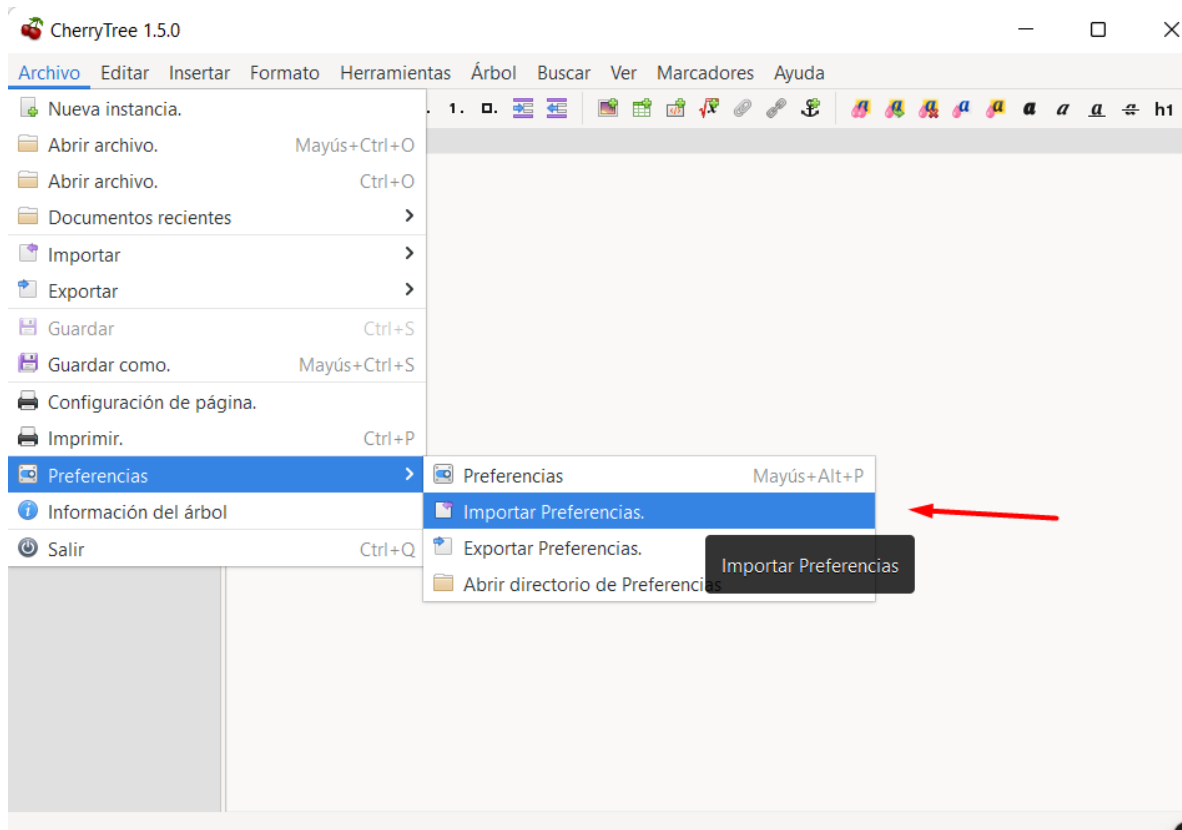




# CHERRY TREE

CherryTree es una aplicación de toma de notas jerárquica que permite organizar información en nodos y subnodos, con soporte para texto enriquecido, código, búsqueda avanzada y exportación, ideal para documentar y centralizar apuntes o procedimientos.

## 1. Instalarlo y configurarlo





## Personalizar consola Kali

```
File Actions Edit View Help
(kali@kali)-[~]
$ echo $$
4116
```

```
(kali@kali)-[~]
$ cd /proc
```

```
kali@kali: /proc/4116
File Actions Edit View Help
(kali@kali)-[/proc]
$ cd /proc/4116

(kali@kali)-[/proc/4116]
$ ls
arch_status      fd               net              setgroups
attr             fdinfo           ns               smaps
autogroup        gid_map          numa_maps        smaps_rollup
auxv             io              oom_adj          stack
cgroup          ksm_merging_pages oom_score        stat
clear_refs      ksm_stat         oom_score_adj    statm
cmdline         limits           pagemap          status
comm            loginuid         patch_state      syscall
coredump_filter map_files        personality       task
cpu_resctrl_groups maps             projid_map       timens_offsets
cpuset          mem              root             timers
cwd             mountinfo        sched            timerslack_ns
environ         mounts           schedstat        uid_map
exe             mountstats       sessionid        wchan
```



```
(kali㉿kali)-[/proc/4116]  
$ ls -l exe  
lrwxrwxrwx 1 kali kali 0 Aug 12 09:39 exe → /usr/bin/zsh
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ ls -l /proc/$$/exe  
lrwxrwxrwx 1 kali kali 0 Aug 12 09:36 /proc/2335/ex  
e → /usr/bin/zsh  
(kali㉿kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ sh  
$  
$  
$  
$ ls -l /proc/$$/exe  
lrwxrwxrwx 1 kali kali 0 Aug 12 09:39 /proc/3652/exe → /usr/bin/dash  
$
```



Para facilitar la gestión de la configuración de zsh, instalamos ohmyzsh:  
<https://github.com/ohmyzsh/ohmyzsh/wiki>

```
sh -c "$(curl -fsSL https://raw.githubusercontent.com/ohmyzsh/ohmyzsh/master/tools/install.sh)"
```

```
kali@kali:~  
File Actions Edit View Help  
From https://github.com/ohmyzsh/ohmyzsh  
* [new branch]      master    -> origin/master  
branch 'master' set up to track 'origin/master'.  
Already on 'master'  
/home/kali  
  
Looking for an existing zsh config...  
Found /home/kali/.zshrc. Backing up to /home/kali/.zshrc.pre-oh-my-zsh  
Using the Oh My Zsh template file and adding it to /home/kali/.zshrc.  
  
oh my zsh ....is now installed!  
  
Before you scream Oh My Zsh! look over the `zshrc` file to select plugins, themes, and options.  
• Follow us on X: https://x.com/ohmyzsh  
• Join our Discord community: https://discord.gg/ohmyzsh  
• Get stickers, t-shirts, coffee mugs and more: https://shop.planetargon.com/collections/oh-my-zsh  
→ ~ █
```

Instalamos el tema powerlevel10k: <https://github.com/romkatv/powerlevel10k>

## Clonar

```
git clone --depth=1 https://github.com/romkatv/powerlevel10k.git ${ZSH_CUSTOM:-$HOME/.oh-my-zsh/custom}/themes/powerlevel10k
```



```
kali@kali:~  
File Actions Edit View Help  
→ ~ git clone --depth=1 https://github.com/romkatv/powerlevel10k.git ${ZSH_CUSTOM:-$HOME/.oh-my-zsh/custom}/themes/powerlevel10k  
Cloning into '/home/kali/.oh-my-zsh/custom/themes/powerlevel10k' ...  
remote: Enumerating objects: 92, done.  
remote: Counting objects: 100% (92/92), done.  
remote: Compressing objects: 100% (75/75), done.  
remote: Total 92 (delta 18), reused 63 (delta 13), pack-reused 0 (from 0)  
Receiving objects: 100% (92/92), 349.80 KiB | 1.05 MiB/s, done.  
Resolving deltas: 100% (18/18), done.  
→ ~
```

```
kali@kali:~  
File Actions Edit View Help  
→ ~ git clone --depth=1 https://github.com/romkatv/powerlevel10k.git ${ZSH_CUSTOM:-$HOME/.oh-my-zsh/custom}/themes/powerlevel10k  
Cloning into '/home/kali/.oh-my-zsh/custom/themes/powerlevel10k' ...  
remote: Enumerating objects: 92, done.  
remote: Counting objects: 100% (92/92), done.  
remote: Compressing objects: 100% (75/75), done.  
remote: Total 92 (delta 18), reused 63 (delta 13), pack-reused 0 (from 0)  
Receiving objects: 100% (92/92), 349.80 KiB | 1.05 MiB/s, done.  
Resolving deltas: 100% (18/18), done.  
→ ~  
→ ~  
→ ~  
→ ~ ls .zshrc  
.zshrc  
→ ~
```

