Penetration Testing

A Vital System Security Assessment Method

Prepared by:

Emad Nabbus

11417 Sunset Hills Road, Suite 228
Reston, VA – 20190
Tel: (703)-437-9451 Fax: (703)-437-9452
http://www.electrosoft-inc.com

November 2007

INTRODUCTION

NIST Special Publication 800-42 (Guideline on Network Security Testing) defines penetration testing as "*Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.*" Penetration testing is an attempt to exploit security weaknesses within a system or network in order to gain access to information for the purpose of reporting state of security of the system to the system owner.

Two differences used to distinguish a penetration tester from an attacker are:

1. **Intent**: A penetration tester's intent is to exploit security weaknesses in an information system or network with the intent of reporting findings to the system owner. The system owner will take this information and apply the appropriate measures to make sure all (or most) vulnerabilities are eliminated. This is in contrast with an attacker who will exploit security weaknesses with the intent of gaining access to information or disrupting service. Penetration testers have good intent while attackers have malicious intent.

2. **Permission**: A penetration tester has permission from the system owner to exploit security weaknesses while an attacker does not. Penetration testing must be performed with the permission and awareness of the system owner; however, testing does not need to be performed with the awareness of individuals who run the day to day operations of the information system. It is preferred that the individuals who are responsible for day to day operations not know to test what type of response they will have to a security breach.

REASONS FOR PENETRATION TESTING

There are many reasons why penetration testing should be performed which include:

1. **Identify vulnerabilities before someone else does:** The main reason penetration testing should be performed is to identify vulnerabilities in a system before an attacker identifies and exploits those vulnerabilities. If an attacker is able to exploit vulnerabilities within a system, the attacker will be able to gain information housed in the system or disrupt service. To a commercial entity or government agency, when information is accessed by attackers, the ramifications include:

    a. Damage to reputation: Government agencies are viewed as a source of authority to citizens. A successful attack on an agency could result in loss of reputation which could lead to a lack of effectiveness of that agency. In a survey conducted by the Ponemon Institute in November 2005, 58% of people said a breach had decreased their sense of trust and confidence in an organization.

    b. Financial loss: Many commercial entities such as banks hold financial data about many businesses and personal data about private citizens. These businesses and private citizens expect banks to protect their data. If an attacker is able to gain access to business information or personal information about customers, the reputation of the bank would be damaged and would result in financial loss. In another survey conducted by the Ponemon Institute in December 2005, 20% of consumers terminated a relationship with a company after being notified of a security breach.

    c. Personal safety: Various systems may hold data which if in the wrong hands, could be used to cause harm to those who the data pertain to. An example of such a case is a

system which may hold data about under cover agents out in the field. If information about the real names of these agents were captured by an attacker via exploitation of a security weakness in the system in which the data is housed, this could cause severe harm or even death to the agents.

2. **Verify configuration settings:** Another reason why a penetration test should be performed is to verify that the configurations and countermeasures in place that protect an information system actually work, as well as to identify misconfigurations. There have been many cases in which administrators misconfigure network equipment or servers which have led to security breaches. Penetration testing can provide management a view of how well the security configurations that are in place protect the data housed on the information system and whether or not there are any misconfigurations or configurations that were thought to secure the system, but actually do not.

3. **Liability:** When an attacker successfully breaches an information system, in many cases, the system owner is liable for all damages caused by the breach. The owner may be subject to a civil or criminal lawsuit. Generally, if it is found that the information owner was negligent in protecting the data, heavy fines and jail time may be a result. It is up to the system owner to prove that due diligence was performed on securing the data. Penetration testing is one way of proving that due diligence was performed and that the information owner was not negligent in protecting the data.

4. **Testing the reliability of third parties:** In many cases, commercial entities or government agencies contract third parties to provide a service. These services can range from network support to database services which are all susceptible to attacks. Commercial entities and government agencies risk their reputations by trusting third parties to provide these services. Penetration testing brings in an additional party to test the security provided by these third parties.

5. **Compliance with standards:** Finally, many commercial and government entities are subject to compliance with a required set of standards. For instance, the Federal Government must comply with the Federal Information Security Management Act (FISMA) of 2002. FISMA is meant to increase computer and network security within the Federal Government by requiring yearly audits. FISMA states "The head of each agency shall ensure that senior agency officials provide information security for the information and information systems that support operations and assets under their control, including through periodically testing and evaluation of information security controls and techniques to ensure that they are effectively implemented." To satisfy this requirement, government agencies require yearly vulnerability scans be performed on their systems as well as certification and accreditation (performed generally every 3 years or whenever a major change occurs to an information system). Although this is a great step, it is not comprehensive. Certification and accreditation (C&A) is a process in which auditors evaluate an information system based on 3 families of controls: Management, operational and technical controls (NIST Special Publication 800-53 has a detailed list of controls). At the end of the assessment, a Designated Approving Authority is given a report on the state of the system and based on the report, will let the system continue to operate or shut the system down. Vulnerability scanning is a part of this process but is also performed on a yearly basis. Vulnerability scanning utilizes an application that is run internally and scans for any vulnerabilities or misconfigurations such as vulnerable ports that may be open, weak passwords and missing patches. These scans do not test the configurations to verify that they are secure. Penetration testing goes one step further by testing to see if the controls in place are actually protecting the system. A comprehensive penetration test includes:

a. External testing: A penetration tester is positioned outside the "walls" of the information system and must attempt to gain access. This consists of:
    - Internet network testing
    - Dial-up testing
    - Social engineering
    - Wireless testing

b. Internal testing: A penetration tester is positioned inside the "walls" of the information system and must attempt to gain access to information that the tester does not have permission to access. This consists of:
    - Network Testing
    - Social Engineering

TESTING EXTERNALLY AND INTERNALLY

A common misconception about penetration testing is that it only includes external testing. Many people think "If someone cannot breach my security from the outside, my system is secure." This is a very dangerous line of thinking. The majority of security breaches are as a direct result of the users of the system whether it may be by mistake or on purpose. 1 in 3 users write down their passwords. This type of behavior by users leads to security breaches. A study conducted by Ponemon Institute and ArcSight in 2006 found that the average cost of insider data breaches is $3.4 million per business per year. Therefore, it is essential that an internal as well as an external penetration test be performed on any system.

FACTORS FOR FINDING VULNERABILITIES

It is important to note that penetration testing will not find all vulnerabilities. Just because a penetration test finds vulnerabilities, does not mean additional vulnerabilities do not exist. There are factors to finding vulnerabilities. They are:

1. **Time limit**: Penetration tests have time limits. A penetration tester has a specific amount of time to find and exploit vulnerabilities within a system. Attackers on the other hand have all the time in the world to find vulnerabilities and exploit them.

2. **New hardware and software exploits are found on a daily basis:** As vendors create security patches for their products, new vulnerabilities are found on a daily basis. Many of these vulnerabilities are not known until an attacker exploits them on a production system.

3. **Continuously changing configurations**: Many information systems go through configuration changes on a weekly or monthly basis. Some of these configuration changes open holes within the system that can be exploited by attackers.

Penetration testing is a vital security assessment method. It is an effective way to assess the security posture of any given information system. It is complimentary to the C&A process as well as to vulnerability scans and should be done on a yearly basis.

BIBLIOGRAPHY

1. Federal Information Security Management Act (FISMA), December 2002 http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

2. NIST SP 800-42, Guideline on Network Security Testing, October 2003 http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

3. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005, http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

4. http://www.entrepreneur.com/encyclopedia/businessstatistics/article82010.html