**Hacking ético y ciberseguridad**

**Instalar VMware y Kali Linux**

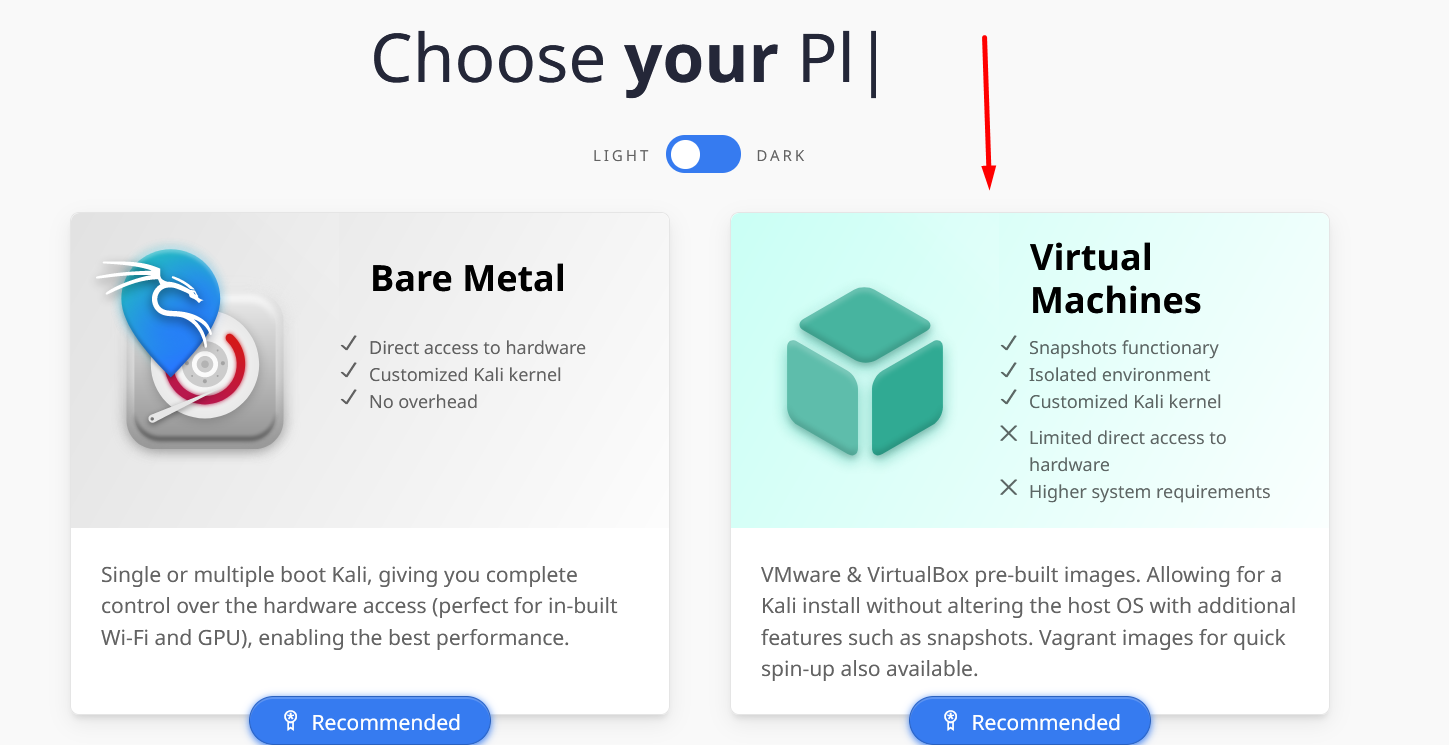
Lo primero que debemos hacer es instalar VMware o VirtualBox

Hay una opción de VMware que es gratuita, yo estoy usando la de pago:

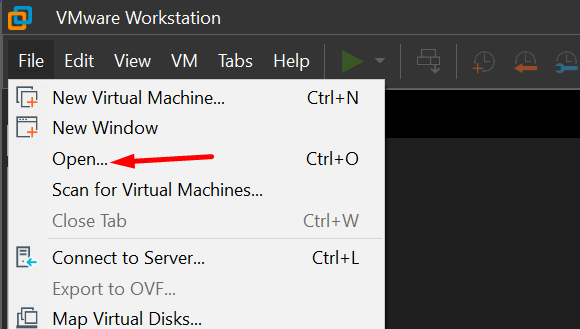
<https://www.vmware.com/es/products/workstation-player/workstation-player-evaluation.html>

Una vez instalado, descargamos el Kali Linux:

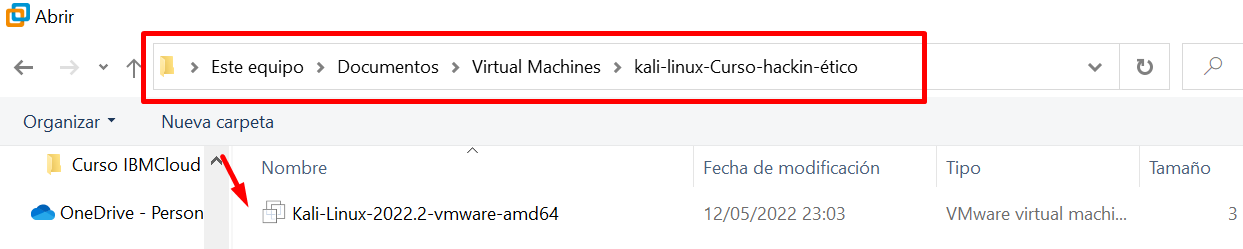
<https://www.kali.org/get-kali/#kali-virtual-machines>



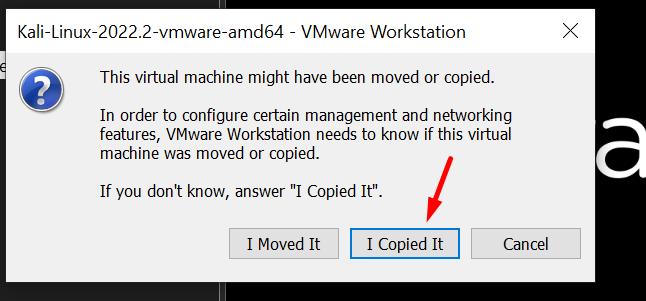
Extraemos el archivo comprimido y procedemos a montar la máquina virtual



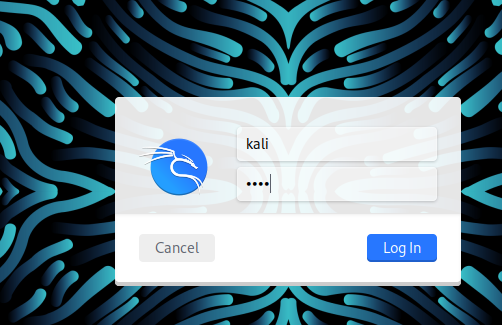
Y seleccionamos la máquina virtual



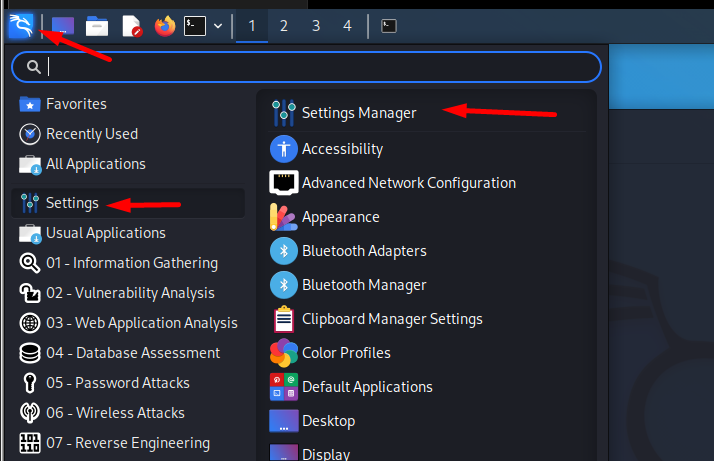
La ejecutamos y pinchamos en la he copiado

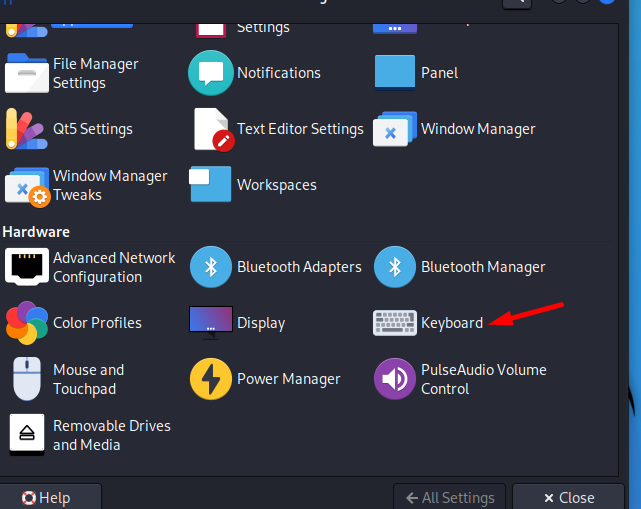


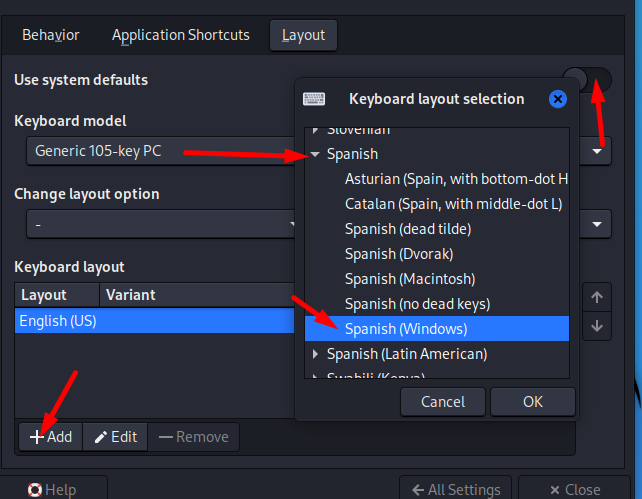
Nos logearmos con el usuario y contraseña por defecto kali



Lo siguiente será cambiar la distribución de teclado a español ya que por defecto viene en ingles







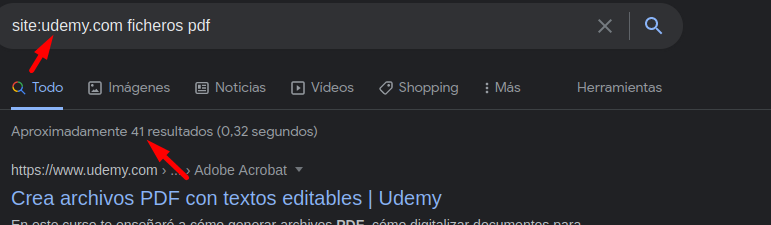
Importante borrar el idioma inglés, después apagar la máquina y aumentar los GB de RAM a 4

**Hacking con buscadores**

Para ello debemos abrir el navegador, esté nos ofrece unas cadenas de texto con la que poder filtrar y así poder encontrar información interesante, algunos de los comandos son:

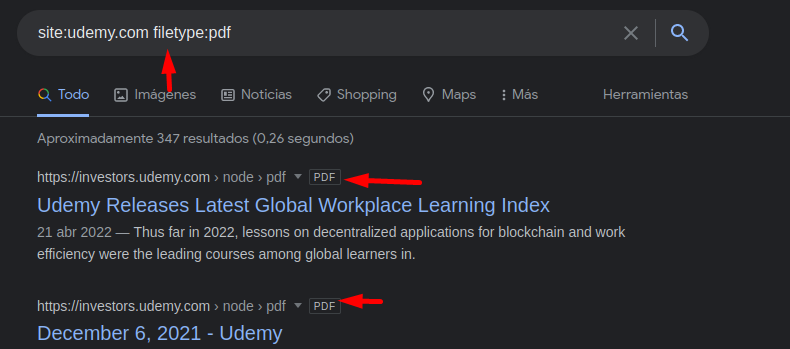
Para filtrar por página

site:udemy.com ficheros pdf



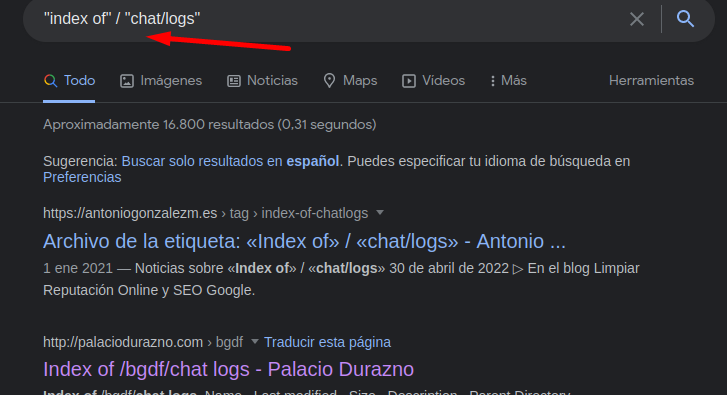
Para filtrar por el tipo de ficheros

site:udemy.com filetype:pdf



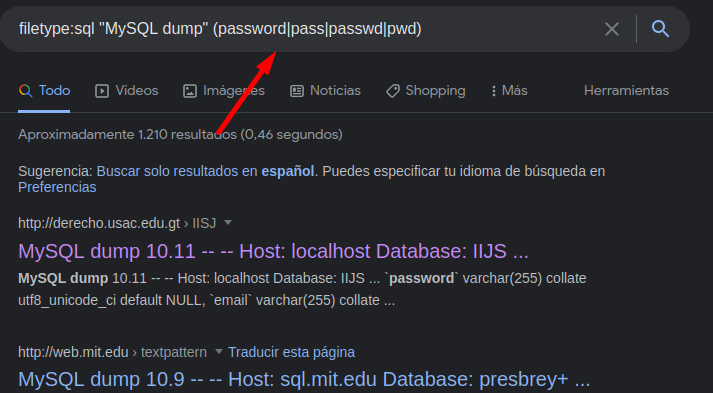
Si usamos comillas nos mostrarán resultados que coincidan exactamente con las cadenas de texto que le hemos pasado

"index of" / "chat/logs"



Con los paréntesis podemos escribir las palabras que queremos que se encuentren dentro de la página web o el fichero

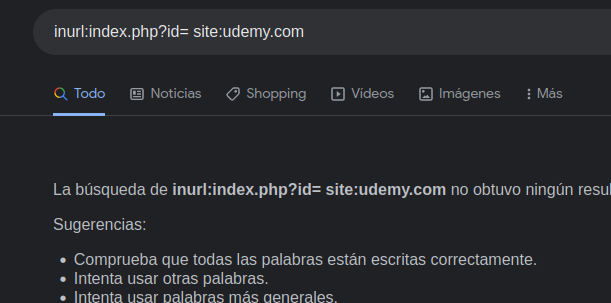
filetype:sql "MySQL dump" (password|pass|passwd|pwd)



Con inurl podemos buscar que es lo que queremos que aparezca en la url de algún sitio web con ?id= le estamos indicando que tenga el parámetro id=

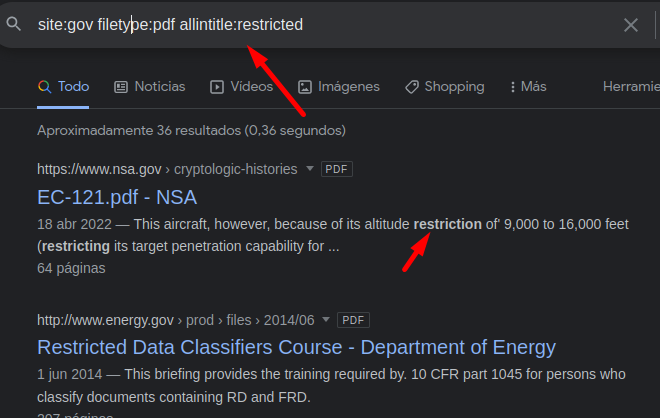
inurl:index.php?id= site:udemy.com

En este caso Udemy esta bien protegido ante esto



Con allintitle podemos decir el titulo que queremos que tenga

site:gov filetype:pdf allintitle:restricted



**Más comandos booleanos en un documento en la carpeta**

Si buscamos en google: Google hacking database y accedemos a la primera página

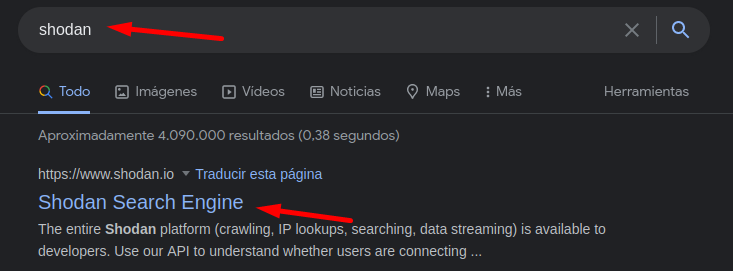
<https://www.exploit-db.com/google-hacking-database>

Nos llevará a una página web donde la gente sube comandos que podemos utilizar para la búsqueda de información de alguna página



**Shodan**

Para acceder a este navegador buscamos shodan en internet



Para usar este navegador debemos registrarnos y logearnos

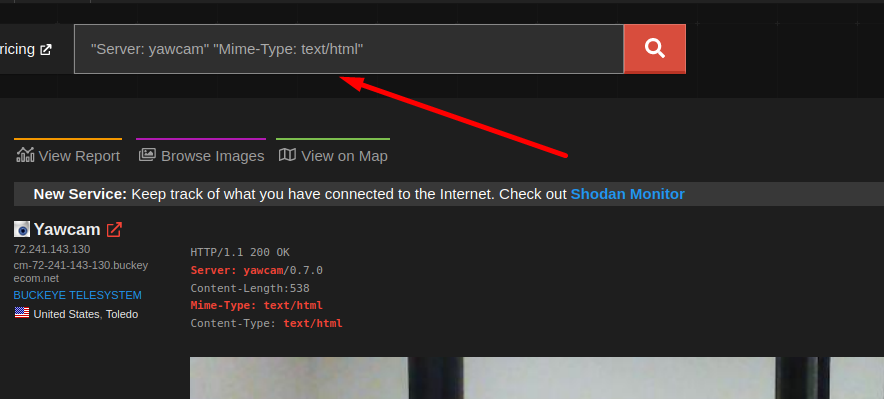
Una vez hecho esto podemos utilizar shodan, shodan es un navegador más potente que google para recopilar información

En la misma carpeta hay un documento con comandos

Repositorios con consultas:

<https://github.com/jakejarvis/awesome-shodan-queries>

Con el siguiente comando podemos acceder a webcams (Está en el repositorio)

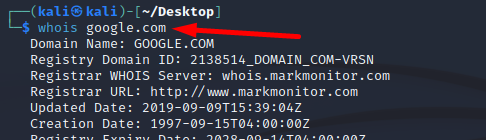


**Censys**

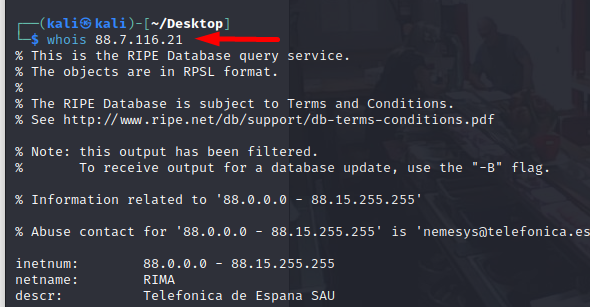
Otra aplicación web como shodan también debemos registrarnos

**Whois**

Desde el terminal usando el comando whois + el nombre de una página web podemos obtener información



También puede hacerse a través de una ip

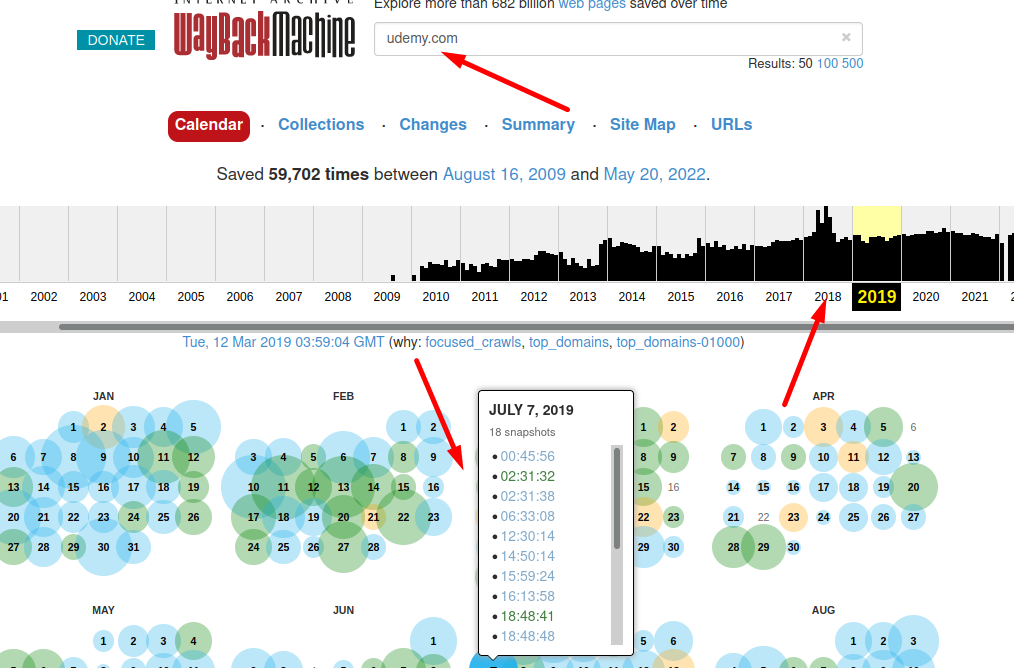


Archive

Se utiliza para recuperar información histórica que ya o se encuentra en internet,

Lo he hace está web ews que va creando spanshots de internet y así nos permite ver la información de años atrás

Enlace: <http://archive.org/>



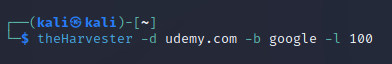
Podemos buscar cosas de GitHub borradas, twists, etc.

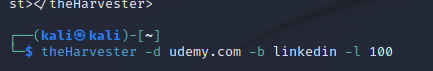
**THeHarvester**

Es otra herramienta de búsqueda, se utiliza a través de la terminal, viene ya instalada en Kali Linux

Algunos ejemplos





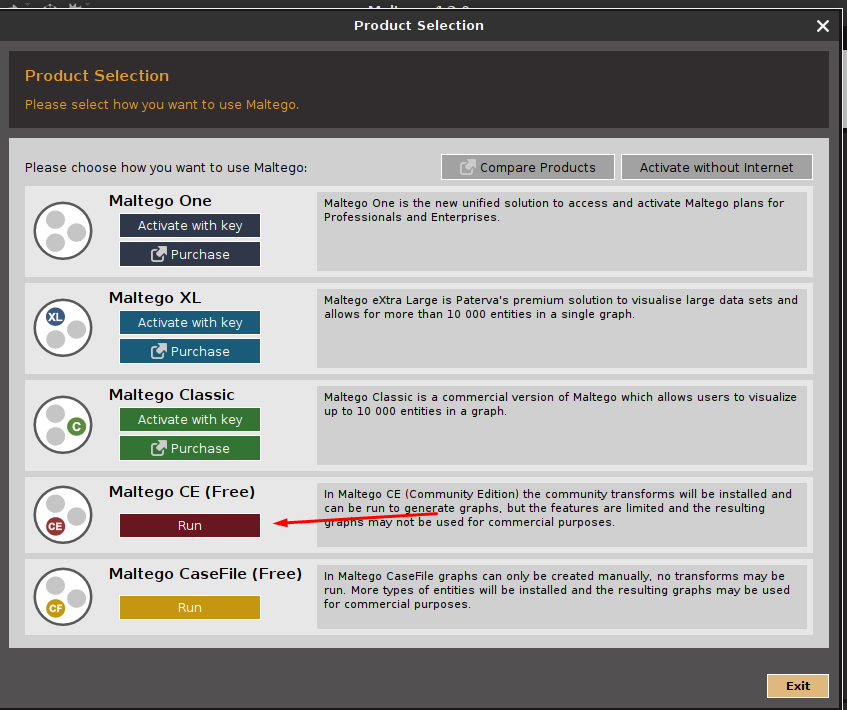


**Maltego**

Para instala primero

sudo apt update

sudo apt install maltego

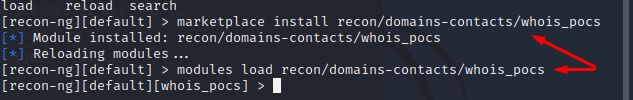


Para poder usar maltego hay que crear una cuenta gratuita

**Recon-ng**

Otra herramienta para recopilar la información, herramienta basada en interfaz de comando

Instalar y cargar módulos



**Herramientas de recopilación semi-pasiva de información**

FOCA: Instalar a través de GitHub

CentralOps: Acceder mediante el navegador

DNSdumpster: Acceder mediante el navegador

Wireshark

TCPdump

**Herramientas de recopilación activa de información**

Nmap

Amap

**Herramientas de análisis de vulnerabilidades**

Nessus

Acunetix

Qualys

AppScan

Nikto

WebApp360

ParosPro

**Herramientas de borrado de evidencias**

Linux

shred

srm

Windows

Meterpreter (el módulo sdel)

**Archivos más relevantes para eliminar**

Windows

Poster Forensics SANS: <https://www.sans.org/posters/windows-forensic-analysis/>

Linux

/var/log/messages: mensajes globales del sistema operativo.

/var/log/secure: información de autenticación y autorización.

/var/log/mail.log: información del servidor de correo del sistema.

/var/log/cron: información sobre cuando el demonio cron empieza una tarea.

/var/log/boot.log: información de cuando el sistema arranca.

/var/log/btmp: logins fallidos (lastb)

/var/log/wtmp: logins y logouts (last)

/var/log/lastlog: logins en el sistema (lastlog)

/var/run/utmp: usuarios en el sistema (who/w)

/var/log/dmesg: logs del kernel (dmesg)

Comandos de shell:

~/.bash\_history

~/.sh\_history

~/.history

Comando less:

~/.lesshst

Clientes de FTP:

~/.lftp/rl\_history y cwd\_history

~/.ncftp/history

Equipos a los que se ha conectado con SSH:

~/.ssh/known\_hosts

Logs del servidor de aplicación

apache/logs/

etc/httpd/logs/

var/www/logs/

var/log/

usr/local/apache/logs/

var/log/apache/

var/log/apache2/