Method for Measuring the Internet Devices and Applications Based on the Features

Chuan GAO [1,2], Han-bingYAN[2,]* and Zi-Xiao JIA[2]

[1]Beihang University, Beijing 100191, China

[2]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100020, China

*Corresponding author

Keywords: Internet device and application, Feature extraction, Active detection, Passive monitoring.

Abstract: With the continuous development of the Internet, the security problem of the Internet is more and more serious. The security postures of the Internet devices and applications have subjected extensive attention of the growing number of Internet users. In this paper, we put forward a measurement method of Internet devices and applications based on the features. Firstly, the features of the Internet devices and applications were extracted. The combined method of the active detection and passive monitoring was used to get the information of devices and applications, by which we could depict the distribution trend of the Internet devices and applications. In the end of the paper, we verified the procedure by measuring three different Internet devices and applications, and detected their distribution and depict the distribution trend chart. Our method can help the administrators understand the situation of Internet devices and applications effectively, find vulnerability and repair them in time.

Introduction

With the rapid development of network technique, the information techniques, especially the Internet have changed people's work and life a lot. As a great invention of human beings, Internet also helps people change and adapt the world.

According to the 38th China Internet network development state statistical report [1], as of June 2016, the number of Chinese netizen has up to 710 million people. The tentacles of the Internet have extended to the work, study and all aspects of netizen's life. However, from Internet development initial period, network security problem has not been received enough attention[2].

Network threat changes rapidly with the development of network technology. Although the defense technology also improves quickly, the network threat still exists. Besides, the information postponement of network administrators also leads to the never-ending battle between defense technology and security threat. According to the statistical report published by Symantec in 2016[3], 1 new "zero-day" is found each week in 2015, and three quarters of the commonly used web sites have significant security hole. The great success of Internet depends on the sharing of internet information, which relies on the openness of network devices, leading to the network threat. The attackers attack network equipment by the behavior of penetration, tampering and forging, and then access to equipment control power and cheat web visitors[4].

In recent years, people have realized install the patch to known vulnerabilities in time can reduce the possibility of network devices being attacked[5]. However, the information postponement of network administrators will affect the response time of security patches. To solve the problem, many international scientific research institutions and universities all establish network measurement systems [6], which can detect the distribution of the device when it exists potential safety hazard, and inform network administrators timely to reduce the network attack effectively and protect the interests of Internet users. Another classic example is that Dr. Paxson does research on network measurement by the behavior feature of routes[7].

Meanwhile, normal behavior and malicious behavior can be differentiated by analyzing the flow of network devices[8], which can reduce the risk of network devices being attacked and protect the rights and interests of Internet users.

Network administrators should be warned beforehand and install patches of vulnerabilities timely to reduce the possibility of network devices being attacked and the reduce losses[9], which make the measurement of network device be an urgent problem.

Although domestic and overseas researchers have an extensive study on the measurement of Internet devices and applications, little organizations or institutions can provide the accurate and wide distribution range of devices and applications, and inform network administrators patch vulnerabilities and prevent invasion.

In this paper, we adopt the way combined active detection and passive monitoring to detect the Internet devices and applications, and do statistical analysis about their distribution. Through the analysis in terms of collected data, the IP address and geographical location of devices and application who have vulnerabilities can be located, which is shown by situation map. Our work can help network administrators improve their work efficiency to patch vulnerabilities of devices and application specifically.

Research Background

Due to historical reasons, the measurement of network device and application have not received enough attention. Recently, new devices and applications appear constantly with the development of Internet. Many research institutions and companies begin to design tools to monitor and detect network devices and applications[6], by which, the distribution of network devices and application can be obtained and the flow of possible similar malicious behaviors can be found.

Insecurity of Internet environment has inspired people to study the protection technology of network security extensively [10]. As an effective network security technology, the measurement of network device and application get more and more attention. The distribution of security vulnerability can be measured by transpositonal consideration to solve the network security issues.

At present, there are related research topic or project hold by many international organizations and universities. They established the detection system of multiple network devices and applications to detect and analyze the distribution of network devices and applications on a global scale.

Dan Farmer and Weitse Venema firstly put forward the thought of network security scan by imitating attack methods of invaders in 1995[11], which can evaluate the security of network devices and applications from the view of attackers. They developed the SATAN scan tool, a port scanning program under Linux, to help network administrators understand how the attackers invade system and ensure the safety of the system.

CVE(Common Vulnerabilities& Exposures) and CNVD(China National Vulnerability Database) are methods of network measurement based on the vulnerability platform, which is similar to a dictionary, providing a public name for the security vulnerabilities had been widely accepted and weaknesses had been exposed. They use public serial number of CVE/CNVD, and can share data in all kinds of vulnerability databases and vulnerability assessment tools. CVE and CNVD are also called keywords of sharing security information. The related repair information and security patches can be found by browsing the CVE/CNVD compatible database[17].

Although the vulnerability databases such as CVE and CNVD helps a lot, network administrators need take manual query to confirm the vulnerability, leading to the lag of information.

Nmap, developed by Fyodor, is an open source network detection and port scanner tool advised and revised by hundreds people. Its design purpose is scanning large - scale networks quickly. Nmap can be used to detect the operation system(OS) type of destination host and services, as well as the port status[13]. What’s more, the network scanner-Zmap, designed by researchers of the university of Michigan leaded by Durumeric[14], can make a common server scan every address of Internet with 44 minutes.But Nmap and Zmap can’t identify the types of the network devices, and infer which devices have vulnerability according to the scan results. They only detect the application and service version, but can’t warn network administrator in time. Besides, Zmap improve the single time of scanning whole network, but it occupies all the upstream bandwidth of scan server every time, and can’t update scan results timely so that information also has a certain lag.

Domestic and international scholars have extensive study on the measurement of network device and application, but little organizations or institutions can provide the accurate and wide distribution range of devices and applications, and remind network administrators to fix vulnerabilities and prevent intrusion from the perspective of a third party. By the method combined active detection and passive monitoring, the distribution of devices and applications of whole network can be measured, whose network administrators can be informed to reduce the network security incidents effectively and do a better job of network security protection.

The Measurement Method of Internet Devices and Applications

Theory of Network Measurement

The complete network measurement can be divided into 4 steps. Step 1: Host or network discovery. Step 2: Collect the information of target host, including the device model, OS, running applications and services. Step 3: Judge target host has vulnerability or not. Step 4: Obtain the information of device and application and discover the malicious behavior by the passive monitoring of the mark device and application.

Host or Network Discovery

The first step of the networkmeasurement task is shrinking the range of a set of IPto a group of active or interested host[15]. Traversing each port of every IP is a difficult and time-consuming task, requiring enormous resources, which is usually unnecessary.

By host discovery, the offline hosts can be excluded effectively, thus specific detection missions can be executed in terms of online hosts to save resources. Host discovery usually achieve by ping. We can judge the host online or not by the returned code according to the ICMPcommunication channel. Malicious attackers can invade target hostsor devices by port. Meanwhile, network administrators can detect the distribution of network device and application by port. By port scanning, if there are returned messages, no matter what kind of information, the host can be judged as online, which can be also used to discover host.

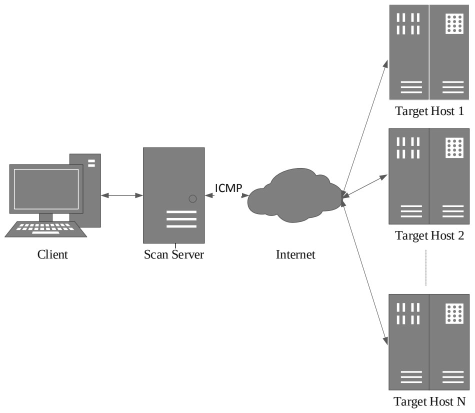

Figure1 The schematic diagram of host discovery and port scanning

Services and Applications Detection

The active hosts and open ports of target network can be ensured by the host discovery and port scanning in step 1, by which we can conduct the services and Applications detection of step 2. It can be concretely divided into OS detection, device models detection and service and version detection.

Network vulnerability is usually related to operation system. Thus, it is the priority task for malicious attackers to detect the OS of devices and applications. Identifying the type of OS also can help network administrators classify, prevent and fix vulnerabilities.

Some specific vulnerabilities are also related to the device model number. Only devices with the certain model number would have vulnerabilities. By detecting device model number, the vulnerable device can be found timely, and then help network administrators fix vulnerabilities purposively. For example, the upgrade patch can be downloaded from the official website.

