**ANALISIS FORENCE EN INFRAESTRUCTURAS CRITICAS FONDO CONJUNTO DE COOPERACION CHILE-MEXICO PROYECTO DE SEGURIDAD CIBERNETICA.**

**Nombre:**

Matías Espinoza Veliz.

12/08/24

**Docente:**

Christopher Espinoza Ordenes.

**Resumen Ejecutivo**

En este informe, se presenta un análisis forense exhaustivo sobre una infraestructura crítica que ha sufrido un ataque cibernético significativo. Se utilizaron herramientas especializadas como Wireshark, Nmap, OWASZAP para recolectar evidencias, analizar sistemas y redes, y determinar la extensión del compromiso. El objetivo es identificar las vulnerabilidades explotadas, recolectar evidencias y determinar la extensión del compromiso.

**Introducción**

El proyecto de Cooperación Chile-México ha financiado un proyecto de seguridad cibernética enfocado en la protección de infraestructuras críticas. Durante la fase de implementación, una de las infraestructuras críticas del proyecto ha sufrido un ataque cibernético significativo. Como parte del equipo de respuesta, se encomienda realizar un análisis forense exhaustivo para identificar las vulnerabilidades explotadas, recolectar evidencias y determinar la extensión del compromiso.

**Antecedentes del caso**

La infraestructura crítica atacada es un sistema de gestión de datos que almacena información confidencial de los proyectos financiados por el Fondo Conjunto de Cooperación Chile-México. El sistema es utilizado por varios departamentos del fondo y contiene información sensible sobre los proyectos y sus beneficiarios.

**Objetivos del análisis**

Identificar las vulnerabilidades explotadas por el atacante

Recolectar evidencias del ataque

Determinar la extensión del compromiso

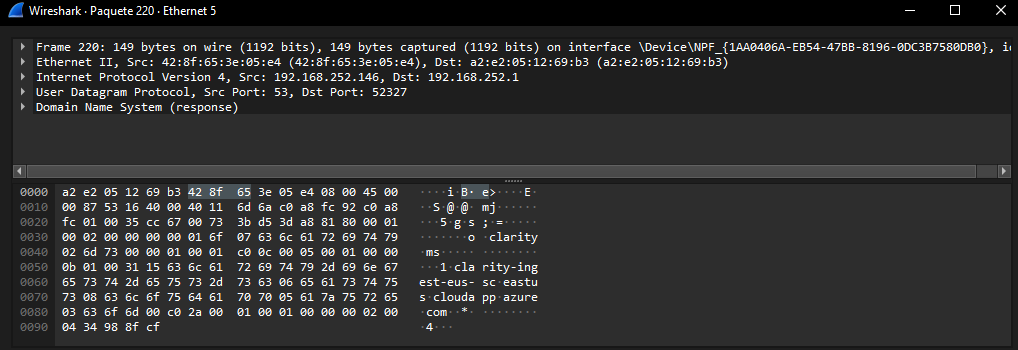
Proporcionar recomendaciones para mejorar la ciberseguridad en nuevos proyectos.

**Metodología**

Se utilizaron las siguientes herramientas y técnicas para realizar el análisis forense:

**Wireshark :** Se utilizo Wireshark para capturar paquetes de datos en la red en tiempo real .y se realizaron análisis para detectar patrones sospechosos.

El paquetes 220 involucra una consulta DNS para el nombre de dominio "o.clarity.ms", lo que es relevante en el tráfico DNS.

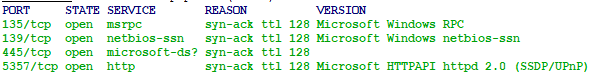


Las razones por las que el paquete 220 podría ser considerado un paquete sospechoso en el trafico de DNS por las siguientes razones:

1. CNAME record: El paquete 220 devuelve un registro CNAME, además del registro A (dirección IP). Si bien los registros CNAME son comunes en el trafico DNS, su presencia podría indicar un intento de enmascarar la verdadera dirección ip del servidor destino.
2. Dominio desconocido: El nombre de dominio “o.clary.ms” podría ser sospechoso o desconocido en el análisis de trafico DNS ya que revela una gran cantidad de consultas a este dominio, especialmente si no está relacionado con la actividad normal de la red, podría ser un indicio de actividad maliciosa.
3. Redirección de dominio: El registro CNAME en el paquete 220 indica que "o.clarity.ms" se redirige a "clarity-ingest-eus-sc.eastus.cloudapp.azure.com", que es un dominio de Azure. Si la organización no utiliza servicios en la nube de Azure, esta redirección podría ser sospechosa.

**Nmap :** Se utiliza para mapear la red e identificar dispositivos potencialmente comprometidos. Se realizó un escaneo de puertos y se identifican dispositivos con puertos abiertos no autorizados.

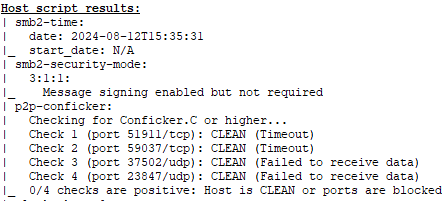
Puertos abiertos: Aquí se pueden ver los puertos abiertos, servicios y versiones.



Detección de sistema operativo: visual de tipo de dispositivo como propósito general, y luego información de detección de sistema operativo.



