SecurityRisk ADVISORS

External Network Penetration Test

Our testing attempts to identify insecure applications, network services, overly-permissive firewall rules, and other configuration settings that could allow an Internet hacker to attempt to compromise systems and data. We perform the following activities in an attempt to demonstrate whether this type of access could lead to data loss, perimeter breach, or reputation harm:

1. Reconnaissance

We begin by creating our own view your Internet presence and perimeter and provide it to you for discussion. We jointly review approved external resources with you, and we use advanced Internet search queries, examine publicly available databases, and manually investigate web pages to profile resources in your Internet-facing perimeter, related subsidiaries and/or approved third-party vendors.

2. Research, Verify & Assess

Based on the services and resources identified, we will prioritize test objectives to focus our testing on key risk areas. Our team manually researches weaknesses and analyzes their susceptibility to attacks. Examples of these risk areas are listed on the right.

If we identify these types of vulnerabilities, we demonstrate their impact and discuss with you whether it may be appropriate to perform additional testing to demonstrate the full impact to your environment and business processes. We provide on-going communication of high risk areas with our points of contact, so that management will be apprised of any critical weaknesses that we may identify.

3. Evidence & Recommend

We present appropriate evidence of our access through screen captures and sample data to illustrate the impact to the business for each observation. We categorize our observations by risk in a detailed observations matrix, and provide recommendations to address any vulnerability that we might find. In addition to short term fixes, we will describe the process-oriented weaknesses and recommend changes designed to prevent the issues from reappearing.

Contact Us

Phone: 215.867.9051
Email: info@securityriskadvisors.com
Website: www.securityriskadvisors.com

Common Risk Areas

Enticement Information
General enticement information found in application source code, error messages or through advanced Internet searches.

Web Application Vulnerabilities
Focus on business logic flaws and custom vulnerability identification. This includes but not limited to those described in the OWASP Top Ten.

Web Server Vulnerabilities
Missing patches and misconfigurations on web servers and proxies.

Remote Access & Administration
Weak passwords and misconfigurations on administration tools such as VPN, Extranets, SharePoint, Citrix, RDP, Telnet, SSH, and VNC.

Database Misconfigurations
Databases that have ports open to the Internet including SQL Server, MySQL, and Oracle.

Network Device Vulnerabilities
Weak passwords, misconfigurations and over-permissive firewall and router access control lists, both inbound and outbound.

Common Network Protocol
Weaknesses in File Transfer Protocol (FTP), Network File System (NFS), Network Information System (NIS), Server Message Block (SMB) and NetBIOS, Domain Name Server (DNS), Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP) vulnerabilities.

Operating System Vulnerabilities
Misconfigurations, missing patches and open ports on externally facing Windows, Unix, Linux, OSX, and ESX servers.

Denial Of Service (DoS)
Vulnerabilities that may be identified based on software versions, but we will not attempt to trigger or exploit them.

Web services vulnerabilities
Including unprotected SOAP XML and REST web service endpoints.

Cloud service Misconfigurations
Including Amazon AWS, Microsoft Azure and Office365 flaws such as improper key management and overly permissive virtual firewall.

Internal Network Penetration Test

Our testing attempts to identify system and network service vulnerabilities to assess whether a motivated insider or visitor could elevate access to steal data for profit or gain access to protected systems and data in your offices, data centers, and other possible business partner connectivity. We will perform the following activities:

1. Reconnaissance

We perform network mapping and passive service enumeration techniques on your internal network and infrastructure. We then attempt to identify vulnerable systems and applications without any prior knowledge of user accounts. We identify and categorize systems by potential business impact, network segment, operating system, patch levels and services installed. Once we have completed this "blind" test, at your direction, we also perform the exercise from the point of view of a Windows domain user, to demonstrate the difference created by that level of access, if applicable.

2. Research, Verify & Assess

Based on the services and resources identified, we prioritize test objectives to focus our testing on the riskiest areas. We analyze the network for the general types of vulnerabilities listed in the section to the right.

While we may identify **one-off** vulnerabilities such as insecurely configured third party systems which can lead to widespread network access, we focus on identifying **pervasive** types of vulnerabilities which can be indicative of process, roles, or security toolset gaps. Examples of these types of vulnerabilities could include, but are not limited to, incomplete coverage of patch management processes, inconsistent server and workstation builds, gaps in detection and monitoring of attacker kill chain activities, and privilege management policy weaknesses.

3. Evidence & Recommend

We present appropriate evidence of our access though screen captures and/or sample data to illustrate and explain the impact to the business for each of our observations. We categorize our observations by risk in a detailed observations matrix and provide appropriate recommendations to address any vulnerability that we might find. In addition to short term fixes, we describe the process-oriented weaknesses and recommend changes designed to prevent the issues from reappearing.

About Our Company

Security Risk Advisors provides expert consulting services with specializations in advanced threats controls implementation and 24x7 operation, red and blue teams, control frameworks, and GRC process improvement. Our approach emphasizes ongoing knowledge transfer and access to our analysts.

Differentiators

Recognized Thought Leadership

Security Risk Advisors contributes to cybersecurity thought leadership conferences, including RSA, Gartner, ISC(2), FS-ISAC, NH-ISAC and other knowledge-building organizations. In 2017 we released a cutting-edge freeware reporting and workflow tool for measuring CyberSOC detection rates and improvement.

Advisory, Engineering, and Operations Experience

Our strategic advice comes from a rounded perspective of working with leading companies to develop strategies and implement complex cybersecurity controls. We also operate modern detection and threat hunting controls for global organizations in our 24x7 CyberSOC, which allows us to credibly relate to our most advanced clients.

Independence

We are not a reseller of security software, so we are independent and neutral to recommend best-fit controls, based on our experience implementing and operating them.

Technical and Compliance Roots

Our strategy team leads have deep experience understanding both technical and compliance-oriented complexities of large organizations. We focus on working with top market clients, but we also maintain broad perspective by working with innovating technology start-ups and mission-oriented non-profits.