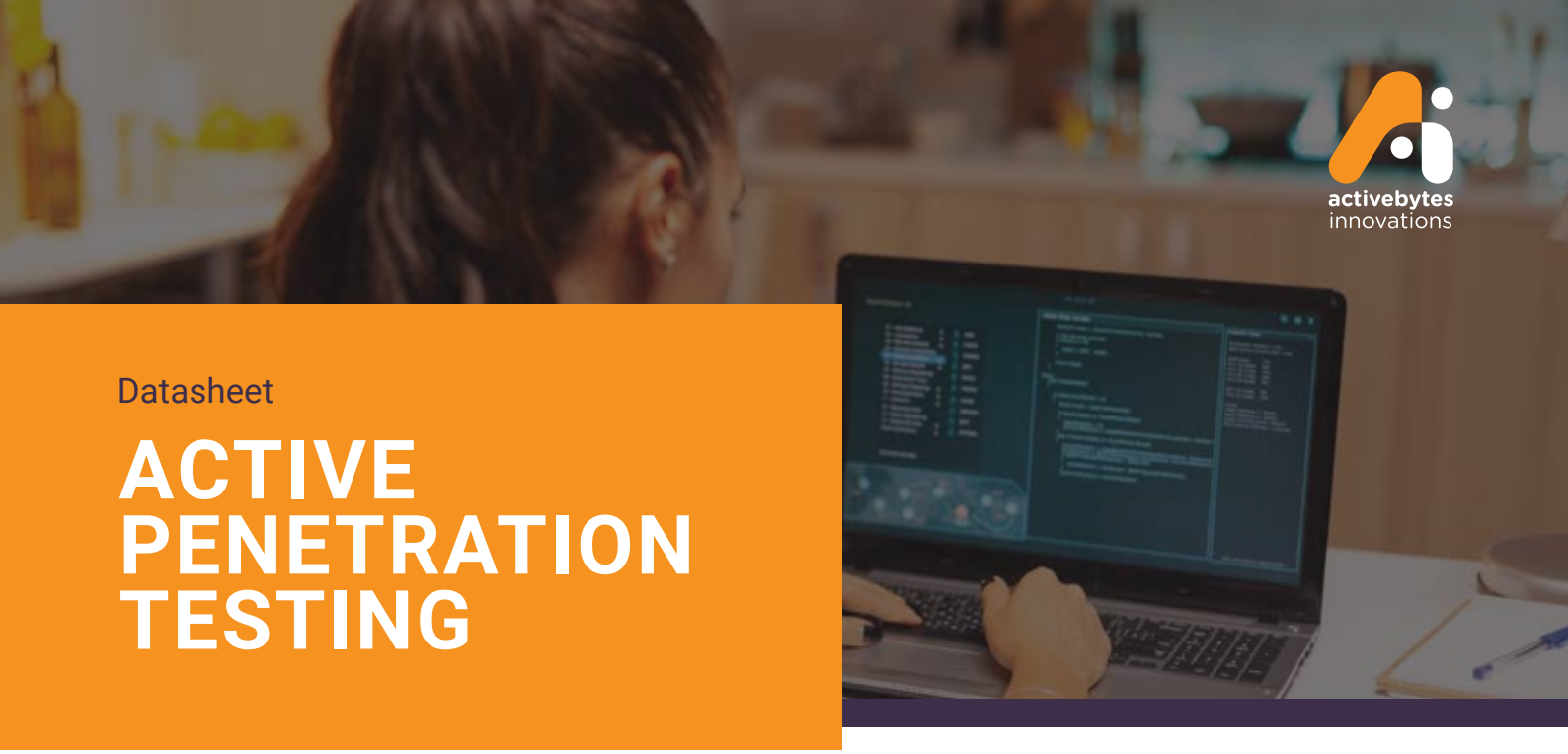


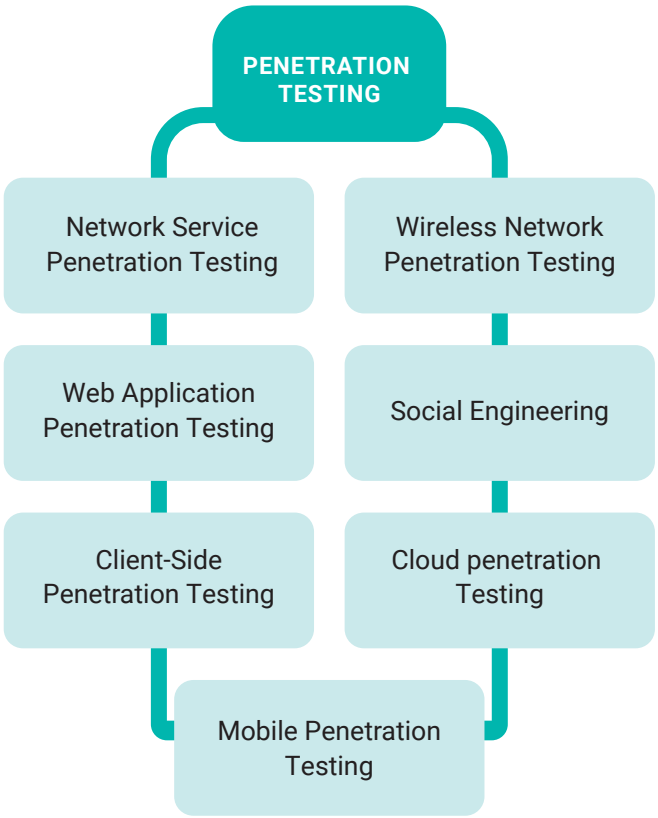
activebytes
innovations

Datasheet

ACTIVE PENETRATION TESTING

We have designed our penetration test services to identify the vulnerabilities that leave your network, web application or client-side exposed, and help you to close any gaps in your IT environment. We will assess the websites, network and IT systems in scope using a combination of full black, grey box web application assessments, as well as automated vulnerability scanning tools. Our approach would be a deep dive one covering all surface vulnerabilities as well as in depth coverage

