

Sistem İzleme

- Disk durumu
- Ram durumu
- CPU durumu
- Ağ durumu

Disk Durumu

- Kullanılan diskin durumunu görmek için **df** komutu kullanılmaktadır.
- Anlaşılır çıktı için -h parametresi kullanılabilir.

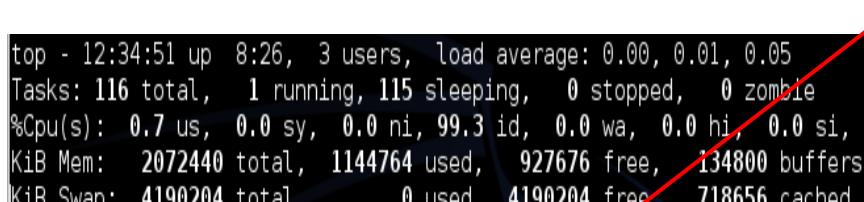
```
root@kali:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
n
rootfs          243G  15G  216G  7% /
udev             10M    0   10M  0% /dev
tmpfs            203M  564K  202M  1% /run
/dev/disk/by-uuid/24e3b18e-4f91-4663-838b-0d34a7c0b4dd  243G  15G  216G  7% /
tmpfs            5.0M    0   5.0M  0% /run/lock
tmpfs            1.2G  560K  1.2G  1% /run/shm
root@kali:~#
```

RAM Durumu

- RAM durumunu görebilmek için **top** komutu çıktısına veya /proc/meminfo dosyasına bakılır.

```
root@kali:~# head -n 24 /proc/meminfo
MemTotal:       2072440 kB
MemFree:        941752 kB
Buffers:        134760 kB
Cached:         718732 kB
SwapCached:      0 kB
Active:          522656 kB
Inactive:        521020 kB
Active(anon):   190220 kB
Inactive(anon): 840 kB
Active(file):   332436 kB
Inactive(file): 520180 kB
Unevictable:     0 kB
Mlocked:         0 kB
HighTotal:      1185672 kB
HighFree:        268940 kB
LowTotal:        886768 kB
LowFree:         672812 kB
SwapTotal:      4190204 kB
SwapFree:        4190204 kB
Dirty:            52 kB
Writeback:        0 kB
AnonPages:      190200 kB
Mapped:          56740 kB
Shmem:           880 kB
root@kali:~#
```

Ram sütunu



PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1882	root	20	0	34924	4132	3392	S	0.3	0.2	0:18.35	vmtoolsd
3746	root	20	0	75832	17m	10m	S	0.3	0.9	0:24.16	gnome-terminal
21832	root	20	0	4444	1416	1048	R	0.3	0.1	0:00.08	top
1	root	20	0	2280	728	628	S	0.0	0.0	0:01.39	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:01.12	ksoftirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
7	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/u:0H
8	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
9	root	20	0	0	0	0	S	0.0	0.0	0:00.03	rcu_bh
10	root	20	0	0	0	0	S	0.0	0.0	0:02.03	rcu_sched
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.13	watchdog/0

CPU Durumu

- CPU durum analizi için iki farklı komut kullanılabilir. Bunlar **vmstat** ve **top** komutlarıdır.
- Ayrıca /proc/cpuinfo dosyası ile CPU durumu hakkında bilgi alınabilir.

CPU Durumu

- Vmstat, sistem açılışından çalıştırıldığı ana kadar geçen süre içerisindeki CPU faaliyetleri hakkında bilgi veren bir komuttur.
- Çalışan, kuyrukta bekleyen kernel threadler, diskler, sistem çağrıları ve CPU aktivitesi ile ilgili istatistiki bilgi verir.
- Kullanımı : vmstat [options] [delay] [count]
- Burada delay parametresi kaç saniyede bir rapor üretileceği, count parametresi ise bu raporun ekrana kaç defa basılacağını ifade eder.

CPU Durumu

```
root@kali:~# vmstat 2 5
procs -----memory----- swap-----io----- system-----cpu-----
 r b swpd   free   buff   cache   si   so    bi    bo   in   cs us sy id wa
 0 0      0 1588864 35560 289316   0   0    92    15   65 193 3 1 94 2
 0 0      0 1588848 35568 289316   0   0     0    12   46 139 0 0 100 0
 0 0      0 1588848 35568 289316   0   0     0     0   38 120 0 0 100 0
 0 0      0 1588848 35568 289316   0   0     0     0   42 127 1 0 99 0
 0 0      0 1588848 35568 289316   0   0     0     0   38 118 1 0 100 0
root@kali:~# █
```

- **Process Bölümü**

- r (Running): Çalıştırılmayı bekleyen proseslerin sayısını gösterir. Tek işlemcisi olan sistemlerde bu değerin 5 ten küçük olması gereklidir.
- b (Blocking): Askıya alınmış proseslerin sayısını gösterir. Sağlıklı çalışan sistemlerde bu değerin '0' olması gereklidir.

- **Memory Bölümü**

- swpd : Kullanılan sanal belleğin miktarını gösterir.
- free : Kullanılmayan bellek alanını gösterir.
- buff : Tampon olarak kullanılan bellek miktarını gösterir.
- cache : Ön bellek olarak kullanılan bellek miktarını gösterir.

CPU Durumu

- **Swap Bölümü**

- si (swap in) : Swap alanına dahil edilen bellek miktarını gösterir.
- so (swap out): Swap ile değiş tokuş edilen bellek miktarını gösterir.

- **io Bölümü**

- bi (blocks in) : Blok aygıtından gelen bloğu gösterir.
- bo (blocks out): Blok aygıta gönderilen bloğu gösterir.

- **System Bölümü**

- in : Saniyede gerçekleşen ortalama kesme sayısını gösterir.
- cs: Saniye başına ortam anahtarlarının sayısını gösterir.

- **Cpu Bölümü**

- us (user) : Çekirdek harici kullanıcı işlemlerinin harcadığı CPU miktarı.
- sy (system): Çekirdeğin harcadığı CPU miktarını gösterir.
- id (idle) : Boş olan CPU miktarı hakkında bilgi verir.
- wa (wait) : I/O işlemleri için harcanan CPU miktarını gösterir.

CPU Durumu

- Top komutu kullanılarak da CPU gözlemlenebilir.

```
top - 05:10:47 up 1:36, 2 users, load average: 0.00, 0.01, 0.05
Tasks: 115 total, 1 running, 114 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 0.3 sy, 0.0 ni, 99.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2072440 total, 484808 used, 1587632 free, 35764 buffers
KiB Swap: 4190204 total, 0 used, 4190204 free, 289460 cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 1 root 20 0 2280 728 628 S 0.3 0.0 0:01.92 init
1930 root 20 0 34924 4132 3392 S 0.3 0.2 0:05.06 vmtoolsd
3270 root 20 0 72220 23m 17m S 0.3 1.2 0:12.98 vmtoolsd
 2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
 3 root 20 0 0 0 0 S 0.0 0.0 0:00.27 ksoftirqd/0
 5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
 7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/u:0H
 8 root rt 0 0 0 S 0.0 0.0 0:00.00 migration/0
 9 root 20 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
10 root 20 0 0 0 S 0.0 0.0 0:00.75 rcu_sched
11 root rt 0 0 0 S 0.0 0.0 0:00.02 watchdog/0
12 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 cpuset
```

- CPU, RAM ve SWAP bilgilerini ekrana döker.
- Sistem üzerindeki iş yükünü gösterir.
- Sistemin ne zamandır açık olduğunu gösterir.
- Ayrıca kaç kullanıcının aktif olduğu, kaç adet prosesin çalıştığı gibi bilgileri de gösterir.

Ağ durumu

- Ağ durum analizi için **netstat** komutu kullanılmaktadır.
- Netstat ağ istatistikleri, yönlendirme tablosu, aktif ve pasif bağlantılar vb. birçok veriyi kullanıcıya sunmaktadır.
- Kullanımı: netstat [seçenekler]
- -s parametresi ile ağ istatistikleri, --route parametresi ile yönlendirme tablosunu, -t parametresi ile tcp bağlantılarını vb. birçok ağ durumunu göstermektedir.



Ağ durumu

- Ağ durumu gösteren ekran görüntülerini söyledir:

```
root@kali:~# netstat --route
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
default         192.168.168.2  0.0.0.0       UG        0 0          0 eth0
192.168.0.0    *              255.255.255.0 U          0 0          0 eth0
```

Yönlendirme tablosu

```
root@kali:~# netstat -s
Ip:
 709 total packets received
 0 forwarded
 0 incoming packets discarded
 706 incoming packets delivered
 516 requests sent out
Icmp:
 1 ICMP messages received
 0 input ICMP message failed.
 ICMP input histogram:
   echo requests: 1
  1 ICMP messages sent
  0 ICMP messages failed
 ICMP output histogram:
   echo replies: 1
IcmpMsg:
  InType8: 1
  OutType0: 1
Tcp:
 82 active connections openings
 0 passive connection openings
 50 failed connection attempts
```

Ağ istatistikleri

```
root@kali:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address      State
tcp      0      0 0.0.0.0:21                0.0.0.0:*           LISTEN
tcp      0      0 192.168.168.131:56401    173.194.39.198:443  ESTABLISHED
tcp      0      0 192.168.168.131:40627    77.223.146.101:80  ESTABLISHED
tcp      0      0 192.168.168.131:40631    77.223.146.101:80  ESTABLISHED
tcp      0      0 192.168.168.131:34054    83.66.162.80:80    ESTABLISHED
tcp      0      0 192.168.168.131:40626    77.223.146.101:80  ESTABLISHED
tcp      0      0 192.168.168.131:53217    173.194.39.243:80  ESTABLISHED
tcp      0      0 192.168.168.131:57374    173.194.39.224:80  ESTABLISHED
tcp      0      1 192.168.168.131:54077    68.232.35.139:80   SYN_SENT
tcp      0      0 192.168.168.131:55291    193.28.225.212:80  ESTABLISHED
tcp      0      1 192.168.168.131:52795    95.100.223.139:80  SYN_SENT
tcp      0      0 192.168.168.131:59768    83.66.162.45:80    ESTABLISHED
tcp      0      1 192.168.168.131:52796    95.100.223.139:80  SYN_SENT
```

TCP bağlantıları

Ağ durumu

- Aktif ağ servisleri aşağıdaki gibi görüntülenebilir.
 - TCP

```
root@kali:~# netstat -ant | grep LISTEN
tcp      0      0 0.0.0.0:21          0.0.0.0:*
tcp6     0      0 :::80              ::::*                LISTEN
root@kali:~#
```

- UDP

```
root@kali:~# netstat -anu | grep -i UDP
udp      0      0 0.0.0.0:7546        0.0.0.0:*
udp      0      0 0.0.0.0:68        0.0.0.0:*
udp6     0      0 :::62499         ::::*                
```