Using w3af to Achieve Automated Penetration Testing By Live DVD / Live USB

Jiun-Kai Ke
Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, Taiwan
Jacky10521@gmail.com

Chung-Huang Yang
Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, Taiwan
chyang@computer.org

Tae-Nam Ahn*
Security Engineering Research Center*
Hannam University, Korea*
taenamahn@hotmail.com

ABSTRACT

As the popularity of the Internet continues growing, there are more and more services appeared, security measures are expected to become all the most important on the Internet. Personal privacy and confidentiality of information also need to be protected and be resolved of vulnerabilities and weaknesses quickly. It is the user the most concerned about one of the topics on the Internet now.

In this research, we developed automated penetration testing tools based on an open source, we just enter the target URL, and we can automate penetration testing with Live DVD/Live USB platform, which can be used any platform.

Keywords

Open source, Penetration testing, Live DVD, Live USB

1. INTRODUCTION

Along with the Internet popularization in recent 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.

Penetration testing is the security practice of a trusted party company attempting to detect and exploit weaknesses in the security of a system. By simulating a live attack, managers can witness the potential of a malicious attacker gaining entry or causing harm to the data assets of that company [13].

According to the Web Application Security Consortium (WASC) says that in-depth manual and automated assessments found nearly 97 percent of sites carry a severe vulnerability.

About 7.72% of applications had a high-severity vulnerability detected during automated scanning, detailed manual and automated assessment using white and black box methods show that probability to detect high-severity vulnerability reaches 96.85 percent [6].

In this research, we developed a user-friendly implementation of automated penetration testing tools based on an open source. It doesn't need to use manual techniques to find vulnerabilities. User just enter the target URL, and the system can automate penetration testing with Live DVD/Live USB platform, which can be used on any operation system. Finally, we setup the whole system into Live DVD or a Live USB based on xubuntu to become a portable automated penetration testing system. Automated Penetration testing tools not only allows testers can focus on analysis of the output data, but also allows beginners easily to use. User uses it with security tools to protect the system quickly [10].

2. RELATED WORKS

2.1. Penetration testing

Penetration testing [2, 8, 14] is an effective complement to vulnerability scan, aimed at uncovering hidden vulnerabilities. The findings or results of the penetration testing are aimed at improving the security posture of a network by presenting countermeasures for the vulnerabilities identified. And it is designed to simulate a real attack and locate path before critical damage happens. Penetration testers can perform three types of tests [5, 13]:

(1) Black-box test: Block box testing is intended to most closely replicate the attacks of a remote. The penetration tester has no prior knowledge of a company network. For example, if it is an external black-box test, the tester might be given a website address or IP address and told to attempt to crack the website as if he were an outside malicious hacker.

ICHIT'09, August 27–29, 2009, Daejeon, Korea.
Copyright ⓒ 2009 ACM 978-1-60558-662-5/09/08…$10.00.

(2) White-box test: White box testing is differ form black box testing in that the testers are given near total access to information about the application they are attacking, the tester has a complete knowledge of the Internet network. The tester might be given network diagrams or a list of operating systems and applications prior to performing tests, although not the most representative of outside attacks, this is the most accurate because it presents a worst-case scenario where the attacker has a complete knowledge of the network.

(3) Gray-box test: Gray box testing is the combination of black box and white box testing. The tester simulates an inside employee. The tester is given an account on the internal network and standard access to the network. This test assesses internal threats from employees within the company.

2.2. W3af

w3af, which is abbreviated from Web Application Attack and Audit Framework, is a complete environment for auditing and attacking web applications. This environment provides a solid platform for auditing and penetration testing. It is easy to use and extend, w3af has more than 130 plugins, like SQL injection test and Cross-Site Scripting (XSS) test, because w3af is a kind of free tools, so tester always uses it to detect the vulnerabilities of web, w3af its core and plugins are written in Python. Therefore, w3af can work in all operating system platforms, which have to install Python. Basically, w3af has three types of plugins: discovery, audit and attack [15].

(1) Discovery plugins have only one responsibility, finding new URLs, forms, and other injection points.

(2) Audit plugins take the injection points found by discovery plugins and send specially crafted data to all of them in order to find vulnerabilities.

(3) Attack plugins objective is to exploit vulnerabilities found by audit plugins. They usually return a shell on the remote server, or a dump of remote tables in the case of SQL injections exploits.

2.3. Live CD

Live CD is a kind of operation system distribution which can be booting without installing into hard disk. Automated hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals, Live CD can be used as a productive Linux desktop, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. Whether you are a security professional or a system administrator, a bootable Linux Live CD can be your best friend, the most widely used the Live CD is Knoppix [9, 10, 16].

Knoppix is designed by Klaus Knoppix who is a Germany programmer. Thus it will be his last name Knopper and Linux together referred to as "Knoppix". It is based on Debian to develop and becomes the most significant feature of without installing it on a dedicated machine [12, 16]

2.4. Security Live CD

Network security increasingly emphasized, Internet Security Live CD has been proposed. Security Live CD is the classification of security tools integrated in a Live CD so that users can boot with a CD-ROM. Security Live CD ranking of the top ten on network in 2006, introduced the following well-known sets of Security Live CD [1, 4].

(1) BackTrack: BackTrack[3] is a Linux distribution distributed as a Live CD which resulted from the merger of WHAX and the Auditor Security Collection, which is used for Penetration testing it is the widely use linux live distribution focused on penetration testing with no installation whatsoever, the analysis platform is started directly from the CD-ROM and is fully accessible within minutes.

(2) Helix: Helix [7] is more than just a bootable live CD. You can also boot into a customized Linux environment that includes customized Linux kernels, it focuses on Incident Response & Forensics tools. Helix is a stable, complete package, with a broad range of great utilities that will significantly increase your ability to respond to problems, threats and incidents in your environment.

(3) PHLAK: PHLAK [11] which is abbreviated from Professional Hacker’s Linux Assault Kit that is a modular live security Linux distribution. PHLAK is a Linux Live CD based on Morphix, PHLAK was created to become the only tool security professionals would need to perform security analysis, penetration testing, forensics, and security auditing.

3. DESIGN AND IMPLEMENTATION

3.1. System architecture

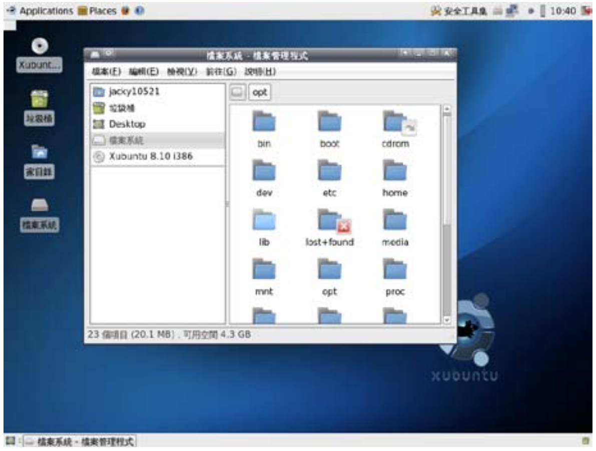


Figure 1. Live DVD/Live USB screenshot

In this research, as shown in Figure 2 .We developed the system based on operator system of xubuntu 8.10, as shown in Figure 1, which is designed for old computers, and take lightweight desktop environment xfce4, which is in order to reduce the system resources, we used the desktop environment xfce4 to classification of all security tools, and then choice the automated penetration testing of menu, and w3af will be started, using windows interface to do prompted for the user, so the tester can only enter the target URL and the complete automation of the penetration testing, the final results to be scanned in order to analysis of website vulnerability.

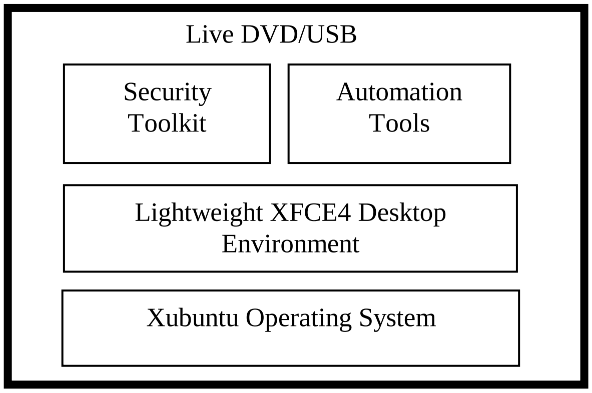


Figure 2. System architecture

Xfce4 desktop environment using the various categories of security tools, as shown in Figure 3, select the automation tools can be penetration testing immediately.

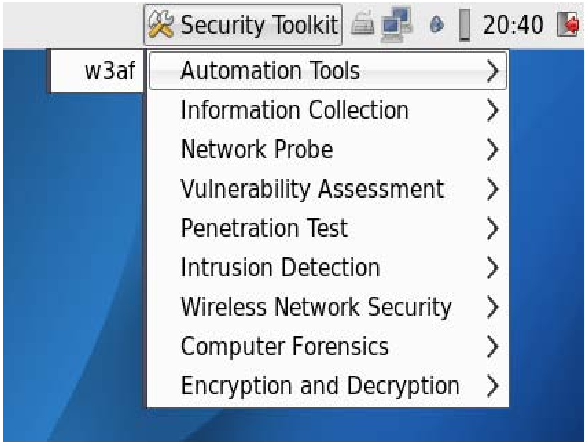
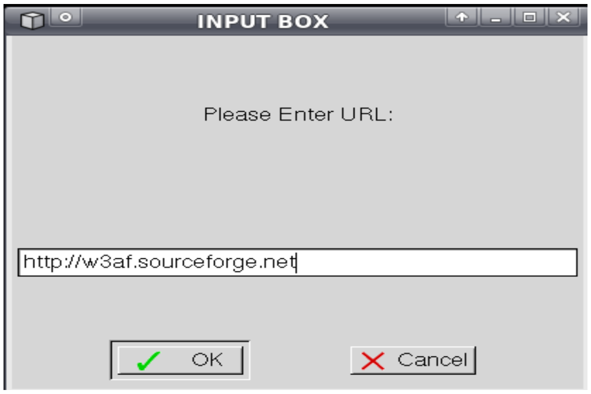


Figure 3. Security tools screenshot

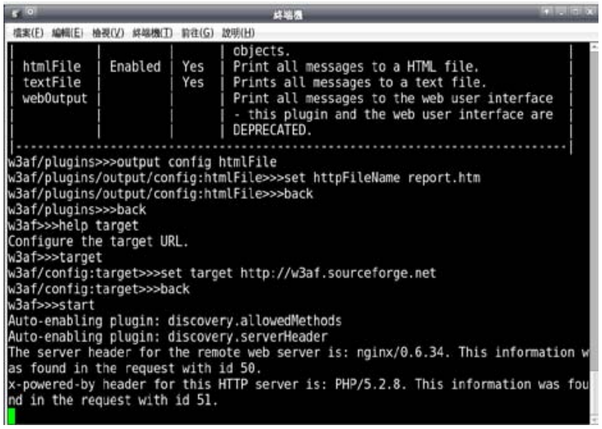
When clicking w3af tools, at this time user just only to enter the target URL in dialog window, as shown Figure 4, and then it can be automated penetration testing immediately. Figure 5 shows automated implement of the screen.



