**Actividad Wazuh Manager**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Configuración del SIEM Wazuh Manager**](#_g59i8ewd3ed3) **2**

[**2.1 Apartado A**](#_ykezcd8mw12i) **2**

[**2.2 Apartado B**](#_42edarmum4vo) **3**

[**3. Acceso no autorizado a Windows con RDP**](#_z49psmzaank0) **4**

[**3.1 Creación de la regla**](#_7c6rosaqnczk) **4**

[**3.2 Ataque exitoso con hydra**](#_268mgv9msml6) **4**

[**3.3 Comprobación**](#_n0164oogn0) **5**

[**4. Cambios no autorizados en archivos de Windows**](#_r250qqzceb9l) **5**

[**4.1 Apartado A**](#_e2zt5dqxieas) **5**

[**4.2 Comprobación**](#_gog4f7oeaytc) **6**

[**4.3 Apartado B**](#_yg6jxtfpsjc5) **7**

[**4.3.1 Creación de reglas**](#_u7l3cwngyci1) **7**

[**4.3.2 Comprobación**](#_r0oieehd4p8n) **8**

[**5. Acceso no autorizado a Linux con SSH**](#_us1hlnmrdxb) **9**

[**5.1 Apartado A**](#_u7iu7bs9n6c2) **9**

[**5.2 Apartado B**](#_didka21wt5ro) **10**

[**6. Monitorización de eventos con Suricata en Wazuh**](#_r71xixqj4jus) **11**

[**6.1 Apartado A**](#_9m5m4areofsw) **11**

[**6.2 Apartado B**](#_j35xtnxhq0mj) **13**

[**6.3 Apartado C**](#_9alduqf9erop) **13**

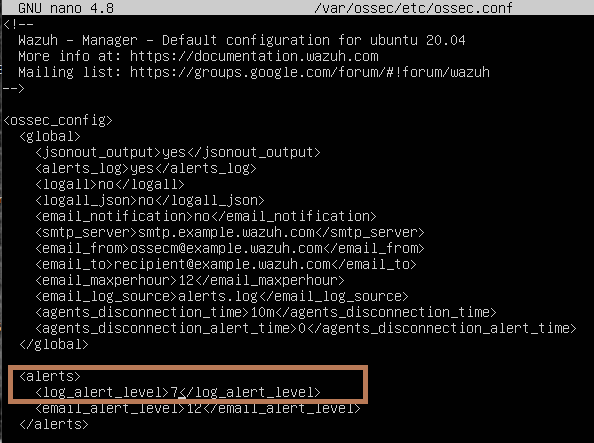
[**6.4 Apartado D**](#_k1rajg7w9ue5) **14**

[**7. Detección de Malware**](#_c68a76rkttfp) **15**

# **2. Configuración del SIEM Wazuh Manager**

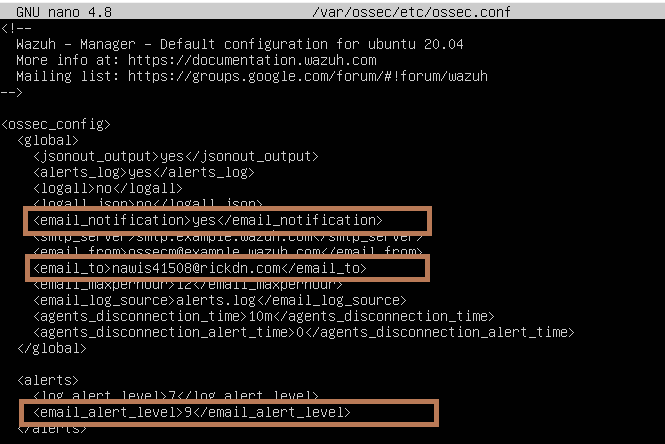
### **2.1 Apartado A**

Nos dirigimos al archivo de configuración de Wazuh Manager y modificamos la línea “log\_alert\_level” con su nuevo valor.

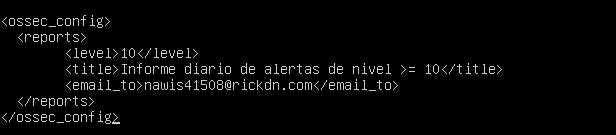


### **2.2 Apartado B**

Esta vez modificaremos las siguientes líneas: “email\_notification”, “email\_to” y “email\_alert\_level” con sus respectivos valores.



También es posible la configuración de un envío de informe a través de correo electrónico, añadiendo lo siguiente a la configuración:



# **3. Acceso no autorizado a Windows con RDP**

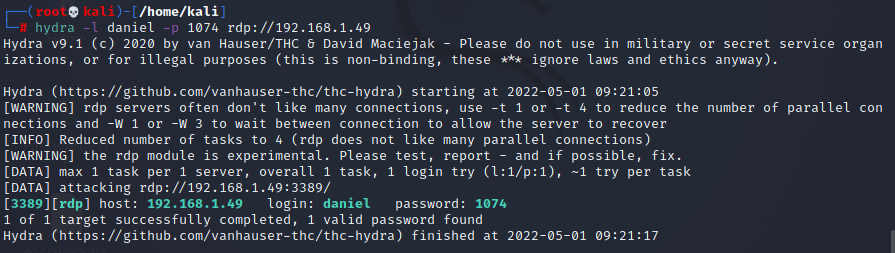
### **3.1 Creación de la regla**

Integramos la nueva regla en el fichero correspondiente para asignar reglas.

