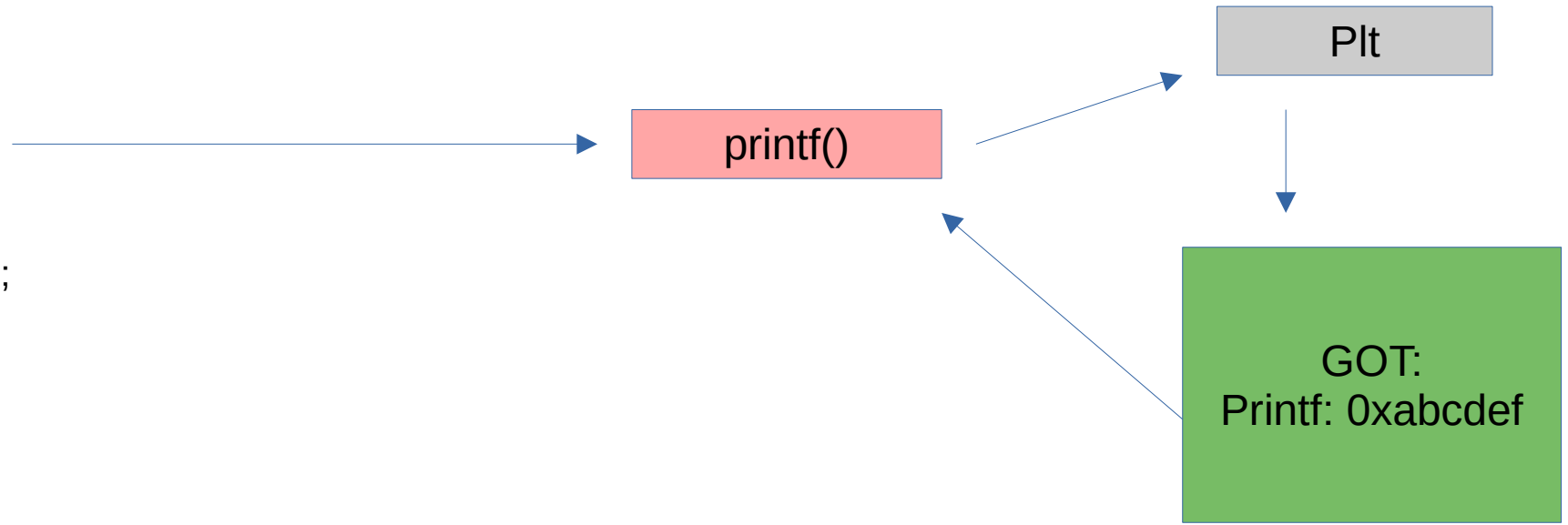
RELRO Exploitations

RELRO stands for Relocation Read Only

Its a protection mechanism that protects data sections of a process from overwriting during exploitation process.

