

KeepCoding Bootcamp Ciberseguridad | Edición IX

Módulo de Blue Team

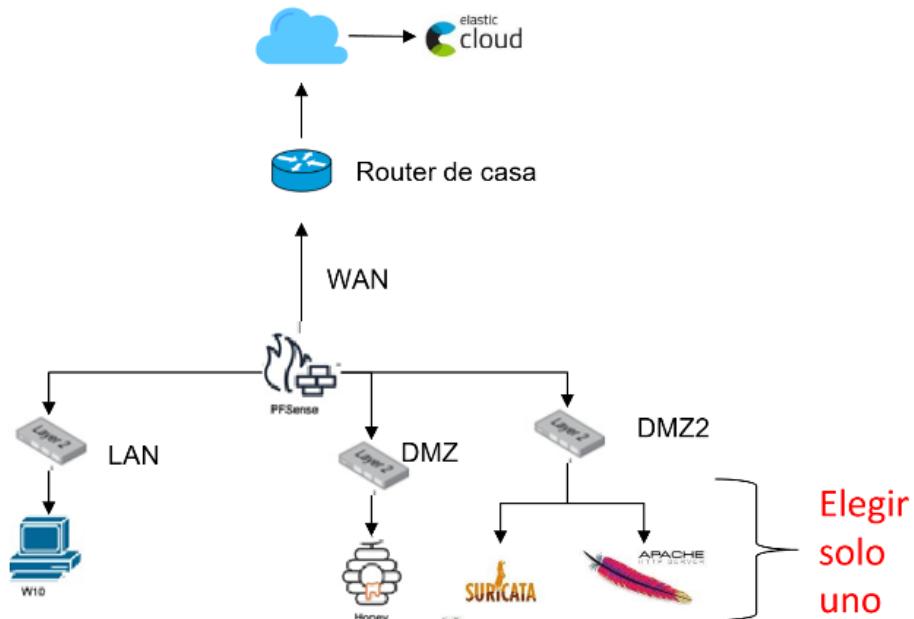
**Informe Práctica Blue Team
SEGUNDA ENTREGA**

**Por: Oscar Uriel Tobar Rios
Fecha del Informe: 26/01/2025**

Contenido

1	EJERCICIO PROPUESTO	3
2	PFSense	3
2.1	Instalación	3
2.2	Configuración	6
2.2.1	Configuración DNS	6
2.2.2	Configuración WAN	7
2.2.3	Configuración LAN	8
2.2.4	Configuración DHCP LAN	9
2.2.5	Configuración REGLAS FIREWALL LAN	10
2.2.6	Configuración DMZ	11
2.2.7	Configuración DHCP DMZ	11
2.2.8	Configuración REGLAS FIREWALL DMZ	13
2.2.9	Configuración DMZ2	13
2.2.10	Configuración DHCP DMZ2	;Error! Marcador no definido.
2.2.11	Configuración REGLAS FIREWALL DMZ2	15
3	SIEM (Elastic)	16
3.1	Configuración Windows 10 (LAN)	16
3.1.1	Configuración del Agente	16
3.1.2	Evidencias de recepción de logs	18
3.2	Configuración Honey (DMZ)	19
3.2.1	Configuración del HoneyPod	19
3.2.2	Configuración del Agente	20
3.2.3	Evidencias de recepción de logs	22
3.3	Configuración Suricata (DMZ2)	23
3.3.1	Configuración Suricata	23
3.3.2	Configuración del Agente	23
3.3.3	Evidencias de recepción de logs	25
3.4	Agentes	25

1 EJERCICIO PROPUESTO



Los requisitos que debe cumplir son los siguientes:

1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
 1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2...) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente. Se propone Suricata o Apache Server como posibles fuentes, pero se deja a elección del alumno.
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.

2 PFSense

Para poder desarrollar el ejercicio lo primero fue hacer la instalación de PFSense. Se utilizó la versión pfSense-CE-2.7.2 y se instaló en una máquina Oracle Linux sobre el virtualizador

2.1 Instalación

Para la Instalación se utilizó la versión pfSense-CE-2.7.2 y se instaló en una máquina Linux con el virtualizador QEMU, donde se montaron las máquinas virtuales de PFSense, Windows, Kali Linux y Parrot Linux.

Para la configuración de la maquina virtual de PfSense se habilitaron 4 tarjetas de red y se ejecutó la instalación como se muestra a continuación:

Etapa 1 of 5

Conexión: QEMU/KVM

Elija cómo le gustaría instalar el sistema operativo

- Medio de instalación local (Imagen ISO o CDROM)
- Instalación por Red (HTTP, FTP, ó NFS)
- Arranque por Red (PXE)
- Importar Imagen de disco existente

Etapa 2 of 5

Ubique el medio de instalación

- Utilice CDROM o DVD
- Utilizar imagen ISO:

No existe un dispositivo presente ▾ Explorar...

Detecta automáticamente un sistema operativo basado en el medio de instalación

Tipo de SO: Desconocido
Versión: Desconocido

Etapa 3 of 5

Elija la configuración de la memoria y de la CPU

Memoria (RAM): - +
Hasta 31906 MiB disponible en el equipo

CPU: - +
Hasta 24 disponible

Etapa 4 of 5

Habilitar almacenamiento para esta máquina virtual

- Crear una imagen de disco para la máquina virtual
- Seleccionar o crear almacenaje personalizado

20,0 - + GiB
34.7 GiB available in the default location

Etapa 5 of 5

Lista para iniciar la instalación

Nombre:

SO: Generic
Instalar: CDROM/ISO local
Memoria: 8192 MiB
CPUs: 4
Almacenamiento: 10.0 GiB ...r/lib/libvirt/images/PFSense2.qcow2
 Personalizar configuración antes de instalar

Selección de red

Red virtual 'default': NAT

pfSense2 en QEMU/KVM@superman.powerteam

Interfaz de Red Virtual

Fuente de red: Dispositivo anfitrión en punto: macvtap

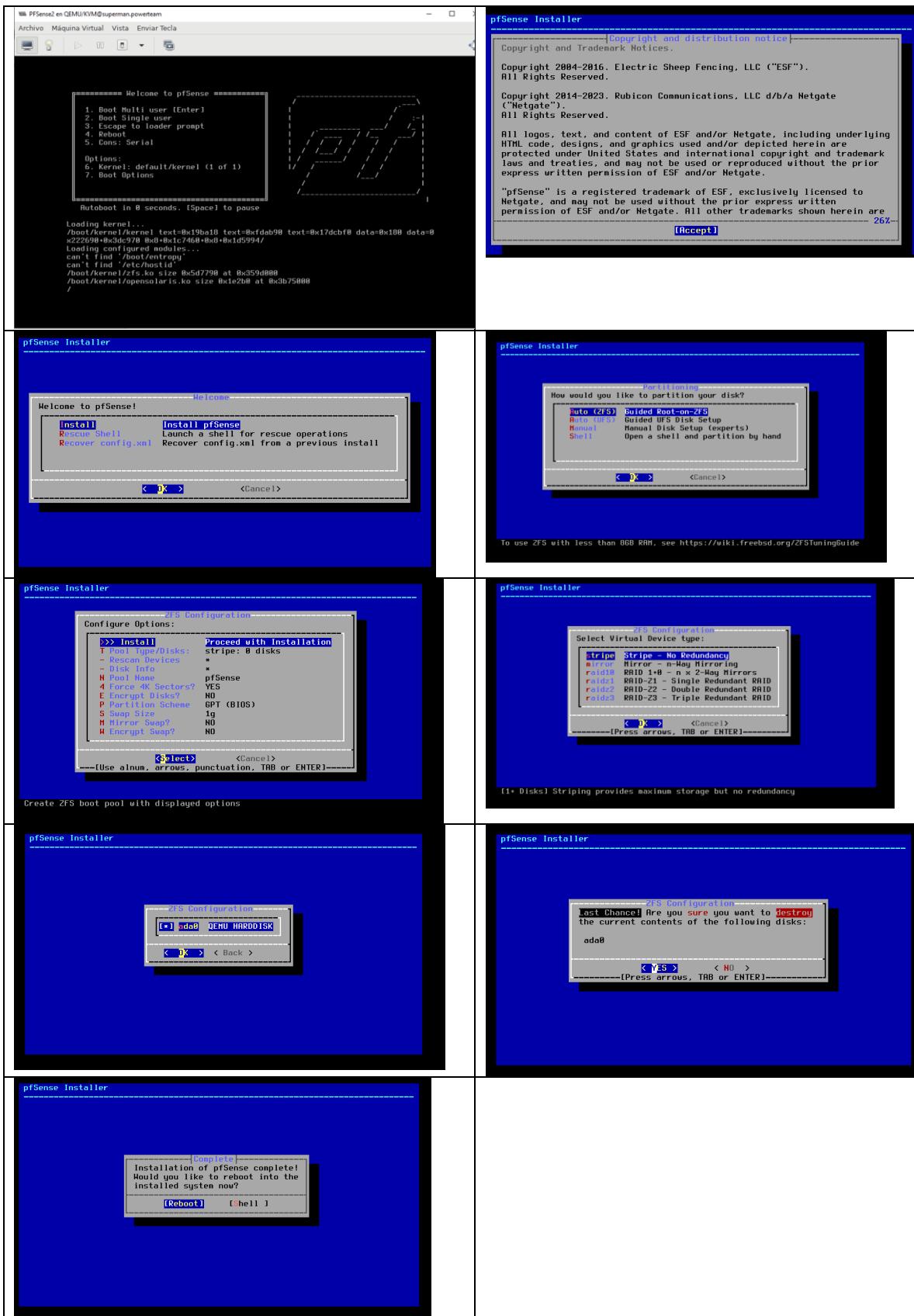
Modo de fuente: Puente

Modelo de dispositivo: Hipervisor por defecto

Dirección MAC: 52:54:00:85:08:d4

Puerto virtual

Agregar hardware ▾ Quitar Cancelar Aplicar



2.2 Configuración

Después de instalar PFSense las tarjetas de Red detectadas son las siguientes:

Interface	Network port	Action
WAN	re0 (52:54:00:a1:67:4f)	
LAN	re1 (52:54:00:2a:d1:df)	Delete
DMZ	re2 (52:54:00:83:a4:f0)	Delete
DMZ2	re3 (52:54:00:3d:29:27)	Delete

Save

2.2.1 Configuración DNS

Para que los equipos que se encuentran en las redes LAN, DMZ y DMZ2 puedan resolver nombre en internet se configuró un servidor DNS con la siguiente configuración:

Services / DNS Resolver / General Settings

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

General Settings Advanced Settings Access Lists

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.	
SSL/TLS Certificate	GUI default (678480beb2b79)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.	
SSL/TLS Listen Port	853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.	
Network Interfaces	All WAN LAN DMZ
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.	
Outgoing Network	All

Network Interfaces	<input type="checkbox"/> All <input type="checkbox"/> WAN <input type="checkbox"/> LAN <input type="checkbox"/> DMZ <input type="checkbox"/> DATA	Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.
Outgoing Network Interfaces	<input type="checkbox"/> All <input type="checkbox"/> WAN <input type="checkbox"/> LAN <input type="checkbox"/> DMZ <input type="checkbox"/> DATA	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. <small>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.</small>	
System Domain Local Zone Type	<input type="checkbox"/> Transparent <small>The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default.</small>	
DNSSEC	<input type="checkbox"/> Enable DNSSEC Support	
Python Module	<input type="checkbox"/> Enable Python Module <small>Enable the Python Module.</small>	
DNS Query Forwarding	<input checked="" type="checkbox"/> Enable Forwarding Mode <small>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).</small>	
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers <small>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.</small>	
DHCP Registration	<input type="checkbox"/> Register DHCP leases in the DNS Resolver <small>If this option is set then machines that provide their hostname when connecting to the DNS server will have their DHCP lease registered in the DNS database.</small>	

2.2.2 Configuración WAN

La tarjeta de Red de la WAN identificado internamente como RE0 se configuro en modo Bridge y desde el DHCP del router se le asigna la ip a esta tarjeta. En este caso se le asigno la IP 192.168.0.9. El resumen de esta interface de red es

Nombre: wan

Id: re0

Tipo: Bridge

Mac: 52:54:00:a1:4f

Red: 192.168.0.0/24

IP: 192.168.0.13

2.2.3 Configuración Firewall WAN

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/12 KiB	IPv4 TCP	*	*	*	222	*	none		Ingreso al Honey	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.200.101	222	*	none		NAT	

Add Delete Toggle Copy Save Separator

2.2.4 Configuración Firewall NAT Port Forward

Firewall / NAT / Port Forward

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	222	192.168.200.101	222		

Add Delete Toggle Save Separator

2.2.5 Configuración LAN

La tarjeta de Red de la LAN identificado internamente como RE1 se configuro en modo de Red interna (solo visible dentro del emulador). Se establecio una dirección IP Fija dentro del segmento de la red 10.10.0.0/16 y se le asignó la primera IP (10.10.0.1).

El resumen de esta interface de red es

Nombre: LAN

Id: re1

Tipo: Interna

Mac: 52:54:00:2a:d1:df

Red: 192.168.100.1/24

Rango de IPs: 192.168.100.1 – 192.168.100.254

IP: 192.168.100.1

2.2.6 Configuración DHCP LAN

Adicionalmente se configuro un servidor DHCP para que entregue direcciones en el rango 192.168.100.10 – 192.168.100.200

LAN	DMZ	DMZ2
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="button" value="Allow all clients"/>	
When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.		
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.	
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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.	
Primary Address Pool		
Subnet	192.168.100.0/24	
Subnet Range	192.168.100.1 - 192.168.100.254	
Address Pool Range	<input type="text" value="192.168.100.10"/>	<input type="text" value="192.168.100.200"/>
From	To	
The specified range for this pool must not be within the range configured on any other address pool for this interface.		
Additional Pools	<input type="button" value="Add Address Pool"/> If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	
Server Options		
WINS Servers	<input type="text" value="WINS Server 1"/>	
	<input type="text" value="WINS Server 2"/>	
DNS Servers	<input type="text" value="192.168.100.1"/>	
	<input type="text" value="1.1.1.1"/>	
	<input type="text" value="8.8.8.8"/>	
	<input type="text" value="DNS Server 4"/>	
	Activar Windows Ve a Configuración para act	

OMAPI

OMAPI Port	<input type="text" value="OMAPI Port"/>	Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.
OMAPI Key	<input type="text" value="OMAPI Key"/>	<input type="checkbox"/> Generate New Key Generate a new key based on the selected algorithm.
Key Algorithm	<input type="text" value="HMAC-SHA256 (current bind9 default)"/>	Set the algorithm that OMAPI key will use.

Other DHCP Options

Gateway	<input type="text" value="192.168.100.1"/>	The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name	<input type="text" value="keepcoding.local"/>	The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List	<input type="text" value="example.com;sub.example.com"/>	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time	<input type="text" value="7200"/>	This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time	<input type="text" value="86400"/>	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

2.2.7 Configuración REGLAS FIREWALL LAN

En el caso de las reglas de firewall para la red LAN se adicionaron las siguientes reglas

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/4.93 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
□ ✓ 0/14 KiB	IPv4 TCP	LAN subnets	*	DMZ2 subnets	22 (SSH)	*	none		Permite conectarse al SSH del Suricata	
□ ✓ 0/0 B	IPv4 TCP	LAN subnets	*	DMZ subnets	22 (SSH)	*	none		Permite conectarse al SSH del Honey	
□ ✓ 0/508 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	
□ ✓ 33/132.65 MiB	IPv4 TCP	*	*	*	sitiosweb	*	none		Trafico Web	
□ ✓ 0/9.18 MiB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
□ ✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	
□ ✘ 0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	*	none	Bloquear otros puertos de la DMZ	
□ ✘ 0/0 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	*	none	Bloquear otros puertos de la DMZ2	

Nota: se han creado reglas para la administración de las máquinas por SSH desde la red LAN.

2.2.8 Configuración DMZ

La tarjeta de Red de la DMZ identificado internamente como RE2 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija 192.168.200.1/24

Nombre: DMZ

Id: re2

Tipo: Interna

Mac: 52:54:00:83:a4:f0

Red: 192.168.200.1/24

Rango de IPs: 192.168.200.1 - 192.168.200.254

IP: 192.168.200.1

2.2.9 Configuración DHCP DMZ

Se configuro un servidor DHCP para la red de DMZ que entregue direcciones en el rango 192.168.200.100 hasta el 192.168.200.150

LAN	DMZ	DMZ2
General DHCP Options		
DHCP Backend	ISC DHCP	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ interface	
BOOTP	<input type="checkbox"/> Ignore BOOTP queries	
Deny Unknown Clients	<input type="button" value="Allow all clients"/> When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.	
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.	
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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.	

Primary Address Pool

Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	<input type="text" value="192.168.200.100"/> <input type="text" value="192.168.200.150"/> From <input type="text" value="192.168.200.100"/> To <input type="text" value="192.168.200.150"/> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
Additional Pools	+ Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Server Options

WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.200.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>
	DNS Server 4
Activar Windows Ve a Configuración para Windows.	

Other DHCP Options

Gateway	<input type="text" value="192.168.200.1"/>
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.	
Domain Name	<input type="text" value="keepcoding.local"/>
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.	
Domain Search List	<input type="text" value="example.com;sub.example.com"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	
Default Lease Time	<input type="text" value="7200"/>
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.	
Maximum Lease Time	<input type="text" value="86400"/>
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.	
Failover peer IP	<input type="text"/>
Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.	
Static ARP	<input type="checkbox"/> Enable Static ARP entries
Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.	
Time format change	<input checked="" type="checkbox"/> Change DHCP display lease time from UTC to local time
By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.	
Activar Windows Ve a Configuración para a	

2.2.10 Configuración REGLAS FIREWALL DMZ

Para las reglas del DMZ se establecieron cuatro reglas así:

The screenshot shows a web-based interface for managing firewall rules. At the top, there's a header with tabs: Floating, WAN, LAN, DMZ (which is selected), and DMZ2. Below the header is a table titled "Rules (Drag to Change Order)". The table has columns for: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are five rows of rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloqueo red lan	
0/17 KIB	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloqueo red DMZ2	
0/0 B	IPv4 *	*	*	192.168.200.101	*	*	none		Habilita todos los puertos a la maquina hony	
39/202 Kib	IPv4 UDP	192.168.200.101	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	
51/4.16 Mib	IPv4 TCP	192.168.200.101	*	*	sitiosweb	*	none		Permitir trafico web	

At the bottom of the table are several action buttons: Add (up/down arrows), Delete, Toggle, Copy, Save, and Separator. A note "Vé a Configuración para activar" is also present.

2.2.11 Configuración DMZ2

La tarjeta de Red de la DMZ2 identificado internamente como RE3 se configuro en modo de Red interna (solo visible dentro del emulador). Se estableció una dirección IP Fija dentro del segmento de la red (192.168.250.1).

