Simulación de Ataque y Configuración de Seguridad en la Nube

1. Introducción

Este informe presenta el desarrollo completo de un ejercicio práctico académico orientado a la seguridad en entornos de computación en la nube. El objetivo es configurar un entorno seguro en la nube, desplegar un servicio web con autenticación, aplicar medidas de seguridad y evaluar su efectividad mediante una simulación de ataque de fuerza bruta. La plataforma utilizada ha sido Amazon Web Services (AWS), y se ha trabajado desde una máquina local con Kali Linux para ejecutar el ataque controlado.

2. Configuración Inicial

Se utilizó AWS para desplegar una instancia EC2 con Ubuntu Server 22.04. A la máquina se accedió mediante SSH utilizando una clave pública autorizada. Esta máquina sirve como servidor para desplegar el servicio web.

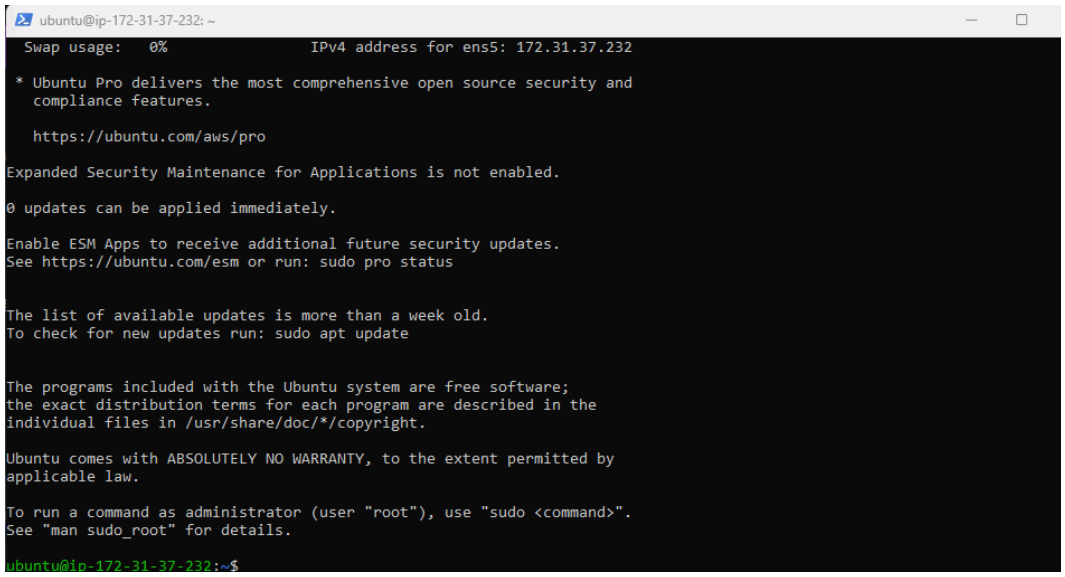

Figura 1. Acceso SSH exitoso a la instancia EC2 en AWS.

3. Montaje del Servicio Web con Autenticación

Se instaló Apache2 en la instancia. Inicialmente se comprobó el correcto funcionamiento del servidor web accediendo a la página por defecto de Apache. Posteriormente se

desplegó una página de login (`login.php`) que simula un sistema de autenticación simple vulnerable, susceptible a ataques de fuerza bruta.

