



Instalación Wazuh y overview de la
aplicación
Incidentes de ciberseguridad

wazuh.

Curso de especialización en ciberseguridad

Histórico de revisiones

Versión	Fecha	Autor de la Revisión	Resumen de Cambios
1.0	29/02/2023	WAZUH TEAM	Creación del documento

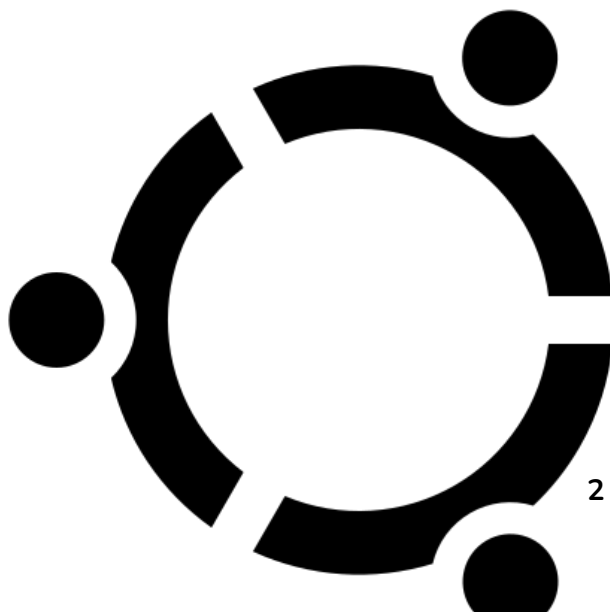
Lucas Gavín Rodríguez
Gonzalo Pascual Romero
Álvaro Rivero Zamora



Herramientas utilizadas	2
WAZUH	3
-¿Qué es Wazuh?	3
Compatibilidades:.....	3
Arquitectura centralizada y multiplataforma:	3
Instalación	4
Instalación administrador	4
INSTALACIÓN AGENTE.....	5
Información del agente	6
Escaneo del sistema	7
PASSED	8
FAILED	8
NOT APPLICABLE.....	9
Eventos de seguridad	10
Vulnerabilidades encontradas en los sistemas	11
Parte regulatoria y de cumplimientos	13
Configuración de las máquinas para establecer los niveles de seguridad	13
Configuración principal.....	13
Monitoreo de políticas	14
Amenazas del sistema y respuesta de incidentes	14
Análisis de los logs.....	14
Seguridad del cloud.....	15
MITRE ATTACK	15
Prueba de ataque	16
Configurando alertas	18
Correcciones	18
Cerrar puerto ssh mientras no se esté usando	18
Cambiar el puerto SSH por defecto en el archivo	19
Creación de clave privada	19

Herramientas utilizadas

- Wazuh
- Kali linux (agente)
- Ubuntu (admin)
- Firefox





WAZUH

De manera introductoria , vamos a explicar un poco por encima que hace la aplicación

-¿Qué es Wazuh?

Wazuh es una solución de seguridad diseñada para monitorizar y proteger sistemas contra amenazas cibernéticas. Sus características clave incluyen:

- Análisis de registro: Wazuh examina los registros del sistema en busca de patrones anómalos o signos de intrusiones.
- Comprobación de integridad: Verifica que los archivos críticos no hayan sido modificados sin autorización.
- Supervisión del registro de Windows: Vigila los eventos del registro de Windows para detectar comportamientos sospechosos.
- Detección de rootkits: Identifica posibles rootkits o malware ocultos en el sistema.
- Alertas basadas en el tiempo: Notifica en tiempo real sobre actividades inusuales.
- Respuesta activa: Puede ejecutar acciones automáticas en respuesta a amenazas

Compatibilidades:

Wazuh es versátil y funciona en diversos sistemas, como:

- Linux
- AIX
- HP-UX
- macOS
- Solaris
- Windows

Arquitectura centralizada y multiplataforma:

Wazuh se basa en una arquitectura centralizada que permite monitorizar múltiples sistemas desde un único punto de control. Esto facilita la administración y la detección temprana de posibles ataques.

En resumen, Wazuh es una herramienta valiosa para la seguridad cibernética, proporcionando detección proactiva y respuesta eficiente ante amenazas en entornos heterogéneos

Instalamos el software en ambos equipos, para proceder a la instalación se ha seguido un manual proporcionado por la misma aplicación

Fuente:

<https://documentation.wazuh.com/current/installation-guide/index.html>



Instalación

Instalación administrador

```
>$"rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH"

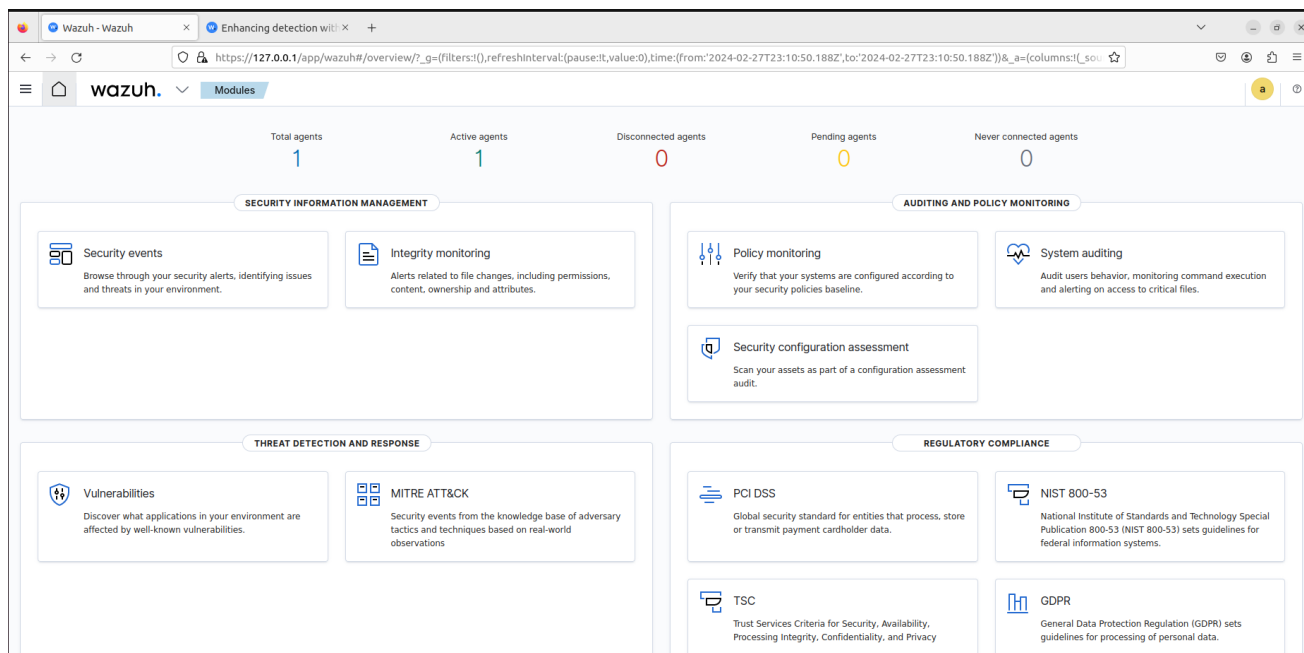
>$"cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF"
```

