Design and Implementation of Vulnerability Detection Tool Based on Port Service Information

Wanggen Xie[1], Xiaoli Wang[2], Rong Fan[2], Haibo Chen[2]
[1]*(Informatization department (Center), Jiangsu University, Zhenjiang, 212013, China)*
[2]*(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, 212013, China)*

Abstract: *With the prosperous development of the Internet, cyber-attacks against web application vulnerability have also emerged. At the same time, different scanners have grown rapidly to make web service more secure, such as NMAP, Hydra, etc. Most of them only achieve few specific functions without information collection. This brings inconvenience to vulnerability detection, because the frequent switching of tools may be time-consuming and error-prone. To assist developers in better vulnerability detecting. In this paper, an automatic vulnerability scanner based on port service information is proposed. Through the experimental results, the tool presents satisfying effects by implementing the combination of port scanning, weak password blasting and directory detection, also indicates great potential for the extensibility.*

Key Word: *Web Security, Information Collection, Port Scanning, Password detection, Directory scanning*

Date of Submission: 11-12-2020 Date of Acceptance: 26-12-2020

I. Introduction

Web service reliability is an important mission that keeps web services running normally, and has been widely adopted in various fields, such as data processing, artificial intelligence and e-commerce [1]. However, it is hard to ensure the absolute security of web due to the open ports which may provide potential invasion opportunity to attackers, many malicious attackers infiltrate the target system and perform wicked operations through security vulnerability, which pose great potential threats to web security [2].

In general, the security issues of web are complex and challenging [4]. Cyber world is facing diverse severe challenges, and wicked invasions emerge endlessly, for example, intruders attack servers maliciously, modify data arbitrarily and even damage systems and hardware through various means and technologies [4]. Although these problems have been reported for a long time, no radical solution is obtained. This highlights the importance of rigorous security testing to identify and fix vulnerability. Take corresponding measures to make defense is considered as a compulsory requirement.

In response to malicious operations in web security, the utilizing of penetration testing for vulnerability scanning attracts more attention [5]. Penetration testing, has been regarded as an efficient testing approach, whose purpose is to eliminate the potential vulnerability of web service by simulating malicious attacks. Typically in penetration testing, information collection is a vital process that need to be constructed in advance to ensure the effect of subsequent scanning, such as host scanning, port scanning and directory scanning etc. all serve as exceptionally critical roles in detecting web vulnerability.

Nowadays, several scanners have been developed to detect web vulnerability [6]. However, most of these tools only concentrated on a single function and carry out corresponding scanning independently, making the inspectors have to do some extra work for information collection to implement different functions, commonly it will increase the pressure of the researchers and time overhead [7]. To address such issues, in this paper, a vulnerability detection tool based on port service information is proposed, which may bring users more convenience. To be exact, this tool integrates three functional modules: port scanning, weak password blasting and directory detection. And it is proved by the experimental result that the scanner shows great efficiency and potential in implementing the integration of these three functions.

The structure of this paper can be summarized as follows, the first section describes the background and status quo of network security vulnerabilities while the second section introduces the implementation of technology and basic concepts related to this tool. We present the overall framework of the scanner in the third section. In the fourth section, the tool was introduced in detail including the specific modules. The fifth section shows the Experimental results and related analysis of the experiment process. Finally, the section 6 presents the conclusion.

II. Related Work

Various work has been done regarding the vulnerability scanning in order to provide high level of assurance. Generally, discovering open ports, identifying running services are the common operations. Only having mastered enough information about the target website or target host can we better detect its vulnerability. As for the scanner proposed in this paper, we mainly focus on port scanning, weak password blasting and directory detection. The working details of these three modules are described in the following paragraphs.

2.1 Penetration Testing

Penetration testing, also known as PT, which is the practice of testing computer systems, networks, or Web applications to discover security vulnerabilities that attackers may exploit [8]. Commonly, penetration test is to access sensitive data by simulating an unauthorized attack internally or externally. With the purpose of making these specific systems safer, by using the same tools and techniques as attackers, security issues can be identified, safeguards can be put in place before real hackers can exploit these vulnerabilities. The common testing process often needs to go through information collection, vulnerability scanning, and other stages. Information collection includes domain name information query, IP information query and open port query. Vulnerability scanning includes host scanning and Web scanning. As for penetration testing, it contains simulation of various vulnerabilities, such as weak password vulnerability, directory browsing vulnerability, SQL injection vulnerability, and so on.

