iBusiness, 2011, 3, 65-70
doi:10.4236/ib.2011.31011 Published Online March 2011 (http://www.SciRP.org/journal/ib)

Developing the Upgrade Detection and Defense System of SSH Dictionary-Attack for Multi-Platform Environment

Yen-Ning Su[1], Guang-Han Chung[2], Benjamin Jenghorng Wu[3]

[1]Department of Engineering Science, National Cheng Kung University, Taiwan, China; [2]Department of Leisure and Information Management, Taiwan Shoufu University, Taiwan, China; [3]Institution of Technology Development and Communication, National University of Tainan, Taiwan, China.
Email:[1]yenning@mail.tn.edu.tw; [2]guanghan999@hotmail.com; [3]whiteben0222@gmail.com

Received November 14th, 2010; revised December 29th, 2010; accepted January 8th, 2011.

ABSTRACT

Based on the improved algorithm for analyzing log and the detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment (*Su, Chen, Chung & Wu*), *we developed the upgrade detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment. In this study, we introduced the current threats and the types of SSH Dictionary-Attack. Then, we explained the functions and differences between the current defense software and defense types of SSH Dictionary-Attack*; *and described the current system of SSH Dictionary-Attack for Multi-Platform Environment. Moreover, based on the study of Su, Chen, Chung and Wu, we improved the algorithm of analyzing log in order to increase the defense capability of SSH Dictionary-Attack. After that, we designed the upgrade detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment. The contribution of this study is to provide the upgrade detection and defense system of SSH Dictionary-Attack which was to keep the functions of original system of SSH Dictionary-Attack, and to improve the effectiveness of the algorithm of analyzing log.*

Keywords: *SSH Dictionary Attak, An Improved Algorithm for Analyzing Log, Multi-Platform Environment*

1. Introduction

The internet grew rapidly, and the operation of server software was getting easy. For public, privet, and academic organizations, they could simply design the web to service the public and provide the easy access for people to reach information.

However, how to ensure the safety of the server became the big issue for the server designers. Simson Garfinkel and Gene Spafford pointed out that there were many online-safety cases happening in the recent years, for example account invaded, the pin numbers were stolen and so on [1]. Those problems cased a lot of damages which were hard to value. According to the annual report of Government Accountability office (in 2009), there were seven major elements of network security, such as network analysis, and early warning capacity [2]. In addition, other related studies and SANS indicated that the attacks for remote network servers mostly focused on SSH, FTP, Telnet and Web, especially attacking SSH, FTP and Telnet servers through violent pin number guesses [3-5]. Hence, if the web-site administrators could focus on the web safety, pay attention on the network connection status, and design the warning system for network attacks, this would increase the safety of the servers.

In the control of the server safety, password system was the first defense [6,7]. Generally, most servers used account and password as the tool for access control. By using those tools, the administrators could control the users to access into the system. However, if the intruders could break the password system, there would be no safety in the server. Based on the study of Su and Chen, the finding indicated that the password system was the most popular used. It was important to ensure the safety of the password system in order to increase the security of the web system [7].

SSH Dictionary-Attack defined as the way for intruders to attack the SSH servers by guessing the combinations of the numbers in order to get the pin number to access into the target accounts. According to Xue's study

(in 2009), SSH Dictionary-Attack was the major way for the intruders to attack network systems. When the administrators checked the records of the network systems, they found out that most intruders used this way to attack system, and this kind behavior cased a lot of troubles for the administrators [8].

In the recent year, because the price of hardware decreased and the technology of virtualization was popular, administrators may need to control many servers at the same time. If the servers were attacked with malice frequently, the administrators would need to spend extra time to maintenance the servers and this would case the extra burden to the administrators.

In 2009, Su and Chen already designed the detection and defense system for SSH Dictionary-Attack which focused on the analysis of the system logs in the single platform [7]. Su, Chen, Chung and Wu proposed the system of SSH dictionary-attack for multi-platform Environment, and after the test, the finding indicated the system had effective results [9]. In this study, the researchers tried to improve the algorithm for analyzing log of SSH dictionary-attack in order to increase the defense capacity. Hence, there were two purposes of the study. First one was to keep the instant share of the attacking resources of SSH dictionary-attack. Second one was to improve the effectiveness of the algorithm for analyzing log of SSH dictionary-attack in order to provide the better way for defending SSH dictionary-attack.

