

WAZUH (SIEM)_PRÁCTICA



WAZUH (SIEM)PRÁCTICA
Victoria Eugenia Pérez González
25/02/2023

ÍNDICE

Actividad 1: Configuración del SIEM Wazuh Manager	3
A) Por defecto, Wazuh Manager nos muestra en su tabla todas las alertas cuyo nivel de severidad sea 3 ó superior.	3
B) Podemos configurar Wazuh Manager para que nos envíe por email las notificaciones de las alertas de seguridad de cierto nivel de peligrosidad que se vayan generando.	4
Actividad 2: Incidente #1 – Acceso no autorizado a Windows con RDP:	6
Actividad 3: Incidente #2 – Cambios no autorizados en archivos de Windows	7
A) Configuraremos el cliente Wazuh Agent del equipo Windows 10 para monitorizar sus archivos de forma que podamos detectar si ocurriera un incidente de este tipo:	8
B) Crear nuevas reglas de alerta correlacionadas que se ejecute cuando ocurra una de las acciones anteriores (creación, modificación y eliminación) sobre archivos del equipo Agente Windows:	10
1.- Crear en el equipo Wazuh Manager una regla de alerta FIM que nos avise cuando el usuario llamado profesor cree (o copie) un nuevo archivo en alguno de los directorios que están siendo monitorizados.	10
2.- Crear otra regla de alerta FIM que nos alerte cuando alguien modifique los permisos un archivo perteneciente a alguno de los directorios monitorizados en el equipo Agente Windows:	11
3.- Añadir otra regla que nos alerte cuando alguien nos borre un archivo de tipo PDF:	12
Actividad 4: Incidente #3 – Acceso no autorizado a Linux con SSH:	14
A) Mejorar la regla de alerta con id 5720 ("sshd: Multiple authentication failures.") que trae definida Wazuh Manager para informar sobre ataques contra el login del servicio SSH.	14
B) Crear una nueva regla de alerta en Wazuh Manager que se active si un empleado inicia sesión en el servidor SSH del Agente Linux usando el usuario llamado Administrador, el usuario profesor o el usuario usuario; y además lo hace fuera del horario laboral de la empresa (6:30-21:00) y desde una dirección IP que no sea la del propio equipo localhost Ubuntu.	17
Actividad 5: Monitorización de eventos con Suricata en Wazuh:	19
Actividad 6: Incidente #4 – Detección de malware:	26
Actividad 7: Incidente #5 – Incidente compuesto:	28

En esta actividad simularemos una red local corporativa compuesta por:

- Una máquina Ubuntu desktop 20.04.3 que ejecutará Wazuh Manager (servidor). Puede ser un equipo Ubuntu Server 20.04.3 ya que ahorrará el consumo de RAM y el escritorio no es necesario porque Wazuh se administra por consola y mediante el dashboard web de Kibana 192.168.1.58
- Una máquina Windows 10 a monitorizar que ejecutará Wazuh Agent (cliente) 192.168.1.19
- Una máquina Ubuntu desktop 20.04.3 a monitorizar que ejecutará Wazuh Agent (cliente) 192.168.1.61

Actividad 1: Configuración del SIEM Wazuh Manager

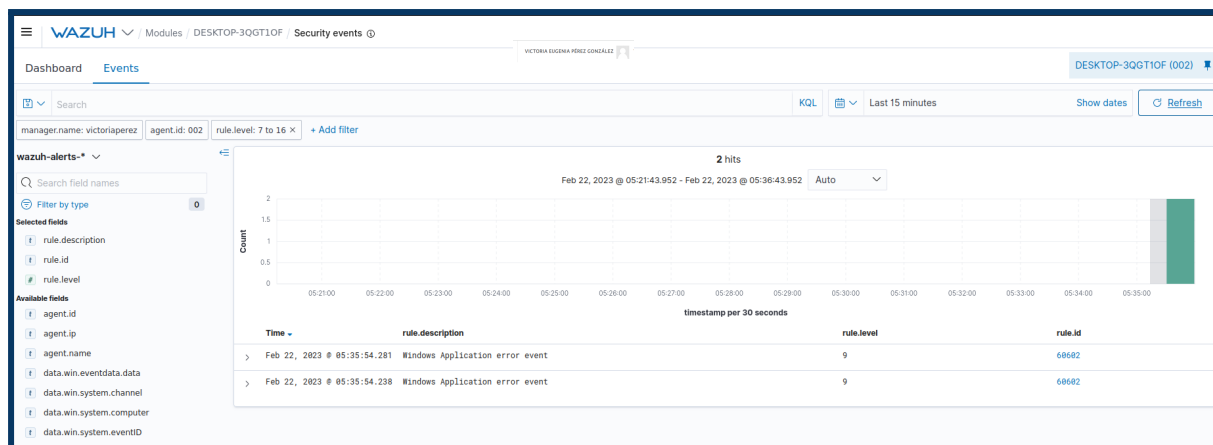
A) Por defecto, Wazuh Manager nos muestra en su tabla todas las alertas cuyo nivel de severidad sea 3 ó superior.

Para que no nos muestre tantas (demasiadas) alertas poco importantes, podemos cambiar el umbral mínimo de alerta y así separaremos el trigo de la paja.

Por ejemplo, subiremos el umbral para que sólo nos muestre las alertas de nivel 7 o superior.

De esta forma lograremos que no muestre todas las alertas independientes debidas a los intentos de login individuales (como es el caso de la regla con id 60122 de nivel 5).

Wazuh Manager comenzará aplicar el nuevo nivel de alerta para los nuevos eventos que se produzcan a partir de ahora. Para comprobarlo, lanzaremos el ataque con hydra varias veces y refrescamos la tabla de eventos de Wazuh Manager (botón Refresh). Comprobaremos que ya no muestra las nuevas alertas de nivel 3, ni de nivel 5; sino que aparecen varias seguidas de nivel 10 (60204) porque son ≥ 7 :



B) Podemos configurar Wazuh Manager para que nos envíe por email las notificaciones de las alertas de seguridad de cierto nivel de peligrosidad que se vayan generando.

Para poder usar una cuenta de GMail para que Wazuh nos envíe alertas con ella, debemos habilitar el "Acceso de aplicaciones poco seguras" en la configuración de Seguridad de nuestra cuenta de correo de GMail.

Ahora cambiaremos el umbral de las alertas para las que Wazuh Manager nos enviará un mail.

Para ello editaremos el archivo `/var/ossec/etc/ossec.conf` y modificaremos el valor de la directiva de la sección para que solo nos envíe emails con las alertas que sean de nivel 9 ó superior.

```
<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>9</email_alert_level>
</alerts>
```

Para aplicar los cambios recargamos el servicio Wazuh Manager:

```
#systemctl reload wazuh-manager
```

```
root@victoriaperez:/home/victoriaperez# systemctl reload wazuh-manager
root@victoriaperez:/home/victoriaperez#
```

Y para comprobarlo, relanzamos el ataque contra RDP usando hydra y refrescamos la tabla de alertas de Wazuh Manager. Debe mostrarnos la alerta de nivel 9 y además nos debe llegar por email su correo de notificación con todos los detalles de la alerta.

Wazuh Manager también nos permite forzar a que una regla siempre nos envíe la alerta por mail aunque su nivel de peligrosidad sea inferior al umbral mínimo definido. Para ello debemos añadirle a la regla la opción `alert_by_email`

```
-->
<rule id="100001" level="5">
  <if_sid>5716</if_sid>
  <srcip>1.1.1.1</srcip>
  <description>sshd: authentication failed from IP 1.1.1.1.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  <options>alert_by_email</options>
</rule>
```

También es posible enviar un informe diario con el resumen de las alertas ocurridas en el día. Este informe podemos personalizarlo indicando el umbral de nivel de peligrosidad de las alertas que deseamos que nos resuma en el informe.

