530 PROJECT PROPOSAL

Heartbleed Web Page

Kaya Zdan

Fall 2023

PROJECT DESCRIPTION

This will be a reteaching project, with aspects of visualization, since the purpose of the project is to teach users about the Heartbleed attack, but will include significant amounts of visualization to go along with the explanations. The project will be a webpage that describes what is Heartbleed, the history of Heartbleed, how it works, and how to protect against it. This webpage will include gifs, and graphics to help readers visualize what is going on (such as a gif showing the heartbeat system). There will be videos showing execution of Heartbleed on a lab environment, to further provide more technical and realistic examples of Heartbleed in action. The web page will also include a quiz at the end of the page to help users demonstrate and test their understanding of Heartbleed and it's underlying systems. The quiz will have multiple sections that focus on the heartbeat component, Heartbleed itself, and how to protect yourself. These sections will make up the overall score, and the user will be able to see their score on each individual portion.

This web page will be created using HTML, CSS, JavaScript, and the gifs and visuals will be made in PowerPoint.

TARGET AUDIENCE

The target audience is people who have very rudimentary networking skills and are interested in seeing a more in depth analysis of a cyberattack. The target audience may include high school and college students with an interest in the cybersecurity field, or people already in a technology or technology adjacent field who want to learn more about Heartbleed and how it works.

AUDIENCE SKILL LEVEL

Varying levels of computer proficiency, but has skills with being able to operate a computer navigate the Internet, and run applications, as well as has access to a computer and Internet.

LEARNING OBJECTIVES

After a participant views or interacts with the project, they should be able to …

Objective 1 – Demonstrate the ability to explain how the heartbeat portion of the TLS/SSL protocol works by passing the heartbeat portion of the quiz with a score of 90%.

Objective 2 – Demonstrate the ability to explain how Heartbleed was able to take advantage of how the heartbeat component works by passing the Heartbleed portion of the quiz with a score of 90%.

Objective 3 – Demonstrate the ability to explain how to protect against the Heartbleed attack, protect their own systems against Heartbleed, and score 90% in the protection portion of the quiz.

Relevance of Topic

This topic is relevant because heartbleed is a serious networking exploit that stems from a vulnerability in the TLS/SSL protocol, which can be argued deals with both the Transport and Application layers of the TCP/IP network model. The topic also requires knowledge of the TLS/SSL heartbeat implementation, which is a good introduction to some intricacies regarding networking protocols. This topic is additionally relevant to due to the great effects this vulnerability had on the security world, and is a great introductory lesson to buffer overflows.

Research and Supporting Materials

Both sites, OWASP and CSOOnline in reference [4] and [1] are great writeups about the details about the Heartbleed bug. These sites will be used a lot as a good reference point for understandable writing regarding the Heartbleed bug.

I have created web pages using HTML/CSS and JavaScript before, and the GeeksforGeeks in reference [2] will be used for help creating the quiz in the web page, however other references may also be used in addition. One limitation is a domain, I do not own a domain, so this page will not be hosted publicly, and instead the source code will be provided for submission. I looked into using GitHub pages as a domain, but I already have plans for my provided GitHub page domain, and they only give you one.

I have found that HackTheBox Valentine has a Heartbleed bug in it, so if I cannot create a lab environment myself, I will use the created environment from HackTheBox instead. Otherwise I will create my own lab environment using VirtualBox, Kali, and doing my own research into creating a script for Heartbleed, and downloading the appropriate SSL version.

The gif animations and visuals will be created using PowerPoint, since I have found that you can do animations rather easily with it. PowerPoint also comes with a lot of good stock icons that I could use for my animations instead of having to create my own.

(In order from the References section)

[4] J. Fruhlinger, “The Heartbleed bug: How a flaw in OpenSSL caused a security crisis,” *CSO Online*, Sep. 06, 2022. https://www.csoonline.com/article/562859/the-heartbleed-bug-how-a-flaw-in-openssl-caused-a-security-crisis.html

[1] “Heartbleed Bug | OWASP,” *owasp.org*. https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug

[2] “How to create a Simple JavaScript Quiz ?,” *GeeksforGeeks*, Aug. 13, 2021. https://www.geeksforgeeks.org/how-to-create-a-simple-javascript-quiz/

Required resources

Audience members will not need any tools to interact with this project. However as this project is a web page, the page will need to be hosted on some domain. Tools used to create the project will include HTML, CSS, JavaScript, PowerPoint, VirtualBox, Kali Linux, Metasploit, HackTheBox Valentine.

