CyStack

DATA SHEET

Penetration Testing

Uncovering your vulnerabilities before others do

Overview

A pentest, or penetration test, is a simulated cyber attack on a computer system, network, or web application in order to identify vulnerabilities that an attacker could exploit. Pentest is performed by security professionals who use a variety of tools and techniques to test the security of the target environment and identify weaknesses that could be exploited by attackers.

Pentest is important because it helps organizations identify and address vulnerabilities in their systems and applications before they can be exploited by attackers. It is a valuable tool for improving the security posture of an organization and for ensuring compliance with industry regulations and standards.

In addition to identifying vulnerabilities, pentest can also help organizations assess the risks of a successful attack, understand the potential impact of a compromise, and develop strategies for defending against attacks. It can also help organizations build a culture of security and improve their incident response capabilities.

Customer Benefits

- Protect sensitive data
- Prevent attacks
- Maintain system integrity
- Meet regulatory requirements

How CyStack Helps

The CyStack Audit Team is a group of highly skilled security testers who use a goal-oriented approach to testing, refined through years of experience and extensive testing. Our team members have a unique blend of app development and security testing expertise, enabling them to conduct comprehensive security evaluations that uncover potential risks for organizations. Members of this team are also regular speakers at world-known cyber security conferences and also talented bug hunters who discovered many critical vulnerabilities in the products and are acknowledged in the Hall of Fame of global tech giants such as IBM, HP, Microsoft, Alibaba, Sea Group, etc.

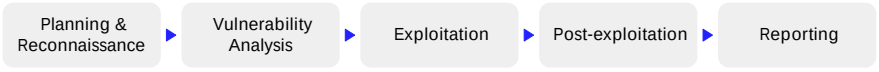
CyStack's pentest service is the perfect solution for organizations looking to improve the security of their systems and applications. One of the key features that sets CyStack apart is the use of traditional pentest methodologies combined with crowd-sourced security. This unique approach leverages the expertise and experience of a team of professional security testers, while also incorporating the insights and perspectives of a global community of security researchers.

In addition, CyStack's pentest service is also designed to provide a comprehensive solution for managing vulnerabilities. The platform is equipped with powerful tools and features that allow organizations to easily track, prioritize, and remediate vulnerabilities in order to improve the security of their systems. This includes the ability to monitor the status of vulnerabilities in real time, generate reports and alerts, and coordinate efforts with other stakeholders.

©2023 CyStack. All rights reserved.

Methodology

The specific stages of a pentest can vary depending on the specific goals and objectives of the test, as well as the specific characteristics of the target environment. However, in general, the CyStack Pentest Methodology strictly adheres to the following steps:



1. **Planning and reconnaissance**: This phase involves defining the scope and objectives of the test, identifying the target systems and networks, and gathering information about the target environment (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.
2. **Vulnerability analysis**: In this phase, the pentester identifies potential vulnerabilities in the target system using techniques such as vulnerability scanning, network scanning, and configuration review. Well-known vulnerabilities (1-day flaws, CVEs) will be used in this stage.
3. **Exploitation**: This is where the pentest happens. In this phase, the pentester attempts to exploit one or more identified vulnerabilities in order to gain unauthorized access or compromise the system's security.
4. **Post-exploitation**: This phase involves maintaining access to the compromised system and escalating privileges within the system, if possible.
5. **Reporting**: The final phase involves preparing a report that summarizes the testing process, the vulnerabilities identified, and the recommendations for improving the system's security.

Key Features

- Gain assurance that your infrastructure and applications are secure
- Tested by talented security pentesters from CyStack and over 3000 researchers from our community
- Manage, track, prioritize, and remediate the findings in the CyStack Vulnerability Management Platform
- Receive actionable recommendations to enhance security
- Reduce your risk and improve operational efficiency

Our Approach

CyStack offers 3 approaches for pentest as below. By default, the black-box pentest is applied:

	Black-Box aka close box penetration testing	**Grey-Box** combination of black box and white box testing	**White-Box** aka open box penetration testing
Goal	Mimic a true cyber attack	Assess an organization's vulnerability to insider threats	Simulate an attack where an attacker gains access to a privileged account
Access Level	Zero access or internal information	Some internal access and internal information	Complete open access to applications and systems
Pros	Most realistic Testing is performed from point of view of attacker	More efficient than black-box and saves on time and money Testing is performed from point of view of attacker	More comprehensive, less likely to miss a vulnerability and faster Testing is performed from point of view of attacker
Cons	Time consuming and more likely to miss a vulnerability	No real cons for this type of testing	More data (ex, source code) is required to be released to the tester and more expensive

©2023 CyStack. All rights reserved.

What We Test

Web Applications

Web applications are important because they are the way that organizations interact with the Internet and their clients, partners, and suppliers. They are a key part of a business and are used to promote the company, generate income, and increase sales. Unfortunately, this also makes web applications a target for attackers, and they are often the source of security breaches that are reported. Besides, internal applications that are used within an organization's internal network are important for conducting business and storing sensitive information such as intellectual property, customer data, employee information, and sales data.
CyStack is committed to following best practices and industry standards when testing the security of web applications. One of the key resources that we rely on when conducting web pentest is the OWASP Testing Guide which is a widely recognized and respected resource in the field of web application security, and it provides a comprehensive set of testing procedures and recommendations for identifying and mitigating common web application vulnerabilities. Specifically, our tests include but are not limited in:

- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client-side Testing
- API Testing

Standards

- OWASP Testing Guide
- The Penetration Testing Execution Standard
- REST API security guidelines
- NIST SP 800-95

Mobile Applications

Mobile applications are an important part of modern life and are used for a wide range of purposes, including communication, entertainment, banking, and shopping. As such, it is important to ensure that mobile applications are secure in order to protect sensitive data, maintain user trust, and prevent attacks that could compromise the security of the device.

We use OWASP Mobile Application Security Testing Guide (MASTG) as the base standard when performing the pentest project for mobile applications. The OWASP MASTG is a comprehensive resource that provides guidelines and recommendations for testing the security of mobile applications. It covers a wide range of topics, including mobile application architecture, secure coding practices, and testing techniques. We focus on the following security requirements:

- Architecture, Design, and Threat Modeling Requirements
- Data Storage and Privacy Requirements
- Cryptography Requirements
- Authentication and Session Management Requirements
- Network Communication Requirements
- Platform Interaction Requirements
- Code Quality and Build Setting Requirements
- Resilience Requirements

©2023 CyStack. All rights reserved.

Web Service and APIs

APIs (Application Programming Interfaces) and web services are important components of modern computing and are used to enable communication and data exchange between different systems and applications. Ensuring the security of APIs and web services is important because they handle sensitive data and are often exposed to the Internet, making them vulnerable to attack.

In general, pen testing for APIs is done similarly to for web applications and also follows the base standards mentioned in the previous section. However, the pentest for APIs also follows several specific guidelines:

- **OWASP API Security Top 10**: This is a list of the top 10 most critical API security risks, as identified by the Open Web Application Security Project (OWASP). The OWASP API Security Top 10 provides a good starting point for identifying common API vulnerabilities and risks.
- **REST API security guidelines**: REST (Representational State Transfer) is a popular architectural style for building APIs, and there are several guidelines and best practices that have been developed specifically for securing REST APIs. These guidelines cover topics such as authentication, authorization, and input validation.
- **Industry standards and regulations**: There may be specific industry standards or regulations that apply to the API being tested, such as PCI DSS for APIs that handle credit card data. It is important to be familiar with any applicable standards or regulations and to ensure that the API being tested is compliant.
- **Custom security requirements**: In addition to general standards and best practices, there may be specific security requirements that apply to the API being tested. These requirements may be defined by the API owner or by industry regulations, and it is important to take them into account when planning and conducting the pentest.