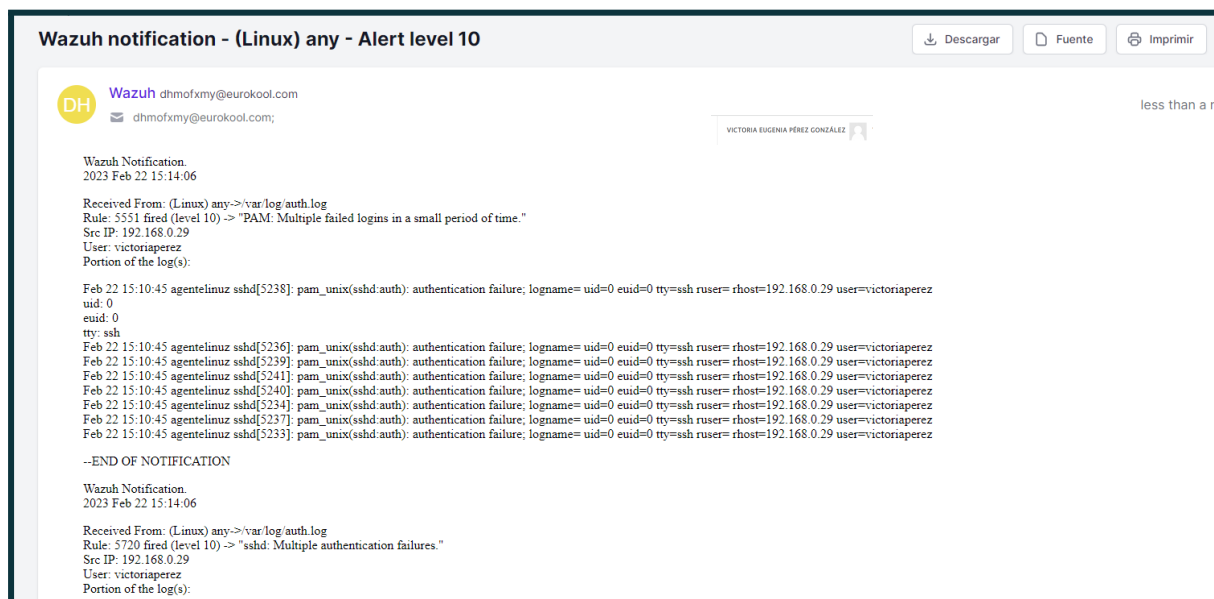
Para configurarlo, editamos nuevamente el archivo `/var/ossec/etc/ossec.conf` de Wazuh Manager y le añadimos las siguientes directivas al final del mismo:

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>no</logall_json>
    <email_notification>yes</email_notification>
    <smtp_server>localhost</smtp_server>
    <email_from>dhmofxmy@eurokool.com</email_from>
    <email_to>dhmofxmy@eurokool.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

Para aplicar los cambios recargamos el servicio Wazuh Manager:

```
root@victoriaperez:/home/victoriaperez# systemctl reload wazuh-manager
```

Se configura un postfix en ubuntu.



Actividad 2: Incidente #1 – Acceso no autorizado a Windows con RDP:

Crear una regla de alerta en Wazuh Manager, con nivel de severidad 10, que se active cuando se inicie sesión a través de RDP en el equipo Wazuh Agent Windows 10 usando el usuario privilegiado Administrador o el usuario profesor (|): authentication_success win.eventdata.ipAddress Administrador|profesor ¡ALERTA!: se ha iniciado sesion via RDP con el usuario privilegiado \$(win.eventdata.targetUserName)

```
<rule id="8888881" level="10" frequency="8" timeframe="60" >
  <if_matched_sid>60106</if_matched_sid>
  <same_field>win.eventdata.targetUserName</same_field>
  <description>¡ALERTA!: intento de acceso RDP no autorizado contra $(win.eventdata.targetUserName) desde $(win.eventdata.ipAddress)</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
</group>
```

Para comprobarlo recargamos el servicio Wazuh Manager y relanzamos el ataque con hydra indicando alguno de esos dos usuarios junto con su contraseña correcta para poder cumplir la regla: #hydra -l Administrador -p contraseña rdp://IPwazuhAgentWindows

```
(kali@kali)-[~]
└─$ hydra -l alumno -P passwords.lst -F rdp://192.168.0.12 -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-22 10:
19:26
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
reduce the number of parallel connections and -W 1 or -W 3 to wait between co
nnection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connecti
ons)
[WARNING] the rdp module is experimental. Please test, report - and if possib
le, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 15 login tries (l:1/p:15),
~4 tries per task
[DATA] attacking rdp://192.168.0.12:3389/
[ATTEMPT] target 192.168.0.12 - login "alumno" - pass "23456" - 1 of 15 [chil
d 0] (0/0)
[ATTEMPT] target 192.168.0.12 - login "alumno" - pass "<<jda" - 2 of 15 [chil
d 1] (0/0)
[ATTEMPT] target 192.168.0.12 - login "alumno" - pass "d" - 3 of 15 [child 2]
(0/0)
[ATTEMPT] target 192.168.0.12 - login "alumno" - pass "d" - 4 of 15 [child 3]
(0/0)
```

Luego refrescamos las alertas de Wazuh Manager (Refresh) para apreciar la nueva alerta creada:



Actividad 3: Incidente #2 – Cambios no autorizados en archivos de Windows

Vamos a analizar un incidente de seguridad consistente en que alguien sin permiso modifique carpetas o archivos del equipo Windows 10 (Wazuh Agent) que estamos monitorizando.

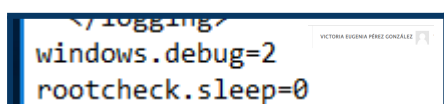
Este tipo de incidentes podría derivar en una exfiltración (fuga de datos), pérdida o modificación de datos (alterar su integridad).

Wazuh Agent es capaz de detectar cuándo se realizan cambios en el File System del equipo (Windows o Linux) puesto que también tiene capacidades FIM (File Integrity Monitoring). Esto nos proporciona detalles importantes para poder analizar el incidente; tales como qué usuario fue, cuándo, o qué cambios hizo sobre qué archivos (son el activo más importante de toda organización).

A) Configuraremos el cliente Wazuh Agent del equipo Windows 10 para monitorizar sus archivos de forma que podamos detectar si ocurriera un incidente de este tipo:

Comenzaremos por modificar el archivo C:\Program Files (x86)\ossec-agent\internal_options.conf cambiando el valor de estas dos directivas

```
windows.debug=2  
rootcheck.sleep=0
```



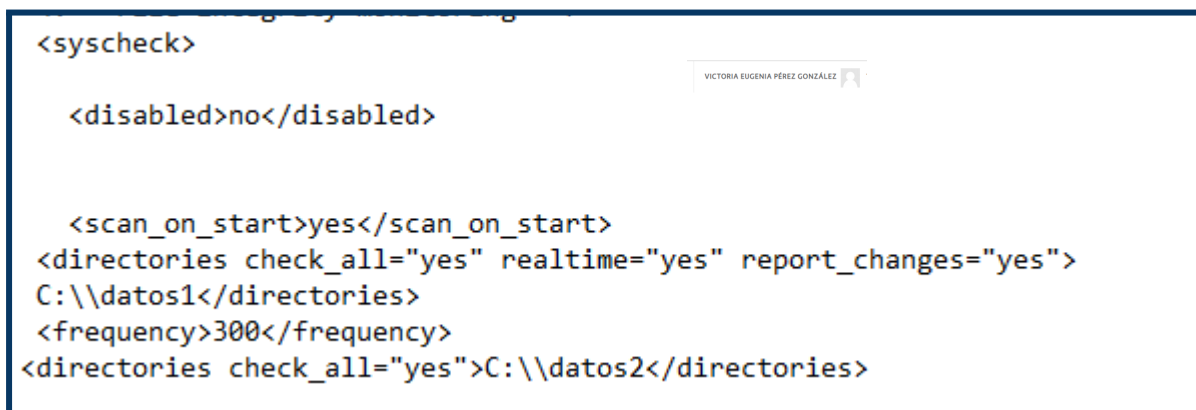
A screenshot of a text editor window showing the configuration file internal_options.conf. The file content is as follows:

```
</logging>  
windows.debug=2  
rootcheck.sleep=0
```

Y le añadiremos esta otra directiva al final del archivo para luego guardar los cambios: syscheck.sleep=0 El siguiente paso será crear dos directorios de prueba en el equipo Agente Windows10:

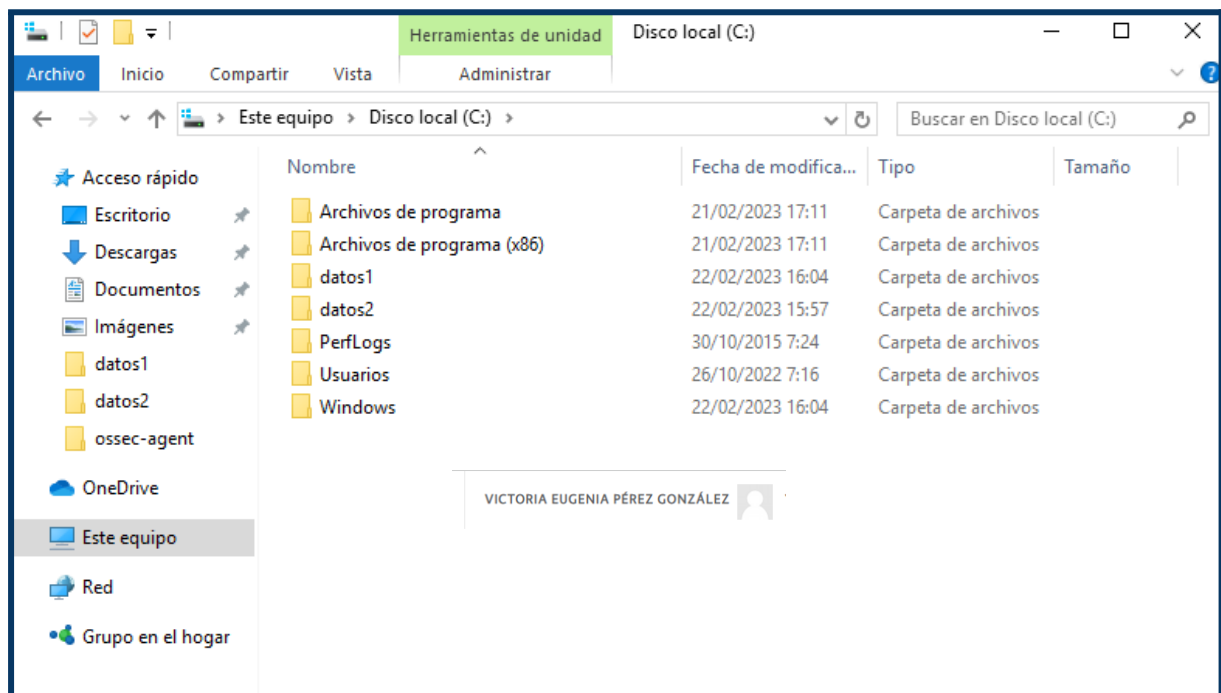
C:\datos1 y C:\datos2 Luego seleccionaremos en la aplicación cliente para Windows Wazuh Agent win32ui.exe la opción de menú View->View Config y sustituir todo el contenido de la sección por este otro:

```
<syscheck>  
<disabled>no</disabled>  
<scan_on_start>yes</scan_on_start>  
<directories check_all="yes" realtime="yes" report_changes="yes">  
C:\\datos1</directories>  
<frequency>300</frequency>  
<directories check_all="yes">C:\\datos2</directories>  
</syscheck>
```



A screenshot of the Win32UI application window. The 'View' menu is open, and the 'View Config' option is selected. The application window title is 'Wazuh Win32UI'. The background shows the same configuration file content as the previous screenshot.

Con ello le indicamos a Wazuh Agent que analice los cambios del directorio C:\datos1 constantemente (en tiempo real); mientras que el directorio C:\datos2 deberá monitorizarse periódicamente cada 5 minutos. Además, cada vez que se produzca un cambio en el contenido de los archivos de C:\datos1 se generará una alerta que incluirá los detalles del contenido que ha cambiado (para ficheros de texto); mientras que si se cambia en C:\datos2 no.



Ahora deberemos guardar los cambios del fichero y recargar el Agente Wazuh de Windows (menú Manage→Restart)

Finalmente, para comprobar su funcionamiento probaremos a crear, borrar y modificar ficheros de los directorios monitorizados por Wazuh; y luego verificaremos que se visualizan las alertas en la sección Integrity monitoring->Events del SIEM Wazuh Manager:

Si hacemos clic sobre una de las alertas podemos analizar en detalle todos sus campos clave

Como puede observarse, Wazuh ejecuta la regla de alerta con id 554 cuando un archivo es creado o copiado, la regla 553 cuando es eliminado y la regla 550 cuando lo modificamos

Time	rule.description	rule.level	rule.id
> Feb 22, 2023 @ 15:55:05.868	File added to the system.	5	554

>	Feb 22, 2023 @ 16:00:27.767	File deleted.	VICTORIA EUGENIA PÉREZ GONZÁLEZ	7	553	
>	Feb 22, 2023 @ 16:00:26.947	Registry Value Integrity Checksum Changed		5	750	SecureTimeLow
>	Feb 22, 2023 @ 16:00:26.902	Registry Value Integrity Checksum Changed	VICTORIA EUGENIA PÉREZ GONZÁLEZ	5	750	SecureTimeHigh

Como puede observarse, Wazuh ejecuta la regla de alerta con id 554 cuando un archivo es creado o copiado, la regla 553 cuando es eliminado y la regla 550 cuando lo modificamos

B) Crear nuevas reglas de alerta correlacionadas que se ejecute cuando ocurra una de las acciones anteriores (creación, modificación y eliminación) sobre archivos del equipo Agente Windows:

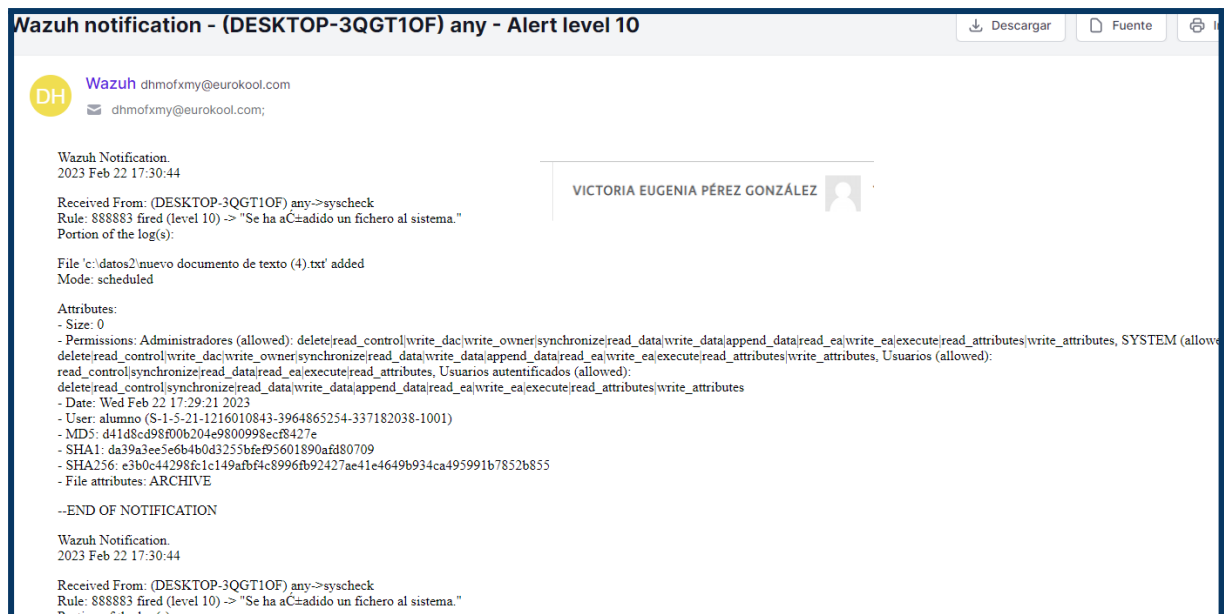
1.- Crear en el equipo Wazuh Manager una regla de alerta FIM que nos avise cuando el usuario llamado profesor cree (o copie) un nuevo archivo en alguno de los directorios que están siendo monitorizados.

Para ello editaremos el archivo `/var/ossec/etc/rules/local_rules.xml` y le añadiremos la regla nueva en la sección existente. Debemos usar un id de regla no repetido

Si se añade un documento o copia un documento.

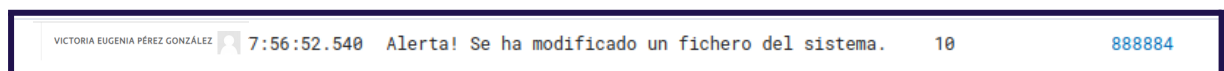
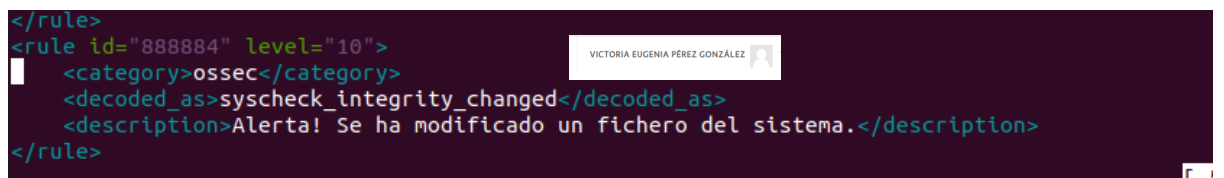
```
<rule id="888883" level="5">
  <category>ossec</category>
  <decoded_as>syscheck_new_entry</decoded_as>
  <description>Se ha añadido un fichero al sistema.</description>
</rule>
```

>	VICTORIA EUGENIA PÉREZ GONZÁLEZ	17:30:44.947	Se ha añadido un fichero al sistema.	10	888883	c:\datos2\nuevo documento de texto.txt
---	---------------------------------	--------------	--------------------------------------	----	--------	--



2.- Crear otra regla de alerta FIM que nos alerte cuando alguien modifique los permisos un archivo perteneciente a alguno de los directorios monitorizados en el equipo Agente Windows:

Se modifica un fichero o los permisos del mismo.



Wazuh Notification.
2023 Feb 22 17:56:52

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Received From: (DESKTOP-3QGT1OF) any->syscheck
Rule: 888884 fired (level 10) -> "Alerta! Se ha modificado un fichero del sistema."
Portion of the log(s):

Registry Value '[x32] HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount' modified
Mode: scheduled
Changed attributes: md5,sha1,sha256
Old md5sum was: '0902c99fdd8c99787ce983431784a114'
New md5sum is : '1a3559386f720d82d26740fe079365fc'
Old sha1sum was: '3498cccf3d8621ecac673d6a746e731d09e58807'
New sha1sum is : '5468d017bc3c0f545f8ede19acad19bae2412645'
Old sha256sum was: '5e801f83538fda8d4524ff52cfc69a78a2a5dcb0f146d0c1dfcf90d513a935f'
New sha256sum is : '69c47754c078995c2690af0a33fa6745b79f444bed0b5e3ba13a4095f405559c'

Attributes:
- Size: 8
- MD5: 1a3559386f720d82d26740fe079365fc
- SHA1: 5468d017bc3c0f545f8ede19acad19bae2412645
- SHA256: 69c47754c078995c2690af0a33fa6745b79f444bed0b5e3ba13a4095f405559c

--END OF NOTIFICATION

Wazuh Notification.
2023 Feb 22 17:56:52

Received From: (DESKTOP-3QGT1OF) any->syscheck
Rule: 888884 fired (level 10) -> "Alerta! Se ha modificado un fichero del sistema."
Portion of the log(s):

3.- Añadir otra regla que nos alerte cuando alguien nos borre un archivo de tipo PDF:

```
<rule id="888882" level="10">  
  <category>ossec</category>  
  <decoded_as>syscheck_deleted</decoded_as>  
  <description>¡ALERTA! Se ha borrado un archivo del sistema.</description>  
</rule>
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Feb 22, 2023 @ 19:14:25.660
Se ha añadido un fichero al sistema.
10
888883

Expanded document
View surrounding documents
View single document

TableJSON

f _id	ftiMeoYBmzU3p88-enIj
f _index	wazuh-alerts-4.x-2023.02.22
# _score	-
f _type	_doc
f agent.id	002
f agent.ip	192.168.0.12
f agent.name	DESKTOP-3QGT1OF
f decoder.name	syscheck_new_entry
f full_log	File 'c:\datos2\2.pdf' added Mode: scheduled
f id	1677093265.4501588

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Wazuh notification - (DESKTOP-3QGT1OF) any - Alert level 10
Descargar
Fuente
Imprimir
Borrar

DH
Wazuh
dhmofxmy@eurokool.com
dhmofxmy@eurokool.com;

1 minute ago

Wazuh Notification.
2023 Feb 22 19:14:25

Received From: (DESKTOP-3QGT1OF) any->syscheck
Rule: 888883 fired (level 10) -> "Se ha aC=adido un fichero al sistema."
Portion of the log(s):

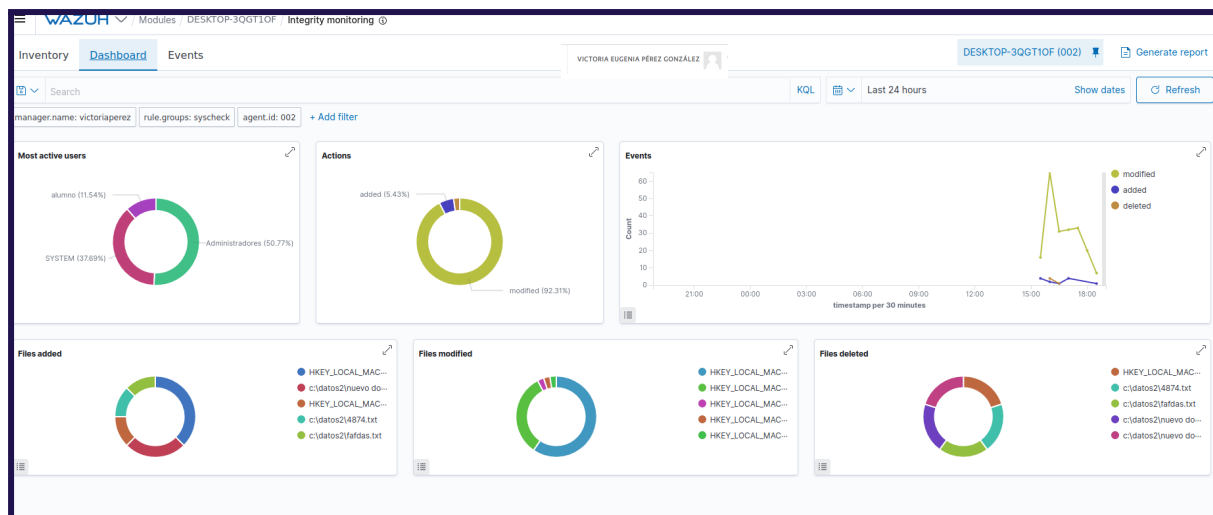
File 'c:\datos2\2.pdf' added
Mode: scheduled

Attributes:
- Size: 37524
- Permissions: Administradores (allowed): delete/read_control/write_dac/write_owner/synchronize/read_data/write_data/append_data/read_ea/write_ea/execute/read_attributes/write_attributes, SYSTEM (allowed): delete/read_control/write_dac/write_owner/synchronize/read_data/write_data/append_data/read_ea/write_ea/execute/read_attributes/write_attributes, Usuarios (allowed): read_control/synchronize/read_data/read_ea/execute/read_attributes, Usuarios autenticados (allowed): delete/read_control/synchronize/read_data/write_data/append_data/read_ea/write_ea/execute/read_attributes/write_attributes
- Date: Wed Feb 22 19:10:11 2023
- User: alumno (S-1-5-21-1216010843-3964865254-337182038-1001)
- MD5: 9f1a182f1cbe1e62249c4eb7ddd49841
- SHA1: 932a35c5221a05ef55c0a63977fb1ac1668859c2
- SHA256: 18c0123869b9e023bf0cdadada989e9b553b21428113badeb4ef4ac1be03e
- File attributes: ARCHIVE, TEMPORARY

--END OF NOTIFICATION

VICTORIA EUGENIA PÉREZ GONZÁLEZ

El último paso será verificar en la web de Wazuh Manager (sección Integrity monitoring) cómo ha detectado esta actividad con los archivos. En la pestaña Dashboard se muestra el resumen estadístico de las alertas FIM ocurridas



Actividad 4: Incidente #3 – Acceso no autorizado a Linux con SSH:

A) Mejorar la regla de alerta con id 5720 ("sshd: Multiple authentication failures.") que trae definida Wazuh Manager para informar sobre ataques contra el login del servicio SSH.

Crearemos una nueva regla de alerta de nivel 10 que se active por agregación de varios eventos consecutivos del mismo tipo. Se activará si previamente se activa varias veces (al menos 5) la regla con id 5716 ("sshd: authentication failed.", level=5) en un periodo de tiempo de un 1 minuto y proveniente siempre desde la misma dirección IP de origen.

```
<rule id="100006" level="10" frequency="5" timeframe="60">
  <if_matched_sid>5716</if_matched_sid>
  <same_source_ip />
  <description>sshd:Alerta login desde $(srcip)</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  <options>alert_by_email</options>
</rule>
```

Luego guardaremos los cambios y recargamos el servicio Wazuh Manager para que los aplique: `#systemctl reload wazuh-manager`

Ahora lanzaremos el ataque al logind de SSH con hydra: #hydra -l usuario -P passwords.lst ssh://IPwazuhAgenteLinux

```
(kali㉿kali)-[~]
└─$ hydra -l victoriaperez -P passwords.lst -F ssh://192.168.0.32 -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-22 14:
34:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15)
, ~1 try per task
[DATA] attacking ssh://192.168.0.32:22/
[ATTEMPT] target 192.168.0.32 - login "victoriaperez" - pass "23456" - 1 of 1
5 [child 0] (0/0)
[ATTEMPT] target 192.168.0.32 - login "victoriaperez" - pass "<<jda" - 2 of 1
5 [child 1] (0/0)
[ATTEMPT] target 192.168.0.32 - login "victoriaperez" - pass "d" - 3 of 15 [c
hild 2] (0/0)
[ATTEMPT] target 192.168.0.32 - login "victoriaperez" - pass "d" - 4 of 15 [c
hild 3] (0/0)
```

Por último refrescamos la tabla de alertas de Wazuh Manager para apreciar la nueva alerta creada entre las últimas alertas :

>	Feb 22, 2023 @ 20:20:24.963	sshd:Alerta login desde 192.168.0.29	VICTORIA EUGENIA PÉREZ GONZÁLEZ	10	100006
---	-----------------------------	--------------------------------------	---------------------------------	----	--------

Además, para evitar que se acumulen en el SIEM varias alertas del mismo tipo, editaremos la regla 5551 ("PAM: Multiple failed logins in a small period of time.", level=10) y le cambiaremos el nivel a 0 para silenciarla. Deberemos editar el archivo /var/ossec/ruleset/rules/0085-pam_rules.xml