Nombre: DMZ2

Id: re3

Tipo: Interna

Mac: 52:54:00:3d:29:27

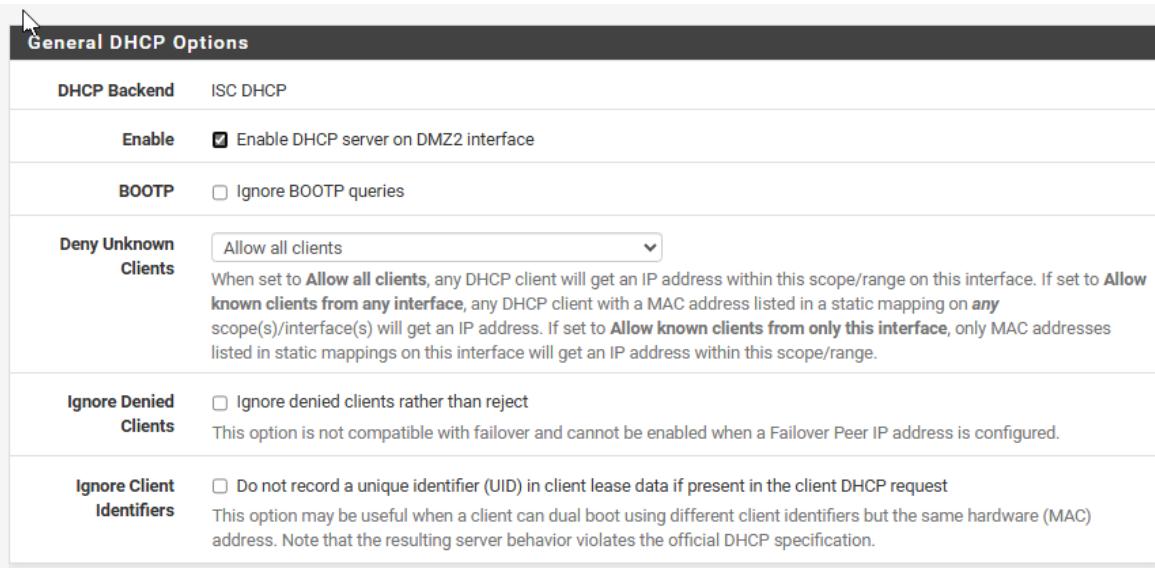
Red: 192.168.250.1/24

Rango de IPs: 192.168.250.1 - 192.168.250.254

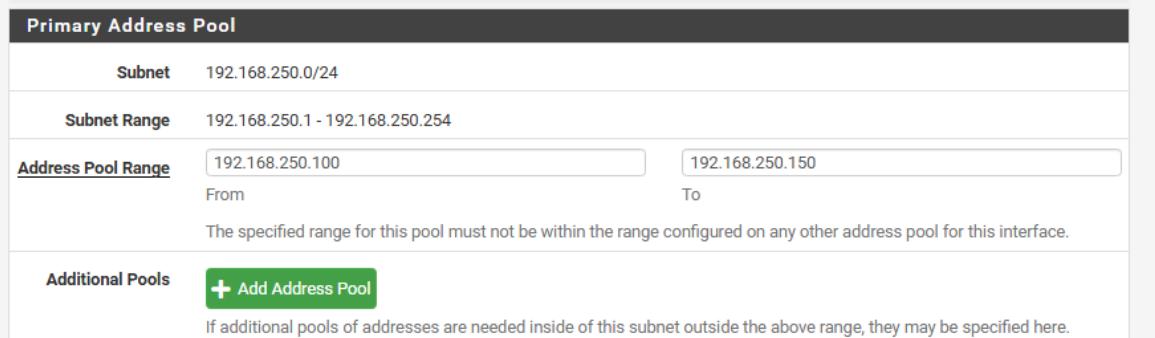
IP: 192.168.250.1

2.2.12 Configuración DHCP DMZ2

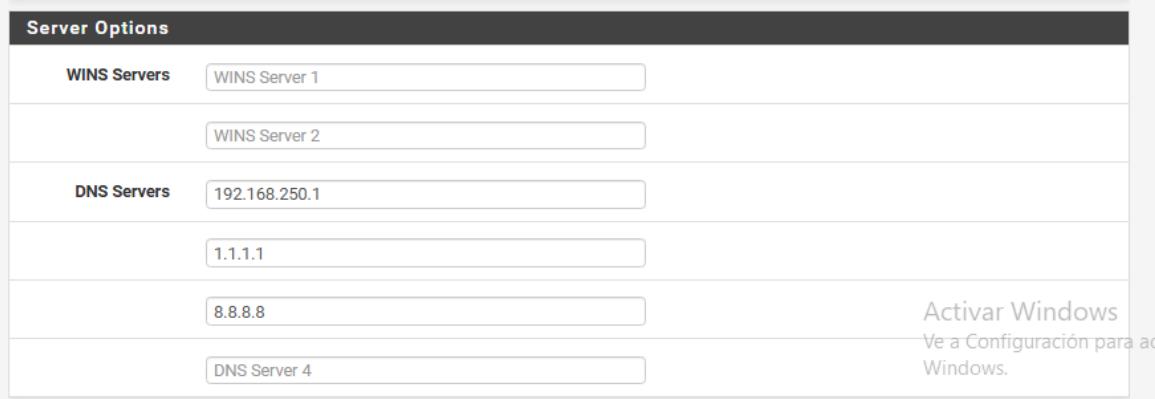
Se configuro un servidor DHCP para la red de DMZ2 que entregue direcciones en el rango 192.168.250.100 hasta el 192.168.250.150

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/> When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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.

Primary Address Pool

Subnet	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	<input type="text" value="192.168.250.100"/> From <input type="text" value="192.168.250.150"/> To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	<input type="button" value="+ Add Address Pool"/> If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.250.1"/> <input type="text" value="1.1.1.1"/> <input type="text" value="8.8.8.8"/>
DNS Server 4	Activar Windows Ve a Configuración para activar Windows.

Other DHCP Options	
Gateway	<input type="text" value="192.168.250.1"/> The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name	<input type="text" value="keepcoding.local"/> The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List	<input type="text" value="example.com;sub.example.com"/> The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time	<input type="text" value="7200"/> This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time	<input type="text" value="86400"/> This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP	<input type="text"/> Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.
Static ARP	<input type="checkbox"/> Enable Static ARP entries Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.
Time format change	<input checked="" type="checkbox"/> Change DHCP display lease time from UTC to local time By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.

