Visualizing Network Risk via Vulnerability Exposure paths for effective mitigation with RedSeal and Nexpose

Solution Overview

In many of today’s organizations that are conducting a vulnerability management program, there can be challenges in addressing the most pressing vulnerabilities. Primarily, which vulnerabilities pose the greatest risk to the organization if not mitigated properly. By integrating Rapid7’s Nexpose rich vulnerability data with RedSeal, an organization has a clear and visual way of seeing their network based risk. Utilizing RedSeal, a security analyst can conduct virtual penetration testing to see full attack path analysis within the network and use that information to prioritize which vulnerabilities pose the greatest threat if successfully exploited. A prioritized report can be generated that will highlight which vulnerabilities need to be addressed first to minimize exploitation impact.

How it works

A Nexpose scan is conducted to assess the risk posture of the systems within an organization. The vulnerability results are then taken and used to calculate the RealRisk™ Score associated with each system. A task in RedSeal is created to query Nexpose on a scheduled basis for the latest vulnerability information. An XML report is generated via the API to export the results. The vulnerability data is processed and stored within RedSeal for further analysis.

Integration Benefits

- **Impact Analysis** via “What-if” scenarios to analyze potential impact for a proposed modification
- **Prioritized Remediation** based on the most critical vulnerabilities in the context of the exploitation path
- **Path Explorer** allows you to see how an attacker traffic can traverse the network
- **Vulnerability Visibility** within RedSeal allows you to see IP and vulnerability correlation
- **Automated Vulnerability** data import on a scheduled basis to correspond with latest scans

Solution Components

What you need:

- Rapid7 Nexpose 5.x
- RedSeal 6.x

Overview of Integration Process

- Step 1: Nexpose performs a security assessment
- Step 2: A task is created to query Nexpose for latest vulnerabilities
- Step 3: RedSeal calls the Nexpose API for the latest XML report
- Step 4: Vulnerabilities get mapped to the network access context
About RedSeal Networks

RedSeal Network is the leading provider of network infrastructure security management solutions that continuously provide network visualization and identify critical attack risk and non-compliance in complex security infrastructure. It provides network, security, and risk management teams with a firm understanding of where security is working, where investment is needed, and where greatest cyber-attack risks lie. This understanding, or “security intelligence”, enables organizations to allocate resources where needed most, embed best practice into daily operations, and take prioritized action where needed. The world’s largest government and commercial organizations use RedSeal security intelligence to build world-class operations that systematically reduce attack risk over time.

About Rapid7

Rapid7’s security solutions deliver visibility and insight that help you make informed decisions, create credible action plans, and monitor progress. They simplify risk management by uniquely combining contextual threat analysis with fast, comprehensive data collection across your users, assets, services and networks, whether on premise, mobile or cloud-based. Rapid7’s simple and innovative solutions are used by more than 2,500 enterprises and government agencies in more than 65 countries, while the Company’s free products are downloaded more than one million times per year and enhanced by more than 200,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a “Top Place to Work” by the Boston Globe. Its products are top rated by Gartner® and SC Magazine. For more information about Rapid7, please visit http://www.rapid7.com.

Contact us today to learn more
1-866-772-7437
1-866-7-RAPID7