There are a wide variety of web servers on Internet. The site operation and running of network application are mostly based on client / server model. If a network application has vulnerabilities, attackers will permeate by the port of application, and invade network devices bearing web services, and even obtain the permissionofnetworkdevice. Detecting the type and version of service can help network administrators fix bug on application layer to reduce the risk of network devices being compromised.

Vulnerability Detection

Vulnerability is a shortcoming caused by the error of security policy of hardware or software. Malicious attackers can take advantage of those vulnerabilities accessing the system without permission or damaging the system. Vulnerability detection is a method to detect the vulnerabilities of remote or local host automatically. Now, there are mainly two kinds methods.

1) Open ports and frequently-used services of target host can be get by port scanning. Vulnerabilities can be found by detecting the version of those services, and match the information with the network vulnerability database, such as CVE and CNVD.
2) Offensive vulnerability detection can be done on target host through imitating malicious behavior. If there is a successful attack, it represents the network device or application have vulnerability.

Vulnerability detection can help network administrators accurately identify whether the network device or application have vulnerability or not, and then fix bug purposively.

Passive Monitor

Passive monitor means that capture packets of cyberspace and have a global third-party monitoring on the packets of target device and application to detect distribution of devices and applications timely and find malicious behavior[16]. Packets monitor system is used by passive monitor, which is deployed on theinternetgatewayofa company.

First, a local experimental platform is set up to do the local packets analysis on target device and application. What' more, simulated attack is conducted on the vulnerable devices and applications. Analyze the initiative behavior of target device and application, traffic behavior and packets of exploiting process of vulnerabilities. Then, feature rules can be extracted and accurate features should be found.

According to the feature rules, monitoring the network traffic by means of packetsmonitorsystem and capturing specific behavior of network traffic can contribute to identifying the information of the devices and applications that send packets proactively, and detecting malicious behavior, as well as tracing malicious attackers.

Passive monitor is also conducive to set filtering rules and avoid attacks once more, which is helpful for judicial process by preserving evidence.

The Measurement of Internet Devices and Applications

Combining with the above discussion of detection technologies about network device and application, we design a detection process of network device and application according to the functional requirement of network device and application detection. It aims to detect the device model and service version of network device, which design thought is shown as follow.

1) The process realizes 6 main function modules, including port scanning, device model and service version detection, vulnerability detection andpassive monitor, as well as module of devices and applications vulnerability verification and presentation module for showing the scan results.
2) The main function modules are independent of each other. The results are

outputted to a database for comprehensive analysis

3) The port scanning module detects target network with the help of Zmap, and find a set of target host with open ports.

4) Devicemodelandserviceversiondetection can be used to detect the model number and service version of device by sending the pre-edit packets.

5) Vulnerability detection detects whether target host has vulnerability or not by analyzing local traffic feature and sending packets.

6) Passive monitor can capture packets and analyze the information of the header of packets through extracting feature rules. It is also used to detect device and application, and trace malicious attackers. The packet capture device used by passive monitor module is deployed on the internet gateway of a company.

7) We compare and combine the process design of measurement of network device and application, and trace malicious attackers. The packet capture device used by passive monitor module is deployed on the internet gateway of a company.

8) We draw the scan results into situation map in data presentation module, which can show the distribution area clearly and then help network administrators manage network devices and applications.

