CYLANCE CONSULTING

Internal Penetration Assessment

Simulate an Attack from Inside the Network

While most networks are reasonably well protected externally, they are not as well defended internally. As a result, they can be easily compromised once an attacker is able to gain a foothold. These attacks have the potential to be more devastating because insiders already have knowledge of what is important within a network and where it's located – something external attackers don't usually know from the start.

An Internal Penetration Assessment is similar to an External Penetration Assessment, but the "attacker" either has some sort of authorized access, or is starting from a point within the internal network. The results typically **demonstrate what assets might be exposed to an unauthorized user** who has network-level access to your corporate IT environment. The assessment can also help **identify the impact of poor access controls as well as mitigate the impact of a malicious or disgruntled employee.**

Service Overview

Cylance® Consulting's Internal Penetration Assessment begins the internal testing from the perspective of an attacker that has gained a foothold on the internal network with the goal of determining what systems can be compromised and what sensitive data can be accessed. An assessment may include:

- Host Discovery
- Footprinting
- Vulnerability Scanning
- Manual Vulnerability Verification
- Penetration Testing
- Vulnerability Analysis

Deliverables

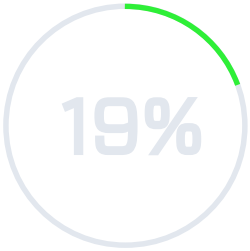
Cylance Consulting will furnish a comprehensive report detailing:

- Vulnerabilities discovered along with recommendations for remediation
- IP addresses and hostnames tested with open ports and listening devices on these systems
- The in-depth anatomy of successful attacks
- Strategic and tactical recommendations

Discover weak points in your internal network with an Internal Network Penetration Assessment. Contact Cylance Consulting or your technology provider for details.

Benefits:

- Detect and remediate weaknesses that could allow a compromise
- Ensure internal user privileges cannot be misused
- Mitigate the impact of a malicious or disgruntled employee
- Facilitate compliance with regulations like PCI-DSS and more
- Test internal monitoring and incident response capabilities
- Improve security strategy through a long-term roadmap
- Identify attack paths that could remain unseen without a penetration assessment



Estimated direct source of security incidents from third party vendors in 2017.

Source: 2018 The Global State of Information Security Survey | PWC

BlackBerry

CYLANCE

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting