



13 de agosto de 2021  
Ficha N° 16 ANUBIS  
CSIRT DE GOBIERNO

## Comando de la semana “ANUBIS”

### I. CONTEXTO

Este documento, denominado, en esta oportunidad, “ANUBIS”, 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 sitios o sistemas web 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#, C++, Golang, JavaScript, PowerShell, Ruby, Java, PHP, Elixir, Elm, Go, Dart, DLang, Pony, TypeScript, Kotlin, Nim, OCaml, Q#<sup>2</sup>, Reason, Rust (RustyBuer), 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.

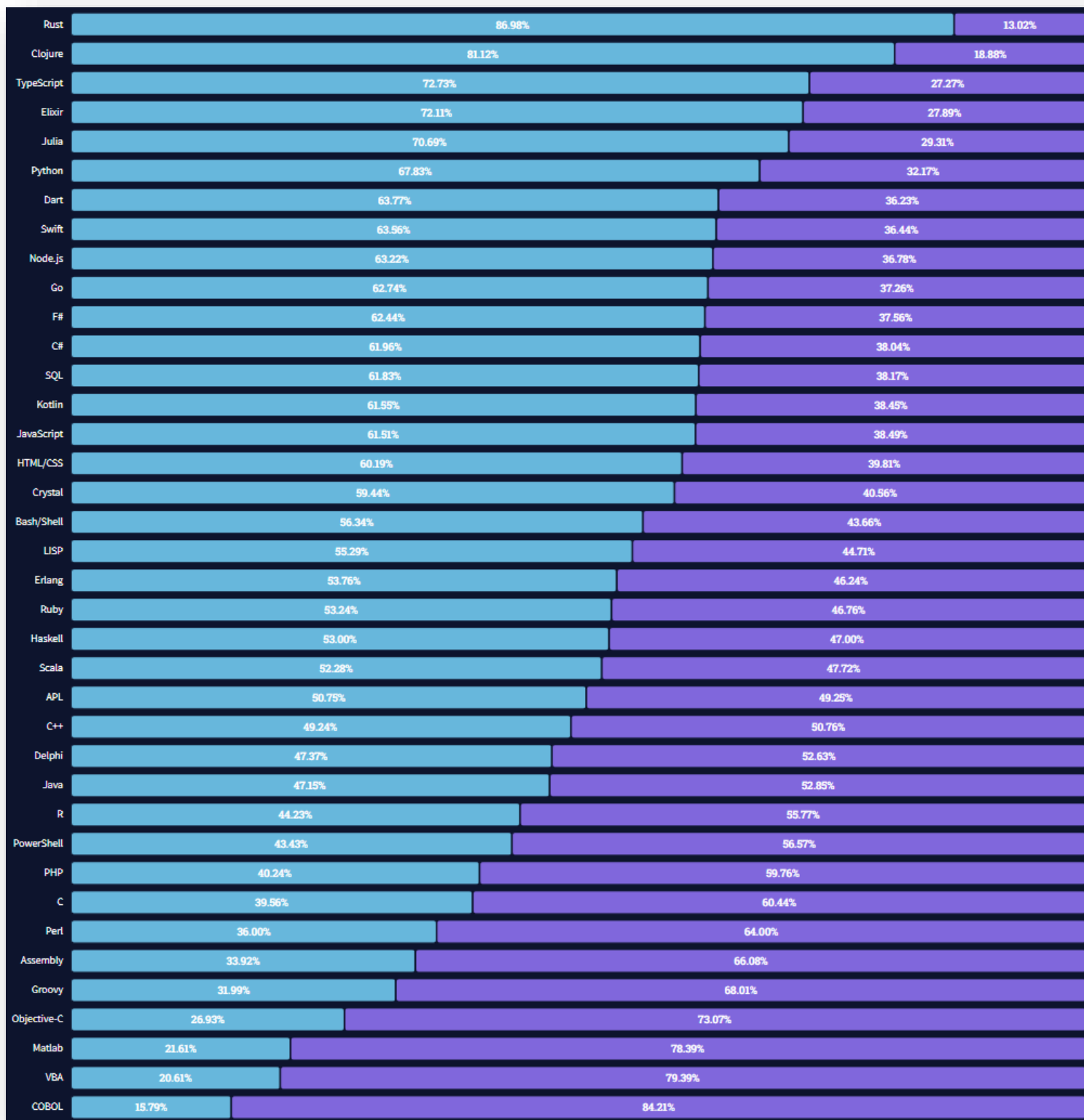
Es importante que conozca al menos lo básico de los lenguajes más nuevos o no convencionales, pues se ha detectado que los desarrolladores de malware van incorporándolos como estrategia de ofuscación, para dificultar la detección y análisis que proveen las soluciones de seguridad.

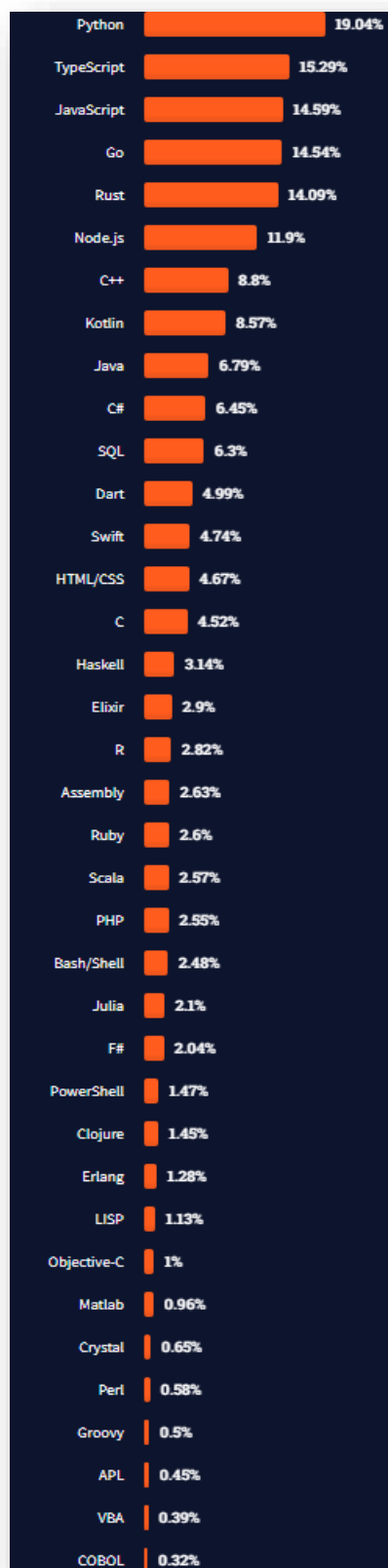
Solo a modo de curiosidad se comparte un gráfico en el que se muestra el resultado de una encuesta entre muchos desarrolladores, dejando ver que lenguajes son más queridos/temidos (primer gráfico) y luego cuales son los más preferidos<sup>3</sup> (segundo gráfico).

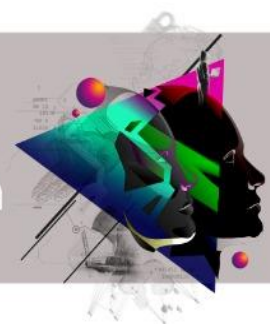
<sup>1</sup> <https://scis.uohyd.ac.in/~apcs/itw/UNIXProgrammingEnvironment.pdf>

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

<sup>3</sup> <https://insights.stackoverflow.com/survey/2021#most-loved-dreaded-and-wanted-language-love-dread>







## II. INTRODUCCIÓN

Una de las tareas regulares que un encargado de ciberseguridad debe realizar es la **ENUMERACIÓN**. La enumeración es una actividad de reconocimiento en la cual se consigue información de usuarios, grupos o dispositivos, dominios relacionados y demás servicios relacionados con un determinado activo expuesto a Internet.

Conocer esta información es importante, pues es lo que un hacker está haciendo en sus primeros pasos para llevar adelante un ataque en etapas posteriores.

En este sentido es importante tener en perspectiva el concepto de Cyber Kill Chain.

La Cyber Kill Chain, es una secuencia de los pasos que en general siguen los ciberdelincuentes cuando atacan nuestros sitios o sistemas expuestos en Internet:

- 1) Reconocimiento: el intruso selecciona el objetivo, lo investiga e intenta identificar las vulnerabilidades en la red objetivo.
- 2) Armamento: el intruso crea un arma de malware de acceso remoto, como un virus o un gusano, adaptada a una o más vulnerabilidades.
- 3) Entrega: el intruso transmite el arma al objetivo (por ejemplo, a través de archivos adjuntos de correo electrónico, sitios web o unidades USB).
- 4) Explotación: se activa el código del programa del arma de malware, que toma medidas en la red objetivo para aprovechar la vulnerabilidad.
- 5) Instalación: el arma de malware instala un punto de acceso (por ejemplo, "puerta trasera") que puede utilizar un intruso.