Después para acceder a la app tenemos que poner la ip que viene por defecto con el puerto que viene por defecto "127.0.0.1:9200" el servicio ha sido montado en local así que usaremos las ip que corresponden

Las credenciales nos la proporciona el cmd durante la instalación

Usuario:administrator

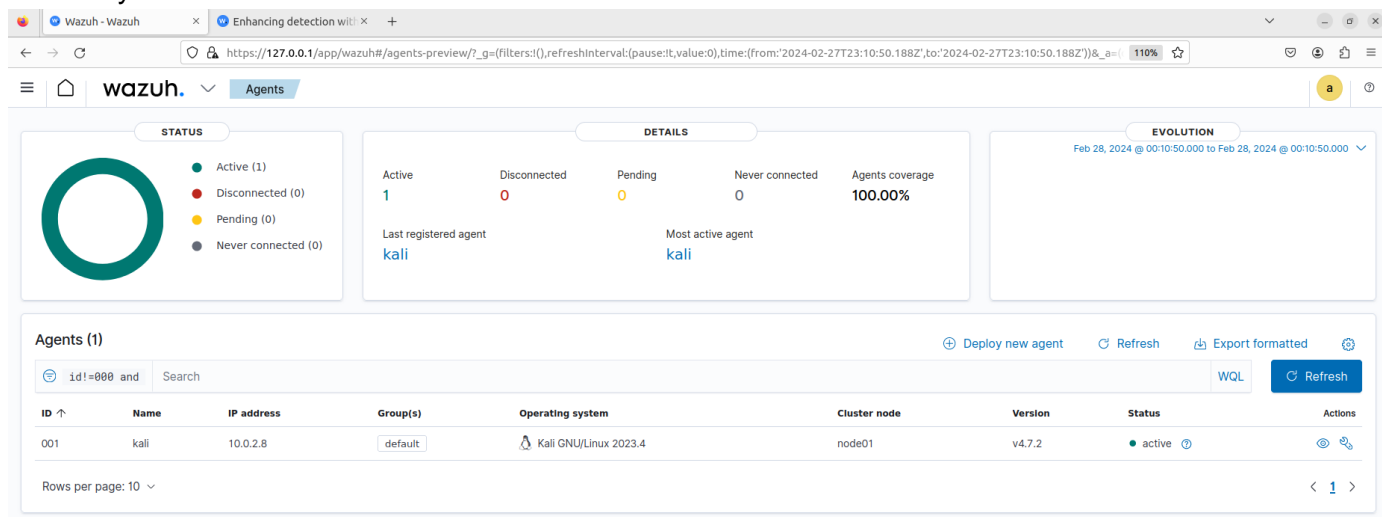
Contraseña:_____





Información del agente

Aquí tenemos un overview del agente, con datos, para saber si está activo, el nombre del sistema y otros datos



