PENETRATION TESTING

VS

RED TEAM TESTING

Finding, evaluating and exploiting vulnerabilities in one dimension.	Finding, evaluating and exploiting targeted and objective driven vulnerabilities.
A penetration test generally involves using a static methodology where testers use commercial pen test tools.	A Red Team test involves using a flexible methodology where the team is encouraged to think creatively and use anything at hand for testing.
The security team and employees in the organisation are warned about the test taking place.	The security team and employees are not given any notice about testing taking place.
Finding and exploiting vulnerabilities.	Measuring the business's ability to identify and respond to attacks.
Test targets are predefined.	Test targets are fluid and cross multiple domains.
Systems are tested independently.	Systems are tested simultaneously.
Identification of exploitable vulnerabilities are assessed based on their level of risk to the organisation with remediation advice and technical recommendation.	Testing people, process & technology shows a 360° view of the organisation's overall security — detection & response capabilities, logical & physical security (includes key issues recommendations).

riskcrew.com

+44 (0) 20 3653 1234