



# HACKTHEBOX

## Informe Técnico Máquina Mario



Este documento es confidencial y contiene información sensible.  
No debería ser impreso o compartido con terceras entidades.



---

## Tabla de contenido

<b>1. Antecedentes</b>	<b>2</b>
<b>2. Objetivos</b>	<b>2</b>
2.1. Consideraciones . . . . .	2
<b>3. Análisis de vulnerabilidades</b>	<b>3</b>
3.1. Reconocimiento inicial . . . . .	3



## 1. Antecedentes

El presente documento contiene los resultados obtenidos durante la fase de auditoria realizada a la máquina Mario de la plataforma [HackTheBox](#).



Figura 1: Datos de la Máquina Mario

## 2. Objetivos

Conocer el estado de seguridad actual del servidor **Mario**, enumerando posibles vectores de explotación y determinando el alcance e impacto que un atacante podría ocasionar sobre el sistema en producción.

### 2.1. Consideraciones

Una vez finalizadas las jornadas de auditoria, se llevará a cabo una fase de saneamiento y buenas prácticas con el objetivo de securizar el servidor y evitar ser víctimas de un futuro ataque en base a los vectores explotados.



Figura 2: Flujo de trabajo

### 3. Análisis de vulnerabilidades

#### 3.1. Reconocimiento inicial

Se comenzó realizando un análisis inicial del sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera:



Figura 3: Reconocimiento inicial sobre el sistema objetivo

Una vez localizado, se realizó un escaneo a través de la herramienta **nmap** para la detección de puertos abiertos, obteniendo los siguientes resultados:

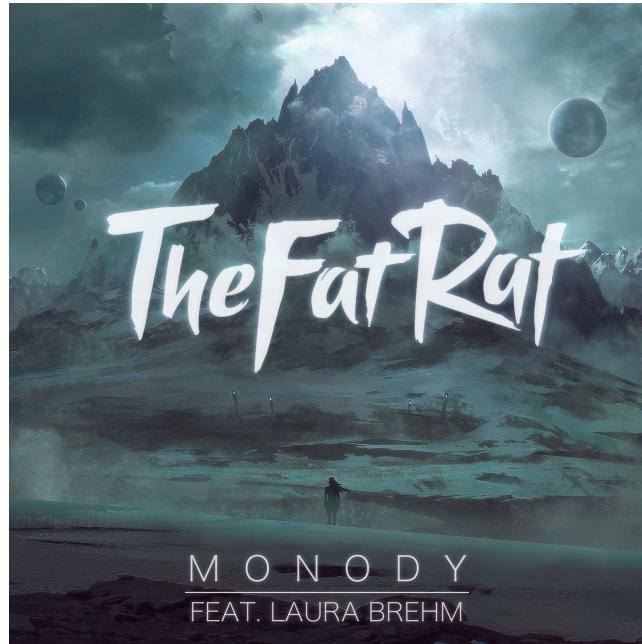


Figura 4: Reconocimiento con nmap

Asimismo, con el objetivo de evitar falsos positivos, se diseño un script en **Bash** para enumerar posible puertos adicionales que la herramienta nmap no llegara a detectar.

```

1 #!/bin/bash
2 for port in $(seq 1 65535); do
3     timeout 1 bash -c "echo > /dev/tcp/10.10.10.52/$port" > /dev/null 2>&1 && echo "$port/tcp"
4     &
5 done; wait

```

Código 1: Script personalizado para enumerar puertos

A través de este script, fue posible detectar puertos adicionalmente abiertos:

TCP
Puertos
593, 1337

Una vez finalizada la fase de enumeración de puertos, se detectaron los servicios y versiones que corrían bajo estos, representando a continuación los más significativos bajo los cuales fue posible explotar el sistema:

Tal y como se aprecia en la figura 5



Figura 5: Enumeración de servicios y versiones