EPJ Web of Conferences **214**, 07016 (2019) https://doi.org/10.1051/epjconf/201921407016
CHEP 2018

Cyber security detection and monitoring at IHEP private cloud for web services

Tian Yan[1,2,*], *Shan* Zeng[1], *Mengyao* Qi[1], *Qingbao* Hu[1], and *Fazhi* Qi[1]

[1]Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, P.R.China

[2]Key Laboratory of Network Assessment Technology, CAS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, P.R.China

Abstract. To improve hardware utilization and save manpower in system maintenance, most of the web services in IHEP have been migrated to a private cloud build upon OpenStack. However, cyber security attacks becomes a serious threats to the cloud progressively. Therefore, a cyber security detection and monitoring system is deployed for this cloud platform. This system collects various security related logs as data sources, and processes them in a framework composed of open source data store, analysis and visualization tools. With this system, security incidents and events can be handled in time and rapid response can be taken to protect cloud platform against cyber security threats.

1 Introduction

In recent years, cloud computing becomes more and more popular in operation of High Energy Physics (HEP) data centers [1, 2]. Cloud technology can improve hardware utilization and save manpower in system management. At Institute of High Energy Physics (IHEP), China, we deployed a cloud platform for elastic batch job scheduling and another platform for hosting public web services. The web services hosted by physical machines were migrated to the cloud platform in recent years.

During the operation and maintenance of this cloud platform for web services, we find that cyber security attacks becomes more and more frequent. This is a serious threat to the cloud platform. Therefore, based on an analysis of the security threats, we setup a security risk control model. In this model, a detection and monitoring system plays an important role. This system collects various security related data and analyzes these data with open source data processing tools. Therefore, malicious behaviors and attacks can be detected and visualized. This model allows the security status of the cloud platform to be monitored effectively.

In this paper, we present the design of the cyber security detection and monitoring system for cloud web services. The paper is organized as follows: The IHEP private cloud for web services is introduced in section 2. Then, we present the main cyber security threats we faced in recent years and the security risk control model in section 3. In section 4, the detection and monitoring system is described. Finally, we present our conclusion.

*e-mail: yant@ihep.ac.cn

2 The IHEP private cloud for web services

The IHEP computing center is responsible for designing and deploying the public web services for all IHEP users and hosting the web services designed and maintained by different research groups. The current architecture for web services platform is shown in Figure 1. It can be divided to five layers, at the bottom is a private cloud, above it there are database services which are provided as a service for web application developers. Then we have some fundamental web services such as Single Sign On (SSO), Academic Resource Planning (ARP) system, Human Resources (HR) system, Assets and project management system. Above these basic services are various public web services and special web services for research groups. They may have user portal in web or mobile app form. Aside these five layers, there are policy and management module for regulating the management of the platform and all web services, as well as operation and security module for supporting the platform running smoothly.

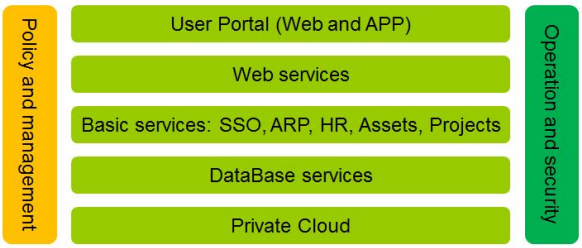

Figure 1. Architecture for IHEP web services

The platform is based on a private cloud built upon OpenStack[3]. OpenStack is an open-source software platform for cloud computing. It consists of related components that control various hardware pools of computing, storage and networking resources. The Openstack project began in 2010 and becomes the de facto standard for Infrastructure-as-a-Service (IaaS) clouds. In the year 2013 we started the deployment of our cloud platform with OpenStack Grizzly release, and then upgraded to the Newton release in 2017. Web services hosted by physical machines have been migrating to the cloud platform gradually in recent years. Currently about 130 virtual machines are running on this platform.

3 Cyber security threats and the risk control model

As an IT system, the cloud platform interacts with the internet. For example, most of the web services are opened to users who may travel around the world, some services such as GitLab[4] require that the SSH port opened to the internet. Therefore, the Virtual Machines (VM) in cloud platform faces various cyber security threats. In recent years, the main cyber security threats we faced are:

(1) Intrusion. The VMs may be cracked by the intruder through password guessing or system vulnerabilities.

(2) Malware for mass scanning, Distributed Denial of Service (DDoS) attack, etc.

