

## CS0403

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:52:3e
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:523e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5627 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1730 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:394491 (385.2 KB)  TX bytes:166780 (162.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:156 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50421 (49.2 KB)  TX bytes:50421 (49.2 KB)
```

Sfruttando il tool metasploit, attraverso la vulnerabilità vsfptd sono riuscito ad aprire una shell con permessi di amministratore su una macchina target metasploitable