



23 de julio de 2021  
Ficha N° 13 WPSCAN de Comandos  
CSIRT DE GOBIERNO

## Comando de la semana “WPSCAN”

### I. CONTEXTO

Este documento, denominado, en esta oportunidad, “WPSCAN”, tiene como objetivo ilustrar sobre una herramienta que puede ser de utilidad para el lector, a objeto de ir potenciando las capacidades locales de autochequeo, detección simple de vulnerabilidades que están expuestas a internet en sus activos de información y, a su vez, la obtención de una verificación de la subsanación de aquellas que se les han sido reportadas, facilitando la interacción con el CSIRT de Gobierno. El objetivo no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por “CSIRT GOB CL”. Todas estas herramientas al contar con la posibilidad de ser usadas desde una línea de comando permiten en algún grado la integración dentro de script o lenguajes de automatización o programación como PERL, AWK, Shell Scripting<sup>1</sup>, Expect, Python, C, C++, Golang, JavaScript, PowerShell, Ruby, Java, PHP, Elixir, Elm, Go, Dart, Pony, TypeScript, Kotlin, Nim, OCaml, Q#<sup>2</sup>, Reason, Rust, Swift entre otros con miras a automatizar estas actividades y concentrar el tiempo de los especialistas en el análisis de los datos para encontrar los problemas relevantes y descartar los falsos positivos.

### II. INTRODUCCIÓN

Una de las tareas regulares que en ciberseguridad se realizan es la verificación de los sitios o sistemas que están expuestos a Internet, y en particular de los Gestores de Contenidos o CMS<sup>3</sup> por sus siglas en inglés. Aunque no se recomienda mantener el CMS expuesto a Internet, es decir, se debiera aplicar una estrategia de separación del CMS respecto del sitio o sistema web resultante, a veces los encargados de ciberseguridad se enfrentarán a un CMS expuesto directamente a Internet.

---

<sup>1</sup> <https://scis.uohyd.ac.in/~apcs/itw/UNIXProgrammingEnvironment.pdf>

<sup>2</sup> <https://github.com/Microsoft/QuantumKatas/>

<sup>3</sup> Un sistema de gestión de contenidos hace lo que su nombre indica: te ayuda a «gestionar» el contenido de tu sitio web de forma «sistematizada». En lugar de tener que trabajar con código cada vez que quieras añadir contenido a tu sitio web, un CMS te permite trabajar en un editor fácil de usar.



En la práctica existen muchos gestores de contenidos que aportan diferentes funcionalidades para poder generar un sitio o sistema web funcional a los propósitos de sus creadores, pero no están exentos de vulnerabilidades.

Dentro de los CMS más utilizados podemos encontrar a WordPress, Joomla, Drupal, Magento, Blogger, Shopify, Squarespace, Magnolia, Weebly, Wix, Bynder, HubSpot, Kentico, dotCMS, Contentful, Zephyr, Canvas CMS, Grav, Craft CMS, Sitefinity, BigCommerce, Umbraco CMS, Agility CMS, Adobe Experience Manager, Oracle WebCenter Content, Ghost, entre otros varios más.

















En este contexto, presentaremos la herramienta WPSCAN que es de utilidad para apoyar la identificación de vulnerabilidades de uno de los CMS más utilizados: WordPress.

### ¿Qué es WPSCAN?

WPScan es un escáner de vulnerabilidades de WordPress de caja negra que se puede usar para escanear instalaciones remotas de WordPress para encontrar problemas de seguridad.

La herramienta WPScan utiliza una base de datos de 23,107 vulnerabilidades de WordPress.

### ¿Qué comprueba WPScan?

-  La versión de WordPress instalada y las vulnerabilidades asociadas.
-  Qué complementos están instalados y las vulnerabilidades asociadas
-  Qué temas están instalados y las vulnerabilidades asociadas
-  Enumeración de nombre de usuario
-  Usuarios con contraseñas débiles a través de la fuerza bruta de contraseñas
-  Archivos wp-config.php respaldados y accesibles públicamente
-  Volcados de base de datos que pueden ser de acceso público
-  Si los complementos exponen registros de errores
-  Enumeración de archivos multimedia
-  Archivos Timthumb vulnerables
-  Si el archivo Léame de WordPress está presente
-  Si WP-Cron está habilitado
-  Si el registro de usuario está habilitado
-  Divulgación de ruta completa
-  Subir listado de directorio
-  Y mucho más...

**NOTA IMPORTANTE 1:** Dado que es relevante un buen manejo de los comandos básicos de Linux, tanto para posteriores manejos de los datos o archivos como para usos de la información resultante de la ejecución de los comandos, es que el comité editorial decidió que se incluya en esta edición y en las subsiguientes un anexo de comandos Linux que son de utilidad para moverse en este sistema



operativo. Se sugiere dominarlos todos para facilitar el acceso y manipulación de la información. En futuras ediciones se irán incorporando nociones más avanzadas sobre el uso de estos comandos para procesamiento de archivos, procesos, y de sus usos en scripting.

#### **Vea anexo I: Comandos básicos de Linux**

**NOTA IMPORTANTE 2:** Dado que un altísimo porcentaje de los equipos de usuarios y servidores operando en un entorno Windows, el comité editorial ha decidido ir incorporando tips para este entorno computacional.

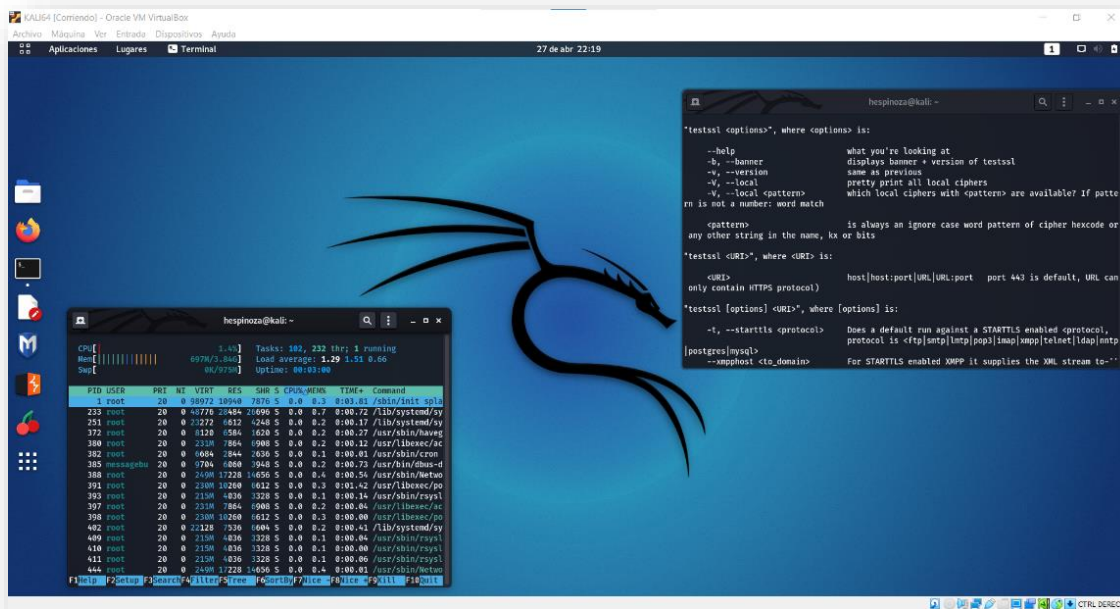
#### **Vea anexo II: Comandos o aplicativos básicos para Windows**



### III. PASO A PASO

#### PASO 1: Un entorno adecuado para trabajar.

Primero debe contar con una distribución de Kali<sup>4</sup> Linux funcionando ya sea en una máquina física o en una máquina virtual<sup>5</sup>.



#### Instalación de Kali Linux

La instalación de Kali Linux (arranque único) en su computadora es un proceso sencillo. Esta guía cubrirá la instalación básica (que se puede realizar en una máquina virtual invitada o sobre un equipo entero), con la opción de cifrar la partición. En ocasiones, es posible que tenga datos confidenciales que preferiría cifrar con Full Disk Encryption (FDE). Durante el proceso de instalación, puede iniciar una instalación cifrada LVM en el disco duro o en las unidades USB.

Primero, necesitará hardware de computadora compatible. Kali Linux es compatible con plataformas amd64 (x86\_64 / 64-Bit) e i386 (x86 / 32-Bit). Siempre que sea posible, el fabricante recomienda utilizar las imágenes amd64. Los requisitos de hardware son mínimos como se enumeran en la

<sup>4</sup> <https://www.kali.org/downloads/>  
<sup>5</sup>

[https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop\\_end\\_user\\_computing/vmware\\_workstation\\_player/16\\_0](https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0)

<sup>6</sup> <https://www.virtualbox.org/wiki/Downloads>



sección siguiente, aunque un mejor hardware naturalmente proporcionará un mejor rendimiento. Debería poder usar Kali Linux en hardware más nuevo con UEFI y sistemas más antiguos con BIOS.

Las imágenes i386, de forma predeterminada, utilizan un kernel PAE, por lo que puede ejecutarlas en sistemas con más de 4 GB de RAM.

En el ejemplo que se menciona más adelante, se instalará Kali Linux en una nueva máquina virtual invitada, sin ningún sistema operativo existente preinstalado.

### Requisitos del sistema

Los requisitos de instalación para Kali Linux variarán según lo que le gustaría instalar y su configuración. Para conocer los requisitos del sistema:





En el extremo inferior, puede configurar Kali Linux como un servidor Secure Shell (SSH) básico sin escritorio, utilizando tan solo 128 MB de RAM (se recomiendan 512 MB) y 2 GB de espacio en disco.

En el extremo superior, si opta por instalar el escritorio Xfce4 predeterminado y el kali-linux-default metapaquete, realmente debería apuntar a al menos 2 GB de RAM y 20 GB de espacio en disco.

Cuando se utilizan aplicaciones que consumen muchos recursos, como Burp Suite, recomiendan al menos 8 GB de RAM (¡e incluso más si se trata de una aplicación web grande!) O utilizar programas simultáneos al mismo tiempo.

### Requisitos previos de instalación<sup>7</sup>

Esta la guía se harán las siguientes suposiciones al instalar Kali Linux:

-  Usando la imagen del instalador de amd64.
-  Unidad de CD / DVD / soporte de arranque USB.
-  Disco único para instalar.
-  Conectado a una red (con DHCP y DNS habilitados) que tiene acceso a Internet saliente.

### Preparación para la instalación




-  Descargue Kali Linux<sup>8</sup> (el fabricante recomienda<sup>9</sup> la imagen marcada como Instalador).

<sup>7</sup> Dependiendo del tipo de instalación que seleccione, se pueden borrar todos los datos existentes en el disco duro, así que haga una copia de seguridad de la información importante del dispositivo en un medio externo.

<sup>8</sup> <https://www.kali.org/docs/introduction/download-official-kali-linux-images/>

<sup>9</sup> <https://www.kali.org/docs/introduction/what-image-to-download/#which-image-to-choose>



-  Grabe<sup>10</sup> la ISO de Kali Linux en un DVD o una imagen de Kali Linux Live en una unidad USB. (Si no puede, consulte la instalación en red<sup>11</sup> de Kali Linux).
-  Realice una copia de seguridad de la información importante del dispositivo en un medio externo.
-  Asegúrese de que su computadora esté configurada para arrancar desde CD / DVD / USB en su BIOS / UEFI.

Un vez que tiene preparado todos los materiales y el entorno para comenzar la instalación siga los pasos indicados en la sección “Kali Linux Installation Procedure” del siguiente enlace:

<https://www.kali.org/docs/installation/hard-disk-install/>



<sup>10</sup> <https://www.kali.org/docs/usb/live-usb-install-with-windows/>

<sup>11</sup> <https://www.kali.org/docs/installation/network-pxe/>



## PASO 2: Instalar el comando.

Una vez que se cuenta con este sistema operativo de manera funcional podemos instalar los comandos; algunos ya vienen preinstalados en la distribución KALI<sup>12</sup>, pero si no fuere así puede instalarlos con los siguientes comandos, **previamente tomando privilegios de usuario "root"**:

```
# apt update && apt full-upgrade
```

```
# apt install wpscan
```

```
# apt search ^wpscan
```

```
Ordenando... Hecho
```

```
Buscar en todo el texto... Hecho
```

```
wpscan/kali-rolling,now 3.8.18-0kali1 all [instalado]
```

```
Black box WordPress vulnerability scanner
```

Nota: el símbolo "^" indica que busque los patrones que comienza por lo indicado en la línea de comando.

```
root@V: ~  
# apt install wpscan  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
wpscan ya está en su versión más reciente (3.8.18-0kali1).  
fijado wpscan como instalado manualmente.  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
python3-babel-localedata python3-babel python3-gevent python3-gevent-websocket  
python3-greenlet python3-jupyter-core python3-m2crypto python3-nbformat  
python3-parameterized python3-plotly python3-zope.event  
Utilice «apt autoremove» para eliminarlos.  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
  
(root@V)~  
# apt search ^wpscan  
Ordenando... Hecho  
Buscar en todo el texto... Hecho  
wpscan/kali-rolling,now 3.8.18-0kali1 all [instalado]  
Black box WordPress vulnerability scanner  
  
(root@V)~  
#
```

<sup>12</sup> <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>





### PASO3: Verificar su instalación.

Una vez que se ha instalado podemos verificar y explorar las múltiples opciones que ofrece para su ejecución:

En una consola de su KALI, dentro del directorio donde quedó instalada la aplicación, ejecute el comando para que muestre la ayuda: “wpscan -h”<sup>13</sup>.

```
root@V: ~  
# wpscan -hh  
  
WPSecan®  
WordPress Security Scanner by the WPSecan Team  
Version 3.8.18  
  
@_WPSecan_, @ethicalhack3r, @erwan_lr, @firefart  
  
Usage: wpscan [options]  
    --url URL                The URL of the blog to scan  
                             Allowed Protocols: http, https  
                             Default Protocol if none provided: http  
                             This option is mandatory unless update or help  
-h, --help                  Display the simple help and exit  
--hh                        Display the full help and exit  
--version                   Display the version and exit  
-v, --verbose               Verbose mode
```

Debiéramos, entonces, lograr desplegar todas las opciones y parámetros de ejecución, junto a su explicación en la consola.

```
wpscan -hh
```

WPSecan®

<sup>13</sup> La opción “-h” es relativamente estándar y cada comando debiera desplegar la ayuda de uso, en algunos casos deberá utilizar “--help”. En algunos casos se puede usar la opción “-hh” para desplegar ayudas con mayor grado de detalles.





```

WordPress Security Scanner by the WPScan Team
Version 3.8.18

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Usage: wpscan [options]
    --url URL
        The URL of the blog to scan
        Allowed Protocols: http, https
        Default Protocol if none
        provided: http
        This option is mandatory
    unless update or help or hh or version is/are supplied
        Display the simple help and
        -h, --help
        exit
        Display the full help and exit
        --hh
        Display the version and exit
        --version
        Verbose mode
        -v, --verbose
        Whether or not to display the
        --[no-]banner
        banner
        Default: true
        -o, --output FILE
        Output to FILE
        -f, --format FORMAT
        Output results in the format
        supplied
        Available choices: cli-no-
        colour, cli-no-color, json, cli
        --detection-mode MODE
        Default: mixed
        Available choices: mixed,
        passive, aggressive
        --user-agent, --ua VALUE
        --random-user-agent, --rua
        Use a random user-agent for
        each scan
        --http-auth login:password
        -t, --max-threads VALUE
        The max threads to use
        Default: 5
        --throttle MilliSeconds
        Milliseconds to wait before
        doing another web request. If used, the max threads will be set to 1.
        --request-timeout SECONDS
        The request timeout in seconds
        Default: 60
        --connect-timeout SECONDS
        The connection timeout in
        seconds
        Default: 30
        --disable-tls-checks
        Disables SSL/TLS certificate
        verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)
        --proxy protocol://IP:port
        Supported protocols depend on
        the cURL installed
        --proxy-auth login:password
        --cookie-string COOKIE
        Cookie string to use in requests,
        format: cookie1=value1[; cookie2=value2]
        --cookie-jar FILE-PATH
        File to read and write cookies
        Default:
        /tmp/wpscan/cookie_jar.txt
        --force
        Do not check if the target is
        running WordPress or returns a 403
        --[no-]update
        Whether or not to update the
        Database
        --api-token TOKEN
        The WPScan API Token to display
        vulnerability data, available at https://wpscan.com/profile
    
```



```
--wp-content-dir DIR
custom or not detected, such as "wp-content"
--wp-plugins-dir DIR
or not detected, such as "wp-content/plugins"
-e, --enumerate [OPTS]
```

5

'\_'

supplied: 1-10

15

must be set to "Plain" for those to be detected

'\_'

supplied: 1-100

values: ','

Backups

vp,vt,tt,cb,db,e,u,m

of each group/s can be used):

```
--exclude-content-based REGEXP_OR_STRING
Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration. Both the headers and body are checked. Regexp delimiters are not required.
```

```
--plugins-detection MODE
enumerate Plugins.
```

passive, aggressive

```
--plugins-version-detection MODE
plugins' versions.
```

passive, aggressive

```
--exclude-usernames REGEXP_OR_STRING
Exclude usernames matching the Regexp/string (case insensitive). Regexp delimiters are not required.
```

```
-P, --passwords FILE-PATH
List of passwords to use during the password attack.
```

supplied, user enumeration will be run.

The wp-content directory if

The plugins directory if custom

Enumeration Process

Available Choices:

vp Vulnerable plugins

ap All plugins

p Popular plugins

vt Vulnerable themes

at All themes

t Popular themes

tt Timthumbs

cb Config backups

db,e Db exports

u User IDs range. e.g: u1-

Range separator to use:

Value if no argument

m Media IDs range. e.g m1-

Note: Permalink setting

Range separator to use:

Value if no argument

Separator to use between the

Default: All Plugins, Config

Value if no argument supplied:

Incompatible choices (only one

- vp, ap, p

- vt, at, t

Exclude all responses matching the enumeration. Both the headers and body are

Use the supplied mode to

Default: passive

Available choices: mixed,

Use the supplied mode to check

Default: mixed

Available choices: mixed,

Exclude usernames matching the

List of passwords to use during

If no --username/s option



<code>-U, --usernames LIST</code>	List of usernames to use during the password attack.
<code>'/tmp/a.txt'</code>	Examples: 'a1', 'a1,a2,a3',
<code>--multicall-max-passwords MAX_PWD</code>	Maximum number of passwords to send by request with XMLRPC multicall
	Default: 500
<code>--password-attack ATTACK</code>	Force the supplied attack to be used rather than automatically determining one.
<code>xmlrpc, xmlrpc-multicall</code>	Available choices: wp-login,
<code>--login-uri URI</code>	The URI of the login page if different from /wp-login.php
<code>--stealthy</code>	Alias for --random-user-agent
<code>--detection-mode passive --plugins-version-detection passive</code>	
[!] To see full list of options use --hh.	



#### Paso 4: Ponerlo en marcha para verificar nuestra infraestructura.

Un ejemplo de ejecución básica para nuestros primeros pasos:

Probaremos el comando SHCHECK con nuestro KALI en un ataque un sitio web determinado:

##### EJEMPLO WPCAN

###### Mirar Ayuda:

```
# wpscan --help
```

###### Hacer un chequeo no intrusivo ...

```
# wpscan --url www.example.com
```

###### Aplicar fuerza bruta de contraseña con base a una lista de palabras (dark0de.lst) sobre usuarios enumerados usando 50 subprocesos ...

```
# wpscan --url www.example.com --wordlist dark0de.lst --threads 50
```

###### Aplicar fuerza bruta de contraseña con base a una lista de palabras (dark0de.lst) sobre un único usuario objetivo: "admin" ...

```
# wpscan --url www.example.com --wordlist dark0de.lst --username admin
```

###### Enumerar complementos instalados ...

```
# wpscan --url www.example.com --enumerate p
```

###### Enumerar temas instalados ...

```
# wpscan --url www.example.com --enumerate t
```

###### Enumerar usuarios ...

```
# wpscan --url www.example.com --enumerate u
```

###### Enumerar timthumbs instalados ...

```
# wpscan --url www.example.com --enumerate tt
```

###### Utilizar un proxy HTTP ...

```
# wpscan --url www.example.com --proxy 127.0.0.1:8118
```

###### Utilizar un proxy SOCKS5 ... (cURL >= v7.21.7 necesario)

```
# wpscan --url www.example.com --proxy socks5://127.0.0.1:9000
```

###### Utilizar un directorio de contenidos personalizado ...

```
# wpscan -u www.example.com --wp-content-dir custom-content
```

###### Utilizar un directorio de complementos personalizado ...

```
# wpscan -u www.example.com --wp-plugins-dir wp-content/custom-plugins
```

###### Actualizar la base de datos de vulnerabilidades ...

```
# wpscan --update
```

###### Obtener un despliegue con detalles nivel Debug ...

```
# wpscan --url www.example.com --debug-output 2>debug.log
```

Es posible que el comando detecte que el sitio web que están explorando no está construido con WordPress, en cuyo caso el resultado será el siguiente:



```
root@V: ~  
(root@V)-[~]  
# wpscan --url www.csirt.gob.cl  
  
WPSecan®  
WordPress Security Scanner by the WPSecan Team  
Version 3.8.18  
@_WPSecan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[i] Updating the Database ...  
[i] Update completed.  
  
Scan Aborted: The remote website is up, but does not seem to be running WordPress.  
  
(root@V)-[~]  
#
```

En el caso de que positivamente sea detectado un CMS WordPress, el comando desplegará todas sus funciones para analizarlo y encontrar información de utilizadas para el Encargado de Ciberseguridad y generar con esta los informes pertinentes para la coordinación con los equipos TIC que deberán corregir o mitigar los hallazgos encontrados.

A continuación se muestra un ejercicio real de ejecución no invasiva con fines educativos, en el cual se ha ofuscado el nombre del sitio web utilizado:

```
## wpscan --url www.SITIOWEBREAL.cl --random-user-agent
```

WPSecan®

WordPress Security Scanner by the WPSecan Team  
Version 3.8.18

Sponsored by Automattic - <https://automattic.com/>  
@\_WPSecan\_, @ethicalhack3r, @erwan\_lr, @firefart

```
[+] URL: http://www.SITIOWEBREAL.cl/ [72.9.154.178]  
[+] Started: Wed Jul 21 11:54:29 2021
```



Interesting Finding(s) :

```
[+] Headers
| Interesting Entries:
|   - Server: LiteSpeed
|   - Referrer-Policy:
|   - Access-Control-Allow-Origin: *
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://www.SITIOWEBREAL.cl/robots.txt
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.SITIOWEBREAL.cl/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 30%
| References:
|   - http://codex.wordpress.org/XML-RPC_Pingback_API
|
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
|   - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
|
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
|
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://www.SITIOWEBREAL.cl/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

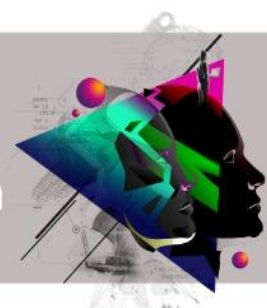
[+] Upload directory has listing enabled: http://www.SITIOWEBREAL.cl/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://www.SITIOWEBREAL.cl/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
|   - https://www.iplocation.net/defend-wordpress-from-ddos
|   - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0.13 identified (Latest, released on 2021-05-13).
| Found By: Rss Generator (Passive Detection)
|
|   - http://www.SITIOWEBREAL.cl/feed/,
<generator>https://wordpress.org/?v=5.0.13</generator>
|   - http://www.SITIOWEBREAL.cl/comments/feed/,
<generator>https://wordpress.org/?v=5.0.13</generator>

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
```



```
[i] Plugin(s) Identified:

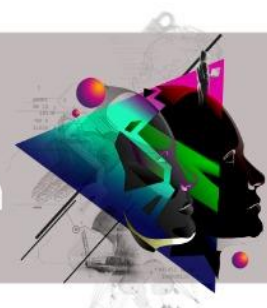
[+] simple-contact-form
| Location: http://www.SITIOWEBREAL.cl/wp-content/plugins/simple-contact-form/
| Latest Version: 14.13 (up to date)
| Last Updated: 2015-12-01T06:01:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 14.13 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/simple-contact-
form/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/simple-contact-
form/readme.txt

[+] w3-total-cache
| Location: http://www.SITIOWEBREAL.cl/wp-content/plugins/w3-total-cache/
| Last Updated: 2021-07-09T20:03:00.000Z
| [!] The version is out of date, the latest version is 2.1.5
|
| Found By: Comment Debug Info (Passive Detection)
|
| Version: 0.9.7 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/w3-total-cache/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/w3-total-cache/readme.txt

[+] wordfence
| Location: http://www.SITIOWEBREAL.cl/wp-content/plugins/wordfence/
| Last Updated: 2021-07-15T18:55:00.000Z
| [!] The version is out of date, the latest version is 7.5.4
|
| Found By: Javascript Var (Passive Detection)
|
| Version: 7.1.20 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/wordfence/readme.txt

[+] wordpress-seo
| Location: http://www.SITIOWEBREAL.cl/wp-content/plugins/wordpress-seo/
| Last Updated: 2021-07-13T07:28:00.000Z
| [!] The version is out of date, the latest version is 16.7
|
| Found By: Comment (Passive Detection)
|
| Version: 9.5 (100% confidence)
| Found By: Comment (Passive Detection)
| - http://www.SITIOWEBREAL.cl/, Match: 'optimized with the Yoast SEO plugin
v9.5 -'
| Confirmed By:
| Readme - Stable Tag (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/wordpress-seo/readme.txt
| Readme - ChangeLog Section (Aggressive Detection)
| - http://www.SITIOWEBREAL.cl/wp-content/plugins/wordpress-seo/readme.txt
```





```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:05 <=====> (137 / 137) 100.00%
Time: 00:00:05

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Wed Jul 21 11:54:43 2021
[+] Requests Done: 173
[+] Cached Requests: 5
[+] Data Sent: 47.98 KB
[+] Data Received: 300.243 KB
[+] Memory used: 177.898 MB
[+] Elapsed time: 00:00:13
```

A simple vista encontró varios plugins o complementos, y lo más relevantes es que informa que algunos de ellos están desactualizados, por lo que debieran ser revisados para tratar de actualizarlos a la brevedad.

Tenga presente que es importante que estas pruebas sean coordinadas con el equipo de operaciones y en ambientes que estén bajo supervisión.

Antes de proceder a aplicar estos comandos revise sus políticas de seguridad de la información interna, sus códigos de ética, los NDA que haya suscrito y las cláusulas de confidencialidad de su contrato de trabajo.

Defina horarios especiales o ambientes de “test o QA” equivalentes a los de “producción”, para mitigar los posibles efectos perjudiciales en los dispositivos de seguridad, el sitio o el sistema web.

Estudie las múltiples opciones de los comandos ilustrados en esta ficha, entienda el significado de sus diferentes parámetros con el objetivo de obtener resultados específicos, para diferentes escenarios de carga o redirigir la salida a un archivo, para su inclusión en informes posteriores.

Tenga presente que para el procesamiento y análisis de los datos es relevante que vaya perfeccionando su manejo de LINUX y comandos PowerShell<sup>14</sup> (si es un usuario de windows).

En próximas ediciones se irán reforzando estos aspectos para facilitar el manejo de los datos y resultados obtenidos, logrando así una mejor comunicación con sus equipos TIC y con el CSIRT de Gobierno.

En caso de cualquier inquietud no dude en consultarnos a [soc-csirt@interior.gob.cl](mailto:soc-csirt@interior.gob.cl).

<sup>14</sup> <https://devblogs.microsoft.com/scripting/table-of-basic-powershell-commands/>



Si encuentra algún error en el documento también es importante que nos lo comunique para introducir las correcciones pertinentes en las versiones futuras de esta ficha.



## Anexo I: Comandos Básicos de Linux

### Comandos básicos

Los comandos son esencialmente los mismos que cualquier sistema UNIX. En las tablas que se presentan a continuación se tiene la lista de comandos más frecuentes.

#### 1. comando “pwd2

Use el comando `pwd` para averiguar la ruta del directorio de trabajo actual (carpeta) en la que se encuentra. El comando devolverá una ruta absoluta (completa), que es básicamente una ruta de todos los directorios que comienza con una barra inclinada (/). Un ejemplo de ruta absoluta es `/home / username`.

#### 2. comando “cd”

Para navegar por los archivos y directorios de Linux, use el comando `cd`. Requiere la ruta completa o el nombre del directorio, según el directorio de trabajo actual en el que se encuentre.

Digamos que estás en `/home / username / Documents` y quieres ir a `Photos`, un subdirectorio de `Documents`. Para hacerlo, simplemente escriba el siguiente comando: `cd Photos`.

Otro escenario es si desea cambiar a un directorio completamente nuevo, por ejemplo, `/home / username / Movies`. En este caso, debe escribir `cd` seguido de la ruta absoluta del directorio: `cd /home / username / Movies`.

Hay algunos atajos que le ayudarán a navegar rápidamente:

- `cd ..` (con dos puntos) para mover un directorio hacia arriba
- `cd` para ir directamente a la carpeta de inicio
- `cd-` (con un guion) para ir a su directorio anterior

En una nota al margen, el shell de Linux distingue entre mayúsculas y minúsculas. Por lo tanto, debe escribir el directorio del nombre exactamente como está.

#### 3. comando “ls”

El comando `ls` se usa para ver el contenido de un directorio. De forma predeterminada, este comando mostrará el contenido de su directorio de trabajo actual.



Si desea ver el contenido de otros directorios, escriba ls y luego la ruta del directorio. Por ejemplo, ingrese ls / home / username / Documents para ver el contenido de Documents.

Hay variaciones que puede usar con el comando ls:

- ls -R también listará todos los archivos en los subdirectorios
- ls -a mostrará los archivos ocultos
- ls -al enumerará los archivos y directorios con información detallada como los permisos, el tamaño, el propietario, etc.

#### 4. comando de “cat”

cat (abreviatura de concatenar) es uno de los comandos más utilizados en Linux. Se utiliza para enumerar el contenido de un archivo en la salida estándar (stdout). Para ejecutar este comando, escriba cat seguido del nombre del archivo y su extensión. Por ejemplo: cat file.txt.

Aquí hay otras formas de usar el comando cat :

- “cat > filename” crea un nuevo archivo
- “cat filename1 filename2> filename3” une dos archivos (1 y 2) y almacena la salida de ellos en un nuevo archivo (3)
- convertir un archivo a mayúsculas o minúsculas, “cat filename | tr az AZ> salida.txt”.

#### 5. comando “cp”

Utilice el comando cp para copiar archivos del directorio actual a un directorio diferente. Por ejemplo, el comando cp scenery.jpg / home / username / Pictures crearía una copia de paisaje.jpg (de su directorio actual) en el directorio de Pictures.

#### 6. comando “mv”

El uso principal del comando mv es mover archivos, aunque también se puede usar para cambiar el nombre de los archivos.

Los argumentos en mv son similares al comando cp. Debe escribir mv, el nombre del archivo y el directorio de destino. Por ejemplo: mv file.txt / home / username / Documents.



Para cambiar el nombre de los archivos, el comando de Linux es “mv oldname.ext newname.ext”.

## 7. comando mkdir

Utilice el comando mkdir para crear un nuevo directorio; si escribe mkdir Music, se creará un directorio llamado Music.

También hay comandos adicionales de mkdir:

- Para generar un nuevo directorio dentro de otro directorio, use este comando básico de Linux mkdir Music / Newfile
- use la opción p (padres) para crear un directorio entre dos directorios existentes. Por ejemplo, mkdir -p Music / 2020 / Newfile creará el nuevo archivo “2020”.

## 8. comando “rmdir”

Si necesita eliminar un directorio, use el comando rmdir. Sin embargo, rmdir solo le permite eliminar directorios vacíos.

## 9. comando “rm”

El comando rm se usa para eliminar directorios y su contenido. Si solo desea eliminar el directorio, como alternativa a rmdir, use rm -r.

Nota: Tenga mucho cuidado con este comando y verifique dos veces en qué directorio se encuentra. Esto eliminará todo y no se puede deshacer.

## 10. comando “touch”

El comando touch le permite crear un nuevo archivo en blanco a través de la línea de comandos de Linux. Como ejemplo, ingrese touch /home/username/Documents/Web.html para crear un archivo HTML titulado Web en el directorio Documentos.