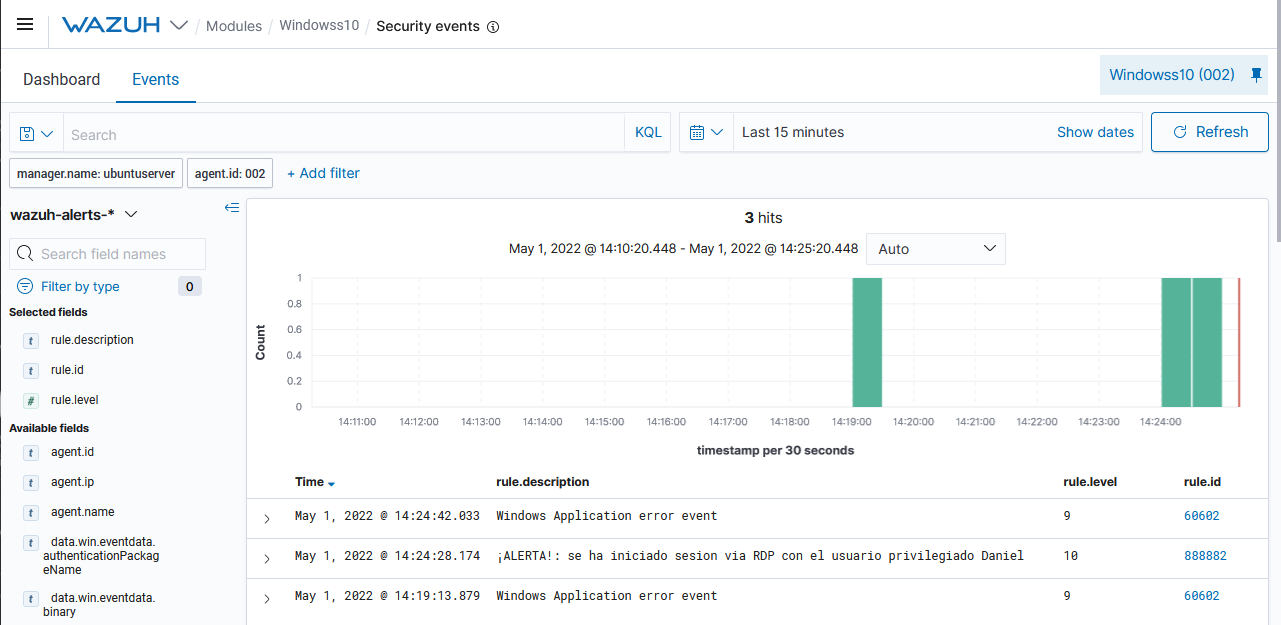


### **3.2 Ataque exitoso con hydra**

Realizaremos un ataque con la herramienta hydra para la comprobación.



