AN INTRODUCTION TO VULNERABILITY REPORTS

After conducting a vulnerability assessment, conveying the results via a report is critical for addressing any uncovered problems. Without a clear and well-structured report, program and organization owners may not understand the scale of the threat they face or what steps they should take to mitigate it.

The vulnerability report starts by clearly summarizing the assessment and the key findings regarding assets, security flaws, and overall risk. It then goes into more detail about the most relevant vulnerabilities for the program owners and how they could impact various aspects of the organization. The main purpose of both the assessment and the subsequent report is to fix the vulnerabilities, so the report should pay special attention to providing guidance and suggesting measures to remedy current problems while preventing future ones.

What is the Vulnerability Assessment?

The assessment on which the report is based is a common cybersecurity measure for identifying, analyzing, and then ranking vulnerabilities in computer systems. Performing vulnerability assessments is useful not only in IT but also in other sensitive systems, such as utilities or energy. IT teams often use aggressive tactics such as ethical hackers and mock attacks to find weak spots and to further understand prevailing threats to their system.

The main steps of the assessment are to evaluate assets of the organization, define their risk level, review current systems to establish a baseline definition, and conduct a vulnerability scan. There are

several types of scans, and selecting the right one depends on the desired results for the organization at hand. After the scan is complete, the next step in the vulnerability assessment process is to write the report.

Key Components of a Vulnerability Report

Executive Summary

The first part of the report focuses on providing an overview of the big-picture results from the assessment. It uses clear and concise language to state the overall risk level of the organization, the kinds of issues that it should address, and how to prioritize them.

It should aim to lay out these main points without overwhelming the readers with too many complex details—leaving such analysis to the more in-depth sections on individual vulnerability findings. For example, the risk level of the organization should communicate the severity of the discovered vulnerabilities through a clear label of low, medium, high, or critical.

The executive summary should also include subsections such as a testing narrative, remediation summary, assessment scope, assessment findings, and primary objectives summary. It should also state important information including the date and times of scans and the names of the scanned servers.

Assessment Overview

This section introduces and summarizes the accomplishments of the vulnerability assessment scans. It should include subsections on the approach and verification of analysis, tools used, and the methodology of the assessment. When reading the assessment overview, the program owner should have a clear idea of the validation, investigation, and deliverables provided by the assessment.

The analysis verification assures that the methods are reliable while also simplifying the results into terms that the program owner can understand. Demonstrating the various open-source, commercial, and custom tools implemented shows the capabilities of the scan and gives the program owner concrete information that they can investigate further if necessary.

Individual Vulnerability Details

Also known as the Assessment Findings or Mitigation Recommendations, this section provides the meat of the report by going into greater detail about each vulnerability found during the assessment.

Each vulnerability should receive a section with the following subsections:

- Vulnerability name
- Date of discovery
- Vulnerability score
- Detailed description of the vulnerability
- Proof of concept (PoC) of the vulnerability/steps to replicate
- Impacts on systems and organization
- Guidance for fixing the vulnerability

This is the most important section in that it highlights the issues, their causes, how the assessment found them, their potential impact, and how to fix them. Order the individual vulnerabilities by severity level with higher risk problems first, and be very explicit about the realities of the situation for each one.

Tips for an Even Stronger Report

With the above sections, any vulnerability report should be robust and useful for a resourceful and dedicated program owner. However, some limitations may appear in the form of a lack of understanding on the part of companies or a hesitancy to implement changes.

To avoid such limitations, there are a few extra steps you can take to make sure it has the greatest impact possible for any organization. Each step is fairly simple on its own, but implementing them all together can hugely improve the effectiveness of the report.

Maintain Direct Communication

During the process of conducting the vulnerability assessment and creating the report, maintain a clear line of communication with the program owners. When first starting the project, be sure to thoroughly read the project scope and rules of engagement, and don't be too shy to ask questions when necessary. This will prevent any misunderstandings and unnecessary backtracking.

Prioritize Vulnerabilities

If the assessment identifies several vulnerabilities, the program owners might not be sure which ones to tackle first. They might even feel too overwhelmed to address any of them at all. Create a clear course of action by listing them in order of priority and clearly stating which ones are highest risk. Particularly focus on high and medium level vulnerabilities with honest explanations of why they deserve prioritized attention.

Use Straightforward Language

Remember that many of the people reading the vulnerability report may not be familiar with technical topics. Write in a conversational and highly descriptive tone for all audiences. For titles, stay away from very short and vague statements. Use the title to efficiently convey the type of vulnerabilities found in the assessment, where they occurred, and the domain or endpoint.

Provide Additional Resources

Within descriptions, include links and references to credible sources that can aid others in understanding, identifying, and solving the issues. For example, Common Vulnerabilities and Exposures (CVE) references or links to the OWASP Foundation can steer program users to even more useful information. But try to avoid less credible or very generic sources such as Wikipedia. Adding extra resources might not be necessary for some readers of the report, but they could make a significant difference for those struggling to keep up.

Make Concrete Suggestions

When proposing a remediation for vulnerabilities, the report should avoid giving vague suggestions for general directions to take. Instead, provide explicit recommendations and directions on actions that can address the problem. You can (and probably should) even go as far as writing a step-by-step plan. Go into great detail and provide all the attachments of images, screenshots, videos, and other aids, allowing you to explain complicated instructions. It might feel like overkill to you, but it could help someone with less technical experience.

Build a Relationship

The primary goal in creating a vulnerability report is to help the program owners. Build a real relationship with them and show genuine concern for their company by putting in your best effort to accomplish that goal. Work to understand how the company functions and how a potential vulnerability truly impacts it. Then communicate this impact to the organization and the importance of implementing changes. Articulate everything clearly and with authority, but be patient if they don't understand and always be willing to help them fully grasp the material.

The vulnerability report can itself be a means of building a strong relationship of trust and ongoing commitment with an organization. If the report is poor, then the response plan will be weak and the vulnerabilities will remain. But if it is successful in both identifying and addressing problems, then the company will be healthier for it, remember your valuable service in the future.