Introduction to Penetration Testing

What is Penetration Testing?

A Penetration Test, also known as a Pen Test is a legal attempt at gaining access to your protected computer systems or networks, often conducted by a third party organisation. The purpose of the test is to identify security vulnerabilities and then attempt to successfully exploit them in order to gain some form of access to the network or computer system.

Should a successful compromise take place, the flaw/vulnerability is classified into a threat level for the organisation; typically low, medium or high. Most penetration tests are concluded with a detailed report on the security findings along with remedies for the threats.

What are the most common types of Penetration Tests?

Two of the more common types of penetration tests are black box and white box penetration testing. In a black box test, no prior knowledge of the corporate system is given to the third party tester. This is often the most preferred test as it is an accurate simulation of how an outsider/hacker would see the network and attempt to break into it. A white box test on the other hand is when the third party organisation is given full IP information, network diagrams and source code files to the software, networks and systems, in a bid to find weaknesses from any of the available information.

Should I hire a Penetration Tester?

Often, this comes down to the size of the organisation and level of funding available to put into the security side of the business. Most penetration tests are priced by IP/node or amount of time estimated the project will take to complete. It also depends on the type of test you ask for. Certain types of tests can be conducted automatically, whereas others require a lot of manual work to validate certain security standards.

Typically for a small to medium website, a penetration test would start at around $1000-$2000 and scale upwards from there.

What are the advantages of a Penetration Test?

Having a penetration test conducted can be extremely useful to people who wish to get extra reassurance when it comes to critical web facing systems, however they can also be useful in a variety of other ways, such as:

- Testing a System Administrator to see if he is keeping systems updated and secured.
- Compliance & the Payment Card Industry (PCI), when operating an online payment system.
- Risk reduction and risk mitigation factors for insurance or other industries.
- Protection of Confidentially, Integrity and Availability (CIA triad) of data

Are there alternatives to Penetration Testing?

Yes, there are network scanners available, however if you don't know enough about the security results displayed in a scanner or how to confirm the results are not false positives, it is highly advised you seek out professional help, rather than taking a chance and putting your business at risk.

Conclusion

A penetration test is useful service if your business can justify the expense and importance of having its web facing equipment properly secured. Rest assured that cybercrime is a growing problem, costing business and the government millions each year. The cyber criminals don't look to be giving up anytime soon and with all this money to be made by them online, who's to say your business won't be next?

Interested in getting a Penetration Test? For further information please visit:

www.security-audit.com

Penetration Testing

Security Audit Systems.