Fuente: Bing Chat AI

Laboratorio 1. Configuración del sistema

DEPARTMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2023 – 2024 (V4.0 *"S-81 Isaac Peral"*)

Contenido

1

2

3

✍️

Bloque 1: Puesta en marcha de la MV

Prerrequisitos

Asegúrate de que tienes una máquina virtual en funcionamiento antes de empezar este laboratorio. Por favor consulta el fichero "***Lab 0A. Creando tu máquina virtual para el curso***" para ver las opciones que tienes para desplegar una máquina virtual *Ubuntu* adecuada para este curso (automatizada vía *Vagrant*, imagen `.ova` preconstruida o instalación manual). Asegúrate de que funciona antes de empezar. **Esto es un prerrequisito para empezar con los laboratorios, así que asegúrate de que lo cumples.**

🔍 ***NOTA: Quizá veas un error de VirtualBox respecto al adaptador Host-only cuando inicies la máquina virtual por primera vez. Si es tu caso, elimina esta interfaz de red de las propiedades de la máquina en VirtualBox y ejecútala de nuevo. Esto generalmente sucede en los laboratorios de la escuela debido a problemas de permisos, pero no debería pasar en tu casa. Recuerda que puedes acceder a la máquina virtual a través de SSH haciendo*** `ssh localhost:2222` ***(solo opción 1 u opción 2).***

1

2

3

Ejercicio L1B1_LOGIN: Entrar en sesión y actualizar la máquina virtual

Descripción de la actividad / Aplicación práctica

Necesitas actualizar tu SO para prevenir vulnerabilidades

Resultados Esperados

Esta actividad se completará cuando se actualice el sistema operativo. Si has escogido *Vagrant* como forma de construir tu máquina virtual automáticamente, es posible que este comando no actualice nada si acabas de construirla. *¿Por qué crees que ocurre esto?*

Otra información necesaria para su realización

Una vez desplegada, debes actualizar la máquina virtual de la siguiente forma.

```
sudo apt update
sudo apt full-upgrade
```

Para ahorrar espacio en disco (potencialmente), también puedes (opcionalmente) ejecutar

```
sudo apt autoremove
sudo apt autoclean
```

En sistemas *Ubuntu* también se usa el gestor de paquetes `snap` para instalar programas. Deberías comprobar que el *software* instalado con él está actualizado con este comando.

```
sudo snap refresh
```

🛠 Ejercicio L1B1_USER: Crear un usuario adecuado

🕵 Descripción de la actividad / Aplicación práctica

Necesitas crear una cuenta de usuario para un usuario nuevo

🎖 Resultados Esperados

Esta actividad se completará cuando el nuevo usuario esté operativo y pueda utilizar `sudo`

📖 Otra información necesaria para su realización

Se debe crear un nuevo usuario `uoxxxxxx` e introducirlo en el grupo `sudo` (para promocionar a `root` si es necesario en operaciones privilegiadas, como la instalación de software). Puedes seguir esta guía: https://www.digitalocean.com/community/tutorials/how-to-create-a-sudo-user-on-ubuntu-quickstart

- Crear el usuario: `sudo adduser <uoxxxxxx>`
- Escribir y confirmar la contraseña del nuevo usuario cuando se le solicite
- Completar la información del nuevo usuario. Vale aceptar los valores predeterminados y dejar toda esta información en blanco.
- Busca cómo usar el comando `usermod` para agregar el usuario al grupo `sudo`. De forma predeterminada en *Ubuntu*, los miembros del grupo `sudo` tienen privilegios `sudo`.

🔍 ***NOTA: Nuestro trabajo futuro SIEMPRE se hará usando la cuenta de usuario cuyo nombre es tu UO. El objetivo es que, sin importar lo que hagas la máquina virtual, siempre haya dos usuarios (siendo tú UO uno de ellos)***

🛠 Ejercicio L1B1_USERCHG: Cambiar entre usuarios correctamente

🕵 Descripción de la actividad / Aplicación práctica

Tienes que asumir varias identidades de usuario en la misma sesión de trabajo para ciertas operaciones

🎖 Resultados Esperados

Esta actividad se completará cuando el cambio de usuario funcione sin fallos

📖 Otra información necesaria para su realización

Ahora que tienes dos usuarios debes practicar cómo cambiar entre ellos. Esto se hace a través del comando `su`, pero **especificando el parámetro `-`** (por ejemplo: `su - ssiuser`) para arrancar un *shell* de inicio de sesión con un entorno idéntico al de un inicio de sesión real. **De lo contrario, ¡algunos programas podrían no funcionar correctamente en el futuro!**

🔍 ***NOTA: Cambiar entre usuarios en línea de comandos (incluso con `su -`) puede impedir que la GUI arranque con el nuevo usuario. Es posible que haya que hacer un cierre de sesión completo normal.***

Bloque 2: Operaciones básicas de seguridad

Ejercicio L1B2_SSH: Instalar un servidor *OpenSSH*

Descripción de la actividad / Aplicación práctica

Necesitas un acceso remoto seguro a tu máquina

Resultados Esperados

Esta actividad se completará cuando puedas conectarte a tu máquina utilizando SSH desde el host

Otra información necesaria para su realización

Instala este servidor de conexiones remotas seguras y comprueba que funciona correctamente desde tu máquina host. Puedes seguir este tutorial: https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/ o leer la documentación del curso sobre *VirtualBox* que proporcionamos. **Asegúrate de que el host pueda conectarse a la máquina virtual antes de continuar con los demás pasos.**

🔍 ***NOTA: Vagrant y la máquina virtual preconstruida ya tienen OpenSSH instalado, por lo que solo debes asegurarte de que puedes conectarte a través de SSH a la máquina virtual.***

Puedes utilizar cualquier cliente SSH que prefieras. Si usas el cliente estándar de línea de comandos, esta imagen te puede ayudar:

Ejercicio L1B2_UFW: Habilitar el *firewall*

Descripción de la actividad / Aplicación práctica

Necesitas bloquear cualquier conexión entrante a cualquier servicio que no autorices expresamente (política más segura)

Resultados Esperados

Esta actividad se completará cuando el *firewall* informe de que está activo y se permita el uso del puerto adecuado para el servicio SSH

Otra información necesaria para su realización

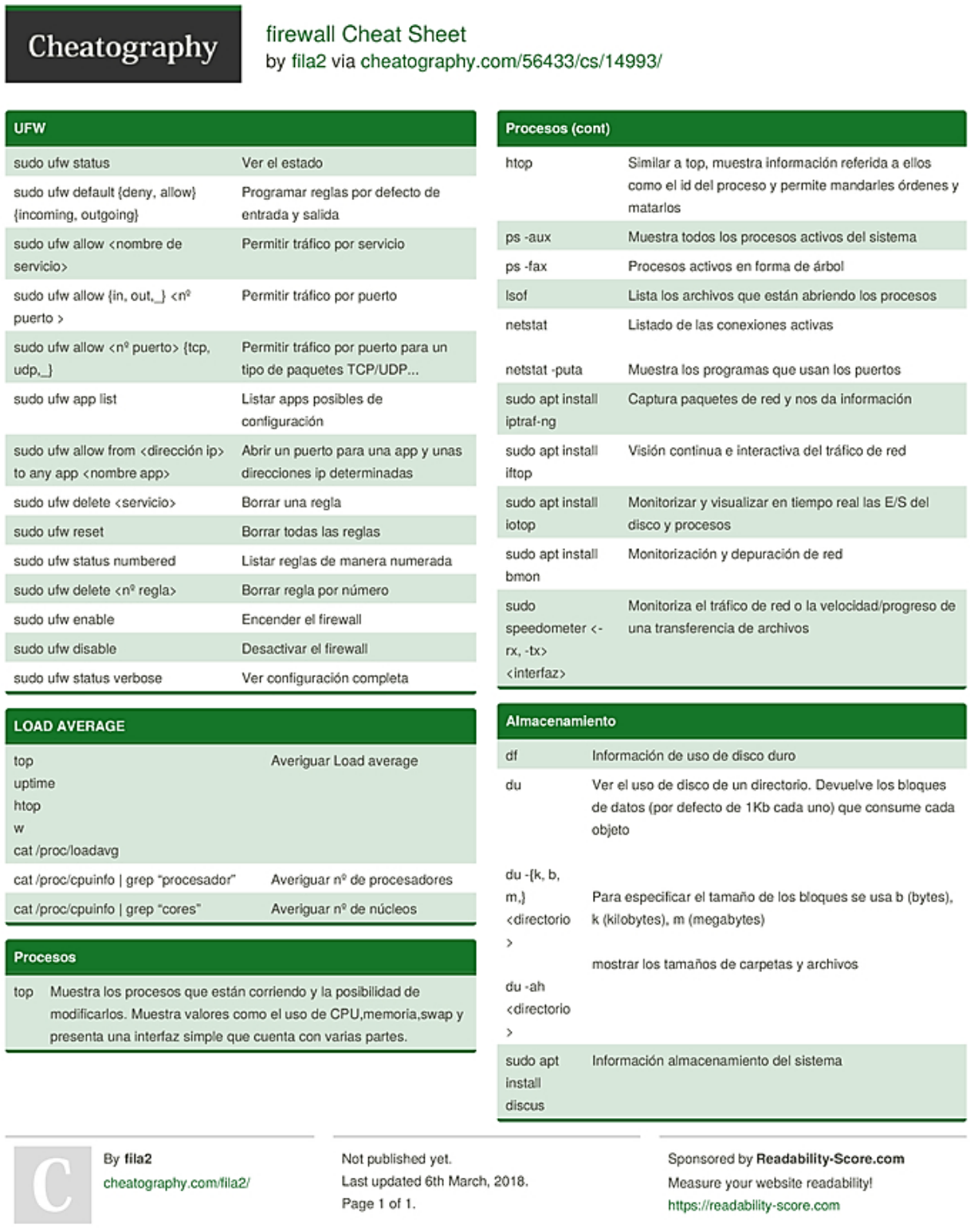
ufw *(Uncomplicated Firewall)* es un *front-end* para el *firewall* tradicional de *Linux* `iptables` que facilita enormemente su gestión. El objetivo de esta parte del laboratorio es doble:

1. Habilitar el *firewall*
2. Permitir solo aquellos puertos que vayan a tener servicios en marcha. Es importante recordar un par de cosas
   - Todos los comandos `ufw` que necesitarás están en el manual oficial: https://help.ubuntu.com/community/UFW
   - Si estás utilizando SSH para acceder a tu máquina, **PRIMERO DEBES abrir el puerto SSH ANTES de habilitar el firewall,** o te bloquearás a ti mismo fuera de la máquina y no podrás acceder al sistema con SSH. **NOTA:** Las consolas de las máquinas virtuales *VirtualBox* no usan SSH, por lo

que puedes usarlas para recuperar el acceso remoto. Si solo utilizas la consola de la máquina virtual para acceder a la máquina, puedes bloquear el puerto/servicio `ssh` por razones de seguridad.

- No olvides abrir el puerto correspondiente cada vez que instales un servicio. Por ejemplo, al instalar un servidor web, debes permitir los servicios `http` y `https` (si se usa) (equivalentes a los puertos 80 y 443)

Usa la siguiente imagen como guía para manejar `ufw`. Comprueba luego el estado del *firewall* y que los puertos se han abierto correctamente.



Cheatography

firewall Cheat Sheet
by fila2 via cheatography.com/56433/cs/14993/

UFW

sudo ufw status	Ver el estado
sudo ufw default {deny, allow} {incoming, outgoing}	Programar reglas por defecto de entrada y salida
sudo ufw allow <nombre de servicio>	Permitir tráfico por servicio
sudo ufw allow {in, out,_} <nº puerto >	Permitir tráfico por puerto
sudo ufw allow <nº puerto> {tcp, udp,_}	Permitir tráfico por puerto para un tipo de paquetes TCP/UDP...
sudo ufw app list	Listar apps posibles de configuración
sudo ufw allow from <dirección ip> to any app <nombre app>	Abrir un puerto para una app y unas direcciones ip determinadas
sudo ufw delete <servicio>	Borrar una regla
sudo ufw reset	Borrar todas las reglas
sudo ufw status numbered	Listar reglas de manera numerada
sudo ufw delete <nº regla>	Borrar regla por número
sudo ufw enable	Encender el firewall
sudo ufw disable	Desactivar el firewall
sudo ufw status verbose	Ver configuración completa

LOAD AVERAGE

top uptime htop w cat /proc/loadavg	Averiguar Load average
cat /proc/cpuinfo | grep "procesador"	Averiguar nº de procesadores
cat /proc/cpuinfo | grep "cores"	Averiguar nº de núcleos

Procesos

top	Muestra los procesos que están corriendo y la posibilidad de modificarlos. Muestra valores como el uso de CPU,memoria,swap y presenta una interfaz simple que cuenta con varias partes.

Procesos (cont)

htop	Similar a top, muestra información referida a ellos como el id del proceso y permite mandarles órdenes y matarlos
ps -aux	Muestra todos los procesos activos del sistema
ps -fax	Procesos activos en forma de árbol
lsof	Lista los archivos que están abriendo los procesos
netstat	Listado de las conexiones activas
netstat -puta	Muestra los programas que usan los puertos
sudo apt install iptraf-ng	Captura paquetes de red y nos da información
sudo apt install iftop	Visión continua e interactiva del tráfico de red
sudo apt install iotop	Monitorizar y visualizar en tiempo real las E/S del disco y procesos
sudo apt install bmon	Monitorización y depuración de red
sudo speedometer <-rx, -tx> <interfaz>	Monitoriza el tráfico de red o la velocidad/progreso de una transferencia de archivos

Almacenamiento

df	Información de uso de disco duro
du	Ver el uso de disco de un directorio. Devuelve los bloques de datos (por defecto de 1Kb cada uno) que consume cada objeto
du -{k, b, m,} <directorio >	Para especificar el tamaño de los bloques se usa b (bytes), k (kilobytes), m (megabytes)
du -ah <directorio >	mostrar los tamaños de carpetas y archivos
sudo apt install discus	Información almacenamiento del sistema

By **fila2**
cheatography.com/fila2/

Not published yet.
Last updated 6th March, 2018.
Page 1 of 1.

Sponsored by **Readability-Score.com**
Measure your website readability!
https://readability-score.com

Ejercicio L1B2_LYNIS: Evaluar la configuración de seguridad de la máquina virtual base: *Lynis*

Descripción de la actividad / Aplicación práctica

Necesitas evaluar rápidamente el nivel de seguridad de tu SO con una puntuación de 0 a 100, además de obtener consejos para mejorar su seguridad

Resultados Esperados

Esta actividad se completará cuando puedas **obtener una puntuación de *Lynis*** de tu sistema.

Otra información necesaria para su realización

NOTA: *Vagrant* y la máquina virtual preconstruida ya tienen instalada la última versión de *Lynis,* **por lo que no hace falta hacer el proceso de instalación y sólo es necesario ejecutarlo**. Si creaste la VM manualmente, debes saber que el paquete *Lynis* que viene con *Ubuntu* no es la última versión estable disponible, por lo que se deben seguir un par de pasos para usar esta última versión correctamente:

- Descarga la clave del proveedor de software *(CISofy)* para utilizar el contenido de su repositorio

```
sudo wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add -
```

- Instala el soporte para descargas seguras (HTTPS) desde repositorios `apt` (necesario para descargar contenidos de *CISofy)*.

```
sudo apt install apt-transport-https
```

- Agrega el repositorio *de Lynis* al sistema operativo

```
echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list
```

- Actualiza la base de datos de paquetes de *Ubuntu* para poder usar los paquetes recién añadidos: `sudo apt update`
- Instala el *software* (`sudo apt install lynis`) y verifica la versión (`lynis show version`) (debería ser 3.0.9 o superior)
- Evalúa el sistema operativo con *Lynis* utilizando la opción adecuada (https://cisofy.com/documentation/lynis/get-started/#first-run). Se recomienda redirigir la salida a un archivo para ver los resultados. Los resultados se ven mejor (colores) usando more sobre el archivo.

Ejercicio L1B2_NMAP: Enumeración básica con *nmap*

Descripción de la actividad / Aplicación práctica

Necesitas localizar máquinas remotas “vivas” en cualquier red

Resultados Esperados

Esta actividad se completará cuando puedas saber si una máquina remota está "viva" o no utilizando `nmap`. Puedes contestar a esta pregunta: *¿Por qué crees que `nmap` es mejor opción que ping a la hora de localizar host "vivos" y sus características?* (prueba a hacer un ping a hosts cualesquiera a ver qué ocurre)

Otra información necesaria para su realización

Ejecuta con `nmap` un escaneo ping básico sobre un host que elijas para verificar si está "vivo" (tu propia máquina host, `scanme.nmap.org`...). Puedes usar este *cheatsheet* para buscar la opción adecuada. **NOTA:** Si por alguna razón `nmap` no está ya instalado, puede instalarse con `sudo apt install nmap`

Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 1: Reconnaissance (Basic)

https://nmap.org/

GENERAL USAGE

nmap [Scan Type(s)] [Options] {target specification}

NOTES

Target specifications can be host names, IP addresses, ranges, networks, etc. (scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254)

Use these options to locate "alive machines" (sometimes only returns that, sometimes they also return some port / service information)

