Indian Journal of Science and Technology, Vol 9(24), DOI: 10.17485/ijst/2016/v9i24/96070, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Brute-force Attacks Analysis against SSH in HPC Multi-user Service Environment

Jae-Kook Lee, Sung-Jun Kim* and Taeyoung Hong

Department of Supercomputing Infrastructure, KISTI, KOREA;
jklee@kisti.re.kr, sjkim@kisti.re.kr, tyhong@kisti.re.kr

Abstract

Background/Objectives: The brute-force attack is one of popular cyber security threats in the secure shell (SSH) service environment. The SANS Institute has warned about SSH brute-force attacks against remote services. **Methods/Statistical Analysis:** We describe two brute-force attack detection methods are applied in the High Performance Computing (HPC) service environment which has been operated by KISTI in KOREA. The first way parses failed authentication logs of systems. The second way analyze dropped events of network firewalls. **Findings:** We analyze SSH brute-force attacks that are detected applying these methods in our service environment. The analysis results show that SSH brute-force attacks are classified '1:N' or 'N:1' types of attack between source and destination IP address. And a duration of attacks that is generally the time it takes to execute attacks keeps enough long times. **Improvements/Applications:** Two detection methods which are deployed in our HPC multi-user service environment are complementary to each other. These methods will be also able to apply for other service environment.

Keywords: Brute-force Attack, Cyber Attack Analysis, SSH, Supercomputer

1. Introduction

KISTI (Korea Institute of Science and Technology Information) National Supercomputing Center had constructed the 4th supercomputer (KISTI-4)-called GAIA and TACHYON-in 2009[1,2]. The KISTI-4 is providing the high performance computing (HPC) service to all researchers who need the resource. They use SSH (which stands for 'secure shell')[3] to log in to the supercomputer from remote another computer (server). SSH is high-security protocol. It uses strong cryptography to protect your connection against eavesdropping, hijacking and other attacks. But brute-force attacks is major security threat against remote services such as SSH. The SSH brute-force attack attempts to get abnormal access by guessing user accounts and passwords pair. It is one of classical security threats but still persists for several decades. The SANS Institute called brute-force attacks against SSH to "the most common form of attack to compromise servers facing the internet." On May 2015, MaAfee Labs show top network attacks in Q1. A brute-force attack has been ranked in top 2. These attacks are very common, accounting for about 25% of all network attacks reviewed in the report.

These SSH brute-force attacks have been detected by two well-known methods that using either log files[4] or network traffic[5]. The first method parses the log file of all hosts in large networks, and thereby imposes heavy maintenance costs on administrators. The second approach analysis network traffic in real time. However, this approach difficult to distinguish between normal and abnormal traffic (attacks) because this approach uses to only capture traffic through a few observation points[6].

In this paper, we describe two way in order to accurately detect SSH brute-force attacks. These methods had been applied to our site. The first way parses failed access logs of systems. Then we cluster of source IP addresses or user account. If the number of failed logs in a group by source IP addresses or user account exceeds the threshold, we detect an attack. The second way analyze dropped

*Author for correspondence

events of network firewalls. It classify by source IP addresses or destination IP addresses and detect attacks by checking whether dropped events above a threshold. We detect SSH brute-force attacks against the supercomputing services through analysis collected log messages and events. We analyze the characteristics of detected brute-force attacks and discuss the distribution of the attack duration

The rest of this paper is organized as follows: Section 2 describe related work about a firewall and a SSH brute-force attack. Section 3 provides detail of SSH brute-force attack detection methods. In Section 4, we evaluate a number of detected attack IP address and analyze attack duration distribution. Finally, we conclude in Section 5.

2. Related Work

2.1 Firewall

A firewall is the most popular network-based security device. Firewall rules are the basic elements of the firewall security policy, and usually the firewall policy is composed of dozens to thousands of rules. Each rule consist of 7 parts: index, action (PASS, DROP), protocol, source IP address, source port, destination IP address, destination port. An index describes priority of rules and an action indicates either allow or deny access of network traffic. A protocol defines network or transport layer protocols such as TCP, UDP, and ICMP. A source and destination IP address denote a computer's address or address range of sender and receiver under the internet protocol. A source and destination port is number used to identify services. These port parts can use specific or any port number.

2.2 SSH Brute-Force Attack

A SSH brute-force attack is attempt to acquire administrator or user permission from the host of the SSH service by repeatedly attempt user accounts and passwords. This attack is one of traditional attacks but it still occur endlessly even in recent days. These attacks have been detected through two well-known methods. The first way parses the log file of every systems and keeps track of inaccessible login attempts against SSH. If the number of unsuccessful login attempts exceeded a pre-defined threshold, user connections are denied by dynamically adding a new rule[6,7]. But this method imposes large maintenance costs on administrators, if there are many servers.

The second way checks a sharp deviation from a pre-defined threshold is obtained by statistical modeling to the network traffic[5,8]. But this method difficult to distinguish between normal and abnormal traffic because there are no way of verifying all network traffic practically.

