



Fuente: IA Stable Diffusion

LABORATORIO 1. CONFIGURACIÓN DEL SISTEMA

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2022 – 2023 (v3.1 "S-81 Isaac Peral")



CONTENIDO

BLOQUE 1: Puesta en marcha de la máquina virtual	3
Prerrequisitos	4
Entrar en sesión y actualizar la máquina virtual	4
Crear un usuario adecuado	4
Cambiar entre usuarios correctamente	5
Bloque 2: Operaciones básicas de Seguridad	6
Instalar un servidor <i>OpenSSH</i>	7
Habilitar el <i>firewall</i>	8
Evaluar la configuración de seguridad de la máquina virtual base: <i>Lynis</i>	8
Enumeración básica con <i>nmap</i>	9
Bloque 3: Operaciones básicas de seguridad adicionales	10
Poner una contraseña adecuada	11
Habilitar el software de escaneo de malware / <i>rootkits</i>	11
<i>Rootkits. Chkrootkit</i>	11
<i>Rootkits. Rkhunter</i>	11
<i>Malware. ClamAV</i>	11
Informes de <i>Lynis</i>	12
El servicio <i>Virustotal</i>	12
<i>Google Safe Browsing</i>	13
Comprobación de vulnerabilidades conocidas de productos mediante encabezados HTTP	13
Rastreo de rutas de paquetes	14
Ver un DNS en acción: <i>dig</i>	14
Insignias y Autoevaluación	17



AVISO

Este material forma parte de la asignatura “Seguridad de Sistemas Informáticos”, impartida en la *Escuela de Ingeniería Informática* de la *Universidad de Oviedo*. Es fruto del trabajo continuado de elaboración, soporte, mejora, actualización y revisión del siguiente equipo de profesores desde el año 2019

- Enrique Juan de Andrés Galiana
- Fernando Cano Espinosa
- Miguel Riesco Albizu
- José Manuel Redondo López
- Luís Vinuesa Martínez

Te pedimos por favor que **NO lo compartas públicamente en Internet**. No obstante, entendemos que puedas considerar este material interesante para otras personas. Por ese motivo, hemos creado una versión de este adaptada para que pueda cursarse de forma online, disponible gratuitamente para todo el mundo y que puedes encontrar en esta dirección: <https://ocw.uniovi.es/course/view.php?id=109>

A diferencia de esta versión, **la versión libre puedes promocionarla todo lo que quieras**, que para eso está 😊

GRACIAS POR TU COLABORACIÓN

BLOQUE 1: PUESTA EN MARCHA DE LA MÁQUINA VIRTUAL

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).

Entrar en sesión y actualizar la máquina virtual

Aplicación práctica: *Necesitas actualizar tu SO para prevenir vulnerabilidades*

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. **NOTA:** Esto es cierto para versiones de *Ubuntu* de la 20.04 en adelante. Si usaste la máquina *.ova* o la *Vagrant*, `snap` no viene instalado (es un *Ubuntu* 18.04), por lo que **esto no hace falta hacerlo**.

```
sudo snap refresh
```

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?*

Crear un usuario adecuado

NOTA: si has escogido *Vagrant* como forma de construir tu máquina virtual automáticamente, y has modificado tu nombre de usuario en el fichero como se indicó, este ejercicio ya estará hecho y esto solo describe el



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

Aplicación práctica: *Necesitas crear una cuenta de usuario para un empleado nuevo*

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.
- Utilizar el comando `usermod` para agregar el usuario al grupo `sudo`: `sudo usermod -aG sudo <uoxxxxxx>`. De forma predeterminada en *Ubuntu*, los miembros del grupo `sudo` tienen privilegios `sudo`.

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

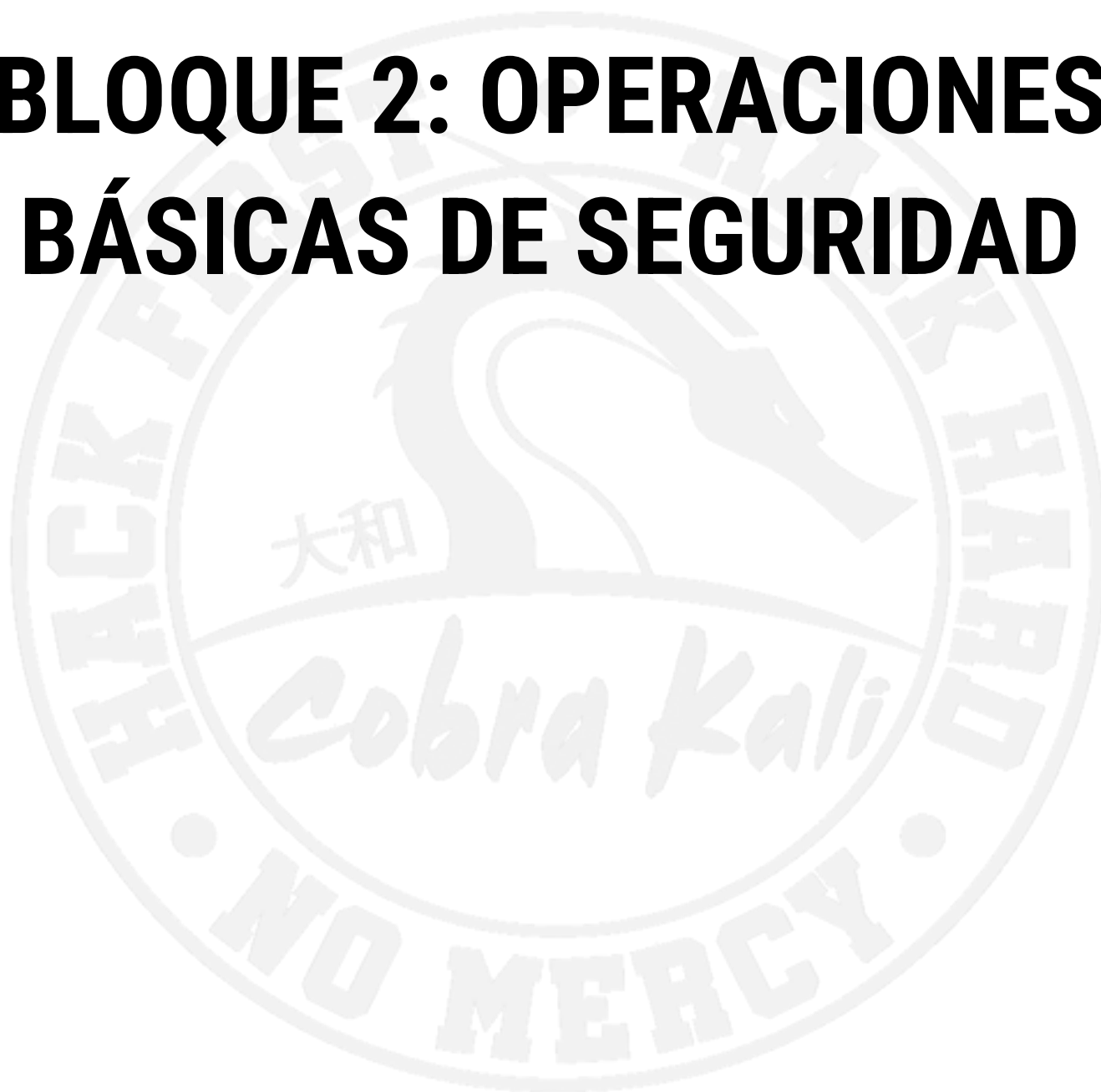
Cambiar entre usuarios correctamente

Aplicación práctica: *Tienes que asumir varias identidades de Usuario en la misma sesión de trabajo para hacer ciertas operaciones*

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. **NOTA:** Las máquinas virtuales implementadas con *Vagrant* ya tienen dos usuarios `sudoer`, `vagrant` y el que se especificó en el archivo `username.txt`.

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

BLOQUE 2: OPERACIONES BÁSICAS DE SEGURIDAD



Instalar un servidor OpenSSH

Aplicación práctica: Necesitas un acceso remoto seguro a tu máquina

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 con los comandos para hacer operaciones típicas:

CHEAT SHEET

SSH - common commands and secure config

BlowStack

SSH connections

- connects to a server (default port 22)
`$ ssh user@server`
- uses a specific port declared in `sshd_config`
`$ ssh user@server -p other_port`
- runs a script on a remote server
`$ ssh user@server script_to_run`
- compresses and downloads from a remote server
`$ ssh user@server "tar cvzf - ~/source" > output.tgz`
- specifies other ssh key for connection
`$ ssh -i ~/.ssh/specific_ssh_fkey`

SSH keys

- generates a new ssh key
`$ ssh-keygen -t rsa -b 4096`
- sends the key to the server
`$ ssh-copy-id user@server`
- converts `ids_rsa` into `ppk`
`$ puttygen current_key -o keyname.ppk`

SSH config

- opens config file (usual location)
`$ sudo nano /etc/ssh/sshd_config`
- changes default SSH port (22)
Port 9809
- disables root login
PermitRootLogin no
- restricts access to specific users
AllowUsers user1, user2
- enables login through ssh key
PubkeyAuthentication yes
- disables login through password
PasswordAuthentication no
- disables usage of files `.rhosts` and `.shosts`
IgnoreRhosts yes
- disables a less secure type of login
HostbasedAuthentication no
- number of unauthenticated connections before dropping
MaxStartups 10:30:100
- no. of failed tries before the servers stops accepting new tries
MaxAuthTries 3
- max current ssh sessions
MaxSessions 1
- disables interactive password authentication
ChallengeResponseAuthentication no
- no empty password allowed
PermitEmptyPasswords no
- disables Rhost authentication
RhostsAuthentication no
- disables port forwarding (blocks i.e MySQL Workbench)
AllowTcpForwarding no
X11Forwarding no
- prints much more info about SSH connections
LogLevel VERBOSE

SSH service

- starts ssh service
`$ (sudo) service ssh start`
- checks ssh service status
`$ (sudo) service ssh status`
- stops ssh service
`$ (sudo) service ssh stop`
- restarts ssh service
`$ (sudo) service ssh restart`

SCP (Secure Copy)

- copies a file from a remote server to a local machine
`$ scp user@server:/directory/file.ext local_destination/`
- copies a file between two servers
`$ scp user@server:/dir/file.ext user@server:/dir`
- copies a file from a local machine to a remote server
`$ scp local_destination/file.ext user@server:/directory`
- uses a specific port declared for SSH in `sshd_config`
`$ scp -P port`
- copies recursive a whole folder
`$ scp -r user@server:/directory local_destination/`
- copies all files from a folder
`$ scp user@server:/directory/* local_destination/`
- copies all files from a server folder to the current folder
`$ scp user@server:/directory/* .`
- compresses data on network using gzip
`$ scp -C`
- prints verbose info about the current transfer
`$ scp -v`

Full articles about cyber security at
<https://blowstack.com/blog/cyber-security>

Author: Piotr Golon, piotr.golon@blowstack.com, <https://blowstack.com>

Amazing ops

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

Habilitar el firewall

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

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)

Por lo tanto, se debe seguir el siguiente procedimiento:

- Escribir primero: `sudo ufw allow ssh`
- Y luego: `sudo ufw enable`
- Comprobar que los puertos abiertos son correctos con `sudo ufw status`

Resultados Esperados: Esta actividad se completará cuando el firewall informe de que está activo y se permita el puerto SSH.

Evaluar la configuración de seguridad de la máquina virtual base: Lynis

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

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 3.0.6 o superior)
- Evalúa el sistema operativo con *Lynis* utilizando la opción adecuada. Se recomienda redirigir la salida a un archivo para ver los resultados. Los resultados se ven mejor (colores) usando `more` sobre el archivo.

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

Enumeración básica con *nmap*

Aplicación práctica: Necesitas localizar máquinas remotas "vivas" en cualquier red

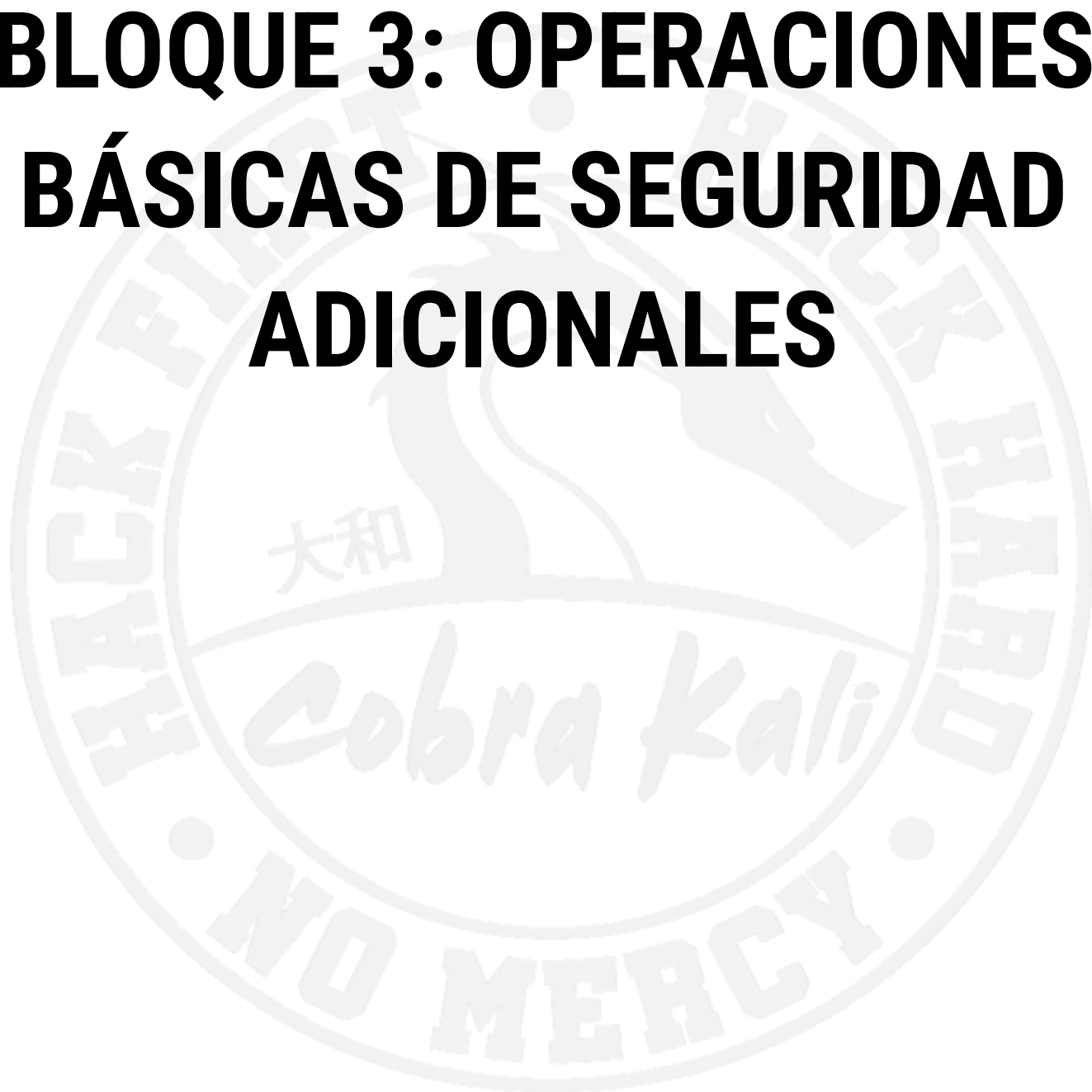
Ejecuta con `nmap` un escaneo ping básico sobre un host que elijas para verificar si está "vivo" (tu propia máquina host, `scanme.nmap.org`...). Puedes usar este *cheatsheet* para buscar la opción adecuada. **NOTA:** Si por alguna razón `nmap` no está ya instalado, puede instalarse con `sudo apt install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

Ahora haz un `ping` y el mismo escaneo `nmap` para www.asturias.es y mira las diferencias. ¿Por qué crees que está pasando esto?

Resultados Esperados: Esta actividad se completará cuando puedas saber si una máquina remota está "viva" o no utilizando `nmap`

BLOQUE 3: OPERACIONES BÁSICAS DE SEGURIDAD ADICIONALES



Poner una contraseña adecuada

Aplicación práctica: Necesitas cambiar la clave de cualquier Usuario por una adecuada y segura

Asegúrate de que tu contraseña de usuario es segura. 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/>

Resultados Esperados: Esta actividad se completará cuando la contraseña elegida sea reportada como muy segura.

Habilitar el software de escaneo de malware / rootkits

Aplicación práctica: Necesitas localizar malware o rootkits bajo demanda en alguno de tus archivos

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>`

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

Informes de Lynis

Aplicación práctica: Necesitas un informe de seguridad acerca del nivel de seguridad actual de tu máquina

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.

Resultados Esperados: Esta actividad se completará cuando puedas obtener un informe HTML de Lynis de tu máquina virtual.

El servicio Virustotal

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

Virustotal es un servicio en línea (<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.

Resultados Esperados: Esta actividad se completará cuando puedas obtener informes de una URL o ejecutable de Virustotal.

Google Safe Browsing

Aplicación práctica: *Necesitas saber si una web está identificada como maliciosa*

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>

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

Comprobación de vulnerabilidades conocidas de productos mediante encabezados HTTP

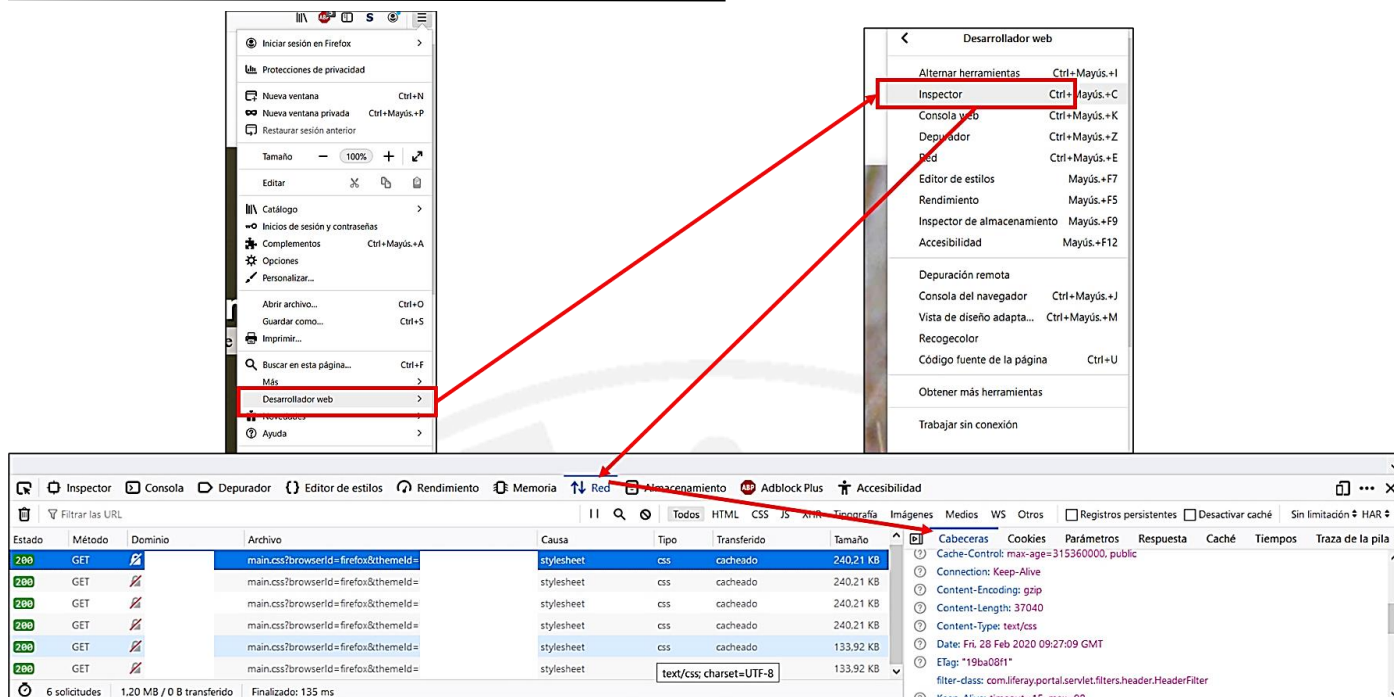
Aplicación práctica: *Necesitas saber si una página web está ejecutando productos/frameworks con vulnerabilidades conocidas*

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/>



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! 😊).

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").

Rastreo de rutas de paquetes

Aplicación práctica: Necesitas saber las rutas que siguen los paquetes que mandas por la red

tcptraceroute es una herramienta que te muestra la ruta seguida por los paquetes de una conexión (si la red proporciona esta información, si no, los "saltos" del paquete se mostrarán como *). Instala esta herramienta (`sudo apt install tcptraceroute`) y comprueba cómo viajan los paquetes a través de la red para llegar a cualquier destino que elijas. Para completar esta actividad debes identificar qué partes pertenecen a tu casa o laboratorio y qué partes están en una red externa. Esto te ayudará a comprender mejor cómo se realizan las conexiones de red.

Resultados Esperados: Esta actividad se completará cuando se pueda ver la ruta del paquete de cualquier solicitud (si la red bloquea esta información, se considerará completa de todos modos)

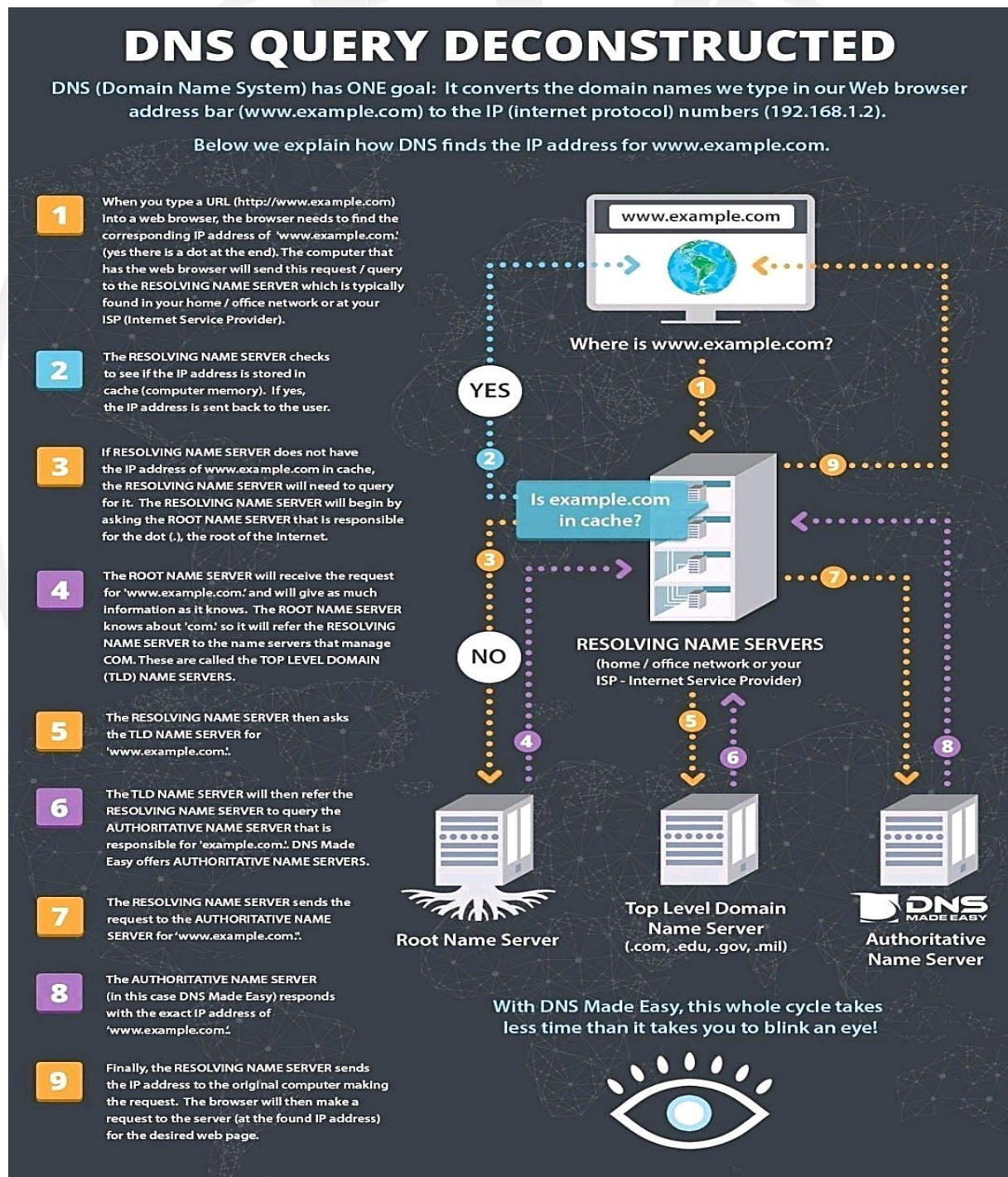
Ver un DNS en acción: dig

Aplicación práctica: Puedes preguntarle a tu servidor DNS cierta información de cualquier nombre de dominio remoto

El comando **dig** se puede usar para consultar a los servidores DNS, obtener información diversa e inspeccionar cómo funciona el sistema DNS, ilustrando el contenido de teoría. Usando este tutorial: <https://www.hostinger.es/tutoriales/comando-dig-linux/>, usa la herramienta de **dig** para realizar estas tres operaciones:

1. Ver la IP correspondiente a un nombre DNS
2. Ver el nombre DNS correspondiente a una IP (**búsqueda inversa**)
3. Hacer un seguimiento de los diferentes servidores DNS que participan en una resolución de nombres

Aunque ya vimos cómo funcionaba el DNS en los temas de teoría, esta imagen puede refrescarte ese conocimiento y ayudarte a entender mejor los resultados de **dig**.



Fuente: <https://www.pinterest.com/pin/465700417690926442/>



NOTA: Si la ejecución de `dig +trace` no muestra información adicional, intenta cambiar la IP del servidor DNS en `/etc/resolv.conf` a `8.8.8.8`.

Resultados Esperados: Esta actividad se completará cuando puedas adivinar las opciones de `dig` que muestran los tres tipos de información mencionados.





















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 <i>VirtualBox</i>	
	Puedes actualizar un sistema <i>Ubuntu</i>	
	Puedes crear un usuario en un sistema <i>Ubuntu</i> y ponerlo en el grupo sudo	
	Puedes cambiar una contraseña de usuario	
	Puedes comprobar si una contraseña es segura	
	Puedes responder a esta pregunta: <i>¿Cuáles son las ventajas de tener una contraseña fuerte, no predeterminada y no conocida?</i>	
	Puedes cambiar correctamente entre los usuarios en un sistema <i>Ubuntu</i>	
	Puedes instalar un servidor <i>OpenSSH</i> 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 rastrear la ruta de los paquetes enviados a cualquier sistema remoto, e identificar si los nodos por los que viajan están en la red de tu casa o en otras redes (si la red lo permite)	
	Puedes probar si hay una conexión entre el host y la máquina virtual base operativa	
	Puedes habilitar y utilizar software de análisis de <i>malware</i> y <i>rootkits</i>	
	Puedes habilitar la actualización de firmas y ejecutar el antivirus <i>ClamAV</i>	
	Puedes habilitar la última versión de <i>Lynis</i> y evaluar la configuración de seguridad actual de tu sistema base	
	Puedes crear informes de seguridad en una máquina <i>Ubuntu</i> con <i>Lynis</i> en HTML	



	Puedes responder a esta pregunta: <i>¿la puntuación Lynis de la máquina mejora una vez que se instale software de detección de malware y rootkits?</i>	
	Debido a la anterior, conoces el procedimiento general para agregar repositorios externos de software a Ubuntu de proveedores externos.	
	Puedes responder a esta pregunta: <i>Según el informe Lynis, ¿crees que una instalación de Ubuntu actualizada base es lo suficientemente segura? ¿por qué?</i>	
	Puedes realizar un escaneo con ping a un servidor remoto	
	Puedes analizar un ejecutable con <i>Virustotal</i> e interpretar sus resultados	
	Puedes analizar una URL con <i>Virustotal</i> y <i>Google Safe Browsing</i> 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: <i>¿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?</i>	
	Puede utilizar dig para ver las conversiones de IP <-> DNS y para realizar un seguimiento de la jerarquía DNS de los servidores DNS que se utilizan para resolver un nombre.	
	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	