BasicAVR writeup

Start with getting to know the achitecture of the elf

`strings BasicAVR.elf | grep atmega`

its atmega2560 based on avr8

now getting the hex of elf using

`avr-objcopy -O ihex -R .eeprom BasicAVR.elf BasicAVR.hex`

I will emulate the program with avr studio 4 and hapsim (both are deprecated)

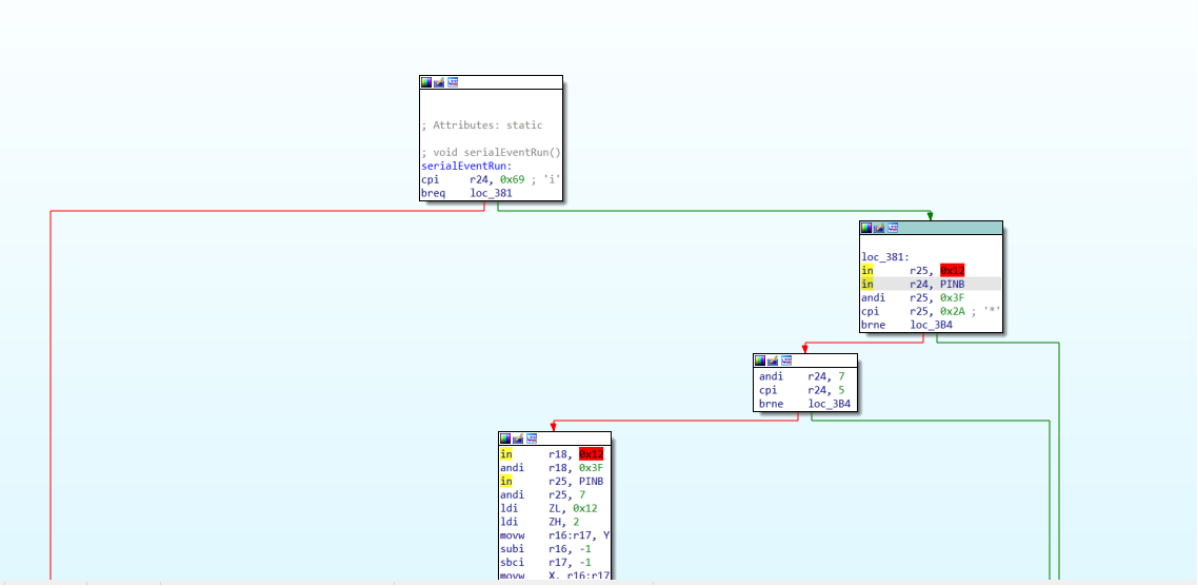
```
Unite2024 Initialized. Patch ELF and Configure port pins corectly. iykyk :)

Unpatched ELF :< NO Run

Unpatched ELF :< NO Run

Unpatched ELF :<
```

We need to patch it ig.

opening the elf in decompiler and searching for terms like port and pin i got

Address	Function	Instruction
.text:00000083	__RESET	
.text:00000382	serialEventRun	in r24, PINB
.text:0000038B	serialEventRun	in r25, PINB
LOAD:000006DB		aTPinsCorrectly:.db "t pins correctly. iykyk :))",0

going to the `serialEventRun` function



we are interested in the PINB instructions part, there we will invert the if statement here.

