Universidad Carlos III

Ingeniería de la Ciberseguridad

Curso 2024-25

Práctica 1

Extracción de contraseñas para binarios y permisos en ACL's

Ingeniería Informática, Cuarto curso

Adrián Fernández Galán (NIA: 100472182, e-mail: 100472182@alumnos.uc3m.es)
César López Mantecón (NIA: 100472092, e-mail: 100472092@alumnos.uc3m.es)
Manuel Gómez-Plana Rodríguez (NIA: 100472092, e-mail: 100472092@alumnos.uc3m.es)

Prof . Antonio Nappa
Grupo: 81

Índice

1. Introducción

En este documento se recoge el proceso de desarrollo de la primera práctica de la asignatura *Ingeniería de la Ciberseguridad*. En esta práctica hemos logrado obtener 9 *flags* mediante el descubrimiento de contraseñas y ataque a archivos binarios.

2. Estrategias para el descubrimiento de contraseñas

Para extraer las contraseñas de los ejecutables se han empleado 2 estrategias distintas: uso de john the ripper para la obtención de contraseñas y ataque sobre los binarios.

2.1. John The Ripper

`John` es una herramienta para la optención de contraseñas débiles a partir de su *hash*. Dado el conocimiento que teníamos de las contraseñas hemos generado una *wordlist* con todas las contraseñas posibles con el alfabeto proporcionado. Esto se reduce a las permutaciones de 5, 6 y 8 elementos de los conjuntos de caracteres usados para generar cada contraseña.

Para generar la *wordlist* se ha empleado el siguiente código de *python*:

```python
import itertools

# charset level 1
charset_level1 = "abcdefg123456lab"

# Generate all permutations of length 5
permutations = itertools.permutations(charset_level1, 5)

with open("level1_wordlist.txt", "w+") as file:
    # Print the result
    for p in permutations:
        file.write(''.join(p) + "\n")

# charset level 2
charset_level2 = "abcdefg123456uc3m"

# Generate all permutations of length 6
permutations = itertools.permutations(charset_level2, 6)

with open("level2_wordlist.txt", "w+") as file:
    # Print the result
    for p in permutations:
        file.write(''.join(p) + "\n")

# charset level 3
charset_level3 = "abcdefg123456profe"

# Generate all permutations of length 8
permutations = itertools.permutations(charset_level3, 8)

with open("level3_wordlist.txt", "w+") as file:
    # Print the result
    for p in permutations:
        file.write(''.join(p) + "\n")
```

Sin embargo, no ha sido posible generar la *wordlist* para *level3* debido gran número de contraseñas posibles.

Gracias a estas *wordlist* hemos podido extraer las contraseñas para los archivos *level1* y *level2*. En la siguiente tabla se recogen los tiempos que ha llevado obtener cada contraseña:

Archivo	Longitud de la *wordlist*	Tiempo
level1	524160	53s
level2	8910720	383s
level3	1764322560	∞

Cuadro 1: Tiempos por contraseña usando *john*

Para el archivo *level3* no hemos empleado esta estategia debido al elevado tiempo de computación que precisa.

2.2. Análisis de binarios

2.3. Comparación de métodos

3. ACL's

4. Conclusión