SDN Virtual Honeynet for Network Attack Information Acquisition

Zhe LIAN*, Xiao-chuan YIN, Ren TAN and Yu-xin CHEN
Institute of Information and Navigation, Air Force Engineering University, Xi’an 710077, China
*Corresponding author

Keywords: Attack information, Software defined networking, Virtual honeynet, On-demand acquisition.

Abstract. Since the existing network defense technology cannot acquire on-demand network attack information, and cannot adjust the network structure according to the threats of network attack dynamically, we propose a SDN virtual honeynet for network attack information acquisition. By constructing the SDN honeynet and using the good expansibility and controllability of the OpenDaylight controller, the problems such as the difficulty of flow control, inconvenient deployment and complex adjustment of the traditional honeynet are solved. Finally, the mininet simulation platform is used to build SDN virtual honeynet, and simulation results show that the SDN virtual honeynet can achieve on-demand acquire network attack information and dynamic adjustment of network structure etc., thereby reducing the network attack threat.

Introduction

In today's increasingly complex network environment, network information security has become a focus of attention. The research of network situation awareness has a relatively deep awareness about the present security states of the network. Moreover, it provides the evaluation and forecast to the states of network, thus, it can offer data support for deciders. Honeynet[1-2] uses a kind of proactive defense mechanism, which means monitoring the behaviors of attackers as well as tempting attackers’ operation by inducing attackers entering the pre-designed honeypot network. Therefore, on the one hand, it plays a certain function on protecting the real network; on the other hand, it can obtained more situation information through inducing attackers, meanwhile, by the use of the analysis, evaluation and prediction which based on these achieved situation information, it provides efficient defense. However, the network environment changes currently, in order to achieve the attack situation information which in accordance with demand, and facing all kinds of network attacking flexibly, this paper poses a kind of virtual honeynet framework which based on the SDN[3] (Software Defined Network).

Comparing to the traditional honeynet system, this framework has lower cost and faster deployment. For satisfying different demands of network resources, it defines the logical network topology through software, uses the virtualization technology to structure the network topology, meanwhile, there is no need to considering the physical topology of the underlying network, and it can realize the dynamic deployment. For one thing, it can change the network structure dynamically in order to decreasing the threat of the networking security, raising the security level of network; then, it provides deciders the data supporting and realizes the proactive defense by achieving specific and valuable situation information which through the dynamic deployment, and by combing the flow table information at the same time.

Relative Research

The raise of the honeypot is due to the fact that there are lots of network securities problems exist, such as: the weakness in security foundation, excessive attacking tools and the unbalance game of the network attack and defense. Thus, in order to change the unbalance situation of the game between the attack and defense, the honeypot can be used. The honeynet, essentially, is a type of investigative and
high-interactive honeypot\textsuperscript{[4]}. Former research mainly focus on the five key technology of the honeynet system: Network spoofing, data capture, data control, attack analysis and feature extraction, early warning and prevention, and suggested a lot of efficient algorithm\textsuperscript{[5]}. Currently, the honeynet has developed to the third generation, and the core technology presented by its expensive honeywall equipment, which increases the cost of safety protection.

Nevertheless, the traditional honeynet has many weaknesses like: the difficulty on controlling the system traffic, the inconvenient deployment of the physical machine, the complexity of the dynamic adjustment, and the expensive honeywall equipment. Because of these weaknesses, the traditional honeynet cannot meet the requirement of the fickle network environment, and it also cannot achieve valuable states information through conducting specific adjustment. Hu Yixun\textsuperscript{[6]} came up with the virtual honeynet which based on the Openflow Protocol in 2015, he proved the honeynet system has low forwarding delay and high dynamic characteristics and the effectiveness of the superimposed virtual honeynet system by making use of the Openflow switch. The Network security situation awareness model based on the Simple Additive Weighting Method and Grey Theory which suggested by Lai Jibao and others can evidently and quantitatively reflect the current status of the network attack\textsuperscript{[7]}

On the base of these former researches, this paper plans to analyze the situation of network attack further, build the SDN virtual honeynet, realize achieving network situation information according to the demand, adjust the network structure basing the network situation, and finally, decrease the threat situation of the network attack.