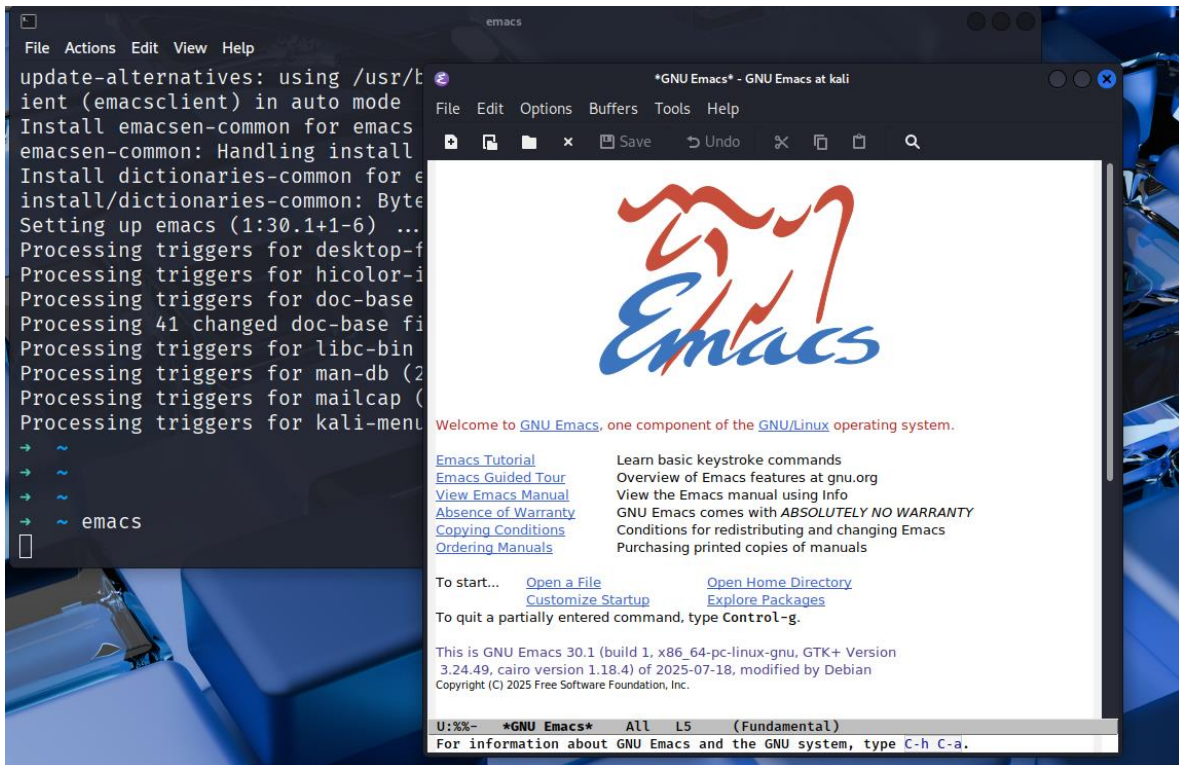
Hacemos un update para instalar emacs



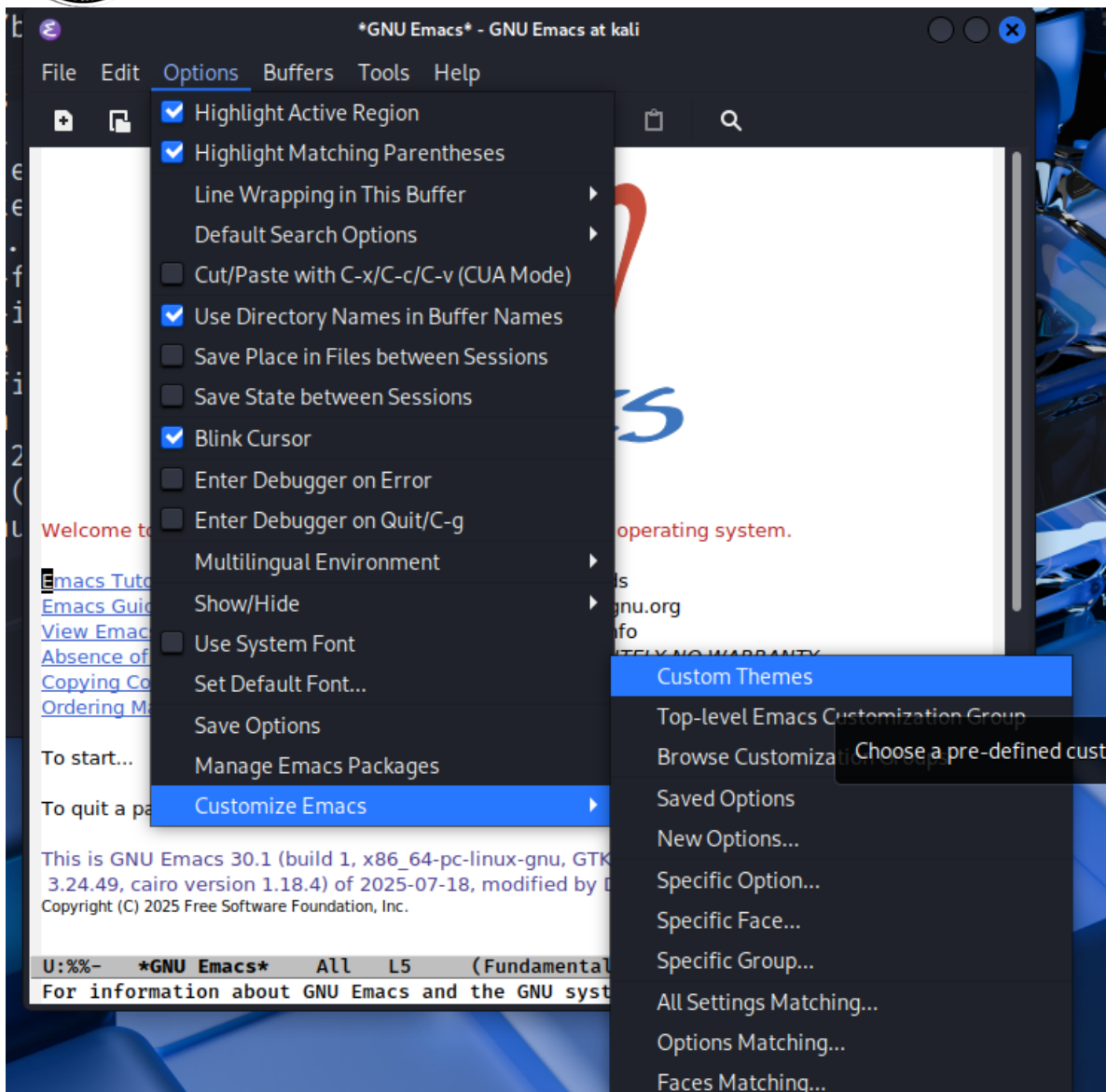


```
→ ~ sudo apt-get update
```

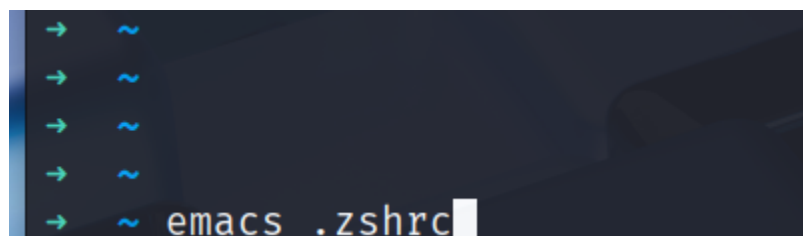
```
→ ~  
→ ~ sudo apt-get install emacs
```



Si quieren configurar el tema



Abrir el fichero .zshrc y modificarlo





```
Save Undo % [Icons]
# If you come from bash you might have to change your $PATH.
# export PATH=$HOME/bin:$HOME/.local/bin:/usr/local/bin:$PATH

# Path to your Oh My Zsh installation.
export ZSH="$HOME/.oh-my-zsh"

# Set name of the theme to load --- if set to "random", it will
# load a random theme each time Oh My Zsh is loaded, in which case,
# to know which specific one was loaded, run: echo $RANDOM_THEME
# See https://github.com/ohmyzsh/ohmyzsh/wiki/Themes
ZSH_THEME="robbyrussell"

# Set list of themes to pick from when loading at random
# Setting this variable when ZSH_THEME=random will cause zsh to load
# a theme from this variable instead of looking in $ZSH/themes/
# If set to an empty array, this variable will have no effect.
# ZSH_THEME_RANDOM_CANDIDATES=( "robbyrussell" "agnoster" )

# Uncomment the following line to use case-sensitive completion.
# CASE_SENSITIVE="true"

# Uncomment the following line to use hyphen-insensitive completion.
# Case-sensitive completion must be off. _ and - will be interchangeable.
# HYPHEN_INSENSITIVE="true"

# Uncomment one of the following lines to change the auto-update behavior
# zstyle ':omz:update' mode disabled # disable automatic updates
# zstyle ':omz:update' mode auto # update automatically without asking
# zstyle ':omz:update' mode reminder # just remind me to update when it's time

# Uncomment the following line to change how often to auto-update (in days).
# zstyle ':omz:update' frequency 13

# Uncomment the following line if pasting URLs and other text is messed up.
# DISABLE_MAGIC_FUNCTIONS="true"
```

```
# Set name of the theme to load --- if set to "random", it will
# load a random theme each time Oh My Zsh is loaded, in which case,
# to know which specific one was loaded, run: echo $RANDOM_THEME
# See https://github.com/ohmyzsh/ohmyzsh/wiki/Themes
ZSH_THEME="powerlevel10k/powerlevel10k"
```

Ojo si quieren volver a configuración **p10k configure**



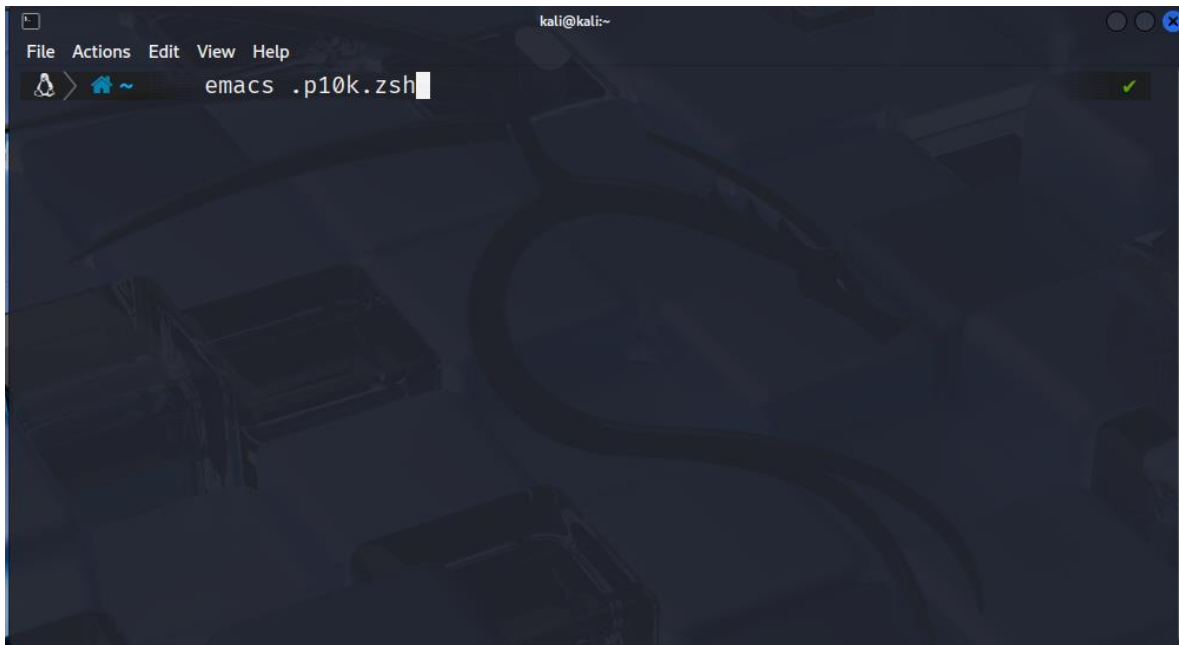


```
kali@kali:~  
File Actions Edit View Help  
This is Powerlevel10k configuration wizard. You are seeing it because you haven't  
defined any Powerlevel10k configuration options. It will ask you a few questions and  
configure your prompt.  
  
Does this look like a diamond (rotated square)?  
reference: https://graphemica.com/%E2%97%86  
→ ◆ ←  
  
(y) Yes.  
(n) No.  
(q) Quit and do nothing.  
Choice [ynq]:
```

```
kali@kali:/home  
File Actions Edit View Help  
🔒 /home
```



Modificamos el fichero de configuracion **/p10k.zsh** y seleccionamos las características que nos interesen.



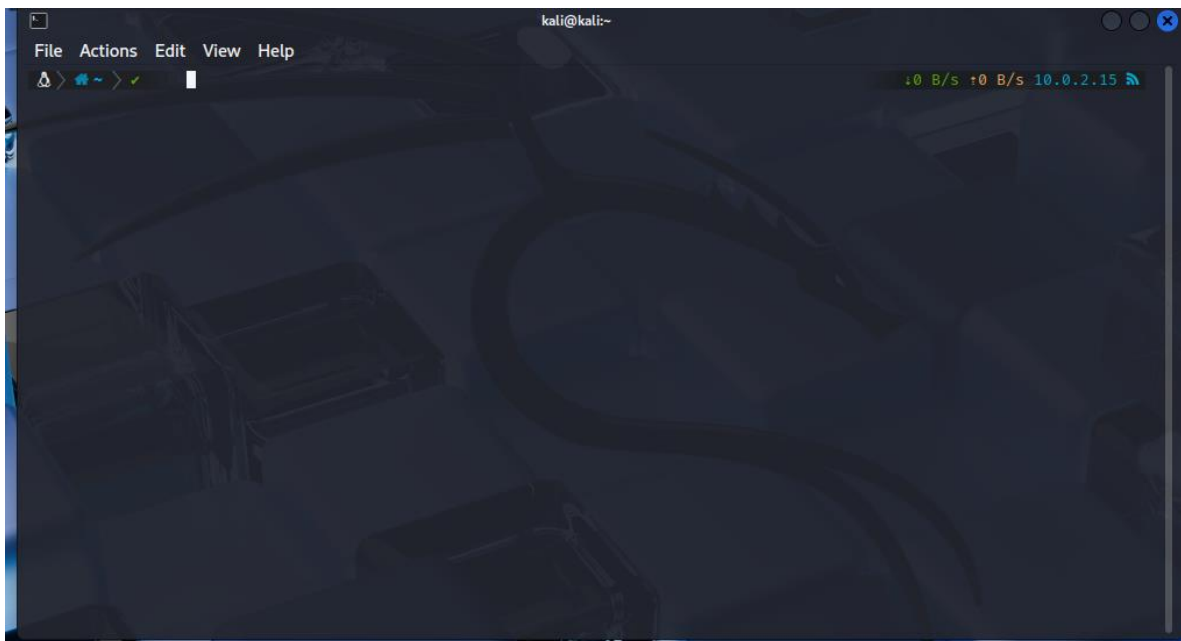
Yo comentarice todo excepto ip

```
#aws_env      # aws elastic beanstalk environment (https://aws.amazon.com/elasticbeanstalk/)
#azure        # azure account name (https://docs.microsoft.com/en-us/cli/azure)
#gcloud       # google cloud cli account and project (https://cloud.google.com/)
#google_app_cred # google application credentials (https://cloud.google.com/docs/authentication/production)
#toolbox      # toolbox name (https://github.com/containers/toolbox)
#context      # user@hostname
#nordvpn      # nordvpn connection status, linux only (https://nordvpn.com/)
#ranger       # ranger shell (https://github.com/ranger/ranger)
#yazi        # yazi shell (https://github.com/sxyazi/yazi)
#nnn         # nnn shell (https://github.com/jarun/nnn)
#lf          # lf shell (https://github.com/gokcehan/lf)
#xplr        # xplr shell (https://github.com/sayanarijit/xplr)
#vim_shell    # vim shell indicator (:sh)
#midnight_commander # midnight commander shell (https://midnight-commander.org/)
#nix_shell    # nix shell (https://nixos.org/nixos/nix-pills/developing-with-nix-shell.html)
#chezmoi_shell # chezmoi shell (https://www.chezmoi.io/)
#vi_mode     # vi mode (you don't need this if you've enabled prompt_char)
#vpn_ip       # virtual private network indicator
#load         # CPU load
#disk_usage   # disk usage
#ram          # free RAM
#swap        # used swap
#todo         # todo items (https://github.com/todotxt/todo.txt-cli)
#timewarrior  # timewarrior tracking status (https://timewarrior.net/)
#taskwarrior  # taskwarrior task count (https://taskwarrior.org/)
#per_directory_history # Oh My Zsh per-directory-history local/global indicator
#cpu_arch     # CPU architecture
#time         # current time
#ip           # ip address and bandwidth usage for a specified network interface
#public_ip    # public IP address
#proxy        # system-wide http/https/ftp proxy
#battery      # internal battery
#wifi         # wifi speed
#example      # example user-defined segment (see prompt_example function below)
)
```



Y en la izquierda copie y pegue la opción status

```
# The list of segments shown on the left. Fill it with the most important segments.
typeset -g POWERLEVEL9K_LEFT_PROMPT_ELEMENTS=(
  os_icon          # os identifier
  dir              # current directory
  status           # exit code of the last command
  # vcs            # git status
  # prompt_char    # prompt symbol
)
```



**Instalamos un modulo para sugerencias automaticas**

```
git clone https://github.com/zsh-users/zsh-autosuggestions  ${ZSH_CUSTOM:~/.oh-my-zsh/custom}/plugins/zsh-autosuggestions
```



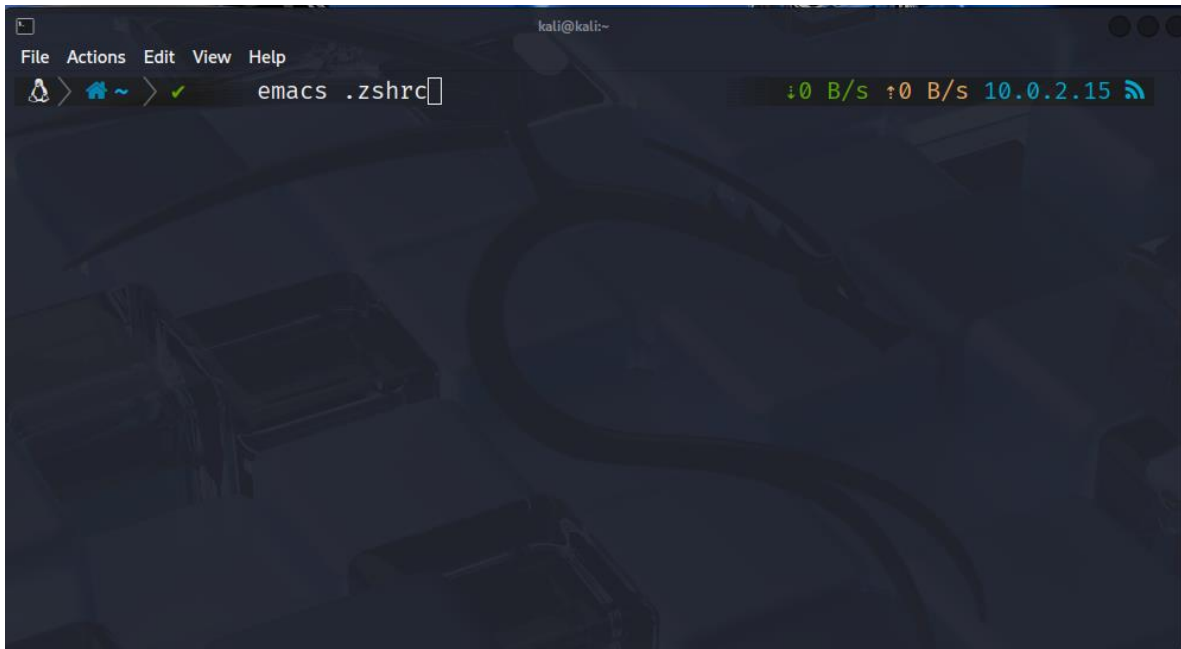
```
kali@kali:~  
File Actions Edit View Help  
git clone https://github.com/zsh-users/zsh-autosuggestions ${ZSH_CUSTOM:~/.oh-my-zsh/custom}/plugins/zsh-autosuggestions  
Cloning into '/home/kali/.oh-my-zsh/custom/plugins/zsh-autosuggestions' ...  
remote: Enumerating objects: 2591, done.  
remote: Counting objects: 100% (154/154), done.  
remote: Compressing objects: 100% (70/70), done.  
remote: Total 2591 (delta 123), reused 84 (delta 84), pack-reused 2437 (from 2)  
Receiving objects: 100% (2591/2591), 597.04 KiB | 1.81 MiB/s, done.  
Resolving deltas: 100% (1655/1655), done.  
4.43 KiB/s +147 B/s 10.0.2.15
```

**Instalamos un plugin que resalta la sintaxis:**

```
git clone https://github.com/zsh-users/zsh-syntax-highlighting.git ${ZSH_CUSTOM:~/.oh-my-zsh/custom}/plugins/zsh-syntax-highlighting
```



**Modificamos el fichero de configuracion ~/.zshrc y añadimos la siguiente sentencia:**





```
kali-linux-2025.2-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

.zshrc - GNU Emacs at kali
File Edit Options Buffers Tools Sh-Script Help
Save Undo Cut Copy Paste Find
# or set a custom format using the strftime function format specifications,
# see 'man strftime' for details.
# HIST_STAMPS="mm/dd/yyyy"

# Would you like to use another custom folder than $ZSH/custom?
# ZSH_CUSTOM=/path/to/new-custom-folder

# Which plugins would you like to load?
# Standard plugins can be found in $ZSH/plugins/
# Custom plugins may be added to $ZSH_CUSTOM/plugins/
# Example format: plugins=(rails git textmate ruby lighthouse)
# Add wisely, as too many plugins slow down shell startup.
plugins=(git

  zsh-autosuggestions
  zsh-syntax-highlighting

)

source $ZSH/oh-my-zsh.sh

# User configuration

# export MANPATH="/usr/local/man:$MANPATH"

# You may need to manually set your language environment
# export LANG=en_US.UTF-8

# Preferred editor for local and remote sessions
# if [[ -n $SSH_CONNECTION ]]; then
#   export EDITOR='vim'
# else
#   export EDITOR='nvim'
# fi

# Compilation flags
# export ARCHFLAGS="-arch $(uname -m)"

# Set personal aliases, overriding those provided by Oh My Zsh libs,
# plugins, and themes. Aliases can be placed here, though Oh My Zsh
# users are encouraged to define aliases within a top-level file in
# the $ZSH_CUSTOM folder, with .zsh extension. Examples:
# - $ZSH_CUSTOM/aliases.zsh
# - $ZSH_CUSTOM/macos.zsh
```

```
# Add wisely, as too many plugins slow down shell startup
plugins=(git

  zsh-autosuggestions
  zsh-syntax-highlighting

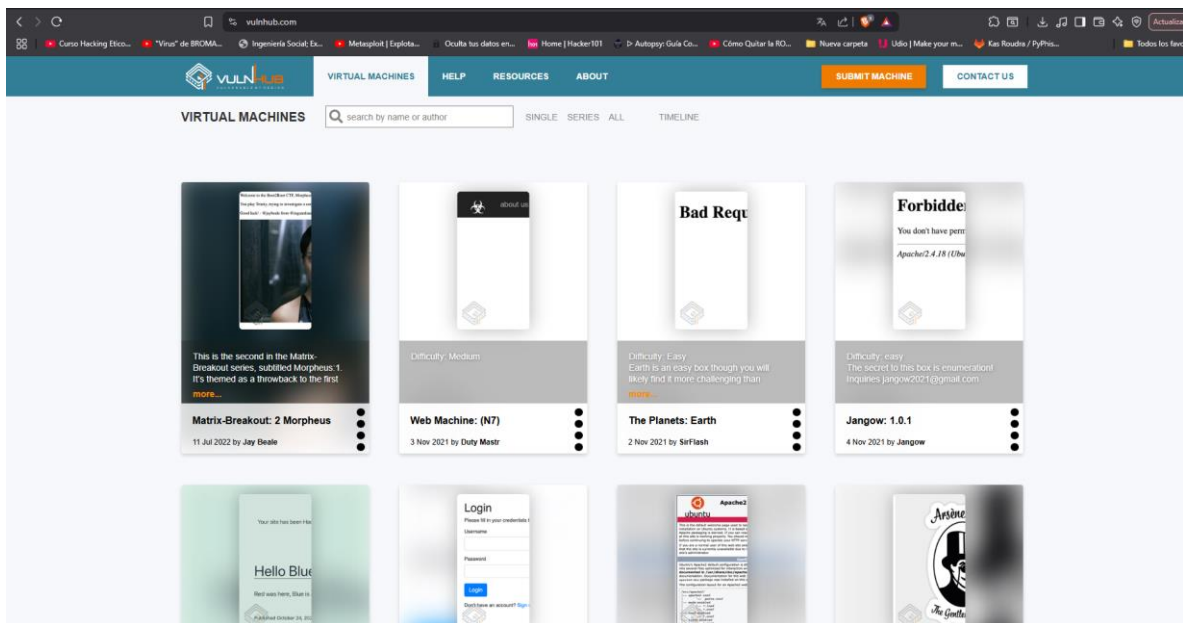
)
```





