secarma®

Red Teaming: Glossary

TERM	DESCRIPTION
Penetration testing	The term has evolved into a methodical testing regime for networks, applications, devices, etc. Typically 5-20 days' duration, it's often used to refer to a single offensive style security test on a single target. Phases include Scoping, Information Gathering, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting. The term can refer to physical or cyber penetration.
Red teaming	Typically campaign/goal-based and broader in scope, focusing on improving security posture organisation-wide by simulating higher level and better-resourced threat actors. Due to their more dynamic nature they are not easily repeatable, and technically they are often quieter to avoid alerting security operations. Test duration is often 2 weeks to 6 months (not always continuous) and can include penetration tests.
Blue team	The Defenders. The internal security team that defends against both real attackers and Red Teams. Different from standard security teams, in that they have a mentality of constant vigilance against attack.
Red team	The Attackers (or Aggressors). External entities brought in to test the effectiveness of a security program, mimicking the behaviours and techniques of likely attackers in the most realistic way possible.
Purple team	Usually a combination of both existing Red Team and Blue Team members coming together.
Scope	The details of the engagement. Including (but not limited to) the dates of testing, system names, tester information, rules of engagement, and reporting requirements. Often a formal document containing everything needed to perform testing activities and provide legal authorisation for testing.
Rules of engagement	The rules by which the testing activity will be governed. Includes specific types of techniques to be performed (such as SQL Injection testing) as well as activities to avoid (such as denial of service). Can be as detailed as needed.
Pre-test activities	Actions taken before security testing begins. Determining target details, type of testing, rules of engagements, cost, reporting, approvals, and any other information needed before testing can take place.
Post-test activities	Actions taken after security testing ends. Involves analysing the report, communicating results to stakeholders, planning remediation of findings, and including trending results to be used in other areas of the target system organisation, or for determining future potential targets.
Reporting	The results of the testing activity. Can be in any format required and is customisable. It is important to include every finding from the testing activity in detail, with importance on technique, details of exploitation, and recommended forms of remediation.

Continued overleaf...

TERM	DESCRIPTION
Active testing	A style of testing that uses techniques more likely to be discovered by existing defensive measures. Examples include sending known malicious commands to a target system, or flooding it with excessive amounts of data. Useful for exploiting vulnerabilities.
Dumpster diving	While the term can literally refer to looking through trash, it is used more often in the context of any method (especially physical methods) by which a hacker might look for information about a computer network.
Exploitation	Leveraging a vulnerability to perform activities to gain extra or further access to information, systems or resources.
Flags	A capturable entity, such as a database or document.
Hacking	A term often associated with penetration testing and red teaming activity. Taking action against a target system for the purposes of discovering vulnerabilities and exploiting them to perform unauthorised actions.
Hostile Reconnaissance	The purposeful physical observation of people, places, vehicles and locations with the intention of collecting information to inform the planning of a hostile act against a target.
KPIs (Key Performance Indicators)	The key factors by which the testing activity is measured for success. Should include factors controllable by the activity – such as timing and cost – not factors such as required number of findings per test.
Metric	Similar to a KPI, but often of less importance to specific activity success, or related to factors outside of testing activity control. Can include items such as Time To Detect (TTD) and Time To Mitigate (TTM).
OSINT (Open Source Intelligence)	Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access.
Passive testing	A purely observational style of testing that uses techniques likely not to be detected on the target system, or by other defensive measures that might exist. The primary purpose of passive testing is stealth. Useful for detecting vulnerabilities, less so for exploitation.
Persistence	The process of ensuring future access to a system or resource. An example is installing a back door exploit kit or creating a user on the target system after exploiting a missing patch to gain initial access, so it can be accessed again in the future.
Requirements	Specific details that the testing activity must include. This normally takes the form of reporting, but can include things like timing windows for activity, specific techniques to be used or aspects of the testing target.
Social engineering	An attack vector that typically involves manipulating people into breaking normal security procedures and best practices to gain access to systems, networks or physical locations, or for financial gain. Can be conducted online (typically through social media profiles), over the phone (such as Vishing) or in person (such as tailgating, piggybacking, eavesdropping or shoulder surfing).
USB drop	A USB device left for people to find and plug into their computers. Typically it will contain one of three types of attack: malicious code, social engineering (the file takes the thumb drive user to a phishing site) or HID (Human Interface Device) spoofing.
Vulnerability	A weakness in a system or environment that can be exploited. It can be the result of missing patches, poor coding, or a combination of wider factors.