ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A study on Penetration Testing

S. Angel*
Assistant Professor KGCAS,
Coimbatore,India
Angel.s@kgcas.com

Dr.S.Sarala
Assistant Professor Bharathiyar University,
Coimbatore, India
sriohmau@yahoo.co.in

Abstract: The process of performing a penetration test is to verify that new and existing applications, networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources. This paper will review the steps involved in preparing for and performing a penetration test. The intended audience for this paper is project directors or managers who might be considering having a penetration test performed. The process of performing a penetration test is complex. Each company must determine if the process is appropriate for them.

I. INTRODUCTION

Over the last few years, companies have been adding additional functionality to existing applications and implementing new applications in an effort to provide more convenience or better service for customers and/or employees [1]. Examples of this functionality could be in the form of World Wide Web access for bank customers or telecommuting options for employees who work at home. Additionally, companies have also determined that a presence on the World Wide Web is a way to increase brand awareness and establish a top-of-mind awareness for their product or service for potential customers. Security is a significant concern for World Wide Web servers. The World Wide Web servers have added a new set of vulnerabilities that companies should consider. However, vulnerabilities are not limited to World Wide Web servers. Vulnerabilities exist and can be unintentionally induced in systems or resources that have been in operation for an extended period.

II. WHAT IS A PENETRATION TEST?

A penetration test is the authorized, scheduled and systematic process of using known vulnerabilities in an attempt to perform an intrusion into host, network or application resources. The penetration test can be conducted on internal (a building access or host security system) or external (the company connection to the Internet) resources. It normally consists of using an automated or manual toolset to test company resources.

III. WHAT IS A PENETRATION TEST IS NOT.

A penetration test is not an uncoordinated attempt to access an unauthorized resource. The event must be coordinated and scheduled with support staff. At a minimum, some of these tests will log alerts in an Intrusion Detection System [2]. Additionally, some tests have the ability to cause an outage of network equipment or systems. For that reason, management and staff awareness is required in most cases. The exception to complete notification could be a penetration test intended to test the Intrusion Detection System (and staff response). Management should also consider providing printed documentation authorizing the test be performed. This will address any legal liabilities that might be associated with the performance of the test.

IV. WHY PERFORM A PENETRATION TEST?

If vulnerability is utilized by an unauthorized individual to access company resources, company resources can be compromised. The objective of a penetration test is to address vulnerabilities before they can be utilized.

V. WHAT SHOULD BE TESTED?

The core services offered by the company should be tested. These include: Mail, DNS, firewall systems, password syntax, File Transfer Protocol (FTP) systems and Web servers [3]. The most recent information indicates that company wireless systems and Public Branch Exchange (PBX) systems should also be tested. Companies should also test other potential methods for accessing the computing, network resources and or obtaining information. These include physical access to the computing/network and backup areas in addition to social engineering access attempts.

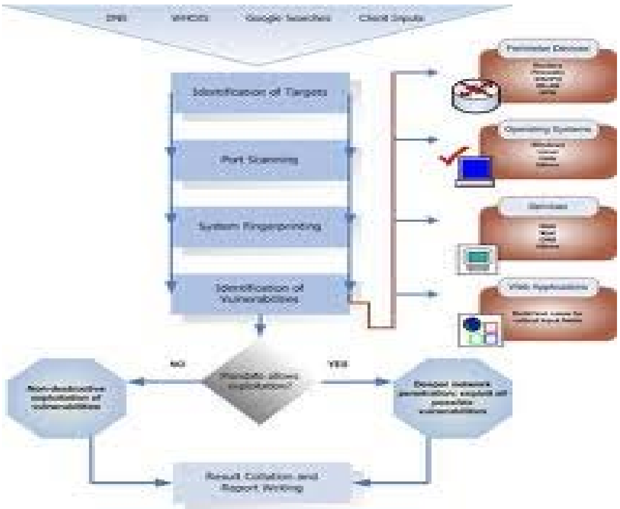
DNS
WHOIS
Google Searches
Client Inputs
Identification of Targets
Port Scanning
System Fingerprinting
Identification of Vulnerabilities
Perimeter Devices
Operating Systems
Services
Web Applications
NO
YES
Mandate allows exploitation?
Non-destructive exploitation of vulnerabilities
Deeper network penetration, exploit all possible vulnerabilities
Result Collation and Report Writing

Figure1: Penetration testing view preparing for the test

Prior to performing a penetration test an organization must have a Computer Security Policy. A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.” When writing a security policy, the value of the company’s information resources and assets should take into account and appropriate security processes assigned. The cost incurred to the company if the data was lost should be the primary factor in determining the appropriate security actions and processes that make up the policy. For example, if the company deals with government information or financial records, the process of deactivating the user ID might be performed differently than at a local college. Further, if a company had proprietary information, trade secrets or even customer lists that a competitor could utilize, a higher value should be assigned to this information and appropriate security steps taken.

The Security Policy should have information about:

□□ The connections to/from the Internet
□□ Dial-up connections
□□ Physical security access
□□ Password management
□□ User rights and responsibilities
□□ Administrator rights and responsibilities
□□ Protection of sensitive information
□□ Emergency procedures
□□ Documentation□Backups
□□ How people go about reporting a security issue
□□ Types of violations that should be reported
□□ Enforcement of the policy
□□ Who is ultimately responsible

VI. INTERNAL VERSUS EXTERNAL PENETRATION TESTS

The threat you are attempting to replicate should factor into the decision on how the test should be conducted, by whom (and to extent who should conduct the test). Tests intended to identify vulnerabilities with physical access or exposures to social engineering are referred to as **internal penetration tests**. Internal penetration tests are intended to determine what vulnerabilities exist for systems that are accessible to authorized network connections (or login Ids) that reside within the network domain of the organization. An internal test might better replicate the efforts a recently terminated employee might take when attempting to access valuable information. Conversely, **external penetration tests** are intended to identify vulnerabilities that are present for connections that have been established through the organization connection to the Internet (also known as the firewall or gateway) [4]. If the primary objective of the test is to ensure that the Payroll Database is sufficiently secure from the corporate Internet site, an external penetration test is more appropriate.

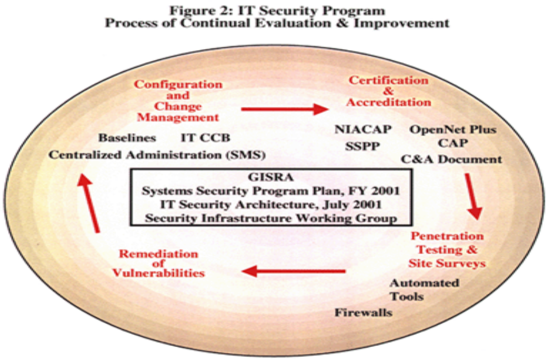
Figure 2: IT Security Program
Process of Continual Evaluation & Improvement
Configuration and Change Management
Certification & Accreditation
Baselines
IT CCB
Centralized Administration (SMS)
NIACAP
SSPP
OpenNet Plus
CAP
C&A Document
GISRA
Systems Security Program Plan, FY 2001
IT Security Architecture, July 2001
Security Infrastructure Working Group
Remediation of Vulnerabilities
Penetration Testing & Site Surveys
Automated Tools
Firewalls

Figure: 2

VII. SCOPE OF THE TEST

Following the selection of team (be it made up of internal staff or a third party) to
Perform the test, the scope of the test should be determined. This will provide the testing parameters that the team will use to identify the vulnerabilities. Some issues that should be determined include:

A. What is the time interval for the test?
B. Who will be notified of the test?
C. What will be used to confirm that unauthorized access was obtained?
D. What systems/resources will be initially tested and how?
E. Firewall configuration
F. Full knowledge (also known as with information)
G. Zero knowledge (also known as without information)
H. Host systems
I. Web servers
J. Production or development system?
K. Password selection
L. Trusts or shares between systems
M. FTP servers
N. Intrusion Detection system
O. DNS servers
P. Dial in modems
Q. Wireless access
R. Public Branch Exchange (PBX)
S. User ID deactivation or employee termination process
T. Physical access
U. Social engineering
V. Desktop computers
W. Password selection
X. Modems set for auto-answer and or remote access software
Y. How will the results be presented?
Z. When will another test be performed to confirm the results of the changes?

