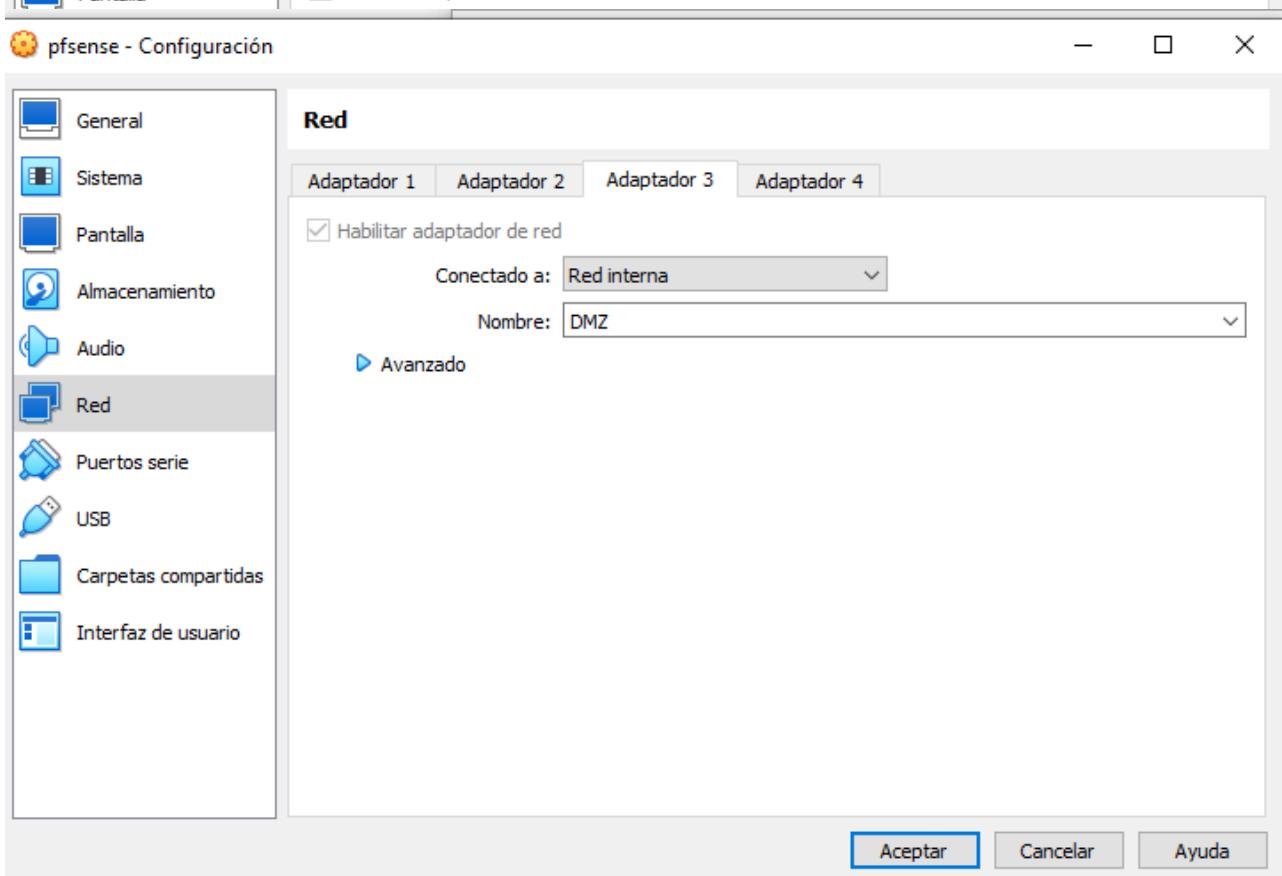
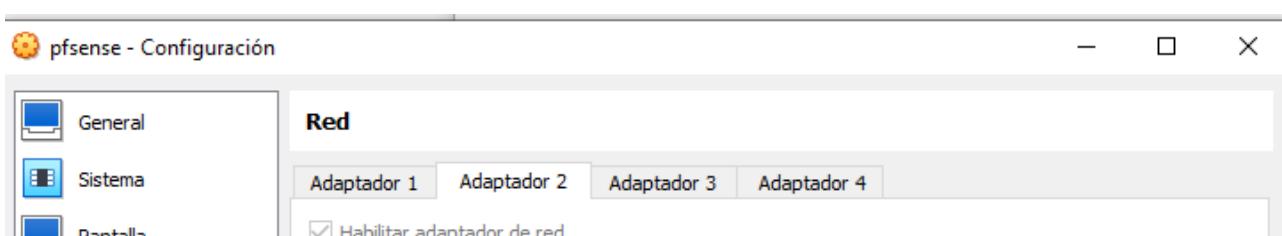
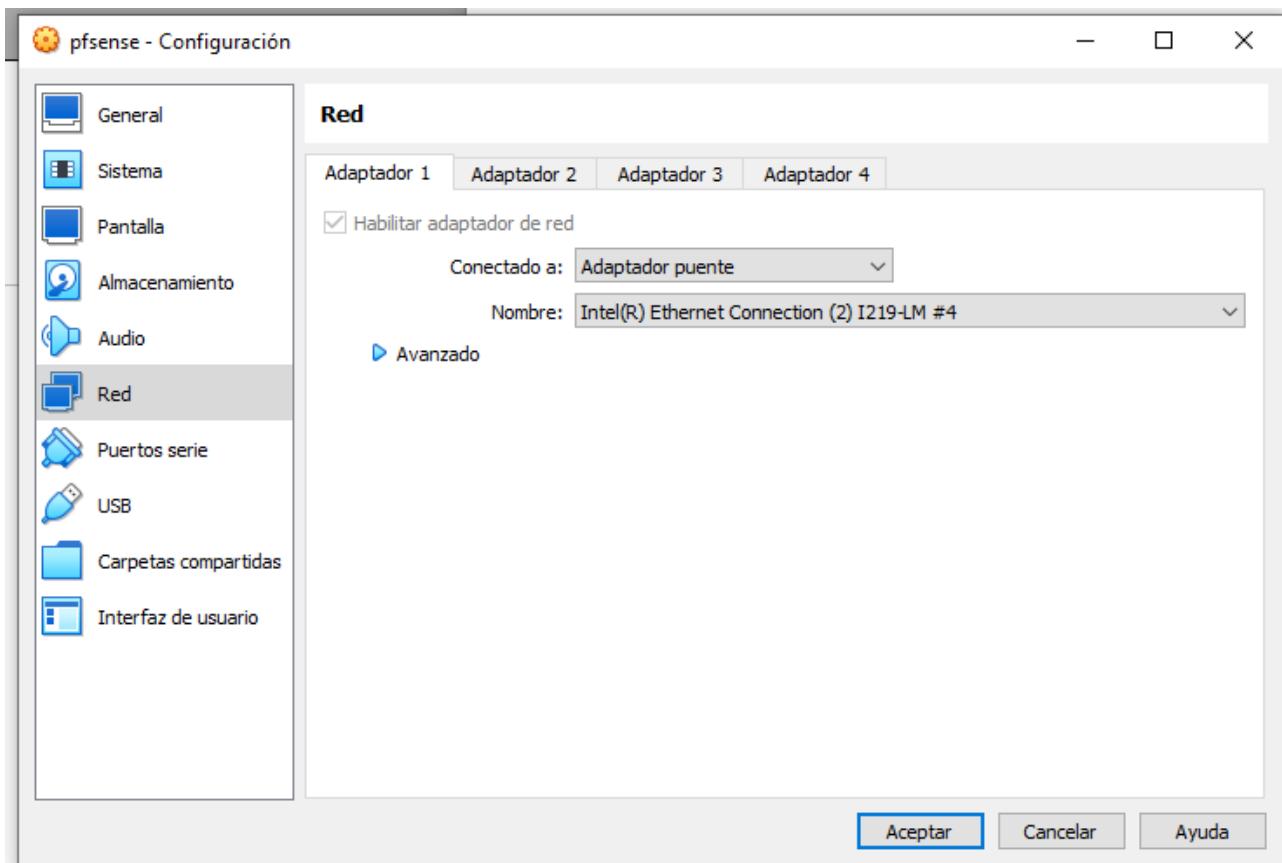
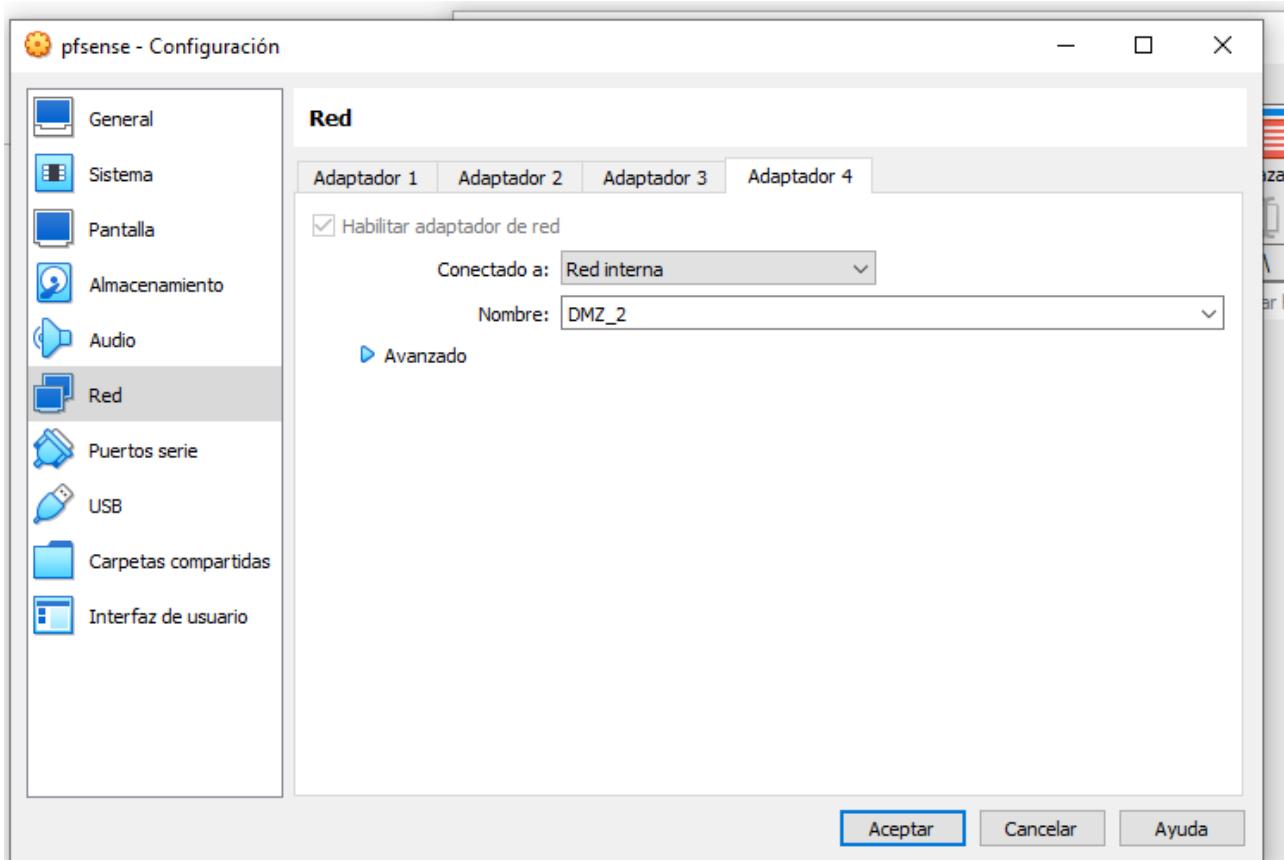