```
<rule id="5551" level="0" frequency="8" timeframes="180">
  <if_matched_sid>5503</if_matched_sid>
  <same_source_ip />
  <description>PAM: Multiple failed logins in a small period of time.</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failures,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_11.4,gpg13_7.8,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nis
</rule>
```

También silenciamos la regla 5720 ("sshd: Multiple authentication failures.", level=10) cambiándole el nivel de alerta a 0 en el archivo: /var/ossec/ruleset/rules/0095-sshd_rules.xml

```
<rule id="5720" level="0" frequency="8">
  <if_matched_sid>5716</if_matched_sid>
  <same_source_ip />
  <description>sshd: Multiple authentication failures.</description>

  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failures,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_11.4,gpg13_7.1,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164
</rule>

<rule id="5721" level="0">
```

Finalmente guardaremos los cambios, recargamos el servicio Wazuh Manager, repetiremos varias veces el ataque al usuario SSH con hydra y comprobaremos cómo el SIEM registra la alerta producida por nuestra nueva regla y ya no registra el resto de alertas similares (5720, 5551)

>	Feb 22, 2023 @ 20:26:50.452	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:50.409	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.433	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.430	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.428	sshd:Alerta login desde 192.168.0.29	10	100006
>	Feb 22, 2023 @ 20:26:48.426	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.422	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.419	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.416	sshd: authentication failed.	5	5716
>	Feb 22, 2023 @ 20:26:48.413	sshd:Alerta login desde 192.168.0.29	10	100006

Wazuh notification - (Linux) any - Alert level 10



Wazuh dhmofoxmy@eurokool.com

dhmofoxmy@eurokool.com;

VICTORIA EUGENIA PÉREZ GONZÁLEZ



Wazuh Notification.
2023 Feb 22 20:26:41

Received From: (Linux) any->/var/log/auth.log
Rule: 100006 fired (level 10) -> "sshd:Alerta login desde 192.168.0.29"
Src IP: 192.168.0.29
User: victoriaperez
Portion of the log(s):

Feb 22 20:26:41 agentelinuz sshd[7386]: Failed password for victoriaperez from 192.168.0.29 port 34864 ssh2
Feb 22 20:26:41 agentelinuz sshd[7384]: Failed password for victoriaperez from 192.168.0.29 port 34860 ssh2
Feb 22 20:26:41 agentelinuz sshd[7389]: Failed password for victoriaperez from 192.168.0.29 port 34870 ssh2
Feb 22 20:26:41 agentelinuz sshd[7380]: Failed password for victoriaperez from 192.168.0.29 port 34852 ssh2
Feb 22 20:26:41 agentelinuz sshd[7388]: Failed password for victoriaperez from 192.168.0.29 port 34868 ssh2

--END OF NOTIFICATION

Wazuh Notification.
2023 Feb 22 20:26:41

Received From: (Linux) any->/var/log/auth.log
Rule: 100006 fired (level 10) -> "sshd:Alerta login desde 192.168.0.29"
Src IP: 192.168.0.29
User: victoriaperez
Portion of the log(s):

Feb 22 20:26:41 agentelinuz sshd[7387]: Failed password for victoriaperez from 192.168.0.29 port 34866 ssh2
Feb 22 20:26:41 agentelinuz sshd[7383]: Failed password for victoriaperez from 192.168.0.29 port 34858 ssh2
Feb 22 20:26:41 agentelinuz sshd[7385]: Failed password for victoriaperez from 192.168.0.29 port 34862 ssh2
Feb 22 20:26:41 agentelinuz sshd[7391]: Failed password for victoriaperez from 192.168.0.29 port 34878 ssh2
Feb 22 20:26:41 agentelinuz sshd[7381]: Failed password for victoriaperez from 192.168.0.29 port 34854 ssh2

--END OF NOTIFICATION

Wazuh Notification.
2023 Feb 22 20:26:44

B) Crear una nueva regla de alerta en Wazuh Manager que se active si un empleado inicia sesión en el servidor SSH del Agente Linux usando el usuario llamado Administrador, el usuario profesor o el usuario usuario; y además lo hace fuera del horario laboral de la empresa (6:30-21:00) y desde una dirección IP que no sea la del propio equipo localhost Ubuntu.

Hay que tener en cuenta que antes de que se ejecute nuestra nueva regla se deberá haber ejecutado previamente la regla con id 5715 ("sshd: authentication success.", level=3, archivo /var/ossec/ruleset/rules/0095-sshd_rules.xml). Por lo tanto habrá correlación de eventos.

Editaremos el archivo /var/ossec/etc/rules/local_rules.xml y añadiremos la nueva regla:

```

</rule>
<rule id="107101" level="9">
  <if_sid>5715</if_sid>
  <if_group>authentication_success</if_group>
  <time>9 pm - 6:30 am</time>
  <description>El usuario se ha logado fuera del horario de trabajo desde $(srcip).</description>
  <group>login_time,pci_dss_10.2.5,pci_dss_10.6.1,gpg13_7.1,gpg13_7.2,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14</group>
</rule>

</group>

```

Luego guardaremos los cambios y recargamos el servicio Wazuh Manager para que los aplique. Para comprobarlo, iniciaremos sesión en el Agente SSH Linux con el usuario Administrador junto con su contraseña correcta desde otro equipo con putty, con el cliente de consola; o bien con: #hydra -l profesor -p sucontraseña ssh://IPAgenteWazuhLinux

```

(kali㉿kali)-[~]
$ hydra -l victoriaperez -P passwords.lst ssh://192.168.0.32

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-24 02:
06:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:1/p:16)
, ~1 try per task
[DATA] attacking ssh://192.168.0.32:22/
[22][ssh] host: 192.168.0.32 login: victoriaperez password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complet
e until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-24 02:
06:56

(kali㉿kali)-[~]
$

```

Luego refrescamos la tabla de alertas de Wazuh Manager para apreciar la nueva alerta generada

nota:se ha cambiado el horario momentáneamente para que saliese la alerta ya que ni a las 9 ni a las 6 y 30 estaba realizando la práctica.

Feb 24, 2023 @ 07:50:38.411	VICTORIA EUGENIA PÉREZ GONZÁLEZ	El usuario se ha logado fuera del horario de trabajo desde 192.168.0.29.	9	107101
--------------------------------	---------------------------------	--	---	--------

Actividad 5: Monitorización de eventos con Suricata en Wazuh:

Wazuh Agent es un HIDS que se puede complementar con un NIDS como Suricata porque ambos trabajan con archivos de log en formato JSON. A) Instalaremos el HIDS Suricata en el equipo Agente Linux para poder detectar otro tipo de alertas mediante firmas (reglas de detección):

```
#add-apt-repository ppa:oisf/suricata-stable
```

```
Victoria Eugenia Pérez González
root@agentelinuz:~# sudo su
[sudo] contraseña para victoriaperez:
root@agentelinuz:/home/victoriaperez# add-apt-repository ppa:oisf/suricata-stable
e
  Suricata IDS/IPS/NSM stable packages
  https://suricata.io/
  https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.
```

```
#apt install suricata
```

```
Victoria Eugenia Pérez González
root@agentelinuz:/home/victoriaperez# apt install suricata
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14
  libhttp2 libhyperscan5 liblua5.1-2 liblua5.1-common liblzma-dev
  libnet1 libnetfilter-queue1
Paquetes sugeridos:
  liblzma-doc
Se instalarán los siguientes paquetes NUEVOS:
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14
  libhttp2 libhyperscan5 liblua5.1-2 liblua5.1-common liblzma-dev
  libnet1 libnetfilter-queue1 suricata
0 actualizados, 12 nuevos se instalarán, 0 para eliminar y 121 no actualizados.
Se necesita descargar 5.195 kB de archivos.
Se utilizarán 24,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Seguidamente editaremos el archivo `/etc/suricata/suricata.yaml` para ajustar el valor de la directiva `HOME_NET` con la dirección IP de nuestra red local y el nombre de la interfaz de red del equipo por la que capturará el tráfico:

```
ars:
# more specific is better for alert accuracy and performance
address-groups:
  HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
  #HOME_NET: "[192.168.0.0/16]"
  #HOME_NET: "[10.0.0.0/8]"
  #HOME_NET: "[172.16.0.0/12]"
  #HOME_NET: "any"

  EXTERNAL_NET: "!$HOME_NET"
  #EXTERNAL_NET: "any"
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

```
# Linux high speed capture support
af-packet:
- interface: enp0s3
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per
  # This is only supported for Linux kernel > 3.1
  # possible value are:
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Luego guardaremos los cambios y reiniciamos el servicio Suricata:

```
#systemctl restart suricata
```

```
root@agentelinuz:/home/victoriaperez# systemctl restart suricata
root@agentelinuz:/home/victoriaperez#
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

```
#systemctl status suricata
```

```
root@agentelinuz:/home/victoriaperez# systemctl restart suricata
root@agentelinuz:/home/victoriaperez# systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; generated)
   Active: active (running) since Fri 2023-02-24 13:31:00 WET; 20s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 12690 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
    Tasks: 8 (limit: 4623)
   Memory: 45.0M
    CGroup: /system.slice/suricata.service
            └─12699 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vv

feb 24 13:31:00 agentelinuz systemd[1]: Starting LSB: Next Generation IDS/IPS...
feb 24 13:31:00 agentelinuz suricata[12690]: Likely stale PID 12465 with /var/run/suricata.pid exists, but process is no
feb 24 13:31:00 agentelinuz suricata[12690]: Removing stale PID file /var/run/suricata.pid
feb 24 13:31:00 agentelinuz suricata[12690]: Starting suricata in IDS (af-packet) mode... done.
feb 24 13:31:00 agentelinuz systemd[1]: Started LSB: Next Generation IDS/IPS.
root@agentelinuz:/home/victoriaperez#
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

El siguiente paso será crear una regla de detección para probar el IDS. Para ello debemos crear el archivo `/var/lib/suricata/rules/suricata.rules` para añadir nuestras propias reglas de detección:

Y le añadiremos la siguiente regla de ejemplo que permitirá detectar cualquier ping: alert icmp any any -> any any (msg:"PING RECIBIDO"; sid:200001;)

```
GNU nano 4.8 suricata.rules
alert icmp any any -> any any (msg:"PING RECIBIDO"; sid:200001;)
```

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Guardaremos los cambios y reiniciamos Suricata para que comience a aplicar la nueva regla: `#systemctl restart suricata`

```
root@agentelinuz:/var/lib/suricata/rules# systemctl restart suricata
root@agentelinuz:/var/lib/suricata/rules#
```

Si deseamos chequear la sintaxis de las reglas que hemos escrito, ejecutaremos: `#suricata -T`

```
root@agentelinuz:/var/lib/suricata/rules# suricata -T
24/2/2023 -- 13:36:57 - <Info> - Running suricata under test mode
24/2/2023 -- 13:36:57 - <Notice> - This is Suricata version 6.0.10 RELEASE running in SYSTEM mode
24/2/2023 -- 13:36:58 - <Notice> - Configuration provided was successfully loaded. Exiting.
root@agentelinuz:/var/lib/suricata/rules#
```

Para probarlo enviaremos pings al equipo Agente Linux que tiene Suricata desde cualquier equipo: `#ping IPwazuhAgenteLinux`

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping 192.168.0.32
PING 192.168.0.32 (192.168.0.32) 56(84) bytes of data.
64 bytes from 192.168.0.32: icmp_seq=1 ttl=64 time=0.729 ms
64 bytes from 192.168.0.32: icmp_seq=2 ttl=64 time=0.357 ms
64 bytes from 192.168.0.32: icmp_seq=3 ttl=64 time=0.748 ms
```

Finalmente consultaremos el log de Suricata para ver cómo lo detecta y lo registra: `#tail -f /var/log/suricata/fast.log`

```
root@agentelinuz:/var/lib/suricata/rules# tail -f /var/log/suricata/fast.log
02/24/2023-13:36:43.870126  [**] [1:200001:0] PING RECIBIDO [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.29:8 -> 192.168.0.32:0
02/24/2023-13:36:43.870148  [**] [1:200001:0] PING RECIBIDO [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.32:0 -> 192.168.0.29:0
```

B) Para integrar Suricata en Wazuh Agent, editaremos el archivo `/var/ossec/etc/ossec.conf` del equipo Agente Linux donde se ejecuta Suricata y Wazuh Agent, y le añadiremos una directiva en la sección para indicarle cuál es la ruta del archivo log de Suricata en formato JSON:

```
<!-- Log analysis -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
  <log_format>syslog</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

Seguidamente guardaremos los cambios y recargamos el Agente Wazuh para que los aplique: `#systemctl reload wazuh-agent`

```
root@agentelinux:/var/lib/suricata/rules# systemctl reload wazuh-agent
```

Dado que las reglas de alerta de Suricata tienen un nivel de peligrosidad 3, debemos garantizarnos que la directiva del archivo de configuración de Wazuh Manager `/var/ossec/etc/ossec.conf` tiene un valor mayor o igual que 3. También sería posible instalar Suricata en el propio equipo Wazuh Manager para que este analizase todo el tráfico de la red local a modo de NIDS. En este caso se configuraría de igual modo (instalar Suricata en el equipo Linux Wazuh Manager e integrarlo en Wazuh Manager añadiéndole la directiva). Para poder comprobar las alertas de Suricata en Wazuh Agent, volveremos a enviar pings al equipo Linux Wazuh Agent:

```
(kali㉿kali)-[~]
$ ping 192.168.0.32
PING 192.168.0.32 (192.168.0.32) 56(84) bytes of data.
64 bytes from 192.168.0.32: icmp_seq=1 ttl=64 time=0.334 ms
64 bytes from 192.168.0.32: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 192.168.0.32: icmp_seq=3 ttl=64 time=0.320 ms
64 bytes from 192.168.0.32: icmp_seq=4 ttl=64 time=0.542 ms

64 bytes from 192.168.0.32: icmp_seq=5 ttl=64 time=0.979 ms
64 bytes from 192.168.0.32: icmp_seq=6 ttl=64 time=1.09 ms
64 bytes from 192.168.0.32: icmp_seq=7 ttl=64 time=0.492 ms
64 bytes from 192.168.0.32: icmp_seq=8 ttl=64 time=0.448 ms
64 bytes from 192.168.0.32: icmp_seq=9 ttl=64 time=0.933 ms
64 bytes from 192.168.0.32: icmp_seq=10 ttl=64 time=0.849 ms
64 bytes from 192.168.0.32: icmp_seq=11 ttl=64 time=0.371 ms
64 bytes from 192.168.0.32: icmp_seq=12 ttl=64 time=0.942 ms
64 bytes from 192.168.0.32: icmp_seq=13 ttl=64 time=0.699 ms
64 bytes from 192.168.0.32: icmp_seq=14 ttl=64 time=0.708 ms
64 bytes from 192.168.0.32: icmp_seq=15 ttl=64 time=0.965 ms
64 bytes from 192.168.0.32: icmp_seq=16 ttl=64 time=0.989 ms
```

Seguidamente recargamos la web del SIEM Wazuh Manager para ver cómo muestra la nueva alerta procedente de Suricata con id 86601:

Generalmente debemos esperar un poco hasta que la web de Wazuh Manager nos muestre las alertas de Suricata, ya que la comunicación del evento y la detección no son inmediatas.

C) Añadir dos nuevas reglas de detección en el IDS Suricata del equipo Linux Wazuh Agent:

- Una regla que alerte cuando desde el equipo Wazuh Agent se visite alguna de estas webs prohibidas: as.com o facebook.com o game.com

```
alert dns any any -> any any (msg:"BLOQUEO WEB"; dns_query;  
pcpre:"/as|facebook|game/"; sid:200002;) -
```

Una regla que alerte cuando el equipo Wazuh Agent reciba un ataque de tipo DoS mediante la técnica ICMP flood

```
alert icmp any any -> any any (msg:"ATAQUE DOS ICMP FLOOD"; itype:8;  
detection_filter:track by_dst,count 5,seconds 5; sid:200003;)
```

Esta regla tiene un filtro de detección para evitar que se muestran muchas alertas seguidas.

```
GNU nano 4.8 suricata.rules Modificado  
alert icmp any any -> any any (msg:"PING RECIBIDO"; sid:200001;)  
  
alert dns any any -> any any (msg:"BLOQUEO WEB"; dns_query; pcpre:"/as|facebook|game/"; sid:200002;  
alert icmp any any -> any any (msg:"ATAQUE DOS ICMP FLOOD"; itype:8; detection_filter:track by_dst,count 5,seconds 5; sid:200003;)
```

Para poder comprobar las reglas guardaremos el archivo y reiniciamos el servicio Suricata::
#systemctl restart suricata

```
root@agentelinux:/var/lib/suricata/rules# systemctl restart suricata  
root@agentelinux:/var/lib/suricata/rules#
```

seguidamente generamos el tráfico necesario para que ocurran los eventos que activen las reglas: - Visitaremos algunas de las webs prohibidas desde el equipo Linux Wazuh Agent:
#curl -L www.as.com

```
root@victoriaperez:/var/ossec/etc# curl -L www.as.com
```

- Enviar pings constantes desde un equipo hacia la IP del equipo Wazuh Agent Linux: #ping IPwazuhAgenteLinux


```
(kali㉿kali)-[~]
$ ping 192.168.0.32
PING 192.168.0.32 (192.168.0.32) 56(84) bytes of data.
64 bytes from 192.168.0.32: icmp_seq=1 ttl=64 time=0.334 ms
64 bytes from 192.168.0.32: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 192.168.0.32: icmp_seq=3 ttl=64 time=0.320 ms
64 bytes from 192.168.0.32: icmp_seq=4 ttl=64 time=0.542 ms

64 bytes from 192.168.0.32: icmp_seq=5 ttl=64 time=0.979 ms
64 bytes from 192.168.0.32: icmp_seq=6 ttl=64 time=1.09 ms
64 bytes from 192.168.0.32: icmp_seq=7 ttl=64 time=0.492 ms
64 bytes from 192.168.0.32: icmp_seq=8 ttl=64 time=0.448 ms
64 bytes from 192.168.0.32: icmp_seq=9 ttl=64 time=0.933 ms
64 bytes from 192.168.0.32: icmp_seq=10 ttl=64 time=0.849 ms
64 bytes from 192.168.0.32: icmp_seq=11 ttl=64 time=0.371 ms
64 bytes from 192.168.0.32: icmp_seq=12 ttl=64 time=0.942 ms
64 bytes from 192.168.0.32: icmp_seq=13 ttl=64 time=0.699 ms
64 bytes from 192.168.0.32: icmp_seq=14 ttl=64 time=0.708 ms
64 bytes from 192.168.0.32: icmp_seq=15 ttl=64 time=0.965 ms
64 bytes from 192.168.0.32: icmp_seq=16 ttl=64 time=0.989 ms
```

Luego refrescamos la tabla de alertas en la sección Events de la web de Wazuh Manager (botón Refresh) para apreciar cómo se registran las nuevas alertas de Suricata:

Time	rule.description	rule.level	rule.id
> Feb 24, 2023 @ 13:41:48.816	¡ALERTA Suricata!: visitado un sitio prohibido	10	666661

> Feb 24, 2023 @ 13:41:34.758	Suricata: Alert - PING RECIBIDO	3	86601
-------------------------------	---------------------------------	---	-------

Como se observa, todas las alertas que genera el Suricata del Wazuh Agent son mostradas en Wazuh Manager con la descripción "Suricata: Alert - ". Además, todas aparecen con el mismo id (86601) y con el nivel de peligrosidad 3; con independencia del tipo de evento de Suricata que sea.

D) Vamos a precisar mejor el tipo de alertas que nos devuelve Suricata. Para ello crearemos 2 reglas nuevas de nivel 10 en Wazuh Manager que permitan distinguir si se ha producido una alerta de Suricata debido a que se ha visitado una web prohibida o que se ha recibido un ataque DoS. Para ello editaremos el archivo /var/ossec/etc/rules/local_rules.xml del equipo Wazuh Manager y añadiremos estas dos nuevas reglas en la sección existente:

> Feb 24, 2023 @ 13:41:34.758	Suricata: Alert - PING RECIBIDO	3	86601
> Feb 24, 2023 @ 13:41:34.758	Suricata: Alert - PING RECIBIDO	3	86601


```

<rule id="666661" level="10">
<if_sid>86601</if_sid>
<match>BLOQUEO WEB</match>
<description>¡ALERTA Suricata!: visitado un sitio prohibido</description>
</rule>
<rule id="666662" level="10" frequency="4" timeframe="4">
<if_matched_sid>86601</if_matched_sid>
<match>ATAQUE DOS ICMP FLOOD</match>
<description>!ALERTA Suricata!: ataque DoS - ICMP flood</description>
</rule>
</group>

```

Luego guardaremos los cambios y recargamos el servicio Wazuh Manager para que los aplique. Para comprobarlo, volveremos a generar el tráfico necesario para que ocurran los eventos que activen las reglas de Suricata y de Wazuh:

- Visitaremos algunas de las webs prohibidas desde el equipo Linux Wazuh Agent: `#curl -L www.as.com`
- Enviar pings constantes desde un equipo atacante hacia la IP del equipo Wazuh Agent: `#ping IPwazuhAgenteLinux` Luego refrescaremos la tabla de alertas de la web de Wazuh Manager para apreciar cómo se registran las alertas de las nuevas reglas (tardaremos un poco en ver los cambios -1 min-):

También es deseable desactivar las alertas generadas por el resto de eventos de Suricata (regla con id="86601") que no deseamos mostrar; así el SIEM no nos mostrará alertas repetidas de Suricata. Para ello editaremos el archivo `/var/ossec/ruleset/rules/0475-suricata_rules.xml` y modificaremos la regla con id 86601 de forma que no genere alertas cuando se cumpla (pese a su nivel).

```

<rule id="86601" level="0">
  <if_sid>86600</if_sid>
  <field name="event_type">^alert$</field>
  <description>Suricata: Alert - $(alert.signature)</description>
  <options>no_full_log</options>
</rule>

```

Le añadiremos la siguiente directiva `no_log` Otra alternativa sería configurar la directiva del archivo de Wazuh Manager `/var/ossec/etc/ossec.conf` con el nivel 5 para que no muestre las alertas de la regla 80601 (nivel 3):

Para comprobarlo, repetiremos la visita a los dominios prohibidos, así como los pings hacia el equipo Wazuh Agent Linux; y refrescamos la tabla de alertas del SIEM Wazuh Manager:

> Feb 24, 2023 @ 13:53:01.451 ¡ALERTA Suricata!: visitado un sitio prohibido	VICTORIA EUGENIA PÉREZ GONZÁLEZ	10	666661
--	---------------------------------	----	--------

> Feb 24, 2023 @ 13:41:34.758 Suricata: Alert - PING RECIBIDO	VICTORIA EUGENIA PÉREZ GONZÁLEZ	3	86601
> Feb 24, 2023 @ 13:41:34.758 Suricata: Alert - PING RECIBIDO	VICTORIA EUGENIA PÉREZ GONZÁLEZ	3	86601

Actividad 6: Incidente #4 – Detección de malware:

Vamos a probar las capacidades que ofrece el HIDS Wazuh Agent para detectar malware. En este caso únicamente deberemos configurar en Wazuh Agent la periodicidad con la que analizará los archivos del sistema en busca de software malicioso.

1.- Para ello editaremos el archivo de configuración del Agente Wazuh Linux `/var/ossec/etc/ossec.conf` y modificaremos la directiva de la sección por el valor 60 para que genere alertas por malware cada minuto.

```
<!-- Frequency that rootcheck is executed - every 12 hours -->
<frequency>60</frequency>
```

2.- Después guardaremos los cambios y los aplicaremos mediante:

```
#systemctl reload wazuh-agent
```

```
victoriaperez@agentelinuz:~$ systemctl reload wazuh-agent
```

3.- Para comprobar su funcionamiento, modificaremos uno de los programas del sistema Linux. En este caso modificaremos el contenido del comando "du" (muestra el espacio en disco).

Comenzaremos por guardar una copia del archivo: `#cp -p /usr/bin/du /usr/bin/du.copia`

```
victoriaperez@agentelinuz:~$ sudo cp -p /usr/bin/du /usr/bin/du.copia
[sudo] contraseña para victoriaperez:
victoriaperez@agentelinuz:~$
```

4.- Y luego modificaremos el archivo `/usr/bin/du` para inyectar código malicioso. Deberemos editarlo y pegarle en su interior el siguiente código:

```
!w0rm|/prof|file\.h!
```


Actividad 7: Incidente #5 – Incidente compuesto:

Muchos incidentes no pueden ser detectados con una única regla porque se han producido mediante una secuencia de acciones (eventos de seguridad). En estos casos es necesario definir varias reglas de alerta correlacionadas para poder recomponer e identificar correctamente el incidente. Estas reglas pueden estar asociadas a eventos del mismo tipo o de tipos diferentes (escaneos de puertos, intentos de intrusión, malware, modificación de archivos, DoS, sniffing...)

Vamos a poner en práctica los conocimientos sobre reglas aprendidos. En este caso deberemos configurar el SIEM Wazuh Manager para que detecte un incidente compuesto por varios eventos: Alertarnos (nivel 15) y notificarnos por email cuando un usuario que no sea el administrador del equipo Wazuh Agent Linux, logre iniciar sesión vía SSH tras intentarlo varias veces (al menos 5 en el último minuto); y una vez logueado nos haya borrado algún archivo del directorio /etc

1.- Comenzaremos por definir una regla que se active si en un periodo de tiempo previo se ha activado varias veces la regla con id 5716 ("sshd: authentication failed.", level=5). En este caso se trata de agregar varios eventos del mismo tipo.

```
<rule id="100001" level="15">
  <if_sid>5716</if_sid>
  <description>sshd: Múltiples fallos de autenticación ssh desde $(srcip).</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failures,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_11.4,pgp13_7.1,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_SI.4,tsc_CC6.1,tsc_CC6.2</group>
  <options>alert_by_email</options>
</rule>
```

2º.- Luego definiremos otra regla que se activará si se ha activado la regla anterior y además ha conseguido iniciar sesión con SSH (se ha cumplido la regla con id 5715, "sshd: authentication success.", level=3), no es el usuario administrador y la conexión proviene de la misma dirección IP de origen que en la regla anterior. En este caso se trata de correlacionar varios eventos de distinto tipo.

```
<rule id="100003" level="15" frequency="4" timeframe="4">
  <if_matched_sid>100001</if_matched_sid>
  <if_sid>5700</if_sid>
  <match>Accepted|authenticated.$</match>
  <description>sshd:Sesión iniciada por ssh desde $(srcip) después de varios intentos fallidos.</description>
  <mitre>
    <id>T1078</id>
    <id>T1021</id>
  </mitre>
  <group>authentication_success,pci_dss_10.2.5,pgp13_7.1,pgp13_7.2,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  <options>alert_by_email</options>
</rule>
```

