INTERNATIONAL JOURNAL OF ENGINEERING INNOVATIONS IN ADVANCED TECHNOLOGY
ISSN [O]: 2582-1431 IJEAT VOLUME-I ISSUE-II, APRIL-JUNE-2019

# Honeypot based Intrusion Detection System to Counter Attacks on SSH

I SAJID ALI [1], SIVA RAMA KRISHNA T.[2]
[1, 2]Department of CSE, JNTUK UCEV, Vizianagaram, India
[1] *sajju1234ali@gmail.com* , [2]*t_srkrishna@yahoo.com*

***Abstract*--Network intrusion attacks are performed quite immensely these days, malicious intruder performs attacks on the infrastructure of a network of organizations. The increase in the number of various intruders and different attacks has made mitigation and security implementation a hard task to be achieved. In order to accomplish felonious access over server attackers target Secure Shell service. In this paper, an intrusion detection operation and web trap for intruders is performed on the SSH service. A fake file system is created which will camouflage itself as the original root. A honeypot system which remains an effective environment in gathering intelligence about the intruder and information is used which are highly sufficient in the identification of the attacker is collected. In this paper, the honeypot is used to by-port the main SSH port and run the fake file system of the honeypot in the main port to mislead and trap the details of the intruder. By the end of the process reports and play logs will be generated on the performed attacks which would be useful for further research phase. Using visualization tools would further help in the analysis of the activity of the attacker.***

***Keywords:Intrusion detection, SSH, by porting, attack, analysis, intruder, honeypot, brute-force.***

## 1. INTRODUCTION

Over the past years, information technology has made a considerable growth in the world. The use of technology in our daily life has made the security of data a major concern. The stupendous use of computers and internet for information exchange and money transactional purposes has become a primary approach in modern-day reality. Malicious intruder launches attacks on the specific targets using diverse attacks to snatch the information of a user. The reason for these attacks could be for financial data or for information related to geopolitical influence. Intruders search for the vulnerable targets over the internet; they search for the servers that can be used to perform their spiteful activities. Remote access administrated setup like SSH service deemed as the most attacked target by the intruder. Using diverse softwares and mechanisms, the intruder tries to have the credentials required for login. The violator tries to make a move on such service-running server, with a successful attempt the compromised server will be used for malicious activity, for instance, attack on other systems, malware setup, and modification of root or denial of service. Distinguishing and defining the attacks of the attacker and recognizing the attackers in real time is a tough job for security providers. Providing policies and developing productive defence strategies play a critical role. To make an impact over the malevolent intruders, security analysts had developed honeypots. Honeypot is an advanced intrusion observation system, which gives notification of up-to-date vulnerabilities. It is a complete activity logging device, which lures the attacker away from the main system. Honeypot acts as a deception tool by exhibiting itself as a vulnerable system and providing a simulated domain to the attacker. It helps the security researchers and analysts with a study over the new techniques of compromising a system by logging the actions performed by an intruder. Honeypots do not have the capability to avert an attack but have the prowess in detection. They produce data about the attacks that can be used for analysis by cyber professional. To provide detail summary of the operation of honeypot to the cyber defence, data visualization and analysis tools are used which compares the sessions and present results in graphical and tabular forms.

In this paper, a Virtual Private Server is set up to log the brute force attacks performed on the SSH honeypot and the activity of the honeypot on the attacks. In this, the information accumulated is analysed by the honeypot by using the visualization tool. By the end, the python play logs generated by honeypot to recollect the exact actions of an intruder.

## 2. THEORITICAL APPROACH

This portion explains a brief synopsis of the hypothesis behind our trail. In this, honeypots are discussed based on their interaction extent and secondly about the tools and their functionality generally used in SSH attacks.

### 2.1 Honeypots classified on their interaction level:

Based on the interaction extent with the attacker, honeypots are distinguished into three categories. Low, medium and high-level honeypot

The primary in these is the low-level interaction honeypot. These deemed as the elementary level honeypots as they are uncomplicated to position and utilize. The maintenance of these honeypots is easiest among the others. The central principle of these is the detection of the intruders and logging their activities. They are the basic level honeypots with very limited data gathering and small network risk. They produce at least level of interaction with the attacker and are possible to capture only know attacks which makes them easily observable the skilled intruder

The secondary is the level medium interaction honeypot. They offer a higher extent of interaction comparative to the low-level pots. They provide a medium level of interaction to the attacker with an average level of information assembling and network risk. Attacker's activities are monitored and recorded by the latent original operating system while they perform their actions on supplied simulated operating system. A virtual operating system is offered to the attacker, which acts as a decoy to the original operating system, this virtual system allows the attacker to enter commands, create or delete directories and also download files. They provide an interface and fake file system, which deceives the attacker that he is in the utilization of the real system.

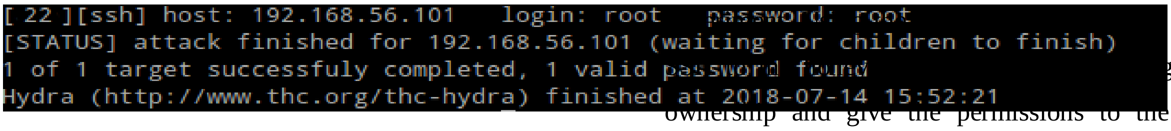
Honeypots with high interaction said to be the final category among the three levels. They present a peak level of interaction to the intruder. These are firm to sustain but have a great level of interaction, which ensures a high level of information assembling and data recording. Unlike medium level honeypots, they offer a real operating system with vulnerability to the attacker. They provide valuable information about the attacker's activities in real time, which helps the security providers to study and prevent future attacks. Their configuration and analysis is a time-consuming process and due to their high interaction extent, they present a serious risk to the network, which must be secured from external resources with the use of firewalls.

### 2.2 Tools and their functionality generally used in SSH attacks:

The protocol which usually used in Linux and Unix operating system is Secure Shell protocol or commonly known as SSH. This protocol allows the authentic users an encrypted remote connection. This protocol generally runs on port 22 with implementation on authentication mechanism. The username and password of the user are used for remote access. The wide usage of SSH protocol with such process could make the attacker simply guessing credentials used by the user or use of brute force attacks. Dictionary text files are created which consists of combinations of passwords us in performing dictionary attacks, which compares each and every password to give a possible result. Over the past years, spiteful attackers have created automated tools to attack a particular service which engages brute-force and dictionary attacks. Few of the well-known tools to attack a system are Medusa, Hydra, Ncrack, and Metasploit. Each of these has their own attack vectors and commands. Other than SSH these tools can perform brute-force on other services like RPD, FTP, and VNC. Some sample command used by hydra to crack SSH password.

```
hydra 192.168.56.101 ssh -l
root -P note.txt -s 22 -vV
```

The above command is used as a test on our SSH service which gave the exact password as the result as shown below figure-1



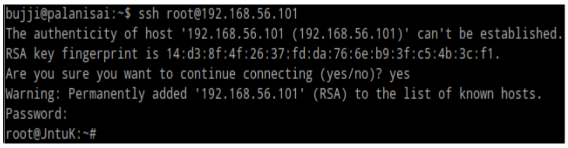
```
[ 22 ][ssh] host: 192.168.56.101   login: root   password: root
[STATUS] attack finished for 192.168.56.101 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-07-14 15:52:21
```

Figure-1The result of brute-force attack on SSH using Hydra

note.txt contained possible passwords where the root is the original. An attacker could use one of these tools to penetrate into the system. Combination of tools and their commands would change depending on the service security strength.

## 3. EXPERIMENTAL APPROACH

This sectionexplains the process and establishment of the experiment. In this, the procedure and overview behind the setup of the experiment are discussed. For the experimental purpose,a virtual system using Oracle virtual box is created with Linux server operating system running in it. AXubuntu server operating system is used which runs as a Virtual Private server. In order to convene an adequate amount of data and evaluate the efficacy,an SSH honeypot is deployed. Using a static IP address have connected this service to the internet and run the Honeypot. An opensource medium interaction honeypot written in python is used which allows itself to interact with the intruder. To establish a secure setup, primarily altering the port number of the SSH service to a free port and bind the honeypot to the default SSH port 22 is discussed. The honeypot runs on the ssh service port 22 and logs the attempts of the connection. In order to store details about the attempts, a database is created for the honeypot using MySQL database and setup MySQL server. The honeypot should never run as a root, which could lead to system compromise when a failure in honeypot occurs. In order to ensure the prevention of access to our other systems, a new user is created and set up the whole 22 of ge the ownership and give the permissions to the user where the honeypot in installed. Honeypot generally runs on its default port,it needs to change this in the configuration file while setup. Asauthbindis used here for by porting so it could use authbind to listen on port 22, preferable change is made in the start script from twistd -y honeypot.tac -l log/honeypot.log --pidfilehoneypot.pid to authbind --deep twistd -y honeypot.tac -l log/honeypot.log --pidfilehoneypot.pid. The Honeypot runs on a varying Pid as a general process. The login authentication works in the same way as the original SSH service with public-private key authentication.



```
bujji@palanisai:~$ ssh root@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
RSA key fingerprint is 14:d3:8f:4f:26:37:fd:da:76:6e:b9:3f:c5:4b:3c:f1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.101' (RSA) to the list of known hosts.
Password:
root@JntuK:~#
```

