Penetration Testing

DATA SHEET

Finding and Fixing Your Vulnerabilities - Ahead of the Bad Guys

Conducting a penetration test will allow you to discover the vulnerabilities in your IT infrastructure and correct them before they can be exploited by hackers and other hostile forces. One of the oldest and most trusted methods for assessing security sisks is penetration testing. Penetration testing is designed to simulate a real-world attack using tools and techniques employed by actual hackers. It provides realistic examples of how a real hacker could compromise sensitive data.

The Compliance Overview

If your organization is subject to IT security mandates such as FDIC, GLBA, HIPAA, HITECH, NCUA, OCC and PCI DSS, you must take measures to prevent unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI). This requires you to know your risks and mitigate them with a combination of practices, procedures, and controls.

To ensure the security of your internal networks, best practices recommend that you perform internal and external penetration tests in addition to regular security assessments.

The TraceSecurity Penetration Testing Overview

Our expert security analysts conduct internal and external penetration tests as separate services. Designed to evaluate the effectiveness of your existing security measures, these tests mimic the action of an actual attacker exploiting weaknesses in network security without the usual dangers. The internal penetration test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network. The external penetration test examines external IT systems in the same manner.

Penetration tests are different from vulnerability assessments because they exploit vulnerabilities to determine what

TraceSecurity's penetration tests follow documented best practices for security testing methodology including:

- Scoping and rules of engagement
- Analysis and identification of attack vectors
- Exploit testing and penetration attacking
- Immediate notification of critical attacks

Test results are provided in an extensive report containing:

- Penetration test methodology
- Executive summary
- Business and technical risks and recommendations
- Exploitation results listed by risk and areas of concern
- Details and exposure of vulnerabilities

Options:

- On-demand network vulnerability scanning
- Extensive information gathering (for External Penetration Testing), including public record search, web presence analysis, email harvesting, DNS interrogation and Whois
- Retest: following completion of the initial penetration test, analysts will conduct retesting of initial findings to determine remediation strategies
- On-demand report generation for executives and technical staff