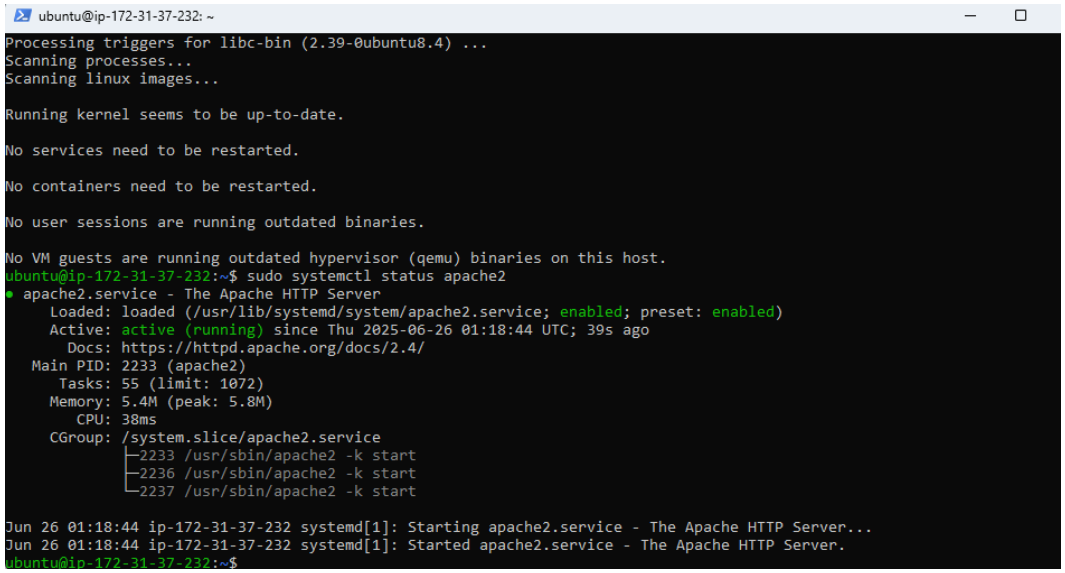

Figura 2. Estado activo del servidor Apache2.

Figura 3. Visualización de la página por defecto de Apache desde el navegador.

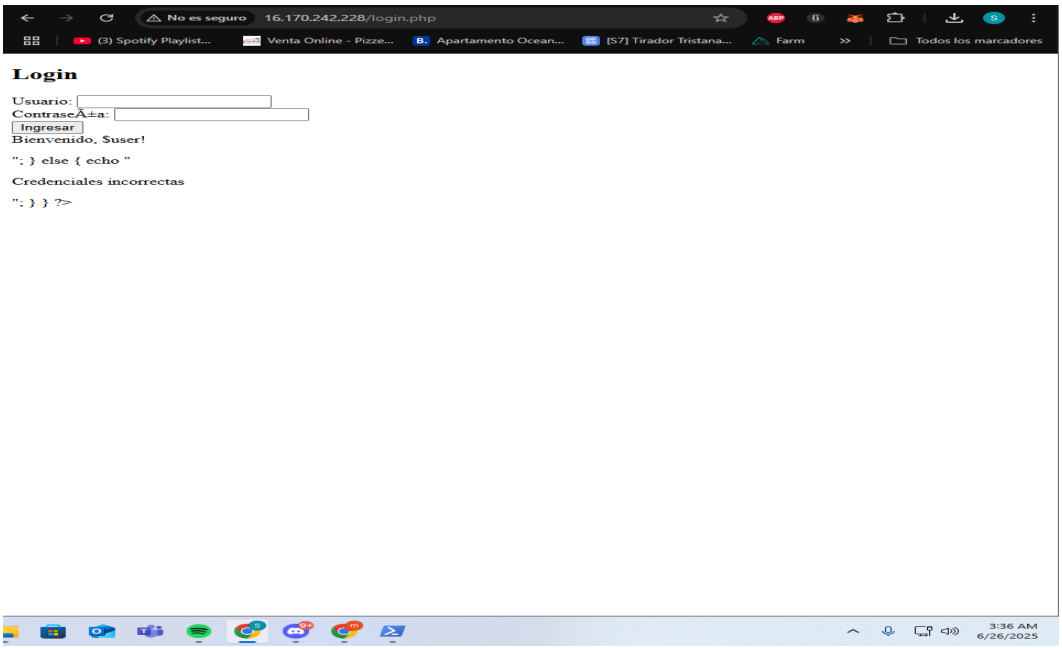

Figura 4. Formulario de login montado en el servidor web.

4. Configuraciones de Seguridad

Se configuraron grupos de seguridad en AWS para limitar el tráfico de red:

- HTTP (80) y HTTPS (443) permitidos desde cualquier IP.

- SSH (22) restringido exclusivamente a la IP del atacante legítimo.

- Se instaló y configuró un certificado SSL autofirmado para cifrar las comunicaciones HTTPS.