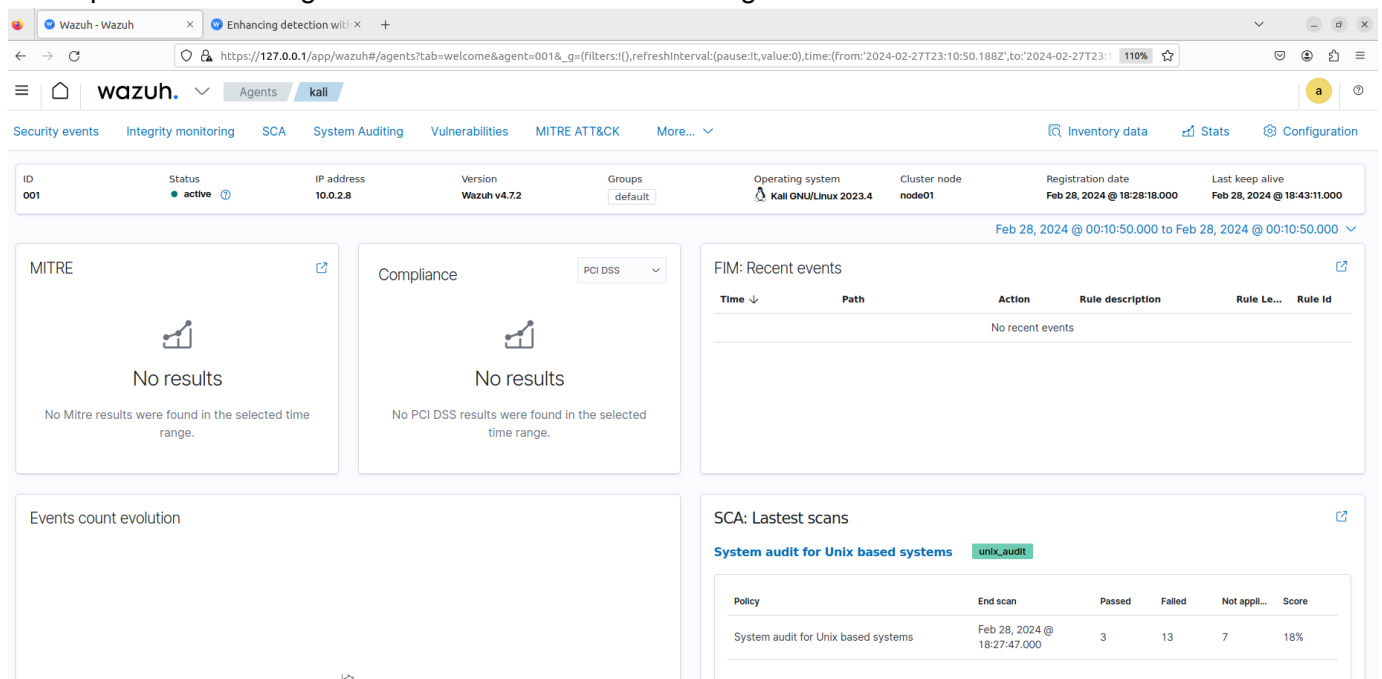
Overview de la información del agente

Si clicamos abajo, donde figura el nombre del sistema cliente tendremos varios datos a nivel mas técnico y avanzado

Mitre: Es una biblioteca, disponible para todos y que se actualiza constantemente, que ayuda a entender cómo actúan los cibercriminales para poder prevenir y combatir sus ataques la utiliza para comparar los ataques al equipo con los de la base de datos

Compliance

La parte de compliance de Wazuh se enfoca en ayudar a las organizaciones a cumplir con los requisitos de las regulaciones relacionadas con la seguridad de la información.

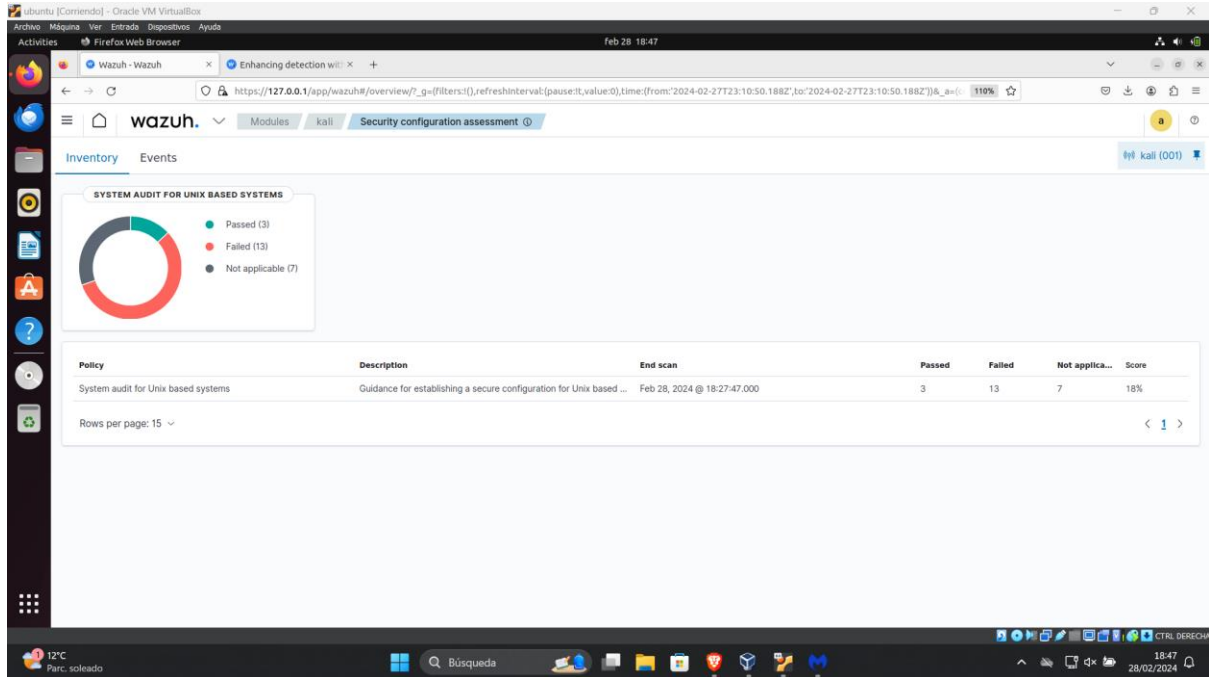




Escaneo del sistema

wazuh hace auditorías automáticas del sistema, te dice lo que está bien, lo que está mal y lo que no es aplicable (recortar las capturas)

En gráficos



Overview del escaneo del sistema

PASSED

Son las configuraciones del sistema que al realizar el análisis el programa sabe que son correctas

En este caso deberíamos tenerlas en cuenta pero al estar ya configuradas sabemos que esa parte no tenemos que tocarla

Passed

3

Failed

13

Not applicable

7

Score

18%

End scan

Feb 28, 2024 @ 18:27:47.000

Checks (23)

Refresh

Export format

Search

ID ↑

Title

Target

Result

3000

SSH Hardening: Port should not be 22

File: /etc/ssh/sshd_config

Failed

3001

SSH Hardening: Protocol should be set to 2

File: /etc/ssh/sshd_config

Failed

3002

SSH Hardening: Root account should not be able to log in

File: /etc/ssh/sshd_config

Failed

3003

SSH Hardening: No Public Key authentication

File: /etc/ssh/sshd_config

Failed

3004

SSH Hardening: Password Authentication should be disabled

File: /etc/ssh/sshd_config

Failed

3005

SSH Hardening: Empty passwords should not be allowed

File: /etc/ssh/sshd_config

Failed

3006

SSH Hardening: Rhost or shost should not be used for authentication

File: /etc/ssh/sshd_config

Failed

3007

SSH Hardening: Grace Time should be one minute or less.