**Prerequisite Knowledge**

**The SDN Structure**

SDN\textsuperscript{[8-9]} arises a type of software defined network structure, which can deploy the specific network equipment by software, and realize the real-time control of the network traffic through specific controller, therefore, achieving the separation between the data control layer and data transfer layer, which decreases the cost of the network deployment, facilitates the dynamic adjustment of the control of the network states, and increases the flexibility and controllability of the network. As shown in the figure 1\textsuperscript{[10]}. 

![Figure 1. SDN basic architecture.](image-url)

Base on this, it is continent to exploiting all kinds of applications, defining the logistic network topology by software can be used to meet variable demands to network resources, without considering the physical topology of the underlying network, therefore, it can realize that controlling network’s function and characteristic according to customers’ demands, through the control of the network traffic which used the SDN controller.

**The Analysis and Development of the MODEL in Literature [7]**

Literature [7] suggests a kind of attacking situation evaluation model based on the Simple Additive Weighting Method, according to the amount of variable services that provided by network and different types of the threat to network. The meanings of relevant symbols, parameter specification
and specific model are shown in Literature [7]. The definition of the current network security was defined as equation (1), the larger the $F$, the greater threat to the network.

$$F = (S, A, C, N, T) = \sum_{i=1}^{n} \beta (\sum_{j=1}^{m} 10^x C_j)$$ (1)

Through the experimental use of the model to the network situation was captured and evaluated, get two sets of data: Table 1 shows the service running status of the network. Table 2 shows the number of attacks and the degree of threat received by the service. The blank indicates that the service is not running during the time period. "0" indicates that the service has not been attacked during the time period. The \{degree of threat (number of attacks)\} indicates the threat status of the service.

Table 1. Service operation condition.

<table>
<thead>
<tr>
<th>Time</th>
<th>Service Name</th>
<th>$\beta$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1$</td>
<td>{FTP, RPC, SOCKET}</td>
<td>{0.335, 0.375, 0.29}</td>
<td>3</td>
</tr>
<tr>
<td>$T_2$</td>
<td>{FTP, RPC, DNS, SOCKET, HTTP}</td>
<td>{0.265, 0.282, 0.103, 0.295, 0.155}</td>
<td>5</td>
</tr>
<tr>
<td>$T_3$</td>
<td>{FTP, RPC, SOCKET, TELNET}</td>
<td>{0.192, 0.391, 0.306, 0.111}</td>
<td>4</td>
</tr>
<tr>
<td>$T_4$</td>
<td>{FTP, RPC}</td>
<td>{0.564, 0.436}</td>
<td>2</td>
</tr>
<tr>
<td>$T_5$</td>
<td>{FTP, RPC, SOCKET, HTTP}</td>
<td>{0.079, 0.295, 0.237, 0.389}</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 2. Number of service attack and threat level.

<table>
<thead>
<tr>
<th>Time</th>
<th>FTP</th>
<th>RPC</th>
<th>DNS</th>
<th>SOCKET</th>
<th>HTTP</th>
<th>TELNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1$</td>
<td>{1(2)}</td>
<td>{1(3)}</td>
<td>{1(5)}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$T_2$</td>
<td>{1(1)}</td>
<td>{2(2)}</td>
<td>{2(2)}</td>
<td>{1(1)}</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$T_3$</td>
<td>{2(2),1(2)}</td>
<td>{1(1)}</td>
<td>{2(1)}</td>
<td></td>
<td></td>
<td>{2(2)}</td>
</tr>
<tr>
<td>$T_4$</td>
<td>{2(1),1(6)}</td>
<td>{1(1)}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$T_5$</td>
<td>{3(1),1(3)}</td>
<td>{1(4)}</td>
<td></td>
<td></td>
<td>0</td>
<td>{1(2)}</td>
</tr>
</tbody>
</table>

