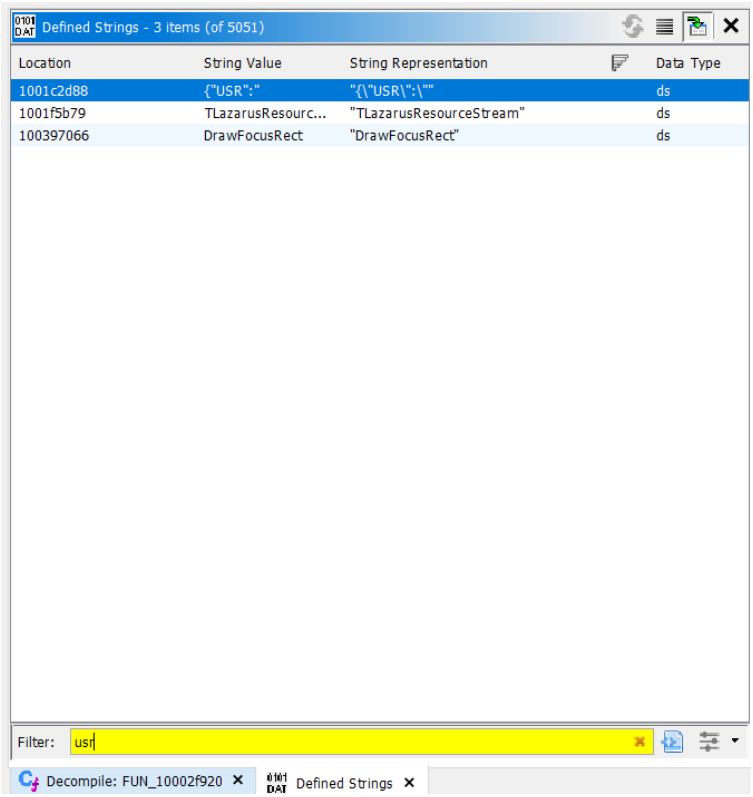
DOCUMENTACIÓN DE PARCHE

Kevin Jacobo Hernández

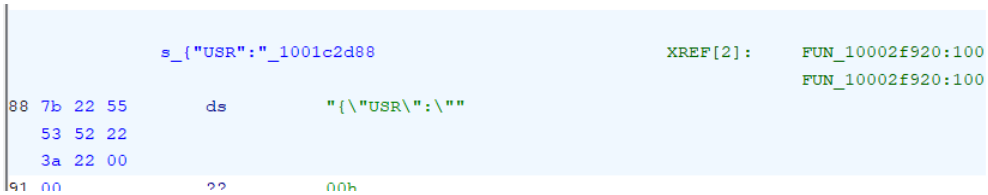
Danilo Romualdo Cruz

Anayeli Rodríguez Zepeda

En el Defined String buscamos el string de USR y nos va a redirección de código ensamblador