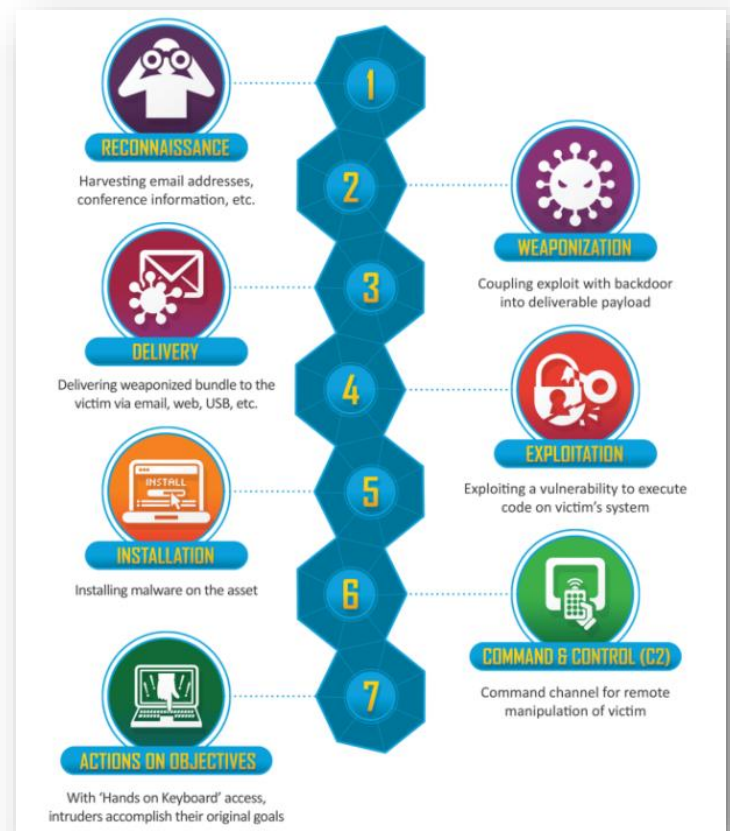


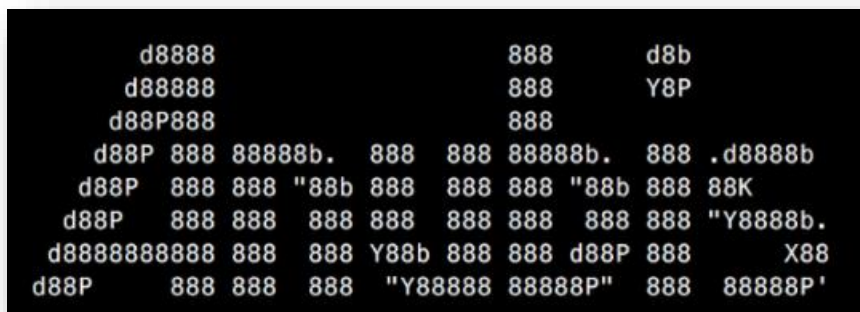
Ilustración 1 Cyber Kill Chain



- 6) Comando y control: el malware permite al intruso tener acceso persistente "con las manos en el teclado" a la red de destino.
- 7) Acciones sobre el objetivo: el intruso toma medidas para lograr sus objetivos, como la exfiltración de datos, la destrucción de datos o el cifrado para obtener un rescate.

### ¿Qué es ANUBIS?

- Anubis es una herramienta de recopilación de información y enumeración de subdominios. Anubis recopila datos de una variedad de fuentes, incluidos HackerTarget, DNSDumpster, certificados x509, VirusTotal, Google, Pkey, Sublist3r, Shodan y NetCraft. Anubis también tiene un proyecto hermano, AnubisDB , que sirve como un repositorio centralizado de subdominios.



**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.

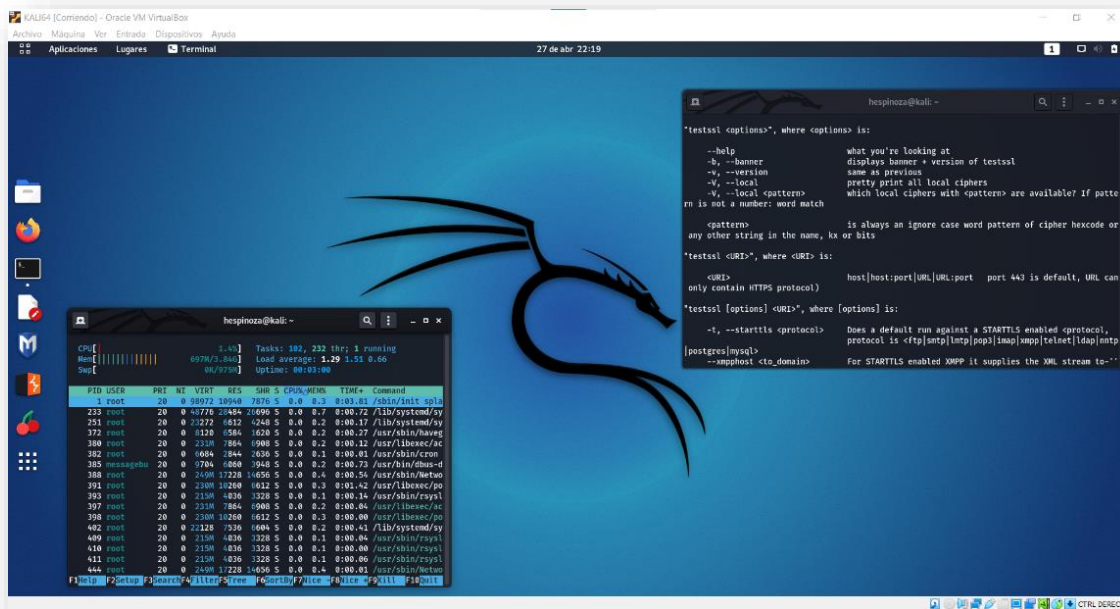
### Vea anexo II: Comandos o aplicativos básicos para Windows: TCPView



### 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”**:

Primero nos aseguramos que los pre-requisitos estén cumplidos:

```
# apt install python3-pip python-dev libssl-dev libffi-dev
```

Leyendo lista de paquetes... Hecho

Creando árbol de dependencias... Hecho

Leyendo la información de estado... Hecho

Nota, seleccionando «python-dev-is-python2» en lugar de «python-dev»

libffi-dev ya está en su versión más reciente (3.3-6).

fijado libffi-dev como instalado manualmente.

python3-pip ya está en su versión más reciente (20.3.4-4).

Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.

gccgo-10 libgo-10-dev libgo16 python-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.

Se instalarán los siguientes paquetes adicionales:

libpython2-dev libpython2.7 libpython2.7-dev python2-dev python2.7-dev

Paquetes sugeridos:

libssl-doc

Se instalarán los siguientes paquetes NUEVOS:

libpython2-dev libpython2.7 libpython2.7-dev libssl-dev python-dev-is-python2 python2-dev python2.7-dev

0 actualizados, 7 nuevos se instalarán, 0 para eliminar y 0 no actualizados.

Se necesita descargar 5.503 kB de archivos.

Se utilizarán 25,3 MB de espacio de disco adicional después de esta operación.

¿Desea continuar? [S/n] S

Des:1 http://mirror.ufro.cl/kali kali-rolling/main amd64 libpython2.7 amd64 2.7.18-8 [1.022 kB]

Des:2 http://mirror.ufro.cl/kali kali-rolling/main amd64 libpython2.7-dev amd64 2.7.18-8 [2.354 kB]

Des:3 http://mirror.ufro.cl/kali kali-rolling/main amd64 libpython2-dev amd64 2.7.18-3 [21,3 kB]

Des:4 http://mirror.ufro.cl/kali kali-rolling/main amd64 libssl-dev amd64 1.1.1k-1 [1.810 kB]

Des:5 http://mirror.ufro.cl/kali kali-rolling/main amd64 python2.7-dev amd64 2.7.18-8 [291 kB]

Des:6 http://mirror.ufro.cl/kali kali-rolling/main amd64 python2-dev amd64 2.7.18-3 [1.216 B]

