**Hacking**

**ético**

# CTF Ubuntu 16

### U3\_E1

Francisco Iván Ramírez Ortega

Curso 2023 - 2024

IES El Rincón

Curso de especialización en Ciberseguridad en entornos de las tecnologías de la información.

| [**CTF Ubuntu 16**](#_ncqwc238sads) **1**  [U3\_E1](#_nn0t2lm50w7z) 1  [**Enumeración**](#_g5dpjuypatr7) **2**  [alumno → jupiter](#_tsq53deel9xm) 5  [Admin → saturno](#_njlj8w95mew9) 7  [Maria -> computer](#_axq6uymb607) 10  [harry -> potter](#_45230nh74jvg) 11  [Credenciales](#_etz230e1gco0) 11  [Ftp](#_c2kbetpxsch5) 12  [Mysql](#_ov3rzfm0u9el) 13  [Clave de root](#_3vvw03txqfpa) 14 |
| --- |
| Enumeración |
| sS |
|  |
| sC |
|  |
|  |
| Ftp server llamado HackTeror |
|  |
| Potencial usuario → alumno |
| Correo → root@HackMeubuntu |
| archivos encontrados |
|  |
| Credencial |
| alumno → jupiter |
| Nuevos usuarios |
|  |
| \*\* ¿permisos en profe y en root? |
| history |
|  |
|  |
|  |
|  |
|  |
| Seguimos el mismo camino del historial. |
|  |
| Actualizamos la lista de usuarios |
|  |
| Vuelvo a realizar el intento de intrusión por ssh con los nuevos usuarios |
|  |
| Admin → saturno |
|  |
| <https://gtfobins.github.io/> |
|  |
|  |
|  |
| Alcanzamos una sesión como **root**, vamos a /root y encontramos una flag. |
| La traemos a nuestra máquina con nc |
|  |
| Nos pide contraseña. Seguimos buscando. |
| Nos aparece una imagen de harry potter. Conseguimos la contraseña de harry. |
| .mysql\_history |
|  |
| Credenciales mysql |
| profe → Snake88 |
|  |
| /root/pista.txt |
|  |
| -Comunicado importante:  -Únicamente decirles que mi nombre es Victor Hugo. Naci el 12 de octubre,  -Por lo visto, el mismo año que mi amigo Chucky el diabolico je, je, je. Es por lo que le he  -Puesto a mi perrito ese mismo nombre. Bueno creo que he dicho demasiado .... |
| \*\*Probar cewl |
| Traigo los archivos shadow y passwd |
| **unshadow passwd.txt shadow.txt > unshadow** |
| **john unshadow** |
| Rápidamente conseguimos dos credenciales nuevas |
| Maria -> computerharry -> potter |

| Credenciales | |
| --- | --- |
| alumno | jupiter |
| Maria | computer |
| harry | potter |
| admin | saturno |
| root | rotciv\_1210 |
| profe | Snake88 |

| Hackteror |
| --- |
| .bash\_history |
|  |
|  |
|  |
| cat |
|  |
|  |
| Se trata de un script de la comunidad para hacer un análisis a un equipo. Lo ejecutamos. |
|  |
|  |
|  |

| Harry |
| --- |
| /home/harry/pista.txt |
|  |
| TopSecret.pdf |
| Se puede hacer un diccionario con crunch pero en poco tiempo se logra jhon y passwd |

### 

| Ftp |
| --- |
|  |

| Mysql |
| --- |
|  |
|  |
| 7z2jhon flag.7z > flagjohn |

| flag.7z |
| --- |
|  |
| cupp output\_dictionary.txt |
|  |
|  |
|  |
|  |
| Clave de root |
|  |