ENPM685 – Final

Version 2.1– April 12th 2022

Background

ENPM685 Waffle Co is a small food/tech start up that is rapidly expanding. What started as a small "mom and pop" waffle shop has blown up to a massive tech startup with the creation of their mobile app. Shortly after releasing their mobile waffle ordering app the company took off as customer's flocked to the app's promise of "push button, get waffle." With the creation of their proprietary "avocado waffle" their customer base has expanded one hundred-fold.

ENPM685 Waffle Co is still a small operation behind the scenes and the former cashier-turned-web developer Nathan is working on improving the company's website. Despite being a mobile app/tech mega power their website until recently just listed information about the business and their waffles. Not wanting to miss out on the opportunity for capturing the "old people who don't know how to use mobile phones" demographic Nathan has begun work on adding online ordering of waffles from their website. To do this he created a development system and begun work. After taking a short vacation he came back to a very panicked Julia, the company's DBA saying that she can no longer log into the dev server and thinks her password may have been changed. Nathan then checked his email and discovered an email message pointing to a Pastebin post claiming to have all of the company's data and offering to sell it to the highest bidder. Nathan believes it's possible that the compromise is related to the development website he has been setting up since it was not "fully setup" and to save time he decided to use production data.

You have been brought in to investigate and provide your write up of the attack. (See "**The Assignment and Requirements**" below for more details.)

Notes from Nathan (The Web Developer/Sysadmin)

- I was making an export of the VM for you but heard an alarm go off and I thought it was the attacker again. In a panic I deleted the VM. It turns out it was just my toaster telling me that my waffle was done. What I was able to export is described below.

- The website is hosted out of /var/www/html/ and is written in PHP. A copy of the web directory is in the **web.tar** tarball.

- The contents of Julia's home directory are in the file **julia-home.tar**

- The logs (everything in /var/log) are in **logs.tar**. I was grabbing them to put into Splunk, maybe that would be helpful for your analysis too?

- For debugging purposes, I had a tcpdump session running which may have captured the attacker's traffic. The pcap is available as **final.pcap**

- These are all contained in the final.tar.gz available in ELMS and also at https://www.glue.umd.edu/~kts/enpm685/final.tar.gz

The Assignment and Requirements

Your mission is to review the collection of files contained in the final.tar.gz file and discover how the attacker got in, what they did, and if sensitive data was stolen. You may not be able to completely follow step by step what the attacker did so you'll have to put your detective cap on and make some educated guesses at some point.

You must write an attack narrative of what the attacker did and answer the following questions:

- How did the attacker get in?
- What did the attacker do once they were on the system?
- Was sensitive data accessed? How can you tell if it was/was not accessed?
- Were you able to learn anything about the attacker? (What were their attack tools, tactics, techniques, and procedures?)

Due Monday May 16th @11:59pm

Review the syllabus for information on the class late policy. **Don't wait until the last minute to get started on this final project!**