ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Web Application Honeypot

Ashwini Pawar[1]
B.E.I.T
Department of Information Technology
Cummins College of Engineering
Pune – India

Kimaya Siddhabhati[2]
B.E.I.T
Department of Information Technology
Cummins College of Engineering
Pune – India

Sadhana Bhise[3]
B.E.I.T
Department of Information Technology
Cummins College of Engineering
Pune – India

Snehal Tamhane[4]
B.E.I.T
Department of Information Technology
Cummins College of Engineering
Pune – India

Abstract: Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods is the use of honeypots. A honeypot is a information system resource whose value lies in unauthorized or illicit use of that resource. Our honeypot captures attacks on the web applications layer. It is a low-interaction honeypot which emulates the HTTP and Telnet service of any system. The HTTP service helps to blacklist malicious IP Addresses and the Telnet Service helps on trace, log, analyze and observe attacks on the Login system of any organization. It is said sometimes that the next world war will not be through weapons but through virtual attacks by hackers from the blackhat community. So it is necessary to get more information of the blackhat community to trace their methods and improve our security systems accordingly. Our honeypot is a small step forward in this area.

Keywords: Honeypot, Malicious IP, HTTP Service, Telnet Service, Intrusion Detection System, Network Security.

I. INTRODUCTION

Lance Spitzner, key member of a research group in the United States called Project Honeynet, defines the term honeypot as follows: “A honeypot is a resource whose value is in being attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information.” A honeypot is a resource, which pretends to be a real target. The main goals are the distraction of an attacker and the gain of information about an attack and the attacker. Honeypots do not help directly in increasing a computer network’s security. On the contrary, they do attract intruders and can therefore attract some interest from the blackhat community on the network, where the honeypot is located. An Intrusion Detection System (IDS) plays an important part in nearly every honeypot, and especially in honeynets, as it is an essential component in gathering information.

There are two categories of honeypots – production honeypots and research honeypots. A production honeypot is used to help mitigate risk in an organization while the second category, research, is meant to gather as much information as possible. These honeypots do not add any security value to an organization, but they can help to understand the blackhat community and their attacks as well as to build some better defenses against security threats.

The way honeypot can be used to add security to an organization’s critical assets is as follows: A honeypot is a resource, which is intended to get compromised. Every traffic from and to a honeypot is suspicious because no productive systems are located on this resource. In general, every traffic from and to a honeypot is unauthorized activity. All data collected by a honeypot is therefore interesting data. A honeypot will in general not produce an awful lot of logs because no productive systems are running on that machine. Analyzing this data should get much easier by these simple facts. Data collected by a honeypot is of high value and can lead to a better understanding and knowledge, which in turn can help to increase overall network security.

II. Literature Review

Although the concept of a honeypot system is not new, the availability of commercial honeypot systems is new. Commercial grade honeypots are relatively new. Freeware honeypots have been used for some time but in a business situation commercial products dominate. Although commercial honeypots are simpler than building a specialized honeypot from scratch using open source freeware, they do not eliminate the need for expertise in monitoring. For example, commercial honeypots send alerts an operator an event has occurred, however, a skilled analyst with attack knowledge is needed to correlate supporting data (packet traces, firewall intrusion detection logs) to analyze, identify, and contain the attack. There are two primary types of honeypots:

(1) Hardware-based servers, switches, or routers that have been partially disabled and made attractive with commonly known configurations

(2) Software simulation honeypots which are deception programs that emulate system software (OS) and services.

Accordingly, some of the popular honeypots today are:

1. Backofficer Friendly (BOF)

BOF is developed by Marcus Ranum. It is a lightweight honeypot and free to distribute. BOF emulates several common services such as http, ftp, telnet, mail and Backoffice. BOF logs, alerts and responses a fake reply whenever someone connects to such ports. BOF user can have clear view of the attacking process.

2. Specter

Specter is a commercial production honeypot whose value lies in detection. Spector can simulate 13 different operating systems in application level including Windows, Linux, Aix, Solaris, MacOS etc. It’s a windows based software which offers 14 different network services and traps. The other character is actively gathering attackers information such as Whois and DNS lookup. Specter is a low interactive honeypot which fakes the reply of attacker’s request. Attacker can’t utilize the application to interact with the OS.

3. Honeyd

Created by Niels Provos, Honeyd is an powerful production honeypot, which can be used for attacks detection and reaction. It represents today’s level of production honeypot in many fields. First, it can emulate over 400 kinds of OS at IP stack level. This hides the guest OS before attacker. Second, emulating hundreds of computers at a single machine by use of *Arp* spoofing. Third, Honeyd is Open Source honeypot system. Honeyd still uses the simulated service reply to attacker’s request, but administrator can customize the reply script to provide attacker more flexibility.

