

```
public class Puzzle3 {  
  
    public static void main(String[] args) {  
        // find and print NOP  
        for(byte b = Byte.MIN_VALUE; b < Byte.MAX_VALUE; b++) {  
            if(b == 0x90) {  
                System.out.print("Found: 0x90 NOP byte");  
            }  
        }  
    }  
}
```

Group Formation

- Count off 1 to 4

Problem 1 (15 minutes)

- Discuss Part C
 - Described exploit file structure
 - Discuss strategies to determine EIP offset and value
- Discuss Part D/E
 - Why is setuid(0) shellcode addition required?
- Discuss Part F/G/H
 - What are these counter-measures and can they be bypassed?

Problem 2 (15 minutes)

- Discuss strategy to exploit MiniShare
 - Follow Up: How to exfiltrate flag?