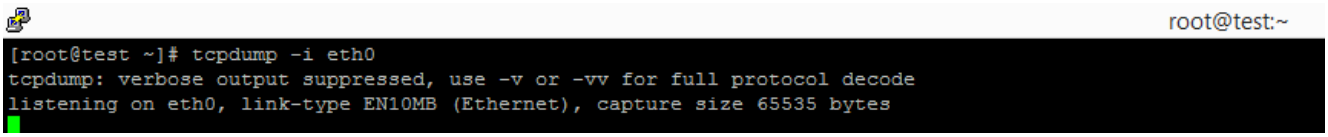
Command umum monitoring server berbasis linux

Halo, kali ini akan dibahas tentang command umum yang biasa digunakan untuk memantau kondisi server, seperti mengecek kapasitas hdd, ram, dan jaringan, dan sebagainya.

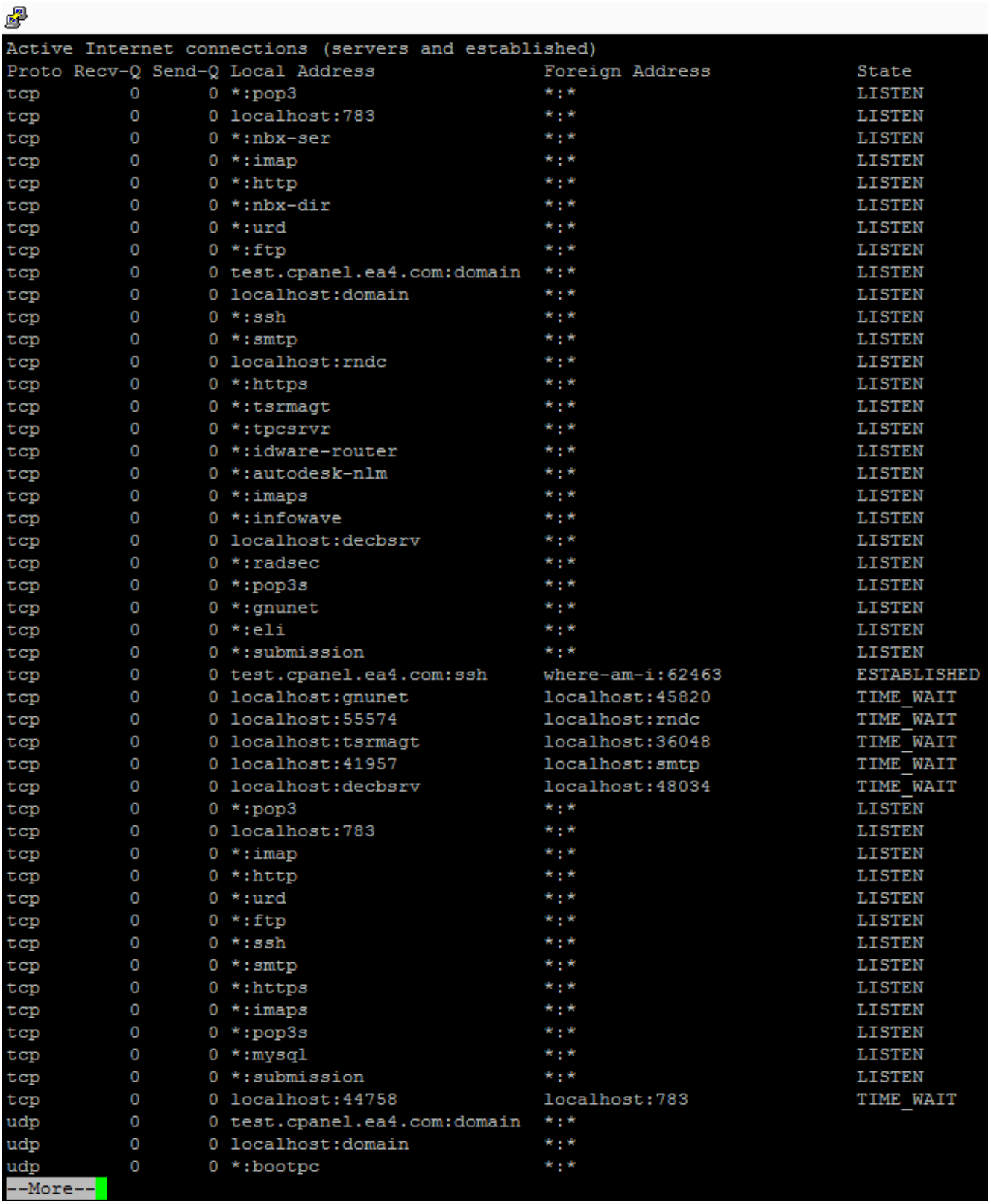
Pertama adalah command **tcpdump -i xxx , contoh : tcpdump -i eth0 (interface internet card kalian, dalam contoh ini interfacenya adalah eth0)** . Tcpdump sendiri adalah command yang umum digunakan untuk mengetahui paket jaringan kalian / dalam hal ini untuk mengetahui lalu lintas paket TCP/IP yang dikirim atau diterima oleh interface jaringan kalian.

Contoh nya adalah sebagai berikut :



Kedua adalah command netstat : **netstat -a | more ,** atau network statistics. Gampangnya, command ini berguna untuk memonitor statistik dari paket jaringan yang masuk dan keluar. Command ini mirip dengan command windows yang juga menggunakan netstat untuk memonitor jaringannya. Dan command ini juga berguna bagi sysadmin jika ada gangguan koneksi jaringan sehingga para sysadmin bisa melihat network mana yang bermasalah / error.

Contohnya adalah sebagai berikut :



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:pop3                      *:*                         LISTEN
tcp        0      0 localhost:783               *:*                         LISTEN
tcp        0      0 *:nbx-ser                   *:*                         LISTEN
tcp        0      0 *:imap                      *:*                         LISTEN
tcp        0      0 *:http                      *:*                         LISTEN
tcp        0      0 *:nbx-dir                   *:*                         LISTEN
tcp        0      0 *:urd                       *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 test.cpanel.ea4.com:domain  *:*                         LISTEN
tcp        0      0 localhost:domain            *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:smtp                      *:*                         LISTEN
tcp        0      0 localhost:rndc              *:*                         LISTEN
tcp        0      0 *:https                     *:*                         LISTEN
tcp        0      0 *:tsrmagt                   *:*                         LISTEN
tcp        0      0 *:tpcsrvr                   *:*                         LISTEN
tcp        0      0 *:idware-router             *:*                         LISTEN
tcp        0      0 *:autodesk-nlm              *:*                         LISTEN
tcp        0      0 *:imaps                     *:*                         LISTEN
tcp        0      0 *:infowave                  *:*                         LISTEN
tcp        0      0 localhost:decbsrv           *:*                         LISTEN
tcp        0      0 *:radsec                    *:*                         LISTEN
tcp        0      0 *:pop3s                     *:*                         LISTEN
tcp        0      0 *:gnunet                    *:*                         LISTEN
tcp        0      0 *:eli                       *:*                         LISTEN
tcp        0      0 *:submission                *:*                         LISTEN
tcp        0      0 test.cpanel.ea4.com:ssh     where-am-i:62463            ESTABLISHED
tcp        0      0 localhost:gnunet            localhost:45820             TIME_WAIT
tcp        0      0 localhost:55574             localhost:rndc              TIME_WAIT
tcp        0      0 localhost:tsrmagt           localhost:36048             TIME_WAIT
tcp        0      0 localhost:41957             localhost:smtp              TIME_WAIT
tcp        0      0 localhost:decbsrv           localhost:48034             TIME_WAIT
tcp        0      0 *:pop3                      *:*                         LISTEN
tcp        0      0 localhost:783               *:*                         LISTEN
tcp        0      0 *:imap                      *:*                         LISTEN
tcp        0      0 *:http                      *:*                         LISTEN
tcp        0      0 *:urd                       *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:smtp                      *:*                         LISTEN
tcp        0      0 *:https                     *:*                         LISTEN
tcp        0      0 *:imaps                     *:*                         LISTEN
tcp        0      0 *:pop3s                     *:*                         LISTEN
tcp        0      0 *:mysql                     *:*                         LISTEN
tcp        0      0 *:submission                *:*                         LISTEN
tcp        0      0 localhost:44758             localhost:783               TIME_WAIT
udp        0      0 test.cpanel.ea4.com:domain  *:*
udp        0      0 localhost:domain            *:*
udp        0      0 *:bootpc                    *:*
--More--
```

Ketiga adalah command **df** , : command ini berfungsi untuk melihat kapasitas hdd pada server, mengenai command ini, banyak variasinya, namun yang umum digunakan adalah command **df -h**

Contohnya adalah sebagai berikut :

```
[root@test ~]# df
Filesystem     1K-blocks    Used Available Use% Mounted on
/dev/vda5       46674904 7464312  36832968  17% /
tmpfs             506928    6648    500280   2% /dev/shm
/dev/vda1         991512   30512    909800   4% /boot
/dev/vda2        9948012   22520   9413492   1% /tmp
[root@test ~]#
```

```
[root@test ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda5        45G  7.2G   36G  17% /
tmpfs           496M  6.5M  489M   2% /dev/shm
/dev/vda1       969M   30M  889M   4% /boot
/dev/vda2       9.5G   22M  9.0G   1% /tmp
[root@test ~]#
```

Keempat adalah command **free** : command ini berfungsi untuk melihat kapasitas ram pada server, dan untuk command free sendiri sama seperti command **df ,** command ini juga banyak variasinya, namun untuk memudahkan melihat sisa ram pada server, bisa menggunakan command **free -h**

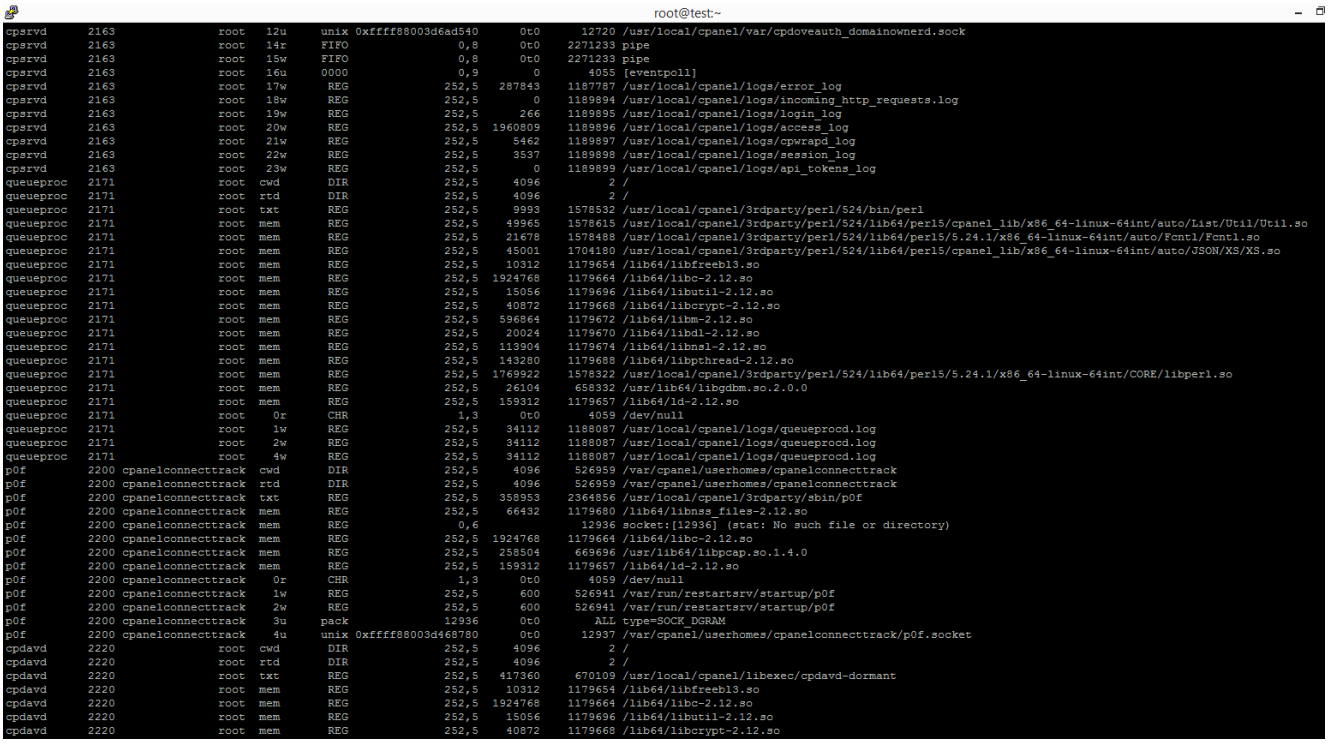
Contohnya adalah sebagai berikut :

```
[root@test ~]# free
             total       used       free     shared    buffers     cached
Mem:       1013860     897408     116452       6920      75164     457452
-/+ buffers/cache:     364792     649068
Swap:      4095996      79920    4016076
[root@test ~]#
```

```
[root@test ~]# free -h
             total       used       free     shared    buffers     cached
Mem:          990M       876M       113M       6.8M        73M       446M
-/+ buffers/cache:       356M       633M
Swap:         3.9G        78M       3.8G
[root@test ~]#
```

Kelima adalah command **lsof :** command ini berfungsi untuk melihat file yang terbuka didalam sistem / server. Seperti proses apa dan di folder apa. Command ini juga sangat berfungsi untuk mengetahui jika ada user / folder yang mencurigakan, yang kemungkinan adalah malware, serta untuk melihat user dengan proses apa yang paling memberatkan server.

Contohnya adalah sebagai berikut :



Ya demikian beberapa command umum yang digunakan untuk memonitor server kalian yang berbasis linux, jika ada kekurangan dalam informasi yang diberikan, silahkan googling atau cari refrensi di forum