PENETRATION TESTING (MANUAL AND SCANNING)

Penetration Testing is usually referred to as testing by an ethical hacker/penetration tester to break into a target network, application or web site with limited information about the target. It is called a black box test.

It requires the bare minimum of information about the targets, usually just the IP addresses, or URL (website address) of the targets to be tested. The testing is performed using a penetration testing tool kit which can comprise of hundreds of custom, commercial and open source tools.

The testing has a very high involvement of a well trained and experienced security tester. The results of a penetration test will usually be free of false positives, and on request, the tester will also conduct exploits and chained exploits on the target systems. Penetration testing can also be conducted on internal networks and on wireless networks. Social engineering techniques may also be used.

Penetration Testing plays an important role in securing Enterprises by verifying the efficacy of existing security measures and mimicking real world network and application attacks by malicious hackers or rogue internal employees. A manual penetration test will start with automated scanning to provide and initial idea of the obvious vulnerabilities, but is no more than a guide and a manual test will find threats that automated scanning will never find.

VULNERABILITY SCANNING

Vulnerability scanning usually refers to running an automated vulnerability scanner against a block of IP addresses or targets. The manual component is limited to the coordination and scheduling of the scanner and delivery of the automated report. The reports are very detailed and long, but are not free of false positives. The extent of false positives would depend on the accuracy of the selected vulnerability scanner.

The scanning process is very quick and generally can be conducted at a pretty low cost by less experienced people. The scanners are sold as perpetual licenses and on subscription in a software-as-a-service model. Vulnerability Scanners play an important role in securing organisations as a key component of security vulnerability management programs, and are ideal for running on say a quarterly basis in between full manual tests. But they are NOT a replacement for a full manual penetration test.

PROS AND CONS

	PENETRATION TESTING	VULNERABILITY SCANNING
GOAL	Use Manual Penetration Testing to verify if networks, applications and websites are secure, what does a hacker see, discover unknown security flaws. Do quarterly or at least annually	Implement Vulnerability Scanning as part of an overall vulnerability management program. Do monthly or at least quarterly.
TOOL TYPES USED	Automated Scanners, Proprietary Tools, Exploit tools, experienced security testers	Automated Vulnerability Scanner
MANUAL COMPONENT	Extensive	Negligible
FALSE POSITIVES	Removed	Present
EXPLOITATION	Yes, on request	No
CHAINED EXPLOITS	Yes, on request	No
DURATION	Days to Weeks	Hours to Days
FLEXIBILITY TO CLIENT NEEDS	High	Low
RECOMMENDED BY REGULATORS	Yes	Only as an interim test between full manual testing. Not a replacement for manual penetration testing