

BlueTeam

Práctica - Reentrega

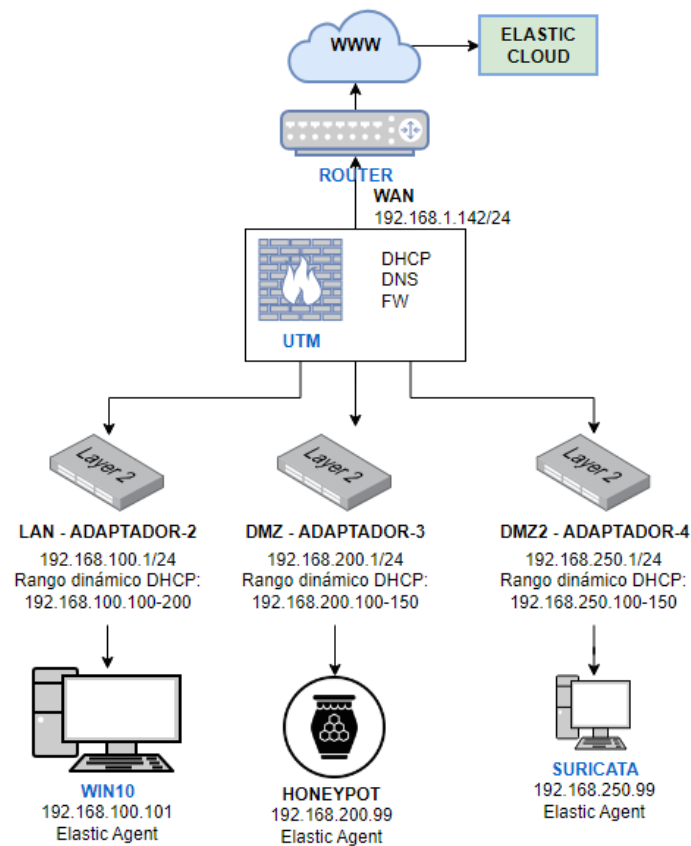
Autor: Carlos Gutiérrez Torrejón
Ref: CGT-KeeCoding-Metasploitable2

Índice

Enunciado	3
1. PFSense	4
1.1 Máquina virtual	4
1.2 Instalando PFSense	4
1.3 Configurar los adaptadores de red	6
1.4 Configuración final	7
1.5 Wizard – First Setup	8
1.6 DNS Resolver	10
1.7 DHCP	11
1.8 DMZ Interfaces	13
1.8.1 Activar DHCP	15
2. Infraestructura de red	18
2.1 LAN – WIN10	18
2.2 DMZ – HoneyPot	19
2.3 DMZ2 – Suricata	20
3. Reglas Firewall	21
4. Configuración Suricata	23
5. Configurando el HoneyPot (Cowrie)	24
5.1 Docker	24
5.2 Cowrie	24
6. Elastic Cloud	26
6.1 Agentes y políticas	27
6.2 Comprobar logs	30
6.2.1 Windows	30
6.2.2 Suricata	31
6.2.3 Cowrie	32

Enunciado

Se ha intentado implementar la siguiente infraestructura de redirigir



Cumple con las siguientes características:

- Un PFSense que interconecta tres redes (LAN, DMZ y DMZ2)
 - En la LAN se ha montado un equipo con Windows 10
 - En la DMZ un HoneyPot
 - En la DMZ2 la aplicación Suricata
- En los tres casos se ha hecho la integración con ElasticCloud al que envían los logs, dónde se almacenan y facilita su análisis.

1 PFSense

1.1 Máquina Virtual

- Nombre: UTM
- Tipo: BSD
- Versión: FreeBSD (64-bit)
- RAM: 2048 MB
- Procesadores: 1 CPU
- Almacenamiento 20 GB

1.2 Instalando PFSense

La instalación comienza automáticamente

Install	Install pfSense
Rescue Shell	Launch a shell for rescue operations
Recover config.xml	Recover config.xml from a previous install

Particionado

Auto (ZFS)	Guided Root-on-ZFS
Auto (UFS)	Guided UFS Disk Setup
Manual	Manual Disk Setup (experts)
Shell	Open a shell and partition by hand

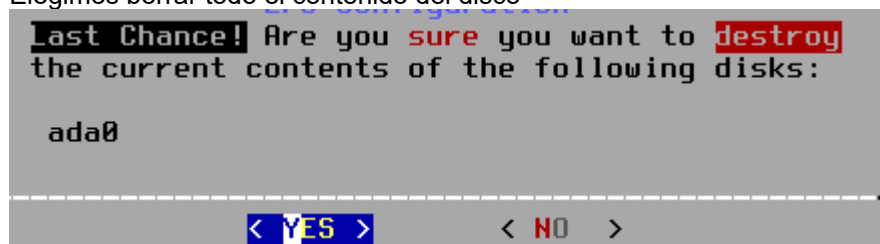
ZFS Configuration

>>> Install	Proceed with Installation
T Pool Type/Disks:	stripe: 0 disks
- Rescan Devices	*
- Disk Info	*
N Pool Name	pfSense
4 Force 4K Sectors?	YES
E Encrypt Disks?	NO
P Partition Scheme	GPT (BIOS)
S Swap Size	1g
M Mirror Swap?	NO
W Encrypt Swap?	NO

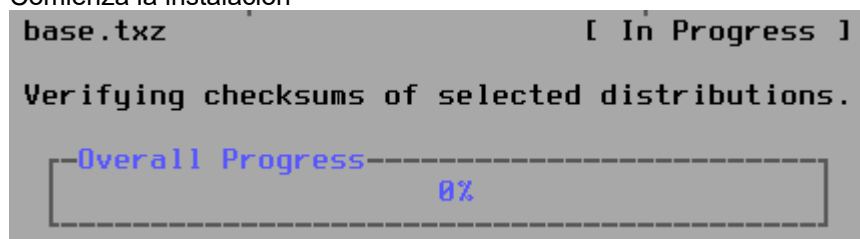
stripe	Stripe - No Redundancy
mirror	Mirror - n-Way Mirroring
raid10	RAID 1+0 - n x 2-Way Mirrors
raidz1	RAID-Z1 - Single Redundant RAID
raidz2	RAID-Z2 - Double Redundant RAID
raidz3	RAID-Z3 - Triple Redundant RAID