MONTAJE DE INFRAESTRUCTURA





arrancamos la Unified Threat Management (UTM)

```
pfSense (UTM funcionando) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: d16b4b90899ec6066e97

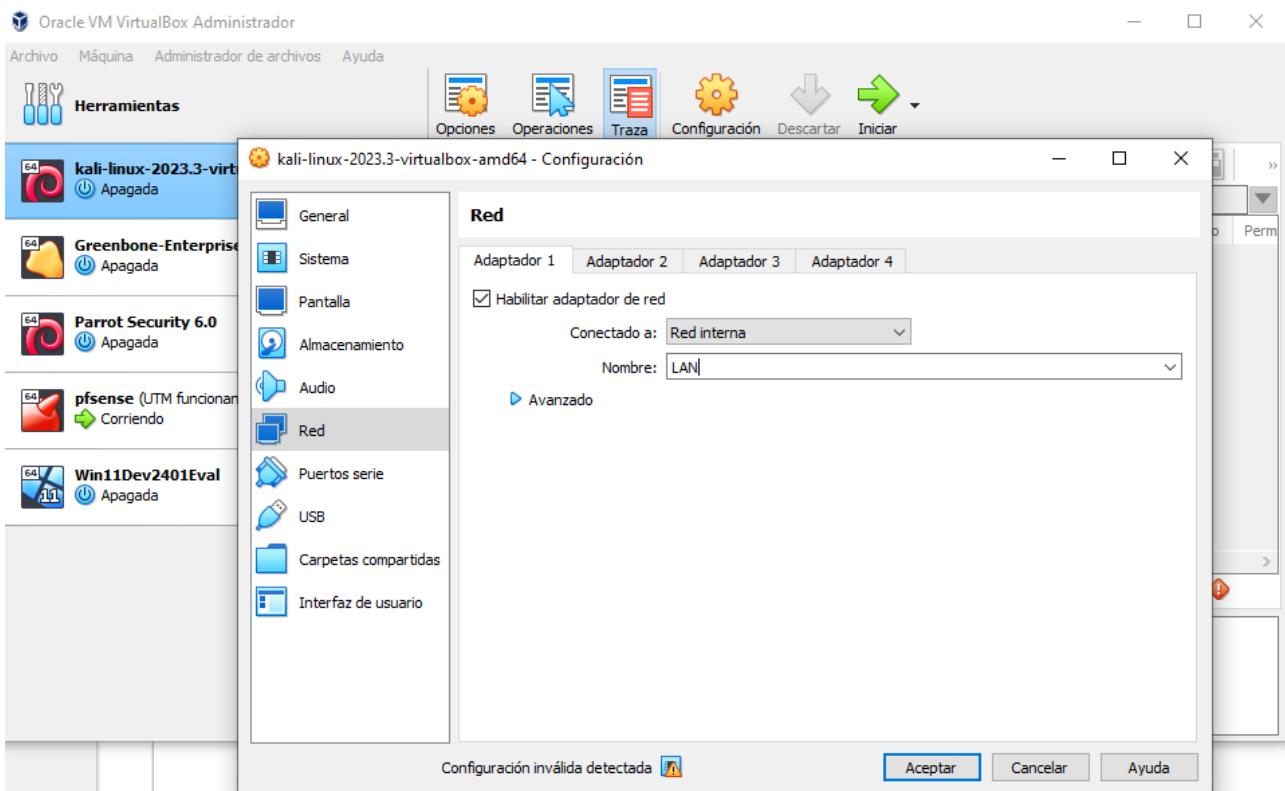
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.16/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

configuramos la kali en red interna LAN



Arrancamos la kali e introducimos en el navegador la ip del adaptador LAN, en mi caso:

192.168.100.1

A screenshot of a web browser displaying the pfSense login interface. The address bar shows the URL '192.168.100.1'. The page features the pfSense logo at the top left and a 'Login to pfSense' link at the top right. The main content area is a 'SIGN IN' form with two input fields: one for 'admin' and another for a password (represented by a series of dots). Below the fields is a green 'SIGN IN' button. At the bottom of the page, there is a small footer note: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.'

usuario admin, password pfsense

System Information

Name	UTM.keepinglocal
User	admin@192.168.100.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: d16b4b90899ec6066e97
BIOS	Vendor: innoteck GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 07 Minutes 17 Seconds
Current date/time	Fri Mar 15 0:22:19 CET 2024
DNS server(s)	• 127.0.0.1 • 192.168.0.1

Netgate Services And Support

Retrieving support information

Interfaces

WAN	1000baseT <full-duplex>	192.168.0.18
LAN	1000baseT <full-duplex>	192.168.100.1

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6

Advanced Options

Use IPv4 connectivity as parent interface	<input type="checkbox"/> Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	<input type="checkbox"/> Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	64
Send IPv6 prefix hint	<input type="checkbox"/> Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	<input type="checkbox"/> Start DHCP6 client in debug mode
Do not wait for a RA	<input type="checkbox"/> Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	<input type="checkbox"/> dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.	
Block bogon networks	<input type="checkbox"/>
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.	
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.	

Save

CONFIGURACIÓN DE LAS INTERFACES

Comprobamos si tenemos accesos a internet en la kali haciendo un ping a 1.1.1.1:

```
(kali㉿kali)-[~]$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=20.5 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=22.0 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=14.7 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=18.5 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=56 time=20.0 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=56 time=14.1 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=56 time=17.1 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=56 time=13.5 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=56 time=14.0 ms
64 bytes from 1.1.1.1: icmp_seq=11 ttl=56 time=12.4 ms
64 bytes from 1.1.1.1: icmp_seq=12 ttl=56 time=27.4 ms
64 bytes from 1.1.1.1: icmp_seq=13 ttl=56 time=328 ms are crypto
64 bytes from 1.1.1.1: icmp_seq=14 ttl=56 time=15.4 ms
64 bytes from 1.1.1.1: icmp_seq=15 ttl=56 time=12.5 ms TI
^Z
zsh: suspended ping 1.1.1.1
```

Uptime: 00 Hour 25 Minutes 23 Seconds
Current date/time: Fri Mar 15 18:03:08 CET 2024
DNS server(s): 127.0.0.1, 212.166.210.80, 212.166.210.101

hacemos ping en nuestro sistema windows a google.com

```
C:\Users\USER>ping google.com

Haciendo ping a google.com [142.250.200.142] con 32 bytes de datos:
Respuesta desde 142.250.200.142: bytes=32 tiempo=14ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=12ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=11ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=13ms TTL=117

Estadísticas de ping para 142.250.200.142:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 11ms, Máximo = 14ms, Media = 12ms

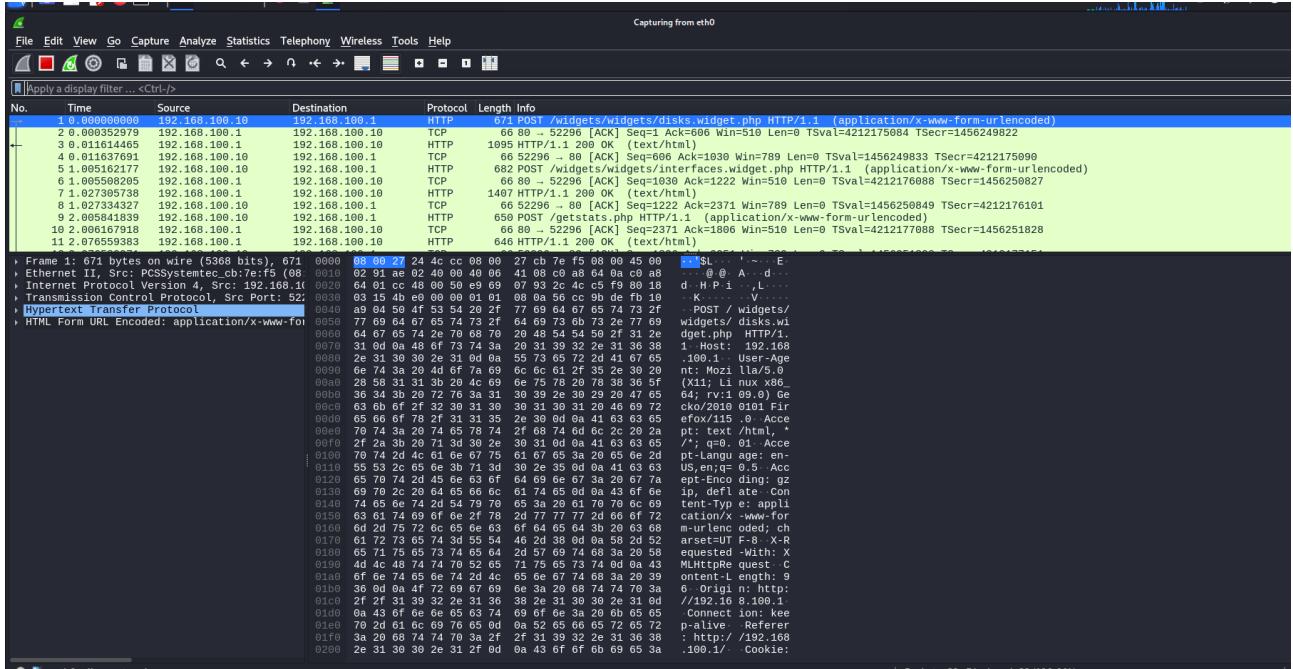
C:\Users\USER>
```

cogemos la ip y la pegamos en kali

```
└─(kali㉿kali)-[~]
$ ping 142.250.200.142
PING 142.250.200.142 (142.250.200.142) 56(84) bytes of data.
64 bytes from 142.250.200.142: icmp_seq=1 ttl=116 time=19.3 ms
64 bytes from 142.250.200.142: icmp_seq=2 ttl=116 time=14.8 ms
64 bytes from 142.250.200.142: icmp_seq=3 ttl=116 time=20.9 ms
64 bytes from 142.250.200.142: icmp_seq=4 ttl=116 time=24.7 ms
64 bytes from 142.250.200.142: icmp_seq=5 ttl=116 time=16.2 ms
64 bytes from 142.250.200.142: icmp_seq=6 ttl=116 time=14.7 ms
64 bytes from 142.250.200.142: icmp_seq=7 ttl=116 time=13.6 ms
^Z
zsh: suspended  ping 142.250.200.142

└─(kali㉿kali)-[~]
$
```

en wireshark podemos ver el tráfico que está pasando por la interface de red eth0:



hacemos click botón derecho en alguna de las tramas, Follow y TCP Stream y vemos todos los paquetes del tráfico:

```

POST /widgets/widgets/disks.widget.php HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html, */*, q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 96
Origin: http://192.168.100.1
Connection: keep-alive
Referer: http://192.168.100.1/
Cookie: PHPSESSID=ba4fb8cfdd7f540d03d2aea1bbc20c0
__crsf_magic=sid:a20c1aae66b5ab314ba9ff0d8872de9bb75bd77,1710521625&ajax=ajax&widgetkey=disks-0HTTP/1.1 200 OK
Server: nginx
Date: Fri, 15 Mar 2024 17:09:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 15 Mar 2024 17:09:08 GMT
Set-Cookie: PHPSESSID=ba4fb8cfdd7f540d03d2aea1bbc20c0; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip

```

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Ethernet II, Src: PCSSystemtec_c [00:0c:29:00:00:04], Dst: 192.168.100.1 [00:0c:29:00:00:01]
`...[REDACTED]`

POST /widgets/widgets/interfaces.widget.php HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html, */*, q=0.01
Accept-Language: en-US,en;q=0.5
108 client pkts, 108 server pkts, 215 turns.

para ver la información del tráfico.

Configuramos el UTM:

vamos a Services y DNS Resolver

Name	UTM.keeping.local
User	admin@192.168.100.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: d164ab90899ec6066e97
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 43 Minutes 15 Seconds

Netgate Services And Support

- Contract type: Community Support
Community Support Only

NETGATE AND pFSENSE COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to

deschekamos el DNSSEC que es un protocolo utilizado para firmar la respuesta DNS (asegura que la respuesta no ha sido modificada):

Outgoing Network Interfaces	<input type="checkbox"/> All <input type="checkbox"/> WAN <input type="checkbox"/> LAN <input type="checkbox"/> WAN IPv6 Link-Local <input type="checkbox"/> LAN IPv6 Link-Local	Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.
Strict Outgoing Network Interface Binding	<input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available. By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.	
System Domain Local Zone Type	<input type="button" value="Transparent"/> The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.	
DNSSEC	<input checked="" type="checkbox"/> Enable DNSSEC Support	
Python Module	<input type="checkbox"/> Enable Python Module Enable the Python Module.	
DNS Query Forwarding	<input type="checkbox"/> Enable Forwarding Mode If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).	
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.	

habilitamos el DNS Query Forwarding para enviar la consulta al servidor secundario el 1.1.1.1, en el caso de que PFSENSE no sea capaz de enviarla:

Interface Binding	By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.	
System Domain Local Zone Type	<input type="button" value="Transparent"/> The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.	
DNSSEC	<input type="checkbox"/> Enable DNSSEC Support	
Python Module	<input type="checkbox"/> Enable Python Module Enable the Python Module.	
DNS Query Forwarding	<input checked="" type="checkbox"/> Enable Forwarding Mode If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).	
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.	

hacemos click en Save para guardar la configuración DNS:

Kali Tools https://www.kali.org/tools/	If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).											
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.											
DHCP Registration	<input type="checkbox"/> Register DHCP leases in the DNS Resolver If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.											
Static DHCP	<input type="checkbox"/> Register DHCP static mappings in the DNS Resolver If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.											
OpenVPN Clients	<input type="checkbox"/> Register connected OpenVPN clients in the DNS Resolver If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.											
Display Custom Options	<input type="button" value="Display Custom Options"/>											
<input style="background-color: #0070C0; color: white; font-weight: bold; padding: 5px; margin-bottom: 5px;" type="button" value="Save"/> ←												
Host Overrides <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; background-color: #0070C0; color: white;">Host</th> <th style="text-align: left; background-color: #0070C0; color: white;">Parent domain of host</th> <th style="text-align: left; background-color: #0070C0; color: white;">IP to return for host</th> <th style="text-align: left; background-color: #0070C0; color: white;">Description</th> <th style="text-align: left; background-color: #0070C0; color: white;">Actions</th> </tr> </thead> <tbody> <tr> <td colspan="5">Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'ns.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.</td> </tr> </tbody> </table>			Host	Parent domain of host	IP to return for host	Description	Actions	Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'ns.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				
Host	Parent domain of host	IP to return for host	Description	Actions								
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'ns.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.												

y damos a Apply Changes:

The changes have been applied successfully.

General DNS Resolver Options

Enable	<input checked="" type="checkbox"/> Enable DNS resolver
Listen Port	53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.	
Enable SSL/TLS Service	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.	

comprobamos en el navegador que tenemos acceso a marca.com

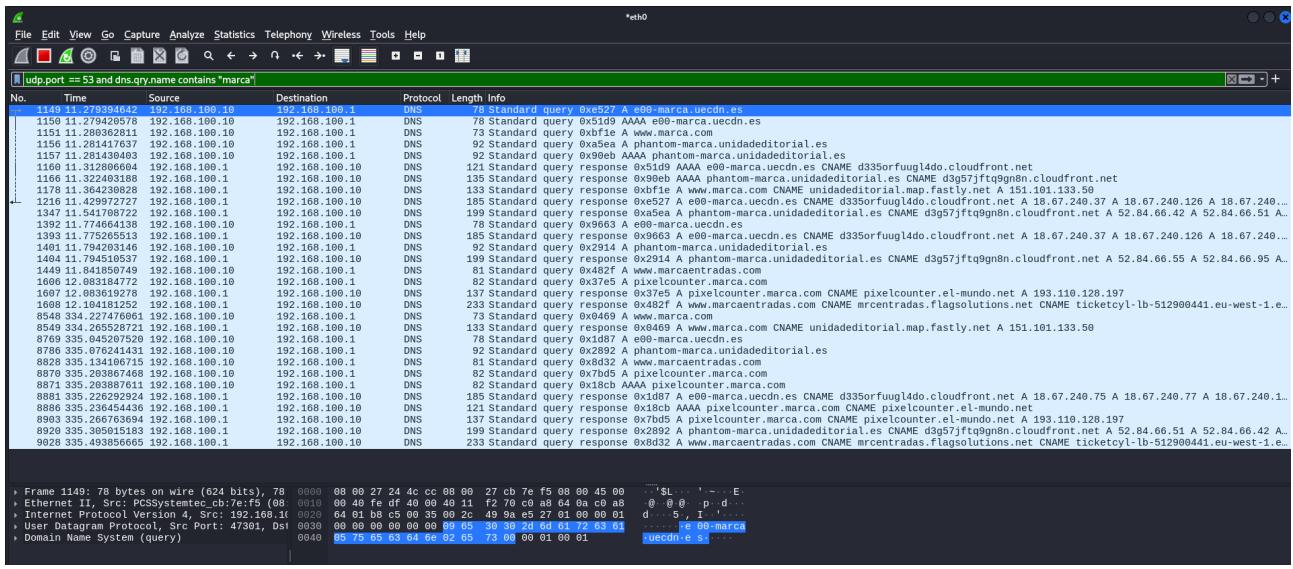
With your consent, we and our partners use cookies or similar technologies to store, access, and process personal data like your visit on this website. You can withdraw your consent or object to data processing based on legitimate interest at any time by clicking on "Learn more" or in our Cookie Policy on this website.

We and our partners process data for the following purposes Actively scan device characteristics for identification, Analizar su idoneidad para ofrecerle soluciones basadas en su red de telecomunicaciones, Create profiles for personalised advertising, Create profiles to personalise content, Develop and improve services, Enriching the profile with third-party information, Measure advertising performance, Measure content performance, Sharing your browsing analysis and interest groups with third parties, Storage and access to geolocation information for targeted advertising purposes, Storage and access to geolocation information to carry out marketing studies, Store and/or access information on a device, Understand audiences

y vemos el tráfico en wireshark con el filtro `tcp.port == 53 or udp.port == 53:`

No.	Time	Source	Destination	Protocol	Length	Info
6755	31.768267747	192.168.100.10	192.168.100.1	DNS	85	Standard query 0x0fc6 AAAA ade.googlesyndication.com
6756	31.781877552	192.168.100.1	192.168.100.10	DNS	142	Standard query response 0xfc6 AAAA ade.googlesyndication.com 60A ns1.google.com
6757	31.781877552	192.168.100.1	192.168.100.10	DNS	142	Standard query response 0xfc6 AAAA ade.googlesyndication.com 60A ns1.google.com
6986	53.431096757	192.168.100.10	192.168.100.1	DNS	74	Standard query 0xfdb5 A px.moatads.com
6987	53.431029269	192.168.100.10	192.168.100.1	DNS	74	Standard query 0x03b4 AAAA px.moatads.com
6988	53.494183169	192.168.100.1	192.168.100.10	DNS	212	Standard query response 0x03b4 AAAA px.moatads.com CNAME wildcard.moatads.com.edgekey.net CNAME e13136.g.akamaiedge.net SOA n0g.ak...
6989	53.515931864	192.168.100.1	192.168.100.10	DNS	170	Standard query response 0xf4b5 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net CNAME e13136.g.akamaiedge.net A 23.213.45.1...
7911	141.76599982	192.168.100.10	192.168.100.1	DNS	85	Standard query 0x03b4 AAAA ade.googlesyndication.com
7912	141.76599988	192.168.100.10	192.168.100.1	DNS	85	Standard query 0xc78e AAAA ade.googlesyndication.com
7915	141.783760971	192.168.100.1	192.168.100.10	DNS	101	Standard query response 0xd1b8 A ade.googlesyndication.com A 142.250.178.162
7922	141.855173945	192.168.100.1	192.168.100.10	DNS	142	Standard query response 0xc70e AAAA ade.googlesyndication.com SOA ns1.google.com

o con el filtro `udp.port == 53 and qry.name contains "marca"`



vemos todo el tráfico que interceptamos con pfsense hacia marca.com.

Configuramos el rang de ips en DHCP Server, desde la 192.168.100.100 hasta la 192.168.100.200 para conseguir la sured que hemos definido en el esquema, también configuramos un DNS secundario 1.1.1.1 y terciario 8.8.8.8 (google):

Ignore client identifiers		<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.	
Subnet	192.168.100.0	Subnet mask	255.255.255.0
Available range	192.168.100.1 - 192.168.100.254		
Range	192.168.100.100	From	192.168.100.200
Additional Pools			
Add	+ Add pool		
If additional pools of addresses are needed inside of this subnet outside of the above Range, they may be specified here.			
Pool Start	Pool End	Description	Actions
Servers			
WINS servers	WINS Server 1		
	WINS Server 2		
DNS servers	192.168.100.1		
	1.1.1.1		
	8.8.8.8		
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.			

así tendría configurada la red LAN

Configuración de DMZ y DMZ2:

Vamos a Interfaces – Assignments y añadimos, nos saldrán OPT1 y OPT2:

192.168.100.1/interfaces_assign.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTricks

pfSense COMMUNITY EDITION

Interfaces ▾

- Assignments
- WAN
- LAN
- OPT1
- OPT2

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIGs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:0d:10:27)
LAN	em1 (08:00:27:24:4c:cc)
OPT1	em2 (08:00:27:86:26:83)
OPT2	em3 (08:00:27:26:f7:bd)

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

192.168.100.1/interfaces.php?f=opt1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTricks

Interfaces / OPT1 (em2)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XXXX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
MTU	1500 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	1460 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP4 header size) and minus 60 for IPv6 (TCP/IP6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.200.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).

The screenshot shows the pfSense web interface at <http://192.168.100.1/interfaces.php?if=opt1>. The top navigation bar includes links for Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Maltego, Tails, Metasploitable2 - Linux, 10 Minute Mail - Free ..., https://dehashed.com/, and HackT. The main menu has options for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red banner at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Interfaces / DMZ (em2)" is shown. A yellow box contains the message: "The DMZ configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying." A green "Apply Changes" button is visible. Under the "General Configuration" section, the "Enable" checkbox is checked.

Configuramos la DMZ2:

The screenshot shows the pfSense web interface at <http://192.168.100.1/interfaces.php?if=opt2>. The top navigation bar and main menu are identical to the previous screenshot. The title "Interfaces / OPT2 (em3)" is shown. Under the "General Configuration" section, the "Enable" checkbox is checked. The "Description" field is set to "DMZ2". The "IPv4 Configuration Type" dropdown is set to "Static IPv4". The "IPv6 Configuration Type" dropdown is set to "None". The "MAC Address" field contains "XX:XX:XX:XX:XX:XX". The "MTU" field is empty. The "MSS" field is empty. The "Speed and Duplex" dropdown is set to "Default (no preference, typically autoselect)". Under the "Static IPv4 Configuration" section, the "IPv4 Address" is set to "192.168.250.1" and the subnet mask is "/24". The "IPv4 Upstream gateway" dropdown is set to "None" and contains a green "+ Add a new gateway" button. A note below the gateway field states: "If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the 'Add' button. On local area network interfaces the upstream gateway should be 'none'."

The screenshot shows the pfSense web interface at <http://192.168.100.1/interfaces.php?if=opt2>. The top navigation bar includes links for Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Maltego, Tails, Metasploitable2 - Linux, 10 Minute Mail - Free..., https://dehashed.com/, and others. The main menu has tabs for System, Interfaces (selected), Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message in a red box states: "WARNING: The 'admin' account has the same password as the root account. This is a security risk. Please change the password in the User Manager." Below this, the "Interfaces / DMZ2" section is selected. A green box at the bottom indicates: "The changes have been applied successfully." The "General Configuration" section contains fields for Enable (checked), Description (DMZ2), IPv4 Configuration Type (Static IPv4), IPv6 Configuration Type (None), and MAC Address (XXXXXX:XXXX:XXXX).

vamos a pfSense y comprobamos todas las redes configuradas:

The screenshot shows a terminal window titled "pfSense (Instantánea 1) [Corriendo] - Oracle VM VirtualBox". The menu bar includes Archivo, Máquina, Ver, Entrada, Dispositivos, and Ayuda. The terminal displays the following text:

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: d16b4b90899ec6066e97

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UTM ***

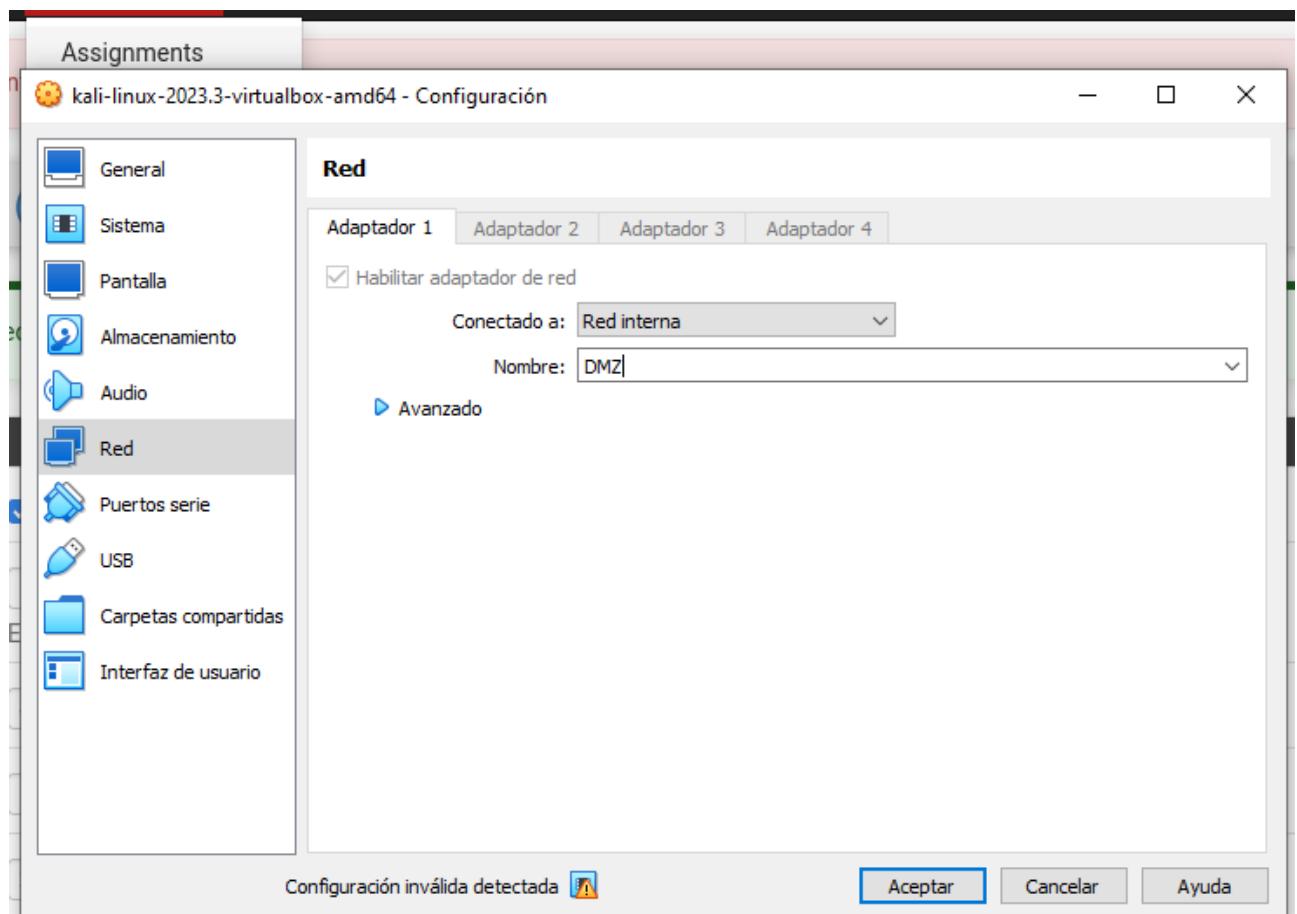
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.18/24
LAN (lan)      -> em1          -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2          -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3          -> v4: 192.168.250.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```

At the bottom right, there is a set of icons for file operations (New, Open, Save, etc.) and a key icon labeled "CTRL DERECHA".

vamos a la kali y cambiamos la red LAN a DMZ



desconectamos el adaptador de red de la kali, lo volvemos a conectar y comprobamos en cmd, que ha cambiado la ip:

```
(kali㉿kali)-[~]
$ ip a
Key Algorithm HMAC-SHA256 (current bind9 default)
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.100/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
            valid_lft 7101sec preferred_lft 7101sec
        inet6 fe80::cdf2:29d0:7fca:5c9c/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:05:32:65:47 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
Domain name: Domain search list: The DHCP Server can dynamically provide domain names to clients.
The DHCP Client will use the domain name provided by the server if it is available.

(kali㉿kali)-[~]
```

Para configurar las reglas, primero configuramos alias y puertos para el firewall

Creamos la reglas para DMZ

damos click en ADD

en Action lo dejamos en Pass para permitir el tráfico, y seleccionamos la DMZ, el protocolo TCP, en Source ponemos any (no me sale la opción DMZ subnets que es la más segura)

En Destination ponemos los puertos webs, que son el 443 y el 80, ponemos la Descripción de la regla: Salida tráfico web

192.168.0.18/firewall_rules_edit.php?if=opt1&after=-1

Protocol: TCP

Choose which IP protocol this rule should match.

Source

Source: any

Destination

Destination: any

Destination Port Range: (other) webs (other) webs

From: Custom To: Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: salida trafico web

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Save

hacemos click en Save y Apply changes

192.168.0.18/firewall_rules.php?if=opt1

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		salida trafico web	

Add **Up** **Down** **Delete** **Save** **Separator**

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		salida trafico web	

cambiamos a LAN en la kali, y comprobamos que tenemos acceso a internet:

REGLAS DMZ2:

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP	*	*	*	*	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		permitir trafico DNS	

ahora añadimos la regla del protocolo UDP:

The screenshot shows the 'Edit Firewall Rule' interface. The 'Action' dropdown is set to 'Pass'. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The 'Disabled' section has an unchecked checkbox for 'Disable this rule'. The 'Interface' is set to 'DMZ'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'UDP'. In the 'Source' section, the 'Source' dropdown is set to 'any'. The 'Destination' section shows 'Destination' set to 'any' and 'Destination Port Range' set to 'DNS (53)'. Under 'Extra Options', there is a 'Log' checkbox which is unchecked. A 'Description' field is present but empty. A 'Save' button is at the bottom.

en Destination elegimos DNS (53)

This screenshot shows the same 'Edit Firewall Rule' interface as above, but with more detailed configuration. The 'Protocol' dropdown is explicitly set to 'UDP'. In the 'Destination' section, the 'Destination Port Range' dropdown is set to 'DNS (53)' with 'From' and 'To' fields both set to 'Custom'. Below the destination section, a note says: 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.' The 'Extra Options' section includes a 'Log' checkbox (unchecked), a 'Description' field (empty), and an 'Advanced Options' section with a 'Display Advanced' button. A 'Save' button is at the bottom.

en Descripción, ponemos permitir tráfico DNS, damos a Save y Apply changes:

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		permitir trafico DNS	
0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		salida trafico web	

volvemos a entrar a PfSense y comprobamos las reglas creadas, es importante el orden:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
6 / 48 KIB	IPv4 UDP	*	*	*	53 (DNS)	*	none		permitir trafico DNS	
121 / 3.80 MiB	IPv4 TCP	*	*	*	webs	*	none		salida trafico web	

Creamos las reglas de DMZ2

Hacemos click en Add

The screenshot shows the pfSense Firewall Rules Edit page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Edit Firewall Rule" section is displayed. It includes fields for Action (Pass), Disabled (unchecked), Interface (DMZ2), Address Family (IPv4), and Protocol (TCP). Under the Source section, the Source field is set to "any". The Destination section shows Destination Port Range from "(other)" to "webs". In the Extra Options section, the Log checkbox is unchecked. A "Save" button is located at the bottom right.

This screenshot shows the same pfSense Firewall Rules Edit page, but with different configurations. The Action is now set to "Block". The Source field is set to "any". The Destination section shows Destination Port Range from "Custom" to "Custom" with "webs" selected. In the Extra Options section, the Log checkbox is checked. A "Save" button is located at the bottom right.

Hacemos click en Save y Apply changes:

192.168.0.18/firewall_rules.php?if=opt2

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTr...

pisense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN DMZ **DMZ2**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none			

Add Add Delete Save Separator

192.168.0.18/firewall_rules_edit.php?if=opt2&after=-1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTr...

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ2

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: UDP

Choose which IP protocol this rule should match.

Source

Source: Invert match any Source Address /

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination: Invert match any Destination Address /

Destination Port Range: DNS (53) From Custom To Custom

The screenshot shows the 'Edit Firewall Rule' page in pfSense. The rule is configured to 'Pass' (Action), 'Disabled' (Disabled), 'DMZ2' (Interface), 'IPv4' (Address Family), 'ICMP' (Protocol), and 'any' (ICMP Subtypes). The source is set to 'any'. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.'

mapeamos una IP estática:

The screenshot shows the 'Edit Static Mapping' page in pfSense. The mapping is for MAC address 08:00:27:cb:7e:f5, IP address 192.168.100.99, and hostname 'kali'. The 'Create an ARP Table Static Entry for this MAC & IP Address pair' checkbox is checked. The WINS servers are set to 'WINS 1' and 'WINS 2'. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.'

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none			

cambiamos el orden, ponemos la más restrictiva arriba:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			

Crearemos una regla para que todo el tráfico que nos llegue a nuestro puerto 80, es decir la red WAN, nos redirija a nuestra red LAN:

192.168.200.1/firewall_nat_edit.php?after=-1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ Help

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule			
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.			
Interface	WAN			
Choose which interface this rule applies to. In most cases "WAN" is specified.				
Address Family	IPv4			
Select the Internet Protocol version this rule applies to.				
Protocol	TCP			
Choose which protocol this rule should match. In most cases "TCP" is specified.				
Source	Display Advanced			
Destination	<input type="checkbox"/> Invert match.	WAN address	Type	Address/mask
Destination port range	Other	80	Other	80
From port Custom To port Custom				
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.				
Redirect target IP	Single host	192.168.100.99		
Type		Address		
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)				
Redirect target port	Other	80	Custom	
Port				

192.168.200.1/firewall_nat.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ Help

disense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor](#) the filter reload progress.

Port Forward 1:1 Outbound NPt

Actions	NAT Ports	NAT IP	Dest. Ports	Dest. Address	Source Ports	Source Address	Protocol	Interface	Selected
Edit Delete Save Separator	80 (HTTP)	192.168.100.99	80 (HTTP)	WAN address	*	*	TCP	WAN	<input checked="" type="checkbox"/>

Legend

- ▶ Pass
- ☒ Linked rule

REGLAS WAN:

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 0 B	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none		NAT Regla apache server	

Add Add Delete Save Separator

REGLAS LAN:

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 14 / 1.35 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

comprobamos el cambio de ip

```

root@kali:~# ifconfig
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.99/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 7196sec preferred_lft 7196sec
    inet6 fe80::cdf2:29d0:7fca:5c9c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:05:32:65:47 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
        Subnet mask 255.255.255.0

```

(kali㉿kali)-[~]

\$

levantamos el servidor APACHE:

```
(kali㉿kali)-[~]
$ service apache2 start
Failed to start apache2.service: Connection timed out
See system logs and 'systemctl status apache2.service' for details.

(kali㉿kali)-[~]
$ sudo service apache2 start
[sudo] password for kali:

(kali㉿kali)-[~]
$
```

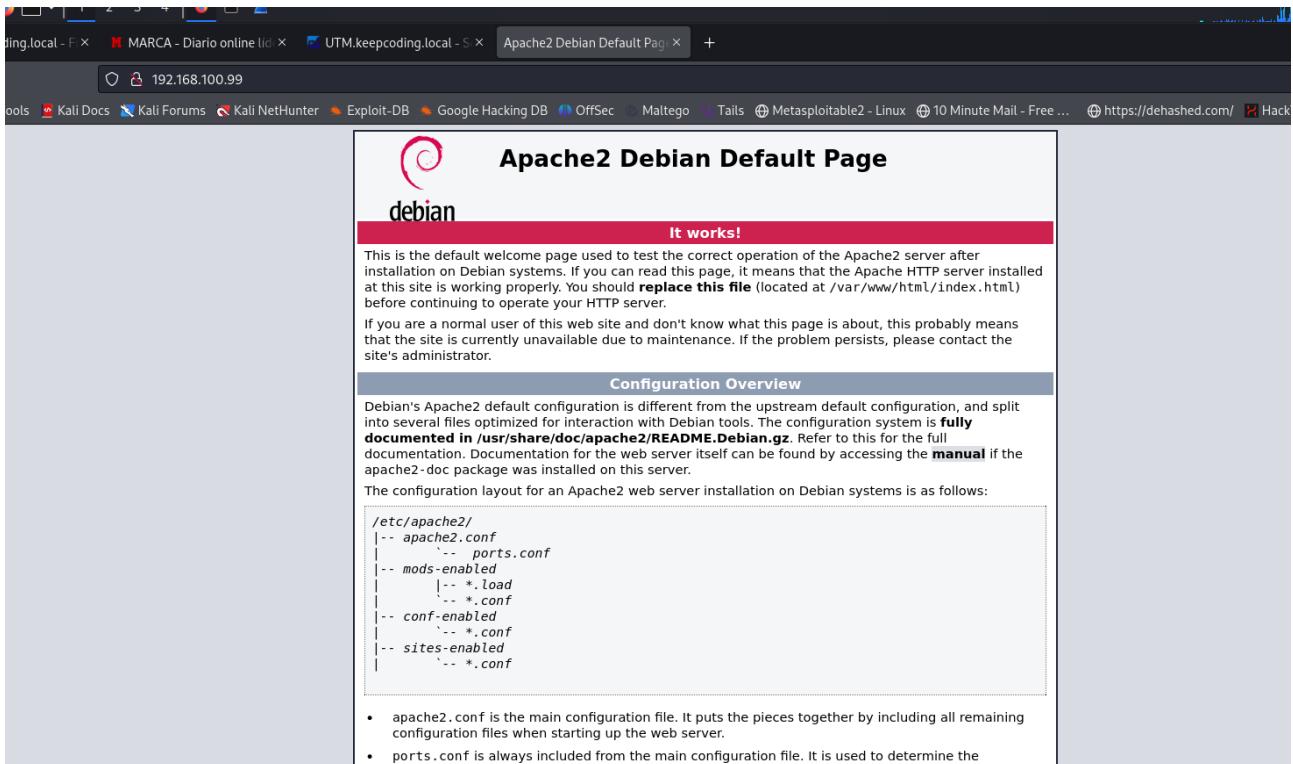
y comprobamos que está levantado el servidor:

```
(kali㉿kali)-[~]
$ sudo service apache2 status
* Apache2 - The Apache HTTP Server
  * Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
    Active: active (running) since Sat 2024-03-16 09:49:14 EDT; 1min 17s ago
      Docs: https://httpd.apache.org/docs/2.4/
  Process: 99091 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 99107 (apache2)
   Tasks: 8 (limit: 13937)
  Memory: 10.4M (peak: 20.2M)
     CPU: 70ms
    CGroup: /system.slice/apache2.service
            └─99107 /usr/sbin/apache2 -k start
                ├─99110 /usr/sbin/apache2 -k start
                ├─99111 /usr/sbin/apache2 -k start
                ├─99112 /usr/sbin/apache2 -k start
                ├─99113 /usr/sbin/apache2 -k start
                ├─99114 /usr/sbin/apache2 -k start
                └─99115 /usr/sbin/apache2 -k start

Mar 16 09:49:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 16 09:49:14 kali apachectl[99106]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Mar 16 09:49:14 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(kali㉿kali)-[~]
```

y comprobamos que se levanta en la ip 192.168.100.99



ahora sí accedemos desde nuestra máquina a la ip del servidor apache

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should [replace this file](#) (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|   |-- mods-enabled
|       |-- Load
|       |-- *.conf
|   |-- conf-enabled
|       |-- *.conf
|   |-- sites-enabled
|       |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/`, and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, and `a2dissite`.

Creamos ahora la VPN, nos vamos a System / Package Manager / Available Packages

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Package Manager / Available Packages

Installed Packages Available Packages

Name	Version	Description	Action
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install

instalamos el openvpn-client-export

Open-VM-Tools	10.1.0_5.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	+ Install
Package Dependencies:			
openvm-tools-12.3.5.2			
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install
Package Dependencies:			
openvpn-client-export-2.6.7 openvpn-2.6.4 zip-3.0_1 7-zip-22.01			
pfBlockerNG	3.2.0_6	Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IORisk IP Reputation Threat Sources.	+ Install

me da error al intentar instalar la vpn

The screenshot shows a browser window with the URL `192.168.200.1/pkg_mgr_install.php`. The page is titled "System / Package Manager / Package Installer". A red warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, another message says: "pfSense-pkg-openvpn-client-export installation failed!". At the bottom, there are tabs for "Installed Packages", "Available Packages", and "Package Installer", with "Package Installer" being the active tab. A sidebar on the left is titled "Package Installation" with a warning: "WARNING: Current pkg repository has a new PHP major version. pfSense should be upgraded before installing any new package.".

Lanzamos en nuestra kali el honeypot Cowrie con el comando:

```
docker run -p 2222:2222 cowrie/cowrie
```

The screenshot shows a terminal window on Kali Linux with the title "kali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

```
(kali㉿kali)-[~] $ docker run -p 2222:2222 cowrie/cowrie
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: CAST5 has been deprecated
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning: CAST5 has been deprecated
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
2024-03-16T16:06:37+0000 [-] Python Version 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0]
2024-03-16T16:06:37+0000 [-] Twisted Version 23.10.0
2024-03-16T16:06:37+0000 [-] Cowrie Version 2.5.0
2024-03-16T16:06:37+0000 [-] Loaded output engine: jsonlog
2024-03-16T16:06:37+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 23.10.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2024-03-16T16:06:37+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2024-03-16T16:06:37+0000 [-] CowrieSSHFactory starting on 2222
2024-03-16T16:06:37+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7fc700b0c350>
2024-03-16T16:06:37+0000 [-] Generating new RSA keypair ...
2024-03-16T16:06:37+0000 [-] Generating new ECDSA keypair ...
2024-03-16T16:06:37+0000 [-] Generating new ed25519 keypair ...
2024-03-16T16:06:37+0000 [-] Ready to accept SSH connections
```

A red warning message at the bottom of the terminal window reads: "WARNING: Current pkg repository has a new PHP major version. pfSense should be upgraded before installing any new package."

se quedará listo para aceptar conexiones.

Con el siguiente comando corremos el amazedostrich:

```
docker run -p 333:3389 amazedostrich/rdpy
```

Hago un docker ps para ver las imágenes docker en ejecución:

```
(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE           COMMAND          CREATED         STATUS          PORTS
d1fab0c055ad   amazedorstrich/rdpy   "/bin/sh -c '/usr/bi..."  14 minutes ago   Up 14 minutes   0.0.0.0:333→3389/tcp
, ::333→3389/tcp
crazy_vaughan
9b9cb5e1f707   cowrie/cowrie       "/cowrie/cowrie-env/..."  41 minutes ago   Up 41 minutes   0.0.0.0:2222→2222/tcp
, ::2222→2222/tcp, 2223/tcp
eager_elgamal

(kali㉿kali)-[~]
└─$
```

con este comando nos abrirá una terminal dentro del docker:

```
(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE           COMMAND          CREATED
 NAMES
d1fab0c055ad   amazedorstrich/rdpy   "/bin/sh -c '/usr/bi..."  21 minutes ago
crazy_vaughan
9b9cb5e1f707   cowrie/cowrie       "/cowrie/cowrie-env/..."  49 minutes ago
eager_elgamal

(kali㉿kali)-[~]
└─$ docker exec -it -u 0 d1fab0c055ad /bin/bash
bash-4.4#
```

con este comando iremos a los logs del honeypot

```
bash-4.4# ls
bin  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
bash-4.4# cd rdp
bash: cd: rdp: No such file or directory
bash-4.4# cd /var/log
bash-4.4# ls
rdpy
bash-4.4# cd rdp
bash-4.4# ls
rdpy.log
bash-4.4#
```

con el comando tail -f rdp.log vemos los logs del honeypot

```
[1]+  Stopped                  tail -f rdp.log
bash-4.4# tail -f rdp.log
[*] INFO:      Build size map
[*] INFO:      (1024, 800) → /home/rdpy/1
[*] INFO:      (800, 600) → /home/rdpy/2
[*] INFO:      (800, 600) → /home/rdpy/3

```

lanzo el siguiente comando para recoger en el archivo cowrie.log, los logs del honeypot en el contenedor de docker:

```
(kali㉿kali)-[~] $ docker run -p 222:2222 cowrie/cowrie > cowrie.log
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg. seconds
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
<cowrie.ssh.factory.CowrieSSHFactory object at 0x7f3f836c9610>
(kali㉿kali)-[~] $ [06+0000 [-] Main loop terminated.
$ [06+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] Stopping factory
<cowrie.ssh.factory.CowrieSSHFactory object at 0x7f3f836c9610>
[06+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] Server Shut Down.
```

en la siguiente pantalla muestro el archivo cowrie.log, donde se guardan los logs:

```
39 2024-06-05T12:22:04+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
40 2024-06-05T12:22:04+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
41 2024-06-05T12:22:04+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
42 2024-06-05T12:22:04+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-
  sessions@openssh.com' request
43 2024-06-05T12:22:04+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120,
  640, 480)
44 2024-06-05T12:22:04+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,
  1,10.0.2.100] Terminal Size: 120 30
45 2024-06-05T12:22:04+0000 [twisted.conch.ssh.session#info] Getting shell
46 2024-06-05T12:22:06+0000 [HoneyPotSSHTransport,1,10.0.2.100] CMD: ls
47 2024-06-05T12:22:06+0000 [HoneyPotSSHTransport,1,10.0.2.100] Command found: ls
48 2024-06-05T12:22:08+0000 [HoneyPotSSHTransport,1,10.0.2.100] CMD: pwd
49 2024-06-05T12:22:08+0000 [HoneyPotSSHTransport,1,10.0.2.100] Command found: pwd
50 2024-06-05T12:22:13+0000 [HoneyPotSSHTransport,1,10.0.2.100] CMD: otro comando
51 2024-06-05T12:22:13+0000 [HoneyPotSSHTransport,1,10.0.2.100] Can't find command otro
52 2024-06-05T12:22:13+0000 [HoneyPotSSHTransport,1,10.0.2.100] Command not found: otro comando
53 2024-06-05T12:25:04+0000 [-] Timeout reached in HoneyPotSSHTransport
54 2024-06-05T12:25:04+0000 [twisted.conch.ssh.session#info] exitCode: 1
55 2024-06-05T12:25:04+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] sending request b'exit-status'
56 2024-06-05T12:25:04+0000 [-] Closing TTY Log: var/lib/cowrie/tty/
  47894536c764d438174bc2f40e3667fea87c278723fad7b4647af416d20a79c7 after 180 seconds
57 2024-06-05T12:25:04+0000 [cowrie.ssh.connection.CowrieSSHConnection#info] sending close 0
58 2024-06-05T12:25:04+0000 [HoneyPotSSHTransport,1,10.0.2.100] avatar root logging out
59 2024-06-05T12:25:04+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
60 2024-06-05T12:25:04+0000 [HoneyPotSSHTransport,1,10.0.2.100] Connection lost after 185 seconds
61 2024-06-05T12:28:06+0000 [-] Received SIGTERM, shutting down.
62 2024-06-05T12:28:06+0000 [-] (TCP Port 2222 Closed)
63 2024-06-05T12:28:06+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Stopping factory
  <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f3f836c9610>
64 2024-06-05T12:28:06+0000 [-] Main loop terminated.
65 2024-06-05T12:28:06+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] Server Shut Down.
66
```

Añadimos los logs a Elastic con “Custom Logs” :

Add Custom Logs integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: log honeypot

Description: logs del honeypot

Custom log file

Log file path: /home/kali/cowrie.log

Dataset name: cowrie

Dataset name description: Set the name for your dataset. Changing the dataset will send the data to a different index. You can't use - in the name of a dataset and only valid characters for Elasticsearch index names.

Save and continue

vemos los logs en Elastic

Discover

honey1

Filter your data using KQL syntax

Jun 5, 2024 @ 14:28:00.000 → Jun 5, 2024 @ 14:29:00.000

Auto interval: No breakdown

Available fields: @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, data_stream.dataset, data_stream.namespace, data_stream.type, ecs.version, elastic.agent.id, elastic.agent.snapshot, elastic.agent.version, event.agent_id_status, event.dataset, event.ingested, host.architecture, host.containerized, host.hostname, host.id

Documents (5) Field statistics

Document

```

{
    "@timestamp": "2024-06-05T14:28:05.500Z",
    "agent": {
        "name": "kali",
        "type": "filebeat"
    },
    "data_stream": {
        "dataset": "generic"
    },
    "log": {
        "file": {
            "path": "/home/kali/cowrie.log"
        }
    },
    "agent": {
        "ephemeral_id": "f2cbd87b-d428-4a58-aa22-cb77faa1a85"
    }
}

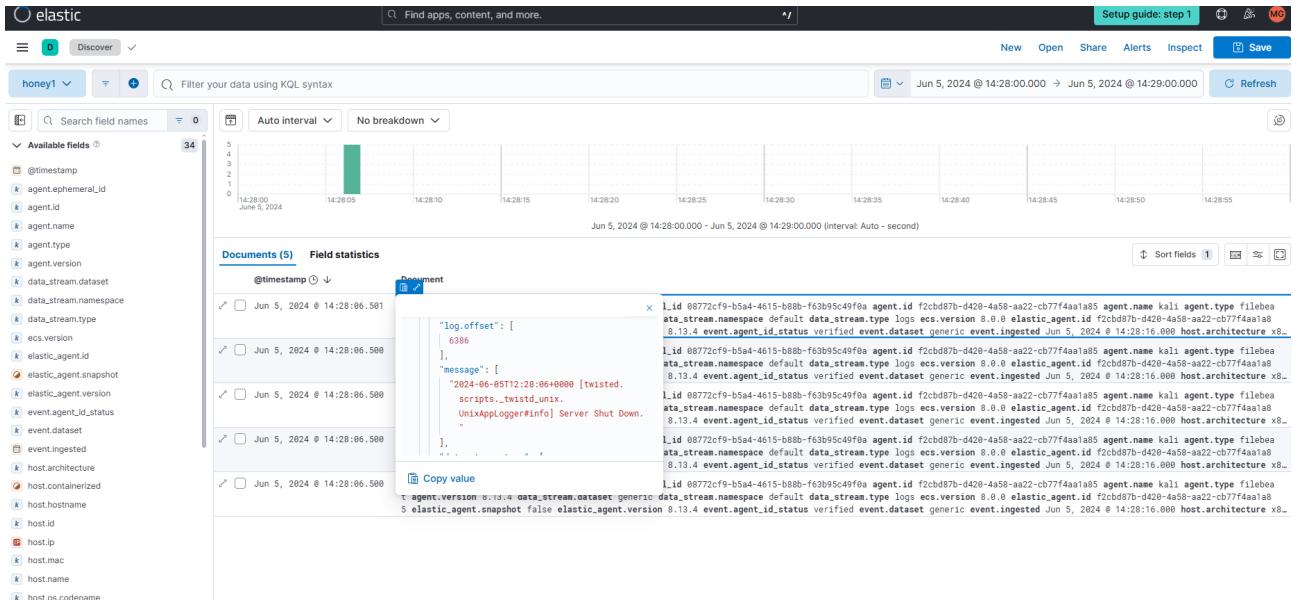
```

Copy value

```

{
    "@timestamp": "2024-06-05T14:28:06.500Z",
    "agent": {
        "name": "kali",
        "type": "filebeat"
    },
    "data_stream": {
        "dataset": "generic"
    },
    "log": {
        "file": {
            "path": "/home/kali/cowrie.log"
        }
    },
    "agent": {
        "ephemeral_id": "f2cbd87b-d428-4a58-aa22-cb77faa1a85"
    }
}

```



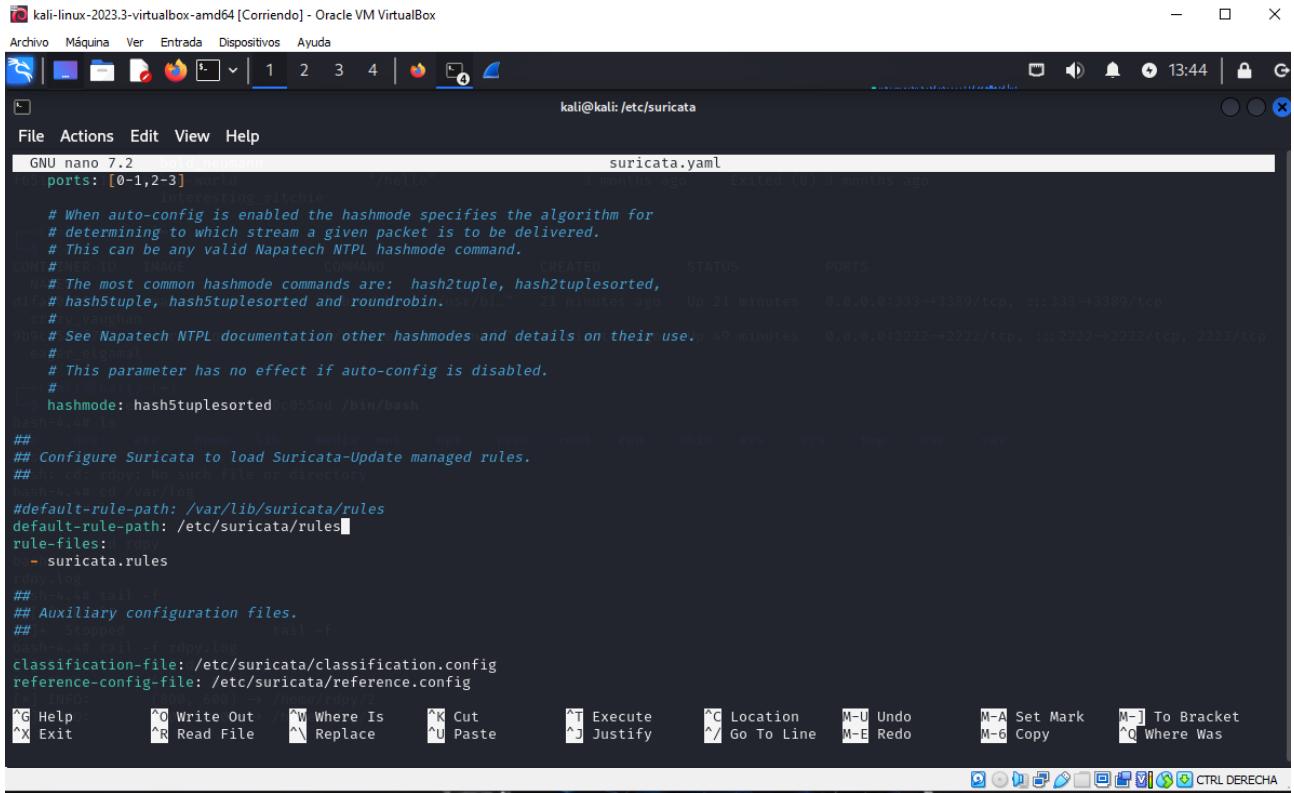
Creamos la regla para suricata

