SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Design and Implementation of a Live CD/DVD for Vulnerability Scanning

Pao-Kuan Wang* Chung-Huang Yang†

Abstract—Along with the Internet popularization recently years, more and more security vulnerabilities were issued, so it is necessary and urgent to realize what kinds of risks that the servers have. Without well-done protection, the servers might become the next victims from hackers. Not only under the protection from firewall passively but also operating vulnerability scanners actively help administrators to find out the drawback of the servers and the network to increase network security effectively.

Nessus is an open source freeware which has the capability of vulnerability assessment. To install Nessus onto Linux and implement it as a Live CD/DVD, the Linux network administrators can easily maintain the security concern without the necessarily certain experience and knowledge, what they need is the basic commonly used commands. More, the servers don't need to update packages frequently.

Keywords: Localization, Vulnerability Scanner, Network Security, Live CD.

1 Introduction

At present, computers in institutions, enterprises and schools all over the world are connecting to the Internet, so the protection task from hackers is essential. The vulnerability scanners are showing up at this time. Using these tools may let us understand which known vulnerability our own server have, and patches as soon as possible. If there exist a backdoor and doesn't fix, the hackers will very great to visit your servers.

Nessus [6] is an open source freeware which has the capability of vulnerability assessment. There are more introductions about Nessus in next section. However, like many other freeware and open source software, Nessus is English software, too. For this reason, this research Chinese-adapted Nessus's Windows client. It can increase the affinity of user interface. About the Chinese-adapted result report [4], the TWCERT [1] have already developed vulnerability database. It can provide the Chinese-adapted Nessus scan result, but this service is not free.

Another purpose of this research is to implement the Nessus Live CD/DVD.It let using Nessus more flexible, and doesn't need tedious installation, configure Linux and Nessus. Only needs one Live CD/DVD, it can do vulnerability scanning to user's server at anytime, so as to strengthens server's security.

2 Nessus

The "Nessus" Project was started by Renaud Deraison in 1998 to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute [7]. It is estimated that the Nessus scanner is used by 75,000 organizations world-wide.

In 2002, Renaud co-founded Tenable Network Security with Ron Gula, creator of the Dragon Intrusion Detection System and Jack Huffard. Tenable Network Security is the owner, sole developer and licensor for the Nessus source code, the Nessus trademark and the nessus.org domain worldwide.

As information about new vulnerabilities are discovered and released into the general public domain, Tenable's research staff designs programs to enable Nessus and NeWT to detect the presence of them. These programs are named 'plugins' and are written in the Nessus Attack Scripting Language (NASL). There are three feeds are available - Direct, Registered and GPL. The access to the GPL feed and to the Registered Feed is free.

Nessus is composed by two parts (Figure. 1). The server part makes the examination (attack), it only can install under the Unix-like system (Solaris,

* Institute of Information and Computer Education, National Kaohsiung Normal University (NKNU), Taiwan,
R.O.C.(paokuan@icemail.nknu.edu.tw)
† NKNU (chyang@computer.org)

FreeBSD, GNU/Linux and others). The Client part is a front end interface that controls and watches the information, it can provide user to login the Nessus server, select the examination, and review the scan result. And Client has three kinds of choices: Win32, Unix-like and Java. This research focus on the Win32 Client's Chinese-adapted.

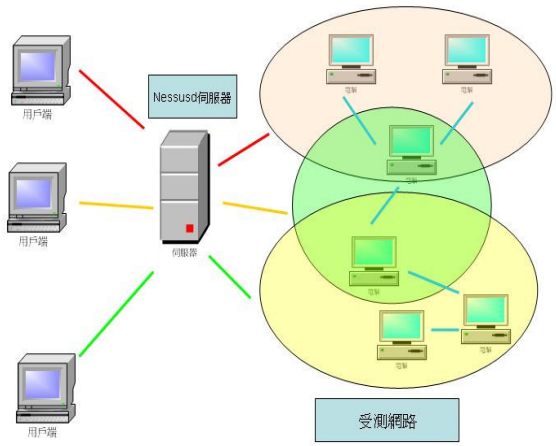

Figure 1: Framework of Nessus

3 Live CD/DVD

Although recent years X-windows interface designed already suitable perfect. But its installation and setting isn't convenient like MS Windows. Fortunately Linux is open source software. Therefore some people rewrite the Linux platform the intensive disc version, lets the user only need a piece of disc to set into CD-ROM, exempts the installment, moreover no need the hard disk, and can run Linux in the memory. Certainly the memory capacity must at least 256MB, or it will run strenuously.

At present had dozens of kind of Live CD release [8], more famous like KNOPPIX [5], Mandrake, Fedora Live CD... and so on. After Live CD starts not only can be a work station, but also a network server.

4 Nessus Live CD/DVD

Live CD/DVD of this research uses Fedora Core 4 O.S. Live CD's capacity is small than DVD, so the installation size must be less than 2.3GB. Therefore the unnecessary modules have to remove. The account /password default is root/fedora. Manufacture step as follows:

(1) Update kernel to version 2.6.13-2.ossii (initial version is 2.6.11-1.1369_FC4), this version supports the function of compressing the system file.