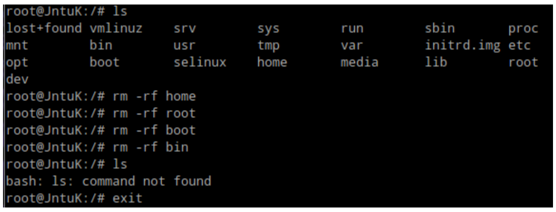
Figure-2 Login Authentication with Public-Private Key Authentication

From the figure-01, honeypot camouflage itself as the same way as the SSH remote authentication acts but logs into the root of the honeypot system. The honeypot decoys itself in the same way as the original system and presents a mirror identical fake file system to deceive the attacker.

## 4. ACTIVITY AND RESULTS

This section discusses the activity of the attacker and the summary of the observed brute-force attacks. This deals with the outcomes gathered and the visualization of the results. This module presents an analysis report on the overview of attacks performed by the intruder.

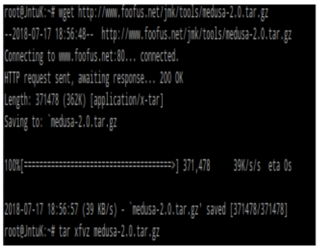
After using the brute-force dictionary attacks to harness the credentials intruder logs in as a normal user with authentication and could perform malicious activities. The intruder could make modification and install malicious software that intends to harm the system. Figure.3 illustrates the actions performed by an amateur attacker using command line interaction. As shown in the figure.3 attacker uses a set of commands like listing the directories, removing home, root, boot, bin directory and exits from the session.



```
root@JntuK:/# ls
lost+found vmlinuz    srv        sys        run        sbin       proc
mnt        bin        usr        tmp        var        initrd.img etc
opt        boot       selinux    home       media      lib        root
dev
root@JntuK:/# rm -rf home
root@JntuK:/# rm -rf root
root@JntuK:/# rm -rf boot
root@JntuK:/# rm -rf bin
root@JntuK:/# ls
bash: ls: command not found
root@JntuK:/# exit
```

Figure-3Actions performed by an amateur attacker using command line interaction

In another session, an intruder downloaded software from http://www.foofus.net/jmk/tools/medusa-2.0.tar.gz , which is a brute-force tool and try to run it before exiting from session shown in the figure.4.1 and 4.2.Figure.4.2 specifies that the intruder gets a symbolic message when the attacker tries to run the downloaded software.

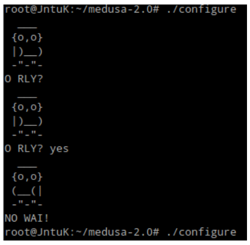


```
root@JntuK:~# wget http://www.foofus.net/jmk/tools/medusa-2.0.tar.gz
--2018-07-17 18:56:48--  http://www.foofus.net/jmk/tools/medusa-2.0.tar.gz
Connecting to www.foofus.net:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 371478 (362K) [application/x-tar]
Saving to: `medusa-2.0.tar.gz

100%[==================================>] 371,478     39K/s/s  eta 0s

2018-07-17 18:56:57 (39 KB/s) - `medusa-2.0.tar.gz' saved [371478/371478]
root@JntuK:~# tar xfvz medusa-2.0.tar.gz
```

Figure-4.1

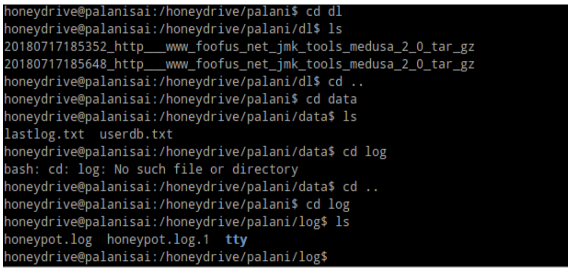


```
root@JntuK:~/medusa-2.0# ./configure
  ___
 {o,o}
 |)__)
 -"-"-
O RLY?
  ___
 {o,o}
 |)__)
 -"-"-
O RLY? yes
  ___
 {o,o}
 (__(|
 -"-"-
NO WAI!
root@JntuK:~/medusa-2.0# ./configure
```

Figure-4.2

Brute-force Attacks

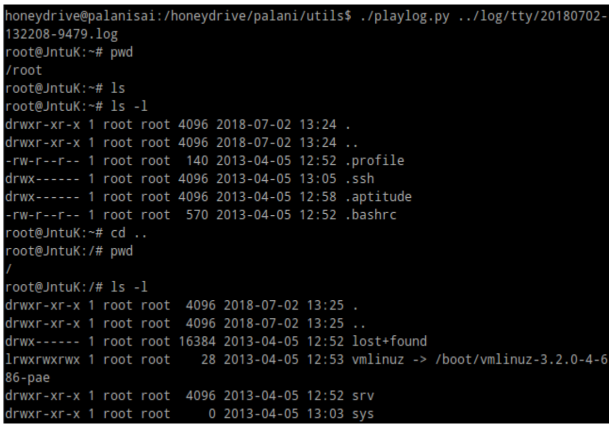
After the performance of attack, security analyst could check the history and details about the performed attacks from the honeypot.Figure-5 shown below shows that files downloaded by an intruder are stored in downloads. It also shows that log files and log data created in their respective directories. By examining these files, security analyst could determine the actions with respective time stamps.



```
honeydrive@palanisai:/honeydrive/palani$ cd dl
honeydrive@palanisai:/honeydrive/palani/dl$ ls
20180717185352_http___www_foofus_net_jmk_tools_medusa_2_0_tar_gz
20180717185648_http___www_foofus_net_jmk_tools_medusa_2_0_tar_gz
honeydrive@palanisai:/honeydrive/palani/dl$ cd ..
honeydrive@palanisai:/honeydrive/palani$ cd data
honeydrive@palanisai:/honeydrive/palani/data$ ls
lastlog.txt  userdb.txt
honeydrive@palanisai:/honeydrive/palani/data$ cd log
bash: cd: log: No such file or directory
honeydrive@palanisai:/honeydrive/palani/data$ cd ..
honeydrive@palanisai:/honeydrive/palani$ cd log
honeydrive@palanisai:/honeydrive/palani/log$ ls
honeypot.log  honeypot.log.1  tty
honeydrive@palanisai:/honeydrive/palani/log$
```

Figure-5 Files downloaded by an intruder

Each activity of the attacker is logged into the honeypot database and python play logs are created which helps the cyber analyst to recollect activity of the intruder sequentially. These play logs replay the actions of the intruder.



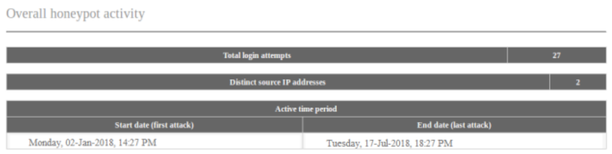
```
honeydrive@palanisai:/honeydrive/palani/utils$ ./playlog.py ../log/tty/20180702-
132208-9479.log
root@JntuK:~# pwd
/root
root@JntuK:~# ls
root@JntuK:~# ls -l
drwxr-xr-x 1 root root 4096 2018-07-02 13:24 .
drwxr-xr-x 1 root root 4096 2018-07-02 13:24 ..
-rw-r--r-- 1 root root  140 2013-04-05 12:52 .profile
drwx------ 1 root root 4096 2013-04-05 13:05 .ssh
drwx------ 1 root root 4096 2013-04-05 12:58 .aptitude
-rw-r--r-- 1 root root  570 2013-04-05 12:52 .bashrc
root@JntuK:~# cd ..
root@JntuK:/# pwd
/
root@JntuK:/# ls -l
drwxr-xr-x 1 root root  4096 2018-07-02 13:25 .
drwxr-xr-x 1 root root  4096 2018-07-02 13:25 ..
drwx------ 1 root root 16384 2013-04-05 12:52 lost+found
lrwxrwxrwx 1 root root    28 2013-04-05 12:53 vmlinuz -> /boot/vmlinuz-3.2.0-4-6
86-pae
drwxr-xr-x 1 root root  4096 2013-04-05 12:52 srv
drwxr-xr-x 1 root root     0 2013-04-05 13:03 sys
```

Figure-6 Reply of the play log filegenerated after the attack

The above figure.6 is the reply of the play log file generated after the attack performed which shows the commands used by the attacker.

## 5. Graph Generated

Visualization of results plays an important part in the purposeful examination of data collected. Visualization helps the security professional to have a detailed overview of the performed operation and enhance astute decision-making capabilities. To present a graphical representation of the data stored in the MySQL database which utilizes a tool written in PHP language called Kippo-Graph. It uses libraries particularly for the purpose of honeypot operations. These libraries are helpful in creating graphs and charts on the activities of operation.



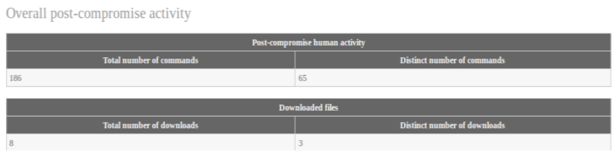
Overall honeypot activity

| Total login attempts | 27 |
|---|---|

| Distinct source IP addresses | 2 |
|---|---|

| Active time period | |
|---|---|
| Start date (first attack) | End date (last attack) |
| Monday, 02-Jan-2018, 14:27 PM | Tuesday, 17-Jul-2018, 18:27 PM |

Figure-7.1 overall honeypot activity



Overall post-compromise activity

| Post-compromise human activity | |
|---|---|
| Total number of commands | Distinct number of commands |
| 186 | 65 |

| Downloaded files | |
|---|---|
| Total number of downloads | Distinct number of downloads |
| 8 | 3 |

Figure-7.2 overall post-compromise activity

Figure.7.1and 7.2 specifies the report on overall honeypot activity and post-compromise activity. From figure7.1, an active time period of honeypot with 27 total login attempts from 2 distinct IP addresses is shown, and figure.7.2 deduces the activity of intruder after compromising the honeypot with 65 unique commands used out of 186 and a total of 8 downloads are made by the intruder with 5 of the same number.

Following, an analysis was performed on username and password combinations. The graph shown below illustrates the Top 10 combinations used by the intruder. From the graph,the username and password combination of root and (123456) is deducted which is a default combination of the honeypot is mostly used.

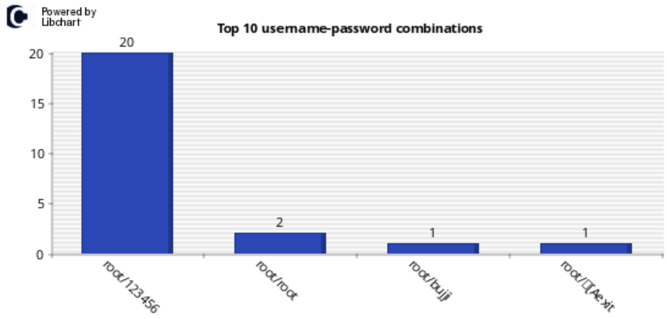
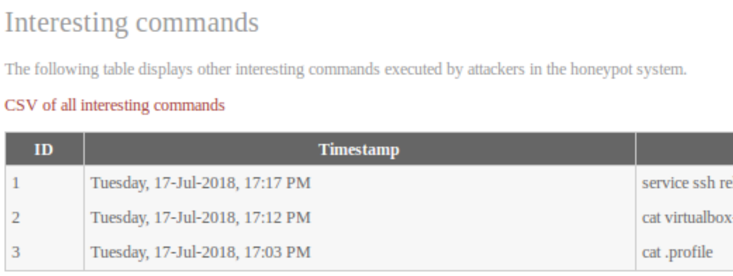


Figure-8 Top 10 username-password combinations

Further, it is noticed that honeypot logs commands that are related to service and system process. The figure-9 below shows the attacker had used some special commands where he tried to reload SSH service and display.profile and Virtual Box settings. Figure-9 also displays the timestamps along with play logs.



Interesting commands

The following table displays other interesting commands executed by attackers in the honeypot system.

CSV of all interesting commands

| ID | Timestamp | |
|---|---|---|
| 1 | Tuesday, 17-Jul-2018, 17:17 PM | service ssh re |
| 2 | Tuesday, 17-Jul-2018, 17:12 PM | cat virtualbox |
| 3 | Tuesday, 17-Jul-2018, 17:03 PM | cat .profile |

Figure-9 Table of interesting commands executed

During the activity, the intruder tries to use multiple commands as inputs. Finally, the analysis was performed on the inputs given by the attackers after compromising the system. Figure-10.1and 10.2

illustrates the commands used by the attackers with ls as most successful and frequent command. From the figures, intruders have given the commands used in changing and listing directories. Removing of root and boot directories along with files has been performed, with root being removed 5 out of 7 attempts. From figures, it is reported that the intruder tries to install and configure some software with./configure command.

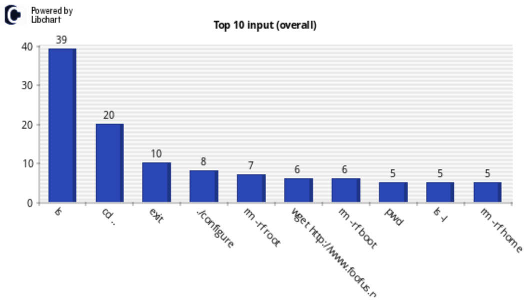


Figure-10.1 Top 10 input (overall)

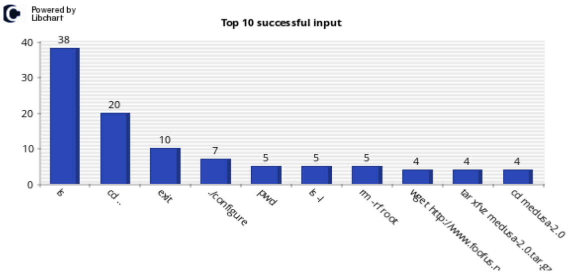


Figure-10.2 Top 10 successful input

## 6. CONCLUSIONS

In this paper, an empirical execution of the Secure Shell honeypot is presented. Many systems run SSH service without appropriate security mechanisms. Absence of protection technologies like firewalls and infrequent updating of system would to the compromise. From our experiment, most of the activities performed on SSH service are brute-force and dictionary attacks, because of inattentive decision in choosing passwords. In this paper, a medium-interaction SSH honeypot is established and accumulated the activity of intruder as results. From the play logs generated, the actions of intruder are replied. Finally, with the use of visualization software a graphical and pictorial representation of certain honeypot is presented in our study. The detailed reports gathered can a give summary of intruder's operations to security investigators.

## REFERENCES

[1]Gokul Kannan Sadasivam, ChittaranjanHota ,” Scalable Honeypot Architecture for Identifying Malicious Network Activities”, International Conference on Emerging Information Technology and Engineering Solutions, 2015.

[2]Abhishek Sharma, "Honeypots In Network Security", International Journal of Technical Research and Applications, 2013.

[3] Know Your Enemy: Passive Honeynets. Honeynet Project.18 January, 2003. http://project.honeynet.org/.

[4]S. A. Budiman, C. Iswahyudi, and M. Sholeh,“Implementasi Intrusion Detection System (IDS) MenggunakanJejaring Sosial Sebagai Media Notifikasi,”in Prosiding Seminar Nasional Aplikasi Sains &Teknologi (SNAST), 2014

[5] Know Your Enemy: Passive Fingerprinting. Honeynet Project.24 May 2000. http://project.honeynet.org/.

[6] Thomas H. Ptacek, Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, 2002. http://secinf.net/info/ids/idspaper/idspaper.html.

[7]Janardhan Reddy Kondra,Sambit Kumar Mishra,Santosh Kumar Mishra,Korra Satya Babu, “Honeypot-Base Intrusion Detection System:A performance Analysis”, 3rd International Conference on

Computing for Sustainable Global Development (INDIACom),2016.

[8]Kippo-Graph [Online] Available: https://bruteforcelab.com/.

[9] J. Owens and J. Matthews, "A Study of Passwords and Methods Used in Brute-Force SSH Attacks." 2008.

[10] "phpMyAdmin." [Online]. Available: http://www.phpmyadmin.net/home_page/index.php.

[11]Zhang Li-juan, "Honeypot-based Defense System Research and Design", IEEE International Conference on Computer Science and Information Technology,2009.