Penetration Testing Presentation Abstract and Outline
Sean Carrick
SSAC

Abstract
The purpose of this presentation is to provide an overview of the application of penetration testing to secure systems administration. As such, the presentation is not overly technical in scope, but covers instead what penetration testing is, what benefits stakeholders in a secure system receive from a test, and how policies can aid or hinder penetration testing.

Penetration testing is a specialized security auditing method where a tester simulates an attack on a secured system. The goal of this is not to cause damage, but instead to identify attack surfaces, vulnerabilities, and other security weaknesses from the perspective of an attacker. Such testing can range across all aspects of a system; the areas of computer, operational, personnel, and physical security can all encompass potential weaknesses that a malicious attacker can exploit, and thus a penetration tester may examine. Depending on the organization's priorities, risk assessment, and policies, some of these areas may be out of scope or not deemed as important, so a reduced scope penetration test may be conducted.

The presentation goes into an example procedure for penetration testing, detailing the steps of footprinting, scanning, enumeration, exploitation, maintaining access, and cleaning tracks. These represent the steps that attackers use in common attacks, with divergences between an authorized tester and an attacker's steps noted. These differences come from the frequent necessity that an authorized tester not damage the system in the process of testing, particularly on a live production system.

Benefits attained from penetration testing are an increased knowledge of a theoretical threat's perspective on the system, and the ability to demonstrate the potential damage that an actualized vulnerability represents to the organization. Viewing a vulnerability offensively allows a different picture of the system's infrastructure and security controls, and the actual exploitation of vulnerabilities can reveal more than a simple checklist audit. For example, it may not be readily apparent that a breach in security for the website could allow financial data to be accessed, but this could be discovered during a test. Tests also allow a system administrator to know what areas their defenses are working in, in addition to where there is room for improvement.

Finally, this presentation also discusses briefly the policies that relate to penetration testing. Some organizations have a specific Vulnerability Assessment or Penetration Testing policy, but others include testing in a more general security policy or acceptable use policy. It is important than the users of the system understand potential dangers and results of security testing, and that an organization is protected by potential complications that arise from testing. Another matter of policy is that penetration tests are often performed unannounced in order to test the readiness of disaster recovery or security personnel, but someone known needs to be accountable for the testers' actions and serve as a point of contact in the case that issues arise.

Outline
Penetration Testing
  ● Sean Carrick
Overview
  ● What is penetration testing?
  ● Why is this kind of testing useful?
  ● How can policy support penetration testing?
Penetration Testing
  ● Definition – a specialized security auditing method whereby a tester simulates an attack in order
to test system security

- Synonyms – Ethical Hacking, Vulnerability Assessment, Offensive Security

**White Hat vs Black Hat**

- A key difference between a penetration test and an actual attack is that the penetration tester is trying to demonstrate vulnerabilities without causing damage
- This is often referred to as White Hat hacking.
- Any hacking attempt without authorization is an attacker, from an organizational perspective.

**White Box vs Black Box**

- White Box - Penetration tests may be performed with full knowledge of the system provided.
  - In the case of a computer network, this would mean the testers have access to the network map, knowledge of what systems serve which purposes, and other insider knowledge.
- Black Box – No prior knowledge of the system to be tested

**Penetration Testing Procedure Overview**

- 1. Footprinting
- 2. Scanning
- 3. Enumeration
- 4. Exploitation
- 5. Maintaining Access
- 6. Cleaning Tracks

**Footprinting**

- The tester gains as much knowledge of the system as possible, generally without direct interaction.
- Differs between black and white box testing
- Examples

**Scanning**

- Using the knowledge gained in footprinting, the tester probes subsystems and gains further knowledge of how the system operates by interacting with it.
- Examples

**Enumeration**

- The tester uses the scanning results to identify specific targets and vulnerabilities in the system.
- Examples

**Exploitation**

- The tester exploits the vulnerabilities in order to circumvent security controls and gain access to the secured areas of the system
- Examples

**Pivoting & Maintaining Access**

- After gaining access, an attacker typically leverages the target system to ensure that continued access is possible
  - Testers may avoid this step depending on scope
- Additionally, the attacker may use their new privilege and vantage point in the system to attack other subsystems.
  - Likewise, testers must be wary of the test's scope
- Examples
  - Rootkits
  - Trust Relationships

**Cleaning Tracks**

- After a successful attack, an attacker typically scrubs or deletes log files, hides backdoors, and generally makes it difficult to forensically analyze the attack.
- Testers may be better off recording what modification to the logging abilities is possible, but not modify the logs.

Examples

Benefits of a Penetration Test
- Penetration tests provide a different view from the defensive security position
- “Thinking like an attacker”
- This form of testing allows an idea of what damage vulnerabilities can cause before an attack happens, allowing better targeting of security controls and mitigations.

Policy Pitfalls and Benefits
- Authorization to test is needed
- Internal or External Pentesters?
  - Confidentiality issues
  - Testers may have the keys to the kingdom in terms of compromising an organization.
- Acceptable Use/Monitoring Policy

Conclusion
- Penetration testing is a very useful tool in testing system security, but even an unsuccessful penetration test does not ensure system security.
- Related: there is no truly secure system that is also usable