Advanced Persistent Threat Assessment

Simulate an All-Out Attack

If an attacker attempted to compromise your organization's sensitive information, they wouldn't just give up after a few failed attempts. With so many avenues for accessing your IT environment, it's likely that they'll try many different techniques in order to breach your systems. Real attacks are not point-in-time events, but rather occur over longer periods of time, slowly defeating different security measures until valuable data is collected. What would happen if an attacker decided to target your organization?

IT security and compliance are a behemoth of constantly evolving threats and regulations. Between penetration tests, zero-day malware, IT audits, new compliance regulations and everything in between, it can be hard to know if your security efforts are actually working to secure your organization. You need a test of your controls at multiple levels – technical controls, personnel and procedural controls and physical controls - to get a true picture of how your organization would hold up against an all-out attack.

Our Methodology

With our Advanced Persistent Threat Assessment (APTA), we'll simulate a brute-force attack as if your organization has become a priority target. Each step in this testing process is designed to simulate an attacker coming at your organization from every angle. Testing includes information gathering, an external penetration test, remote social engineering, a wireless penetration test, onsite social engineering, and an internal penetration test. Each level builds on one another the same way an attacker would use information from other hacking attempts to breach other areas of your IT environment.

Following all testing, our cybersecurity experts will provide you with a single report that can help you easily identify security or control gaps. This comprehensive test will give you the best information on what a real-world attacker could access should your organization become a target. Since you don't want to be a target in the first place, our APTA will allow you to fix vulnerabilities in many areas of your networks before a malicious attacker can find and exploit them.

An APTA Includes:

- **Information Gathering and Reconnaissance**
- **External Penetration Test**
- **Remote Social Engineering**
- **Wireless Penetration Test**
- **Onsite Social Engineering**
- **Internal Penetration Test**

Frequently Asked Questions

How does each level of testing work together?
Reconnaissance involves gathering publicly available information about your organization that an attacker could use in any of the successive testing methods. Your external network can be easily seen by those around your building, so our external penetration test shows what an attacker could access should they breach it. Remote social engineering can be used as a way to inject malicious software into your systems via phishing or compromise network information over the phone that could be used to help facilitate the other penetration tests being performed. Onsite social engineering tests your employee adherence to visitor and escort policies, which if not followed can lead to compromised systems or sensitive information and facilitate the internal penetration test. If an attacker found a way to access your internal network via social engineering or other methods, our internal penetration test will demonstrate how far they could go and what data or systems could be infiltrated.

What is done during reconnaissance?
Our Information Security Analyst will search publicly available information about your organization that an attacker could use in various forms of cyberattacks.

What is the difference between the external penetration test and the internal penetration test?
While both involve manual exploitation of vulnerabilities found on your networks, external penetration testing focuses on your external networks and internal penetration testing focuses on your internal networks. Internal penetration testing is inherently more complicated since organizations typically have many more internally facing IP addresses.

How is the phishing portion of this assessment completed? Do you phish my employees at the same time or in intervals?
The details of the phishing engagement can be determined during the scoping call with our analyst team. The goal for the assessment is to provide a real-life simulation of what attackers typically do when targeting an organization, and we want to ensure we are providing you with the best possible test scenario.

What is the script you use for vishing phone calls?
We do not have just one script that we use. We are open to hearing your ideas, but we can also suggest some that we regularly use and have success with.

What kinds of cover stories do you use during onsite social engineering?
Our analyst will typically pose as an exterminator, inspector, or other trusted agent that would typically be let into more sensitive areas of your organization without question.