2.2 Port Scan

A port is a potential communication channel. From the intruder's point of view, that is, a potential intrusion channel. In general, before a system attack or intrusion in a network, an attacker scans the network to investigate the vulnerabilities of the target system [9]. In particular, port scanning is a useful method to obtain information about the ports used by the target system, and it is crucial to quickly detect suspicious hosts and shut them off from the network in order to prevent further attacks or the spread of malware [10]. As such, defending against them has long been the subject of many researches and modeling efforts. Port scanning scans a section of the target host's port or any designated ports one by one to determine which ports of the target host are open [11]. Through the open port, we can find possible vulnerabilities in the target host and fix them to strengthen the security in time. The principle of scanning is that when a host wants to establish a connection request with the remote server , if the server has installed this service, it will reply, otherwise, it will give no response, Making use of this principle, if the connections between all known ports or some ports selected from a certain range of known ports are established respectively, recording the reply comes from the remote server , by looking at the record you can see which services are installed on the target server. This is the port scanning. Through the port scanning, you can glean a lot of valuable information about the target host.

2.3 Weak Password

Weak password vulnerability means the target site administration entry or external connection to a component such as a database uses a simple character password that is easy to guess, or a default system account password [12]. The strength of a password determines how hard it is to crack a password hash for uncovering the plain text password. Internet users often ignore recommended password guidelines and choose weak passwords that are easy to guess [13]. There is no strict and precise definition of weak passwords, a weak password tends to be compromised easily, either through guessing, cracking, or simulate attacks that compute hashes of possible passwords before for comparison against actual hash passwords. More specific, weak passwords generally refer password that are easily guessed by others or cracked by tools. Similarly, weak password blasting refers using brute force to break user names and passwords.

2.4 Directory Scan

Directory scanning is a security vulnerability due to the lack of validation on the file name that user enters into the web server or web application, leading the attacker can bypass the server security restrictions by using some special characters, such as accessing to any file (can be outside of the root directory of the web document), or commanding execution system [14], finding sensitive files, background files, database files and so on. When we take advantage of the vulnerability to get the account and password, we can then do a directory scan to get the background address [15]. Determining the existence of a file or directory by viewing information about the returned package, which is obtained by submitting an HTTP request. If the status code returned meets the criteria, which means the destination address is a reachable address.

III. Proposed Tool

3.1 Framework of Proposed Tool

The purpose of the proposed vulnerability scanner is to effectively improve the efficiency of information collection in the process of security tests. Fig.1 shows the flow chart of the scanner. The scanner consists of three components: port detection, weak password blasting and directory scanning. Firstly, the system performs a port scan through the user's input IP, which determines port opening through the TCP response. Then the open port list and IP will be taken into the processes of port blasting and directory scanning as the input of the next layer. In the weak password blasting stage, the result of port information detection is input as a verification file to detect whether there is a corresponding active port. If there is, put the corresponding IP into the corresponding weak password detection modules, which contains FTP, SSH and TELNET three weak password detection modules. After the detection, the detection result will be returned in the final output. In the directory scanning phase, IP and directory dictionary will be combined to make HTTP protocol request for connection address, determine whether it is reachable through the status code of the response packet, writing the active address as the result to the file class, and outputting it in the final result.