3 SSH Brute-Force Attacks Detection

In order to detect the SSH brute-force attack, we use two method together, which is shown in Figure 1. SSH servers write user authentication logs in syslog file. The firewall control (PASS or DROP) traffic access towards SSH servers and store/manage events. The first method parses log file of all log in SSH servers and second way analyze all firewall events in HPC service network[9].

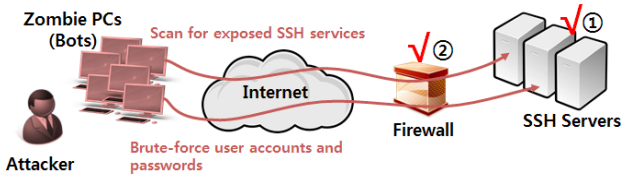

Figure 1. Detection point against SSH brute-force attacks.

3.1 Detection using Failed Authentication Logs

There are a number of SSH servers in a multi-user environment such as HPC. We use the syslog-ng[10] which is the trusted log management software to collect a lot of logs from servers in one place. From collected logs, we seek out failed authentication logs and cluster to source IP address or user account in real time. If the number of failed authentication logs in the clustered group exceed pre-defined thresholds within monitoring time window like below equation (1), then the IP address is detected a SSH brute-force. This detection method is denominated the 'F-LBD (Fail-Logs Based Detection mechanism)' in below.

$$\frac{\sum_{i=1}^{n} f(e_i)}{\Delta t} > Threshold,$$
$$\Delta t = size\ of\ Time\ Sliding\ Window,$$
$$f(e_i) = failed\ Authentication\ Logs\ with\ same\ source\ IP\ address\ or\ user\ account \quad (1)$$

3.2 Detection using Dropped Firewall Events

The firewall monitors and controls network traffic in order to defense against unwanted and disapproved accesses. SSH brute-force attacks sometimes try to access to no service IP addresses. These accesses are dropped by firewall rules. We groups drop events into source or destination IP addresses. Similar to F-LBD, if the number of drop events in the clustered source or destination IP addresses group exceed pre-defined thresholds, then SSH brute-force attacks are detected. In this paper, we called this method 'D-EBD (Drop-Events Based Detection mechanism)'.

4. Analysis of SSH Brute-Force Attacks

Table 1 describes the dataset to analyze SSH brute-force attacks. These are collected data for six months in our HPC environment. If a number of accesses have same SSH process ID then we count it as one access log.

Table 1. Analysis datasets

dataset	
Period	1 Jan. 2015 ~ 30 Jun. 2015
Access logs (SSH)	283,625
Firewall Events	1,274,163,692

We could detect to 983 SSH brute-force attacks using the F-LBD. Figure 2 shows monthly SSH brute-force attack IP addresses and distribution of abnormal access attempts detected by the F-LBD. In Jan., Feb. and Apr., there are less SSH brute-force attack IP addresses than other month. But there are too many abnormal accesses against SSH remote service. It is classified '1:N' type attacks like DoS (Denial of Service). On the contrary, in May, there are many attack IP addresses but on the contrary there are less access attempts with SSH brute-force attack than others. It is classified 'N:1' type attack such as distributed DoS attacks.

Also, we could detect to 2,352 SSH brute-force attacks using D-EBD. Figure 3 shows monthly SSH brute-force attack IP addresses detected by the D-EBD. The D-EBD detects more SSH brute-force attacks than the F-LBD because the D-EBD finds up to SSH scanning attacks try to connect to every IP address in HPC subnetworks.

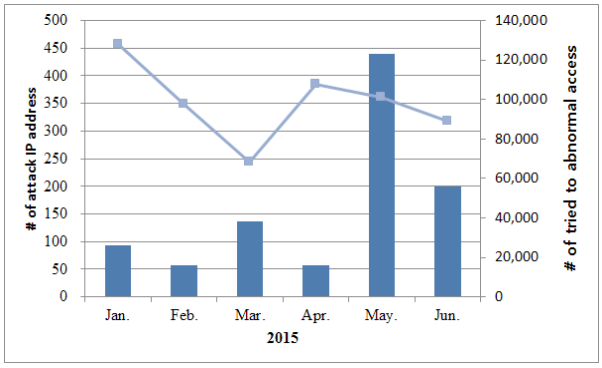

Figure 2. SSH brute-force attacks and abnormal accesses detected by F-LBD (montly).

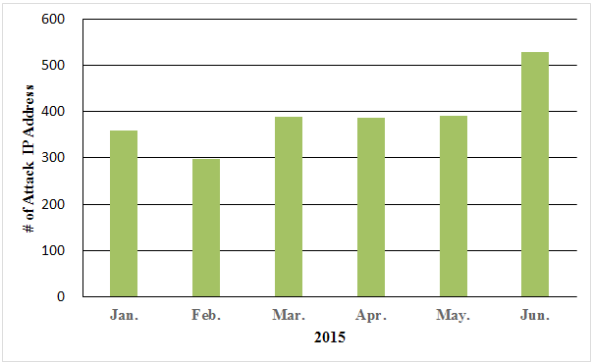

Figure 3. SSH brute-force attacks detected by D-EBD (monthly).