## VULNHUB

1. Ingresar a la pagina <https://www.vulnhub.com/>





2. En el buscado escribir troll y descargar la **troll 1**

**VULNHUB** VIRTUAL MACHINES HELP RESOURCES ABOUT SUBMIT MACHINE CONTACT US

VIRTUAL MACHINES troll SINGLE SERIES ALL TIMELINE

SEARCH RESULT: TROLL (15 RESULTS)

**Tröll: 1**  
14 Aug 2014 by Maleus

**Tröll: 2**  
24 Oct 2014 by Maleus

**Violator: 1**  
4 Jul 2016 by knightmare

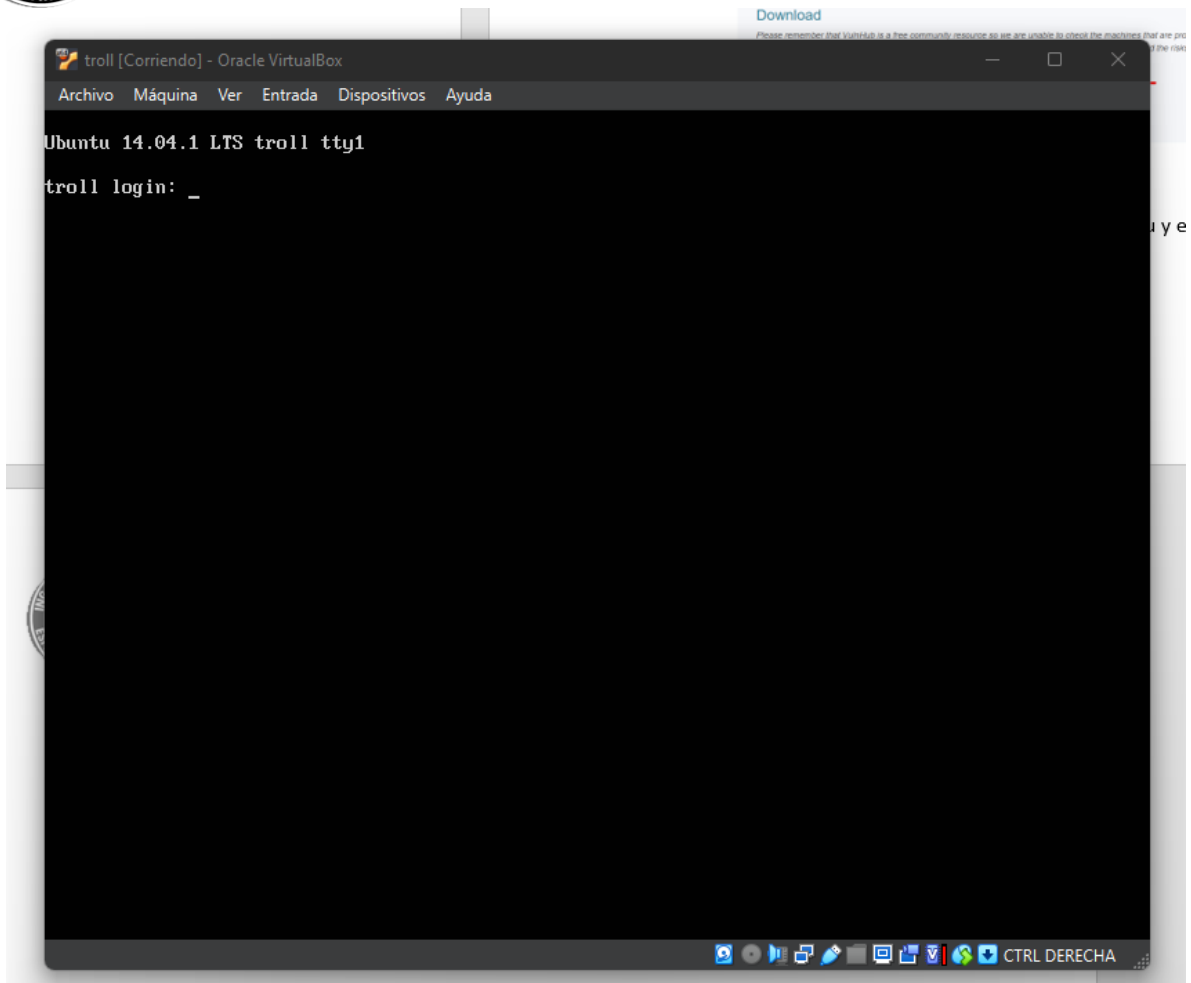
**Breach: 2.1**  
15 Aug 2016 by mrb3n

**Download** [Back to the Top](#)

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

**Tröll.rar** (Size: 434 MB)  
Download: <http://overflowsecurity.com/files/Tröll.rar>  
Download (Mirror): <https://download.vulnhub.com/tröll/Tröll.rar>