According to Table 1 and 2 and the model formula can be calculated for each time period of the attack situation, only the attack situation was calculated and predicted in the literature [7], and did not deal with the attack situation. Based on the analysis of the number of attacks and the degree of threat of different services in Table 1 and 2, this paper designs the dynamic virtual honeynet based on SDN to change the network structure so as to reduce the attack threat by reducing or stopping the high-risk service. And for the current situation, it can on-demand access to more information and provide more services easy to fall, and to achieve the purpose of on-demand acquisition information.

**SDN-based Virtual Honeynet**

**Virtual Honeynet Architecture**

Using the lightweight software defined network test platform mininet\[^{11}\] deploy virtual honeynet, the SDN controller OpenDaylight (ODL) control network traffic forwarding virtual honeynet function, honeynet structure shown is in Figure 2:
Based on the SDN architecture, the network is divided into three layers: the application layer for external users to visit or induce the attack side to attack the honeynet; control layer using ODL controller control virtual honeynet flow forwarding and collect the network flow table information, which can be used as a way to get situation information; virtual infrastructure equipment used to build business network and virtual honeynet, virtual honeynet induce attackers to access attacks, on the one hand can protect the real system from attack; the other hand, according to demand dynamic Adjust the network structure, to lure attackers attack, and then get more effective situation.

**Network Traffic Forwarding Process**

When the attacker attack the SDN virtual honeynet, through the firewall, IDS device monitoring can inform the ODL controller to control the network traffic forwarding, to lure the attackers attack the honeynet, to achieve honeynet function, and access to the situation information. The traffic forwarding process is shown in Figure 3:

**Step 1:** When the attacker accesses the service, it first passes the monitoring analysis of the firewall and the IDS device, and informs the ODL controller when the attacking behavior is detected.

**Step 2:** The ODL controller sends the traffic forwarding command to the service network virtual switch through the flow table.

**Step 3:** The business network switch resolves the flow control command to forward the attacker's request to the honeynet.

**Step 4:** The honeynet switch transfers the traffic to the corresponding service according to the request received.

**Step 5:** The honeynet sends the response traffic to the ODL controller. The ODL controller can change the flow table information and forward the response traffic to the external network through the service switch to complete the information exchange.

**Step 6:** The ODL controller can determine the attack behavior by monitoring and analyzing the shell command or privileged behavior of the honeypot system, and analyze the time and space information of the attacker to achieve the purpose of obtaining the network situation information.

The entire network architecture through the firewall, IDS, ODL controller to monitor and record the network traffic, log and other information, in the case of the attacker was not found to be caught, to capture more information about the network situation and analysis of attack behavior, evaluate the situation, so as to make corresponding countermeasures.
Simulation Experiment

Experimental Deployment

In this paper, the virtual machine software VMware 12 is used, a total of two virtual machines were built. A virtual machine is installed on the Ubuntu system, on which the ODL controller Beryllium version is installed; another virtual machine installs the Ubuntu server version, and installs the Mininet-2.2.1. Two virtual machines will be interconnected. The use of mininet is to establish a virtual honeynet, through the ODL controller to control the flow of honeynet. Virtual machine deployment can be more convenient to realize the construction of virtual honeynet, simple facilities and low cost. Through the mininet deploys SDN network, it can achieve the same effect with the entity machine, it can also support complex topology, easy to use, powerful, and easy to restore.

Simulation Test and Analysis

The purpose of the test is to verify the convenience of dynamic deployment of Honeynet based on SDN architecture and ODL controller, as well as the adjustment of the network situation, and improve the network security. Create two switch nodes by using mininet. Each switch configuration of two hosts, respectively, on behalf of HTTP services and MySQL services. As shown in Figure 4 is the topology which monitored by the ODL controller, where the left switch is the business system, providing two services. The right switch is a honeypot system, which is used to induce the attacker to attack.