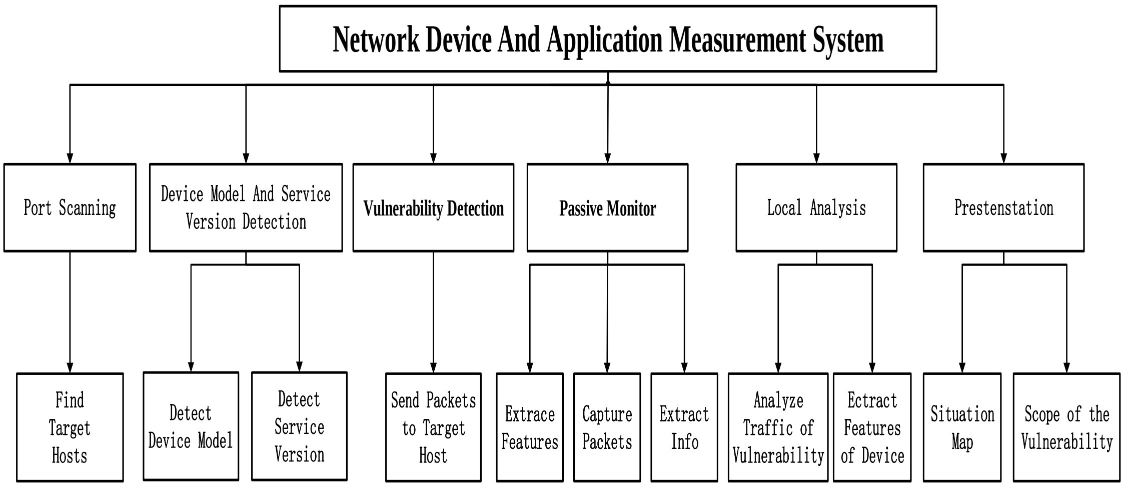
Network Device And Application Measurement System
Port Scanning
Device Model And Service Version Detection
Vulnerability Detection
Passive Monitor
Local Analysis
Prestenstation
Find Target Hosts
Detect Device Model
Detect Service Version
Send Packets to Target Host
Extrace Features
Capture Packets
Extract Info
Analyze Traffic of Vulnerability
Ectract Features of Device
Situation Map
Scope of the Vulnerability

Figure 2. The module design of network measurement

A complete scan task or detection task includes the follow steps. The process design is shown in Figure 3, including the process of active detection and passive monitoring.

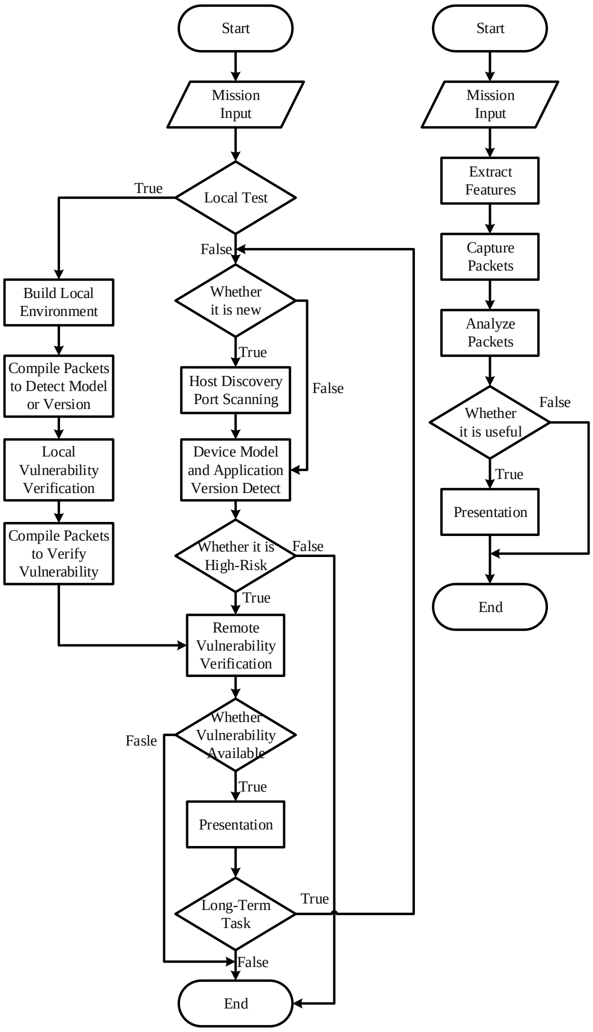

Figure 3. The process design of network measurement

1) Initiate task. Upload the libraries of each module and obtain the basic information of each module.

2) Judge task. If this is the first time to perform a task, then the host discovery or port scanning is needed. We output the scan results into database by means of Zmap. If not, calling Zmap is not need.

3) Analyze the local devices or applications in a simulation environment, and compile the detection packet of device model or application version. Then, the exploit way of vulnerability can be found by analyzing the local vulnerability.

4) For a particular device or service, send the probe packets compiled by step 3 to target device. The device model number and service version can be analyzed by the returned packet, and then the result is stored into database.

5) For target version of high risk vulnerabilities, the exploit way obtained by step 3 is used to vulnerability validation detection. If the exploit way can be used successfully, it means vulnerability is available. Otherwise, there is vulnerability, and store the result in to database.

6) Read the target device or service data from database, and generate distribution diagram to show the result.

7) For the long-term task, data should update and get result termly.

8) For the task needed passive monitoring, extract packet feature and capture packet. After analyzing, we can get the target device or application data and store it into database.
9) Read the target device or service data from database, and generate distribution diagram to show the result.
10) Release all resources and finish.

Experiment

We do experiment of network measurement process validation on 3 vulnerabilities in the CNVD vulnerability library –The "Suspected Backdoor" Program of Netcore Whole Series Routers (CNVD-2015-07800), Oralce Weblogic Server Remote Code Execution Vulnerability(CNVD-2015-07707) and Baidu-Router(Ai-BR100). The results of the measurement are analyzed as follow.

Netcore Whole Series Routers "Suspected Backdoor"

Netcore is a network communication manufacturer whose products mainly involve wireless router, wireless LAN, network interface cards, hubs, switches, broadband routers and other network devices.

On March 19, 2015, the vulnerability numbered CNVD-2015-07800 of CNVD pointed out a program called IGMPT was built in Netcore whole series router, which isdescribed as IGD MPT Interface daemon 1.0. The program will start automatically with the router. And the port 53413 of UDP was opened to public Internet. An attacker can use the program to execute arbitrary system commands, upload and download files without authorization.

Our purpose is detecting the household devices of available backdoors in nationwide network. We use test device- Netcore NW774 to do the local analysis, and find this device make the UDPport

53413 opened by default. By capturing packets, we find that sending the UDP data including the string of *'pa' + '\x00\x00' + 'word' + 'netcore'* can activate the state of backdoorat the beginning of exploitation of vulnerability. Besides, backdoor can support remote to execute MPT command. Thus, we compile the packets including the specific string and command to verify the vulnerability

Up to 0:00 Jan 1, 2016, we learned from the measurement results of Netcore router innational scale that 11363 Netcore devices had the vulnerability triggered by the available backdoor- IGD MPT Interface daemon 1.0 in China's public IP cyberspace. The situation map of Netcore device is shown in Figure 4, which can be seen that there were a lot of devices (2283 devices) without installing patches in Shandong. Besides, Hebei and Liaoning also have many Netcore devices without fixing bug.

Oracle Weblogic Server Remote Code Execution Vulnerability

Oracle Weblogic Server is an application server which can apply to cloud or traditional environment. It provides a light development platform to support the lifecycle management of application from development to production and simplify the deployment and management of application. WLS security is one of security components.

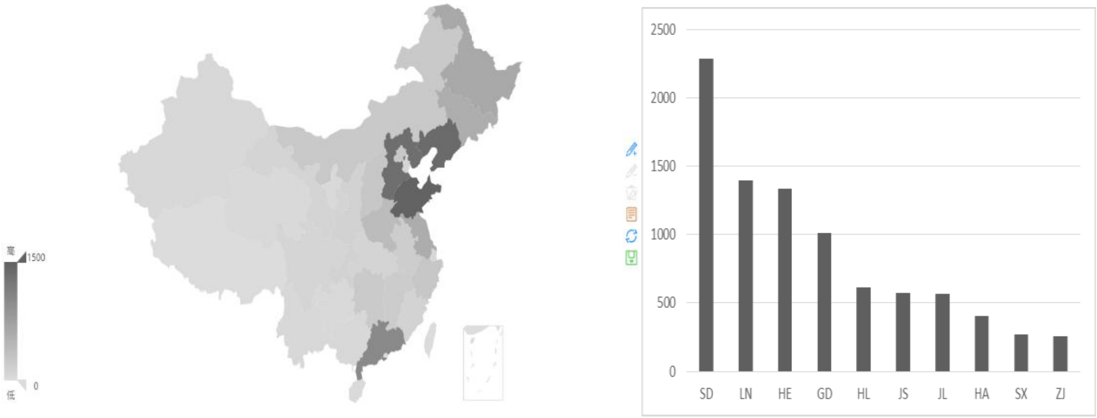

Figure 4. The situation map of Netcore vulnerability distribution

We can find from the CNVD numbered CNVD-2015-07707 on Nov 23th, 2015, the WLS security components exists security vulnerability. The remote attacker can send the serializable Java objects to T3 protocol of 7001 port, and execute arbitrary commands taking advantage of the vulnerability.

