CIS 751 Lecture Assignment 3

Chuck Zumbaugh

September 18, 2025

To overflow the buffer and cause system() to execute "/bin/bash" we would need to not only overwrite the EIP with the address of the system function, but also emulate *call system*. If this was a legitimate instruction, the arguments to system would first be pushed to the stack, followed by the address to return to after executing system(). Thus, we can overflow the buffer as follows:

- Write a NOP sled the size of the offset
- Overwrite the EIP with the address to system
- Overwrite the next 4 bytes with the address to return to after system (the EIP that would have been saved had *call system* been executed.
- Overwrite the next 4 bytes with the command to execute (ie. "/bin/bash")

Thus, the stack will look something like:

Lower Addresses
NOP sled
Address to **system** (EIP)
Address to return to after **system** is finished
Arguments to pass to **system** (*ie. /bin/bash*)
Higher Addresses