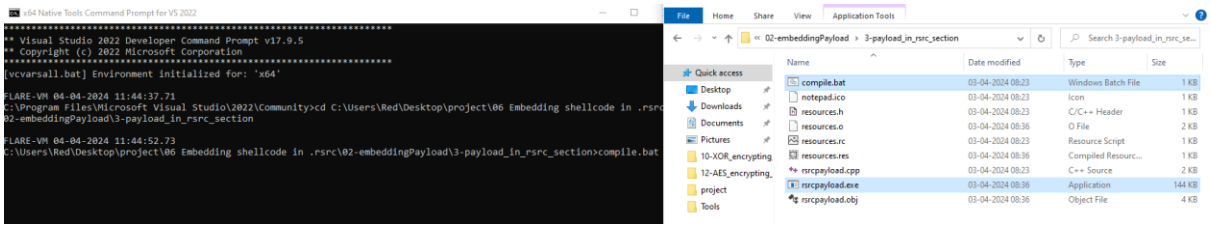
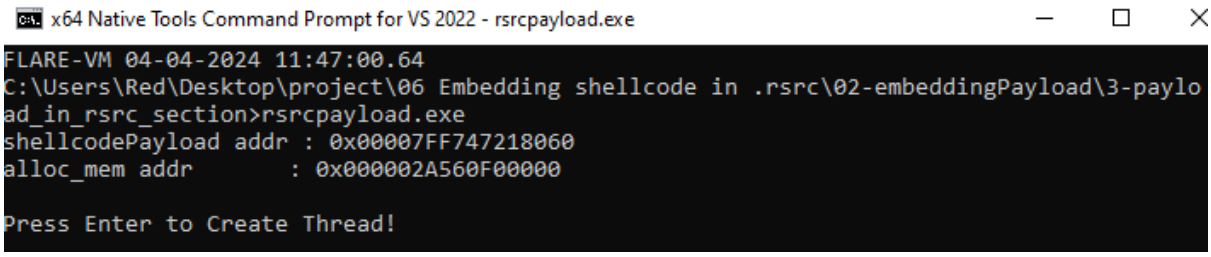
Analyzing Shellcode embedded in .rsrc section, with xdbg

First, run the compile.bat file in native cmd and get a .exe file.



Then execute the .exe file:

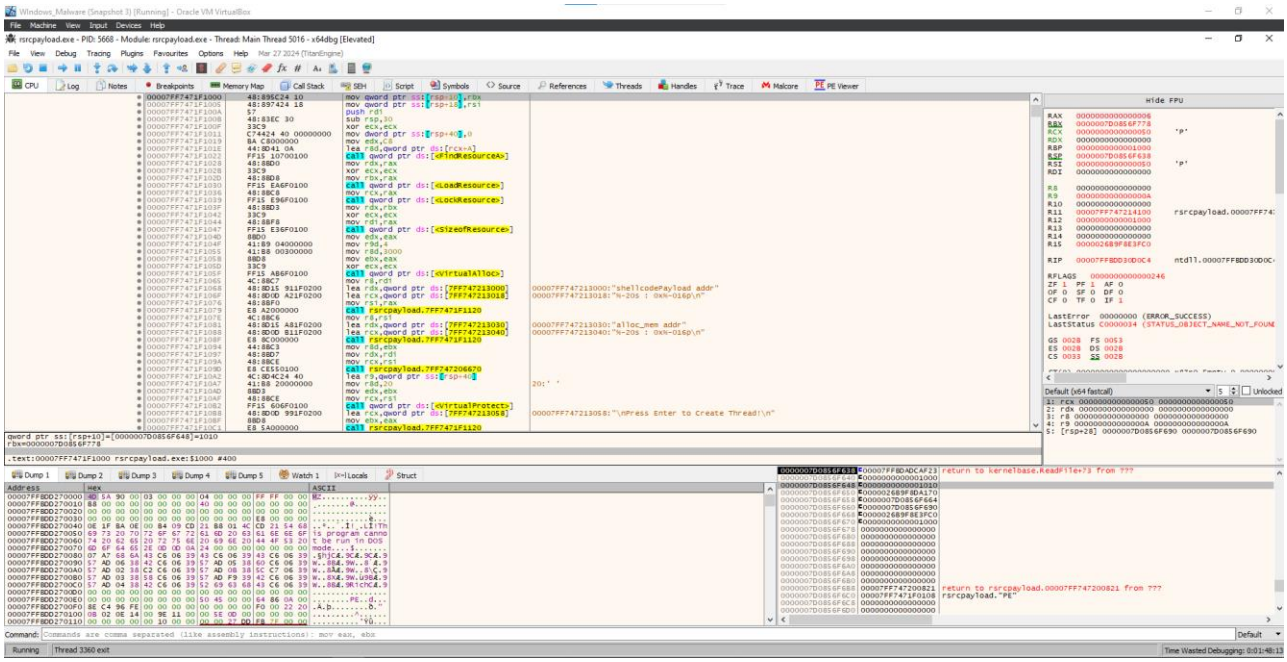


As we can see we got the shellcodePayload address, and the allocated shellcode address.

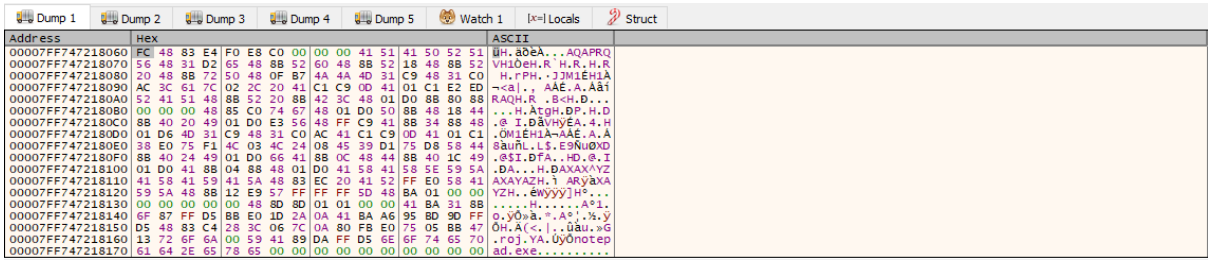
So now we will open the xdbg, to analyze the .exe file, these are the steps you need to follow initially before analyzing the file:

1. First open xdbg, then in the file section, attach the .exe file, which you are running.
2. Then in the symbols section, double-click on the .exe file which you are currently running, then run the program, to sync.
3. Now you are ready to analyze the program.

Here's how the xdbg will look like after you follow each step:



So, now we will go to each shellcodePayload memory in the dump part, and we can see our payload here:



Address	Hex	ASCII
00007FF747218060	FC 48 83 E4 F0 E8 C0 00 00 00 41 51 41 50 52 51	üH.ðèÀ...AQAPRQ
00007FF747218070	56 48 31 D2 65 48 8B 52 60 48 8B 52 18 48 8B 52	VH1ÒeH.R`H.R.H.R
00007FF747218080	20 48 8B 72 50 48 0F B7 4A 4A 4D 31 C9 48 31 C0	H.rPH.·JJM1ÉH1À
00007FF747218090	AC 3C 61 7C 02 2C 20 41 C1 C9 0D 41 01 C1 E2 ED	¬<a|., AÁÉ.A.Áâí
00007FF7472180A0	52 41 51 48 8B 52 20 8B 42 3C 48 01 D0 8B 80 88	RAQH.R .B<H.Ð...
00007FF7472180B0	00 00 00 48 85 C0 74 67 48 01 D0 50 8B 48 18 44	...H.ÀtgH.ÐP.H.D
00007FF7472180C0	8B 40 20 49 01 D0 E3 56 48 FF C9 41 8B 34 88 48	.@ I.ÐãVHÿÉA.4.H
00007FF7472180D0	01 D6 4D 31 C9 48 31 C0 AC 41 C1 C9 0D 41 01 C1	.ÖM1ÉH1À¬AÁÉ.A.Á
00007FF7472180E0	38 E0 75 F1 4C 03 4C 24 08 45 39 D1 75 D8 58 44	8àuñL.L$.E9ÑuØXD
00007FF7472180F0	8B 40 24 49 01 D0 66 41 8B 0C 48 44 8B 40 1C 49	.@$I.ÐfA..HD.@.I
00007FF747218100	01 D0 41 8B 04 88 48 01 D0 41 58 41 58 5E 59 5A	.ÐA...H.ÐAXAX^YZ
00007FF747218110	41 58 41 59 41 5A 48 83 EC 20 41 52 FF E0 58 41	AXAYAZH.ì ARÿàXA
00007FF747218120	59 5A 48 8B 12 E9 57 FF FF FF 5D 48 BA 01 00 00	YZH..éWÿÿÿ]Hº...
00007FF747218130	00 00 00 00 00 48 8D 8D 01 01 00 00 41 BA 31 8B	.....H......Aº1.
00007FF747218140	6F 87 FF D5 BB E0 1D 2A 0A 41 BA A6 95 BD 9D FF	o.ÿÕ»à.*.Aº¦.½.ÿ
00007FF747218150	D5 48 83 C4 28 3C 06 7C 0A 80 FB E0 75 05 BB 47	ÕH.Ä(<.|..ûàu.»G
00007FF747218160	13 72 6F 6A 00 59 41 89 DA FF D5 6E 6F 74 65 70	.roj.YA.ÚÿÕnotep
00007FF747218170	61 64 2E 65 78 65 00 00 00 00 00 00 00 00 00 00	ad.exe..........

And we can see here in Dump1 that it is ending with notepad.exe, which is our shellcode

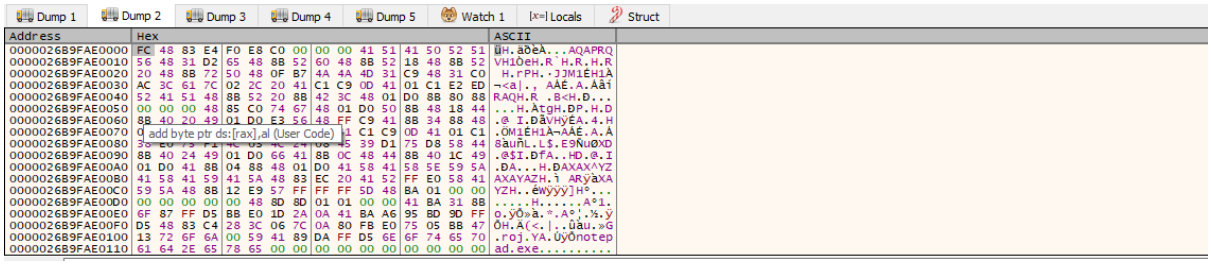
Even in the Memory Map part, we can find the shellcode payload memory and can see under the info column, we can see it is as ".rsrc"

00007FF747218000	0000000000001000	User	".rsrc"		IMG	-RWC-	ERWC-

And for the allocated memory, we can see in the Memory Map, initially the Protection was just read and written, and now it is read and executed.

0000026B9FAE0000	0000000000001000	User			PRV	ER---	-RW--

We can even follow the allocated memory in the dump section.



Now when we press enter in the cmd, the program gets terminated, and we can see Notepad is open.