Please Enter URL:

http://w3af.sourceforge.net

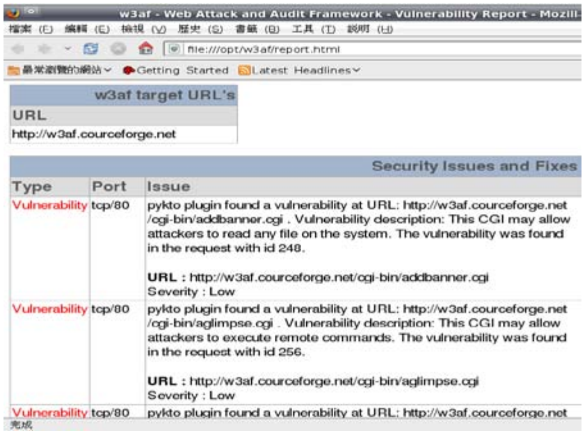
Figure 4. Dialog window screenshot



```
|            |          |       | objects.                                         |
| htmlFile   | Enabled  | Yes   | Print all messages to a HTML file.               |
| textFile   |          | Yes   | Prints all messages to a text file.              |
| webOutput  |          |       | Print all messages to the web user interface     |
|            |          |       | - this plugin and the web user interface are     |
|            |          |       | DEPRECATED.                                      |
|-----------------------------------------------------------------------------------|
w3af/plugins>>>output config htmlFile
w3af/plugins/output/config:htmlFile>>>set httpFileName report.htm
w3af/plugins/output/config:htmlFile>>>back
w3af/plugins>>>back
w3af>>>help target
Configure the target URL.
w3af>>>target
w3af/config:target>>>set target http://w3af.sourceforge.net
w3af/config:target>>>back
w3af>>>start
Auto-enabling plugin: discovery.allowedMethods
Auto-enabling plugin: discovery.serverHeader
The server header for the remote web server is: nginx/0.6.34. This information w
as found in the request with id 50.
x-powered-by header for this HTTP server is: PHP/5.2.8. This information was fou
nd in the request with id 51.
```

Figure 5. Automated running screenshot

Finally, after scanning of w3af, which will be the results of a scan, using the results can be known the details of vulnerabilities, update the revision to improve the security of the website. Otherwise, it will be attacked by hackers. Figure 6 shows the screenshot of viewing reports.


w3af - Web Attack and Audit Framework - Vulnerability Report - Mozill
檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
file:///opt/w3af/report.html
最常瀏覽的網站
Getting Started
Latest Headlines
完成

w3af target URL's

URL
http://w3af.courceforge.net

Security Issues and Fixes

Type	Port	Issue
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://w3af.courceforge.net /cgi-bin/addbanner.cgi . Vulnerability description: This CGI may allow attackers to read any file on the system. The vulnerability was found in the request with id 248. **URL :** http://w3af.courceforge.net/cgi-bin/addbanner.cgi Severity : Low
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://w3af.courceforge.net /cgi-bin/aglimpse.cgi . Vulnerability description: This CGI may allow attackers to execute remote commands. The vulnerability was found in the request with id 256. **URL :** http://w3af.courceforge.net/cgi-bin/aglimpse.cgi Severity : Low
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://w3af.courceforge.net

Figure 6. Generated report of w3af

Figure 7 shows the workflow for the system, the research to achieve automated by shell script, at click on the desktop menu would call shell script, at this time the shell script will be started Xdialog, when user enter the target URL. It will be started and completed plugins setting, scanning depth, setting the name of the output files. Finally, the report will be output after scanning. At this point penetration tester can concentrate on analysis of statements.

Tester can work on any platform by Live DVD/Live USB, and then any operating system environment can be automated penetration testing device through the network on the target to penetration testing.

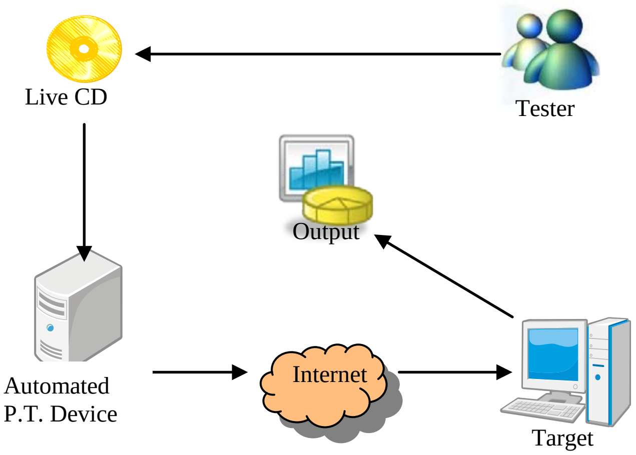


Figure 7. Workflow of automated P.T.