[*] **ada0** **VBOX HARDDISK**

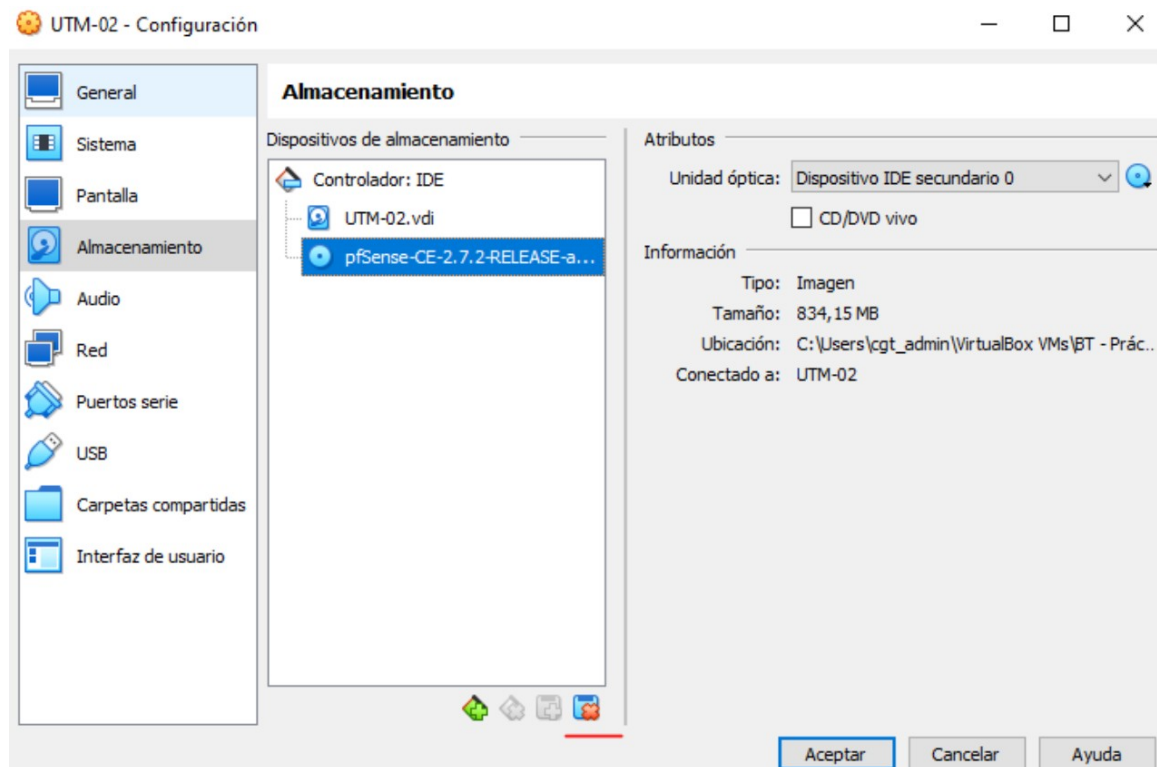
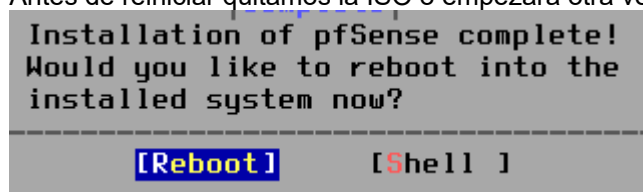
Elegimos borrar todo el contenido del disco



Comienza la instalación



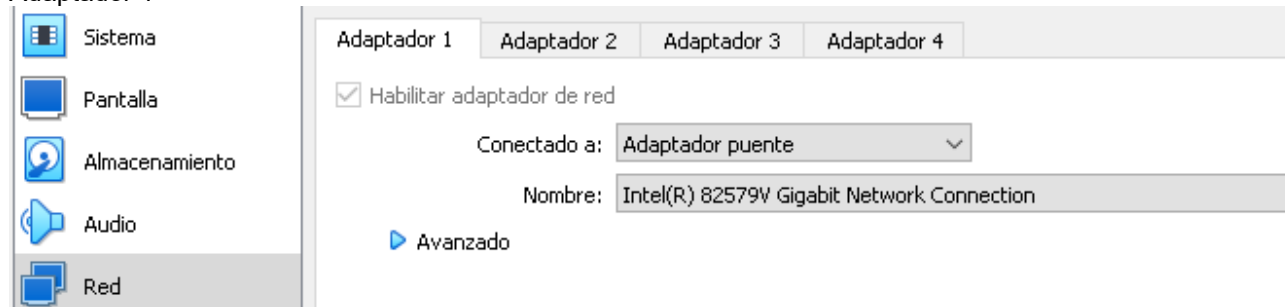
Antes de reiniciar quitamos la ISO o empezará otra vez la instalación



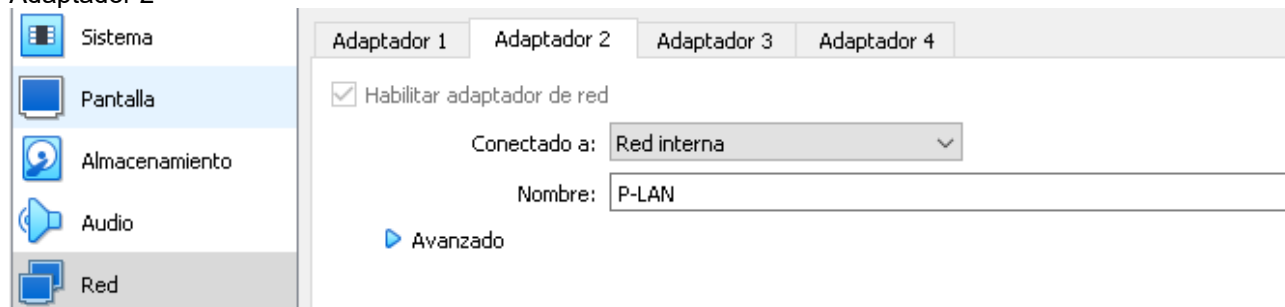
1.3 Configurar los adaptadores de red

Hay que configurar varios adaptadores de red para montar la infraestructura de firewall que permita aislar la red interna de la práctica del entorno de red local

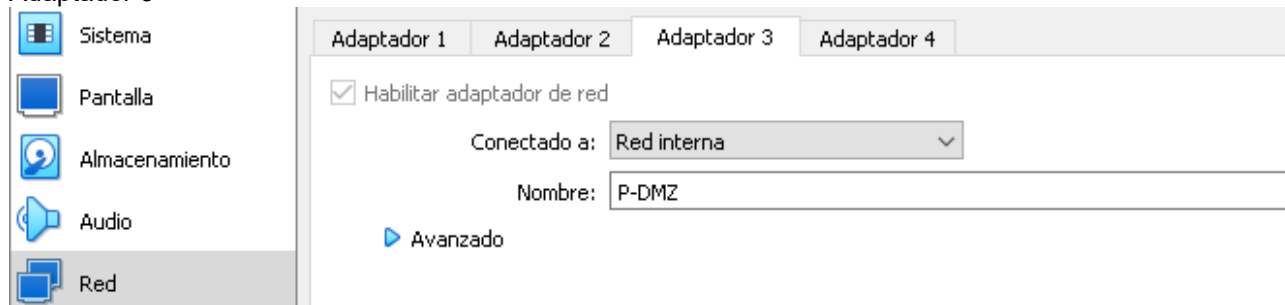
Adaptador 1



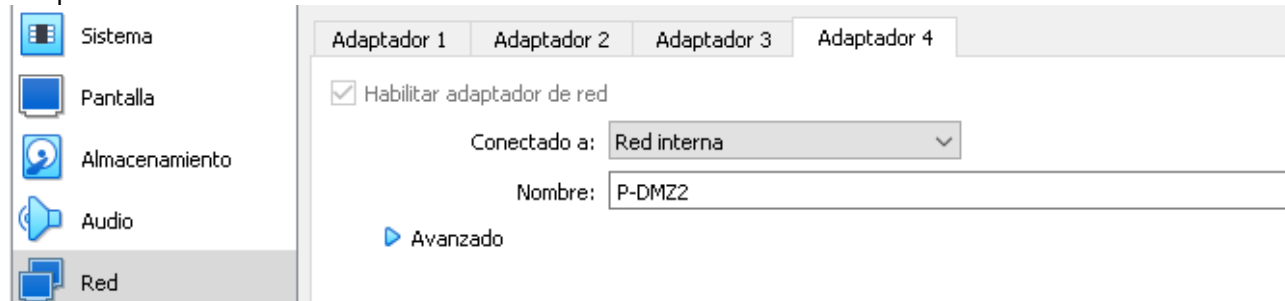
Adaptador 2



Adaptador 3



Adaptador 4



1.4 Configuración final

Quedan definidas las redes WAN y LAN

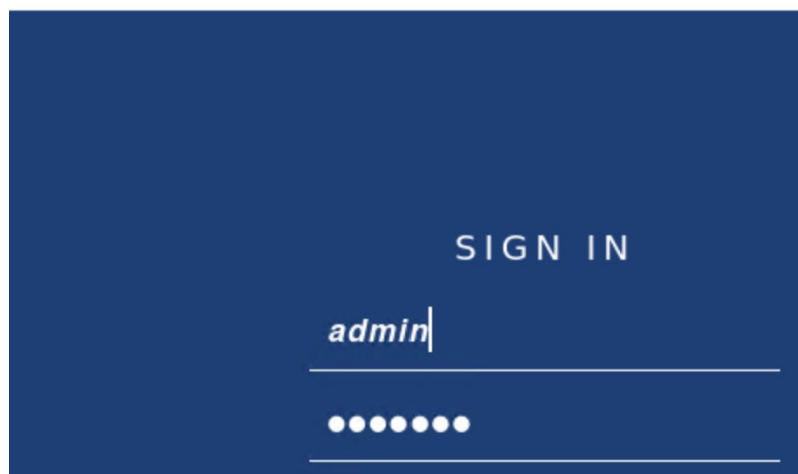
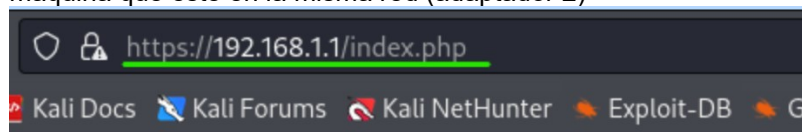
```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 49165cd0c54fad264a38

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.142/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
```

Para acceder al portal de PFSense, lo haremos desde un navegador poniendo la dirección LAN, desde una máquina que esté en la misma red (adaptador 2)



1.5 Wizard – First Setup

Accedemos al portal de PFSense

- IP: 192.168.1.1
- User: admin
- Password: pfsense

Arranca el Wizard y vamos completando la configuración:

- General Information
 - Hostname: UTM
 - Domain: keepcoding.local
 - Primary DNS Server: 127.0.0.1
 - Secondary DNS Server: 1.1.1.1
- Time Server Information
 - Timezone: Europe/Madrid
- Configure WAN Interface
 - Selected Type: DHCP
 - Subnet Mask: 32

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private use (RFC1918). This option should generally be left turned off.

Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private use. These addresses should never appear in the Internet routing table, and obviously should not be routed to the Internet.

- Configure LAN Interface
 - Cambiamos el rango de direcciones. La puerta de enlace será la 192.168.100.1

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

192.168.100.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

24

- Set Admin WebGUI Password
 - Como buena práctica cambiaremos la contraseña admin por defecto
 - 12345

- Reload configuration
 - Aplicamos los cambios

Reload configuration

Click 'Reload' to reload pfSense with new changes.

» Reload

- Una vez que ha cargado la nueva configuración podemos comprobar que ha cambiado la IP de la LAN

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 49165cd0c54fad264a38
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.142/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
```

1.6 DNS Resolver

El sistema aún no resuelve nombres, tenemos que configurar un DNS

```
(kali@kali-01)-[~] terminal client
$ ping elpais.com
ping: elpais.com: Temporary failure in name resolution
```

Services > DNS Resolver

- Deshabilitamos DNSSEC, sirve para firmar una consulta DNS

DNSSEC ☐ Enable DNSSEC Support

- Habilitamos el modo Forwarding
 - Si PFSense no pudiera responder las consultas DNS, las derivaría al segundo servidor configurado (1.1.1.1)

DNS Query Forwarding

☒ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the up
interfaces such as DHCP, PPP, or OpenVPN (if DNS Server C

- Salvamos y aplicamos los cambios y ya deberíamos resolver nombres

```
(kali@kali-01)-[~]
$ ping elpais.com
PING elpais.com (212.230.153.97) 56(84) bytes of data:
64 bytes from 212.230.153.97: icmp_seq=1 ttl=60 time=3.38 ms
64 bytes from 212.230.153.97: icmp_seq=2 ttl=60 time=3.77 ms
64 bytes from 212.230.153.97: icmp_seq=3 ttl=60 time=4.17 ms
64 bytes from 212.230.153.97: icmp_seq=4 ttl=60 time=3.18 ms
```

1.7 DHCP

Services / DHCP Server / LAN

Vamos a configurar el servidor DHCP en la LAN para generar el siguiente rango dinámico:
192.168.1.100-200

Comprobamos que el servicio esté habilitado

LAN

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="checkbox"/> Allow all clients

Modificamos el rango IPs que viene por defecto para que entregue IPs dentro del rango que hemos elegido

Primary Address Pool

Subnet	192.168.100.0/24
Subnet Range	192.168.100.1 - 192.168.100.254
Address Pool Range	<div> <div>192.168.100.100</div> <div>192.168.100.200</div> </div> <div>From To</div>

The specified range for this pool must not be within the range configured on any other address pool for

Añadimos los servidores DNS

Server Options

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.100.1
	1.1.1.1
	8.8.8.8
	DNS Server 4

Definimos la puerta de enlace

Other DHCP Options

Gateway

192.168.100.1

The default is to use the IP address of this firewall interface on the local network. Enter "none" for no gateway assignment.

Salvamos y aplicamos los cambios.

En la Kali que tenemos conectada a la red LAN, reiniciamos la tarjeta de red y comprobamos que se asigna una IP dentro del rango especificado.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.100 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::df4b:cee7:8333:404 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 1139 bytes 791463 (772.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

1.8 DMZ Interfaces

Interfaces / Interface Assignments

De momento hemos usado los dos primeros adaptadores que configuramos en VirtualBox

- **Adaptador-1:** WAN
- **Adaptador-2:** LAN

Desde está sección vamos a añadir los otros dos para configurar las distintas DMZ que usaremos en la práctica.

- **Adaptador-3:** DMZ
- **Adaptador-4:** DMZ-2

Interface	Network port
WAN	em0 (08:00:27:2d:1a:be) ▼
LAN	em1 (08:00:27:30:b2:0a) ▼ Delete
Available network ports:	em2 (08:00:27:c8:32:f2) ▼ + Add

OPT1

Vamos a configurar la primera de las interfaces (OPT1) que será la DMZ

- IPv4 Address: 192.168.200.1/24

General Configuration

Enable ☒ Enable interface

Description DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4 ▼

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.

OPT2

Configuramos la interfaz para la segunda de las DMZs

- IPv4 Address: 192.168.250.1/24

General Configuration

Enable ☒ Enable interface

Description

DMZ-2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

192.168.250.1

/ 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.

Ya tenemos configuradas nuestras cuatro interfaces

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 49165cd0c54fad264a38
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.142/24
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
```

1.8.1 Activar DHCP

Tenemos que activar el servidor DHCP para ambas DMZs y configurar el rango de IPs que se van a utilizar. También configuraremos los servidores DNS y la puerta de enlace.

Services / DHCP Server / DMZ

General DHCP Options

DHCP Backend

ISC DHCP

Enable



Enable DHCP server on DMZ interface

BOOTP



Ignore BOOTP queries

Primary Address Pool

Subnet

192.168.200.0/24

Subnet Range

192.168.200.1 - 192.168.200.254

Address Pool Range

192.168.200.100

From

192.168.200.150

To

The specified range for this pool must not be within the range configured on any other address pool.

Server Options

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

192.168.200.1

1.1.1.1

8.8.8.8

Other DHCP Options

Gateway

192.168.200.1

The default is to use the IP address of this firewall interface as the gateway network. Enter "none" for no gateway assignment.

