



16 de septiembre de 2021
Ficha N° 22 LYNIS
CSIRT DE GOBIERNO

Comando de la semana “LYNIS”

I. CONTEXTO

Este documento, denominado, en esta oportunidad, “LYNIS”, 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 Scripting¹, Expect, Python, C, C#, C++, Golang, JavaScript, PowerShell, Ruby, Java, PHP, Elixir, Elm, Go, Dart, DLang, Pony, TypeScript, Kotlin, Nim, OCaml, ~~Q#~~², 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 preferidos³ (segundo gráfico).

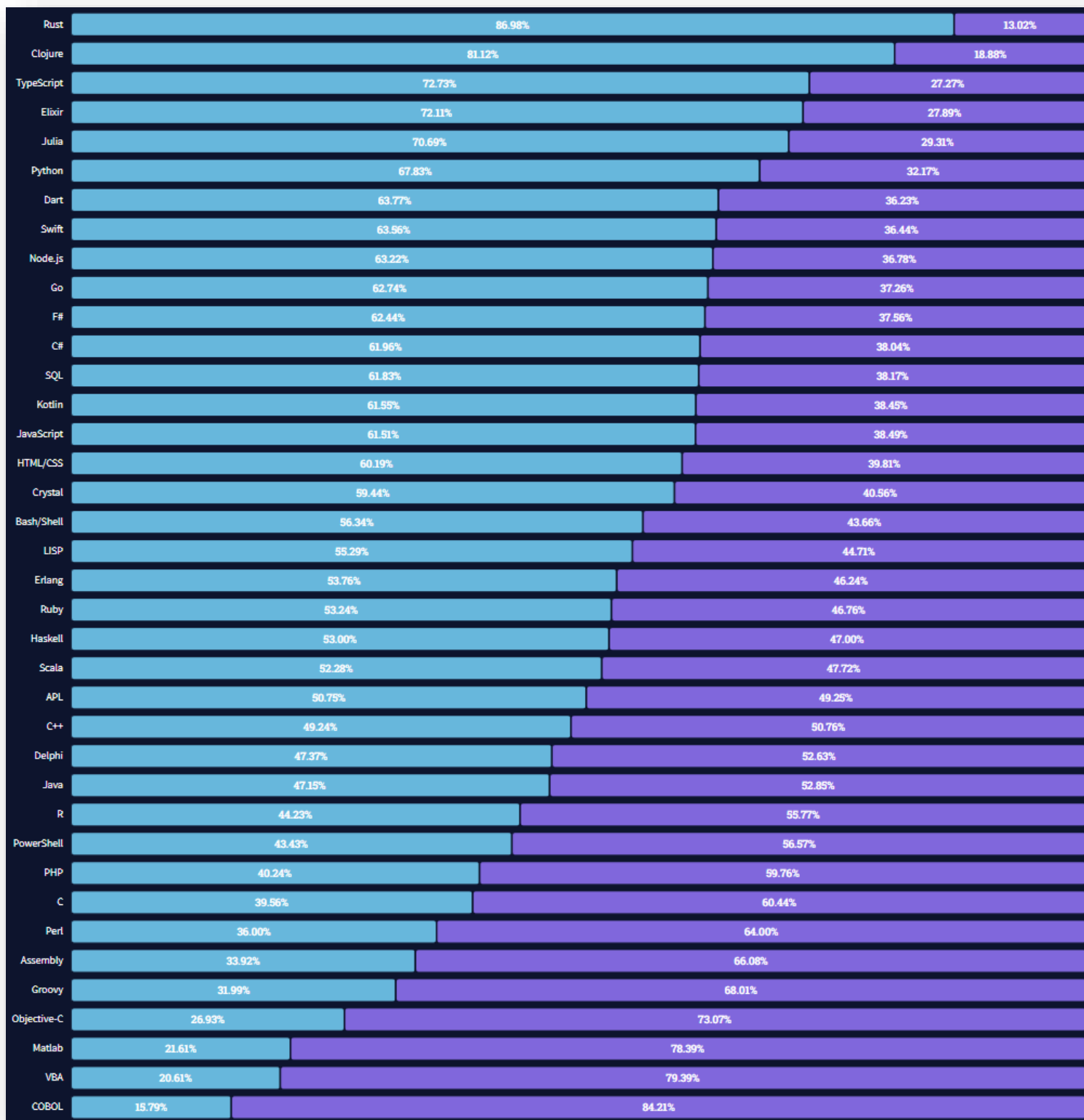
¹ <https://scis.uohyd.ac.in/~apcs/itw/UNIXProgrammingEnvironment.pdf>

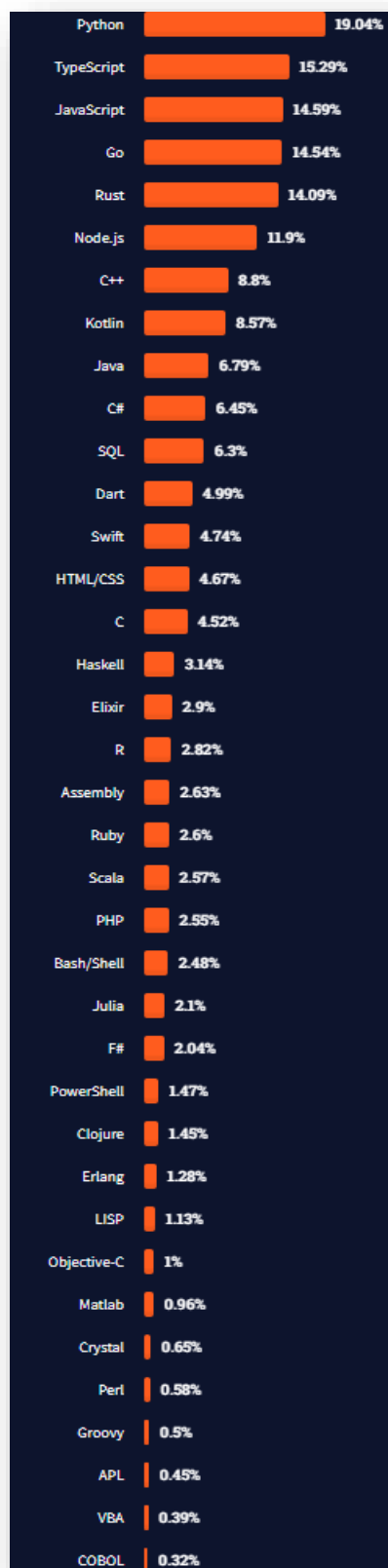
² <https://github.com/Microsoft/QuantumKatas/>

³ <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

Hardening⁴ (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso.

Entonces para recordar en una frase:

Por hardening entenderemos a un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo o servidor.

El propósito del hardening es entorpecer la labor del ciberdelincuente y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos es que no necesariamente logrará establecer equipos “invulnerables”. Es importante recordar que, según el modelo de defensa en profundidad, el host es sólo una capa de éste.

En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender “globalmente” un sistema. Entre las actividades propias de un proceso de hardening se pueden contar las siguientes:

- ❖ Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.
- ❖ Instalación segura del sistema operativo. Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (una para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos⁵ que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.
- ❖ Activación y/o configuración adecuada de servicios de actualizaciones automáticas, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una institución, es adecuado instalar un servidor

⁴ <https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/index.cfm>

⁵ <https://www.factor.mx/portal/base-de-conocimiento/sistemas-de-archivos/>



de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.

- 🛡️ Instalación, configuración y mantención de programas de seguridad tales como Antimalware, Antispyware, EDR, HIDS, y un filtro Antispam según las necesidades del sistema.
- 🛡️ Configuración de la política local del sistema, considerando varios puntos relevantes: Política de contraseñas robusta, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas. Renombramiento y posterior deshabilitación de cuentas estándar del sistema, como administrador e invitado. Asignación correcta de derechos de usuario, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.
- 🛡️ Configuración de opciones de seguridad generales, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.
- 🛡️ Restricciones de software, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.
- 🛡️ Activación de auditorías de sistema, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.
- 🛡️ Configuración de servicios de sistema. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.
- 🛡️ Configuración de los protocolos de Red. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo. Por ejemplo si internamente no utiliza IPv6 deshabilítelo y solo deje activo IPv4.
- 🛡️ Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Una correcta definición y asignación de permisos a nivel de carpetas y archivos es clave para evitar un acceso no deseado al contenido de los mismos.
- 🛡️ Configuración de opciones de seguridad de los distintos programas, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.
- 🛡️ Configuración de acceso remoto. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número



muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH⁶.

- ❖ Configuración adecuada de cuentas de usuario, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de usuarios para realizar labores administrativas en vez de iniciar sesión como administradores.
- ❖ Cifrado de archivos o unidades según las necesidades del sistema, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.
- ❖ Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

El espectro de actividades que deben ser llevadas a cabo dentro de este proceso es amplio y tiene actividades de todo tipo. Sin embargo, el objetivo para todas estas actividades es siempre el mismo: **Dejar el sistema operativo lo más restringido posible.**

En consecuencia, el Hardening es una ayuda indispensable para ahorrarse bastantes problemas por parte de los administradores de sistemas. Entre sus ventajas, se puede contar la disminución de incidentes de ciberseguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas, y finalmente la posibilidad – en muchos casos – de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos.

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

⁶ <https://www.ccn-cert.cni.es/informes/abstracts/4880-medidas-de-seguridad-para-acceso-remoto/file.html>









¿Qué es LYNYS?

Lynis es una herramienta de auditoría de seguridad, de código abierto. Su principal objetivo es auditar y fortalecer los sistemas basados en Unix y Linux (hardening). Escanea el sistema realizando muchas comprobaciones de control de seguridad. Los ejemplos incluyen buscar software instalado y determinar posibles fallas de configuración.

Muchas pruebas son parte de pautas y estándares de seguridad comunes, además de pruebas de seguridad adicionales. Después del escaneo, se mostrará un informe con todos los hallazgos descubiertos.

Lynis funciona en casi todos los sistemas y versiones basados en UNIX, incluyendo

-  AIX
-  FreeBSD
-  HP-UX
-  Linux
-  macOS
-  NetBSD
-  NixOS
-  OpenBSD
-  Solaris
-  y otros

Incluso se ejecuta en sistemas como la Raspberry Pi, dispositivos IoT y dispositivos de almacenamiento QNAP.

Cómo funciona

La exploración de Lynis es modular y oportunista. Esto significa que sólo utilizará y probará los componentes que pueda encontrar, como las herramientas del sistema disponibles y sus bibliotecas. La ventaja es que no es necesario instalar otras herramientas, por lo que puede mantener sus sistemas limpios.

Al utilizar este método de escaneo, la herramienta puede funcionar casi sin dependencias. Además, cuantos más componentes descubra, más extensa será la auditoría. En otras palabras: Lynis siempre realizará escaneos adaptados a su sistema. Ninguna auditoría será igual.

Ejemplo: Cuando Lynis detecta que está ejecutando Apache, realizará una ronda inicial de pruebas relacionadas con Apache. Luego, cuando realiza las pruebas específicas de Apache, también puede



descubrir una configuración SSL/TLS. Entonces realiza pasos adicionales de auditoría basados en eso. Un buen ejemplo es la recopilación de los certificados descubiertos, para que puedan ser escaneados posteriormente también.

Pasos de auditoría

Esto es lo que ocurre durante un análisis típico con Lynis:

- 🛡 Inicialización
- 🛡 Realiza comprobaciones básicas, como la propiedad de los archivos
- 🛡 Determinar el sistema operativo y las herramientas
- 🛡 Buscar los componentes de software disponibles
- 🛡 Comprobar la última versión de Lynis
- 🛡 Ejecutar los plugins habilitados
- 🛡 Ejecutar pruebas de seguridad por categoría
- 🛡 Realizar la ejecución de sus pruebas personalizadas (opcional)
- 🛡 Informar del estado del escaneo de seguridad

Además del informe y de la información mostrada en pantalla, todos los detalles técnicos del análisis se almacenan en un archivo de registro (lynis.log). Los resultados, como las advertencias y las sugerencias, se almacenan en un archivo de informe independiente (lynis-report.dat).

Pruebas de Lynis (controles)

Lynis realiza cientos de pruebas individuales. Cada prueba ayuda a determinar el estado de seguridad del sistema. La mayoría de las pruebas están escritas en shell script y tienen un identificador único (por ejemplo, KRNL-6000).

Flexibilidad

Con los identificadores únicos es posible ajustar un análisis de seguridad. Por ejemplo, si una prueba es demasiado estricta para su apetito de escaneo, simplemente desactívela. De este modo, obtendrá una auditoría del sistema óptima para su entorno.

Lynis es modular y permite ejecutar sus propias pruebas. Incluso puede crearlas en otros lenguajes de scripting o programación.

Plugins de Lynis

Los plugins son extensiones modulares de Lynis. Con la ayuda de los plugins, Lynis realizará pruebas adicionales y recogerá más información del sistema.



Cada plugin tiene el objetivo de recoger datos específicos. Estos datos se almacenan en el archivo de informes de Lynis (lynis-report.dat). Dependiendo de su uso de Lynis, los datos recogidos pueden proporcionar información valiosa entre los sistemas o entre las exploraciones individuales.

Los plugins proporcionan el mayor valor en entornos con más de 10 sistemas. Algunos plugins están disponibles en la sección de descargas⁷.





Plugins adicionales

Como parte de nuestra oferta Lynis Enterprise, los desarrolladores del núcleo mantienen un conjunto de plugins para nuestros clientes. Los datos que se recogen de forma centralizada (SaaS o autoalojado), proporcionan información adicional, como los usuarios disponibles, los procesos y los detalles de la red. Otra área importante es la de las pruebas de conformidad, en la que los puntos de datos ayudan a probar los estándares comunes y las guías de endurecimiento.

