Article

Sep 2022

Is Pentesting The Same As Hacking?

The short answer is yes. Does that make you a little surprised?

Iain Batty
Technical Security Assessment Lead
Email iain.batty@waterstons.com

The short answer is yes. Does that make you a little surprised?

However, this bears some explanation, as while their methodologies may be similar, motives and purposes are completely different. Keep reading, as we differentiate the key terms so you don't get caught out.

What is pentesting?

Pentesting, also known as penetration testing or ethical hacking, is the process of testing a computer system, network, or web application to find security vulnerabilities that could be exploited by threat actors. The main goal of pentesting is to identify weaknesses and vulnerabilities so they can be fixed before attackers have a chance to exploit them.

It can be used to test both external and internal systems. External pentesting focuses on testing how well a system can withstand attacks from outside its network, while internal pentesting assesses how well it can defend against attacks from inside its network.

Pentesting can be performed manually, with automated tools or both. Incorporating both manually & with automated tools is often considered more effective because it allows testers to get a better understanding of a system and it's potential vulnerabilities.

Automated tools speed up the process of identifying low hanging fruit leaving security engineers with more time to discover complicated or obscure vulnerabilities often missed by automated scanning tools. All reputable pentesting companies like Waterstons uses a combination of tools and internal intelligence to bring together the best results.

What is hacking?

Computer hacking is the practice of modifying computer hardware or software to achieve a outcome unintended by the original designer. Regardless of the motivation, hacking requires a deep understanding of how computers work and how to exploit their weaknesses.

Used for malicious purposes, hacking can enable the stealing personal information, destroying or modification of data, denying access to a website or even the encryption of sensitive documents or whole networks and holding them to ransom.

While some hackers use their knowledge for criminal purposes, others use their skills to help organisations to test for vulnerabilities and improve their security systems. In either case, computer hacking is a complex and sophisticated form of electronic trespass.

While hacking and penetration testing may pull from the same skill set and rely on a similar mindset to be successful, a good penetration test will follow a set of methodologies and processes, have repeatable findings and be thoroughly documented. Ultimately a pentest is about helping a business understand the efficacy of the security controls it has in place and the improvement of those controls over time.

Is your enterprise ready to put it's controls to the test?

Speak to Waterstons about how we help your company reach it's cyber security goals.

info@waterstons.com.au