

# **PRAKTIKUM PENGELOLAAN PROSES DI LINUX DAN WINDOWS**

**Nama : Najla Permata Nugroho**

**NIM : 0920240007**

**Kelas : TRPL 1B**

## **Tujuan Praktikum**

1. Memahami konsep pengelolaan proses pada sistem operasi Linux dan Windows.
2. Mampu melihat daftar proses yang berjalan.
3. Mampu mengirim sinyal dan menghentikan proses.
4. Mampu mengubah prioritas proses.
5. Mampu menerapkan konsep message passing melalui pipelining dan redirecting.

## **Catatan:**

**Screenshot untuk setiap hasil praktikum/soal yang dikerjakan.**

---

## **I. Percobaan di Linux**

### **1. Melihat Proses yang Berjalan**

1. Jalankan terminal.
2. Gunakan perintah berikut untuk melihat daftar proses:

**ps aux**

## pgrep nano

```
najela@najela:~$ nano &
[1] 1065
najela@najela:~$ pgrep nano
1065

[1]+  Stopped                  nano
najela@najela:~$
```

catatan: nano adalah text editor linux

### Soal:

- Apa perbedaan output antara ps aux dan top?

#### ps aux :

- Sifat outputnya berupa statis
- langsung selesai setelah eksekusi
- cocok buat cek kondisi proses yang sekali waktu

#### top :

- Sifat outputnya real time
- Buat keluarnya harus klik huruf "q" dulu
- Cocoknya buat yang bisa mantau prosesnya yang berubah terus menerus

- Bagaimana cara menampilkan proses yang dimulai oleh user tertentu saja?

```
najela@najela:~$ ps -u najela
  PID TTY          TIME CMD
 1030 ?                00:00:00 systemd
 1031 ?                00:00:00 (sd-pam)
 1040 tty1            00:00:00 bash
 1197 tty1            00:00:00 ps
```

- Bandingkan hasil ps aux dengan htop. Apa kelebihan htop dibanding ps aux?

#### ps aux :

- Output dari ps aux bisa ditampilkan dengan berdasarkan kata kunci yang menggunakan grep, agar hanya terlihat proses yang sesuai dengan apa yang ingin dicari
- Cocok untuk melihat daftar semua proses secara cepat dalam satu waktu saja

#### htop :

- Tampilan lebih berwarna

→ Navigasinya bisa menggunakan keyboard

→ Bisa langsung kill, renice, dan filter proses dari interface tanpa perlu untuk mengetik secara manual

```
0[
3[
3[
3[
Mem[|||||]
Swap[
Main[
CPU
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
1 root 20 0 22876 12760 9952 S 0.0 0.0 0:01.04 /sbin/init
339 root 19 -1 50440 15164 14168 S 0.0 0.0 0:00.17 /usr/lib/systemd/systemd-journald
392 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.02 /sbin/mtiocthd -B -S
410 root 20 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
411 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
412 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
413 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
414 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
415 root RT 0 282M 27136 8576 S 0.0 1.3 0:00.00 /sbin/mtiocthd -d -S
416 root 20 0 29060 7680 4864 S 0.0 0.4 0:00.03 /usr/lib/systemd/systemd-udevd
576 systemd 20 0 16992 9344 8320 S 0.0 0.5 0:00.06 /usr/lib/systemd/systemd-networkd
628 systemd 20 0 21576 13800 10624 S 0.0 0.6 0:00.14 /usr/lib/systemd/systemd-resolved
634 systemd 20 0 91820 7080 6912 S 0.0 0.4 0:00.06 /usr/lib/systemd/systemd-timesyncd
729 systemd 20 0 91820 7080 6912 S 0.0 0.4 0:00.00 /usr/lib/systemd/systemd-timesyncd
758 systemd 20 0 4772 5240 4400 S 0.0 0.3 0:00.00 edbus-daemon --system --address=systemd: --nofork --noptfile --systemd-activation --syslog=0
763 polkitd 20 0 3748 3548 7296 S 0.0 0.5 0:00.11 /usr/lib/polkit-1/polkitd --no-debug
768 root 20 0 17988 8704 7680 S 0.0 0.4 0:00.07 /usr/lib/systemd/systemd-logind
770 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
784 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
790 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
792 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
799 root 20 0 107M 22312 13568 S 0.0 1.1 0:00.28 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
802 syslog 20 0 217M 5888 4400 S 0.0 0.3 0:00.07 /usr/sbin/rsyslogd -n -iNONE
808 polkitd 20 0 3748 3548 7296 S 0.0 0.5 0:00.00 /usr/lib/polkit-1/polkitd --no-debug
809 polkitd 20 0 3748 3548 7296 S 0.0 0.5 0:00.00 /usr/lib/polkit-1/polkitd --no-debug
818 polkitd 20 0 3748 3548 7296 S 0.0 0.5 0:00.00 /usr/lib/polkit-1/polkitd --no-debug
822 root 20 0 382M 12544 10624 S 0.0 0.6 0:00.11 /usr/sbin/ModemManager
832 syslog 20 0 217M 5888 4400 S 0.0 0.3 0:00.00 /usr/sbin/rsyslogd -n -iNONE
834 syslog 20 0 217M 5888 4400 S 0.0 0.3 0:00.00 /usr/sbin/rsyslogd -n -iNONE
835 syslog 20 0 217M 5888 4400 S 0.0 0.3 0:00.00 /usr/sbin/rsyslogd -n -iNONE
838 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
840 root 20 0 382M 12544 10624 S 0.0 0.6 0:00.00 /usr/sbin/ModemManager
845 root 20 0 382M 12544 10624 S 0.0 0.6 0:00.00 /usr/sbin/ModemManager
845 root 20 0 382M 12544 10624 S 0.0 0.6 0:00.00 /usr/sbin/ModemManager
853 root 20 0 457M 13312 11264 S 0.0 0.7 0:00.00 /usr/libexec/udisks2/udisksd
870 root 20 0 107M 22312 13568 S 0.0 1.1 0:00.00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
882 root 20 0 6824 3688 1568 S 0.0 0.1 0:00.01 /usr/sbin/cron -f -P
901 root 20 0 7084 4736 3768 S 0.0 0.2 0:00.03 /bin/login -p --
1030 root 20 0 20348 11520 7472 S 0.0 0.6 0:00.15 /usr/lib/systemd/systemd --user
```

## 2. Mengirimkan Sinyal ke Proses

1. Jalankan proses berikut di background:

**sleep 100 &**

2. Gunakan perintah berikut untuk melihat PID dari proses sleep:

**ps aux | grep sleep**

3. Kirim sinyal SIGSTOP untuk menghentikan sementara proses:

**kill -STOP <PID>**

4. Lanjutkan kembali proses yang dihentikan:

**kill -CONT <PID>**

```

najela@najela:~$ sleep 100 &
[2] 1439
najela@najela:~$ ps aux | grep sleep
najela      1439  0.0  0.0   5684  1920 tty1      S   04:17   0:00 sleep 100
najela      1441  0.0  0.1   6544  2304 tty1      S+  04:18   0:00 grep --color=auto sleep
najela@najela:~$ kill -STOP 1439
najela@najela:~$ ps aux | grep sleep
najela      1439  0.0  0.0   5684  1920 tty1      T   04:17   0:00 sleep 100
najela      1444  0.0  0.1   6544  2304 tty1      S+  04:19   0:00 grep --color=auto sleep
[2]+  Stopped                  sleep 100
najela@najela:~$ kill -CONT 1439
najela@najela:~$ ps aux | grep sleep
najela      1446  0.0  0.1   6544  2304 tty1      S+  04:19   0:00 grep --color=auto sleep
[2]-  Done                    sleep 100

```

### Soal:

- Jika sleep 100 & dijalankan tanpa &, apakah perbedaannya?

```

najela@najela:~$ sleep 100

```

→ Kalau yang menggunakan "&" itu prosesnya akan berjalan di background, terminalnya langsung bisa dipakai untuk perintah yang lain

→ Kalau yang tidak menggunakan "&" it prosesnya akan berjalan di foreground (terminalnya akan diam sampai selesai)

- Apa perbedaan antara SIGSTOP, SIGTERM, dan SIGKILL?

→ SIGSTOP : untuk menghentikan prosesnya untuk sementara (pause) dan prosesnya tidak bisa menolak

→ SIGTERM : untuk meminta proses supaya berhentinya dengan sopan (prosesnya bisa menangani atau mengabaikan)

→ SIGKILL : untuk memaksa proses berheti

- Bagaimana cara mengirim sinyal SIGINT ke proses tanpa mengetahui PID-nya?

→ Bisa menggunakan perintah "pkill" atau "pkill -SIGINT nama\_proses", pkill bakal mencari proses berdasarkan dengan namanya, jadi ga perlu menggunakan PID, perintah tersebut bakal ngirim sinyal SIGINT (sinyal interrupt, sama kayak kita klik Ctrl+C) ke semua proses dengan nama yang sesuai

## 3. Mematikan Proses

1. Jalankan gedit di terminal:

gedit

## 2. Cari PID dari gedit:

pgrep gedit

```
najela@najela:~$ pgrep nano
1056
```

## 3. Hentikan proses gedit:

kill <PID>

```
najela@najela:~$ kill 1056
najela@najela:~$
```

### Soal:

- Apa yang terjadi jika kill digunakan tanpa PID?  
→ Kalau kill digunakan tanpa menggunakan PID maka tidak akan jalan karena kill itu butuh untuk tahu PID nya apa
- Bagaimana cara menghentikan semua proses gedit tanpa menggunakan pgrep?  
→ Dengan menggunakan perintah "pkill gedit" jadi nanti akan langsung matiin semua proses gedit tanpa cari tahu PID nya dulu
- Mengapa kill -9 <PID> lebih efektif dibanding kill <PID>?  
→ Lebih efektif dikarenakan kill -9 <PID> akan langsung memaksa proses untuk berhenti tanpa nunggu dulu prosesnya telah melakukan shutdown dengan baik atau belum, jadi tidak bisa ditolak oleh proses

## 4. Meningkatkan Prioritas Proses

### 1. Jalankan proses gedit dengan prioritas rendah:

nice -n 10 nano

```
najela@najela:~$ nice -n 10 nano &
[1] 1051
```

### 2. Lihat prioritasnya dengan:

ps -eo pid,comm,nice | grep nano

```
najela@najela:~$ ps -eo pid,comm,nice | grep nano
1051 nano 10
[1]+ Stopped nice -n 10 nano
```

### 3. Tingkatkan prioritas proses nano:

**renice -5 -p <PID>**

```
najela@najela:~$ renice -5 -p 1051
renice: failed to set priority for 1051 (process ID): Permission denied
najela@najela:~$
```

**Soal:**

- Apa yang terjadi jika nilai nice lebih kecil dari -20?  
→ Ga akan bisa dikarenakan nilai nice yang paling kecil itu Cuma di -20 atau batas maksimal prioritas tertingginya itu -20
- Bisakah user biasa mengubah prioritas menjadi -10? Mengapa?  
→ Ga akan bisa dikarenakan cuman root yang bisa menaikkan prioritas ke nilai negatif, karena itu dibutuhkan izin dari admin
- Bagaimana cara meningkatkan prioritas semua proses yang dimiliki oleh user tertentu?  
→ Dengan menggunakan perintah renice untuk semua proses user, contohnya yaitu “sudo renice -n -10 -u username”, -n -10 itu artinya untuk menaikkan prioritas, dan -u username itu untuk semua prosesnya yaitu si pemilik user itu

## 5. Message Passing (Pipelining dan Redirecting)

1. Gunakan pipelining untuk menampilkan hanya 5 proses pertama dari daftar proses:

**ps aux | head -n 5**

```
najela@najela:~$ ps aux | head -n 5
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.3   0.6  22104 12964 ?        Ss   13:51   0:01 /sbin/init
root         2   0.0   0.0      0     0 ?        S    13:51   0:00 [kthreadd]
root         3   0.0   0.0      0     0 ?        S    13:51   0:00 [pool_workqueue_release]
root         4   0.0   0.0      0     0 ?        I<   13:51   0:00 [kworker/R-rcu_g]
```

2. Redirect output daftar proses ke dalam file:

**ps aux > daftar\_proses.txt**

**ls daftar\_proses.txt**

```
najela@najela:~$ ps aux > daftar_proses.txt
najela@najela:~$ ls daftar_proses.txt
daftar_proses.txt
```

**Soal:**

- Bagaimana cara menyimpan output ps aux ke file sekaligus tetap menampilkannya di layar?  
→ Untuk menyimpan output perintah “ps aux” ke file sekaligus tetap melihat hasilnya di layar itu bisa menggunakan perintah “tee”. Perintah “tee” itu berfungsi untuk mengambil output dari suatu perintah, lalu akan menuliskannya ke file dan tetap menampilkan ke layar, contohnya yaitu “ps aux | tee output.txt”
- Jelaskan perbedaan antara > dan >> dalam redirection.  
→ “>” adalah untuk nulis ke file, tapi kalau file yang dituju sudah ada isinya, isinya bakal diganti dari yang sebelumnya, tapi kalau belum ada akan dibuat file baru. Contohnya itu “echo “Halo” > file.txt” nah ini bakal bikin file.txt isinya cuma “Halo” aja. Kalau sebelumnya ada isi yang lain, bakal kehapus isi yang sebelumnya itu  
→ “>>” artinya itu nambahin ke bagian akhir file tanpa ngapus isi yang udah ada, mirip seperti catatan yang ga menghilangkan catatan yang lama. Contohnya itu “echo “Baris baru” >> file.txt” nah ini bakal nambahin tulisan “Baris baru” di bawah isi file.txt yang sebelumnya udah ada isinya
- Buat perintah untuk menampilkan daftar proses, menyaring yang memiliki nama bash, dan menyimpannya ke file.  
→ Menggunakan “ps aux” untuk menampilkan semua proses  
→ Menggunakan “grep” untuk mencari proses yang mengandung kata “bash”  
→ Menggunakan “tee nama\_file.txt” untuk menyimpan outputnya ke file  
→ Jadi nanti akan menggunakan perintah seperti “ps aux | grep bash | tee nama\_file.txt”

## II. Latihan Linux

1. Seorang user menjalankan perintah berikut di background:

**ping google.com > hasil.txt &**

- Apa fungsi & dalam perintah tersebut?  
→ “&” itu dipakai untuk menjalankan perintah di background, jadi terminal tetap akan bisa
- Bagaimana cara menghentikan proses ini tanpa mengetahui PID-nya?



→ Yaitu dengan menggunakan "pkill ping" (contohnya), ini akan menghentikan semua proses "ping" yang sedang berjalan

2. Anda ingin memastikan bahwa hanya satu instance nano yang berjalan. Jika ada lebih dari satu, matikan yang lain. Bagaimana perintahnya?

→ Cek dulu jumlah prosesnya dengan menggunakan perintah "pgrep nano" lalu kalau PID nya ada lebih dari satu yang keluar matikan yang lain dengan menggunakan perintah "pkill -o nano" (-O itu akan mematikan proses "nano" yang paling lama berjalan, dan akan menyisakan yang terbaru)

3. Sebuah server mengalami masalah karena load CPU terlalu tinggi. Bagaimana cara menemukan proses yang menghabiskan CPU terbanyak?

→ Yaitu dengan menggunakan perintah "top" atau "htop", setelah itu dilihat di urutan paling atas di kolom %CPU. Atau bisa juga menggunakan perintah satu baris yaitu contohnya "ps aux --sort=-%cpu | head -n 5" nah nanti akan menunjukkan 5 proses yang paling banyak memakan CPU

4. Anda menjalankan sleep 500 &, lalu menutup terminal. Apakah proses tetap berjalan? Bagaimana cara memastikan bahwa proses tetap berjalan setelah terminal ditutup?

→ Tidak berjalan, proses akan berhenti kalau terminalnya ditutup

→ Caranya yaitu dengan jalankan menggunakan "nohup" atau menggunakan "disown", nah itu perintah yang digunakan jika ingin prosesnya tetap berjalan tetapi terminalnya ditutup

5. Anda ingin melihat daftar proses yang telah berjalan lebih dari 1 jam. Bagaimana perintahnya?

→ Dengan menggunakan perintah "ps -eo pid,etime,cmd | grep -E '[0-9]+:[0-9]{2}:[0-9]{2}', nah kolom "etime" itu akan menunjukkan waktu yang berjalan

### **III. Percobaan di Windows**

#### **1. Melihat Proses yang Berjalan**

1. Buka Command Prompt atau PowerShell.
2. Gunakan perintah berikut untuk menampilkan daftar proses:

**powershell**

**tasklist**

```
PS C:\Users\userrrr> tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	1,232 K
Registry	124	Services	0	28,356 K
smss.exe	428	Services	0	152 K
csrss.exe	624	Services	0	2,100 K
wininit.exe	712	Services	0	752 K
csrss.exe	724	Console	1	4,396 K
services.exe	796	Services	0	7,748 K
lsass.exe	804	Services	0	12,012 K
winlogon.exe	884	Console	1	4,604 K
svchost.exe	1004	Services	0	25,200 K
fontdrvhost.exe	376	Console	1	5,692 K
fontdrvhost.exe	408	Services	0	552 K
svchost.exe	828	Services	0	17,040 K
svchost.exe	1048	Services	0	4,512 K
svchost.exe	1196	Services	0	10,176 K
svchost.exe	1224	Services	0	5,180 K
svchost.exe	1232	Services	0	4,576 K
svchost.exe	1308	Services	0	7,708 K
IntelCpHDCPSvc.exe	1324	Services	0	1,492 K
svchost.exe	1344	Services	0	5,592 K
svchost.exe	1404	Services	0	3,976 K
svchost.exe	1484	Services	0	3,856 K
dwm.exe	1532	Console	1	210,260 K
IntelCpHeciSvc.exe	1772	Services	0	1,680 K
svchost.exe	1796	Services	0	7,324 K
svchost.exe	1900	Services	0	9,428 K
svchost.exe	2004	Services	0	5,164 K
ibmpmsvc.exe	1392	Services	0	2,148 K
LITSSvc.exe	1416	Services	0	2,196 K
svchost.exe	2088	Services	0	7,300 K
svchost.exe	2108	Services	0	7,644 K
svchost.exe	2204	Services	0	6,836 K
svchost.exe	2228	Services	0	3,968 K
svchost.exe	2236	Services	0	5,264 K
ETDService.exe	2244	Services	0	1,404 K

3. Gunakan perintah berikut untuk melihat detail proses tertentu:

**powershell**

**tasklist | findstr notepad**

```
PS C:\Users\userrrr> tasklist | findstr notepad
notepad.exe          5472 Console          1         4,064 K
notepad.exe          2164 Console          1        10,784 K
```

## 2. Mengirimkan Sinyal ke Proses

1. Jalankan Notepad.
2. Cari PID dari Notepad dengan:

**powershell**

**tasklist | findstr notepad**

```
PS C:\Users\userrrr> tasklist | findstr notepad
notepad.exe          5472 Console          1      4,064 K
notepad.exe          2164 Console          1     10,784 K
```

### 3. Hentikan proses Notepad:

powershell

**taskkill /PID <PID>**

```
PS C:\Users\userrrr> taskkill /PID 5472
SUCCESS: Sent termination signal to the process with PID 5472.
```

### 3. Meningkatkan Prioritas Proses

1. Jalankan Notepad.
2. Ubah prioritasnya menjadi tinggi:

powershell

**wmic process where name="notepad.exe" call setpriority 128**

```
PS C:\Users\userrrr> wmic process where "name='notepad.exe'" call setpriority 128
Executing (\\NAJELA\ROOT\CIMV2:Win32_Process.Handle="5472")->setpriority()

Method execution successful.

Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
Executing (\\NAJELA\ROOT\CIMV2:Win32_Process.Handle="2164")->setpriority()

wmic :
At line:1 char:1
+ wmic process where "name='notepad.exe'" call setpriority 128
+ ~~~~~
    + CategoryInfo          : NotSpecified: (String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

Method execution successful.

Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
```

### 4. Message Passing (Pipelining dan Redirecting)

1. Gunakan pipelining untuk menampilkan hanya 5 proses pertama dari daftar proses:

powershell

**tasklist | Select-Object -First 5**

```
PS C:\Users\userrrr> tasklist | Select-Object -First 5
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	1,232 K

## 2. Redirect output daftar proses ke dalam file:

powershell

tasklist > daftar\_proses.txt

## IV. Latihan di Windows

1. Tampilkan hanya proses yang dijalankan oleh user tertentu.

Microsoft Windows [Version 10.0.19045.5608]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\userrrr>tasklist /FI "USERNAME eq userrrr"

Image Name	PID	Session Name	Session#	Mem Usage
ETDCtrl.exe	4680	Console	1	6,196 K
sihost.exe	6700	Console	1	23,024 K
svchost.exe	6748	Console	1	14,172 K
igfxEM.exe	6804	Console	1	5,672 K
svchost.exe	6812	Console	1	30,220 K
taskhostw.exe	6916	Console	1	15,296 K
PowerMgr.exe	6928	Console	1	4,164 K
ctfmon.exe	4048	Console	1	32,548 K
explorer.exe	7280	Console	1	198,948 K
svchost.exe	8188	Console	1	17,356 K
StartMenuExperienceHost.e	8532	Console	1	82,228 K
RuntimeBroker.exe	8812	Console	1	19,888 K
SearchApp.exe	9092	Console	1	271,164 K
RuntimeBroker.exe	9328	Console	1	23,384 K
igfxext.exe	10976	Console	1	4,584 K
svchost.exe	10172	Console	1	18,612 K
RuntimeBroker.exe	11900	Console	1	21,748 K
TextInputHost.exe	12252	Console	1	15,104 K
SecurityHealthSystray.exe	7452	Console	1	3,508 K
dllhost.exe	1884	Console	1	10,612 K
msedge.exe	12008	Console	1	143,424 K
msedge.exe	5672	Console	1	2,932 K
msedge.exe	12428	Console	1	35,416 K
msedge.exe	12436	Console	1	31,332 K
msedge.exe	12560	Console	1	6,444 K
Discord.exe	13912	Console	1	47,092 K
Discord.exe	13180	Console	1	2,548 K
Discord.exe	13744	Console	1	12,260 K
Discord.exe	13864	Console	1	20,120 K
CompPkgSrv.exe	14132	Console	1	4,220 K
Discord.exe	14376	Console	1	118,164 K
Lightshot.exe	15120	Console	1	2,240 K
ms-teams.exe	15356	Console	1	38,048 K
Discord.exe	7644	Console	1	8,264 K
ShellExperienceHost.exe	2052	Console	1	31,620 K
RuntimeBroker.exe	15584	Console	1	21,428 K
RuntimeBroker.exe	15644	Console	1	1,952 K
RtkAudUService64.exe	15692	Console	1	2,220 K
msedgewebview2.exe	16296	Console	1	59,812 K
msedgewebview2.exe	16316	Console	1	2,160 K
msedgewebview2.exe	14516	Console	1	23,652 K
msedgewebview2.exe	15080	Console	1	67,344 K
msedgewebview2.exe	2792	Console	1	6,116 K
msedgewebview2.exe	10556	Console	1	307,028 K
ms-teams.exe	16480	Console	1	38,508 K

2. Cari PID dari proses chrome.exe.
3. Hentikan semua proses chrome.exe.



```

C:\Users\userrrr>tasklist | findstr chrome.exe
chrome.exe      11740 Console           1      192,812 K
chrome.exe      9368 Console           1         2,780 K
chrome.exe     10860 Console           1     154,408 K
chrome.exe     10876 Console           1      46,552 K
chrome.exe     10504 Console           1       9,296 K
chrome.exe      6020 Console           1      11,500 K
chrome.exe      5280 Console           1       8,512 K
chrome.exe      8792 Console           1     42,268 K
chrome.exe      1092 Console           1      74,812 K
chrome.exe     23240 Console           1       4,584 K
chrome.exe      4420 Console           1       4,924 K
chrome.exe     14704 Console           1     284,552 K
chrome.exe     25288 Console           1      34,464 K
chrome.exe     27236 Console           1     42,080 K
chrome.exe     27384 Console           1     49,612 K
chrome.exe     13724 Console           1    357,004 K
chrome.exe     20196 Console           1     75,640 K
chrome.exe     17348 Console           1     28,812 K
chrome.exe     17516 Console           1     50,156 K

C:\Users\userrrr>taskkill /IM chrome.exe /F
SUCCESS: The process "chrome.exe" with PID 11740 has been terminated.
SUCCESS: The process "chrome.exe" with PID 9368 has been terminated.
SUCCESS: The process "chrome.exe" with PID 10860 has been terminated.
SUCCESS: The process "chrome.exe" with PID 10876 has been terminated.
SUCCESS: The process "chrome.exe" with PID 10504 has been terminated.
SUCCESS: The process "chrome.exe" with PID 6020 has been terminated.
SUCCESS: The process "chrome.exe" with PID 5280 has been terminated.
SUCCESS: The process "chrome.exe" with PID 8792 has been terminated.
SUCCESS: The process "chrome.exe" with PID 1092 has been terminated.
SUCCESS: The process "chrome.exe" with PID 23240 has been terminated.
SUCCESS: The process "chrome.exe" with PID 4420 has been terminated.
SUCCESS: The process "chrome.exe" with PID 14704 has been terminated.
SUCCESS: The process "chrome.exe" with PID 25288 has been terminated.
SUCCESS: The process "chrome.exe" with PID 27236 has been terminated.
SUCCESS: The process "chrome.exe" with PID 27384 has been terminated.
SUCCESS: The process "chrome.exe" with PID 13724 has been terminated.
SUCCESS: The process "chrome.exe" with PID 20196 has been terminated.
SUCCESS: The process "chrome.exe" with PID 17348 has been terminated.

```

4. Hentikan proses firefox.exe secara paksa.

```

C:\Users\userrrr>taskkill /IM firefox.exe /F
SUCCESS: The process "firefox.exe" with PID 13580 has been terminated.
SUCCESS: The process "firefox.exe" with PID 14304 has been terminated.
SUCCESS: The process "firefox.exe" with PID 24024 has been terminated.
SUCCESS: The process "firefox.exe" with PID 18280 has been terminated.
SUCCESS: The process "firefox.exe" with PID 13552 has been terminated.
SUCCESS: The process "firefox.exe" with PID 22824 has been terminated.
SUCCESS: The process "firefox.exe" with PID 22872 has been terminated.
SUCCESS: The process "firefox.exe" with PID 13396 has been terminated.
SUCCESS: The process "firefox.exe" with PID 20004 has been terminated.
SUCCESS: The process "firefox.exe" with PID 1596 has been terminated.
SUCCESS: The process "firefox.exe" with PID 21980 has been terminated.
SUCCESS: The process "firefox.exe" with PID 14252 has been terminated.
SUCCESS: The process "firefox.exe" with PID 18236 has been terminated.
SUCCESS: The process "firefox.exe" with PID 26932 has been terminated.
SUCCESS: The process "firefox.exe" with PID 1336 has been terminated.
SUCCESS: The process "firefox.exe" with PID 27248 has been terminated.
SUCCESS: The process "firefox.exe" with PID 5244 has been terminated.
SUCCESS: The process "firefox.exe" with PID 24228 has been terminated.
SUCCESS: The process "firefox.exe" with PID 12024 has been terminated.
SUCCESS: The process "firefox.exe" with PID 18188 has been terminated.

```

5. Atur prioritas cmd.exe menjadi rendah.

```
C:\Users\userrrr>wmic process where name="cmd.exe" call setpriority 64
Executing (\\NAJELA\R00T\CIMV2:Win32_Process.Handle="384")->setpriority()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
```

6. Tampilkan prioritas dari semua proses yang berjalan.

```
C:\Users\userrrr>wmic process get Name,ProcessId,Priority
Name                                Priority  ProcessId
System Idle Process                0        0
System                             8        4
Registry                           8       124
smss.exe                           11      428
csrss.exe                           13      624
wininit.exe                         13      712
csrss.exe                           13      724
services.exe                       9       796
lsass.exe                           9       804
winlogon.exe                       13      884
svchost.exe                         8     1004
fontdrvhost.exe                    8       376
fontdrvhost.exe                    8       408
svchost.exe                         8       828
svchost.exe                         8     1048
svchost.exe                         8     1196
svchost.exe                         8     1224
svchost.exe                         8     1232
svchost.exe                         8     1308
IntelCpHDCPSvc.exe                 8     1324
svchost.exe                         8     1344
svchost.exe                         8     1404
svchost.exe                         8     1484
dwm.exe                            13     1532
IntelCpHeciSvc.exe                 8     1772
svchost.exe                         8     1796
svchost.exe                         8     1900
```

7. Jalankan dir C:\Windows lalu alihkan outputnya ke file output.txt.

```

C:\Users\userrrr>dir C:\Windows > output.txt

C:\Users\userrrr>type output.txt
Volume in drive C has no label.
Volume Serial Number is 4283-90CA

Directory of C:\Windows

03/13/2025  12:30 AM    <DIR>          .
03/13/2025  12:30 AM    <DIR>          ..
12/07/2019  04:51 PM    <DIR>          addins
10/31/2024  08:00 AM    <DIR>          appcompat
01/17/2025  08:44 AM    <DIR>          apppatch
03/19/2025  07:42 AM    <DIR>          AppReadiness
09/01/2024  02:27 PM    <DIR>          assembly
03/13/2025  12:30 AM    <DIR>          bcastdvr
02/13/2025  02:22 PM             93,696 bfsvc.exe
09/01/2024  01:48 PM    <DIR>          Boot
12/07/2019  04:14 PM    <DIR>          Branding
03/12/2025  11:38 PM    <DIR>          CbsTemp
09/01/2024  02:29 PM             753 comsetup.log
12/07/2019  05:16 PM    <DIR>          Containers
06/15/2024  05:17 PM    <DIR>          CSC
12/07/2019  04:14 PM    <DIR>          Cursors
09/13/2024  03:36 PM    <DIR>          debug
09/01/2024  02:32 PM             7,623 diagerr.xml
12/07/2019  04:31 PM    <DIR>          diagnostics
11/15/2024  09:27 AM    <DIR>          DiagTrack
09/01/2024  02:32 PM             7,623 diagwrn.xml

```

8. Gabungkan dua perintah: tasklist dan findstr chrome.

```

C:\Users\userrrr>tasklist | findstr chrome
chrome.exe             19940 Console             1      132,828 K
chrome.exe             13592 Console             1         2,744 K
chrome.exe             23036 Console             1       86,144 K
chrome.exe             17676 Console             1      33,772 K
chrome.exe             27416 Console             1      14,388 K
chrome.exe             23504 Console             1         8,992 K
chrome.exe             22928 Console             1      12,556 K
chrome.exe             17540 Console             1      39,468 K
chrome.exe             18408 Console             1       56,268 K
chrome.exe             16176 Console             1      59,076 K
chrome.exe             20016 Console             1     129,596 K
chrome.exe              4908 Console             1       85,832 K
chrome.exe             22792 Console             1       74,680 K

```

9. Anda menjalankan Notepad dan ingin memastikan bahwa tidak ada proses Notepad yang berjalan lebih dari 5 menit. Bagaimana cara mengeceknya?

```

C:\Users\userrrr>wmic process where "name='notepad.exe'" get Name,CreationDate
CreationDate           Name
20250319092854.712737+420 notepad.exe
20250319104031.140519+420 notepad.exe

```

10. Sebuah proses bernama svchost.exe menggunakan terlalu banyak memori. Bagaimana cara menghentikan hanya proses svchost.exe tertentu yang menghabiskan lebih dari 500MB RAM?

→ Cek proses svchost.exe yang sedang berjalan yaitu dengan menggunakan perintah "tasklist /FI "IMAGENAME eq svchost.exe" nah ini akan menampilkan semua proses svchost.exe beserta dengan PID dan juga penggunaan memori



→ Lalu cari memori nya yang melebihi 500 MB itu di kolom 'Mem Usage' dan catat PID dari svchost.exe yang penggunaan memorinya besar

→ Lalu hentikan proses tersebut dengan menggunakan perintah "taskkill /PID <PID> /F"

11. Anda ingin menampilkan semua proses yang memiliki nama mengandung "chrome" dan menyimpan hasilnya ke file. Bagaimana caranya?

```
C:\Users\userrrrr>tasklist | findstr /I "chrome"
chrome.exe             19940 Console             1      131,684 K
chrome.exe             13592 Console             1         2,876 K
chrome.exe             23036 Console             1       75,756 K
chrome.exe             17676 Console             1       33,652 K
chrome.exe             27416 Console             1       13,284 K
chrome.exe             23504 Console             1         8,940 K
chrome.exe             22928 Console             1       12,492 K
chrome.exe             17540 Console             1       26,588 K
chrome.exe             18408 Console             1       55,000 K
chrome.exe             16176 Console             1       59,280 K
chrome.exe             20016 Console             1      123,516 K
chrome.exe             23360 Console             1       88,248 K
chrome.exe             22636 Console             1       60,260 K
chrome.exe             19148 Console             1       78,820 K
chrome.exe             24580 Console             1       32,124 K
```

12. Anda menemukan bahwa Windows berjalan lambat karena banyak proses latar belakang. Buat perintah untuk menampilkan hanya proses dengan prioritas "Tinggi".

```
PS C:\Users\userrrrr> Get-WmiObject Win32_Process | Where-Object { $_.Priority -ge 13 } | Select-Object ProcessId, Name, Priority
ProcessId Name          Priority
-----
624 csrss.exe      13
712 wininit.exe    13
724 csrss.exe      13
884 winlogon.exe   13
1532 dwm.exe       13
4040 esif_uf.exe   13
5004 WUDFHost.exe  13
4048 ctfmon.exe    13
5472 notepad.exe   13
2164 notepad.exe   13
```

13. Sebuah aplikasi tidak merespons. Anda mencoba menghentikannya dengan taskkill, tetapi tidak berhasil. Apa kemungkinan penyebabnya dan bagaimana solusi lainnya?

→ Kemungkinan penyebabnya yaitu :

- Aplikasi sedang dalam kondisi "stuck" atau deadlock jadi tidak merespons perintah seperti perintah normal
- Aplikasi berjalan dengan hak akses lebih tinggi (misal yaitu sebagai sistem atau administrator), jadi taskkill tanpa elevated permission (tidak dijalankan sebagai admin) tidak bisa menghentikan.
- Proses dilindungi oleh windows, contohnya proses sistem inti yang tidak bisa dihentikan dengan perintah biasa

- Ada proses turunan (child process) yang membuat proses utama gabisa untuk dihentikan langsung

→ Solusinya adalah dengan :

- ❖ Memastikan terlebih dahulu kalau Command Prompt sudah berjalan sebagai administrator
  - Klik Start → lalu ketik cmd → lalu klik kanan → setelah itu di Run as Administrator
- ❖ Menggunakan taskkill dengan opsi paksa dan semua proses anak (child process)
  - Yaitu dengan menggunakan perintah "taskkill /IM <namaprogram.exe> /F /T
- ❖ Menggunakan Task Manager secara manual
  - Klik tombol Ctrl + Shift + Esc
  - Lalu cari aplikasi yang tidak merespons
  - Setelah itu, klik kanan → End Task
  - Kalau gabisa di tab "Processes", coba buka tab Details dan cari proses yang sesuai, lalu di End Ts dari sana
- ❖ Menggunakan Resource Monitor (lebih detail)
  - Pertama klik tombol windows + R lalu ketik "resmon" dan di enter
  - Lalu pergi ke tab CPU
  - Carilah aplikasi yang tidak merespons
  - Lalu klik kanan dan di End Process
- ❖ Kalau semua solusi tetap tidak berhasil
  - Restart komputer adalah solusi yang terakhir