



1 de octubre de 2021  
Ficha N° 23 BING-IP2HOSTS  
CSIRT DE GOBIERNO

## Comando de la semana “BING-IP2HOSTS”

### I. CONTEXTO

Este documento, denominado, en esta oportunidad, “BING-IP2HOSTS ”, 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's o programas escritos en lenguajes que facilitan la automatización tales 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 así poder invertir el tiempo de los especialistas o analistas en el estudio e investigación 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).

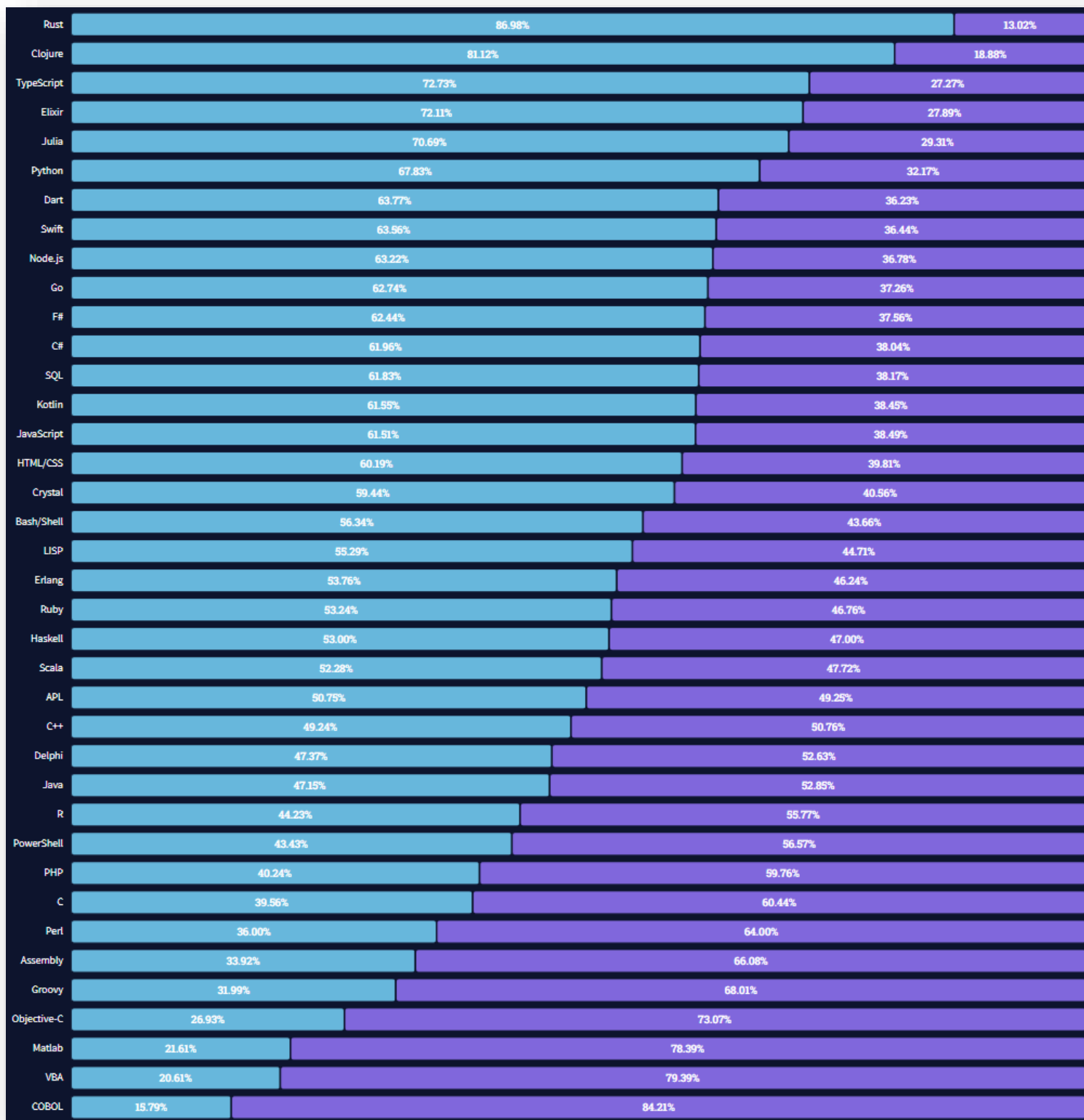
<sup>1</sup> <https://scis.uohyd.ac.in/~apcs/itw/UNIXProgrammingEnvironment.pdf>

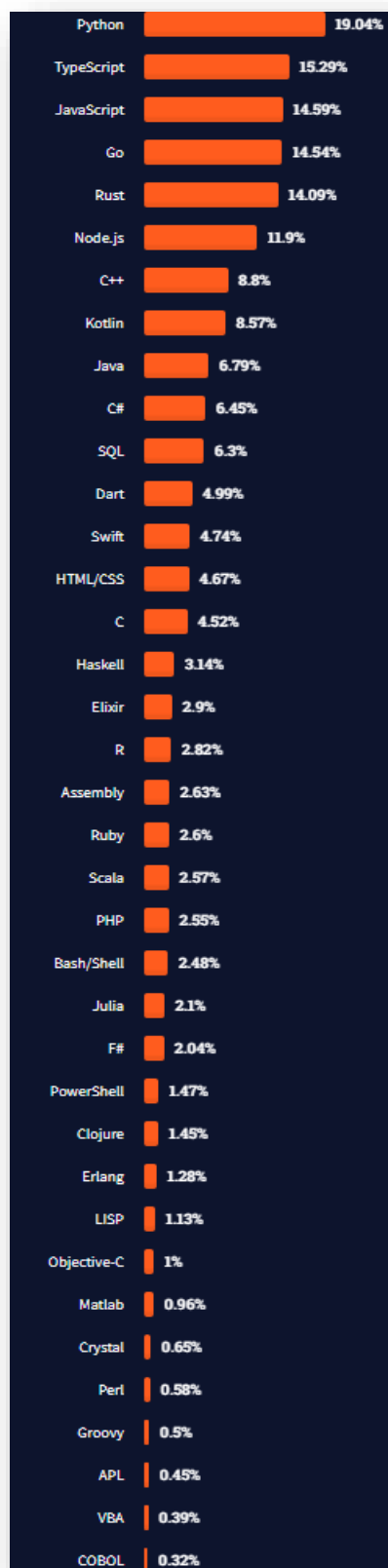
<sup>2</sup> <https://github.com/Microsoft/QuantumKatas/>

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



Al final de este documento se presenta, a modo de curiosidad, el tradicional “Hola, Mundo” escrito en algunos de estos lenguajes, con el objetivo de motivar al lector a conocerlos, estudiarlos y aplicarlos a sus entornos de trabajo.







## II. INTRODUCCIÓN

Una de las tareas regulares que un encargado de ciberseguridad debe realizar es la ENUMERACIÓN o RECONOCIMIENTO. La enumeración es una actividad de reconocimiento en la cual se consigue información de usuarios, grupos o dispositivos, dominios relacionados, vulnerabilidades 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.
- 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.



*Ilustración 1 Cyber Kill Chain by Lockheed Martin*

En este contexto se inserta la herramienta que les presentamos en esta edición del “comando de la semana”: BING-IP2HOSTS.



## ¿Qué es BING-IP2HOSTS?

Bing.com es un motor de búsqueda propiedad de Microsoft anteriormente conocido como MSN Search y Live Search. Tiene una función única para buscar sitios web alojados en una dirección IP específica. Bing-ip2hosts utiliza esta función para enumerar todos los nombres de host que Bing ha indexado para una dirección IP específica. Esta técnica se considera la mejor práctica durante la fase de reconocimiento de una prueba de penetración para descubrir una superficie de ataque potencial más grande. Bing-ip2hosts está escrito en el lenguaje de secuencias de comandos Bash para Linux.

**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

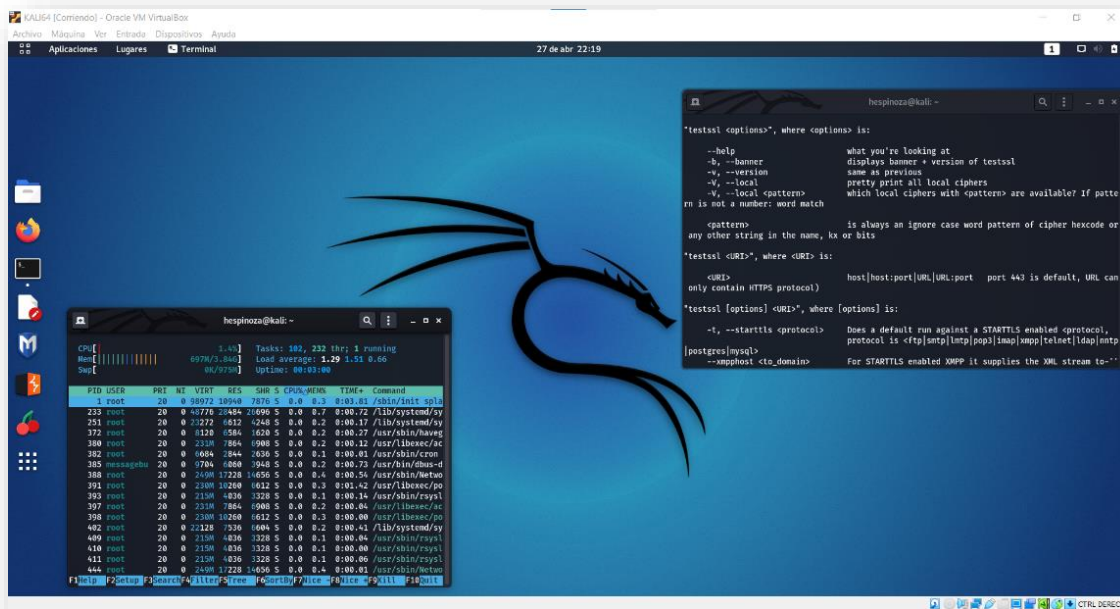
*Bonus Track: Ejemplos muy básicos y simples del clásico “Hello, World!” escrito en diferentes lenguajes. El objetivo es despertar su curiosidad por estos lenguajes y ojalá se entusiasme y emprenda la cruzada de aprenderlo en profundidad, para luego aplicarlo en su quehacer cotidiano y dentro de lo posible comparta sus conocimientos con la comunidad.*



