Ahmed Alkaysi

10/23/2016

Nessus Assignment Executive Summary

For this assignment, I conducted a Nessus vulnerability scan on a Samsung Smart TV. I picked a smart TV to scan because I figured that although it is a device that is used by a majority of people, it might not be as secure a computer or other devices. People forget that Smart TVs need to have their software updated with the latest patches as much as their computers and phones do. How often do we hear about the latest update we need to do for our smart TVs? Rarely. Thus, I conducted a scan on my smart TV to see what kind of vulnerabilities would be uncovered.

I used the Advanced Scan policy with the default settings available in Nessus for the vulnerability scan. The scan took about 10 minutes to complete and uncovered 27 vulnerabilities. The breakdown of the vulnerabilities were: 1 High, 5 Medium, 2 Low, and 39 Info.

The high vulnerability was an interesting one. It was titled: Cisco ASA Software CLI Invalid Command Invocation. This vulnerability was due to the Cisco ASA “missing a vendor-supplied security patch.” This vulnerability opens the door for an “authenticated, local attacker” to exploit by using “command-line Interface (CLI)” to process “invalid commands” that could cause denial of service or “execution of arbitrary code.” This vulnerability had a CVSS V3.0 base score of 7.8. As stated in the Nessus Vulnerabilities section, the solution to this issue would be to “upgrade to the relevant fixed version referenced in Cisco Security Advisory cisco-sa-20160817-asa-cli.” In other words, it seems like if I updated to the latest Samsung firmware, this issue would be solved.

The 5 Medium and 2 Low vulnerabilities were all SSL related. Some of the issues included the SSL Certificate cannot be trusted, SSL Certificate signed using a weak hashing algorithm, and SSL Certificate chains contains RSA keys less than 2048 bits. These vulnerabilities make the remote host susceptible to man-in-the-middle attacks. The CVSS score ranged from a low of 2.6 to a high of 6.4. The solution from Nessus for these issues included: generating a proper certificate for the service, having a certificate reissued by the Certificate Authority, and reconfiguring the application to avoid using weak SSL ciphers.

Many of the vulnerabilities that were discovered in the Nessus scan seemed like it would be solved with a simple firmware update. I know for a fact that there is an update available for my Samsung smart TV. The TV has not been update yet because it seems like a hassle to manually go in and look for and install an update through Settings in the menu. If there was a way where I can turn on automatic updates in settings, I would probably do that. It would be a good idea to have a feature like that available by default, so that the chances of having high or medium vulnerabilities would be mitigated. Hopefully in the future, the public will become more aware on the importance of keeping their Smart TV’s firmware up to date, I know I will.