

କୁଳାଳ ମାତ୍ରାଙ୍କ ପିଲାଙ୍କ ଦିଲାନ ପରିଚାର ଏହି କିମ୍ବା

gdb debugger ғиелүү

b func-name

14n

## የኢትዮጵያ አጠቃላይ ሰነድ

לפניהם נקבעו פונקציות  $f$  ו- $g$  ב- $\mathbb{R}$  על מנת ש- $f(g(x)) = g(f(x))$  עבור כל  $x \in \mathbb{R}$ .

```

string.h
sys/socket.h
func-stack-protector req.c -o auth -Wl,-no_pie
(lldb) target create "auth"
Current executable set to "auth" (x86_64).
x80\0\x00\0\x00\0\x00\x00\xf9\xbf\xed\x8
X 8
word="eran123";
lPasswords(){
    intf("%s\n",password);
}
_req(void) {
    bool suc = true;
    hasnt("please enter your password \n");
    gets(buf);
    if(strcmp(buf,password) == 0)
        suc = true;
    return suc;
}
int argc, char** argv) {
proposix
Desktop
Pictures
Documents

```

Authenticating with the password "eran123". The password is correctly matched.

```

Breakpoint 1: where = auth'read_req + 8 at req.c:24:7, address = 0x000000010000e68
(lldb) r
Process 26983 launched: '/Users/erankaufman/Dropbox/untitled/auth' (x86_64)
Process 26983 stopped
* thread #1, queue = 'com.apple.main-thread', stop reason = breakpoint 1.1
frame #0: 0x000000010000e68 auth'read_req at req.c:24:7
21
22     bool read_req(void) {
23
24         bool suc = false;
25         char buf[MAX]={1,2,3,4,5,6,7};
26         printf("please enter your password \n");
27         gets(buf);
Target 0: (auth) stopped.
(lldb) p suc
$0 = false
(lldb) p $suc
$1 = 0x00007ffecfbff8e7
(lldb) p &buf
$2 = 0x00007ffecfbff8e7
(char *)$2 = 0x00007ffecfbff8e7
(lldb) x 0x00007ffecfbff8e7
0x00007ffecfbff8e7: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7ffecfbff8e7: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7ffecfbff8e7: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
(lldb) 

```

The password "eran123" is entered, but the program fails to match it due to a buffer overflow or similar issue.

$x = \text{examinc}$

$n = n_{\text{exec}}$

$n_{\text{exec}} \rightarrow \text{SIG fault or die}$

`dis -n func-name (ex main)`

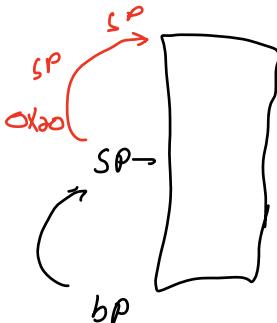
SP = SP-4  
 in C = 4 bytes  
 Push ) Nf 20  
 0:0N 0x1011  
 10 0x1010  
 20 0x1010

כפלריה נזקן (תג'ר) יונתן שטרן Stackptr

structured base for the mov `drsp, r1sp`

רַבְמָן גִּיאָת תְּמָנָה 0x20 יְלִי תְּמָנָה Suby 0x20, 'ISP

header e. גַּם בְּפָ

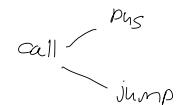


The Why - Recan - Stack

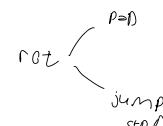
```
(lldb) target create "auth"
(lldb) b read_req
Breakpoint 1: where = auth'>read_req + 8 at req.c:24:7, address = 0x00000010000040
(lldb) dis - main
26
```

movq %rsi, 0x100000e40  
callq 0x100000f01, %al

read\_req



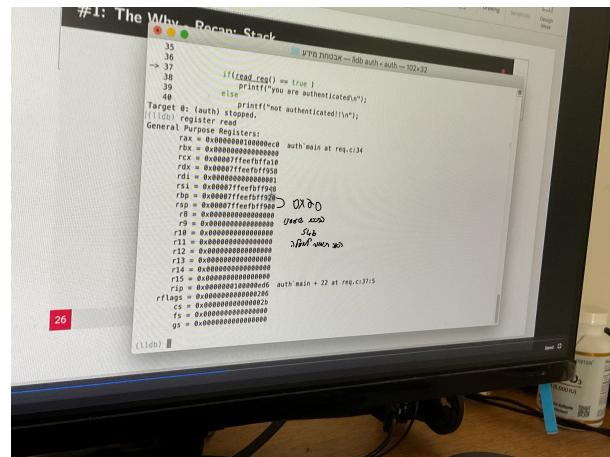
SP → RBP ← RNC | PCLW LCN | instances?)



Current executable set to 'auth' (x86\_64).

```
(lldb) b read_req
Breakpoint 1: where = auth'>read_req + 8 at req.c:24:7, address = 0x00000010000040
(lldb) dis - main
26
```

Auth by read\_req P=1 ret



```
r12 = 0x0000000000000000
r13 = 0x0000000000000000
r14 = 0x0000000000000000
r15 = 0x0000000000000000
rip = 0x00000000010000d6 auth`main + 22 at req:c:37:5
rflags = 0x0000000000000296
cs = 0x0000000000000002
fs = 0x0000000000000000
gs = 0x0000000000000000

[(!lldb) c
Process 27024 resuming
Process 27024 stopped
* thread #1, queue = 'com.apple.main-thread', stop reason = breakpoint 1.1
frame #0: 0x000000010000e48 auth_read_req at req:c:24:7
21         bool read_req(void {
22             bool suc = false;
23             char buf[MAX] = {1,2,3,4,5,6,7};
24             printf("please enter your password \n");
25             gets(buf);
26         }
27     Target 0: (auth) stopped.

[(!lldb) p $buf
(char *) $17) $0 = 0x00007fffeefbf8e8
[(!lldb) x $0x00007fffeefbf8e8
0x7fffeefbf8e8: db 00 00 00 00 00 00 00 00 20 19 bf ef fe 7f 00 00
0x7fffeefbf8f8: db 00 00 00 01 00 00 00 00 20 19 bf ef fe 7f 00 00
.....
7777....
```

start to be nervous when you open your stack } 1 can do it

Prov  $\rightarrow$  New  
base points

7ffe fc bf f9 20

return address

return address: 0x0000000000401000 / 0x0000000000401000 01:16:29

## Show\_passwords .שׁוֹוּפַסְוּוֹרָדָס