Penetration Testing vs. Vulnerability Assessment

The Confusion
There seems to be a certain amount of confusion within the I.T arena about the differences between Penetration Testing and Vulnerability Assessment, they are often classified as the same thing when in fact they are not. Penetration Testing does sound a lot more exciting, but in our experience we have found that most clients actually require a comprehensive Vulnerability Assessment or V.A. and not a more intrusive Penetration Test.

They are similar projects and do cover many of the same bounds, the main different being a Penetration Test is more aggressive and more intrusive, it actually goes one step further and involves trying to technically break into the systems or servers and prove they are vulnerable.

The problem with this is it can be risky as exploits are making use a flaw in the software running or the operating system so can cause instability, when we are testing the live servers of a client this is the last thing we want to happen.

The Penetration Test
A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.

In case of PT

• A set of procedures designed to bypass the security controls of a system or organization
• Real life test of the organization's exposure to known security threats
• Performed to uncover the security weakness of a system
• Focuses on exploiting network and systems vulnerabilities that an unauthorized user would exploit
In this case the security auditor or the penetration tester not only has to scan for the Vulnerabilities in the server or application but also has to exploit them to gain access to the remote server.

PT Scope Includes:

- The PT test is done both internally and externally
- Vulnerabilities are exploited
- Dangerous attacks like DOS and Buffer Overflow attacks are used depending upon the customer’s willingness to do so
- Automated vulnerability scanning tools and as well as exploits are used

The Vulnerability Assessment

Most clients actually want a Vulnerability Assessment, even though they may label it a Penetration Test. In the majority of cases the systems we are testing for flaws are live
production systems and can't afford to be disrupted by active exploits which might crash the system or cause some kind of unpredictable behaviour or instability.

Vulnerability assessment is a much broader term and can be applied to many things; it's related closely to Risk Assessment (Also involved in Business Continuity Planning and Disaster Recovery Development) and involves the process of identifying and quantifying vulnerabilities in a system. In this case it's technical vulnerabilities within the system known as exploits. These of course put the systems at risk.

In this case the security auditor has to only scan for the vulnerabilities in the server or application and filter out the false positives from the scan output by mapping them with the actual vulnerabilities associated with the target host.

VA Scope Includes:
• The VA test can be done both internally and externally
• No vulnerabilities are exploited
• No dangerous attacks like DOS and Buffer Overflow attacks are used
• Automated vulnerability scanning tools line Nessus, Retitiina are used

**Summary**

• Vulnerability Analysis is the process of identifying vulnerabilities on a network, whereas a Penetration Testing is focused on actually gaining unauthorized access to the tested systems and using that access to the network or data, as directed by the client.

• A Vulnerability Analysis provides an overview of the flaws that exist on the system while a Penetration Testing goes on to provide an impact analysis of the flaws identifies the possible impact of the flaw on the underlying network, operating system, database etc.

• Vulnerability Analysis is more of a passive process. In Vulnerability Analysis you use software tools that analyze both network traffic and systems to identify any exposures that increase vulnerability to attacks. Penetration Testing is an active practice wherein ethical hackers are employed to simulate an attack and test the network and systems’ resistance.

• Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is just a process of identifying and quantifying the security Vulnerabilities in a system. Vulnerability Analysis doesn’t provide validation of Security Vulnerabilities. Validation can be only done by Penetration testing.
The scope of a Penetration Testing can vary from a Vulnerability Analysis to fully exploiting the targets to destructive testing. Penetration Testing consists of a Vulnerability Analysis, but it goes one step ahead where in you will be evaluating the security of the system by simulating an attack usually done by a Malicious Hacker.

For instance a Vulnerability Analysis exercise might identify absence of anti-virus software on the system or open ports as a vulnerability. The Penetration Testing will determine the level to which existing vulnerabilities can be exploited and the damage that can be inflicted due to this.

A Vulnerability Analysis answers the question: “What are the present Vulnerabilities and how do we fix them?” A Penetration Testing simply answers the questions: “Can any External Attacker or Internal Intruder break-in and what can they attain?”

A Vulnerability Analysis works to improve security posture and develop a more mature, integrated security program, where as a Penetration Testing is only a snapshot of your security program’s effectiveness.