Services / DHCP Server / DMZ2

General DHCP Options

DHCP Backend ISC DHCP

Enable ☒ Enable DHCP server on DMZ2 interfaceBOOTP ☐ Ignore BOOTP queries

Primary Address Pool

Subnet 192.168.250.0/24

Subnet Range 192.168.250.1 - 192.168.250.254

Address Pool Range

192.168.250.100

From

192.168.250.150

To

The specified range for this pool must not be within the range configured on any other address pool

Server Options

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

192.168.250.1

1.1.1.1

8.8.8.8

Other DHCP Options

Gateway

192.168.250.1

The default is to use the IP address of this firewall interface for the default gateway. Enter "none" for no gateway assignment.

Cambiamos el adaptador de la Kali que estamos usando para gestionar la red y le asignamos el de la DMZ (P-DMZ) para comprobar que funciona correctamente el servidor DHCP. Haremos lo mismo con la DMZ-2 (P-DMZ2)

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: Red interna

Nombre: P-DMZ

▶ Avanzado

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.100 netmask 255.255.255.0 broadcast 192.168.200.255
    inet6 fe80::df4b:cee7:8333:404 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 4715 bytes 2044614 (1.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

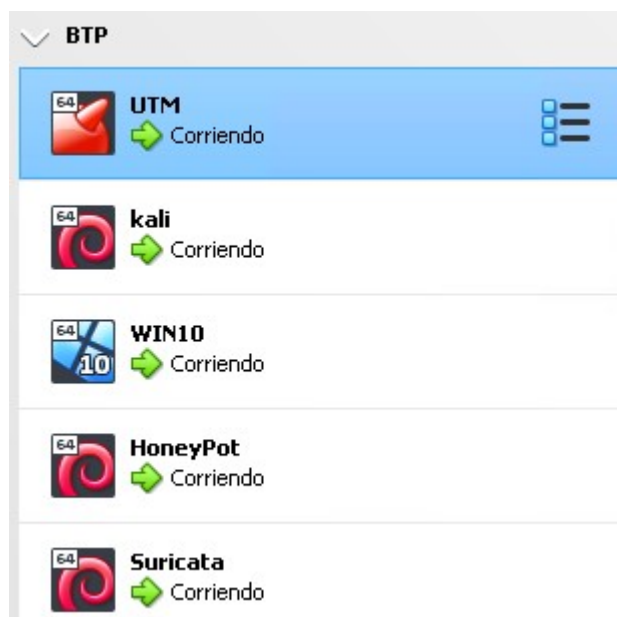
Conectado a: Red interna

Nombre: P-DMZ2

▶ Avanzado

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.250.100 netmask 255.255.255.0 broadcast 192.168.250.255
    inet6 fe80::df4b:cee7:8333:404 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 4726 bytes 2046404 (1.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

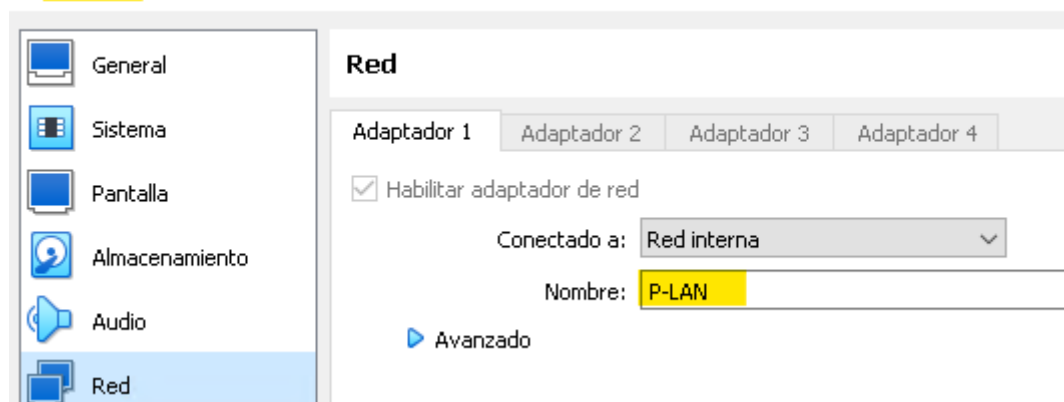
2. Infraestructura de red



2.1 LAN – WIN10

Se ha creado una máquina virtual con un Windows 10 y se ha añadido a la red LAN.

WIN10 - Configuración



```
C:\Users\carlos>ipconfig


Windows IP Configuration

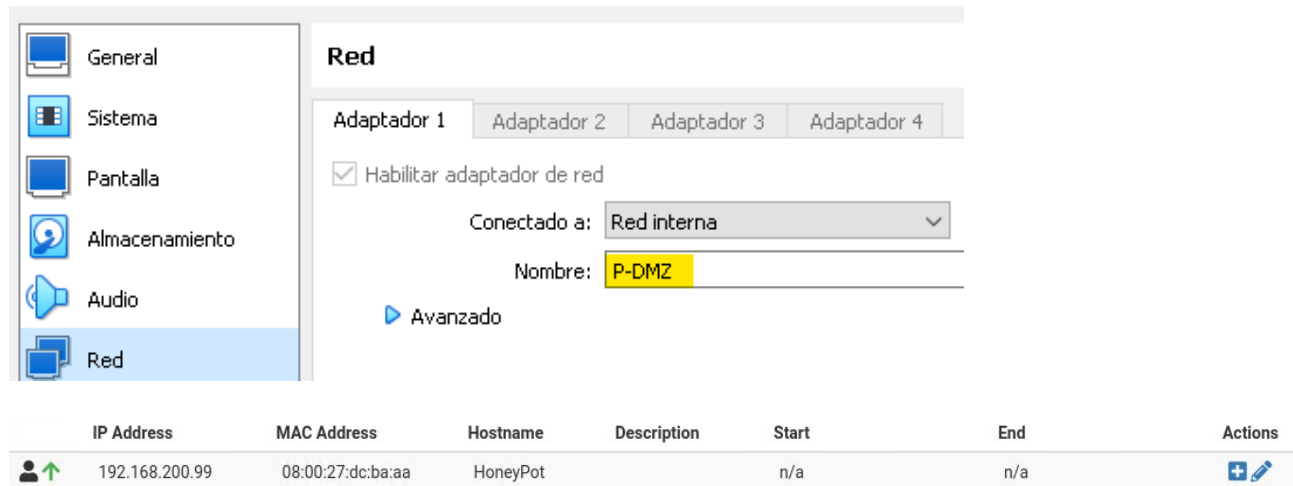
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : keepcoding.local
    Link-local IPv6 Address . . . . . : fe80::bd1d:3f59:b72b:12c1%3
    IPv4 Address. . . . . : 192.168.100.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::a00:27ff:fe25:6028%3
                               192.168.100.1
```




2.2 DMZ – HoneyPot

Se ha creado una máquina virtual con un Kali para actuar como HoneyPot y se ha incluido en la red DMZ. También se le ha asignado una IP estática (192.168.200.99)

 HoneyPot - Configuración



The screenshot shows the 'Red' configuration window for a virtual machine. On the left is a sidebar with icons for General, Sistema, Pantalla, Almacenamiento, Audio, and Red. The 'Red' tab is selected. The main area shows 'Adaptador 1' selected, with 'Habilitar adaptador de red' checked. The 'Conectado a' dropdown is set to 'Red interna', and the 'Nombre' field contains 'P-DMZ'. Below this is an 'Avanzado' button. At the bottom, a table lists the network configuration:

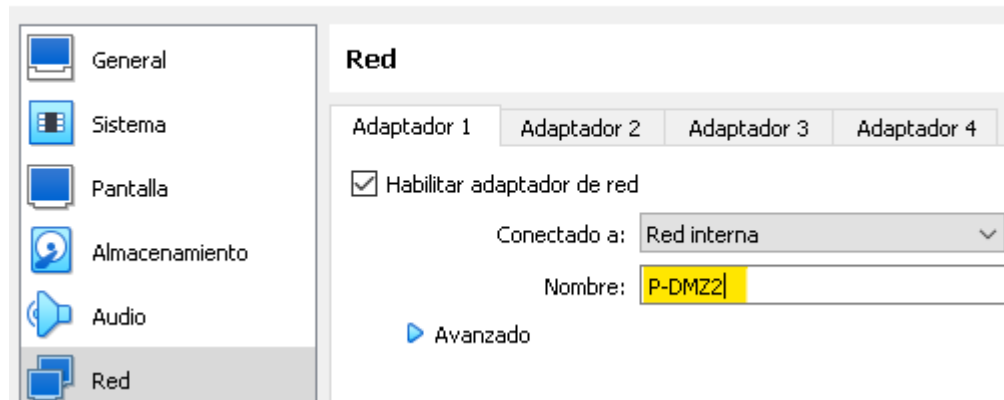
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
	192.168.200.99	08:00:27:dc:ba:aa	HoneyPot		n/a	n/a	 



```
(kali@HoneyPot)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.99 netmask 255.255.255.0 broadcast 192.168.200.255
    inet6 fe80::91e1:99c7:d3dc:c316 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dc:ba:aa txqueuelen 1000 (Ethernet)
    RX packets 9 bytes 2252 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 60 bytes 9861 (9.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2.3 DMZ2 – Suricata

Se ha añadido a la DMZ2 una máquina Kali para implementar Suricata. También se le ha asignado una IP estática (192.168.250.99)

 Suricata - Configuración



	192.168.250.99	08:00:27:de:d5:35	Suricata	n/a	n/a	
---	----------------	-------------------	----------	-----	-----	---

```
(kali@Suricata)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.250.99 netmask 255.255.255.0 broadcast 192.168.250.255
    inet6 fe80::91e1:99c7:d3dc:c316 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:de:d5:35 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 1730 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 9642 (9.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```




3. Reglas Firewall

Se van a crear las siguientes reglas de Firewall

- Bloqueo entre las redes internas: LAN – DMZ – DMZ2
- Permitir la salida de tráfico web y DNS para las tres redes
- Permitir la entrada de tráfico para la red DMZ
- Reglas de administración:
 - Acceso por SSH desde la LAN a DMZ y DMZ2
 - Permitir PING desde LAN a DMZ y DMZ2
- Redirección de tráfico

WAN

Port Forward	1:1	Outbound	NPt
--------------	-----	----------	-----

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	2222	192.168.200.99	2222	HoneyPot - Redirección puerto 222	  

LAN

Floating

WAN

LAN

DMZ

DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/2.35 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/504 B	IPv4 ICMP any	LAN subnets	*	DMZ subnets	*	*	none		Permitir Ping LAN -> DMZ	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	LAN address	*	DMZ2 subnets	*	*	none		Permitir Ping LAN -> DMZ2	
<input type="checkbox"/>	0/21 KiB	IPv4 TCP	LAN subnets	*	DMZ subnets	22 (SSH)	*	none		Acceso SSH LAN -> DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	DMZ2 subnets	22 (SSH)	*	none		Acceso SSH LAN -> DMZ2	
<input type="checkbox"/>	0/2 KiB	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Bloqueo de LAN a DMZ2	
<input type="checkbox"/>	0/168 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Bloqueo de LAN a DMZ	
<input type="checkbox"/>	0/187 KiB	IPv4 UDP	LAN subnets	*	*	53 (DNS)	*	none		Permitir salida tráfico DNS	
<input type="checkbox"/>	36/31.00 MiB	IPv4 TCP	LAN subnets	*	*	PuertosWeb	*	none		Permitir salida tráfico web	
<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	

DMZ

Floating

WAN

LAN



















DMZ

DMZ2





Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div><div></div><div></div></div>	✖	0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none	Bloqueo a DMZ2	<div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✖	0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none	Bloqueo a LAN	<div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✔	0/0 B	IPv4 *	*	*	192.168.200.99	*	*	none	HoneyPot - Permitir tráfico entrante	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✔	0/0 B	IPv4 UDP	192.168.200.99	*	*	53 (DNS)	*	none	HoneyPot - Permitir salida tráfico DNS	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✔	0/0 B	IPv4 TCP	192.168.200.99	*	*	PuertosWeb	*	none	HoneyPot - Permitir salida tráfico web	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>

DMZ2

Floating WAN LAN DMZ DMZ2											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/504 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloqueo de DMZ2 a DMZ	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloqueo de DMZ2 a LAN	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none		Permitir salida tráfico DNS	    
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	DMZ2 subnets	*	*	PuertosWeb	*	none		Permitir salida tráfico web	    

También se va a crear una redirección del puerto 222 hacia el HoneyPot. Creará automáticamente una regla en la interface WAN

Firewall / NAT / Port Forward ?										
Port Forward 1:1 Outbound NPt										
Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	✓  WAN	TCP	*	*	WAN address	2222	192.168.200.99	2222	HoneyPot - Redirección puerto 222	  

4. Configurando Suricata

Instalar Suricata

- `sudo apt install suricata`

En la siguiente ruta tenemos las reglas de Suricata. Aquí crearemos un archivo con nuestras propias reglas.

- `/etc/suricata/rules`
- `sudo nano suricata.rules`

```
kali@Suricata: /etc/suricata/rules x | kali@Suricata: /etc/suricata/rules x | kali@Suricata: /etc/suricata/rules x |
GNU nano 7.2 suricata.rules
alert tcp any any -> any any (msg:"Tráfico detectado"; sid:1; priority:1;)
alert tcp any any -> 192.168.250.99 22 (msg:"Tráfico SSH detectado"; sid:2; classtype:attempted-admin;)
```

Editamos el archivo `suricata.yaml` para indicar dónde está nuestro archivo de reglas