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



```
Des:7 http://mirror.ufro.cl/kali kali-rolling/main amd64 python-dev-is-python2 all 2.7.18-9 [1.528
B]
Descargados 5.503 kB en 6s (910 kB/s)
Seleccionando el paquete libpython2.7:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 538185 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../0-libpython2.7_2.7.18-8_amd64.deb ...
Desempaquetando libpython2.7:amd64 (2.7.18-8) ...
Seleccionando el paquete libpython2.7-dev:amd64 previamente no seleccionado.
Preparando para desempaquetar .../1-libpython2.7-dev_2.7.18-8_amd64.deb ...
Desempaquetando libpython2.7-dev:amd64 (2.7.18-8) ...
Seleccionando el paquete libpython2-dev:amd64 previamente no seleccionado.
Preparando para desempaquetar .../2-libpython2-dev_2.7.18-3_amd64.deb ...
Desempaquetando libpython2-dev:amd64 (2.7.18-3) ...
Seleccionando el paquete libssl-dev:amd64 previamente no seleccionado.
Preparando para desempaquetar .../3-libssl-dev_1.1.1k-1_amd64.deb ...
Desempaquetando libssl-dev:amd64 (1.1.1k-1) ...
Seleccionando el paquete python2.7-dev previamente no seleccionado.
Preparando para desempaquetar .../4-python2.7-dev_2.7.18-8_amd64.deb ...
Desempaquetando python2.7-dev (2.7.18-8) ...
Seleccionando el paquete python2-dev previamente no seleccionado.
Preparando para desempaquetar .../5-python2-dev_2.7.18-3_amd64.deb ...
Desempaquetando python2-dev (2.7.18-3) ...
Seleccionando el paquete python-dev-is-python2 previamente no seleccionado.
Preparando para desempaquetar .../6-python-dev-is-python2_2.7.18-9_all.deb ...
Desempaquetando python-dev-is-python2 (2.7.18-9) ...
Configurando libpython2.7:amd64 (2.7.18-8) ...
Configurando libpython2.7-dev:amd64 (2.7.18-8) ...
Configurando libssl-dev:amd64 (1.1.1k-1) ...
Configurando libpython2-dev:amd64 (2.7.18-3) ...
Configurando python2.7-dev (2.7.18-8) ...
Configurando python2-dev (2.7.18-3) ...
Configurando python-dev-is-python2 (2.7.18-9) ...
Procesando disparadores para libc-bin (2.31-13) ...
Procesando disparadores para man-db (2.9.4-2) ...
Procesando disparadores para kali-menu (2021.2.3) ...
Scanning processes...
Scanning candidates...
Scanning processor microcode...
Scanning linux images...

The processor microcode seems to be up-to-date.

Restarting services...
Service restarts being deferred:
```



```
systemctl restart NetworkManager.service  
/etc/needrestart/restart.d/dbus.service  
systemctl restart docker.service  
systemctl restart gdm.service  
systemctl restart gdm3.service  
systemctl restart systemd-logind.service  
systemctl restart user@1000.service  
systemctl restart wpa_supplicant.service
```

No containers need to be restarted.

No user sessions are running outdated binaries.

Luego instalamos el comando propiamente tal:

#### # pip3 install anubis-netsec

```
Collecting anubis-netsec  
  Downloading anubis_netsec-1.0.3-py2.py3-none-any.whl (24 kB)  
Collecting censys==1.1.0  
  Downloading censys-1.1.0-py2.py3-none-any.whl (25 kB)  
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from anubis-netsec)  
(52.0.0)  
Requirement already satisfied: shodan==1.25.0 in /usr/lib/python3/dist-packages (from anubis-  
netsec) (1.25.0)  
Requirement already satisfied: requests==2.25.1 in /usr/lib/python3/dist-packages (from anubis-  
netsec) (2.25.1)  
Requirement already satisfied: docopt==0.6.2 in /usr/lib/python3/dist-packages (from anubis-  
netsec) (0.6.2)  
Collecting dnspython==2.1.0  
  Downloading dnspython-2.1.0-py3-none-any.whl (241 kB)  
|████████████████████████████████████████████████████████████████████████████████| 241 kB 5.1 MB/s  
Collecting python-nmap==0.6.1  
  Downloading python-nmap-0.6.1.tar.gz (41 kB)  
|████████████████████████████████████████████████████████████████████████████████| 41 kB 104 kB/s  
Collecting backoff  
  Downloading backoff-1.11.1-py2.py3-none-any.whl (13 kB)  
Building wheels for collected packages: python-nmap  
  Building wheel for python-nmap (setup.py) ... done  
  Created wheel for python-nmap: filename=python_nmap-0.6.1-py3-none-any.whl size=19325  
sha256=3be8d3db4913dcc2a757f3bd7aab380247c4dcdfc3282c841c4f3c6725c0337e
```



```
Stored                               in                               directory:
/root/.cache/pip/wheels/b2/eb/df/9c2e680e24254f766895752b1d6e639b8fd91837a74f278156
Successfully built python-nmap
Installing collected packages: backoff, python-nmap, dnspython, censys, anubis-netsec
Attempting uninstall: dnspython
  Found existing installation: dnspython 2.0.0
  Not uninstalling dnspython at /usr/lib/python3/dist-packages, outside environment /usr
  Can't uninstall 'dnspython'. No files were found to uninstall.
Successfully installed anubis-netsec-1.0.3 backoff-1.11.1 censys-1.1.0 dnspython-2.1.0 python-
nmap-0.6.1
```



### 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: “anubis -h”.

```
root@V: ~  
  
(root@V) ~  
#  
  
(root@V) ~  
# anubis -h  
Usage:  
  anubis (-t TARGET | -f FILE) [-o FILENAME] [-abinoprsv] [-w SCAN] [-q NUM]  
  anubis -h  
  anubis --version  
  
Options:  
  -h --help                show this help message and exit  
  -t --target              set target (comma separated, no spaces, if multiple)  
  -f --file               set target (reads from file, one domain per line)  
  -n --with-nmap          perform an nmap service/script scan  
  -o --output             save to filename  
  -i --additional-info    show additional information about the host from Shodan (requires API key)  
  -p --ip                 outputs the resolved IPs for each subdomain, and a full list of unique ips  
  -a --send-to-anubis-db  send results to Anubis-DB  
  -r --recursive          recursively search over all subdomains  
  -s --ssl                run an ssl scan and output cipher + chain info  
  -S --silent             only out put subdomains, one per line  
  -w --overwrite-nmap-scan SCAN overwrite default nmap scan (default -nPn -sV -sC)  
  -v --verbose            print debug info and full request output  
  -q --queue-workers NUM  override number of queue workers (default: 10, max: 100)  
  --version              show version and exit  
  
Help:  
  For help using this tool, please open an issue on the Github repository:  
  https://github.com/jonluca/anubis  
  
(root@V) ~  
#  
  
(root@V) ~  
#
```



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

Un ejemplo de ejecución básica para nuestros primeros pasos:

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

```

                                EJEMPLO 1 ANUBIS

                                Analizamos el dominio "csirt.gob.cl"

# anubis -t csirt.gob.cl

      d8888      888      d8b
      d88888      888      Y8P
      d88P888      888
      d88P 888 88888b. 888 888 88888b. 888 .d8888b
      d88P 888 888 "88b 888 888 888 "88b 888 88K
      d88P 888 888 888 888 888 888 888 "Y8888b.
      d8888888888 888 888 Y88b 888 888 d88P 888      X88
      d88P      888 888 888 "Y88888 88888P" 888 88888P'

Searching for subdomains for 163.247.172.147 (csirt.gob.cl)
Working on target: csirt.gob.cl
Testing for zone transfers
Searching HackerTarget
Searching for Subject Alt Names
Searching NetCraft.com
Searching crt.sh
Searching DNSDumpster
Searching Anubis-DB
Found 26 subdomains
-----
ws.diariooficial.interior.gob.cl
subinterior.gob.cl
www.csirt.gob.cl
*.extranjeria.gob.cl
reportes.ciberseguridad.gob.cl
www.diariooficial.interior.gob.cl
csirt.gob.cl
www.concienciadigital.gob.cl
concienciadigital.gob.cl
www.cecipu.gob.cl
*.interior.gov.cl
interior.gob.cl
pagos.diariooficial.cl
www.ciberseguridad.gob.cl
nic.gob.cl
wspagos.diariooficial.interior.gob.cl
ciberseguridad.gob.cl
www.subinterior.gob.cl
cecipu.gob.cl
*.minterior.gov.cl
*.interior.gob.cl
*.csirt.gob.cl
boletinoficialdemineria.cl
www.boletinoficialdemineria.cl

```





```
www.diariooficial.cl  
indicadores.ciberseguridad.gob.cl  
Subdomain search took 0:00:01.526
```

Otro ejemplo y como se vería en un browser el archivo report.html:

#### EJEMPLO 2 ANUBIS

Analizamos el dominio "reddit.com" incorporando un NMAP y grabando el resultado en un archivo "temp.txt"

```
# anubis -t reddit.com --with-nmap -o temp.txt -i --overwrite-nmap-scan "-F -T5"
```

Searching for subdomains for 151.101.65.140 (reddit.com)

Testing for zone transfers

Searching for Subject Alt Names

Searching HackerTarget

Searching VirusTotal

Searching Pkey.in

Searching NetCraft.com

Searching crt.sh

Searching DNSDumpster

Searching Anubis-DB

Searching Shodan.io for additional information

Server Location: San Francisco, US - 94107

ISP or Hosting Company: Fastly

To run a DNSSEC subdomain enumeration, Anubis must be run as root

Starting Nmap Scan

Host : 151.101.65.140 ()

-----

Protocol: tcp

port: 80 state: open

port: 443 state: open

Found 195 subdomains

-----

nm.reddit.com

ne.reddit.com

sonics.reddit.com

aj.reddit.com

fo.reddit.com

f5.reddit.com

... (truncated for readability)

Sending to AnubisDB

Subdomain search took 0:00:26.579

Otro ejemplo, pero esta vez incorporando una función de información adicional vía shodan:

```
anubis -t reddit.com -ip
```



```
d8888      888   d8b
d88888      888   Y8P
d88P888      888
d88P 888 88888b. 888 888 88888b. 888 .d8888b
d88P 888 888 "88b 888 888 888 "88b 888 88K
d88P 888 888 888 888 888 888 888 888 "Y8888b.
d88888888888 888 888 Y88b 888 888 d88P 888   X88
d88P 888 888 888 "Y88888 88888P" 888 88888P'
```

Searching for subdomains for 151.101.65.140 (reddit.com)

Working on target: reddit.com

Testing for zone transfers

Searching HackerTarget

Searching for Subject Alt Names

Searching NetCraft.com

Searching crt.sh

Searching DNSDumpster

Searching Anubis-DB

Searching Shodan.io for additional information

Server Location: San Francisco, US - None

ISP or Hosting Company: Fastly

Found 678 subdomains

```
-----
py.reddit.com: 151.101.1.140
n2.reddit.com: 151.101.1.140
zj.reddit.com: 151.101.1.140
rhs.reddit.com: 52.0.168.221
of.reddit.com: 151.101.1.140
android.reddit.com: 151.101.1.140
bt.reddit.com: 151.101.1.140
rachelbilson.reddit.com: 151.101.1.140
edgebucket.reddit.com: 151.101.1.140
hs.reddit.com: 151.101.1.140
cyberpunk.reddit.com: 151.101.1.140
69.reddit.com: 151.101.1.140
mc.reddit.com: 151.101.1.140
lk.reddit.com: 151.101.1.140
sp-oi.reddit.com: 151.101.1.140
cf.reddit.com: 151.101.1.140
fa-10.reddit.com: 151.101.1.140
mf.reddit.com: 151.101.1.140
medicine.reddit.com: 151.101.1.140
zz-di.reddit.com: 151.101.1.140
m1.reddit.com: 151.101.1.140
```



westernunion.com: 66.218.161.27  
sc.reddit.com: 151.101.1.140  
www.i.reddit.com: 151.101.1.140  
c1.reddit.com: 151.101.1.140  
k1.reddit.com: 151.101.1.140  
nb.reddit.com: 151.101.1.140  
gr.reddit.com: 151.101.1.140  
mm.reddit.com: 151.101.1.140  
za.reddit.com: 151.101.1.140  
mx03.reddit.com: 151.101.1.140  
democraciv.reddit.com: 151.101.1.140  
x5.reddit.com: 151.101.1.140  
go.reddit.com: 151.101.1.140  
op.reddit.com: 151.101.1.140  
fm.reddit.com: 151.101.1.140  
oa.reddit.com: 151.101.1.140  
mx.reddit.com: 151.101.1.140  
er.reddit.com: 151.101.1.140  
feet.reddit.com: 151.101.1.140  
h.reddit.com: 151.101.1.140  
fe.reddit.com: 151.101.1.140  
mr.reddit.com: 151.101.1.140  
03.reddit.com: 151.101.1.140  
conspiracy.reddit.com: 151.101.1.140  
vi.reddit.com: 151.101.1.140  
mx-03.reddit.com: 54.172.97.247  
code.reddit.com: 151.101.1.140  
ny.reddit.com: 151.101.1.140  
ti.reddit.com: 151.101.1.140  
w.reddit.com: 151.101.1.140  
as.reddit.com: 151.101.1.140  
fa-02.reddit.com: 151.101.1.140  
gm.reddit.com: 151.101.1.140  
www.reddit.com: 151.101.1.140  
hc.reddit.com: 151.101.1.140  
wh.reddit.com: 151.101.1.140  
oe.reddit.com: 151.101.1.140  
l1.reddit.com: 151.101.1.140  
bd.reddit.com: 151.101.1.140  
pc.reddit.com: 151.101.1.140  
sr.reddit.com: 151.101.1.140  
nintendo.reddit.com: 151.101.1.140  
ak.reddit.com: 151.101.1.140  
ep.reddit.com: 151.101.1.140



wu.reddit.com: 151.101.1.140  
sendbird.reddit.com: 151.101.1.140  
va.reddit.com: 151.101.1.140  
ku.reddit.com: 151.101.1.140  
ft.reddit.com: 151.101.1.140  
googlesheets.reddit.com: 151.101.1.140  
filthyfrank.reddit.com: 151.101.1.140  
bs.reddit.com: 151.101.1.140  
events.reddit.com: 151.101.1.140  
jc.reddit.com: 151.101.1.140  
lb.reddit.com: 151.101.1.140  
un.reddit.com: 151.101.1.140  
nsfwhardcore.reddit.com: 151.101.1.140  
qx.reddit.com: 151.101.1.140  
ho.reddit.com: 151.101.1.140  
qs.reddit.com: 151.101.1.140  
ua.reddit.com: 151.101.1.140  
d.reddit.com: 151.101.1.140  
alpha.reddit.com: 151.101.1.140  
static.reddit.com: 151.101.1.140  
actuallesbians.reddit.com: 151.101.1.140  
no-sp.reddit.com: 151.101.1.140  
1hp.reddit.com: 151.101.1.140  
yt.reddit.com: 151.101.1.140  
ld.reddit.com: 151.101.1.140  
bi.reddit.com: 151.101.1.140  
sa.reddit.com: 151.101.1.140  
ro-no.reddit.com: 151.101.1.140  
xx-di.reddit.com: 151.101.1.140  
us.reddit.com: 151.101.1.140  
gk.reddit.com: 151.101.1.140  
fa.reddit.com: 151.101.1.140  
po.reddit.com: 151.101.1.140  
www.pt.reddit.com: 151.101.1.140  
mailp236.reddit.com: 151.101.1.140  
ye.reddit.com: 151.101.1.140  
xx-me.reddit.com: 151.101.1.140  
eu.reddit.com: 151.101.1.140  
hg.reddit.com: 151.101.1.140  
fl.reddit.com: 151.101.1.140  
fq.reddit.com: 151.101.1.140  
it.reddit.com: 151.101.1.140  
al.reddit.com: 151.101.1.140  
darknetmarkets.reddit.com: 151.101.1.140



indieheads.reddit.com: 151.101.1.140  
ff.reddit.com: 151.101.1.140  
tr.reddit.com: 151.101.1.140  
ni.reddit.com: 151.101.1.140  
rx.reddit.com: 151.101.1.140  
ii.reddit.com: 151.101.1.140  
ads.reddit.com: 151.101.1.140  
francophonie.reddit.com: 151.101.1.140  
zy.reddit.com: 151.101.1.140  
artstore.reddit.com: 151.101.1.140  
gl.reddit.com: 151.101.1.140  
wahoostipi.reddit.com: 151.101.1.140  
pz.reddit.com: 151.101.1.140  
kr-01.reddit.com: 151.101.1.140  
askgsm.reddit.com: 151.101.1.140  
to.reddit.com: 151.101.1.140  
uq.reddit.com: 151.101.1.140  
worldofwarships.reddit.com: 151.101.1.140  
stcatharineson.reddit.com: 151.101.1.140  
k2.reddit.com: 151.101.1.140  
ll.reddit.com: 151.101.1.140  
w2.reddit.com: 151.101.1.140  
mj.reddit.com: 151.101.1.140  
ie.reddit.com: 151.101.1.140  
tipofmypenis.reddit.com: 151.101.1.140  
ln.reddit.com: 151.101.1.140  
fo.reddit.com: 151.101.1.140  
dn.reddit.com: 151.101.1.140  
www.h.reddit.com: 151.101.1.140  
sq.reddit.com: 151.101.1.140  
fa-15.reddit.com: 151.101.1.140  
anime.reddit.com: 151.101.1.140  
fc.reddit.com: 151.101.1.140  
mh.reddit.com: 151.101.1.140  
gv.reddit.com: 151.101.1.140  
ow-25.reddit.com: 151.101.1.140  
ga.reddit.com: 151.101.1.140  
milf.reddit.com: 151.101.1.140  
vm.reddit.com: 151.101.1.140  
ow.reddit.com: 151.101.1.140  
uu.reddit.com: 151.101.1.140  
tc.reddit.com: 151.101.1.140  
cx.reddit.com: 151.101.1.140  
bl.reddit.com: 151.101.1.140



