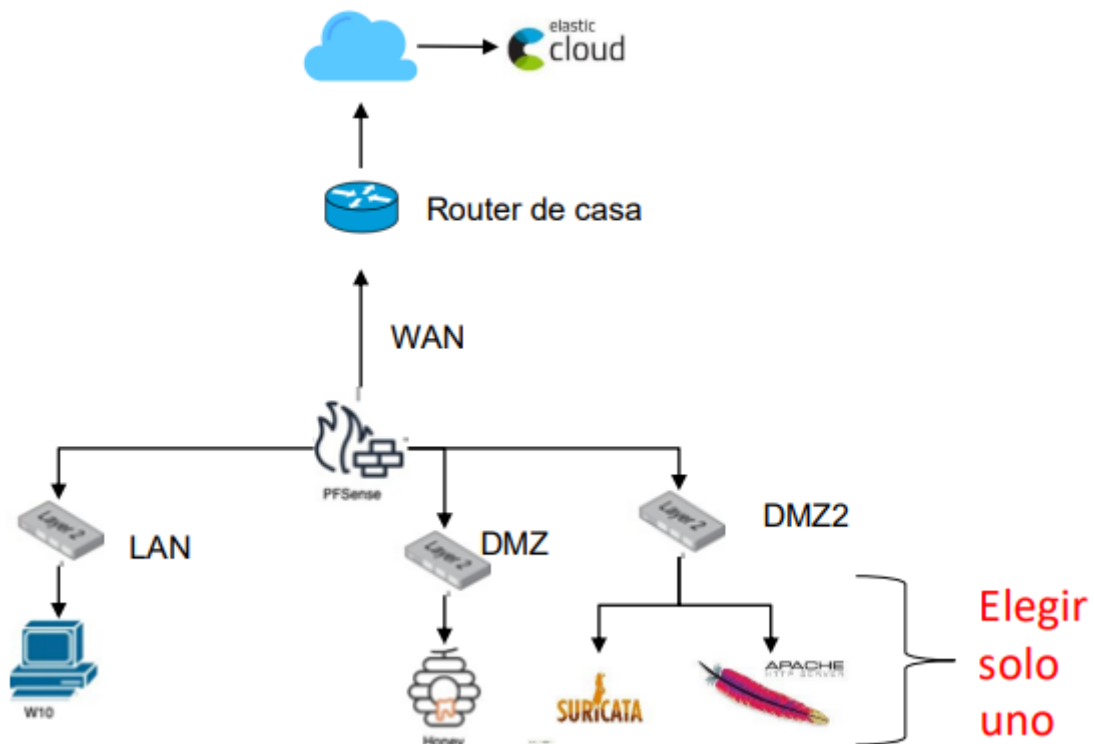


INFRAESTRUCTURA DE RED



La configuración del firewall tiene 3 adaptadores:

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a:

Nombre:

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a:

Nombre:

[▶ Avanzado](#)

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a:

Nombre:

☒ Habilitar adaptador de red

Conectado a:

Nombre:

Y estas son las reglas que he establecido para cada uno:

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule		
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule		
<div><div> Add</div><div> Add</div><div> Delete</div><div> Toggle</div><div> Copy</div><div> Save</div><div> Separator</div></div>												

Floating

WAN

LAN

DMZ

DMZ2

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	2222	*	none			
<input type="checkbox"/>	8/802.34 MiB	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	9300	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	9200	*	none			
<input type="checkbox"/>	2/138 KiB	IPv4 TCP/UDP	DMZ subnets	*	*	53 (DNS)	*	none		Salida de trafico DNS	
<input type="checkbox"/>	0/504 B	IPv4 ICMP any	DMZ subnets	*	*	*	*	none		tcp/udp	