### 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:

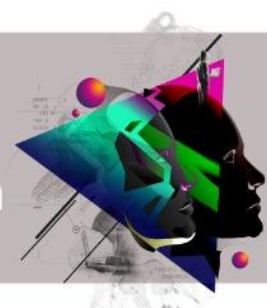
<https://www.kali.org/docs/installation/hard-disk-install/>



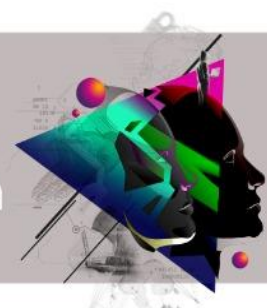
Otras distribuciones que puede considerar son las siguientes:

<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/>



Nombre	Link	Descripción
<b>ARCHSTRIKE</b>	<a href="https://archstrike.org/">https://archstrike.org/</a>	Distribución linux con foco en ciberseguridad.
<b>BACKBOX</b>	<a href="https://www.backbox.org/">https://www.backbox.org/</a>	Distribución de Linux orientada a pruebas de penetración y evaluación de seguridad que proporciona un conjunto de herramientas de análisis de redes y sistemas.
<b>BLACKARCH</b>	<a href="http://blackarch.org/">http://blackarch.org/</a>	Herramientas para pruebas de penetración basada en Arch Linux.
<b>BLACKBUNTU</b>	<a href="https://archiveos.org/blackbuntu/">https://archiveos.org/blackbuntu/</a>	Es una distribución GNU / Linux basada en Ubuntu y diseñada con Pentest, Seguridad y Desarrollo en mente para la mejor experiencia.
<b>BUGTRAQ</b>	<a href="https://archiveos.org/bugtraq/">https://archiveos.org/bugtraq/</a>	Distribución GNU / Linux destinada a análisis forense digital, pruebas de penetración, laboratorios de malware y análisis forense.
<b>CAINE</b>	<a href="http://www.caine-live.net/">http://www.caine-live.net/</a>	CAINE (Computer Aided INvestigative Environment) es una distribución GNU / Linux italiana creada como un proyecto de Digital Forensics.
<b>CYBORG HAWK LINUX</b>	<a href="https://archiveos.org/cyborg-hawk/">https://archiveos.org/cyborg-hawk/</a>	Distribución de Linux basada en la plataforma Ubuntu con el último kernel para profesionales de la seguridad cibernética.
<b>DEFT LINUX</b>	<a href="http://www.deftlinux.net/">http://www.deftlinux.net/</a>	DEFT es un sistema operativo Linux creado especialmente para profesionales y expertos de seguridad que necesiten un ecosistema para analizar datos, redes y dispositivos y poder recopilar de ellos la mayor cantidad de información posible.
<b>DRACOS LINUX</b>	<a href="https://dracos-linux.org/">https://dracos-linux.org/</a>	Dracos Linux es un sistema operativo de código abierto que proporciona pruebas de penetración.
<b>FEDORA SECURITY LAB</b>	<a href="https://labs.fedoraproject.org/en/security/">https://labs.fedoraproject.org/en/security/</a>	Entorno de prueba seguro para trabajar en auditoría de seguridad, análisis forense, rescate de sistemas y enseñanza de metodologías de prueba de seguridad en universidades y otras organizaciones.
<b>GNACK TRACK LINUX</b>	<a href="https://archiveos.org/gnacktrack/">https://archiveos.org/gnacktrack/</a>	Distribución de Linux basada en Ubuntu que proporciona un conjunto de pruebas de penetración.
<b>JONDO</b>	<a href="https://anonymous-proxy-servers.net/en/jondo-live-cd.html">https://anonymous-proxy-servers.net/en/jondo-live-cd.html</a>	Entorno seguro y preconfigurado para navegación anónima.
<b>KALI</b>	<a href="https://www.kali.org/">https://www.kali.org/</a>	Distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa.
<b>LIVE HACKING DVD</b>	<a href="http://www.livehacking.com/live-hacking-cd/download-live-hacking/">http://www.livehacking.com/live-hacking-cd/download-live-hacking/</a>	Distribución de Linux basada en Ubuntu que proporciona un conjunto de pruebas de penetración.
<b>MATRIUX</b>	<a href="http://matriux.sourceforge.net/">http://matriux.sourceforge.net/</a>	Distribución de seguridad con todas las funciones que consta de un montón de herramientas poderosas, de código abierto y gratuitas que se pueden utilizar para varios propósitos, incluidos, entre otros, pruebas de penetración, piratería ética, administración de sistemas y



		redes, investigaciones forenses cibernéticas, pruebas de seguridad, análisis de vulnerabilidades y mucho más.
<b>MOKI</b>	<a href="https://github.com/mokics/moki">https://github.com/mokics/moki</a>	Modificación de Kali para incorporar varias herramientas ICS / SCADA esparcidas por Internet, para crear un Kali Linux personalizado dirigido a profesionales de pentesting ICS / SCADA.
<b>NETWORK SECURITY TOOLKIT (NST)</b>	<a href="https://sourceforge.net/projects/nst/files/">https://sourceforge.net/projects/nst/files/</a>	Un kit de herramientas de monitoreo y análisis de seguridad de red para distribución de Linux.
<b>NODEZERO</b>	<a href="https://sourceforge.net/projects/nodezero/">https://sourceforge.net/projects/nodezero/</a>	Linux basado en Ubuntu diseñado como un sistema completo que también se puede utilizar para pruebas de penetración.
<b>PENTOO</b>	<a href="https://pentoo.org/">https://pentoo.org/</a>	Live CD y Live USB diseñado para pruebas de penetración y evaluación de seguridad. Basado en Gentoo Linux, Pentoo se proporciona como livecd instalable de 32 y 64 bits.
<b>PARROT SECURITY OS</b>	<a href="https://www.parrotsec.org/">https://www.parrotsec.org/</a>	Distribución GNU / Linux basada en Debian y diseñada pensando en la seguridad y la privacidad.
<b>SAMURAI WEB TESTING FRAMEWORK</b>	<a href="https://www.samuraiwtf.org/">https://www.samuraiwtf.org/</a>	Linux completo para su uso en la formación de seguridad de aplicaciones. Es gratuito y de código abierto, distribuido como VM preconstruidas y como código fuente. La fuente consta de un Vagrantfile, activos estáticos y scripts de compilación. Durante el proceso de construcción, recupera una variedad de herramientas y objetivos de entrenamiento.
<b>SECURITY ONION 2</b>	<a href="https://securityonionsolutions.com/">https://securityonionsolutions.com/</a>	Distribución de Linux de código abierto y gratuito para la búsqueda de amenazas, la supervisión de la seguridad empresarial y la gestión de registros. ¡El asistente de configuración fácil de usar le permite crear un ejército de sensores distribuidos para su empresa en minutos! Security Onion incluye Elasticsearch, Logstash, Kibana, Suricata, Zeek (antes conocido como Bro), Wazuh, Stenographer, TheHive, Cortex, CyberChef, NetworkMiner y muchas otras herramientas de seguridad.
<b>TAILS</b>	<a href="https://tails.boum.org/">https://tails.boum.org/</a>	Sistema operativo portátil que protege la privacidad.
<b>QUBES OS</b>	<a href="https://www.qubes-os.org/">https://www.qubes-os.org/</a>	Sistema operativo gratuito y de código abierto orientado a la seguridad para la informática de escritorio de un solo usuario. Qubes OS aprovecha la virtualización basada en Xen para permitir la creación y gestión de compartimentos aislados llamados qubes.
<b>WIFISLAX</b>	<a href="https://www.wifislax.com/">https://www.wifislax.com/</a>	Linux para auditorías Wireless.
<b>DEMONLINUX</b>	<a href="https://demonlinux.com">https://demonlinux.com</a>	Distribución de Debian Linux con tema de prueba de penetración.



## 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"**:

Si el comando no estuviere pre-instalado en la distribución KALI, proceda con la siguiente instrucción:

### **# apt-get update && apt-get install bing-ip2hosts**

Luego verifique que haya quedado instalada:

### **# apt install bing-ip2hosts**

Leyendo lista de paquetes... Hecho

Creando árbol de dependencias... Hecho

Leyendo la información de estado... Hecho

bing-ip2hosts ya está en su versión más reciente (1.0.4-0kali1).

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

baobab caribou cryptsetup-run folks-common gccgo-10 gir1.2-caribou-1.0 gir1.2-handy-0.0  
gnome-characters gnome-contacts gnome-core gnome-font-viewer gnome-logs gnome-online-  
miners

gnome-tweak-tool golang-1.15-go golang-1.15-src gstreamer1.0-packagekit libamtk-5-0 libamtk-  
5-common libavif9 libcaribou-common libcaribou0 libdav1d4 libepsilon1 libfolks-eds26

libfolks26 libgdal28 libgeos-3.9.0 libgfbgraph-0.2-0 libgo-10-dev libgo16 libhandy-0.0-0 libidn11  
libkdecorations2private7 libkwineffects12a libkwinglutils12 libkwinxrenderutils12

libmusicbrainz5-2 libmusicbrainz5cc2v5 libntfs-3g883 libplacebo72 libproxy1-plugin-webkit  
libquvi-0.9-0.9.3 libquvi-scripts-0.9 libstd-rust-1.48 libstd-rust-1.49 libtepl-5-0

libtracker-control-2.0-0 libtracker-miner-2.0-0 libtracker-sparql-2.0-0 liburcu6 libx265-192  
libxmlb1 libyara4 libzapotit-0.0-0 lua-bitop lua-expat lua-json lua-socket python3-gevent

python3-gevent-websocket python3-greenlet python3-ipynon-genutils python3-jupyter-core  
python3-m2crypto python3-nbformat python3-parameterized python3-plotly python3-  
zope.event

r-cran-freetyperharfbuzz r-cran-gdtools x11proto-xext-dev

Utilice «apt autoremove» para eliminarlos.

