Vulnerability Scanning

This is also known as Network Vulnerability Assessment (NVA), and can be undertaken against external facing systems, that is, a system which can be addressed over the Internet, for example a Corporate Web Server. They can also be conducted on the internal segments of a target network where Database Servers or Intranet Servers are located.

They are a quick and cost effective way of identifying many of the common exploits that may exist in the client's infrastructure. These range from Windows NT Servers running old or out of date services patches, to Web Servers with vulnerable CGI code or that have development code still installed.

This type of test cannot hope to find all possible types of vulnerabilities that might exist and the results are not normally validated.

Tools used for these types of Scan are normally of the commercially available type, and unless time or the severity of the exploit is sufficiently high, no further validation of the results is undertaken.

A Port scan of the relevant Systems is conducted over a range of well known TCP and UDP Ports. These cover such services as, FTP, Telnet, HTTP, POP3, CIM, Socks, and many others as well as a range of default well known ports used by Trojan and Back Door programs 12345 and 31337 for example.
The list is not definitive. The port scan is used to provide a certain validation when compared with the Vulnerability scanners output.

Penetration Testing (Pen Test) IT Health Check

This Service is often known as Vulnerability Scanning in the United States and the terms can lead to confusion.

With a Pen Test, a far more in-depth set of tools and tests are run against the target network. As with Vulnerability scanning, this type of assessment can be run against External or Internal IT systems.

These tests are far more rigorous than the basic Vulnerability Scan and as a consequence can take far more time to complete and for the data to be analysed. For example, it can often take over a day to map a Firewall and in the case of a professionally configured one it is often impossible to produce useful data.

As with Vulnerability Scanning, a Port scan is conducted against the target infrastructure but is far more comprehensive, covering the full 65,535 TCP ports if required. Other custom tools are run against the Firewall(s) and Router(s) in an effort to map the rules and identify the type(s) of the Operating Systems and suppliers.

Commercial Vulnerability scanners are used to provide a quick bulk assessment of the target architecture and potential vulnerabilities.

The results from these types of 'scans' are then used to allow targeted investigation using tools from the Open Source and both 'Black Hat' and 'White Hat' communities.
They are used to confirm that the vulnerability does in fact exist and is apparently exploitable. Denial of Service (DoS) type attacks are not within the scope of the Pen Test.

Ethical Hacking

This is term used for the 'anything goes' type test.
It is as close as possible to a real hacker or disgruntled employee attacking your internal or external networks. Any method can be valid including social engineering, theft of back-up tapes, telephone taps and room bugging.

Terminology

Hacker

A hacker is the term given to a person or group who attempt to gain access to a computer system and either control it or view/remove information from it.

Hackers have gained notoriety in the popular press over the past few years and the meaning of the term has changed. In the 'old' days of Unix systems, a hacker was considered as one who had a strong understanding of the system and could 'hack' up code to solve problems. The old school hacker did not attack systems or destroy them; they were the guru's of the day. Nowadays, the term hacker has come to mean computer criminal, a person who attacker computer systems for fun or profit.

Script Kiddie

The script kiddie is a modern term, and covers the large number of not so technical computer literate attackers. They use scripted or automated programs, hence the term script kiddie, and often have less technical knowledge than many system administrators or network administrators. The scripted attacks, commonly written to run from Windows Operating System platforms (Win32) require no more work than to enter a range of IP addresses of systems to target. This group are the ones who create all the 'hacker' hysteria in the press.

Vulnerability

This is the term given to hole or bug in a program or the Operating system code. Vulnerabilities can vary in severity from low, where little damage can be done to the system, to high, where the attacker, by exploiting this vulnerability, can gain system level control or the vulnerable system.

Exploit

An exploit is the name given to the method of leveraging a vulnerability, this is normally achieved using exploit code but can be as simple as entering a mis-formed URL into the web browser.