2.2.13 Configuración REGLAS FIREWALL DMZ2

Para las reglas del DMZ2 se establecieron dos reglas así:

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X 0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloqueo red DMZ	 
<input type="checkbox"/>	X 0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloqueo red LAN	 
<input type="checkbox"/>	✓ 22/1.41 MiB	IPv4 TCP	DMZ2 subnets	*	*	sitiosweb	*	none		Trafico web	 
<input type="checkbox"/>	✓ 32/126 KiB	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none		Permitir Trafico del DNS	 

3 SIEM (Elastic)

Basados en la configuración establecida como se muestra a continuación

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

WAN (wan)      -> re0          -> v4/DHCP4: 192.168.0.13/24
LAN (lan)      -> re1          -> v4: 192.168.100.1/24
DMZ (opt1)     -> re2          -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> re3          -> 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: █
```

Se procedió a configurar en Elastic CLOUD la configuración de los agentes para configurar en Elvio de logs

3.1 Configuración Windows 10 (LAN)

3.1.1 Configuración del Agente

En una máquina virtual de Windows 10 llamada DESKTOP-PGGB831 que instaló el agente de Elastic elastic-agent-8.17.0 para Windows

Para su instalación en Windows después de descomprimirlo se ejecuto la instalación con este comando

```
.\elastic-agent.exe install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RlbDhwczQybjE6aDZXYzQtR0tSYXlpdTN6QU01ekN3QQ==
```

< View all agents

DESKTOP-PGGB831

Actions ▾

[Agent details](#) [Logs](#) [Diagnostics](#)

Overview

CPU	1.82 %	View more agent metrics
Memory	170 MB	
Status	Healthy	
Last activity	29 seconds ago	
Last checkin message	Running	
Agent ID	da9a681c-3265-4f44-a820-d74d0444418d	
Agent policy	Políticas LAN rev. 2	
Agent version	8.17.0	
Host name	DESKTOP-PGGB831	
Host ID	caa1d453-ab67-4999-bba9-2a27f98fe24d	
Output for integrations	Default output	
Output for monitoring	Default output	
Logging level	info	
Privilege mode	Running as root	
Agent release	stable	
Platform	windows	
Monitor logs	Enabled	
Monitor metrics	Enabled	
Tags	-	

Integrations

- > windows-1
- > system-2

Una vez instalado desde Elastic cloud que añadió una integración para leer los logs de Windows así:

< Cancel

Edit Windows integration

Modify integration settings and deploy changes to 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: windows-1
Description: Optional

[Advanced options](#)

Collect events from the following Windows event log channels:

[Change defaults ^](#)

AppLocker/EXE and DLL
Microsoft-Windows-AppLocker/EXE and DLL channel

Preserve original event
Preserves a raw copy of the original XML event, added to the field event.event.original

[Advanced options](#)

AppLocker/MSI and Script
Microsoft-Windows-AppLocker/MSI and Script channel

Preserve original event
Preserves a raw copy of the original XML event, added to the field event.event.original

[Advanced options](#)

Packaged app-Deployment
Microsoft-Windows-AppLocker/Packaged app-Deployment channel

Preserve original event
Preserves a raw copy of the original XML event, added to the field event.event.original

Collect Windows perfmon and service metrics Change defaults ↗

Windows perfmon metrics
Collect Windows perfmon metrics

Perfmon Group Measurements By Instance
 Enabling this option will send all measurements with a matching perfmon instance as part of a single event.

Perfmon Ignore Non Existant Counters
 Enabling this option will make sure to ignore any errors caused by counters that do not exist

Perfmon Refresh Wildcard Counters
 Enabling this option will cause the counter list to be retrieved after each fetch, rather than once at start time.

Perfmon Queries

```
- object: 'Process'
  instance: ['*']
  counters:
    - name: '% Processor Time'
      field: cpu_perc
      format: "float"
    - name: "Working Set"
```

Period

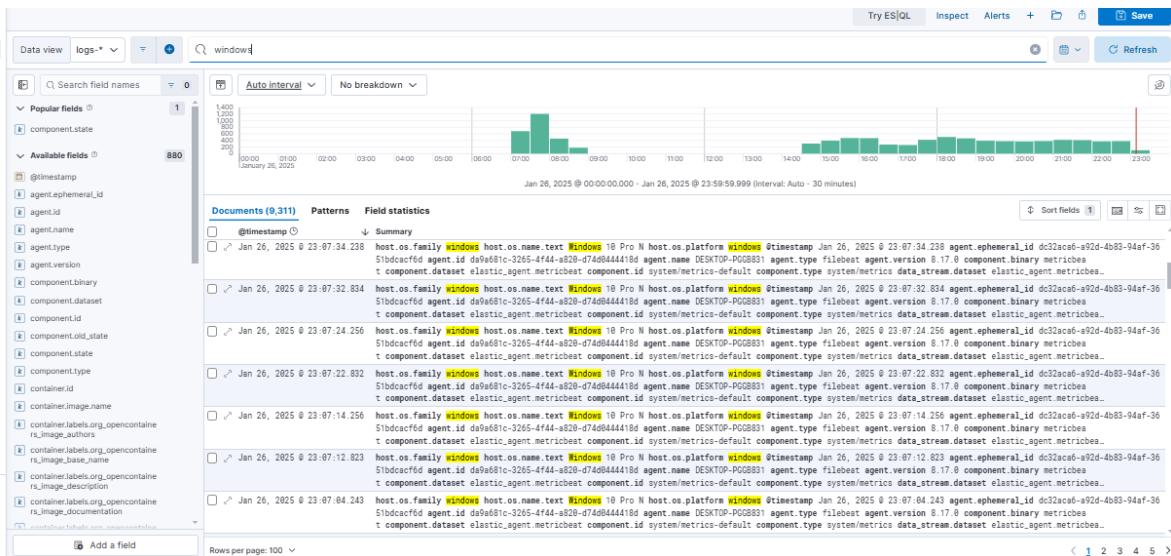
[Advanced options](#)

Windows service metrics
Collect Windows service metrics

Period

Processors Options ↗

3.1.2 Evidencias de recepción de logs



Se deja un ejemplo de uno de los mensajes en

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciaswindows3.txt>

EL archivo comprimido con todos los mensajes desde la maquina Windows recibidos en Elastic y exportado para el día 26 de Enero es este

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/windows3.zip>

3.2 Configuración Honey (DMZ)

3.2.1 Configuración del HoneyPod

En la Maquina Kali Linux se instalo el Honey que para el ejercicio se instalo un HoneyPod de SSH llamado cowrie

Inicio de honey

docker run -d -p 2222:2222 cowrie/cowrie:latest

