innigma Security

https://notificame.claro.com.gt

RESULTADOS ETHICAL HACKING INTERNO

Febrero de 2025

16 calle 6-17 zona 10, edificio Pialé, oficina 301.

Índice

--- REPORTE TRUNCADO POR PRIVACIDAD ---

Introducción

El propósito de este documento es presentar los resultados de la auditoría tecnológica realizada por Innigma Security a la infraestructura tecnológica de UBIQUO, tal como se definió dentro del alcance del proyecto, llevado a cabo del 13/01/2025 al 03/01/2025. Durante este período, se han realizado pruebas técnicas de seguridad con el fin de demostrar el nivel de seguridad de la infraestructura tecnológica donde se almacena, procesa o transmite la información, así como para determinar la viabilidad de exposición a ataques informáticos por parte de usuarios externos contra los sistemas que soportan el negocio. El principal objetivo es garantizar la confidencialidad, disponibilidad e integridad de la información alojada en la infraestructura.

Las pruebas se realizaron sin ningún conocimiento previo de la infraestructura de red existente. Esta metodología, conocida como análisis de caja negra, permite evaluar el nivel de riesgo del sistema frente a ataques dirigidos contra la organización por parte de usuarios o empresas no asociadas con UBIQUO, en los sistemas definidos en el alcance. La verificación del entorno se llevó a cabo con base en metodologías de seguridad utilizadas en la actualidad, ya sean internas, definidas por el auditor, y/o utilizando metodologías libres y reconocidas internacionalmente como OSSTMM (Open Source Security Testing Methodology Manual) y OWASP (Open Web Application Security Project).

Metodología

La metodología utilizada para la prueba de penetración es la siguiente:

- **Análisis de visibilidad:** Se identifican los activos y todos aquellos métodos o puertas de enlace que pueden ser utilizados para acceder a los recursos de la organización. El resultado de esta tarea permite generar tarjetas de puntuación con una evaluación inicial de riesgos basada en la exposición de los activos.

- **Evaluación de vulnerabilidades:** Se prueban los sistemas para el descubrimiento de vulnerabilidades existentes. Esto consiste en las siguientes fases:

    - Investigación de vulnerabilidades
    - Verificación de vulnerabilidades

- **Explotación específica:** Evaluación y explotación manual de las vulnerabilidades encontradas. Esto consiste en las siguientes fases:

    - Investigación manual de vulnerabilidades
    - Intrusión específica en la vulnerabilidad encontrada

- **Identificación de contramedidas:** Análisis detallado de cada una de las evidencias obtenidas en las fases anteriores y propuesta de medidas correctivas, siguiendo el consenso del equipo técnico encargado de poner las aplicaciones en producción.

Algunas de las herramientas utilizadas: Burpsuite, WPscan, Spoofcheck, Nessus, Censys, Nmap, SQLMap, Shodan.

Resumen Ejecutivo

En enero de 2025, **Innigma Security** llevó a cabo una evaluación de **pentesting externo** sobre la infraestructura tecnológica de https://notificame.claro.com.gt/ para identificar vulnerabilidades y evaluar el nivel de exposición de sus activos ante ataques externos. La prueba se realizó sin conocimiento previo de la infraestructura, aplicando una metodología basada de caja negra en estándares reconocidos como **OSSTMM y OWASP.**

Los hallazgos revelan que el objetivo analizado posee medidas de seguridad de acuerdo los estándares OSSTMM y OWASP, encontrando mejoras a realizar de nivel **BAJO RIESGO.**

Recomendaciones y hallazgos

--- REPORTE TRUNCADO POR PRIVACIDAD ---