

Detección y análisis de ataques de fuerza bruta en Wazuh

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

2. Herramientas. - Para este laboratorio se utilizaron:

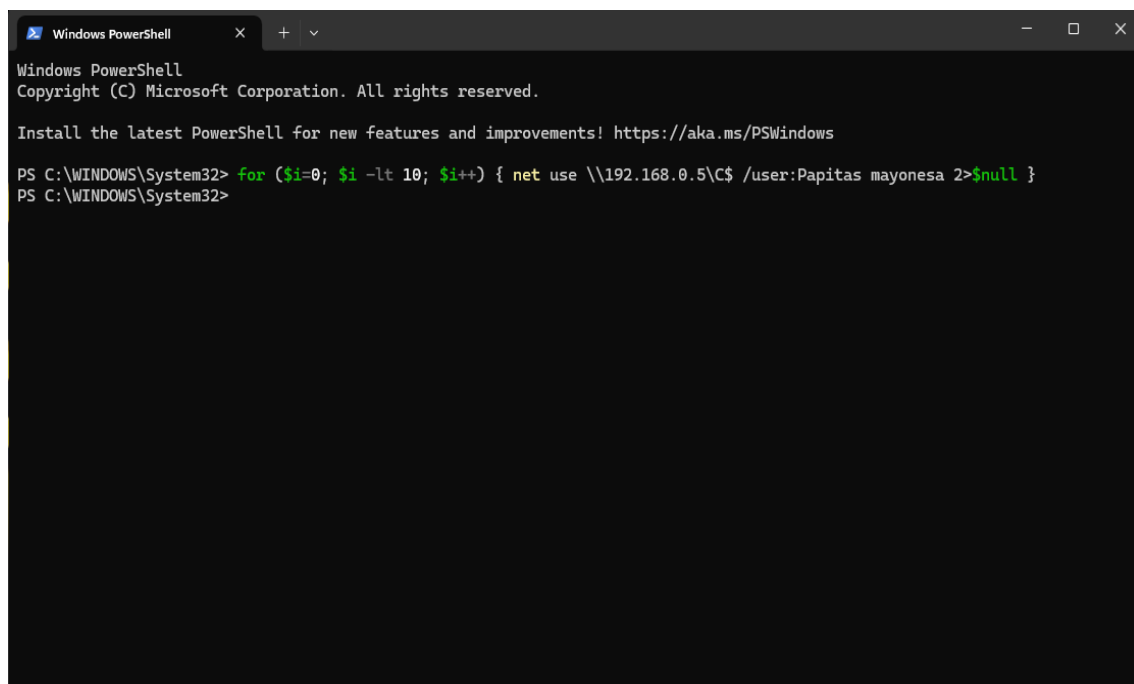
- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)
- Wazuh
- Agente Windows Wazuh

3. Metodología / Análisis realizado

Esta sección identifica y analiza los eventos de autenticación fallida simulados desde un agente Windows. Las acciones reales de contención o mitigación no forman parte del alcance del laboratorio.

3.1 Simulación de fuerza bruta

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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\System32> for ($i=0; $i -lt 10; $i++) { net use \\192.168.0.5\C$ /user:Papitas mayonesa 2>$null }
PS C:\WINDOWS\System32>
```

Figura 1. Simulación de intentos fallidos en el agente Windows

3.2 Identificación de registros de autenticación

Se ingresó a la pestaña Threat Hunting→ Events del servidor Wazuh, en donde se visualizó los diferentes eventos de autenticaciones fallidas que se hizo desde un agente Windows. (ver Figura 2)

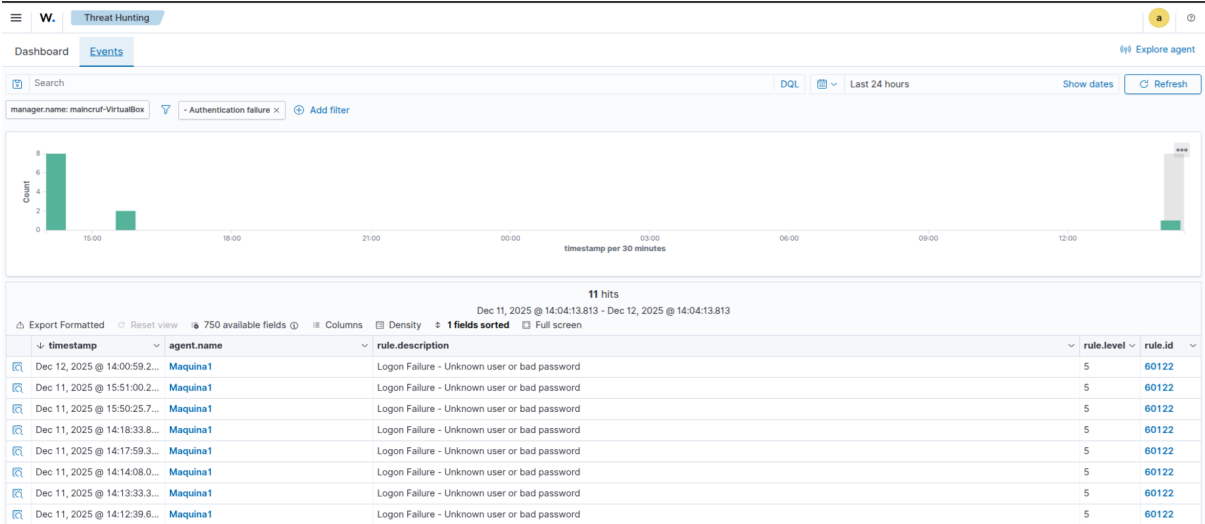


Figura 2. Eventos de autenticaciones fallidas.

3.3 Detalles de registros de autenticación

Los detalles de eventos registraron el código de error 0xc0000064, el cual indica el intento de autenticación utilizando un usuario inexistente. Asimismo, se identificó que se usó la red Logontype 3, utilizando protocolo de autenticación NTLM, desde una IP de origen específica. Este comportamiento es consistente con actividad de enumeración de usuarios o intentos de fuerza bruta en la red. (ver Figura 3)

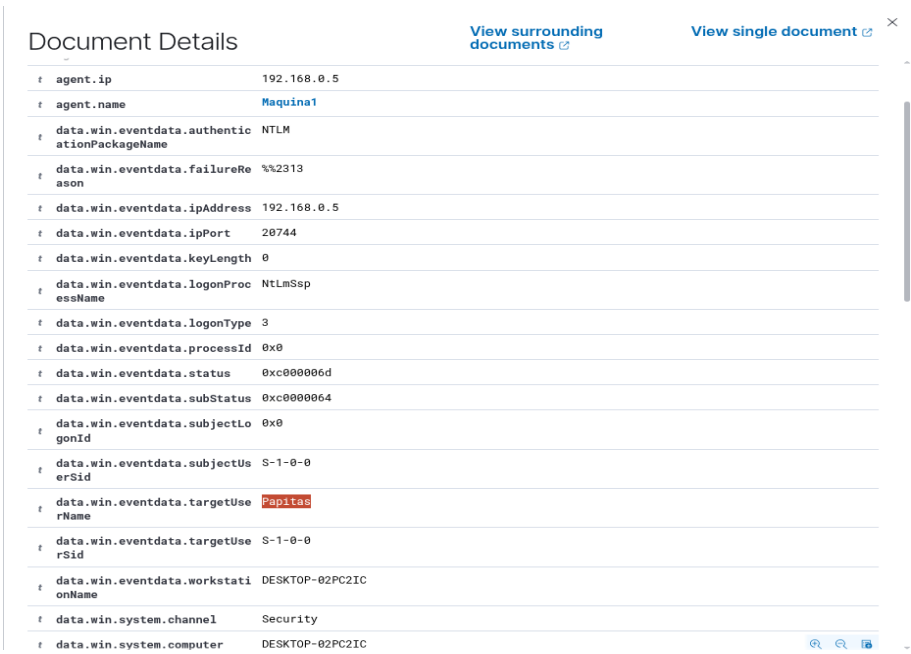


Figura 3. Detalles completos del evento de autenticación.

4. Acciones recomendadas

Ante la detección de múltiples intentos de autenticaciones fallidas, 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

5. Resultados obtenidos

Durante el laboratorio se simuló exitosamente un ataque de fuerza bruta desde un agente Windows, generando eventos de autenticación fallida, que fueron detectados y visualizados en el dashboard de Wazuh. Asimismo, se analizó en profundidad los detalles de los eventos de autenticación para una toma de decisiones precisa y fortalecer la seguridad de forma efectiva.

6. Reflexión final

Este laboratorio permitió comprender como los intentos de autenticación fallida se reflejan en un entorno real de monitoreo, destacando la importancia del SIEM en la detección temprana y el análisis de actividades sospechosas. Además, se percató la importancia de revisar detalles de los eventos para diferenciar errores legítimos de usuarios y posibles intentos de ataque, creando una oportuna respuesta ante incidentes de seguridad.