CATEGORIES OF SECURITY ASSESSMENTS

There are following categories of security Assessments:

1. Vulnerability Assessment
2. Penetration Test
3. White/Grey/Black-Box Assessment
4. Risk Assessment
5. Threat Assessment

1.Vulnerability Assessment:

1. Vulnerability assessment, is also known as Vulnerability analysis.
2. It is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.
3. It is used by network administrators to evaluate the security architecture and defense of a network against possible vulnerabilities and threats.
4. The key objective of this assessment is to find any vulnerabilities that can compromise the overall security, privacy and operations of the network.

2. Penetration Test Assessment:

1. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.
2. Penetration tests find exploitable flaws and measure the severity of each.
3. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system.

4. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

3.White/Grey/Black-Box Assessment:

1. The white/grey/black assessment parlance is used to indicate how much internal information a tester will get to know or use during a given technical assessment.
2. The levels map light to internal transparency, so a white-box assessment is where the tester has full access to all internal information available, such as network diagrams, source code, etc.
3. A grey-box assessment is the next level of opacity down from white, meaning that the tester has some information but not all.
4. In Black box assessment ,the tester has zero internal knowledge about the environment, i.e. it's performed from the attacker perspective.

4.Risk Assessment:

1. Risk assessment is the determination of quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat (also called hazard).
2. Quantitative risk assessment requires calculations of two components of risk (R): the magnitude of the potential loss (L), and the probability (p) that the loss will occur.
3. Risk Assessments commonly involve the rating of risks in two dimensions: probability, and impact, and both quantitative and qualitative models are used.

5.Threat Assessment:

1. A threat assessment is a type of security review that's somewhat different than the others mentioned.
2. The primary focus of a threat assessment is to determine whether a threat (think

bomb threat or violence threat) that was made, or that was detected some other way, is credible.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer