IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

SYSTEM AUDITING THROUGH PENETRATION TESTING FOR ASSESSING SECURITY OF REMOTE SITE

Er. Ashish Kharvar[1], Darshan R. Chauhan[2]
Assistant Prof., Information Technology Department, SCET, Surat, Gujarat, India
Assistant Prof., Computer Department, SNPITRC, Bardoli, Gujarat, India

Abstract: Penetration testing is the art of evaluating the security of target system/network by simulating tools, methods that an IS auditor would use. From the penetration testing we can find out loop holes in the target system which will be useful to establish control procedure. In this paper, we have discussed penetration testing on site www.vidpk.com with the use of retina-network security scanner tool.

I. INTRODUCTION

Penetration testing is the art of evaluating the security of a system/network by simulating the tools, methods that a cyber criminal would use. This evaluation allows discovery of known and unknown security loopholes.

In penetration testing it is important to put oneself into the shoes of a cyber criminal means one should think like a cyber criminal to find out vulnerabilities.

Penetration tests are sometimes called “white hat attacks” because in a pen test, the good guys are attempting to break in.

II. METHODS

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target system, identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

(i) Manual penetration testing: It is very time consuming process which rarely used in IT industry considering load on IT employees .So it better to used software based automated testing tool.

(ii) Automated testing: Which could be carried out with various tools like Nessus, Retina, Core Impact, SARA, SAINT etc. I have carried out penetration testing on www.vidpk.com with the use of retina network security scanner tool.

III. PENETRATION TESTING ON WWW.VIDPK.COM

www.vidpk.com is the Pakistani web site which basically provides various entertainment features.
Following is the detail report of this testing

Scanner name: Retina
Scanner version: 6.0
Scan start time: 12:23 PM
Scan duration: 7 min 13 sec
Total Open port detected: 4
Total Vulnerability detected: 7

Details of Open ports

Port Number	Description
TCP:21	FTP – File Transfer protocol
TCP:25	SMTP- Simple mail transfer protocol
TCP:80	WWW-HTTP-Hyper text transfer protocol
TCP:3306	MYSQL

Details of Vulnerabilities

Vulnerability Name	Count
CGI - Excite Search	1
Mysql server detected	1
FTP Service	1
ICMP Timestamp request	1
Apache User enumeration	1
HTTP TRACE method supported	1
Php5 php_sprintf_appendstring() Remote integer overflow	1

IV. RESULT ANALYSIS

Open ports shown in reports could be used by an attacker to gain access into system. As well as vulnerabilities mention in above table could be exploited to attack and crash system.
For example CGI-Excite search could be used to detect IIS and attack on this internet service or Remote integer overflow could be used to write certain malicious script or crash this program.

V. COUNTERMEASSURES

Close all unused ports so that we can protect our system and try to resolve vulnerabilities by optimizing code or applying other countermeasures.

VI. CONCLUSION

From this discussion we conclude that with penetration testing we can find out vulnerabilities in target site that will be very useful to establish control procedures and protect our system from attacker.

REFERENCES

[01] Websites: http://www.darknet.org.uk/2008/03/hacking-windows-nt-through-iis-ftp/

[02] Courses: Ankit Fadia certified ethical hacker (AFCEH)