Estándares soportados

Otras herramientas suelen utilizar los mismos archivos de datos para realizar las pruebas. Lynis no se limita a una distribución específica de Linux, por lo que utiliza el conocimiento de más de 10 años de una amplia gama de fuentes. Puede ayudarle a automatizar o probar las mejores prácticas de seguridad de fuentes como

Puntos de referencia del CIS

-  NIST
-  NSA
-  Datos de OpenSCAP
-  Guías y recomendaciones de los proveedores (por ejemplo, Debian Gentoo, Red Hat)

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

⁷ <https://cisofy.com/lynis/plugins/>



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

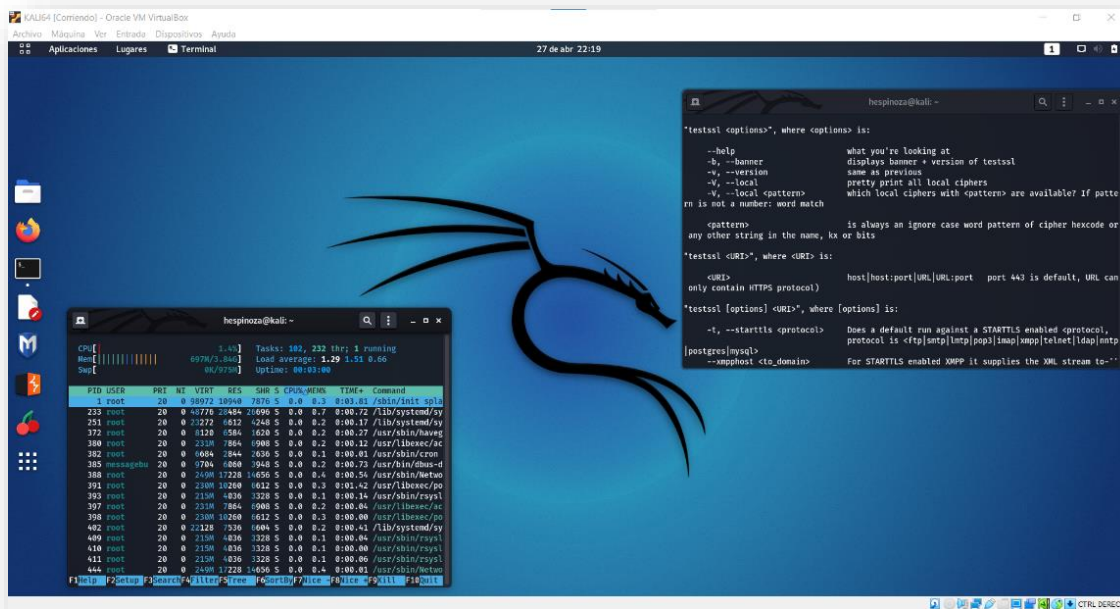
Bonus Track: Ejemplos muy básicos y simples del clásico “Hello, World!” escrito en diferentes lenguajes. El objetivo es despertar su curiosidad por estos lenguajes y ojalá se entusiasme y emprenda la cruzada de aprenderlo en profundidad, para luego aplicarlo en su quehacer cotidiano y dentro de lo posible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



III. PASO A PASO

PASO 1: UN ENTORNO ADECUADO PARA TRABAJAR.

Primero debe contar con una distribución de Kali⁸ Linux funcionando ya sea en una máquina física o en una máquina virtual^{9,10}.



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

⁸ <https://www.kali.org/downloads/>
⁹

https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0

¹⁰ <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 instalación¹¹

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 Linux¹² (el fabricante recomienda¹³ la imagen marcada como Instalador).

¹¹ 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.

¹² <https://www.kali.org/docs/introduction/download-official-kali-linux-images/>

¹³ <https://www.kali.org/docs/introduction/what-image-to-download/#which-image-to-choose>



- 🛡️ Grabe¹⁴ 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 red¹⁵ 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:

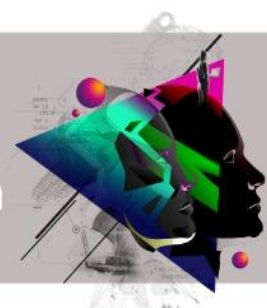
<https://www.kali.org/docs/installation/hard-disk-install/>



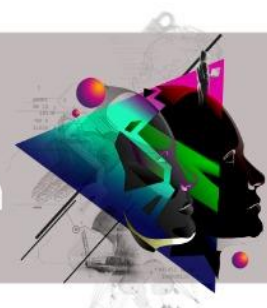
Otras distribuciones que puede considerar son las siguientes:

¹⁴ <https://www.kali.org/docs/usb/live-usb-install-with-windows/>

¹⁵ <https://www.kali.org/docs/installation/network-pxe/>



Nombre	Link	Descripción
ARCHSTRIKE	https://archstrike.org/	Distribución linux con foco en ciberseguridad.
BACKBOX	https://www.backbox.org/	Distribución de Linux orientada a pruebas de penetración y evaluación de seguridad que proporciona un conjunto de herramientas de análisis de redes y sistemas.
BLACKARCH	http://blackarch.org/	Herramientas para pruebas de penetración basada en Arch Linux.
BLACKBUNTU	https://archiveos.org/blackbuntu/	Es una distribución GNU / Linux basada en Ubuntu y diseñada con Pentest, Seguridad y Desarrollo en mente para la mejor experiencia.
BUGTRAQ	https://archiveos.org/bugtraq/	Distribución GNU / Linux destinada a análisis forense digital, pruebas de penetración, laboratorios de malware y análisis forense.
CAINE	http://www.caine-live.net/	CAINE (Computer Aided INvestigative Environment) es una distribución GNU / Linux italiana creada como un proyecto de Digital Forensics.
CYBORG HAWK LINUX	https://archiveos.org/cyborg-hawk/	Distribución de Linux basada en la plataforma Ubuntu con el último kernel para profesionales de la seguridad cibernética.
DEFT LINUX	http://www.deftlinux.net/	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.
DRACOS LINUX	https://dracos-linux.org/	Dracos Linux es un sistema operativo de código abierto que proporciona pruebas de penetración.
FEDORA SECURITY LAB	https://labs.fedoraproject.org/en/security/	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.
GNACK TRACK LINUX	https://archiveos.org/gnacktrack/	Distribución de Linux basada en Ubuntu que proporciona un conjunto de pruebas de penetración.
JONDO	https://anonymous-proxy-servers.net/en/jondo-live-cd.html	Entorno seguro y preconfigurado para navegación anónima.
KALI	https://www.kali.org/	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.
LIVE HACKING DVD	http://www.livehacking.com/live-hacking-cd/download-live-hacking/	Distribución de Linux basada en Ubuntu que proporciona un conjunto de pruebas de penetración.
MATRIUX	http://matriux.sourceforge.net/	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.
MOKI	https://github.com/moki-ics/moki	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.
NETWORK SECURITY TOOLKIT (NST)	https://sourceforge.net/projects/nst/files/	Un kit de herramientas de monitoreo y análisis de seguridad de red para distribución de Linux.
NODEZERO	https://sourceforge.net/projects/nodezero/	Linux basado en Ubuntu diseñado como un sistema completo que también se puede utilizar para pruebas de penetración.
PENTOO	https://pentoo.org/	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.
PARROT SECURITY OS	https://www.parrotsec.org/	Distribución GNU / Linux basada en Debian y diseñada pensando en la seguridad y la privacidad.
SAMURAI WEB TESTING FRAMEWORK	https://www.samuraiwtf.org/	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.
SECURITY ONION 2	https://securityonionsolutions.com/	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.
TAILS	https://tails.boum.org/	Sistema operativo portátil que protege la privacidad.
QUBES OS	https://www.qubes-os.org/	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.
WIFISLAX	https://www.wifislax.com/	Linux para auditorías Wireless.
DEMONLINUX	https://demonlinux.com	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 KALI¹⁶, 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 dotdotpwn
```

Luego verifique que haya quedado instalada:

```
# apt install lynis
```

Leyendo lista de paquetes... Hecho

Creando árbol de dependencias... Hecho

Leyendo la información de estado... Hecho

lynis ya está en su versión más reciente (3.0.2-1).

fijado lynis como instalado manualmente.

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 gstreamer1.0-packagekit libamtk-5-0

libamtk-5-common libavif9 libcaribou-common libcaribou0

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 libntfs-3g883

libplacebo72 libproxy1-plugin-webkit

libstd-rust-1.48 libstrictures-perl libtepl-5-0 libtracker-control-2.0-0 libtracker-miner-2.0-0

libtracker-sparql-2.0-0 libyara4 libzapojit-0.0-0

python3-gevent python3-gevent-websocket python3-greenlet python3-ipython-genutils

python3-jupyter-core python3-m2crypto python3-nbformat

python3-parameterized python3-plotly python3-zope.event

Utilice «apt autoremove» para eliminarlos.

0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 124 no actualizados.

```
# apt search ^lynis
```

Ordenando... Hecho

Buscar en todo el texto... Hecho

lynis/kali-rolling,now 3.0.2-1 all **[instalado]**

security auditing tool for Unix based systems

¹⁶ <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: “lynis -h”.

```
root@V: ~  
(root@V) ~  
# lynis -h  
  
[ Lynis 3.0.2 ]  
  
#####  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are  
welcome to redistribute it under the terms of the GNU General Public License.  
See the LICENSE file for details about using this software.  
  
2007-2020, CISOfy - https://cisofy.com/lynis/  
Enterprise support available (compliance, plugins, interface and tools)  
#####  
  
[+] Initializing program  
-----  
  
Usage: lynis command [options]  
  
Command:
```

El despliegue total de la ayuda es la siguiente:

```
# lynis -h  
  
[ Lynis 3.0.2 ]  
  
#####  
#  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are  
welcome to redistribute it under the terms of the GNU General Public License.  
See the LICENSE file for details about using this software.
```



```
2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####
#

[+] Initializing program
-----

Usage: lynis command [options]

Command:

audit
  audit system           : Perform local security scan
  audit system remote <host> : Remote security scan
  audit dockerfile <file>  : Analyze Dockerfile

show
  show                   : Show all commands
  show version           : Show Lynis version
  show help              : Show help

update
  update info            : Show update details

Options:

Alternative system audit modes
--forensics              : Perform forensics on a running or
mounted system
--pentest                : Non-privileged, show points of interest
for pentesting

Layout options
--no-colors              : Don't use colors in output
--quiet (-q)             : No output
--reverse-colors         : Optimize color display for light
backgrounds
--reverse-colours        : Optimize colour display for light
backgrounds

Misc options
--debug                  : Debug logging to screen
--no-log                 : Don't create a log file
--profile <profile>      : Scan the system with the given profile
file
--view-manpage (--man)   : View man page
--verbose                : Show more details on screen
--version (-V)           : Display version number and quit
--wait                   : Wait between a set of tests
--slow-warning <seconds> : Threshold for slow test warning in seconds
(default 10)
```



Enterprise options

--plugindir <path>

: Define path of available plugins

--upload

: Upload data to central node

More options available. Run '/usr/sbin/lynis show options', or use the man page.



PASO 4: PONERLO EN MARCHA PARA VERIFICAR NUESTRA INFRAESTRUCTURA.

Un ejemplo de ejecución básica para nuestros primeros pasos:

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

EJEMPLO 1

Analizamos las debilidades de un host "X" basado en la distribución de Linux "Debian" para ilustrar que acciones de hardening podrían mejorar su postura de seguridad.

```
# lynis audit system
```

```
[ Lynis 3.0.2 ]
```

```
#####  
#  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are  
welcome to redistribute it under the terms of the GNU General Public License.  
See the LICENSE file for details about using this software.  
  
2007-2020, CISOfy - https://cisofy.com/lynis/  
Enterprise support available (compliance, plugins, interface and tools)  
#####  
#
```

```
[+] Initializing program
```

```
-----  
- Detecting OS... [ DONE ]  
- Checking profiles... [ DONE ]  
- Detecting language and localization [ es ]  
-----
```

```
-----  
Program version: 3.0.2  
Operating system: Linux  
Operating system name: Kali Linux  
Operating system version: kali-rolling  
Kernel version: 5.10.0  
Hardware platform: x86_64  
Hostname: V  
-----
```

```
-----  
Profiles: /etc/lynis/default.prf  
Log file: /var/log/lynis.log  
Report file: /var/log/lynis-report.dat  
Report version: 1.0  
Plugin directory: /etc/lynis/plugins  
-----
```

```
-----  
Auditor: [Not Specified]  
Language: es  
Test category: all  
Test group: all  
-----
```

```
- Program update status... [ NO UPDATE ]
```



```
[+] System tools
-----
- Scanning available tools...
- Checking system binaries...

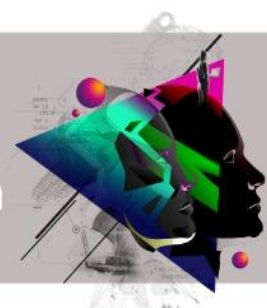
[+] Plugins (fase 1)
-----
Nota: los plugins contienen pruebas más extensivas y toman más tiempo

- Plugin: debian
  [
[+] Debian Tests
-----
- Checking for system binaries that are required by Debian Tests...
- Checking /bin... [ FOUND ]
- Checking /sbin... [ FOUND ]
- Checking /usr/bin... [ FOUND ]
- Checking /usr/sbin... [ FOUND ]
- Checking /usr/local/bin... [ FOUND ]
- Checking /usr/local/sbin... [ FOUND ]
- Authentication:
  - PAM (Pluggable Authentication Modules):

[WARNING]: Test DEB-0001 had a long execution: 13.660322 seconds

- libpam-tmpdir [ Not Installed ]
- File System Checks:
  - DM-Crypt, Cryptsetup & Cryptmount:
- Software:
  - apt-listbugs [ Not Installed ]
  - apt-listchanges [ Not Installed ]
  - needrestart [ Installed ]
  - debsecan [ Not Installed ]
  - debsums [ Not Installed ]
  - fail2ban [ Not Installed ]
]

[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DESACTIVADO ]
- Checking presence GRUB2 [ ENCONTRADO ]
  - Checking for password protection [ NONE ]
- Check running services (systemctl) [ HECHO ]
  Result: found 28 running services
- Check enabled services at boot (systemctl) [ HECHO ]
  Result: found 25 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
  - ModemManager.service: [ MEDIUM ]
  - NetworkManager.service: [ EXPOSED ]
  - accounts-daemon.service: [ UNSAFE ]
  - colord.service: [ EXPOSED ]
  - cron.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - docker.service: [ UNSAFE ]
  - elasticsearch.service: [ EXPOSED ]
  - emergency.service: [ UNSAFE ]
```



```
- filebeat.service: [ UNSAFE ]
- gdm.service: [ UNSAFE ]
- getty@tty1.service: [ UNSAFE ]
- getty@tty2.service: [ UNSAFE ]
- haveged.service: [ OK ]
- inetutils-inetd.service: [ UNSAFE ]
- kibana.service: [ UNSAFE ]
- lynis.service: [ UNSAFE ]
- opendistro-performance-analyzer.service: [ UNSAFE ]
- packagekit.service: [ UNSAFE ]
- plymouth-start.service: [ UNSAFE ]
- polkit.service: [ UNSAFE ]
- rc-local.service: [ UNSAFE ]
- rescue.service: [ UNSAFE ]
- rpc-gssd.service: [ UNSAFE ]
- rpc-svcgssd.service: [ UNSAFE ]
- rsync.service: [ EXPOSED ]
- rsyslog.service: [ UNSAFE ]
- rtkit-daemon.service: [ MEDIUM ]
- smartmontools.service: [ UNSAFE ]
- ssh.service: [ UNSAFE ]
- systemd-ask-password-console.service: [ UNSAFE ]
- systemd-ask-password-plymouth.service: [ UNSAFE ]
- systemd-ask-password-wall.service: [ UNSAFE ]
- systemd-fsckd.service: [ UNSAFE ]
- systemd-initctl.service: [ UNSAFE ]
- systemd-journald.service: [ OK ]
- systemd-logind.service: [ OK ]
- systemd-networkd.service: [ OK ]
- systemd-rfkill.service: [ UNSAFE ]
- systemd-udev.service: [ EXPOSED ]
- thin.service: [ UNSAFE ]
- udisks2.service: [ UNSAFE ]
- upower.service: [ OK ]
- user@1000.service: [ UNSAFE ]
- user@136.service: [ UNSAFE ]
- wazuh-manager.service: [ UNSAFE ]
- wpa_supplicant.service: [ UNSAFE ]
```

[+] Kernel

```
-----
- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE) [ ENCONTRADO ]
  CPU support: PAE and/or NoeXecute supported
- Checking kernel version and release [ HECHO ]
- Checking kernel type [ HECHO ]
- Checking loaded kernel modules [ HECHO ]
  Found 138 active modules
- Checking Linux kernel configuration file [ ENCONTRADO ]
- Checking default I/O kernel scheduler [ NO ENCONTRADO ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration
  - configuration in systemd conf files [ DEFAULT ]
  - configuration in etc/profile [ DEFAULT ]
  - 'hard' configuration in security/limits.conf [ DEFAULT ]
  - 'soft' configuration in security/limits.conf [ DEFAULT ]
- Checking setuid core dumps configuration [ DESACTIVADO ]
- Check if reboot is needed [ NO ]
```



[+] Memoria y Procesos

- | | |
|---------------------------------------|-------------------|
| - Checking /proc/meminfo | [ENCONTRADO] |
| - Searching for dead/zombie processes | [NO ENCONTRADO] |
| - Searching for IO waiting processes | [NO ENCONTRADO] |
| - Search prelink tooling | [NO ENCONTRADO] |

[+] Users, Groups and Authentication

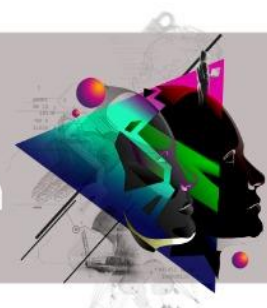
- | | |
|---|-------------------|
| - Administrator accounts | [OK] |
| - Unique UIDs | [OK] |
| - Consistency of group files (grpck) | [OK] |
| - Unique group IDs | [OK] |
| - Unique group names | [OK] |
| - Password file consistency | [OK] |
| - Password hashing methods | [OK] |
| - Checking password hashing rounds | [DESACTIVADO] |
| - Query system users (non daemons) | [HECHO] |
| - NIS+ authentication support | [NOT ENABLED] |
| - NIS authentication support | [NOT ENABLED] |
| - Sudoers file(s) | [ENCONTRADO] |
| - Permissions for directory: /etc/sudoers.d | [PELIGRO] |
| - Permissions for: /etc/sudoers | [OK] |
| - Permissions for: /etc/sudoers.d/kali-grant-root | [OK] |
| - Permissions for: /etc/sudoers.d/README | [OK] |
| - PAM password strength tools | [SUGERENCIA] |
| - PAM configuration files (pam.conf) | [ENCONTRADO] |
| - PAM configuration files (pam.d) | [ENCONTRADO] |
| - PAM modules | [ENCONTRADO] |
| - LDAP module in PAM | [NO ENCONTRADO] |
| - Accounts without expire date | [SUGERENCIA] |
| - Accounts without password | [OK] |
| - Locked accounts | [OK] |
| - Checking user password aging (minimum) | [DESACTIVADO] |
| - User password aging (maximum) | [DESACTIVADO] |
| - Checking expired passwords | [OK] |
| - Checking Linux single user mode authentication | [OK] |
| - Determining default umask | |
| - umask (/etc/profile) | [NO ENCONTRADO] |
| - umask (/etc/login.defs) | [SUGERENCIA] |
| - LDAP authentication support | [NOT ENABLED] |
| - Logging failed login attempts | [ENABLED] |

[+] Shells

- | | |
|---|----------|
| - Checking shells from /etc/shells
Result: found 14 shells (valid shells: 14). | |
| - Session timeout settings/tools | [NONE] |
| - Checking default umask values | |
| - Checking default umask in /etc/bash.bashrc | [NONE] |
| - Checking default umask in /etc/profile | [NONE] |

[+] File systems

- | | |
|------------------------------|----------------|
| - Checking mount points | |
| - Checking /home mount point | [SUGERENCIA] |
| - Checking /tmp mount point | [SUGERENCIA] |



```

- Checking /var mount point                [ SUGERENCIA ]
- Query swap partitions (fstab)             [ OK ]
- Testing swap partitions                   [ OK ]
- Testing /proc mount (hidepid)             [ SUGERENCIA ]
- Checking for old files in /tmp            [ OK ]
- Checking /tmp sticky bit                  [ OK ]
- Checking /var/tmp sticky bit              [ OK ]
- ACL support root file system              [ ENABLED ]
- Mount options of /                       [ NON DEFAULT ]
- Mount options of /dev                    [ PARTIALLY HARDENED ]
]
- Mount options of /dev/shm                [ PARTIALLY HARDENED ]
]
- Mount options of /run                    [ HARDENED ]
- Total without nodev:6 noexec:10 nosuid:4 ro or noexec (W^X): 10 of total 25
- Checking Locate database                  [ NO ENCONTRADO ]
- Disable kernel support of some filesystems
  - Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf

[+] USB Devices
-----
- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization           [ ENABLED ]
- Checking USBGuard                           [ NO ENCONTRADO ]

[+] Storage
-----
- Checking firewire ohci driver (modprobe config) [ NOT DISABLED ]

[+] NFS
-----
- Query rpc registered programs               [ HECHO ]
- Query NFS versions                         [ HECHO ]
- Query NFS protocols                        [ HECHO ]
- Check running NFS daemon                   [ NO ENCONTRADO ]

[+] Name services
-----
- Searching DNS domain name                  [ ENCONTRADO ]
  Domain name: acme.cl
- Checking /etc/hosts
  - Duplicate entries in hosts file           [ NONE ]
  - Presence of configured hostname in /etc/hosts [ ENCONTRADO ]
  - Hostname mapped to localhost              [ NO ENCONTRADO ]
  - Localhost mapping to IP address           [ OK ]

[+] Ports and packages
-----
- Searching package managers
  - Searching dpkg package manager            [ ENCONTRADO ]
    - Querying package manager
  - Query unpurged packages                  [ ENCONTRADO ]
- Checking security repository in sources.list file or directory [ PELIGRO ]
- Checking vulnerable packages (apt-get only) [ HECHO ]
- Checking package audit tool                [ INSTALLED ]
  Found: apt-get
- Toolkit for automatic upgrades (unattended-upgrade) [ ENCONTRADO ]

```



```
[+] Networking
-----
- Checking IPv6 configuration                [ ENABLED ]
  Configuration method                      [ AUTO ]
  IPv6 only                                [ NO ]
- Checking configured nameservers
  - Testing nameservers
    Nameserver: 8.8.8.8                     [ OK ]
  - Minimal of 2 responsive nameservers    [ PELIGRO ]
  - DNSSEC supported (systemd-resolved)    [ DESCONOCIDO ]
- Checking default gateway                  [ HECHO ]
- Getting listening ports (TCP/UDP)        [ HECHO ]
- Checking promiscuous interfaces          [ OK ]
- Checking waiting connections              [ OK ]
- Checking status DHCP client
- Checking for ARP monitoring software     [ NO ENCONTRADO ]
- Uncommon network protocols               [ 0 ]

[+] Printers and Spools
-----
- Checking cups daemon                     [ NO ENCONTRADO ]
- Checking lp daemon                       [ NO ESTÁ CORRIENDO ]
]

[+] Software: e-mail and messaging
-----

[+] Software: firewalls
-----
- Checking iptables kernel module          [ ENCONTRADO ]
- Checking iptables policies of chains     [ ENCONTRADO ]
- Checking for empty ruleset               [ OK ]
- Checking for unused rules                [ ENCONTRADO ]
- Checking host based firewall             [ ACTIVE ]

[+] Software: webserver
-----
- Checking Apache (binary /usr/sbin/apache2) [ ENCONTRADO ]
  Info: Configuration file found (/etc/apache2/apache2.conf)
  Info: No virtual hosts found
  * Loadable modules                     [ ENCONTRADO (119) ]
]
  - Found 119 loadable modules
    mod_evasive: anti-DoS/brute force      [ NO ENCONTRADO ]
    mod_reqtimeout/mod_qos                 [ ENCONTRADO ]
    ModSecurity: web application firewall  [ NO ENCONTRADO ]
- Checking nginx                           [ NO ENCONTRADO ]

[+] SSH Support
-----
- Checking running SSH daemon              [ ENCONTRADO ]
- Searching SSH configuration              [ ENCONTRADO ]
- OpenSSH option: AllowTcpForwarding      [ SUGERENCIA ]
- OpenSSH option: ClientAliveCountMax    [ SUGERENCIA ]
- OpenSSH option: ClientAliveInterval    [ OK ]
- OpenSSH option: Compression             [ SUGERENCIA ]
- OpenSSH option: FingerprintHash        [ OK ]
- OpenSSH option: GatewayPorts            [ OK ]
```



```
- OpenSSH option: IgnoreRhosts [ OK ]
- OpenSSH option: LoginGraceTime [ OK ]
- OpenSSH option: LogLevel [ SUGERENCIA ]
- OpenSSH option: MaxAuthTries [ SUGERENCIA ]
- OpenSSH option: MaxSessions [ SUGERENCIA ]
- OpenSSH option: PermitRootLogin [ OK ]
- OpenSSH option: PermitUserEnvironment [ OK ]
- OpenSSH option: PermitTunnel [ OK ]
- OpenSSH option: Port [ SUGERENCIA ]
- OpenSSH option: PrintLastLog [ OK ]
- OpenSSH option: StrictModes [ OK ]
- OpenSSH option: TCPKeepAlive [ SUGERENCIA ]
- OpenSSH option: UseDNS [ OK ]
- OpenSSH option: X11Forwarding [ SUGERENCIA ]
- OpenSSH option: AllowAgentForwarding [ SUGERENCIA ]
- OpenSSH option: AllowUsers [ NO ENCONTRADO ]
- OpenSSH option: AllowGroups [ NO ENCONTRADO ]

[+] SNMP Support
-----
- Checking running SNMP daemon [ NO ENCONTRADO ]

[+] Databases
-----
No database engines found

[+] LDAP Services
-----
- Checking OpenLDAP instance [ NO ENCONTRADO ]

[+] PHP
-----
- Checking PHP [ ENCONTRADO ]
- Checking PHP disabled functions [ ENCONTRADO ]
- Checking expose_php option [ OFF ]
- Checking enable_dl option [ OFF ]
- Checking allow_url_fopen option [ ON ]
- Checking allow_url_include option [ OFF ]
- Checking listen option [ OK ]

[+] Squid Support
-----
- Checking running Squid daemon [ NO ENCONTRADO ]

[+] Logging and files
-----
- Checking for a running log daemon [ OK ]
- Checking Syslog-NG status [ NO ENCONTRADO ]
- Checking systemd journal status [ ENCONTRADO ]
- Checking Metalog status [ NO ENCONTRADO ]
- Checking RSyslog status [ ENCONTRADO ]
- Checking RFC 3195 daemon status [ NO ENCONTRADO ]
- Checking minilogd instances [ NO ENCONTRADO ]
- Checking logrotate presence [ OK ]
- Checking remote logging [ NOT ENABLED ]
- Checking log directories (static list) [ HECHO ]
- Checking open log files [ HECHO ]
- Checking deleted files in use [ FILES FOUND ]
```



```
[+] Insecure services
-----
- Installed inetd package [ NO ENCONTRADO ]
- Checking enabled inetd services [ OK ]
- Installed xinetd package [ OK ]
- xinetd status
- Installed rsh client package [ OK ]
- Installed rsh server package [ OK ]
- Installed telnet client package [ OK ]
- Installed telnet server package [ NO ENCONTRADO ]
- Checking NIS client installation [ OK ]
- Checking NIS server installation [ OK ]
- Checking TFTP client installation [ SUGERENCIA ]
- Checking TFTP server installation [ SUGERENCIA ]

[+] Banners and identification
-----
- /etc/issue [ ENCONTRADO ]
- /etc/issue contents [ WEAK ]
- /etc/issue.net [ ENCONTRADO ]
- /etc/issue.net contents [ WEAK ]

[+] Scheduled tasks
-----
- Checking crontab and cronjob files [ HECHO ]

[+] Accounting
-----
- Checking accounting information [ NO ENCONTRADO ]
- Checking sysstat accounting data [ DESACTIVADO ]
- Checking auditd [ NO ENCONTRADO ]

[+] Time and Synchronization
-----
- Checking for a running NTP daemon or client [ PELIGRO ]

[+] Cryptography
-----
- Checking for expired SSL certificates [0/134] [ NONE ]

[WARNING]: Test CRYPT-7902 had a long execution: 38.968805 seconds

- Found 0 encrypted and 1 unencrypted swap devices in use. [ OK ]
- Kernel entropy is sufficient [ SI ]
- HW RNG & rngd [ NO ]
- SW prng [ SI ]

[+] Virtualization
-----

[+] Containers
-----
- Docker
- Docker daemon [ CORRIENDO ]
- Docker info output (warnings) [ 1 ]
- Containers
- Total containers [ 1 ]
```



- Unused containers	[1]
- File permissions	[OK]
[+] Security frameworks	

- Checking presence AppArmor	[ENCONTRADO]
- Checking AppArmor status	[ENABLED]
Found 115 unconfined processes	
- Checking presence SELinux	[NO ENCONTRADO]
- Checking presence TOMOYO Linux	[NO ENCONTRADO]
- Checking presence grsecurity	[NO ENCONTRADO]
- Checking for implemented MAC framework	[OK]
[+] Software: file integrity	

- Checking file integrity tools	
- dm-integrity (status)	[DESACTIVADO]
- dm-verity (status)	[DESACTIVADO]
- Checking presence integrity tool	[NO ENCONTRADO]
[+] Software: System tooling	

- Checking automation tooling	
- Automation tooling	[NO ENCONTRADO]
- Checking for IDS/IPS tooling	[NONE]
[+] Malware	

- Revisando chkrootkit	[ENCONTRADO]
[+] File Permissions	

- Starting file permissions check	
File: /boot/grub/grub.cfg	[OK]
File: /etc/crontab	[SUGERENCIA]
File: /etc/group	[OK]
File: /etc/group-	[OK]
File: /etc/hosts.allow	[OK]
File: /etc/hosts.deny	[OK]
File: /etc/issue	[OK]
File: /etc/issue.net	[OK]
File: /etc/motd	[OK]
File: /etc/passwd	[OK]
File: /etc/passwd-	[OK]
File: /etc/ssh/sshd_config	[SUGERENCIA]
Directory: /etc/cron.d	[SUGERENCIA]
Directory: /etc/cron.daily	[SUGERENCIA]
Directory: /etc/cron.hourly	[SUGERENCIA]
Directory: /etc/cron.weekly	[SUGERENCIA]
Directory: /etc/cron.monthly	[SUGERENCIA]
[+] Home directories	

- Permissions of home directories	[PELIGRO]
- Ownership of home directories	[OK]
- Checking shell history files	[OK]
[+] Kernel Hardening	