The purpose of this part of the experiment is detecting the distribution state of available Weblogic Server remote code execution vulnerability.

We build the virtual environment (Ubuntu 14.04, Weblogic Server 10.3.2) to analyze the remote code execution vulnerability, and capture packets to analyze the traffic. Weblogic Server applies the T3 protocol of TCP protocol to exchange data, which can receive the serializable Java objects and do the deserialization for objects on the server. The deserialization of apache commons collections library used by server doesn’t check the serializable objects.Thus, we can execute command by remotely calling *Runtime* class and reflectively calling *getMethod* clsss. So we can check the availability of vulnerability by compiling the specific Java class and deserialize it to target host.

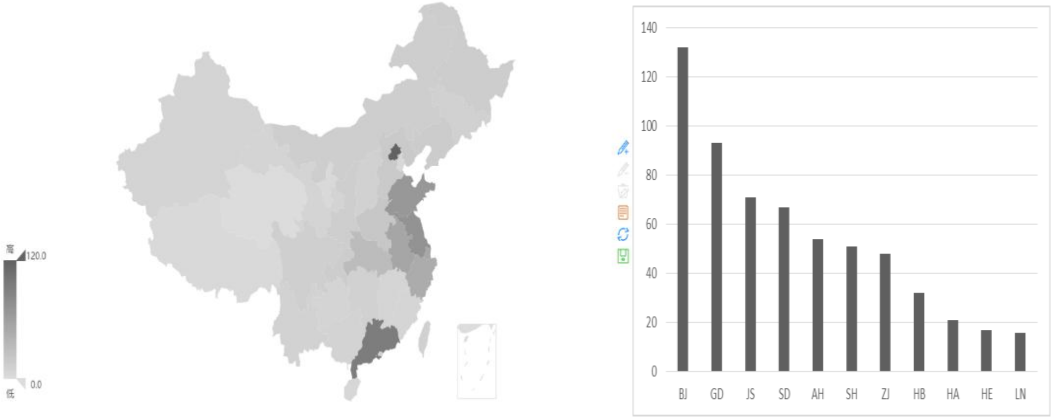

Figure 5. The situation map of Weblogic Server vulnerability distribution

The situation map of weblogic server vulnerability is shown in Figure 5. By analyzing the scan results, we can see that 785 running weblogic servers have deserialization vulnerability of remote code execution vulnerability, spreading a number of versions. There are 132servers in Beijing, which is the severely afflicted area ofsecurity vulnerability.

Baidu-Router(Ai-BR100)

Baidu-Router(Ai-BR100) is a smart router product released by Baidu, which can transfer cloud data optionally and remotely download video resources. It also can achieve remoting control devices by Baidu account bound with devices.

Baidu-Router is produced by Baidu and Aigale with the product model of Ai-BR100.The purpose of this experiment is detecting the alive Baidu-Router devices and describe the situation map.

We design the local test by means of device Ai-BR100 and capture packet. The analysis results are described as follow.

1) The router will send POST request to domain device.baidu.com and request to register device when it turns on., by which can bound with servers of Baidu and achieve the function of remote control. The packet includes the information of device model and system version.
2) The router will send POST request periodically to domain x.baidu.com to request to update device firmware. The packet also includes the information of device model and system version. If the device firmware is newest, then the error code 304 is returned.

Therefore, the feature of packets of register and update can be used to passive monitoring, monitoring the alive Ai-BR100 router and drawing the situation map.

Figure 6 shows the distribution of Baidu Ai-BR100 in china. 28 Baidu routers (Ai-BR100) are found in Taiwan, which is largest in all provinces, while 24 Baidu routers are detected in Beijing.