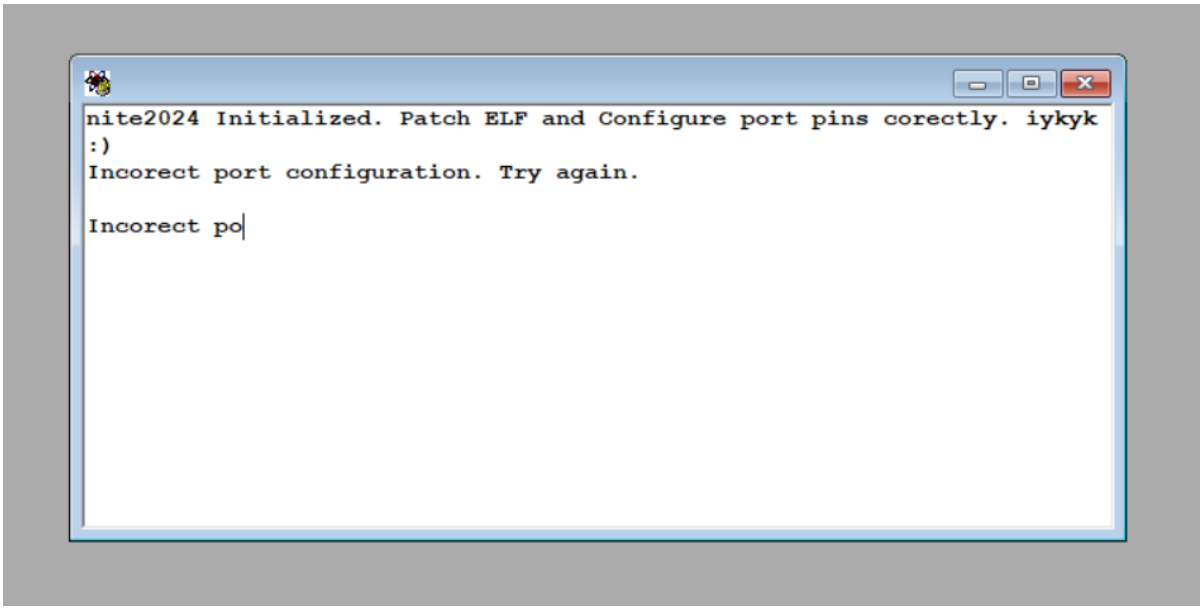
now first reading about breq and brne from the datasheet [AVR® Instruction Set Manual]

I have to set 2 bit of 2 byte of breq to 1 to invert it to brne

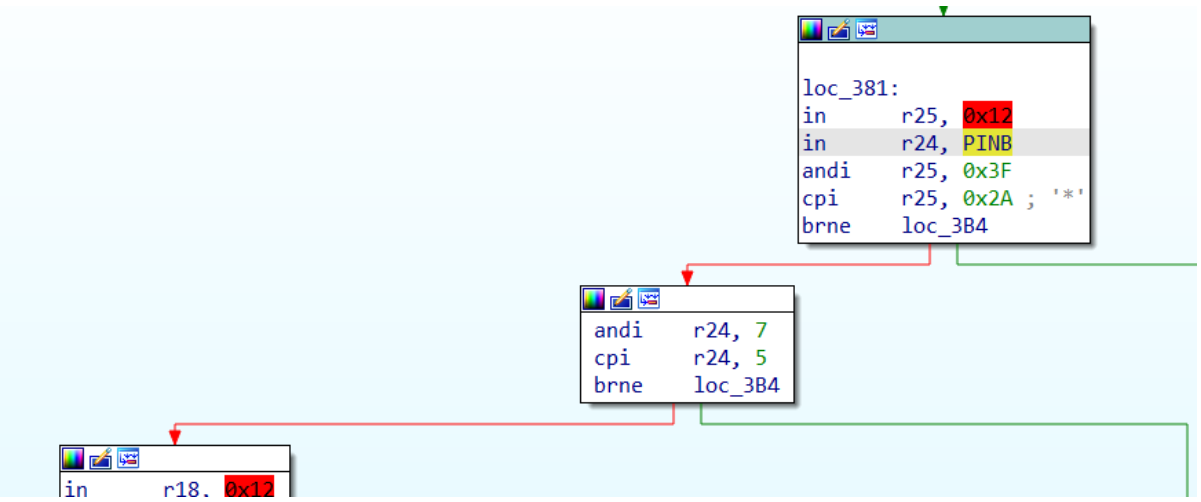
```
70  9180 0060 3689 F469 E78E E092 940E 01F7  92FF 92EF 940E 03EE 900F 900F 940E 01B9
80  CFEF B392 B183 739F 329A F571 7087 3085  F559 B322 732F B193 7097 E1E2 E0F2 018E
90  5F0F 4F1F 01D8 252B 259A 9181 2782 9582  2789 938D 16CE 06DF F7C1 ED80 E092 940E
A0  01EA 0148 E18C 0E88 1C91 01F8 9161 018F  EE81 E092 940E 014C 1508 0519 F7B1 E28E
B0  E092 940E 01EA CFCA EA87 E092 940E 01F7  CFC5 EEE1 E0F2 8213 8212 EE88 E093 E0A0
C0  E0B0 8384 8395 83A6 83B7 E084 E092 8391  8380 EC85 E090 8795 8784 EC84 E090 8797
D0  8786 EC80 E090 8B91 8B80 EC81 E090 8B93  8B82 EC82 E090 8B95 8B84 EC86 E090 8B97
E0  8B86 8E11 8E12 8E13 8E14 9508 0FEE 1FFF  1F88 BF8B 9007 91F6 2DE0 9419 93CF 93DF
F0  B7CD B7DE 01AE 5F4A 4F5F 01FA 9161 9171  01AF 9180 0380 9190 0381 940E 0402 91DF
00  91CF 9508 922F 923F 924F 925F 926F 927F  928F 929F 92AF 92BF 92CF 92DF 92EF 92FF
10  930F 931F 93CF 93DF D000 D000 D000 921F  921F B7CD B7DE 017C 013B 018A 01FC 8217
```

