Prescriptive

Support Hour Options:
Weekday: 8am-6pm 365 24/7

Penetration Testing

To Give You Peace of Mind

Regular penetration testing is essential for maintaining a strong cybersecurity posture. It helps organizations identify vulnerabilities and weaknesses before they can be exploited by attackers, reducing the risk of data breaches and other cyber attacks.

The Process

The penetration testing process starts with pre-engagement, where the scope and rules are set. Then, information gathering collects data about the target. Vulnerability assessment identifies security weaknesses, followed by exploitation, where these weaknesses are tested. Post-exploitation involves maintaining access and gathering more information. Reporting summarizes vulnerabilities and suggests fixes. Finally, post-engagement reviews results and plans future tests.

PRE-ENGAGEMENT

INFORMATION GATHERING

VULNERABILITY ASSESSMENT

EXPLOITATION

POST-EXPLOITATION

REPORTING

POST - ENGAGEMENT

Services Included in every penetration test:

- Recon and OSINT gathering
- Vulnerability Scanning
- Verification/Exploitation of Discovered Vulnerabilities
- Penetration Test Report
  - Executive Summary of Findings
  - OSINT/Recon Report
  - Technical Breakdown of Findings
  - Recommendations and Fixes

*Testing for compliance (PCI-DSS, HIPAA, etc. compliance tests will add at least 10% to the final cost for specific testing requirements.)

Prescriptive

Support Hour Options:
Weekday: 8am-6pm 365 24/7

Penetration Testing

Types of Tests:

- **Web Application Testing:** This type of testing involves evaluating the security of web applications by identifying vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.
- **Network Testing:** Network testing focuses on assessing the security of an organization's network infrastructure. This includes testing for vulnerabilities in firewalls, routers, switches, and other network devices.
- **Cloud Testing:** Cloud testing involves evaluating the security of cloud-based infrastructure and services. This includes testing for vulnerabilities in cloud storage, virtual machines, and cloud applications.
- **IoT Testing:** IoT testing focuses on assessing the security of Internet of Things (IoT) devices and their associated networks. This includes testing for vulnerabilities in device firmware, communication protocols, and data storage.

Testing Methodology

Grey Box - ($) - A combination of black and white box testing, where the tester has partial knowledge of the system. This method simulates both internal and external threats. Grey box testing provides a balanced approach, combining the thoroughness of white box testing with the external perspective of black box testing while also typically being the cheaper option.

White Box - ($$) - The tester is given full knowledge of the system, including source codes, network architecture, and internal configurations. This method is ideal for identifying internal vulnerabilities. White box testing allows for a thorough examination of the internal workings of your systems, uncovering vulnerabilities that might not be visible from an external perspective

Black Box - ($$$) - The tester has no prior knowledge of the system, simulating an external attack. This method is comprehensive, requires more time, and is typically more expensive. Black box testing closely mimics the actions of a real attacker, providing valuable insights into how your system would withstand an external threat. However, this type of testing should be reserved for more mature organizations. If an organization is performing their first penetration test, it is often not beneficial for the test to be performed via black box methodology.

Email: info@prescriptive.solutions
Phone: 888.252.3182
www.prescriptive.solutions

Scan the QR code to contact us directly!

Prescriptive

Support Hour Options:
Weekday: 8am-6pm 365 24/7

10 REASONS YOUR BUSINESS NEEDS A PENETRATION TEST

1. Identify Vulnerabilities:

- Proactive Detection: Pen tests help identify security weaknesses before malicious actors can exploit them.
- Comprehensive Analysis: They provide a detailed report of vulnerabilities in applications, networks, and systems.

2. Enhance Security Posture:

- Strengthen Defenses: By understanding where vulnerabilities lie, enterprises can take steps to strengthen their security measures.
- Patch Management: Helps prioritize patching and remediation efforts based on the severity of identified vulnerabilities.

3. Compliance and Regulatory Requirements:

- Meeting Standards: Many industries require regular penetration testing to comply with standards like PCI-DSS, HIPAA, and GDPR.
- Audit Preparation: Helps prepare for audits by demonstrating a commitment to security and compliance.

4. Risk Management:

- Risk Reduction: Identifies and mitigates risks that could lead to data breaches, financial loss, or reputational damage.
- Informed Decision-Making: Provides actionable insights that help in making informed security investment decisions.

5. Improve Incident Response:

- Test Response Plans: Simulates real-world attacks to test the effectiveness of incident response plans.
- Enhance Readiness: Helps improve the readiness and efficiency of the incident response team.

6. Protect Customer Trust and Brand Reputation:

- Prevent Breaches: Reduces the likelihood of data breaches, thereby protecting customer data and maintaining trust.
- Brand Integrity: Demonstrates a commitment to security, which can enhance the enterprise's reputation in the market.

7. Cost Savings:

- Avoid Costs of Breaches: Prevents the financial losses associated with data breaches, including legal fees, fines, and loss of business.
- Efficient Resource Allocation: Helps allocate resources more effectively by focusing on critical vulnerabilities.

8. Gain Insights into Attack Vectors:

- Understand Threat Landscape: Provides insights into how attackers might exploit vulnerabilities and the methods they use.
- Adapt Security Measures: Allows the enterprise to adapt and evolve its security measures to counter emerging threats.

9. Employee Awareness and Training:

- Security Culture: Promotes a culture of security awareness among employees.
- Training Opportunities: Identifies areas where additional training or awareness is needed.

10. Third-Party Validation:

- Independent Assessment: Offers an objective, third-party evaluation of the enterprise's security posture.
- Credibility: Adds credibility to the enterprise's security claims when communicating with stakeholders, customers, and partners.

Email: info@prescriptive.solutions
Phone: 888.252.3182
www.prescriptive.solutions

Scan the QR code to contact us directly!