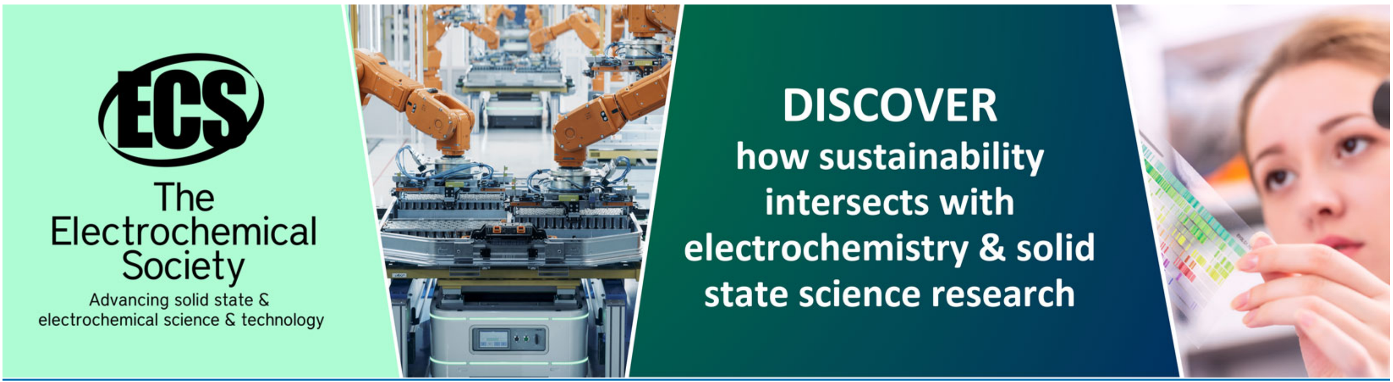
IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Research on Network Defense Strategy Based on Honey Pot Technology

To cite this article: Jianchao Hong and Ying Hua 2018 *IOP Conf. Ser.: Mater. Sci. Eng.* **322** 052033

View the article online for updates and enhancements.



Research on Network Defense Strategy Based on Honey Pot Technology

Jianchao Hong[1,*], Ying Hua[2]

[1]School of Mathematics and Computer Science, Northwest Minzu University, Lanzhou Gansu, China

[2]School of Foreign Languages, Northwest Minzu University, Lanzhou Gansu, China

[*] Corresponding author e-mail:29077401@qq.com

Abstract. As a new network security technology of active defense，The honeypot technology has become a very effective and practical method of decoy attackers. The thesis discusses the theory, structure, characteristic, design and implementation of Honeypot in detail. Aiming at the development of means of attack, put forward a kind of network defense technology based on honeypot technology, constructing a virtual Honeypot demonstrate the honeypot's functions.

1. Introduction

With the rapid development of computer network technology, the Internet has become more and more widely touched by the field, to bring convenience to people at the same time, computer network security issues are increasingly prominent. The computer network is an open network, the network of shared resources in the uncertainty, leading to the computer and the network vulnerable to hackers, computer viruses and other dangerous behavior attacks, in addition, the openness of the computer network protocol, anarchy management status, but also a network security risks of a reason. In order to make people more secure and safe to use the network, the study of computer network security defense measures become particularly important.

There are many ways and means to detect cyber-attack, but most of them are passive defense. We need to take the initiative to prevent network attacks, that is, to establish an active defense system to prevent attacks. Now the most representative of a means of active defense detection is the honeypot technology, which is by constructing a system with obvious loopholes to lure the intruder to attack, monitor and record the intruder information, extract the attack characteristics to send a new letter Intrusion, the unknown attack to play an effective prevention.

2. Introduction of honeypot technology

2.1. The basic concept of honeypots

Famous network security expert honeypot project team founder LaneeSPitzner, has made the following definition of honeypot: honeypot is a kind of information system resources, its value is reflected in the detection, attack or attack. From here we can know that it does not provide any useful information, cannot store any data, it is only used to lure the network attack, and to monitor, detect and analyze these attacks. This means that it will not directly improve the security of computer networks, but it is the other security policy irreplaceable an active defense technology.

2.2. Honeypot risks and disadvantages

Honeypots are a powerful tool through which you can collect various threat information. While getting this information, you must allow an attacker and malicious code to access your honeypot. The price you pay for is the risk of being broken. You have to determine which risks are important to you, once the break is likely to become a hacker to attack a third party springboard. In addition, existing rules honeypot systems are basically using rules written manually after being added to the rule base, and this anti-virus software, you need to be upgraded regularly updated, which greatly limits the use honeypot system Value, it is unknown intrusion attacks can’t do anything.

