Ejercicio de Seguridad
Solución

Sistemas Operativos

1er cuatrimestre 2023

1. Explicación resumida

Ataque: Hay un integer overflow, que a su vez genera un stack overflow, y eso termina derivando en una ejecución de código arbitrario con escalamiento de privilegios dado que se está utilizando setuid(0).

Explicación del código: Se inicializa un arreglo fmt, en cuya primera posición se pone el caracter " %". Luego se hace un scanf de un número de hasta 4 dígitos, y se lo guarda en la posición de memoria apuntada en fmt+1. Por ejemplo, si el número es 1025, fmt termina quedando " %1025" El resultado de atoi se está guardando en una variable de tipo unsigned char, cuyo máximo valor representable es 255, y en donde cualquier valor superior se va a truncar, resultando en el resto de dividir el valor por 256. En el caso anterior, $1025\,\%256 = 1$, por lo que la variable max_size termina valiendo 1. Usando este valor se inicializa un arreglo "clave" el cual va a ser utilizado para guardar la clave. En este caso el arreglo se iniciaría con tamaño 1+1=2. Luego se modifica fmt para agregar una "s" y el caracter nulo al final, que siguiendo con el ejemplo quedaría fmt=" %1025s". Finalmente se usa este valor como string de formato para scanf, guardando el input leído en el arreglo clave y limitando la lectura a 1025 caracteres. El problema es que en este caso a causa del integer overflow, scanf lee a lo sumo 1025 caracteres, pero clave solo tiene espacio para dos caracteres (uno de los cuales debe ser el caracter nulo); cualquier otro caracter escrito más allá del segundo caracter se encuentra por fuera del buffer. De este modo es posible pisar la dirección de retorno, logrando el objetivo del ejercicio.

2. Explicación detallada

(Pendiente...)