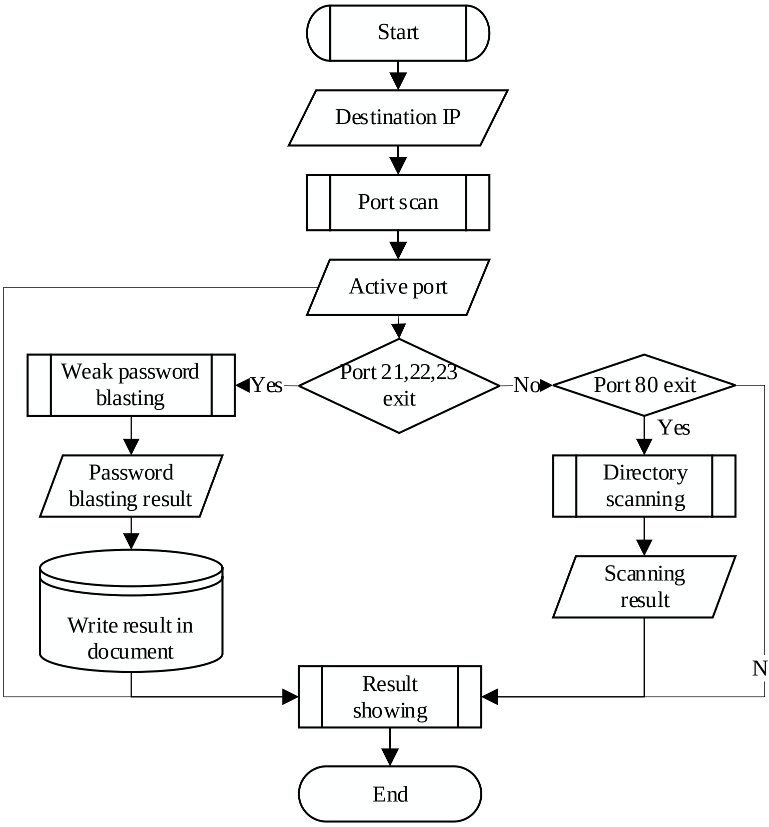


Fig.1 Flow chart of the scanner.

3.2 Modules Design

The implementation of the tool presented in this paper adopts C/S mode. It is written in Python. Because Python is easy to run on a variety of systems, writing in this language can reduce the deployment costs of security personnel to other environments. We can see from the overall frame diagram of the system in Fig.2, the design of the scanner mainly includes three functional modules, namely 1)port scanning module, 2)weak password blasting module, 3) directory scanning module .In the following, we will introduce these three modules in detail.

1) Port Scanning Module

The purpose of the port scanning module is to detect the active ports on the destination host. In this paper, the process of port scanning is based on the TCP full connection, using the conventional three-time handshake principle. First, the user inputs the destination IP address, and the host tries to establish a TCP connection with the destination host according to the obtained IP, After the successful establishment of the connection, the NMAP tool will be used to detect the ports, NMAP can use TCP when scanning instead of UDP, while other scanning tools such as ZMAP and MASSCAN cannot. NMAP is a connection-oriented scanner which maintains connections during scanning, further increasing the reliability, and the corresponding scanning result information will be returned. For each listening port, the correct connection will be returned if the port is open, otherwise a connection error is returned, indicating that the port is not accessible. By this mean, the NMAP result information will be filtered in order to extract all the active ports. These active ports will be sent to subsequent password blasting and directory detection modules.

