Global Information Assurance Certification Paper

Guidelines for Developing Penetration 'Rules of Behavior'

Introduction

Penetration testing has been well popularized by the media. Many companies are now offering penetration services to identify vulnerabilities in systems and the surrounding processes [4]. Several reasons are given for the popularity of penetration testing.. One of these is the mystique that has been associated with the 'hacker' image. In some instances, prospective target organizations may be attracted to this type of service more from the perceived value rather than the actual value. After the completion of the penetration test and the 'hacker' mystique dissipates, the target organization will be looking for substantive value from the penetration test such as corrective and improvement solutions. This may include in depth analysis of the penetration techniques with the target organization's information technology experts [8].

Alternatively, penetration testing has also become a commodity characterized by the performance of a series of substantive test procedures. In many industries, a penetration study has become a required audit. Under these conditions, penetration services may be perceived as low value. Accordingly, it is often necessary to review the specific test procedures and provide the necessary audit evidence to support conclusions drawn from the penetration test [8].

Regardless of the reason that draws the target organization to engage a 'tiger team' to simulate hacker network attacks, the penetration testing organization has many challenges in interpreting and delivering on the client's requirements. Clearly, understanding the target organization's expectations is the most critical part of planning and implementing the penetration test. The penetration 'rules of behavior' document serves an important role in formalizing the results of the planning phase for the penetration test.

What are Penetration 'Rules of Behavior'?

Penetration 'rules of behavior' are basically a test agreement that outlines the framework for external and internal penetration testing. Prior to testing, this agreement is signed by representatives from both the target organization and the penetration testing organization to ensure there is a common understanding of the limitations, constraints, liabilities, and indemnification considerations between the target organization and the assessment team throughout the penetration test [5].

The specific 'rules of behavior' are necessary to ensure that testing will be performed in a manner that will minimize operational impact while maximizing

the usefulness of the penetration test. The penetration rules will also serve to ensure that unplanned events are addressed through an incident response protocol [4].

Depending upon organizational legal requirements, a separate Release and Authorization form may be required (in addition to the 'rules of behavior') that states that the penetration testing organization will be held harmless and not criminally liable for unintentional interruptions and loss or damage to damage and equipment [6]

The Main Ingredients

The 'rules of behavior,' at a minimum, address the type of tests to be performed, the scope of the penetration test and the risks involved in performing a penetration test. The penetration rules establish the scope by defining targets, time frames, rules, and points of contact. They also provide authorization to proceed with the penetration test [5].

Limitations of Testing

In a penetration test, the test team plays the role of a hostile attacker who tries to compromise systems security. To do this, the team identifies potential holes with emphasis on the ones they believe are the most fruitful and least likely to be detected (from the attacker's perspective). At that point, the target organization sees what potentially could result from the exploitation of these vulnerabilities [8].

There are obviously severe restrictions on the validity of penetration testing -- largely related to time and expense issues of the penetration test, which may be conducted over the course of several days, or several weeks at most. A typical penetration test is not intended to be a comprehensive evaluation of security, since many security issues and configuration problems may not be identified [3]. As a result, the amount of information that can be gathered in a given time period is a major consideration in evaluating the validity of a given penetration test [4]. If the limited nature of a penetration test is not understood, the test can give the target organization a false sense of security.

Both the limitations of approach and techniques of attacks should be summarized and included in the penetration 'rules of behavior.' The limitations of attack serves to control the severity of penetration test procedures and the rigor in which it may be applied [4].

The penetration 'rules of behavior' should describe limitations of testing that are related to the objectives, approach, and techniques which have been agreed

upon when planning the penetration test. For example, generally, the target organization will want to limit the attacks to non-destructive methods, in which user accounts are not disabled and normal business operations are not disrupted. Also, the target organization will frequently require that penetration testing exclude denial of service attacks, which may disrupt Internet connectivity. Another limitation of testing may include the automated dialing of blocks of telephone numbers in search of auto-answering modems (also known as war dialing), which is outlawed in some states [6].

Criteria of Success

It is essential to determine the timing and conditions to start and complete the penetration study. No test procedures should be executed outside of the prescribed penetration study timeframe.

The 'rules of behavior' should be developed with success criteria in mind. An agreed-upon success state is necessary to determine when the suggested end conditions are met for the test. Once the success criteria is accomplished, all penetration attempts should be promptly and safely terminated [4].

Specific goals must be set for the penetration test. Some examples of goals include:

- Access to internal resources;
- Reading restricted files;
- Altering restricted files;
- Reading transaction data;
- Executing a program or transaction;
- Access to any user account;
- Access to supervisor privileges;
- Controlling network management systems; and
- Demonstrating ability to control resources [4].

Clearly, failure to properly define conditions for terminating the penetration test can result in unmet expectations, misunderstandings about successful penetration of security, or, probably, the worst possible outcome, a false sense of security [4].

Penetration Approaches

Penetration tests are typically aimed at environments prevalent in most organization, including Internet, intranet, extranet, and dial-up. While there are specific techniques for each environment, it is important to determine the type of

attack before executing the test and to document the approach in the penetration 'rules of behavior' [3]

At a high level, there are basically three types of approaches for penetration testing, a zero-knowledge test, a full knowledge test, and a partial knowledge test. In a zero-knowledge attack, the test team has no real information about the target environment and must generally begin with information gathering. This type of test is obviously designed to provide the most realistic penetration test possible [3].

In a partial knowledge test, the target organization provides the test team with the type of information a motivated attacker is likely to find, and hence, saves time and expense. A partial knowledge test may also be chosen if there is a specific kind of attack or specific targeted host that the target organization wants to have the test team focus on. To conduct a partial knowledge test, the test team is provided with such documents as policy and network topology documents, asset inventory, and other valuable information [6].

The last type of approach for penetration testing is a full-knowledge attack, in which the test team has as much information about the target environment as possible. This approach is designed to simulate an attacker who has intimate knowledge of the target organization's systems, such as an actual employee [3].

Techniques of Attack

The rules of behavior should describe the testing techniques for external and internal testing. A comprehensive description of these techniques is essential to minimize or avoid inadvertent damage or loss of information on the target systems.

Penetration methodologies may vary among companies providing penetration services, but the primary phases should basically be the same:

- **Discovery**, in which information is gathered on the target organization through Web sites and mail servers, public records and databases (Address and Name Registrars, DNS, Whois, EDGAR, etc.) [6];
- **Enumeration** in which the penetration team actively tries to obtain user names, network share information and application version information of running services [3];
- **Vulnerability mapping** in which the test team maps the profile of the environment to publicly know vulnerabilities [3]; and
- **Exploitation**; in which the test team will attempt to gain privileged access to a target system by exploiting the identified vulnerabilities [3].

Depending on the approach used, testing will consist of several phases, during

which various tools and techniques will be used to gain information and identify vulnerabilities associated with the target organization's computer systems and subsequent attempts to penetrate the network [1].

External penetration testing is conducted from a remote computer system to determine if potential vulnerabilities of Internet barriers (e.g., firewalls) are exploitable from the Internet. During the external network testing, the target organization maintains its normal network configuration while the penetration test team attempts penetration over the Internet from its testing laboratory. The assessment usually consists of external scans to determine the level of vulnerability and war dialing to identify telephone computer connections to the sites and to attempt to penetrate these connections [3].

Internal penetration testing is conducted using automated software, including scanning tools, to detect potential vulnerabilities in target organization's IS infrastructure. Network scans are performed to discover unknown or unauthorized devices and systems on the target network as well as to help point out unknown perimeter points on the target network (e.g., unauthorized remote access servers). Host-based scanners may also be employed to find vulnerabilities on servers that run critical file, email, web, directory, remote access, database, and other application services. To verify scan results, the penetration test team may also attempt to gain privileged access to resources on the internal network [2].

Examples of vulnerabilities that may be exploited during penetration testing include, but are not limited to: cracking of captured passwords, share access and exploitation of inherent system trust relationships, improper configuration problems, deploying 'sniffers' to capture passwords, keystroke loggers, trojans, and various computer forensic techniques that may reveal user and system login or account information [5].

Incident Response

Key representatives of the target organization and the penetration testing organization should be listed by name and role in the 'rules of behavior' document. The target organization is required to have a primary point of contact (as well as an alternate point of contact) available for assistance during the penetration testing and to provide any further coordination deemed necessary. This contact person will be fully aware of the testing scope and schedule and relevant details of testing procedures [4].

This contact will also be an integral part of the incident response process. It is important to document notification and escalation procedures for handling and resolving unplanned security incidents throughout the course of the penetration test in the event that certain alarms or events are triggered by the procedures

that the test team perform [4].

Reporting

Throughout the penetration test, the test team must maintain a detailed journal of activities to account for effects and results of the penetration testing procedures. This document will serve to distinguish the test team's activities from any other anomalies during the course of the penetration test. Additionally, the journal will serve as an audit trail to reference as needed in the restoration of original system configurations and states. Some techniques for journaling include the use of echo and logging during telnet or ftp sessions. When appropriate, the use of screen captures may be an option [5].

At the completion of the penetration test and depending upon the detailed reporting requirements agreed upon, the penetration test organization will provide the target organization with reporting documentation. Some of the information that may be provided to the target organization includes:

- the detailed results of the testing performed;
- what the results indicate; and
- recommendations on types of corrective actions [6].

In conclusion, if planned and executed appropriately, penetration testing can be a very useful tool for determining the current security posture of an organization. A well-planned penetration test can vividly illustrate the potential impact of exploited security vulnerabilities for the target organization's present business environment. Formal penetration 'rules of behavior', which document the results of the test planning phase, play a critical role for successful penetration testing.

References and Bibliography:

[1] Gula, Ron. "Broadening the Scope of Penetration Testing Techniques". July 1999. URL: http://www.network-defense.com/papers/pentest.html (13 August, 2001)

[2] Internet Security Systems. "Network and Host-based Vulnerability Assessment". URL: http://documents.iss.net/whitepapers/nva.pdf (13 August, 2001)

[3] Kurtz, George and Chris Prosise. "Penetration Testing Exposed - Part 3 'Audits, Assessments & Tests (Oh, My)'". September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features3.shtml (13 August, 2001)

[4] Moyer, Philip. "What to Demand from Penetration Testers". March 1998. Computer Security Alert. URL: http://www.gocsi.com/penet.htm (13 August, 2001)

[5] OUSPG Glossary of Vulnerability Testing Terminology. URL: http://www.ee.oulu.fi/research/ouspg/sage/glossary/ (13 August, 2001)

[6] Piscitello, David. "Your First Penetration Test". WatchGuard LiveSecurity. URL: http://www.corecom.com/external/livesecurity/pentest.html (13 August, 2001)

[7] Ryan, Dan. "Reality Check". April 16, 2001. Federal Computer Week. URL: http://www.fcw.com/fcw/articles/2001/0416/tec-ryan-04-16-01.asp (13 August, 2001)

[8} Winkler, Ira, "Audits, Assessments & Tests (Oh, My)". July 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/july00/features4.shtml (13 August, 2001)

Enclosure
[A] Penetration Test Sample Rules of Behavior