Design and Implementation of a High Performance Network Scanning System for Vxworks Hosts

Minlei Zhang*, Yancang Chen, Huan Chen, Yaxin Zhao, Pei Wei and Sai Sui
Luoyang Electronic Equipment Test Center, Luoyang, China
*Corresponding author

***Abstract*—Host scanning is an important technique for vulnerability mining and penetration testing, which is crucial to analyzing the safety of information system. Through the research into developed scanning systems both at home and abroad, such as Shodan, Zoomeye etc., this essay proposes a design model of a rapid scanning system for all Vxworks hosts based on Vxworks' own characteristics. On the basis of digitalization and Internet, the model aims to scan the operating system versions, available services, open ports and location, etc. of all Vxworks hosts. The model in this essay combines Zmap and Nmap, thus it can ensure the rapidity as well as accuracy of scanning. The model is fully automatic and timely updates the information of Vxworks hosts, it also supplies humanized management interface and elaborate scan report. Moreover, this essay provides method of software implementation.**

Keywords-host scanning; Vxworks; Zmap; Nmap

I. INTRODUCTION

Vxworks is an embedded real-time operating system developed by American Wind River Company. Because of its excellent reliability and outstanding real time, it has been widely applied to many fields requiring highly sophisticated technology and advanced real time, such as communication, military, aviation and spaceflight. Wind River declares that at least 1.5 billion devices utilize Vxworks. The devices have a high risk of being attacked, so the security of Vxworks arises high attention. Mainly employed in embedded fields, if the system is not updated in time, hackers can make use of Vxworks' defect and the known vulnerability of various software within Vxworks, to attack systems. The result can be catastrophic. If the known vulnerability of Vxworks and its software can be detected in advance, the risk of being attacked by hackers would be immensely reduced. Host scanning as an important technique for vulnerability mining and penetration testing, it is very effective in detecting known vulnerability and penetration testing unknown vulnerability, serving as a good resolution to the problem.

II. RELEVANT WORK

Even though there is plenty of domestic and international research into host scanning, formed products are few, among which the international representative of the products is Shodan [1] [2] [3] [4], while the domestic one is Zoomeye. Below is their detailed introduction, respectively.

A. Shodan

Shodan is applied to search all online hosts on the Internet, as a search engine assisting in detecting vulnerability of Internet system. In security field, Shodan is called "dark" Google. Shodan's server ceaselessly collects information of online devices[1], such as servers, cameras, printers, routers, switches and etc.. Even though Google has been viewed as the most powerful search engine, Shodan actually is the most frightening[2]. The differences between Google and Shodan: Google uses Web crawlers[5] to collect data online and indexes downloaded pages, so that users can search efficiently; Shodan searches for hosts and ports and acquires the intercepted information, then indexing them. Shodan's truly startling power is that it can find almost all the devices connected to the Internet. Yet it is supposed to reflect on the security since most devices connected to the Internet are not installed with preventive systems and even have security vulnerability.

B. Zoomeye

Zoomeye, namely, "Eye of Zhong Kui" in Chinese, is a search engine for cyberspace, powered by Knownsec, Inc. It is a powerful searching tool for security testing. This search engine is able to conduct a comprehensive search into all host devices and Web components connected to the Internet, and further to find the potential known and unknown vulnerability within the devices and components. Zoomeye is as powerful as Shodan in terms of host search engine, and its many functions of searching hosts are borrowed from Shodan. Nevertheless, Zoomeye is different from Shodan owing to the former's power of searching for Web components, the theory of which is similar to Google, viz., Web crawlers. Now many of hackers' attack aims at Web components, so that once the flaw of some Web component is found, all websites with the same kind web component would be hacked. Hosts and Web components comprise Zoomeye's cyberspace; thus Zoomeye is designed for constantly collecting information of fingerprints[6] within its cyberspace and opening search engine, as well as further promoting the development of global Internet security.

III. DESIGN

This chapter will first elaborate the design of host scanning model and then will present database of this system in a detailed way.

A. Design of Host Scanning Model

The model mainly contains three modules: hosts scanning, data analysis and Web management system. Functional structure of host scanning system is shown in Figure I, system's comprehensive structure is shown in Figure II.

