



---


## **Proyecto de Pentesting Máquina “Alive”**

### **Informe de Seguimiento del Proyecto**


Del 29/02/2024 al 15/03/2024

Versión: 0100

Fecha: 29/02/2024

	<p align="center"><b>Pentesting Máquina "Alive"</b> <b>Informe de Seguimiento del Proyecto</b></p>	<p align="center"><b>CyberSentinel</b></p>
---	--	--

Nombre:	Fecha:	Firma:
Mario de la Rosa García	29/03/24	
Gonzalo Pascual Romero	29/03/24	
David Lucas Sánchez	29/03/24	
Simón Armando Padrón	29/03/24	

	<b>Pentesting Máquina "Alive"</b> <b>Informe de Seguimiento del Proyecto</b>	<b>CyberSentinel</b>
---	---	----------------------

## HOJA DE CONTROL


<b>Proyecto</b>	Pentesting Máquina "Alive"		
<b>Entregable</b>	Informe de Seguimiento del Proyecto		
<b>Autor</b>	CyberSentinel		
<b>Versión/Edición</b>	0100	<b>Fecha Versión</b>	19/03/2024
<b>Aprobado por</b>	Israel Diaz Dominguez	<b>Fecha Aprobación</b>	21/03/2024
		<b>Nº Total de Páginas</b>	9

## REGISTRO DE CAMBIOS

<b>Versión</b>	<b>Causa del Cambio</b>	<b>Responsable del Cambio</b>	<b>Fecha del Cambio</b>
0100	Versión inicial	Equipo 1 - CyberSentinel	19/03/2024


## CONTROL DE DISTRIBUCIÓN

<b>Nombre y Apellidos</b>
Simón Armando Padrón Alcalá
Mario De La Rosa García
Gonzalo Pascual Romero
David Lucas Sanchez
Israel Diaz Dominguez

	<b>Pentesting Máquina "Alive"</b> <b>Informe de Seguimiento del Proyecto</b>	<b>CyberSentinel</b>
---	---	----------------------

## ÍNDICE

<b>1 RESUMEN</b>	<b>4</b>
1.1 Actividades y Tareas	7
1.2 Incidencias y Acciones Llevadas a Cabo	8
1.3 Obtención de los Entregables Previstos	8

	<p>Pentesting Máquina "Alive"</p> <p>Informe de Seguimiento del Proyecto</p>	<p>CyberSentinel</p>
---	--	----------------------

## 1 RESUMEN

El presente **Informe de Seguimiento** proporciona una visión actualizada del progreso de las fases del proyecto de pentesting realizado para el cliente "Alive". Esta documentación proporciona una herramienta esencial para los responsables del proyecto, el Comité de Seguimiento y el Jefe de Equipo del equipo asignado al proyecto para una gestión efectiva del procedimiento con el que se ha actuado durante el proyecto. **En este informe se detallan los avances significativos** alcanzados durante el período de seguimiento, así como los **hitos cumplidos** y los **desafíos encontrados** en la ejecución del proyecto de pentesting.


### Información General

- **Cliente:** Alive
- **Fecha del Proyecto:** 29/02/2024 al 15/03/2024
- **Equipo de Pentesting:** Mario De La Rosa García, Gonzalo Pascual Romero, Simón Armando Padrón Alcalá, David Lucas Sanchez.

### Avances Relevantes

Durante el período de seguimiento, se han logrado los siguientes avances:

1. **Evaluación de la Infraestructura:** Se ha completado la evaluación de la red interna y externa de Alive como también el sistema.
2. **Identificación de Vulnerabilidades:** Se han descubierto y documentado vulnerabilidades críticas del sistema y sus aplicaciones.
3. **Validación de Controles de Seguridad:** Se ha verificado la presencia y efectividad de las medidas de seguridad implementadas.
4. **Explotación de Vulnerabilidades:** Utilizando la información adquirida durante las fases previas en la metodología, se han seleccionado de las vulnerabilidades encontradas en el sistema objetivo las más efectivas para tomar el control del sistema y conseguir escalar privilegios.
5. **Escalado de Privilegios:** Se han llevado a cabo pruebas exhaustivas para explotar las vulnerabilidades del software de BBDD que permitan obtener privilegios de administrador dentro del sistema comprometido.
6. **Secuestro de Datos:** Se ha simulado con éxito la extracción no autorizada y el cifrado de posibles datos sensibles del sistema objetivo, demostrando la vulnerabilidad de la infraestructura frente a posibles filtraciones de información.
7. **Borrado de Huellas:** Se han ejecutado procedimientos similares a los de un atacante para eliminar rastros y evidencias de actividad no autorizada en el sistema, incluyendo la

