Vulnerability Assessment Report Templates

Reading

40m

Status | Incomplete

Introduction

You already know about how vulnerabilities are recorded and documented, so Cyber Security professionals can learn about details and recommended remediations. You have considered how vulnerability assessments fit into Risk Management processes, and the wider organizational implications and industry best practices for these processes. You've even had some hands-on practice conducting a vulnerability assessment.

> **A Small Part of an Important Picture**
>
> This perspective can help you see how crucial a single vulnerability assessment and report is to the security of your organization's assets.

The final stage is to look into the vulnerability assessment report itself. This section explores:

- Sections of the report
- Details to include in each section
- Tips to approach the writing of the report

Understanding the Vulnerability Assessment Report

A vulnerability assessment report is a document used to collect the results from a vulnerability assessment, summarize what those results actually mean to the business, and recommend to the business decision makers what to do next, in what order, and why.

As you are writing a report, there are going to be some distinct sections that you want to make sure you include.

Executive Summary

The report will start with an executive summary, which summarizes the content that will be found in the report.

The executive summary should include:

- The date(s), purpose, and scope of tests that were run.
- The status of the assessment.

- A brief summary of the findings.
- A short overview of what is recommended.

> ℹ **Tip:** Although the executive summary is the first section in the report, it should actually be the last portion of the report that you write. After all, the best way to know what you need to summarize is to have already written the contents.

Scan Results

The scan results section of the report talks about how you are categorizing the results that were found from the scan. The purpose of this section is to give the reader the information they need to understand what you are telling them in the rest of the report.

The scan results section will include:

- Definitions of the various severity levels used to describe vulnerabilities that were found.
- How the recommendations are organized.
- An overview of the types of reports and results that will be found in the rest of the report.

Methodology

The methodology section describes exactly what your team did. The purpose of this section is to give the reader perspective on what was actually done, methods that were used, and approaches that were taken. This can give the reader useful context on how you gathered the information.

A report methodology section should include:

- What tools and tests were used to complete the vulnerability scanning.
- The specific purpose of each tool, test, and scan that was completed.
- The environments in which each test was run.

Findings

Now that you have laid the groundwork so that your reader understands what you have done and how to interpret the results you will share with them, you need to tell them what happened.

Your findings section will describe:

- What was scanned.
- What was not scanned.
- Explanations for any scans that were supposed to be included, but were not completed.

Risk Assessment

The Risk Assessment section of the report catalogues and categorizes the vulnerabilities you have found, as well as their relevant severity. You will start with an index of all vulnerabilities that have been identified, and categorize each vulnerability according to its severity level: Critical, High, Medium, or Low. This will be followed by an extended section listing each vulnerability and giving details about it.

Details given for each vulnerability should include:

- Name of the vulnerability.
- Date of its discovery.
- Score based on CVE and CVSS.
- Detailed description of the vulnerability.
- Detailed description of the affected systems.
- Details of the process to correct the vulnerability.

Presentation Matters

Your reader is a very busy executive. They want to understand the information quickly.

When you present this information, choose a consistent organization and format that makes it easier for people to interpret and understand.

You may find that a table format makes the most sense for parts of this section.

Recommendations

The final section of your report is where you bring it all together, and help your reader determine the impact of your assessment and the next steps needed.

The recommendation section should include a summary of the most critical things that your team feels require attention:

- The order they should be addressed in.
- What steps should be taken in each case.
- The effect on the network's security posture.
- Any recommended security policy or configuration adjustments.

Consider your Audience

When pressed for time, an executive might flip directly to the recommendations section.

What critical takeaways do you want to make absolutely sure they read?

Compiling and Organizing

At first glance, the amount of information to include in the report may seem overwhelming. While not all of the details will be included by the scanning tool as part of the scan results, you will have spent the time investigating the vulnerabilities, and will likely know where to find all the information you need. If you have taken the right steps in your Vulnerability Assessment Process, the report is really just collecting and organizing the information you already have.

Additional Tips

Do not assume that your readers are technically trained: include explanations of any technical information or processes that non-technically trained readers will be able to understand.

Get information across as quickly and as simply as possible: use direct, clear, and short sentences. Keep in mind that though it will take you a while to write the report, your readers won't have an equal amount of time to dedicate to reading it.

Be clear about the potential effects of the vulnerabilities that you find: the decision makers need to understand the cost of fixing the problem, but also the cost of *not* fixing it. That is your area of expertise, so provide clear and detailed information. This is where your extra research into the vulnerabilities, their effects, and mitigations is going to pay off.

Provide clear and actionable recommendations: avoid hesitant language or unclear suggestions. Make sure you are giving measurable actions that the organization can implement effectively. Include clear reasons for your recommendations.

Further Reading

The resources below provide some additional guidance on writing vulnerability assessment reports.

> Read through each set of guidelines and add to your notes from this page to compile a full list of report-writing tips for yourself.
>
> Store these tips and links in your PKM for future reference.

RSI Security: Tips for Creating a Strong Vulnerability Assessment Report

Security for Everyone: 5 Steps of Vulnerability Assessment Report and How to Write an Assessment Report

EC-Council Cybersecurity Exchange: How to Write a Vulnerability Assessment Report

Conclusion

Writing the report is one of the most crucial parts of your Vulnerability Assessment Process. It is vital to ensure the report is detailed, thorough, gives potential costs and effects of the vulnerabilities, recommends actions that can be taken to remediate the negative effects and help protect the organization and its assets going forward, and is understandable by all those that will be reading it.

In the next section, you will learn about various formats to organize your information by comparing and contrasting some existing templates.

✓ Mark Completed

← Previous
Vulnerability Management Process Knowledge Check

Next
Report Templates Review →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D4

Thu Jul 25

› Lectures (1)

⌄ Work (8)

6 hrs

- </> Case Study: Vulnerability Assessment Scan
- ⚡ Discussion: Vulnerability Assessment Scan Case Study
- ? Vulnerability Assessments Knowledge Check
- Vulnerabilities and the Risk Management Process
- Vulnerability Management Best Practices

- ? Vulnerability Management Process Knowledge Check
- Vulnerability Assessment Report Templates
- Report Templates Review

W05D4 Schedule »

Powered by Lighthouse Labs.