- `nano /etc/suricata/suricata.yaml`

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
- suricata.rules
```

En la siguiente ruta encontraremos los logs.

- `/var/log/suricata/`

5. Configurando el HoneyPot (Cowrie)

Hostname: HoneyPot

IP: 192.168.200.99

Vamos a usar como honeypot Cowrie desde una imagen de docker.

5.1 Docker

Nos permite ejecutar Cowrie de forma virtualizada

- Instalar Docker
 - `sudo apt update`
 - `sudo apt install /y docker.io`
- Habilitar e iniciar Docker
 - `sudo systemctl enable docker --now`
- Agregar el usuario actual al grupo "Docker"
 - `sudo usermod -aG docker $USER`

5.2 Cowrie

Es un honeypot SSH y Telnet para registrar ataques de fuerza bruta y la interacción del shell realizada por un atacante.

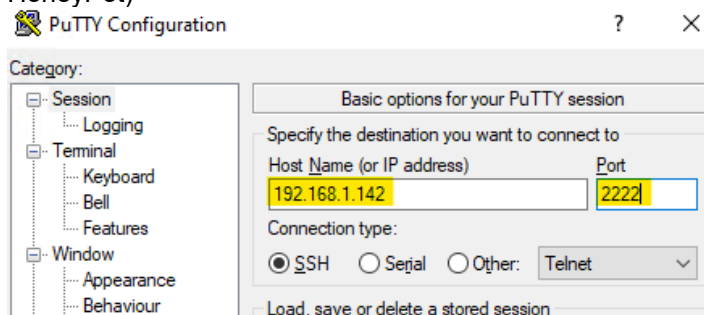
Aquí podemos ver como ejecutarlo

<https://hub.docker.com/r/cowrie/cowrie>

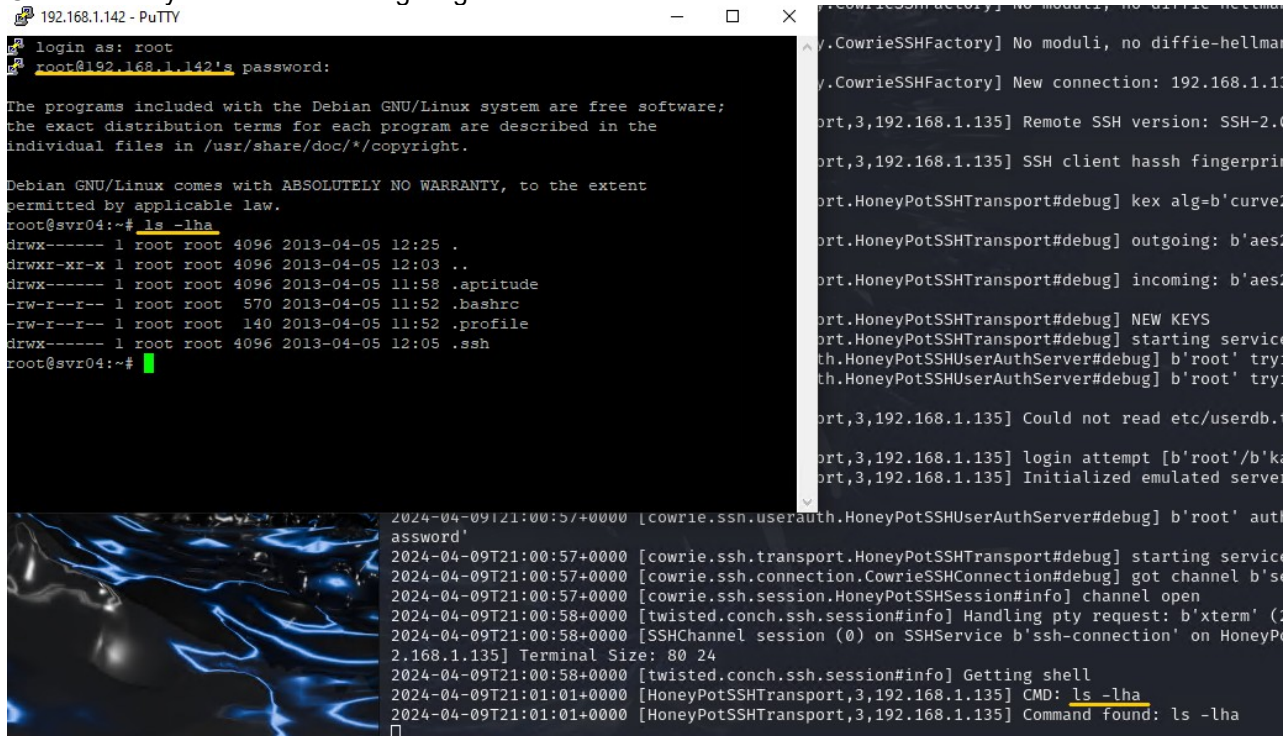
- Ejecución
 - `sudo docker run -p 2222:2222/tcp cowrie/cowrie`
- Se ha creado una regla NAT que redirija el tráfico entrante a la WAN por el puerto 2222 hacia la máquina del HoneyPot (192.168.1.142)

Probamos a conectar

Desde fuera de la red de prácticas lanzamos un putty a nuestra WAN (debería redirigir el tráfico hacia el HoneyPot)



Conectamos y vemos como recoge logs



```

192.168.1.142 - PuTTY
login as: root
root@192.168.1.142's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# ls -lha
drwx----- 1 root root 4096 2013-04-05 12:25 .
drwxr-xr-x 1 root root 4096 2013-04-05 12:03 ..
drwx----- 1 root root 4096 2013-04-05 11:58 .aptitude
-rw-r--r-- 1 root root 570 2013-04-05 11:52 .bashrc
-rw-r--r-- 1 root root 140 2013-04-05 11:52 .profile
drwx----- 1 root root 4096 2013-04-05 12:05 .ssh
root@svr04:~#