3º.- Finalmente definiremos otra regla que se activará si se ha activado previamente la regla anterior y además el intruso (el usuario se debe llamar administrador) nos ha borrado (se ha

cumplido la regla FIM con el id 553) algún fichero del directorio /etc. En este caso se vuelve a correlacionar varios eventos de distinto tipo.

```
<rule id="100000" level="15">
  <if_matched_ssaid:100003:/if_matched_ssaid>
  <category:ossec/>
  <decoded_as:syscheck_deleted/>
  <description:Fichero borrado del directorio /etc $(syscheckpath).</description>
  <mitre>
    <id:T1107/>
    <id:T1485/>
  </mitre>
  <group>syscheck,syscheck_entry_deleted,syscheck_file,pcl_dss_11.5,gpg13_4.11,gdpr_11.5.1.f,hipaa_164.312.c.1,hipaa_164.312.c.2,nist_800_53_SI.7,tsc_P11.4,tsc_P11.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_
</rule>
```

Para notificar email se modifica ossec.conf.

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>yes</email_notification>
    <smtp_server>localhost</smtp_server>
    <email_from>dhmofxmy@eurokool.com</email_from>
    <email_to>dhmofxmy@eurokool.com</email_to>
    <email_maxperhour>60</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>9</email_alert_level>
  </alerts>
```

```
(kali@kali)-[~]
$ hydra -l victoriaperez -P passwords.lst -F ssh://192.168.0.32
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2023-02-26 04:26:31

[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://192.168.0.32:22/

1 of 1 target completed, 0 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2023-02-26 04:26:35

```
(kali@kali)-[~]
$ sudo nano passwords.lst
```

```
(kali@kali)-[~]
$ ssh victoriaperez@192.168.0.32
```

victoriaperez@192.168.0.32's password:

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.15.0-60-generic x86_64)

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

Se pueden aplicar 121 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: `apt list --upgradable`

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Feb 26 09:19:24 2023 from 192.168.0.29

victoriaperez@agentelinuz:~\$

```
(kali@kali)-[~]
$ ssh victoriaperez@192.168.0.32
victoriaperez@192.168.0.32's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.15.0-60-generic x86_64)
```

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

Se pueden aplicar 121 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: `apt list --upgradable`

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Feb 26 09:19:24 2023 from 192.168.0.29

victoriaperez@agentelinuz:~\$ cd /etc

victoriaperez@agentelinuz:/etc\$ ls

acpi	brltty	debian_version	geoclue	hp	libblockdev	modprobe.d	passwd	rc3.d	shells	ub
adduser.conf	brltty.conf	default	ghostscript	ifplugd	libnl-3	modules	passwd-	rc4.d	skel	uc
alsa	ca-certificates	deluser.conf	glvnd	init	libpaper.d	modules-load.d	pcmcia	rc5.d	smp	ue
alternatives	ca-certificates.conf	depmod.d	gnome	init.d	locale.alias	mtab	perl	rc6.d	speech-dispatcher	uf
anacrontab	ca-certificates.conf.dpkg-old	dhcpc	groff	initramfs-tools	locale.gen	mttools.conf	pki	rc5.d	ssh	uf
app	calendar	dictionaries-common	group	inputrc	localtime	mysql	pm	resolv.conf	ssl	up
apparmor	chatscripts	dpkg	group	insync.conf.d	logcheck	nanorc	pm2ppa.conf	ret	subgid	up
apparmor.d	console-setup	e2scrub.conf	grub.d	iproute2	login.defs	netplan	polkit-1	rpc	subuid	up
appstream	cracklib	emacs	gshadow	issue	logrotate.conf	network	popularity-contest.conf	rsyslog.conf	subuid	UP
apt	cron.d	environment	gshadow	issue.net	logrotate.d	networkd-dispatcher	ppp	rsyslog.d	subuid-	us
apt	cron.daily	environment.d	gss	kernel	lsh-release	NetworkManager	printcap	rygel.conf	sudors	vi
avahi	cron.hourly	ethertypes	gtk-2.0	kernel-img.conf	ltrace.conf	networks	profile	sane.d	sudors.d	va
bash.bashrc	cron.monthly	firefox	gtk-3.0	kerneloops.conf	machine-id	newt	profile.d	security	suricata	vt
bash_completion	crontab	fonts	hdparm.conf	ldap	magic	nsswitch.conf	protocols	selinux	sysctl.conf	va
bash_completion.d	cron.weekly	fstab	hosts.conf	ld.so.cache	magic.mime	openvpn	pulse	sensors3.conf	sysctl.d	wp
bindresvport.blacklist	cups	fwupd	hostid	ld.so.conf	mailcap	opt	python3	sensors.d	systemd	X1
bluetooth	cupsshelpers	gai.conf	hostname	ld.so.conf.d	mailcap.order	os-release	python3.8	services	terminfo	xa
brlapi.key	dconf	gamecode.ini	hosts	legal	manpath.config	PackageKit	rc0.d	signal	thermal.d	xa
victoriaperez@agentelinuz:/etc\$ sudo cp gai.conf g	debconf.conf	gdb	hosts.allow	libao.conf	mime.types	pam.conf	rc1.d	shadow	timezone	xa
[sudo] contraseña para victoriaperez:	brlapi.conf	gdm3	hosts.deny	libaudit.conf	mke2fs.conf	pam.d	rc2.d	shadow-	tmpfiles.d	zs
victoriaperez@agentelinuz:/etc\$ sudo rm -r g										
victoriaperez@agentelinuz:/etc\$										

>	Feb 26, 2023 @ 09:33:13.272	/etc/g	deleted	File deleted.	VICTORIA EUGENIA PÉREZ GONZÁLEZ	15	100008
>	Feb 26, 2023 @ 09:26:48.076	sshd:	Sesión iniciada por ssh desde 192.168.0.29 después de varios intentos fallidos.		VICTORIA EUGENIA PÉREZ GONZÁLEZ	15	100003
>	Feb 26, 2023 @ 09:26:34.038	sshd:	Múltiples fallos de autenticación ssh desde 192.168.0.29.		VICTORIA EUGENIA PÉREZ GONZÁLEZ	15	100001

Wazuh notification - (agentelinuz) any - Alert level 15

Des



Wazuh dhmfxfmy@eurokool.com

dhmfxfmy@eurokool.com;

VICTORIA EUGENIA PÉREZ GONZÁLEZ



Wazuh Notification.
2023 Feb 26 09:26:48

Received From: (agentelinuz) any->/var/log/auth.log
Rule: 100003 fired (level 15) -> "sshd:SesiC³n iniciada por ssh desde 192.168.0.29 despC³tes de varios intentos fallidos."
Src IP: 192.168.0.29
User: victoriaperez
Portion of the log(s):

Feb 26 09:26:47 agentelinuz sshd[13523]: Accepted password for victoriaperez from 192.168.0.29 port 54152 ssh2

--END OF NOTIFICATION

Wazuh notification - (agentelinuz) any - Alert level 15



Wazuh dhmfxfmy@eurokool.com

dhmfxfmy@eurokool.com;

VICTORIA EUGENIA PÉREZ GONZÁLEZ



Wazuh Notification.
2023 Feb 26 09:26:22

Received From: (agentelinuz) any->/var/log/auth.log
Rule: 100001 fired (level 15) -> "sshd: MC³r³tiples fallos de autenticaci³³n ssh desde 192.168.0.29."
Src IP: 192.168.0.29
User: victoriaperez
Portion of the log(s):

Feb 26 09:26:21 agentelinuz sshd[13513]: Failed password for victoriaperez from 192.168.0.29 port 54142 ssh2

--END OF NOTIFICATION



Wazuh dhmfxfmy@eurokool.com

dhmfxfmy@eurokool.com;

Wazuh Notification.
2023 Feb 26 09:33:13

Received From: (agentlinux) any->syscheck
Rule: 100008 fired (level 15) -> "File deleted."
Portion of the log(s):

File '/etc/g' deleted
Mode: scheduled

Attributes:

- Size: 1180
- Permissions: rw-r--r--
- Date: Sun Feb 26 09:32:06 2023
- Inode: 262325
- User: root (0)
- Group: root (0)
- MD5: 065ce63fdb093bc7d3717c04c4de94fd
- SHA1: 501641ebb023f288273cd4a51b685d579cbe0dd9
- SHA256: ad99ddef967988c25581a0c8558f58a12bd4936b49f1569261ad4135b9b9a1e3

--END OF NOTIFICATION

VICTORIA EUGENIA PÉREZ GONZÁLEZ

