Research on the Security Early Warning Model of Campus Network Based on Log

Derong Zhou

Network Information Center Sichuan Minzu College, Kangding Sichuan, China
zhoudr0310@163.com

Abstract. The safe and stable operation of campus network is core problems which network administrators focused on. This paper takes safety management of campus network as a main research object to analyze the weakness in safety management and threat management of campus network, which can put forward safety warning of campus network that based on log. What’s more, it also analyzes the protocol standard and related technologies of log acquisition, studies the log acquisition, threat assessment, security warning in the model to provide the core process for system implementation. This model can quickly find out and timely cope with the network safety threats, it also plays positive guiding roles in improving the safety and stability of network operation and reducing the workload of network management.

1. Introduction

With continuous development of internet, network safety is increasingly important. Campus network is a special network providing integrated information service for teaching, research, management, life of teachers and students, featuring large size of network, large number of users, many types of network equipment, open network environment, etc. As campus network evolves continuously, it faces more and more security threats, so it becomes a hot spot problem focused on by network administrator to ensure safe, stable operation of campus network.

Traditional network security management mainly depends on separate network security equipment or network management software to collect data, because equipment and software are interdependent, collected data is poorly interlinked, without unified security threat early warning and assessment mechanism. When network security incident occurs, people are needed to detect, find and deal with security threat, with issues such as high requirement for technical capability of personnel, failure to find, deal with security threat, etc. It is a key to quickly find abnormality in campus network, thoroughly monitor, precaution and deal with security of every component in the network in time.

Network security monitoring includes package capture based technology and log analysis based technology, package capture based technology need s to analyze every data package, with high requirement for data processing speed. Log analysis effectively monitors network security by collecting the log produced by network components with small volume of information. Central analysis of logs of key network component such as server, firewall, switch, application system, etc., can detect security threat perfectly. Aiming at defects in security monitoring and management of dealing with security threat of existing campus network, a campus network security early warning model based on log is proposed.
2. Data collection techniques

2.1. Syslog protocol
Log is a kind of record of system states and activities. Syslog, as a standard log protocol, which is widely used in computer system, especially network operation and safety management. In August 2001, IETF issued the description of RFC 3164 to information format of syslog protocol. According to the regulation of RFC 3164, the maximum length is 1024 bytes for each piece of information, and there are PRI, headers and MSG that formed a piece of complete syslog information. PRI is the priority value that can show the information sources (Facilities) and severities in digital form. RFC 3164 stipulates the sources of common information and the severities of the log information. the calculation method for the priority value of PRI is as follows:

\[
\text{Priority value} = \text{Facility} \times 8 + \text{Emergency}
\]

For example, a kernel message (Facility=0) with a Severity of Emergency (Severity=0) would have a Priority value of 0. Also, a "UUCP subsystem” message (Facility=8) with a Severity of Notice (Severity=3) would have a Priority value of 67.

The HEADER of the syslog information includes the timestamp, machine name or host address of the event. However, HEADER must be made up of printed characters. The MSG of syslog is the content of event information. There are two fields, TAG and CONTENT for MSG, TAG field is the program name that generated the event, and CONTENT shows the event details. However, MSG must be made up of printed characters.

2.2. Log data collection technology

2.2.1. Log data collection of syslog. Log collector is the program or equipment used to collect log information produced by various equipment and program, mainstream log collector includes syslog, rsyslog, etc., and rsyslog is enhanced version of syslog, with powerful function, supporting collect and store log information to database, its configuration file in Linux is /etc/rsyslog.conf, in configuration file the log is managed by configuring filter and action, the rule is defined by using the following format:

Filter  action

When rsyslog finds logs meeting filter rule, it will send the log to the action specified by action to process. Rsyslog provides three filter methods such as facility priority based filter, attribute based filter and expression based filter.

Action defines what operation to be implemented when assigned filter is matched, if multiple actions are to be assigned, use & to connect multiple actions.