```
kali㉿kali: /etc/suricata/rules
File Actions Edit View Help
GNU nano 7.2 suricata.rules
alert tcp any any → any any (msg:"Trafico detectado"; sid:1; priority:1;)
133Fd37e275 festive_dijkstra
cowrie/cowrie "/cowrie/cowrie-env/_" 11 days ago Created
c54fb701bb5a cowrie/cowrie "/cowrie/cowrie-env/_" 11 days ago Exited (0) 11 days ago
c2c6fdcc3eaf webgoat/webgoat-desktop "/init"
bold_neumann
65155932a11 hello-world "/hello"
interesting_ritchie

--(kali㉿kali)-[~]
$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
 NAMES
df1ab0c055ad amazdedostrich/rdpv "/bin/sh -c '/usr/bi..." 21 minutes ago Up 21 minutes 0.0.0.0:333→3389/tcp, :::333→3389/tcp
_crazy_vaughan
0b9cb8e1707 cowrie/cowrie "/cowrie/cowrie-env/_" 49 minutes ago Up 49 minutes 0.0.0.0:2222→2222/tcp, :::2222→2222/tcp, 2222/tcp
eager_elgammal

--(kali㉿kali)-[~]
$ docker exec -it df1ab0c055ad /bin/bash
bash-4.4# ls
bin dev etc home lib media mnt opt proc root run sbin srv sys tmp user var
bash-4.4# cd rdpv
bash-4.4# cd rdpv
bash: cd: rdpv: No such file or directory
bash-4.4# cd /var/log
bash-4.4# ls
rdpy
bash-4.4# cd rdpy
bash-4.4# ls
rdpy.log
bash-4.4# tail -f
[[A'H'H'H'Z
1]+ Stopped tail -f
bash-5.4# tail -f rdpy.log
[*] INFO: Build size map
[*] INFO: (1024, 600) → /home/rdpy/1
[*] INFO: (800, 600) → /home/rdpy/2
[*] INFO: [ File 'suricata.rules' is unwritable ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-J To Bracket
^X Exit ^R Read File ^R Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-B Copy ^Q Where Was
```

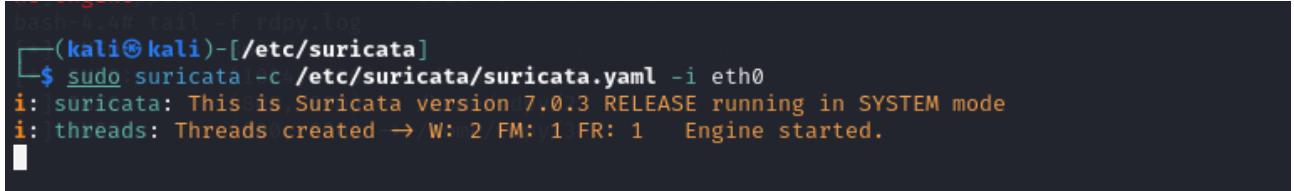
en el archivo suricata.yaml, cambiamos lo siguiente:



```
GNU nano 7.2                               suricata.yaml
--- ports: [0-1,2-3]                         3 months ago   Exited (0) 3 months ago
# When auto-config is enabled the hashmode specifies the algorithm for
# determining to which stream a given packet is to be delivered.
# This can be any valid Napatech NTPL hashmode command.
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
# The most common hashmode commands are: hash2tuple, hash2tuplesorted,
# hash5tuple, hash5tuplesorted and roundrobin. $ ./01... 21 minutes ago Up 21 minutes 0.0.0.0:333→3389/tcp, :::333→3389/tcp
# See Napatech NTPL documentation other hashmodes and details on their use. 49 minutes ago 0.0.0.0:2222→2222/tcp, :::2222→2222/tcp, 2223/tcp
# This parameter has no effect if auto-config is disabled.
# hashmode: hash2tuple
hashmode: hash5tuplesorted$055ad /bin/bash
hash-4:~# ls
## Configuration files.
## Configure Suricata to load Suricata-Update managed rules.
## cat rdp.log: No such file or directory
## bash>cd /var/log
#default-rule-path: /var/lib/suricata/rules
default-rule-path: /etc/suricata/rules
rule-files: d rdp
- suricata.rules
copy log
## head -n tail -f
## Auxiliary configuration files.
## tail -f
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
[+ INFO]: (800, 600) → /home/rdpy/2
^G Help      ^O Write Out    ^W Where Is    ^X Cut          ^T Execute      ^C Location     M-U Undo      M-A Set Mark    M-] To Bracket
^X Exit      ^R Read File    ^A Replace     ^U Paste        ^J Justify      ^Y Go To Line   M-E Redo      M-6 Copy       ^Q Where Was
```

para que nos coja por defecto el archivo suricata.rules que hemos creado

ejecutamos Suricata:



```
bash-4.4# tail -f rdp.log
[(kali㉿kali)-[/etc/suricata]]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 / FM: y13 FR: 1   Engine started.
```

vemos los logs:

se me peta windows 11 y no puedo hacer nada con él

ELASTIC CLOUD

Welcome to Elastic Cloud

Hosted deployments

Deployment	Status	Version	Cloud provider & region	Actions
Mik	Healthy	8.12.2	GCP - Iowa (us-central1)	Open Manage

Support

New to Elastic? Check out our step-by-step [getting started resources](#). For advanced guidance, see our [documentation](#).

[Contact support](#)

Training

Get started with our free training

Build essential skills and learn Elastic with free introductory training in the Elastic Learning Portal

[Elastic Learning Portal](#)

News

Switching from the Java High Level Rest Client to the new Java API Client MARCH 14, 2024 [New!](#)

Modernizing financial services: A deep dive into Elastic Cloud on AWS for Observability, Security, and more MARCH 8, 2024 [New!](#)

Machine learning vs. AI: Understanding the differences MARCH 7, 2024 [New!](#)

Community

Join an ElasticON event Hear success stories, lessons learned, tips, tricks, best practices, and funny anecdotes from Elastic experts from...

Real-World AI & ML in E-commerce with Elastic MARCH 20, 10:00

vamos a Management – Integrations

Welcome home

Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[Setup guides](#) [Add integrations](#) [Try sample data](#) [Upload a file](#)

Management

[Dev Tools](#) [Stack Management](#)

Find apps, content, and more.

[Live Chat](#) [Setup guide: step 1](#)

Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) [Installed integrations](#)

All categories 368

Search for integrations

Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

APM
Collect performance metrics from your applications with Elastic APM.

1Password
Collect logs from 1Password with Elastic Agent.

AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

ActiveMQ
Collect logs and metrics from ActiveMQ instances with Elastic Agent.

y luego a Elastic Defend

The screenshot shows the 'Elastic Defend' integration page in the Elastic Cloud interface. The top navigation bar includes links like 'KeepCoding Online', 'My Vaughan - Inicia...', 'Discord', 'Hex to Base64: Enc...', 'KeepCodingCiber7 ...', 'Fork - CyberChef', 'Software Clases de...', 'Formulario Entrega...', 'Iniciar reunión - Zo...', 'criptografia/codigo...', 'ChatGPT', 'Live Chat', and 'Setup guide: step'. A search bar at the top right contains the placeholder 'Find apps, content, and more.' Below the header, there's a sidebar titled 'Elastic Defend Integrations' with sections for 'Compatibility' (Windows, macOS, Linux) and 'Logs' (alerts, file, library, network, process, registry, security). The main content area has a title 'Elastic Defend' with a version of '8.12.0' and 'Agent policies 0'. It features tabs for 'Overview' (selected), 'Integration policies', 'Assets', 'Settings', 'Configs', and 'Advanced'. The 'Overview' tab displays the 'Elastic Defend Integration' section, which describes the product's capabilities for prevention, detection, and response across various operating systems. It lists several key features: Prevent complex attacks, Alert in high fidelity, Detect threats in high fidelity, Triage and respond rapidly, and Secure your cloud workloads. To the right of this section is a 'Requirements' table and a 'Details' table. The 'Requirements' table includes 'Permissions' (root privileges). The 'Details' table provides information about the integration, such as its category (EDR/XDR, Security), Elasticsearch assets (Index templates 2, Transform 2, Ingest pipelines 1, Log pipelines 5), features (logs, metrics), subscription (basic), developer (Elastic), license (LICENSE.txt), and changelog (View Changelog).

instalamos el agente en la kali, copiando el script:

Find apps, content, and more.

Elastic Defend > Add integration

Set up Elastic Defend integration

Install Elastic Agent Add the integration Confirm incoming data

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#).

1 **Install Elastic Agent on your host**

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.2-linux-x86_64
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=UTg4ZUdvNEJD...U5jTE80cmtkUVA6ZWV3Nkc5MXJRM...TNGE3N1k2QVphdw=
```

Copy to clipboard

2 **Confirm agent enrollment**

```
(kali㉿kali)-[~]
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=UTg4ZUdvNEJD...U5jTE80cmtkUVA6ZWV3Nkc5MXJRM...TNGE3N1k2QVphdw=
```

kali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

The Wireshark Analyze File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help

```
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/tomcat.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/traefik.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/uwsgi.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/vsphere.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/windows.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zeek.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zookeeper.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zoom.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zscaler.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.http.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.icmp.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.tcp.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquery-extension.ext
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osqueryd
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent.spec.yml
elastic-agent-8.12.2-linux-x86_64/.elastic-agent.active.commit
elastic-agent-8.12.2-linux-x86_64/.elastic-agent
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:
```

No Packets

instalado el agente:

```

kali@kali: ~/elastic-agent-8.12.2-linux-x86_64
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osqueryd
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/elastic-agent
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/package.version
elastic-agent-8.12.2-linux-x86_64/.elastic-agent.active.commit
elastic-agent-8.12.2-linux-x86_64/elastic-agent
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
[ =] Service Started [34s] Elastic Agent successfully installed, starting enrollment.
[   ] Waiting For Enroll ... [35s] {"log.level": "info", "@timestamp": "2024-03-17T07:52:22.521-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 496}, "message": "Starting enrollment to URL: https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0"}
[   ] Waiting For Enroll ... [37s] {"log.level": "info", "@timestamp": "2024-03-17T07:52:25.065-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 461}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2024-03-17T07:52:25.067-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 285}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
[ =] Done [37s] User's Guide | Wiki | Questions and Answers | Mailing Lists | SharkFest | Wireshark Discord | Donate
Elastic Agent has been successfully installed.

```

(kali㉿kali)-[~/elastic-agent-8.12.2-linux-x86_64]

No Packets

Profile: Default

damos en Add the itegration

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#).

Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

[Linux Tar](#) [Mac](#) [Windows](#) [RPM](#) [DEB](#) [Kubernetes](#)

```

curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-cent

```

Copied

Agent enrollment confirmed

✓ 1 agent has been enrolled.

Go back

Add the integration

Set up Elastic Defend integration

Install Elastic Agent Add the integration Confirm incoming data

We'll save your integration with our recommended defaults.



✓ Windows, macOS, and Linux event collection

You can edit these settings later in the Elastic Defend integration policy. [Learn more](#)

Go back

Confirm incoming data

aquí vemos los logs que vienen de kali:

Set up Elastic Defend integration

Install Elastic Agent Add the integration Confirm incoming data

✓ Incoming data received from 1 enrolled agent.

Preview of incoming data:

```

Mar 17, 2024 @ 12:52:27.183 container.id: "elastic-agent-de80bb" agent.name: "kali" agent.type: "filebeat"
t" agent.version: "8.12.2" log.file.inode: "3066218" log.file.path: "/opt/Elastic/Age
nt/data/elastic-agent-de80bb/logs/elastic-agent-watcher-20240317.ndjson"
n" log.file.device_id: "2049" log.offset: 0 elastic_agent.version: "8.12.
2" elastic_agent.snapshot: false process.pid: 7347 message: "Upgrade Watcher starte
d" input.type: "filestream" log.origin.file.line: 67 log.origin.file.name: "cmd/watc
h.go" ecs.version: "8.0.0" data_stream.type: "logs" data_stream.dataset: "elastic_ag
ent"
Mar 17, 2024 @ 12:52:22.829 container.id: "elastic-agent-de80bb" agent.name: "kali" agent.type: "filebeat
t" agent.version: "8.12.2" log.file.inode: "3066198" log.file.path: "/opt/Elastic/Age
nt/data/elastic-agent-de80bb/logs/elastic-agent-watcher-20240317.ndjson"
n" log.file.device_id: "2049" log.offset: 0 log.source: "elastic-ag
ent" elastic_agent.version: "8.12.2" elastic_agent.snapshot: false process.pid: 7166
message: "Elastic Agent started" input.type: "filestream" log.origin.file.line: 157
log.origin.file.name: "cmd/run.go" ecs.version: "8.0.0" data_stream.type: "log"
Mar 17, 2024 @ 12:52:27.183 container.id: "elastic-agent-de80bb" agent.name: "kali" agent.type: "filebeat
t" agent.version: "8.12.2" log.file.inode: "3066218" log.file.path: "/opt/Elastic/Age
nt/data/elastic-agent-de80bb/logs/elastic-agent-watcher-20240317.ndjson"
n" log.file.device_id: "2049" log.offset: 220 elastic_agent.version: "8.12.
2" elastic_agent.snapshot: false message: "update marker not present at '/opt/Elasti
cAgent/data'" input.type: "filestream" log.origin.file.line: 75

```

Add another integration View assets

damos click a ver assets (ver activos)

nos vamos a Fleet para ver las políticas, que son las reglas para recoger los logs:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	My first agent policy rev. 2	0.27 %	26 MB	17 seconds ago	8.12.2	...
Healthy	57d606d90412	Elastic Cloud agent policy rev. 5	N/A	N/A	24 seconds ago	8.12.2	...

podemos integrar Suricata para recoger los logs de Suricata.

elastic

Find apps, content, and more.