VIII. GATHERING INFORMATION ABOUT SYSTEMS (INVENTORY SCAN)

The Inventory scan process involves obtaining as much information as possible about the system that is targeted for the penetration test. Information of value: Operating System (including version number) in use, applications and application versions. With the Operating System and application specific information, only the known vulnerabilities that exist for the specific Operating System and or application need be tested[5][6]. This is the distinction between an indiscriminate address space probe for any open ports (also known as script kiddies) and an actual penetration test.

IX. EXPLOITATION OF VULNERABILITIES

The exploitation phase of the penetration test is performed by using a vulnerability scanner to identify problems with the configuration of a system. There are number of freeware and commercial tools that perform specific functions. The tools (subset of the tools mentioned include:

A. ***Nessus*** –A network vulnerability scanner tool for Unix systems.

B. ***SARA*** **–**The second successor to the **SATAN** vulnerability scanner tool (first successor was **SAINT**)

C. ***Firewalk*** **–**A traceroute like tool that allows the Access Control Lists of a firewall to be determined and a network map can be created.

D. ***John the Ripper*** **–**John is an active password cracking tool to identify weak password syntax.

E. **Crack / Libcrack –**A password cracking tool for Unix systems.

F. ***NAT (NetBIOS Auditing tool)*** –A tool to identify vulnerabilities in a NetBIOS configuration of a **NT** system.

G. ***Toneloc*** **–** A war dialer to check for modems on desktop systems that are set for auto-answer and or run remote access software.

X. PROVIDING THE RESULTS OF THE TEST

The results of the test should include solutions to reduce or eliminate the vulnerabilities. This is what differentiates a penetration test and a security audit. The significant vulnerabilities identified should be addressed first and a schedule determined to verify that the vulnerabilities have been addressed [8] [9]. The next department, network or system can then be selected for the same penetration testing process.

The solutions implemented will be dependent on the vulnerabilities identified, the loss to the company if conditions triggering the vulnerability occurred, and the cost (and effectiveness) of the available solutions [10] [11]. One solution might require that a new system running a web server must pass a vulnerability test before the web port is opened at the firewall. Another solution might require that all mail within the domain is sent to a central mail system and delivered to local host systems by the central mail server.

Enforcement of the existing policy might be the only condition required to address certain vulnerabilities [12]. In the case of desktop security, remote administration software might be already prohibited at the company. But a better job needs to be done to ensure compliance.

There will also be vulnerabilities that can be addressed by applying the most recent version of the application or operating system patch [7]. The results of the report should be closely guarded. If the information fell into the wrong hands, an unauthorized individual could exploit the recently identified vulnerabilities before the vulnerabilities have been addressed.

XI. TEST LIMITATIONS

Penetration test is just a snapshot of the systems and networks at a specific time. The test was only performed on the vulnerabilities that were known by the various tools or packages and on the systems accessible at that time. The process of application, system and network security is a continuous one because as soon as the test is complete, another system or application could be added to the business that might produce different results if the test were again performed.

XII. REFERENCES

[1]. Fraser, B “Site Security Handbook” September 1997 URL http://www.ietf.org/rfc/rfc2196.txt?number=2196

[2]. Herzog, Pete “THE OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL” May 25, 2001 URL http://www.ideahamster.org/osstmm.htm

[3]. Kaye, Krysta “Vulnerability Assessment of a University Computing Environment” May 28, 2001 URL http://rr.sans.org/casestudies/univ_comp.php

[4]. N/A “Risk Assessment Tools and Practices for Information System Security” URL http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML

[5]. Klikushina, Natalya “Firewall Penetration” URL http://shrike.depaul.edu/~mchen/420/natalya.html N/A

[6]. “Nmap Free Stealth Security Scanner” URL http://nmap.org

[7]. Corcoran, Tim “An Introduction to NMAP” Oct 25, 2001 URL http://rr.sans.org/audit/nmap2.php

[8]. N/A “Quality Security Tools” URL http://nmap.org/tools.html

[9]. N/A “Internet Security Systems” URL http://www.iss.net

[10]. Kurtz, George and Promise, Chris “Security Strategies” Information Security Magazine September 00 (also available at URL http://www.infosecuritymag.com/articles/september00/features3.shtml

[11]. Antionline.com - http://www.antionline.com/index.php?action=forums

[12]. Moyer, Philip “Penetration Testing: Issues for Management”. Computer Security Institute’s Alert Magazine March 1998 (also available at URL http://www.gocsi.com/penet.htm)