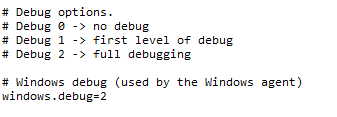
### **3.3 Comprobación**

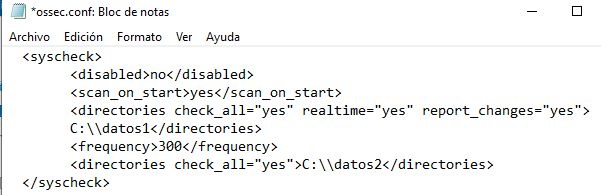


# **4. Cambios no autorizados en archivos de Windows**

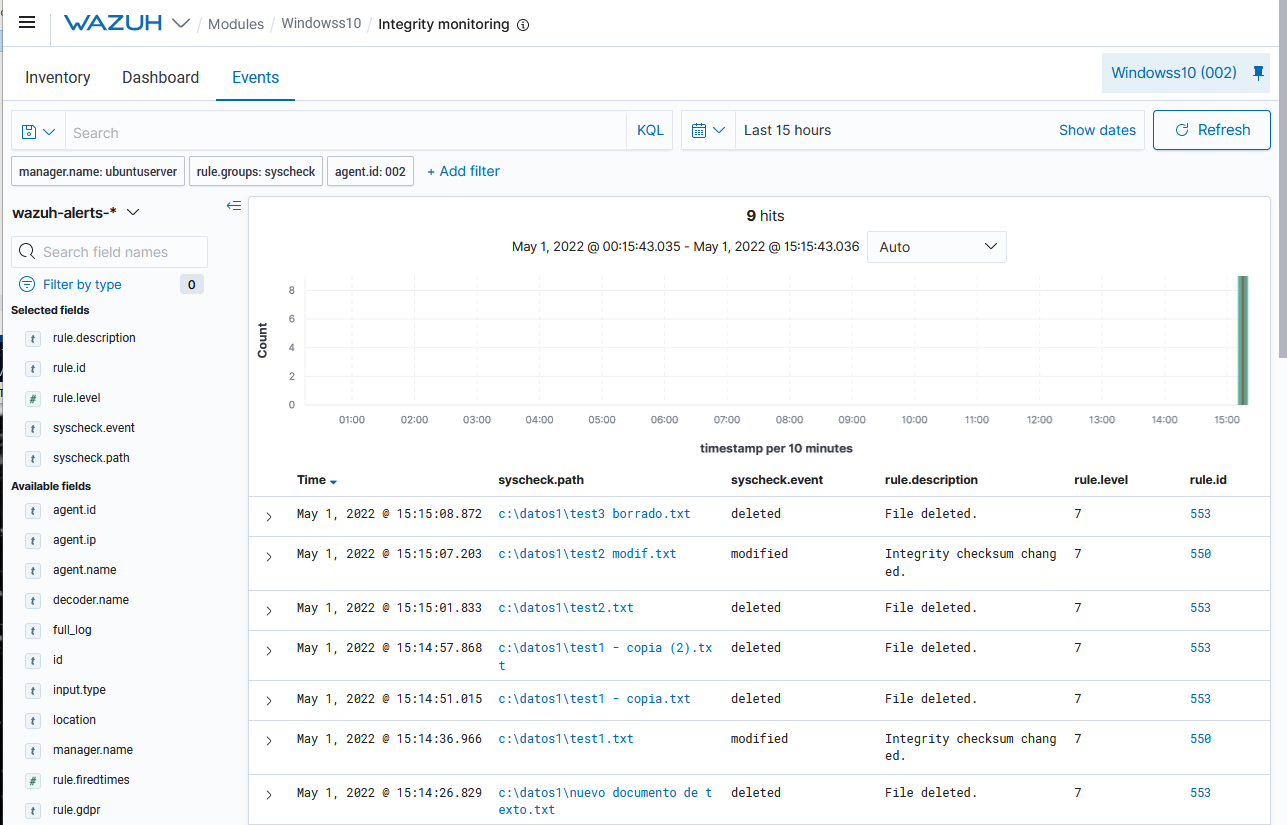
### **4.1 Apartado A**

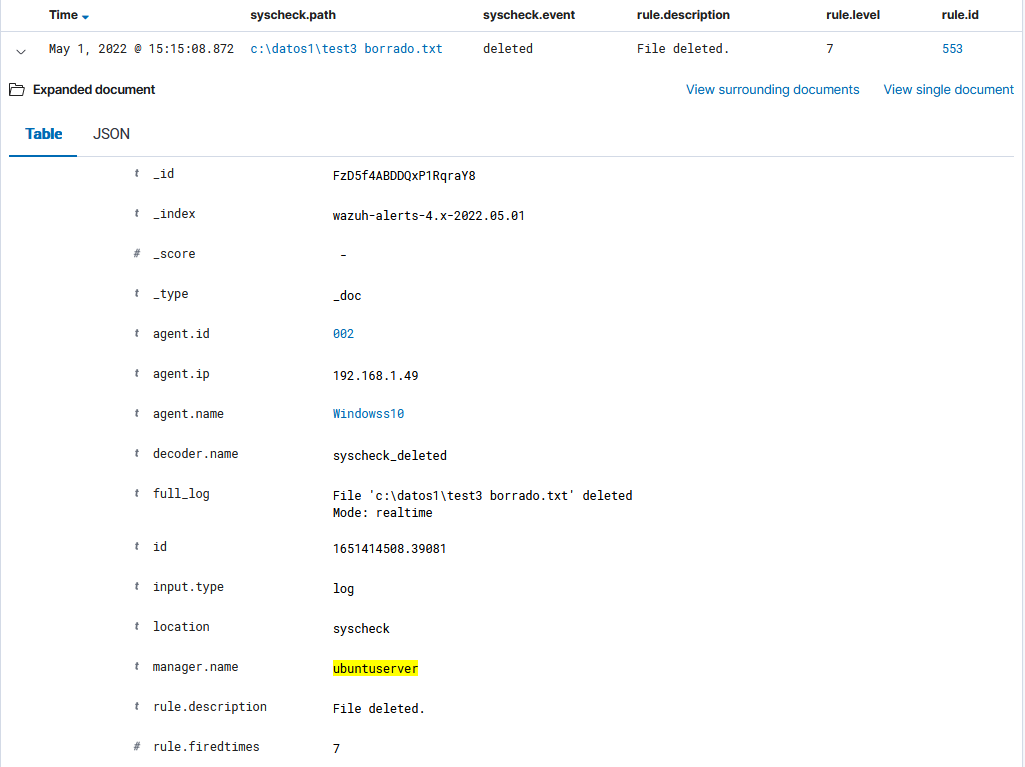
En el archivo C:\Program Files (x86)\ossec-agent\internal\_options.conf modificamos los siguientes valores: windows.debug=2, rootcheck.sleep=0 y syscheck.sleep=0