```
-----
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [ DIFFERENT ]
- fs.protected_fifos (exp: 2) [ DIFFERENT ]
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_regular (exp: 2) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ OK ]
- kernel.core_uses_pid (exp: 1) [ DIFFERENT ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ OK ]
- kernel.kptr_restrict (exp: 2) [ DIFFERENT ]
- kernel.modules_disabled (exp: 1) [ DIFFERENT ]
- kernel.perf_event_paranoid (exp: 3) [ OK ]
- kernel.randomize_va_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ DIFFERENT ]
- kernel.unprivileged_bpf_disabled (exp: 1) [ DIFFERENT ]
- kernel.yama.pttrace_scope (exp: 1 2 3) [ DIFFERENT ]
- net.core.bpf_jit_harden (exp: 2) [ DIFFERENT ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp_filter (exp: 1) [ DIFFERENT ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
- net.ipv4.tcp_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
- net.ipv6.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]

[+] Hardening
-----
- Installed compiler(s) [ ENCONTRADO ]
- Installed malware scanner [ ENCONTRADO ]

[+] Pruebas personalizadas
-----
- Running custom tests... [ NONE ]

[+] Plugins (fase 2)
-----

=====
=

-[ Lynis 3.0.2 Results ]-

Warnings (2):
```



```
-----
! Can't find any security repository in /etc/apt/sources.list or sources.list.d
directory [PKGS-7388]
- Solution :
  https://cisofy.com/lynis/controls/PKGS-7388/

! Couldn't find 2 responsive nameservers [NETW-2705]
- Solution :
  https://cisofy.com/lynis/controls/NETW-2705/

Suggestions (61):
-----
* This release is more than 4 months old. Check the website or GitHub to see
if there is an update available. [LYNIS]
- Solution :
  https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT
installation. [DEB-0810]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0810/

* Install apt-listchanges to display any significant changes prior to any
upgrade via APT. [DEB-0811]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0811/

* Install debsecan to generate lists of vulnerabilities which affect this
installation. [DEB-0870]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0870/

* Install debsums for the verification of installed package files against MD5
checksums. [DEB-0875]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0875/

* Install fail2ban to automatically ban hosts that commit multiple
authentication errors. [DEB-0880]
- Solution :
  https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration
(e.g. boot in single user mode without password) [BOOT-5122]
- Solution :
  https://cisofy.com/lynis/controls/BOOT-5122/

* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
- Solution :
  https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in
/etc/security/limits.conf file [KRNL-5820]
```



```
- Solution :  
https://cisofy.com/lynis/controls/KRNL-5820/  
  
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9230/  
  
* Install a PAM module for password strength testing like pam_cracklib or  
pam_passwdqc [AUTH-9262]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9262/  
  
* When possible set expire dates for all password protected accounts [AUTH-  
9282]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9282/  
  
* Configure minimum password age in /etc/login.defs [AUTH-9286]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9286/  
  
* Configure maximum password age in /etc/login.defs [AUTH-9286]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9286/  
  
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  
- Solution :  
https://cisofy.com/lynis/controls/AUTH-9328/  
  
* To decrease the impact of a full /home file system, place /home on a separate  
partition [FILE-6310]  
- Solution :  
https://cisofy.com/lynis/controls/FILE-6310/  
  
* To decrease the impact of a full /tmp file system, place /tmp on a separate  
partition [FILE-6310]  
- Solution :  
https://cisofy.com/lynis/controls/FILE-6310/  
  
* To decrease the impact of a full /var file system, place /var on a separate  
partition [FILE-6310]  
- Solution :  
https://cisofy.com/lynis/controls/FILE-6310/  
  
* The database required for 'locate' could not be found. Run 'updatedb' or  
'locate.updatedb' to create this file. [FILE-6410]  
- Solution :  
https://cisofy.com/lynis/controls/FILE-6410/  
  
* Consider disabling unused kernel modules [FILE-6430]  
- Details : /etc/modprobe.d/blacklist.conf  
- Solution : Add 'install MODULENAME /bin/true' (without quotes)  
https://cisofy.com/lynis/controls/FILE-6430/  
  
* Disable drivers like USB storage when not used, to prevent unauthorized  
storage or data theft [USB-1000]  
- Solution :  
https://cisofy.com/lynis/controls/USB-1000/
```




```
* Disable drivers like firewire storage when not used, to prevent unauthorized
storage or data theft [STRG-1846]
- Solution :
  https://cisofy.com/lynis/controls/STRG-1846/

* Purge old/removed packages (2 found) with aptitude purge or dpkg --purge
command. This will cleanup old configuration files, cron jobs and startup scripts.
[PKGS-7346]
- Solution :
  https://cisofy.com/lynis/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good
database. [PKGS-7370]
- Solution :
  https://cisofy.com/lynis/controls/PKGS-7370/

* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-
2705]
- Solution :
  https://cisofy.com/lynis/controls/NETW-2705/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
- Solution :
  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
- Solution :
  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]
- Solution :
  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
- Solution :
  https://cisofy.com/lynis/controls/NETW-3200/

* Check iptables rules to see which rules are currently not used [FIRE-4513]
- Solution :
  https://cisofy.com/lynis/controls/FIRE-4513/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts
[HTTP-6640]
- Solution :
  https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks
[HTTP-6643]
- Solution :
  https://cisofy.com/lynis/controls/HTTP-6643/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowTcpForwarding (set YES to NO)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
```



```
- Details : ClientAliveCountMax (set 3 to 2)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Compression (set YES to NO)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : LogLevel (set INFO to VERBOSE)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxAuthTries (set 6 to 3)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxSessions (set 10 to 2)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Port (set 22 to )
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : TCPKeepAlive (set YES to NO)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

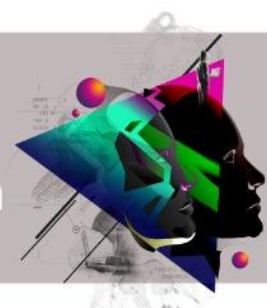
* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (set YES to NO)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (set YES to NO)
- Solution :
  https://cisofy.com/lynis/controls/SSH-7408/

* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable
downloads via PHP [PHP-2376]
- Solution :
  https://cisofy.com/lynis/controls/PHP-2376/

* Enable logging to an external logging host for archiving purposes and
additional protection [LOGG-2154]
- Solution :
  https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]
- Solution :
  https://cisofy.com/lynis/controls/LOGG-2190/
```



```
* It is recommended that TFTP be removed, unless there is a specific need for
TFTP (such as a boot server) [INSE-8318]
- Solution :
  https://cisofy.com/lynis/controls/INSE-8318/

