The protective measures taken by net users to protect data

Science, Computer Science

Purpose

The vulnerability assessment is used in the cyber security field of the computer science. The purpose of this report template is to effectively convey information conducted from a penetration test on a company’s network.

Background

The vulnerability assessment report is comprised of any exploit or possible weaknesses found in a company’s network while conducting a penetration test as well as a level of risk and how it can be addressed [2]. A penetration test is usually performed by an internal team member to exploit vulnerabilities that they find within a network. Penetration test is like a software attack targeted towards a computer system where it can look for a security weakness or a particular goal [1]. The test will try different ways to attain the desired goal. Once a security weakness or a particular goal is acquired a vulnerability assessment report is then filled out. The employee who conducted the test has to give a detailed expiation of the methods and tests they used to find the desired exploit [2]. Along with a level of risk and a description of the impact that exploit could have to the company [2]. When a vulnerability assessment is done it is usually giving to a IT Director or a technical leader who will then assess the problem and try to fix it based off of the communication within the report [1].

Daniel DeCloss is Director of IT Security at Scentsy incorporated in Meridian, Idaho. After Daniel graduated from Northwest Nazarene University with a bachelor in computer science, he went on to further his education and joined the Naval Postgraduate School [1]. There he received a masters in computer science with a security emphasis. Currently, Daniel has over ten years of experience in computer security, penetration testing, computer forensics, and programming. Nowadays, Daniel’s duties as Director of IT Security is to make sure assets are secure, networks are secure, users are trained, and mitigating cyber attacks [1]. Daniel’s goal is to set the foundation and grow out a program that will set Scentsy’s people up for success [1].

Analysis

Audience

Vulnerability assessment reports are intended for other IT Directors or technical leaders like the Chief Information Officer (CIO) of a company [1]. The vulnerability assessment must have enough technical detail that people responsible for fixing the weakness can reproduce how the weakness was found to have a better understanding of what needs to be done to fix the problem. Therefore, the technical detail must be written in a way that effectively communicates without confusing the audience. Then audience can replicate what the writer did to get a better understanding of how to fix the problem at hand without any misunderstandings.

Formatting

The vulnerability assessment report is formatted in a way to communicate a lot of technical detail and information in a clear effective manor. The intended audience will be able to find needed information fast and easy because of the formatting style of the different headings and sections. The numbered headers separate the document into different segments which organizes the information efficiently. Under each header are names of numbered sections that give the audience an idea of what they are about to read [2]. For example, under the header “ 1. Executive Summary” there is a section called “ 1. 3 Summary of Findings” [2]. Some of the sections also include the use of bullet points and numbered list making information even easier to find while skimming through [2]. Overall, the format of the vulnerability assessment report was done in a technical style but with professional manner that made the document look aesthetically pleasing for the audience while still conveying important information clearly.

Visuals

The visuals included in the vulnerability assessment report are used to explain information shown in more of a data format. For example, figure 1 explains the different threat levels a possible exploit could have in different sections separated by colors and a word. The use of color coordination makes communicating information more effective. In figure 2, because the box is yellow the audience will know that data provided in figure 2 will relate to the yellow definition provided in figure 1. From the definition provided in figure 1 the audience will be able to understand the possible exploit or weakness in the network more. From there they can take the steps needed to fix the problem [2].

Conclusion

In any computer science field, technical communication will be needed to convey any technical details to people with different backgrounds. The purpose of the vulnerability assessment report is to communicate enough technical detail that the audience will be able to reproduce what the writer did in order to get a good understanding of how to fix the vulnerability.

Through my interview with Daniel DeCloss, I discovered that taking the initiative to learn certain programs on my own will set me apart from others in my career [1]. Not only doing stuff in class but learning outside of class to will help my chances of attainment an internship. Having an internship experience in a computer science field will be incredibly valuable and will strengthen my career in cyber security.

Recommendations

In a computer science field, knowing who the audience is and accommodating to their background is important. The audience for the vulnerability assessment report might know a lot of the technical details provide in the report. However, an audience for other reports, emails, memos, and letters might not know a lot of technical detail and should be taken into consideration [1]. The writing has to make sense to someone who might not have the same job you.

In order to set oneself apart from others in the cyber security field is to learn how to write and read code. In the interview, Daniel recommended learning programs like as C++, Python, and Java script [1]. These skills will provide a better understanding of computer programs that one might be trying protecting or trying to hack into. Trying to protect data or hack without the skills of understanding computer programs will be more difficult. Learning these skills will also open a lot more opportunities in the field. Internships will also look for characteristics like these when deciding to hire [1].