## 11. comando “locate”



Puede usar este comando para ubicar o localizar un archivo, al igual que el comando de búsqueda en Windows. Además, el uso del argumento `-i` junto con este comando hará que no distinga entre mayúsculas y minúsculas, por lo que puede buscar un archivo incluso si no recuerda su nombre exacto.

Para buscar un archivo que contenga dos o más palabras, use un asterisco (\*). Por ejemplo, el comando `"locate -i escuela*nota"` buscará cualquier archivo que contenga la palabra "escuela" y "nota", ya sea en mayúsculas o minúsculas.

## 12. comando "find"

Similar al comando `"locate"`, el uso de `"find"` también busca archivos y directorios. La diferencia es que el comando `"find"` se usa para ubicar archivos dentro de un directorio determinado.

Como ejemplo, el comando `find / home / -name notes.txt` buscará un archivo llamado `notes.txt` dentro del directorio de inicio y sus subdirectorios.

Otras variaciones al usar el hallazgo son:

- Para buscar archivos en el directorio actual, `"find. -nombre notes.txt"`
- Para buscar directorios desde la raíz, llamados `home`, use `"find / -type d -name home"`

## 13. comando "grep"

Otro comando básico de Linux que sin duda es útil para el uso diario es `grep`. Te permite buscar en todo el texto de un archivo determinado.

Para ilustrar, `grep blue notepad.txt` buscará la palabra `azul` en el archivo del bloc de notas. Las líneas que contienen la palabra buscada se mostrarán completamente.

## 14. comando "sudo"

Abreviatura de " SuperUser Do ", este comando le permite realizar tareas que requieren permisos administrativos o de root. Sin embargo, no es recomendable utilizar este comando para el uso diario porque podría ser fácil que ocurra un error si hiciste algo mal.



### 15. comando “df”

Utilice el comando df para obtener un informe sobre el uso de espacio en disco del sistema, que se muestra en porcentaje y KB. Si desea ver el informe en megabytes, escriba df -m.

### 16. comando “du”

Si desea comprobar cuánto espacio ocupa un archivo o un directorio, el comando du (Uso del disco) es la respuesta. Sin embargo, el resumen de uso del disco mostrará los números de bloque de disco en lugar del formato de tamaño habitual. Si desea verlo en bytes, kilobytes y megabytes, agregue el argumento -h a la línea de comando.

### 17. comando “head”

El comando head se usa para ver las primeras líneas de cualquier archivo de texto. De forma predeterminada, mostrará las primeras diez líneas, pero puede cambiar este número a su gusto. Por ejemplo, si solo desea mostrar las primeras cinco líneas, escriba head -n 5 filename.ext.

### 18. comando “tail”

Este tiene una función similar al comando head, pero en lugar de mostrar las primeras líneas, el comando tail mostrará las últimas diez líneas de un archivo de texto. Por ejemplo, tail -n filename.ext.

### 19. comando “diff”

Abreviatura de diferencia, el comando diff compara el contenido de dos archivos línea por línea. Después de analizar los archivos, generará las líneas que no coinciden. Los programadores suelen utilizar este comando cuando necesitan realizar modificaciones en el programa en lugar de reescribir todo el código fuente.

La forma más simple de este comando es diff file1.ext file2.ext

### 20. comando “tar”





El comando tar es el comando más utilizado para archivar varios archivos en un tarball, un formato de archivo común de Linux que es similar al formato zip, con la compresión opcional.

Este comando es bastante complejo con una larga lista de funciones, como agregar nuevos archivos a un archivo existente, enumerar el contenido de un archivo, extraer el contenido de un archivo y muchas más. Consulte algunos ejemplos prácticos para saber más sobre otras funciones.

## 21. comando “chmod”

chmod es otro comando de Linux, que se utiliza para cambiar los permisos de lectura, escritura y ejecución de archivos y directorios. Como este comando es bastante complicado, puede leer el tutorial completo para ejecutarlo correctamente.

## 22. comando “chown”

En Linux, todos los archivos pertenecen a un usuario específico. El comando chown le permite cambiar o transferir la propiedad de un archivo al nombre de usuario especificado. Por ejemplo, chown linuxuser2 file.ext hará que linuxuser2 sea el propietario del file.ext .

## 23. comando “jobs”

El comando jobs mostrará todos los trabajos actuales junto con sus estados. Un trabajo es básicamente un proceso que inicia el shell.

## 24. comando “kill”

Si tiene un programa que no responde, puede terminarlo manualmente usando el comando kill. Enviará una cierta señal a la aplicación que no funciona correctamente y le indicará a la aplicación que se cierre.

Hay un total de sesenta y cuatro señales que puede usar, pero las personas generalmente solo usan dos señales:



- SIGTERM (15): solicita que un programa deje de ejecutarse y le da algo de tiempo para guardar todo su progreso. Si no especifica la señal al ingresar el comando kill, se usará esta señal.
- SIGKILL (9): obliga a los programas a detenerse inmediatamente. El progreso no guardado se perderá.

Además de conocer las señales, también necesita conocer el número de identificación del proceso (PID) del programa que desea matar. Si no conoce el PID, simplemente ejecute el comando “ps ux”.

Después de saber qué señal desea usar y el PID del programa, ingrese la siguiente sintaxis:

kill [opción de señal] PID .

## 25. comando “ping”

Utilice el comando ping para verificar el estado de su conectividad a un servidor. Por ejemplo, simplemente ingresando ping google.com, el comando verificará si puede conectarse a Google y también medirá el tiempo de respuesta.

## 26. comando “wget”

La línea de comandos de Linux es muy útil; incluso puede descargar archivos de Internet con la ayuda del comando wget. Para hacerlo, simplemente escriba wget seguido del enlace de descarga.

## 27. comando “uname”

El comando uname , abreviatura de Unix Name, imprimirá información detallada sobre su sistema Linux, como el nombre de la máquina, el sistema operativo, el kernel, etc.

## 28. comando “top”

Como terminal equivalente al Administrador de tareas en Windows, el comando “top” mostrará una lista de procesos en ejecución y cuánta CPU usa cada proceso. Es muy útil monitorear el uso de recursos del sistema, especialmente sabiendo qué proceso debe terminarse porque consume demasiados recursos. Busque referencias sobre “htop”.



### 29. comando “history”

Cuando haya estado usando Linux durante un cierto período de tiempo, notará rápidamente que puede ejecutar cientos de comandos todos los días. Como tal, ejecutar el comando “history” es particularmente útil si desea revisar los comandos que ha ingresado antes.

### 30. comando “man”

¿Confundido acerca de la función de ciertos comandos de Linux? No se preocupe, puede aprender fácilmente cómo usarlos directamente desde el shell de Linux usando el comando man. Por ejemplo, ingresar man tail mostrará la instrucción manual del comando tail.

### 31. comando “echo”

Este comando se usa para mover algunos datos a un archivo. Por ejemplo, si desea agregar el texto "Hola, mi nombre es Juan" en un archivo llamado nombre.txt, debe escribir “echo Hola, mi nombre es Juan >> nombre.txt”.

### 32. comando “zip,unzip”

Use el comando zip para comprimir sus archivos en un archivo zip y use el comando unzip para extraer los archivos comprimidos de un archivo zip.

### 33. comando “hostname”

Si desea saber el nombre de su host / red, simplemente escriba hostname. Si agrega un -i al final, se mostrará la dirección IP de su red.

### 34. comando “useradd, userdel”

Dado que Linux es un sistema multiusuario, esto significa que más de una persona puede interactuar con el mismo sistema al mismo tiempo. useradd se usa para crear un nuevo usuario, mientras que



passwd agrega una contraseña a la cuenta de ese usuario. Para agregar una nueva persona llamada John escriba, useradd John y luego para agregar su tipo de contraseña, passwd 123456789.

Eliminar un usuario es muy similar a agregar un nuevo usuario. Para eliminar el tipo de cuenta de usuario, userdel UserName

#### Notas:

- Utilice el comando “clear” para limpiar la terminal si se llena de demasiados comandos anteriores.
- Pruebe el botón TAB para completar automáticamente lo que está escribiendo. Por ejemplo, si necesita escribir Documentos, comience a escribir un comando (vayamos con cd Docu, luego presione la tecla TAB) y el terminal completará el resto, mostrándole Documentos de cd.
- Ctrl + C y Ctrl + Z se utilizan para detener cualquier comando que esté funcionando actualmente. Ctrl + C detendrá y terminará el comando, mientras que Ctrl + Z simplemente pausará el comando.
- Si accidentalmente congela su terminal utilizando Ctrl + S, basta con descongelar usando Ctrl + Q.
- Ctrl + A lo mueve al principio de la línea, mientras que Ctrl + E lo mueve al final.
- Puede ejecutar varios comandos en un solo comando utilizando el “;” para separarlos. Por ejemplo Command1; Command2; Command3. O use && si solo desea que el siguiente comando se ejecute cuando el primero sea exitoso.



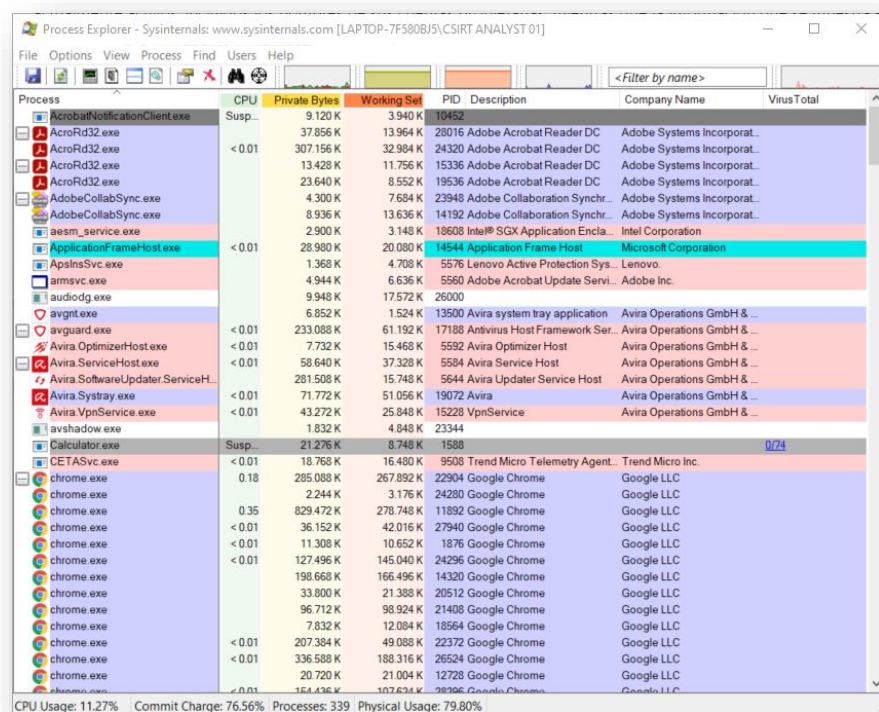
## Anexo II: Comandos o aplicativos básicos para Windows

En esta primera versión de comandos o aplicativos para Windows mencionaremos el aplicativo “ProcessExplorer de la suite SYSINTERNALS”.

¿Alguna vez se preguntó qué programa tiene abierto un archivo o directorio en particular? Ahora puedes averiguarlo. Process Explorer le muestra información sobre qué identificadores y procesos DLL se han abierto o cargado.

La pantalla del Explorador de procesos consta de dos subventanas. La ventana superior siempre muestra una lista de los procesos actualmente activos, incluidos los nombres de sus cuentas propietarias, mientras que la información que se muestra en la ventana inferior depende del modo en el que se encuentre “Process Explorer”: si está en modo de control, verá el manejo que el proceso seleccionado en la ventana superior se ha abierto; si Process Explorer está en modo DLL, verá las DLL y los archivos asignados en memoria que ha cargado el proceso. Process Explorer también tiene una poderosa capacidad de búsqueda que le mostrará rápidamente qué procesos tienen identificadores particulares abiertos o DLL cargados.