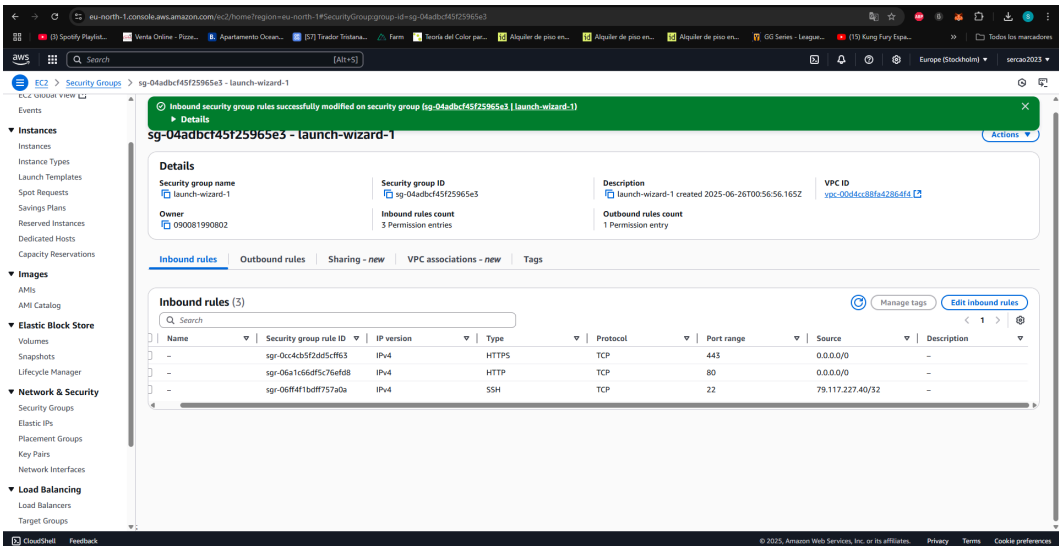

Figura 5. Grupo de seguridad con reglas aplicadas.

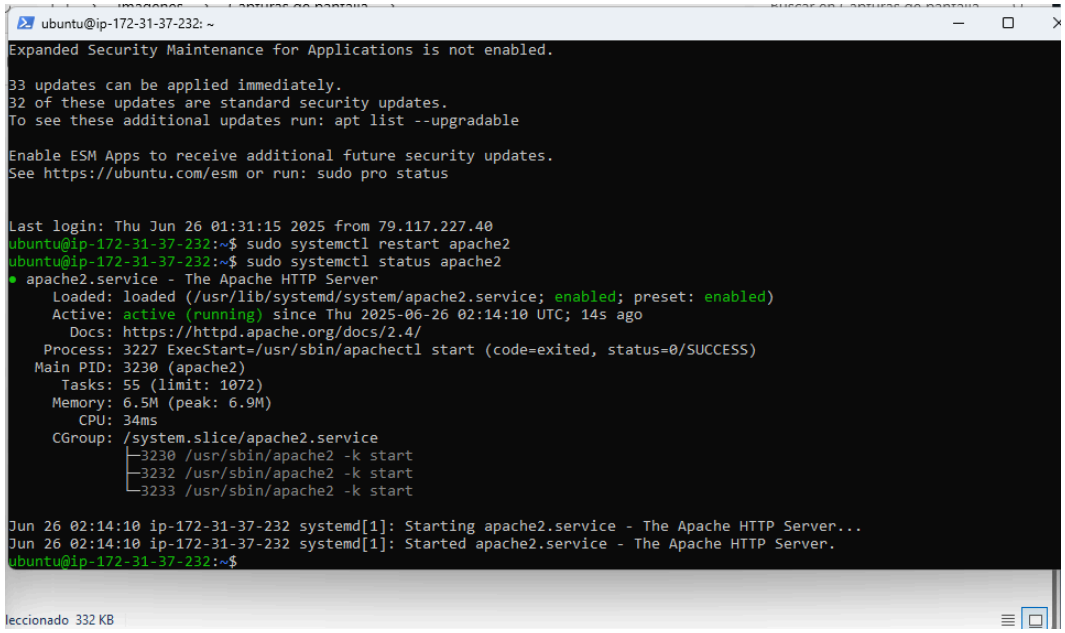

Figura 6. Reinicio y verificación de estado del servidor Apache.