### **4.2 Comprobación**



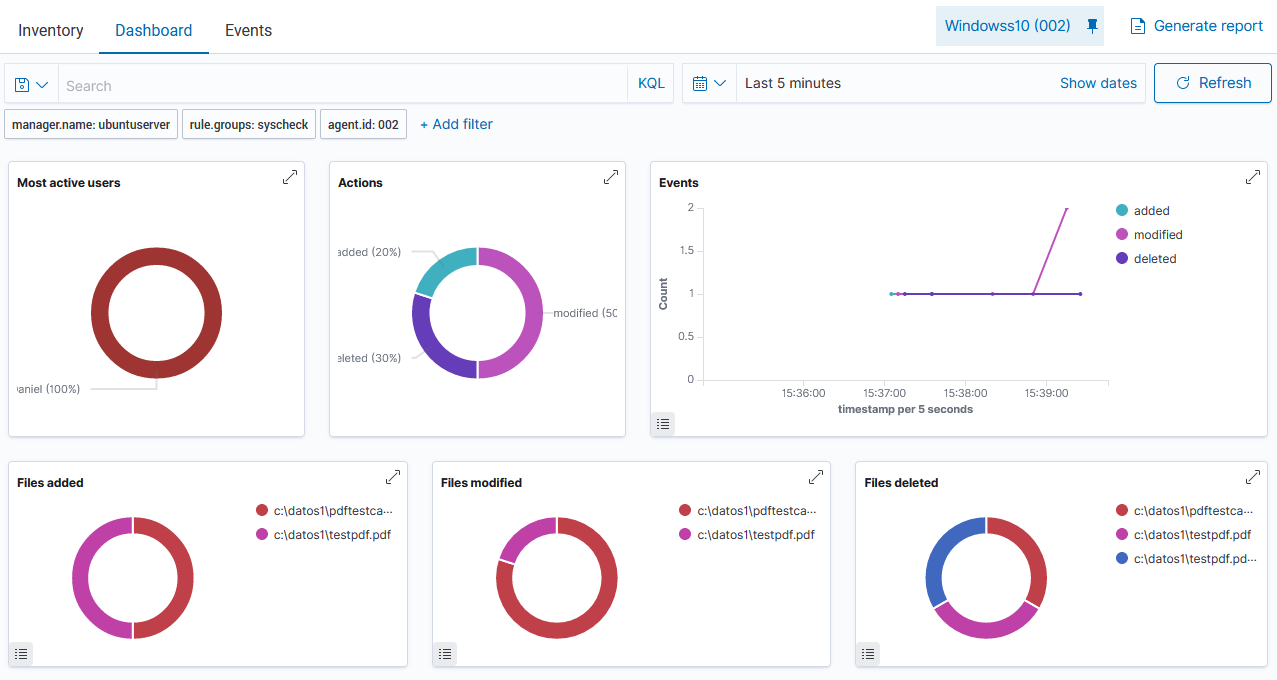


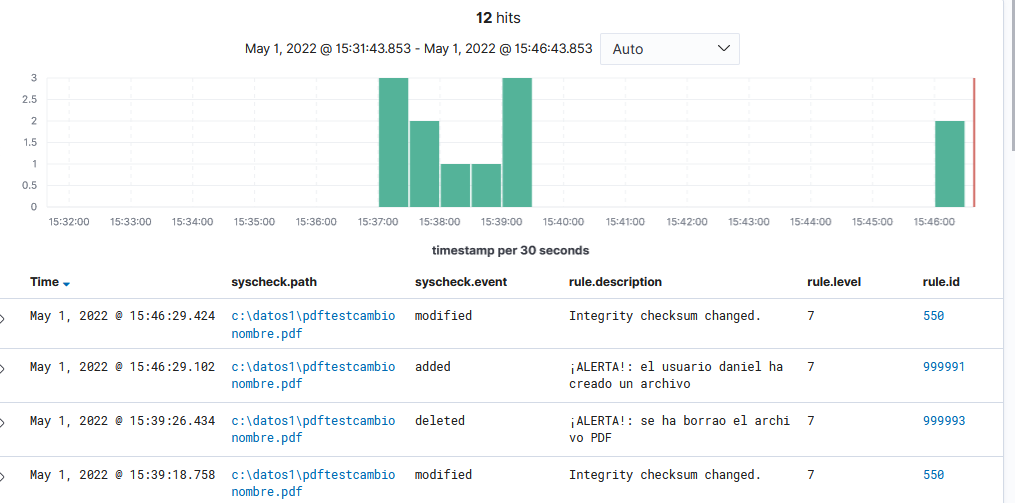
### **4.3 Apartado B**

#### **4.3.1 Creación de reglas**



#### **4.3.2 Comprobación**

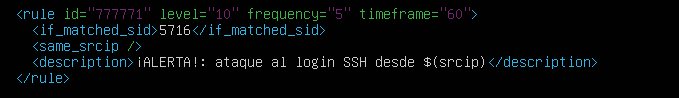


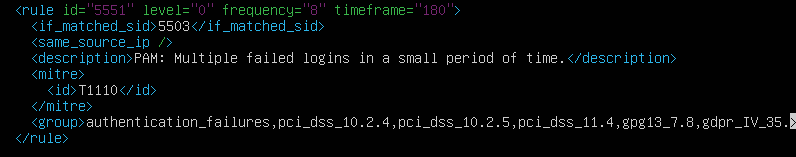


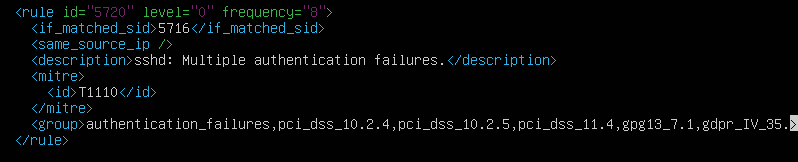
# **5. Acceso no autorizado a Linux con SSH**

