ATTACK AND PENETRATION SERVICES

Exposing Weakness to Validate Your Security Program

OVERVIEW

Protecting assets can be a daunting task. How do you know that your current controls are working and that you have your bases covered? That's where Dscifer can help. Using a combination of automated tools and elite attackers, researchers and practitioners, we can help you find and mitigate vulnerabilities. Whether you require white, grey or black box services, we are here to answer the call. We provide solutions for companies new to testing, or for organizations with mature vulnerability management programs.

Dscifer has a team of researchers at the ready to help test your systems. Our approach exposes weaknesses in systems and identifies paths vulnerable to exploitation - before a malicious actor does. Our mature methodology provides actionable steps for better securing your systems. Engaging with our team will uncover vulnerabilities and highlight actions that help you make informed decisions in reducing risk within the business. We also assist clients with achieving or maintaining compliance by meeting testing requirements in standards such as the Payment Card Industry Data Security Standard (PCI DSS).

Expose weaknesses in systems and **identify paths vulnerable** to exploitation - **before a malicious actor does.**

Attack and Penetration Services:

We help our clients identify points of failure in their existing technology, people and process. By emulating your adversary, we help to uncover critical exploitable vulnerabilities and provide detailed guidance for remediation, leaving you better protected and less vulnerable to attack. Our services can scale to meet your needs, from compliance testing to adversarial incident simulations. Engaging with us will reveal access points to your critical systems, help close pathways of attack and leave you with a smaller attack surface. The thought of an attack can be daunting. We give you less to worry about.

Benefits of working with us:

- Identify weakness in your technologies, processes and people
- Remediate vulnerabilities and minimize the attack surface
- Reduce risk and meet compliance requirements

Among data breaches that resulted from **known vulnerabilities,**

99.9% **involved vulnerabilities for which patches had been available for over a year.***

23% of **recipients now open phishing messages** and 11 percent click on attachments.

How long does an attacker have to wait before someone responds to a typical phishing attack?*

Just 82 seconds.

Identify points of failure across technology, people and process.

* Verizon 2015 Data Breach Investigations Report

Breach Simulation

Goal

Operate outside of traditional testing methodologies and scope limitations to perform complex breach simulations. Perform opportunistic blended attacks using social engineering, physical security and network and application attack techniques to operate outside the rules and simulate real world threats. Highlight the impact of a breach to an organization, the board and the executive team.

Overview

Simulating an attacker's actions, our team will use subterfuge and distraction while identifying points of weakness, exploit your critical systems, exfiltrate data and create a series of events that mimic an actual breach.

REVIEW PHASES

› Remote Breach Simulation
› On-site Breach Simulation

BENEFITS

› Take Your Recurring Penetration Testing Activities to the Next Level
› Identify Weaknesses that Traditional Control-based Testing Methodologies Miss
› Prepare Your Staff in the Event of a Crisis › Vet Your Incident Response Plan
› Communicate the Importance of Security, Security Training, Policies and Procedures

Risk Validation

Goal

Understand, quantify and document the real-world risk of an attack scenario.

Overview

During a penetration test, our experts will attempt to breach the information security controls of your organization. Using an arsenal of techniques and tools, our penetration testers will try to exploit your critical network, applications and systems and access and exfiltrate sensitive data or other specified targets. We conduct penetration testing on a variety of systems and from various perspectives to help you understand your true risk. If a system is compromised, post-exploitation techniques identify additional risks, allowing lateral and vertical pivoting through the network.

SERVICES

› Targeted Penetration Test
› Comprehensive Penetration Test › Physical Security Penetration Test › Product Penetration Test

BENEFITS

› Identify Weaknesses in Your Systems
› Understand the Multiple Points of Failure that Can Lead to a Breach or Disclosure
› Identify Lateral and Vertical Exploitation Vulnerabilities that Lead to Privilege Escalation and Sensitive Data Loss
› Document and Remediate Vulnerabilities
› Verify Security Controls

Security Controls Assessments

Goal

Evaluate your enterprise security effort at a technical and program level.

Overview

As part of our enterprise security assessment process, we examine and assess various controls, technologies and procedures to identify points of failure. Our trained experts can evaluate select systems or entire environments. This service includes a validation of your policies, procedures, infrastructure implementations and security controls from an offensive perspective.

SERVICES

› Vulnerability Assessment
› Social Engineering Assessment ›
Wireless Security Assessment ›
Voice Over IP Assessment
› War Dialing Assessment

BENEFITS

› Understanding of Security Issues in Critical Systems ›
Recommendations for Remediation
› Expertise to Help Identify Your Most Critical Weaknesses

Vulnerability Discovery

Goal

Identify, quantify and rank vulnerabilities in your systems.

Overview

Our vulnerability discovery services provide an in-depth look at your security posture. Using tools, we find weaknesses, evaluate their severity and make recommendations for mitigation. As a result, you will receive a report detailing our findings and recommendations for addressing vulnerabilities.

SERVICES

› Public Information Profile ›
Vulnerability Scan
› Rapid Response Zero Day Vulnerability Detection

BENEFITS

› Locate Weak Spots in Your Security Infrastructure ›
Document Risks in Your Environment
› Receive Recommendations to Address Those Risks

Bespoke Engagements

Dscifer's security researchers and practitioners have years of penetration and attack testing experience. We routinely assist organizations with assessing policies, procedures and the human element of complex systems. As part of our commitment to quality and client service, we deliver detailed documentation of our findings along with actionable recommendations to eliminate problems now and in the future.

DSCIFER

Dscifer.com

Dscifer specializes in comprehensive pure-play Cyber Security, Digital Forensic & E-Discovery, Risk Management, Healthcare, Aerospace and Defense Systems solutions. Our diverse and talented employees are committed to help businesses, governments and educational institutions plan, build and run successful management programs through the right combination of products, services and solutions.