2. Literature Review

Dictionary-attack defined as the attack model which used violent password guesses. The intruders who belonged to this attack type often attacked the system by using the combination of numbers, and continued the error testing until they broken the system or gave up the trying [7,8]. The definition of SSH Dictionary-Attack in this study is on-line password guessing attack [6-8,10]. This model is that the intruders tried to connect with the target computers, and continued attacking the servers by error testing until they have the correct password to access the system [7,8].

In the passed studies, there were many defenses models for SSH Dictionary-Attack, for example 1) changing port; 2) connecting with accepted lists; 3) connecting with rejected lists; 4) asymmetric encryption of public and private key; 5) using attacking detection program; 6) analyzing the log files; 7) intensifying codes. By changing port, it changed the original Port22 to other port in order to increase the cover of SSH service. Then, connecting with accepted lists allowed the certain online resources to use SSH service. In the other hand, connecting with rejected lists allowed all resources to use SSH service. But the system would reject connecting with the online resources from the rejected lists. Asymmetric encryption of public and private key was to exchange the public and private key for server and client. Client could access to the server without verifying the password [11]. Attacking detection program could detect the attacking behaviors from remote resources. If the defection program was correct, the administrators could get the early warning and blockade [8]. Analyzing the log files used the attacking records of SSH Dictionary-Attack, and found out the malice attacking resources and block the sources in order to defense SSH Dictionary-Attack [7]. Finally, intensifying codes was to use complex combinations of words and numbers in order to reduce the chance for cracking by SSH Dictionary-Attack [12]. This part belonged to the safety of the information system.

The software which currently sell in the market for defending SSH Dictionary-Attack are ssdfilter, Fail2Ban, denyhosts, sshit and the software developed by Su and Chen. The common parts of these software were all using “connecting with rejected lists” and “analyzing the log files” as the defense models for SSH Dictionary-Attack [7,8,12-14]. Especially, the software developed by Su and Chen was effective more than others in immediate function [9].

In the following studies, Su, Chen, Chung and Wu designed the detection and defense models of SSH Dictionary-Attack for Multi-Platform Environment. The new function could help multi-servers to blockade the resources from the rejected lists. After the testing, this program actually could defend SSH Dictionary-Attack in multi-platform Environment [9].

Moreover, the researchers found that the system could sharing the rejected lists, and have the better instant defense capacity. However, when the log got more data, the administrators were hard to define the accurate numbers for calculation. This would reduce the accuracy of the defense function of SSH Dictionary-Attack. Hence, in this study, the researchers tried to find the solutions for this problem and hope to improve the algorithm for analyzing log and the system of SSH Dictionary-Attack for multi-platform Environment.

3. System Architecture

Based on the study of Su, Chen, Chung and Wu, the researchers designed “the detection and defense model of SSH Dictionary-Attack for Multi-Platform Environment. The system included a main server and several SSH servers. For the structure of the system, please see **Figure 1** [9].

The defense and detection models of SSH Dictionary-Attack for Multi-Platform Environment (Su, Chen, Chung and Wu) was designed based on the study of Su

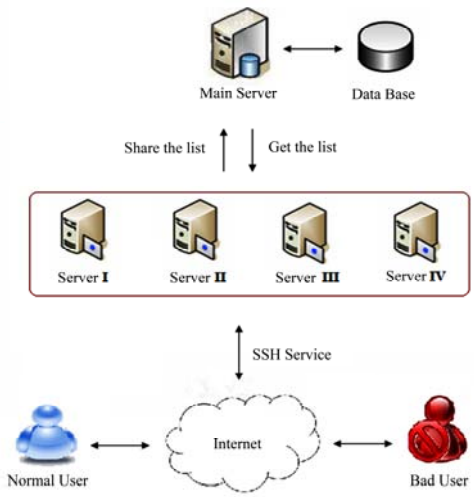

Figure 1. System architecture.

and Chen. The operational process was detecting the connections of SSH through TCP-Wrapper and the trigger tools. For the operational process, please see **Figure 2** [7,9].

In this study, the researchers tried to improve the analysis of log. In the update system, the researchers not only use "sharing the rejected lists", but also saved the numbers of attacking ip Address into the database. The numbers of attacking ip Address from all sources were set up as zero. Then, if the ip address connected with other servers, the system would record all error testing in the log. Every time, the error record was renewed, and the system would add the attack numbers automatically. When the attack numbers from the ip address reached the maxima of the system setting, the update defense program will blockade this ip address in order to achieve the purpose for defending SSH Dictionary-Attack. Please see **Figure 3** for the update system.

In addition, in order to limit the numbers of error testing for the single connection from the ip address, the researchers adjusted sshd_config of MaxAuthTries, and changed the presetting number six to number 1. Hence, it would solve the problem which was several error testing

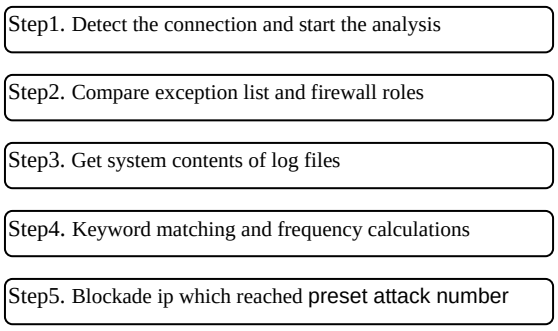

Figure 2. Defenses and detection model from Su & Chen.

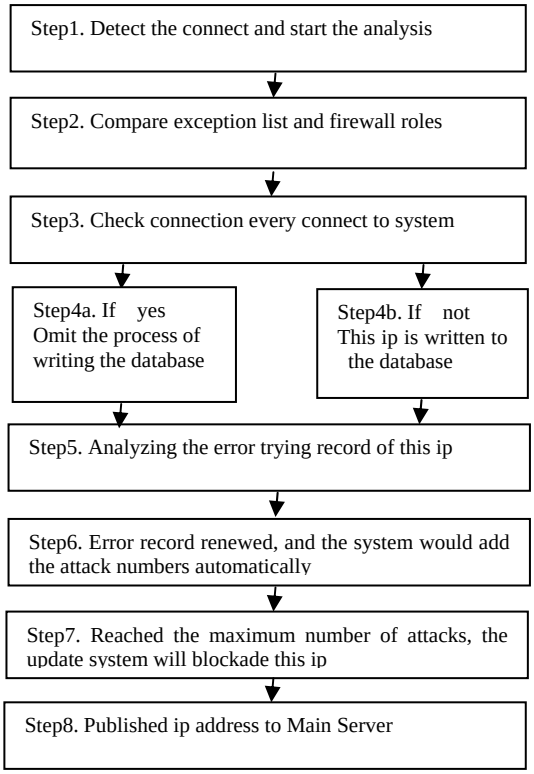

Figure 3. Defenses and detection model from Su, Chen, Chung & Wu.

for the single connecting from one ip address. This function could make sure that it would happen certain times of error testing from the single connecting. This also helped the research to improve the algorithm for analyzing log and to increase the accuracy of distinguishing SSH Dictionary-Attack.

Moreover, please see **Figure 4** for the process of sharing the rejected lists [9].

4. System Development and Presentation

The researchers improved the algorithm for analyzing log based on the study of Su and Chen [7], and also using the idea of sharing the rejected lists [9], to develop the update detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment.

For improving the algorithm for analyzing log, the

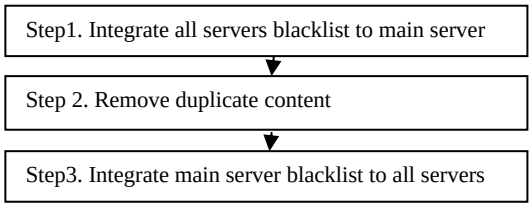

Figure 4. The process of integrate blacklist.

researchers saved the numbers of attack into the database, and the system could calculate the numbers of attack from different ip address independently. Also, these numbers would be the basis for blockading ip address. For the content list of the number of attack, please see **Figure 5.**

Figures 6 and **7** were the files of analyzing the log and the decision making process for cumulating the numbers of attack. If the ip address did not connect with the system through SSH service, the databases would not have information about this ip address. Hence, the defense system would set up a new file for this ip address, and the number of attack started with zero. Please see **Figure 6.**

Until the ip address connected with the server, the system would check error testing record for this ip address. If any error testing happened, the system would automatically add the numbers together. Please see **Figure 7.**

If the numbers of attack from the same ip address reached the maximum of the setting, the defense system would report this ip address to the firewall (IPFW) to blockade the address. Please see **Figure 8**.

