Case Study: Vulnerability Assessment Report

Assignment

2h - 2h15m

Status | Incomplete

Overview of Case Study

> This case study draws on the results from your scan completed for vulnerability assessment scan assignment. Access and review your files from that assignment to get started.

In this project, you will analyze the results, complete additional research, and write a vulnerability assessment report that suits the scenario.

Case Study Notes

In this case study, you will finish analyzing the results from the vulnerability assessment scan assignment, completed before this activity, to decide what the most severe of the discovered vulnerabilities are. Then you will complete additional research on the vulnerabilities you decided are of the most concern and that should be considered for mitigation to ensure you have as much complete and up-to-date information on each of them as possible.

You will finish this case study by writing a vulnerability assessment report on your scan results that will conclude with your recommendation of a prioritized list of threats to be mitigated including what mitigations you feel should be implemented and why.

Scenario

Cat's Company Vulnerabilities

Cat needs your help providing critical information to the executive team to help them make decisions and preparations that uphold the security of the organization.

Now that you have completed the vulnerability assessment scan Cat has asked you to do, she has asked you to collect all the information to prioritize the vulnerabilities that were found from highest risk to lowest, and determine what information would be necessary for the executive team to make decisions and preparations to have them mitigated.

Cat wants to make sure the executive team has all the information they need, but she knows that they don't have a lot of time. She has asked you to write a vulnerability assessment report on your findings that explains the issues you found, what is affected, what it might mean to the business, and what suggestions you recommend to fix the issues.

Cat will also need to make a presentation to the executive team about your report and recommendations, so she has asked you to create a five to seven minute briefing summarizing your report and recommendations for her to present.

Tasks

Step 1: Review Results and Perform Additional Research

Go back to the results from your vulnerability assessment scan in the Unit 2 case study, and decide what the most severe of the discovered vulnerabilities are.

Conduct additional research on each vulnerability you decided was of the most concern and that should be considered for mitigation. You may use tools and techniques that you have learned throughout this course or other tools at your disposal. Your goal is to ensure you have the most complete and up-to-date information on each vulnerability.

> Keep track of your research tools and methods, and the information that you collect.
>
> The more organized and detailed your notes are, the easier it will be to create the report.

Step 2: Write your Vulnerability Assessment Report

Use what you have learned about vulnerability assessment reports and best practices to aid you with writing a detailed report with recommendations for Cat's company.

Your report should contain the following components:

- **Executive summary:** a short summarization of the assessment that was carried out and why, what results were found, and an overview of the end recommendations you are proposing.
- **Scan results:** detailed explanation of the results gotten from the scan, how the results have been categorized, and how the vulnerabilities are ordered.
- **Methodology:** tools and tests used, purposes for each scan, tool, and test, and what environment each tool was used in.
- **Findings:** what systems were scanned successfully or not and why.
- **Risk assessment**: index of all vulnerabilities found, categorized Critical, High, Medium, or Low severity, explanations of risk categories, list of all vulnerabilities with details on vulnerable target/service/software etc., description, solution, and how many affected.
- **Recommendations:** full list of actions that should be taken in prioritized order with explanations on why you recommend the order you do, recommendations on security policies, and configurations.

Report Preparation Tips

> The final version of your report will be the document that you will submit for evaluation.
>
> *Do not rush this step of the process.*

Be sure you are thoroughly researching your discovered vulnerabilities before deciding what order you will recommend they be addressed in.

You should be considering:

- What the vulnerability will expose or allow a bad actor to get access to or do

- How costly an exploitation of the vulnerability might be to the organization, and how much of the organization
- How likely the vulnerability is to be exploited
- IoCs that might indicate the vulnerability is being exploited

Refer to the resources and content you have seen in this unit to guide you on what kinds of details you should be including in sections of the report, and to ensure you are including all the information required in an organized, well structured, and supported fashion.

> As the final project in this unit, you will need to submit a link to a github file or Google doc that contains your report.
>
> Keep this in mind as you select the file type of your report.

Step 3: Prepare your Briefing

Your briefing should be approximately five to seven minutes (usually about two to three pages typed) in length and can be in any format you choose. You should include a summary of your report and key recommendations that Cat can share with the executive team.

Your briefing should include a slidedeck to aid Cat with covering all your important points and staying organized.

> **You may want to make changes to your report following the peer review task.**
>
> There is a chance that feedback from your colleagues, or even the experience of delivering your briefing may highlight some changes you want to make to your report.
>
> *Keep your report in an editable format, so you can make edits before submitting.*

Conclusion

Completing this case study allows you to assess your understanding and practice your skills to:

- Complete thorough research of discovered vulnerabilities and document all contributing factors in order to give decision makers as much information as possible for deciding what to mitigate, and in what order.
- Prepare a written report for business executive consumption and understanding.

In the next section, you will present your briefing to your colleagues, and get some feedback that you may want to apply to your report before submitting.

W05D5

Fri Jul 26

Lectures (1)

Work (9)

8 hrs

- Case Study: Vulnerability Assessment Report
- Peer Review: Assessment Report Briefing
- Project: Cat's Company Vulnerabilities
- Course Reflection
- Overview - Incident Response
- Introduction to Incident Response
- Pre-Incident Planning
- Response Preparation for Action
- Planning and Building CSIRT

Other (1)

W05D5 Schedule »