4. Honeynet

Honeynet represents the highest level of research honeypot. It can also be modified to production honeypot for attacks detection and reaction. New methods of data capture and data control proposed by Honeynet project show greater flexibility and higher access control ability, which can he applied both research honeypot and research honeypot.

III. Proposed System

a. System Architecture

The system architecture vaguely shows how any honeypot is placed in the network environment. The internet is the public network which contains users of the organization's network that we want to protect. These users can be normal users who use the system in a legitimate way and it also has users who want to attack the system or bring the system down. The network then has a 2-port router that sits on the edge of the network and also acts as a firewall through the Access Control List. The router directs the traffic to the 24-port switch. The switch is generally used here to different between the different virtual LANs inside the organizations network. The switch enables the entire traffic to pass through the honeypot first rather the to the organization's production network. The honeypot logs all the data and then passes the traffic to the organization's production (main) network. In this way we can trace the attacker's activities first. Since honeypot is a completely defensive system, we need the attacker to take the initiate. So, in a perfectly safe network the honeypot may see no malicious logs. But whenever it captures the data, this data would be useful to track the attacker's method to attack the network.

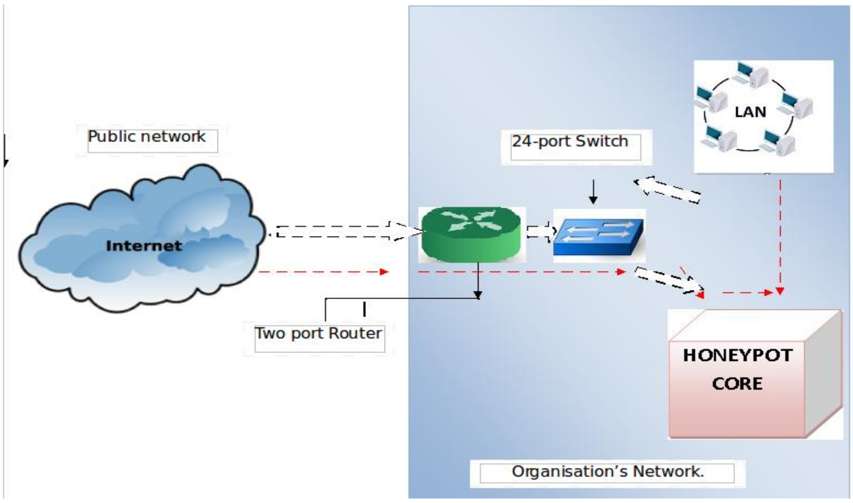


Figure 1: System Architecture

b. Honeypot Architecture

In the system architecture we saw how the honeypot is placed in any network. The diagram above shows what our honeypot consists of. Our honeypot falls under the category of low-interaction research honeypot. It emulates the HTTP and Telnet service. The function of each component in the honeypot architecture is as follows:

1. All traffic entering the network first reaches the honeypot core. The honeypot core redirects the incoming traffic according to its type i.e. HTTP or Telnet.
2. The Graphical User Interface (GUI) is for the administrator to go through the data collected by the honeypot. It displays the logs, allows the admin to control the servers, enables the admin to get more information about any specific IP, etc. It also displays various statistics related to the gathered data.
3. The WinSock is the interface between the honeypot core and the GUI. It is required in the event where we need number of instances of the UI for remote administration.
4. The HTTP server is where the incoming data that can be IP, TCP, UCP or ICMP headers. These headers and their related data is stored or logged onto the honeypot core.
5. The Telnet server is where the username and password authentication system resists on the network. Every activity regarding this is logged onto the telnet server.

6. If the honeypot captures any malicious IP then it may create a blacklist of malicious IPs so that we can prevent them from attacking the production network.

