Construction of large-scale honeynet Based on Honeyd

Jun Wang\textsuperscript{a,b}  * Jing Zeng\textsuperscript{a}

\textsuperscript{a}Department of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang, China
\textsuperscript{b}De Montfort University, England, UK

Abstract

Honeyd is a tool for simulating computer system on the network layer. A framework of Honeyd is introduced in this paper. The development concept and the way of working of Honeyd are analyzed. A virtual large-scale network is constructed by Honeyd, and which includes network delay, network packet loss. The topology of virtual network, host operating system and system services are tested. Honeyd configuration file is listed in this paper. It shows that Honeyd can simulate large-scale network successful.

Keywords: Honeyd, Simulation, Honeynet;

1. Introduction

As a independent system, Honeypot comes from the document, “An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied”, which is published by Bill Cheswick in 1991. The author notes that although there have been some security tools could detect hacking, but not all the hackings. For providing more information, the author opens some forged services on the port, and attracts hacker. And then the activity of the hacker will be record. The so-called forged services are imitating some actions of normal server software, such as establishing a connection, prompting the users to input user name and password. As Bill Cheswick mentioned forged services again in the book called “Feriwall and Internet
Security: Repelling the Wily Hacker”, which is published by the cooperation with Stevne M. Bellovin, and the word of Honeypot is used. He mentioned especially that the function of Honeyd on recording hacker’s information could be used as the purpose of detecting [1].

Honeynet is a high-level interaction Honeyd. Actually, Honeyd can hardly provide high-level interaction. The concept of Honeynet is simple: to construct a network system and to observe the network system when it is set up behind some kinds of access control equipment (Firewall). Attacker can probe, attack and use any system in Honeynet, and then provide integrated operating system and applications for interaction. The system in Honeynet may be any kind of system: Solaris system includes Oracle Database, or Windows XP includes IIS Web Server, or a Cisco route. In one word, the system in Honeynet must be a really production system.

2. Honeyd

Honeyd is a background program for creating the hosts in virtual network, which could provide any service by configuration. Using personalized treatment, the hosts display that they run in a particular version of operating system [2]-[4].

2.1. Development concept of Honeyd

The design and development of Honeyd mainly consider the following points: How to lead the information which has been sent to virtual Honeyd into Honeyd hosts; How to make virtual hosts real to attackers, at the same time, make Honeyd hosts safe; How to simulate any topology; How to support Honeyd hosts to communicate with hosts in other systems by tunnel network; How to record network connection and malicious attacks; How to configure Honeyd by simple configuration grammar.

2.2. The work way of Honeyd

When a virtual IP in system is attacked, Honeyd will have a role of the victim and interact with attackers. It doesn’t allocate thousands of IP address to itself to complete this job once. On the contrary, just one IP: a unique IP is allocated to it. This port is the same with the management port of Honeyd that we used. That same port will monitor the suspicious activity in network.

The running principle of Honeyd is as follow: when it receives a connection to the system which does not exist, it assumes that the attempt of this connection is hostile, which is likely a probe, scan or attack. When Honeyd receives this kind of flow, it will assume that its IP is the destination address (to make it as a victim). Then it will start virtual service to the port which the connection attempts. Once virtual service started, it will interact with attacker and capture attacker’s all activity. When attacker completes his activity, virtual service will exit and stop running. And then, Honeyd will wait for more flow or connection attempts to the system which does not exist. Just as receiving a connection attempt to the system which is not exist, Honeyd will assume that IP and run virtual service. This is a very efficient method.

As Honeyd receives more attack, it will repeat this procedure. It will assume to be target’s IP, start relevant virtual service to attack, interact with attacker, capture attack, and exit at last. It can simulate many IP and interact with different attackers.
The knack of Honeyd is making honeypot to receive the inexistence system’s flow. How to know which system is not exist? How to receive the activities? Honeyd will not distinguish these systems, and will not routing this attack to itself. There are two methods to accomplish: One is that it will route all flow to Honeyd in the network system without any active. The other one is that it sends the inexistence system’s flow to Honeyd in the network system with active and inexistence system.

3. The characteristic of Honeyd in Simulation Network

It is always active program that Honeynet is researched by simulation network based on the virtual host of Honeyd. Honeyd is a kind of characteristic, small daemon process. It can not only simulate many operating systems features, but also provide many TCP services, like HTTP, FTP, SMTP, SSL service. In the research of Honeynet, the typical role of Honeyd is to set up many virtual honeypots which are used to confuse the enemy. Its structure is shown as Fig 1. [5].

