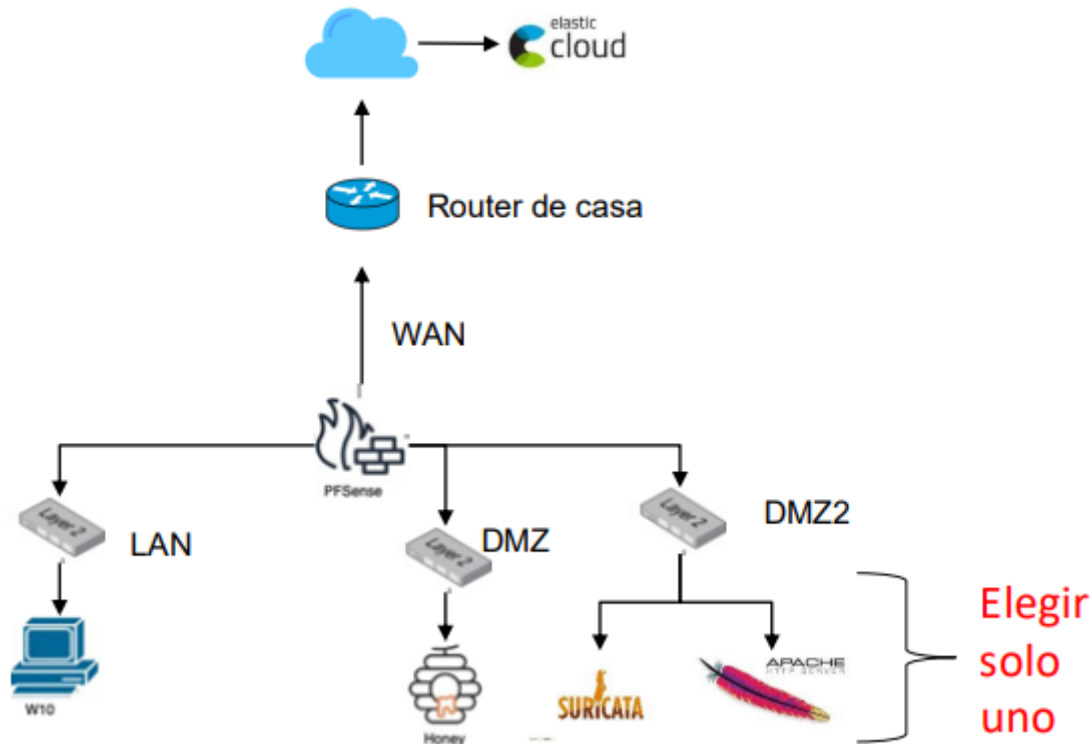


# Practica Blue team: Montaje de Infraestructura.

→ La Creación de la infraestructura será la siguiente:



→ La configuración de los adaptadores de red de las diferentes máquinas será:

- PFSense
- Windows (LAN)
- Honeypot (DMZ)
- Servidor Apache (DMZ2)

Dentro de PFSense tenemos la siguiente configuración:

























## WAN

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	*	*	DMZ subnets	2222 - 2223	*	none		Permitir el acceso de WAN a DMZ Honeypot	<a href="#">⚙</a> <a href="#">📄</a> <a href="#">🗑</a> <a href="#">✖</a>
<input type="checkbox"/>	✓ 0/120 B	IPv4 TCP	*	*	*	*	*	none			<a href="#">⚙</a> <a href="#">📄</a> <a href="#">🗑</a> <a href="#">✖</a>
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	*	*	*	4194	*	none		Regla Wan VPN	<a href="#">⚙</a> <a href="#">📄</a> <a href="#">🗑</a> <a href="#">✖</a>
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none		NAT Regla apache	<a href="#">⚙</a> <a href="#">📄</a> <a href="#">🗑</a> <a href="#">✖</a>




































Regla en WAN para el honeypot:

- **Interface:** WAN
- **Protocol:** TCP
- **Source:** any
- **Destination:** DMZ subnet
- **Destination port range:** from: 2222 to: 2223
- **Description:** Allow WAN to DMZ Honeypot access

## LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/198 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	 0/728.23 MiB	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	     
 Add  Add  Delete  Toggle  Copy  Save  Separator											

## DMZ

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	DMZ subnets	*	LAN subnets	*	*	none		Bloquear DMZ Honeypot a LAN	     
<input type="checkbox"/>	 0/0 B	IPv4 TCP	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloquear DMZ Honeypot a DMZ2	     
<input type="checkbox"/>	 0/0 B	IPv4 TCP	DMZ subnets	*	LAN subnets	443 (HTTPS)	*	none		Permitir que DMZ Honeypot se vea a través de elastic	     
<input type="checkbox"/>	 12/502 KiB	IPv4 UDP	DMZ subnets	*	*	53 (DNS)	*	none		Salida de trafico DNS	     
<input type="checkbox"/>	 6/35.70 MiB	IPv4 TCP/UDP	DMZ subnets	*	*	Webs	*	none		Salida de trafico WEB	     

