CYB 400 Project One

Douglas Few

June 9th, 2022

Scheduled Maintenance

Upon acquiring BrainMeld, an analysis was performed on their network to determine if there were any vulnerabilities. In the category of scheduled maintenance, or vulnerabilities that can be reasonably addressed in the span of one week, there were many vulnerabilities that simply required updates that were offered by the vendor. This is to say that software being run on the network was out of date, and needed only for an individual to download the necessary updates from the vendor’s website. One such vulnerability in particular was Microsoft SQL Server End of Life detection. This means that the product is no longer being supported in its current form and needs to be updated to a newer version in order to maintain support.

Policy Update

In the category of vulnerabilities that can be expected to be addressed in the span of a month, or policy update vulnerabilities, the assessment yielded several results. One result specifically was the presence of brute force login attempts. While these attempts may never be easily stopped, we can significantly lower the success rate of such attempts by requiring users to regularly update their passwords. Most IT experts recommend that users change their passwords every three months, so I would suggest updating company policy to reflect this recommendation (Sheil, 2022).

Another vulnerability that was identified was the transmission of sensitive information in cleartext via HTTP. In other words, sensitive information was being transmitted in text that was unencrypted and readable by unauthorized sniffers. The recommended solution for this is to make sure the data is encrypted before transmission, and then ensure the information is only transmitted over SSL or TLS connections (CWE, 2022). It is also important to make sure that the SSL connection is maintained from the beginning of connection to the connection’s termination. Otherwise, the possibility presents itself for a sniffer to intercept the information regardless.

Other Security Issues

The two vulnerabilities identified from the Other Security Issues category are as follows: SSL/TLS: Report Weak Cipher Suites and SSL/TLS: Certificate Signed Using A Weak Signature Algorithm. The former report basically states that some of the SSL and TLS ciphers accepted by a service are considered to be weak and require changing (SecuritySpace, 2012). Ciphers using 64 bit or less are vulnerable to brute force attacks and anything using 1024 bit or less is considered to be insecure and therefore weak. The solution is to reconfigure the software to no longer accept cipher suites that are considered to be weak.

The latter vulnerability states that a certificate was signed using a weak hashing algorithm, which means that an attacker might be able to easily replicate the certificate and disguise it as the authentic service (Tenable, 2021). The solution for this issue is to purchase or generate a new certificate that utilizes a stronger hashing algorithm so that it is better equipped to stand against attackers.

Implementation

I would begin with implementing the policy updates first because I believe it would make the greatest impact in the shortest amount of time. Protecting against brute force login attempts and sensitive information being transmitted in cleartext format is important on account of the damage that can be done by succumbing to either of these vulnerabilities. While the scheduled maintenance vulnerabilities can likely be handled in a shorter amount of time, I believe that they are simply not as important in the short term as the outdated software is still serviceable for the time being. I would most likely attempt to handle those vulnerabilities in tandem with the policy updates, though I would choose to focus on the former if it came down to it.

Resources

CWE. (2022, April 28). *Common weakness enumeration*. CWE. Retrieved June 11, 2022, from https://cwe.mitre.org/data/definitions/319.html#:~:text=The%20software%20transmits%20sensitive%20or,be%20sniffed%20by%20unauthorized%20actors.&text=Many%20communication%20channels%20can%20be,by%20attackers%20during%20data%20transmission.

SecuritySpace. (2012). *SSL/TLS: Report Weak Cipher Suites*. SSL and TLS : SSL/TLS: Report Weak Cipher Suites. Retrieved June 11, 2022, from http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.103440

Sheil, J. (2022, April 19). *How often should you change your password: Password tips*. Electric. Retrieved June 11, 2022, from https://www.electric.ai/blog/how-often-should-you-change-your-password#:~:text=IT%20experts%20recommend%20that%20people,account%20for%20a%20short%20time.

Tenable. (2021, November 26). *SSL/TLS certificate signed using weak hashing algorithm*. Tenable. Retrieved June 11, 2022, from https://www.tenable.com/plugins/was/112542