Bitdefender

SERVICE BRIEF

Bitdefender Penetration Testing Services

Trusted. Always.

Service Brief

Our experienced and certified consultants are able to conduct assessments or simulated attacks to identify vulnerabilities, through delivering a number of different services:

- Web Applications
- Mobile Applications
- Networks
- Thick Client Applications
- Web Services / API
- Wireless Access Points

The purpose of a penetration test is to identify key security weaknesses so they can be remediated, thereby improving the security of applications, and by extension, the organization undergoing testing.

How It Works

Scoping

Penetration testers determine the effort needed to conduct the assessment. More details in the Scoping Card.

Reconnaissance

This phase begins with passive and active reconnaissance techniques to compile and collate information on the targets. Exposed services will be interacted with to determine their versions and supported functionality. The results from both passive and active reconnaissance will be compiled and analyzed, for use in the next phase.

Vulnerability Identification

Identification of vulnerabilities is performed using an automated scanner and manual testing. During manual verification, the consultants will look out for more complex vulnerabilities, such as business logic flaws, access control bypass, and injections, that the automated scanner does not pick up easily.

Exploitation

Our consultants will try to exploit and compromise the target hosts. The objective is to simulate malicious actors and their possible motivations to gain value out of the target hosts. In certain scenarios, the consultants will chain vulnerabilities to achieve the maximum possible impact on the target company. When the exploitation is successful, the consultants will review the results and perform reconnaissance on any newly found access or information. The cycle repeats until there is no new attack vector.

Reporting

The report will contain assessment and vulnerability details, including issue title, risk rating, description, reproduction steps, implication, recommendation, and evidence screenshots. Internal report review will be conducted to ensure quality assurance.

Different Types of Penetration Testing

- **Black-box Testing**
  - No information or access is given, other than the scope of work; testing from an anonymous user perspective
  - Typically given only the target URL or IP addresses
  - The testing is limited to the access that the tester managed to find or exploit
- **Grey-box Testing**
  - Limited information and access may be provided
  - Credentials accessing the targets
  - Limited documentation on the targets, e.g. API documentation, network architecture diagrams
  - Limited Technical Support from the developer/administrator
  - Include the black-box testing approach
  - The testing will be more comprehensive as the consultants will be able to test into the functions accessible by the internal users
- **White-box Testing**
  - Full access to information about the targets
  - Full Admin access to the target application and servers
  - Full documentation on the target, e.g. Technical Specification, Security requirements, detailed network architecture diagrams
  - Full Source code
  - Full support from the technical stakeholders (e.g. developer and administrator)
  - It will be most comprehensive among all. Additional efforts will be required for reviewing all the information provided to identify all possible vulnerabilities

Who Should Consider Penetration Testing?

- Cybersecurity Leaders that seek to fulfill penetration testing requirements (e.g. MAS TRM Notice)
- C-suite executives seeking to perform due diligence in avoiding exploitable vulnerabilities that lead to data breaches
- Development and Infrastructure teams seeking to validate new security controls (e.g. automated tests in CI pipeline, zero trust network segmentation)

What Do We Require To Provide a Quote?

- Objective of test (compliance to regulatory requirements)
- Scope of test (URLs, IP addresses)
- Access Control Matrix (functions accessible to each user role)
- Information on workflows (user manuals, user acceptance test documents, walkthroughs)
- Security controls that may reduce testing efficiency (end-to-end message encryption, jailbreak detection, Web Application Firewall rate-limits)
- Assessment preferences (location, time of testing)
- Assessment type (e.g. Black-box or grey-box approach)
- Technical scoping to be conducted by the delivery consulting teams

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-ServiceBrief-PenTest-creat7364-en_EN
CD-10/20/23 • MD-November 3, 2023 4:26 pm