The Design of Website Security Defense System Based on Honeypot Technology

Jun Yao[1, a], Jing Chen[2, b]

[1]Communication and Information System, Xi'an University of Science and Technology, Xi'an, 710054, China

[2]Communication and Information System, Xi'an University of Science and Technology, Xi'an, 710054, China

[a]email: 542339854@qq.com, [b]email:184649260@qq.com

Keywords: Honeypot; Log; Virtual Machine; Network Security

Abstract. With the rapid development of Internet, network security has become increasingly important, the existing network security technologies are all passive defense, which has its inherent disadvantages. In summary, to defense the constantly updated network attacks technology, the emergence of active defense system is inevitable. The honeypot technology which belongs to active defense technology has introduced spoofing technology of the traditional means of attack into the field of security and defense. The honeypot deals with network security issues from a new direction. Combining honeypot technology and the site security, this paper simulated a small, low-interaction honeypot for securing information of website.

Introduction

With the rapid development of internet, network interconnection, information sharing has increasingly become a reality. For various types of network attacks growing with each passing day, network security has been confronted with unprecedented challenges, so network security has become an urgent problem to be solved as internet continues to expand the scope and depth. Faced with a variety of network security problems such endless, traditional network security technology has been unable to meet the demand because of their own vulnerabilities, firewall's flaw is that date transfer is not passed by it can not be tested, but also can not prevent security threats caused by improper policy configuration or configuration errors; IDS(Intrusion Detection System) affected by its properties, can only monitor passively[1]. Honeypot technology as a new network security technology and its unique active defense can quickly be valued by us. Honeypot technology is a security technology based on the proactive security policy, which can master hackers' attack techniques and tools in order to take proactive defensive measures to protect information systems, finally realized the real-time, efficient and independent network security.Honeypot technology combining with traditional network security technologies can build a new active local area network security defense system, simultaneously form a new site safety management system.

Honeypot Technology

Honeypot is a security resource whose value is being scanned, attacked or captured[2]. Through this defining we can understand that, build a honeypot system's aim is to let unauthorized users to detect and attack it. Honeypot itself does not fix any problems, it only provides additional, valuable information for us, and will not provide real valuable service to the outside world. What's more, all attempts to access the honeypot is considered suspicious because of any attempt behavior which would connect honeypot can be considered a potential attacks, and the core value of the honeypot is to monitor, detect and analyze these attacks. Honeypot will not directly improve computer network security, but as an active defense technology it can not be replaced by other security strategy.

According to the degree of interaction honeypot can be divided into low-interaction, medium-interaction and high-interaction honeypots. Below for the three different kinds of interactive honeypot from complexity, operating system, risk, information gathering and configuration maintained several aspects were compared, as shown in the table 1[3].

Table 1. low medium and high interaction honeypot comparison

Performance	Low-interaction Honeypot	Medium-interaction Honeypot	High-interaction Honeypot
Complexity	Low	Medium	High
Provide real OS	No	No	Yes
Risk	Low	Medium	High
Information Gathering	Link	Request	All
possible system is compromised	No	No	Yes
apply required knowledge	Less	Less	More
knowledge for develop	Low	Medium	High
to maintain the time it takes	Less	Less	Very much

From analysis of the table can be seen, honeypot technology's disadvantages are higher degree of the interaction system, the higher risk it existent, what's more, if it compromised the result in loss will be bigger and bigger.

Design of the honeypot system

The design is divided into two parts, the first is the ides of the design, the second is the realization of the system.

The first part, the ideas of the design is as fellows:

Construct honeypot aim is to use the surface of the loopholes to attract hackers' intrusions and recorded it, according to records analysis understanding the motivation and subsequent behavior, which takes into account the main security problems is must guarantee honeypot itself is not was found and compromised and controlled to attack another host by hackers. Designing the simulation of general network services is to achieve this purpose, which using general network services to give the appropriate deceptive response to these interactive attackers and can also monitor the behavior of the intruders. The method described above can not only achieve the purpose of obtaining information on the intruder, but also effectively protect the security of the real system.

This design mainly completes the design and implementation of a low interaction honeypot system, that is, under the specific operating system to simulate common network services, such as basic website system development and get access. The main function of the system is to response the attacker's connection request; process system commands sent by the attacker and give response with false information; record all activities when an attacker log into the system; then according to the information recording to analyze the safety degree of the attacker[4].

The input of the system comes from the data sent by the attacker through the network connection; the output of the system includes the response information of the data sent by the attacker and the log file of the attacker's activity.

The concrete realization of the design is to complete a website system and make a virtual system be identical with the previous one which deployed on the current host. Secondly, using another PC on the LAN to attack this website remotely and get logs. Finally, to analyze with the existing log files: if normal access, the site is imported on the host; if not normal visit, be imported on the virtual systems, and to anti-tracking this non-normal visitor.

The second part, the realization of the system is as fellows:

The premise of the design is to build an issue environment. Firstly establish VMware on windows operating system and then install the Windows operating system on VMware, Secondly use web application development technology to built a simulation with virtual interactive website. Finally, by automatically reading and processing the analog website log files, and finally to judge the visitors of the interactive platform of website whether security or not. With realistic camouflage, data acquisition, data analysis, and intrusion redirection technology are used in this design, the purpose of intruder redirection between virtual and real system had come true. Flowchart in Figure 1 below for the system implementation[5].

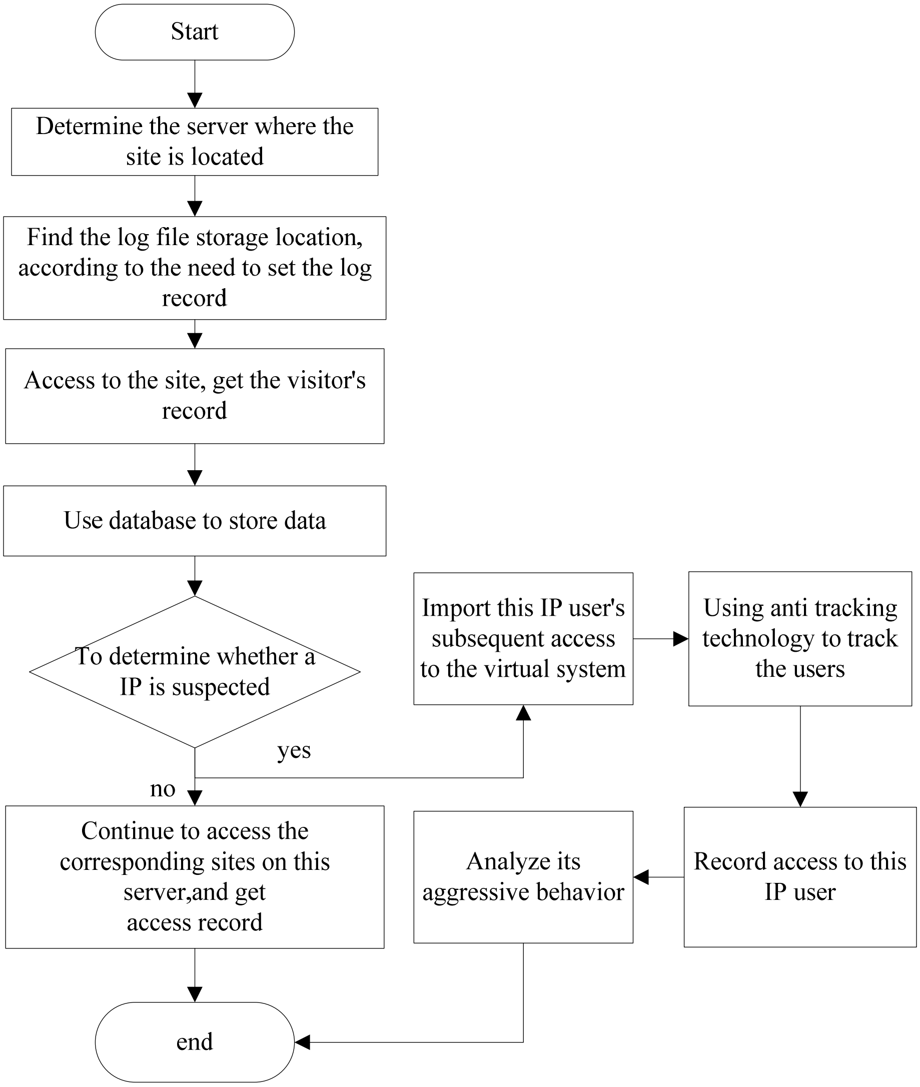
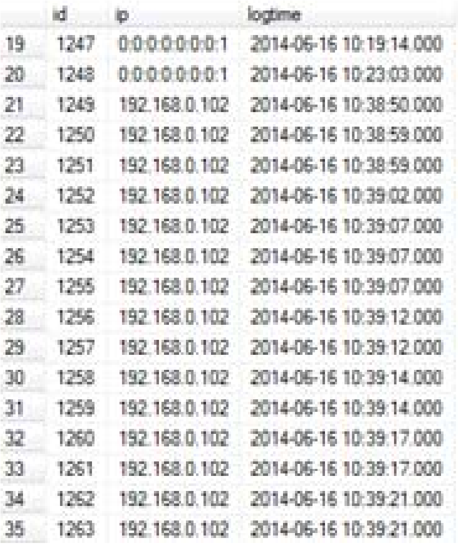

Start
Determine the server where the site is located
Find the log file storage location, according to the need to set the log record
Access to the site, get the visitor's record
Use database to store data
To determine whether a IP is suspected
yes
no
Import this IP user's subsequent access to the virtual system
Using anti tracking technology to track the users
Continue to access the corresponding sites on this server,and get access record
Analyze its aggressive behavior
Record access to this IP user
end

Figure 1. The Flowchart of Design Ideas

The main implementation system is divided into five modules: decoy system module, intrusion redirection module, data acquisition module, data analysis module and anti tracking module. To implement the decoy system module in the design need VMWorkstation virtual machine and its own deployment of the website system. What's more, website system needs MySQL database and server Tomcat. Implementation of intrusion redirection based on the configuration of Tomcat server. Data acquisition module is still based on the Tomcat server access log records. Data analysis module based on the Java language programming and database to achieve.Anti-tracking module manually track visitors in question after the results of the data analysis.

The core value of a honeypot is to collect an attacker's information and carries on the effective analysis. On this paper, the honeypot's collect information can get directly in the log file, and then apply the Java programming language to efficiently store data into the database and effectiveness analysis. Figure 2 is a specific display of data in the database.



	id	ip	logtime
19	1247	0:0:0:0:0:0:0:1	2014-06-16 10:19:14.000
20	1248	0:0:0:0:0:0:0:1	2014-06-16 10:23:03.000
21	1249	192.168.0.102	2014-06-16 10:38:50.000
22	1250	192.168.0.102	2014-06-16 10:38:59.000
23	1251	192.168.0.102	2014-06-16 10:38:59.000
24	1252	192.168.0.102	2014-06-16 10:39:02.000
25	1253	192.168.0.102	2014-06-16 10:39:07.000
26	1254	192.168.0.102	2014-06-16 10:39:07.000
27	1255	192.168.0.102	2014-06-16 10:39:07.000
28	1256	192.168.0.102	2014-06-16 10:39:12.000
29	1257	192.168.0.102	2014-06-16 10:39:12.000
30	1258	192.168.0.102	2014-06-16 10:39:14.000
31	1259	192.168.0.102	2014-06-16 10:39:14.000
32	1260	192.168.0.102	2014-06-16 10:39:17.000
33	1261	192.168.0.102	2014-06-16 10:39:17.000
34	1262	192.168.0.102	2014-06-16 10:39:21.000
35	1263	192.168.0.102	2014-06-16 10:39:21.000

Figure 2. valid data stored in the database

In this experiment, to determine whether a IP is an attacker is based on click numbers statistics on the link to the website in the specified time.Within a database, can clearly read out an IP access number, if the IP for suspected IP, then check the IP access to records, judge by the length of the IP access time see visit is normal, if according to interviews judge a visitor may be intruders will mark this IP and then make the IP attack into virtual system.

The judgment in the main database are as fellows:

```
select ip,count(*)as number
from logtable
group by ip
```

From the above query results and in front of the threshold determined to find an IP which is in high access frequency and suspected attack exists, then to recall the IP records, check its visit period. If data corresponds to this IP analyzed on threat then let the user into the virtual system, carrying out tracking analysis simultaneously.