File: /etc/ssh/sshd_config

Failed

3008

SSH Hardening: Wrong Maximum number of authentication attempts

File: /etc/ssh/sshd_config

Failed

3009

SSH Hardening: Ensure SSH HostbasedAuthentication is disabled

File: /etc/ssh/sshd_config

Failed

Rows per page: 10

<

1

2

3



Configuraciones correctas

FAILED

En esta sección tenemos los errores de seguridad que el sistema ha encontrado, en este caso nos da en su mayoría puertos abiertos que por defecto se conectan por el mismo, lo importante es cambiarlos o un sistema de claves asimétricas

https://127.0.0.1/app/wazuh/overview/?tab=sca&redirectPolicyTable=unix_audit&_g=(filters(),refreshInterval:(pause:it,value:0),time:(from:"2024-02-27T23:10:30.188Z",to:""))110%

wazuh

ModuleskallSecurity configuration assessment

Passed3Failed13Not applicable7Score18%End scanFeb 28, 2024 @ 18:27:47.000

Checks (13)

RefreshExport formattedWQL

ID ↑	Title	Target	Result
3000	SSH Hardening: Port should not be 22	File: /etc/ssh/sshd_config	Failed
3001	SSH Hardening: Protocol should be set to 2	File: /etc/ssh/sshd_config	Failed
3002	SSH Hardening: Root account should not be able to log in	File: /etc/ssh/sshd_config	Failed
3003	SSH Hardening: No Public Key authentication	File: /etc/ssh/sshd_config	Failed
3004	SSH Hardening: Password Authentication should be disabled	File: /etc/ssh/sshd_config	Failed
3005	SSH Hardening: Empty passwords should not be allowed	File: /etc/ssh/sshd_config	Failed
3006	SSH Hardening: Rhost or shost should not be used for authentication	File: /etc/ssh/sshd_config	Failed
3007	SSH Hardening: Grace Time should be one minute or less.	File: /etc/ssh/sshd_config	Failed
3008	SSH Hardening: Wrong Maximum number of authentication attempts	File: /etc/ssh/sshd_config	Failed
3009	SSH Hardening: Ensure SSH HostbasedAuthentication is disabled	File: /etc/ssh/sshd_config	Failed

Rows per page: 10<12>

Configuraciones pendientes de parchear

NOT APPLICABLE

Son sistemas de seguridad que el programa detecta y que se recomienda y se sabe que se pueden cambiar pero en el contexto de nuestro sistema no se pueden realizar dichos cambios

<div>Passed3Failed13Not applicable7Score18%End scanFeb 28, 2024 @ 18:27:47.000</div>				
Checks (7) <div>result="not applicable"</div> <div>RefreshExport formattedWQL</div>				
ID ↑	Title	Target	Result	
3010	Ensure retry option for passwords is less than 3	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3011	Ensure passwords are longer than 14 characters	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3012	Ensure passwords contain at least one digit	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3013	Ensure passwords contain at least one lowercase character	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3014	Ensure passwords contain at least one uppercase character	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3015	Ensure passwords contain at least one special character	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	
3017	Ensure password hashing algorithm is SHA-512	File: /etc/pam.d/common-password,/etc/pam.d/password-auth,/etc/pam.d/system-auth,/etc/pam.d/system-auth-ac,/etc/pam.d/passwd	Not applicable	

Configuraciones no aplicables



También se puede descargar en formato CSV para tener una base de datos de nuestros sistemas en el momento en el que se escanearon

A	B	C	D	E	F	G
condition	Policy ID	File	ID	Result	Title	Description
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3010	not applicable	Ensure retry option for passwords is less than 3	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3011	not applicable	Ensure passwords are longer than 14 characters	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3012	not applicable	Ensure passwords contain at least one digit	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3013	not applicable	Ensure passwords contain at least one lowercase character	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3014	not applicable	Ensure passwords contain at least one uppercase character	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3015	not applicable	Ensure passwords contain at least one special character	The pam_pwquality.so module and pam_cracklib.so module (d
all	unix_audit	/etc/pam.d/common-password/etc/pam.d/password-auth/etc/pam.d/system-auth/etc/pam.d/system-auth-ac/etc/pam.d/passwd	3017	not applicable	Ensure password hashing algorithm is SHA-512	The commands below change password encryption from md5 t

CSV del scan del sistema

Eventos de seguridad

WAZUH te ofrece una interfaz para visualizar los eventos de seguridad de tu infraestructura.

Funcionalidades:

- Lista de eventos:
- Muestra una lista de todos los eventos de seguridad que se han generado, con información detallada sobre cada uno, como:
 - Fecha y hora del evento
 - Tipo de evento
 - Fuente del evento
 - Gravedad del evento
 - Descripción del evento
 - Usuario o proceso que generó el evento
 - Sistema o dispositivo donde se generó el evento
- Filtros: Puedes filtrar la lista de eventos por diferentes criterios, como:
 - Tipo de evento
 - Fuente del evento
 - Gravedad del evento
 - Usuario o proceso
 - Sistema o dispositivo
 - Rango de fechas

Búsqueda: Puedes buscar eventos específicos por nombre, descripción, etc.



Detalles del evento: Puedes ver información detallada sobre un evento específico, como:

- Todos los datos del evento
- Cualquier alerta o regla que se haya activado
- Cualquier acción que se haya tomado en respuesta al evento

Visualizaciones:

- Puedes ver diferentes visualizaciones de los eventos de seguridad, como:
- Gráficos de tendencias
- Mapas de calor
- Tablas
- Beneficios:

Visibilidad completa:

Te permite tener una visión completa de la actividad de seguridad en tu infraestructura.

Detección temprana de amenazas:

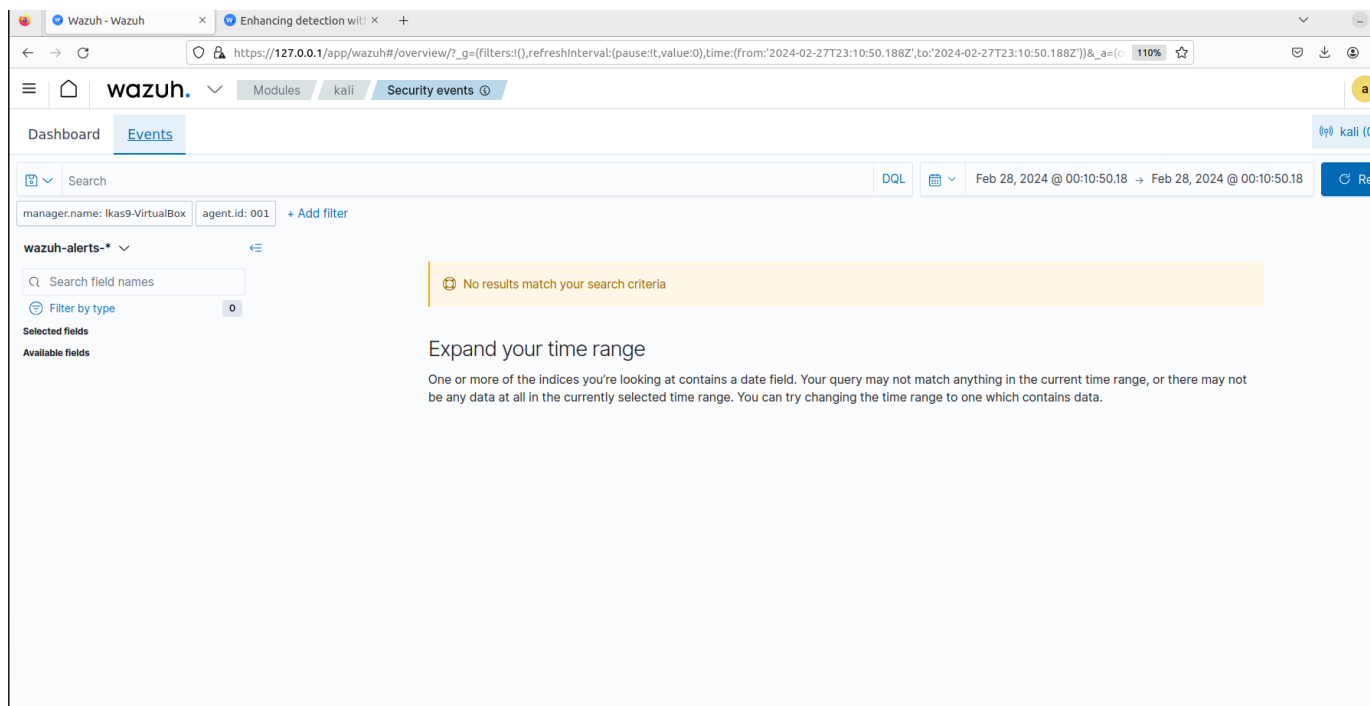
Te ayuda a identificar las amenazas de forma temprana y prevenir ataques.

Investigación de incidentes:

Te permite investigar incidentes de seguridad de forma rápida y eficaz.

Respuesta rápida a incidentes:

Te permite tomar medidas rápidas para responder a las amenazas.



Interfaz de eventos de seguridad

Vulnerabilidades encontradas en los sistemas

La app WAZUH SIEM te ofrece una interfaz intuitiva para visualizar los eventos de seguridad de tu infraestructura.

Funcionalidades:

- Lista de eventos: Muestra una lista de todos los eventos de seguridad que se han generado, con información detallada sobre cada uno, como:
- Fecha y hora del evento
- Tipo de evento
- Fuente del evento
- Gravedad del evento
- Descripción del evento
- Usuario o proceso que generó el evento
- Sistema o dispositivo donde se generó el evento

Filtros: Puedes filtrar la lista de eventos por diferentes criterios, como:

- Tipo de evento
- Fuente del evento
- Gravedad del evento
- Usuario o proceso



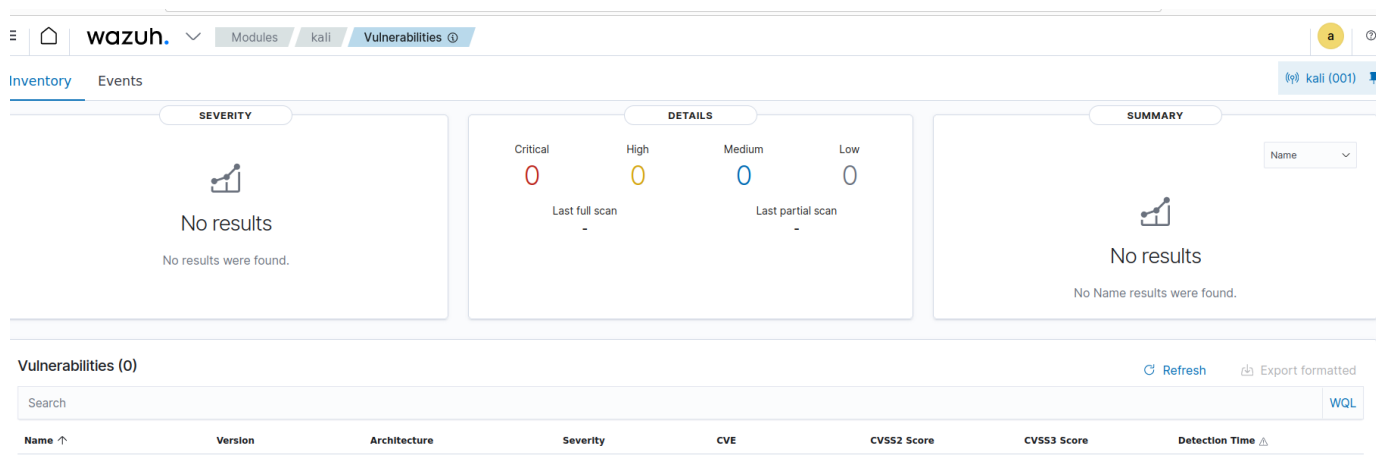
- Sistema o dispositivo
- Rango de fechas
- Búsqueda: Puedes buscar eventos específicos por nombre, descripción, etc.

Detalles del evento: Puedes ver información detallada sobre un evento específico, como:

- Los datos del evento
- Cualquier alerta o regla que se haya activado
- Cualquier acción que se haya tomado en respuesta al evento

Visualizaciones: Puedes ver diferentes visualizaciones de los eventos de seguridad, como:

- Gráficos de tendencias
- Mapas de calor
- Tablas

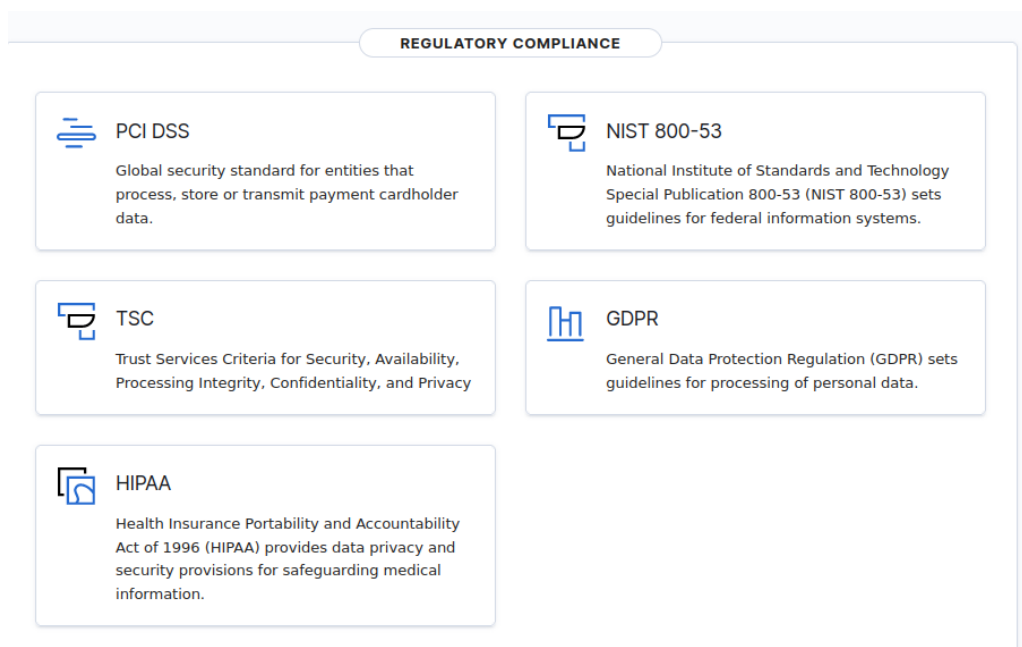


Overview de las vulnerabilidades encontradas

Parte regulatoria y de cumplimiento

Aquí podemos verificar que la integridad y la configuración de los sistemas se ajustan a las leyes regulatorias

Debajo de cada parte de cumplimiento tiene su pequeña descripción, desde protección de datos personales hasta de datos bancarios



Configuración de las máquinas para establecer los niveles de seguridad

Configuración principal

Aquí podemos configurar a nivel general el equipo agente, también nos permite configurar como se comporta el agente en relación al administrador

Es importante tener esta parte bien configurada ya que así se puede gestionar correctamente que usuarios se pueden conectar a nuestro SIEM y evitar intrusos en el sistema

Groups: [default](#)

Configuration SYNCHRONIZED

Main configurations

Name	Description
Global Configuration	Logging settings that apply to the agent
Communication	Settings related to the connection with the manager
Anti-flooding settings	Agent bucket parameters to avoid event flooding
Labels	User-defined information about the agent included in alerts

Configuración principal

Monitoreo de políticas

Aquí podemos auditar las políticas del sistema, tenemos openScap que es el que nos permite implementar las políticas y CIS-CAT que compara la configuración del sistema con la de las políticas para asegurarse de que todo funciona correctamente



Auditing and policy monitoring

Name	Description
Policy monitoring	Configuration to ensure compliance with security policies, standards and hardening guides
OpenSCAP	Configuration assessment and automation of compliance monitoring using SCAP checks
CIS-CAT	Configuration assessment using CIS scanner and SCAP checks

Overview del monitoreo de políticas

Amenazas del sistema y respuesta de incidentes

En esta sección tenemos la sección de amenazas del sistema y respuesta a incidentes, en el que nos quedan los logs de un supuesto ataque, el listener del docker para saber quien ha intentado acceder y la respuesta activa configurada respecto a los incidentes

Esta sección es muy importante en el ámbito del threat hunting y el análisis de vulnerabilidades

También hay que contar con estos logs, ya que en el caso de una fuga de datos, en una supuesta declaración de como ha ocurrido un incidente, estos datos ayudan a los cuerpos del estado a concluir en las razones

System threats and incident response

Name	Description
Osquery	Expose an operating system as a high-performance relational database
Inventory data	Gather relevant information about system operating system, hardware, networking and packages
Active response	Active threat addressing by immediate response
Commands	Configuration options of the Command wodle
Docker listener	Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events

Overview de las amenazas del sistema y respuesta a incidentes

Análisis de los logs

En la parte del análisis de los logs, tenemos un escaneo mas en profundidad de los logs, también podemos subir nuestros logs y que sean guardados en el sistema

Otra cosa a valorar es para verificar integridad revisa si un archivo ha sido editado



Log data analysis

Name	Description
Log collection	Log analysis from text files, Windows events or syslog outputs
Integrity monitoring	Identify changes in content, permissions, ownership, and attributes of files

Overview del análisis de los logs

Seguridad del cloud

En el caso de tener un cloud vinculado a nuestros SIEM, tiene logs y configuraciones orientadas a cómo funcionan estos clouds, desde GitHub hasta el cloud de google

La parte de Github es muy interesante ya que en el caso de tener una empresa de programación, los branches y todo lo gestionado en nube se puede securizar y detectar amenazas en este ámbito

Cloud security monitoring

Name	Description
Amazon S3	Security events related to Amazon AWS services, collected directly via AWS API
Google Cloud Pub/Sub	Configuration options of the Google Cloud Pub/Sub module
GitHub	Detect threats targeting GitHub organizations

MITRE ATTACK

La base de datos MITRE es un conocimiento público y gratuito que describe las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios cibernéticos. Contiene información sobre tipos de amenazas, grupos de ataque, fases del ataque y técnicas específicas.

Wazuh integra la base de datos MITRE para enriquecer la información sobre las alertas de seguridad. Esto permite identificar con mayor precisión la naturaleza del ataque, priorizar las alertas en función de su severidad e impacto potencial, investigar los incidentes de forma más rápida y eficaz y responder a las amenazas de forma más eficiente.

Ejemplo: Si Wazuh detecta una actividad sospechosa en un sistema, puede compararla con la base de datos MITRE para determinar si se trata de una técnica de ataque conocida. Si se confirma la amenaza, Wazuh puede generar una alerta con información detallada sobre el ataque, como el tipo de amenaza, el grupo de ataque y las técnicas utilizadas.



En resumen, la integración de la base de datos MITRE en WAZUH permite una mejor comprensión de las amenazas, una respuesta más rápida a los incidentes y una mayor protección de la infraestructura.

The screenshot shows the Wazuh web interface with the MITRE ATT&CK framework overview. The interface includes a search bar, filters, and a table of tactics and techniques.

Tactics	Techniques
Credential Access	T1557 - Adversary-in-the-Middle
Execution	T1556.003 - Pluggable Authentication Modules
Impact	T1056.001 - Keylogging
Persistence	T1101.001 - Password Guessing
Privilege Escalation	T1003 - OS Credential Dumping
Lateral Movement	T1171 - LLMNR/NBT-NS Poisoning and Relay
Defense Evasion	T1539 - Steal Web Session Cookie
Exfiltration	T1552.005 - Cloud Instance Metadata API
Discovery	T1555.002 - Securityd Memory
Collection	T1522 - Cloud Instance Metadata API
	T1110.002 - Password Cracking
	T1555.001 - Keychain
	T1003.004 - LSA Secrets
	T1606.002 - SAML Tokens
	T1167 - Securityd Memory
	T1214 - Credentials in Registry
	T1003.007 - Proc Filesystem
	T1555.005 - Password Managers
	T1040 - Network Sniffing
	T1552.002 - Credentials in Registry
	T1556.002 - Password Filter DLL
	T1558.004 - AS-REP Roasting
	T1558 - Steal or Forge Kerberos Tickets
	T1555 - Credentials from Password Stores
	T1552 - Unsecured Credentials
	T1139 - Bash History
	T1503 - Credentials from Web Browsers
	T1145 - Private Keys
	T1555.003 - Credentials from Web Browsers
	T1557.003 - DHCP Spoofing
	T1552.004 - Private Keys

Overview de la base de datos de MITRE

Prueba de ataque

Hemos realizado un ataque desde nuestra máquina ubuntu haciendo un ataque de fuerza bruta al agente

```
lkas9@lks9-VirtualBox:~$ hydra -l admin -p test ssh://10.0.2.8
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
y).

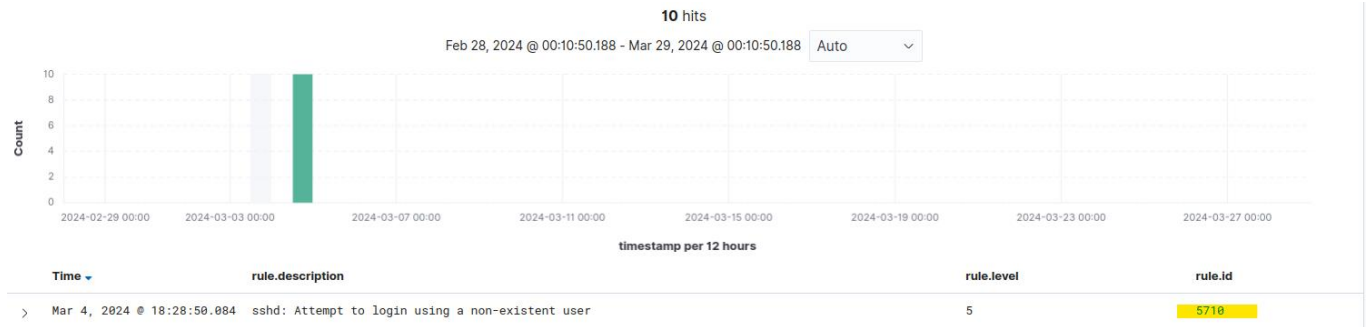
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-04 18:33:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.2.8:22/
[ERROR] could not connect to ssh://10.0.2.8:22 - Connection refused
lks9@lks9-VirtualBox:~$
```

Prueba de ataque SSH con hydra

Ha rechazado la conexión el ssh ya que no cuenta con las claves ni emplea contraseñas conocidas, pero mostraremos cómo el Wazuh nos muestra el ataque y como resolverlo

Basándonos en la documentación oficial podemos comprobar cuales son los IDs asociados al ataque de fuerza bruta

Linux - rule.id: (5551 OR 5712). Other related rules are 5710, 5711, 5716, 5720, 5503, 5504.