5. Simulación de Ataque con Hydra

Se ejecutó un ataque de fuerza bruta con la herramienta Hydra desde una máquina Kali Linux. El ataque se dirigió al formulario de login utilizando listas comunes de usuarios y contraseñas. Se capturaron los resultados del ataque y la respuesta del servidor objetivo.

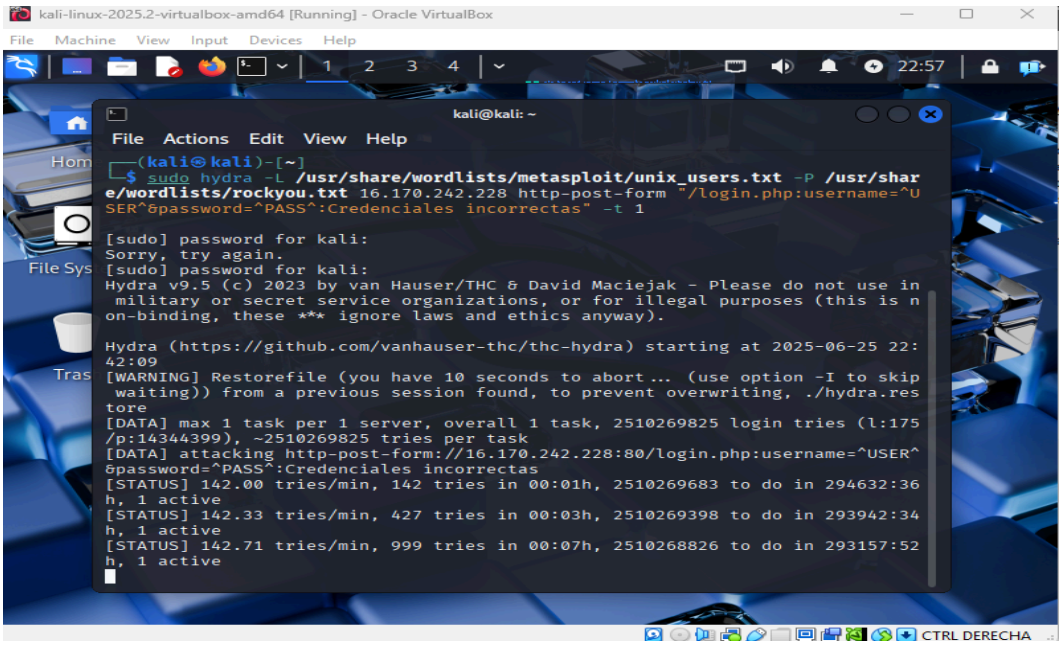

Figura 7. Ejecución del ataque con Hydra hacia login.php.

