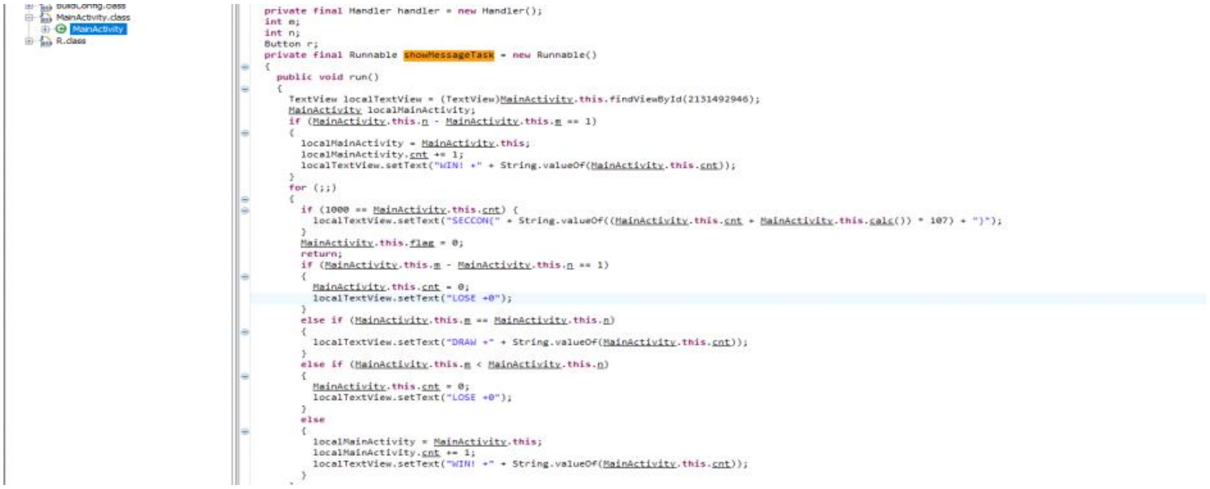
SECCON 2015 – CTF [Jeopardy]

Monday, July 22, 2019   1:38 AM

1. Decompile the apk
2. Convert dex to jar to show application code.
3. Now open jar file you see there is a activity named: MainActivity.class

All code is written in mainactivity.class
There are three button and three text view

We got an interesting method :



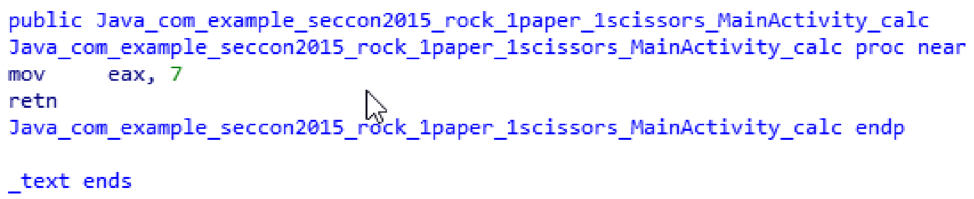
```
private final Handler handler = new Handler();
int m;
int n;
Button r;
private final Runnable showMessageTask = new Runnable()
{
  public void run()
  {
    TextView localTextView = (TextView)MainActivity.this.findViewById(2131492946);
    MainActivity localMainActivity;
    if (MainActivity.this.n - MainActivity.this.m == 1)
    {
      localMainActivity = MainActivity.this;
      localMainActivity.cnt += 1;
      localTextView.setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
    }
    for (;;)
    {
      if (1000 == MainActivity.this.cnt) {
        localTextView.setText("SECCON{" + String.valueOf((MainActivity.this.cnt + MainActivity.this.calc()) * 107) + "}");
      }
      MainActivity.this.flag = 0;
      return;
      if (MainActivity.this.m - MainActivity.this.n == 1)
      {
        MainActivity.this.cnt = 0;
        localTextView.setText("LOSE +0");
      }
      else if (MainActivity.this.m == MainActivity.this.n)
      {
        localTextView.setText("DRAW +" + String.valueOf(MainActivity.this.cnt));
      }
      else if (MainActivity.this.m < MainActivity.this.n)
      {
        MainActivity.this.cnt = 0;
        localTextView.setText("LOSE +0");
      }
      else
      {
        localMainActivity = MainActivity.this;
        localMainActivity.cnt += 1;
        localTextView.setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
      }
```

You got an condition statement :

if (1000 == MainActivity.this.cnt) {
    localTextView.setText("SECCON{" + String.valueOf((MainActivity.this.cnt + MainActivity.this.calc()) * 107) + "}");

From above method you see MainActivity.this.cnt =1000 because flag is shown when (1000 == MainActivity.this.cnt)

2. And another calc() method is called which is defined in native library.
3. No open libcalc.so in ida pro
4. And analyze



```
public Java_com_example_seccon2015_rock_1paper_1scissors_MainActivity_calc
Java_com_example_seccon2015_rock_1paper_1scissors_MainActivity_calc proc near
mov     eax, 7
retn
Java_com_example_seccon2015_rock_1paper_1scissors_MainActivity_calc endp

_text ends
```

5. From above code . It return 7.
6. Now flag is:

SECCON{(1000+7)*107}