Ejemplo de exploit

principal.c

[crayon-6a9d505b8c1d2598220531/]

vuln2.c

[crayon-6a9d505b8c1d8911866089/]

Aquí hay un resumen general del código

1. **Shellcode**: Contiene instrucciones de ensamblador en hexadecimal que representan el código máquina para ejecutar /bin/sh, que es la shell en sistemas Linux.
2. **Main Function**:
3. **Buffer Allocation**:
4. **Cálculo de la Dirección de Retorno**:
5. **Llenado del Buffer**:
6. **Finalización del Buffer**:
7. **Ejecución del Programa Vulnerable**:

Este código está diseñado para ilustrar cómo podría ser explotada una vulnerabilidad de desbordamiento de búfer para ejecutar código arbitrario.