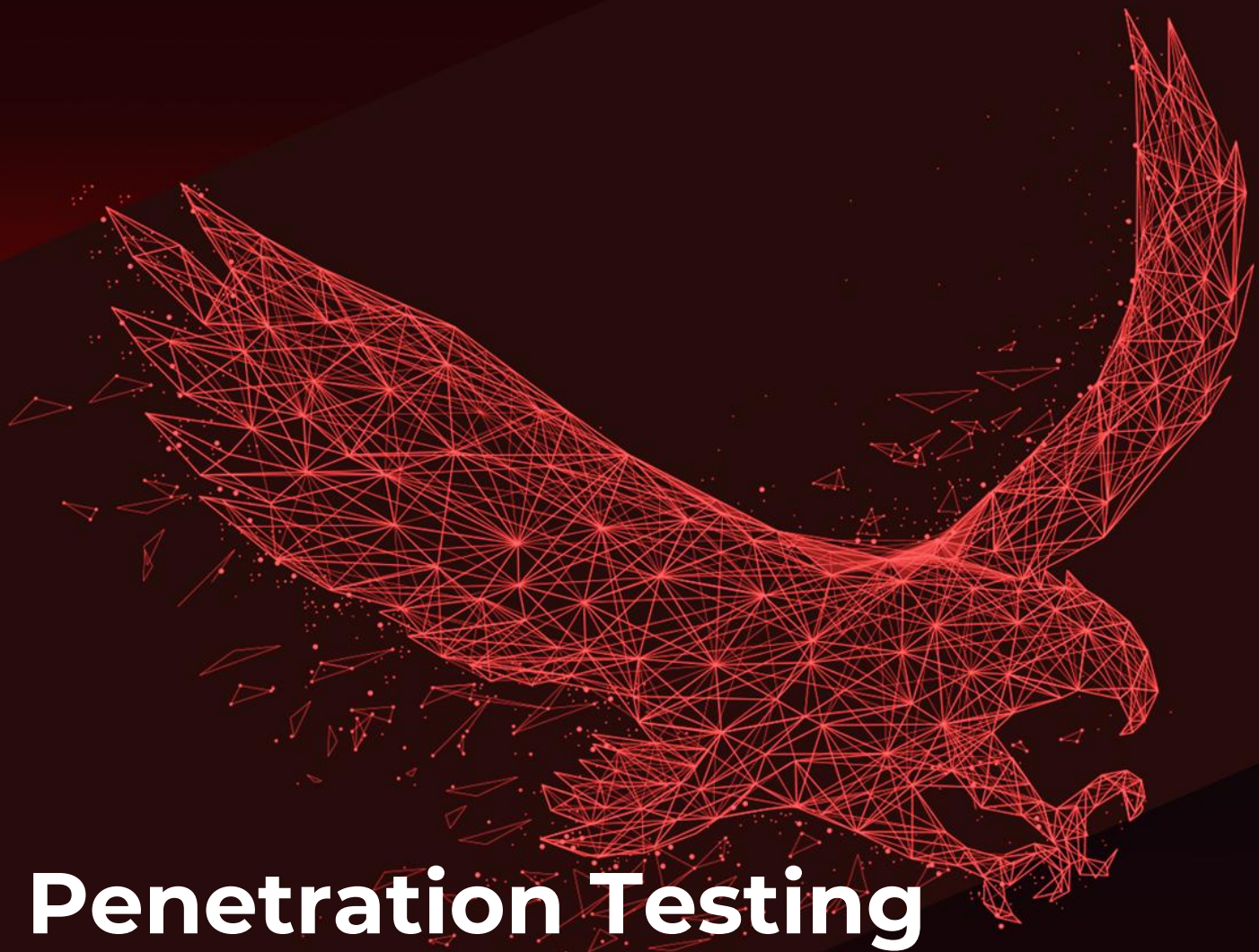
Privia SECURITY



Penetration Testing (Pentest) Service

Professional Offensive Security Services

"Identify Vulnerabilities, Manage Risks!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“Through real-time testing, we identify your weak points and strengthen your muscles in these areas.”

Penetration testing, also known as Pentest service, is a special cyber security consultancy service carried out by experts in the field in order to prevent any security vulnerability and make systems more secure by revealing problems, errors and vulnerabilities in information systems.