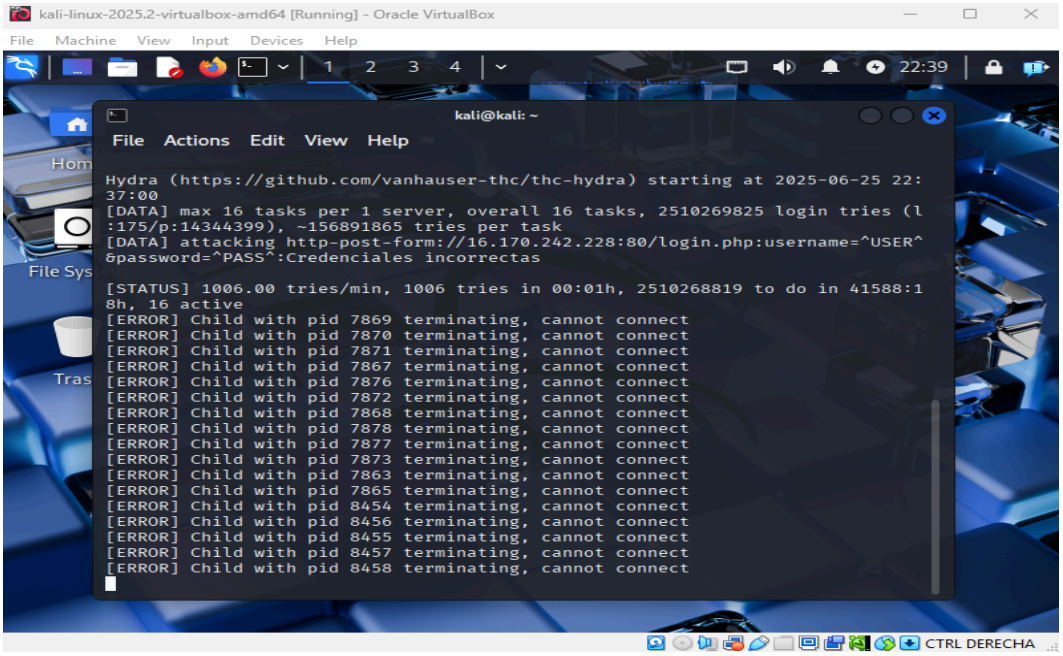

Figura 8. Rechazo de conexión por parte del servidor tras múltiples intentos.

6. Evaluación de la Efectividad

El ataque de fuerza bruta no logró comprometer el sistema. Además, el servidor comenzó a rechazar conexiones posteriores, lo que indica la presencia de mecanismos pasivos de defensa (como sobrecarga del servicio o limitación de peticiones). Las medidas de seguridad aplicadas resultaron efectivas para este tipo de amenazas.

7. Respuestas a las Preguntas Finales

- • ¿Por qué es importante implementar medidas de seguridad en entornos en la nube?

Porque los entornos en la nube están expuestos a internet y son objetivos frecuentes de ataques automatizados y manuales. Las medidas de seguridad ayudan a proteger los recursos, datos y accesos críticos.

- • ¿Cuál es el propósito de configurar grupos de seguridad en la nube?

Restringir el tráfico entrante y saliente a lo estrictamente necesario. Actúan como firewall virtual a nivel de red.

- • ¿Por qué es importante cifrar la comunicación con los servicios en la nube?

Para proteger los datos transmitidos frente a interceptaciones. HTTPS evita ataques como sniffing, man-in-the-middle y fuga de credenciales.

- • ¿Qué es un ataque de fuerza bruta y cuál es su objetivo?

Es una técnica de ataque que intenta adivinar contraseñas o credenciales enviando múltiples combinaciones hasta encontrar la correcta.

- • ¿Qué resultados obtuviste durante la simulación de ataque y por qué crees que ocurrieron?

El ataque falló. El formulario no devolvió acceso válido, y eventualmente el servidor dejó de aceptar conexiones, lo que indica una respuesta pasiva efectiva ante el abuso.

- • ¿Cómo podrías mejorar la configuración de seguridad para prevenir futuros ataques?

Aplicar límite de intentos, usar CAPTCHA, implementar autenticación multifactor (MFA), e instalar herramientas como fail2ban o WAF (Firewall de Aplicaciones Web).

- • ¿Cuál es la importancia de mantener actualizados los sistemas y aplicaciones en la nube?

Las actualizaciones corrigen vulnerabilidades que pueden ser explotadas por atacantes. Un sistema sin parches es un objetivo fácil.

- • ¿Qué aprendiste sobre la relación entre la configuración segura y la prevención de ataques?

Una configuración básica pero bien aplicada puede detener ataques simples y proteger servicios expuestos. La prevención comienza en el diseño del sistema.

- • ¿Cómo se podría aplicar este conocimiento en un entorno empresarial real?

Aplicando políticas de control de acceso, protección en la capa de aplicación, monitoreo de tráfico, segmentación de redes y entrenamiento de personal.

- • ¿Qué recomendaciones darías a otros estudiantes para realizar ejercicios similares de manera efectiva?

Seguir los pasos ordenadamente, tomar capturas a tiempo, probar todas las medidas de seguridad y documentar los errores para mejorar.

8. Referencias

- Amazon Web Services – https://aws.amazon.com/

- OWASP Foundation – https://owasp.org/

- THC Hydra – https://github.com/vanhauser-thc/thc-hydra