Attack Simulation and Penetration Testing

What are the differences and why would you need both?

Attack Simulation and Penetration Testing are two types of Security Testing activities that share some similarities but also have key differences. In this paper, we will discuss those differences and demonstrate why a mature organization would still require both types of testing, albeit under different circumstances, and how each can be used to satisfy different requirements and provide value to the organization.

A penetration test is a technical assessment designed to identify vulnerabilities which may exist on a specific asset, or set of assets, for an organization. In this context, an asset could be anything from an external perimeter network, an internal network, an active directory environment, a web or mobile application, or indeed, it could be a specific device or software solution which is in place. The penetration test is squarely aimed at a 'known technical scope' providing a picture of how exploitable those in-scope assets are. Additionally, an organization is often aware of the penetration test taking place and so is likely to ignore the testing activities and any alerts generated from defensive technologies in-place.

By contrast, the scope of an Attack Simulation is not a specific set of assets, but an authorized attack aimed at the whole organization, ensuring all domains of information security (people, process and technology) are generally in scope.

The Attack Simulation seeks to mimic the actions of a determined real-world attacker and achieve specific, pre-agreed objectives by emulating the Tactics, Techniques and Procedures (TTPs) of the most pertinent threats an organization is likely to be facing. It should be noted that the defensive teams are not typically notified of the Attack Simulation taking place and therefore these types of assessment can also be used to measure an organizations' ability to respond to any threats it faces.

If we compare both assessment types side-by-side, we will see some differences:

Characteristic	Penetration Testing	Attack Simulation
Security assessment	✓	✓
Attacker behaviour	✓	✓
Specific adversary simulation		✓
Asset based scope	✓	
Cross-domain scope		✓
Identify all vulnerabilities	✓	
Identify key vulnerabilities and attack paths		✓
Evade technical security controls and defensive tools		✓
Organisational awareness (prior notification)	✓	
Defensive capabilities assessed		✓
Assessment of organizational security posture and maturity		✓

As the table shows, Penetration Testing would still be a very useful tool for when a client has a requirement to perform an in-depth evaluation of any security controls that have been implemented to protect specific assets against attack. They are generally shorter term than an Attack Simulation and provide validation of efforts that have been made to secure the in-scope targets. In contrast to Penetration Testing, Attack Simulation is a targeted assessment looking at the whole organization as one with a view to determining how ready the target organization is to a real-world cyber-attack and how well their defences stand up to emulation of particular adversaries.

In conclusion, Penetration Testing continues to be a well-established and very useful tool for organizations that would like an in-depth evaluation of the implemented security controls in place on their assets. Attack Simulation engagements, on the other hand, are particularly useful for determining an organizations ability to detect and respond to a real-world attack before one happens.

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com/cyber-uk

IE/International

Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie