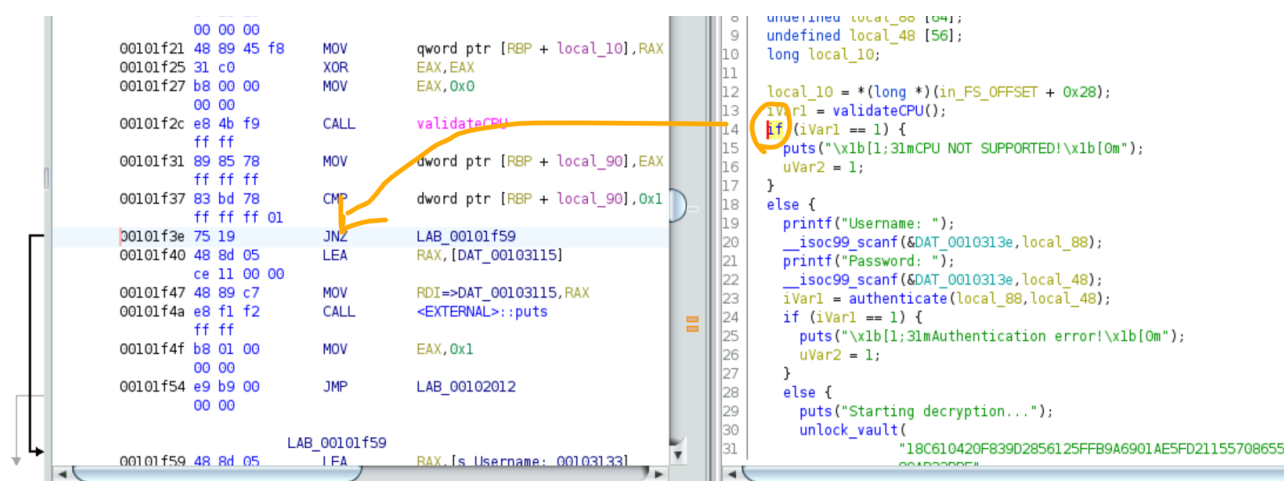


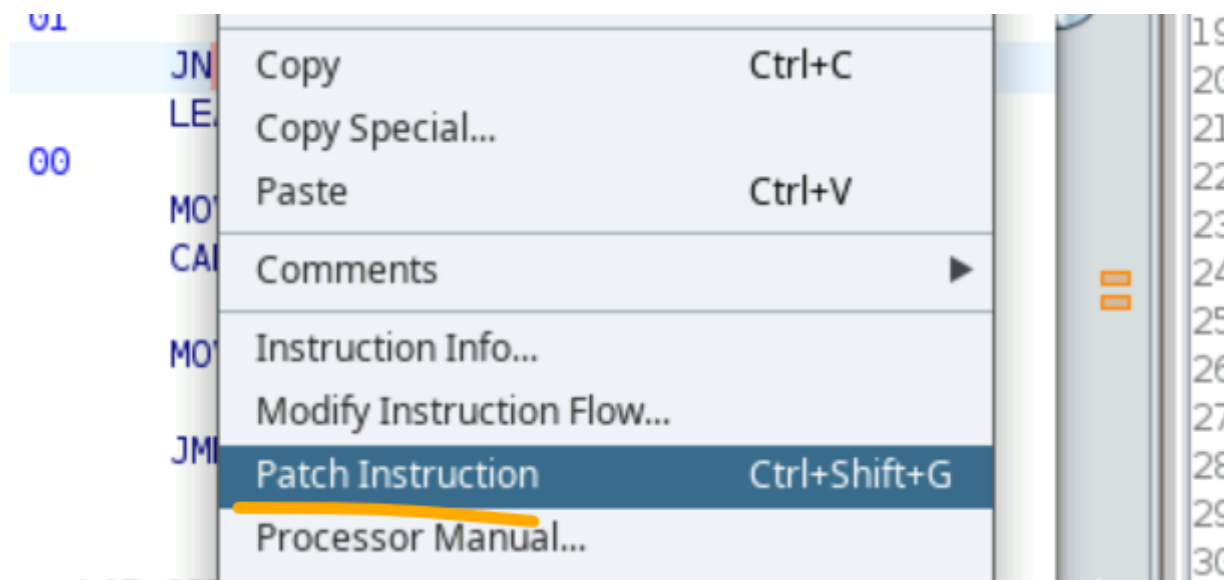
Patching

其实就是通过更改判断条件的汇编代码，使得改变程序的control flow，让它bypass各种判断限制。

```
root@kali:~/Desktop# ./target
CPU NOT SUPPORTED!
root@kali:~/Desktop#
```



可以修改汇编码，比如JNZ 改为 JZ。



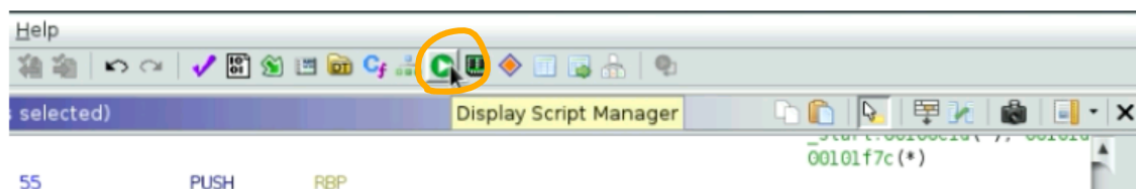
CALL	validateCPU	13	local_10 = validateCPU();
MOV	dword ptr [RBP + local_90],EAX	14	iVar1 = validateCPU();
CMP	dword ptr [RBP + local_90],0x1	15	if (iVar1 == 1) {
JZ	LAB_00101f59	16	printf("Username: ");
LEA	RAX,[DAT_00103115]	17	_isoc99_scanf(&DAT_0010313e,local_88);
MOV	RDI=>DAT_00103115,RAX	18	printf("Password: ");
CALL	<EXTERNAL>::puts	19	_isoc99_scanf(&DAT_0010313e,local_48);
		20	iVar1 = authenticate(local_88,local_48);
		21	if (iVar1 == 1) {
		22	puts("\x1b[1;31mAuthentication error!\n");
		23	uVar2 = 1;
		24	}

更改完后，highlight它，然后按script manager，找savePatch.py.

In order to save the patch you've made, **highlight** the specific instructions you changed:



Then open the **Script Manager** by clicking on the green play icon on the toolbar:

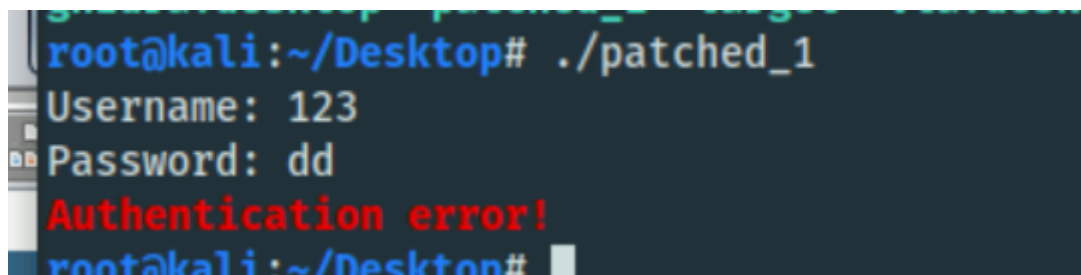


Search for the **SavePatch.py** script and double-click on the result to run the script:

SavePatch 是一个plugin，允许你manually control the changes exported.

Note: While Ghidra does allow exporting binaries from the **File > Export Program** menu, it not only saves the changed instructions but also any automatic changes made when the project was originally imported and analyzed, meaning you are likely to get a non-working binary as a result. Therefore, it is better to use the **SavePatch** plugin which allows you to manually control the changes exported. This plugin has already been installed for you.

这个时候允许你修改的文件，就不是CPU Warning了。



第二个patch

highlight第二个patch.

Due to the way the **SavePatch** script works, it will not remember any previous patches. So, only selecting this change is not enough. This would leave the previous change unsaved (though the authentication check would be bypassed, the CPU check would not be bypassed). You could import the previously patched binary into Ghidra and analyze and patch it then, but this approach can be too time-consuming.

Instead, you can **highlight both of your patches** at once and then use the **SavePatch** script to apply the changes. You have to highlight the whole memory range between the patches – just highlighting the changed lines individually won't work. You can use the black markers on the side to find the changes you've made.

After you have selected both instructions, run the **SavePatch** script and save the binary to

`/root/Desktop/patched_2`.

The screenshot displays the Ghidra IDE interface. On the left, the assembly view shows instructions for the 'main' function, with addresses 00101fd7 to 00101fd9 highlighted. The decompiled code on the right shows the corresponding C-like code, with the authentication logic highlighted. The Script Manager at the bottom lists various scripts, with 'SavePatch.py' selected and checked.

```
00101fd7 75 16 JNZ LAB_00101fef
00101fd9 48 8d 05 LEA RAX, [DAT_00103150]
00101fe0 48 89 c7 MOV RDI=>DAT_00103150, RAX
00101fe3 e8 58 f2 CALL <EXTERNAL>::puts
00101fe8 b8 01 00 MOV EAX, 0x1
00101fe9 00 00 JMP LAB_00103013
```

```
18  __isoc99_scanf(&DAT_0010313e, local_48);
19  iVar1 = authenticate(local_88, local_48);
20  if (iVar1 == 1) {
21  puts("\x1b[1;31mAuthentication error!\x1b[0m");
22  uVar2 = 1;
23  }
24  else {
25  puts("Starting decryption...");
26  unlock_vault(
```

In Tool	Status	Name	Description	Key	Category	Modified
<input type="checkbox"/>		AskScript.java	An example of asking for user input. Not...		Examples	08/04/2021
<input type="checkbox"/>		AskScriptPy.py	An example of asking for user input. Not...		Examples->Py...	08/04/2021
<input type="checkbox"/>		AutoVersionTrackingScript.java	An example of how to create Version Tr...		Examples->V...	08/04/2021
<input type="checkbox"/>		CountAndSaveStrings.java	Counts the number of defined strings in ...		CustomerSub...	08/04/2021
<input type="checkbox"/>		CreateAppliedExactMatchingSessionScr...	An example of how to create Version Tr...		Examples->V...	08/04/2021
<input type="checkbox"/>		OpenVersionTrackingSessionScript.java	An example of how to open an existing ...		Examples->V...	08/04/2021
<input checked="" type="checkbox"/>		SavePatch.py	Write the selected memory (including p...		Memory	04/15/2025

选完savePatch后，按右上角的开始按钮，保存Patch。

```
ghidra.desktop patched_1 patched_2 target vta.desktop
root@kali:~/Desktop# ./patched_2
Username: d
Password: d
Starting decryption...
Vault contents:
the flag is: c8653486d60b3401ec4bd0a69bfe3eac
root@kali:~/Desktop#
```