

# Monitoreo de actividad con usuarios en agentes

El primer objetivo a cumplir es el de realizar un registro de logs en el sistema para los agentes monitoreados. Para esto utilizando la maquina virtual de prueba nos dirigimos al archivo de configuración.

```
nano /etc/rsyslog.conf
```

Agregamos al archivo:

```
auth,authpriv.* /var/log/auth.log  
systemctl restart rsyslog.service
```

Es recomendable quitar el comentario a la linea LogLevel para una información mas precisa.

```
# Logging  
#SyslogFacility AUTH  
LogLevel INFO
```

El archivo “**/var/log/auth.log**” tendrá los registros con lo que probaremos los distintos tipos de eventos que pueden darse.

Ejemplo "useradd"

Recuperamos la salida en auth.log y así tendremos ejemplos de logs para poder ser analizados por wazuh manager:

Para agregar usuario

```
Sep  5 11:27:26 xubuntu-VM useradd[205364]: new user: name=ejemplo, UID=1001, GID=1001,  
home=/home/ejemplo, shell=/bin/sh, from=/dev/pts/1
```

Introducimos el log generado en nuestro terminal en la herramienta **Ruleset test** de Wazuh manager para comprobar si es que existen reglas asociadas a este tipo de eventos.

## Ruleset Test

```
Sep  5 11:27:26 xubuntu-VM useradd[205364]: new user: name=ejemplo, UID=1001, GID=1001, home=/home/ejemplo, shell=/bin/sh, from=/dev/pts/1
```

```
**Phase 1: Completed pre-decoding.  
  full event: 'Sep  5 11:27:26 xubuntu-VM useradd[205364]: new user: name=ejemplo, UID=1001, GID=1001, home=/home/ejemplo, shell=/bin/sh, from=/dev/pts/1'  
  timestamp: 'Sep  5 11:27:26'  
  hostname: 'xubuntu-VM'  
  program_name: 'useradd'  
  
**Phase 2: Completed decoding.  
  name: 'useradd'  
  parent: 'useradd'  
  dstuser: 'ejemplo'  
  gid: '1001'  
  home: '/home/ejemplo'  
  shell: '/bin/sh,'  
  uid: '1001'  
  
**Phase 3: Completed filtering (rules).  
  id: '5902'  
  level: '8'  
  description: 'New user added to the system.'  
  groups: '["syslog","adduser"]'  
  firetimes: '1'  
  gdpr: '["IV_35.7.d","IV_32.2"]'  
  gpg13: '["4.13"]'  
  hipaa: '["164.312.b","164.312.a.2.I","164.312.a.2.II"]'  
  mail: 'false'  
  mitre.id: '["T1136"]'  
  mitre.tactic: '["Persistence"]'
```

En este caso observamos que tienen reglas asociadas a este tipo de eventos y la extracción de este tipo de datos que se pueden observar como el nombre de la acción **useradd** y datos como el nombre del usuario creado así como los identificadores de usuario o grupo y la interfaz de línea de comandos que en este caso es /bin/sh.

Para probar los logs registramos 3 eventos con un nombre cualquiera.

```
useradd cuatro  
usermod -aG cuatro  
userdel cuatro
```

Revisamos los logs del archivo en /var/log/auth.log

```
Sep  6 09:55:29 xubuntu-VM useradd[220043]: new user: name=cuatro, UID=1001, GID=1001,  
home=/home/cuatro, shell=/bin/sh, from=/dev/pts/3  
Sep  6 09:55:56 xubuntu-VM usermod[220054]: add 'cuatro' to shadow group 'sudo'  
Sep  6 09:56:00 xubuntu-VM userdel[220061]: delete user 'cuatro'
```

Para lo cual se generan las alertas de usuario agregado y usuario eliminado por defecto en wazuh manager.

En el caso del comando useradd tenemos:

✓	Sep 6, 2023 @ 09:55:30.310	T1136	Persistence	New user added to the system.	8	5902
Table	JSON	Rule				
@timestamp		2023-09-06T13:55:30.310Z				
._id		bpfGao0Btfq4GhwC2aj7				
agent.id		010				
agent.ip		192.168.24.73				
agent.name		xubuntu-VM				
data.dstuser		cuatro				
data.gid		1001				
data.home		/home/cuatro				
data.shell		/bin/sh,				
data.uid		1001				
decoder.name		useradd				
decoder.parent		useradd				
full_log		Sep 6 09:55:29 xubuntu-VM useradd[220043]: new user: name=cuatro, UID=1001, GID=1001, home=/home/cuatro, shell=/bin/sh, from=/dev/pts/3				
id		1694008530.55010				
input.type		log				
location		/var/log/auth.log				
manager.name		ubuntu				
predecoder.hostname		xubuntu-VM				
predecoder.program_name		useradd				
predecoder.timestamp		Sep 6 09:55:29				
rule.description		New user added to the system.				

En el caso del comando userdel tenemos:

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
✓ Sep 6, 2023 @ 09:56:02.350	T1531	Impact	Group (or user) deleted from the system.	3	5903
Table	JSON	Rule			
@timestamp		2023-09-06T13:56:02.350Z			
._id		cJfHao0Btfq4GhwCYq1			
agent.id		010			
agent.ip		192.168.24.73			
agent.name		xubuntu-VM			
data.srcuser		cuatro			
decoder.name		open-userdel			
full_log		Sep 6 09:56:00 xubuntu-VM userdel[220081]: delete user 'cuatro'			
id		1694008562.56087			
input.type		log			
location		/var/log/auth.log			
manager.name		ubuntu			
predecoder.hostname		xubuntu-VM			
predecoder.program_name		userdel			
predecoder.timestamp		Sep 6 09:56:00			
rule.description		Group (or user) deleted from the system.			
rule.firedtimes		2			
rule.gdpr		IV_35.7.d, IV_32.2			
rule.gpg13		4.13			
rule.groups		syslog, adduser			

Debido a que no se tiene una alerta para el evento de asignación de privilegios al usuario tenemos que crear la regla personalizada analizando el log generado en **/var/log/auth.log** y crear el decodificador para dicho evento específico.

Log: Sep 5 19:47:44 ubuntu usermod[19978]: add 'prueba' to shadow group 'sudo'

El decodificador queda de la siguiente manera:

```

114 <decoder name="usermod">
115   <program_name>usermod</program_name>
116 </decoder>
117
118 <decoder name="usermod-p">
119   <parent>usermod</parent>
120   <prematch>add</prematch>
121   <regex offset="after_prematch">^ '(\S+)' to shadow group '(\S+)'</regex>
122   <order>user,group</order>
123 </decoder>

```

Realizamos la prueba en Decoders Test para verificar que se reconocen los parámetros.

```

**Messages:
  WARNING: (7003): '76cd293f' token expires
  INFO: (7202): Session initialized with token 'f862de17'

**Phase 1: Completed pre-decoding.
  full event: 'Sep  5 19:47:44 ubuntu usermod[19978]: add 'prueba' to shadow group 'sudo''
  timestamp: 'Sep  5 19:47:44'
  hostname: 'ubuntu'
  program_name: 'usermod'

**Phase 2: Completed decoding.
  name: 'usermod'
  parent: 'usermod'
  dstuser: 'prueba'
  group: 'sudo'

```

Observamos que se pueden extraer los datos de nombre de usuario y grupo al que fue asignado por lo cual se realizara la regla personalizada para este evento.

```

277                                     <!-- PRIVILEGIOS DE USUARIO -->
278
279 <group name="usermod-privilegios,">
280 <rule id="100060" level="10">
281   <decoded_as>usermod</decoded_as>
282   <match>to shadow group</match>
283   <description>Evento sospechoso: un usuario ha sido añadido al grupo sudo</description>
284   <group>usermod,sudo</group>
285 </rule>
286 </group>

```

Una vez realizada esta regla probamos el log con **Ruleset Test** de Wazuh para ver si se genera de manera correcta.

```

**Messages:
  INFO: (7202): Session initialized with token 'dfe09325'

**Phase 1: Completed pre-decoding.
  full event: 'Sep  5 19:47:44 ubuntu usermod[19978]: add 'prueba' to shadow group 'sudo''
  timestamp: 'Sep  5 19:47:44'
  hostname: 'ubuntu'
  program_name: 'usermod'

**Phase 2: Completed decoding.
  name: 'usermod'
  parent: 'usermod'
  dstuser: 'prueba'
  group: 'sudo'

**Phase 3: Completed filtering (rules).
  id: '100060'
  level: '9'
  description: 'Usuario añadido al grupo sudo'
  groups: '["usermod-privilegios","usermod","sudo"]'
  firetimes: '1'
  mail: 'false'

**Alert to be generated.

```

Realizadas las pruebas utilizaremos la maquina virtual para proceder con la generación de alertas de niveles 8 y 10 respectivamente:

Usuario creado:

▼	Sep 6, 2023 @ 11:13:15.488	T1136	Persistence	New user added to the system.	8	5902
Table	JSON	Rule				
@timestamp		2023-09-06T15:13:15.488Z				
_id		JZcOa4o8ttq4GhwCIKmS				
agent.id		010				
agent.ip		192.168.24.73				
agent.name		xubuntu-VM				
data.dstuser		diez				
data.gid		1001				
data.home		/home/diez				
data.shell		/bin/sh				
data.uid		1001				
decoder.name		useradd				
decoder.parent		useradd				
full_log		Sep  6 11:13:14 xubuntu-VM useradd[220781]: new user: name=diez, UID=1001, GID=1001, home=/home/diez, shell=/bin/sh, from=/dev/pts/1				
id		1694013195.82264				
input.type		log				
location		/var/log/auth.log				
manager.name		ubuntu				
predecoder.hostname		xubuntu-VM				
predecoder.program_name		useradd				
predecoder.timestamp		Sep  6 11:13:14				
rule.description		New user added to the system.				

Escala de privilegios:

Sep 6, 2023 @ 11:13:45.523		Evento sospechoso: un usuario ha sido añadido al grupo sudo	10	100060
Table	JSON	Rule		
@timestamp		2023-09-06T15:13:45.523Z		
_id		JpcOa4oBttq4GhwCgdk6		
agent.id		010		
agent.ip		192.168.24.73		
agent.name		xubuntu-VM		
data.dstuser		diez		
data.group		sudo		
decoder.name		usermod		
decoder.parent		usermod		
full_log		Sep 6 11:13:44 xubuntu-VM usermod[220792]: add 'diez' to shadow group 'sudo'		
id		1694013225.82859		
input.type		log		
location		/var/log/auth.log		
manager.name		ubuntu		
predecoder.hostname		xubuntu-VM		
predecoder.program_name		usermod		
predecoder.timestamp		Sep 6 11:13:44		
rule.description		Evento sospechoso: un usuario ha sido añadido al grupo sudo		
rule.firedtimes		1		
rule.groups		usermod-privilegios, usermod, sudo		
rule.id		100060		

Eliminación de usuario:

Time ↓		Technique(s)	Tactic(s)	Description	Level	Rule ID
Sep 6, 2023 @ 11:13:53.501		<a href="#">T1531</a>	Impact	Group (or user) deleted from the system.	3	<a href="#">5903</a>
Table	JSON	Rule				
@timestamp		2023-09-06T15:13:53.501Z				
_id		KZcOa4oBttq4GhwCvKnS				
agent.id		010				
agent.ip		192.168.24.73				
agent.name		xubuntu-VM				
data.srcuser		diez				
decoder.name		open-userdel				
full_log		Sep 6 11:13:52 xubuntu-VM userdel[220799]: delete user 'diez'				
id		1694013233.83953				
input.type		log				
location		/var/log/auth.log				
manager.name		ubuntu				
predecoder.hostname		xubuntu-VM				
predecoder.program_name		userdel				
predecoder.timestamp		Sep 6 11:13:52				
rule.description		Group (or user) deleted from the system.				
rule.firedtimes		4				
rule.gdpr		IV_35.7.d, IV_32.2				
rule.gpg13		4.13				
rule.groups		syslog, adduser				

En el agente de Wazuh agregamos este bloque en el archivo de configuración para monitorizar el archivo sudoers.

```
❗ Para verificar que el archivo sudoers no fue modificado ➡  
<directories check_all="yes" report_changes="yes" realtime="yes">/etc/sudoers</directories>
```

Esto realizará un monitoreo en tiempo real del archivo para enviar una alerta de modificaciones. Con distintos escenarios podemos incrementar la cantidad de reglas a partir de diferentes eventos como mostraremos a continuación:

```

246 * <group name="usermod-privilegios,">
247
248 * <rule id="100060" level="10">
249     <decoded_as>usermod</decoded_as>
250     <match>sudo|admin</match>
251     <description>Evento sospechoso: un usuario ha sido añadido a un grupo con privilegios</description>
252     <group>usermod,sudo</group>
253 </rule>
254 * <rule id="100061" level="8">
255     <decoded_as>usermod</decoded_as>
256     <match>to shadow group</match>
257     <description>Evento sospechoso: un usuario nuevo ha sido añadido a un grupo</description>
258     <group>usermod,sudo</group>
259 </rule>
260
261 * <rule id="100062" level="12">
262     <if_sid>550</if_sid>
263     <match>/etc/sudoers</match>
264     <description>Evento critico: el archivo de configuracion sudoers ha sido modificado</description>
265     <group>usermod,sudo,syscheck</group>
266 </rule>
267
268 * <rule id="100063" level="13">
269     <if_sid>5903</if_sid>
270     <match>'root'</match>
271     <description>Evento critico: el usuario root ha sido eliminado</description>
272     <group>usermod,sudo,syscheck</group>
273 </rule>
274
275 </group>

```

Las reglas se modificaron de la siguiente manera:

- 100060 Se realizó la regla para activarse en caso de que un usuario se añada ya sea al grupo sudo o al grupo admin que poseen privilegios de ejecución.
- 100061 Esta regla actúa de manera similar a la anterior sin embargo es de menor nivel por que indica que un usuario nuevo se añade a un grupo existente no necesariamente con privilegios.
- 100062 Se creó en base a la regla generada de integridad de archivos. Si se ejecuta un cambio en los directorios monitoreados en tiempo real y además es coincidente con “/etc/sudoers” esta alerta se activara con nivel crítico.
- 100063 Se creó en base a la regla 5903 cuando se elimina un usuario. Si se detecta la eliminación y además es coincidente con “root” se genera una alerta de nivel crítico.





---

Revision #5

Created 8 abril 2024 18:18:10 by Ricardo Alberto

Updated 10 abril 2024 12:16:47 by Ricardo Alberto