Add

Add

Delete

Toggle

Copy

Save

Separator

Floating

WAN

LAN

DMZ

DMZ2

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✓</div><div>0/0 B</div></div>	IPv4 TCP	*	*	*	21 (FTP)	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>8/47 KiB</div></div>	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>16/20.77 MiB</div></div>	IPv4 TCP/UDP	*	*	*	443 (HTTPS)	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/0 B</div></div>	IPv4 TCP/UDP	*	*	*	9300	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/0 B</div></div>	IPv4 TCP/UDP	*	*	*	9200	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>2/331 KiB</div></div>	IPv4 TCP/UDP	DMZ2 subnets	*	*	53 (DNS)	*	none		Salida de trafico DNS	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/0 B</div></div>	IPv4 ICMP any	DMZ2 subnets	*	*	*	*	none		tcp/udp	<div><div></div><div></div><div></div><div></div><div></div></div>

↑

Add

↓

Add

Delete

Toggle

Copy

Save

+

Separator

Equipo Windows:

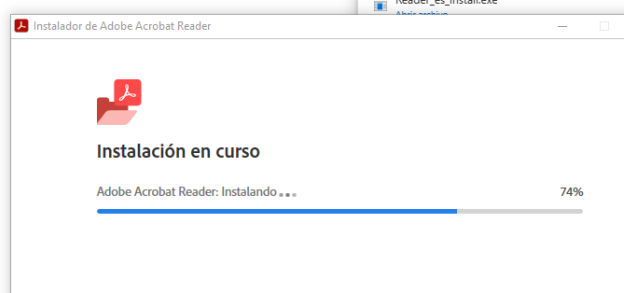
1. Instalamos Agente de Elastic

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

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

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://d860addf0cb74820bd
a548887f383eac.fleet.us-centrall1.gcp.cloud.es.io:443 --enrollment-token=d3c5a05JNEI5NDJrY0c1M2FBaEI6Rjh5aTBsZHNhVGVKZWY
NTF6OHFmdw== $ProgressPreference = 'SilentlyContinue'
```

2. Procedo a realizar una instalación con el fin de generar logs:



3. Los resultados:

Details for log entry Sw-vNI4B942kcG53Mz7H Investigate

From index .ds-logs-endpoint.events.registry-default-2024.03.12-000001

process.code_signature.subject_name	Microsoft Windows
process.code_signature.trusted	true
process.entity_id	YjFINjNiZjQlZTI0MC00OTY1LWExZTAiZmYzMDNIYTJmNmQ0LTM1NTItMTcxMDI3ODkyNC42NDUyMTMyMDA=
process.executable	C:\Windows\explorer.exe
process.executable.caseless	c:\windows\explorer.exe
process.executable.text	C:\Windows\explorer.exe
process.name	explorer.exe
process.name.caseless	explorer.exe
process.name.text	explorer.exe
process.pid	3552
registry.data.strings	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Adobe Acrobat.lnk, C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
registry.data.type	REG_MULTI_SZ
registry.hive	HKEY_USERS
	S-1-5-21-3538088021-214005281-3663136422-

Equipo HoneyPot:

- ➔ He elegido una maquina kali y he instalado un honeypot ssh para generar logs a través de Elastic

1. Descargo el repositorio de github y lo ejecuto con docker mediante el puerto 2222

```
(kali@kali)~[/cowrie]
$ sudo docker run -p 2222:2222 cowrie/cowrie:latest
/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),
2024-03-17T17:19:02+0000 [-] Python Version 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0]
2024-03-17T17:19:02+0000 [-] Twisted Version 23.10.0
2024-03-17T17:19:02+0000 [-] Cowrie Version 2.5.0
2024-03-17T17:19:02+0000 [-] Loaded output engine: jsonlog
2024-03-17T17:19:02+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 23.10.0 (/cowrie/cowrie-env/bin/py
thon3 3.11.2) starting up.
2024-03-17T17:19:02+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreac
tor.EPollReactor.
2024-03-17T17:19:02+0000 [-] CowrieSSHFactory starting on 2222
2024-03-17T17:19:02+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFa
ctory object at 0x7fb2e14510>
2024-03-17T17:19:02+0000 [-] Generating new RSA keypair ...
2024-03-17T17:19:02+0000 [-] Generating new ECDSA keypair ...
2024-03-17T17:19:02+0000 [-] Generating new ed25519 keypair ...
2024-03-17T17:19:02+0000 [-] Ready to accept SSH connections
```

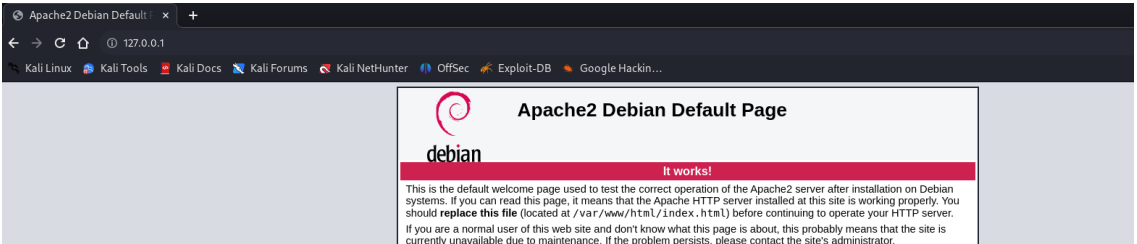
2. Estos son los logs al ejecutar el servicio:

Documents		Field statistics
↓ @timestamp		Document
✓	Mar 17, 2024 @ 18:19:02.287	process.args [/usr/sbin/docker-proxy, -proto, tcp, -host-ip, ::, -host-port, 2222, -container-ip, 172.17.0.2, -container-port, 2222] @timestamp Mar 17, 2024 @ 18:19:02.287 agent.id c31ee679-8888-4aff-a562-4df063774eab agent.type endpoint agent.version 8.12.2 data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id c31ee679-8888-4aff-a562-4df063774eab event.action exec event.agent_id status verified event.category process event.created Mar 17, 2024 @ 18:19:02.287 event.dataset
✓	Mar 17, 2024 @ 18:19:02.284	process.args [/usr/sbin/docker-proxy, -proto, tcp, -host-ip, 0.0.0.0, -host-port, 2222, -container-ip, 172.17.0.2, -container-port, 2222] @timestamp Mar 17, 2024 @ 18:19:02.284 agent.id c31ee679-8888-4aff-a562-4df063774eab agent.type endpoint agent.version 8.12.2 data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id c31ee679-8888-4aff-a562-4df063774eab event.action exec event.agent_id status verified event.category process event.created Mar 17, 2024 @ 18:19:02.284 event.dataset
✓	Mar 17, 2024 @ 18:19:02.284	process.args [/usr/sbin/iptables, --wait, -t, nat, -A, POSTROUTING, -j, MASQUERADE] @timestamp Mar 17, 2024 @ 18:19:02.284 agent.id c31ee679-8888-4aff-a562-4df063774eab agent.type endpoint agent.version 8.12.2 data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id c31ee679-8888-4aff-a562-4df063774eab event.action exec event.agent_id status verified event.category process event.created Mar 17, 2024 @ 18:19:02.284 event.dataset
✓	Mar 17, 2024 @ 18:19:02.282	process.args [/usr/sbin/iptables, --wait, -t, nat, -A, POSTROUTING, -j, MASQUERADE] @timestamp Mar 17, 2024 @ 18:19:02.282 agent.id c31ee679-8888-4aff-a562-4df063774eab agent.type endpoint agent.version 8.12.2 data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id c31ee679-8888-4aff-a562-4df063774eab event.action exec event.agent_id status verified event.category process event.created Mar 17, 2024 @ 18:19:02.282 event.dataset
✓	Mar 17, 2024 @ 18:19:02.282	process.args [/usr/sbin/iptables, --wait, -t, nat, -C, POSTROUTING, -j, MASQUERADE] @timestamp Mar 17, 2024 @ 18:19:02.282 agent.id c31ee679-8888-4aff-a562-4df063774eab agent.type endpoint agent.version 8.12.2 data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id c31ee679-8888-4aff-a562-4df063774eab event.action exec event.agent_id status verified event.category process event.created Mar 17, 2024 @ 18:19:02.282 event.dataset

3.

Equipo con Apache

- ➔ He elegido una maquina kali
- ➔ Una vez levantado el apache entramos en localhost(127.0.0.1)

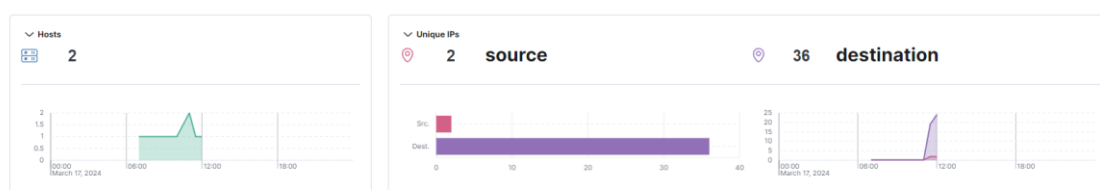


1.

2. Comprobamos que Elastic recoge el proceso

Hosts

Last event: 53 seconds ago



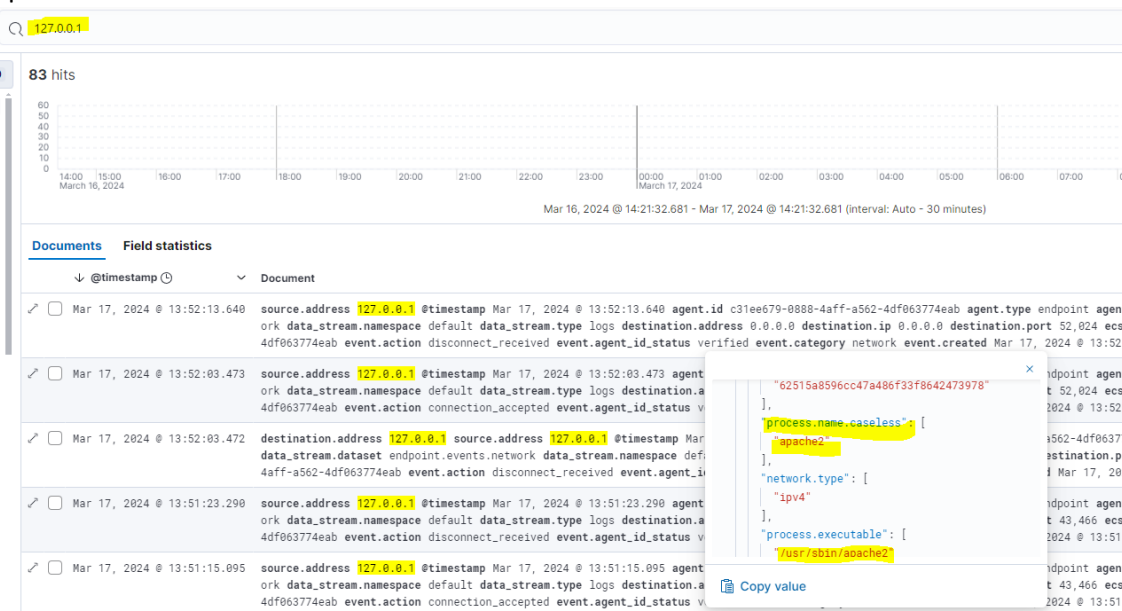
All hosts Uncommon processes Anomalies Events Host risk Sessions

Uncommon processes

Showing 29 processes

Process name	Hosts	Instances	Host names	Last command	Last user
apache2	1	1	kali	/usr/sbin/apache2	root
cat	1	1	kali	cat	kali

3. En los log podemos comprobar como que estamos accediendo a localhost a través de apache



4. Por si queda alguna duda comprobamos que el agent name es "kali"



5.