La aplicación nos muestra que se ha intentado conectar a nuestro agente por SSH

Aquí nos muestra en forma de gráfico el intento de ataques y la prioridad

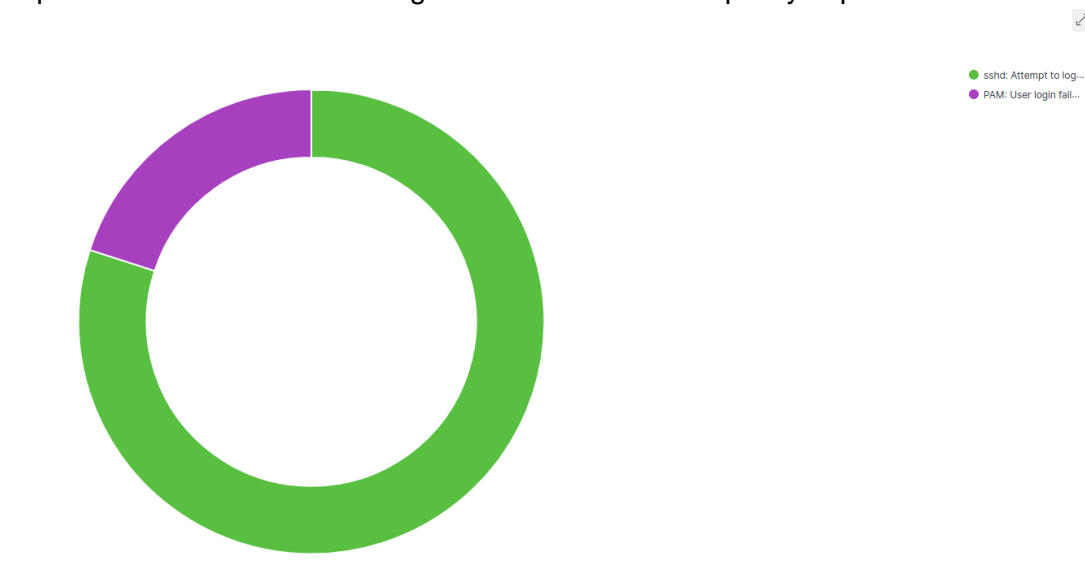
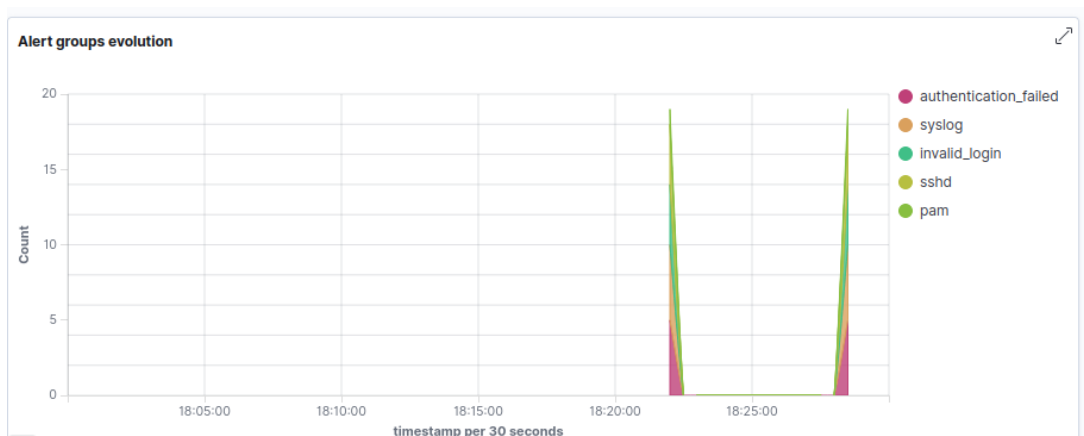


Gráfico ataques

Aquí podemos comprobar las alertas y cuando han sucedido, hemos hecho dos pruebas de ataque y se muestran en la gráfica





Configurando alertas

Primero creamos una alerta en el wazuh para que nos muestre las conexiones en el caso de que se produzcan

Para ello añadimos el `<active response>` en el archivo

`/var/ossec/etc/ossec.conf`

```
<command>
  <active-response>
    <name>firewall-drop</name>
    <executable>firewall-drop</executable>
    <timeout_allowed>yes</timeout_allowed>
  </active-response/>
</command>
```

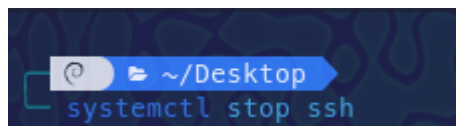
Después de otro intento de conexión aquí tenemos las alertas

Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Mar 4, 2024 @ 18:28:50.084	000	Ikas9-VirtualBox	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Mar 4, 2024 @ 18:28:48.083	000	Ikas9-VirtualBox	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Mar 4, 2024 @ 18:28:48.083	000	Ikas9-VirtualBox	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Mar 4, 2024 @ 18:28:48.083	000	Ikas9-VirtualBox	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Correcciones

Cerrar puerto ssh mientras no se esté usando



Por qué:

Protege tu sesión: Cuando cierras la sesión SSH, se termina la conexión segura entre tu dispositivo y el servidor remoto. Esto significa que cualquier persona que intente acceder a la sesión después de que la hayas cerrado no podrá hacerlo.

Evita el acceso no autorizado: Si dejas tu sesión SSH abierta, alguien podría acceder a tu dispositivo o al servidor remoto sin tu permiso. Esto puede permitirles robar datos, instalar malware o realizar otras acciones no deseadas.

Cambiar el puerto SSH por defecto en el archivo

`/etc/ssh/ssh_config`



```
Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP no
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
Port 1478
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
```

Por qué:

Reduce la exposición a ataques automatizados: Los bots y scripts que escanean Internet en busca de servidores vulnerables suelen buscar el puerto 22, que es el puerto por defecto de SSH. Si cambias el puerto, tu servidor será menos vulnerable a estos ataques automatizados.

Dificulta la detección de tu servidor SSH: Si el puerto SSH no es el 22, los atacantes tendrán que saber qué puerto estás usando para poder intentar acceder a tu servidor. Esto puede dificultar la detección de tu servidor por parte de atacantes que no estén específicamente buscando servidores con puertos SSH no estándar.

Creación de clave privada

```
ssh-keygen

Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519): kay.txt
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kay.txt
Your public key has been saved in kay.txt.pub
The key fingerprint is:
SHA256:riMAkcMi40gbu8YYOR2GkwarXrJLFcqfS2LVakVDETY kali@kali
The key's randomart image is:
+--[ED25519 256]--+
|B=o  Eo          |
|&@ .o .          |
|%=.. o           |
|*+. + .          |
|+B + o S         |
|o 0 + .          |
| * B .           |
|o = o ..         |
|. . . . .        |
+-----[SHA256]-----+
```

