

Aquí podemos ver La Wan que se asigna automáticamente, y las direcciones de cada interfaz de red que les asigne.

pfSense

Community Edition

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Status / Dashboard

System Information

Name

UTM.Keepcoding.local

User

admin@192.168.250.100 (Local Database)

System

VirtualBox Virtual Machine
Netgate Device ID: 73aa7ede3d612f2c6117

BIOS

Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006

Version

2.7.2-RELEASE (amd64)
built on Wed Dec 6 21:10:00 CET 2023
FreeBSD 14.0-CURRENT

The system is on the latest version.
Version information updated at Sat Oct 12 9:28:23 CEST 2024

CPU Type

Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz
AES-NI CPU Crypto: Yes (Inactive)
QAT Crypto: No

Hardware crypto

Inactive

Kernel PTI

Enabled

MDS Mitigation

Inactive

Uptime

00 Hour 47 Minutes 13 Seconds

Current date/time

Sat Oct 12 10:14:27 CEST 2024

DNS server(s)

127.0.0.1

100.100.1.1

100.90.1.1

2a0c:5a80:0:2::1

2a0c:5a84:0:2::1

fe80::1

1.1.1.1

Last config change

Fri Oct 11 20:10:09 CEST 2024

State table size

0% (88/305000) Show states

MBUF Usage

1% (5334/1000000)

Load average

0.49, 0.56, 0.58

CPU usage

6%

Memory usage

10% of 3059 MIB

SWAP usage

0% of 1024 MIB

Disks

Mount

Used

Size

Usage

> /

843M

15G

6% of 15G (zfs)

Netgate Services And Support

Contract type

Community Support

Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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

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

• Upgrade Your Support

• Community Support Resources

• Netgate Global Support FAQ

• Official pfSense Training by Netgate

• Netgate Professional Services

• Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces

WAN

↑

1000baseT <full-duplex>

192.168.1.206
2a0c:5a80:320b:6800:a00:27ff:fe4d:8b0b

LAN

↑

1000baseT <full-duplex>

192.168.100.1

DMZ

↑

1000baseT <full-duplex>

192.168.200.1

DMZ2



↑

1000baseT <full-duplex>


192.168.250.1

Aquí de una forma mas detallada, en status – interfaces:

WAN Interface (wan, em0)

Status	up 
DHCP	up  <input type="checkbox"/> Relinquish Lease
MAC Address	08:00:27:4d:8b:0b
IPv4 Address	192.168.1.206
Subnet mask IPv4	255.255.255.0
Gateway IPv4	192.168.1.1
IPv6 Link Local	fe80:a00:27ff:fe4d:8b0b%em0
IPv6 Address	2a0c:5a80:320b:6800:a00:27ff:fe4d:8b0b
Subnet mask IPv6	128
Gateway IPv6	fe80::1%em0
DNS servers	100.100.1.1 100.90.1.1 2a0c:5a80:0:2::1 2a0c:5a84:0:2::1 fe80::1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	233215/88163 (285.32 MiB/9.83 MiB)
In/out packets (pass)	233215/88163 (285.32 MiB/9.83 MiB)
In/out packets (block)	77/0 (10 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	71097 (24/s)


LAN Interface (lan, em1)

Status	up 
MAC Address	08:00:27:03:12:2d
IPv4 Address	192.168.100.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80:a00:27ff:fe03:122d%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	67913/214731 (6.46 MiB/281.75 MiB)
In/out packets (pass)	67913/214731 (6.46 MiB/281.75 MiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0
Interrupts	78815 (27/s)

DMZ Interface (opt1, em2)

Status	up 
MAC Address	08:00:27:05:48:8e
IPv4 Address	192.168.200.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80:a00:27ff:fe05:488e%em2
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0
Interrupts	3 (0/s)

DMZ2 Interface (opt2, em3)

Status	up 
MAC Address	08:00:27:f7:e7:f7
IPv4 Address	192.168.250.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80:a00:27ff:fe7f:e7f7%em3
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	16852/15205 (3.74 MiB/5.34 MiB)
In/out packets (pass)	16852/15205 (3.74 MiB/5.34 MiB)
In/out packets (block)	26/0 (35 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	19444 (7/s)

FIREWALL

Firewall / Rules / WAN

Floating **WAN** LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/2 KB	IPv4 ICMP	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/41 KB	IPv4 *	*	*	192.168.200.99	*	*	none		permitir acceso de wan a dmz	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.250.100	*	*	none		dejar pasar a apache	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	4194	*	none		Regla FW VPN	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.200.99	222	*	none		ssh honey	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN address	*	DMZ address	*	*	none		permitir acceso a .206	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LAN

Floating WAN **LAN** DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 9/357.79 MB	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

Los agentes de elastic

Agents

Find apps, content, and more. Setup guides

Send feedback

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 Fleet Server Add agent

Filter your data using KQL syntax Status 4 Tags 0 Agent policy 6 Upgrade available

Showing 5 agents Clear filters Healthy 4 Unhealthy 0 Updating 0 Offline 1 Inactive 0 Unenrolled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input type="checkbox"/>	Healthy	kali	Politica APA Kali rev. 2	1.62 %	212 MB	23 seconds ago	8.15.2	...
<input type="checkbox"/>	Offline	kali	Politica APA Kali rev. 1 Outdated policy	N/A	N/A	yesterday	8.15.2	...
<input type="checkbox"/>	Healthy	WinDev2407Eval	politica windows rev. 1	1.72 %	162 MB	36 seconds ago	8.15.2	...
<input type="checkbox"/>	Healthy	kali	MIPrimeraPolitica rev. 1	1.25 %	198 MB	37 seconds ago	8.15.2	...
<input type="checkbox"/>	Healthy	99e9cd78a056	Elastic Cloud agent policy rev. 5	N/A	N/A	14 seconds ago	8.15.2	...

Firewall / Rules / DMZ

Floating

WAN

LAN

DMZ

DMZ2

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ address	*	DMZ2 subnets	*	*	none		bloquear de DMZ a DMZ2	
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ address	*	LAN subnets	*	*	none		bloquear de DMZ LAN	
<input type="checkbox"/>	0/2 K/B	IPv4 ICMP any	*	*	*	*	*	none		regla ICMP any	
<input type="checkbox"/>	8/1.28 M/B	IPv4 *	*	*	DMZ2 subnets	*	*	none			
<input type="checkbox"/>	0/3 K/B	IPv4 *	192.168.200.99	*	WAN subnets	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	13/25.96 M/B	IPv4 TCP	*	*	*	web	*	none		regla trafico web	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / DMZ2

Floating

WAN

LAN

DMZ

DMZ2

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	37/2.41 G/B	IPv4+6 *	*	*	*	*	*	none		permitir trafico DMZ2	
<input type="checkbox"/>	0/3 K/B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		APACHE 80	
<input type="checkbox"/>	0/1.97 M/B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/1008 B	IPv4 ICMP any	*	*	*	*	*	none		regla ICMP any	
<input type="checkbox"/>	0/987 K/B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	0/865.06 M/B	IPv4 TCP	*	*	*	web	*	none		regla trafico web	

Add Add Delete Toggle Copy Save Separator

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

13

Firewall / NAT / Port Forward

Port Forward

1:1

Outbound

NAT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>		DMZ2	ANY	*	*	*	*	*	trafico DMZ2 apache		
<input type="checkbox"/>		WAN	TCP/UDP	*	*	WAN address	222	192.168.200.99	222	docker 222 honeypot	

Add Add Delete Toggle Save Separator

Reglas NAT

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"/>	<input checked="" type="checkbox"/>		DMZ2	ANY	*	*	*	*	trafico DMZ2 apache	
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP/UDP	*	*	WAN address	222	192.168.200.99 222	docker 222 honeypot

↑ Add

↓ Add

Delete

Toggle

Save

Separator

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

Other

From port

222

Custom

Other

To port

222

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

Type

192.168.200.99

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80*) to local scope (::1)

Redirect target port

Other

Port

222

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the 'From port' above.

Description

docker 222 honeypot

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

None

Rule Information

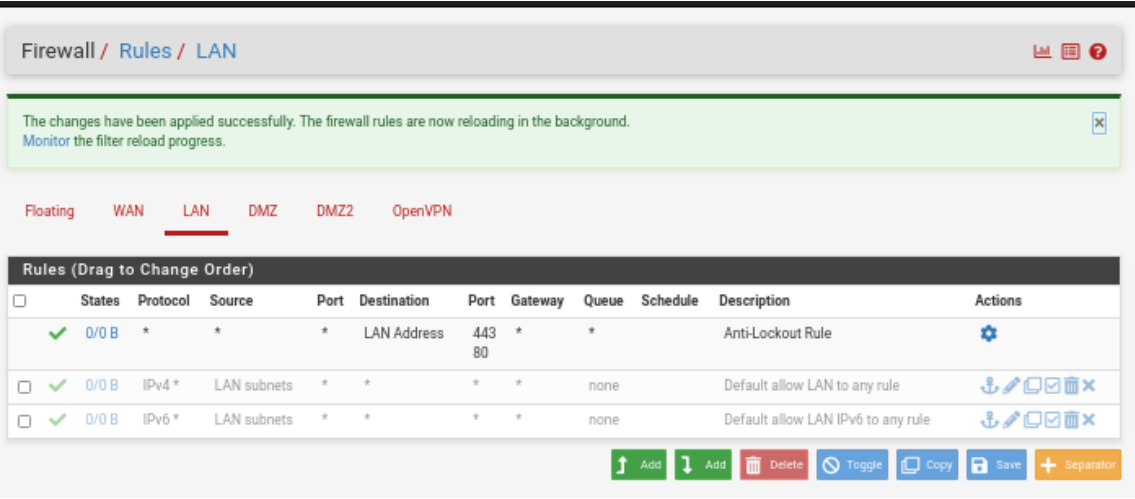
Created

10/11/24 16:49:25 by admin@192.168.250.100 (Local Database)

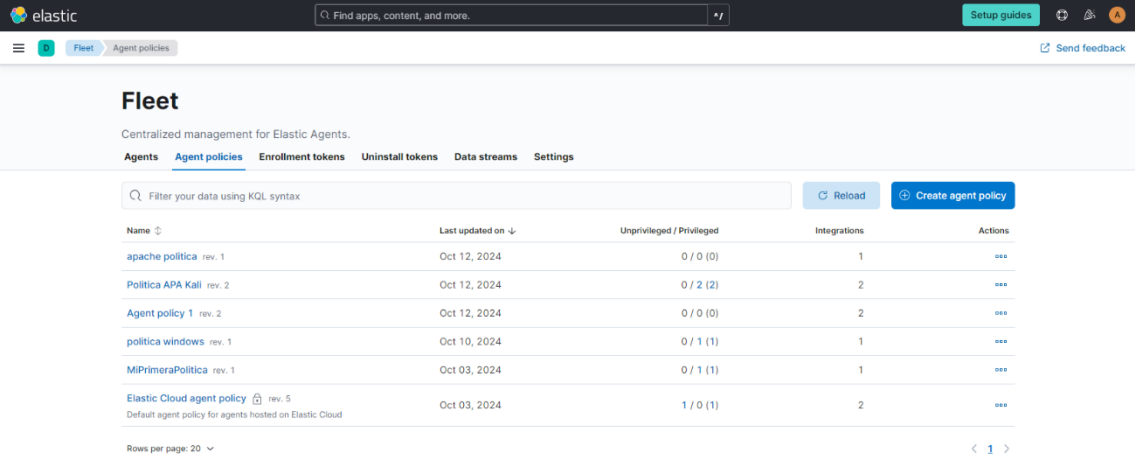
Updated

10/13/24 12:22:57 by admin@192.168.250.99 (Local Database)

Reglas firewall



Políticas de elastic:



2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.

Este es un ejemplo de log desde elastic:

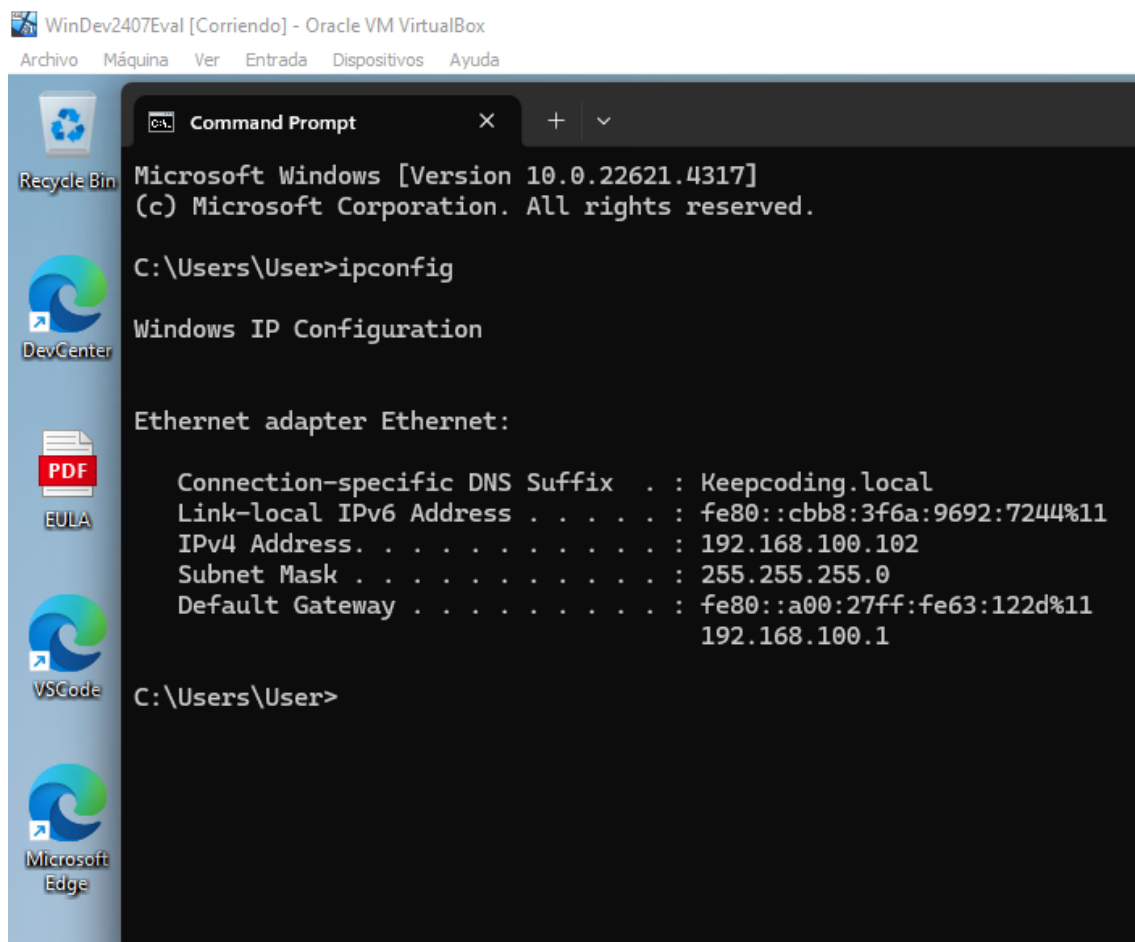
```
agent.name WinDev2407Eval @timestamp Oct 12, 2024 @ 09:37:26.164 agent.ephemeral_id c4342c3c-568e-41dd-9e97-15cda4016a39 agent.id ec9f3b4b-48cb-4161-8986-b420f5f99acd agent.type filebeat agent.version 8.15.2 data_stream.dataset system.security data_stream.namespaces default data_stream.type logs ecs.version 8.11.0 elastic_agent.id ec9f3b4b-48cb-4161-8986-b420f5f99acd elastic_agent.snapshot false elastic_agent.version 8.15.2 event.action logged-in-special event.agent_id_status verified event.category iam event.code 4672 event.created Oct 12, 2024 @ 09:37:27.542 event.dataset system.security event.ingested Oct 12, 2024 @ 09:37:37.000 event.kind event event.module system event.outcome success event.provider Microsoft-Windows-Security-Auditing event.type admin host.architecture x86_64 host.hostname windev2407eval host.id 64e4a60a-fde0-45ac-84f2-82edb1871856 host.ip [fe80::cbb8:3f6a:9692:7244, 192.168.100.102] host.mac 08-00-27-C3-FF-56 host.name windev2407eval host.os.build 22621.4317 host.os.family windows host.os.kernel 10.0.22621.4317 (WinBuild.160101.0800) host.os.name Windows 11 Enterprise Evaluation host.os.platform windows host.os.type windows host.os.version 10.0 input.type winlog log.level information message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege related.user SYSTEM user.domain NT AUTHORITY user.id S-1-5-18 user.name SYSTEM winlog.activity_id {3df6fff0-1cc4-0002-2d00-f73dc41c0b01} winlog.api wineventlog winlog.channel Security winlog.computer_name WinDev2407Eval winlog.event_data.PrivilegeList [SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege] winlog.event_data.SubjectDomainName NT AUTHORITY winlog.event_data.SubjectLogonId 0x3e7 winlog.event_data.SubjectUserName SYSTEM winlog.event_data.SubjectUserSid S-1-5-18 winlog.event_id 4672 winlog.keywords Audit Success winlog.logon_id 0x3e7 winlog.opcode Info winlog.process.pid 804 winlog.process.thread_id 86 winlog.provider_guid {54849625-5478-4994-a5ba-3e3b8328c30d} winlog.provider_name Microsoft-Windows-Security-Auditing winlog.record_id 1670 winlog.task Special Logon _id GDKpf5IBTs0CcQa8VRMC _ignored - _index .ds-logs-system.security-default-2024.10.10-000001 _score -
```

- host.os.name: "Windows 11 Enterprise Evaluation"
- host.os.version: "10.0"

- host.os.build: "22621.4317"
- agent.name: "WinDev2407Eval"
- event.provider: "Microsoft-Windows-Security-Auditing"
- host.ip: ["fe80::cbb8:3f6a:9692:7244", "192.168.100.102"]
- host.mac: ["08-00-27-C3-FF-56"]

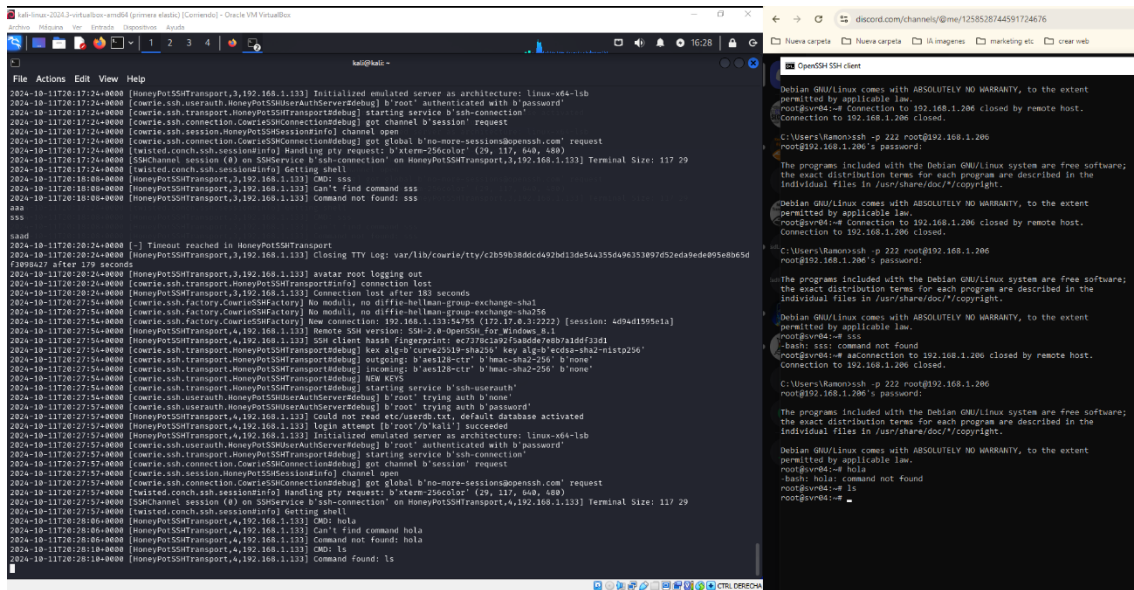
Estos campos indican claramente que el log está generado por una máquina con Windows 11 Enterprise Evaluation, con la dirección de mi maquina.

A continuación presento la maquina de Windows 11 presentando su dirección.

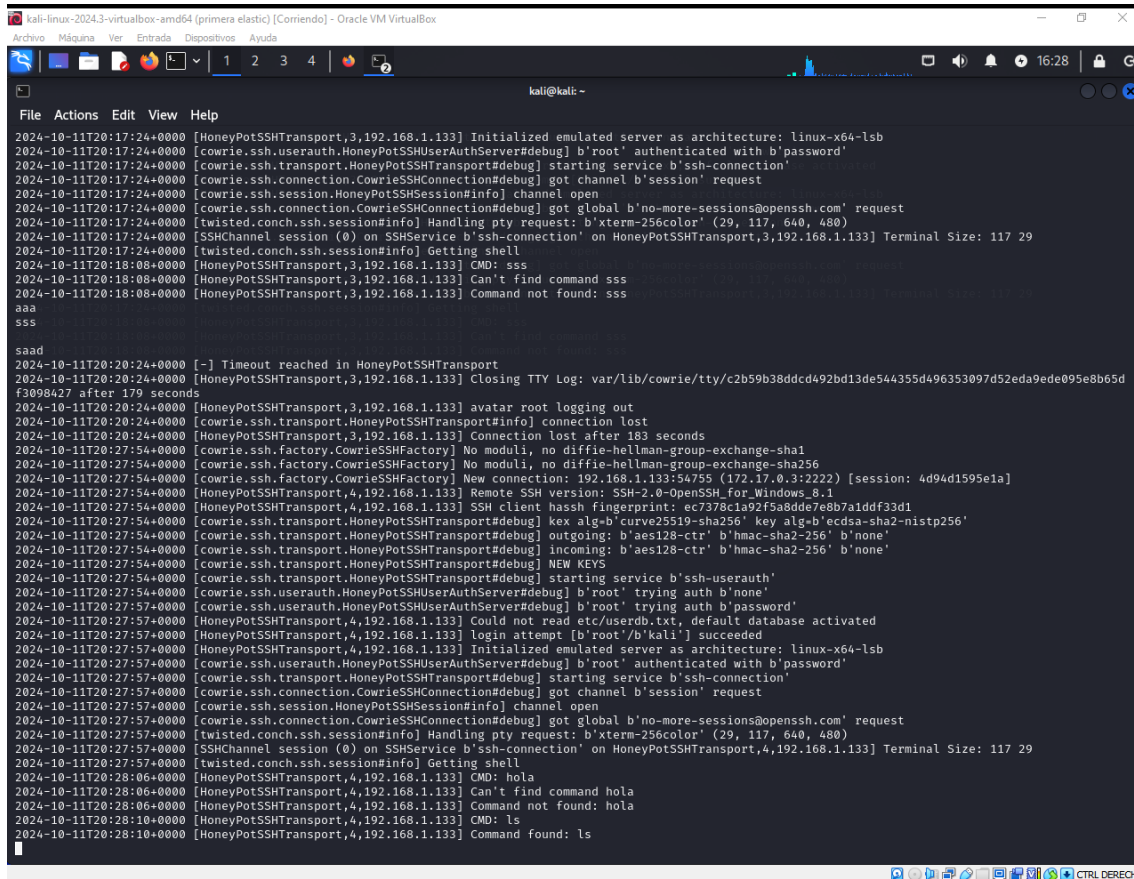


3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.

He de decir que al principio le di la dirección 192.168.200.102 despues lo cambie a la 192.168.200.99 cuando estuve haciendo la parte del apache.



docker logs -f 81ad3158fbfe



El ssh desde la terminal de windows

```
C:\Users\Ramon>ssh -p 222 root@192.168.1.206
root@192.168.1.206'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:~# hola
-bash: hola: command not found
root@svr04:~# ls
root@svr04:~#
```

¿Cómo enviar los logs a elastic?

```
(kali@kali)-[~]
$ docker run -p 222:2222 cowrie/cowrie
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning: Blowfish has been deprecated and will be removed in a future release
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: CAST5 has been deprecated and will be removed in a future release
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning: Blowfish has been deprecated and will be removed in a future release
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning: CAST5 has been deprecated and will be removed in a future release
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
2024-10-11T17:54:51+0000 [-] Python Version 3.11.2 (main, Aug 26 2024, 07:20:54) [GCC 12.2.0]
2024-10-11T17:54:51+0000 [-] Twisted Version 24.7.0
2024-10-11T17:54:51+0000 [-] Cowrie Version 2.5.0
2024-10-11T17:54:51+0000 [-] Loaded output engine: jsonlog
2024-10-11T17:54:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.7.0 (/cowrie/cowrie-env/bin/twistd) starting up.
2024-10-11T17:54:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet._pollReactor.
2024-10-11T17:54:51+0000 [-] CowrieSSHFactory starting on 2222
2024-10-11T17:54:51+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7ff035ecc110>
2024-10-11T17:54:51+0000 [-] Generating new RSA keypair ...
2024-10-11T17:54:52+0000 [-] Generating new ECDSA keypair ...
2024-10-11T17:54:52+0000 [-] Generating new ed25519 keypair ...
2024-10-11T17:54:52+0000 [-] Ready to accept SSH connections
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-ex
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-ex
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.133:54127 (
on: a2970ea29f98]
2024-10-11T18:08:54+0000 [HoneyPotSSHTransport,0,192.168.1.133] Remote SSH version: SSH-2.0-OpenSSH_
2024-10-11T18:08:54+0000 [HoneyPotSSHTransport,0,192.168.1.133] SSH client hassh fingerprint: ec7378
3d1
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha2
2-nistp256'
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b
```

```
kali-linux-2024.3-virtualbox-amd64 (primera elastic) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

(kali@kali)-[~]
$ docker logs -f 81ad3158bfbe
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning:
removed in a future release
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning:
moved in a future release
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning:
removed in a future release
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning:
moved in a future release
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
2024-10-11T17:54:51+0000 [-] Python Version 3.11.2 (main, Aug 26 2024, 07:20:54) [GCC 12.2.0]
2024-10-11T17:54:51+0000 [-] Twisted Version 24.7.0
2024-10-11T17:54:51+0000 [-] Cowrie Version 2.5.0
2024-10-11T17:54:51+0000 [-] Loaded output engine: jsonlog
2024-10-11T17:54:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.7.0 (/cowrie/cowrie-env/bin
2024-10-11T17:54:51+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epoll
2024-10-11T17:54:51+0000 [-] CowrieSSHFactory starting on 2222
2024-10-11T17:54:51+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieS
2024-10-11T17:54:51+0000 [-] Generating new RSA keypair ...
2024-10-11T17:54:52+0000 [-] Generating new ECDSA keypair ...
2024-10-11T17:54:52+0000 [-] Generating new ed25519 keypair ...
2024-10-11T17:54:52+0000 [-] Ready to accept SSH connections
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha2
2024-10-11T18:08:54+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.133:54127 (172.17.0.3:2
2024-10-11T18:08:54+0000 [HoneyPotSSHTransport,0,192.168.1.133] Remote SSH version: SSH-2.0-OpenSSH_for_Windows
2024-10-11T18:08:54+0000 [HoneyPotSSHTransport,0,192.168.1.133] SSH client hash fingerprint: ec7378c1a92f5a8dde
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-2
2024-10-11T18:08:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-2
2024-10-11T18:08:59+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2024-10-11T18:08:59+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2024-10-11T18:08:59+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthService#debug] b'root' trying auth b'none'
```

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS      PORTS
81ad3158bfbe   cowrie/cowrie  "/cowrie/cowrie-env/..." 3 hours ago   Up         2223/tcp, 0.0.0.0:222→2222/tcp, [::]:222→2222/tcp
b39ff0c62fa4   amazedostrich/rdpy  "/bin/sh -c '/usr/bi..." 35 hours ago   Up         0.0.0.0:333→3389/tcp, [::]:333→3389/tcp
er eloquent_w

(kali@kali)-[~]
$
```

```
docker run -p 222:2222 cowrie/cowrie
```

```
docker ps
```

para ver los contenedores copié el número del contenedor ID y luego lance otro comando con `docker logs -f` y el número del contenedor y después `cd /var/log`

Para pasar esos logs a otro archivo hice el `sudo docker logs -f número del contenedor >>logs_cowrie`

```
cd /var/log
```

```
cat logs_cowrie
```

```
cd /opt
```

```
Sudo su
```

```
Cd Elastic/Agente
```

```
nano /home/kali/elastic-agent-8.15.2-linux-x86_64/elastic-agent.yml
```

en la ultima fila pongo:

```
inputs:
```

```
id: logfile-logs
```

```
type: logfile
```

```
streams:
```

```
id: logfile-log.logs
```

```
data_stream:
```

```
dataset: null
```

```
paths: null
```

```
ignore_older: 72h
```

Después voy a elastic y creo la integración.

en la integración tengo que poner la dirección del `logs_cowrie`.

Uso Custom Logs

Back to integrations

Custom Logs

Elastic Agent

OverviewIntegration policiesAssetsSettingsConfigs

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
log-1	v2.3.2	Agent policy 2 rev. 2	<div><div></div>system</div>	4 days ago	1	<div></div>

Rows per page: 20

Version2.3.2

Agent policies1

Add Custom Logs

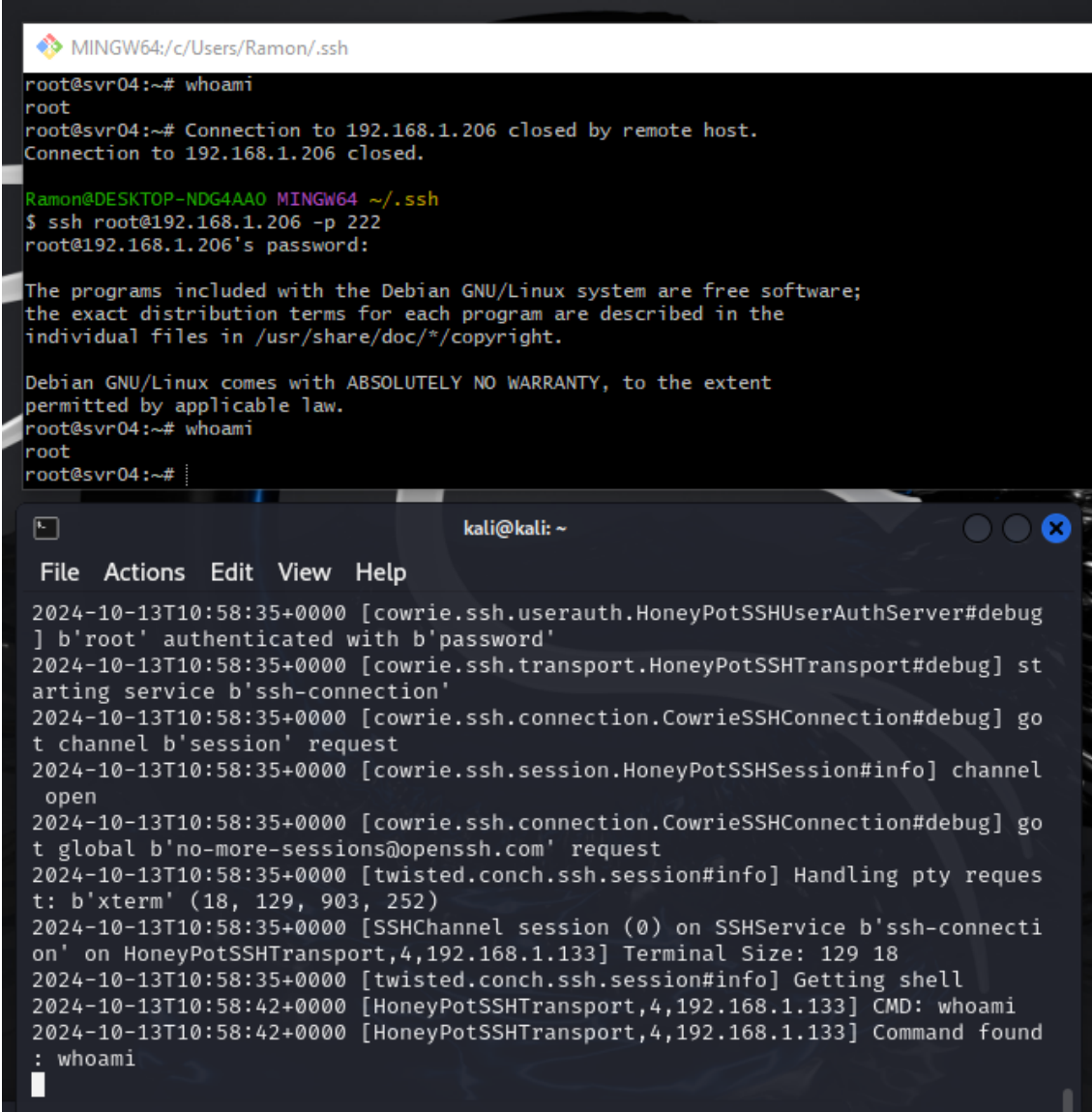
A continuación puedo generar logs como este:

```
@timestamp Oct 18, 2024 @ 12:28:03.245 agent.ephemeral_id 86665f93-298c-49c5-aef-844517ff4294 agent.id c98318bd-add5-45e0-a306-4922dd54b5b8 agent.name kali agent.type filebeat agent.version 8.15.3 container.id cowrie.log data_stream.dataset cowrie data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id c98318bd-add5-45e0-a306-4922dd54b5b8 elastic_agent.snapshot false elastic_agent.version 8.15.3 event.agent_id_status verified event.dataset cowrie event.ingested Oct 18, 2024 @ 12:28:07.00 host.architecture x86_64 host.containerized false host.hostname kali host.id 98662c5c81d4191bd244a79c97d2e0 host.ip [192.168.200.99, fe80::b2e2:c470:1807:28c6, 172.17.0.1, fe80::42:fcff:fe2e:53c9, fe80::c54:75ff:fefb:b0d2, fe80::a837:67ff:febd:9e54] host.mac [02-42-FC-2E-53-C9, 08-00-27-AD-25-87, 0E-54-75-FB-B0-D2, AA-37-67-B0-9E-54] host.name kali host.os.codename kali-rolling host.os.family debian host.os.kernel 6.10.9-amd64 host.os.name Kali GNU/Linux host.os.platform kali host.os.type linux host.os.version 2024.3 input.type log log.file.path /home/kali/testdir/elastic-agent-8.15.2-linux-x86_64/cowrie.log log.offset 5,526 message 2024-10-18T10:28:02+0000 [HoneyPotSSTransport,3,192.168.1.133] Connection lost after 0 seconds _id _Tlrn5IBTs0CcQaBmf4N _ignored - _index .ds-logs-cowrie-default-2024.10.18-000001 _score -
```

3.1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2...) y debe ser

accesible desde el exterior (red WAN) en ambos sentidos.

vuelvo a entrar desde mi pc, desde fuera:



The image shows two terminal windows. The top window is a MINGW64 terminal running on a Windows machine (Ramon@DESKTOP-NDG4AA0). It shows a failed connection to 192.168.1.206, followed by a successful SSH connection to the same IP. The user 'root' is authenticated with the password 'password'. The terminal displays the Debian GNU/Linux system's free software notice and the user's identity. The bottom window is a Kali Linux terminal (kali@kali: ~) showing the debug output of the Cowrie SSH server. It logs the authentication process, including the user 'root' being authenticated with the password 'password', the opening of a channel, and the execution of the 'whoami' command, which returns 'root'.

```
MINGW64:/c/Users/Ramon/.ssh
root@svr04:~# whoami
root
root@svr04:~# Connection to 192.168.1.206 closed by remote host.
Connection to 192.168.1.206 closed.

Ramon@DESKTOP-NDG4AA0 MINGW64 ~/.ssh
$ ssh root@192.168.1.206 -p 222
root@192.168.1.206'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:~# whoami
root
root@svr04:~#
```

```
kali@kali: ~
File Actions Edit View Help
2024-10-13T10:58:35+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug]
] b'root' authenticated with b'password'
2024-10-13T10:58:35+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] st
arting service b'ssh-connection'
2024-10-13T10:58:35+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] go
t channel b'session' request
2024-10-13T10:58:35+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel
open
2024-10-13T10:58:35+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] go
t global b'no-more-sessions@openssh.com' request
2024-10-13T10:58:35+0000 [twisted.conch.ssh.session#info] Handling pty reques
t: b'xterm' (18, 129, 903, 252)
2024-10-13T10:58:35+0000 [SSHChannel session (0) on SSHService b'ssh-connecti
on' on HoneyPotSSHTransport,4,192.168.1.133] Terminal Size: 129 18
2024-10-13T10:58:35+0000 [twisted.conch.ssh.session#info] Getting shell
2024-10-13T10:58:42+0000 [HoneyPotSSHTransport,4,192.168.1.133] CMD: whoami
2024-10-13T10:58:42+0000 [HoneyPotSSHTransport,4,192.168.1.133] Command found
: whoami
```

desde la maquina del honeypot a WAN

```
File Actions Edit View Help
└─$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:40ff:fe5d:1b38 prefixlen 64 scopeid 0x20<link>
    ether 02:42:40:5d:1b:38 txqueuelen 0 (Ethernet)
    RX packets 149 bytes 19423 (18.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 204 bytes 26973 (26.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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::b2e2:c470:1807:28c6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 110458 bytes 52091043 (49.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 177803 bytes 58489614 (55.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 108179 bytes 15756285 (15.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 108179 bytes 15756285 (15.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth8bf15d9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::502d:8ff:fe66:38bf prefixlen 64 scopeid 0x20<link>
    ether 52:2d:08:66:38:bf txqueuelen 0 (Ethernet)
    RX packets 149 bytes 21509 (21.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 219 bytes 28119 (27.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└─$ ping 192.168.1.206
PING 192.168.1.206 (192.168.1.206) 56(84) bytes of data.
64 bytes from 192.168.1.206: icmp_seq=1 ttl=64 time=0.437 ms
64 bytes from 192.168.1.206: icmp_seq=2 ttl=64 time=0.571 ms
64 bytes from 192.168.1.206: icmp_seq=3 ttl=64 time=0.548 ms
64 bytes from 192.168.1.206: icmp_seq=4 ttl=64 time=0.239 ms
```


la DMZ no puede hacer ping a las demás maquinas:

```
File Actions Edit View Help

(kali@kali)-[~]
$ ping 192.168.250.99
PING 192.168.250.99 (192.168.250.99) 56(84) bytes of data.
^C
— 192.168.250.99 ping statistics —
21 packets transmitted, 0 received, 100% packet loss, time 20476ms

(kali@kali)-[~]
$ ping 192.168.100.102
PING 192.168.100.102 (192.168.100.102) 56(84) bytes of data.
```

FIREWALL

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/2 KiB	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/41 KiB	IPv4 *	*	*	192.168.200.99	*	*	none		permitir acceso de wan a dmz	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.250.100	*	*	none		dejar pasar a apache	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	4194	*	none		Regla FW VPN	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.200.99	222	*	none		ssh honey	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN address	*	DMZ address	*	*	none		permitir acceso a .206	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LAN

Floating LAN WAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 9/357.79 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

Firewall / Rules / DMZ

Floating WAN LAN **DMZ** DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ address	*	DMZ2 subnets	*	*	none		bloquear de DMZ a DMZ2	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ address	*	LAN subnets	*	*	none		bloquear de DMZ LAN	
<input type="checkbox"/>	✓ 0/2 KiB	IPv4 ICMP any	*	*	*	*	*	none		regla ICMP any	
<input type="checkbox"/>	✓ 8/1.20 MiB	IPv4 *	*	*	DMZ subnets	*	*	none			
<input type="checkbox"/>	✓ 0/3 KiB	IPv4 *	192.168.200.99	*	WAN subnets	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	✓ 13/25.96 MiB	IPv4 TCP	*	*	*	web	*	none		regla trafico web	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / DMZ2

Floating WAN LAN DMZ **DMZ2** OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 37/2.41 GiB	IPv4+6 *	*	*	*	*	*	none		permitir trafico DMZ2	
<input type="checkbox"/>	✓ 0/3 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		APACHE 80	
<input type="checkbox"/>	✓ 0/1.97 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0/1008 B	IPv4 ICMP any	*	*	*	*	*	none		regla ICMP any	
<input type="checkbox"/>	✓ 0/987 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	✓ 0/865.06 MiB	IPv4 TCP	*	*	*	web	*	none		regla trafico web	

Add Add Delete Toggle Copy Save Separator

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

Rules

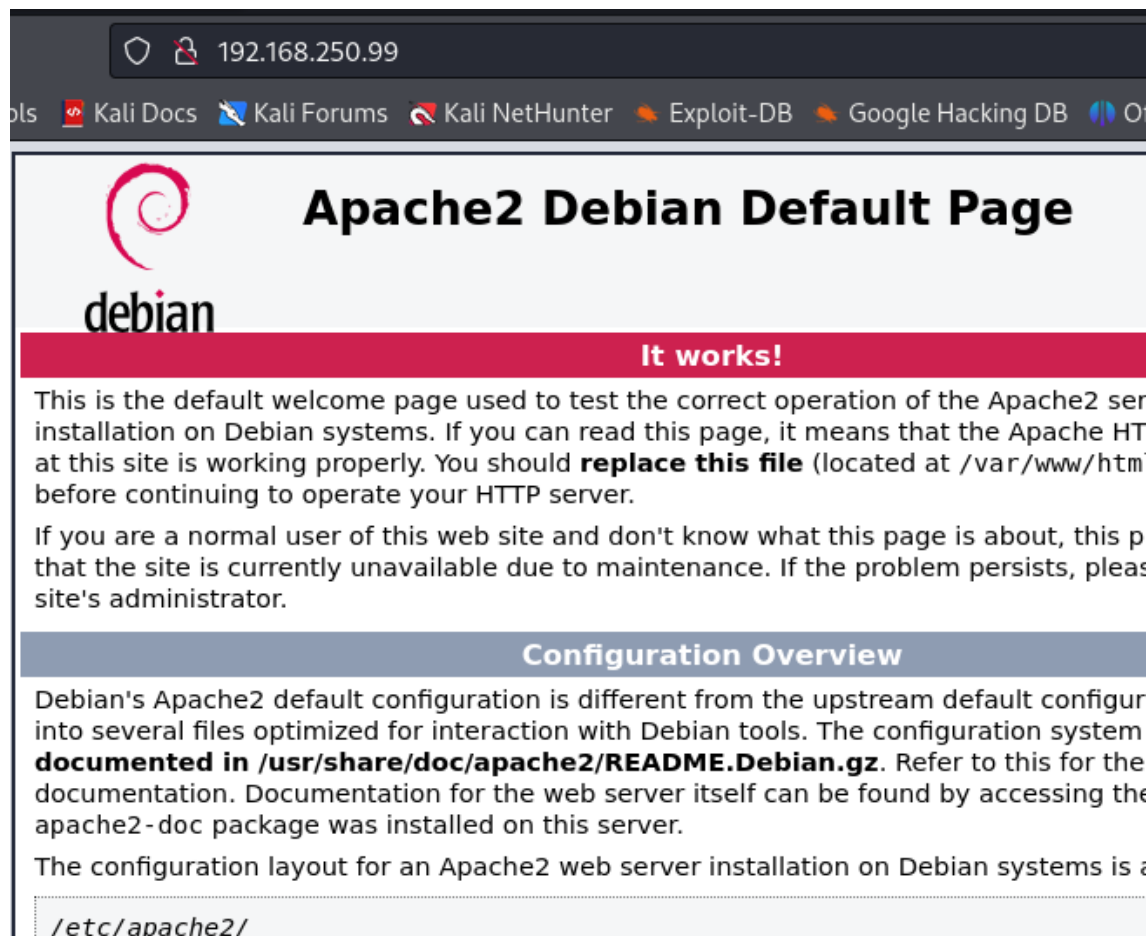
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	DMZ2	ANY	*	*	*	*	*	*	trafico DMZ2 apache	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	222	192.168.200.99	222	docker 222 honeypot	

Add Add Delete Toggle Save Separator

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.

Lo hago con el apache.




The screenshot shows a web browser window with the address bar displaying '192.168.250.99'. The browser's tab bar includes links to 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'O'. The main content area features the Debian logo and the title 'Apache2 Debian Default Page'. A prominent red banner with the text 'It works!' is displayed. Below this, a paragraph explains that the page is the default welcome page for testing Apache2 installation on Debian systems. It advises replacing the file at '/var/www/html' and provides instructions for normal users. A section titled 'Configuration Overview' follows, detailing the configuration files and documentation for the Debian Apache2 installation. The path '/etc/apache2/' is shown at the bottom.

192.168.250.99

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB O

Apache2 Debian Default Page



It works!

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

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

Configuration Overview

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

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