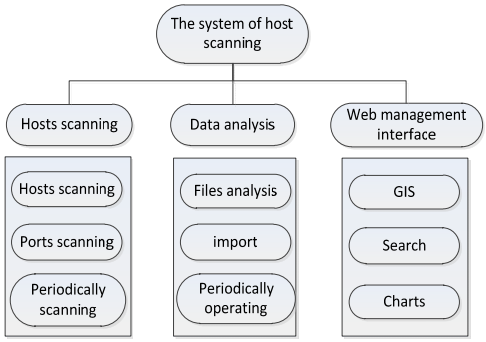

FIGURE I. FUNCTIONAL STRUCTURE

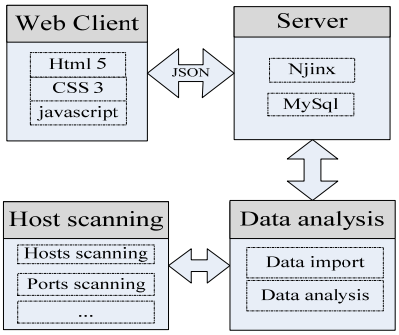

FIGURE II. MODEL'S COMPREHENSIVE STRUCTURE

1) Hosts scanning: it realizes scanning Vxworks hosts, a rapid and accurate scanning of host ports; there are three methods, Nmap scanning, Zmap scanning and self-developed exclusive tool scanning; the format of scanning is periodic, centralized and multi-threaded.

2) Data analysis: analyzing the data of host scanning and put them in storage.

3) Web management system:

Analysis, management and graphic display of the acquired information of Vxworks hosts; friendly human-computer interaction and convenience for users to analyze and manage. Web management system employs B/S (Browser/Server) mode. With the popularity of Internet technology, more and more application use B/S mode. B/S mode unifies the client and concentrates the central part of realizing system's functions on the server; it simplifies the system's development, maintenance and usage. B/S mode has the advantages of simple maintenance and upgrade, low cost and more choice.

B. Design of Database

The system's database uses MySQL. Based on the system's requirement analysis, the service logic can be abstracted into three entity charts. According to functions of the whole host scanning system, they can be divided into the following parts.

1) User model

User model is a User chart, containing the detailed information of administrators. It is mainly used for login and authentication. User chart is mainly for the storage of administrators' accounts' login names and codes. Web management system only accepts administrators' accounts.

2) Host model

Host model contains two charts of hosts and ports. Hosts and ports form a many-to-many relationship. Host chart is a data chart, for storage of the scanned data of Vxworks hosts, including id, IP of hosts, operation system, the version of operation system, hosts' location—country, longitude and latitude, the latest time of scanning this host, the condition of the host as well as the information of the port. Port chart contains information of all scanned ports, including id, ports, names of ports, and description of ports.

IV. IMPLEMENTATION

The last chapter detailedly introduces the design of host scanning model, in this chapter, the implementation of host scanning model will be demonstrated.

A. Host Scanning

This section will first briefly introduce the theory of host scanning and then elaborate the realization process of host scanning in a detailed way.

1) Theory of host scanning

Host scanning means seeking for the existing hosts and their related information. The method is to send probe packets to hosts and to monitor their acknowledgement packets. If the protocol packet could be compared to a package in the post office, then scanning a host is to send a package to the IP address of this host. No matter whether it is delivered successfully, the post office will inform you. Based on the acknowledgement packet and fingerprint[7] database, information about the other's about port, version, operation system would be figured out. Thus, Through constructing abundant different types of protocol packets, different information will be obtained. The host scanning system in this essay includes four basic procedures.

a) Hosts discovery

Hosts discovery refers to discovering whether the target host is turned on or not. The theory of hosts discovery is similar to that of ping command: sending testing packet to the target host, if receiving acknowledgement, then the target host is turned on. For instance, the host scanner located at IP address 192.168.1.100 sends ICMP echo request to the target host 192.168.1.101, if the request message is successfully delivered to the target host without being intercepted midway by the firewall, then the target host will inevitably respond ICMP echo reply packet.

b) Port scanning

Port scanning is applied to ensure the open state of the target host's TCP/UDP port. By default, it needs to scan the most possibly open TCP/UDP port. The theory of port scanning is similar to that of hosts discovery: sending testing packet to the target host's particular port, if receiving acknowledgement, then the port is open. Take TCP/SYN port scanning as an example, the scanner sends SYN to the target host's port: if the scanner receive the acknowledgement of SYN/ACK, then the port is judged as open; if it receives RST packet, then the port is closed; if it receives no answer, then the port is filtered, which means the state of the port is unclear and needs other scanning methods to further ensure its state.

c) Version detection

Version detection is to detect the detailed service and version information operating at the open ports of the target host. Firstly, construct port-scanning lists according to the port scanning results, only including "open" and "open/filtered" ports. Take TCP port as an example, try establishing TCP connections and waiting for a while; the scanner will receive "Welcome Banner" sent by the target host, and then compare the received Banner with the signature stored in the database, to locate the name and version information of the corresponding service.

d) Operating system detection

Operating system detection is responsible for confirm the device type of the target host as well its operating system. Usually, the usage of TCP/ IP protocol fingerprinting helps decide accurately the type of the operating system. In RFC, some situations do not strictly regulate the realization of TCP/ IP; therefore, different TCP/ IP protocols have their own special features. According to these differences in details, the types of the operating systems. Usually, the scanning tools send different types of testing signals to the hosts, and narrow down the search range of the operating systems.

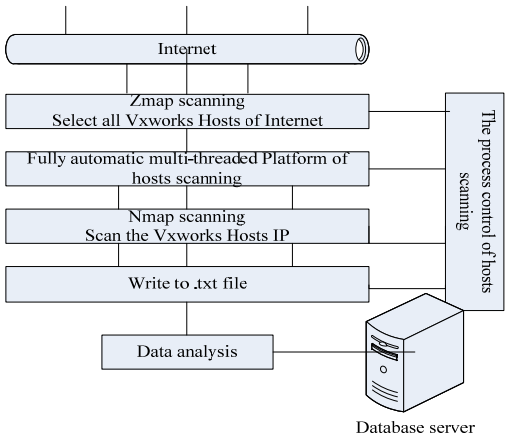

FIGURE III. IMPLEMENTATION OF HOSTS SCANNING

2) Implementation of host scanning

The process of realizing hosts scanning is shown in Figure III. There are many developed scanning softwares, such as Zmap[8][9], Nmap, Nessus etc. Zmap is characteristically rapid. It is able to scan the whole Internet within one hour[9], but the result is not accurate and detailed enough. In contrast, the scanning result of Nmap[10] is very detailed, but it is neither fast nor multi-threaded. Nessus primarily focuses on scanning systems' vulnerability and does not involve ports or hosts. According to the characteristics of Zmap and Nmap, this design makes best use of their advantages and avoids their disadvantages: firstly, use Zmap to select all Vxworks hosts of internet; then through self-developed centralized and multi-threaded Nmap scanning platform, all Vxworks hosts are to be scanned for the second time. Accordingly, both the accuracy and efficiency of the scanning result are assured.

B. Data Analysis

The data analysis module of this design is responsible for analyzing and denoising data in text format from the host-scanning platform, as well as their storage and management. It ultimately realizes managing the database of all Vxworks hosts on Internet. Because the system is fully automatic, the host-scanning platform will scan periodically all Vxworks hosts; then the data analysis module will need to deal with the scanning result regularly and update the database. In the data analysis module, the scanning result will first be analyzed and then denoised (namely, remove error data), and further decided whether they are in the database or: if they are not in the database, they will be inserted into the database, if yes, further decided whether they are changed or: if the data be changed and then it should be updated, if not, then abandon them.

C. UI Realization

The Web management system is based on Bootstrap, Django and MySQL. The system's front-end employs the current most popular open-source framework of front-end Bootstrap, and the back-end uses the latest Django, and its database is MySQL database.

Compared with the ordinary MVC development framework, Django is slightly different since it uses MTV development framework. M refers to Model, which is responsible for the input and output of data. T is Template, which usually refers to some specially formatted HTML texts, supporting simple logical structure. V means View. Django's View not only needs to provide views, but also plenty logical process, whose function is similar to that of the control layer of the traditional MVC development framework. The system's background processing is shown in Figure IV.

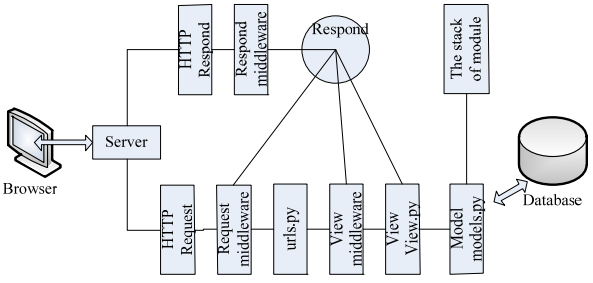

FIGURE IV. THE DEAL PROCESS OF SERVER

Based on the map display interface, the realization result is shown in Figure V. The distribution information of hosts is shown on 3D globe. If one area or country on 3D globe is selected, the detailed distribution information of hosts in this area or country will be displayed on the right side of this interface. 3D globe and map employ ECharts plug-in, which is a chart library with only Javascript. ECharts plug-in can operates fluently in PCs and mobile devices, and is compatible with almost all browsers (IE8/9/10/11, Chrome, Firefox, Safari, etc.). It is dependent on the Canvas class library, ZRender. It can provide data visualization diagrams, direct, vivid, interactive and highly individual and customizable.

FIGURE V. BASED ON THE MAP DISPLAY INTERFACE

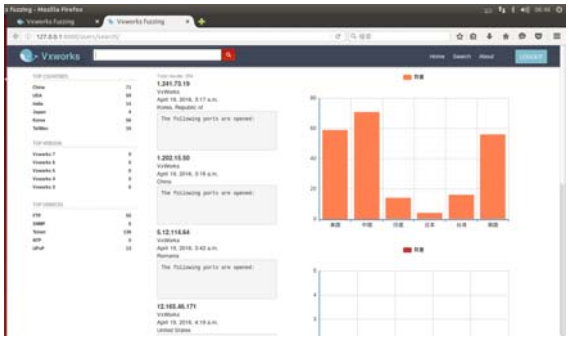

FIGURE VI. THE DISPLAY OF SEARCH REASULT

As shown in Figure VI, the system realizes the conditional query of Vxworks hosts. The query criteria include country, version of Vxworks, open services of hosts. On the left side of the interface is the statistical information of query, in the middle is the list of the query result, and on the right side is the diagram of the query result. For instance, querying hosts in America: “country: usa”; querying Vxworks hosts of version 5.0: “version: 5”; querying hosts operating ftp service: “service: ftp”.

V. CONCLUSION

The Host scanning as an active discovery technology of information security, plays a crucial role in strengthening the security of devices and Internet. This essay presents a comprehensive design, which, through host scanning system, aims to scan all Vxworks hosts on Internet in a rapid, accurate and efficient way with database management of the scanning results. In this way it will provide users with humanistic management interface and diversified analysis report. The essay also promotes the realization methods in terms of software. The system has several evident characteristics as follows.

- The design thought is constructional. Software’s structure is strictly in accordance with module in development, which possesses excellent extensibility.
- The combination between Zmap and Nmap, along with multi-threaded method of scanning, ensures both the accuracy and the efficiency of scanning result.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (Grant No. 61303061) and State Key Laboratory of high performance computing (Grant No.201513-01).

REFERENCES

[1] Roland C. Bodenheim. Impact of the Shodan computer search engine on Internet-facing Industrial Control System devices. Master's thesis, Air Force Institute of Technology, Wright-Patterson AFB OH, USA, March 2014 (ADA601219).

[2] Bodenheim, R., Butts, J., Dunlap, S., and Mullins, B. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection. vol. 7, no. 2, pp. 114-123, 2014.

[3] B. Genge and C. Enachescu, Shovat: Shodan-based vulnerability assessment tool for Internet-facing services, Security Comm. Networks, 2015.

[4] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by Internet-wide scanning. In 22nd ACM Conference on Computer and Communications Security, Oct. 2015.

[5] Shkapenyuk V, Suel T. Design and implementation of a high-performance distributed web crawler. IEEE International Conference on Data Engineering (ICDE), 2002. IEEE Computer Society, 2002.

[6] M. Mulazzani, P. Reschl, M. Huber, M. Leithner, S. Schrittwieser, and E. Weippl. Fast and reliable browser identification with javascript engine fingerprinting. In Web 2.0 Workshop on Security and Privacy (W2SP), May 2013.

[7] Z. Shamsi, A. Nandwani, D. Leonard, and D. Loguinov, Hershel: Single-Packet OS Fingerprinting. in Proc. ACM SIGMETRICS, Jun. 2014, pp. 195–206.

[8] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-wide scanning and its security applications. In Proc. 22nd USENIX Security Symposium, Aug. 2013.

[9] D. Adrian, Z. Durumeric, G. Singh, and J. A. Halderman. Zippier ZMap: Internet-wide scanning at 10 Gbps. In 8th USENIX Workshop on Offensive Technologies, Aug. 2014.

[10] G. F. Lyon. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure, USA, 2009.