LABWAZUH 2 – Fuerza Bruta (failed logins)

1. Objetivo. – Realizar repetidos intentos con credenciales incorrectas para generar alertas de autenticaciones fallidas, y lograr visualizarlas en Wazuh.

2. Alcance.- Este laboratorio enfoca la detección y el monitoreo de eventos de autenticación, las acciones reales de contención o mitigación no forman parte del alcance del laboratorio.

3. Herramientas. - Para este laboratorio se utilizarán:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)
- Wazuh
- Agente Windows Wazuh

4. Procedimiento

1. Desde el agente Wazuh Windows, se ejecuta un comando en PowerShell que simula el ingreso de credenciales erróneas en 10 intentos, con el nombre de usuario Papitas y su contraseña mayonesa, ademas utilizando la IP de nuestro agente. (ver Figura 1)

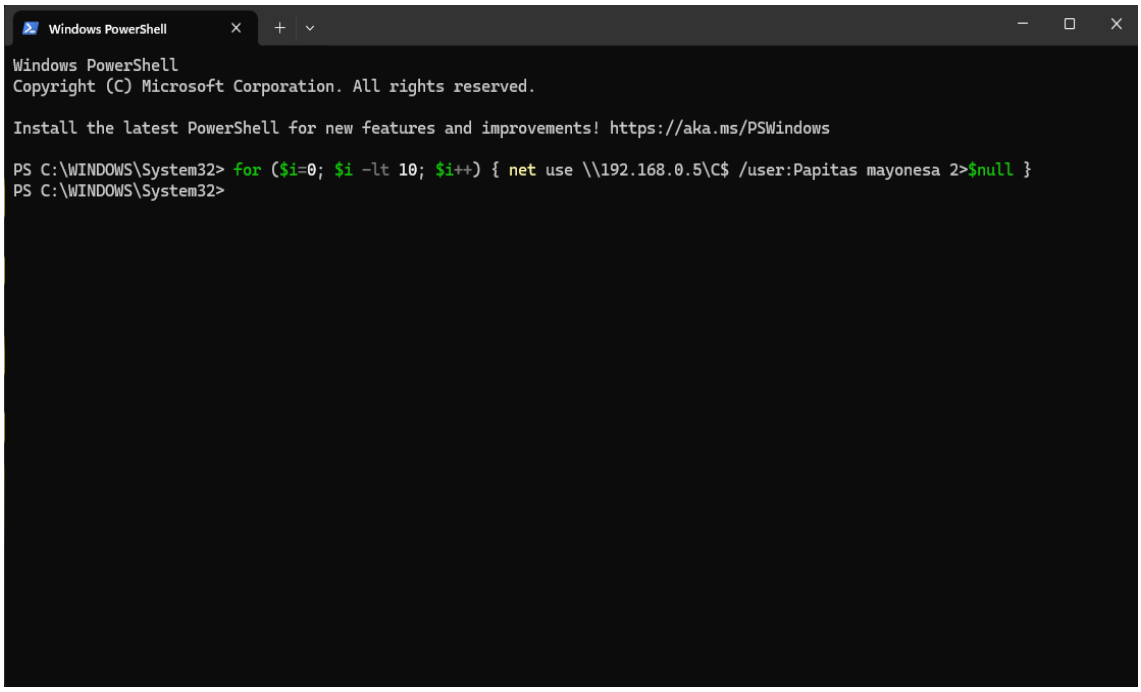

Figura 1. Simulación de intentos fallidos en el agente Windows

2. En el servidor Wazuh de Linux, en la pestaña Threat Hunting→ Events, se logra visualizar las diferentes autenticaciones fallidas que se hizo desde nuestro agente Windows. (ver Figura 2)

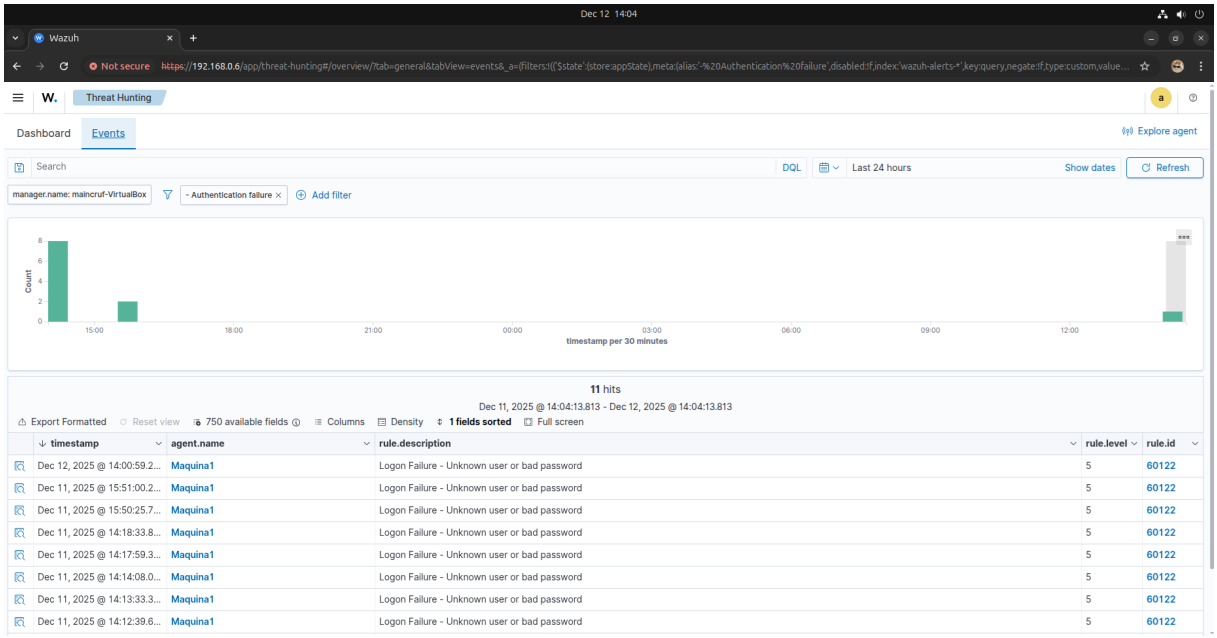

Figura 2. Eventos de autenticaciones fallidas.

3. Al entrar en los detalles de los eventos de las autenticaciones fallidas, se muestra específicamente la IP de nuestro agente Windows y el nombre de usuario que se usó. (ver Figura 3)

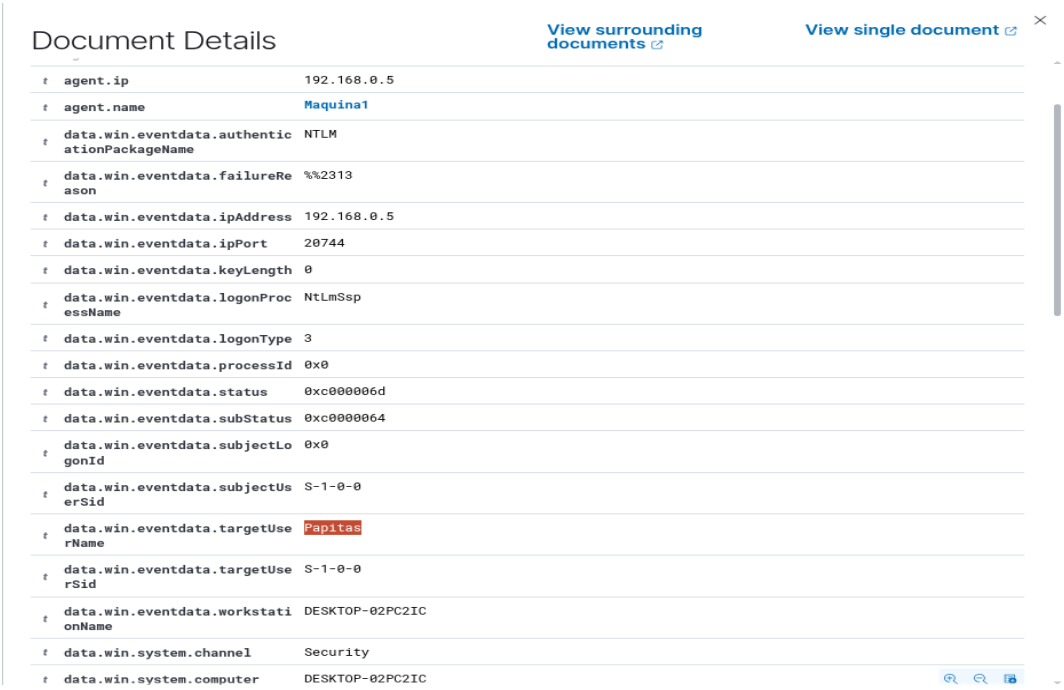

Figura 3. Información completa de la autenticación fallida.

5. Acciones Recomendadas. - Ante la detección de múltiples intentos de autenticación fallida, se recomienda aplicar las siguientes medidas:

- Analizar la recurrencia de los intentos fallidos y su origen, para evitar falsos positivos.
- Evaluar el bloqueo temporal de la dirección IP de origen.
- Considerar deshabilitar temporalmente la cuenta afectada.
- Mantener un monitoreo continuo de eventos similares

6. Resultados Obtenidos. - Durante el laboratorio se logro satisfactoriamente simular un ataque de fuerza bruta desde el agente Windows, generando eventos de autenticación fallida, y poder visualizarlos en el dashboard de Wazuh, permitiendo su análisis.

7. Reflexión final. – Este laboratorio permitió observar de forma clara y detallada ataques que suceden en la vida real y como lograr visualizarlos en un SIEM, mostrando la importancia de este en el campo de la ciberseguridad, permitiendo que se logre una detección temprana de eventos sospechosos, y que, sin un buen monitoreo estos ataques pasarían desapercibidos.