Penetration tests, which aim to assess the security levels of organizations against cyber-attacks and manage the identified risks, go beyond detecting vulnerabilities and show how authorized access can be obtained in the relevant system using the identified vulnerabilities and what they can result in. It also provides a complete risk assessment by showing the strengths of the system.

The penetration test, which is applied within predetermined scenarios according to each asset type, is based on both national and international methodological approaches. After the test, a more targeted and effective security assessment is provided with the report prepared by our expert team.

Service Components

Determining Test Methodology and Approach

The success of penetration testing depends on the accuracy of the methodology applied. Black Box, White Box and Gray Box approaches allow systems to be tested from different angles. In accordance with international standards such as OWASP and NIST, the scope of testing is determined. Each test method helps to understand how the system performs against internal and external threats. This approach enables both foreseeing vulnerabilities through threat modeling and identifying weak points of the defense through attack simulations.

Information Gathering and Vulnerability Analysis

In the information gathering phase, passive and active research is conducted on the system to identify the potential attack surface. Methods such as DNS scans, port scans and social engineering are used. In vulnerability analysis, in-depth analysis is performed with manual tests as well as automatic scanning tools. The information obtained in this process is critical for narrowing the possible attack surface and anticipating risks. The goal is to take precautions by identifying all vulnerabilities in advance.

Authentication and Access Management Tests

Authentication and access authorizations of systems are critical components for cybersecurity. At this stage, mechanisms such as multi-factor authentication (MFA) and session management are tested. Unauthorized access is prevented by determining whether there are vulnerabilities in access controls. Verify that models such as role-based access control (RBAC) are implemented correctly. The tests performed reveal how strong the system's security policies are.

Network Security and Cryptographic Analysis

In network security tests, data traffic and encryption protocols between systems are examined in detail. The effectiveness of secure communication protocols such as HTTPS, TLS is verified. Misconfigured networks and weak encryption algorithms are detected and reported. The effectiveness of network segmentation and firewall policies are also evaluated.

Infiltration and Privilege Escalation

In this phase, attempts are made to infiltrate systems through identified vulnerabilities. Tests from the attacker's perspective show how vulnerabilities can be used in the real world. With rights escalation steps, authorized access is obtained and more authorized levels (e.g. AD, FW, KVM, etc.) are reached in the system. The goal is to simulate in advance any action that attackers can take.

Reporting and Solution Suggestions

At the end of the tests, a detailed report of the vulnerabilities and risks identified is prepared. The reports prioritize each vulnerability by indicating its severity. In addition, technical solutions are proposed for each vulnerability and ways of improvement are explained. With summary reports presented at the management level, decision makers are provided with the opportunity to take quick action.

Continuous Security and Compliance Audit

The ever-changing nature of security threats necessitates regular monitoring and testing of systems. Periodic penetration tests and automated vulnerability scans provide proactive defense against emerging threats. Compliance audits with standards such as PCI DSS, GDPR, ISO 27001, BRSA, TSE, EMRA, CMB and SGT are conducted to ensure full compliance with legal regulations. Security gaps are identified and closed in a timely manner through continuous monitoring and improvement processes.

Audit and Closing

Upon completion of the tests, a verification audit is performed and the findings are checked for closure. At the closing meeting, the results of the tests performed and the actions taken are detailed. Based on the results, remaining risks are identified and solutions are proposed. With the final report, strategic recommendations are presented to plan future security steps. It ensures that the testing process is completed in a holistic manner and the systems are secured.

FAQ

What is a penetration test?

Penetration testing is a controlled cyber attack to assess the security of an organization's network, application or system. The tests simulate attackers' methods to identify security weaknesses in the system.

Why should I have a penetration test?

Penetration testing is a critical tool for organizations to ensure data security. By identifying potential vulnerabilities, it helps you close these weaknesses and build a proactive defense against potential cyberattacks. In addition, compliance with legal regulations and increasing customer confidence are also important benefits of these tests.

What is the difference between penetration testing and automated vulnerability scanning?

Automated vulnerability scans are tools that detect known vulnerabilities, but penetration tests offer a more in-depth analysis. Penetration tests simulate real attack scenarios and provide a more comprehensive security assessment.

How does the penetration testing process work?

The penetration testing process consists of planning, information gathering, vulnerability analysis, exploitation, reporting and closure in accordance with international standards. First, the scope and objectives of the test are determined, then data is collected about the system using passive and active information gathering techniques. In this phase, vulnerabilities are identified and analyzed manually with automated tools. In the next phase, attempts are made to penetrate the systems using the vulnerabilities, which shows how effective the vulnerabilities are. The test results are presented in a detailed report with recommendations for prioritizing and closing the identified vulnerabilities.

How often should penetration tests be performed?

Penetration tests are generally recommended once every six months. However, more frequent testing is recommended in cases of significant system changes or new application deployment. Regular testing is essential to prevent new vulnerabilities from emerging.

Will my systems be affected during penetration testing?

A well-planned penetration test is carried out with minimal impact on systems. However, since every test can have a potential impact, it is important to communicate well in advance and plan carefully.

What kind of reports will I receive after a penetration test?

When testing is complete, a comprehensive report is provided with the vulnerabilities identified and recommendations. This report includes technical details as well as managerial summaries, so that the steps needed for security improvements are clearly laid out.

Is penetration testing a legal requirement?

In many industries, legal regulations require penetration tests to be performed at regular intervals. Especially in areas with sensitive data such as the energy, finance, aviation and healthcare sectors, these tests are critical to ensure legal compliance.

What should be done after a penetration test?

Based on the test results, identified vulnerabilities need to be prioritized and remediated. This process should be part of a continuous improvement process to strengthen the organization's security posture and minimize potential threats.

1. What are the penetration test phases?

Privia Security follows a comprehensive analysis process to detect and prevent security vulnerabilities in penetration tests, consisting of the following 13 phases.

- **Vulnerability Leveling:** Vulnerabilities identified during the penetration testing process are leveled according to the extent to which they threaten the security of the system.
- **Information Gathering:** In order to conduct a thorough penetration test, all possible information about the target is collected.
- **Passive Information Gathering:** In the information gathering phase, information is gathered through search engines without direct contact with the target systems.
- **Active Information Gathering:** In the information gathering phase, target systems are contacted one-to-one and information about the systems is collected.
- **Port Scaning:** After the information gathering phase, when all possible information about the target is available, a more technical approach is applied to analyze the target network and its resources.
- **Vulnerability Scanning:** After collecting information about the target system, port scanning and service detection, the information obtained is evaluated and vulnerability scanning is performed.
- **Enumeration:** Information such as which services are using the ports that are detected to be open, which manufacturer's services these services belong to and their versions are learned.
- **Exploitation:** After the vulnerability scanning and enumeration phases, attempts are made to exploit the vulnerabilities detected and attempts are made on the target system and its security.
- **Privilege Escalation:** Detected vulnerabilities are exploited to gain access to the target system.
- **Post Exploitation:** The post-exploitation phase involves determining the value of the compromised system and maintaining control of the system for later use.

- **Undoing Actions Taken:** In this phase, all changes made to the systems are rolled back before the test is finished.
- **Reporting:** If requested in writing by the client, the printed version of the report shall be marked “Confidential” and delivered in a sealed envelope.
- **Presentation:** After the delivery of the reports, if requested, a summary presentation of the penetration test is made to the personnel of the organization. In this way, the staff of the organization gains the opportunity to exchange views on the test with our experts who performed the penetration test.

2. What are the tools and methodologies used in the testing process?

Our penetration tests are based on both national and international methodological approaches and apply both external (Internet) and internal (Internal) penetration tests to uncover security vulnerabilities. This approach provides an effective risk analysis by identifying existing vulnerabilities.

Our testing team does not rely on automated vulnerability scanning applications. It leverages a range of open source and commercial penetration testing tools to manually perform tasks such as attack surface mapping, network and asset discovery to detect hidden and complex vulnerabilities.

Our tests are based on security norms, methodologies and standards such as OWASP (Open Web Application Security Project), PTES (Penetration Testing Execution Standard), OSSTM (Open Source Security Testing Methodology Manual), NIST and ISSAF (Information Applications Security Assessment Framework), including active, dynamic and static analysis of the target system.

Our penetration testing methodologies play a vital role in strengthening defenses against evolving cyber threats by providing a standardized framework for communication and resource optimization.

OWASP: This widely known standard is developed and updated by a community that keeps up with the latest cyber threats. It accounts for application vulnerabilities as well as logic errors in processes.

PTES: It is a pentest methodology designed by a team of information security experts. The goal of PTES is to create a comprehensive and up-to-date standard for penetration testing, as well as to raise awareness among businesses about what to expect from a penetration test.

OSSTMM: It is one of the most widely used and recognized penetration testing standards. It is based on a scientific approach to penetration testing with adaptable guidelines for testers.

NIST: It provides very specific penetration testing guidelines to the testing team to help improve the accuracy of the test. Both large and small companies in various industries can benefit from this framework for penetration testing.

ISSAF: It is a pentesting guide sponsored by the Open Information Systems Security Group. This methodology is no longer updated, however, it is still used due to its comprehensive nature

4. Which industries require penetration testing?

We recommend that companies that process sensitive data or have a high risk of cyber-attack, such as healthcare organizations, public institutions, R&D-intensive companies, financial institutions and e-commerce businesses, should have a penetration test at least once every three months.

With strict compliance requirements and regular penetration testing, such organizations can develop an effective defense mechanism against data breaches while ensuring regulatory compliance, as they may face higher risks if data is compromised.

6. What are the precautions to be taken after a penetration test?

After receiving the report we provide to your company after the penetration test, you can follow the recommendations we offer below to prioritize vulnerabilities, create a remediation plan and quickly implement the necessary security measures:

Prioritize vulnerabilities: Prioritize the vulnerabilities we identified in the report based on their risk level and impact and decide which ones to address first.

Assign responsibilities: Assign responsibilities for remediating vulnerabilities to relevant parties, such as developers, IT staff, or third-party vendors. Communicate the remediation objectives, scope, timeline, expected results and the roles and responsibilities of each party.

Implement the recommendations: Follow the recommendations found in our penetration test report to fix vulnerabilities, contact us if you have any questions or doubts.

Verify and confirm the correction: Confirm that the remediation was successful and that the vulnerabilities have been fixed. Also, update your documentation and records to reflect the current state of the system.

7. How does penetration testing affect your systems?

The duration of a penetration test depends on the objectives, the approach and the size and complexity of the environment (attack surface) to be tested. A penetration test for an application or SMB (SMB) can be completed in a few days, but a large and complex environment can take longer. The testing process can be lengthened due to the nature and complexity of the systems to be tested.

Throughout this process, Privia Security performs penetration testing in accordance with the strictest legal and technical ethical standards. Testing minimizes the risk of disrupting business operations and in most cases, operational continuity is maintained without even realizing that testing is ongoing. When we need to test a system that could impact availability, your company will be notified and your needs will be addressed.

8. How soon the penetration test results are reported?

On average, a penetration test conducted by Privia Security takes 2 to 4 weeks to complete and report. However, factors such as the size of the potential attack surface and the extent of existing cybersecurity defenses can affect this time and cause the process to increase.

Our report starts with an executive summary, summarizes the vulnerabilities and their impact on the business and makes recommendations to fix the vulnerabilities.

9. Who performs penetration testing?

Privia Security penetration testing is carried out by our personnel with national and international certifications (such as TSE, OSCP).

Our team of experts has a strong understanding of various operating systems, networks and applications, a deep knowledge of vulnerabilities and exploits and competence in various security testing tools and techniques.

10. How to protect data obtained during penetration testing?

In a penetration test conducted by Privia Security, security protocols that comply with both national and international standards are applied to protect data. In addition, within the scope of the Non-Disclosure Agreement (NDA) we sign with our customers, this data is never shared with third parties. The information obtained during the testing process is only used to improve the customer's security posture. After the prepared report is submitted, it is deleted from the systems with secure data deletion methods.

12. How penetration testing helps meet our compliance requirements?

After a penetration test conducted by Privia Security, our test team prepares a pentest report. In this report, the vulnerabilities and remediation steps are documented and presented to your company. After the vulnerabilities are fixed, a re-scan is performed to verify that all gaps have been fixed and your system is protected.

This type of testing is mandated in various industries to ensure your company meets certain local and global security compliances. There are many industry standards that require penetration testing such as PCI, SOC 2, HIPAA, GDPR, etc.

- HIPAA for healthcare organizations
- PCI-DSS for payment processing companies, TSE
- RBI-ISMS, BRSA, CMB, TSE for banks and non-banking financial institutions
- SGT for Civil Aviation companies, TSE
- SOC 2 for service organizations
- ISO 27001 for any organization willing to do business around information security

The results of penetration testing can be used by auditors to comply with regulatory requirements. This type of testing provides important evidence to demonstrate the effectiveness of your business's security measures and manage potential risks.

15. How long the penetration test results are stored?

After the verification test is completed, the report presented to the customer is permanently destroyed from our system with secure data deletion methods and recorded.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—

Privia
SECURITY