### **5.1 Apartado A**

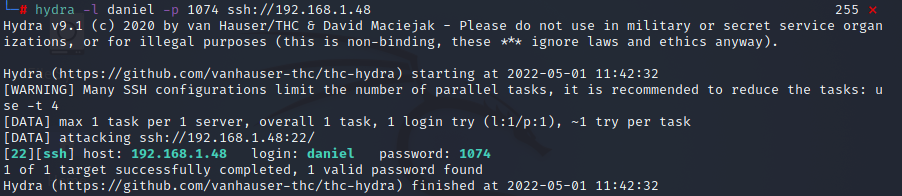
Creamos las nuevas reglas:

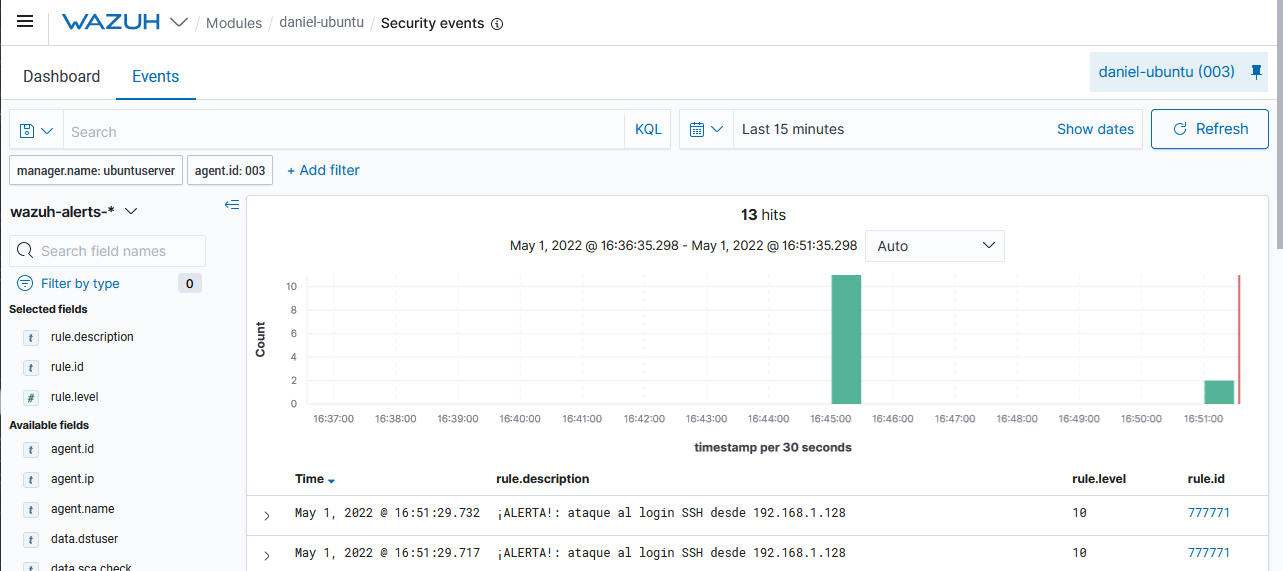






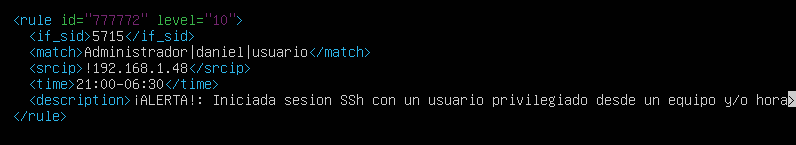
Lanzamos un ataque exitoso con hydra y comprobamos.



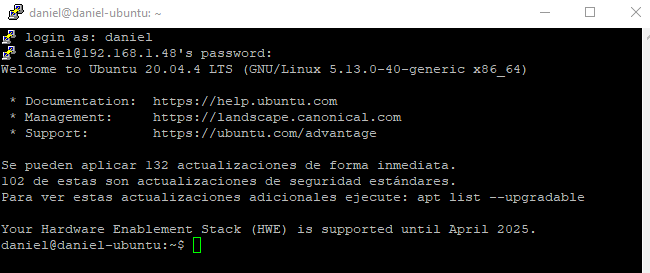


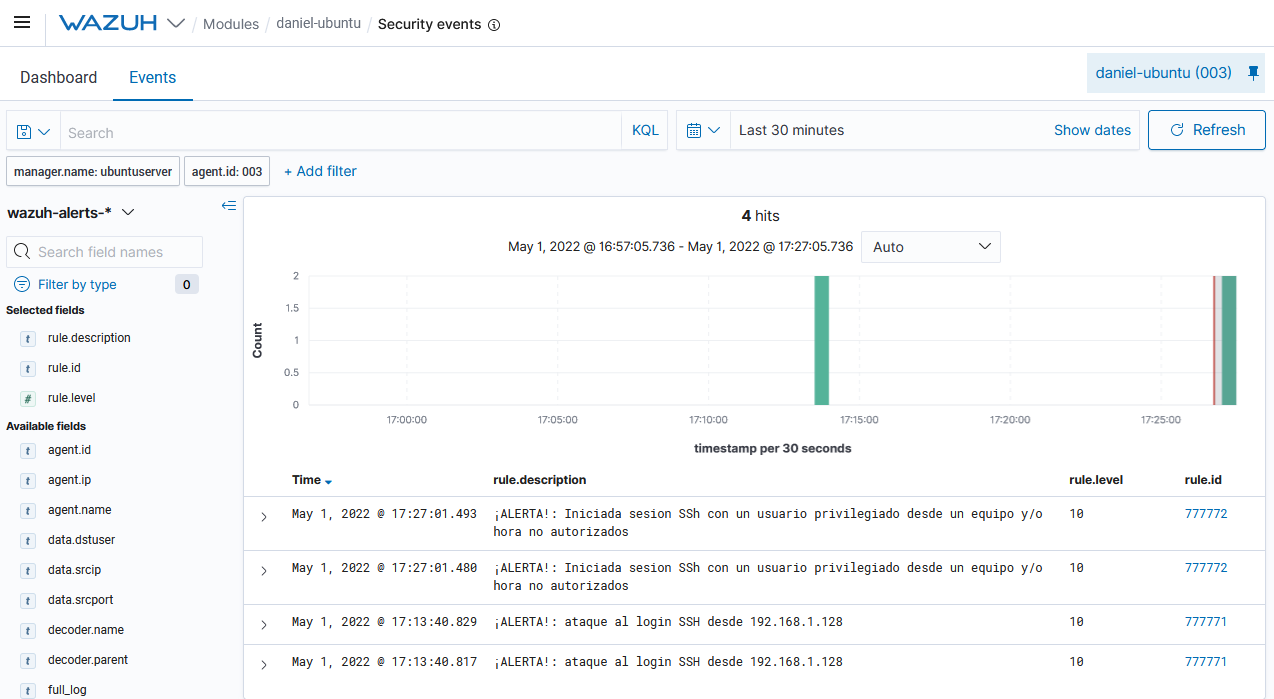
### **5.2 Apartado B**

Nuevamente creamos la regla en el archivo



Realizamos la conexión por SSH a través del software PuTTy y comprobamos.

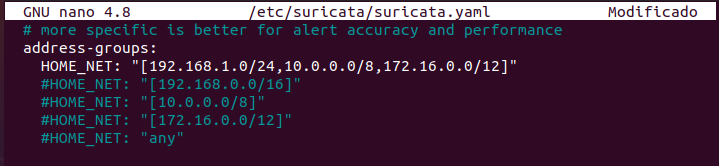


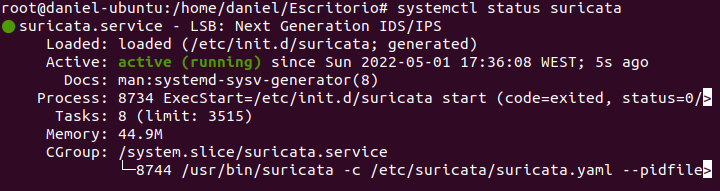


# **6. Monitorización de eventos con Suricata en Wazuh**

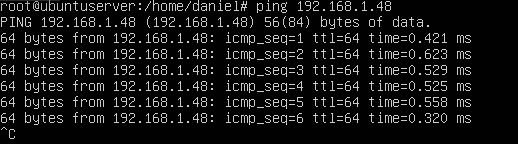
### **6.1 Apartado A**

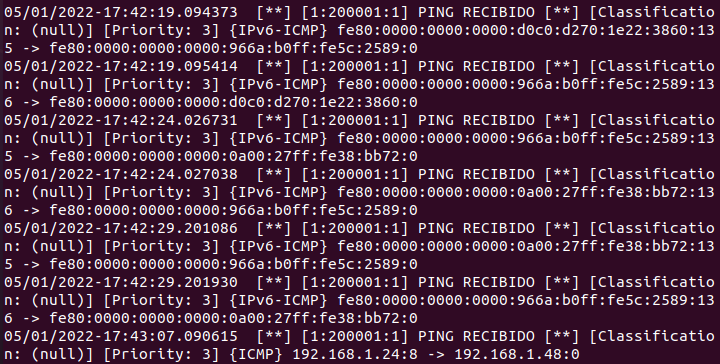
Descargamos, instalamos y configuramos suricata de modo que nos alerte cuando reciba un ping.





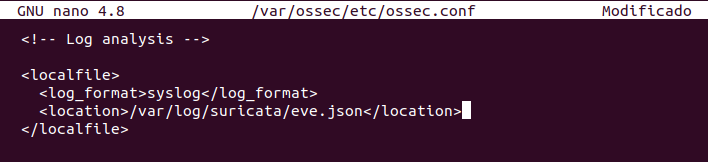


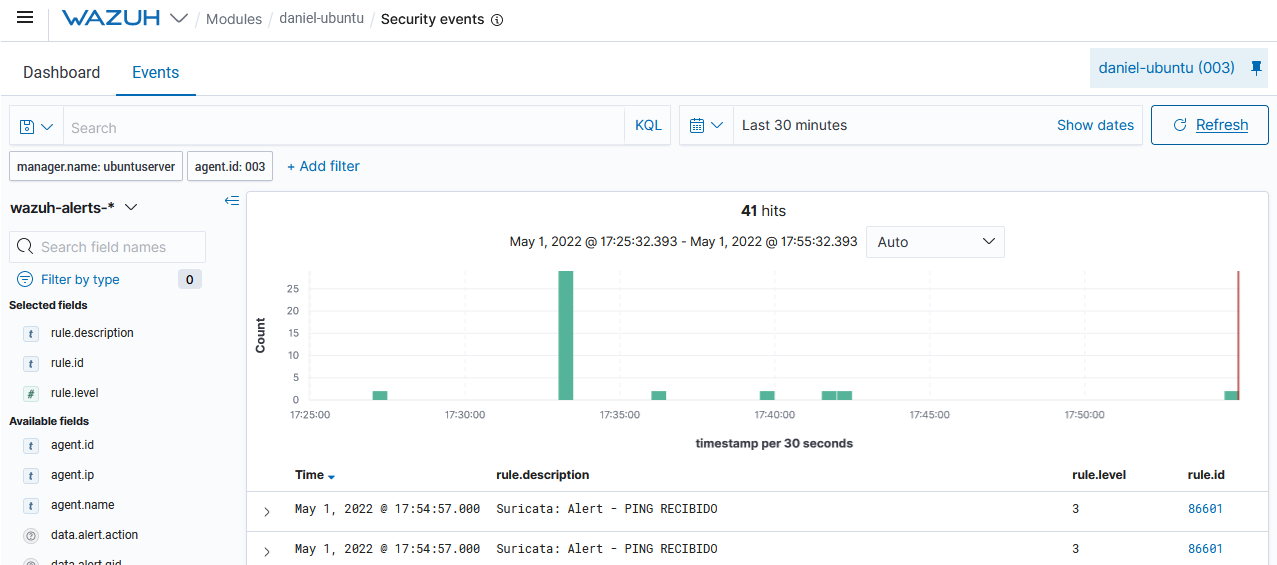




### **6.2 Apartado B**

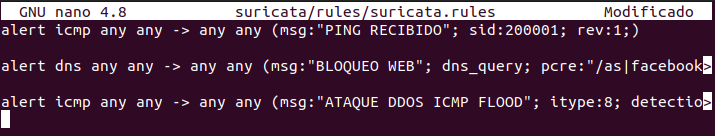
Configuramos el ingesta de datos a través del log, una vez realizado esto, comprobamos.

