410 exploit

Patrick Thomasma

CIS410

Exercise 2

410 exploit

Patrick Thomasma

CIS410

Exercise 2

The exploit for this server involves an overflow of the buffer to run malicious commands onto the server. When Server.c is ran it will wait for messages from the client and the messages are read into a buffer that is n \* 4096 bytes long, however if the message is overflowed into the buffer then the function pointer will be overwritten. With the exploit I overwrite the function pointer with an address that is in the middle of the buffer. The buffer is mostly filled with no instructions but the malicious shellcode will sit in the high addresses of the buffer with the middle filled with no instruction. So when we overwrite the function pointer with our shellcode it will be in the middle of the no instruction pointer until the counter rises for it to hit our malicious shellcode. So my address range of the buffer was 0xf7791000- oxf7792000 and then the s.fp was set to 0xf00000000. When the shellcode runs shell\_reverse\_tcp this will allow the attacker to listen in to the client port. So when attacker runs nc -I 9009 and the exploit program than the attacker is able to run the shell commands onto the server and be able to access and look into the contents of the server.