at.reddit.com: 151.101.1.140  
xanaxcartel.reddit.com: 151.101.1.140  
ri-ck.reddit.com: 151.101.1.140  
zh.reddit.com: 151.101.1.140  
lu.reddit.com: 151.101.1.140  
\*.reddit.com:  
mg.reddit.com: 151.101.1.140  
di.reddit.com: 151.101.1.140  
brooklyn.reddit.com: 151.101.1.140  
aa.reddit.com: 151.101.1.140  
redditama.reddit.com: 151.101.1.140  
zz-an.reddit.com: 151.101.1.140  
xi.reddit.com: 151.101.1.140  
ffxiv.reddit.com: 151.101.1.140  
xo.reddit.com: 151.101.1.140  
buttons.reddit.com: 151.101.1.140  
onions.reddit.com: 151.101.1.140  
i.www.reddit.com: 151.101.1.140  
kratom.reddit.com: 151.101.1.140  
pt.reddit.com: 151.101.1.140  
te.reddit.com: 151.101.1.140  
gw.reddit.com: 151.101.1.140  
on.reddit.com: 151.101.1.140  
theredpill.reddit.com: 151.101.1.140  
lgbteens.reddit.com: 151.101.1.140  
hx.reddit.com: 151.101.1.140  
xu.reddit.com: 151.101.1.140  
gc.reddit.com: 151.101.1.140  
bo.reddit.com: 151.101.1.140  
ki.reddit.com: 151.101.1.140  
lgbtpolitics.reddit.com: 151.101.1.140  
pm.reddit.com: 151.101.1.140  
xx-he.reddit.com: 151.101.1.140  
coyotes.reddit.com: 151.101.1.140  
nu.reddit.com: 151.101.1.140  
sh-it.reddit.com: 151.101.1.140  
gg.reddit.com: 151.101.1.140  
dt.reddit.com: 151.101.1.140  
sf.reddit.com: 151.101.1.140  
nc-nm.reddit.com: 151.101.1.140  
kt.reddit.com: 151.101.1.140  
pl.reddit.com: 151.101.1.140  
www.tls-test-1.reddit.com: 151.101.1.140  
africa.reddit.com: 151.101.1.140





s8.reddit.com: 151.101.1.140  
c4.reddit.com: 151.101.1.140  
xl.reddit.com: 151.101.1.140  
sfgiants.reddit.com: 151.101.1.140  
tp.reddit.com: 151.101.1.140  
mailgun.org: 44.240.48.222  
xq.reddit.com: 151.101.1.140  
amp.reddit.com: 151.101.1.140  
de.reddit.com: 151.101.1.140  
nz.reddit.com: 151.101.1.140  
tls-test-2.reddit.com: 151.101.1.140  
ag.reddit.com: 151.101.1.140  
mk.reddit.com: 151.101.1.140  
doctorwho.reddit.com: 151.101.1.140  
fa-04.reddit.com: 151.101.1.140  
baseball.reddit.com: 151.101.1.140  
bostonbruins.reddit.com: 151.101.1.140  
clashofclans.reddit.com: 151.101.1.140  
iv.reddit.com: 151.101.1.140  
fn.reddit.com: 151.101.1.140  
dh.reddit.com: 151.101.1.140  
bettertouchtool.reddit.com: 151.101.1.140  
fa-11.reddit.com: 151.101.1.140  
em.reddit.com: 151.101.1.140  
no.reddit.com: 151.101.1.140  
dell.com: 143.166.147.101  
lm.reddit.com: 151.101.1.140  
lg.reddit.com: 151.101.1.140  
ty.reddit.com: 151.101.1.140  
im.reddit.com: 151.101.1.140  
xe.reddit.com: 151.101.1.140  
le.reddit.com: 151.101.1.140  
politics.reddit.com: 151.101.1.140  
if.reddit.com: 151.101.1.140  
nt.reddit.com: 151.101.1.140  
ads-api.reddit.com: 151.101.1.140  
chicubs.reddit.com: 151.101.1.140  
thesilphroad.reddit.com: 151.101.1.140  
jailbreak.reddit.com: 151.101.1.140  
zz.reddit.com: 151.101.1.140  
ms.reddit.com: 151.101.1.140  
fs.reddit.com: 151.101.1.140  
rr.reddit.com: 151.101.1.140  
nr.reddit.com: 151.101.1.140



p1.reddit.com: 151.101.1.140  
timberwolves.reddit.com: 151.101.1.140  
esotools.reddit.com: 151.101.1.140  
minnesota.reddit.com: 151.101.1.140  
xh.reddit.com: 151.101.1.140  
ae.reddit.com: 151.101.1.140  
tls-test-1.reddit.com: 151.101.1.140  
orlando.reddit.com: 151.101.1.140  
dota2.reddit.com: 151.101.1.140  
lp.reddit.com: 151.101.1.140  
trustpositifkominfo:  
psx.reddit.com: 151.101.1.140  
vip.reddit.com: 151.101.1.140  
xy.reddit.com: 151.101.1.140  
wwwold.reddit.com: 151.101.1.140  
learnprogramming.reddit.com: 151.101.1.140  
netsec.reddit.com: 151.101.1.140  
rc.reddit.com: 151.101.1.140  
hz.reddit.com: 151.101.1.140  
stlouis.reddit.com: 151.101.1.140  
ja.reddit.com: 151.101.1.140  
ko.reddit.com: 151.101.1.140  
ha.reddit.com: 151.101.1.140  
an.reddit.com: 151.101.1.140  
dc.reddit.com: 151.101.1.140  
sj.reddit.com: 151.101.1.140  
hu.reddit.com: 151.101.1.140  
new.reddit.com: 151.101.1.140  
ro-ge.reddit.com: 151.101.1.140  
cu.reddit.com: 151.101.1.140  
ig.reddit.com: 151.101.1.140  
el.reddit.com: 151.101.1.140  
unitedkingdom.reddit.com: 151.101.1.140  
b3.reddit.com: 151.101.1.140  
ps.reddit.com: 151.101.1.140  
gql.reddit.com: 151.101.1.140  
www.amd.com: 23.59.25.40  
xn.reddit.com: 151.101.1.140  
lo.reddit.com: 151.101.1.140  
je.reddit.com: 151.101.1.140  
excons.reddit.com: 151.101.1.140  
dl.reddit.com: 151.101.1.140  
bj.reddit.com: 151.101.1.140  
av.reddit.com: 151.101.1.140



01.reddit.com: 151.101.1.140  
sd.reddit.com: 151.101.1.140  
mu.reddit.com: 151.101.1.140  
fy.reddit.com: 151.101.1.140  
s0.reddit.com: 151.101.1.140  
me.reddit.com: 151.101.1.140  
qf.reddit.com: 151.101.1.140  
michigan.reddit.com: 151.101.1.140  
casualconversation.reddit.com: 151.101.1.140  
cumsluts.reddit.com: 151.101.1.140  
gentlemanboners.reddit.com: 151.101.1.140  
oauth.reddit.com: 151.101.1.140  
smoking.reddit.com: 151.101.1.140  
ge.reddit.com: 151.101.1.140  
cb.reddit.com: 151.101.1.140  
newenglandrevolution.reddit.com: 151.101.1.140  
cv.reddit.com: 151.101.1.140  
garlicoin.reddit.com: 151.101.1.140  
r1.reddit.com: 151.101.1.140  
nd.reddit.com: 151.101.1.140  
halloween.reddit.com: 151.101.1.140  
houston.reddit.com: 151.101.1.140  
e.reddit.com: 151.101.1.140  
nc.reddit.com: 151.101.1.140  
about.reddit.com: 151.101.1.140  
cr.reddit.com: 151.101.1.140  
gf.reddit.com: 151.101.1.140  
store.reddit.com: 151.101.1.140  
zv.reddit.com: 151.101.1.140  
globaloffensive.reddit.com: 151.101.1.140  
f2.reddit.com: 151.101.1.140  
ph.reddit.com: 151.101.1.140  
bass.reddit.com: 151.101.1.140  
caps.reddit.com: 151.101.1.140  
pokemon.reddit.com: 151.101.1.140  
gateway.reddit.com: 151.101.1.140  
www.vip.reddit.com: 151.101.1.140  
kf.reddit.com: 151.101.1.140  
wn.reddit.com: 151.101.1.140  
b1.reddit.com: 151.101.1.140  
d7.reddit.com: 151.101.1.140  
email.reddit.com: 44.240.48.222  
magicdeckbuilding.reddit.com: 151.101.1.140  
javdownloadcenter.reddit.com: 151.101.1.140



ghana.reddit.com: 151.101.1.140  
ym.reddit.com: 151.101.1.140  
mtgfinance.reddit.com: 151.101.1.140  
zooneydeschanel.reddit.com: 151.101.1.140  
hb.reddit.com: 151.101.1.140  
bh.reddit.com: 151.101.1.140  
legs.reddit.com: 151.101.1.140  
ow-01.reddit.com: 151.101.1.140  
os.reddit.com: 151.101.1.140  
nq.reddit.com: 151.101.1.140  
hl.reddit.com: 151.101.1.140  
beta.reddit.com: 151.101.1.140  
dr.reddit.com: 151.101.1.140  
08.reddit.com: 151.101.1.140  
d4.reddit.com: 151.101.1.140  
fw.reddit.com: 151.101.1.140  
sarah.reddit.com: 151.101.1.140  
videos.reddit.com: 151.101.1.140  
i.reddit.com: 151.101.1.140  
xj.reddit.com: 151.101.1.140  
xf.reddit.com: 151.101.1.140  
addons.reddit.com: 151.101.1.140  
ay.reddit.com: 151.101.1.140  
londonbookclub.reddit.com: 151.101.1.140  
hawks.reddit.com: 151.101.1.140  
gs.reddit.com: 151.101.1.140  
ap.reddit.com: 151.101.1.140  
raerth.reddit.com: 151.101.1.140  
transhealth.reddit.com: 151.101.1.140  
ip.reddit.com: 151.101.1.140  
old.reddit.com: 151.101.1.140  
rd.reddit.com: 151.101.1.140  
darknetmarketsnoobs.reddit.com: 151.101.1.140  
d5.reddit.com: 151.101.1.140  
askgaybros.reddit.com: 151.101.1.140  
niger.reddit.com: 151.101.1.140  
c6.reddit.com: 151.101.1.140  
casualmtg.reddit.com: 151.101.1.140  
ow-31.reddit.com: 151.101.1.140  
en.reddit.com: 151.101.1.140  
re.reddit.com: 151.101.1.140  
sk-en.reddit.com: 151.101.1.140  
nl.reddit.com: 151.101.1.140  
yb.reddit.com: 151.101.1.140



sp.reddit.com: 151.101.1.140  
oaklandraiders.reddit.com: 151.101.1.140  
reddit.com: 151.101.65.140  
jn.reddit.com: 151.101.1.140  
iq.reddit.com: 151.101.1.140  
w1.reddit.com: 151.101.1.140  
ex.reddit.com: 151.101.1.140  
ke.reddit.com: 151.101.1.140  
ro-co.reddit.com: 151.101.1.140  
mod.reddit.com: 151.101.1.140  
pg.reddit.com: 151.101.1.140  
emmawatson.reddit.com: 151.101.1.140  
id.reddit.com: 151.101.1.140  
yg.reddit.com: 151.101.1.140  
jg.reddit.com: 151.101.1.140  
jz.reddit.com: 151.101.1.140  
ow-09.reddit.com: 151.101.1.140  
bg.reddit.com: 151.101.1.140  
boxing.reddit.com: 151.101.1.140  
portland.reddit.com: 151.101.1.140  
s9.reddit.com: 151.101.1.140  
beerporn.reddit.com: 151.101.1.140  
ssl.reddit.com: 151.101.1.140  
td.reddit.com: 151.101.1.140  
origin.reddit.com: 151.101.1.140  
rj.reddit.com: 151.101.1.140  
mi.reddit.com: 151.101.1.140  
la.reddit.com: 151.101.1.140  
gonewild.reddit.com: 151.101.1.140  
s.reddit.com: 151.101.1.140  
cm.reddit.com: 151.101.1.140  
bettiepage.reddit.com: 151.101.1.140  
gi.reddit.com: 151.101.1.140  
pixel.reddit.com: 151.101.1.140  
vc.reddit.com: 151.101.1.140  
lc.reddit.com: 151.101.1.140  
st.reddit.com: 151.101.1.140  
gt.reddit.com: 151.101.1.140  
tinder.reddit.com: 151.101.1.140  
nj.reddit.com: 151.101.1.140  
6n.reddit.com: 151.101.1.140  
denvernuggets.reddit.com: 151.101.1.140  
chicago.reddit.com: 151.101.1.140  
sonics.reddit.com: 151.101.1.140



qu.reddit.com: 151.101.1.140  
fa-08.reddit.com: 151.101.1.140  
alb.reddit.com: 151.101.1.140  
ec.reddit.com: 151.101.1.140  
ux.reddit.com: 151.101.1.140  
jeep.reddit.com: 151.101.1.140  
tw.reddit.com: 151.101.1.140  
fa-01.reddit.com: 151.101.1.140  
aj.reddit.com: 151.101.1.140  
67.reddit.com: 151.101.1.140  
ni-te.reddit.com: 151.101.1.140  
xb.reddit.com: 151.101.1.140  
hd.reddit.com: 151.101.1.140  
freegamesonios.reddit.com: 151.101.1.140  
mo.reddit.com: 151.101.1.140  
m3.reddit.com: 151.101.1.140  
bu.reddit.com: 151.101.1.140  
blog.reddit.com: 151.101.1.140  
t2.reddit.com: 151.101.1.140  
gaming.reddit.com: 151.101.1.140  
se.reddit.com: 151.101.1.140  
nf.reddit.com: 151.101.1.140  
vd.reddit.com: 151.101.1.140  
04.reddit.com: 151.101.1.140  
au.reddit.com: 151.101.1.140  
iu.reddit.com: 151.101.1.140  
xd.reddit.com: 151.101.1.140  
vr.reddit.com: 151.101.1.140  
og.reddit.com: 151.101.1.140  
e1.reddit.com: 151.101.1.140  
qb.reddit.com: 151.101.1.140  
vf.reddit.com: 151.101.1.140  
www.reddit.com: 151.101.1.140  
gb.reddit.com: 151.101.1.140  
ra.reddit.com: 151.101.1.140  
twinpeaks.reddit.com: 151.101.1.140  
uv.reddit.com: 151.101.1.140  
tuscaloosa.reddit.com: 151.101.1.140  
vo.reddit.com: 151.101.1.140  
tn.reddit.com: 151.101.1.140  
ww.reddit.com: 151.101.1.140  
ma.reddit.com: 151.101.1.140  
noveltranslations.reddit.com: 151.101.1.140  
ni-nm.reddit.com: 151.101.1.140





sv.reddit.com: 151.101.1.140  
overwatch.reddit.com: 151.101.1.140  
oi.reddit.com: 151.101.1.140  
mexico.reddit.com: 151.101.1.140  
tu.reddit.com: 151.101.1.140  
nk.reddit.com: 151.101.1.140  
rp.reddit.com: 151.101.1.140  
fappeningdiscussion.reddit.com: 151.101.1.140  
libertarian.reddit.com: 151.101.1.140  
tt.reddit.com: 151.101.1.140  
ac.reddit.com: 151.101.1.140  
pr.reddit.com: 151.101.1.140  
science.reddit.com: 151.101.1.140  
ce.reddit.com: 151.101.1.140  
sissyhypno.reddit.com: 151.101.1.140  
nsfw.reddit.com: 151.101.1.140  
askscience.reddit.com: 151.101.1.140  
cfnm.reddit.com: 151.101.1.140  
na.reddit.com: 151.101.1.140  
he.reddit.com: 151.101.1.140  
cf-nm.reddit.com: 151.101.1.140  
e2.reddit.com: 151.101.1.140  
ly.reddit.com: 151.101.1.140  
r2.reddit.com: 151.101.1.140  
austin.reddit.com: 151.101.1.140  
programming.reddit.com: 151.101.1.140  
pk.reddit.com: 151.101.1.140  
www.m.reddit.com: 151.101.1.140  
od.reddit.com: 151.101.1.140  
out.reddit.com: 151.101.1.140  
ru.reddit.com: 151.101.1.140  
ro-di.reddit.com: 151.101.1.140  
ng.reddit.com: 151.101.1.140  
meta-api.reddit.com: 151.101.1.140  
old.www.reddit.com: 151.101.1.140  
d1.reddit.com: 151.101.1.140  
emulation.reddit.com: 151.101.1.140  
nw.reddit.com: 151.101.1.140  
tx.reddit.com: 151.101.1.140  
vl.reddit.com: 151.101.1.140  
t3.reddit.com: 151.101.1.140  
accounts.reddit.com: 151.101.1.140  
s2.reddit.com: 151.101.1.140  
zx.reddit.com: 151.101.1.140