F069 to F469

after this i ran the program again and looked into the serial output



ok we one step ahead



now for the ports , refer to [ATmega640/1280/1281/2560/2561 datasheet]

but important stuff for this challenge

Initial Value	0	0	0	0	0	0	0	0

13.4.22 PING – Port G Input Pins Address

Bit	7	6	5	4	3	2	1	0	
0x12 (0x32)	–	–	PING5	PING4	PING3	PING2	PING1	PING0	PING
Read/Write	R	R	R/W	R/W	R/W	R/W	R/W	R/W	
Initial Value	0	0	N/A	N/A	N/A	N/A	N/A	N/A	

13.4.23 PORTH – Port H Data Register

PING is 0x12

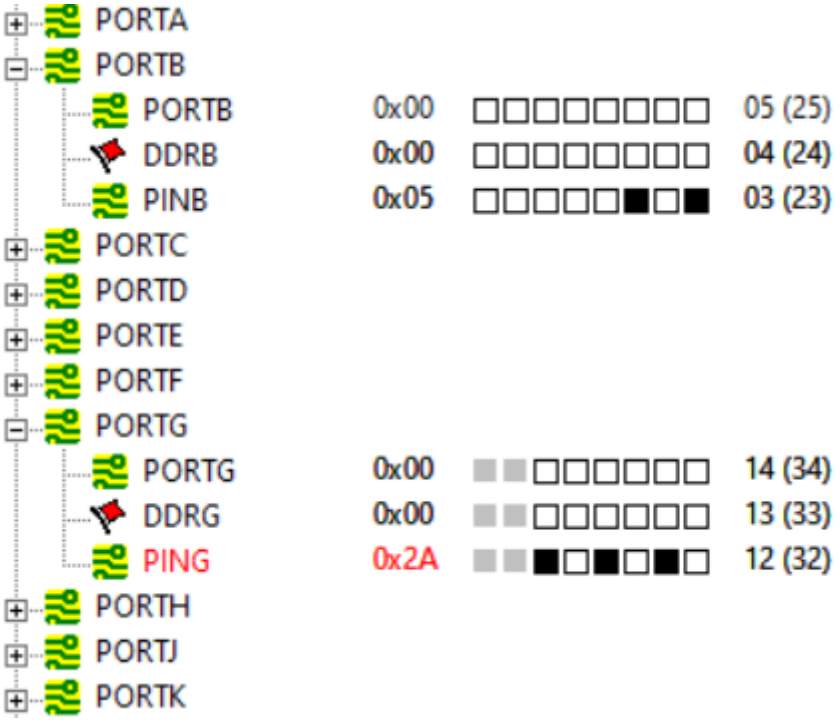
we already know PINB

now looking at the instructions it looks like we need

PING = 0x2A

PINB = 0x5

we can manipulate pins in avr studio 4 lets do that



after this i ran the program again

and here is the flag