### Regla en DMZ para permitir envío de logs a Elastic:











- **Interface:** DMZ
- **Protocol:** TCP
- **Source:** DMZ subnet (honeypot IP)
- **Destination:** LAN subnet (Elastic server IP)
- **Destination port range:** from: 9200 to: 9200
- **Description:** Allow DMZ Honeypot to Elastic








### Regla en DMZ para bloquear acceso a LAN y DMZ2:

- **Interface:** DMZ
- **Protocol:** Any

- **Source:** DMZ subnet (honeypot IP)
- **Destination:** LAN subnet, DMZ2 subnet
- **Description:** Block DMZ Honeypot to LAN and DMZ2

## DMZ2

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	4/3.06 MiB	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none	Salida de trafico DNS	    
<input type="checkbox"/>	✓	2/56.53 MiB	IPv4 TCP/UDP	DMZ2 subnets	*	*	Webs	*	none	Salida de trafico WEB	    

 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator

### Regla en DMZ2 para la fuente de logs (Apache Server):

- **Interface:** DMZ2
- **Protocol:** TCP
- **Source:** any
- **Destination:** DMZ2 subnet (IP del servidor Apache)
- **Destination port range:** from: 80 to: 80 (para HTTP)
- **Description:** Allow HTTP traffic to Apache Server in DMZ2

## Elastic con servidor apache (instalado en una kali)

1. Añadimos la integración de Apache para poder leer los logs
2. La vinculamos a nuestra máquina Linux
3. Y para generar algo de ruido y por lo tanto logs, introduzco la ip en el buscador para entrar en la página web originada apache

< View all agents

kali

Agent detailsLogsDiagnostics

Overview

CPU ⓘ0.80 %

View more agent metrics

Memory ⓘ157 MB

Status

Healthy

Last activity13 seconds ago

Last checkin messageRunning

Agent IDf7bf6fd1-a673-452c-af5a-8f02e89756af

Agent policyAgent policy 1 rev. 2

Agent version8.14.1

Host namekali

Integrations

> system-1

apache-1

Inputs

Logs

Healthy

Metrics

Healthy

Stream

elastic\_agent.id:f7bf6fd1-a673-452c-af5a-8f02e89756af and (data\_stream.dataset:elastic\_agent.filebeat)

CustomizeHighlights

Last 1 day

Replay

Jun 17, 2024event.datasetMessage

15:25:01.409elastic\_agent.filebeat<address>Apache/2.4.58 (Debian) Server at 192.168.250.100 Port 80</address></body></html>

15:25:01.409elastic\_agent.filebeat[elastic\_agent.filebeat][info] Process another repeated request.

15:25:01.410elastic\_agent.filebeat[elastic\_agent.filebeat][info] Process another repeated request.

15:25:01.410elastic\_agent.filebeat[elastic\_agent.filebeat][error] Error while processing http request: failed to collect first response: failed to execute http POST: server responded with status code 404: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><hr><address>Apache/2.4.58 (Debian) Server at 192.168.250.100 Port 80</address></body></html>

15:25:01.410elastic\_agent.filebeat[elastic\_agent.filebeat][error] Error while processing http request: failed to collect first response: failed to execute http POST: server responded with status code 404: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><hr><address>Apache/2.4.58 (Debian) Server at 192.168.250.100 Port 80</address></body></html>

06 PM

09 PM

09 PM

Mon 17

03 AM

06 AM

09 AM

12 PM

03 PM

## Elastic con Maquina Windows 10

1. Añadimos la integración de Windows para poder leer los logs
2. La vinculamos con nuestra máquina Windows
3. Y tras generar algo de ruido cambian la configuración de los usuarios o instalando nuevos servicios en el sistema nos empieza a enseñar logs:

## desktop-m7jipk0

Actions

Agent details Logs Diagnostics

## Overview

CPU ⓘ	0.64 %	<a href="#">View more agent metrics</a>
Memory ⓘ	157 MB	
Status	Healthy	
Last activity	8 seconds ago	
Last checkin message	Running	
Agent ID	760ba1a9-6797-4bf5-890f-d6b2ea7bceb4	
Agent policy	For windows10 rev. 2	
Agent version	8.14.1	
Host name	desktop-m7jipk0	
Logging level	info	

