TESTING CYBER DEFENSES

Organizations do all that they can to protect their critical cyber assets, but they don't always systematically test their defenses.

Penetration tests – otherwise known as pen testing – are a type of ethical hacking that can be used to evaluate the security of a network regularly. Our team of highly-skilled cybersecurity experts utilizes a combination of tactical and strategic approaches to discover and exploit vulnerabilities in our clients' Information Technology (IT) systems.

Securicon's penetration tests:

- Gather information about the target before the test (i.e., exploration)
- Identify possible entry points and attempting to break in
- Report the outcome through a detailed assessment

PROPRIETARY, PROVEN TESTS

Average security companies often blur the lines between penetration tests and vulnerability assessments. At Securicon, our proprietary pen testing methodology is based on years of experience in areas such as network administration, integration engineering, incident forensics, and response.

We combine penetration techniques with vulnerability assessment activities, configuration reviews, and architecture analysis. In some cases, we even evaluate policies and host interactive discussions with client staff members.

Whether we are testing an application or network environment, Securicon's pen testing will not only identify vulnerabilities, but it will also demonstrate them through exploitation – definitively determining if unauthorized access or other malicious activity is possible.

MORE MEANINGFUL RESULTS

In the hands of a Securicon Senior Pen Tester, even limited penetration provides a more in-depth view of network and application interrelationships than any other company's pen testing can.

SECURICON
Information Security Solutions

We use pen testing as a tool to delve deeper into the systems and networks that need to be assessed. If our engineers find a weakness, we conduct a thorough review - checking details that would otherwise not be visible during a routine vulnerability assessment.

We examine how:

- Authentication and data traffic flows throughout the network, establishing the roles of various systems within the network

- Different systems support the business functions of the organization, recognizing what is important to who

- Communication moves between a system and its users, giving us the vital information we need to design protective control mechanisms

- By performing this thorough analysis, Securicon can assign risk ratings to vulnerabilities, ensuring that our risk-remediation recommendations are cost-effective and appropriate for their environment.

Are you ready to test your cyber defenses?

Learn more about Securicon's expert solutions by giving us a call at 571-253-6565 or email us at sales@securicon.com.

SECURICON
Information Security Solutions