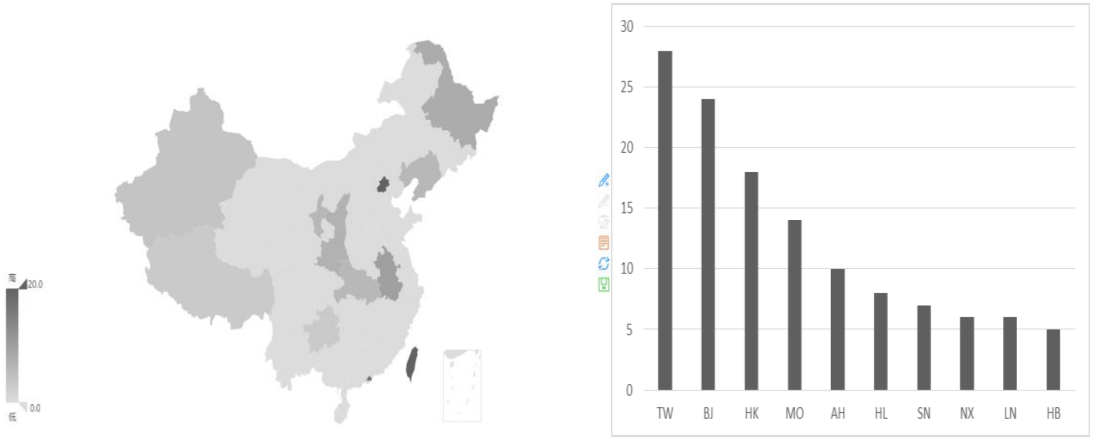

Figure 6. The situation map of Weblogic Server vulnerability distribution

Conclusion

In this paper, we put forward a measurement method combined active detection and passive monitoring to detect the Internet devices and applications, and the results are shown by situation map.

The validity of the method to Internet devices and applications is verified by 3 experiments. Compared with simple vulnerability publishing platform, such as CVE, our method can locate devices and applications accurately. Compared with the Internet survey technology, such as Nmap, the method can eliminate invalid scan results by matching feature to reduce false alarm rate.

Compared with the previous research methods, our method can solve the trouble of information lag for network administrator effectively. The situation map can help network administrator monitor vulnerable devices and applications and find malicious traffic, which will make the traceability of malicious behavior stronger.

The purpose of this study is measuring the Internet device and application, and draw the situation map according to the scan results. However, because of the limitation of system we adopted, the data used by passive monitoring is not covering the entire cyberspace, so that the result of passive monitoring may in disparity with the real result. In the future research, we will improve the integrity of result on the basis of validity.

References

[1] 38th China Internet network development state statistical report. CNNIC. 2016

[2] Householder, A., Houle, K., & Dougherty, C. Computer attack trends challenge internet security. Computer, 2002,35(4), 5-7.

[3] Internet security threat report. Symantec. 2016

[4] Kang Xiaolong. Research of Network Attack and Security Detection Technology by the Means of Attack.In Chinese. Xidian University, 2005

[5] Qin Sihan. Network attack and defense technology theory and actual combat.In Chinese. Science press, 2004

[6] Tan Jie, Li xing. Network measurement review.In Chinese. Application Research of Computers, 2006, 23(2):5-8.

[7] Paxson V E. Measurements and Analysis of End-to-End Internet Dynamics[J]. Office of Scientific & Technical Information Technical Reports, 1997, 31(4):373-374.

[8] He Changlin, Dang Xiaochao. Network measurement and flow gathering technology review.In Chinese. Computer Era, 2011(7):14-15.

[9] Li Xiaohui, Zhang Xihong. Network Port Scanning and Vulnerability Detection Research. Journal of Ordnance Engineering College, 2003, 15(1):46-49.

[10]An Luping. Computer Network Security Protection Technology. Heilongjiang Science and Technology Information.In Chinese, 2009(36):112-112.

[11]Ram P, Rand D K. Satan: Double-Edged Sword[J]. Computer, 1995, 28(6):82-83.

[12]Dan F, Venema W, Dan F, et al. System Administrator Tool for Analyzing Networks Security Administrator Tool for Analyzing Networks[J]. Tract, 2011.

[13]Lyon G F. Nmap Network Scanning: The Official Nmap sProject Guide to Network Discovery and Security Scanning[J]. Insecure, 2009.

[14] Wiemer S, Zúñiga F R. A Software Package to Analyze Seismicity: ZMAP[J]. Seismological Research Letters, 1994, 72(3):373-382.

[15] Tang hong et al. IP Network Measurement.In Chinese. Science Press, 2009.

[16] Wang Haitao, Fu Ying. Network Measurement Method and Key Technology.In Chinese. Telecom Engineering Technics and Standardization, 2010, 23(07).

[17] Wang Shun. Web vulnerability scanning and infiltration attack tools.In Chinese. Tsinghua University Press, 2016.