Analysis of SSH attacks of Darknet using Honeypots

Shaik Bhanu[1], Girish Khilari[2], Varun Kumar[3]
[1]Computer Science, Veltech University (CDAC), Pune, India
[2]IT Network & Systems, CDAC, Pune, India
[3]Computer Science, Veltech University, Chennai, India.

***Abstract* - A Darknet is a private network and the connections are made only between trusted friends. In the field of computer security, honeypot is an internet attached server that acts as a decoy, to trap the hackers in order to study their activities and monitor how they are able to break into a system. In this paper we present the results of SSH honeypot operations in which it undertook the web trap of attackers who target SSH service in order to gain illegal services. A medium interaction honeypot offers a high interaction level to the attacker and when a connection attempt is made to system port, the honeypot can reply back with specially crafted packets that emulate of a real network services. The fake system has remained online and fully operational, capturing attacks and logging all malicious activity. Lastly we collect the data and analyzed the information.**

***Index Terms* - honeypot systems; ssh; security Analysis**

I. INTRODUCTION

In the context of more challenging world of internet security, one thing is not changed is some malware for Linux systems. Even recently many studies show that there have been several intentions to create malware that makes Linux operating systems, but brute force attacks is most common way of penetrating such systems [1]. Attackers are searching the internet for servers that can be used for their malicious activity. One of the most prominent target is servers on which the administrator has set up a remote access service (SSH).

When an attacker finds such a server that runs the particular service, the attacker will try to connect it by using various combinations of authentication credentials, if login attempt is successful then the attacker gains remote access to the server and then uses it for malicious activity. Many definitions for honeypot exists but one of the definition is most accurately belongs to Lance Spitzner who defines a honeypot as information system resource whose values lies in unauthorized or illicit use of resource [2].

A honeypot is a computer system with no production value. There is no legitimate user to use it directly and if any communication attempt is done with the system it is automatically considered malicious and it is classified as follows: detection, attack or network scanning [3]. Honeypots are both deceit tools and traps. It cannot prevent cyber attacks against the network but helps in identifying and detecting them when used with other defense-oriented tools such as firewalls. Honeypots often generate a small amount of data of high value, but depending upon the circumstances the analysis of this dataset can be more problematic for information security professionals [4]. As the number of attacks grows very large over time, it becomes impossible to analyse the each and every captured session [5].

So, we focus on SSH brute-force and dictionary attacks. We analyse data collected from a large number of SSH attacks against a Virtual Private Server (VPS) which was set up as a honeypot to log all malicious activity [6].Our goal was to build a profile of short-term behavior of attacker by capturing all the activities in minutes and hours after the attacker was trapped.

II. HONEYPOT SYSTEMS

A honeypot is a computer system on the internet that is set up to attract and trap people who attempt to penetrate other people computer systems.

Classification:

The honeypot systems can be classified according to their level of interaction as:-

- Low- interaction honeypot: It provides emulated services and no operating to access. Information is limited to transactional information and attacker activities.
- Medium-interaction honeypot: It specifies specific services but with certain level of access to the underlying operating system.
- High-interaction honeypot: It exposes fully operating system in which it offers fully compromising activities.

An easy way to comply with the paper formatting requirements is to use this document as a template and simply type your text into it.

III. SSH HONEYPOT

SSH are an encrypted remote connection mechanism, commonly used in Linux and UNIX based operating system. It provides a secure data communication over a insecure network. The protocol was defined by Ylonen and Lonvick in Internet Engineering Task Force’s RFC4254 and allows users to authenticate to remote machines gaining access to a secure shell. By default, SSH uses port 22 and it implements a username and password authentication and also we have secure methods like public key authentication. Due to this attacks against SSH protocol is quite common. The SSH protocol is open and well-defined and software libraries exist allowing the creation of SSH client.

A. Experimental setup:

First we deploy a SSH honeypot using a VPS. It was connected to internet using a static IP address and software for web trap. So, we use Kippo SSH honeypot in which the software is written Python programming language. Kippo is a medium interaction honeypot in which it allows interaction with attacker and binds to SSH default TCP port22 and log each connection attempt with server.

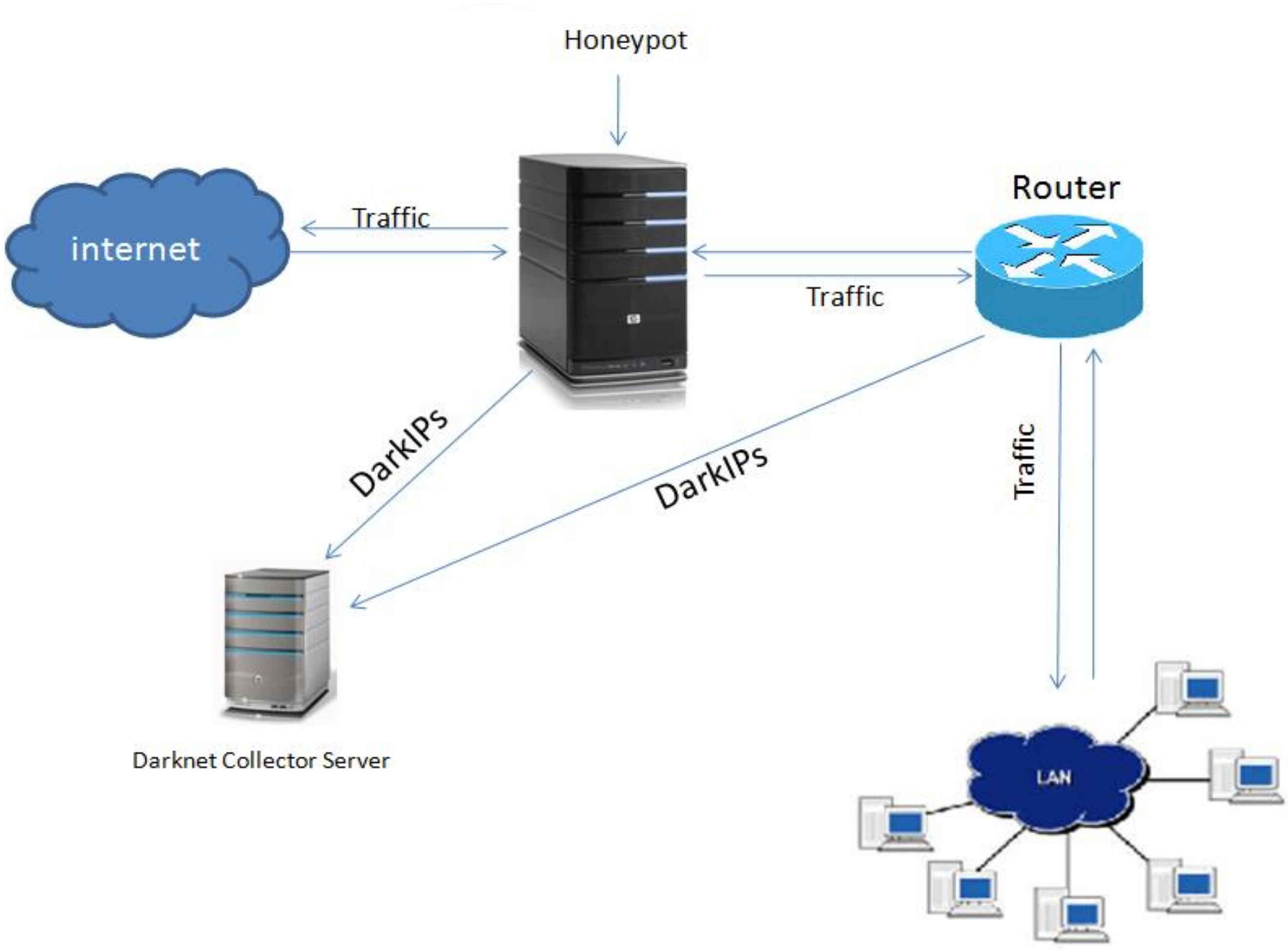
To monitor attacker activity, the following tools: an openSSH server to collect attempted passwords, syslogging to remotely log important system events, logins and password changes. Sebek tool is used to collect secretly all keystrokes on incoming SSH connections. Only single line of code is added to openSSH to record all passwords being tried.

A honeypot had one original root account and five non-privileged user accounts. We use common usernames: admin, root, user, bin, guest and passwords were ‘123456’, ‘toor’, ‘password’,’ user’, ‘0000’ . We use these five passwords for each username. We encourage attackers to enter the non-privileged user accounts instead of the root account.

