Equifax Data Breach

BY: KILIK WHITE

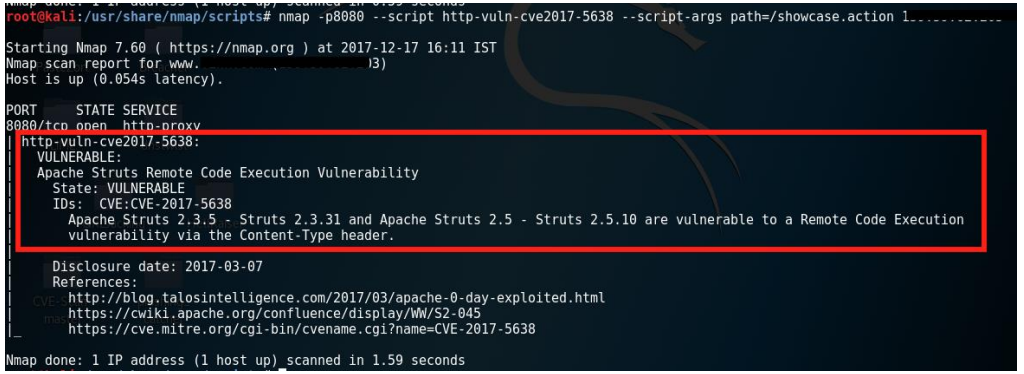
Overview

- Equifax is a Credit Bureau that keeps track of a person's credit and is the third largest credit reporting agency.
- This company had a data breach in March 2017 that had a massive theft of important data.
- The important data that was stolen from 143 million people was...
  - Names, Addresses, dates of birth, SOCIAL SECURITY NUMBERS, drivers' license numbers, and CREDIT CARD NUMBERS

EQUIFAX

What failed to cause this breach

- The Equifax data breach was caused by an older version of Apache Struts (an open-source development framework for java).
- It turns out the older version of Apache had a vulnerability called CVE-2017-5638 where the attackers can send HTTP requests with malicious code in the content-type header and Struts will run it regardless.
- This will cause the code to open even more towards the system that Struts was working on.
- However the people who made Apache Struts noticed the issue and made a patch that fixed it BUT.....



How the breach occurred

- When the people who made Apache Struts told the Equifax administrators to apply the patch to the whole system that is linked towards the outdated Apache Struts, there was an employee that did not apply the patch to the system.
- Equifax's IT department scanned the system to see if the systems were not patched but the scan of the system shows that it is patched while it truly wasn't.
- Then between May and July of 2017 the attackers managed to access multiple Equifax databases containing a lot of key information on people.
- Equifax for a while could not see the suspicious activity that was happening until July 2019 where Equifax found out about the data breach.

Strategies to prevent something like this in the future

- The first and biggest thing to do to prevent something like this from ever happening is to quickly install the latest patch of the hardware so any exploits will be removed.
- Another way to prevent this is to program a better patch scanner that deeply looks at all the programs that use the same hardware and return a list of recent versions of the program that does not match the version patch number.
- Finally the IT people could run the program and try to Hack into it since it shows a test of it working and if the person is able to hack through it, it shows a vurnerablility in the program that needs to be fixed.

Work Cited

- https://en.wikipedia.org/wiki/Equifax
- https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
- https://www.devbridge.com/articles/equifax-fallout-how-organizations-can-prevent-data-breaches/ (was used as a reference for slide 5)