2.2.2. Log data collection of SNMP. SNMP was proposed by IETF, has become de facto standard protocol in network management. SNMP protocol consists of administrator, administered equipment proxy, management information base and object of management protocol. SNMP protocol provides 4 types of management operation including get, get-next, set, trap, SNMP runs and draws topology through SNMP proxy, monitors and manages administered equipment through SNMP massage. It typically collect log data by using SNMP Trap mechanism, SNMP Trap is based on SNMP MIB which defines triggering condition of equipment information being collected and equipment being defined Trap, only events meeting the condition of triggering trap can be sent out. Because Trap mechanism is a event based drive, proxy only informs the management system when monitoring fault. The SNMP object composition shown in Fig. 1.
Figure 1. SNMP object schematic

In general, the network device log is reported by SNMP Trap, and the key information of a network device can be obtained through the interpretation of Trap field value in SNMP data message. To send a log to the specified device as an SNMP Trap by configuring the device to, as an example, enter the following commands in the global configuration mode:

a) Snmp-server community cisco ro; Configure read only communication character string as cisco.

b) Snmp-server community cisco rw; Configure read and write communication character string as cisco.

c) Snmp-server enable traps; configure the equipment to allow SNMP Trap of all types sent out.

d) Snmp-server host 192.168.1.100 scun; Assign the receiver of switch SNMP Trap 192.168.1.100, adopt scun as communication character string when transmitting Trap.

e) Snmp-server trap-source loopback0; Use IP address of loopback0 interface as original address transmitting SNMP Trap.

3. System requirements

To protect normal operation of network equipment, network application in campus network is basic demand of campus network security management. It is the problems need to be solved urgently in campus network security management to actively find network attack, timely send out and automatically process security early warning while providing efficient and quality network communication and information service. Main demand of the model is as follows:

a) Collection, central storage, formatting, merging and associating processing of log data of key network equipment and applications in campus network.

b) Detect internal security threat of campus network according to log data, establish relevant model according to type, and finish network security hazard assessment against behavior characteristic base.

c) Acquire result of network security threat assessment, realize sending early warning information to the administrator in multiple ways according to the result of security threat assessment; or trigger
administrative behavior to directly execute administrative operation according to the result of risk assessment.

The system is required good expansibility, compatible with equipment and network application systems of different manufacturers.

4. Model design

4.1. Functional design

Based on system requirements analysis finish system design mainly consisting of log collection module, threat assessment module, security early warning module, system management module.

4.1.1. Log collection module. The module is mainly responsible for log information collection of various network equipment and soft system, the data stream of log information collection is shown in figure 2. The module can collect log information of log source such as switch, firewall, and server and application system with the method of syslog or snmp trap and delete useless information, send them to the log storage server in unified format to store in log database. Aiming at different log source store log information into different tables respectively, meanwhile, in order to increase efficiency of log inquiry, when storing large amount of log information store log information into different partition by time.

4.1.2. Threat assessment module. The module is the core of system, mainly comparing, associating and analyzing acquired log information based on threat behavioral characteristic base, assessing threat to get quantitative result, the procedure of threat assessment is as follows:

![Figure 2. Data stream chart of log collection](image)

a) Determinate the target of analysis, classify acquired event information to confirm which type of threat it is;
b) Establish behavioral database, analyzing and screening acquired log data, finishing rule organization of type of network threat, event warning information for every network threat to update behavioral database continuously;
c) Based on type of network threat and problems to be solved, use data mining technology to find and establish threat model and perfect the model.
d) Based on preset threat behavioral database and threat model, match log information with rule to quantify hazard and assess effectiveness of the model.
4.1.3. **Security warning.** Security warning includes the perception of the network threats, the control function of the network safety risks and warning notices.

The perception of the network Security threats is a perception in specific network safety threats and situations of network safety threats for network managers by perceptual analysis on the log information.