Table 1. Comparison of Security Live CD

Type	Our System	BackTrack	Helix
Chinese input	Yes	No	No
Categories of security tools	11	11	2
Package update	Automation	Manual	Manual
Automation Tools	Yes	No	No
Low cost	Yes	Yes	No

4. CONCLUSIONS

There are many penetration testing tools on network, but it is required professional knowledge of the tools, with a Live DVD could run automated penetration testing on your systems to check whether there are security-related problems. Automated penetration testing tools not only allows testers can focus on analysis of the output data, but also allows beginners easily to use. Finally, we setup the whole system into Live DVD or a Live USB based on xubuntu to become a portable automated penetration testing system, so user can use it on different environments.

In this research, we developed a user-friendly implementation of automated penetration testing tools based on an open source. There are many Internet security companies provide the service of penetration testing, but it has to take a lot of money. So if it is not a very urgent need to detect vulnerabilities, very few companies will be asked to do penetration testing, automated penetration testing tools are easy to be used, as long as entering the target URL can be scanned immediately to obtain information.

5. REFERENCES

[1] 10 Best Security Live CD Distros (Pen-Test, Forensics &Recovery). http://www.darknet.org.uk/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery, April 2009.

[2] B. Arkin, S. Stender, and G. McGraw, Software Penetration Testing, IEEE Security & Privacy, Vol. 3, No. 1, 2005, pp. 84-87. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1392709

[3] BackTrack.http://www.remote-exploit.org/backtrack.html, April 2009.

[4] M.J. Decker, Penetration Test: Not Just a Hack Job. THE ISSA Journal, April 2004, pp. 24-26.

[5] D. Geer, and J. Harthorne, Penetration Test: A Duet, Computer Security Applications Conference, 18th Annual, 2002, pp. 185-195.

[6] K.J. Higgins, Web Application Security Consortium, Report: In-Depth Analysis Finds More Severe Web Flaws, October 2008.

[7] Helix. http://www.e-fense.com/products.php, April 2009.

[8] T.J. Klevinsky, S. Laliberte, and A. Gupta, Hack I.T.: Security Through Penetration Testing, Pearson Education, Inc., 2002. http://www.google.com/books?hl=zh-TW&lr=&id=31Kis_vaadwC&oi=fnd&pg=PR13&dq=Security+Through+Penetration+Testing&ots=_4exQ1ujYa&sig=JJX5IwnDFxqthdi4JmoTH2nbRjU#v=onepage&q=&f=false

[9] P. Lougher and R. Lougher, Squashfs – a squashed read-only filesystem for linux, 2002.

[10] P. Midian, How to ensure an effective penetration test, Information Security Technical Report, Vol. 8, No 4, April 2003.

[11] PHLAK.http://www.phlak, April 2009.

[12] K. Rankin, Knoppix Hackers:100 Industrial-Strength Tips & Tools, O'Reilly, October 2004.

[13] H. Thompson, Application penetration testing, Security & Privacy Magazine, IEEE, Vol. 3, No. 1, 2005, pp. 66-69.http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1392704

[14] J. Wack, M. Tracy, and M. Souppaya, Guideline on Network Security Test [NIST SP 800-42], US Department of Commerce, National Institute of Standards and Technology, 2003.

[15] w3af - Web Application Attack and Audit Framework. http://w3af.sourceforge.net, April 2009.

[16] C. Wright, J. Dave, P. Gupta, H. Krishnan, D. Quigley, E. Zadok, and M. Zubair, Versatility and Unix semantics in namespace unification, ACM Transactions on Storage (TOS), Vol. 2, No. 1, 2006, pp. 74-105. DOI=http://doi.acm.org/10.1145/1138041.1138045