

CYBERSECURITY SERVICES

BlueSky's talented ethical hacking team will use various exploitation tactics to conduct in-depth testing of your network infrastructure and expose security gaps.

PENETRATION TESTING

Understanding Pen-Testing

A penetration test, or pen-test, is a safe way to evaluate the security of your IT infrastructure by attempting to exploit critical vulnerabilities. By testing whether unauthorized access or malicious activity is possible, we help to identify areas of weakness and fix them in order to stop future attacks.

BlueSky penetration tests include some or all of the following security zones:

- Social Engineering
- Physical Security
- External Systems
- Internal Systems

The pen-test services that BlueSky offers cover a wide range of needs, and can include anything from minimally invasive tests to more aggressive efforts to compromise your network.

Types of Pen-Tests

Black Box: In a real-world attack scenario, the attacker(s) will not likely know all the details of the IT infrastructure of a corporation. Because of this, he or she will launch a brute force attack against the IT infrastructure, in hopes of trying to find a vulnerability or weakness on which they latch onto. In this type of pen-test, there is no information given to the tester about the internal workings of the architecture.

White Box: Also known as "Clear Box Testing," in this test the tester has full knowledge and/or access to the target(s) or organization. Because of this, a White Box Test can be accomplished in a much quicker time frame when compared to a Black Box Test; and a more thorough test can be completed.

Gray Box: As the name implies, this type of test is a combination of both Black Box and White Box testing. In other words, the penetration tester only has a partial knowledge of the internal workings of the target(s) or organization.

Contact us to learn how pen-tests can improve and transform your cybersecurity efforts.