There were many attacks to SSH servers among detected attacks by the D-EBD. Practically we find 1,086 attacks toward servers among detected 2,352 SSH brute-force attacks by D-EBD. We expect detection of attacks ahead SSH servers through the D-EBD. It can function and reduce the load of servers as a pre-filter. Figure 4 shows monthly ratio of pre-filtered brute-force attacks. The average ratio is more than 46% although there is a discrepancy in monthly ratio.

Figure 5 shows distribution of attack duration. An attack duration T_d is period of time between start times (T_s) and end times (T_e) of attack like in below equation (2). In chart, horizontal axis represents date and vertical axis represents attack duration. As shown in graph, a SSH brute-force attacks have continued for a long time, rather than ending in a short period of time. The maximum attack duration is about 4,224 hours. It indicates to try constantly and consistently during 6 months.

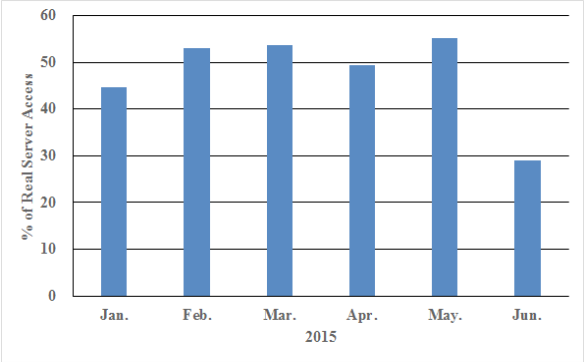

Figure 4. Ratio of pre-filtered SSH brute-force attacks by D-EBD (monthly).

$$T_d = T_e - T_s,$$
$$T_d = attack\ duration$$
$$T_s = start\ time\ of\ attack \quad (2)$$
$$T_e = end\ time\ of\ attack$$

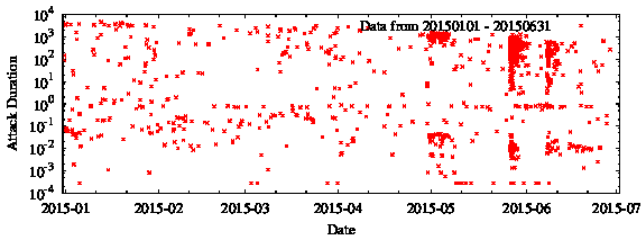

Figure 5. Attack duration distribution.

5. Conclusion

The SSH brute-force attack attempts to get abnormal access by guessing user accounts and passwords pair. It is one of classical security threats but still persists for several decades. In this paper, we describe two detection methods (F-LBD, D-EBD) against SSH brute-force attack in supercomputing service environment. The F-LBD parses failed authentication logs of SSH servers and The D-EBD use dropped firewall events. In our HPC environment, the F-LBD detected 983 SSH brute-force attacks and the D-EBD detect 2,352 SSH brute-force attacks during 6 months in 2015. The analysis results show that SSH brute-force attacks have 1:N or N:1 types of attack between source IP address and destination IP address. And we also confirmed that attackers keep enough long time to success the SSH brute-force attack.

6. References

1. Ahn BY, Jang JH, Ahn SI, Kim MI, On NR, Hong JH, Lee S. Study of high performance computing activation strategy. International Journal of Multimedia and Ubiquitous Engineering. 2014 Jun; 9(6):59–66.
2. Lee J-K, Kim S-J, Park CY. Performance Evaluation and Analysis of Network Firewalls in High Speed Network. Indian Journal of Science and Technology. 2015 Oct; 8(25):1–5
3. Ylonen T, Lonvick C. The Secure Shell (SSH) Transport Layer Protocol. IETF RFC 4253, 2006.
4. Thames JL, Abler R, Keeling D. A distributed active response architecture for preventing SSH dictionary attacks. IEEE SoutheastCon 2008. 2008 Apr; 84–9.
5. Sperotto A, Sadre R, de Boer P-T, Pras A. Hidden Markov Model modeling of SSH brute-force attacks. Lecture Notes in Computer Science. 2009 Oct; 5841:164–76.
6. Satoh A, Nakamura Y, Ikenaga T. A flow-based detection method for stealthy dictionary attacks against Secure Shell. Journal of Information Security and Applications. 2015 Apr; 21(C):31–41.
7. Su Y-N, Chung G-H, Wu BJ. Developing the upgrade detection and defense system of SSH dictionary-attack for multi-platform environment. Journal of iBusiness. 2011 Mar; 3(1):65–70.
8. Sperotto A, Schaffrath G, Sadre R, Morariu C, Pras A, Stiller B. An overview of IP flow-based intrusion detection. IEEE Communication Survey and Tutorial. 2010 Aug; 12(3):343–56.
9. Lee J-K, Kim S-J, Woo J, Park C-Y. Analysis and Response of SSH Brute Force Attacks in Multi-user Computing Environment. KIPS Tran on Computer and Communication Systems. 2015 Jun; 4(6):205–12.
10. Syslog-ng. Available from: https://syslog-ng.org. Date accessed: 06/12/2016.