El Conjuro

Descripción

En la noche de Halloween, te enfrentas a un antiguo ritual prohibido: **El Conjuro de la Pila**. Este conjuro está dividido en cuatro partes y requiere de precisión y poder para ser c>

Cada vez que ingreses el símbolo correcto del conjuro, avanzarás al siguiente nivel. Pero cuidado, si fallas, el ritual se rompe y tendrás que empezar de nuevo.

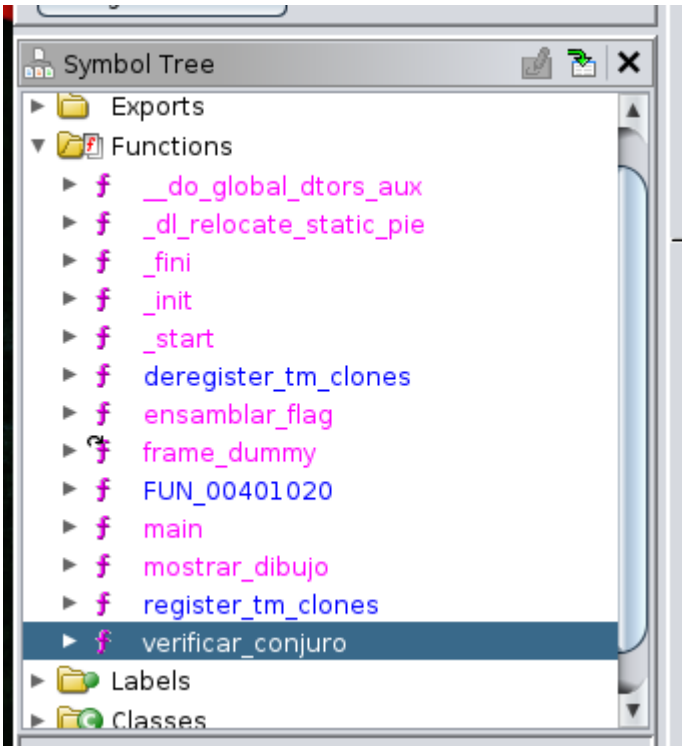
Desafío

Este reto desafía al usuario a descubrir un conjuro de cuatro partes en el orden correcto. Cada nivel pide una letra específica, y si el usuario ingresa el input correcto en cada nivel, pasará al siguiente hasta completar el ritual y revelar la flag final. Si el usuario se equivoca en cualquier nivel, el ritual falla y el programa termina.

