CYLANCE CONSULTING

External Penetration Assessment

Evaluate the Effectiveness of
Your Network Security Program

Benefits

- Identify and verify vulnerabilities before they are discovered by a malicious party
- Assess the impact that exploiting those vulnerabilities has on affected systems and resources
- Recognize select high-risk weaknesses that exist due to a combination of smaller vulnerabilities
- Identify weaknesses and gaps that are impossible to detect through just automated vulnerability scanning
- Meet legal or compliance requirements from PCI-DSS, ISO 27001, and other regulations requiring pen testing

$4,000,000

On average, the cost of a breach has risen to $4 million per incident – up 29% since 2013.

Source: IBM 2016 Cost of Data Breach Study – United States

CYLANCE

+1-877-97DEFEND
proservices@cylance.com
www.cylance.com/consulting
18201 Von Karman Avenue
Suite 700, Irvine, CA 92612

While network threats have existed for decades, the time between vulnerability and exploit is shrinking. Organizations are forced to spend more money on investigations, notifications and response when sensitive and confidential information is lost or stolen. Protecting Internet-facing infrastructure from external threats begins with identifying external system attack surfaces.

Cylance® Consulting's External Penetration Assessment helps **identify vulnerabilities that may be difficult or impossible to detect with scanning software.** We also provide **recommendations for remediating these vulnerabilities** BEFORE an attack can occur.

Service Overview

The objective of an External Penetration Assessment is to conduct a thorough test of Internet defenses. Technical experts use a mix of manual and automated testing techniques in an attempt to gain access to the system and/or sensitive data on the system.

The activities performed may include:

- Footprinting
- Vulnerability Scanning and Analysis
- Manual Vulnerability Verification
- Penetration Testing and Exploitation

Information is collected about the organization's security practices, policies, and procedures through survey responses, staff interviews, tools, company documentation, and site walk downs.

Deliverables

Cylance Consulting will furnish a comprehensive report that includes:

- Detailed descriptions of vulnerabilities with actionable advice for remediation
- Detailed anatomy of attacks that where successful during the assessment
- Tactical and strategic recommendations
- Next steps and security roadmap recommendations
- IP addresses and hostnames of all tested systems
- Open ports and listening devices on these systems

Strengthen your security infrastructure to reduce the possibility of an external attacker compromising confidential information. Contact Cylance Consulting or your technology provider for details.