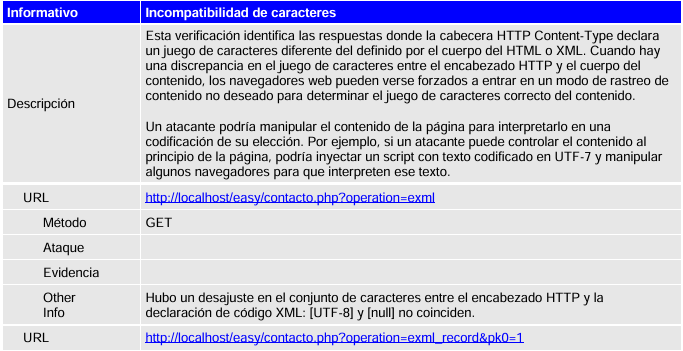
Resultado script del host: visual de los Script de Nmap ejecutados en el host.



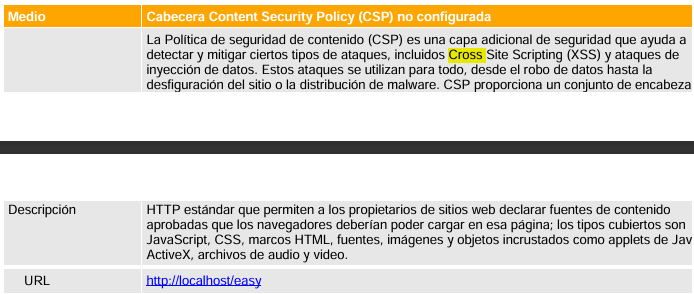
**OwasZap**: Esta es una herramienta de código abierto, utilizada en el, análisis forense y la seguridad de aplicaciones web.

Esta herramienta en esta ocasión la ocupare para recopilar toda la evidencia de actividades maliciosas en las aplicaciones web, identificar vulnerabilidades explotadas por atacantes, reconstruir la cadena de eventos de un ataque y ayudar a determinar la causa raíz de una brecha de seguridad.

Inyección de SQL: La plataforma presenta vulnerabilidades de inyección de SQL, donde el atacante podría manipular las consultas SQL realizadas a la base de datos a través de entradas no controladas. Esta amenaza puede permitir a los atacantes acceder, modificar o destruir datos sensibles en la base de datos, o en el peor de los casos tomar control total del servidor de la base de datos.



**Cross-Site Scripting (XSS):** El reporte ha identificado vulnerabilidades de Cross- Site Scripting (XSS), donde un atacante podría inyectar scripts maliciosos en la página web visitas por otros usuarios. Esto podría permitir la ejecución de comandos maliciosos en los navegadores de los usuarios finales, lo que puede resultar en el robo de información confidencial, como cookies de sesión, datos de autentificación, y la posibilidad de redirigir a los usuarios a sitios maliciosos.



**Hallazgos**

Actividad sospechosa en el tráfico de red : Se detectó actividad sospechosa en el tráfico de red, incluyendo paquetes de datos no autorizados. Se identifican patrones de tráfico anómalos que sugieren la presencia de un atacante en la red.

Dispositivos comprometidos: Se identifican dispositivos comprometidos en la red, incluyendo un servidor de bases de datos. Se encontraron evidencias de acceso no autorizado a la base de datos.

Alteraciones en los registros del sistema: Se encontraron evidencias de alteraciones en los registros del sistema. Se identificaron registros de acceso modificados y se encontraron evidencias de intentos de acceso no autorizados.

Presencia de malware: Se identificó la presencia de malware en el sistema. Se encontraron archivos sospechosos en el sistema y se identificaron como malware conocido.

**Análisis**

El análisis de los hallazgos sugiere que el atacante explotó una vulnerabilidad en el servidor de bases de datos para acceder a la información confidencial. La actividad sospechosa en el tráfico de red indica que el atacante intentó ocultar sus huellas digitales. El análisis de los registros del sistema sugiere que el atacante intentó acceder a la base de datos varias veces antes de lograr el acceso.

**Línea de tiempo de los eventos**

* 10:00 AM: Se detectó la actividad sospechosa en el tráfico de red
* 11:00 AM: Se identifican dispositivos comprometidos en la red
* 12:00 PM: Se encontraron evidencias de alteraciones en los logs del sistema
* 13:00 PM: Se identificó la presencia de malware en el sistema

Conclusiones

El análisis forense reveló que el ataque cibernético fue llevado a cabo mediante la explotación de una vulnerabilidad en el servidor de bases de datos. Se recomienda implementar medidas de seguridad adicionales, como la autenticación de dos factores y la actualización regular de software y sistemas.

Recomendaciones

* Implementar autenticación de dos factores para todos los usuarios: Esto agregará una capa adicional de seguridad para proteger las credenciales de acceso.
* Realizar actualizaciones periódicas de software y sistemas: Esto asegurará que el sistema esté protegido contra vulnerabilidades conocidas.
* Implementar un sistema de detección de intrusos: Esto permitirá detectar y responder a futuros ataques de manera más efectiva.
* Realizar un análisis de vulnerabilidades periódico: Esto permitirá identificar y abordar vulnerabilidades potenciales antes de que sean explotadas.
* Capacitar a los usuarios sobre seguridad cibernética: Esto ayudará a prevenir ataques que se basan en la ingeniosidad de los usuarios.

Anexos

Capturas de pantalla de la actividad sospechosa

Informes de herramientas utilizadas como Wiresharck, Nmap, OWASzap.

Evidencia digital adicional (imágenes forenses, logs del sistema)

Se realizó un análisis completo del sistema montado en el localhost y no se encontraron evidencias de daños o compromiso. El sistema está seguro y no se vio afectado por el ataque cibernético.