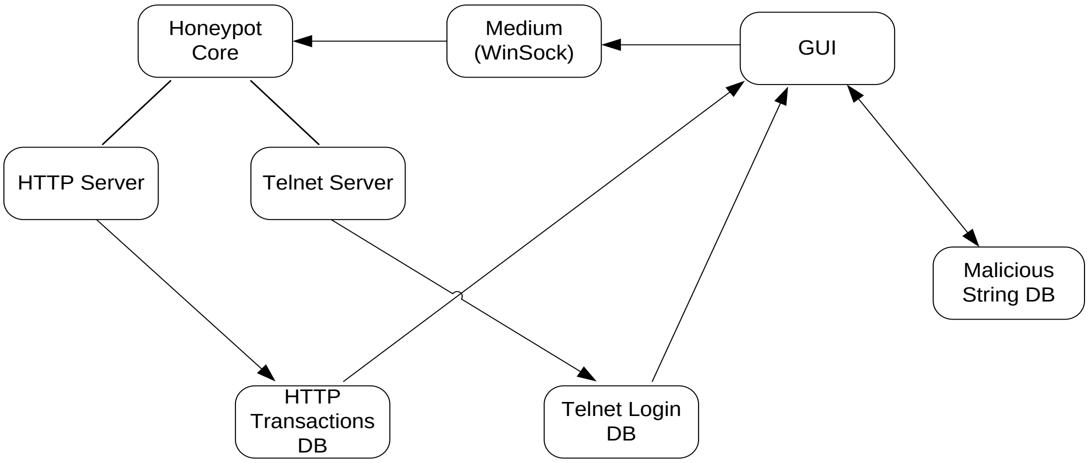


Figure 2.1: Honeypot Architecture

IV. HOW THE SYSTEM WORKS

a) The system first presents the login screen to the any user. If the user is an admin, he has the total administrative control over the system such as control the server, view the logs and statistics, etc. If anyone other than the admin uses this telnet service his activity is logged onto the server.

b) On the other hand all the traffic entering the network in the form of TCP, IP, UDP or ICMP form and their details including their payloads in logged onto the server.

c) The administrator first enables the two servers by starting them on. Then the processing of the logged data can be done.

d) The Traffic captured through the HTTP service is processed as follows:

The logs containing the malicious IPs are displayed along within their cause, number of hits on the database and date of first and last hit. To categorize any IP as malicious we have written some filters. These filters are like IP packets with version number other than 4/6, unusal source or destination address, reserved ips entering the network, illegal combination of TCP flags in the TCP header or illegal contents in the UDP and ICMP headers. The attackers generally used specially crafted packets with these illegal settings. Any IP that gets trapped into these filters is termed as malicious.

e) Then the admin may click on any malicious IP to get more information about it. This enables the IP Address Inspector screen to be opened. This contains the following contents:

1. The overview about the IP: It has the IP address and its URL listed. We have also tracked the IP using the GeoLocation service. So it also displays the Country, State and City of the IP along with its longitude and latitude. We also have a facility to track the IP though Google maps here.

2. The Settings service: It shows he User Agent, Connection and Host settings like browser, Operating System, etc.

3. The LOOKUP IP service: These enables the admin to lookup the IP and get more information about it like check in various blacklists worldwide, look over its reputation, etc. For this we provide 6 options namely domaintools.org, cisco's senderbase.org, spamhaus.com, spamcom.net, Google groups and Google itself.

4. Traceroute: This facility shows the hops required to reach the malicious IP from the source that is it traces the route from source to destination.

f) In the sameway the admin can look up the telnet logs consisting of the information like username, password, session time in, session time out, IP address used, etc.

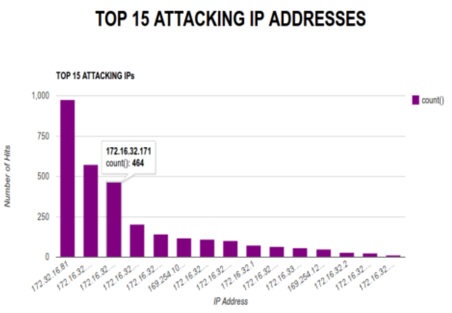
g) Then we present different the statistics to the admin on the basis of the gathered data. This graphical and statistical views may help him to take decision or devise methods to improve the current security system. Some of the reports are as displayed in the results and analysis section below. Please refer to it.

V. RESULT AND ANALYSIS

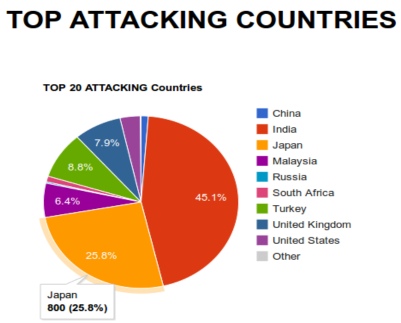
The result and analysis section of our honeypot is divided into two important parts: HTTP reports and Telnet reports.

The HTTP reports contain: Top 15 Attacking IP according to the number of hits on the database, Top attacking countries whose data is gathered according to the location tracked in the IP address inspector, Area charts that show how much of data is processed by the http service daily and the other chart shows how much of it is actually malicious, pie-chart showing the preferred browsers by the attackers and the pie-chart showing prefferd OS by the attackers.