3. Instalar en virtual box maquina nueva Ubuntu y en las opción de disco duro elegir un archivo de dd existente





```
C:\Windows\system32\cmd.exe

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::d7a9:5ce3:24c:7066%18
Dirección IPv4 de configuración automática: 169.254.127.178
Máscara de subred . . . . . : 255.255.0.0
Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 4:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::9e5d:4ac9:5973:594d%58
Dirección IPv4. . . . . : 192.168.99.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :

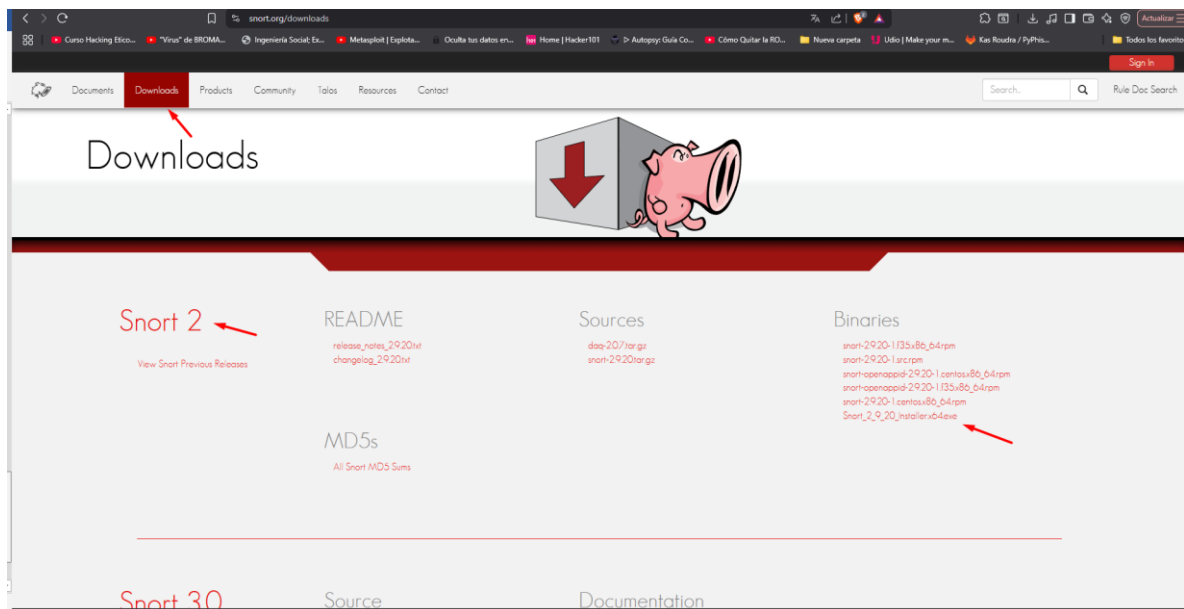
Adaptador de LAN inalámbrica Conexión de área local* 11:

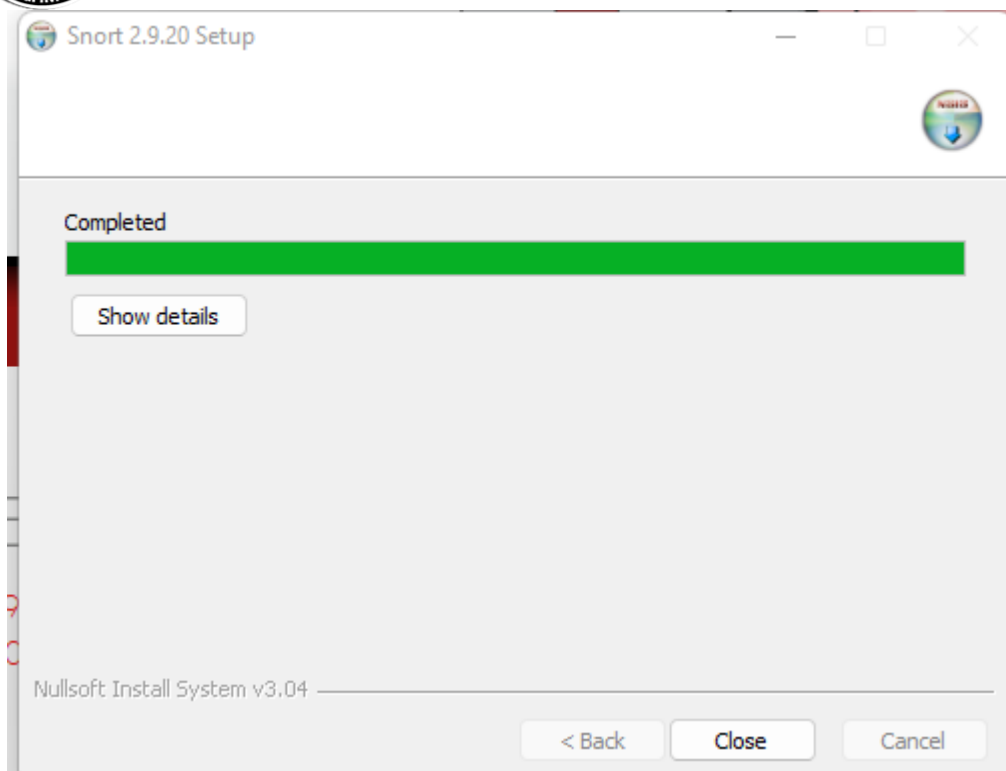
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :

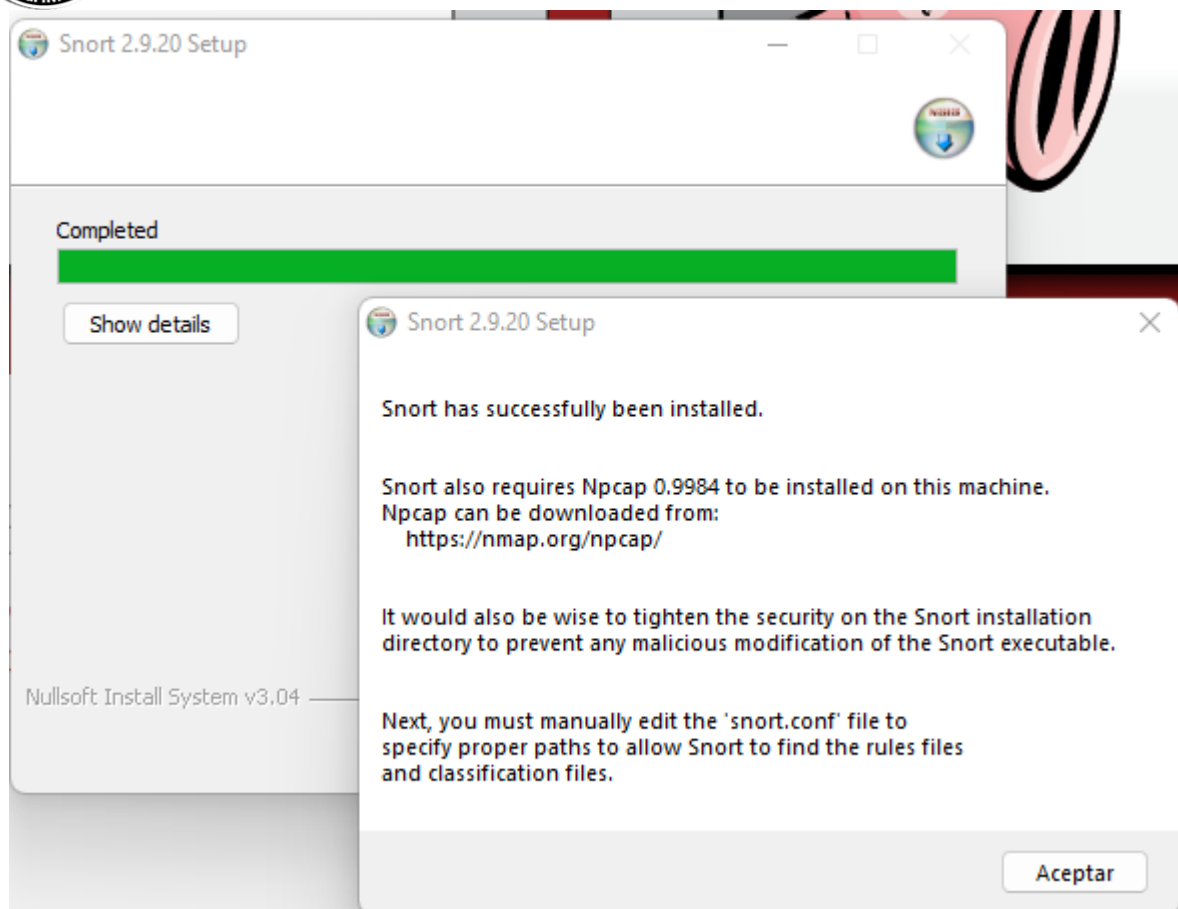
Adaptador de LAN inalámbrica Conexión de área local* 12:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
```

#### 4. Instalar snor en Windows en el host







**Nos pide el ncap**






Google

Todo Videos Imágenes Shopping Noticias Web Videos cortos Más Herramientas

Se muestran resultados de **npcap download**  
Buscar, en cambio, [npcap download](#)

 Npcap  
<https://npcap.com> · Traducir esta página

**Npcap: Windows Packet Capture Library & Driver**  
... Download Npcap Npcap License Npcap Changelog 1.83 2025-08-01. Packet capture library for Windows. Npcap is the Nmap Project's packet capture (and sending) ...

**WinPcap for Windows 10**  
Just download the latest installer. Npcap works great with ...

**Npcap OEM**  
... Npcap.com Seclists.org Sectools.org Insecure.org · Docs ...

**Npcap release archive**  
Npcap release archive. The latest Npcap release is version 1.83 ...

**WinPcap**  
Just download the latest installer. Npcap works great with ...

**Developing software with Npcap**

## Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems ([free license details](#)). It may also be used on unlimited systems where it is only used with [Nmap](#), [Wireshark](#), and/or [Microsoft Defender for Identity](#). Simply run the executable installer. The full source code for each release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the [Npcap Changelog](#).

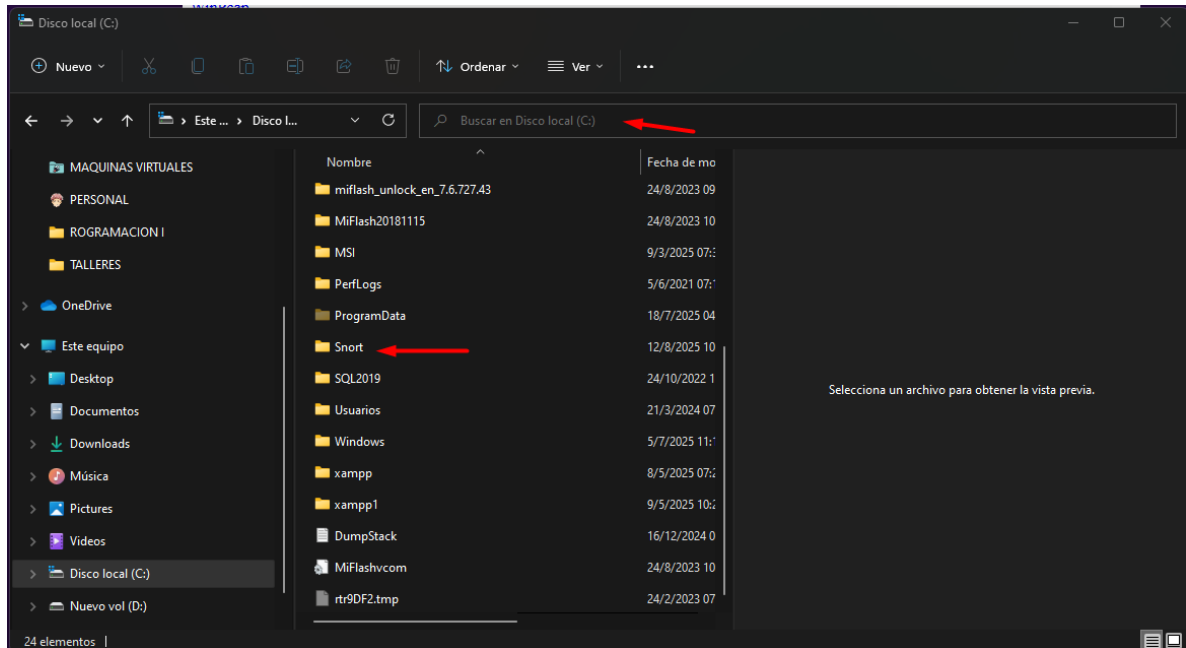
- [Npcap 1.83 installer](#) for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019, 11 (x86, x64, and ARM64).
- [Npcap SDK 1.15](#) (ZIP).
- [Npcap 1.83 debug symbols](#) (ZIP).
- [Npcap 1.83 source code](#) (ZIP).

The latest development source is in our [Github source repository](#). Windows XP and earlier are not supported; you can use [WinPcap](#) for these versions.

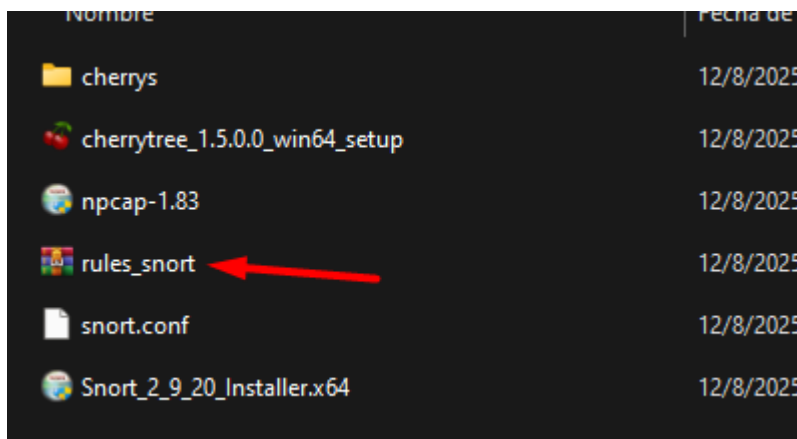
## Npcap OEM for Commercial Use and Redistribution



Luego ir a la carpeta origen del SNORT



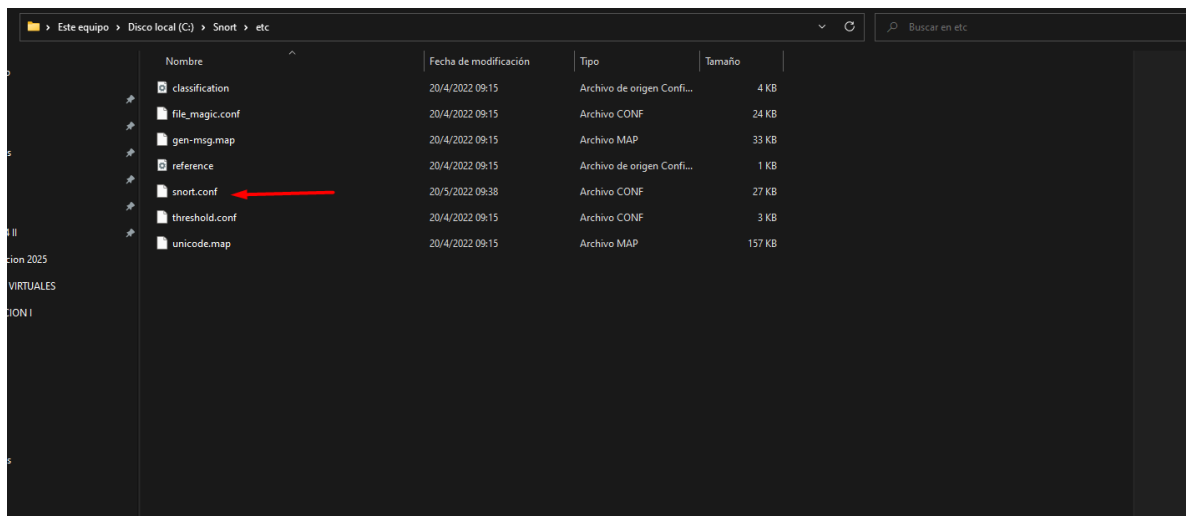
Y pasar los archivos rules y el .conf





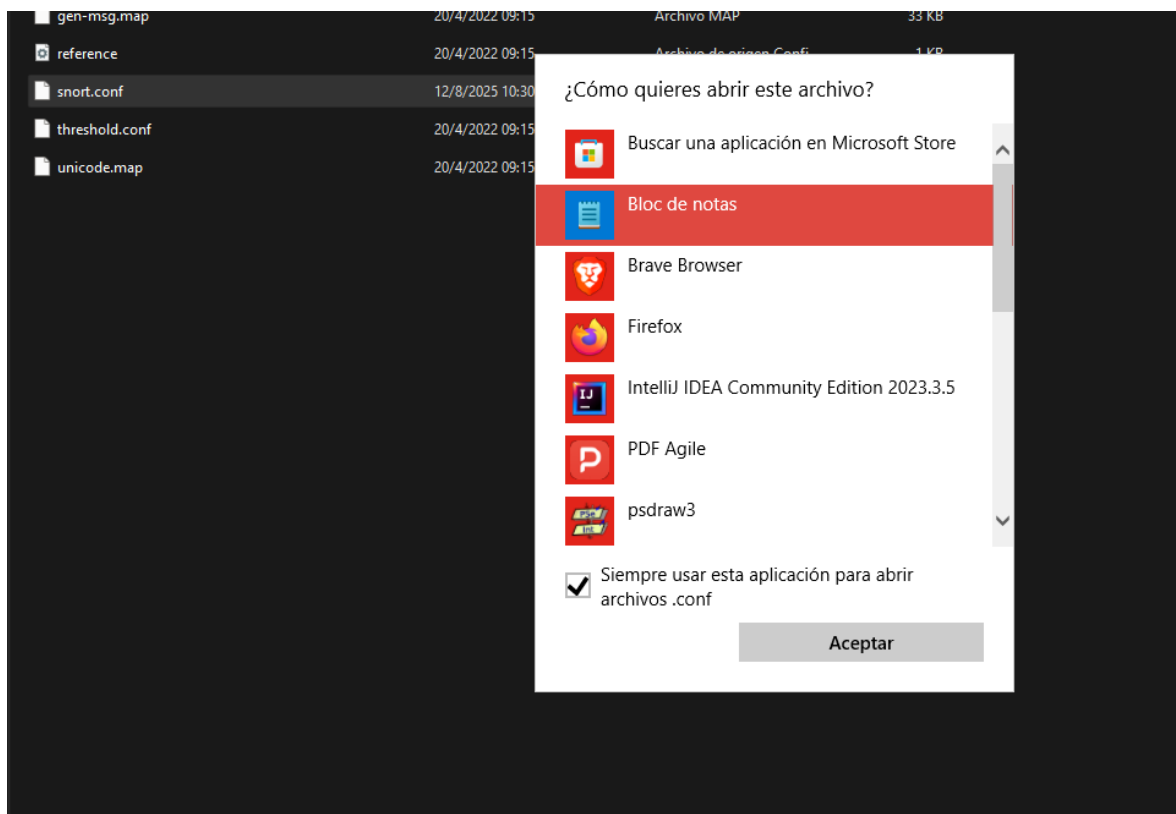
Descomprimir la carpeta rules, copiarla, ir al disco c y eliminar la carpeta rules por defecto y pegar la que se paso

Lo mismo con el archivo de configuración





Abrir y modificar la ip por la que se creo o se dejo solo anfitrion





```
Archivo  Editar  Ver
# This configuration file enables active response, to run snort in
# test mode -t you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#-----
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.20.0/24
# Set up the external network addresses.  Leave as "any" in most situations
ipvar EXTERNAL_NET any
# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET
# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET
```

```
C:\Windows\system32\cmd.exe
Adaptador de Ethernet Ethernet 2:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::d7a9:5ce3:24c:7066%18
  Dirección IPv4 de configuración automática: 169.254.127.178
  Máscara de subred . . . . . : 255.255.0.0
  Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 4:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::9e5d:4ac9:5973:594d%58
  Dirección IPv4. . . . . : 192.168.99.1
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 11:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 12:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet Ethernet 3:
  Sufijo DNS específico para la conexión. . . :
```

Abrir power shell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\ING FABIAN>
```

Ir a la ruta de snort



```
PS C:\snort> ls

Directorio: C:\snort

Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025  10:27 AM                bin
d-----            8/12/2025  10:27 AM                doc
d-----            8/12/2025  10:35 AM                etc
d-----            8/12/2025  10:27 AM                lib
d-----            8/12/2025  10:27 AM                log
d-----            8/12/2025  10:27 AM          preproc_rules
d-----            8/12/2025  10:33 AM            rules
-a-----            8/12/2025  10:27 AM          52666 Uninstall.exe

PS C:\snort>
```

Ver interfaces que están arriba

```
PS C:\snort\bin> .\snort.exe -W
```

```
Windows PowerShell
~a----- 4/20/2022 9:15 AM 53326 WanPacket.dll
~a----- 4/20/2022 9:15 AM 208974 wpcap.dll
~a----- 4/20/2022 9:15 AM 73728 zlib.dll

PS C:\snort\bin> .\snort.exe -U

-> Snort! <*-
o ~~~~~
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address  IP Address  Device Name  Description
-----
1 00:00:00:00:00:00 disabled \Device\NPF_{CD893D7E-CBD0-4180-AB9E-CC34E85D38A4} WAN Miniport (Network Monitor)
2 00:00:00:00:00:00 disabled \Device\NPF_{16A62D16-255C-40D4-8949-FFFA9C94081F} WAN Miniport (IPv6)
3 00:00:00:00:00:00 disabled \Device\NPF_{7FCDF9C0-BF79-45A5-9B98-AB4DB433C4CD} WAN Miniport (IP)
4 38:24:32:A0:F6:76 169.254.26.125 \Device\NPF_{20AD3833-26C1-4672-AD29-C5AEDF8CAFCD} Bluetooth Device (Personal Area Network) #2
5 38:24:32:A0:F6:72 169.254.135.179 \Device\NPF_{2ECC9C8-9157-4EFD-9E4E-C733C06D4099} Intel(R) Dual Band Wireless-AC 8265
6 5C:53:10:4E:62:E3 192.168.100.14 \Device\NPF_{5E53D088-33E2-4CB9-80FF-1944170DE27C} USB2.0 Ethernet Adapter
7 32:24:32:A0:F6:72 169.254.255.93 \Device\NPF_{440B6486-3758-46F4-80D1-2D690CAF22C2} Microsoft Wi-Fi Direct Virtual Adapter #4
8 38:24:32:A0:F6:73 169.254.197.208 \Device\NPF_{7BE8A158-1178-41DF-B6FF-5DFA482DFE1C} Microsoft Wi-Fi Direct Virtual Adapter #3
9 00:00:27:00:00:30 192.168.99.4 \Device\NPF_{5D3BD24E-8584-4535-B6ED-493F3F4B7B2C} VirtualBox Host-Only Ethernet Adapter #2
10 00:00:27:00:00:12 192.168.56.120 \Device\NPF_{CBA103EB-41C1-4D86-B6F5-69D11672BD343} VirtualBox Host-Only Ethernet Adapter
11 00:00:00:00:00:00 0000:0000:0000:0000:0000:0000 \Device\NPF_{Loopback Adapter} for loopback traffic capture
12 4C:CC:6A:83:A4:6C 169.254.59.122 \Device\NPF_{BAE00E71-6BAC-4393-A195-60F8B9735501} Killer E2400 Gigabit Ethernet Controller

PS C:\snort\bin>
```

Ahora configurarlo para que nos muestre las alestas en el power Shell

PS C:\snort\bin> .\snort.exe -i 9 -A console -c C:\Snort\etc\snort.conf

```
PS C:\snort\bin> .\snort.exe -i 9 -A console -c C:\Snort\etc\snort.conf
```





```
Windows PowerShell
Match Lists : 1.01
DFA
1 byte states : 1.02
2 byte states : 13.96
4 byte states : 0.00

[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{5D3BD24E-0584-4535-B6ED-493F3F4B7B2C}".
Decoding Ethernet

==== Initialization Complete ====

--> Snort! <--
Version 2.9.20-UNIX GRE (Build 02)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 (Build 1)
Preprocessor Object: SF_SSLPP Version 1.1 (Build 4)
Preprocessor Object: SF_SSH Version 1.1 (Build 3)
Preprocessor Object: SF_SMP Version 1.1 (Build 9)
Preprocessor Object: SF_SIP Version 1.1 (Build 1)
Preprocessor Object: SF_SDP Version 1.1 (Build 1)
Preprocessor Object: SF_REPUTATION Version 1.1 (Build 1)
Preprocessor Object: SF_POP Version 1.0 (Build 1)
Preprocessor Object: SF_MODBUS Version 1.1 (Build 1)
Preprocessor Object: SF_IMAP Version 1.0 (Build 1)
Preprocessor Object: SF_GIP Version 1.1 (Build 1)
Preprocessor Object: SF_FIPIELNET Version 1.2 (Build 13)
Preprocessor Object: SF_DNS Version 1.1 (Build 4)
Preprocessor Object: SF_DMP3 Version 1.1 (Build 1)
Preprocessor Object: SF_DCERPC2 Version 1.0 (Build 3)
Commencing packet processing (pid=55732)
```

Ir a Kali hacer un escaneo

```
File Actions Edit View Help
sudo nmap -sS -n 192.168.99.0/24
```

```
File Actions Edit View Help
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at
Nmap scan report for 192.168.99.2
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.99.2 are
Not shown: 1000 filtered tcp ports (proto-
MAC Address: 08:00:27:51:00:FE (PCS System

Nmap scan report for 192.168.99.4
Host is up (0.00049s latency).
Not shown: 998 filtered tcp ports (no-resp-
PORT STATE SERVICE
80/tcp open http
7070/tcp open realserver
MAC Address: 0A:00:27:00:00:3A (Unknown)

Nmap scan report for 192.168.99.5
Host is up (0.00033s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 08:00:27:B7:F8:A1 (PCS System

Nmap scan report for 192.168.99.3
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.99.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.71 seconds

11.27 KiB/s +2.63 KiB/s 192.168.99.3
```



```
kali-linux-2023.2-virtualbox-amd64 [Comandos] - Oracle VM VirtualBox
File Actions Edit View Help
1 2 3 4
sudo nmap -sn -n 192.168.99.
Starting Nmap 7.95 ( https://nmap.org ) at 20:
Nmap scan report for 192.168.99.2
Host is up (0.00023s latency).
MAC Address: 08:00:27:51:0D:FE (PCS Systemtec)
Nmap scan report for 192.168.99.4
Host is up (0.00023s latency).
MAC Address: 0A:00:27:00:00:3A (Unknown)
Nmap scan report for 192.168.99.5
Host is up (0.00061s latency).
MAC Address: 08:00:27:B7:F8:A1 (PCS Systemtec)
Nmap scan report for 192.168.99.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scan

Windows PowerShell
1 byte states : 284
2 byte states : 11
4 byte states : 0
Characters : 21751
States : 64795
Transitions : 863888
State history : 1842
Patterns : 5841
Match States : 3856
Memory (MB) : 16.98
Patterns : 0.51
Match Lists : 1.81
MB
1 byte states : 1.62
2 byte states : 13.36
4 byte states : 0.00
Number of patterns truncated to 20 bytes: 1020
Nmap DDoS configured to passive.
The Nmap version does not support nmapd.
Acquiring network traffic from "Device\NPF_{5D3B024E-8584-4535-B6ED-493F3F4B702C}".
Decoding Internet
---- Initialization Complete ----
--> Snort! <--
Version 3.9.2.0-VPM64-GIT (Build 02)
By Martin Rensch & the Snort team: http://www.snort.org/contactteam
Copyright (C) 1998-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Emerging Inc., et al.
Using CMake version 3.18.0108-06-25
Using LLVM version 12.1.1
Rules Engine: SF_SNORT DETECTION ENGINE Version 3.2 (Build 1)
Preprocessor Object: SF_SLOW Version 1.0 (Build 0)
Preprocessor Object: SF_SSH Version 1.1 (Build 3)
Preprocessor Object: SF_SMP Version 1.0 (Build 85)
Preprocessor Object: SF_SIP Version 1.1 (Build 15)
Preprocessor Object: SF_SMB Version 1.0 (Build 12)
Preprocessor Object: SF_REPUTATION Version 1.1 (Build 1)
Preprocessor Object: SF_POW Version 1.0 (Build 1)
Preprocessor Object: SF_PROXY Version 1.0 (Build 1)
Preprocessor Object: SF_TINY Version 1.0 (Build 1)
Preprocessor Object: SF_CIP Version 1.1 (Build 1)
Preprocessor Object: SF_PIPELINED Version 1.2 (Build 13)
Preprocessor Object: SF_DNS Version 1.1 (Build 1)
Preprocessor Object: SF_SMP Version 1.1 (Build 1)
Preprocessor Object: SF_ICMP Version 1.0 (Build 3)
Commencing packet processing (pid=60744)
```