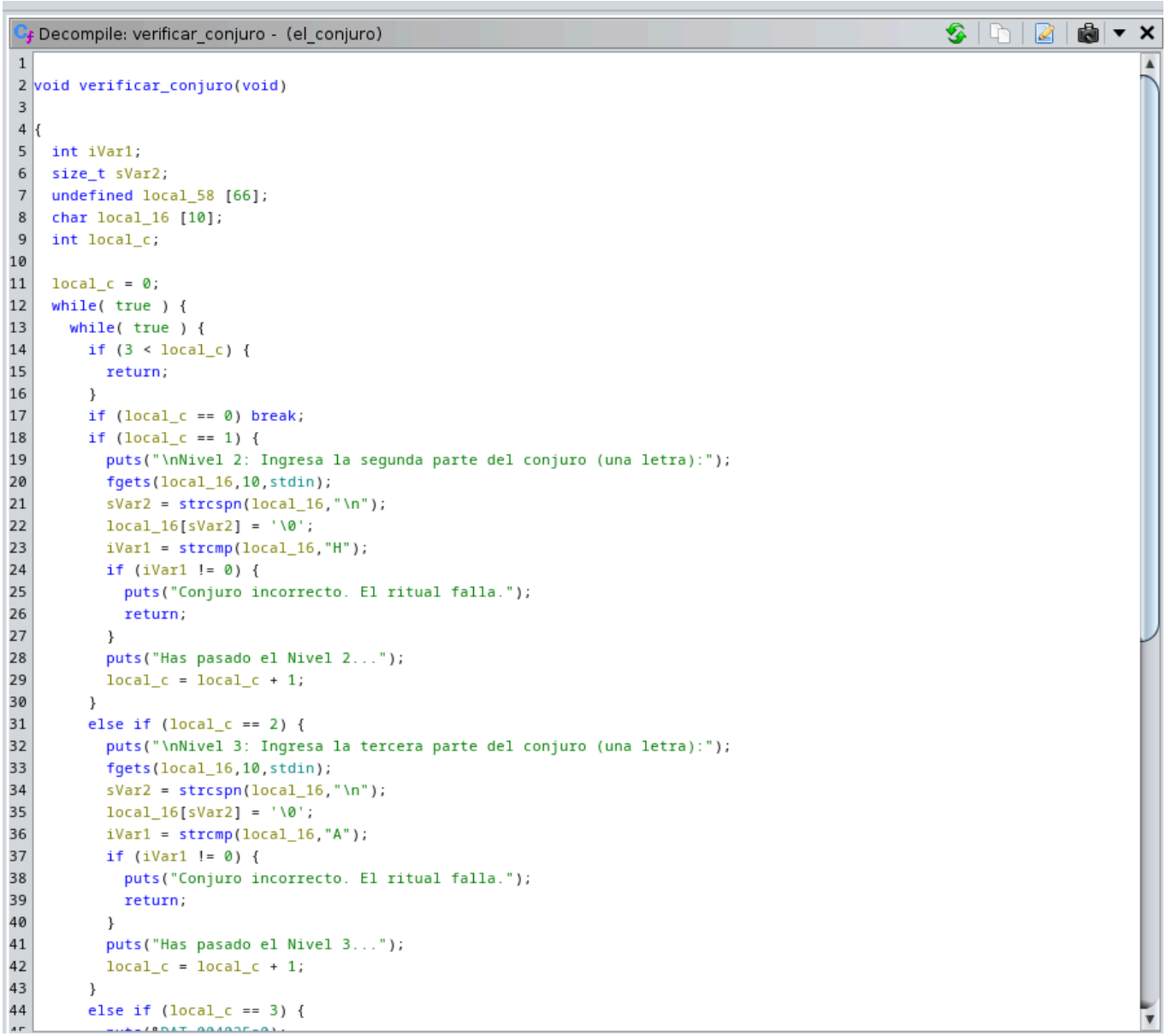
Solución

Ghidra

Usarémos la herramienta `Ghidra` para desensamblar el código y analizarlo a detalle, al entrar podemos acceder al apartado de `Symbol Tree` > `Functions`, ahí tendremos varias, sin embargo la más interesante es `verificar_conjuro`.



Con doble click podremos irnos directamente al apartado dónde se encuentra el código de esta validación.



Aquí el código completo:

```
void verificar_conjuro(void)

{
  int iVar1;
  size_t sVar2;
  undefined local_58 [66];
  char local_16 [10];
  int local_c;

  local_c = 0;
  while( true ) {
    while( true ) {
      if (3 < local_c) {
        return;
      }
```

```
    if (local_c == 0) break;
    if (local_c == 1) {
      puts("\nNivel 2: Ingresa la segunda parte del conjuro (una letra):");
      fgets(local_16,10,stdin);
      sVar2 = strcspn(local_16,"\n");
      local_16[sVar2] = '\0';
      iVar1 = strcmp(local_16,"H");
      if (iVar1 != 0) {
        puts("Conjuro incorrecto. El ritual falla.");
        return;
      }
      puts("Has pasado el Nivel 2...");
      local_c = local_c + 1;
    }
    else if (local_c == 2) {
      puts("\nNivel 3: Ingresa la tercera parte del conjuro (una letra):");
      fgets(local_16,10,stdin);
      sVar2 = strcspn(local_16,"\n");
      local_16[sVar2] = '\0';
      iVar1 = strcmp(local_16,"A");
      if (iVar1 != 0) {
        puts("Conjuro incorrecto. El ritual falla.");
        return;
      }
      puts("Has pasado el Nivel 3...");
      local_c = local_c + 1;
    }
    else if (local_c == 3) {
      puts(&DAT_004025a0);
      fgets(local_16,10,stdin);
      sVar2 = strcspn(local_16,"\n");
      local_16[sVar2] = '\0';
      iVar1 = strcmp(local_16,"U");
      if (iVar1 == 0) {
        ensamblar_flag(local_58);
        puts(&DAT_004025e0);
        printf(&DAT_0040261d,local_58);
      }
      else {
        puts("Conjuro incorrecto. El ritual falla.");
      }
      return;
    }
  }
  puts("\nNivel 1: Ingresa la primera parte del conjuro (una letra):");
  fgets(local_16,10,stdin);
```

```
    sVar2 = strcspn(local_16,"\n");
    local_16[sVar2] = '\0';
    iVar1 = strcmp(local_16,"A");
    if (iVar1 != 0) break;
    puts("Has pasado el Nivel 1...");
    local_c = local_c + 1;
  }
  puts("Conjuro incorrecto. El ritual falla.");
  return;
}
```

Análisis de la Función verificar_conjuro

Al analizar el código en Ghidra, podemos observar que la función `verificar_conjuro` utiliza un bucle `while(true)` que avanza a través de diferentes niveles, controlados por la variable `local_c`. La lógica está organizada en cuatro niveles consecutivos, y cada nivel requiere que el usuario ingrese una letra específica para avanzar.

Variables Clave

1. `local_c`: Esta variable se utiliza para llevar el conteo de los niveles. Comienza en 0 y se incrementa cada vez que el usuario pasa un nivel.
2. `local_16`: Un arreglo que guarda el input del usuario, leído con `fgets`.
3. `local_58`: Una variable de tipo `undefined` en la cual se almacena la flag cuando el usuario completa todos los niveles correctamente.

Desglose por Niveles

El análisis en Ghidra muestra que cada nivel de la función solicita una letra específica, la cual debe ingresarse en el orden correcto. Aquí tienes el análisis paso a paso:

Nivel 1: `local_c == 0`

Mensaje: El programa imprime:

```
Nivel 1: Ingresa la primera parte del conjuro (una letra):
```

Input esperado: El programa utiliza fgets para capturar el input en local_16, y lo compara con la letra `"A"`:

```
iVar1 = strcmp(local_16, "A");
```

Condición:
Si el input es `"A"`, el programa imprime:

```
Has pasado el Nivel 1...
```

Luego, `local_c` se incrementa a 1, y el programa pasa al Nivel 2.
Si el input no es `"A"`, el programa muestra:

```
Conjuro incorrecto. El ritual falla.
```

El ritual falla y el programa termina.

Nivel 2: `local_c == 1`

Mensaje: El programa imprime:

```
Nivel 2: Ingresa la segunda parte del conjuro (una letra):
```

Input esperado: Se captura en `local_16` y se compara con la letra `"H"`:

```
iVar1 = strcmp(local_16, "H");
```

Condición:
Si el input es `"H"`, el programa imprime:

```
Has pasado el Nivel 2...
```

Luego, `local_c` se incrementa a 2, y el programa pasa al Nivel 3.
Si el input no es `"H"`, el programa muestra:

```
Conjuro incorrecto. El ritual falla.
```

El ritual falla y el programa termina.

Nivel 3: `local_c == 2`

Mensaje: El programa imprime:

```
Nivel 3: Ingresa la tercera parte del conjuro (una letra):
```

Input esperado: Se captura en `local_16` y se compara con la letra `"A"`:

```
iVar1 = strcmp(local_16, "A");
```

Condición:
Si el input es `"A"`, el programa imprime:

```
Has pasado el Nivel 3...
```

Luego, `local_c` se incrementa a 3, y el programa pasa al Nivel 4.
Si el input no es `"A"`, el programa muestra:

```
Conjuro incorrecto. El ritual falla.
```

El ritual falla y el programa termina.

Nivel 4: `local_c == 3`

Mensaje: El programa imprime:

```
Nivel 4: Ingresa la última parte del conjuro (una letra):
```

Input esperado: Se captura en `local_16` y se compara con la letra `"U"`:

```
iVar1 = strcmp(local_16, "U");
```

Condición:
Si el input es `"U"`, se llama a la función `ensamblar_flag(local_58)`, que ensambla y muestra la flag.
El mensaje final es:

```
¡Has completado el conjuro y liberado el secreto prohibido!
Aquí está tu flag: ShByte{c0njur4nd0_c0n_gh1dr4_3n_sh4d0w33n}
```

Si el input no es `"U"`, el programa muestra:

```
Conjuro incorrecto. El ritual falla.
```

Ejecución Paso a Paso

Para completar el reto, el usuario debe ingresar la secuencia exacta de letras en cada nivel. La secuencia correcta es: `A`, `H`, `A`, `U`. Si se sigue esta secuencia, el conjuro se completará y se mostrará la flag.

¡Has completado el conjuro y liberado el secreto prohibido!
Aquí está tu flag: ShByte{c0njur4nd0_c0n_gh1dr4_3n_sh4d0w33n}