Analysis of Network Intrusion Attacks using Honeypots

N. Ramakrishnaiah
Dept. of Computer Science & Engineering,
University College of Engineering, JNTUK,
Kakinada-533003, A.P., India

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 an intruder is performed on 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 is used and information which is highly sufficient in the identification of the attacker is collected. In this, 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. Visualization tools would further help in the analysis of the activity of the attacker**.**

General Terms
Network Intrusion, Security, Trap.

Keywords
Intrusion detection, SSH, attack, analysis, intrude, honeypot, brute-force.

1. INTRODUCTION
Over the past years, information technology has made a considerable growth in the world. The use of technology in daily life has made data security as a major concern. The stupendous use of computers and internet for information exchange and financial transactions has become a primary approach in modern-day reality. Malicious intruder launches attacks on the specific targets to have the information of a user[1][2]. The reason for these attacks could be financial data or 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 software and mechanisms, the intruder tries to have the credentials required for login. The violator tries to make a move on such service-running server which later will be used for malicious activities such as attack on other systems, malware setup, and modification of root or denial of service. Distinguishing and defining the attacks and recognizing the attackers in real time is a tough job for security providers. Providing policies and developing productive defense strategies play a critical role. To make an impact over the malevolent intruders, security analysts had developed honeypots. Honeypot[3] 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[4][5]. Honeypots do not have the capability to avert an attack but have the expertise 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 defense, 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 by the honeypot is analyzed by using the visualization tool. At the end, the python play logs generated by honeypot are recollected to exact actions of an intruder.

2. THEORITICAL APPROACH
This section deals with two aspects regarding honeypots. One is regarding honeypots based on their interaction extent and another one is about the tools and their functionality generally used in SSH attacks.

2.1 Classification of Honeypots based on Interaction Level
Based on the interaction extent with the attacker, honeypots are distinguished into three categories namely low-level, medium-level 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 known attacks which makes them easily observe the skilled intruder.

The secondary is medium-level interaction honeypot. It offers 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 trap 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 the medium ones, 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 General Tools and Functionality used in SSH attacks

The protocol which commonly used in Linux/Unix operating system is Secure Shell protocol which is 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 the credentials used by the user or usage of brute force attacks.

Dictionary text files are created which consists of combinations of passwords used in performing dictionary attacks, which compares each and every password to give a possible result[6][7]. 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.

Sample command used by hydra to crack SSH password is

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

note.txt contained possible passwords where the root is the original. The above command can be used as a test on SSH service which gave the exact password as the result. Figure 1 shows this.

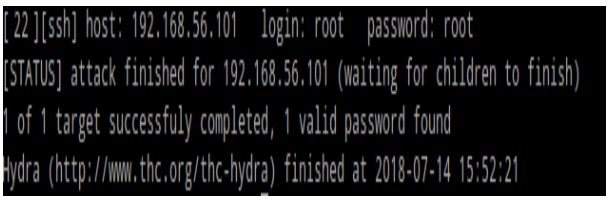

Figure 1: Result of brute-force attack on SSH using Hydra

3. EXPERIMENTAL APPPROACH

This section focuses on the process and establishment of the experiment that covers the procedure and overview behind the setup of the experiment. For the experimental purpose, a virtual system is created using Oracle Virtual Box with Linux server operating system running in it. Xubuntu server operating system which runs as a Virtual Private server is used here. In order to convene an adequate amount of data and evaluate the efficacy, an SSH honeypot is deployed. Using a static IP address, this service is connected to the internet and run the Honeypot. The experimental setup used an open source medium interaction honeypot written in python[8] which allows itself to interact with the intruder. To establish a secure setup, the port number of the SSH service is altered to a free port and bind the honeypot to the default SSH port 22. 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 MySQL server is setup. The honeypot should never run as a root, which could lead to the compromise of the system when honeypot fails. In order to ensure the prevention of access to our other systems, a new user is created and the whole experiment is setup. Using the authbind software, port 22 of SSH is by ported to the honeypot, changed the ownership and gave the permissions to the user where the honeypot in installed. Honeypot generally runs on its default port, this need to be changed in the configuration file while setup. Since authbind is used for by porting so it could use authbind to listen on port 22, a preferable change is made in the start script from *twistd -y honeypot.tac -l log/honeypot.log --pidfile honeypot.pid* to *authbind --deep twistd -y honeypot.tac -l log/honeypot.log --pidfile honeypot.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.