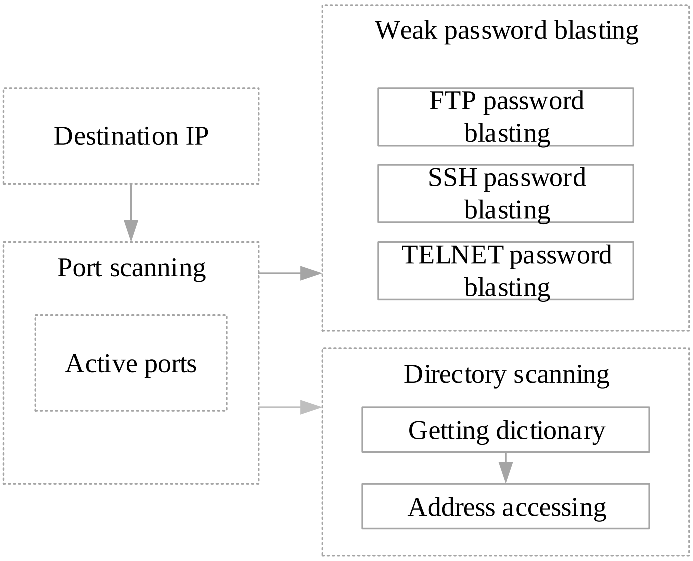


Fig.2 Framework of the proposed scanner

2) Weak Password Blasting

In the weak password blasting stage, the result of port information detection is input as a verification file to detect whether there is a corresponding active port and try to establish the corresponding connection with it. If the connection is successfully established, then the blasting function is achieved. The weak password blasting module described in this paper mainly include FTP, SSH and TELNET blasting. At the beginning, the scanner receive the result of active ports from the stage of port scanning as the input, According to the scanning results, selecting the destination host with the corresponding port which is in open state ,Here we take port 21 as an example. If port 21 on this host is open, then calling the corresponding weak password burst function to simulate the login packet request to the FTP server. A password and account dictionary need to be prepared in advance, which contains some commonly used username and password. Scanner can through certain interception function to grab the username and password when they login the FTP server, with the login password and account which from the dictionary file to make a connection with the server, if the connection session failed, then determining the account password is wrong. Continuing to call the next account until the invoking sequence of the account password is finished. Finally, if there is a session connection successful, the account password is thought to be correct and the corresponding result is returned. That’s to say the port blasting is achieved successfully.

3) Directory Scanning

Directory scanning allows us to find out how many directories on destination host, and try to explore the overall structure of the site. Through directory scanning we can also scan sensitive files, background files, database files, and information leakage files, and so on. The most common form of directory scanning is blasting through a dictionary, and the accuracy of the dictionary determines the completeness of your scan. Before performing the directory scan, the user needs to prepare a dictionary file. After obtaining the information returned in the port scan phase, the user enters IP as a variable and uses the directory dictionary combined with the HTTP service known to be opened to obtain the directory. Scanner will call the corresponding method to establish a TCP connection, first of all, determine whether port 80 exit, if exits, trying to get access to the dictionary file directory, by returning the response code to determine the viability of the destination address, if the corresponding code value is 200, which represents the address is survival,
then write it to file class and output it in the final results.

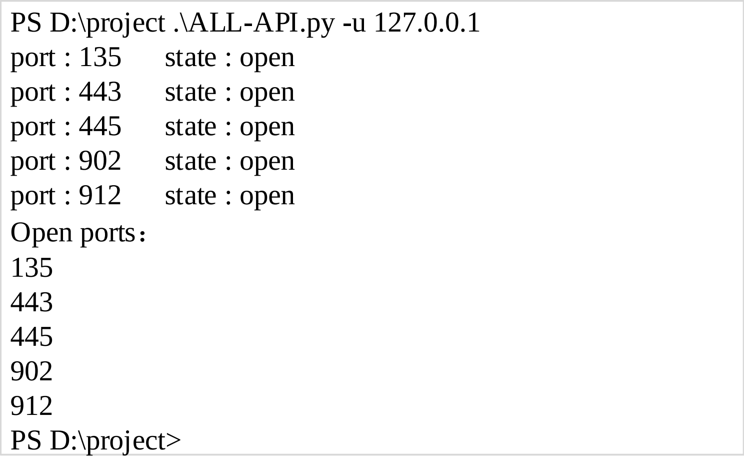
IV. Implements and Results

A. Environment Selection

Since the scope of this tool involves blasting attacks, there are limitations in the environmental options. We carried out functional experiments in five aspects, namely port scanning, SSH weak password blasting, FTP weak password blasting, TELNET weak password blasting and directory detection. Virtual machine server, cloud server and BAIDU server were selected as our test objects. And the scanning tool is run on Window system.

B. Implement of Port Scanning

In the port scanning test, the virtual machine server is simulated as the target host, and the direct verification method is adopted to judge whether the function is successfully implemented. The scanner uses NMAP to scan the destination host's ports, and the scanning results are shown in Fig.3. According to the scanning results, the open ports on the destination host are port 135, port 443, port 445, port 902 and port 912.After the scan results are obtained, checking the port monitoring status of the destination host and finding that it is consistent with the scan results, which means, the correctness of the port detection function is verified.



```
PS D:\project .\ALL-API.py -u 127.0.0.1
port : 135      state : open
port : 443      state : open
port : 445      state : open
port : 902      state : open
port : 912      state : open
Open ports：
135
443
445
902
912
PS D:\project>
```

