Bandit-Overthewire

Bandit es una maquina a la que vamos a acceder mediante ssh y vamos a ir avanzando niveles si resolvemos los problemas que nos presentan, cada nivel es otro usuario diferente dentro del dominio de bandit.labs.overthewire.org

Nivel 0 - 1

En el nivel 0 hemos tenido que loggear con ssh en la maquina de bandit, password: bandit0 y user: bandit0, la ip como he dicho antes es bandit.labs.overthewire.org

Para pasar al nivel 1 lo que teniamos que hacer era hacer un ls para ver que ahi estaba el archivo readme donde se encuentra la contraseña para hacer otro ssh a bandit1

hacemos un cat al archivo readme.txt y la contraseña es: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Nivel 1 - 2

La contraseña esta en un archivo denominado "-", que por ser un carácter especial intenta acceder a otra parte de la maquina por lo tanto hay que especificar al 100% usando cat "<" o "./", de esta manera descubrimos la contraseña para el nivel 2 y es: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Nivel 2 - 3

En el nivel 2 lo que hay que hacer es leer un archivo con espacios en el nombre y habria que hacerle el cat pero dentro de comillas el nombre si no no se puede la contraseña es : MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Nivel 3 - 4

En el nivel 3 hemos tenido que movernos al inhere directory que estaba creado, hacer un ls a para descubrir que el nombre del archivo oculto se llama . . . hidingfrom-you y hacerle un cat

la contraseña del nivel 3 es: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Nivel 4 - 5

En el nivel 4 tenemos que entrar en el directory inhere, dentro hay archivos denominados -file00 que van del 00 al 09, uno de ellos es legible por el ser humano, para poder leerlo ya que su nombre es un tanto peculiar deberemos hacer el comando: cat – -file00 el archivo legible finalmente era el -file07 y la contraseña era: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Nivel 5 - 6

En el nivel 5 lo que tenemos que hacer es buscar la contraseña en un archivo human-readable

- 1033 bytes in size
- not executable

para ello lo que tenemos que hacer es ejecutar este simple comando : find . -type f -size 1033c ! -executable -exec file {} + | grep “text” de esta manera nos indica dentro del monton de archivos que existen el que buscamos exactamente.

La contraseña es: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Nivel 6 - 7

Las condiciones para encontrar la contraseña en un archivo dentro del servidor de bandit6 son estas:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Para encontrar el archivo usamos el comando: find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

Con find empezamos a buscar un archivo desde el directorio root, filtramos con user la condicion de que el archivo es de la propiedad de user bandit7 con group que pertenece a bandit6, el size 33c para decir su tamaño en bytes exacto y la ultima parte del comando sirve para eliminar errores que nos popearian por intentar acceder a directorios a los que no tenemos acceso

La contraseña es: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Nivel 7 - 8

En el siguiente nivel tenemos que buscar la contraseña almacenada en el archivo data.txt junto a la palabra millionth

Para encontrar la contraseña tenemos que hacer un grep millionth data.txt

La contraseña es: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Nivel 8 - 9

En el siguiente nivel hay que buscar la contraseña en data.txt de nuevo pero esta vez la condicion es que esta en la unica linea que solo ocurre una vez

Para encontrarla tenemos que hacer un sort data.txt | uniq -c nos saldrá todas las veces que se repite cada linea solo hay que coger la no se repite, tambien podemos hacer el mismo comando pero en vez de -c se puede usar -u que solo nos saca la que no se repite

La contraseña es: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Nivel 9 - 10

En el siguiente nivel lo que tenemos que hacer es encontrar la contraseña en el archivo data.txt en uno de los pocos strings leibles por humano y precedido de varios caracters “=”

Lo que hay que hacer para encontrarlo es usar este comando: grep -o -a ’=+ .*’ “data.txt” el -a es obligatorio en este caso porque el grep toma el data.txt como archivo binario por contener caracteres raros y hay que usarlo para que lo tome como u texto simple

La contraseña es: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Nivel 10 - 11

En el siguiente nivel tenemos que conseguir la contraseña en el archivo data.txt que esta codeado con base 64 simplemente le hacemos un cat, lo copiamos y en cyberchef lo desencriptamos usando la receta de from base64

La contraseña es: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Nivel 11 - 12

En el siguiente nivel tenemos que sacar la contraseña de data.txt donde todas las mayusculas de la A-Z y las minusculas de la a-z han sido rotadas 13 posiciones

Para encontrarla tenemos que hacer: echo 'Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4' | tr 'A-Za-z' 'N-ZA-Mn-za-m'

También podemos usar el cyberchef y usar la receta de ROT13

La contraseña es: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4