Perspective Matters

To Best Calculate Exposure Risk, Understand the Security Approach

By Ted Harrington, Executive Partner
Independent Security Evaluators (ISE)
5 December 2013

Abstract:
To improve the security posture of digital systems, progressive organizations engage third party security experts to assess risk and provide hardening guidance. The most suitable approach for most industries is *white box vulnerability assessment.* However, confusion about different security approaches has led IT executives to commonly request the notably ineffective approach of *black box penetration testing*. Most executives may be surprised to discover that this approach actually undermines the very risk assessment objectives they seek to achieve. This article will analyze trends, contrast different tests and methodologies, and outline best practices.

	BLACK BOX	WHITE BOX
PENETRATION TEST	**Risk Confidence:** Low **Goal:** Breach Defenses **Knowledge:** Incomplete **Term:** Short **Scope:** Known Vulnerabilities **Automation:** Heavily Used **Suitability:** Casual Attackers **Results:** Incomplete **Tailoring:** Commodity **Pricing:** Highly Variable	**Risk Confidence:** Medium **Goal:** Breach Defenses **Knowledge:** Complete **Term:** Short **Scope:** Known Vulnerabilities **Automation:** Heavily Used **Suitability:** Casual Attackers **Results:** Incomplete **Tailoring:** Commodity **Pricing:** Slightly Variable
VULNERABILITY ASSESSMENT	**Risk Confidence:** Low **Goal:** Identify All Weaknesses **Knowledge:** Incomplete **Term:** Medium to Ongoing **Scope:** Entire System **Automation:** Minimal Use **Suitability:** Targeted Attacks **Results:** Incomplete **Tailoring:** Custom, Manual **Pricing:** Highly Variable	**Risk Confidence:** High **Goal:** Identify All Weaknesses **Knowledge:** Complete **Term:** Medium to Ongoing **Scope:** Entire System **Automation:** Minimal Use **Suitability:** Targeted Attacks **Results:** Complete; High Value **Tailoring:** Custom, Manual **Pricing:** Firm

White box vulnerability assessments provide the most accurate barometer by which to determine and mitigate risk of digital asset exposure. Recently however, entertainment IT organizations have demonstrated a preference for the far lesser effective approach of *black box penetration testing*. This incongruous situation may be a result of confusion, wherein executives procuring security guidance (and even some firms providing such guidance) do not fully understand the distinction between different evaluation types and methodologies. In this article, we attempt to disambiguate the terms and analyze the trend.

Evaluation Types

An evaluation is an investigation of security features and functionality. Although there are many different types of evaluations, the two most relevant to most industry use-cases are *vulnerability assessment* and *penetration test*.

The objective of a *vulnerability assessment* is to determine the full scope of exposures that exist – quite simply, a *vulnerability assessment* is a risk assessment. Unlike a *penetration test*, a *vulnerability assessment* seeks to identify all ways in which asset compromise might be possible. It considers assets, threats, workflow, whole system configuration, and internal defenses, as well as future developments of the infrastructure or application. The threats addressed go beyond the drive-by adversary, and consider the more likely adversaries who would be interested in compromising high-value digital assets: targeted attacks, insider threats, advanced persistent threats, and the accidental (perhaps inevitable) security breach. By contrast, the goal of a *penetration test* is simply to determine if defenses can be breached. In terms of risk assessment, it provides primarily a binary risk rating – can be breached or cannot be breached.

Beyond definition and primary objective, these engagements typically differ in other notable ways. *Penetration tests* often rely heavily on automated tools, only leverage known vulnerabilities, and seek to identify low-hanging fruit. *Vulnerability assessments* use these same tools as part of the process, but incorporate the results into a custom evaluation, and seek to identify all potential vulnerabilities, not just those that can be found through automation.

