Anthony Constantino
3/22/17
HW 12

Modern Day Buffer Overflow

Even though a buffer overflow attack is one of the oldest tricks in the book, they are still a large problem with software today. Exploring the National Vulnerability Database there have been several fixes that have been made to various buffer overflow vulnerabilities in just the past few days. There can be found pages of exploits ranging from mild to critical in severity. One notable critical flaw that was fixed two days ago, was a buffer overflow in Cerberus FTP.

This vulnerability allowed remote attackers to cause a denial of service (ddos) crash and possibly give the attack access to data they should not have access to. The method of attack was very simple and was as easy as providing a long MLST command when using the FTP service. The MLST command is designed to provide the user with data only on the object specified in the command and should not give information on anything else. The reason this vulnerability was so critical is due to the fact that it is not that hard to do. All you have to do is open a socket and send the MLST appended with a char “A” multiplied by theoretically any large number. Another reason for its severity is because the accessibility was open to network exploit making it relatively easy to get access. This means the attacker could be anywhere and perform this kind of attack on the system without having direct access to the system.

It really is surprising that an attack so simple could still be executed with little to no effort at this day and age. Especially with so much data out there that could be used to inflict so much harm. To have a exploit so easy to manipulate such as this one with Cerberus FTP, with all the advances that have been made to further security measures implemented to protect against attacks like these, is quite eye opening to say the least.