![Figure 4. Virtual honeynet topology.](image)

Compared with static honeypot, dynamic virtual honeynet has the advantages of Identification difficulty and low cost, it will be widely used in the future, and virtualization technology more in line with the future development of the network environment. The architecture can define network topology by custom Python scripts, the core code is shown in Figure 5, it can accord need to increase and delete service hosts, dynamic adjustment of network structure, reduce network threat, and improve network security.

![Figure 5. Define topology core code.](image)

Based on the experimental data obtained from the literature [7], the \( T_2 \) and \( T_3 \) time periods are taken as examples, the security situation of the two time periods is \( F_2 = 83.2, F_3 = 100.95 \). In Table 1, 2
can be seen at $T_2$ time the number of attacks and threats degree of RPC and DNS service is relatively large, but the proportion of RPC services is relatively large, through the SDN virtual honeynet can achieve rapid change of network structure, stop the RPC service. When the RPC service is stopped, the weight of the system service changes:

$$\beta_i = \frac{\beta_i}{\sum_{i=1}^{n} \beta_i}$$  \hspace{1cm} (2)

After changing the network topology, the weight of each service is shown in Table 3:

<table>
<thead>
<tr>
<th>Time</th>
<th>Service Name</th>
<th>$\beta_i$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_2$</td>
<td>{FTP,DNS,SOCKET,HTTP}</td>
<td>{0.324,0.126,0.361,0.189}</td>
<td>4</td>
</tr>
</tbody>
</table>

At this point the network security situation is $T_2 = 32.05 < 83.2 = T_3$. Through the virtual honeynet to adjust the network structure can reduce the network security situation, and improve network security.

For the time, when the network FTP, RPC, HTTP services suffered more serious attacks, in order to obtain more information about the means of attack, time and space information, you can dynamically adjust the network structure, add more bait honeypot host to obtain the status information, to achieve for the purpose of on-demand acquisition information, and for the actual service to provide more targeted protection and defense. When the attacker attacked for some time, once again dynamic adjustment the honeynet system, always change the network state, only the network state is changing in time to ensure the network opacity, so that the network is effectively protected.

Experiments show that the dynamic virtual honeynet based on SDN can solve the difficult problems of traditional honeynet flow control and the inconvenient and dynamic deployment complexity of physical machine deployment. Combining the network attack situation assessment model based on Simple Additive Weighting Method, it further validates the SDN dynamic virtual honeynet can be achieved on-demand situation information, according to the situation needs to dynamically adjust the network structure, thereby reducing the network situation threat situation, and get more effective situation information.

**Conclusion**

Based on the previous research, this paper combines the network attack situational awareness research and SDN correlation technology, and uses the SDN architecture to design a dynamic virtual honeynet by combining the ODL controller with mininet. The architecture can realize the basic function of the honeynet system in the traditional sense. It can facilitate the deployment of honeynet, add or remove all kinds of services, save more cost, deploy more convenient and make the system easier to restore. This paper validates the significance of SDN dynamic virtual honeynet based on the research of network attack situation: on the one hand, it can improve the security of network system by dynamically stopping high-risk service, reducing network security situation and improving network security. On the other hand, by analyzing the network situation on-demand dynamically deploy honeypot services, can get more information about the situation and provide support for decision-making.

Because mininet belongs to the lightweight software definition network test platform, the function service is limited. In the later research work, we can use multiple virtual machines to realize the software defined network architecture. On this basis, deploy virtual honeynet which more complex and functional services is more perfect. The Secondly, we can make full use of the ODL controller, combining the flow table information and the traditional network situational awareness analysis algorithm, analyze the network security situation, provide the support of the situation information.
References