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. Figure 2, depicts it.

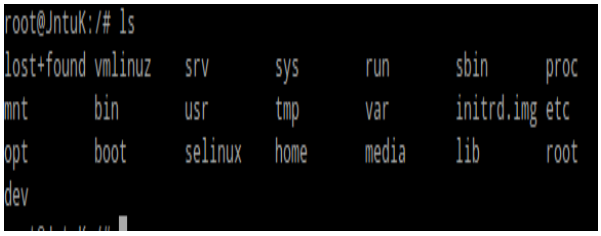

Figure 2: Fake files system by the honeypot

4. RESULTS

This section deals with the activity of the attacker and the summary of the observed brute-force attacks. It also focuses on the outcomes gathered and the visualization of the results[9][10]. It 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, the attacker uses a set of commands like listing the directories, removing home, root, boot, bin directory and exits from the session.

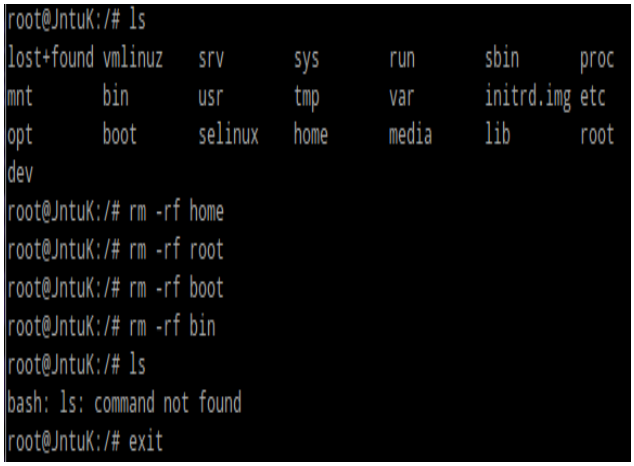

Figure 3: Attacker operations

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 which are shown in Figure 4 and Figure 5. Figure 5 specifies that the intruder gets a symbolic message when the attacker tries to run the downloaded software.

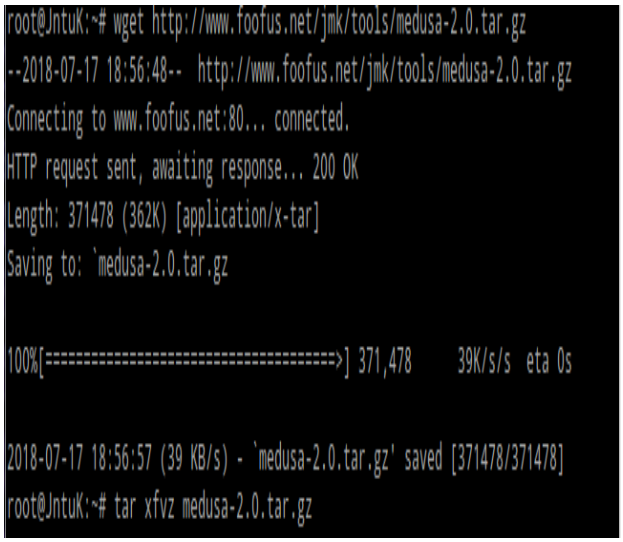

Figure 4: An intruder downloading software

After the attack, security analyst could check the history and details about the performed attacks from the honeypot.

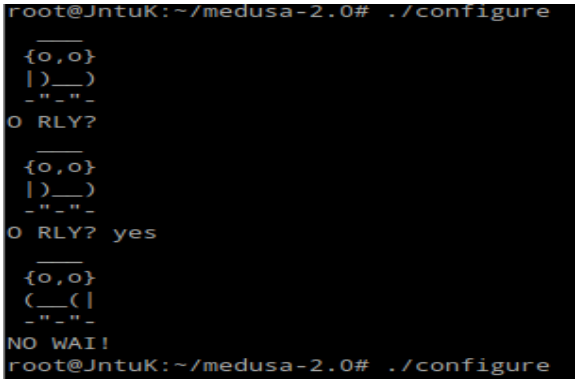

Figure 5: Symbolic message to the intruder

Figure 6 shows the files downloaded by an intruder that is 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.

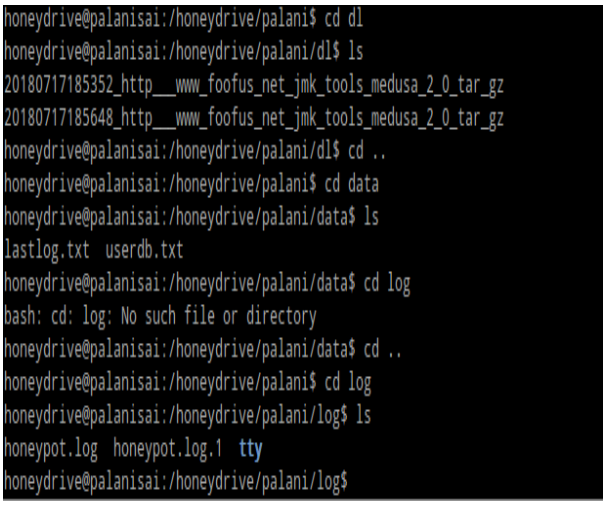

Figure 6: Files downloaded by the intruder and their information

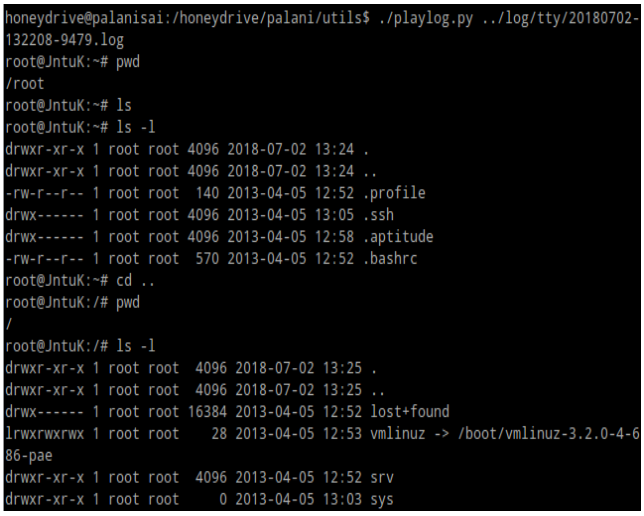

Figure 7: Log file of attacker actions

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.

Figure 7 is the reply of the play log file generated after the attack performed which shows the commands used by the attacker.

To present a graphical representation of the data stored in the MySql database, a tool written in PHP language called Kippo-Graph is used. It uses libraries specifically 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 8: Overall honeypot activity

Figure 8 gives an active time period of honeypot with 27 total login attempts from 2 distinct IP addresses, and Figure 9 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

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 9: Post compromise activity

Further, an analysis was performed on username and password combinations. The graph shown in Figure 10 illustrates the Top 10 combinations used by the intruder. From the graph, it can be deduced that the username and password combination of root and (123456) which is a default combination of the honeypot is mostly used. Further, it is noticed that honeypot logs are having commands that are related to service and system process.

