Ben Walker
11-13-18
CSC 495: Reading Assignment 2

Blind Return Oriented Programing (BROP) and Return Oriented Programming (ROP) are very similar. ROP is the core method of hacking that is used between these two. However, with BROP it builds upon ROP and extends it. The blind part of the attack comes from the ability to not need to know the specifics of the vulnerable program. It allows for the attacker to point an automated script at a remote process and it will auto detect the vulnerability. It then will find the pop-pop-ret gadgets and exploit them. Both of these processes use the understanding found in ROP with how there will be certain addresses that can be called on a system, regardless of address randomization. As well they both need pop-pop-ret gadgets to function properly as a disguised process. While a script can be used with ROP, it seems that BROP requires automation due to the time and try requirements for a successful attack. While in ROP you can usually check information on the process that is being attacked, BROP has little to no access to information about the process. ROP is all guided by the attacker, BROP has limited guidance. I would say that the biggest factor that makes BROP successful is the automation of the process, rather than the individual performing the attack, such as with ROP.