

# Linux Sistem Yöneticisi Cheat Sheet

Fatih T. tarafından yayımlandı

Bu yazımda sizlere Linux işletim sistemlerinde kullanılan bazı komutlardan bahsedeceğim. Bu komutları Linux sistem yöneticileri de kullanabileceği gibi siber güvenlik alanında ilgi duyan arkadaşların da bilmesi gerektiğini düşünüyorum. Bu komutları belli başlıklar altında toplayarak sizlere kolaylık sağlamaya çalıştım. Ama sizleri bir konuda uyarmak isterim. Buradaki komutların hepsi tek bir Linux dağıtımında çalışmayabilir. Kullandığınız Linux dağıtımına göre farklılık göstermesi doğaldır.

Sizler için topladığım konu başlıkları şu şekildedir:

1. **SİSTEM BİLGİSİ**
2. **DONANIM BİLGİLERİ**
3. **PERFORMANS İZLEME VE İSTATİSTİK**
4. **KULLANICI BİLGİLERİ VE YÖNETİM**
5. **DOSYA VE DİZİN KOMUTLARI**
6. **PROCESS YÖNETİMİ**
7. **DOSYA İZİNLERİ**
8. **AĞ BİLGİLERİ**
9. **ARŞİVLER (TAR DOSYALARI)**
10. **PAKETLERİN KURULUMU**
11. **ARAMA**
12. **SSH GİRİŞLERİ**
13. **DOSYA TRANSFERLERİ**
14. **DİSK KULLANIMI**
15. **DİZİN GEZİNTİSİ**

## 1 – SİSTEM BİLGİSİ

# Linux sistem bilgilerini görüntüleyin

uname -a

# Çekirdek sürüm bilgilerini görüntülemek için

uname -r

# Redhat dağıtımının sürümünü görüntülemek için

cat /etc/redhat-release

# Sistemin ne kadar süredir çalıştığını görmek isterseniz

uptime

# Sistemin hostname bilgisini görüntülemek isterseniz

hostname

# Host'un IP adresini görüntülemek isterseniz

hostname -I

# Sistem yeniden başlatma geçmişini görüntülemek için

last reboot

# Geçerli tarih ve saati görüntülemek için

date

# Bulunduğunuz ayın takvimini göster

cal

# Sistemde kimin çevrimiçi olduğunu görüntülemek için

w

# Kim olarak giriş yaptığınızı görüntülemek için

whoami

# Bir ortam değişkeni ayarlamak için kullanılacak komut

export

# Normal bir kullanıcı iseniz terminalde görünecek simge

'\$'

# Root kullanıcısı iseniz terminalde görünecek simge

'#'

## 2 – DONANIM BİLGİLERİ

# Kernel mesajlarını görüntülemek için

dmesg

# CPU bilgilerini görüntülemek için

cat /proc/cpuinfo

# RAM bilgilerini görüntülemek için

cat /proc/meminfo

# Boş ve kullanılmış belleği görüntüleyin (insan tarafından okunabilir format için -h, MB için -m, GB için -g.)

free -h

# USB cihazlarını görüntülemek için

lsusb -tv

# BIOS'tan DMI / SMBIOS'u (donanım bilgisi) görüntüleyin

dmidecode

# SDA Disk hakkında bilgileri görüntülemek için

hdparm -i /dev/sda

# SDA Disk üzerinde bir okuma hızı testi gerçekleştirmek için

hdparm -tT /dev/sda

# SDA Disk üzerinde okunamayan blokları test etmek için

badblocks -s /dev/sda

## 3 – PERFORMANS İZLEME VE İSTATİSTİK

# En önemli process'leri görüntülemek için

top

# şlemciyle ilgili istatistikleri görüntülemek için

mpstat 1

# Virtual memory istatistiklerini görüntülemek için

vmstat 1

# I/O istatistiklerini görüntülemek için

iostat 1

# Son 100 syslog mesajını görüntülemek için (Debian tabanlı sistemler için /var/log/syslog kullanın.)

tail 100 /var/log/messages

# eth0 arayüzündeki tüm paketleri yakalamak ve görüntülemek için

tcpdump -i eth0

# 80 numaralı porttaki tüm trafiği izlemek için ( HTTP )

tcpdump -i eth0 'port 80'

# Sistemdeki tüm açık dosyaları listelemek için

lsuf

# Kullanıcı tarafından açılan dosyaları listelemek için

lsuf -u <kullanıcı adı>

# Boş ve kullanılmış belleği(RAM) görüntülemek için (insan tarafından okunabilir format için -h, MB için -m, GB için -g.)

free -h

# periyodik güncellemeleri göstermek için

watch df -h

## 4 – KULLANICI BİLGİLERİ VE YÖNETİM

# Mevcut kullanıcınızın kullanıcı ve grup kimliklerini görüntülemek için

id

```
# Sisteme giriş yapan son kullanıcıları görüntülemek için
```

```
last
```

```
# Yeni bir grup oluşturmak için
```

```
groupadd <grup ismi>
```

```
# "John Smith" comment(yorum) değerine sahip john adında bir hesap oluşturun ve kullanıcının ana dizinini oluşturun.
```

```
useradd -c "John Smith" -m john
```

```
# Kullanıcı hesabı silmek için
```

```
userdel <kullanıcı ismi>
```

```
# Bir kullanıcıyı bir gruba eklemek için
```

```
usermod -aG <grup ismi> <kullanıcı ismi>
```

---

## 5 – DOSYA VE DİZİN KOMUTLARI

```
# Tüm dosyaları uzun liste (ayrıntılı) biçiminde listelemek için
```

```
ls -al
```

```
# Mevcut çalışma dizinini görüntüleyin
```

```
pwd
```

```
# Yeni bir dizin oluşturmak için
```

```
mkdir <dizin ismi>
```

```
# Dosya silmek için
```

```
rm <dosya ismi>
```

```
# Onay istemeden zorla dosyayı kaldırmak için
```

```
rm -f <dosya ismi>
```

```
# Dizini yinelemeli olarak zorla kaldırmak için
```

```
rm -rf <dizin ismi>
```

```
# dosya1'i dosya2'ye kopyala
```

```
cp dosya1 dosya2
```

```
# Boş bir dosya oluşturmak için
```

```
touch <dosya ismi>
```

```
# Dosyanın içeriğini oluşturmak için
```

```
cat <dosya ismi>
```

```
# Metin dosyasına kısaca göz atmak için
```

```
less <dosya ismi>
```

```
# Dosyanın ilk 10 satırını görüntülemek için
```

```
head <dosya ismi>
```

```
# Dosyanın son 10 satırını görüntülemek için
```

```
tail <dosya ismi>
```

```
# Dosyanın son 10 satırını görüntülemek ve dosyaya yeni satırlar eklendikçe takip etmek için
```

```
tail -f file
```

```
# önceki komutların geçmişini listelemek için
```

```
history
```

```
# Makineyi yeniden başlatmak için
```

```
reboot
```

---

## 6 – PROCESS YÖNETİMİ

```
# Şu anda çalışan process'leri görüntülemek için
```

```
ps aux
```

```
# Sistemde şu anda çalışan tüm process'leri görüntülemek için
```

```

ps -ef
# Herhangi bir process için process bilgilerini görüntüle için
-----

ps -ef | grep <process ismi>
# Bir process'i pid değerine göre sonlandırma
-----

kill <pid değeri>
# Bir process'i ismine göre sonlandırmak için
-----

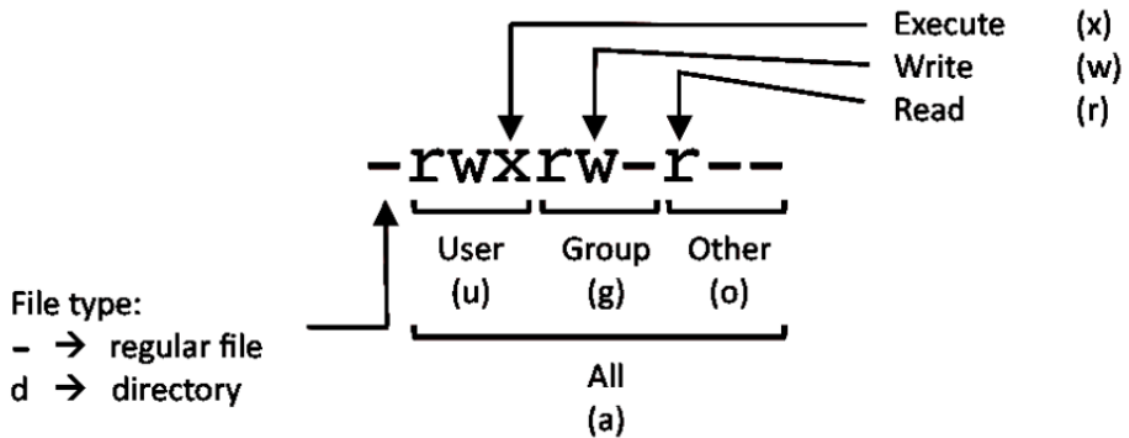
killall <process ismi>
# Durdurulan veya arka planda çalışan işleri göstermek için
-----

bg
# Mevcut çalışan işlemleri bir ağaç olarak görüntülemek için
-----

pstree

```

## 7 – DOSYA İZİNLERİ



PERMISSION	EXAMPLE
U G W	
rwX rwX rwX	chmod 777 <dosya ismi>
rwX rwX r-X	chmod 775 <dosya ismi>
rwX r-X r-X	chmod 755 <dosya ismi>
rw- rw- r--	chmod 664 <dosya ismi>
rw- r-- r--	chmod 644 <dosya ismi>

