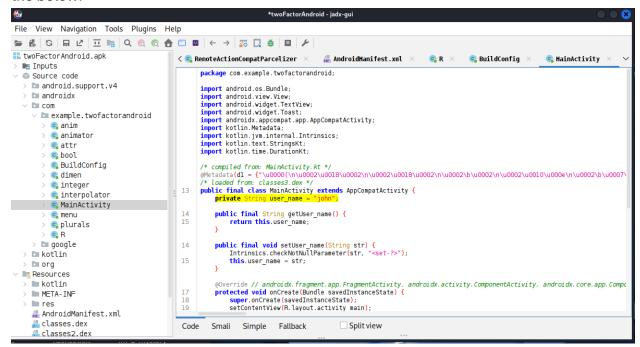
StudentID: 6A5723ED

Challenge: Two Factor Android

Date: 4/7/2025

Challenge Solution:

- 1. The challenge provides two links. One to an Android .apk file, and another to a 2FA portal that looks like it will be more useful after we understand the app.
- 2. Dropped the twoFactorAndroid.apk file into Kali
- 3. Ran "sudo apt install jadx"; JADx is a tool for pulling apart and analyzing .apk files, which is exactly what is needed here.
- 4. "./bin/jadx-gui" opens up a nice GUI for us to analyze the apk with; much easier to understand than a command line in a case like this.
- 5. Opened twoFactorAndriod.apk using JADx GUI.
- 6. It seems like the majority of the interesting Java code behind this app is in *Source Code/com/example.twofactorandroid/MainActivity* directory. This is where we find the below:



- 7. So we have a hardcoded variable, user_name, set equal to john
- 8. Further down, we have some logic that appears to be generating the 2FA keys, but it looks like it relies on the username to do some math, which creates a chance for us

to pivot from this version, which gives us John's 2FA codes to the Admin account.

```
File View Navigation Tools Plugins Help
를 뽑 G 및 단 호 및 Q @ @ 合 □ ■ ← → 등 및 및 표 및 F
twoFactorAndroid.apk

⟨ ¶ RemoteActionCompatParcelizer × 

                                                                                                                         # AndroidManifest.xml
                                                                                                                                                                                  BuildConfig
                                                                                                                                                                                                                 MainActivity
> Mmm Inputs
                                                                              public final void setUser_name(String str) {
    Intrinsics.checkNotNullParameter(str, "<set-?>");
                                                                 14
Source code
   > mandroid.support.v4
                                                                 15
   > 🖿 androidx
                                                                              @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.Compo
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity.main);
    TextView welcomeViev = (TextView) findViewById(R.id.textView_welcome);
    welcomeView.setText("Welcome" + this.user_name + '!');
}

∨ ■ example.twofactorandroid

                                                                 17
18
19
20
              🕵 anim
             animator
              attr 👊
              c bool
              BuildConfig
                                                                 24
                                                                              public final void gen_code(View view) {
   Intrinsics.checkNotNullParameter(view, "view");
   Toast toast = Toast.makeText(getApplicationContext(), do_math(this.user_name), 0);
   text toat().
             dimen
           > 🔍 integer
              interpolator
           > 🥵 MainActivity
               🧠 menu
                                                                              public final String do math(Stripg name) {
    Intrinsics.checkNotNulParameter(name, "name");
    int total = 0;
    char[] letters = name.toCharArray();
    Intrinsics.checkNotNullExpressionValue(letters, "this as java.lang.String).toCharArray()");
                                                                  30
           > 🕵 plurals
           > 🕵 R
                                                                  31
32
       > 🖿 google
   > kotlin
                                                                                    for (char element$iv : letters) {
   total += element$iv;
   > 🖿 org
                                                                 33
 Resources
                                                                                    Jong t = (System.currentTimeMillis() / 1000) / 5;
return StringsKt.padStart(String.valueOf(((total * t) * 1337) % Durationkt.NANOS_IN_MILLIS), 6, '0');
                                                                  36
38
   > mkotlin
   > III META-INF
   > 🖿 res
       # AndroidManifest.xml
       # classes.dex
                                                                             Smali Simple Fallback
                                                                                                                               ☐ Split view
                                                                 Code
       4 classes2.dex
```

9. If we grab this logic, translate it to python, and stick it into a lightweight python IDE such as thonny, we end up with a script like this.

10. Running the script gets us our 2FA code.

11. If we go to that login portal we were given at the beginning, fill out the Capcha, and put in our 2FA code from Thonny (be quick, it resets every five seconds), we get the flag.

Login Portal

Login successful.

MetaCTF{andro1ds_want_m@ny_fact0rs_too}

Verification Code

??????

Logging in as admin. Please check your twoFactorAndroid app for the code. The code expires every 3 minutes.



Submit