(2) Install Fedora Live CD manufacture tool which provide by OSS integral institute [2].

(3) Install Nessus and set default account /password: admin/nessus.

(4) Create a new folder named "nessus" under /etc. Because /usr is read only folder of this Live CD, so we must modify the path setting in "nessusd.conf", like plugin_folder, logfile, dumpfile,…etc. All above effected will move or redirect to new path.

(5) Start Nessus daemon and test the connection between server and client is normal. (It will appear request of making certificate, make default certificate by hint.)

(6) Remove nonessential file again, use Fedora Live CD manufacture tool to compress the file system, and then manufacture it as iso file.

(7) Burning the iso file to CD/DVD.

(8) Insert the CD/DVD into CD/DVD-ROM and reboot. It will load Live CD/DVD automatically. Figure 2 displays the reboot screen.

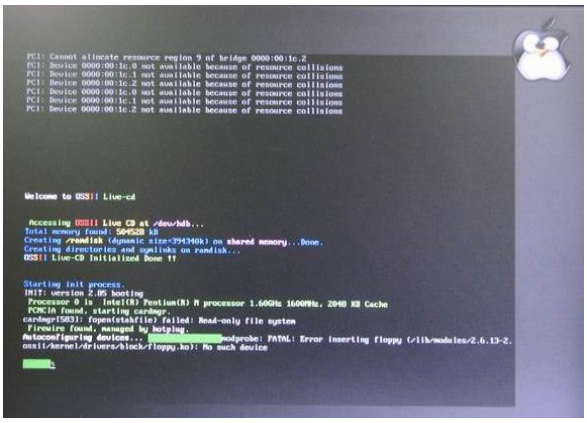

Figure 2: The reboot screen of Nessus Live CD/DVD

After login O.S., There is an icon named "Ramdisk" (see Figure 3 red circle part), it means using memory as hard disk. Click it will show some folders, they can read and write.

Figure 3: Nessus Live CD/DVD desktop

5 Nessus's client with Chinese interface

In this research, Nessus's client on Windows platform is developed by MS Visual C++ 6.0. Source code version is 1.4.5c. Figure 4 is original version and Figure 5 is Chinese-adapted version.

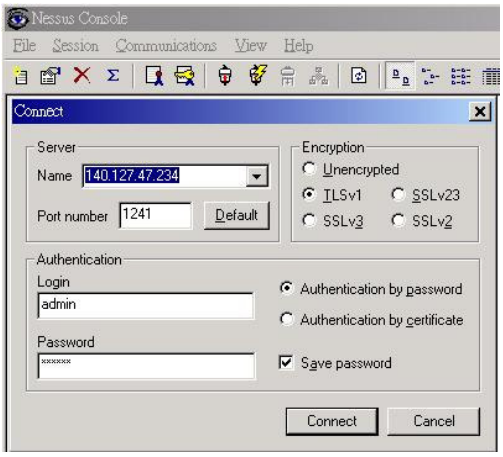

Figure 4: Original version

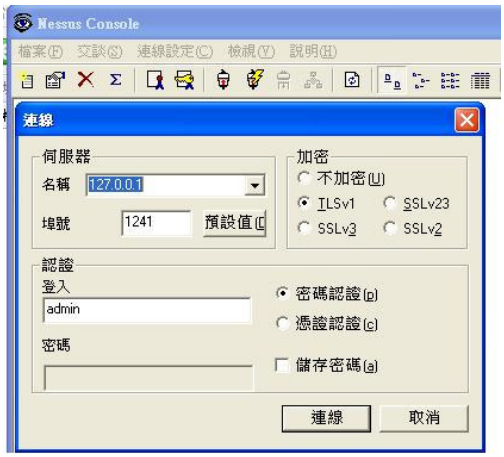

Figure 5: Chinese-interface version.

6 Conclusion

The results of this research are suitable for individual, the campus network and the enterprises. It can provide network supervisors a free using and powerful vulnerability scanner, so as to protect servers and personal computers. And they don't have to waste a computer especially to install Linux and Nessus, the Linux network administrators can easily maintain the security concern without the necessarily certain experience and knowledge, what they need is the basic commonly used commands. More, the servers don't need to update packages frequently. Chinese-adapted Windows client can reduce the barriers caused by unacquainted language. Increase the familiarity degree with application, and reduce the learning and fumbling time.

The future research might focus on the Chinese-adapted work of Linux client. It will be more convenient to use Nessus.

Reference

[1] TWCERT/CC, https://www.cert.org.tw/
[2] OSS integral institute, http://opendesktop.org.tw
[3] Pei-Gi Zheng and Chung-Huang Yang, "Design and Implementation of a Live-CA CD on an Open Source Environment", ICIM2005, FU-JEM Catholic University, May 2005.
[4] Kun-Ye Lai, "Localization for Vulnerability Scanner", Information Management Institute of National Sun Yat-sen University, Master's thesis, 2004
[5] KNOPPIX, http://www.knoppix.org/
[6] Nessus, http://www.nessus.org
[7] SANS Institute, http://www.sans.org/
[8] The Live CD List, http://www.livecdlist.com/