mail-p236.reddit.com: 184.173.153.236  
hayday.reddit.com: 151.101.1.140  
t1.reddit.com: 151.101.1.140  
cn.reddit.com: 151.101.1.140  
m2.reddit.com: 151.101.1.140  
oq.reddit.com: 151.101.1.140  
ru-fi.reddit.com: 151.101.1.140  
ps4.reddit.com: 151.101.1.140  
vq.reddit.com: 151.101.1.140  
lj.reddit.com: 151.101.1.140  
cryptocurrency.reddit.com: 151.101.1.140  
api.reddit.com: 151.101.1.140  
afl.reddit.com: 151.101.1.140  
no-md.reddit.com: 151.101.1.140  
ob.reddit.com: 151.101.1.140  
bp.reddit.com: 151.101.1.140  
ca.reddit.com: 151.101.1.140  
chicagobulls.reddit.com: 151.101.1.140  
fn-15.reddit.com: 151.101.1.140  
iz.reddit.com: 151.101.1.140  
lgbtnews.reddit.com: 151.101.1.140  
um.reddit.com: 151.101.1.140  
cw.reddit.com: 151.101.1.140  
ad.reddit.com: 151.101.1.140  
ot.reddit.com: 151.101.1.140  
sn.reddit.com: 151.101.1.140  
li.reddit.com: 151.101.1.140  
ov.reddit.com: 151.101.1.140  
ij.reddit.com: 151.101.1.140  
ou.reddit.com: 151.101.1.140  
kk.reddit.com: 151.101.1.140  
iy.reddit.com: 151.101.1.140  
firespin.reddit.com: 151.101.1.140  
bb.reddit.com: 151.101.1.140  
ud.reddit.com: 151.101.1.140  
economics.reddit.com: 151.101.1.140  
wa.reddit.com: 151.101.1.140  
letsnotmeet.reddit.com: 151.101.1.140  
xz.reddit.com: 151.101.1.140  
oilporn.reddit.com: 151.101.1.140  
losangeleskings.reddit.com: 151.101.1.140  
so.reddit.com: 151.101.1.140  
fj.reddit.com: 151.101.1.140  
np.www.reddit.com: 151.101.1.140



f1.reddit.com: 151.101.1.140  
pay.reddit.com: 151.101.1.140  
lz.reddit.com: 151.101.1.140  
pp.reddit.com: 151.101.1.140  
windowsphone.reddit.com: 151.101.1.140  
wf.reddit.com: 151.101.1.140  
f4.reddit.com: 151.101.1.140  
gonets.reddit.com: 151.101.1.140  
eo.reddit.com: 151.101.1.140  
tb.reddit.com: 151.101.1.140  
xg.reddit.com: 151.101.1.140  
ne.reddit.com: 151.101.1.140  
azcardinals.reddit.com: 151.101.1.140  
ea.reddit.com: 151.101.1.140  
49ers.reddit.com: 151.101.1.140  
vita.reddit.com: 151.101.1.140  
thumbs.reddit.com: 151.101.1.140  
woww.reddit.com: 151.101.1.140  
linux.reddit.com: 151.101.1.140  
dg.reddit.com: 151.101.1.140  
f6.reddit.com: 151.101.1.140  
ss.reddit.com: 151.101.1.140  
02.reddit.com: 151.101.1.140  
undelete.reddit.com: 151.101.1.140  
up.reddit.com: 151.101.1.140  
07.reddit.com: 151.101.1.140  
or.reddit.com: 151.101.1.140  
hm.reddit.com: 151.101.1.140  
ww11.reddit.com: 151.101.1.140  
fa-05.reddit.com: 151.101.1.140  
qq.reddit.com: 151.101.1.140  
jk.reddit.com: 151.101.1.140  
nm.reddit.com: 151.101.1.140  
summonerschool.reddit.com: 151.101.1.140  
06.reddit.com: 151.101.1.140  
dauntless.reddit.com: 151.101.1.140  
gundeals.reddit.com: 151.101.1.140  
watches.reddit.com: 151.101.1.140  
k3.reddit.com: 151.101.1.140  
ro.reddit.com: 151.101.1.140  
x2.reddit.com: 151.101.1.140  
f3.reddit.com: 151.101.1.140  
wr.reddit.com: 151.101.1.140  
oc.reddit.com: 151.101.1.140



sw.reddit.com: 151.101.1.140  
pb.reddit.com: 151.101.1.140  
guyana.reddit.com: 151.101.1.140  
rv.reddit.com: 151.101.1.140  
pv.reddit.com: 151.101.1.140  
mailwww.reddit.com: 151.101.1.140  
ds.reddit.com: 151.101.1.140  
sl.reddit.com: 151.101.1.140  
en-us.reddit.com: 151.101.1.140  
wl.reddit.com: 151.101.1.140  
ab.reddit.com: 151.101.1.140  
dm.reddit.com: 151.101.1.140  
hw.reddit.com: 151.101.1.140  
mail.reddit.com: 151.101.1.140  
scifi.reddit.com: 151.101.1.140  
ev.reddit.com: 151.101.1.140  
yi.reddit.com: 151.101.1.140  
ef.reddit.com: 151.101.1.140  
ow-02.reddit.com: 151.101.1.140  
mn.reddit.com: 151.101.1.140  
indianapolis.reddit.com: 151.101.1.140  
fp.reddit.com: 151.101.1.140  
mp.reddit.com: 151.101.1.140  
np.reddit.com: 151.101.1.140  
cg.reddit.com: 151.101.1.140  
vb.reddit.com: 151.101.1.140  
linguistics.reddit.com: 151.101.1.140  
ol.reddit.com: 151.101.1.140  
eq.reddit.com: 151.101.1.140  
ru-in.reddit.com: 151.101.1.140  
m4.reddit.com: 151.101.1.140  
pw.reddit.com: 151.101.1.140  
fullmoviesonvimeo.reddit.com: 151.101.1.140  
mx-02.reddit.com: 52.205.61.79  
animesketch.reddit.com: 151.101.1.140  
fx.reddit.com: 151.101.1.140  
fa-06.reddit.com: 151.101.1.140  
dk.reddit.com: 151.101.1.140  
p4.reddit.com: 151.101.1.140  
tl.reddit.com: 151.101.1.140  
e3.reddit.com: 151.101.1.140  
es.reddit.com: 151.101.1.140  
aa-bw.reddit.com: 151.101.1.140  
pa.reddit.com: 151.101.1.140



u2.reddit.com: 151.101.1.140  
mtggore.reddit.com: 151.101.1.140  
co.reddit.com: 151.101.1.140  
wo.reddit.com: 151.101.1.140  
x6.reddit.com: 151.101.1.140  
xx.reddit.com: 151.101.1.140  
www.np.reddit.com: 151.101.1.140  
zo.reddit.com: 151.101.1.140  
u1.reddit.com: 151.101.1.140  
xc.reddit.com: 151.101.1.140  
hk.reddit.com: 151.101.1.140  
hp.reddit.com: 151.101.1.140  
olf.reddit.com: 151.101.1.140  
m.reddit.com: 151.101.1.140  
we.reddit.com: 151.101.1.140  
tz.reddit.com: 151.101.1.140  
fa-14.reddit.com: 151.101.1.140  
bv.reddit.com: 151.101.1.140  
ml.reddit.com: 151.101.1.140  
oj.reddit.com: 151.101.1.140  
f5.reddit.com: 151.101.1.140  
eg.reddit.com: 151.101.1.140  
amd.com: 104.118.37.73  
ch.reddit.com: 151.101.1.140  
nfl.reddit.com: 151.101.1.140  
f7.reddit.com: 151.101.1.140  
ew.reddit.com: 151.101.1.140  
tk.reddit.com: 151.101.1.140  
procss.reddit.com: 151.101.1.140  
dd.reddit.com: 151.101.1.140  
ts.reddit.com: 151.101.1.140  
xt.reddit.com: 151.101.1.140  
mx02.reddit.com: 151.101.1.140  
qc.reddit.com: 151.101.1.140  
championmains.reddit.com: 151.101.1.140  
55.reddit.com: 151.101.1.140  
05.reddit.com: 151.101.1.140  
cd.reddit.com: 151.101.1.140  
fr.reddit.com: 151.101.1.140  
cc.reddit.com: 151.101.1.140  
askwomen.reddit.com: 151.101.1.140  
Found 11 unique IPs  
66.218.161.27  
151.101.65.140



```
44.240.48.222
184.173.153.236
52.205.61.79
151.101.1.140
52.0.168.221
143.166.147.101
23.59.25.40
54.172.97.247
104.118.37.73
Subdomain search took 0:00:59.884
```

Luego de que ha finalizado la ejecución del comando, podemos revisar el reporte y entender que es lo que está viendo de nuestros dominios un ciberdelincuente, y evaluar posteriormente la seguridad de cada uno de los activos que se encuentran visibles. Es importante tener en consideración que la seguridad debe estar presente en TODOS los activos, pues los ciberdelinquentes buscarán aquellos más débiles para actuar y lograr sus objetivos: exfiltrar datos, destruir los sistemas, encriptar información para cobrar un rescate posteriormente, interceptar información confidencial, robar propiedad intelectual o propiedad industrial, entre otras acciones delictivas posibles.

Tenga presente que es importante que estas pruebas deben ser 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>13</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.