To find an specific IP access records in the database's SQL statement as fellows:

```
select ip,logtime
from logtable
where ip='***.***.***.***'
```

Test

The realization of this design is based on the web site system to lure the attacker to visit. Test method: in the local area network with other PC to perform remote access attack, according to the log file for analysis of whether visitors have suspected attack, then the intrusion redirection will be used to import the suspect users to the website of the virtual system, and record their access behavior, achieve anti tracking at same time.Test system design ideas as shown in Figure 3 below:

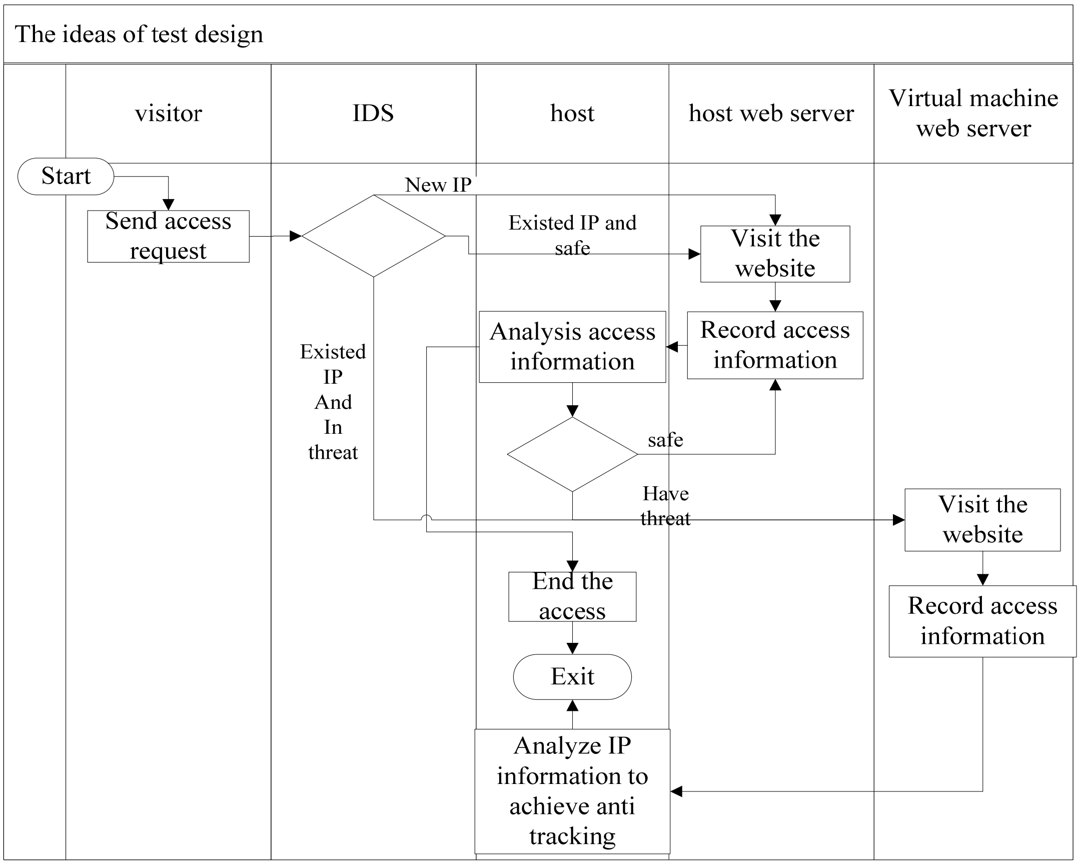
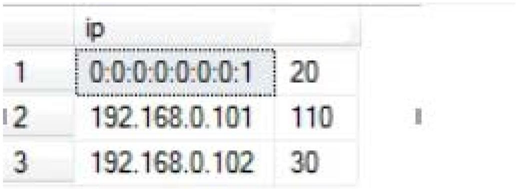


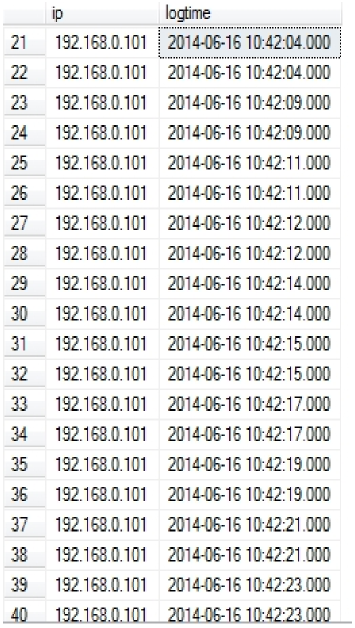
Figure 3. The ideas of test design

IP access statistics result of data analysis after testing is shown in figure 4.From the above query results and threshold mentioned on front determined to find IP 192.168.0.101 visits' access times is abnormal, suspected attack existing, then to recall the IP records, check its visit period. The specific IP access records is shown in figure 5.



	ip	
1	0:0:0:0:0:0:0:1	20
2	192.168.0.101	110
3	192.168.0.102	30

Figure 4. Analysis of the number of invasion records



	ip	logtime
21	192.168.0.101	2014-06-16 10:42:04.000
22	192.168.0.101	2014-06-16 10:42:04.000
23	192.168.0.101	2014-06-16 10:42:09.000
24	192.168.0.101	2014-06-16 10:42:09.000
25	192.168.0.101	2014-06-16 10:42:11.000
26	192.168.0.101	2014-06-16 10:42:11.000
27	192.168.0.101	2014-06-16 10:42:12.000
28	192.168.0.101	2014-06-16 10:42:12.000
29	192.168.0.101	2014-06-16 10:42:14.000
30	192.168.0.101	2014-06-16 10:42:14.000
31	192.168.0.101	2014-06-16 10:42:15.000
32	192.168.0.101	2014-06-16 10:42:15.000
33	192.168.0.101	2014-06-16 10:42:17.000
34	192.168.0.101	2014-06-16 10:42:17.000
35	192.168.0.101	2014-06-16 10:42:19.000
36	192.168.0.101	2014-06-16 10:42:19.000
37	192.168.0.101	2014-06-16 10:42:21.000
38	192.168.0.101	2014-06-16 10:42:21.000
39	192.168.0.101	2014-06-16 10:42:23.000
40	192.168.0.101	2014-06-16 10:42:23.000

Figure 5. The specific IP partial query results

As shown in Figure 5, IP 192.168.0.101 access time is from 10:41:42 to 10:42:41, in this close to a minute time, there are 51 access times the visit had made, as the previous set, this IP user is an invader. We need to mark the IP and make its link to the virtual system, at the same time to record the behavior of this IP, finally to achieve anti tracking the IP address users manually.

Summary

The final function of this design is to give the response information to the website system, which can correctly record the different activities of different users, and ensure the security of the real system and the log file. System in order to make the system more high simulation to deceive the intruders, the use of deceptive techniques of camouflage simulation technology, makes the intruder is not easy to suspect the authenticity of the system. Secondly, in order to make the intruder cannot destroy the real system, the intrusion redirection technology will be used to introduce the intruder's attack to the virtual honeypot. Thirdly, for the invasion of the invaders, the analysis of behavior should be done to record their behavior, and then analyze logs for the prevention, it used the information capture, information control and data analysis technology. Finally, for the honeypot system, it needs intrusion detection technology and firewall technology to work together to achieve active defense.

References

[1]Xu XianYue, Zhang FengBin. Research and Design on Two Mechanisms about Honeypot[C]. March 2009.

[2]Lance Spitzner. Honeypot-Definition Sand Value of Honeypots[J]. Addison-Wesley Reading. 2000,(8):125-129

[3]Zhao Hong, Wang LingXia. The design and implementation of campus network security defense system based on Honeypot Technology[J]. Automation & Instrumentation,2015,No.18503:134-136.

[4]Wang Jie, Yang Liu. Design and Implementation of Intrusion detection System Based on Honeypot[J]. Application Research of Computers. 2012,02:667-671.

[5]Chen Yang. The Design of Website Security Defense System Based on Honeypot[J]. Value Engineering. 2016,01:191-193.

[6]A Novel Approach for Redirecting Module in Honeypot Systems[J]. The Journal of China Universities of Posts and Telecommunications,2005,03:58-62.

[7]Tung-Ming Koo,Hung-Chang Chang,Ya-Ting Hsu,Huey-Yeh Lin. Malicious Website Detection Based on Honeypot Systems[C]. Proceedings of 2013 2nd International Conference on Advances in Computer Science and Engineering(CSE 2013) ,2012,4.