Fig. 1. The structure of Honeyd

One practical feature of Honeyd is to simulate a whole topology on one host, including simulation hop count, packet loss rate, and propagation delay. Therefore, we could simulate kinds of complex topologies in the experimental environment. The structures of network can make enemy believed easily who falls into Honeynet [6][7].

The features of Honeyd could be used to simulate network:

1. Simulation large-scale topology;
2. Network features can be set, like delay, packet loss rate, and bandwidth;
3. To support multi-entry route;
4. Physical host can connect to topology;
5. To support asymmetric route;
6. To support GRE tunnel protocol used to construct distributed network.

Honeyd can simulate different brands and types of routes, and also can simulate delay and loss of network connection. When we use tools like traceroute to network map, network data flow will display the same with route configured and the structure of network. When we simulate routing topology, it is not allowed to send packet to Honeyd host by ARP spoofing. We must configur routing to make virtual honepot map to Honeyd host.

Typically, virtual route topology is a tree-structure. The tree regards the entrance of simulation topology which network packet enters as root. Every internal node represents a route. Every edge
represents a link with delay and loss. Tree’s terminal nodes correspond with the host nodes in network. The structure of Honeyd supports many parallel and coexistence web entrances.

When it is receiving packet, system will find appropriate routing entry. It starts from the root and travels around routing tree, until find the node which contains the target IP of the packet. The loss rate and delay of packet are accumulated to determine to abandon or put off.

4. Simulation network delay and network packet loss

A host is used to simulate network delay and network packet loss rate. Simulation network is consisted of 6 virtual hosts and 3 Cisco route. The topology is shown as Fig 2. Route R1 separates 192.168.0.0/24 and 10.0.1.0/24. Route R2 separates 10.0.1.0/24,10.1.0.0/16 and 10.1.0.0/24. Route R3 separates 10.1.0.0/24 and 10.1.1.0/24. Route R1’s access address is 192.168.0.x/24. Route R2’s access address is 10.0.1.x/24. Route R3’s access address is 10.1.0.x/24. The virtual host 1, 2 are in 10.0.1.0/24. The virtual host 3, 4 are in 10.1.0.0/16. The virtual host 5, 6 are in 10.1.1.0/24. It can access directly 10.0.1.0/24 via R1. It can access directly 10.1.0.0/16 via R2. It can access directly 10.1.1.0/24 via R3.

Fig. 2. Topology

Honeyd configuration file:

```plaintext
##Router
create R3
set R3 personality "Cisco 7206 router (IOS 11.1(17)"
set R3 default icmp action open
set R3 default tcp action reset
set R3 default udp action reset
bind 10.1.0.150 R3
route entry 10.1.0.150 network 10.1.1.0/24
route 10.1.0.150 link 10.1.1.0/24

create R2
set R2 personality "Cisco 7206 router (IOS 11.1(17)"
set R2 default icmp action open
set R2 default tcp action reset
set R2 default udp action reset
bind 10.0.1.150 R2
route entry 10.0.1.150 network 10.1.0.0/16
route 10.0.1.150 link 10.1.0.0/16
```
route 10.0.1.150 add net 10.1.1.0/24 10.1.0.150 latency 300ms loss 0.1

create R1
set R1 personality "Cisco 7206 router (IOS 11.1(17)"
set R1 default icmp action open
set R1 default tcp action reset
set R1 default udp action reset
bind 192.168.0.151 R1
route entry 192.168.0.151 network 10.0.1.0/24
route 192.168.0.151 link 10.0.1.0/24
route 192.168.0.151 add net 10.1.0.0/24 10.0.1.150

5. Summary

Honeyd is the most widely used in the frame of honeypot system with low-interaction and protection currently. It has mature applications in areas of computer and network security [10]. Honeyd is not simulating all sides of operating system, but just network protocol stack of operating system for simulating specific operating system. Honeyd works in network layer. That intruder only can interact with Honeyd system in network layer. Even if Honeyd is broke, these intruders do not get access to the real system forever. However system can still get details of the invasion.

Acknowledgements

I am very grateful CSS&JLU INFO-TECH CO., LTD who designs this device and software. The main experimental platform and scheme come from the company. Now, this work is partially supported by Natural Science Foundation of Liaoning Province #20102178, Liaoning Provincial Office of Education Fund #2009S078, #LS2010123 and #2009B149.

References