ISEC 400 Homework 10 Name: Megan Leonard

Answer the following questions based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. **[5 points]** Demonstrate a Google search that finds secrets embedded in publically available source code on GitHub. Paste the search URL and a screenshot of some found secrets.

site:github.com inurl:login

A screenshot of a computer

Description automatically generated

1. **[7 points]** Read the paper “‘Security Through Obscurity’ Ain’t What They Think It Is” by Jay Beale at [http://web.archive.org/web/20070202151534/http://www.bastille-linux.org/jay/obscurity-revisited.html](http://web.archive.org/web/20070202151534/http:/www.bastille-linux.org/jay/obscurity-revisited.html). Summarize the author’s main points. Do you agree or disagree? Why?

The first point the author talks about is how security through obscurity does not really work well, which I agree with as by hiding it you are hoping that no one knows it is there and that they do not think of looking for it which is not always the case. There is also not an extra layer of security like passwords in play when using obscurity. Security through obscurity does not work well if it is the only security measure the other point the author makes it that it is not always bad which I can agree with. As long as we have multiple security measures in place then security through obscurity would be good as it just adds another layer of protection.

1. **[8 points]** Now read “Port Knocking: Beyond the Basics,” by Dawn Isabel at <https://www.sans.org/reading-room/whitepapers/sysadmin/port-knocking-basics-1634>. In light of Beale’s arguments from problem 2 above, is port knocking a new layer of defense for applications or is it “security by obscurity,” as some have said? Why?

Port knocking can be seen as a security key to security by obscurity. To gain access you need to give a specific knock pattern which helps protect against hackers just scanning the system. Now when I say it is a security key I mean is that to be able to gain access you need to provide the correct sequence of the knocks. If you do not then you will not be told to try again, you could pass over without knowing that there was something behind the port knocks. We can look at it in a similar way as how in some media you see the character talking to another person and using a code to gain access to information. If you do not know the code and that the person is holding the information then they might just look like another random person you pass by. So while it is not a new layer of defense it is also not just security by obscurity. It is an extra layer to the security by obscurity.

1. **[5 points]** Describe the problems and solutions associated with directory traversal vulnerabilities.

Directory traversal vulnerabilities can lead to attackers reading files that they should not be able to access. This can cause problems with sensitive files being read and information being taken or even altered. Solutions against this would be to work on blocking user input to file systems or even adding validation and white or blacklists.

1. **[5 points]** In approximately 300 to 400 of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered this week in class. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Ask at least one question that your instructor can answer in the returned assignment or class discussion.

This week we looked at more security this time surrounding files. There are many different ways to secure files and just as many different attacks. The first topic of file security is security and obscurity which allows us to add levels of security to files and still be obscure enough that you may not know what they are from the outside. We went through different attacks like file inclusion and directory traversal. Files are something that we use every day and can store some of our most important information. Security by obscurity was a topic that was interesting to me but I believe I like the security and obscurity more as it adds that extra layer that felt like security by obscurity was missing. My question this week is which one do you like more security by obscurity or security and obscurity?