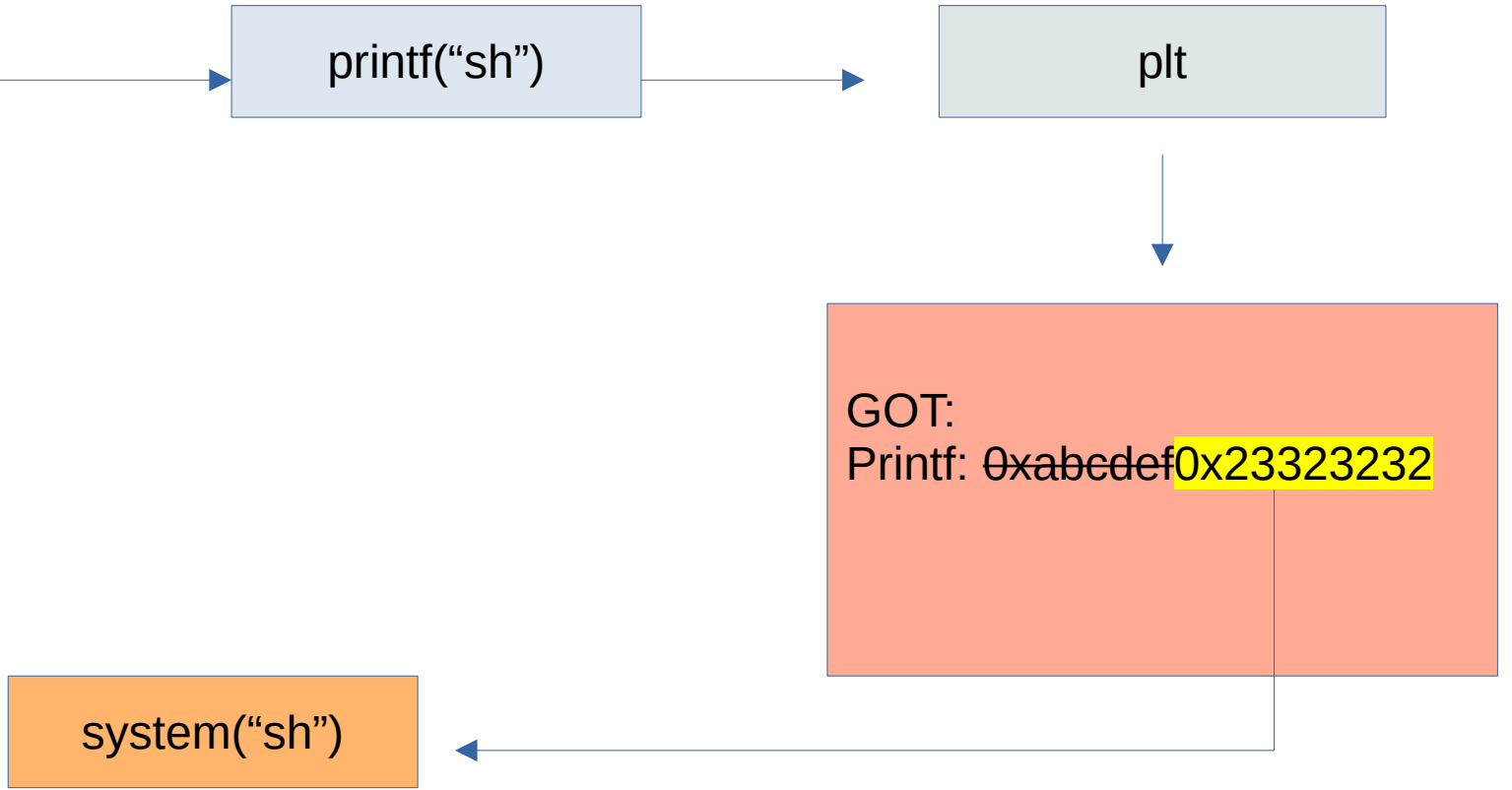
Global offset table

```
Int main(int argc,char **argv)
{


printf("sh");


        return 0;
}
```