(3) Crypto currency mining. As the price of Bitcoin rises, performing crypto currency mining becomes attractive for cyber criminals.

(4) Ransomware. Once affected, it encrypts useful documents and you have to pay money to decrypt them.

(5) Attacking third-party. The VMs may be controlled by the intruder and act as a springboard for attacking others.

(6) Webshell. Some vulnerable web services may be attacked and implanted a webshell which yields remote code execution.

The historical statistics shows that we have about 10 security events every year.

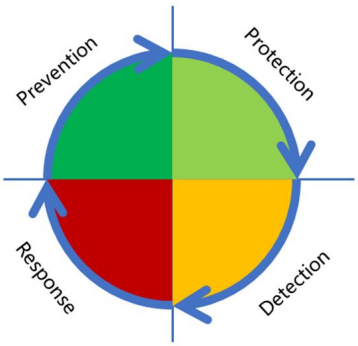

Figure 2. Cyber security risk control model

To protect the web services from these cyber security threats, we followed a cyber security risk control model as shown in Figure 2. It consists of four phases: prevention, protection, detection and response. For prevention, we perform user security awareness and training, security policy review, security assessment and audit. For protection, we deploy firewall, Intrusion Protection System (IPS), and Web Application Firewall (WAF) at the margin of our network. We also scan the vulnerabilities regularly and fix up them as soon as possible, and block malicious IPs and URLs. For detection, we analyze the traffic and system/web logs with help of threat intelligence sharing. And finally, we have emergency procedure for security incident response.

4 Cyber security detection and monitoring system

A cyber security detection and monitoring system was designed for the cloud platform for web services. It's architecture is shown in Figure 3. The threat intelligence, traffic analysis logs, system logs and vulnerability scan results are collected and act as the input of data analysis module. The assets databases and security policy databases also act as input. The result of this data analysis is used in the visualization platform for security status monitoring, as well as an input data for security operation. The security operation is the maintenance activities of security team, it may change the assets and policy databases.

4.1 Data sources

For security data sources, we have threat intelligence, traffic analysis logs, system logs and vulnerability scan results. The threat intelligence is shared with the community by an open

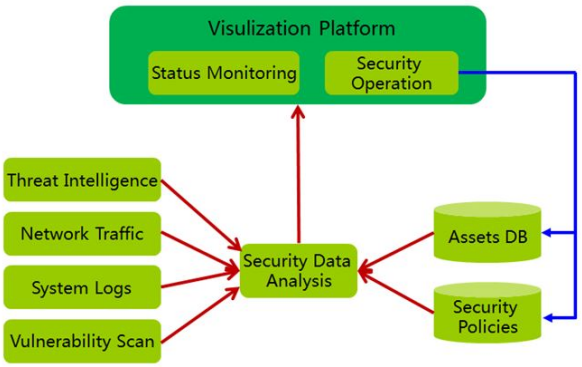

Figure 3. Architecture of security detection and monitoring system

source tool called Malware Information Sharing Platform (MISP)[5]. The network traffic of subnetworks are mirrored by a network shunt, including the Dedicated Demilitarized Zone (DMZ) for public web services. Various monitoring/detection/analysis systems can be connected to the shunt to get data as input source. An open source intrusion detection system named Bro [6] is deployed to analysis the mirrored traffic of cloud DMZ, it is a flexible and powerful tool for traffic analysis and abnormality detection. Bro can integrate the threat intelligence data from MISP as an input. The output of Bro is a set of logs which records various aspects of the network activities. System and web logs on VMs are collected by a lightweight log collector called filebeat [7]. Honeypot VMs are also deployed to collect attack information. The vulnerability scan results are collected from an open source scanning tool OpenVAS [8].

4.2 Data analysis

For security data analysis, we take the WLCG SOC architecture [9] as a reference and designed a simple data process architecture.

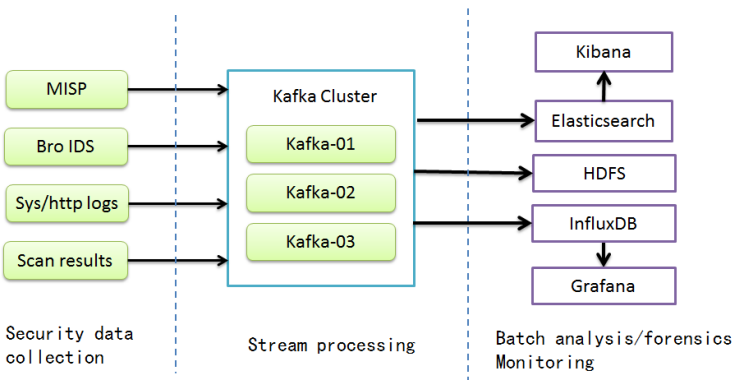

Figure 4. Architecture of security detection and monitoring system

As shown in Figure 4, The left part is security data collection as described above. The middle part is a Kafka cluster [10] for real-time data pipeline and streaming processing. The right part is data storage and visualization. The time series data are stored at InfluxDB [11] and displayed by Grafana [12]. Data in recent three months are stored in Elasticsearch [13] and is quickly searchable by Kibana [14]. For long term (a year) data store and offline analysis, we use HDFS [15]. Apache Spark [16] is used as analytics engine for data processing. It has Spark Streaming library for real-time streaming processing, as well as MLlib for machine learning in offline data analysis.

4.3 User interfaces

For User Interfaces (UI), we use Grafana for time series data visualization, and Kibana for log search. At the same time, AlienVault Open Source SIEM (OSSIM) [17] was deployed and we use its UI for integrated monitoring. OSSIM is a widely used open source Security Information and Event Management system (SIEM).

5 Conclusion

In this paper we presented the cyber security detection and monitoring for web services at IHEP private cloud. Since most of our public web services are migrated to cloud platform, they become centralized and are easily targeted by cyber attackers. This security detection and monitoring system can collect, analyze the traffic and logs, and visualize the malicious behaviors so that the security operator and web system administrator can discover and handle the risk and issues more rapidly and accurately than before. It helps reduce the manpower requirements in the operation and security maintenance for the public web services.

Acknowledgement

This work is supported by open project of CAS Key Laboratory of Network Assessment Technology and National Natural Science Foundation of China under grant no. 11675199 and 11605224.

References

[1] C. Cordeiro, L. Field, B. Garrido Bear, et al. J. Phys.: Conf. Ser. **898**, 082030 (2017)
[2] Y. K. Li, F. Z. Qi, G. Chen, et al. J. Phys.: Conf. Ser. **898**, 082051 (2017)
[3] The OpenStack project. https://www.openstack.org/
[4] The GitLab project. https://about.gitlab.com/
[5] The MISP project, "MISP" [software], version 2.4, 2018. Available from https://www.misp-project.org/download/ [accessed 2018-12-03]
[6] The Bro project, "Bro" [software], version 2.6, 2018. Available from https://www.bro.org/download/index.html [accessed 2018-12-03]
[7] Elasticsearch B.V. "Filebeat" [software], version 6.5.1, 2018. Available from https://www.elastic.co/downloads/beats/filebeat [accessed 2018-12-03]
[8] The OpenVAS project, "OpenVAS" [software], version 9, 2018. Available from http://www.openvas.org/download.html [accessed 2018-12-03]
[9] D. Crooks and L. Valsan, Proceedings of Science, **293**, 25 (2017)
[10] The Apache Kafka project, "Kafka" [software], version 2.1.0, 2018. Available from http://kafka.apache.org/downloads [accessed 2018-12-03]

[11] InfluxData, Inc., "InfluxDB" [software], version 1.7.1, 2018. Available from https://portal.influxdata.com/downloads [accessed 2018-12-03]
[12] Grafana Labs, "Grafana" [software], version 5.4.0, 2018. Available from https://grafana.com/grafana/download [accessed 2018-12-03]
[13] Elasticsearch B. V., "Elasticsearch" [software], version 6.5.1, 2018. Available from https://www.elastic.co/downloads/elasticsearch [accessed 2018-12-03]
[14] Elasticsearch B. V., "Kibana" [software], version 6.5.1, 2018. Available from https://www.elastic.co/downloads/kibana [accessed 2018-12-03]
[15] The Apache Hadoop project, "HDFS" [software], version 3.1.1, 2018. Available from https://hadoop.apache.org/releases.html [accessed 2018-12-03]
[16] The Apache Spark project, "Spark" [software], version 2.4.0, 2018. Available from https://spark.apache.org/downloads.html [accessed 2018-12-03]
[17] AlienVault, Inc. "OSSIM" [software], version 5.6, 2018. Available from https://www.alienvault.com/products/ossim [accessed 2018-12-03]