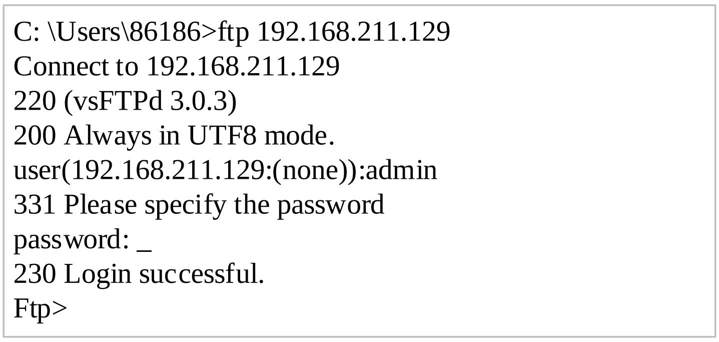
Fig.3. Scanning result of port

C. Implement of Weak Password Blasting

In the weak password experiments, blasting experiment of FTP and TELNET was carried out on the virtual machine server, and the blasting experiment of SSH was carried out on the cloud server, we adopted the login verification method. After accessing the result of the live ports, first we call the scanner to scan the FTP server, through scanning, finding port 21 was in an open state, before blasting, we will use the related method to generate two account password dictionary files: duser and dpwd, which are used to store some common usernames and passwords. Then we use the relative method for connection blasting. Using the accessed account password for trying to connect the corresponding FTP server, the result is shown in Fig.4, the result indicating that the account password can login successfully into the server. SSH and TELNET servers also conducted similar experiment operations like FTP server, the scanner perform the corresponding active port scan to the server, then call the corresponding blasting method to get the account password, using the account password to login into the server, then seeing if the connection is successful, if the session connection is successful, it is proved that account password was correct. According to the experimental results, the expected functions are achieved in these three password blasting modules of FTP, SSH and TELNET.

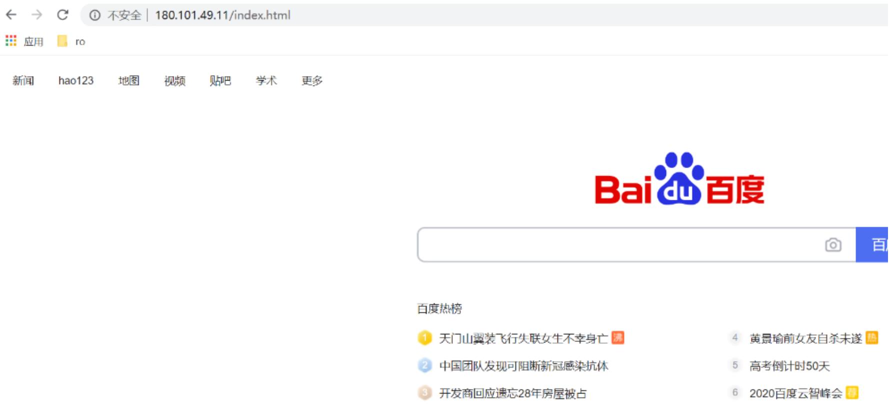
D. Implement of Directory Scanning

In the directory scanning test, the scanner is called to scan the Baidu server (in this experiment the IP address is 180.101.49.11). 'Dirfile' is used to store the directory dictionary, and the request address comes from the dictionary file. According to the scan result, port 80 is on, then the directory scan method interface file 'func_dirscan' is called to get the corresponding accessible directory. We attempt to access the specified directory address to verify accessibility. Here we visit the address of http://180.101.49.11/index.html as an example, the result is shown in Fig.5. It's proved the accessibility of corresponding address verification is successful.



```
C: \Users\86186>ftp 192.168.211.129
Connect to 192.168.211.129
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
user(192.168.211.129:(none)):admin
331 Please specify the password
password: _
230 Login successful.
Ftp>
```

Fig.4 Account password verification of FTP



1 天门山翼装飞行失联女生不幸身亡 沸
2 中国团队发现可阻断新冠感染抗体
3 开发商回应遗忘28年房屋被占
4 黄景瑜前女友自杀未遂 热
5 高考倒计时50天
6 2020百度云智峰会 荐

Fig.5 The result of accessing target address

E. Result and Analysis

As we can see from Table 1, the designed scanner realizes the integration of port scanning, weak password blasting and directory scanning. In the whole process of experiment, the open ports can be obtained correctly, the weak password can be found successfully, and the output address results are reachable. The experimental results show that functions achieved by the scanner are relatively accurate and can effectively complete the collection of some basic information.

