**Reverse Engineering HW4:**

**Mori Levinzon 308328467**

**Omri Klein 318733565**

**Dry part:**

1. It is possible to get this gadget. If we would be scouting the code after the combination of the two commands opcodes (60 and C3) ,we may took part of another command in order to find the opcode 60 which is not so common.

For example : if we had the following commands at the end of some function in the code:

add    esp,0x60

ret

this is two commands that we can find in allot of function (as we need to return the stack pointer to it's original state before we reti=urn from the function).

the opcode of the two commands is translated to :

83 c4 60

C3

And the last two opcode is exactly what we need.

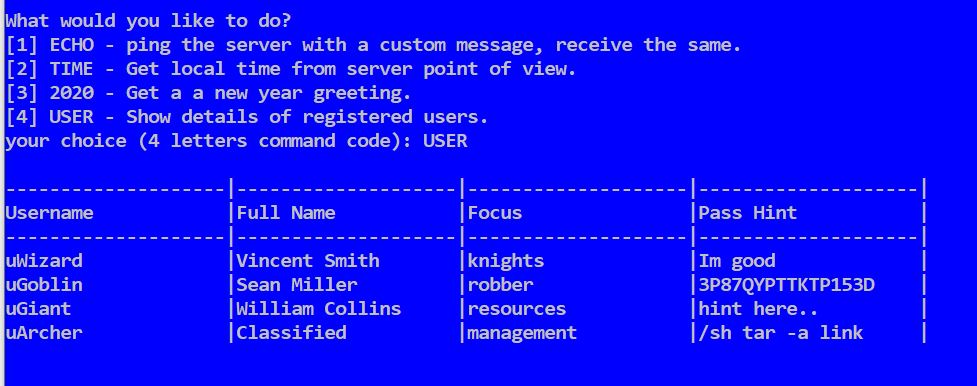
1. Here is a look at the stack :

**Wet part:**

Part 1:

At first glance of hw4\_client.exe trough IDA everything seems in order. There is a request for username and password that is checked through the server using the methods we already saw (send and recv) . after going trough couple of check up to find to any vulnerability, we found out that whilst the username length is limited to up to 31 letters there is no such limitation on the password length, and therefore the exe is exposed to buffer overflow. We needed a way to pass trough the username and password checks that are been done after we are returning from the function. So we decided to use the buffer overflow to overwrite the return address from the function and instead of making the function return to the rest of the code (and the authentication check ) in address 401C3B we decided to changed it to loc\_401CAE, after the authentication part and on to printing the menu and the rest of the desired user table. We wrote python script the opens a process and insert to it "MENU" as a user name in order to make the program print the menu in the branch later on located next to loc\_401CAE. Afte that we needed to insert a password. The problem is that the password address is located higher than the username address, so in order to reach the return address and changed it we needed to assemble the password carefully, avoiding rewriting the username in the processs. We padded the start of the menu with couple of "A" till we reached the username address where we kept it as is ("MENU" with null), after that we kept on padding with "A" till we reach the return address and replaced it with "401CAE".

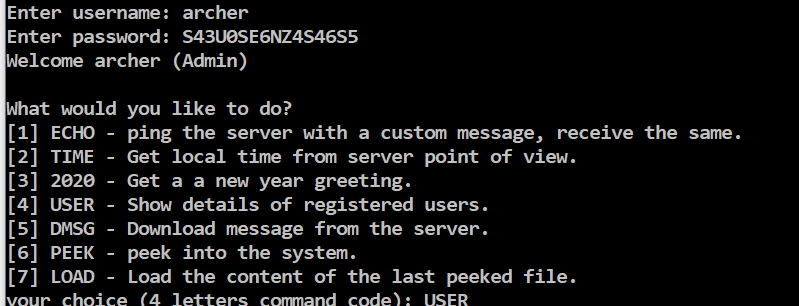
Running the users.py and requesting the users table file gave us the following result:



Part 2:

As we we saw from the table printed to us the only given password is the one that belongs to the goblin. We tried to log in with the goblin as a username and his password and got the same table, but this time it had an additional option: DMSG. The same option that prints the message that we decypherd in the previous assignment.

We noticed that the goblin password is the same one that we found in the 1st assignment, so we tried to log in with all of the accounts. The Wizrds and the giant showed us the same menu and messages as the goblin did. But when we logged using the archer account we found out that he is an admin and there fore has more permissions and his menu contained more options:



Part 3: