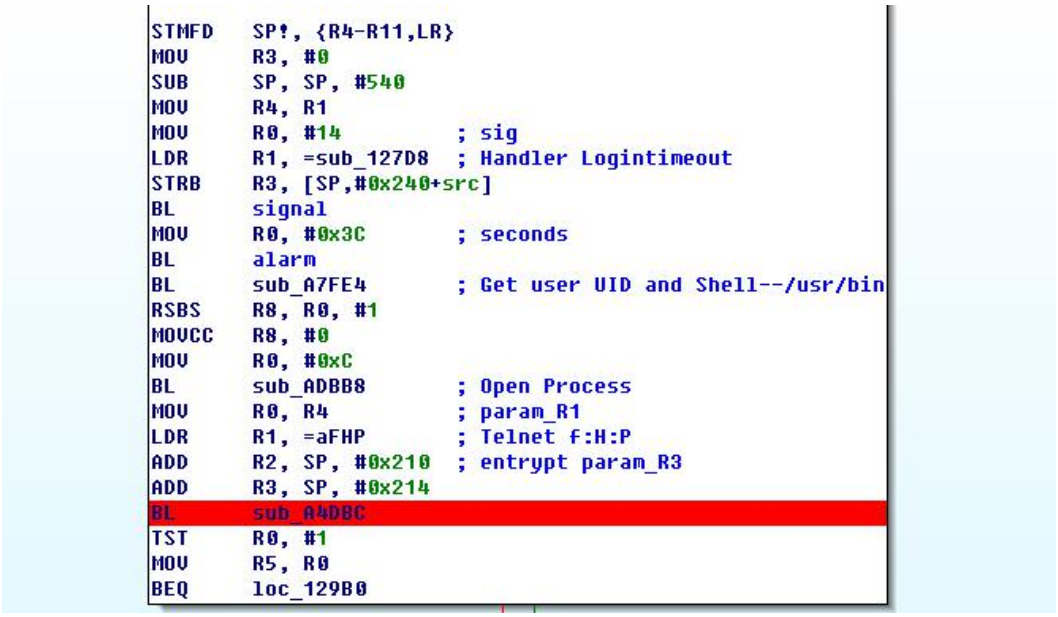
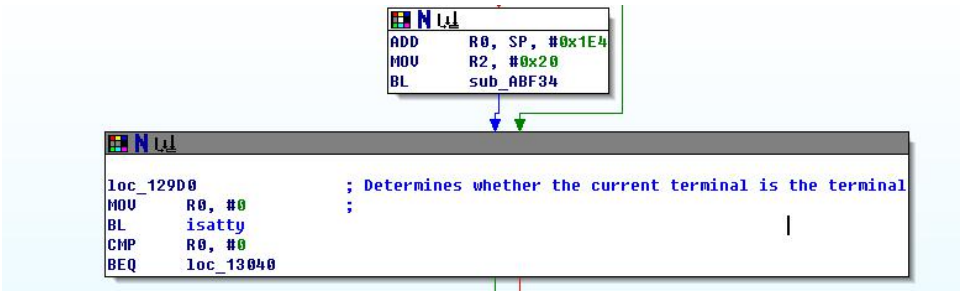
The backdoor is stored in the Telnetd file. Telnetd is responsible for opening telnet and providing services. Here we can see the preparation of a series of services after opening the Telnet service.



```
STMFD   SP!, {R4-R11,LR}
MOV     R3, #0
SUB     SP, SP, #540
MOV     R4, R1
MOV     R0, #14         ; sig
LDR     R1, =sub_127D8  ; Handler Logintimeout
STRB    R3, [SP,#0x240+src]
BL      signal
MOV     R0, #0x3C       ; seconds
BL      alarm
BL      sub_A7FE4       ; Get user UID and Shell--/usr/bin
RSBS    R8, R0, #1
MOVCC   R8, #0
MOV     R0, #0xC
BL      sub_ADBB8       ; Open Process
MOV     R0, R4          ; param_R1
LDR     R1, =aFHP       ; Telnet f:H:P
ADD     R2, SP, #0x210  ; entrypt param_R3
ADD     R3, SP, #0x214
BL      sub_A4D8C
TST     R0, #1
MOV     R5, R0
BEQ     loc_129B0
```

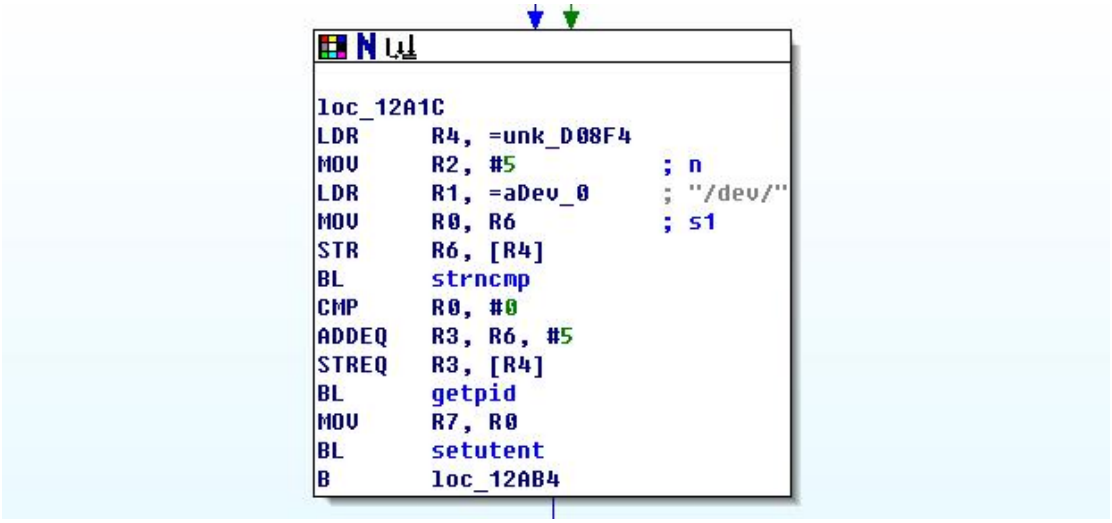
And then judged the local environment.



```
ADD     R0, SP, #0x1E4
MOV     R2, #0x20
BL      sub_ABF34
```

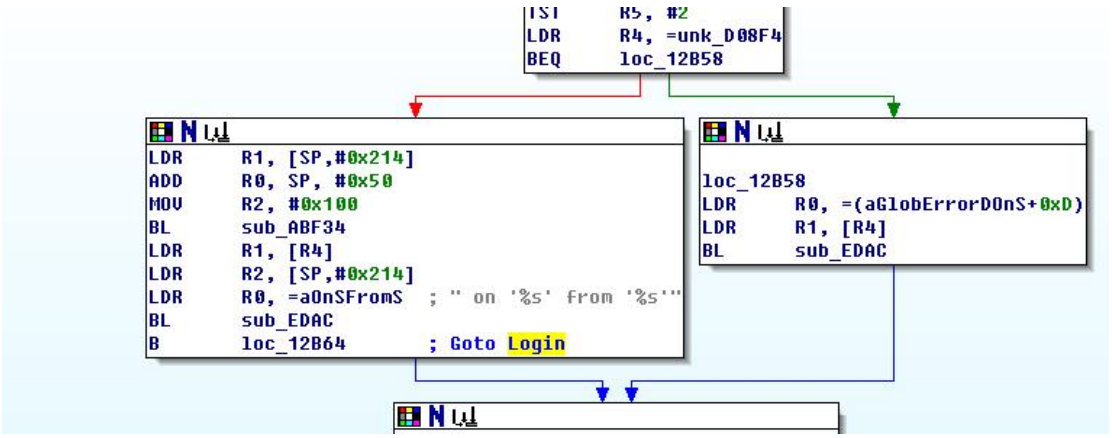
```
loc_129D0               ; Determines whether the current terminal is the terminal
MOV     R0, #0          ;
BL      isatty
CMP     R0, #0
BEQ     loc_13040
```

Get user information

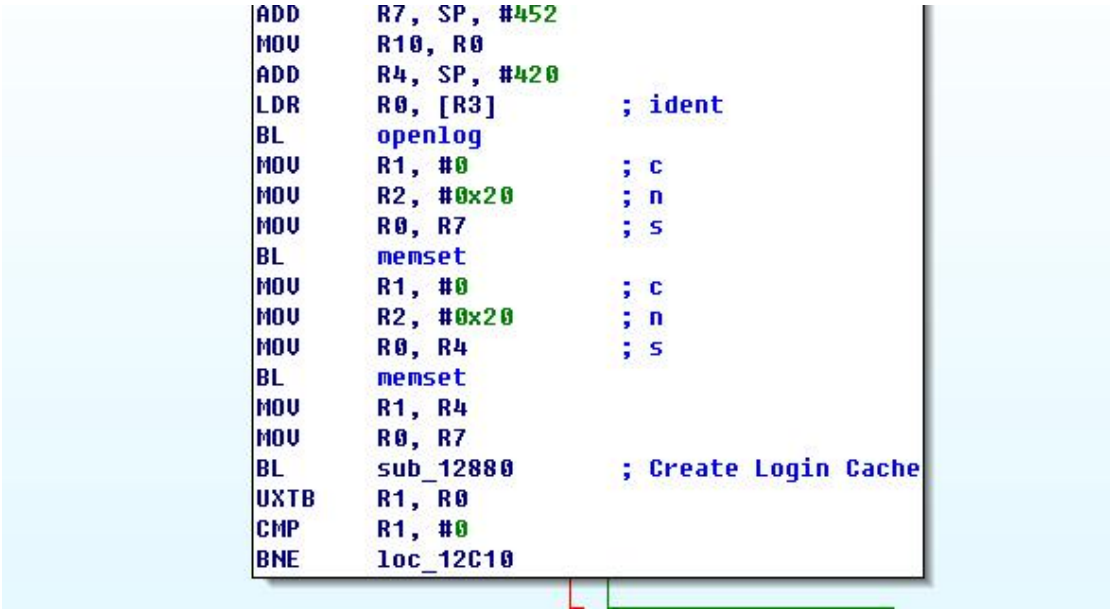


```
loc_12A1C
LDR     R4, =unk_D08F4
MOV     R2, #5          ; n
LDR     R1, =aDev_0     ; "/dev/"
MOV     R0, R6          ; s1
STR     R6, [R4]
BL      strncmp
CMP     R0, #0
ADDEQ   R3, R6, #5
STREQ   R3, [R4]
BL      getpid
MOV     R7, R0
BL      setutent
B       loc_12AB4
```

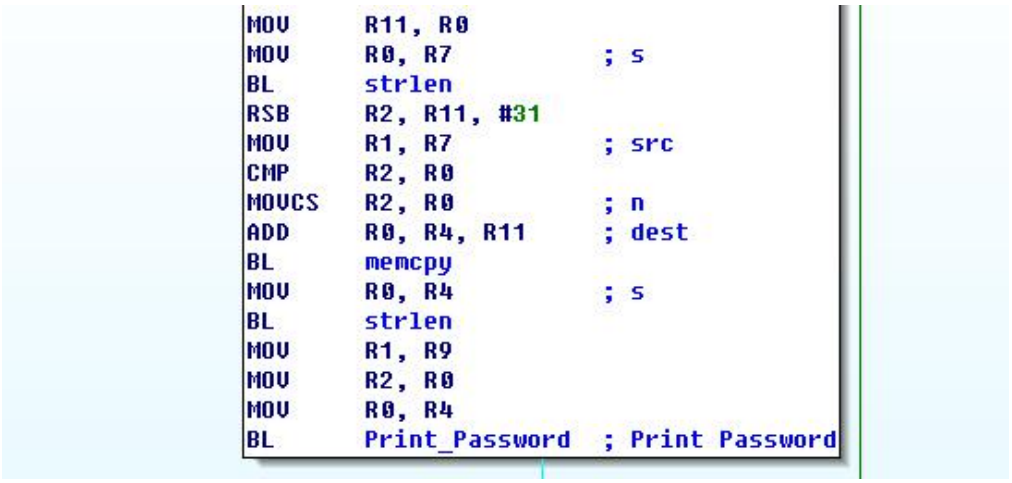
Goto Login



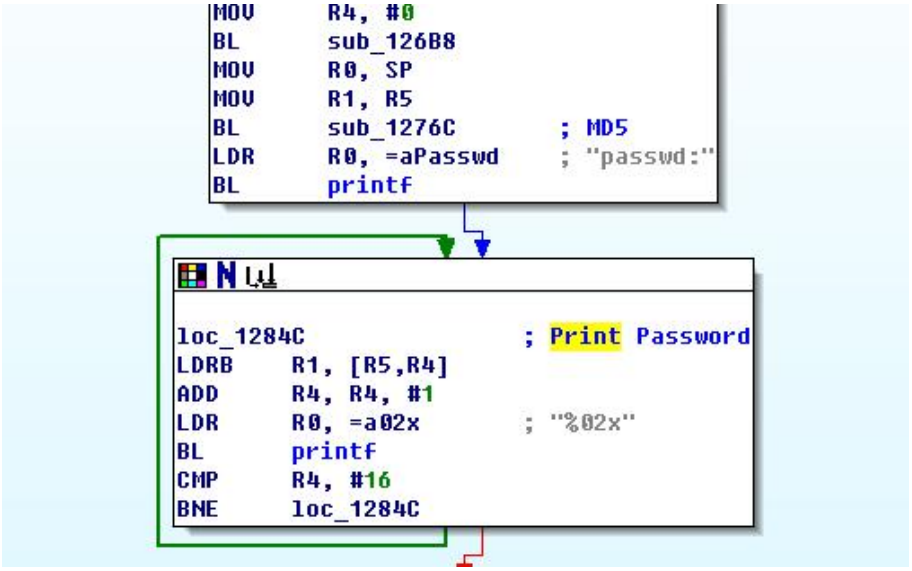
Create Login Cache



In the end, it was executed Print_Password().We gotoPrint_Password().



As you can see, the function uses MD5 encryption and returns.



Telnet Login