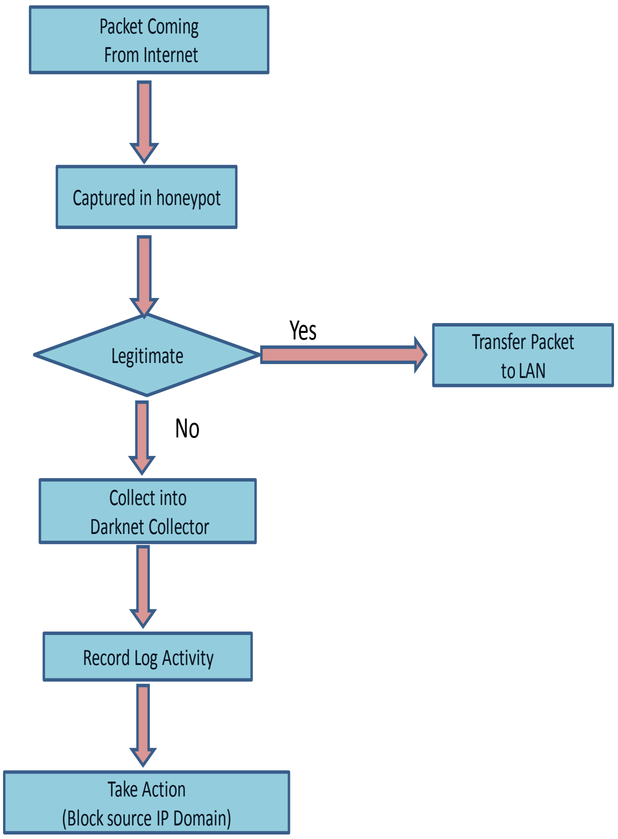
TABLE: ATTACKERS STATISTICS IN SSH ATTACKS

Username	Password	Attempted
admin	123456	210
root	toor	156
user	password	93
bin	user	62
guest	0000	35

B.BLOCK DIAGRAM



C.FLOWCHART


Packet Coming From Internet
Captured in honeypot
Legitimate
Yes
Transfer Packet to LAN
No
Collect into Darknet Collector
Record Log Activity
Take Action (Block source IP Domain)

D. RELATED WORKS

In recent years, large number of studies of SSH attacks have been carried out and it mostly included in the hacker activities after they gained illegal system access. In our scope also we have included post-compromising activities [6]. Regarding the visualization of attacks on networks, a lot of research has been done, but it is mostly focus on visualizing NetFlow data coming from attacks logged by IDS [7].

In 2008, the tool NFlowVis in which it is used to visually analyze large scale networks using NetFlow data from IDS attack logs[8]. In 2009, the tool VIAssist was created, which can provide details of specified network. However, VIAssist has no valuable practical use for the analysis of SSH attacks since it only visualizes NetFlow data [9]. Focusing more on visualizing malicious activities using honeypots a visualization tool name Carniwwwhore and it is developed for the Dionaea malware honeypot. Dionaea is successor of Nepenthes honeypot and Carniwwwhore tool has similar capabilities in comparison to our tool that was developed during this course of work [10]. Authors performed detailed analysis of post-compromising attacks behaviour and the analysis is done for long term duration.

IV. CONCLUSION

We built a profile of attacker behavior and collecting the important data on attempted usernames and passwords. Most of our results are surprisingly very low percentage of successful attacks even with common passwords. Downloading, installing and running the software is the most common way to have a successful attack. The analysis of the data is done in a less time in which after the attacker is trapped by our honeypot.

V. ACKNOWLEDGEMENT

The first author would like to thank Chakravarthy and Vaishali Maheshkar for their valuable comments and help.

REFERENCES

[1] L.Spitzner," Honeypots: Catching the Insider threat", in 19th Annual Computer Security Applications conference 2003.
[2] L.Spitzner, Honeypots: Tracking Hackers.Boston Addison Wesley,2003.
[3] L.Spitzner, Honeypots: Strategies & issues in network magazine,2003.
[4] C.Seifert,"malicious SSH login attempts",Security Focus, Infocus 1876,2006.
[5] "Kippo honeypot: https://code.google.com/p/kippo/.
[6] http://www.honeynet.org/tools/sebek/.
[7] Robin Berthier, center for risk and Reliability, University of Maryland, college park, IEEE 2013
[8] Team cymru- The Darknet project"[online].
[9] Honeypots & spams- A obied in 2007.