ret2libc chaining

is invoke on arbitrary number of functions
Leave "/etc/passwd"

```c
fd2 = open("/etc/passwd", 0, 0);

n = read(fd2, buf, sizeof(buf));

write(stdout, buf, n);

exit(0);
```
Leave "/etc/passwd"

open ("etc/passwd", O, O);

sendfile (fd, fd, O, UINT_MAX);

exit (0);
ret2libc chaining

Is invoke on arbitrary number of functions

%esp lifting

Move %esp to the right location in the stack (stack frame) to allow for the execution of the "next" function

add $ur, %esp; ret
pop %r; pop %r; ...; ret

add $0xc, %esp; ret