* Removing the atftpd package decreases the risk of the accidental (or
intentional) activation of tftp services [INSE-8320]
- Solution :
  https://cisofy.com/lynis/controls/INSE-8320/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
- Solution :
  https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
- Solution :
  https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
- Solution :
  https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]
- Solution :
  https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
- Solution :
  https://cisofy.com/lynis/controls/ACCT-9628/

* Use NTP daemon or NTP client to prevent time issues. [TIME-3104]
- Solution :
  https://cisofy.com/lynis/controls/TIME-3104/

* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
- Solution :
  https://cisofy.com/lynis/controls/CONT-8104/

* Install a file integrity tool to monitor changes to critical and sensitive
files [FINT-4350]
- Solution :
  https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]
- Solution :
  https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
  https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict
enough. [HOME-9304]
- Solution :
  https://cisofy.com/lynis/controls/HOME-9304/
```



```
* One or more sysctl values differ from the scan profile and could be tweaked
[KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-
6000:<sysctl-key>)
https://cisofy.com/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
- Solution :
https://cisofy.com/lynis/controls/HRDN-7222/

Follow-up:
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
=

Lynis security scan details:

Hardening index : 63 [#####          ]
Tests performed : 271
Plugins enabled : 1

Components:
- Firewall          [V]
- Malware scanner   [V]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit    [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat

=====
=

Lynis 3.0.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
=

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/etc/lynis/default.prf for all settings)
```



```
root@V: ~
- Authentication:
  - PAM (Pluggable Authentication Modules):

[WARNING]: Test DEB-0001 had a long execution: 13.660322 seconds

  - libpam-tmpdir [ Not Installed ]
- File System Checks:
  - DM-Crypt, Cryptsetup & Cryptmount:
- Software:
  - apt-listbugs [ Not Installed ]
  - apt-listchanges [ Not Installed ]
  - needrestart [ Installed ]
  - debsecan [ Not Installed ]
  - debsums [ Not Installed ]
  - fail2ban [ Not Installed ]
]

[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DESACTIVADO ]
- Checking presence GRUB2 [ ENCONTRADO ]
  - Checking for password protection [ NONE ]
- Check running services (systemctl) [ HECHO ]
  Result: found 28 running services
```

La interfaz de comando muestra los hallazgos y destaca con colores tipo semáforo los problemas detectados. El analista debe tomar los resultados desde la sección “-[Lynix 3.0.2 Results]-” en adelante y estudiar la solución propuesta para aplicarla y mejorar la seguridad del servidor.

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, cryptojacking¹⁷ 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.

¹⁷ <https://www.eset.com/es/caracteristicas/cryptojacking/>



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 PowerShell¹⁸ (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.

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.

¹⁸ <https://devblogs.microsoft.com/scripting/table-of-basic-powershell-commands/>



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:

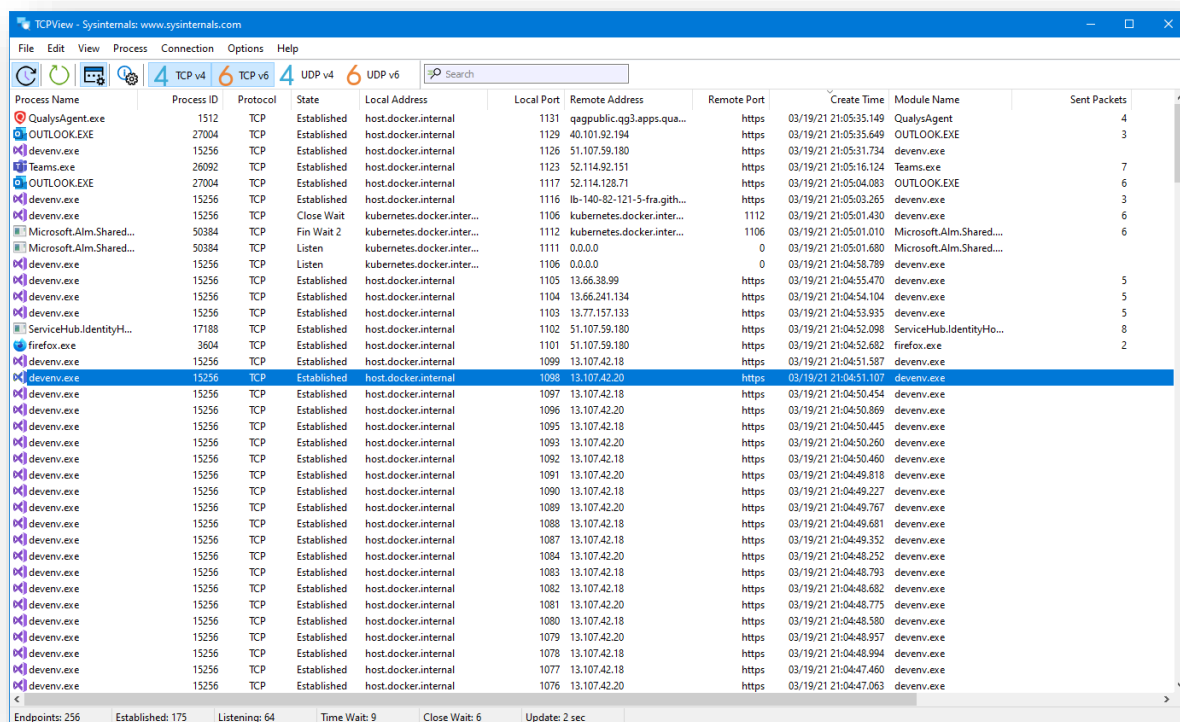
- Utilice el comando “clear” para limpiar la terminal si se llena de demasiados comandos anteriores.
- Pruebe el botón TAB para completar automáticamente lo que está escribiendo. Por ejemplo, si necesita escribir Documentos, comience a escribir un comando (vayamos con cd Docu, luego presione la tecla 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 Tcpcvcon, 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	4
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...	1102	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...	6
devenv.exe	15256	TCP	Listen	kubernetes.docker.inter...	1106	0.0.0.0	0	03/19/21 21:04:58.789	devenv.exe	6
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	2
devenv.exe	15256	TCP	Established	host.docker.internal	1098	13.107.42.20	https	03/19/21 21:04:51.107	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1097	13.107.42.18	https	03/19/21 21:04:50.454	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1096	13.107.42.20	https	03/19/21 21:04:50.869	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1095	13.107.42.18	https	03/19/21 21:04:50.445	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1093	13.107.42.20	https	03/19/21 21:04:50.260	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1092	13.107.42.18	https	03/19/21 21:04:50.460	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1091	13.107.42.20	https	03/19/21 21:04:49.818	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1090	13.107.42.18	https	03/19/21 21:04:49.227	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1089	13.107.42.20	https	03/19/21 21:04:49.767	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1088	13.107.42.18	https	03/19/21 21:04:49.681	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1087	13.107.42.18	https	03/19/21 21:04:49.352	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1084	13.107.42.20	https	03/19/21 21:04:48.252	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1083	13.107.42.18	https	03/19/21 21:04:48.793	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1082	13.107.42.18	https	03/19/21 21:04:48.682	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1081	13.107.42.20	https	03/19/21 21:04:48.775	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1080	13.107.42.18	https	03/19/21 21:04:48.580	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1079	13.107.42.20	https	03/19/21 21:04:48.957	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1078	13.107.42.18	https	03/19/21 21:04:48.994	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1077	13.107.42.18	https	03/19/21 21:04:47.460	devenv.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1076	13.107.42.20	https	03/19/21 21:04:47.063	devenv.exe	2

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 Tcpcvcon 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>
```