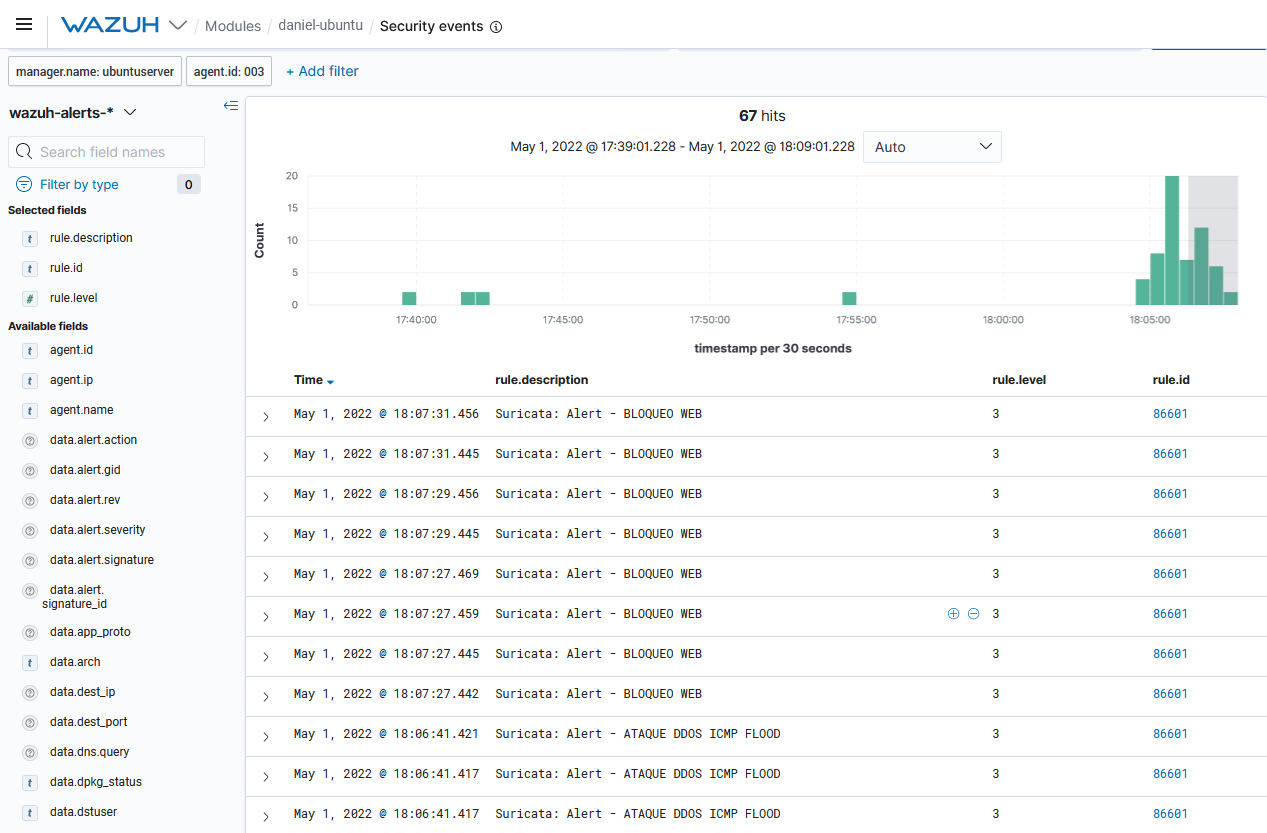




### **6.3 Apartado C**

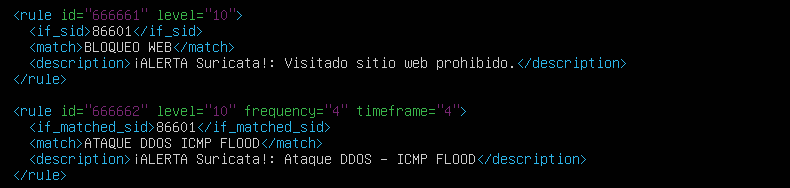
Crearemos dos nuevas alertas en suricata y comprobamos su funcionamiento.

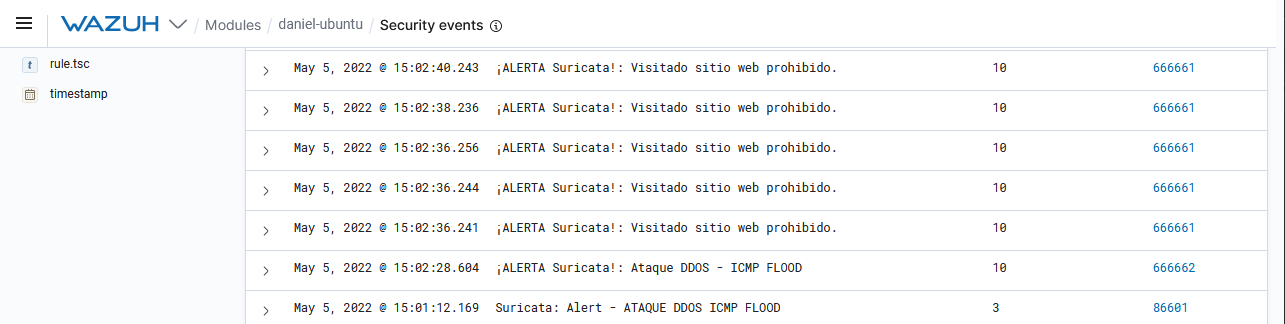




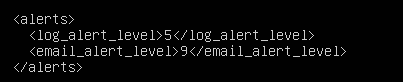
### **6.4 Apartado D**

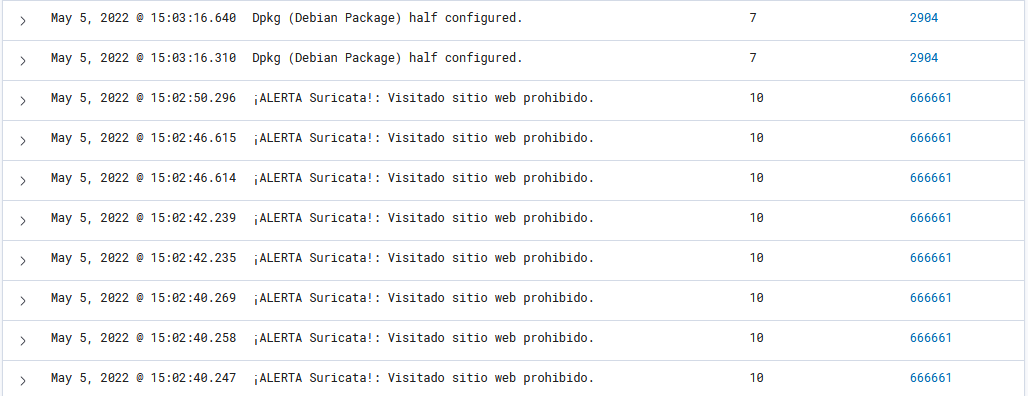
Ahora, crearemos unas reglas desde Wazuh-Manager para que registre cuando recibimos una alerta a través de suricata y comprobamos.





Modificamos el valor de la directiva log\_alert\_level para que no aparezcan las alertas generadas de forma automática por suricata, ya que son de nivel 3.





# **7. Detección de Malware**

Accedemos al archivo de configuracion de Wazuh-Manager y modificamos el valor del atributo frequency a 60.

### 

Añadimos el código malicioso en un comando, en este caso “du”, reiniciamos el agente y comprobamos.