Las capacidades únicas de Process Explorer lo hacen útil para rastrear problemas de la versión DLL o manejar fugas, y brindan información sobre la forma en que funcionan Windows y las aplicaciones.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virus Total
AcrobatNotificationClient.exe	Susp...	9,120 K	3,940 K	10452			
AcroRd32.exe		37,856 K	13,964 K	28016	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AcroRd32.exe	< 0.01	307,156 K	32,984 K	24320	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AcroRd32.exe		13,428 K	11,756 K	15336	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AcroRd32.exe		23,640 K	8,552 K	19536	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AdobeCollabSync.exe		4,300 K	7,684 K	23948	Adobe Collaboration Synchr...	Adobe Systems Incorporat...	
AdobeCollabSync.exe		8,936 K	13,636 K	14192	Adobe Collaboration Synchr...	Adobe Systems Incorporat...	
aesm_service.exe		2,900 K	3,148 K	18608	Intel® SGX Application Encla...	Intel Corporation	
ApplicationFrameHost.exe	< 0.01	28,980 K	20,080 K	14544	Application Frame Host	Microsoft Corporation	
ApslnsSvc.exe		1,368 K	4,708 K	5576	Lenovo Active Protection Sys...	Lenovo	
armsvc.exe		4,944 K	6,636 K	5560	Adobe Acrobat Update Servi...	Adobe Inc.	
audiodg.exe		9,948 K	17,572 K	26000			
avgnt.exe		6,852 K	1,524 K	13500	Avira system tray application	Avira Operations GmbH & ...	
avguard.exe	< 0.01	233,088 K	61,192 K	17188	Antivirus Host Framework Ser...	Avira Operations GmbH & ...	
Avira.OptimizerHost.exe	< 0.01	7,732 K	15,468 K	5592	Avira Optimizer Host	Avira Operations GmbH & ...	
Avira.ServiceHost.exe	< 0.01	58,640 K	37,328 K	5584	Avira Service Host	Avira Operations GmbH & ...	
Avira.SoftwareUpdater.ServiceH...	< 0.01	281,508 K	15,748 K	5644	Avira Updater Service Host	Avira Operations GmbH & ...	
Avira.Sys tray.exe	< 0.01	71,772 K	51,056 K	19072	Avira	Avira Operations GmbH & ...	
Avira.VpnService.exe	< 0.01	43,272 K	25,848 K	15228	VpnService	Avira Operations GmbH & ...	
avshadow.exe		1,832 K	4,848 K	23344			
Calculator.exe	Susp...	21,276 K	8,748 K	1588			0/74
CETASvc.exe	< 0.01	18,768 K	16,480 K	9508	Trend Micro Telemetry Agent...	Trend Micro Inc.	
chrome.exe	0.18	285,088 K	267,892 K	22904	Google Chrome	Google LLC	
chrome.exe		2,244 K	3,176 K	24280	Google Chrome	Google LLC	
chrome.exe	0.35	829,472 K	278,748 K	11892	Google Chrome	Google LLC	
chrome.exe	< 0.01	36,152 K	42,016 K	27940	Google Chrome	Google LLC	
chrome.exe	< 0.01	11,308 K	10,652 K	1876	Google Chrome	Google LLC	
chrome.exe	< 0.01	127,496 K	145,040 K	24296	Google Chrome	Google LLC	
chrome.exe		198,668 K	166,496 K	14320	Google Chrome	Google LLC	
chrome.exe		33,800 K	21,388 K	20512	Google Chrome	Google LLC	
chrome.exe		96,712 K	98,924 K	21408	Google Chrome	Google LLC	
chrome.exe		7,832 K	12,084 K	18564	Google Chrome	Google LLC	
chrome.exe	< 0.01	207,384 K	49,088 K	22372	Google Chrome	Google LLC	
chrome.exe	< 0.01	336,588 K	188,316 K	26524	Google Chrome	Google LLC	
chrome.exe		20,720 K	21,004 K	12728	Google Chrome	Google LLC	
chrome.exe	< 0.01	154,436 K	107,636 K	28396	Google Chrome	Google LLC	

CPU Usage: 11.27% Commit Charge: 76.56% Processes: 339 Physical Usage: 79.80%

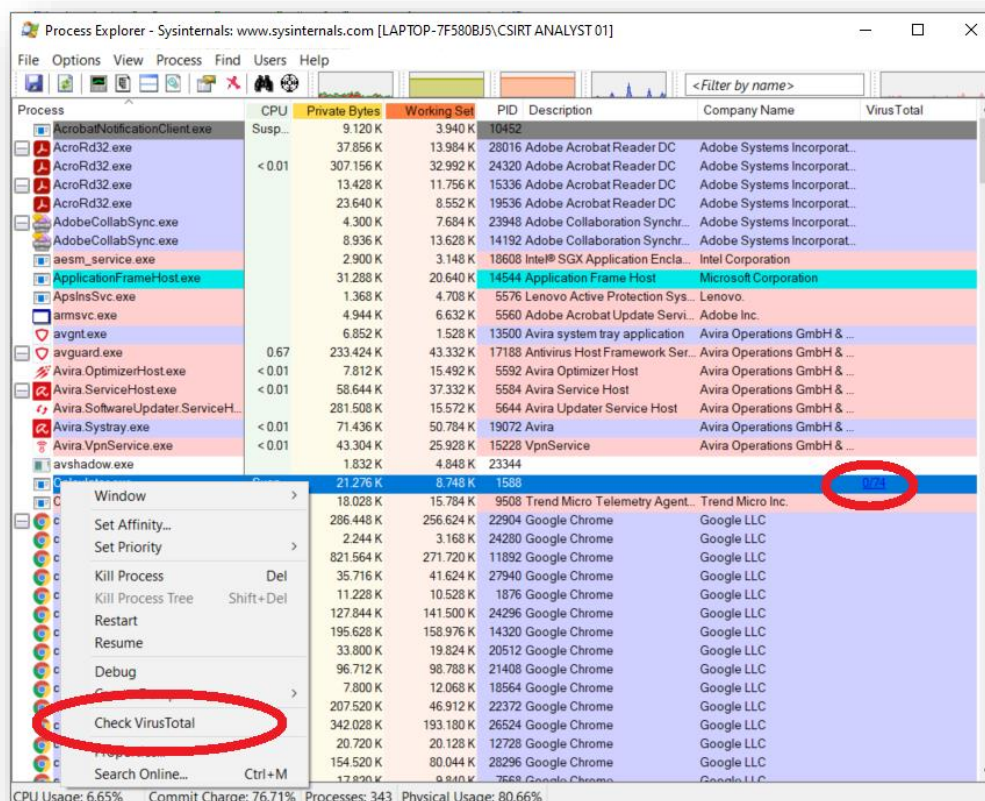


Este programa puede descargarlo desde:

<https://download.sysinternals.com/files/ProcessExplorer.zip>

Cuando el usuario lo analice verá que tiene funciones similares al taskmanager o administrador de tareas que viene nativamente en Windows, pero lo sorprenderán gratamente otras potentes funciones aplicadas a seguridad, como por ejemplo la posibilidad de con un click lanzar un chequeo de un proceso sospechoso contra la base de datos VirusTotal, desplegándonos en la misma pantalla el resultado.

A modo de ejemplo, suponemos que el proceso Calculator.exe es sospechoso. Con el botón derecho del mouse, nos aparece un menú contextual con la opción de "Check VirusTotal". La seleccionamos y en esa misma pantalla en la última columna "Virus Total" se mostrará el SCORE que este sistema entrega para el HASH de ese proceso. En este caso muestra "0/74", que quiere decir que de los 74 antivirus ninguno lo reconoce como malicioso.



Con estos tips básicos buscamos incentivarlo a explorar esta herramienta y sus múltiples usos para ciberseguridad.