Design and Implementation of an Integrated System for Security Assessment Based on LiveDVD/LiveUSB

Chia-Huan Wu * Chung-Huang Yang †

Abstract—There are many network security tools on the internet, and each of these tools maintain its own scanned results that cannot be shared by each other. In this research, we integrate several famous network security tools, and propose a knowledge base database scheme to share each scanned results. Moreover, due to there are more and more attacks focus on web applications, we take extra vulnerability assessment on web applications, and use results saved in knowledge base database to generate a complete reports written in Chinese for easily understood purpose. Finally, we setup the whole system into a LiveDVD/LiveUSB based on Debian GNU/Linux to become a portable security assessment system.

Keywords: Localization, vulnerability scanning, penetration testing, LiveDVD, LiveUSB

1 Introduction
Security testing can be categorized into several different types, like network scanning, virus detection, war dialing, and so on [1]. There are many powerful security tools existing on the internet, and each of these tools has its suitable scope that cannot exchange information directly. In this paper, we integrate several well-known security assessment tools into a portable operating system, and discuss relevant issues in later sections.

1.1 Network scanning
Network scanning, also known as network mapping, is a methodology by using a port scanner to identify opened ports and the service listen on [2, 3]. Usually we enforce network scanning tasks to gain the information about targets, i.e., protocols, network applications, etc. The results of network scanning can be reused for further assessment tasks.

1.2 Vulnerability scanning
After network scanning complete, we can get into the next level to confirm targets’ weakness by performing vulnerability scanning, also known as vulnerability assessment [4]. In other words, vulnerability scanning will cause advanced explorations carried out to acquire more valuable information. By executing vulnerability scanning during auditing, we can at least estimate the risk degree of the targets.

1.3 Penetration testing
Penetration testing is designed to simulate a real attack and locate the accurate attack path before critical damage happens [5, 6]. It is extremely useful to company’s applications that may face to unknown threats. Since penetration testing acts like real intruders, testers have to get formal companies’ permission for the tasks. Further more, testers require well expertise to minimize the impact during conducting penetration testing.

2 Design
2.1 Nmap
Nmap is one of famous port scanning tools, it can not only identify the state of port, the network services operating on that port, but also can guess the operation system of the target by using novel techniques. Besides, nmap can also produce raw IP packets for IDS evasion idea. In this research, nmap will play the role of network scanning stage to obtain common information.

2.2 Nessus
Nessus, which is a well-known vulnerability scanner, can identity security holes on network hosts [7]. The main difference between Nessus and other famous vulnerability scanners is that Nessus has its own scripting language engine called NASL for developing auditing plug-ins. With NASL, you can add security testing plug-ins into Nessus quickly and easily, without modifying Nessus itself. In our system architecture, Nessus will be responsible for finding out the weak of network services.

* Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, Taiwan. Email: willie@ice.nknu.edu.tw
† The same as *. Web: http://crypto.nknu.edu.tw/, Email: chyang@computer.org.
2.3 Metasploit

Metasploit is an advanced framework for contributing, testing, and using exploits [8]. It provides variable modules, like payloads, encoders, and other useful functions to conducting exploits efficiently. In our system, we integrate Metasploit to be in the character of penetration testing.

2.4 W3af

W3af, which is abbreviate from Web Application Attack and Audit Framework, is a platform aiming to audit web applications. It has many profitable plug-ins, like SQL injection test and XSS attack test, making it possible to automate audit progress. Moreover, testers can enable exploit modules to enforce W3af causing damage to network hosts. W3af is integrated into our system for additional web security assessing purpose.

2.5 LiveDVD/LiveUSB

Live Distro is a kind of operation system distribution which can be booting without installing into hard disk. Usually, we named this operation system depending on what media it stores. Consequently, it is named LiveDVD because its media is DVD-ROM, and so does LiveUSB. As concepts of Squashfs [9] and Unionfs [10] are proposed and implemented, it breaks physical limitations of media, and makes live distro broad applied in different domain. Since procedure for installing tools described above may be inconvenience and complex, we setup our system into LiveDVD/LiveUSB. Therefore, this system becomes portable, and easily deploys even moving to different network environment. Figure 1 shows operative screenshot with well Chinese locale support on LiveDVD/LiveUSB we made.

3 Implementation

3.1 System architecture

We design a system architecture to combine the capabilities of security tools described in previous section. This system is divided into two parts: server-side program and client-side program. Server-side program does the mainly tasks, it receives request, start assessment tasks by calling nmap, nessus, etc., and then return the scanned results. In contrast, client-side one is a graphical user interface program, network manager needs to specify IP and port that they want to scan, and everything will be done automatically. All data transmitted between server-side and client-side is XML format encoded in base64, therefore client-side can be easily replaced by constructing in other languages. Figure 2 shows the whole system architecture.

3.2 Workflow

Figure 3 shows the workflow when taking an assessment task. When server-side program receives the request packets, it will perform following steps:

1. Fork a child process to handle this task.
2. This process creates two threads named web-task and va-task. The thread which named web-task will execute nmap and w3af by order, and then save the results into knowledge base database. The other one will execute nessus and metasploit
in turn, and integrate the results into database after both of them ended.

3. Generate XML-format results by fetching results in database.

4. Send the results to client-side program.

After client-side program gets the results packets, it can show the results to network manager or generate detailed report by parsing the XML-format results.

3.3 Program presentation

The server-side program is developed in python language. Since python can be run in many different operating systems, the server-side program can be easily ported to other operating system like FreeBSD. Figure 4 shows the screenshot while server-side program is running on LiveDVD/LiveUSB.

Client-side program is different from server-side one. For efficient purpose, we developed this one by using GTK+. GTK+ is a toolkit for creating graphical user interface, and applications written in GTK+ can be compiled in multi platforms like Windows.

In the end, we can generate well-formed html reports. Figure 5 shows the screenshot of viewing reports.

4 Conclusion

In this research, we not only integrate security tools by sharing each scanned results in knowledge base database, but also make efforts on web applications assessment. Additionally, we use these results data to produce an integrated report in Chinese, and integrate this whole system with LiveDVD/LiveUSB, to help network manager to easily find the vulnerabilities and take necessary actions.

References


