Ingeniería de la Ciberseguridad G81

PRÁCTICA 1: Password Cracking & ACLs

31-Octubre-2024

Prof: Antonio Nappa
Nombre del grupo: **GrupoAJA**

Alejandro Isla Álvarez (**100472228**)
József Iván Gafo(**100456709**)
Ángel Pérez Navas (**100472200**)

Level 1

Para descubrir el password del **level 1** hemos usado la fuerza bruta usando el siguiente comando "***john --mask='?1?1?1?1?1'' --1='abcdefg123456l' unshadow***", donde unshadow está el sha512 de level1, el alfabeto (**--1**) es la unión del charset="**abcdefg123456**" y de la palabra "**lab**" y la máscara especificamos que sea de 5 caracteres de longitud (poniendo 5 veces ?1). Al ejecutar este comando obtendremos la contraseña "**bg36l** ", y luego para obtener el flag debemos ejecutar el file "***./level1***", introduciendo la contraseña de level 1 y obtenemos la flag "**381be452224b8c433de45944645043aeb183eedda444b1c0157914e9b5d613f1**"

```
rover@44ff3f06c810:/hackme$ ./level1
Enter Password: bg36l
Correct! The flag is: 381be452224b8c433de45944645043aeb183eedda444b1c0157914e9b5d613f1
rover@44ff3f06c810:/hackme$
```

Level 2

Para el **level 2**, la palabra en la wordlist es "uc3m", por lo que modificamos nuestra wordlist y añadimos las letras "u" y "m" que son las que no tenemos en nuestra wordlist inicial. Ejecutamos el siguiente comando:

"john --mask='?1?1?1?1?1?1' --1='abcdefg123456um' unshadow"

Previamente en unshadow, guardamos la contraseña encriptada para seguidamente, ejecutarla desde la terminal usando el comando "john". Al realizar este proceso, obtenemos la siguiente contraseña: "**3bcfc5**"

Al introducir la contraseña en level 2, obtenemos finalmente la siguiente flag:

"**8175e45e05c9f26a57270a10258f744f7674b86d1256d9f9fa6b1b624135b85e**"

```
rover@44ff3f06c810:/hackme$ ./level2
Enter Password: 3bcfc5
Correct! The flag is: 8175e45e05c9f26a57270a10258f744f7674b86d1256d9f9fa6b1b624135b85e
rover@44ff3f06c810:/hackme$
```

Level 3

Para el **level 3**, usamos el siguiente comando en la terminal:

objdump -d level3 > level3.asm

Con este comando, somos capaces de ver el código assembly de level 3. Acto seguido, analizamos el código assembly, y vemos que en una parte del código, en la función main, se carga un valor en %rax, en concreto **0x6b6566766838743a**, este

valor hexadecimal se almacena en memoria en la dirección **-0x99(%rbp)**. Como estamos trabajando en little-endian, los bytes se ordenan de la siguiente manera:
3a 74 38 68 76 66 65 6b y los caracteres ASCII corresponden a los siguientes valores:
':' 't' '8' 'h' 'v' 'f' 'e' 'k', por lo que la cadena inicial es **:t8hvfek**
Luego se llama a la función 'decode_password' y dentro se realiza una operación donde a cada carácter se le resta 4 (**movzbl (%rax),%eax**, **lea -0x4(%rax),%ecx**, **mov %dl,(%rax)**).
Aplicando esta operación, tenemos lo siguiente:

Carácter inicial	Código ASCII	Código ASCII - 4	Carácter final
':'	58	54	'6'
't'	116	112	'p'
'8'	56	52	'4'
'h'	104	100	'd'
'v'	118	114	'r'
'f'	102	98	'b'
'e'	101	97	'a'
'k'	107	103	'g'

Por lo tanto, la contraseña final es **6p4drbag**, con la cual obtenemos el siguiente flag:
d44dc911d8e307c474e87c27560b1a37123eea4701d776ab0184132724eee901

```
rover@44ff3f06c810:/hackme$ ./level3
Enter Password: 6p4drbag
Correct! The flag is: d44dc911d8e307c474e87c27560b1a37123eea4701d776ab0184132724eee901
```

/challenge/flag.txt

Observamos en la ACL correspondiente que para acceder a la flag localizada en */challenge/flag.txt* los usuarios que tienen permiso de lectura son el propietario, el usuario admin, los miembros del grupo propietario y otros usuarios. El propietario es root, al cual no tenemos acceso, por lo que esa vía queda descartada, y root es el único usuario de su grupo. Podemos acceder con admin, cambiando a él con *su admin* y la contraseña *password*, la cual averiguamos fácilmente. *admin* tiene

permisos de lectura (r--), los cuales son efectivos al tener el ACL *mask::r--.* Con este usuario entramos en el archivo y encontramos tres flags correspondientes a level 7, 8 y 9:

88d4d9794572e6739332f662dc1403cc406e4291a7c027cc9fcf7ff846c4ead7
ee71cddc1acfd0be48f9fced4b0d8af06f29d5e09a5615db98ad615147789285
54bc2e28293fd4e88dcd60766b25d959abb834f699cef3ace3f0f6612ec83341

/projects/subproject/flag.txt

En este caso parece que podemos entrar con *student1*, que tiene permisos de lectura. Sin embargo, ningún usuario específico tiene acceso al directorio *projects*, aunque al tener este el ACL *other::r-x* cualquier otro usuario tiene acceso al directorio. Podemos entrar, por ejemplo, con *level1*, y, luego al subdirectorio *subproject* con el usuario *1004* o *student1*, aunque podemos seguir con *level1*. También con *level1* podemos acceder a las **flag** de **level 5** y **level 6**:

22ae3cdbc52c1c4e7ccb995914817c3654c1c201e9915b2411b69c65e5a00071
8391e901cad82fda5489a13d4366e3d40ceceedf58dc926bbe1850c73c284759

/secret/flag.txt

Podemos acceder también con ***admin***, que tiene acceso específico o incluso con **level1**, ya que en todos los ACL *other* tienen permisos de lectura. Obtenemos la flag para **level4**:

5f4a3fff2de065aae2e2a3a91fff5bdfeff3bdf912153706a4cdc24eb8c5c6c3