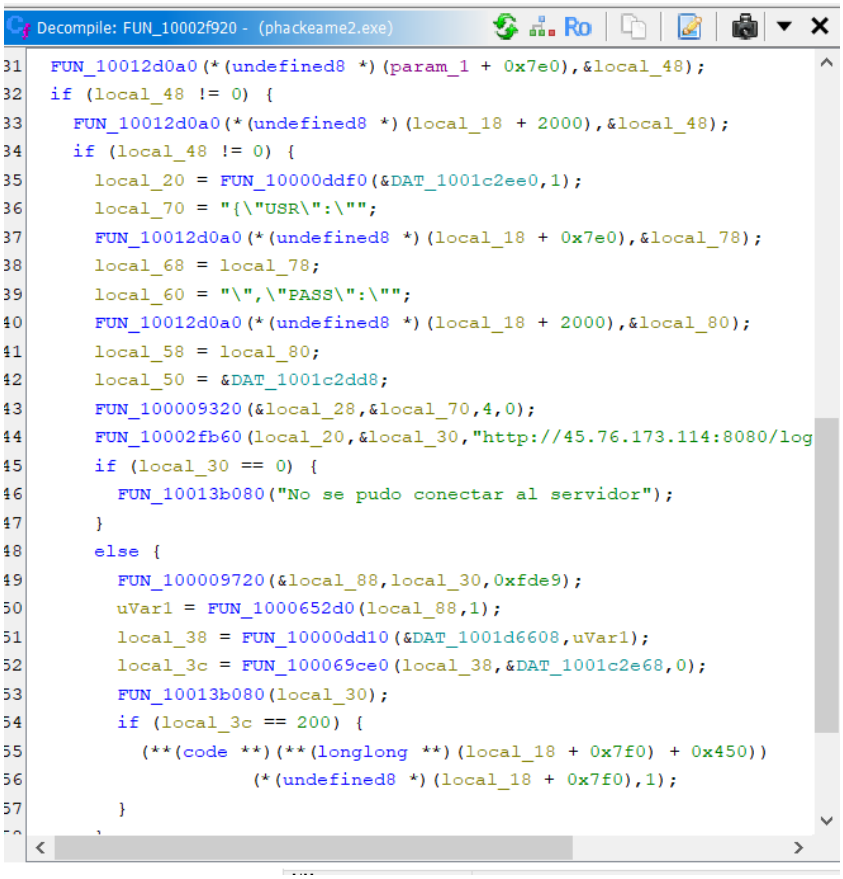


Vamos a darle click en el FUN_1002f920

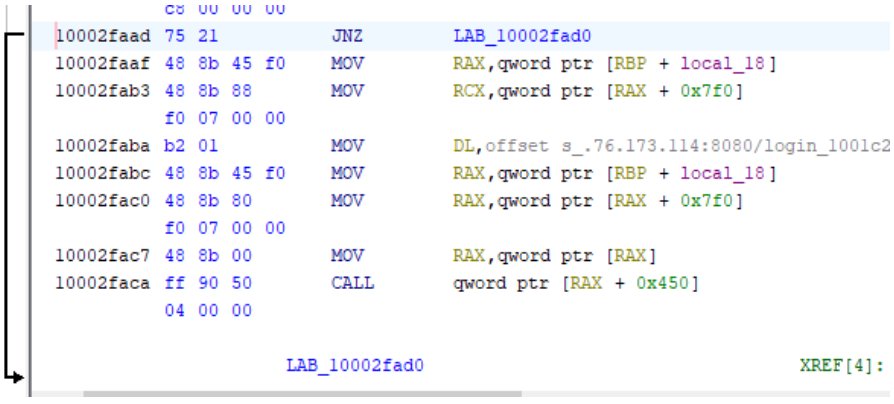


En el apartado de descompile tenemos lo siguiente:

Y vamos a ir la línea 54, vamos a darle click y tenemos al if y nos devolvemos al apartado de ensamblador



Al darle click vemos que nos redirecciona a esta línea en el ensamblador, por lo que tenemos que cambiar ese JNZ LAB_10002fad0 por un No operation y por lo que quedaría de este código:



A este:

Por lo que ya no va existir esa comparación en el código gracias al NOP

```
10002faad 48 90          NOP
10002faaf 48 8b 45 f0    MOV        RAX,qword ptr [RBP + local_18]
10002fab3 48 8b 88       MOV        RCX,qword ptr [RAX + 0x7f0]
          f0 07 00 00
10002faba b2 01          MOV        DL,offset s_.76.173.114:8080/login_1001c2
10002fabc 48 8b 45 f0    MOV        RAX,qword ptr [RBP + local_18]
10002fac0 48 8b 80       MOV        RAX,qword ptr [RAX + 0x7f0]
          f0 07 00 00
10002fac7 48 8b 00       MOV        RAX,qword ptr [RAX]
10002faca ff 90 50       CALL       qword ptr [RAX + 0x450]
          04 00 00
```

Resultados del Decompiler:

```
if (local_30 == 0) {
  FUN_10013b080("No se pudo conectar al servidor");
}
else {
  FUN_100009720(&local_88,local_30,0xfde9);
  uVar1 = FUN_1000652d0(local_88,1);
  local_38 = FUN_10000dd10(&DAT_1001d6608,uVar1);
  local_3c = FUN_100069ce0(local_38,&DAT_1001c2e68,0);
  FUN_10013b080(local_30);
  (**(code **)(**(longlong **)(local_18 + 0x7f0) + 0x450))
            (*(undefined8 *)(local_18 + 0x7f0),1);
}
```

Al parchearlo de esa manera tenemos que dando igual el usuario y contraseña estaremos entrando al botón de “Presióname”.