3. The core technology of honeypots

Honeypot as a member of an intrusion detection system, in the entire defense system is mainly used in the network spoofing technology, based on the data to capture information, and control intruder access and other technologies. Several key technologies of honeypots: data control, data collection, data analysis.

3.1. Internet spoofing technology

Honeypot we can also call it a decoy attack system. Only the intruder to attack it, in order to reflect its value lies. The main role of network spoofing technology is to detect the intruder's offensive means, to obtain their offensive purposes, cost the intruder a lot of time and resources to protect the real network. Now honeypot technologies include several such deception: ip address spoofing, the simulation system vulnerabilities luring attacks, network traffic simulation, dynamic port configuration of the system and so on.

3.2. Data analysis

Data analysis is the main function of the honeypot system, the ultimate goal of our establishment of the honeypot system is to analyze the data. The analysis of the honeypot system logarithmic analysis is mainly about the characteristics of the attack behavior, which is also a difficult problem of the honeypot system, because the honeypot collects a lot of information, and there is no necessary connection between the information, if you want to better analyze the information, we need to establish a data analysis module to analyze the information, so the behavior of the attacker establish a data analysis model.

3.3. Data collection

Data collection refers to the honeypot to monitor all activities to record, is the honeypot design of the core module. It is a challenge for us to collect as much threat as possible throughout the intrusion detection process. The more information we capture, the better we can analyze these attacks, analyze the attacker's motivation, strategy, and the tool.

3.4. Data control

Data control can curb network intrusion, which can mitigate the potential of attackers to exploit honeypots to attack or harm non-honeypot systems. We have to make every effort to ensure that once the attacker has entered our honeypot system, reduce the harm to the non-honeypot system. We can only minimize the risk, different data control techniques and methods have different degrees of risk, but can’t completely eliminate the risk.

4. The design of the defense system

The original intrusion prevention systems generally cannot detect unknown attacks, which there is a certain danger, we use honeypot technology in intrusion detection systems to reduce the incidence of such things. As long as the intruder visits the honeypot, we can record some of the information it visits, honeypots can also interact with intruders, data analysis module analysis of these logs, you can predict the purpose of intruders, attack methods, the use of attack tools, this can make up for the lack of traditional intrusion prevention system, to the real system to provide a more secure guarantee, timely make up for system vulnerabilities.

4.1. System design ideas

This new intrusion prevention system is based on honeypot technology to achieve. When it detects intrusion, it matches the intrusion rules in the intrusion detection rule base, if it is a new intrusion, it will call the data analysis module to analyze these intrusion behavior, generate new intrusion detection rules, and update the intrusion rule base, this will improve the defense capability of the intrusion prevention system, thus enhancing the security of the network system.

4.2. System module design

The intrusion prevention system designed in this paper is mainly composed of five modules, the central control module, the intrusion detection module, data entry module, a data analysis module, spoofing module. The central control module is implemented by the console, the data analysis module is implemented by the data analysis center, the spoofing module and the data entry module are implemented by the honeypot, the intrusion detection module is mainly for the detection of abnormal information.

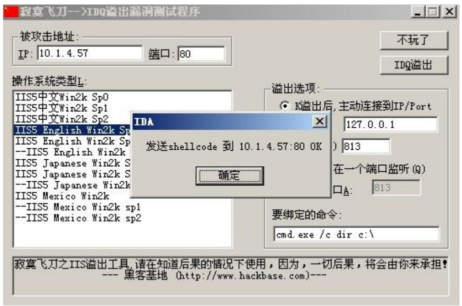
When the intruder is looking for a vulnerable host to attack, it will find the honeypot system in the defense system. This time the honeypot system, once found to be monitored, will use its own spoofing system to generate interactive data traffic with the outside world, forging some outbound traffic, so that the intruder believes it is a real network where they are interested information lures them to attack the honeypot system. Intruder will use various means to immediately carry out their attacks on the honeypot system, get useful information, carry out sabotage activities, at the same time the honeypot system will try to interact with its implementation in order to delay the attack time of the intruder, so that the data record module can leave ample time to record the attack information, and pass these information as quickly as possible to the data analysis module and the database stored to prevent the intruder to access the information to modify or delete operations. At the same time intrusion detection module will respond to this, to find the best way to deal with intruders. Any intruder's operation on the honeypot system will be captured by the intrusion detection system, and then the intrusion detection system will send these early warning information to the central control module, the central control module monitor the intruder, this is to avoid the honeypot system once broken, to protect the entire system of other host security, according to information recorded by the honeypot system, at the same time it will give instructions to the data analysis module, let him analyze the data recorded in the honeypot log, analyze it to extract useful rules, stored in the regular database for future intrusion detection system defense intruders attack again.

5. Analog Test System

Here we use some intrusion attacks to test the honeypot system and analyze the data recorded by the honeypot to discover the true intentions of the intruder and generate new rules for storage into the intrusion detection database.

5.1. Overflow attack test

We use a hacker tool to simulate the test, with iis idq overflow program to test.



被攻击地址: IP: 10.1.4.57 端口: 80

操作系统类型L:

```
IIS5中文Win2k Sp0
IIS5中文Win2k Sp1
IIS5中文Win2k Sp2
IIS5 English Win2k Sp
IIS5 English Win2k Sp
--IIS5 English Win2k
IIS5 Japanese Win2k S
IIS5 Japanese Win2k S
--IIS5 Japanese Win2k
IIS5 Mexico Win2k
--IIS5 Mexico Win2k sp1
--IIS5 Mexico Win2k sp2
```

● K溢出后，主动连接到IP/Port 127.0.0.1) 813

在一个端口监听(Q) 口A: 813

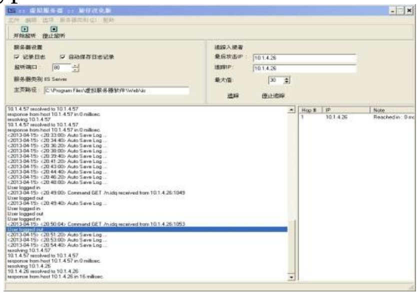
要绑定的命令: cmd.exe /c dir c:\

IDA: 发送shellcode 到 10.1.4.57:80 OK

寂寞飞刀之IIS溢出工具,请在知道后果的情况下使用，因为，一切后果，将会由你来承担!
--- 黑客基地 (http://www.hackbase.com)---

Figure 1. iis idq overflow program test graph

Once the program sends iis idq overflow attacks, we can see the attack log on the “trapserver”, This can achieve the purpose of the honeypot.


:: 虚拟服务器 :: 旋仔汉化版
文件 编辑 选项 服务器类别(J) 帮助
开始监听
停止监听
服务器设置
追踪入侵者
追踪
停止追踪

☑ 记录日志 ☑ 自动保存日志记录

监听端口: 80

服务器类别 IIS Server

主页路径: C:\Program Files\虚拟服务器软件\Web\iis

最后攻击IP: 10.1.4.26

追踪IP: 10.1.4.26

最大值: 30

```
10.1.4.57 resolved to 10.1.4.57
response from host 10.1.4.57 in 0 millisec.
resolving 10.1.4.57
10.1.4.57 resolved to 10.1.4.57
response from host 10.1.4.57 in 0 millisec.
<2013-04-15> <20:33:00> Auto Save Log ...
<2013-04-15> <20:34:40> Auto Save Log ...
<2013-04-15> <20:36:20> Auto Save Log ...
<2013-04-15> <20:38:00> Auto Save Log ...
<2013-04-15> <20:39:40> Auto Save Log ...
<2013-04-15> <20:41:20> Auto Save Log ...
<2013-04-15> <20:43:00> Auto Save Log ...
<2013-04-15> <20:44:40> Auto Save Log ...
<2013-04-15> <20:46:20> Auto Save Log ...
<2013-04-15> <20:48:00> Auto Save Log ...
User logged in
<2013-04-15> <20:49:00> Command GET /n.idq received from 10.1.4.26:1049
User logged out
<2013-04-15> <20:49:40> Auto Save Log ...
User logged in
User logged out
User logged in
<2013-04-15> <20:50:04> Command GET /n.idq received from 10.1.4.26:1053
User logged out
<2013-04-15> <20:51:20> Auto Save Log ...
<2013-04-15> <20:53:00> Auto Save Log ...
<2013-04-15> <20:54:40> Auto Save Log ...
resolving 10.1.4.57
10.1.4.57 resolved to 10.1.4.57
response from host 10.1.4.57 in 0 millisec.
resolving 10.1.4.26
10.1.4.26 resolved to 10.1.4.26
response from host 10.1.4.26 in 16 millisec.
```

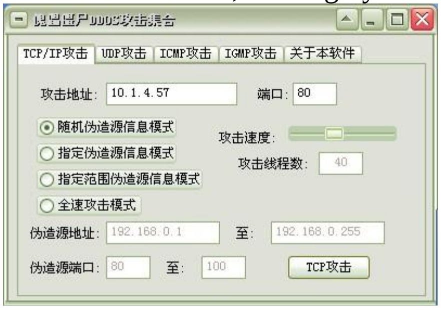
Hop #	IP	Note
1	10.1.4.26	Reached in : 0 m

Figure 2. Attack record graph

5.2. *Denial of Service Attack*

Here we are on the system TCP / IP attacks, UDP attacks, ICMP attacks and IGMP attack test, using a puppet zombie attack set.

