



Your **Final Step**  
in Coordinated,  
**Defense-Oriented**  
approach to security

Securing company assets and maintaining regulatory compliance is an increasing challenge. The threat environment is evolving as attacks are becoming more sophisticated and script kiddies have easy access to them over internet. As the threat level increases, so do the consequences of inadequate information security. At stake is valuable information, customer data, intellectual capital and financial transactions. The impact of an intrusion or lack of regulatory compliance may carry with it unforeseen financial costs and bring harm to your company's brand image. Having a clear understanding of your organization vulnerabilities and risks is a good first step toward securing your network, prioritizing security investments and achieving regulatory compliance.

## Why Secure Bytes?

### Knowledge and Expertise

- Secure Bytes staff has more than 150 years of accumulated Information Technology Network and Security experience.
- Secure Bytes security experts hold different security certifications, such as CISSP, CISM, CISA, CCIE & CCNP.
- Secure Bytes maintains a staff of multiple network engineers.
- Secure Bytes is Microsoft, Oracle and McAfee, Partner.

## How we Differ !

- Secure Bytes will assist in information gathering.
- Secure Bytes provides easy-to-read reports with findings sorted by associated risk with solution.
- Reports include a detailed review with a Secure Bytes security expert.
- Secure Bytes offers full Penetration Tests, not just inadequate port scans.
- In-depth testing is performed using multiple tools from different perspectives.
- Secure Bytes Penetration Tests are much more than an automated scan. Human perspective, observation, and experience help identify vulnerabilities.

## Attack Simulation

Secure Bytes Penetration Testing can help determine your network's current vulnerabilities while demonstrating how attackers can significantly impact your business. Secure Bytes Penetration Testing is an exercise performed by security experts, to validate existing security controls and to quantify real-world risk. The result is a detailed security roadmap that prioritizes areas of weakness and specifies remediation steps to improve organization security posture. According to the scope following attacks can be simulated:-

### Authentication

- Brute Force
- Insufficient Authentication
- Weak Password Recovery Validation

### Logical Attacks

- Abuse of Functionality
- Denial of Service
- Insufficient Antiautomation
- Insufficient Process Validation

### Information Disclosure

- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

### Authorization

- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation
- Client-side Attacks
- Content Spoofing
- Cross-site Scripting

### Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

## Approach

INFORMATION GATHERING

FINGERPRINTING

PORT SCANNING

SERVICES ENUMERATION

AUTOMATED VULNERABILITY SCANNING

EXPLOITATION - ESCALATION OF PRIVILEGES

PENETRATION TEST REPORTING

## Service Benefits

The key benefit of penetration testing comes after the policy has been defined, assessed and the systems have been evaluated.

- Penetration Tests reduce significant risks of information leakage thus enhancing information integrity.
- Result of Penetration Test prioritizes the detected risks by setting their level of severity
- The final stage of the service, which is the analysis and deliverable, provides guidance on how to mitigate the detected vulnerabilities
- Detecting vulnerabilities during the development stages of a system's lifecycle by conducting a Penetration Test increases security.

For further information:  
[sales@secure-bytes.com](mailto:sales@secure-bytes.com)