REDSEAL

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT


## INTRODUCTION

Vulnerability management is crucial to network security. Not only are known vulnerabilities propagating dramatically, but so is their severity and complexity. Organizations cannot afford to neglect vulnerability management and still expect to maintain system availability and protect sensitive data. As part of a defense-in-depth security strategy, the best approach is proactive: Identify vulnerabilities and weaknesses before security issues arise.

Most organizations utilize network vulnerability assessment scans that enable the security team to identify networked devices, applications, and vulnerabilities. This is accomplished by scanning the IP addresses of an organization's network segments to identify open network ports and the associated application and operating system. The scanner probes the open ports, determines the patch level and configuration of applications and operating systems and identifies vulnerabilities present. The end-product is a list of hosts and network devices reachable with the operating attributes, including running services, software and operating system version and vulnerabilities. While this identifies the network vulnerabilities present, the raw data is overwhelming. Key challenges remain:

- How to prioritize meaningful remediation efforts. The raw data generated by scanners creates a "phone book" listing of up to tens of thousands of vulnerabilities. Organizations can filter by host attribute such as OS version level, or by application type such as SQLNet, or by vulnerability attribute such as severity. Still, looking at a filtered list makes it hard to demonstrate how addressing those vulnerabilities are actually improving security.
- Limited remediation options. Scan results are host-centric. They don't correlate or understand the relationships between assets. So the only option for remediation is to install a software patch or make a host configuration change. Patching is expensive. It requires the host to be taken off-line to apply the patch.

Organizations are realizing that vulnerability assessment scanners provide only the view of the vulnerabilities accessible to them. Also, multiple scanners are often deployed throughout the network and network access policies are altered to grant the scanners wider access. This architecture makes it extremely difficult to understand how a given vulnerability may be exposed to a threat source or, if deeper within the network, may be exposed to other attackable hosts. However, there are products that (a) identify which network vulnerabilities pose a threat to the enterprise, (b) efficiently prioritize remediation efforts, and (c) present a choice of multiple remediation options.

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

**This paper:**

- Examines the current state of vulnerability management, how it has evolved and how new products are improving the security landscape.
- Introduces a powerful and cost-effective tool to identify and remediate the most important vulnerabilities in your network.
- Shows you why analyzing vulnerabilities in the context of your network is necessary to prioritize vulnerability remediation and determine all options beyond patching and configuration changes.
- Explains how to choose the optimal security decision-whether patching, changing configurations, deploying compensating controls, altering network access policies or even re-architecting the network.

## IDENTIFYING THE MOST IMPORTANT VULNERABILITIES TO REMEDIATE

To ensure that your remediation efforts do the most to improve security, it is best to start with the vulnerabilities posing the greatest threat. Suppose 1,000 hosts were scanned and an average of five vulnerabilities were found on each. You would have 5,000 vulnerabilities to review and evaluate to identify the best action you can take to reduce any potential business impact. And, you have to decide which to fix first, prioritizing vulnerabilities by the risk to your business-not to the device or host.

Many organizations take a host-centric approach to prioritizing vulnerabilities. Often the vulnerabilities are sorted by severity. Using the example of 5,000 vulnerabilities, suppose the scan found 1,000 high-, 1,500 medium-, and 2,500 low-severity vulnerabilities. Additional filtering or grouping can be done based on application, operating system, or even business unit. Once these vulnerabilities have been sorted, you review the list to determine which vulnerabilities to fix. Considerations may include:

- **Severity of the vulnerability:** Is the severity of the vulnerability so high that it needs to be patched immediately? Is it worth taking the server down or spending the time to implement the patch? Can the vulnerability be easily exploited? Could an attacker easily gain administrator-access to the server?
- **Regulatory implications:** Is the host under regulatory requirements with regard to security? Is there an explicit regulatory requirement to patch the vulnerability?
- **Business impact:** If exploited, would the vulnerability affect system availability or performance?

While this approach seems logical, it reveals little insight into what will actually improve security because it looks at the problem using limited data. It does not consider the enterprise as a whole, nor does it evaluate how the hosts are interconnected and what is reachable from untrusted networks. In other words, more questions need answers:

**Is the vulnerable host exposed to an untrusted network? Should the host be exposed to the untrusted network?**

**Is the vulnerable host reachable from a “weak” upstream host?**

**Should the host be protected by a firewall?**

Bottom-line: the enterprise network is the sum of its parts. And it requires a view beyond individual devices.

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

## PROTECTING HOSTS EXPOSED TO UNTRUSTED NETWORKS

Most important to your network's security are the hosts exposed to untrusted networks. To attackers, they are the doors to your network. The most important and often overlooked step of vulnerability management is to determine if the host should be exposed in the first place. Often due to configuration drift, network changes, bringing up hosts/services and shutting them down, hosts are inadvertently exposed to the untrusted network.

A second problem is that scanning the public IP address space of an enterprise only identifies the hosts directly exposed to the Internet which is just one of many untrusted networks today. Others to consider:

- **Extranet:** Most enterprises today have connections to a variety of business partners- outsourcing, supply chain and codevelopment to name a few. Since these connections provide a pathway into your network and are controlled by a third-party, it is essential to secure any exposed host.
- **Internal end-user networks:** In the last few years much focus has been placed on insider threats to sensitive data. Malicious employees, contractors and malware are legitimate threats. Indeed, any network where endusers actively operate is a possible source of attack.
- **Wireless networks:** Simply based on the lack of physical control inherent in wireless networks, it is important to consider the possibility of an attacker gaining access via these networks. PCI specifically calls out the need to segment valuable assets from wireless networks.
- **VPN networks:** Remote end-users often connect to enterprises using some form of VPN technology (IPSec, SSL, etc.). Usually the user is utilizing a third-party network such as a home Internet connection or hotel wireless network to initiate their VPN connection. A third-party network cannot be considered "trusted".

It would be extremely difficult and burdensome to the network to perform a vulnerability scan from every possible entry or untrusted network access point. An ideal vulnerability management solution can dynamically identify untrusted network segments and reveal hosts exposed to those networks. The host vulnerability data can be prioritized according to what is exposed to the untrusted networks. Exposed hosts are determined by analyzing the various network access policies controlling traffic between untrusted and trusted networks.

Here, computer automation is invaluable.

Once you identify the directly exposed hosts, you need to answer a series of questions to further prioritize remediation efforts. First, determine if there is a business or technical requirement for the host to be exposed incorrectly. Most often an incorrectly exposed host is the result of a misconfigured access policy on a router or firewall or because access was opened to troubleshoot an issue and the administrator forgot to go back and close access.

The final step is to analyze the network to determine the access the directly exposed hosts have to other hosts and vulnerabilities deeper in the network. This analysis helps you understand how much of a threat one exposed host is compared to another. For example, suppose you analyzed the access of two exposed hosts, A and B, to the untrusted network. Exposed host "A" has a vulnerability that enables an attacker to jump to another host deeper in the network. Host "A" also has a vulnerability that would enable an attacker to leapfrog to a regulated database deep in the network, which contains sensitive customer data. The other exposed host "B" has the same vulnerability, but its leapfrog target is an internal test server with no business impact. "A" may be part of a legacy network and is no longer used, but it is directly exposed to the untrusted network and has a leapfrog vulnerability that can reach a critical, regulated data repository. Clearly, host A presents a higher risk to the business than host B does. Now you know which host to remediate first.

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

## FIND THE MOST EFFECTIVE AND REALISTIC WAY TO REMEDIATE THE VULNERABILITY

Vulnerability assessment may identify numerous vulnerabilities but remediating some of them may conflict with other IT priorities. For example, a scan may identify a severe vulnerability in a primary database utilized by customers or vendors. Patching the vulnerability may necessitate taking the database offline for installation and testing, which may conflict with operational priorities driven by service level agreements with specific availability requirements.

The administrator managing the database may be reluctant to remediate the vulnerability, rationalizing that the database sits deep within the network, behind one or more firewalls, thus reducing the chances of the vulnerability being exploited.

Because the security team doesn't take the network into consideration when prioritizing vulnerabilities, the database administrator may be correct that there is a low chance of the vulnerability being exploited. But what if the security team could demonstrate the magnitude of the threat and how exploitable the vulnerability actually is? What if the team could prove that, despite the database being deep within the network, an upstream host with a pivotable vulnerability could be compromised by exposure to an untrusted network? Perhaps due to a misconfiguration on the network, the database got exposed to an untrusted network. Here, the security team is correct that the database is at risk but they may not understand that the exposure could be mitigated by patching the host exposed to the untrusted network (or by filtering traffic between the data base and the upstream host if the current network access is deemed unnecessary for business).

The above example reveals two major challenges faced by security teams when trying to remediate vulnerabilities: (1) understanding and communicating how much of a threat a vulnerability is to the organization and (2) recognizing all possible remediation options. Without an understanding of the network it is impossible to initiate action and identify the most appropriate remediation steps.

By analyzing vulnerabilities in the context of the network, security teams can be much more effective at communicating the level of risk that a vulnerability poses and make more informed decisions about appropriate remediation. Inadequate network understanding leaves security teams with two options for remediation: (1) install a software patch that addresses the vulnerability or (2) simply disable the vulnerable service on the host. These options are extremely host-centric, and the latter requires costly downtime. Compare that to the additional remediation options available with comprehensive network understanding:

- Network ACL Change: There are cases where vulnerable hosts are incorrectly exposed. In that case, remediation may be as simple as having the network team make a change to an ACL on the router allowing the traffic.
- Compensating Controls: The team can deploy a security solution to remediate the threat such as a firewall to block the traffic, an intrusion prevention system, an application-level firewall, or an inline patching system.
- Remediate an Upstream Host: When dealing with hosts not directly exposed to an untrusted network, upstream-host remediation may be a viable option.

Analyzing vulnerabilities in the context of the network enables security teams to communicate the risk posed to the enterprise and to identify the most appropriate remediation action to boost security.

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

## THE REDSEAL APPROACH

RedSeal lets you see your network as it actually is. It verifies that your network is designed to allow only authorized access, that your devices are configured to meet industry-standard best practices, and that your changes make your network more secure. And, it prioritizes fixes based on the value and accessibility of your asset as well as the severity of the vulnerability

### MODEL

Understanding the interconnectedness of an enterprise's assets is fundamental to vulnerability management. RedSeal examines your device configurations along with your cloud and virtualized networks and builds an accurate model of your "as built" network. It calculates all access paths from any point to any other point in the network and highlights problem access.

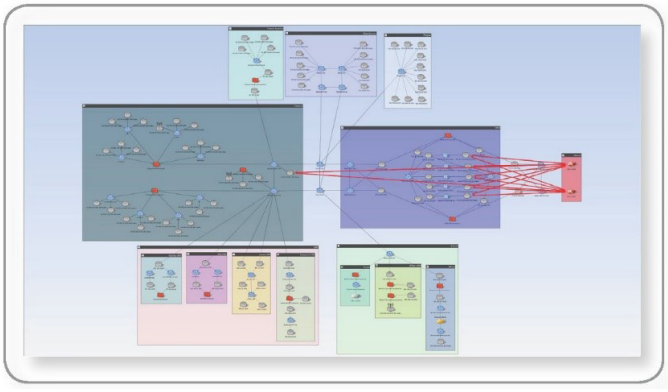
### TEST

RedSeal then collects host data from vulnerability assessment scanners and current threat lists from the National Vulnerability Database (NVD), including CVE IDs and CVSS scores. It combines this information with the detailed network model and identifies security risks based on network exposure.

### PRIORITIZE and REMEDIATE

From the host data collected above, RedSeal assigns an "asset value" based on the primary service available on that host (e.g. database, email, web server, etc.) It then calculates a risk score for each vulnerability and host based on asset value, vulnerability severity and, importantly, network exposure – either direct exposure or downstream risk. You get a prioritized list of security issues to remediate – and all the information you need to make the necessary changes.

- You can review all threats that originate from untrusted networks, including leapfrog exposure to points further into the network.
- You can identify and prioritize directly exposed hosts. The metric is based on the severity of the vulnerabilities present and the network access allowed from high risk hosts to other points in the network.



Graphical view of all access allowed to a network and the details including source, destination, port and protocol

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

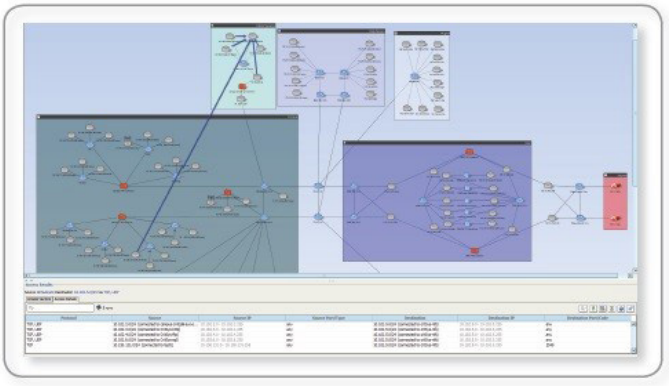
## DETERMINE ACTIONS THAT PROVIDE GREATEST SECURITY IMPROVEMENT

In addition to helping organizations prioritize their remediation efforts, RedSeal provides all the information needed to make needed changes. Security teams can consider the best remediation option –patching, preventing access or disabling the exposed service.

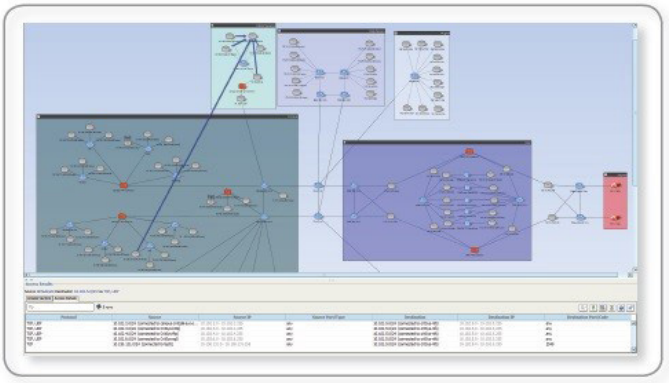
To help security teams identify the best actions to take, RedSeal enables users to review all traffic between any two points in the network. Users specify source and destination in the network and RedSeal returns the traffic allowed between the source and destination.

RedSeal enables security teams to review all threats to any host in the network, especially threats from untrusted networks. This enables security teams to consider a number of remediation options for a host, including changing the access policies on an upstream network device or identifying other hosts that, if remediated, would eliminate the exposure.

RedSeal enables organizations to overcome the challenges discussed in this whitepaper. While some of the approaches to overcoming these challenges could be performed manually, the complexity warrants the need for an automated software solution.



**Graphical view of all access allowed to a network and the details including source, destination, port and protocol.**



**Graphical view of all threat vectors to a subnet and the details of each threat including source, destination and vulnerability information.**

# ADDING NETWORK INTELLIGENCE TO VULNERABILITY MANAGEMENT

## CONCLUSION

Network vulnerability assessment scanners are excellent for identifying existing vulnerabilities, but the results often leave organizations with more data than they can effectively handle. By themselves, scan results are difficult to prioritize since scanners are unable to identify which hosts are exposed to untrusted networks. What's more, the host-centric nature of scan results makes it difficult to understand or communicate the true urgency for remediation or provide any more remediation options besides installing a software patch or making a configuration change to the host.

The optimal way to overcome these challenges is to analyze the results of a vulnerability scan in the context of the network. In this context you can analyze the relationships between hosts and untrusted networks by understanding the network architecture and access policies that define the relationships. By including the network context in the analysis of vulnerability data, security teams can easily identify the vulnerabilities that present the greatest threat to the enterprise, communicate the urgency to remediate these threats, and identify the remediation steps that will provide the greatest impact to business security. RedSeal's platform enables organizations to overcome these challenges and protect their most valuable assets.



REDSEAL

1600 Technology Drive, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net

AUGUST 2019