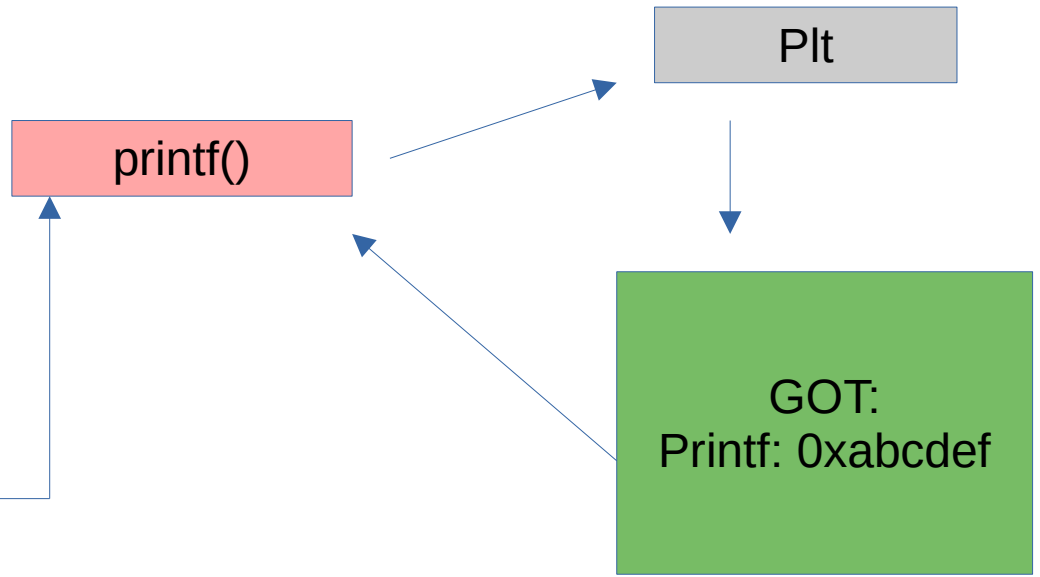


Bypassing RELRO

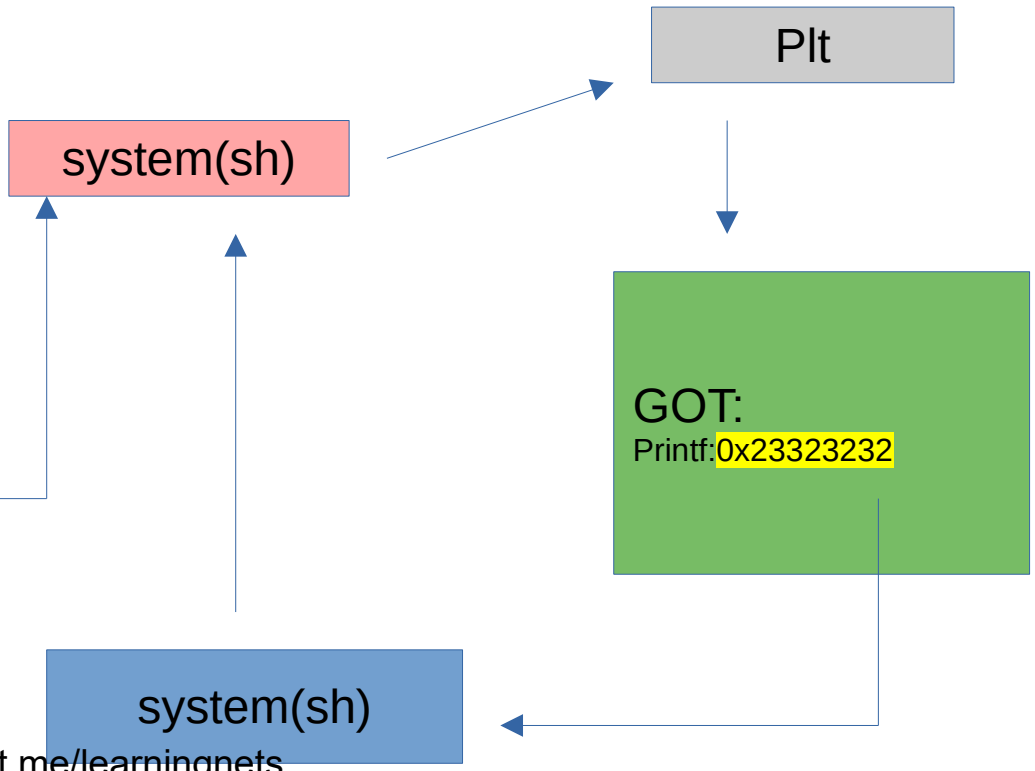
```
Int main(int argc,char **argv)
{
        printf("sh");

        return 0;
}
```



```
Int main(int argc,char **argv)
{
        char *pointer[4];
        char second[4];

        strncpy(pointer,argv[1],4);

        strncpy(*pointer,argv[2],4);

        printf("sh");


        return 0;
}
```



```
Int main(int argc,char **argv)
{
        char *pointer[4];
        char second[4];

        strncpy(pointer,argv[1],4);

        strncpy(*pointer,argv[2],4);

        printf("sh");


        return 0;
}
```