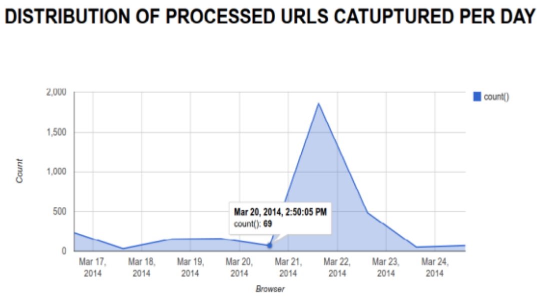
The Telnet report shows 5 reports: Username distribution that shows which usernames are generally used by users, password length analysis which generally shows that 5-8 is the most preferred password lengths, worst password report which compares the passwords in our databases to a 10,000 password file which contains worst passwords gathered all around the world by passwordresearch.net and a report showing the probable brute force attacks on the network. Some of the examples for these reports can be seen below:



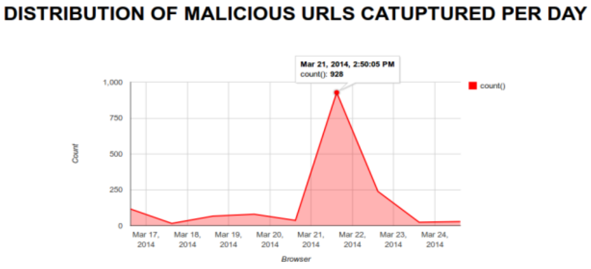
Top 15 Attacking Addresses



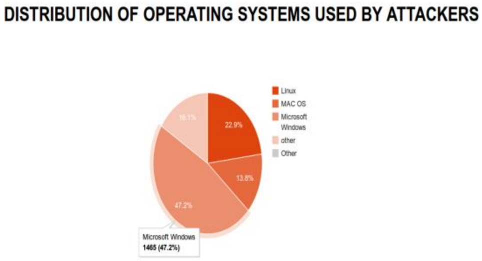
Top Attacking Countries



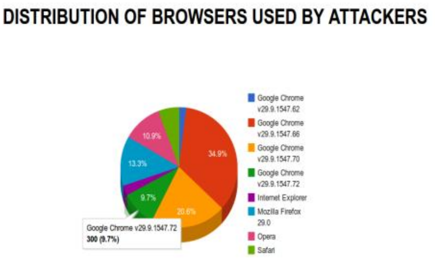
Distribution of Processed URL'S



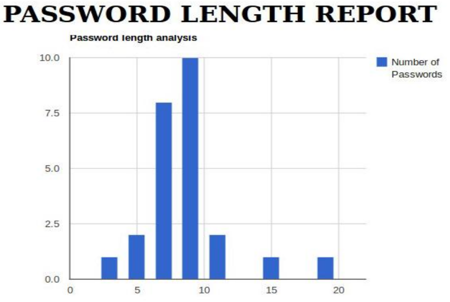
Distribution of Processed URL's

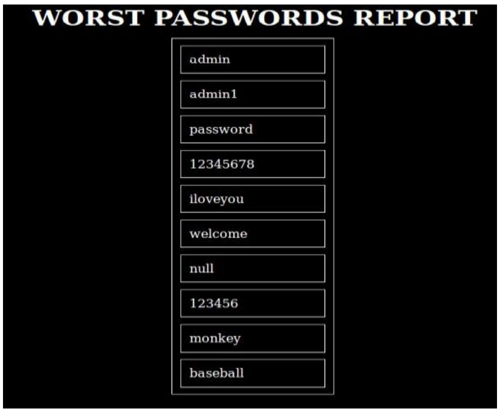


Distribution of Operating Systems used



Distribution of Browsers Used By Attacker

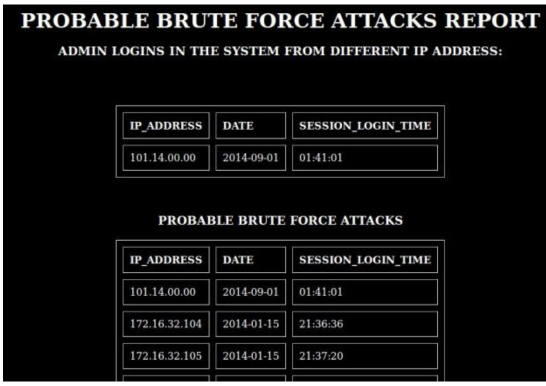




WORST PASSWORDS REPORT

admin
admin1
password
12345678
iloveyou
welcome
null
123456
monkey
baseball

Worst Password Report



PROBABLE BRUTE FORCE ATTACKS REPORT

ADMIN LOGINS IN THE SYSTEM FROM DIFFERENT IP ADDRESS:

IP_ADDRESS	DATE	SESSION_LOGIN_TIME
101.14.00.00	2014-09-01	01:41:01

PROBABLE BRUTE FORCE ATTACKS

IP_ADDRESS	DATE	SESSION_LOGIN_TIME
101.14.00.00	2014-09-01	01:41:01
172.16.32.104	2014-01-15	21:36:36
172.16.32.105	2014-01-15	21:37:20

VI. Implications

1. Research Honeypot help us in three ways that is prevention, detection and how we react to an attack.
2. New information gathered from the honeypot can be used by security organisations to design new security system and update their Intrusion Detection Systems.
3. Government organisations if use a honeypot can find out who is attacking them and how. This data can be critical in terms of the country's security.
4. More examinations can be obtained by looking at the type of the malicious behaviours. It can help to understand more attacks that may happen.
5. For the only malicious traffic, there is no need for huge data storage. There is no need for new technology to maintain. Any computer can be used as a honeypot system. Thus, it does not cost additional budget to create such a system.
6. Honeypots divert exploits away from the main production system. This help to first log the information then move towards the actual network so that every activity can be traced.
7. Because they are non-production systems, they allow you to experiment in a (relatively) safe environment. It allows trying out counter exploits with greater freedom.

VII. Conclusion

A. Concluding Remarks

Honeypots can be a valuable addition to a security system. They serve the community through their ability to collect and record information on blackhat activities. A Honeypot's strength is its ability to divert an attacker from the main production system. Once diverted, the attack can be studied and a countermeasure can be developed. The data gathered through the different logs from our HTTP service can help any organization to create or update their Blacklist for IP Addresses that are malicious so as not to allow then from reaching the production systems. The Telnet service will help the administrator to detect attacks on the login system and have an analysis of the usernames and passwords in the system. This information can help him to protect the most common form of authentication required by any user to enter into the system. As we are working to improve and update our network security through systems like the honeypot, the Bad guys are also devising methods to break, bypass or detect them. So we need to constantly be alert and working in this area to protect our data.

B. Future Work

Honeypots are a huge field for research in the network security domain. So the future scope is very wide. Every organization can improvise and customize upon the honeypot that they use. Our honeypot emulates the HTTP and Telnet Service. Likewise, this honeypot can be extended to emulate even the FTP, SMTP, etc services too. Also the honeypots need a administrator to configure themselves into the network. So dynamic honeypots that adjust quickly by themselves can be developed.

References

1. Anandamoy Roychowdhary, Dhanashree Bahirat, Prof. Rajesh Ingle, Shirish Doshi, Sujata Yeldi, Sweta Gupta, Tanmay Ganacharya 0-7803-765, 2003,Enhancing Network Intrusion Detection System .With Honeypot.
2. Hassan Artail ,Iyad Kuwatly, Malek Sraj and Zaid AI Masri 0-7803-8577-2/04 , 2004 A Dynamic Honeypot Design for Intrusion Detection.
3. Azman Samsudin, Chuah Wee Heong, Rahmat Budiarto, Salah Noori, 0-7803-8482-U04 ,2004 , Honeypots: Why We Need A Dynamics Honeypots.
4. Brian Scottberg, David Doss, ,William Yurcik, 0-7803-7824-0/02 ,2002, Internet Honeypots: Protection or Entrapment.

AUTHOR(S) PROFILE

Miss. Ashwini Pawar currently pursuing her B.E degree in Information Technology from Cummins College of Engineering, Pune (University of Pune). Also received the Diploma in Computer Engineering from B.V.J.N.I.O.T. (MSBTE) in 2011.

Miss. Kimaya Siddhabhatti currently pursuing her B.E degree in Information Technology from Cummins College of Engineering, Pune (University of Pune). Also received the Diploma in Computer Engineering from B.V.J.N.I.O.T. (MSBTE) in 2011.

Miss. Sadhana Bhise currently pursuing her B.E degree in Information Technology from Cummins College of Engineering, Pune (University of Pune). Also received the Diploma in Computer Engineering from B.V.J.N.I.O.T. (MSBTE) in 2011.

Miss. Snehal Tamhane currently pursuing her B.E degree in Information Technology from Cummins College of Engineering, Pune (University of Pune). Also received the Diploma in Computer Engineering from B.V.J.N.I.O.T. (MSBTE) in 2011.