Brendan Song
b7song
20466121

CS458 A1

Sploit 2:
- This sploit makes use of the vulnerability of sprintf
- This is a string format exploit and is passed in through the cmd parameter
- The string passed in finds the end of the stack and writes over the saved eip to return to the shellcode script
- It writes the correct amount of bytes to each memory address to modify the value of the saved eip
- This can be patched by avoiding the use of sprintf or checking for viruses on all input arguments

Sploit 3:
- I wasn't able to get this one working but there is a buffer overflow vulnerability when copying files
- Since the src file is read character by character, it does not know when to end and is open to buffer overflows
- The exploit needs to find the correct amount of 'garbage' to fill up then modify the return addr to the shellcode script
- This can be patched by avoiding the use of fgetc and not accepting an arbitrary amount of characters into the buffer at a time