The control ability of network Security threats is an ability that network administrators can control network components, such as equipment, host, software and so on. There are mainly two kinds, direct control and indirect control. Direct control is to allocate and modify the related parameters directly for the managed objects, or directly send the control instruction to it, which can control the network components. Indirect control is a way to manage the behaviors of the managed objects by controlling connection link with truncation and restriction. However, indirect control method is mainly used in practical application to complete network access control, network intermediate control and server control. It controls the network components on the basis of the instructions that issued by the managed objects, for example, operating the switch can achieve control ability through SNMP Set.

Warning notices include two functions, one is warning information is issued to the network administrators in time when network safety threats happened, the other one is the reasons that cause bad network behaviors and solutions should be informed to the network users through the safety alarm in text messages, WeChat and E-mail.

4.1.4. **System management.** System management is mainly about manager management, management of log sources, and query of network security threats and so on. Manager management can realize manager add, deletion, modification, lookup function and manage in different levels with different permissions. The management of the log sources is to manage the network components for the log that collected from the platform and the basic information in the software system, such as IP, system name, function description, and network levels the equipment belonged to. Query of network safety threats can look up the log record what is identified as the attack and know about detailed description of the log that be attacked.

4.2. **Core procedure**

There are information acquisition of network safety threats, confirmation of threat type, rule matching, hazard assessment and safety warning for the core procedure by analyzing the system. It includes log acquisition, threat assessment, safety warning, system procedure is shown in figure 3:

System operating mode is to send the log information of network components with the centralize acquisition in SNMP Trap or syslog way by the syslog server, and make pretreatment and unified format to the information. Moreover, the information is stored in the threat information database. Keywords extracted in log information should compare with items in the preset rule bases, if they do not match, they can be skipped. If they match, they should be made the safety threat assessment based on the number of attacks, duration and so on. According to the evaluation results, it can enter into safety alarm. According to the quantitative evaluation results, it can trigger management rules, thus can issue management strategies or triggered alarm to the network equipment which is closest to network safety threats.
5. Conclusion
Campus network is a complex network system, this paper proposes a log based campus network security early warning model aiming at problems in security management of existing campus network, the system is designed around log information collection, security analysis, security early warning and decision, mainly discussing such functions as daily information collection, network security threat assessment, security early warning, etc., the model can quickly find and timely deal with network security threat, reduce work load of network administrator to some extent, increase stability, reliability of campus network operation, with certain referencing value for ensuring safe, stable operation of campus network.

Acknowledgments
This paper was financially supported by the natural research project of the Education Department of Sichuan Province (NO:16ZA0361),This article is one of the phased objectives of the project.

References
[1] ZHA Gui-ting, PENG Qi-jun LOU Gou-fu Problem and Policy of Security System in Campus Network [J]. Application Research of Computers, 2005, 22 (3): 150-152.
[2] Du Yun. Campus Network Security Problems and Solving Strategies [J]. Information Security and Technology, 2015, (05): 13-15.
[3] Chris S. Applied Network Security Monitoring [M]. 2013.
[4] Zhang W, Li X A. Study of Integrated Solutions to Campus Network Security [J]. 2006.
[5] Schmidt K J, Chuvakin A A, Phillips C. Logging and Log Management [M]. 2012
[6] Li Chen-guang. UNIX/Linux network log analysis and traffic monitoring [M]. China Machine Press, 2015
[7] Lonvick C. The BSD Syslog Protocol [J]. RFC 3164 (Informational, 2001).
[8] Mauro D R, Schmidt K J. Essential SNMP, Second Edition [M]. 2016.
[9] Presuhn R. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) [J]. Anvari Net, 2002, 23 (1): 4-6.
[10] Kocharians N, Paluch P, Vinson T. CCIE Routing and Switching v5.0 Official Cert Guide Library, 5th Edition [M] // CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1. WebEx Communications, 2015.