In order to make sure that there will be certain error testing happened, the researchers used sshd_config of MaxAuthTries, and changed the reset data 6 to 1 in order to continue the following calculation. Please see **Figure 9.**

For the implementation, **Figure 10** showed the contents of the numbers of attack, and the cumulative value for each ip address.

Figure 11 displayed that when the attacking numbers from the ip address reached the maximum of the system setting, the update detection and defense system will

```
# Operating System (FreeBSD(ipfw) ; Linux(iptables))
OS="FreeBSD"

# Test Mode
test="NO"

# System Log File
run_log2="/root/home/network/log.txt"

# Share Bad List (Server's ip Address)
mainserver="127.0.0.1"

# Bad List File (Remote Machine)
remotefile="~/bad_list"

# ip Log File
ip="/root/home/network/ip/"
```

Figure 5. The number of attacks record.

```
echo "0" > "$ip""$badhost"

# Time
t=`echo $date | sed 's/ /:/g' | sed 's/::/:/g' | cut -d
# Month
m=`echo $date | sed 's/ /:/g' | sed 's/::/:/g' | cut -d

# Account exists,  Password incorrect
rule1=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

# Account is not exist
rule2=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

# Account is not exist
rule3=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

num=`$cmd_cat "$ip""$badhost"`
sum=`expr $rule1 + $rule2 + $rule3`

 {
   if [ "$sum" -ge "1" ]; then
     count=`expr $num + 1`
```

Figure 6. Create and write initial value.

```
# Account exists,  Password incorrect
rule1=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

# Account is not exist
rule2=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

# Account is not exist
rule3=`$cmd_cat "$s_log" | $cmd_grep $t | $cmd_grep $m

num=`$cmd_cat "$ip""$badhost"`
sum=`expr $rule1 + $rule2 + $rule3`

 {
   if [ "$sum" -ge "1" ]; then
     count=`expr $num + 1`
     echo $count > "$ip""$badhost"
   fi
 }

fi

badcount=`cat "$ip""$badhost"`
```

Figure 7. Analysis of error trying record.

```
badcount=`cat "$ip""$badhost"`


if [ "$badcount" -ge "$countloginFail" -o "$test" = "YES" ]; then
{
  if [ "$badhost" != "" ]; then
    {
      # Deny bad ip address
      $cmd_ipfw add deny ip from "$badhost" to me

      # Send message to remote server
      `ssh yenning@$mainserver "echo $badhost >> $remotefile"`

      echo "$date $cmd_ipfw add deny ip from $badhost to me" >> "$run_log"
      #Test Mode
      echo "Time:$date ; bad ip:$badhost" >> "$run_log2"
```

Figure 8. The maximum number of attacks to be blocked.

```
# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
MaxAuthTries 1
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

Figure 9. Sshd_config of MaxAuth tries setting.

