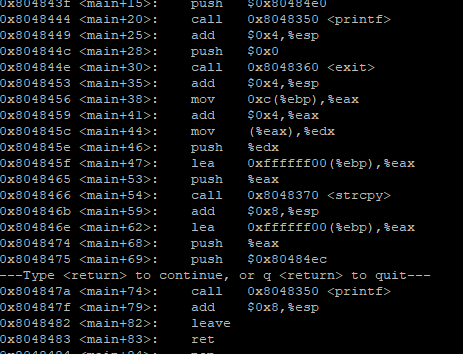
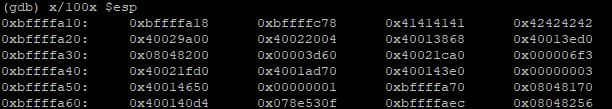
우선 gremlin을 gdb로 disassemble하려 했지만 권한이 없어서 할 수가 없었다.

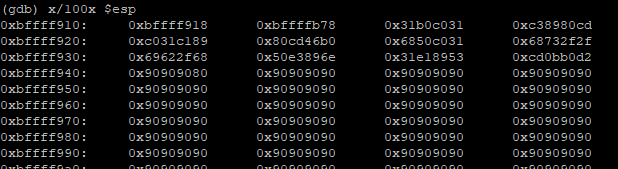
그래서 cp명령어로 복사본을 만든 뒤 disassemble을 해보았다.



함수를 호출하는 부분이 보이는데 strcpy함수로 ret를 조작할 수 있을 것 같다.

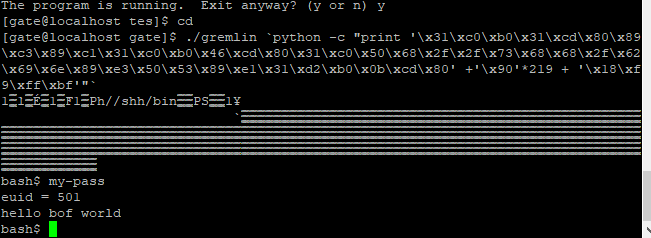


AAAABBBB를 입력해보았더니 0xbffffa18부터 채워지는 것이 보였다.



그런데 막상 payload를 입력해보니 주소가 0x100만큼 밀려있었다.

그래서 주소를 다시 수정해보았다.



그랬더니 성공

Bash를 bash2로 바꾸지않아서 여러가지 방법을 쓰다가 하나도 되는게 없어서 오래걸렸다…..