MEMORANDUM

TO: Dr.Flammia
FROM: Emmanuel Tarantino
DATE: March 4, 2020
SUBJECT: Design Decisions

Introduction

For this assignment, I have decided to run a penetration test on a friend's business network. As a student in the Information Technology field, with hopes of focusing my career in cyber-security, this was an excellent opportunity to experience some of what the future may entail.

Purpose

The purpose of a penetration test is to test a network in such a way that certain vulnerabilities may be discovered, exposed, and ultimately exploited. The majority of cases where a network is exploited are the results of malicious attackers who are often seeking to exploit the target financially, or sell the exploit to some other entity with malicious intent. As a result, it is recommended that a business have their network tested by professional cyber-security individuals who then produce a report to inform their client of any vulnerability that may have been found in the network, and how to remediate them. The purpose of this assignment was to create such report and present it in a simplified and digestible format that the client may understand, as well as an IT professional.

Design Decisions

A penetration test report is a technical document, and with that in mind, I took inspiration from sources and individuals whom I admire professionally. With technical documents such as a penetration test report, I believe it's important to keep the audience in mind. For instance, a report such as this would be read by someone with no technical background, as well as a senior team member of an information technology team. With that being said, I strongly believe that it is in my best interest, as the writer and representative of my company, to strike a balance with the flow of information in such a way that it is easy to follow for that individual with little technical background and for that senior IT member. One of the ways I tried to achieve this is by providing images, such as the network topology, and color-coded charts, such as the severity ratings chart.

Arrangement and Emphasis

The arrangement of the report was chosen to present the information in a chronological and cause-and-effect manner. First and foremost, the first few pages of the report address some of the legal matters associated with a penetration test report. The nature of a test such as this is very intrusive, and as a result, confidentiality statements and disclaimers seem to be a requirement in documents that deal with such matters. Following the confidentiality statement and disclaimer, I thought it would be important to have a contact information table. As projects become bigger, and more people are involved, this table becomes an important part of the report that provides at a quick glance those individuals and their responsibilities.

Then, we dive into the 'meat' of the report, where the design approach was, as mentioned earlier, a chronological and cause-and-effect method for leading the reader along the process.

The assessment summary provides a quick overview of the methods that I employed, and a visual of what the approach is. There is a description of the steps accompanied by a visual for that person without a deep background in technology to get a better grasp of the method. Also, there is a link to the official national Institute of Standards and Technologies website where a technical document can be found, and this is intended for someone with a background in technology.

Then, the assessment components detail the techniques that would be used as part of the testing method. In this case, I conducted an external penetration testing, which is explained in the report.

Next, I included an industry-standard scoring system used for vulnerabilities. The 'Common Vulnerability Scoring System' (CVSS) is used in the cyber-security industry to score a vulnerability using a score from 1-10. I chose to display the information in a chart and color-code the five types of severities in order to make it easier to understand.

When it comes to penetration testing, a scope refers to what I'm allowed to test. In this case, I was given one IP address, which I included in the report. With a larger client, this list would be much larger, which is why I chose to display it using a table. It's also important to name anything that is not part of the testing in order to be clear of what is and isn't in the scope.

In the executive summary is where I start providing the results of the report. I decided to begin with a visual that shows the topology of the client's network. This helps visualize what devices are connected to what and how. Then, I used the cause-and-effect method I mentioned previously. I ran a command to scan the target's open ports and presented my results by providing screenshots. I also provided a chart explaining what each port does. Finally, I detailed the security strengths and weaknesses I found.

Lastly, I conclude with a remediation suggestion. I chose to use a "who," "vector," and "action" method of delivering my findings. I believe this is easy to follow for both types of individuals I described before, that one with no technical background as well as the IT professional.

Clarity and Conciseness

Clarity and conciseness are achieves in this report by using consistent font, proper spacing and separation of topics, as well as providing a table of contents in the opening pages of the report. Any visuals used in the report and accompanied by explanations, charts are well identified, and the color-coding is intuitive (such as using the color red for “critical” items).

Tone and Ethos

The report is a deliverable that is the product of my work. I promote the idea that my work is concise and thorough, and as a result, the final report should reflect that. This is why I’ve decided to keep the report very well organized and cleanly designed, avoiding as much clutter as possible. Also, I want to set the expectation that I can be approached by any member of the client company, whether it’s a high level executive with little background knowledge of cyber-security, all the way to the senior security engineer. As mentioned earlier, I try to accomplish this by making the report understandable by individuals with different levels of technical knowledge.

Project Stages

I would divide the stages of the project into an early, middle, and final stage. The final stage being producing the penetration testing report, which I’ve discussed its components to some length already. In essence, the final stage represents the marriage between the early and middle stages, which I would like to explain.

In the early stage, this is often considered the “reconnaissance” stage, or information gathering. In this stage of the project I am basically poking around the network minimally, gathering information as to how the network processes my requests. From my point of view, it is simply observing and taking note of certain outputs. At this stage, I have only drafted the legal sections of the report, which are standard and would likely change slightly from client to client. Also, at this point I would have discussed the components and scope of the project with the client.

The middle stage is perhaps where most of the work is done, and this is where the project starts taking its shape. At this point I have an idea of what the network looks like, and have added the visual of the topography to the report. I begin using tools and identifying vulnerabilities which get added to the report. In this case, the screenshot provided in the port scanning section gets added to the report in rough form and without a table detailing each port.

Finally, once the testing has been completed, I start parsing the data and notes I have taken, and make it presentable in the form of tables and visuals.

Client's Reaction

Upon reviewing the report with the client, the reaction was one of surprise. The client didn't expect that a penetration test could be as intricate as this, because his expectations were different. As someone who's not at all familiar with cyber-security, he expressed that the report would probably be a number of passwords I tried, or something along those lines. He did not expect to find a detailed list of open ports, and in fact, didn't know what ports were. He also didn't know that one could often try to brute-force their way into a system by trying different passwords, one by one, for as long as one desires. It was a welcomed reaction where I could explain some technical matters in such a way that he could understand, and most importantly, provide feedback and suggestions which he accepted.

My Reaction

I was excited to produce a penetration testing report of my own for the first time. I now appreciate even more the work and time that goes into producing such reports. The network I tested was small and the scope was narrow compared to what is done in the industry. With this newly acquired perspective, I have more respect for professionals in the field and the work they do, and can't wait to be among one of them.