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

### **# apt search ^bing-ip2hosts**

Ordenando... Hecho

Buscar en todo el texto... Hecho

**bing-ip2hosts/kali-rolling,now 1.0.4-0kali1 all [instalado]**

Enumerate hostnames for an IP using bing.com

<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: "bing-ip2hosts -h".

```
root@V: ~
"#####"                                @#Gmmem###G
,i,                                     ,s2e,    ##
,                                     " `  %#    ##
]# ]#,#M5@#p                          #b    #H#H%#@#    s#M5O#o    ,#MSSM    W@##W=    s#SSW
]# ]#p    ^#p                        ,#M    ##    @#    #'    'O#    S#,    ]#    #b
]# ]#    #M    ,#M                    ##    @#    #o    O#    "SXm    ]#    ^"@#
]# ]##,    ,##    ,#2                ##    @#    7#.    .#O    ,    ]#    ]#Q    ,#s
]# ]#####'    #####x                ##    @#    s#####o    #####^    #Tt    #####^
]#
]#
]#      bing-ip2hosts (1.0.4) by Andrew Horton @urbanadventurer
]#      https://morningstarsecurity.com/research/bing-ip2hosts
]#      https://github.com/urbanadventurer/bing-ip2hosts

[Press Enter]
bing-ip2hosts is a Bing.com web scraper that discovers websites by IP address.
Use for OSINT and discovering attack-surface of penetration test targets.

Usage: /usr/bin/bing-ip2hosts [OPTIONS] IP|hostname

OPTIONS are:
-o FILE Output hostnames to FILE.
-i FILE Input list of IP addresses or hostnames from FILE.
-n NUM Stop after NUM scraped pages return no new results (Default: 5).
-l Select the language for use in the setlang parameter (Default: en-us).
-m Select the market for use in the setmkt parameter (Default is unset).
```

El despliegue total de la ayuda es la siguiente:

```
# plecost -h
m,                                     .,recon:,    ,
#####    ]##"^^"%##m    %##b
####b    ]##    `##b
####b    ]##    ##    i##    @#b,#####m    ,#####m ##b
####b 1mw,    ]##MMM####    i##    ]###`    %##    ###`    `@##
####b 1#####Nw,    ]##`    @#b    i##    ]##    ###    ###    j##
####i    %#####[    ]##    @##    i##    ]##    ###    ##g    j##
####n    2#####[    ]##    @##    i##    ]##    ###    @##    {##
####g    ,#####b    ]##    ,e###    j##    ]##    ###    7##m,,sM##
#####M^    'WWWWW%b^    ii    'nn    nn*    `1337` g##
#####"
"###"                                @#Gmmem###G
,i,                                     ,s2e,    ##
,                                     " `  %#    ##
]# ]#,#M5@#p                          #b    #H#H%#@#    s#M5O#o    ,#MSSM    W@##W=    s#SSW
```



```
]# j#p ^#p ,#M ## @# #' 'O# S# , ]# #b
]# j# #M ,#M ## @# #o O# "SXm ]# ^"@#
]# j##, ,## ,#2 ## @# 7#. .#O , ]# ]#Q ,#s
]# j#####' #####x ## @# s#####o ####^ #Tt #####^
j#
j#
j# bing-ip2hosts (1.0.4) by Andrew Horton @urbanadventurer
j# https://morningstarsecurity.com/research/bing-ip2hosts
j# https://github.com/urbanadventurer/bing-ip2hosts

[Press Enter]
bing-ip2hosts is a Bing.com web scraper that discovers websites by IP address.
Use for OSINT and discovering attack-surface of penetration test targets.

Usage: /usr/bin/bing-ip2hosts [OPTIONS] IP|hostname

OPTIONS are:
-o FILE Output hostnames to FILE.
-i FILE Input list of IP addresses or hostnames from FILE.
-n NUM Stop after NUM scraped pages return no new results (Default: 5).
-l Select the language for use in the setlang parameter (Default: en-us).
-m Select the market for use in the setmkt parameter (Default is unset).
-u Only display hostnames. Default is to include URL prefixes.
-c CSV output. Outputs the IP and hostname on each line, separated by a
comma.
-q Quiet. Disable output except for final results.
-t DIR Use this directory instead of /tmp.
-V Display the version number of bing-ip2hosts and exit.
```





#### PASO 4: PONERLO EN MARCHA PARA VERIFICAR NUESTRA INFRAESTRUCTURA.

Un ejemplo de ejecución básica para nuestros primeros pasos:

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

##### EJEMPLO 1

¿Qué otros dominios encontramos asociados a la IP de `csirt.gob.cl`, almacenando el resultado en un archivo llamado `csirt.txt`?

```
# bing-ip2hosts -o csirt.txt csirt.gob.cl
```

```
m,          -----[ bing-ip2hosts v1.0.4 ]-----
#####      | Searching      : 163.247.175.147
####b       | Found         : 28
####b       | Scraped pages: 8
####b 1mw,   |
####b 1#####Nw, | Page Title   : ip:163.247.175.147 . - Bing
####i %#####[ | Results     : 70-71 of 71
####n      2#####[ | Pagination  : 1 ... 6 7 8
####g ,#####b | New         : 0 new
#####M^       |
#####"        |
"%##"          | CTRL-C to stop

[!] /search?q=ip%3A163.247.175.147+.&qs=n&first=70&FORM=PERE&setlang=en-us&setm
http://www.denunciaseguro.cl
http://www.fondonacional.cl
```

```
Stopping. This is the last page of results.
https://ciberseguridad.gob.cl/
https://cmv.interior.gob.cl/
http://denunciaseguro.cl/
http://lazos.spd.gob.cl/
https://reformacarabineros.gob.cl/
https://www.cecipu.gob.cl/
http://www.denunciaseguro.cl/
http://www.dsp.gob.cl/
http://www.dsp.gov.cl/
https://www.extranjeria.gob.cl/
http://www.fnsp.gob.cl/
http://www.fnsp.gov.cl/
http://www.fondodeseguridadpublica.gob.cl/
http://www.fondonacional.cl/
http://www.fondonacional.gob.cl/
https://www.interior.gob.cl/
http://www.oep.gov.cl/
http://www.pasosfronterizos.gob.cl/
```





```
http://www.pasosfronterizos.gov.cl/  
http://www.prevenciondeldelito.gob.cl/  
http://www.prevenciondeldelito.gov.cl/  
http://www.seguridadciudadana.gob.cl/  
http://www.shoa.gob.cl/  
http://www.spd.gob.cl/  
http://www.spd.gov.cl/  
https://www.ssdefensa.cl/  
http://www.ssi.gov.cl/  
https://www.subinterior.gob.cl/
```

✓ Found 28 results after scraping 8 pages.

Podemos verificar el contenido del archivo csirt.txt

```
# cat csirt.txt  
http://2010-2014.gob.cl/  
https://ciberseguridad.gob.cl/  
https://cmv.interior.gob.cl/  
https://digempol.interior.gob.cl/  
http://lazos.spd.gob.cl/  
https://reformacarabineros.gob.cl/  
http://tratadepersonas.subinterior.gob.cl/  
https://www.cecipu.gob.cl/  
https://www.csirt.gob.cl/  
http://www.denunciaseguro.cl/  
http://www.dsp.gob.cl/  
http://www.dsp.gov.cl/  
http://www.estadioseguro.gob.cl/  
https://www.extranjeria.gob.cl/  
http://www.fnsp.gob.cl/  
http://www.fondonacional.cl/  
http://www.fondonacional.gob.cl/  
http://www.fondoseguridadpublica.gov.cl/  
https://www.interior.gob.cl/  
http://www.oep.gov.cl/  
http://www.pasosfronterizos.gob.cl/  
http://www.prevenciondeldelito.gob.cl/  
http://www.prevenciondeldelito.gov.cl/  
http://www.seguridadciudadana.gob.cl/  
http://www.shoa.gob.cl/  
http://www.spd.gob.cl/  
https://www.ssdefensa.cl/  
https://www.subinterior.gob.cl/  
https://ciberseguridad.gob.cl/  
https://cmv.interior.gob.cl/  
http://denunciaseguro.cl/  
http://lazos.spd.gob.cl/  
https://reformacarabineros.gob.cl/  
https://www.cecipu.gob.cl/  
http://www.denunciaseguro.cl/  
http://www.dsp.gob.cl/  
http://www.dsp.gov.cl/  
https://www.extranjeria.gob.cl/  
http://www.fnsp.gob.cl/  
http://www.fnsp.gov.cl/  
http://www.fondodeseguridadpublica.gob.cl/  
http://www.fondonacional.cl/
```



```
http://www.fondonacional.gob.cl/  
https://www.interior.gob.cl/  
http://www.oep.gov.cl/  
http://www.pasosfronterizos.gob.cl/  
http://www.pasosfronterizos.gov.cl/  
http://www.prevenciondeldelito.gob.cl/  
http://www.prevenciondeldelito.gov.cl/  
http://www.seguridadciudadana.gob.cl/  
http://www.shoa.gob.cl/  
http://www.spd.gob.cl/  
http://www.spd.gov.cl/  
https://www.ssdefensa.cl/  
http://www.ssi.gov.cl/  
https://www.subinterior.gob.cl/
```

```
root@V: ~  
m, -----[bing-ip2hosts v1.0.4]-----  
##### | Searching : 163.247.175.147  
###b | Found : 28  
###b | Scraped pages: 8  
###b lmw,  
###b 1#####Nw, | Page Title : ip:163.247.175.147 . - Bing  
###i %##### | Results : 70-71 of 71  
###n 2##### | Pagination : 1 ... 6 7  
###g ,#####b | New : 0 new  
#####M^  
#####  
"###" | CTRL-C to stop  
  
[O] /search?q=ip%3A163.247.175.147+.&qs=n&first=70&FORM=PERE&setlang=en-us&setm  
http://www.denunciaseguro.cl  
http://www.fondonacional.cl  
  
  
Stopping. This is the last page of results.  
https://ciberseguridad.gob.cl/  
https://cmv.interior.gob.cl/  
http://denunciaseguro.cl/  
http://lazos.spd.gob.cl/  
https://reformacarabineros.gob.cl/  
https://www.cecipu.gob.cl/  
http://www.denunciaseguro.cl/  
http://www.dsp.gob.cl/  
http://www.dsp.gov.cl/  
https://www.extranjeria.gob.cl/  
http://www.fnsp.gob.cl/  
http://www.fnsp.gov.cl/  
http://www.fondodeseguridadpublica.gob.cl/  
http://www.fondonacional.cl/  
http://www.fondonacional.gob.cl/  
https://www.interior.gob.cl/
```



La interfaz de comando muestra los hallazgos que amplían la superficie de ataque, los que pueden ser utilizados en subsecuentes análisis que van profundizando la información que está expuesta respecto de nuestros sitios y sistemas en Internet.