Live Chat Setup guides Send feedback M

Integrations > Suricata > Add integration

Add Suricata integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: Suricata-1

Description: logs de suricata

Namespace: default

Change the default namespace inherited from the selected Agent policy. This setting changes the name of the integration's data stream. [Learn more](#)

Data retention settings

By default all logs and metrics data are stored on the hot tier. [Learn more](#) about changing the data retention policy for this integration.

Collect Suricata eve logs (input: logfile) Change defaults

Suricata eve logs (log)

Paths: /var/log/suricata/eve.json

Cancel Preview API request Save and continue

The screenshot shows the 'Add Suricata integration' configuration page in the Elastic Stack interface. It includes fields for 'Integration name' (Suricata-1), 'Description' (logs de suricata), 'Namespace' (default), and 'Data retention settings'. Under 'Log collection', it shows 'Suricata eve logs (log)' with a path of '/var/log/suricata/eve.json'. At the bottom, there are 'Cancel', 'Preview API request', and 'Save and continue' buttons. A large black rectangular redaction box covers the bottom portion of the page content.

The screenshot shows the 'Suricata' integration page in the Elastic Stack interface. At the top, there's a navigation bar with the Elastic logo, a search bar, and links for 'Live Chat' and 'Setup guide: step'. Below the navigation is a breadcrumb trail: 'Integrations > Suricata'. The main content area has a title 'Suricata' with a logo, a version '2.21.0' indicator, and a 'Add Suricata' button. A 'Suricata Integration' section contains tabs for 'Overview', 'Settings', 'Configs', and 'API reference'. The 'Overview' tab is selected, showing a brief description of the integration for Suricata, its compatibility with v4.0.4, and an example event JSON. To the right, there are 'Screenshots' and 'Details' sections.

This screenshot shows the 'Add Suricata integration' configuration dialog. It includes a 'Cancel' button, a title 'Add Suricata integration', and a 'Configure an integration for the selected agent policy' message. It lists two agent policies: 'Agent policy' and 'Agent policy 2'. A 'Configure integration' step is shown with a sub-dialog titled 'Suricata integration added'. This sub-dialog instructs the user to add an Elastic Agent to their hosts. It features a 'Collect Suricata eve logs (input: logfile)' checkbox (which is checked), a 'Paths' field containing '/var/log/suricata/eve.json', and a 'Preserve original event' option. Buttons for 'Add Elastic Agent later' and 'Add Elastic Agent to your hosts' are present. The background of the main dialog shows the configuration options for the integration.

The screenshot shows the 'Suricata' integration management page. It features a navigation bar with the Elastic logo, a search bar, and links for 'Live Chat' and 'Setup guide: step 1'. Below the navigation is a breadcrumb trail: 'Integrations > Suricata'. The main content area has a title 'Suricata' with a logo, a version '2.21.0' indicator, and a 'Add Suricata' button. A 'Integration policies' section contains tabs for 'Overview', 'Integration policies', 'Assets', 'Settings', 'Configs', and 'API reference'. The 'Integration policies' tab is selected, showing a table with one row: 'suricata-1' (Version v2.21.0, Agent policy rev. 2, Last updated by system 3 hours ago). There are buttons for 'Add agent' and 'Actions'. At the bottom, there are pagination controls and a 'Rows per page: 20' dropdown.

Aquí vemos la integración que tiene nuestra máquina kali con suricata, para poder tener logs de suricata.

[View all agents](#)

kali

Agent details Logs Diagnostics

Overview

CPU ⓘ	0.27 %	View more agent metrics
Memory ⓘ	81 MB	
Status	Healthy	
Last activity	13 seconds ago	
Last checkin message	Running	
Agent ID	c435ee86-b772-47c0-a498-ee378a2b763d	
Agent policy	My first agent policy rev. 3	
Agent version	8.12.2	
Host name	kali	
Logging level	info	
Agent release	stable	
Platform	kali	
Monitor logs	Enabled	
Monitor metrics	Enabled	
Tags	-	

Integrations

- endpoint-1
 - Inputs
 - Policy Response
- suricata-2
 - Inputs
 - Logs
 - Healthy

[Actions ▾](#)

The screenshot shows the Elastic Fleet interface for the 'suricata' policy. At the top, there's a search bar with placeholder text 'Find apps, content, and more.' and a 'Live Chat' button. Below the header, the 'Fleet' tab is selected, followed by 'Agent policies' and 'suricata'. On the right, there's a 'Send feedback' link. The main area displays the 'suricata' policy details: Revision 2, Integrations 2, Agents 1, Last updated on Apr 12, 2024, and an 'Actions' dropdown menu. Below this, there are tabs for 'Integrations' (selected) and 'Settings'. A search bar with placeholder 'Search...' and an 'Add integration' button are also present. The 'Integrations' table lists one entry: 'suricata-1' (Suricata v2.21.0) in the 'default' namespace.

Name	Integration	Namespace	Actions
suricata-1	Suricata v2.21.0	default	...

Aquí podemos ver los logs de Suricata:

The screenshot shows the Elastic Stack interface with the following details:

- Header:** elastic, Find apps, content, and more, Live Chat, Setup guide, Save.
- Left sidebar:** Discover, logs, suricata.
- Available fields:** @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, component.binary, component.dataset, component.id, component.old_state, component.state, component.type, container.id, data_stream.dataset, data_stream.namespace, data_stream.type, duration, ecs.version, elastic.agent.id, elastic.agent.snapshot, elastic.agent.version, enterprise.search.access_all_engines, enterprise.search.change.apache.key, enterprise.search.change.apache_key.
- Search bar:** suricata.
- Time range:** Auto interval, No breakdown, April 11, 2024 to April 12, 2024 @ 16:27:29.132 - April 12, 2024 @ 16:27:29.132 (interval: Auto - 30 minutes).
- Documents (5) Field statistics:** Get the best look at your search results, Sort fields.
- Table Headers:** Take the tour, Dismiss, @timestamp, Document.
- Table Data:** 5 rows of log entries from April 12, 2024, related to Suricata events.

Integracion de los logs de Honeypot en Elastic

The screenshot shows two pages from the Elastic Stack interface:

- Custom Logs Package Details:** This page displays the "Custom Logs" package version 2.3.1. It includes sections for Overview, Settings, Configs, and API reference. A "Details" sidebar provides metadata like Version 2.3.1, Category Custom, Custom Logs, and License LICENSE.txt. A "Custom Logs Package" icon is shown on the left.
- Add Custom Logs Integration:** This page shows the configuration for a new integration named "log-honeypot". It's associated with an "Agent policy honeypot". The "Configure integration" step 1 is active, showing "Integration settings" with fields for "Integration name" (log-honeypot) and "Description" (honeypot). It also includes a "Custom log file" section with a "Log file path" set to "/home/kali/cowrie.log". A "Dataset name" dropdown is set to "cowrie". Buttons at the bottom include "Cancel", "Preview API request", and "Save and continue".

podemos crear los conjuntos de datos que queremos ver

The screenshot shows the second step of the 'Add integration' wizard. It is titled 'Where to add this integration?' and has a sub-section '2'. The 'Existing hosts' tab is selected. Under 'Agent policy', it shows 'honeypot' selected. At the bottom right are 'Cancel', 'Preview API request', and a large blue 'Save and continue' button.

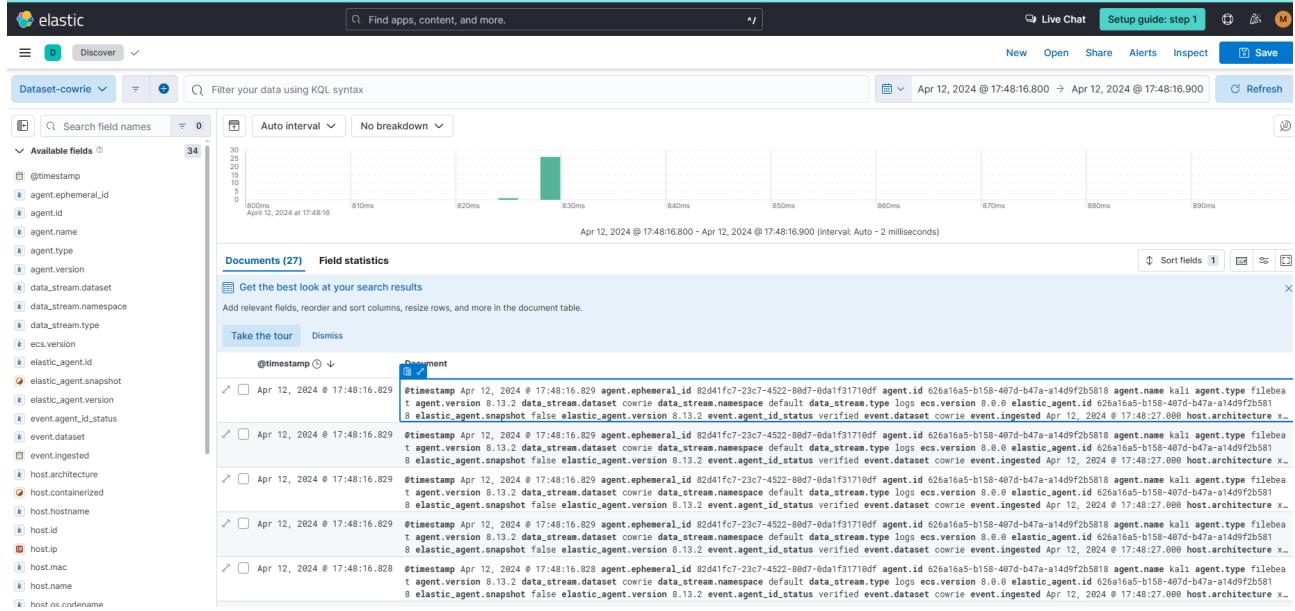
The screenshot shows the 'Agent policies' page with the 'honeypot' policy selected. It displays the following details:

- honeypot**: The name of the agent policy.
- Agent policies**: Used to manage a group of integrations across a set of agents.
- Agents**: 0 agents are enrolled with the selected agent policy.
- Last updated on**: Apr 12, 2024.

Creamos un Dataset para el honeypot (Cowrie)

The screenshot shows the 'Create data view' dialog. The 'Name' field is set to 'Dataset-cowrie-2'. The 'Index pattern' field contains 'logs-cowrie*'. The 'Timestamp field' is set to '@timestamp'. The 'Matching sources' section shows 'All sources' and 'Matching sources' for 'logs-cowrie-default'. The 'Data stream' button is highlighted. At the bottom are 'Close', 'Use without saving', and a large blue 'Save data view to Kibana' button.

comprobamos los logs del honeypot (Cowrie)

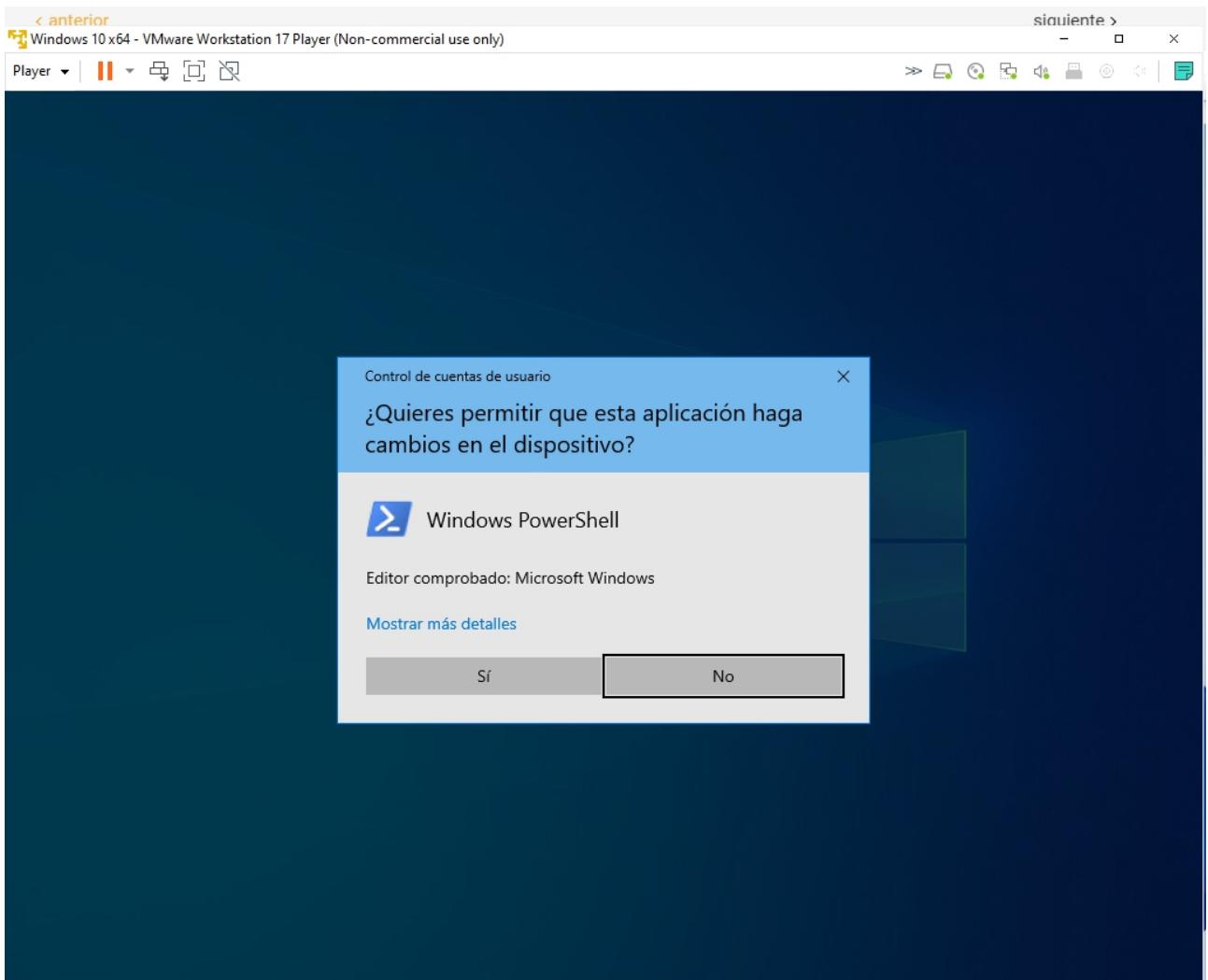


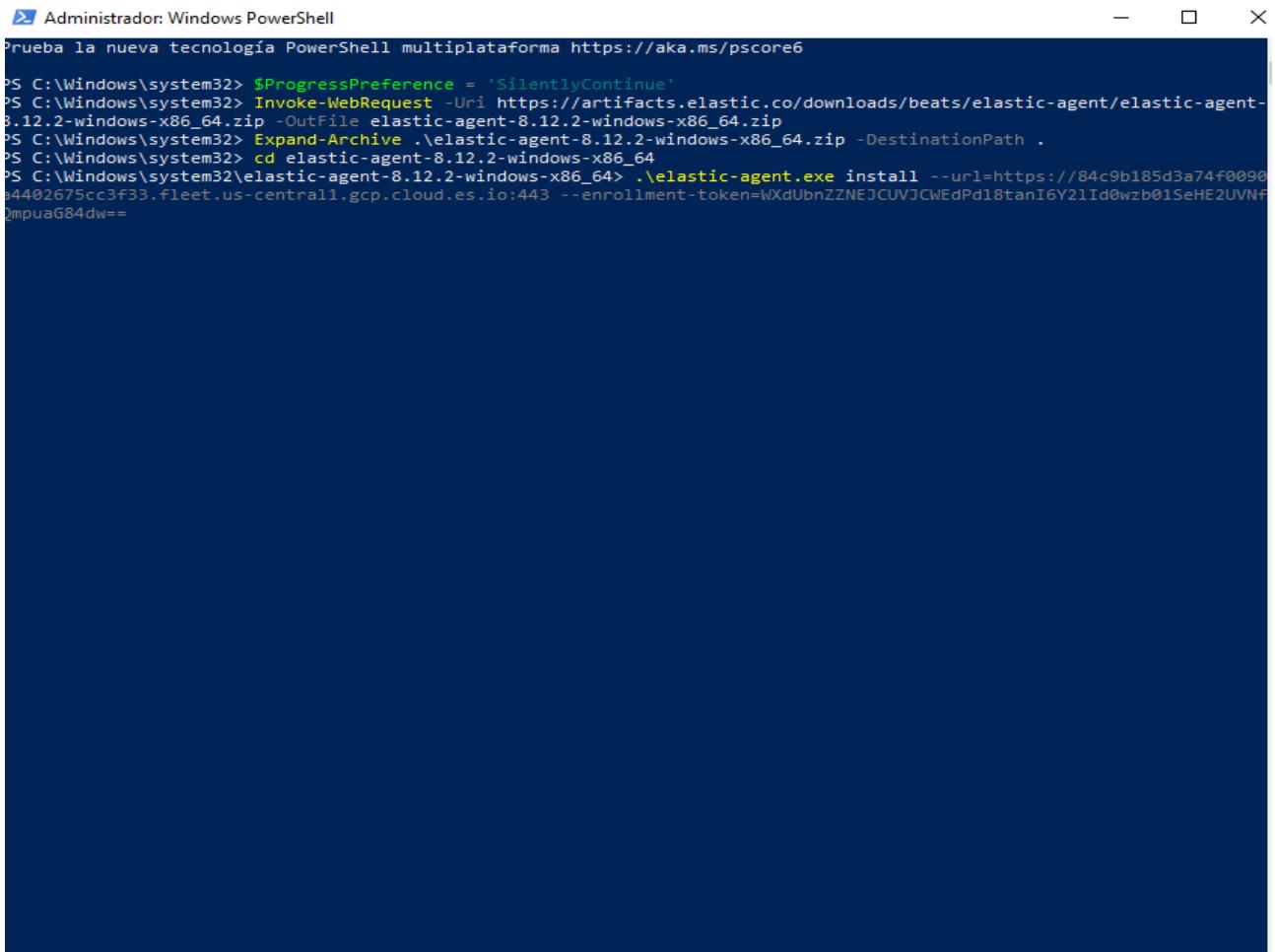
Integración con Windows 10:

Screenshot of the 'Set up Elastic Defend integration' guide on the elastic website. The guide shows three steps: 'Install Elastic Agent' (selected), 'Add the integration', and 'Confirm incoming data'. A note below says: 'These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#)'. Under 'Install Elastic Agent on your host', there are tabs for Linux Tar, Mac, Windows (selected), RPM, DEB, and Kubernetes. A command-line snippet for Windows is shown:

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-  
Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.12.2-windows-x86_64  
.\\elastic-agent.exe install --url=https://04c9b185d3a74f0090a4402675cc3f33.fleet.us-centr  
...  
  
Copied
```

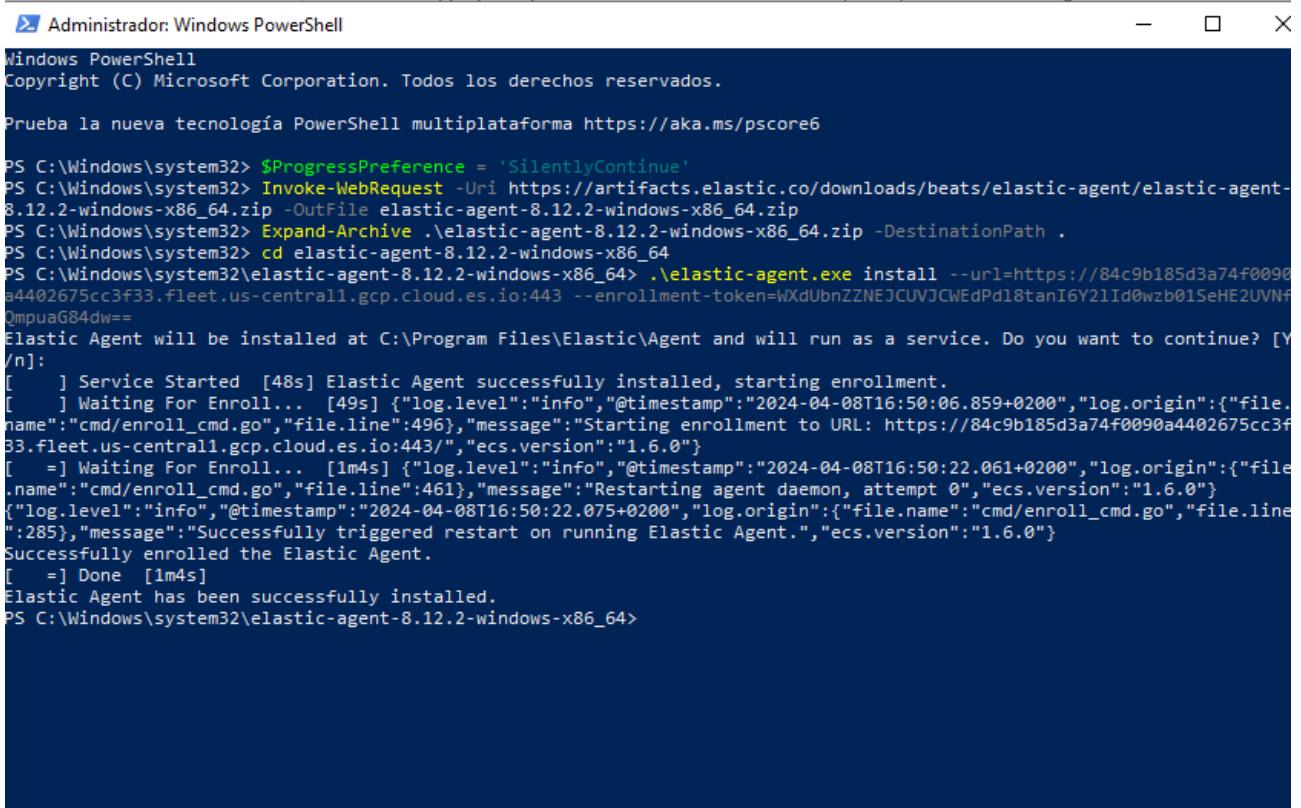
copiamos el comando, y nos vamos a PowerShell de windows 10, lo ejecutamos como administrador:





```
PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-windows-x86_64.zip -Outfile elastic-agent-8.12.2-windows-x86_64.zip
PS C:\Windows\system32> Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .
PS C:\Windows\system32> cd elastic-agent-8.12.2-windows-x86_64
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64> .\elastic-agent.exe install --url=https://84c9b185d3a74f0090a4402675cc3f33.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=WXdUbnZZNEJCUVJCWEdPdl8tanI6Y2lId0wzb01SeHE2UVNFQmpuaG84dw==
```

comprobamos que Elastic Agent ha sido instalado:



```
PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-windows-x86_64.zip -OutFile elastic-agent-8.12.2-windows-x86_64.zip
PS C:\Windows\system32> Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .
PS C:\Windows\system32> cd elastic-agent-8.12.2-windows-x86_64
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64> .\elastic-agent.exe install --url=https://84c9b185d3a74f0090a4402675cc3f33.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=WXdUbnZZNEJCUVJCWEdPdl8tanI6Y2lId0wzb01SeHE2UVNFQmpuaG84dw==

Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:
[   ] Service Started [48s] Elastic Agent successfully installed, starting enrollment.
[   ] Waiting For Enroll... [49s] {"log.level":"info","@timestamp":"2024-04-08T16:50:06.859+0200","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":496},"message":"Starting enrollment to URL: https://84c9b185d3a74f0090a4402675cc3f33.fleet.us-central1.gcp.cloud.es.io:443/","ecs.version":"1.6.0"}
[   ] Waiting For Enroll... [1m4s] {"log.level":"info","@timestamp":"2024-04-08T16:50:22.061+0200","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-04-08T16:50:22.075+0200","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":285},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"} Successfully enrolled the Elastic Agent.
[   ] Done [1m4s]
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64>
```

The screenshot shows the 'Integrations' section of the Elastic Cloud interface. A step-by-step guide is displayed:

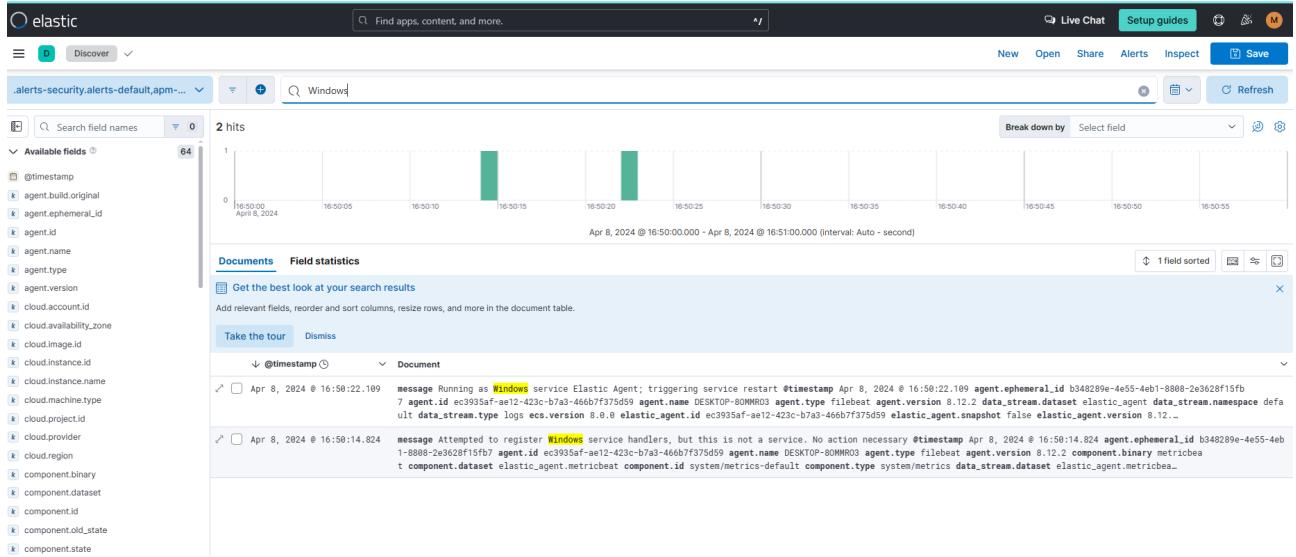
- Install Elastic Agent on your host**: This step provides instructions and a command-line script for installing the Elastic Agent on Windows. The script uses PowerShell to download the agent from the official website, extract it, and run the installation command. A 'Copied' button is visible below the script.
- Agent enrollment confirmed**: This step indicates that one agent has been enrolled successfully.

The screenshot shows the 'Security' section of the Elastic Cloud interface. A step-by-step guide is displayed:

- Select the integration you want to use**: This step shows a dropdown menu where 'Windows 10' is selected.
- Enroll your agents enabled with Elastic Defend through Fleet**: This step provides instructions and a 'Enroll Agent' button.

Damos click a Enroll Agent

Aquí podemos ver los logs de windows:



FIN DE PRÁCTICA