Penetration Testing

Penetration testing has gained almost universal support within the security industry as a valuable tool for highlighting an organisation's security exposure. It uses tools, methods and techniques similar to those used by the "hacker" community to test networks and systems. But are all penetration testing services the same? The scope, levels of automation, tools and deliverables can vary greatly between providers. These factors in turn affect the quality and value of the offering.

Determining the Scope

A comprehensive test needs to include all networks owned by the organisation and incorporate testing against the infrastructure, operating systems, applications, and custom written web applications contained within the environment. Custom web applications are often ignored, yet over two thirds of all attacks now occur at this layer. Problems such as SQL injection and Cross-site Scripting are a serious threat and are being actively exploited in the wild. Once vulnerabilities have been identified as part of a test, they should be exploited in a controlled fashion to highlight the true risk and access that can be obtained. This is the major distinction between a vulnerability assessment and a penetration test.

Automation vs Manual Testing

The number of identified security vulnerabilities and rate at which new vulnerabilities are detected has reached the point where complete manual testing is no longer practical. Although automated testing tools can significantly reduce cost and human error, automated tools can also make mistakes. It is not uncommon to see platform specific vulnerabilities reported by automated scanners against an unrelated technology. Manual testing by an experienced tester in conjunction with automated testing is the key to reducing false positives, and no-one likes receiving a report documenting vulnerabilities that don't actually exist!

Penetration Testing Tools

Relying on a single tool is rarely the best approach, yet many providers follow this practice as it saves time and simplifies reporting. e.g. Using Nessus which is a popular free scanner. In these cases, you may get better value if you download the tool and run it yourself - and you should be doing this on a regular basis anyway. Using a suite of tools ensures that results are verified and cross-referenced whilst minimising false positives and negatives.

Deliverables

This is a written record of the work undertaken and needs to clearly state the work performed and recommended remedial actions. To have real value, it also needs to be written within the context of an organisation's business and operating environment. Failing to consider these elements generally leads to some risks being overstated while others are downplayed. This is a common complaint with pre-canned reports issued by some providers.