References

[1] “Heartbleed Bug | OWASP,” *owasp.org*. https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug

[2] “How to create a Simple JavaScript Quiz ?,” GeeksforGeeks, Aug. 13, 2021. https://www.geeksforgeeks.org/how-to-create-a-simple-javascript-quiz/

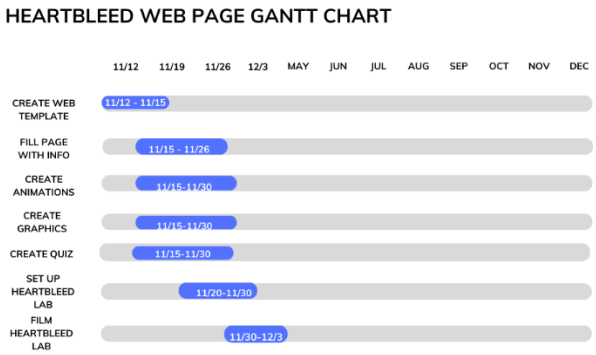
[3] D. A. Wheeler, "Preventing Heartbleed," in Computer, vol. 47, no. 8, pp. 80-83, Aug. 2014, doi: 10.1109/MC.2014.217.

[4] J. Fruhlinger, “The Heartbleed bug: How a flaw in OpenSSL caused a security crisis,” *CSO Online*, Sep. 06, 2022. https://www.csoonline.com/article/562859/the-heartbleed-bug-how-a-flaw-in-openssl-caused-a-security-crisis.html

[5] M. Carvalho, J. DeMott, R. Ford, and D. A. Wheeler, "Heartbleed 101," in IEEE Security & Privacy, vol. 12, no. 4, pp. 63-67, July-Aug. 2014, doi: 10.1109/MSP.2014.66.

[6] S. Kyatam, A. Alhayajneh and T. Hayajneh, "Heartbleed attacks implementation and vulnerability," 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2017, pp. 1-6, doi: 10.1109/LISAT.2017.8001980.

Project Timeline



When each task will be considered complete depends on the task. The web template will be considered complete when it is up and running. Filling the page with info will be complete when a full detailed write up from start to finish about Heartbleed has been added to the webpage. Creating the graphics and animations will be considered complete when a sufficient amount of them have been added to the web page (at least 2). The quiz will be considered complete when each question has been added and the scores tally correctly. The lab set up will be considered complete when it is set up and executes correctly. The filming of the lab will be completed when the lab execution has been filmed and edited and published to the webpage.

Each task will have unforeseen setbacks most likely, and as a result has been given a generous timeline. Each timelines include Thanksgiving break as a consideration, and as such have days that overlap before or after the break. Since working during Thanksgiving is anticipated, the dates have been included, but padding of a couple days is also included due to the nature of the break.

In the case that a setback is so great that the task cannot be completed, an alternative will be found. For example, if creating the quiz in JavaScript cannot be completed, then an alternative may include creating the quiz using Google Forms. However these are the last case scenario and would only be done to ensure a complete product will all the promised components.

Task Dependencies & Potential Issues

-Issues getting the heartbleed lab to work.

-Issues with coding the quiz.

-Issues with getting the gifs to look good.

Expected Outcomes, Evaluation, and Assessment

The deliverables of this project will be a HTML/CSS and JavaScript based web page that explains and showcases the Heartbleed exploit in a manner that is accessible to learners. The success of this project will be based upon having a completed project that includes the following components: gifs and visual diagrams for visual aid, quiz component, video including the execution of a Heartbleed attack, text paragraphs explaining the history of, how it works, and how to protect yourself regarding Heartbleed, and information about the heartbeat component of TLS/SSL.

Given sufficient time, the project may be presented to friends who are not tech related, to evaluate the success of the explanations. The friends will take the quiz given at the end of the webpage, and if they score above the required 90%, it will be considered a passing grade and show their knowledge of Heartbleed.

Personal Learning Goals

My personal learning goals resulting from this project will include a more thorough and detailed understanding of Heartbleed, as well as experimenting with it in a lab environment. I will learn more about TLS/SSL and not just with how Heartbleed works, but the underlying system that enabled it. I will also learn more about setting up and experimenting with a personal lab environment for the purpose of analyzing a cyber attack/vulnerability. I will gain experience creating interactive web pages for the purpose of educating the public, and experience creating visual diagrams and aids for enhancing understanding.

Additional Information