TARGET SPECIFICATION

-iL <inputfilename>: Input from from file a list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

RECONOISSANCE EXAMPLES

nmap -sn scanme.nmap.org

sudo nmap -PS22,80 scanme.nmap.org

sudo nmap --traceroute scanme.nmap.org

```
operario@kali:~$ nmap -sn 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:38 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00085s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

```
operario@kali:~$ sudo nmap -PS22,80 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:42 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

HOST DISCOVERY OPTIONS (WAYS TO CHECK "ALIVE" MACHINES)

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-Pn: Treat all provided hosts as online -- skip host discovery

-PO[protocol list]: IP Protocol Ping

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

Bloque 3: Operaciones básicas de seguridad adicionales

Ejercicio L1B3_PWD: Poner una contraseña adecuada

Descripción de la actividad / Aplicación práctica

Necesitas cambiar la clave de cualquier usuario por una adecuada y segura

Resultados Esperados

Esta actividad se completará cuando la contraseña elegida **sea reportada como muy segura**

Otra información necesaria para su realización

Debes cambiar la contraseña de tu usuario UO de la máquina virtual por algo que supere un nivel mínimo de seguridad, para así comprender cómo se crean contraseñas seguras. Puedes utilizar herramientas como estas para evaluar las posibles contraseñas que quieras poner:

- http://www.passwordmeter.com
- https://password.kaspersky.com

Cambia la contraseña usando `passwd`: https://www.linuxtechi.com/10-passwd-command-examples-in-linux/

Ejercicio L1B3_MALSCAN: Habilitar el *software* de escaneo de *malware* / *rootkits*

Descripción de la actividad / Aplicación práctica

Necesitas localizar *malware* o *rootkits* bajo demanda en alguno de tus archivos

Resultados Esperados

Esta actividad se completará cuando puedas ejecutar con éxito las herramientas mencionadas.

Otra información necesaria para su realización

Es importante que un sistema seguro pueda detectar y detener posibles *malware* / *rootkits* que puedan estar presentes en él. Para ello, debes instalar las siguientes herramientas

Rootkits. Chkrootkit

- Instalar: `sudo apt install chkrootkit`
- Ejecuta el programa (requiere privilegios de `root`) y redirige la salida a un archivo. Comprueba el archivo para ver si se ha detectado algo.

Rootkits. Rkhunter

- Instala la aplicación con `sudo apt install rkhunter`. La aplicación está preparada para enviar alertas por correo electrónico, pero necesitamos un servidor de correo electrónico para hacerlo. Como no instalaremos uno en nuestro laboratorio de pruebas, lo configuramos para que envíe solo correos electrónicos locales, dejando el resto de las opciones por defecto.
- Ejecuta y envía la salida a un archivo, comprobando que todo está correcto: `sudo rkhunter -c` (**NOTA:** Puede tardar tiempo en completarse)

Malware. ClamAV

- Instalar el *software*: `sudo apt install clamav`
- Realizar una actualización de las firmas del software antimalware: `sudo freshclam`
- **NOTA:** Si la actualización de las firmas se queja de que el archivo de registro está bloqueado para escritura, haz: `sudo service clamav-freshclam stop` y, a continuación, vuelve a realizar la actualización de las firmas. **Si el servidor remoto parece estar caído, omite la actualización**.
- Escanear un directorio: `sudo clamscan -r -i<DIRECTORY>`

Ejercicio L1B3_LYNISREPORT: *Informes de Lynis*

Descripción de la actividad / Aplicación práctica

Necesitas un informe de seguridad acerca del nivel de seguridad actual de tu máquina

Resultados Esperados

Esta actividad se completará cuando puedas obtener un informe HTML de *Lynis* de tu máquina virtual y puedas localizar correctamente en el informe **el nº que describe el nivel de seguridad de esta**.

Otra información necesaria para su realización

Lynis escribe sus resultados en la salida estándar utilizando colores. Sin embargo, no todos los visores pueden mostrar estos colores. Hay un truco para enviar estos resultados a HTML, preservando formatos y colores y haciéndolos mucho más fáciles de ver:

- Instala el paquete `kbtin`, que incluye la herramienta `ansi2html`.
- Ejecuta `sudo lynis audit system | ansi2html > report.html` y verifica el resultado con cualquier navegador.

Ejercicio L1B3_VIRUST: El servicio *Virustotal*

Descripción de la actividad / Aplicación práctica

Necesitas escanear URL sospechosas para ver si apuntan a una web maliciosa conocida

Resultados Esperados

Esta actividad se completará cuando puedas obtener informes de una URL o ejecutable de *Virustotal*.

Otra información necesaria para su realización

Virustotal es un servicio web (https://www.virustotal.com/gui/home/upload) que **escanea cualquier archivo** que se le cargue en busca de *malware* conocido, utilizando más de 50 motores antivirus diferentes. También **escanea URLs** para detectar la presencia de *malware* conocido en las páginas que designan (https://www.virustotal.com/gui/home/url). Se puede utilizar para

- Aumentar la certeza sobre la seguridad de un archivo o documento ejecutable desconocido que estás considerando abrir.
- Probar un archivo de tu máquina para ver si está infectado (eso puede indicar que hay una infección más grande en tu sistema).
- Aumentar la certeza de que una URL que vas a visitar no oculta potencialmente malware.

Para realizar esta actividad, debes cargar y escanear con el servicio un ejecutable que elijas. Además, también debes inspeccionar la URL que quieras.

Ejercicio L1B3_USERGSAFEB: *Google Safe Browsing*

Descripción de la actividad / Aplicación práctica

Necesitas saber si una web está identificada como maliciosa por *Google*

Resultados Esperados

Esta actividad se completará cuando puedas obtener un informe de *Google Safe Browsing* de cualquier URL que elijas.

Otra información necesaria para su realización

Google Safe Browsing escanea miles de millones de URL para localizar sitios web inseguros. Descubre miles de nuevos sitios inseguros diariamente, muchos de los cuales son sitios web legítimos que han sido pirateados. Cuando detecta sitios web inseguros, muestra advertencias en la *Búsqueda de Google* y en los navegadores web que utilizan esta tecnología. Además, puedes buscar manualmente una URL para ver si es peligroso visitar su sitio web aquí: https://transparencyreport.google.com/safe-browsing/search

⚒ Ejercicio L1B3_CVEHTTP: Comprobación de vulnerabilidades conocidas de productos mediante encabezados HTTP

🕵 Descripción de la actividad / Aplicación práctica

Necesitas saber si una página web está ejecutando productos/*frameworks* con vulnerabilidades conocidas sin usar herramientas especiales

🏅 Resultados Esperados

Esta actividad se completará cuando localices **la lista CVE de vulnerabilidades conocidas** de cualquier producto que prefieras (preferible desde encabezados HTTP, pero vale cualquier producto si no tienes suerte encontrando una página web "indiscreta").

📖 Otra información necesaria para su realización

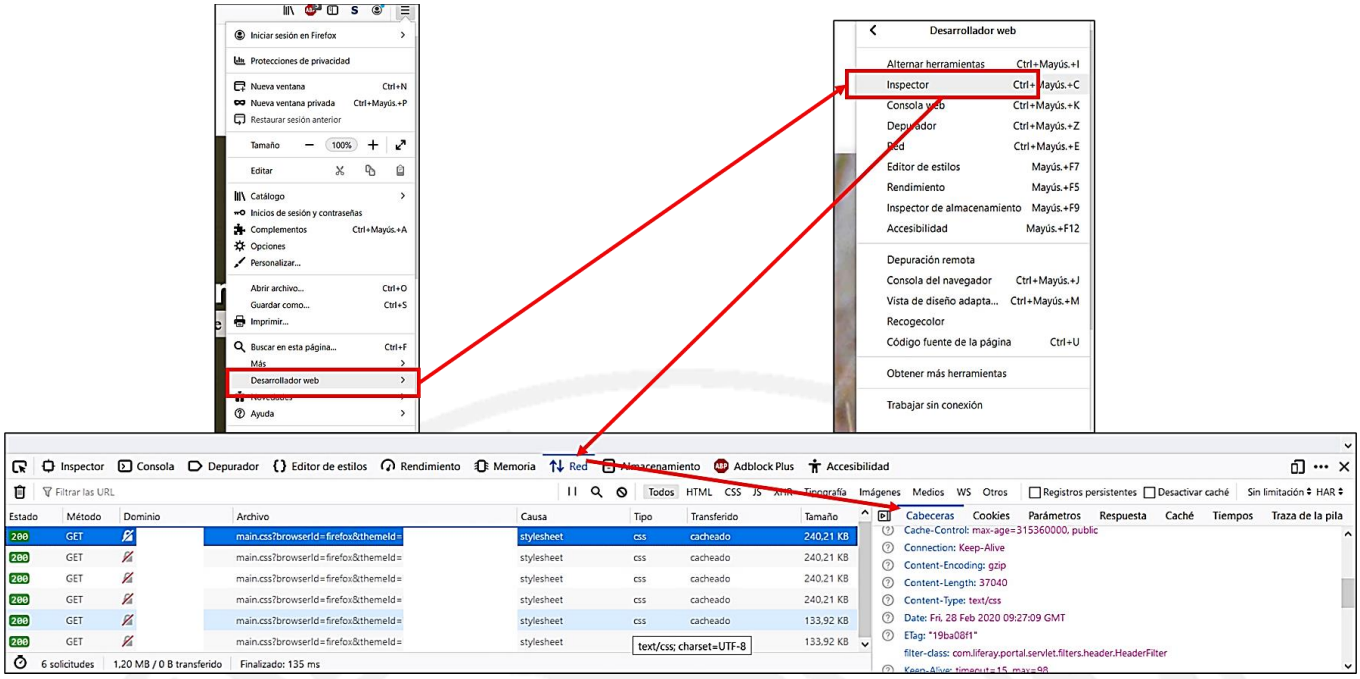
Siempre que nos conectamos a una web, aparte del contenido (HTML) también recibimos información adicional del protocolo HTTP: **las cabeceras HTTP**. Estas cabeceras contienen información del protocolo pero, a veces, también contienen información excesiva que podemos aprovechar muy fácilmente: información de **tipo de producto y versión.** Esta información puede parecer trivial, pero se puede usar para localizar las vulnerabilidades conocidas de la versiones de los productos que el servidor web usa, y que nos está proporcionando amablemente de forma gratuita 😊

🔍 ***Ni siquiera se necesita un software especial para hacer esto, ya que el propio navegador puede mostrar esta información. El siguiente diagrama muestra cómo hacer esto en Firefox, pero otros navegadores también tienen esta opción.***

Una vez hagas esto solo tienes que localizar una página web que proporcione este exceso de información al navegador (no todas lo hacen) y contrastar esa información contra bases de datos CVE como las que se muestran en teoría:

- https://cve.mitre.org/
- https://www.cvedetails.com/

1
2
3



Esto puede ser una vulnerabilidad de seguridad grave, así que no esperes que páginas web de empresas importantes te de esta información gratuita fácilmente (¡aunque nunca se sabe! 😊).

🛠 Ejercicio L1B3_NEXTDNS: Usar un DNS seguro para tu protección: *NextDNS*

Descripción de la actividad / Aplicación práctica

Puedes usar el servicio *NextDNS* de forma gratuita, incluso sin crear una cuenta, para poder navegar de manera mucho más segura de manera transparente, para entender la enorme importancia del servicio DNS en tu navegación.

Resultados Esperados

El objetivo de este ejercicio es que te des cuenta de que **sin un servidor DNS** que resuelva tus peticiones a IPs realmente **no podrías navegar**. Por ello, si ese servicio de resolución **tiene "inteligencia" que impida navegar a webs que se sepan que son perjudiciales**, podríamos lograr una web más segura (aun con un riesgo de censura). *NextDNS* es esto, pero que además te permite controlar esa "inteligencia". Una vez lo pruebes, la idea es que puedas contestar estas preguntas:

- *¿Entiendes que al usar NextDNS estás poniendo en marcha una gran cantidad de medidas de seguridad de forma transparente (sin que seas consciente de ello)?*
- *¿Qué servicios de los que proporcionan NextDNS crees que te pueden resultar más útiles?*
- *¿Has notado alguna diferencia a la hora de navegar (errores, velocidad...) o algún problema con alguna página web?*
- *A la vista de tu experiencia con el servicio, ¿Lo instalarías en tu casa? ¿Lo harías en una máquina virtual que tengas para "navegación segura" junto con otras medidas de seguridad?*

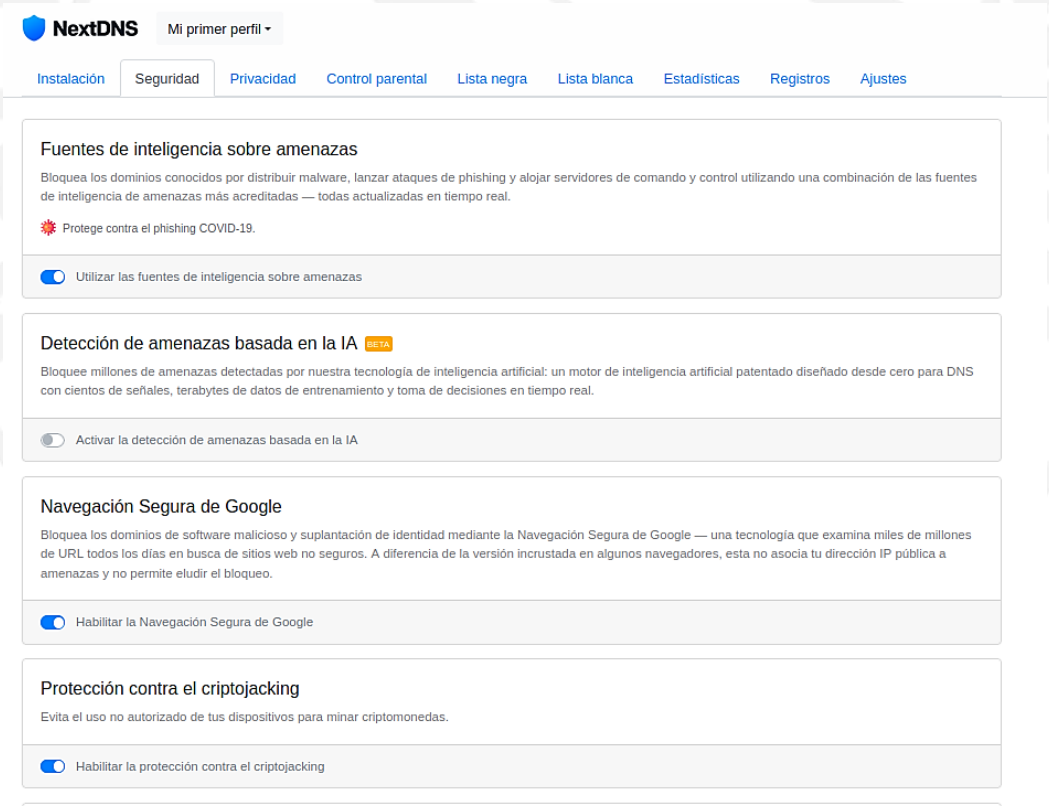
Otra información necesaria para su realización

El servicio *NextDNS* (https://nextdns.io/) realmente es una forma de librarnos de muchos problemas de una manera transparente, y que se puede usar para tener una navegación mucho menos propensa a problemas. Una vez se configure en los navegadores o máquinas, el servicio se encargará automáticamente de **bloquear cualquier tipo de acceso bien directo o indirecto** (porque otra página lo cargue) a dominios que se consideren amenazas, o que pertenezcan a empresas anunciantes, que no estén aprobadas por este servicio centralizado de DNS.

🔍 ***La ventaja de este servicio es que ni siquiera te tienes que hacer una cuenta para usarlo, y si te la haces es para guardar tu configuración particular. Tampoco hace falta instalar nada si no quieres. Si bien el servicio gratuito está limitado a 300000 peticiones al mes, después de las cuales seguirá sirviéndote páginas web pero no tendrás protección, ese volumen de peticiones es suficiente para una navegación normal de cualquier usuario de conocimientos básicos.***

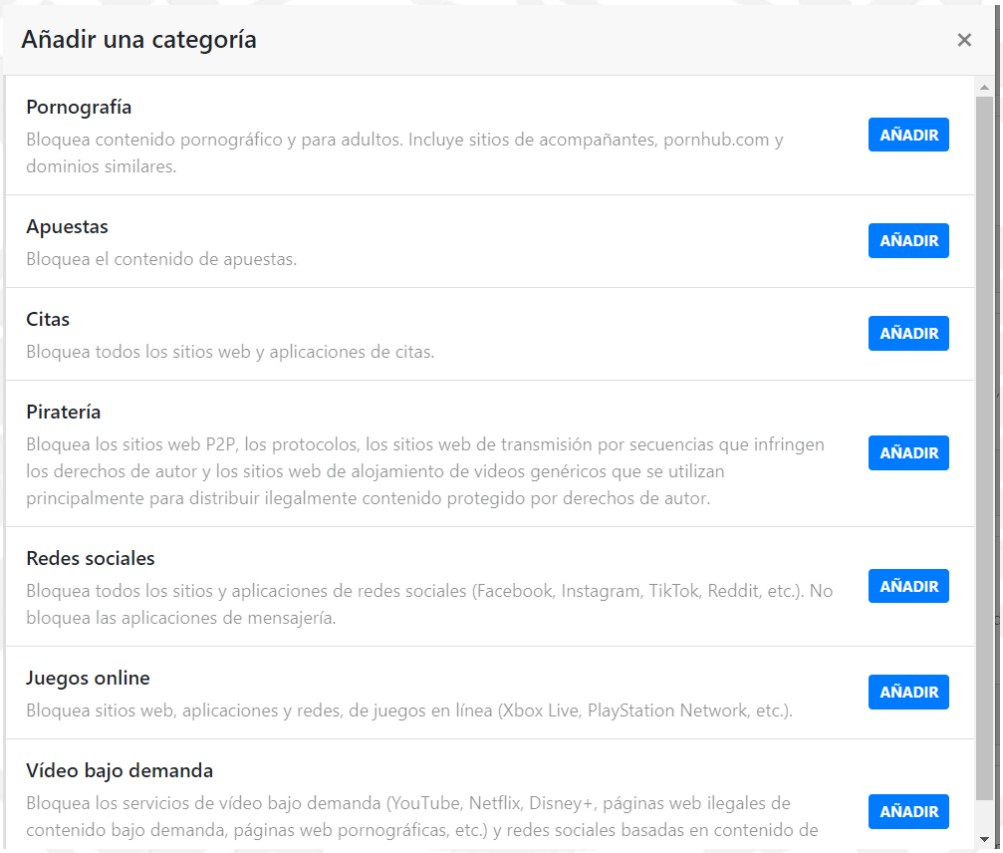
Para usar este servicio tenemos que ir a su web y usar la opción "***Try it now***" de su página principal, tras lo cual iremos a una URL que tiene este aspecto: `https://my.nextdns.io/<código de letras y nºs aleatorio>/setup`. En esa URL podremos configurar las opciones de seguridad del servicio y ver las opciones de instalación en nuestra máquina si finalmente queremos usarlas.

Como se ve, en la primera pestaña de ***Seguridad*** tenemos activas una serie de medidas por defecto, y se recomienda activarlas todas inicialmente a ver cómo se comporta con nuestra navegación habitual:

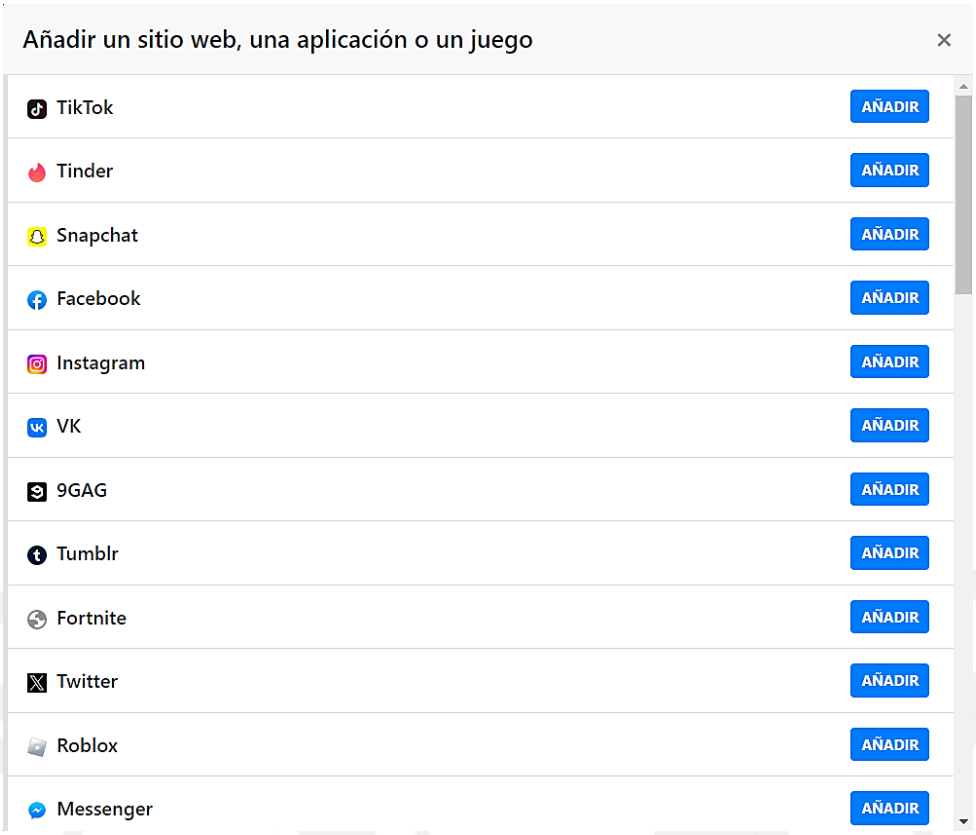


Hay un gran nº de medidas que podemos activar, por lo que se recomienda recorrer toda la sección y activar todas inicialmente. Ten en cuenta que cada medida tiene una explicación de lo que es exactamente. Aunque no la entendamos, se recomienda su activación, y sólo desactivarlas si hay algún problema en nuestro uso habitual. El ejercicio consiste en **recorrer todas las opciones** que nos da *NextDNS* y activar todas las que creamos útiles para nuestro caso de uso particular:

- La opción de **bloquear TLDs** sirve para bloquear el acceso a páginas cuyo dominio acabe en un prefijo concreto (`.es`, `.com`, etc.). Puedes encontrar una lista completa aquí: https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains.
- En el apartado de **privacidad** podemos encontrar una característica muy útil: **las listas de bloqueo**. Son básicamente listas de dominios que el servicio no resolverá por pertenecer a anuncios, páginas maliciosas o servicios intrusivos o sin interés que se han considerado perjudiciales de alguna forma. Aunque el servicio viene con una ya cargada, podemos mejorarlo usando listas que están disponibles por Internet creadas para *NextDNS*. En este enlace puedes encontrar algunas: https://github.com/hagezi/dns-blocklists.
- *NextDNS* tiene también un apartado de **control parental** donde puedes limitar la búsqueda y el uso de Internet a las horas y dominios clasificados que quieras. Si vas a usar esta opción, ten en cuenta que implica que las páginas web a las que navegues **deben estar clasificadas por NextDNS dentro de la categoría a la que pertenecen**, o especificarla (y no todas lo hacen). La **lista de categorías de sitios** usada por *NextDNS* es muy elocuente:



- El **límite de acceso a aplicaciones y juegos** consiste en seleccionar algunos de una lista que el servicio tiene y que queramos prohibir.



- **El resto del servicio** son listas de bloqueo de sitios concretos que queramos, listas para permitir sitios sin importar que encajen en alguna restricción que hayamos puesto, y estadísticas de bloqueo y uso del servicio para que lo tengamos controlado.
- En el apartado de **instalación** tenemos instrucciones para poner en marcha el servicio en cualquier sistema operativo (de PC o de móvil), navegadores concretos (si no queremos hacerlo para todo el sistema operativo) o incluso en ***routers***, pero solo modelos concretos que permitan la ejecución de los comandos que nos indican.

Ten en cuenta que **se genera una nueva configuración** (distinto bloque de nºs y letras en la URL) cada vez que entras en el servicio con el botón para probarlo que hemos visto. **Apunta cuál es tu identificador** para poder seguir configurando el servicio más tarde, y ten en cuenta que la configuración en los navegadores o SO usan ese identificador para distinguir tu configuración de la de los demás.

Si quieres empezar por algo sencillo para probar qué tal funciona, lo mejor es **configurar uno de tus navegadores** solamente con la configuración que has puesto y ver qué tal va.

Android iOS Windows macOS Linux Chrome OS **Navegadores** Enrutadores

Google Chrome

1. Ve a Ajustes.
2. En la sección Privacidad y seguridad, haz clic en Seguridad.
3. En la sección Avanzado, habilita Usar DNS seguro.
4. Selecciona Con: Personalizado, luego introduce **https://dns.nextdns.[redacted]**.

Firefox

Solo Windows, macOS y Linux

1. Abre Preferencias.
2. Desplázate hacia abajo hasta la sección Configuración de red y haz clic en Configuración.
3. Desplázate hacia abajo y marca Habilitar DNS sobre HTTPS.
4. Selecciona Personalizado, introduce **https://dns.nextdns.[redacted]7** y haz clic en Aceptar.
5. Introduce "about:config" en la barra de direcciones (y haz clic en ¡Acepto el riesgo! si te le solicita).
6. Establece network.trr.mode a **3**.

✍ Insignias y Autoevaluación

NOTA: Tienes una versión de esta tabla de insignias en formato editable disponible en el *Campus Virtual*. Puedes usar este archivo para crear un documento en el formato que desees y tomar notas extendidas de tus actividades para crear un log de lo que has hecho. Recuerda que el material que elabores se puede llevar a los exámenes de laboratorio.

Nivel de insignia	Desbloqueado cuando	¿Desbloqueado?
	Puedes desplegar máquinas virtuales en *VirtualBox*	
	Puedes actualizar un sistema *Ubuntu*	
	Puedes crear un usuario en un sistema *Ubuntu* y ponerlo en el grupo `sudo`	
	Puedes cambiar una contraseña de usuario	
	Puedes comprobar si una contraseña es segura	
	Puedes responder a esta pregunta: *¿Cuáles son las ventajas de tener una contraseña fuerte, no predeterminada y no conocida?*	
	Puedes cambiar correctamente entre los usuarios en un sistema *Ubuntu*	
	Puedes instalar un servidor *OpenSSH* operativo	
	Puedes activar el firewall `ufw` y restringir todos los puertos, excepto el `ssh`	
	Entiendes por qué `nmap` es mucha mejor forma de localizar hosts “vivos” que `ping`	
	Puedes probar si hay una conexión entre el host y la máquina virtual base operativa	
	Puedes habilitar y utilizar software de análisis de *malware* y *rootkits*	
	Puedes habilitar la actualización de firmas y ejecutar el antivirus *ClamAV*	
	Puedes habilitar la última versión de *Lynis* y evaluar la configuración de seguridad actual de tu sistema base	
	Puedes crear informes de seguridad en una máquina *Ubuntu* con *Lynis* en HTML	

	Puedes responder a esta pregunta: *¿la puntuación Lynis de la máquina mejora una vez que se instale software de detección de malware y rootkits?*	
	Debido a la anterior, conoces el procedimiento general para agregar repositorios externos de software a *Ubuntu* de proveedores externos.	
	Puedes responder a esta pregunta: *Según el informe Lynis, ¿crees que una instalación de Ubuntu actualizada base es lo suficientemente segura? ¿por qué?*	
	Puedes analizar un ejecutable con *Virustotal* e interpretar sus resultados	
	Puedes analizar una URL con *Virustotal* y *Google Safe Browsing* e interpretar sus resultados	
	Puedes comprobar las vulnerabilidades conocidas de cualquier producto inspeccionando sus CVEs. En particular, puedes hacerlo a partir de la información que un servidor web puede proporcionar sobre los productos software que usa	
	Puedes responder a la siguiente pregunta: *¿qué se debe esperar del estado general de la seguridad de una página web que proporciona tipos de productos y versiones en sus encabezados HTTP?*	
	Entiendes cómo configurar una máquina o navegador para usar *NextDNS* y todas las características de protección que proporciona	
	**Puedo hacer esto todo el día**: Puedes desplegar una máquina virtual base, evaluar su seguridad y realizar algunas operaciones iniciales relacionadas con la seguridad que te permiten comprender mejor los conceptos de teoría	