The most telling difference between these types of evaluation can be seen in how they are (or should be) priced. As with any service engagement, one pays for time and materials, with a premium for quality and skill. The cost of a *vulnerability assessment* relates to the effort required for a team of experts with full access to evaluate a system front-to-back, address all threat vectors, propose mitigations, and assign risk. The scope of effort is more or less fixed and limited by the size of the supply chain, infrastructure, application, or subset thereof. Conversely, the price of a *penetration test* is largely driven by budget: the amount of resources devoted to simulating an attack determines the cost, and budget parameters are met simply by manipulating effort input, irrespective of how the effort input affects result output. Due to heavy reliance on automation, *penetration tests* typically cost less than *vulnerability assessments*. However, *penetration tests* also produce woefully incomplete results, leaving blind spots that are not factored into risk calculation.

Methodologies

In addition to selecting a type of evaluation, IT executives must also select a methodology to apply to that evaluation. The two methodologies most relevant are *white box* and *black box*.

The most succinct distinction between these methodologies comes down to knowledge. In a *white box* assessment, the evaluator has full detailed knowledge of system functionality. In a *black box* assessment, the evaluator has very limited knowledge, obtaining information only from outputs that result from varying test inputs, and with no knowledge about the inner workings of the system.

The results of a *white box* methodology are of very high value in calculating risk, as it can be determined with high confidence that most or all of the vulnerabilities present in the target technology have been identified. However, IT executives have recently been trending towards a preference for *black box*. This seems to stem from an interest in having an evaluator assume similar conditions to that of a real world adversary, i.e. with limited system knowledge. This intuition is flawed in that with a *black box* methodology it is ultimately the tester that is evaluated, rather than the target system. Results may determine the risk of that specific evaluator succeeding, but proves little about what other adversaries might achieve or about the entire range of weaknesses that may exist. Furthermore, the results of a *black*

box methodology are of lower value in calculating risk: if vulnerabilities are discovered, there is no way of knowing that all vulnerabilities have been discovered, and as a corollary, if no vulnerabilities are found, it does not mean there are not any vulnerabilities.

As with the distinct types of evaluations, pricing also reveals notable differences between distinct methodologies. Pricing of a *white box* approach is related to project completion, and scope is scaled to meet budget parameters by adding or omitting components. Although component omission creates blind spots, the existence of such blind spots is known and thus accounted for in risk assessment. Conversely, pricing for a *black box* assessment correlates to effort invested, and scope is scaled to meet budget only by modifying effort input. However, reducing effort (i.e., as a method to reduce cost) only reduces the thoroughness and usefulness of results in determination of risk. Blind spots are unknown, significantly weakening the confidence of the resulting risk assessment.

Best Practices

The most effective calculation of risk is derived from the combination of *white box* methodology and *vulnerability assessment*. A *white box vulnerability assessment* empowers an IT executive to best prioritize future development cycles in order to address most crucial weaknesses first. IT executives should migrate away from current trend preference for *black box penetration tests,* which produce a false sense of confidence in otherwise heavily exposed systems, and migrate towards the more effective approach of *white box vulnerability assessment*.

About the Author

Ted Harrington drives thought leadership initiatives for ISE, the Baltimore-based cyber-threat mitigation and solutions entity widely recognized for its groundbreaking research and enterprise consulting practice. Harrington holds a Psychology degree from Georgetown University, which he applies to drive ISE's proprietary threat modeling. Where many security experts are satisfied with understanding the *attack*, Harrington advocates progressive modeling by understanding the *attacker*. A strong grasp of the adversarial methodology determines the most effective security mitigations.

About ISE

Founded in 2005 out of the PhD program at the elite Johns Hopkins' Information Security Institute, ISE is a sophisticated security consulting firm dedicated to aggressive defense strategies through advanced science. This select team of hackers, computer scientists, reverse engineers, and cryptographers utilizes a unique perspective typically perpetrated by the adversary.

ISE is most commonly recognized for being the first company to exploit the iPhone[1], an achievement that garnered international attention. Other high profile compromises include ExxonMobil SpeedPass, Texas Instruments RFID, Diebold eVoting Machines, and numerous others. ISE's most recent research discovered systemic issues in SOHO routers[2] and web browsers[3].

---

[1] http://www.nytimes.com/2007/07/23/technology/23iphone.html?_r=2&

[2] http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp

[3] http://securityevaluators.com/content/case-studies/caching/index.jsp