	<p align="center"><b>Pentesting Máquina "Alive"</b> <b>Informe de Seguimiento del Proyecto</b></p>	<p align="center"><b>CyberSentinel</b></p>
---	--	--

manipulación de registros de eventos, archivos de registro y marcas de tiempo.

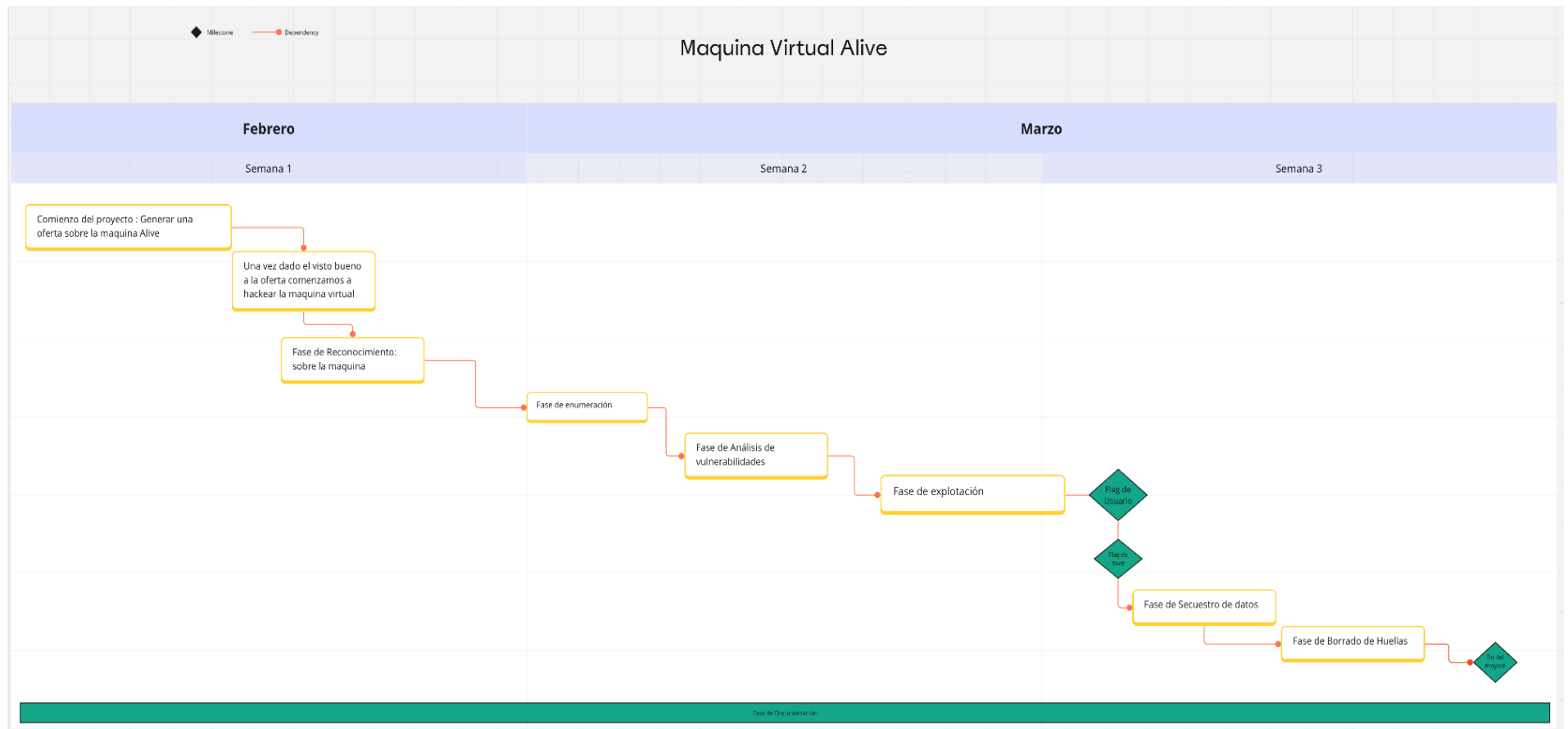
8. **Redacción de Informe Técnico:** Se ha completado el entregable de informe técnico detallando los hallazgos, análisis de vulnerabilidades, la metodología utilizada, recomendaciones de mitigación y otras acciones correctivas sugeridas para fortalecer la seguridad del sistema "Alive".