2024-04-09T21:00:57+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' aut
password'
2024-04-09T21:00:57+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting servic
2024-04-09T21:00:57+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b's
2024-04-09T21:00:57+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2024-04-09T21:00:58+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm' (
2024-04-09T21:00:58+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyP
2.168.1.135] Terminal Size: 80 24
2024-04-09T21:00:58+0000 [twisted.conch.ssh.session#info] Getting shell
2024-04-09T21:01:01+0000 [HoneyPotSSHTransport,3,192.168.1.135] CMD: ls -lha
2024-04-09T21:01:01+0000 [HoneyPotSSHTransport,3,192.168.1.135] Command found: ls -lha

```

De cara a la integración con Elastic lo ejecutaremos con el siguiente comando para que guarde los logs en un archivo

- `sudo docker run -p 2222:2222/tcp cowrie/cowrie > cowrie.log`

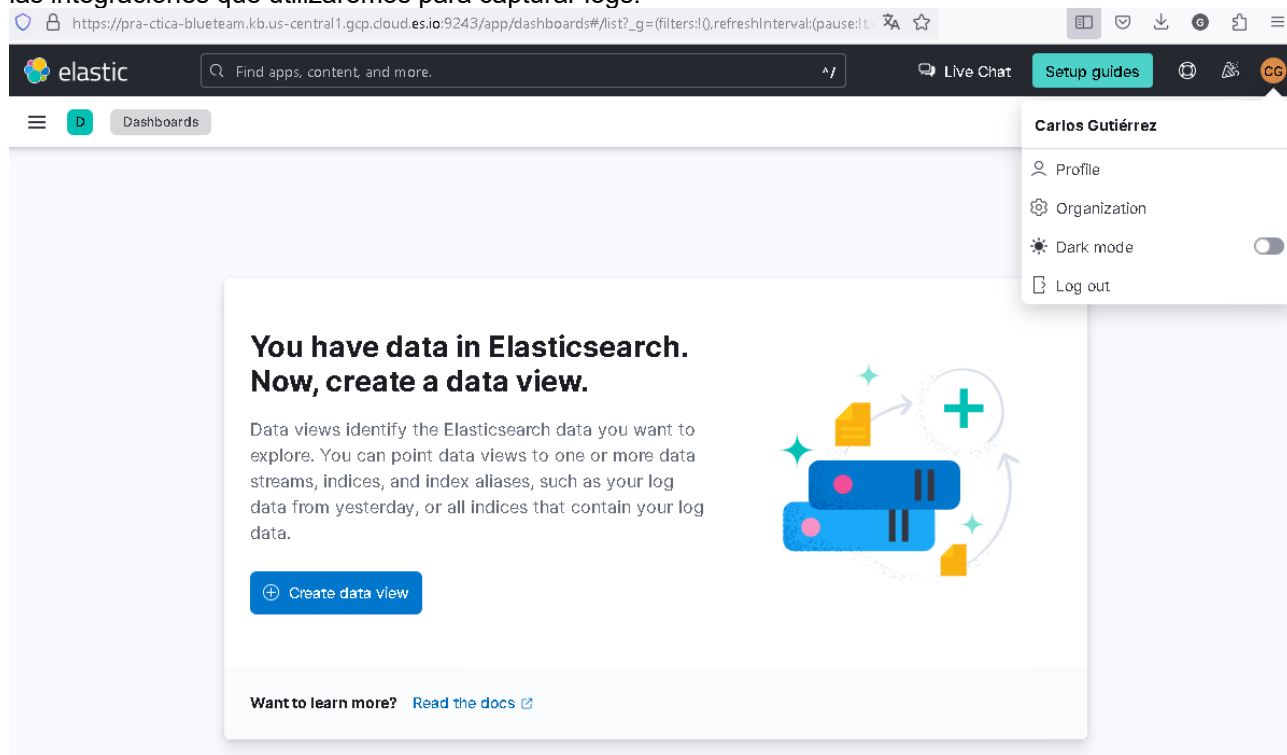
6. Elastic Cloud

<https://www.elastic.co/es/cloud>

Para la práctica utilizaremos la prueba gratuita, dándonos de alta con una cuenta de correo temporal (<https://temp-mail.org/es/>).

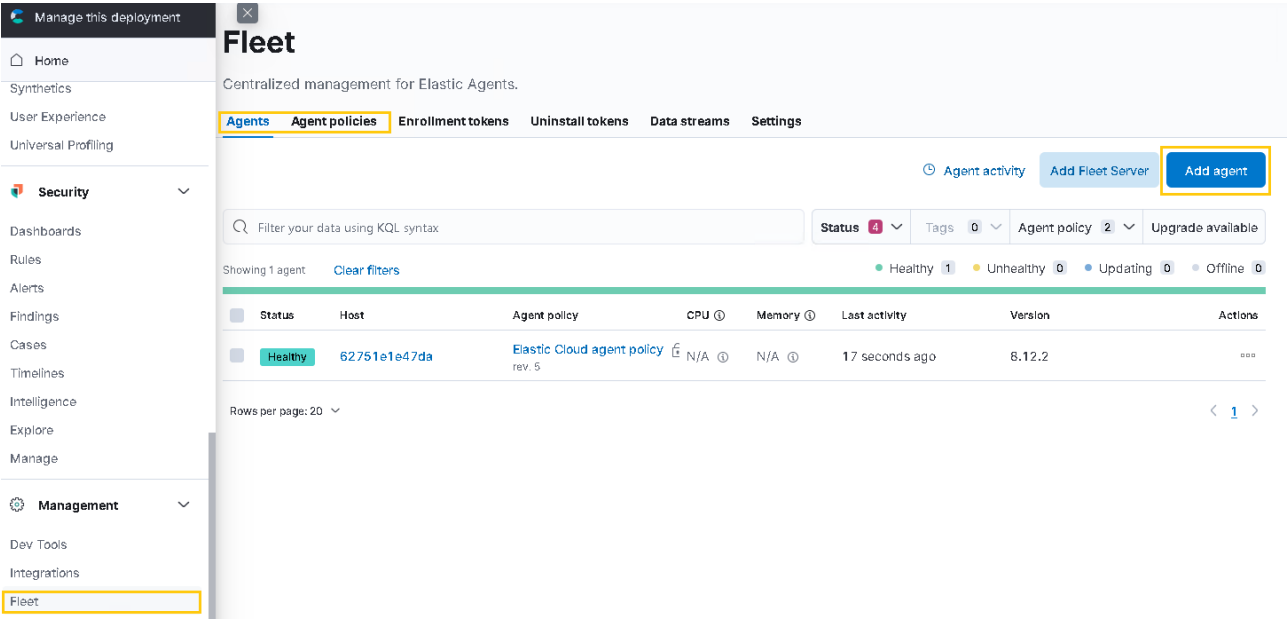
mail: yigiwa7610@storesr.com

Una vez creada la cuenta ya podemos empezar a desplegar los agentes en nuestras máquinas y configurar las integraciones que utilizaremos para capturar logs.

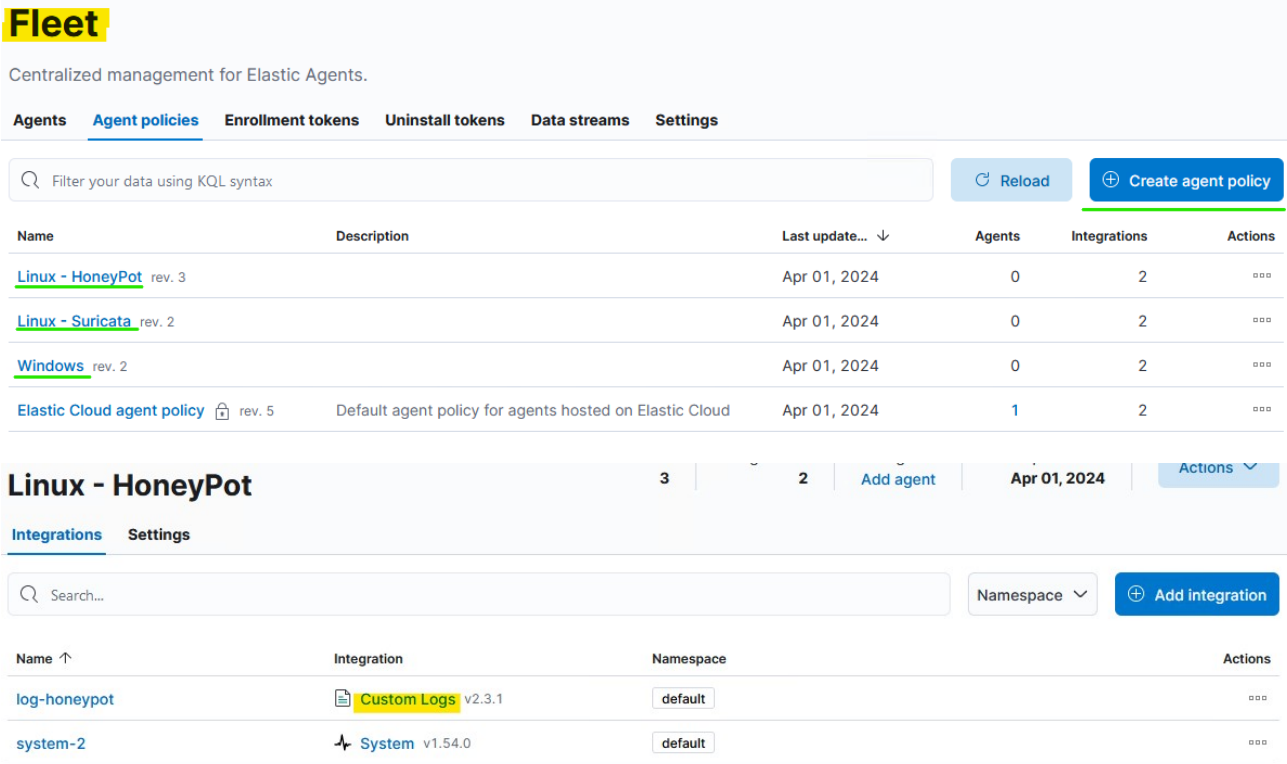


6.1 Agentes y Políticas

En la sección Fleet podemos añadir nuestros agentes y políticas



Primero vamos a crear las políticas a las que luego añadiremos los agentes. También incluiremos cada una de las integraciones que usaremos para extraer los logs de cada máquina.



Linux - Suricata

2

2

Add agent

Apr 01, 2024

Actions

Integrations

Settings

Search...

Namespace

Add integration

Name ↑	Integration	Namespace	Actions
suricata-practica	Suricata v2.21.0	default	...
system-3	System v1.54.0	default	...

Windows

2

2

Add agent

Apr 01, 2024

Actions

Integrations

Settings

Search...

Namespace

Add integration

Name ↑	Integration	Namespace	Actions
Windows Logs	Elastic Defend v8.12.0	default	...
system-1	System v1.54.0	default	...

Ahora añadiremos los agentes y los instalaremos en cada una de las máquinas. Al añadirlo seleccionamos la política a la que queremos añadirlo y copiaremos el código que nos indica según Sistema Operativo para ejecutarlo en la máquina.

Windows