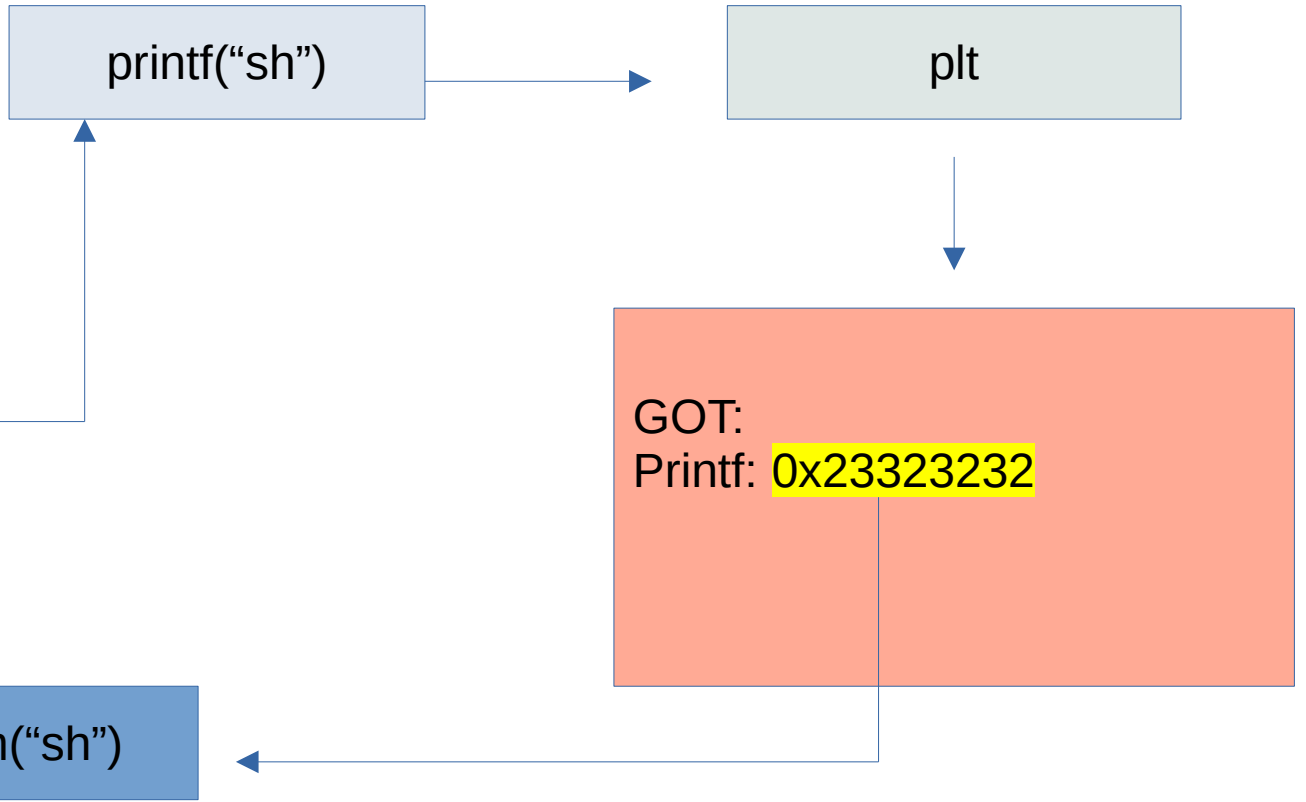


```
Int main(int argc,char **argv)
{
        char *pointer[4];
        char second[4];

        strncpy(pointer,argv[1],4);

        strncpy(  *pointer,  argv[2],     4);

        printf("sh");


        return 0;
}
```

printf()

printf()

system()



Moral of the story is ..