```
(kali㉿kali)-[~/logs/ssh]
$ docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED      STATUS        PORTS
           S
b84ed29c370f   cowrie/cowrie:latest   "/cowrie/cowrie-env/..."   15 minutes ago
             Up 15 minutes   0.0.0.0:2222→2222/tcp, :::2222→2222/tcp, 2223/tcp   kind
               _cori
```

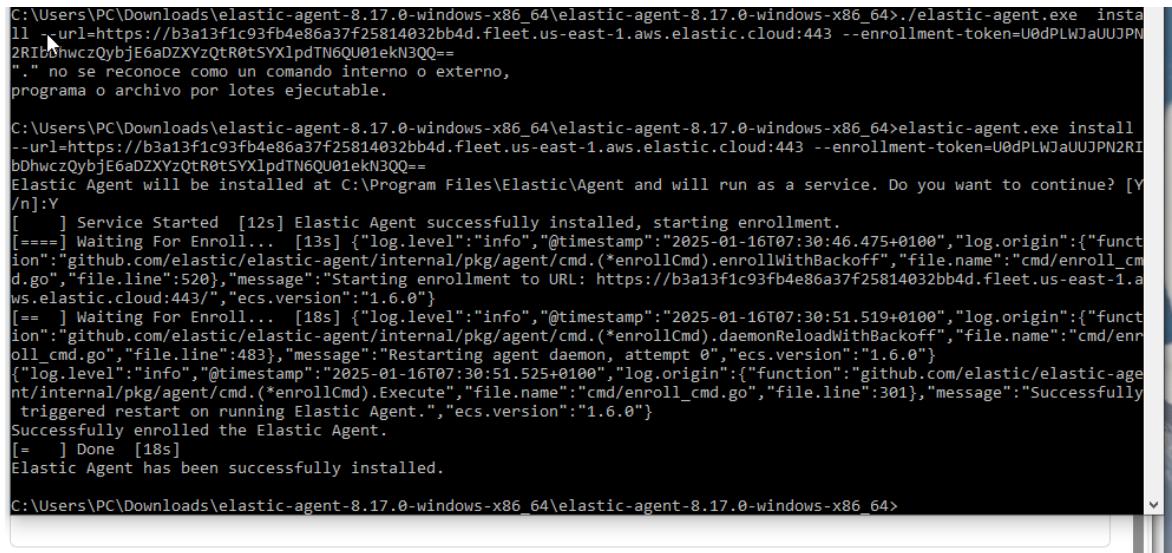
docker logs -f kind_cori > cowri.log

```
(kali㉿kali)-[~/logs/ssh]
$ docker logs -f kind_cori > cowri.log
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
    b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

3.2.2 Configuración del Agente

Una vez funcionando que instalo en agente de elastic asi:

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz  
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz  
cd elastic-agent-8.17.0-linux-x86_64  
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=QTJNMWJKUUJPN2RlbDhwC2tXbFU6ZVIGSWlHZGJTbFNKajhETWlnd2J5dw==
```



The screenshot shows a terminal window on a Windows operating system. The command being run is:

```
C:\Users\PC\Downloads\elastic-agent-8.17.0-windows-x86_64\elastic-agent-8.17.0-windows-x86_64>./elastic-agent.exe install  
--url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=U0dPLWJaUUJPN2RlbDhwC2tXbFU6ZVIGSWlHZGJTbFNKajhETWlnd2J5dw==  
" ." no se reconoce como un comando interno o externo,  
programa o archivo por lotes ejecutable.
```

After this, the user is prompted for enrollment:

```
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]: Y
```

The process continues with logs indicating the agent is starting and enrolling:

```
[=] Service Started [12s] Elastic Agent successfully installed, starting enrollment.  
[==] Waiting For Enrollment... [13s] {"log.level": "info", "@timestamp": "2025-01-16T07:30:46.475+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": 520}, "message": "Starting enrollment to URL: https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-1.aws.elastic.cloud:443/", "ecs.version": "1.6.0"}  
[==] Waiting For Enrollment... [18s] {"log.level": "info", "@timestamp": "2025-01-16T07:30:51.519+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": 483}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}  
{"log.level": "info", "@timestamp": "2025-01-16T07:30:51.525+0100", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute", "file.name": "cmd/enroll_cmd.go", "file.line": 301}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}  
Successfully enrolled the Elastic Agent.  
[=] Done [18s]  
Elastic Agent has been successfully installed.
```

The terminal ends with the path:

```
C:\Users\PC\Downloads\elastic-agent-8.17.0-windows-x86_64\elastic-agent-8.17.0-windows-x86_64>
```

Luego en Elastic se configuro una integración para logs personalizados en la maquina Kali asi

Overview

CPU ⓘ	2.19 %
Memory ⓘ	252 MB
Status	Healthy
Last activity	21 seconds ago
Last checkin message	Running
Agent ID	a84ffcc3-fe20-432e-94ad-4fc01e4f4098
Agent policy	Políticas DMZ rev. 12
Agent version	8.17.0 + Upgrade available
Host name	kali
Host ID	30e662c5c81d4191bd2444a79c97d2e0
Output for integrations	Default output
Output for monitoring	Default output
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	kali
Monitor logs	Enabled

Integrations

- > Docker docker-1
- > System system-1 (copy)
- > Log log cowri

Adicionalmente Tambien se tomo una integración para leer los logs del docker

Edit Docker integration

Modify integration settings and deploy changes to 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: docker-1

Description: Integracion ssh

Optional

Advanced options

Collect Docker metrics Change defaults ▾

Collect Docker container logs Change defaults ▾

Collect Docker container logs

Condition: Condition to filter when to apply this datastream. Refer to Docker provider to find the available keys and to Conditions on how to use the available keys in conditions.

Advanced options

2 Where to add this integration?

For existing hosts:

Agent policies

Agent policies are used to manage a group of integrations across a set of agents.

Agent policies: Políticas DMZ

1 agent is enrolled with the selected agent policies.

3.2.3 Evidencias de recepción de logs

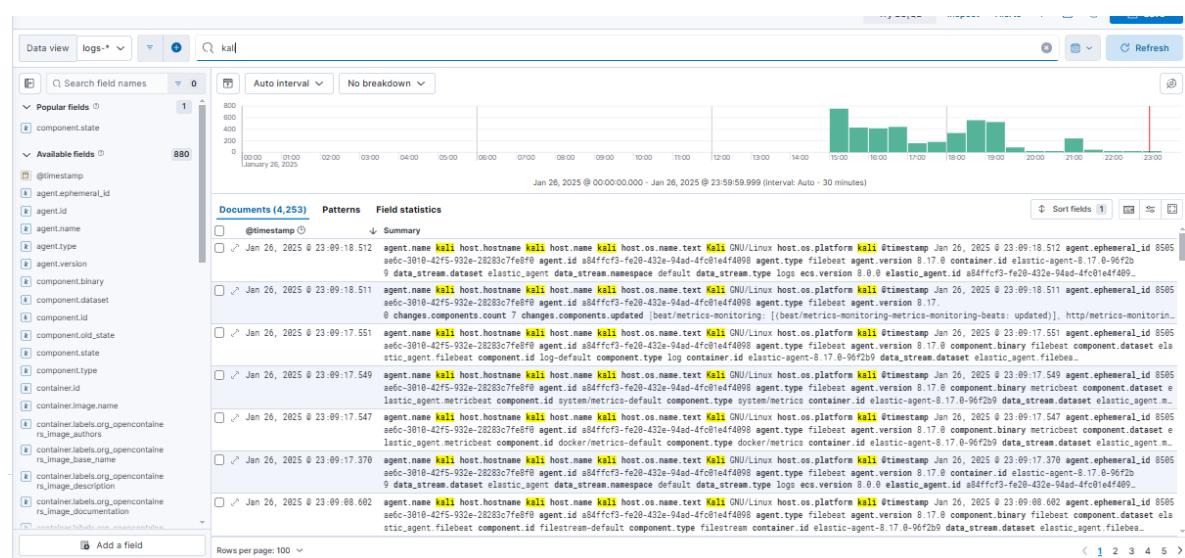
Para el ejemplo se utilizó el honeyPod del ssh instalado para evidenciar que si se genera el log y se transmitió al elastic así:

```
C:\Users\PC\.ssh>ssh root@192.168.16.50 -p 2222
root@192.168.16.50'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:~# cd a
bash: cd: a: No such file or directory
root@svr04:~# ls
root@svr04:~# mkdir a
root@svr04:~# cd a
root@svr04:~/a# ls
root@svr04:~/a#
```



Se deja un ejemplo dos de los mensajes de el Honey de SSH en

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciassh3.txt>

El archivo comprimido con todos los mensajes desde la maquina Kali recibidos en Elastic y exportado para el día 26 de Enero es este

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/kali-ssh3.csv>

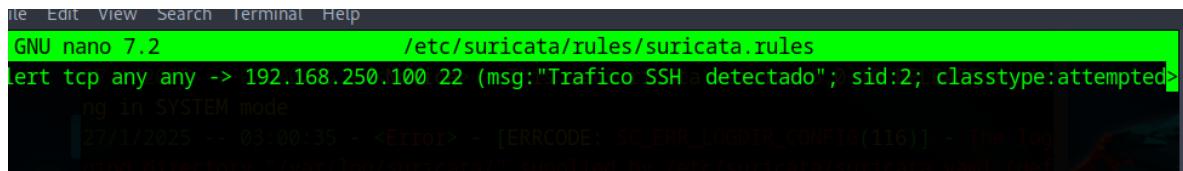
3.3 Configuración Suricata (DMZ2)

3.3.1 Configuración Suricata

Para la instalación de suricata en el Parrot Linux se ejecutaron estos comandos

```
sudo apt update  
sudo apt install suricata
```

se creo el archivo /etc/suricata/rules/suricata.rules y se aplico esta regla



```
File Edit View Search Terminal Help  
GNU nano 7.2 /etc/suricata/rules/suricata.rules  
alert tcp any any -> 192.168.250.100 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted;)  
ng in SYSTEM mode  
[27/1/2025 -- 03:00:35 - <Error> - [ERRCODE: SC_ERR_LOGDIR_CONFIG(116)] - The log
```

Luego como administrador se inicio el programa asi:

```
suricata -c /etc/suricata/suricata.yaml -i ens3
```

3.3.2 Configuración del Agente

Se instalo el agente para Linux de elastic asi

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-  
linux-x86_64.tar.gz
```

```
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
```

```
cd elastic-agent-8.17.0-linux-x86_64
```

```
sudo ./elastic-agent install --url=https://b3a13f1c93fb4e86a37f25814032bb4d.fleet.us-east-  
1.aws.elastic.cloud:443 --enrollment-  
token=QTJNMWJKUUJPN2RlbDhwC2tXbFU6ZVlGSWIHZGJTbFNKajhETWlnd2J5dw==
```

Luego desde Elastic se configuro una nueva integración asi

View all agent policies	Revision 6	Integrations 2	Agents 1 agent	Last updated on Jan 16, 2025	Actions
Linux/Suricata					
Integrations Settings					
<input type="text" value="Search..."/>			Namespace ▼	Add integration	
Integration policy ↑	Integration ↓	Namespace	Output	Actions	
suricata-2	Suricata v2.21.4	default ①	Default output ①	...	
system-1	System v1.63.2	default	Default output ①	...	

1 Configure integration

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

Integration name	suricata-2
Description	Optional
Advanced options	

Collect Suricata eve logs (input: logfile) [Change defaults](#) ^

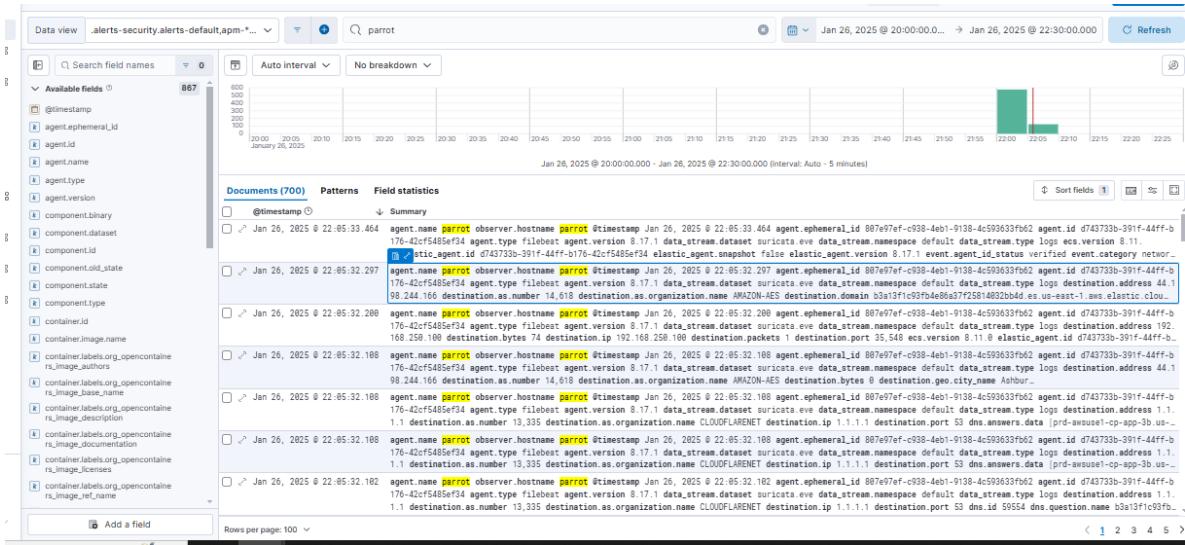
<input checked="" type="checkbox"/> Suricata eve logs (log)	Paths
Collect Suricata eve logs using log input	/var/log/suricata/eve.json
Add row	
<input checked="" type="checkbox"/> Preserve original event	
Preserves a raw copy of the original event, added to the field event.original	
Advanced options	

2 Where to add this integration?

For existing hosts:

Agent policies Agent policies are used to manage a group of integrations across a set of agents.	Agent policies
Linux/Suricata	X ▼
1 agent is enrolled with the selected agent policies.	

3.3.3 Evidencias de recepción de logs



La información de un mensaje lo puede ver aquí

<https://github.com/oscartobar/practicaskeepcoding/blob/main/BlueTeam/evidenciasuricata3.txt>

La información de todos los logs de suricata recibidos en elastic y transmitidos desde el parrot el día 26 de enero se dejan aquí

3.4 Agentes

La información resumida de los agentes configurados en Elastic es la siguiente:

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. [Learn more](#).

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

Ingest Overview Metrics Agent Info Metrics Agent activity [Add agent](#)

Filter your data using KQL syntax Status 4 Tags 0 Agent policy 3 Upgrade available

Showing 3 agents [Clear filters](#) Healthy 3 Unhealthy 0 Updating 0 Offline 0 Inactive 0 Unenrolled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last acti...	Version	Actions
<input type="checkbox"/>	Healthy	DESKTOP-PGGB831	Politicas LAN rev. 2	1.74 %	170 MB	25 seconds ago	8.17.0	
<input type="checkbox"/>	Healthy	parrot	Linux/Suricata rev. 6	2.70 %	233 MB	16 seconds ago	8.17.0	
<input type="checkbox"/>	Healthy	kali	Politicas DMZ rev. 9	2.40 %	240 MB	14 seconds ago	8.17.0	

Rows per page: 20 < 1 >

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

Filter your data using KQL syntax Reload Create agent policy

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Politicas DMZ rev. 9 Politicas para servidores en DMZ	Jan 18, 2025	0 / 1 (1)	4	
Linux/Suricata rev. 6	Jan 16, 2025	0 / 1 (1)	2	
Politicas LAN rev. 2	Jan 16, 2025	0 / 1 (1)	2	

Rows per page: 20 < 1 >

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

Dataset		Type	Namespace	Integration	Last activity	Size	Actions
elastic_agent.elastic_agent	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	37.11mb	...
elastic_agent.filebeat	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	18.03mb	...
elastic_agent.filebeat_input	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	7.26mb	...
elastic_agent.metricbeat	metrics	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:18:17 PM	31.61mb	...
windows.service	metrics	default	windows	windows	Jan 18, 2025 @ 2:18:15 PM	47.79mb	...
fleet_server.agent_status	metrics	default	fleet_server	fleet_server	Jan 18, 2025 @ 2:17:40 PM	1.18mb	...
fleet_server.agent_versions	metrics	default	fleet_server	fleet_server	Jan 18, 2025 @ 2:17:40 PM	686.23kb	...
system.application	logs	default	system	system	Jan 18, 2025 @ 2:17:36 PM	1.04mb	...
elastic_agent	logs	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.18mb	...
elastic_agent.filebeat	logs	default	elastic_agent	elastic_agent	Jan 18, 2025 @ 2:12:39 PM	1.32mb	...
system.security	logs	default	system	system	Jan 18, 2025 @ 2:12:36 PM	19.72mb	...
system.system	logs	default	system	system	Jan 18, 2025 @ 12:43:43 PM	597.16kb	...
docker.container_logs	logs	default	docker	docker	Jan 18, 2025 @ 11:32:22 AM	390.52kb	...
generic	logs	default	log	log	Jan 18, 2025 @ 11:32:22 AM	94.71kb	...
docker.event	metrics	default	docker	docker	Jan 18, 2025 @ 11:06:00 AM	24.08kb	...
windows.powershell	logs	default	windows	windows	Jan 18, 2025 @ 9:54:14 AM	87.4kb	...
windows.powershell_operational	logs	default	windows	windows	Jan 18, 2025 @ 1:31:22 AM	27.58kb	...

Rows per page: 20 ▾

◀ 1 2 ▶

[View all agent policies](#)

Políticas DMZ

Políticas para servidores en DMZ

[Integrations](#) [Settings](#)

Revision 12 | Integrations 3 | Agents 1 agent | Last updated on Jan 26, 2025

[Actions](#) ▾

Integration policy	Integration	Namespace	Output	Actions
docker-1	Docker v2.13.1	default	Default output	...
log cowri	Custom Logs v2.3.3	default	Default output	...
system-1 (copy)	System v1.63.2	default	Default output	...

< View all agent policies

Linux/Suricata

Integrations Settings

Revision 6 Integrations 2 Agents 1 agent Last updated on Jan 16, 2025 Actions

Search... Namespace Add integration

Integration policy	Integration	Namespace	Output	Actions
suricata-2	Suricata v2.21.4	default	Default output	...
system-1	System v1.63.2	default	Default output	...