```
116.228.1.50    120.114.12.44    123.196.113.11    194.106.168.130  205.185.125.158  211.115.234.145
119.39.227.196  122.123.241.57   140.116.243.66    202.112.126.217  210.216.230.202  60.240.242.207
tdc# cat 194.106.168.130
3
tdc# cat 116.228.1.50
0
```

Figure 10. The numbers of attack data.

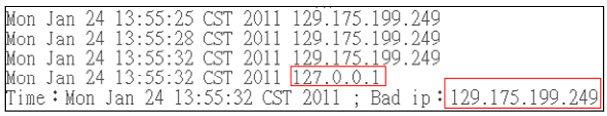

Figure 11. Ip address blockade.

blockade this ip address. Also, the system will send the ip address to the main server. In this study, because the main server and experimental server were in the same machine, the ip was 127.0.0.1.

Figure 12 showed that the ip address of malicious sources was sent to the main server. After organizing the data, the main server sent out the ip address of malicious sources to other SSH server.

5. Conclusions

In the study, the researchers designed the defense and detection system of SSH Dictionary-Attack for Multi-Platform Environment in order to provide an effective model based on the study of Su, Chen, Chung and Wu [9]. The advantages of the update system were:

1) Convenience: the administrators only need to install the detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment, and connect the main server into other servers. The system will defend SSH Dictionary-Attack automatically. This function helped the administrators to save time in monitor the system.

2) Security: by using the concept of sharing the rejected lists, adding the server into the group of the defense servers could share the new lists of malicious sources at any time. It will increase the safety of the server and reduce the chance from attacking by the same source.

In addition, the update system has the function of instant defense as the system which was developed by Su and Chen [7]. By using TCP-Wrapper to detect the connection with SSH and starting the analysis program, the server could define whether the remote connection is a malicious source or not in order to blockade it. Hence, the update system has the instant function for defense.

The update system, "the detection and defense system of SSH Dictionary-Attack for Multi-Platform Environment", improved the defense function of the old system. For the log problem, the update system saved the numbers of attack into database, and based on each ip Address, the system could calculate the numbers. Hence, by

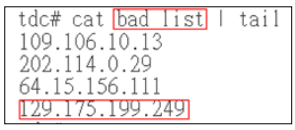

Figure 12. Ip address blacklist.

improving algorithm for analyzing log, the system could increase the effectiveness of the defense capacity of SSH Dictionary-Attack for Multi-Platform Environment.

For the future study, the researchers plan to analyze the common used models of SSH Dictionary-Attack, for example particular account and password, and the changes of network traffic. Also, the following studies will try to combine decision tree algorithm in order to increase the accuracy of defense system and to help the administrators to maintain the servers.

6. Acknowledgments

The article was presented in the International Conference on Internet Technology and Applications (iTAP 2010) on August 22, 2010. The researchers appreciated that the experts and participants gave professional suggestions. The contents of this research was revised and expanded. The researchers express thanks to iTAP.

REFERENCES

[1] S. Garfinkel, G. Spafford. "Practical UNIX and Internet Security (3rd Ed.)," O'Reilly Media, 2003.

[2] U.S.G.A.O. "Continued Federal Efforts Are Needed to Protect Critical Systems and Information," 2009.

[3] S. Christey and R. Martin, "Common Weakness Enumeration. Vulnerability Type Distributions in CVE," May 22, 2007. Internet Available: http://cwe.mitre.org/documents/ vuln-trends/index.html

[4] SANS Institute. "SANS Top-20 2007 Security Risks(2007 Annual Update)", 2007. Internet Available: http://www.sans.org/top20/2007/

[5] J. Owens and J. Matthews, "A Study of Passwords and Methods Used in Brute-Force Ssh Attacks," *Technical Report*, Department of Computer Science, Clarkson University, 2008.

[6] S. William, "Stallings: Network Security Essentials:Applications and Standards 2/E", Pearson, 2005.

[7] Y. N. Su and Y. H. Chen, "Block Online Password Guessing Attacks to a SSH Service with Analyzing System Log Files," *Journal of Computer Science and Application*, Vol. 5, No. 2, December 2009, pp.108-122.

[8] Y. J. Hsueh, "A Study of Using NetFlow Traffic Data to Detect and Track SSH Dictionary Attack," Master Thesis, Department of Asia-Pacific Industrial and Business Management, National University of Kaohsiung, Taiwan, 2009.

[9] Y. N. Su, Y. H. Chen, G. H. Chung and B. J. H. Wu, "Developing a SSH Dictionary Attack Defense System in the Multi Platform Environment through the Analyzing Log". *International Conference on Internet Technology and Applications*, China, 2010.
doi:10.1109/ITAPP.2010.5566560

[10] R. Corin, J. Doumen and S. Etalle, "Analysing Password Protocol Security Against Off-Line Dictionary Attacks,"

Electronic Notes in Theoretical Computer Science, Vol. 121, No. 4, 2005, pp. 47-63. doi:10.1016/j.entcs.2004.10.007

[11] D. M. Tsai, "Bird's Linux: Basic Learning", GrandTech, 2003.

[12] R. Wichmann, "Defending against Brute Force Ssh Attacks", 2008. Internet Available: http://la-samhna.de/library/brutessh.html

[13] S. Shit, "The SSH/FTP Brute Force Blocker," 2010, Internet Available: http://anp.ath.cx/sshit/

[14] V. Goyal, *et al*., "A New Protocol to Counter Online Dictionary Attacks," *Computers & Security*, Vol. 25, No. 2, 2006, pp. 114-120. doi:10.1016/j.cose.2005.09.003

