CTF 戦記 スペイン編

tyage

CTF (Capture The Flag) というコンテストをご存知でしょうか。これはコンピュータセキュリティに関する技術や知識で競うコンテストです。具体的にはバイナリ解析・パケット解析・フォレンジック・Web セキュリティ・暗号・トリビアなどの知識を使って競技します。セキュリティの知識を利用したプログラミングコンテストのようなものを想像してもらうとわかりやすいかと思います。最近は日本でも普及しつつあり各地でコンテストが開かれているためご存知の方もいるかもしれません。
ここではスペインで行われた No cON Name Facebook CTF[*1]（以下、Facebook CTF）での私と私のチームの体験談を述べていきます。

Facebook CTF is ...?

先ほど CTF はプログラミングコンテストに近いと述べたのですが、CTF はチーム戦であることが多く、また競技方法が大きく分けて 2 種類であるという特徴があります。1 つ目の種類が Jeopardy と呼ばれるクイズ形式のもので、主催者が出題する問題の答えを回答して得点を得る形式です。2 つ目の種類が Attack-Defence（攻防戦）形式です。各チームが配布されたプログラムを起動してサービスを運営しており、他チームのサービスに攻撃しパスワードを得ると得点になります。同時に自チームへの攻撃をできないよう、パッチをあてる等して防御します。各チームで領土を奪い合う戦争ゲームのようなものを想像してもらうと分かりやすいかと思います。
今回紹介する Facebook CTF では、予選は前者の Jeopardy、決勝は後者の Attack-Defence に近いものとなっているのですが、どちらも少し特殊な形式となっていました（詳しくは後ほど述べることとします）。

[*1] http://noconname.org/files/CTF_NocONName_2013_ENG.pdf