



**Fix your weak links
before the network
breaks down**



Vulnerability Assessment and Penetration Testing



Overview

Vulnerability Assessment is the process of identifying and quantifying vulnerabilities in a system and Penetration Testing evaluates the security of a computer system or network by simulating an attack. The process may involve an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. This includes fixed and wireless networks.

Business Drivers

- Rapidly evolving new threats to the organizational security.
- Rapidly growing IT assets
- Increasing leverage of IT infrastructure for Business transactions
- Manageability of growing security concerns and issues
- Compliance
- End users resistance to the established practices on Security

How Apara adds value

- Industry proven and Tested methodologies for rapid and cost-effective IT Security deployments
- Breadth of expertise, thought leadership and research in security methodologies and technologies
- APARA possesses vast expertise in technology solutions and Intellectual Property acquired through a decade of domain expertise with skilled and certified resources.
- We follow a strategic delivery approach in each of the Assessment and Testing phases.
- Practice systematic and structured approach to services in each of the phases
- Strong Project Management handling skills
- Enjoy unique partnership with Enterprise Security Ecosystem companies

Deliverables

Apara's approach gives an in-depth report with increased assurance to the validity of vulnerabilities found. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. Service deliverables include:

- Actual security assessment findings and results
- Assessment report highlighting security risks and impact levels
- Follow up review on corrective actions

Business Benefits

- Identifies vulnerabilities and risks in your IT infrastructure
- Validates the effectiveness of current security safeguards
- Quantifies the risk to internal systems and confidential information
- Raises executive awareness of corporate liability
- Provides detailed remediation steps to prevent network compromise
- Validates the security of system upgrades
- Helps to achieve and maintain compliance