# NOT: 777 iznini mümkün oldukça az kullanmaya çalışın!

LEGEND  
 U = User  
 G = Group  
 W = World

r = Read  
 w = write  
 x = execute  
 - = no access

## 8 – AĞ BİLGİLERİ

```

# Tüm ağ arayüzlerini ve ip adresini görüntülemek için
-----

ifconfig -a
# Eth0'ın IP adresini ve ayrıntılarını göstermek için
-----

ifconfig eth0
# Network submask değerini ayarlamak için
-----

netmask
# Routing tablosuna yeni kayıtlar girmek için
-----

route
# Ağ sürücüsü ve donanım ayarlarını sorgulamak veya kontrol etmek için
-----

ethtool eth0
# ICMP echo paketleri göndermek için
-----

ping <host IP>

```

```
# Sorgulayacağınız IP adresinin whois sorgusu yapmak için
-----

whois <domain IP Adresi>

# Sorgulayacağınız IP adresinin DNS bilgilerini görüntülemek için
-----

dig <domain IP Adresi>

# Reverse lookup of IP_ADDRESS
-----

dig -x IP_ADDRESS

# tcp ve udp bağlantı noktalarını ve ilgili programları görüntülemek için
-----

netstat -nutlp
```

---

## 9 – ARŞİVLER (TAR DOSYALARI)

```
# Dizini içeren "archive.tar" adlı tar dosyası oluşturun oluşturmak için
-----

tar cf archive.tar <dizin ismi>

# .tar uzantılı dosyayı çıkarmak için
-----

tar xf <tar uzantılı dosya ismi>
```

---

## 10 – PAKETLERİN KURULUMU

```
# Anahtar kelimeye göre bir paket aramak için
-----

yum search <anahtar kelime>

# Bir package yüklemek için
-----

yum install <package ismi>

# Paket hakkında açıklama ve özet bilgileri görüntülemek için
-----

yum info <package ismi>

# Paketi kaldırmak için
-----

yum remove <package ismi>
```

---

## 11 – ARAMA

```
# Dosya içinde bir kelime aramak için
-----

grep <aranacak kelime> <dosya ismi>

# Bir kelimeyi dizin içinde aramak için
-----

grep -r <aranacak kelime> <dizin ismi>

# Dosya ve dizin bulmak için
-----

locate <dosya ismi>

# "/home/john" dizini içinde "örnek" ile başlayan dosyaları bulmak için
-----

find /home/john -name 'örnek*'
```

---

## 12 – SSH GİRİŞLERİ

```
# Kullanıcı adı ile ssh bağlantısı kurmak için
-----

ssh <host>

# Bir kullanıcı olarak sisteme ssh bağlantısı ile bağlanmak için
-----

ssh user@host

# Özel bir port kullanarak ssh bağlantısı kurmak için
-----

ssh -p port user@host

# public/private anahtar çifti üretmek için
-----

ssh-keygen
```

---

## 13 – DOSYA TRANSFERLERİ

```
# file.txt sunucudaki /tmp klasörüne güvenli olarak kopyalamak için
-----
```

```
scp file.txt server:/tmp
```

---

## 14 – DİSK KULLANIMI

```
# Dosya sisteminde boş alanı görüntülemek için
```

```
df -h
```

```
# Disk bölümlerini görüntülemek için
```

```
fdisk -l
```

```
# Tüm dosyalar ve dizinler için disk kullanımını okunabilir formatta görüntülemek için
```

```
du -ah
```

```
# Geçerli dizindeki toplam disk kullanımını göstermek için
```

```
du -sh
```

---

## 15 – DİZİN GEZİNTİ

```
# Dizinden bir seviye yukarı çıkmak için
```

```
cd ..
```

```
# $HOME dizinine gitmek için
```

```
cd
```

```
# Sistem çapında konfigürasyon dosyaları burada bulunur
```

```
/etc
```

```
# Kullanıcı hesap bilgileri burada bulunur
```

```
/etc/passwd
```

```
# Şifrelerin gerçekte tutulduğu yer
```

```
/etc/shadow
```

```
# Syslog kayıtlarının tutulduğu yer
```

```
/etc/syslog.conf
```

```
# Log dosyalarının tutulduğu yer
```

```
/var/log
```

```
# Host yapılandırılmasının yapıldığı yer
```

```
/etc/hosts
```

```
# Network bilgilerinin tutulduğu yer
```

```
/etc/networks
```

---

Buraya kadar olan kısımda elimden geldiğince fazla noktaya değinmeye çalıştım. Aslında biraz Linux komutlarını tanıtmış gibi olduk ama hepsi Linux sistem yöneticisinin hakim olması gereken komutlardır. Umarım sizler için bir faydası olmuştur.

Şimdiden okuyan herkese teşekkür ederim. Bir sonraki yazımda görüşmek üzere 😊