Desktop Applications

Desktop applications are software programs that run on a computer and are used for various purposes, such as productivity, communication, and entertainment. Ensuring that these applications are secure is important for protecting sensitive data, preventing attacks, and maintaining the reliability of the system. It is also necessary for meeting regulatory requirements and avoiding penalties. Maintaining the security of desktop applications is a crucial aspect of computer security.

Pentesting desktop applications involves following the same guidelines for security testing as mobile applications. In order to identify the most dangerous vulnerabilities in desktop applications, we refer to the OWASP Top 10 Desktop Application Security Risks like Injections, Broken Authentication & Session Management, Hardcoded Secrets in files, Missing Code-Signing and Verification for File Integrity, or Usage of Outdated Softwares, or Usage of Obsolete Components/Services of Windows/3rd Party vendors.

Infrastructure

Infrastructure is a critical component for every application where the application is deployed. Infrastructure security testing is important because infrastructure is often a target for attackers due to the sensitive data it stores and processes, and the critical role it plays in supporting an organization's operations. A security breach or attack on an organization's infrastructure could result in data loss, system downtime, and other negative consequence.

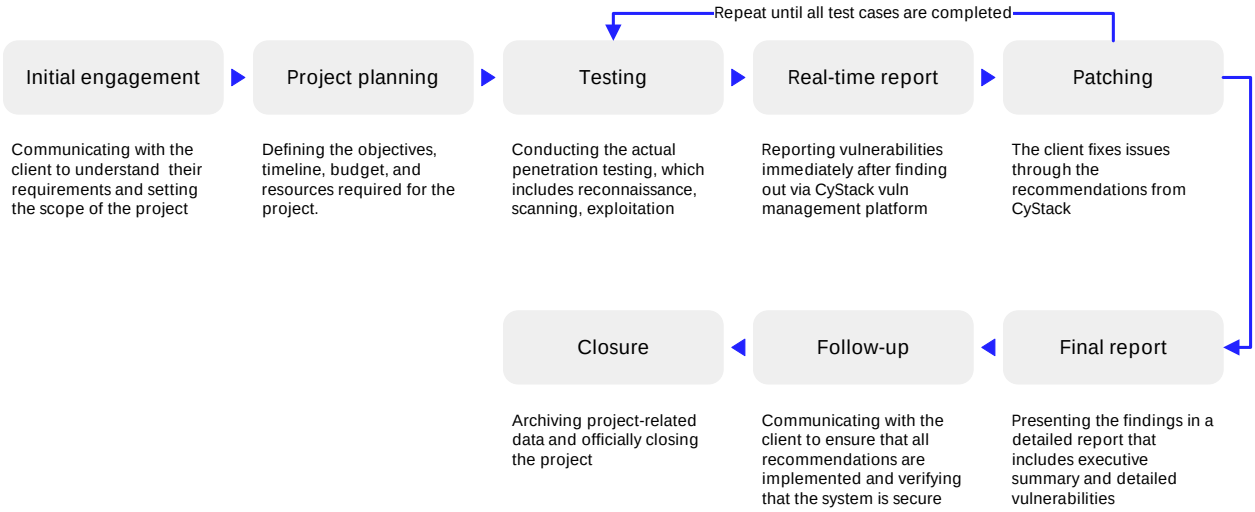
Our pentest will help customers to assess the security of the entire infrastructure, including the Cloud infrastructure, external network, and internal network.

Custom Applications

Thick client software, which is often custom-made or used by organizations to manage important business operations, can be tested by CyStack for vulnerabilities such as the exposure of sensitive information, weaknesses in client-server communication, and potential for data or system exploitation. CyStack also offers Whitebox Testing to analyze and identify vulnerabilities in mission-critical IT systems used by large enterprises for their business or offered as a service to customers. This comprehensive approach combines static and dynamic analysis of each component in the ecosystem and has a proven track record of discovering vulnerabilities before they can be exploited by attackers.

©2023 CyStack. All rights reserved.

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net

©2023 CyStack. All rights reserved.