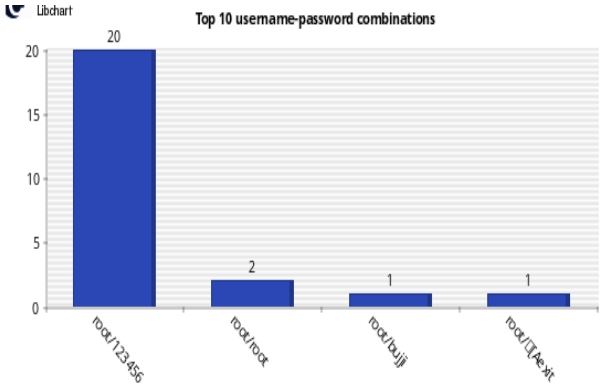

Figure 10: Graph analyzing username-password combinations

Figure 11 shows that the attacker had used some special commands where he tried to reload SSH service and tried to display profile and Virtual Box settings. It also displays the timestamps along with play logs. During the activity, the intruder tries to use multiple commands as inputs.

CSV of all interesting commands

ID	Timestamp	Input	Play Log
1	Tuesday, 17-Jul-2018, 17:17 PM	service ssh reload	Play
2	Tuesday, 17-Jul-2018, 17:12 PM	cat virtualbox-guest-4.1.18	Play
3	Tuesday, 17-Jul-2018, 17:03 PM	cat .profile	Play

Figure 11: Special commands executed by attacker

Finally, the analysis was performed on the inputs given by the attacker after compromising the system. Figure 12 and Figure 13 illustrate the commands used by the attackers with ls as most frequent and successful command.

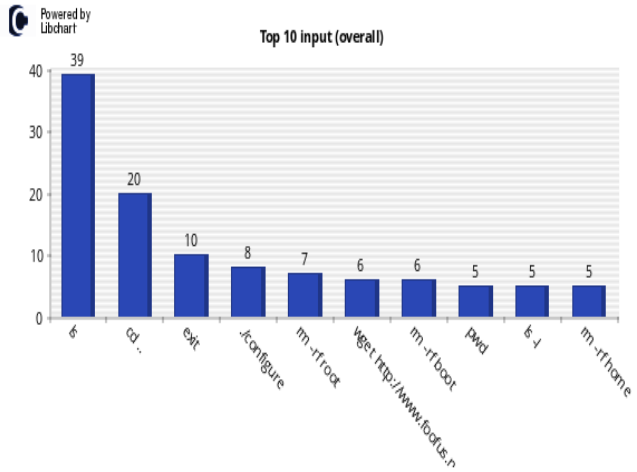

Figure 12: Graph showing the frequency of commands used by the attackers

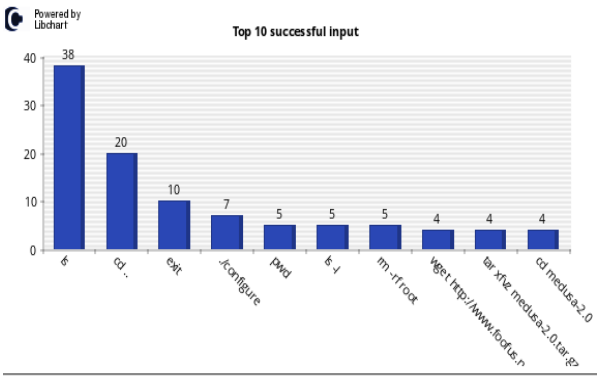

Figure 13: Graph showing most successful commands by the attackers

5. CONCLUSION

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 the proposed experiment, most of the activities performed on SSH service are brute-force and dictionary attacks, because of inattentive decision in choosing passwords. 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 identtifid. Finally, with the use of visualization software the graphical and pictorial representation of certain honeypot are presented.

6. REFERENCES

[1] S. A. Budiman, C. Iswahyudi, and M. Sholeh, 2014, "Implementasi Intrusion Detection System (IDS) Menggunakan Jejaring Sosial Sebagai Media Notifikasi,"in *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST).*

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

[3] Gokul Kannan Sadasivam, Chittaranjan Hota, 2015, " Scalable Honeypot Architecture for Identifying Malicious Network Activities", International Conference on Emerging Information Technology and Engineering Solutions.

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

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

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

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

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

[9] Janardhan Reddy Kondra, Sambit Kumar Mishra, Santosh Kumar Mishra, Korra Satya Babu, 2016, "Honeypot-Base Intrusion Detection System:A performance Analysis", 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

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