```
/etc/apache2/
```

Con esta regla asigno una dirección IP a un dispositivo dentro de mi red DMZ2, así recibirá la misma dirección ip, asegurando una gestión mas predecible y controlada de mi red.

Services / DHCP Server / DMZ2 / Static Mapping / Edit

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.

Static DHCP Mapping on DMZ2

DHCP Backend	ISC DHCP		
MAC Address	<input type="text" value="08:00:27:ca:b5:c8"/>	<button>Copy My MAC</button>	MAC address of the client to match (6 hex octets separated by colons).
Client Identifier	<input type="text"/>		
	An optional identifier to match based on the value sent by the client (RFC 2132).		
IP Address	<input type="text" value="192.168.250.99"/>		IPv4 address to assign this client. Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.
ARP Table Static Entry	<input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.		
Hostname	<input type="text" value="kali"/>		Name of the client host without the domain part.
Description	<input type="text" value="apache servidor"/>		A description for administrative reference (not parsed).

Integración:

Back to integrations

Apache HTTP Server

Elastic Agent

Version1.25.0

Agent policies2

Add Apache HTTP Server

Overview

Integration policies

Assets

Settings

Configs

API reference

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
apache-2	v1.25.0	Politica APA Kali rev. 2	<div><div>S</div>system</div>	last week	2	<div></div>
apache-1	v1.25.0	Agent policy 1 rev. 2	<div><div>S</div>system</div>	last week	<div><div>+</div>Add agent</div>	<div></div>

Rows per page: 20

<

1

>

Este es un log que proviene del apache, se ve que pone apache, y la dirección: 192.168.250.99.

```
@timestamp: Oct 12, 2024 @ 22:58:22.000 agent.ephemeral_id: 70b17599-8d9c-43df-9706-967979e80b71 agent.id: aefabfc6-721b-42b9-b8b0-1159c27d7e09 agent.name: kali agent.type: filebeat agent.version: 8.15.2 apache.access.remote_addresses: 127.0.0.1 data_stream.dataset: apache.access data_stream.namespace: default data_stream.type: logs ecs.version: 8.11.0 elastic_agent.id: aefabfc6-721b-42b9-b8b0-1159c27d7e09 elastic_agent.snapshot: false elastic_agent.version: 8.15.2 event.agent_id_status: verified event.category: web event.created: Oct 12, 2024 @ 22:58:23.422 event.dataset: apache.access event.ingested: Oct 12, 2024 @ 22:58:38.000 event.kind: event event.module: apache event.outcome: success host.architecture: x86_64 host.containerized: false host.hostname: kali host.id: 30e662c5c81d4191bd2444a79c97d2e0 host.ip: [192.168.250.99, fe80::6dd5:2eec:8c79:74f5, 172.17.0.1] host.mac: [02:42:04-6A-C5-9E, 08-00-27-CA-B5-C8] host.name: kali host.os.codename: kali-rolling host.os.family: debian host.os.kernel: 6.10.9-and64 host.os.name: Kali GNU/Linux host.os.platform: kali host.os.type: linux host.os.version: 2024.3 http.request.method: GET http.response.body.bytes: 663 http.response.status_code: 200 http.version: 1.1 input.type: log log.file.path: /var/log/apache2/access.log log.offset: 3.955 related.ip: 127.0.0.1 source.address: 127.0.0.1 source.ip: 127.0.0.1 tags: apache-access url.original: /server-status?auto url.path: /server-status url.query: auto user_agent.device.name: Other user_agent.name: Other user_agent.original: Elastic-Metricbeat/8.15.2 (linux; amd64; 26daf71e4ec87172523af7f0e916cba9f79dc8d0; 2024-09-19 09:24:35 +0000 UTC) user_agent.os.name: Linux _id: UTK5qp1BTs0CcQaBsLnR _ignored: - _index: .ds-logs-apache.access-default-2024.10.12-000001 _score: -
```

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.

Este ejercicio se responde con los anteriores.