Análisis de procesos y conexiones de red con PowerShell

Listar los procesos que tengan consumo alto de tiempo de CPU
[crayon-6a9d689a6f195760431941/]

```
PS C:\WINDOWS\system32> Get-Process | select cpu,id,name | sort cpu -Descending

        CPU   Id Name
        ---   -- ----
 6792,03125  900 svchost
  2426,4375  992 svchost
2272,453125    4 System
 1278,59375 1480 MsMpEng
 199,671875 2536 SearchIndexer
   144,3125  464 svchost
     76,125  744 svchost
    73,9375 1108 svchost
  71,703125 4756 chrome
   65,59375  624 lsass
   55,34375 2612 svchost
  49,609375  928 svchost
  42,515625 1564 vmware-authd
  39,609375 4064 chrome
       37,5  872 svchost
  24,328125 1572 chrome
    21,4375 1576 dwm
  20,578125 4668 chrome
  17,953125 1664 powershell_ise
    17,8125  616 services
   11,34375  696 svchost
    10,5625 2868 explorer
  10,453125 3332 chrome
   8,546875 4736 Taskmgr
     5,3125 3360 chrome
```

Obtener más información sobre los procesos (línea de comandos)
[crayon-6a9d689a6f19e254972006/]

Desde el Administrador de tareas obtenemos información sobre procesos

Analizar las conexiones de red para los procesos que hemos obtenido anteriormente
[crayon-6a9d689a6f1a1337484760/]

```
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       900 -PROCESO-> svchost 900
TCP    [::]:1027              [::]:0                 LISTENING       900 -PROCESO-> svchost 900
UDP    0.0.0.0:3544           *:*                                    900 -PROCESO-> svchost 900
UDP    127.0.0.1:1900         *:*                                    2612 -PROCESO-> svchost 900
UDP    192.168.1.35:1900      *:*                                    2612 -PROCESO-> svchost 900
UDP    192.168.1.35:57778     *:*                                    900 -PROCESO-> svchost 900
UDP    192.168.171.1:1900     *:*                                    2612 -PROCESO-> svchost 900
UDP    192.168.229.1:1900     *:*                                    2612 -PROCESO-> svchost 900
UDP    [::1]:1900             *:*                                    2612 -PROCESO-> svchost 900
UDP    [fe80::15d3:43bb:e53d:4023%10]:1900  *:*                                  2612 -PROCESO-> svchost 900
UDP    [fe80::51d5:792d:4203:57a8%8]:1900  *:*                                   2612 -PROCESO-> svchost 900
UDP    [fe80::a540:cd7e:8144:9c31%4]:1900  *:*                                   2612 -PROCESO-> svchost 900
```

Otra forma de analizar las conexiones de red

[crayon-6a9d689a6f1a4517178877/]

```
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       900
TCP    192.168.1.35:37912     131.253.14.153:80      FIN_WAIT_1      900
TCP    [::]:1027              [::]:0                 LISTENING       900
UDP    0.0.0.0:3544           *:*                                    900
UDP    127.0.0.1:1900         *:*                                    2612
UDP    192.168.1.35:1900      *:*                                    2612
UDP    192.168.1.35:57778     *:*                                    900
UDP    192.168.171.1:1900     *:*                                    2612
UDP    192.168.229.1:1900     *:*                                    2612
UDP    [::1]:1900             *:*                                    2612
UDP    [fe80::15d3:43bb:e53d:4023%10]:1900  *:*                                  2612
UDP    [fe80::51d5:792d:4203:57a8%8]:1900  *:*                                   2612
UDP    [fe80::a540:cd7e:8144:9c31%4]:1900  *:*                                   2612
```

Obtener información sobre la IP obtenida

[crayon-6a9d689a6f1a6556768453/]

Información sobre el Whois