RED TEAM
Penetration Testing

Can your security measures withstand a targeted attack?

Every day we hear news reports of organizations that have been breached by malicious actors. These attacks are generally sophisticated and well-coordinated. They can lead to remote access of internal networks and exfiltration of sensitive data. Although your organization has policies, procedures, and technical barriers in place to prevent a breach, how can you be certain they will work when put to the test?

The best way to get peace of mind is through rigorous, proactive testing. Digital Defense, Inc.'s Red Team Penetration Testing (RTPT) holistically assesses your attack surface and identify weaknesses before they are exploited. RTPT combines open source intelligence collection and social engineering, along with internal and external penetration testing to evaluate your organization's susceptibility to a targeted attack. Using RTPT allows you to gauge the efficacy of your defenses, as well as your detection and response capabilities.

Through collaboration with your team, Digital Defense designs scenarios that mimic current threat vectors being seen in the real-world. This tailored approach enables RTPT to accurately test for technical and organizational vulnerabilities and provide action-able recommendations to mitigate any identified security gaps.

The RTPT process begins with an intelligence collection phase. Our analysts search for your organization's sensitive information on social media networks, corporate job postings, and even in data dumps posted on the dark web. This type of information is used by attackers to gain a foothold through credential reuse or for targeted social engineering campaigns. RTPT will test your susceptibility to both.

The social engineering phase of RTPT can be remote, onsite, or a combination. Digital Defense has a wealth of experience in social engineering engagements and is flexible to meet your demands. If your organization is hardened enough to keep our analysts out through technical barriers as well as social engineering, Digital Defense will then work with you to conduct a simulated internal attack and make attempts to gain access to the data your organization values most.

Let our Red Team Penetration Testing help strengthen your security posture.

Red Team Penetration Testing benefits include:

- **Insight** into your externally exposed information
- **Proactive discovery** of physical, technical, social vulnerabilities
- **Evaluation of your team's** ability to detect and thwart attackers
- **Identifying your weakest points** for improvement prioritization
- **Actionable reports** with suggested mitigations

Discover Your Weaknesses Before They are Exploited

Contact: sales@digitaldefense.com

For more information visit: www.DigitalDefense.com

DIGITAL DEFENSE INCORPORATED

9000 Tesoro Drive, Suite 100
San Antonio TX 78217
Toll Free: 888.273.1412