<sup>13</sup> <https://devblogs.microsoft.com/scripting/table-of-basic-powershell-commands/>





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

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:

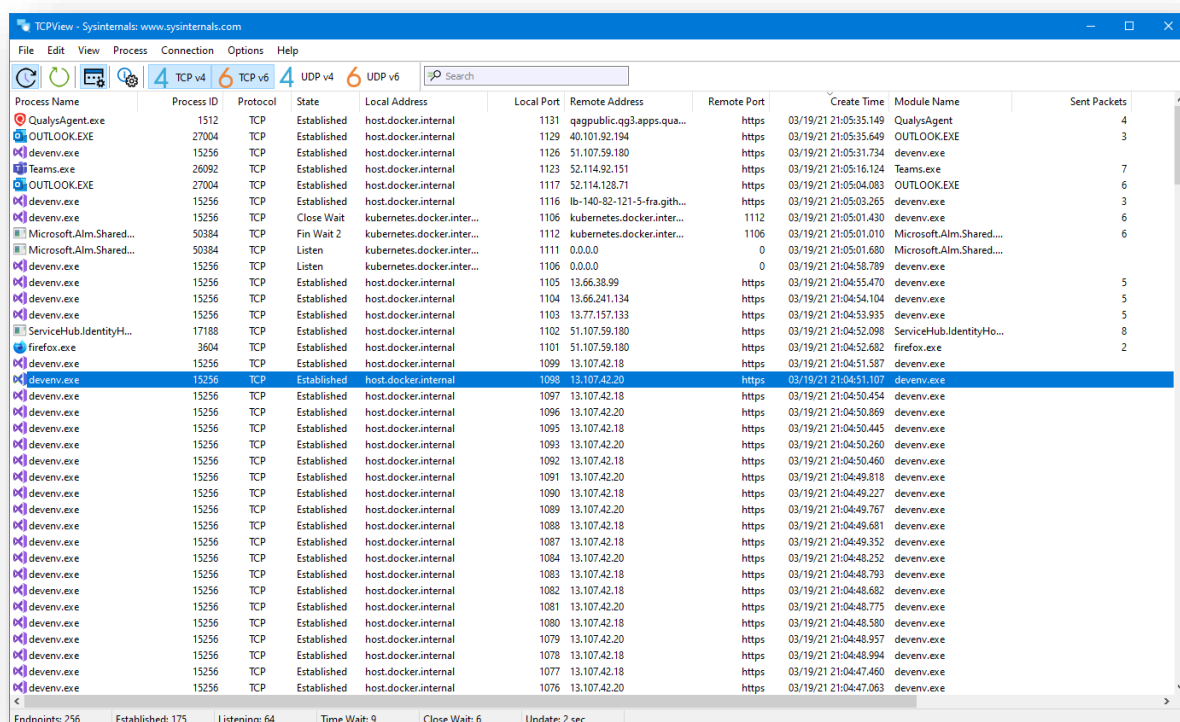
- Utilice el comando “clear” para limpiar la terminal si se llena de demasiados comandos anteriores.
- Pruebe el botón TAB para completar automáticamente lo que está escribiendo. Por ejemplo, si necesita escribir Documentos, comience a escribir un comando (vayamos con cd Docu, luego presione la tecla 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: TCPView

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

TCPView es un programa de Windows que le mostrará listados detallados de todos los puntos finales TCP y UDP en su sistema, incluidas las direcciones locales y remotas y el estado de las conexiones TCP. En Windows Server 2008, Vista y XP, TCPView también informa el nombre del proceso propietario del endpoint. TCPView proporciona un subconjunto más informativo y convenientemente presentado del programa Netstat que se envía con Windows. La descarga de TCPView incluye Tcpsvcon, una versión de línea de comandos con la misma funcionalidad.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
QualysAgent.exe	1512	TCP	Established	host.docker.internal	1131	qagpublic.cg3.apps.qua...	https	03/19/21 21:05:35.149	QualysAgent	4
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1129	40.101.92.194	https	03/19/21 21:05:35.649	OUTLOOK.EXE	3
devenv.exe	15256	TCP	Established	host.docker.internal	1126	51.107.59.180	https	03/19/21 21:05:31.734	devenv.exe	
Teams.exe	26092	TCP	Established	host.docker.internal	1123	52.114.92.151	https	03/19/21 21:05:16.124	Teams.exe	7
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1117	52.114.128.71	https	03/19/21 21:05:04.083	OUTLOOK.EXE	6
devenv.exe	15256	TCP	Established	host.docker.internal	1116	lb-140-82-121-5-fra.git...	https	03/19/21 21:05:03.265	devenv.exe	3
devenv.exe	15256	TCP	Close Wait	kubernetes.docker.inter...	1106	kubernetes.docker.inter...	1112	03/19/21 21:05:01.430	devenv.exe	6
Microsoft.Alm.Shared...	50384	TCP	Fin Wait 2	kubernetes.docker.inter...	1112	kubernetes.docker.inter...	1106	03/19/21 21:05:01.010	Microsoft.Alm.Shared...	6
Microsoft.Alm.Shared...	50384	TCP	Listen	kubernetes.docker.inter...	1111	0.0.0.0	0	03/19/21 21:05:01.680	Microsoft.Alm.Shared...	
devenv.exe	15256	TCP	Listen	kubernetes.docker.inter...	1106	0.0.0.0	0	03/19/21 21:04:58.789	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1105	13.66.38.99	https	03/19/21 21:04:55.470	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1104	13.66.241.134	https	03/19/21 21:04:54.104	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1103	13.77.157.133	https	03/19/21 21:04:53.935	devenv.exe	5
ServiceHub.IdentityH...	17188	TCP	Established	host.docker.internal	1102	51.107.59.180	https	03/19/21 21:04:52.098	ServiceHub.IdentityHo...	8
firefox.exe	3604	TCP	Established	host.docker.internal	1101	51.107.59.180	https	03/19/21 21:04:52.682	firefox.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1099	13.107.42.18	https	03/19/21 21:04:51.587	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1098	13.107.42.20	https	03/19/21 21:04:51.107	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1097	13.107.42.18	https	03/19/21 21:04:50.454	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1096	13.107.42.20	https	03/19/21 21:04:50.869	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1095	13.107.42.18	https	03/19/21 21:04:50.445	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1093	13.107.42.20	https	03/19/21 21:04:50.260	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1092	13.107.42.18	https	03/19/21 21:04:50.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1091	13.107.42.20	https	03/19/21 21:04:49.818	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1090	13.107.42.18	https	03/19/21 21:04:49.227	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1089	13.107.42.20	https	03/19/21 21:04:49.767	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1088	13.107.42.18	https	03/19/21 21:04:49.681	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1087	13.107.42.18	https	03/19/21 21:04:49.352	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1084	13.107.42.20	https	03/19/21 21:04:48.252	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1083	13.107.42.18	https	03/19/21 21:04:48.793	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1082	13.107.42.18	https	03/19/21 21:04:48.682	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1081	13.107.42.20	https	03/19/21 21:04:48.775	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1080	13.107.42.18	https	03/19/21 21:04:48.580	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1079	13.107.42.20	https	03/19/21 21:04:48.957	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1078	13.107.42.18	https	03/19/21 21:04:48.994	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1077	13.107.42.18	https	03/19/21 21:04:47.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1076	13.107.42.20	https	03/19/21 21:04:47.063	devenv.exe	

Endpoints: 256   Established: 175   Listening: 64   Time Wait: 9   Close Wait: 6   Update: 2 sec

Este programa puede descargarlo desde:

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

Cuando inicie TCPView, enumerará todos los puntos finales TCP y UDP activos, resolviendo todas las direcciones IP en sus versiones de nombre de dominio. Puede utilizar un botón de la barra de herramientas o un elemento de menú para alternar la visualización de los nombres resueltos.



TCPView muestra el nombre del proceso que posee cada punto final, incluido el nombre del servicio (si corresponde).

De forma predeterminada, TCPView se actualiza cada segundo, pero puede utilizar el elemento de menú Opciones | Frecuencia de actualización para cambiar la frecuencia. Los puntos finales que cambian de estado de una actualización a la siguiente se resaltan en amarillo; los que se eliminan se muestran en rojo y los nuevos puntos finales se muestran en verde.

Puede cerrar las conexiones TCP / IP establecidas (aquellas etiquetadas con un estado de ESTABLECIDO) seleccionando Archivo | Cerrar conexiones, o haciendo clic con el botón derecho en una conexión y eligiendo Cerrar conexiones en el menú contextual resultante.

Puede guardar la ventana de salida de TCPView en un archivo usando el elemento del menú Guardar.

Nota adicional para “tcpvcon”:

El uso de Tcgvcon es similar al de la utilidad netstat incorporada de Windows:

Uso:

cmd

 Copiar

```
tcpvcon [-a] [-c] [-n] [process name or PID]
```

Parámetro	Descripción
-a	Mostrar todos los puntos finales (el valor predeterminado es mostrar las conexiones TCP establecidas).
-C	Imprime la salida como CSV.
-norte	No resuelva las direcciones.

Con estos tips básicos buscamos incentivarlo a explorar estas herramientas y sus múltiples usos para ciberseguridad.