Metasploit Lit Review

What is Metasploit?

How it counters security in the wrong hands

How it improves the cyber security of an organisation

Scenario 2 Overview

Windows 7 had all support for the operating system halted in January of 2020. Windows 7 was certainly a user favourite and the end of support saw quite a few users disgruntledly switch to either Windows 8 or 10 to continue to get security focused support and patches. At this point, the support for windows 7 has been defunct for almost 2 years and as such many new exploits have likely surfaced. Nonetheless, even before Windows 7 met its end-of-life there were still many exploits that could be performed on the system that were sequentially fixed in the new versions of Windows. One such vulnerability present in Windows 7 is that the default version of Windows Media Centre will execute any code saved as a “.mcl” file.

Scenario 2 Counter measures

The most useful countermeasure to this, and typically, any security related vulnerability is user vigilance. A user should be aware of what files, services, websites, etc. should typically look like in their daily usage f a computer system and, as such, should be able to identify when one of these, and in this case a file, looks suspicious and should be scanned via some program before using or opening it.

Furthermore, it is also important since this exploit made use of a .mcl and .exe file that a user makes use of some form of antivirus or antimalware software and in this particular case, ones that are signature based. The reasoning for this is because the executable in this scenario is one that has been created and is typically used in a large scale.

It is also vital to understand the exploits you are vulnerable to. In the tutorial we demonstrated that the file could be run and Windows only alerts that it comes from an untrusted, meaning un-certified, source which nowadays is something that happens with most applications as the typically programmer does not have access to particular licencing on their applications. In this case, having a more rigorous firewall or settings for it may have restricted the reverse\_tcp from functioning.

Apart from this, the main fix to this particular issue was to install a patch provided by Microsoft on their site, and as such having some sort of patch management system is also vital to users. This could be simply regularly checking each application download page for the newest version or patch. However, there are applications and programs that automate this process and keep all your programs up to date. It should also be noted that most programs tend to offer a “Check for updates” feature when installing the program and likely also in the settings after the fact.

Josh Reflection

Working on this project has taught me several different things both within and outside of computer security. The most notable to me personally would be the fact that GitHub allows each user to create and then host a single static website. This is what was used to host the blog section of this project but will also be used by me in a personal capacity for a personal website in future. Apart from this, seeing the sheer amount of exploits that Metasploit has available to use is a bit disconcerting as it covers a wide array of different machines, programs and means of execution and has definitely made me that much more critical of everything I do online. This project also allowed me the chance to learn how to use HTML and CSS when writing the blog, which also forced me to switch up my usual writing style for one that is more colloquial for the general public instead of assuming the people reading the writing are already knowledgeable on the topics.