410 exploit

Patrick Thomasma

CIS410

Exercise 2

In order to prevent the exploit from running I had to find the vulnerability in the server program which is in line 68 with the read(fd, &(s.nbytes), sizeof(s)); the line will read sizeof(s) into the buffer with the &(s.nbytes) with fd. So the line will read nbytes into buffer starting with the memory address but since nbytes + 4 is read in the struct also contains a function pointer that takes 4 bytes. So if more pages are received than the buffer is going to overflow. I rewrote the line as read(fd, &(s.nbytes), sizeof(s.nbytes); to prevent this. So this limits the bytes written to s.nbytes and now when I try to run the exploit I am no longer able to change s.fp and I cannot use the malicious payload. When I run the exploit program all that prints is okay and a newline so the server is not giving me access.