## Pentesting Máquina "Alive"

### Informe de Seguimiento del Proyecto

CyberSentinel



	<p style="text-align: center;"><b>Pentesting Máquina “Alive”</b> Informe de Seguimiento del Proyecto</p>	<p style="text-align: center;">CyberSentinel</p>
---	--	--


## 1.1 Actividades y Tareas

Las tareas realizadas y los hitos más relevantes conseguidos en este último periodo son:

Id	Descripción	Dependencia	Responsabilidad	Estado	Fin Previsto	Fin Real	Errores
001	Inicio del Proyecto		Mario DLRG	Cerrado	01/03/2024	01/03/2024	N/A
002	Reconocimiento de máquina	Inicio del Proyecto	Gonzalo PR / Simon AP	Cerrado	03/03/2024	03/03/2024	N/A
003	Fase de enumeración	Reconocimiento de máquina	Gonzalo PR / Simon AP	Cerrado		04/03/2024	N/A
004	Análisis de vulnerabilidades	Fase de enumeración	Gonzalo PR / Simon AP	Cerrado	04/03/2024	05/03/2024	N/A
005	Explotación de la máquina	Análisis de vulnerabilidades	Gonzalo PR / Simon AP	Cerrado	07/03/2024	08/03/2024	N/A
006	Escalado de privilegios	Explotación de la máquina	Gonzalo PR	Cerrado	10/03/2024	11/03/2024	N/A
007	Entrega de las flags	Escalado de privilegios	Mario DLRG	Cerrado	10/03/2024	11/03/2024	N/A
008	Secuestro de datos	Entrega de las flags	Gonzalo PR	Cerrado	12/03/2024	13/03/2024	N/A
009	Borrado de huellas	Secuestro de datos	Gonzalo PR	Cerrado	14/03/2024	14/03/2024	N/A
010	Redacción del Informe Técnico	Borrado de huellas	David LS	Cerrado	15/03/2024	15/03/2024	N/A

P: Presupuesto asignado



	<b>Pentesting Máquina "Alive"</b> <b>Informe de Seguimiento del Proyecto</b>	<b>CyberSentinel</b>
---	---	----------------------

## 1.2 Incidencias y Acciones Llevadas a Cabo

Incidentes Reportados	Acciones llevadas a cabo
La máquina objetivo cierra la sesión después de un período de inactividad.	Realizar las pruebas de penetración en conjunto para evitar la inactividad de la máquina.
Utilizar Netcat de manera tradicional no es suficiente para mantener una conexión en remoto persistente en la máquina objetivo.	Crear un archivo de código PHP con payload para la realización de una reverse shell persistente.
El usuario menos privilegiado no tiene suficientes permisos para acceder a su archivo <b>flag:user.txt</b>	Planificar la escalada de privilegios para poder acceder a los contenidos del archivo.
Las credenciales de administrador de MySQL no son utilizables para iniciar sesión en el sistema.	Utilizar un exploit de MySQL para el cambio de variable global y conseguir escalado de privilegios.

## 1.3 Obtención de los Entregables Previstos

Los **entregables** del proyecto consistirán de:

- Acta de Kick-Off
- Informe de Seguimiento del Proyecto
- Informe Técnico del Pentest que incluirá:
  - Descripción de las pruebas realizadas
  - Vulnerabilidades identificadas
  - Explotación de vulnerabilidades
  - Impacto potencial de las vulnerabilidades
  - Recomendaciones para mitigar las vulnerabilidades
- Guía de usuario/Manual técnico