, these precautions could bring along negative impact to legal applications (i.e. RealAudio adopting UDP as transmission mechanism).

3.2 Network transport layer

Supplement could also be made to the control on network transmission layer in the following. Linear service quality (QoS) and access control independent of the layer, has improved the capacity of improving network transmission device's protection of data flow completeness. In traditional router, certification mechanism (i.e. filtering false grouping with inner address) requires flow to reach router edge, and comply with the standard in access control list. However, maintaining access control list is not only time-consuming, but greatly enlarges the router's consumption. In contrast, linear-speed multi-layer switch could realize various access controls based on strategy in a flexible manner. Such access control capacity independent of the layer could separate security decision-making from network structure decision-making completely, making network administrator could effectively deploy DoS

precautions, without needing to adopt inferior routers or exchange topologies.

As a result, network administrator and service supplier could integrate the whole MAN, data center or control standard based on strategy in enterprise network environment in a seamless manner, without considering whether it adopts a complex core service based on router, or a relatively simple layer-2 exchange. In addition, linear-speed handling data certification could be executed at background, without any performance delay basically.

3.3 Customized filtering and "Neighbor Trust" mechanism

The advantage of intelligent multi-layer access control is to realize the customization of filtering operation in a simple manner, i.e. control granularity to system response according to specified standard customization. Multi-layer exchange could promote grouping to a specified QoS configuration file limited by max. bandwidth, rather than to prepare a simple "Pass" or "Abandon" strategy for potential DoS attack groups. In this way, it could not only prevent DoS attacks, but reduce the risk of discarding legal data packages. Another advantage is to customize access strategy, and support "neighbor trust" relationship among specific systems, to prevent unauthorized usage of inner routers.

3.4 Customize network login configuration

Network login adopts unique username and password, and carries out identification certification before user's authorized login. Network login is done via transmitting dynamic host configuration protocol (DHCP) to switch via user's browser, while switch will capture user identification, and send requests to RADIUS server, to carry out identification certification. Only after certification, switch would allow grouping flow sent out by this user to pass by network.

4 SNORT NETWORK SECURITY INVASION DETECTION SYSTEM CONSTRUCTION AND CONFIGURATION

Snort is a cross-platform and light-weight data network security invasion detection system with strong function, viewing from invasion detection classification of invasion data, Snort should be data invasion detection software based on data network and misuse. It could runs on all mainstream operation systems. Snort is an open-source code invasion detection software compiled in C language, for it is a data open-source and free of charge, many security invasion detection systems studying and using data network start from Snort, so Snort plays a very important role in data network security invasion detection system. Users could download source code, install executable files under Linux and Windows environments, and could download regular files describing invasion detection characteristics. Fig. 1 displays Snort's main system composition and basic data handling process.

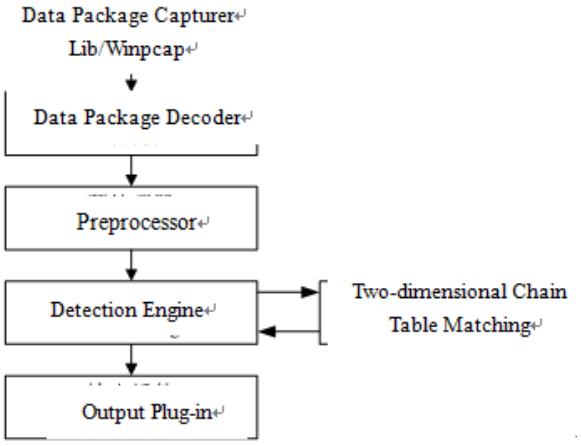

Fig. 1 Snort Process Flow Chart

4.1 Grouping data package capture library

Network security invasion detection system based on network needs to capture and analyze all network data transmitted to monitoring network card, and this needs package capturing technology, while Snort realizes this via two mechanisms, one is to set network card into a mixing mode, and the other mode to use Libpcap/Winpcap function library to capture network grouping data packages from network card.

Grouping data package capturing function library is an independent software tool, which could obtain grouping data packages from network card. This function library is developed by Lawrence Berkeley National Laboratory Research Institute of Berkeley University, and Libpcap supports all operation systems based on transplantable operation system interfaces (Portable Operating System Interface of Unix, POSIX), i.e. Linux and Unix etc., later in order to support trans-platform features, Windows version is also developed (http:// www.winpcap.org), while function callings under Windows and Linux are almost the same, and Snort is to capture grouping data packages from network devices via calling such library function.

4.2 Grouping data package decoder

Grouping data package decoder is mainly to carry out parsing and preprocess on grouping data packages on various invasion detection protocol stacks, so as to submit to invasion detection engine to carry out regular matching. Decoder is running on various invasion detection protocol stacks, from data

link layer to transport layer, and to application layer finally. For data flow speed is very fast in the current invasion detection network, so how to guarantee a higher speed is a key point of invasion detection decoder subsystem.

4.3 Preprocessor

The function of preprocessor module is to carry out data preprocessing on grouping data packages currently captured, so as to carry out data processing operation on grouping data packages for subsequent processing modules. For issues such as max. data transmission unit (MTU) limit and data network delay etc., the router will carry out slicing data processing on grouping data packages. However, malicious attackers will also send grouping data packages after being processed by software data deliberately, so as to distribute an attacking grouping data package to small grouping data packages. This may disturb transmission sequence of grouping data packages, which are transmitted to target data hosts in multiple times. So, processing on abnormal grouping packages is also an important content of network security invasion detection system.