```
Administrator: Windows PowerShell

PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
>> 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
>> 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://585e99bd8d034c6b810550741801bd4b.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=bXk5bm1ZNEJEaQswOW1FcDVWbjk6Nz15a1ZXWmtUeldRNE10eF9TdVg4Zw==
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 [1m45s] Elastic Agent successfully installed, starting enrollment.
[== ] Waiting For Enroll... [1m55s] {"log.level":"info","@timestamp":"2024-04-01T21:14:51.192+0200","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":496},"message":"Starting enrollment to URL: https://585e99bd8d034c6b810550741801bd4b.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version":"1.6.0"}
[== ] Waiting For Enroll... [2m19s] {"log.level":"info","@timestamp":"2024-04-01T21:15:11.082+0200","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0", "ecs.version":"1.6.0"}
[= ] Waiting For Enroll... [2m19s] {"log.level":"info","@timestamp":"2024-04-01T21:15:11.095+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 [2m19s]
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64>
```

Linux

```
(kali@MoneyPot)-[~]
$ 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://585e99bd8d034c6b810550741801bd4b.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=bXk5bm1ZNEJEaQswOW1FcDVWbjk6Nz15a1ZXWmtUeldRNE10eF9TdVg4Zw==
```

```
(kali@Suricata)-[~]
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_
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://585e99bd8d034c6b810550741801bd4b.fleet.us-central1.gcp.cloud.e
1FcFdGazg6Q25zRXlNT3dUenktcXIwcWtwbF92UQ==
```

<input type="checkbox"/>	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version
<input type="checkbox"/>	Healthy	suricata	Linux - Suricata rev. 2	9.46 %	325 MB	15 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	honeypot	Linux - HoneyPot rev. 3	3.25 %	142 MB	32 seconds ago	8.12.2
<input type="checkbox"/>	Healthy	win10	Windows rev. 2	4.70 %	153 MB	41 seconds ago	8.12.2

6.2 Comprobar logs

En el apartado Discover podemos consultar los logs que se hayan ido recopilando. Podemos crear y aplicar diversos filtros para obtener la información que buscamos.

6.2.1 Windows

Creamos un data view que nos muestre los eventos de seguridad

6.2.2 Suricata

Creamos el data view para filtrar los logs de Suricata

Edit data view

[Manage settings and view field details](#)

Name

Suricata

Index pattern

logs-su*

Timestamp field

@timestamp

✓ Your index pattern matches 1 source.

All sources

Matching sources

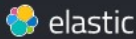
logs-suricata.eve-default

Data stream

Rows per page: 10

<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:47:48.532	network.protocol ssh @timestamp Apr 2, 2024 @ 01:47:48.532 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99 destination.bytes 28,638...
<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:47:48.066	network.protocol ssh @timestamp Apr 2, 2024 @ 01:47:48.066 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99 destination.bytes 28,638...
<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:46:48.485	network.protocol ssh suricata.eve.event_type ssh @timestamp Apr 2, 2024 @ 01:46:48.485 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99...
<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:46:48.485	network.protocol ssh suricata.eve.event_type ssh @timestamp Apr 2, 2024 @ 01:46:48.485 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99...
<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:41:47.430	network.protocol ssh suricata.eve.event_type ssh @timestamp Apr 2, 2024 @ 01:41:47.430 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99...
<input checked="" type="checkbox"/>	Apr 2, 2024 @ 01:41:47.430	network.protocol ssh suricata.eve.event_type ssh @timestamp Apr 2, 2024 @ 01:41:47.430 agent.ephemeral_id 6ddab9f1-ba29-4234-b92e-0e6c17acc40b agent.id 9cfaf4ca-7a4b-4d08-ac99-db3ee8fb1e3c agent.name Suricata agent.type filebeat agent.version 8.12.2 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.250.99...

6.2.3 Cowrie



logs-*

+

Search field names

0

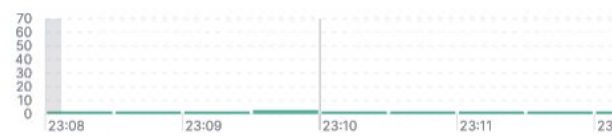
Available fields

67

@timestamp

agent.build.original

173 hits



☒ Apr 9, 2024 @ 23:22:40.397 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:40.397 agent.ephemeral_id 6bdb9d52-2983-46a5-bc8e-b9a972f09cdd agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id system/metrics-default component.type system/metrics container.id elastic-agent-t-de80b0 data_stream.dataset elastic_agent.metricbeat data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49_

☒ Apr 9, 2024 @ 23:22:37.067 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:37.067 agent.ephemeral_id 6bdb9d52-2983-46a5-bc8e-b9a972f09cdd agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 component.binary filebeat component.dataset elastic_agent.filebeat component.id log-default component.type log container.id elastic-agent-de80b0 data_stream.dataset elastic_agent.filebeat data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49_

☒ Apr 9, 2024 @ 23:22:10.399 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:10.399 agent.ephemeral_id 6bdb9d52-2983-46a5-bc8e-b9a972f09cdd agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id system/metrics-default component.type system/metrics container.id elastic-agent-t-de80b0 data_stream.dataset elastic_agent.metricbeat data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49_

☒ Apr 9, 2024 @ 23:22:07.054 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:07.054 agent.ephemeral_id 6bdb9d52-2983-46a5-bc8e-b9a972f09cdd agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 component.binary filebeat component.dataset elastic_agent.filebeat component.id log-default component.type log container.id elastic-agent-de80b0 data_stream.dataset elastic_agent.filebeat data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49_

☒ Apr 9, 2024 @ 23:22:04.542 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:04.542 agent.ephemeral_id e7ad4d71-3851-4211-a0ca-195df085a9a4 agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 data_stream.dataset generic data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 elastic_agent.snapshot false elastic_agent.version 8.12.2 event.agent_id_status verified event.dataset generic event.ingested Apr 9, 2024 @ 23:22:16.000 host.architecture x86_64_

☒ Apr 9, 2024 @ 23:22:04.542 agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:04.542 agent.ephemeral_id e7ad4d71-3851-4211-a0ca-195df085a9a4 agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 agent.type filebeat agent.version 8.12.2 data_stream.dataset generic data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 12405309-9a46-4759-ae6f-28c97e2fdf49 elastic_agent.snapshot false elastic_agent.version 8.12.2 event.agent_id_status verified event.dataset generic event.ingested Apr 9, 2024 @ 23:22:16.000 host.architecture x86_64_

Document

agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:40

agent.version 8.12.2 component.binary metricbeat component.dataset elastic_agent.metricbeat

agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:37

agent.version 8.12.2 component.binary filebeat component.dataset elastic_agent.filebeat data_stream.namespace default data_stream.type logs

agent.name HoneyPot @timestamp Apr 9, 2024 @ 23:22:10

agent.version 8.12.2 component.binary metricbeat component.dataset elastic_agent.metricbeat

host.architecture	x86_64
host.containerized	false
host.hostname	honeypot
host.id	62515a8596cc47a486f33f8642473978
host.ip	[192.168.200.99] fe80::91e1:99c7:d3c2:6cff:fe84:6b44, fe80::d844:2fff:fe84:6b44
host.mac	[02-42-6C-84-6B-44, 08-00-27-DC-BA-A0]
host.name	honeypot