## Integrations

>  system-2	
▼  windows-1	
▼ Inputs	
▼  winlog	Healthy
▼  Metrics	Healthy

## Stream

	<input type="text" value="elastic_agent.id:760ba1a9-6797-4bf5-890f-d6b2ea7bceb4 and (data_stream.dataset:elastic_agent or data_stream.dataset:elastic_agent.endpoint_security or data_stream.dataset:elastic_agent.endpoint_security)"/>			Last 1 day		5 s
	Customize		Highlights			
Jun 16, 2024	event.dataset	Message				
15:03:09.607	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] initializing HostFS values under agent: /				
15:03:09.607	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] got DiagnosticSetup request for system/memory				
15:03:09.607	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] registering callback with filesystem-filesystems				
15:03:09.607	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] registering callback with filesystem-mounts				
15:03:09.624	elastic_agent	[elastic_agent][info] Unit state changed system/metrics-default-system/metrics-system-5395bb26-de21-402f-a46c-d43401cb2a31 (STARTING->HEALTHY): Healthy				
15:03:09.682	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] Metricbeat process and system info: {"OSVersion":{"Major":6,"Minor":2,"Build":9200},"Arch":"amd64","NumCPU":1,"User":{"SID":"S-1-5-18","Account":"SYSTEM","Domain":"NT AUTHORITY","Type":1},"ProcessPrivs":{"SeAssignPrimaryTokenPrivilege":{"enabled":false},"SeAuditPrivilege":{"enabled_by_default":true,"enabled":true},"SeBackupPrivilege":{"enabled":false},"SeChangeNotifyPrivilege":{"enabled_by_default":true,"enabled":true},"SeCreateGlobalPrivilege":{"enabled_by_default":true,"enabled":true},"SeCreatePagefilePrivilege":{"enabled_by_default":true,"enabled":true},"SeCreatePermanentPrivilege":{"enabled_by_default":true,"enabled":true},"SeCreateSymbolicLinkPrivilege":{"enabled_by_default":true,"enabled":true},"SeDebugPrivilege":{"enabled_by_default":true,"enabled":true},"SeDelegateSessionUserImpersonatePrivilege":{"enabled_by_default":true,"enabled":true},"SeImpersonatePrivilege":{"enabled_by_default":true,"enabled":true},"SeIncreaseBasePriorityPrivilege":{"enabled_by_default":true,"enabled":true},"SeIncreaseQuotaPrivilege":{"enabled":false},"SeLockMemoryPrivilege":{"enabled_by_default":true,"enabled":true},"SeLoadDriverPrivilege":{"enabled":false},"SeProfileSingleProcessPrivilege":{"enabled_by_default":true,"enabled":true},"SeRestorePrivilege":{"enabled":false},"SeSecurityPrivilege":{"enabled":false},"SeShutdownPrivilege":{"enabled":false},"SeSystemEnvironmentPrivilege":{"enabled":false},"SeSystemProfilePrivilege":{"enabled_by_default":true,"enabled":true},"SeSystemtimePrivilege":{"enabled":false},"SeTakeOwnershipPrivilege":{"enabled":false},"SeTcbPrivilege":{"enabled_by_default":true,"enabled":true},"SeTimeZonePrivilege":{"enabled_by_default":true,"enabled":true},"SeUndockPrivilege":{"enabled":false}}}				
15:03:09.682	elastic_agent.metricbeat	[elastic_agent.metricbeat][info] SeDebugPrivilege is enabled. SeDebugPrivilege=(Default, Enabled)				

## Elastic con Honeypot(Instalado en una Kali)

- Instalamos Docker en la kali
- Instalamos el honeypot cowrie y lo ejecutamos
  - sudo docker pull cowrie/cowrie
  - sudo docker run -d -p 2222:2222 -p 2223:2223 --name cowrie cowrie/cowrie
- Comprobamos que nos está soltando logs
  - sudo docker logs cowrie
- Creamos la carpeta dentro de /var/log/
  - mkdir honeypot o cowrie
- Asignamos a la carpeta los permisos necesarios
  - chgrp docker honeypot o cowrie
  - chmod g+w honeypot o cowrie
- Mandamos los log de cowrie a nuestra carpeta con:
  - sudo docker run -p 222:2222 cowrie/cowrie > /var/log/log\_honeypot.log o log\_cowrie.log

Cancel

Edit Custom Logs integration

Agent policy

Honeypot(cowrie)

Modify integration settings and deploy changes to the selected agent policy.

Integration settings

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

Integration name

logs for cowrie

Description

Advanced options

Custom log file

Change defaults

Log file path

/var/log/honeypot/log\_honeypot.log

Add row

Path to log files to be collected

Dataset name

generic

Set the name for your dataset. Changing the dataset will send

```
message 2024-06-18T14:14:23+0000 [twisted.scripts._twistd_unix.UnixAppLogger$info] [twistd 24.3.0 (/cowrie/cowrie-env/bin/python3 3.11.2)]
285 agent.ephemeral_id 32f85dcf-ffc9-44bc-a830-c0332e53f46f agent.id 39d5fd1d-5258-48e8-84e1-85d67663e45c agent.name kali agent.type file
eneric data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 39d5fd1d-5258-48e8-84e1-85d67663e45c elasti
message 2024-06-18T14:14:23+0000 [-] Cowrie Version 2.5.0 @timestamp Jun 18, 2024 @ 16:22:08.285 agent.ephemeral_id 32f85dcf-ffc9-44bc-a8
```

```

Archivo  Editar  Búsqueda  Ver  Documento  Ayuda
2024-06-18T14:14:23+0000 [-] Python Version 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0]
2024-06-18T14:14:23+0000 [-] Twisted Version 24.3.0
2024-06-18T14:14:23+0000 [-] Cowrie Version 2.5.0
2024-06-18T14:14:23+0000 [-] Loaded output engine: jsonlog
2024-06-18T14:14:23+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] twisted 24.3.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.

```

→ Podemos apreciar que la versión del log originado en la máquina y la que se muestra en Elastic coinciden demostrando así que Elastic recoge la información de nuestro honeypot