Our team will perform the testing with privileges of an unauthenticated user and with commercial and open-source application scanners, identify common and publicly reported vulnerabilities. We will do a manual penetration testing to identify specific threat scenarios using various combinations of results from automated testing as well as using custom-developed exploits. Our manual tests include business logic and authorization flaws that automated tools cannot find.



Our Approach

PREPARATION

After a kickoff meeting between the organization and ActiveBytes Penetration Testing Team the scope and objective of the penetration test will be discussed. With the test we will demonstrate the exploitable vulnerabilities that exist in your organization's network infrastructure. The test will be performed during the timing and duration as agreed.

APPLICATION PENETRATION TESTING

Our web application penetration test will identify exploitable vulnerabilities in your applications before hackers discover and exploit them.

Our team will

- Identify application security flaws present in your environment
- Understand the level of risk for your organization
- Help address and fix identified application flaws

ActiveBytes Penetration Testing Team produce findings in written reports and provide your team with the guidance necessary to effectively remediate any issues we uncover. We perform our assessments with a combination of manual and automated security testing procedures. We use industries best practice assessment techniques of the OWASP Top 10, OSSTMM, SANS and Penetration Testing Execution Standard.

RECONNAISSANCE & MAPPING

ActiveBytes testing team shall perform active and passive reconnaissance of the target system. During our Mapping phase, we will identify all the publicly available services running in the target system. In the Web Application Penetration Test, we will discover all the pages, files and directories present in the web application environment. We also perform

- DNS Querying and Brute forcing
- Host Mapping
- Spidering
- Web Services and Web 2.0Enumeration
- Enumeration to Rich Internet Interfaces – Flash etc.
- Enumeration of Services and Infrastructure related services
- Port scanning and service enumeration
- Enumeration of SSL and other session layer technologies used if any

DISCOVERY

Our testing team will identify all possible vulnerabilities in the target system with help of automated and manual discovery processes to identify the most deep-seated vulnerabilities in the target system like flaws in coding practices, security misconfiguration etc.

In web application Penetration Tests, we also perform Business Logic Security Testing, which identifies business logic flaws that are not identified by any tools or automated vulnerability scanning tools. Some of the other flaws we check include Injection Flaws, Cross-Site Scripting, Broken Authentication and Session Management Flaws, Request Authentication Flaws, Local and Remote File Inclusion Flaws, AJAX And JSON information Leakage, Insecure Cryptographic Storage Flaws, SSL Flaws, malicious File Execution and File Injection Flaws, Authorization and Privilege Escalation Flaws, Insecure Deployment and Management Flaws. ActiveBytes Web application methodology will focus on OWASP Top Ten 2021web application vulnerabilities

EXPLOITATION

ActiveBytes testing team exploits the target system based on the vulnerabilities discovered in the discovery phase. Our exploitation techniques are predominantly manual, with a healthy combination of automated exploit tools at our disposal.

ANALYSIS & REPORTING

Our Testing team will prepare the Vulnerability Assessment and Penetration Testing Report with risk ranking of High, Medium and Low will be populated with the findings of the test Executive Summary. The report shall contain

Scope and Objective of the Work, Detailed Vulnerability Statistics, Specific Vulnerability Information - with URL, Parameter, Attack Vector, Classification of Vulnerability with multiple Vulnerability References, Evidence of Exploit of Discovery (if any), Recommendations

Benefits

- Find security risks and prioritize before an attack
- Detect unnoticed weakness by proactively testing for vulnerabilities.
- Demonstrate compliance with regulatory standards.
- Lessen financial setbacks from legal fees, lost revenue etc.
- Mitigate identified vulnerabilities to protect reputation & client trust

Wireless Network penetration testing

We understand that by performing security testing, organizations could experience

- Decreased incident response costs
- Increased collaboration among employees
- Enhanced customer service experience etc

Our effective planning begins with a detailed wireless security assessment of your organization. Our team starts wireless penetration tests by taking a holistic approach, by working with your team to identify and scope a customized vulnerability assessment to meet your organization's specific needs. This approach allows us to identify all existing attack vectors and demonstrate the impact of a real-world attack. Finally, we will provide a comprehensive report detailing exploitable findings, risk ratings, and business impact, evidence of findings including screenshots, and actionable recommendations for remediation. We also provide re-testing on all mitigated vulnerabilities which were identified during primary testing phases to make sure that the issue is closed.

Our approach for wireless penetration test includes

- War dialing the client's network to identify wireless access points outside permissible bounds
- Identifying rogue access points
- Capturing wireless handshakes
- Breaking the encryption methods/keys deployed in WLAN
- Reporting – vulnerability findings, recommendations, and high-level mitigation steps

Benefits

- Seal Wi-Fi signals from wardriving attempts
- identify weak and insecure applications from a wireless connectivity standpoint
- Discover faulty and vulnerable points within the networks
- Ensure secure configuration

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com