A Denied-Events based Detection Method against SSH Brute-force Attack in Supercomputing Service Environment

Jae-Kook Lee[1], **Sung-Jun Kim**[1], **and Taeyoung Hong**[1]
[1]Department of Supercomputing Infrastructure, KISTI, Daejeon, KOREA

Abstract— *The brute-force attack is one of general cyber security threats in supercomputing service environment using a secure shell (SSH) protocol. First we analyzed SSH brute-force attacks had been detected through the log file parsing method of servers in the KISTI. We found that SSH brute-force attacks are classified '1:1', '1:N' or 'N:1' types of attack between source and destination IP address. And the duration of attacks that is generally the time it takes to execute attacks keeps enough long time. In this paper, we propose a SSH brute-force attack detection method using denied-events of firewalls and evaluate the effectiveness of the method. The analysis results show that our method filter beforehand by 46% on average that the attack traffic flow to active servers.*

Keywords: Brute-force attack; Supercomputer; Security; SSH, Attack Detection

1. Introduction

The brute-force attacks is the major security threat against remote services such as SSH [1]. The SSH brute-force attack attempts to gain abnormal access by guessing a user account and password pair. The SANS Institute called brute-force attacks against SSH to "the most common form of attack to compromise servers facing the internet [2]." And on May 2015, MaAfee Labs show top network attacks in Q1 [3]. A brute-force attack has been ranked in top 2. Thus it is one of classical security threats but still persists for several decades.

In this paper, we analyze SSH brute-force attacks are detected in the KISTI supercomputing service environment using the log file parsing method of servers [4]. In [4], parsed log files are clustered together in the same Src. IP or user account. If the number of failed logs in a group by Src. IP or user account exceeds the threshold, then it is detected a SSH brute-force attack. Analysis result shows that SSH brute-force attacks are classified '1:1', '1:N' or 'N:1' types of attack between Src. and Dst. IP. And the duration of attacks that is generally the time it takes to execute attacks keeps enough long time.

In order to reduce the load of active servers from long time attacks, we propose a SSH brute-force attack detection method using denied-events of network firewalls. In order to detect a SSH brute-force attack, this approach classifies by Src. IP or Dst. IP and detects attacks by checking whether dropped events above a pre-defined threshold. If there are attacks, the Src. IP is inserted to the new firewall rule automatically. We evaluate the effectiveness of the method in our environment. The result show that the attack traffic directed to active servers are reduced.

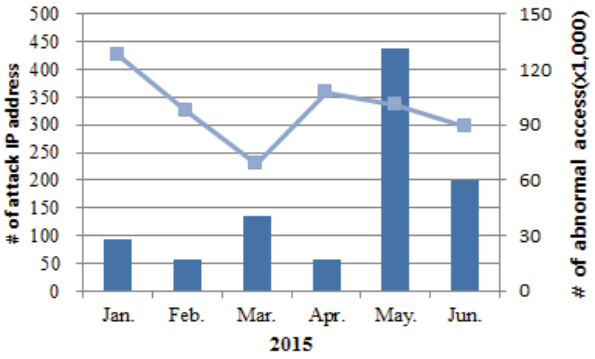

Fig. 1: Detected SSH brute-force attacks and abnormal accesses by [4] (monthly).

The rest of this paper is organized as follows: Section 2 analysis SSH brute-force attacks that are detected using the log file parsing method of servers in the KISTI. And we provides detail of SSH brute-force attack detection methods using denied-events of a firewall and evaluate the effectiveness of the method in Section 3. Finally, we conclude in Section 4.

2. SSH brute-force attacks analysis

We could detect to 983 SSH brute-force attacks using the fail-log based detection method was proposed in [4] for 6 months. If a number of accesses have same SSH process ID then we count it as one access log. Fig. 1 shows monthly SSH brute-force attack IP and distribution of abnormal access attempts detected by [4]. In Jan., Feb. and Apr., there are less SSH brute-force attack IP than other month. But there are too many abnormal accesses against SSH remote service. It is classified '1:N' type attacks such as DoS (Denial of Service). On the contrary, in May, there are many attack IP 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.

Attack duration is the time difference from the point of first traffic occurrence and the point of final traffic

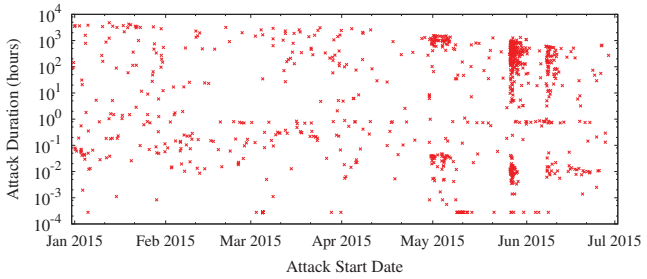

Fig. 2: Attack duration of SSH brute-force attacks.

Table 1: Events of the KISTI supercomputer firewalls

	Data
Date	2015.1.1 - 2015.6.30
Total log file size	231.96 Gbytes
Total firewall events	1,274,163,692

occurrence within the relevant period. Fig. 2 shows the distribution of SSH brute-force attacks. Fig. 2 is a log-linear plot where the horizontal axis represents the first access time and the vertical axis represents the attack duration. Each (red) dot represents an attack that occurred from one Src. IP. As shown in Fig. 2, attack duration is widely distributed in the log-linear scale.

3. Denied-events based detection method

In order to reduce the load of active servers from long time attacks, we propose a denied-events based detection method using events of firewall. SSH brute-force attacks sometimes try to access to inactive servers. These accesses are denied by firewall rules. We groups denied events into Src. or Dst. IPes. If the number of denied events in the clustered Src. or Dst. IP group exceed pre-defined thresholds, then SSH brute-force attacks are detected. In this paper, we called this method 'DEBD (Drop-Events Based Detection mechanism).'

Table 1 describes firewall events were collected in our supercomputing service environment. We could detect to 2,352 SSH brute-force attacks by DEBD. Fig. 3 shows monthly SSH brute-force attack IPes. The DEBD detects more SSH brute-force attacks than the [4] because the DEBD finds up to SSH scanning attacks try to connect to every IP in supercomputing service subnetworks.

There are many attacks to SSH servers among detected attacks by the DEBD. Practically we find 1,086 attacks toward servers among detected 2,352 SSH brute-force attacks by DEBD. We expect detection of attacks ahead SSH servers through the DEBD. It can reduce the load of servers as a pre-filter. Fig. 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.

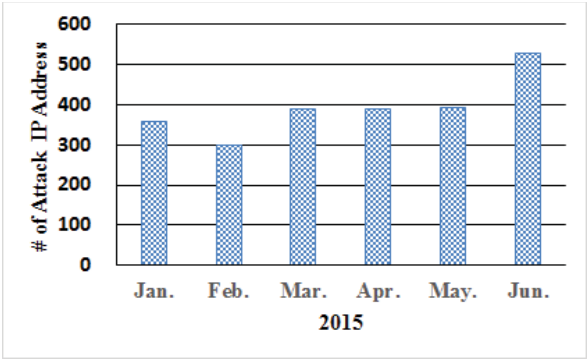

Fig. 3: Detected SSH brute-force attacks by DEBD (monthly).

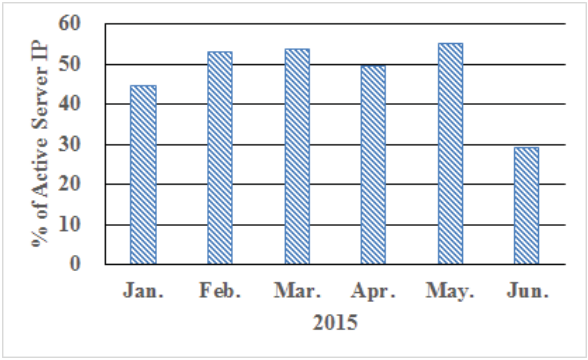

Fig. 4: Ratio of active servers IP among the detected attacks.

4. Conclusions

In this paper, we propose DEBD method against SSH brute-force attack. In our environment, the [4] detected 983 SSH brute-force attacks and the proposed DEBD detect 2,352 SSH brute-force attacks during 6 months in 2015. The proposed method filter beforehand by 46% on average that the attack traffic flow to active servers.

References

[1] T. Ylonen and C. Lonvick, The Secure Shell (SSH) Transport Layer Protocol, RFC 4253, 2006
[2] Owens, Jim, and Jeanna Matthews, "A Study of Passwords and Methods Used in Brute-Force SSH Attacks," USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008
[3] McAfee Labs Threats Report (2015). [Online]. Available:http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf
[4] Jae-Kook Lee, Sung-Jun Kim, Joon Woo, and Chan-Yeal Park, "Analysis and Response of SSH Brute Force Attacks in Multi-user Computing Environment," KIPS Tran. on Computer and Communication Systems, Vol. 4, No. 6, Jun. 2015.
[5] Thames, J. Lane, Randal Abler, and David Keeling, "A distributed active response architecture for preventing SSH dictionary attacks," IEEE Southeast Con., 2008.
[6] A. Satoh, Y. Nakamura, and T. Ikenaga, "A flow-based detection method for stealthy dictionary attacks against Secure Shell," Journal of Information Security and Applications, 2014, Vol. 21, pp.31-41