

Forum:[Hack Forums](#)

Thread: [Is this considered a BOF?](#)

GhostSniper - August 15, 2010, 7:12 pm

Code section .data

```
msg: db 'Test',0
```

section .text

```
global _start
```

```
_start:
```

```
mov ecx,msg
```

```
mov edx,4
```

```
call _read
```

```
mov ecx,msg
```

```
call _print
```

```
call _exit
```

```
;#####
```

```
;#####=-Functions=-#####
```

```
_read:
```

```
mov eax,3
```

```
mov ebx,0
```

```
mov edx,4
```

```
int 0x80
```

```
RET
```

```
_print:
```

```
mov eax,4
```

```
mov ebx,1
```

```
int 0x80
```

```
RET
```

```
_exit:
```

```
mov eax,1
```

```
mov ebx,0
```

```
int 0x80
```

```
RETExample of what happens:
```

```
Code [Dean@Fedora-13 asm]$ nasm -f elf template.asm -o temp.o
```

```
[Dean@Fedora-13 asm]$ ld -s temp.o -o test
```

```
[Dean@Fedora-13 asm]$ ./test
```

```
1234echo Buffer overflow?
```

```
1234
```

```
[Dean@Fedora-13 asm]$ echo Buffer overflow?
```

```
Buffer overflow?
```

[Dean@Fedora-13 asm]\$I know my buffer is only 4 bytes. But is reading in 24, so is it forcing the terminal to read in the rest of the bytes? Anyone care to clear this up?

g4143 - August 15, 2010, 7:49 pm

(Aug 15, 2010 07:12 PM)GhostSniper Wrote: [\[CITE\]](#) Code section .data

```
msg: db 'Test',0
```

section .text

```
global _start
```

```

_start:
    mov ecx,msg
    mov edx,4
    call _read
    mov ecx,msg
    call _print
    call _exit
;##
;##=-Functions-=##
_read:
    mov eax,3
    mov ebx,0
    mov edx,4
    int 0x80
    RET
_print:
    mov eax,4
    mov ebx,1
    int 0x80
    RET
_exit:
    mov eax,1
    mov ebx,0
    int 0x80

```

RETEExample of what happens:

Code [Dean@Fedora-13 asm]\$ nasm -f elf template.asm -o temp.o

[Dean@Fedora-13 asm]\$ ld -s temp.o -o test

[Dean@Fedora-13 asm]\$./test

1234echo Buffer overflow?

1234

[Dean@Fedora-13 asm]\$ echo Buffer overflow?

Buffer overflow?

[Dean@Fedora-13 asm]\$I know my buffer is only 4 bytes. But is reading in 24, so is it forcing the terminal to read in the rest of the bytes? Anyone care to clear this up?

The program only reads 4 bytes into the buffer and then dumps the remainder when the program exits..Where are the extra bytes before the program exits? The bytes are maintained by the operating system or kernel and so are not considered a BOF.