Table 1: Result of testing

Test functions	Test objects	Verification methods	Verification results
Port scanning	Virtual machine server Cloud server Baidu server	Direct verification	Scan successfully
SSH weak password blasting	Cloud server	Login verification	Login successfully
FTP weak password blasting	Virtual machine server	Login verification	Login successfully
TELNET weak password blasting	Virtual machine server	Login verification	Login successfully
Directory scanning	Baidu server	Access verification	Access successfully

V. Conclusion

As the work of information collection is playing an increasingly important role in network security, there are corresponding tools both at home and abroad for various detections. But the biggest drawback is that these tools can only be used in isolation, which inevitably consumes a lot of inspectors' time. So it’s necessary to develop a tool that could integrate many function modules to save time and facilitate researchers’ work. In this paper, a vulnerability detection tool based on port service information is proposed, which solves the problem of frequent switching between different tools. Moreover, the experimental results also show that the designed scanner embodies the great advantages of the integrated tool when it effectively completes the functions of port scanning, weak password blasting and directory detection. The three functions are well realized in one tool. In addition to implementing the above mentioned functions, the tool also provides an interface foundation for future extensibility development. In future work, in order to better solve vulnerability of service information in network security, we will further improve each function in the information collection stage.

References

[1]. Vugrin, Eric D., et al. "Cyber threat modeling and validation: port scanning and detection." Proceedings of the 7th Symposium on Hot Topics in the Science of Security. 2020.

[2]. Calzavara, Stefano., et al. "Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery." IEEE Security and Privacy Magazine 18(3) (2020): 8-16.

[3]. Qin, Jiawei., et al. "Vulnerability Detection on Android Apps‐Inspired by Case Study on Vulnerability Related with Web Functions." IEEE Access 8 (2020): 106437-106451.

[4]. Makino, Yuma., and V. Klyuev. "Evaluation of web vulnerability scanners." IEEE International Conference on Intelligent Data Acquisition & Advanced Computing Systems: Technology & Applications. IEEE, 1 (2015): 399-402.

[5]. Chen, Chung Kuan., et al. "Penetration Testing in the IoT Age." Computer 51(4) (2018):82-85.

[6]. Kals, Stefan., et al. "SecuBat: A Web Vulnerability Scanner." International Conference on World Wide Web, (2006): 247-356.

[7]. Cai, Yun-Zhan., et al. "Improving Scanner Data Collection in P4-based SDN." 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS) . IEEE, 2020.

[8]. Yadav, Geeta., et al. "IoT-PEN: An E2E Penetration Testing Framework for IoT." Journal of Information Processing 28(2020):633‐642.

[9]. Lee, Cynthia Bailey, C. Roedel, and E. Silenok. "Detection and characterization of port scan attacks." Univeristy of California, Department of Computer Science and Engineering, 2003.

[10]. Ono, Daichi., et al. "A Design of Port Scan Detection Method Based on the Characteristics of Packet-In Messages in OpenFlow Networks." 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2020: 120-125.

[11]. Yuan, Chao., et al. "The Design of Large Scale IP Address and Port Scanning Tool." Sensors 20(16) (2020): 4423.

[12]. Weber, James E., et al. "Weak Password Security: An Empirical Study." Information Systems Security 17(1) (2008): 45-54.

[13]. Helble, Sarah C., Alexander J. Gartner., and Jennifer A. McKneely. "Increasing the Security of Weak Passwords: the SPARTAN Interface." arXiv preprint arXiv:1905.08199 (2019).

[14]. Flanders, Michael. "A Simple and Intuitive Algorithm for Preventing Directory Traversal Attacks." arXiv preprint arXiv:1908.04502 (2019).

[15]. Amankwah, Richard., et al. "An automated framework for evaluating open-source web scanner vulnerability severity." Service Oriented Computing and Applications 14(4) (2020): 297-307.

Wanggen Xie, et. al. “Design and Implementation of Vulnerability Detection Tool Based on Port Service Information.” *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(6), 2020, pp. 01-07.