Heap OverFlow attack

By Tysen Radovich (j86j296), Allen Simpson (r29b821), Spencer Lawry(w58z387) and Arash Ajam (f63m331)

In our project we are going to be doing a Heap Overflow attack. First of all we have to give an idea of what a stack and buffer overflow is before we can best explain a heap overflow. This is much like a stack overflow attack where we are giving the buffer more than what it can hold causing it to overflow. This then allows it to write into parts of the memory location it probably should not thus allowing malicious code to run. Now much like a stack buffer overflow attack a heap overflow attack works in a similar way. To do a Heap overflow we need to have a chunk of memory that has already been allocated in the heaps memory that can be overwritten by an overflow. The goal of this project is to fully research and understand how a heap overflow attack would work. To do this we need to fully describe what they are and how they work. By researching them we hope to gain the knowledge of how both userspace and kernelspace are affected by heap overflows. We will also be looking at ways to help mitigate heap overflows from ever happening.

During this project there will be many parts that have to be researched. First of all a large number of the group have never heard of a stack overflow. This means that they will have to learn exactly what that means before they can fully understand what a heap overflow will do. To do this since one of the members has taken another class about security he has been able to help explain and overflow attacks and how it works. We have all decided to understand as much as we can about what a heap overflow does. What it affects and what can be done to stop an attack using it.

Our time schedule is to have everything understood by Sunday the 2nd of November. This means that we also are about ⅓ the way through writing the technical report. The next checkpoint we have is that we want to be fully done with it 5 days before we turn it in. This means that by November 10 we want to be fully done with the project meaning that the report is done and we have plenty of time to go through and edit if we need to.

Tysen, Allen, Spencer and Arash will all be fully responsible for the technical report. This means that not one person will just write the entire thing; it means that each person will equally contribute to the project. This means that after every time someone puts something in the project they should be able to explain what it does and why it is important to the rest of the group. This allows the person to not only show that they have learned the material but have also understood it enough that they can describe it to someone else who may have never heard of it.