



セキュリティキャンプ CTF 2011 レポート

文=上野宣 (TIP)

❖ CTF って何?

CTFは「Capture the Flag」の略で、旗取りゲームのことだ。ただし取るのは旗ではない。問題文や問題ファイルなどが提示され、そこからキーワードなどを探す。問題の難易度や解いたスピードなどによって点数が変わり、その合計得点によって勝敗が決まるという競技だ。

キャンプのCTFは、昨年に引き続き2回目の開催となる。CTFのチームは各クラスの参加者が含まれていて8名ほどで構成される。その他、チューターや特別ゲストとして参加していただいた「sutegoma2」の有志者数名によるチームも参戦した。これらのメンバーにより6時間の熱戦が繰り広げられた。今回CTF終了後に解答者から発表があった問題を2問紹介する。

出題例その1 謎の文字列を解説せよ

問題文には「JT11JTMjYyJT11…」という長い謎の文字列が書かれている。

解答者によると、まず4バイトごとの規則性を見出したことにより、Base64ではないかと推測した。そして試しにBase64でデコードした結果「%25%32%62%25%34%64%25…」といった文字列が現れた。

さらにこれはパーセントエンコーディングだと推測し、デコードを試した結果「+MF0wbjBgMIA-」という文字列が現れた。解答者は「+」で囲まれたこの文字列を直感でUTF-7だとわかったという。そしてさらにデコードすると「そのだむ」という文字が現れた。これが解答だった。



CTF会場の様子。終了時間ギリギリまで激しい争いが行われた

ちなみに「そのだむ」はキャンプのファシリテーター園田氏の愛称である。

出題例その2 prog4.exe を解析せよ

問題は「prog4.exe」というファイルが置かれているだけだ。

解答者によると、とりあえずWindowsのコマンドプロンプトで実行してみたところ「Password: 0x02DD1995」と「Password: xxxxxxxxxx」という文字列が現れた。この「xxxxxxxxxxx」という部分に解答が入るはずだと推測し、デバッガーのOllyDbgにかけて解析を始めることにした。

画面に表示する部分は「printf」のはずなので、この付近に当たりを付けて探し始めたという。その結果「password」という文字列がスタックに現れる部分を見つけたという。

しかし、passwordの中ですべての文字列について、何かハッシュ値のようなものを計算していたが、何を計算していたかはわからなかったという。「password」が出現したら「worz」を書き換えて実行するだけで解答を導き出したという。

❖ 勝者は誰だ?

CTFは最後まで勝敗がわからない混戦模様で、終了間際の最後の5分で1位と2位とが入れ替わるという一幕もあった。その結果、熱戦を制したのはキャンプ参加者で構成されたチームだった。

続いてキャンプ卒業生で構成されるチューターチームが2位で、sutegoma2は3位だった。しかし、sutegoma2は他チームの半数ほどの人数で戦ったのでかなり健闘している。実際、個人得点の1位2位はsutegoma2チームから出ている。

キャンプCTFはおおむね盛り上がりを見せており、キャンプ終了後にTwitterなどでCTF大会を開催したいとか、sutegoma2以外のチームを作ってチャレンジしたいというような声も聞かれた。キャンプ卒業生たちが今後世界のCTF大会で活躍するのを楽しみにしたい。