Es importante tener en consideración que la seguridad debe estar presente en TODOS los activos, pues los ciberdelincuentes 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, introducir ransomware, cryptojacking<sup>13</sup> 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.

Use la información obtenida para visualizar sus activos desde la perspectiva de un externo e identifique vulnerabilidades a mitigar o datos/directorios a proteger.

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 ataques 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).

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.

<sup>13</sup> <https://www.eset.com/es/caracteristicas/cryptojacking/>

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



## Anexo I: Comandos Básicos de Linux: GREP o EGREP

Grep es una de las herramientas más usadas en la línea de comandos de GNU/Linux. A pesar de ser una herramienta muy simple, permite realizar gran cantidad de operaciones. Se usa especialmente junto con las tuberías, para poder localizar puntos concretos en la salida de un comando previo, etc. Pero también existe una herramienta conocida como egrep que equivale a ejecutar grep con la opción -E.

La e proviene de «Extended regex», que es lo que activa la opción -E y lo que tiene en egrep por defecto sin necesidad de usar esa opción. Es decir, que podrá usar las expresiones regulares extendidas.

Puede buscar una línea o palabra concreta en uno o varios archivos, como también sucede con grep. Por ejemplo, imagine que quiere buscar la palabra ubuntu en un archivo llamado snap.txt y también en todos los .txt del directorio actual:

- `egrep ubuntu snap.txt`
- `egrep ubuntu *.txt`

La búsqueda puede ser también recursiva para buscar en todo el contenido del directorio actual:

- `egrep -r "hola mundo" *`

Hasta aquí se buscaban palabras o cadenas exactas, es decir, teniendo en cuenta mayúsculas y minúsculas (case-sensitive), pero si quiere hacerlo en modo case-insensitive, sin importar si son mayúsculas o minúsculas, puedes usar lo siguiente (si agrega w busca solo coincidencias completas):

- `egrep -i "ejemplo" documento.txt`
- `egrep -iw "ejemplo" documento.txt`

También puede mostrar, no las coincidencias, sino los nombres de archivos donde se han encontrado esas coincidencias:

- `egrep -l hola *.txt`

Mostrar solo el patrón o palabra buscada dentro de un documento:

- `egrep -o printf hola.c`

Puede combinar varias de las opciones vistas anteriormente, o las puede complementar con otras opciones como -A n y -B n, siendo n el número de líneas que quiere mostrar antes (Before) y después (After) de la coincidencia o ambas a la vez (C), para que así pueda ver lo que rodea a dicha coincidencia:



- `egrep -A 2 "printf" hola.c`
- `egrep -B 2 "printf" hola.c`
- `egrep -C 2 printf hola.c`

Suprimir las líneas que contienen una coincidencia y solo mostrar las que no coinciden:

- `egrep -v "dos" números.doc`

O si lo prefiere, puede usar varias palabras o coincidencias con `-e`. Por ejemplo:

- `egrep -v -e "uno" -e "dos" -e "tres" números.txt`

Si usa `-c` se pueden solo contar el número de coincidencias, o invertirlo con `-v` para que muestre el número de líneas no coincidentes. Por ejemplo:

- `egrep -c "include" main.c`
- `egrep -v -c "include" main.c`

E incluso mostrar el número de línea donde se ha producido la coincidencia, y también la posición que ocupa respectivamente:

- `egrep -n "void" hola.c`
- `egrep -o -b "printf" hola.c`

Y junto con las expresiones regulares se pueden ampliar sus capacidades. Por ejemplo, buscar una línea que comience por Hola y termine por adiós, o que comience por Hola seguida de lo que sea y luego aparezca la coincidencia adiós respectivamente:

- `egrep '^Hola.*adiós$' ejemplo.txt`
- `egrep "Hola.*adiós" ejemplo.txt`

Puede también buscar rangos alfanuméricos, o valores concretos, como por ejemplo para localizar ciertas IPs:

- `cat /etc/networks | egrep "192.168.1.[5-9]"`
- `cat /etc/networks | egrep "192.168.[1-3].[5-9]"`
- `cat /etc/networks | egrep "192.168.1.[0-3] | [5-9]"`
- `egrep 192.168.4.[10,40] networks`



Si lo prefiere, puede usar otras expresiones regulares para hacer búsquedas más concretas. Por ejemplo | para buscar una coincidencia o la otra:

- `egrep -i '^(printf|scanf)' hola.c`

Incluso puede localizar mayúsculas, minúsculas, caracteres alfabéticos solo, o alfanuméricos, etc., usando otras expresiones como: `[:alnum:]`, `[:alpha:]`, `[:digit:]`, `[:lower:]`, `[:print:]`, `[:punct:]`, `[:space:]`, `[:upper:]`, etc. Por ejemplo, para buscar mayúsculas:

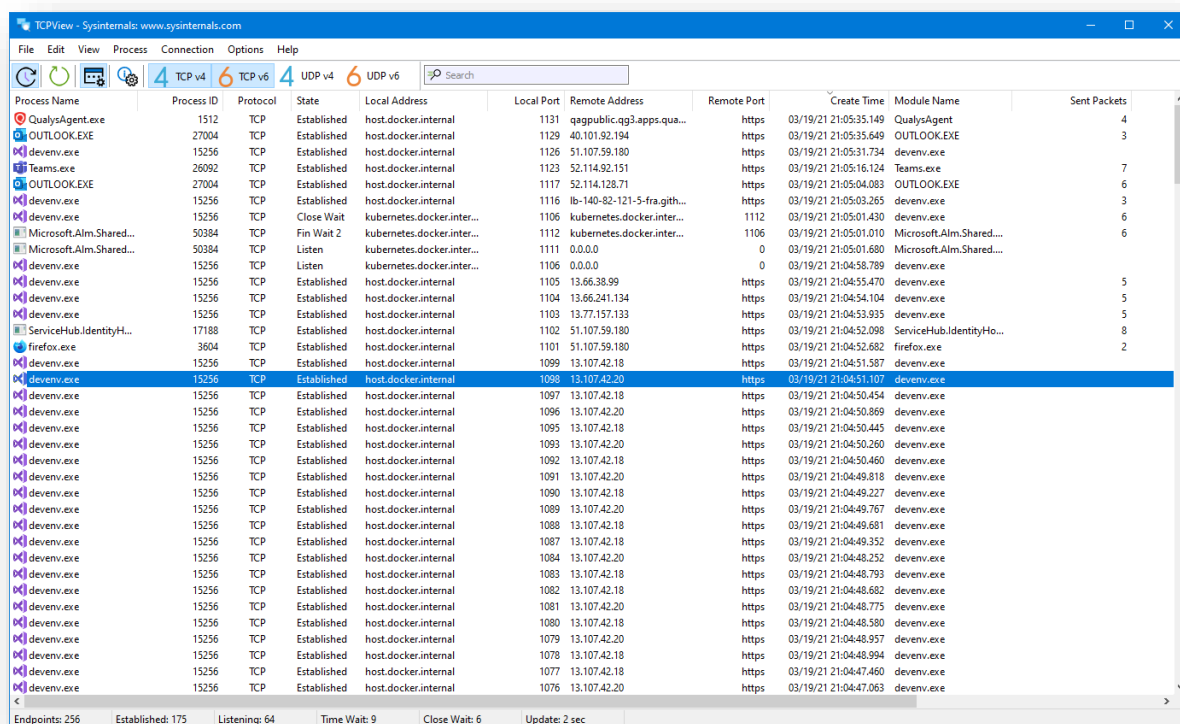
- `egrep [[:upper:]] diccionario`



## 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.qg3.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.gith...	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...	1106	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 21:04:48.380	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.





## “HOLA, MUNDO” EN OTROS LENGUAJES

RUST:

```
fn main() {  
  println!("Hello World!");  
}
```

---

CLOJURE

```
(ns clojure.examples.hello  
  (:gen-class))  
(defn hello-world []  
  (println "Hello, World!"))  
(hello-world)
```

---

TYPESCRIPT

```
let message: string = 'Hello, World!';  
console.log(message);
```

---

ELIXIR

```
IO.puts("Hello, World!")
```

---

JULIA

```
print("Hello World!")
```

---

PYTHON:

```
print('Hello, world!')
```

---

DART

```
void main() {  
  print('Hello, World!');  
}
```

---



## SWIFT

```
import UIKit
```

---

```
var str = "Hello, World!"
```

## NODE JS

```
// server.js  
'use strict';  
const http = require('http');  
const server = http.createServer(function (req, res) {  
    res.writeHead(200, {'content-type': 'text/plain'});  
    res.end('Hello, World!');  
});  
server.listen(8000);
```

---

## GO

```
package main  
import "fmt"  
func main() {  
    fmt.Println("Hello, World!")  
}
```

---

## F#

```
#light
```

---

```
let main =  
    printfn "Hello, World!"
```

---

```
do main
```

## C#

```
using System;  
using System.Collections.Generic;  
using System.Linq;  
using System.Text;  
using System.Threading.Tasks;
```

---



```
namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            Console.WriteLine("Hello, World!");

            Console.ReadLine();
        }
    }
}
```

---

#### Kotlin

```
fun main(args: Array<String>) {
    println("Hello World")
}
```

---

#### JavaScript

```
<!DOCTYPE HTML>
<html>
<body>
    <p>Before the script...</p>
    <script>
        alert( 'Hello, world!' );
    </script>
    <p>...After the script.</p>
</body>
</html>
```

---

#### Crystal

```
puts "Hello World"
```

---



## BASH

```
#!/bin/bash  
echo "Hello World"
```

---

## LISP

```
CL-USER> (defun hello ()  
            (format t "Hello, World!~%"))  
HELLO  
CL-USER> (hello)  
Hello, World!  
NIL  
CL-USER>
```

---

## ERLANG

```
-module(primer).  
-export([hello_world/0]).  
  
hello_world() ->  
    "hello world".
```

---

## RUBY

```
ruby -e 'print "Hola Mundo\n"'
```

---