
📄 **Informe de Actividades - CTFs y Pruebas de Penetración**

Autor: Javier Mauricio Carrasco Guzmán
Fecha: 22 de agosto de 2025
Herramientas usadas: Nmap, Gobuster, xfreerdp, MongoDB, Enum4linux, Hydra

---

1. Introducción

Durante estas actividades, se realizaron distintos **laboratorios CTF** orientados a pentesting y enumeración de servicios expuestos.
El objetivo fue **reconocer, enumerar, explotar y extraer información sensible** simulando escenarios reales de pruebas de penetración.

---

2. Metodología empleada

Se siguió una metodología basada en pasos usados en **pentesting profesional**:

1. **Reconocimiento activo:** Descubrimiento de puertos y servicios abiertos.
2. **Enumeración de directorios y archivos ocultos.**
3. **Acceso remoto mediante RDP usando xfreerdp.**
4. **Conexión y extracción de datos desde bases de datos MongoDB.**
5. **Identificación de información sensible (flags, credenciales, secretos).**

---

3. Procedimiento detallado

3.1. Reconocimiento de servicios (Nmap)

Se identificaron los servicios activos en las máquinas objetivo:

nmap -Pn -sV 10.129.123.27

Resultado principal:

- Puerto **80/tcp** → **HTTP** (nginx 1.14.2)
- Puerto **3389/tcp** → **RDP**

- Puerto **21017/tcp** → **MongoDB**

3.2. Enumeración de directorios ocultos (Gobuster)

Para encontrar paneles, archivos sensibles y rutas ocultas:

gobuster dir -u http://10.129.123.27 -w /usr/share/wordlists/dirb/common.txt -x php -t 50

Hallazgos importantes:

- /admin.php
- /login.php
- /config.php
- /uploads/

Estos endpoints pueden servir para **fuerza bruta**, **SQLi**, **LFI** o **subida de shells**.

3.3. Acceso a RDP con xfreerdp

Se detectó un servidor **Microsoft Terminal Services** abierto (puerto 3389).
Intentamos conectarnos de forma anónima:

xfreerdp /v:10.129.123.27 /u: /p: /cert:ignore /sec:nla

Aunque no se logró acceso en esa etapa, la información obtenida ayudó a la enumeración de usuarios y credenciales.

3.4. Conexión a MongoDB

Identificamos un servicio **MongoDB** expuesto en el puerto **21017**.
La conexión se realizó exitosamente:

mongo --host 10.129.139.230 --port 21017

Una vez dentro, se listaron las bases de datos:

show dbs

Resultado:

admin

config

local

sensitive_information

users

3.5. Extracción de información sensible

Dentro de la base sensitive_information:

use sensitive_information

show collections

db.flag.find().pretty()

En la base users:

use users

show collections

db.users.find().pretty()

Esto permitió **enumerar credenciales y datos críticos** que serían usados en fases posteriores.

---

4. Hallazgos relevantes

Servicio	Puerto	Hallazgo	Riesgo potencial
HTTP	80	Archivos .php expuestos	Credenciales, RCE
RDP	3389	Servicio detectado	Fuerza bruta, acceso remoto
MongoDB	21017	Acceso sin autenticación	Exfiltración de datos

---

5. Conclusiones

- Se identificaron **servicios expuestos sin autenticación**, como **MongoDB**.

- Se encontraron **archivos PHP ocultos** que podrían ser explotados para comprometer el sistema.
- Se extrajo información sensible como **credenciales** y **flags** de bases de datos sin medidas de seguridad.
- Estas actividades refuerzan habilidades en **reconocimiento, enumeración, explotación y análisis de datos**.