Here to TCP / IP attack, for example, the attack address is set to 10.1.4.57, the port is 80, the attack mode is set to "random forged source information mode", the attack thread number is set to 40, the forgery source address is 192.168.0.1 to 192.168.0.255, the forgery source port is 80.



攻击地址: 10.1.4.57 端口: 80

● 随机伪造源信息模式
○ 指定伪造源信息模式
○ 指定范围伪造源信息模式
○ 全速攻击模式

攻击速度:

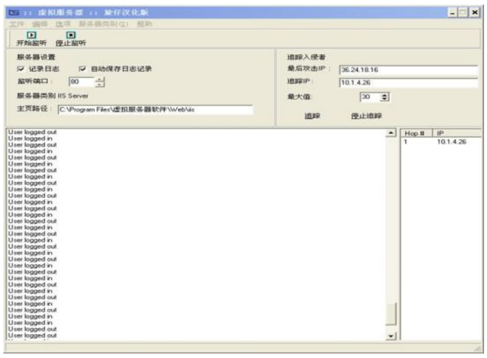
攻击线程数: 40

伪造源地址: 192.168.0.1 至: 192.168.0.255

伪造源端口: 80 至: 100

Figure 3. TCP / IP attack graph

During the attack, we can see the attack record on the honeypot virtual software "trapserver". As shown in Figure 4:


:: 虚拟服务器 :: 旋仔汉化版
文件 编辑 选项 服务器类别(J) 帮助
开始监听
停止监听
服务器设置
追踪入侵者
追踪
停止追踪

☑ 记录日志 ☑ 自动保存日志记录

监听端口: 80

服务器类别 IIS Server

主页路径: C:\Program Files\虚拟服务器软件\Web\iis

最后攻击IP: 36.24.18.16

追踪IP: 10.1.4.26

最大值: 30

```
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged out
User logged in
User logged in
User logged out
User logged out
```

Hop #	IP
1	10.1.4.26

Figure 4. Attack record graph

6. Summary and outlook

My research work on the honeypots is just the beginning, the honeypot related to all aspects of network technology and technology also need to further study and conduct a detailed study, so as to better improve the honeypot system. For example, the data collection technology to further study, because the honeypot is through the collection of relevant activities to master their traces, rules of activities, improve the efficiency of data analysis, and thus better for network defense services. How to better protect the honeypot system log not to be destroyed by the intruder, which is a focus should be the content of the study. With the development of technology, the emergence of virtual honeynet technology, but also for the honeypot technology research provides technical support.

Acknowledgment

The work is supported by Central colleges and universities Basic research business projects of Northwest Minzu University (No. 31920160083) and Natural Science Foundation of China (No. 61662065).

References

[1] Xueguang Zhou et al. Information Security. Beijing: Mechanical Industry Press, 2003.3
[2] Dong Yuge, etc. Network Attack and Protection - Network Security and Practical Protection Technology. Beijing: People's Posts and Telecommunications Press, 2002.8
[3] (US) Heith E. Strassberg waiting. Li Ang and other translation. Firewall technology Daquan. Beijing: Machinery Industry Press, 2003.3
[4] Wenjuan He, honeypot technical analysis and honeynet design, Anhui University, 2011
[5] Bo Wang, based on the honeynet security strategy firewall, Beijing University of Posts and Telecommunications, 2010
[6] Zhijun Lu, Huang Hao. Distributed real-time intrusion detection system under high speed network, computer research and development. Vol. 41 No. 4 April 2004
[7] Zhai Guangqun, Chen Xiangdong, Hu Guijiang.Study and design of linkage system of honeypot and intrusion detection technology [J]. Computer Engineering and Design, 2009 30 (21): 4847.
[8] Cai Xiaozhou, computer network security and countermeasures research, Silicon Valley, 2012 15 period.
[9] Li Xiaoping. Intrusion prevention system research and design. Microcomputer information, 2006 22
[10] Zhuge Jianwei. Honeypot and honeypot system technology brief, the North God hunting Goddess project team technical report [R], 2004