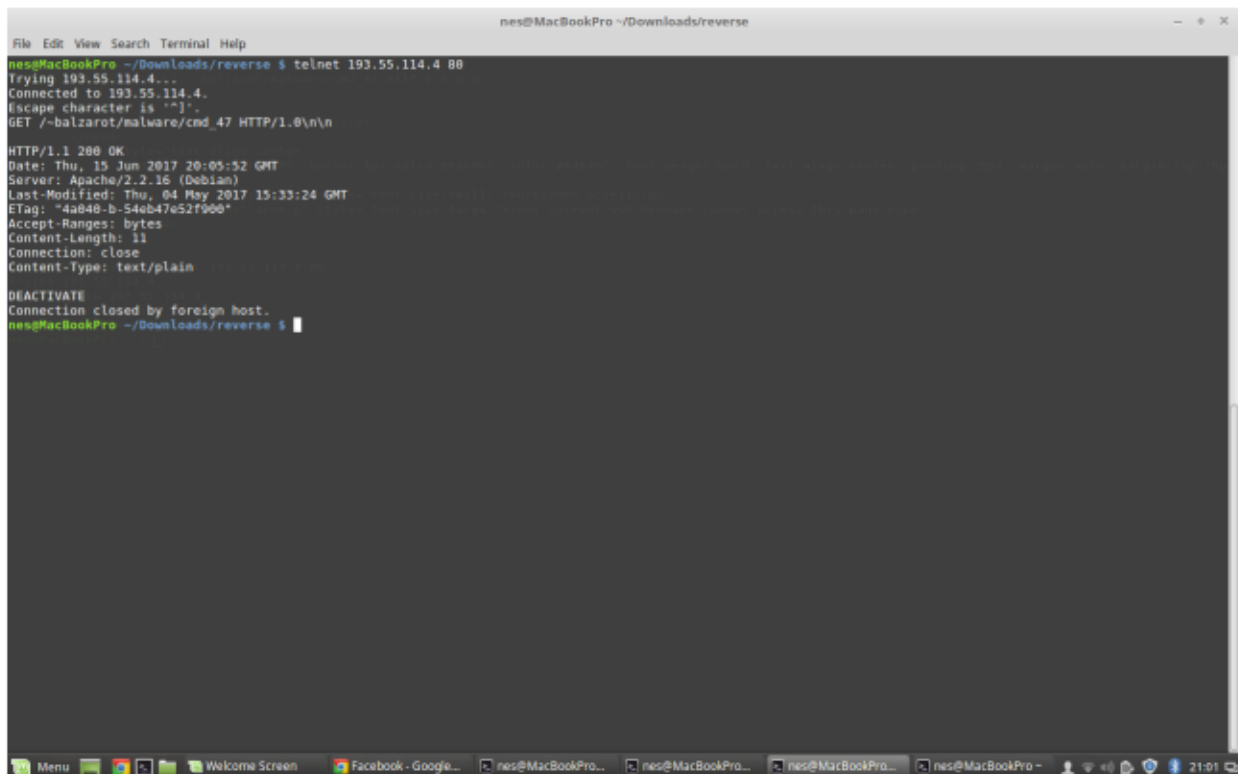


After decompiling the instruction code at 0x400a66 with Ida, I discovered that the program connects to 193.55.114.4 then performs a GET request to /~balzarot/malware/cmd_47 HTTP/1.0\n\n and reads a buffer returned by the website. Using telnet, I tried to perform the same action in order to determine the value returned : As you can see, the program gets DEACTIVATE



```
nes@MacBookPro ~/Downloads/reverse
File Edit View Search Terminal Help
nes@MacBookPro ~/Downloads/reverse $ telnet 193.55.114.4 80
Trying 193.55.114.4...
Connected to 193.55.114.4.
Escape character is '^]'.
GET /~balzarot/malware/cmd_47 HTTP/1.0\n\n
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2017 20:05:52 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Thu, 04 May 2017 15:33:24 GMT
ETag: "4a848-b-54eb47e52f900"
Accept-Ranges: bytes
Content-Length: 11
Connection: close
Content-Type: text/plain

DEACTIVATE
Connection closed by foreign host.
nes@MacBookPro ~/Downloads/reverse $
```

Then the program makes some operation on this string via the sub4009E6 function. After looking at the address 0x004009e6 and decompiling the code I noticed that this function transforms each character of DEACTIVATE except the last one by adding to it the next character and doing an xor between the result of the sum and a character from the array at address 0x00400de8. (basically for each character it performs this operation : $a[i] = (a[i] + a[i+1]) \wedge b[i]$ with $a[i]$ being a character from DEACTIVATE and $b[i]$ a character from the array at 0x00400de8) When I go to 0x00400de8, I can see the content of the array which is [168,199,199,197,178,220,250,180,199,10] (After transforming the hexadecimal result to decimal). Now all I have to do is to write a C script that performs the xor operation in order to get the key but since IDA already did the hard work I am just going to modify the code I obtained after decompiling the instructions at 0x004009e6. The script is :

```
#include<stdio.h>
#include<stdint.h>

int array1[9]={ 168,199,199,197,178,220,250,180,199};
int main(){
char a[]="DEACTIVATE";
int v1;
char key[10];
int i;
for ( i = 0; i <= 8; ++i )
{
```

```
*(char *)(i + a) += *(char *)(i + 1LL + a);  
v1 = *(char *)(i + a);  
key[i] = v1 ^ array1[i];  
*(char *)(a + i) = v1 ^ array1[i];  
}  
printf("%s\n",key); }
```

The result obtained by running the code is !ACR/Cm!^ Since the program does not modify the last character the key should be !ACR/Cm!^E