Preprocessor mainly includes the following functions: 1) Plug-in data simulating TCP/IP stack function, i.e. IP fragments reconstructing data, TCP flow reconstructing plug-in data; 2) various decoding plug-in data: HTTP decoding plug-in data, Unicode decoding plug-in data, RPC decoding plug-in data and Telnet decoding plug-in data etc.; 3) regular matching could not perform plug-in data used during attacking detection: Port scanning plug-in data, Spade abnormal invasion detection plug-in data, Bo detection plug-in data, ARP spoofing detection plug-in data etc. A conclusion could be drawn on this plug-in data function according to various preprocessing plug-in data filenames.

4.4 Detection Engine

Detection data engine is the core content of network security invasion detection system, and Snort uses a 2-dimensional chain table to store its detection regulations, among which one dimension is called regular data head, and the other dimension is regular data option. Some public property data characteristics are placed in regular data head, while some invasion data characteristics are placed in regular data option. Snort reads the location of regular data file from configuration file, and read data regulation from regular file, to store to a 2-dimensional chain table.

Snort data detection is a process of 2-dimensional regular chain table and network data matching, once matching succeeds, data detection result will be output to output data plug-in. In order to improve data detection speed, usually the most frequently used data source/target IP data address and data port information are placed in data regular head chain table, while some unique data detection mechanism is only to carry out detection on the currently established data chain table option, when grouping data package meets one data regular, corresponding data operation will be triggered. Snort's detection mechanism is very flexible, and users could add required data regular module into data regular chain table in a convenient manner. Grouping data package matching data algorithm adopts classic matching data calculation – multiple modulus matching data algorithm (AC-BM), which adopts 2-dimensional data chain table and classic data matching algorithm are provided to improve matching speed with data network grouping data package, so as to improve data invasion detection speed.

4.5 Log and alarm subsystem

Output method adopts output data plug-in method, and output data plug-in makes Snort become more flexible while providing formatted data output. Data output plug-in runs at Snort's alarming and calling subsystem which records data. Logs and alarming data subsystem could carry out selection during running Snort in a data form of command line exchange, if output switch data of data command line has been specified during running, output data plug-in specified in Snort regular file will be replaced. At present, there're three log types for selection, and six data for alarming type. Snort could carry out data records for grouping data package in the form of text data after decoding or TCP Dump binary data. Data form after decoding could be used by data system to carry out data analysis on data, while TCP Dump data format could guarantee completing data disc recording function quickly, while the third log data mechanism is to shut down log data service, without doing anything. Using database output plug-in, Snort could record data logs into database.

Network security invasion detection system could detect ARP protocol spoofing frequently performed with respect to campus data network.. The main function of ARP protocol spoofing is to complete data exchange from IP address data to MAC address data. When data communication is carried out among campus network hosts, all hosts must know MAC address data of the target host. While MAC address data could only be obtained via address parsing protocol, and corresponding MAC address data could be found via searching for target host's IP address data, so as to carry out data communication smoothly. When IP address data of the target host is searching for MAC address data, it is not possible to find corresponding MAC address data, so it is required to obtain address data via broadcasting in Ethernet. For when the host is sending request data,

it is carried out in the form of broadcasting, so multiple hosts could send ARP acknowledge data at any time, among which counterpart's acknowledge data faked by attackers is possibly contained, only if the originally received data is effective, even faced with attacker's acknowledge, MAC address corresponding to IP data address would be written into host high-speed cache unconditionally, thus to produce ARP spoofing, making computer of this network segment unable to receive data information from other computers, which will cause data communication fault, or even cause large-scale paralysis in data network when the condition is serious. Data network security invasion detection system now could detect such attack data, and could identify data of such attacking behaviors, via alarming information of attacking results. It could also prevent such deceptive attack via binding IP address data with MAC address data in a static manner.

5 CONCLUSION

In order to guarantee campus network data's security in a better way, we use firewall and network security invasion detection technology in campus data network. Via application of such data network security technology, especially the usage of network security invasion detection technology, network security issues appeared in campus data network could be solved effectively, which could not only guarantee normal operation of campus network, but provide highly safe campus data network security environment for students. At present, via some campus networks, distributed data network security invasion detection system has been adopted, which could greatly effect campus computer data network management, and establish a data network security barrier.

REFERENCES

[1] Zhang Yan, Zhao Fei. Network Security Solutions Based on SSH. Modern Electronic Technology, 2004 (11).

[2] Lai Guoge. Discussion on the Design and Implementation of High Availability Network. Guangdong Technology, 2007 (15).

[3] TomMarkham, Charlie Payne. Security at the Network Edge, Adistributed Firewall Arehiteeture, 2001, 9 (8): 288-315.

[4] Nathalie Weller. Honey Pots for Distributed Denial of Service Attacks. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative EnterPrises. June, 2002: 10.12.

[5] Yan Hua. Application of Security Technology in Campus Network. Fujian Computer, 2007 (12).