Internal Penetration Testing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Threats Are Closer Than You Think

You never think it will happen to you, but the second an employee gets upset or an unauthorized person gets into your building, information can be compromised – fast. It's hard enough trying to defend against outside hackers, but what if a disgruntled employee decides they want to steal sensitive company information? They are already in your network, making it much easier for them to access records and a lot of other confidential information.

What We've Noticed

The most common vulnerabilities discovered during an IPT are related to network configuration. Many default systems that organizations use to communicate over their networks actually allow malicious attackers to capture information as it travels through the network, leaving your organization vulnerable to a breach. Another common vulnerability comes from your device and service configurations. Leaving default configurations on any device may not seem harmful, but it provides an easy access point for attackers to access sensitive areas.

Know Where You Stand

Our Internal Penetration Testing (IPT) simulates what could happen once your external measures have been breached, an employee went rogue, or someone walked through the front door of the facility and found an open Ethernet port to plug into. An IPT will determine any weaknesses in your internal security measures and see what someone could access once inside as well as how far they can go. Beyond vulnerability scanning, our analysts will also use manual attacks to actually exploit any discovered vulnerabilities as well as use other common techniques in an attempt to gain access to sensitive systems or information.

Internal Penetration Testing Features:

- **Determines weaknesses of internal security measures**
- **Manual testing of discovered vulnerabilities**
- **Utilizes tools and techniques used by real-world attackers**
- **Comprehensive report with actionable recommendations for remediation**

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?
Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?
This is extremely unlikely. We very rarely have any reported problems. We do not attempt any denial of service attacks.

How do you perform this service?
We can perform an IPT remotely or onsite. If remote, we connect through the TraceCSO Vulnerability Scanner.

Do I need an 8-hour IPT or a 16-hour IPT?
This depends on the organization's goal for the assessment. The more time we have, the more thorough we can be in our testing. We generally recommend one over the other based on your asset size.

What kinds of questions are asked in the scoping call?
We ask for target IP addresses and exclusions, account lockout policies so that we can mitigate the risk of locking out domain users during testing, times you want vulnerability scans to run, and confirm the date/time that we will be testing.

Is there a difference in approach between IPT and EPT?
The approach is very different between IPT and EPT because there are many more IP addresses with open ports on an internal network. Testing each and every open port on internal systems could take weeks to months. In an EPT, we are usually able to test each open port due to a smaller number of IP addresses. In an IPT, our information security analysts use their expertise to identify attack vectors with the highest possibility of success to compromise a host or network.

Why does an IPT cost more than an EPT and take more time?
An IPT requires more hours and expertise, and more systems are involved.

What if the test only takes you 3 hours? Why am I paying for 8 hours?
An IPT will almost always take the full 8 hours due to the amount of time it takes our analysts to gain an understanding of the network and what is available.