# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| El protocolo de red que se identifica en las capturas de paquetes durante la investigación es el protocolo de transferencia de hipertexto (HTTP). Este protocolo se utiliza para transmitir datos entre el navegador web y el servidor web, y pertenece a la capa de aplicación del modelo TCP/IP. El protocolo HTTP se puede observar en el registro de tráfico DNS y HTTP al ver las líneas que comienzan con “GET” o “POST”, que son los métodos más comunes de solicitud HTTP. | |
|

| **Section 2: Document the incident** |
| --- |
| El incidente ocurrió el 25 de enero de 2024, cuando se detectó un ataque de fuerza bruta contra el servidor web de la empresa. Un ataque de fuerza bruta es un método de prueba de error que consiste en intentar todas las combinaciones posibles de contraseñas hasta encontrar la correcta. El ataque se descubrió mediante el análisis de los registros de tráfico DNS y HTTP, que mostraban un número anormalmente alto de solicitudes HTTP al servidor web desde una misma dirección IP. El ataque duró aproximadamente 15 minutos y se detuvo cuando el firewall bloqueó la dirección IP del atacante. No se sabe si el atacante logró acceder a alguna cuenta o información confidencial. Las fuentes de información y pruebas son el archivo de registro DNS y HTTP generado con tcpdump y el registro del firewall. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Una medida de seguridad que puede ayudar a prevenir los ataques de fuerza bruta es la autenticación de dos factores (2FA). La autenticación de dos factores es un método que requiere que el usuario proporcione dos formas de verificación para acceder a una cuenta o servicio. Por ejemplo, además de introducir una contraseña, el usuario puede recibir un código por SMS, correo electrónico o una aplicación que debe introducir para completar el inicio de sesión. La autenticación de dos factores es eficaz porque dificulta que un atacante pueda acceder a una cuenta solo con adivinar o robar la contraseña. Además, la autenticación de dos factores puede alertar al usuario legítimo si recibe un código sin haber iniciado sesión, lo que indica un posible intento de intrusión. |