# 0から始めるゲームハッキング体験

## やること

- ハッキングってなに？
- 実行ファイルを書き換えてみよう
- ハッキングを学ぶ

## ハッキングってなに？

### ハッキングとクラッキング

- ハッキング
  コンピュータを用いたエンジニアリング(開発)行為を広く指す言葉
- クラッキング
  悪意を持って脆弱性(安全性の穴)を攻撃しシステムを改ざんしたり情報を抜き取ったりすることを指す言葉

### 「ハッキング」をする理由

セキュリティ(安全性)を保つためには、攻撃者がどのような手法を持って攻めてくるかを知る必要がある
→ 知らない攻撃から身を守ることはできない

VRやビットコインなど、いろいろなものの「仮想化」が進む社会ではセキュリティがとても大切

意外と身近なところにセキュリティの危険性が潜んでいる！

- インターネットを介した通信内容の盗聴
- 暗号化されたデータの解読
- webサイトから不正にパスワードを入手
- ゲームを不正に書き換える(チート行為)

ハッキングをするためのツールが無料で配られている
→簡単に悪用することができる **(**違法なので絶対にダメです**)**

## 実際にやってみよう

ソーシャルゲームのガチャを真似た簡易的なプログラム「gacha」を実行してみる

手順
端末を開き、`./gacha`と打ち込んでエンターキーを押す

排出率

| レアリティ | 排出率 |
|---|---|
| SSR | 3% |
| SR | 10% |
| R | 87% |

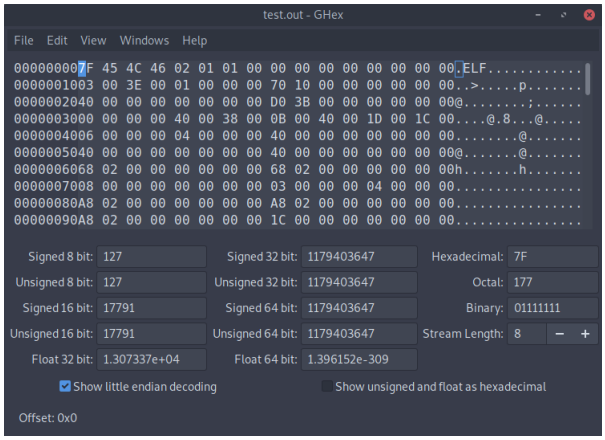
## 実行ファイルの中身

実行ファイル：コンピュータが実行できる形式のファイル
中身は0と1の羅列で、通常のテキストエディタ(メモ帳など)では開くことができないが、特殊なエディタ(バイナリエディタ)を用いることで中身を閲覧・編集できる

実行ファイルの中身(バイナリ)を実際に見てみる

手順
端末を開き、ghex gachaと打ち込んでエンターキーを押す

以下のような画面が表示されます↓




表示されているのは0と1の羅列(2進数)を16進数に変換したもの

**2**進数と**16**進数：データを0と1のパターンで表す2進数とデータを0~9,a~fで表す16進数は相互に変換することができる

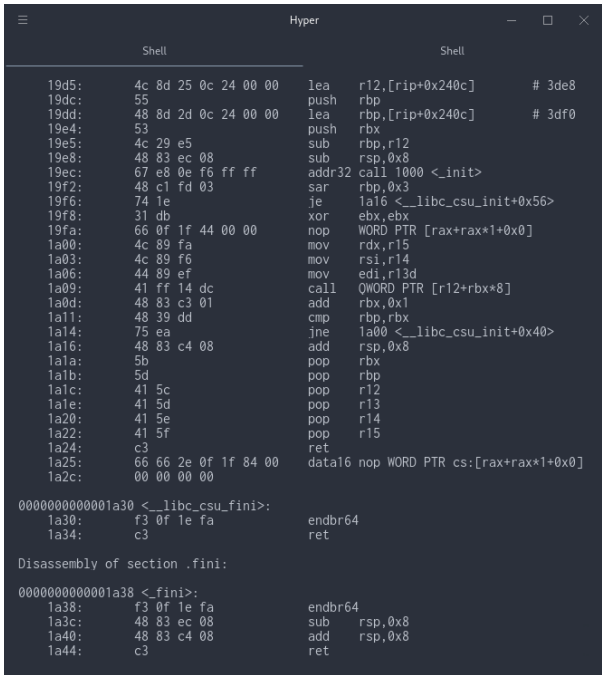
## バイナリの意味

人間が一見しただけでは意味のわからない文字の羅列に見えるバイナリ(機械語)を人間に読みやすく変換することができる

手順

ghexを一度閉じ、端末に`objdump -M intel -S gacha`と打ち込んでエンターキーを押す

以下のような画面が表示されます




左半分にバイナリ、右半分に人間に読みやすく変換されたアセンブリ言語というものが表示される

上にスクロールして、`0000000000000186c <gacha>:`と書かれた行を探す(ガチャの本体がここに記述されています)

`191b: 7f 1e jg 193b <gacha+0xcf>`
「レアリティがRのアイテムを排出する」という処理をする行
→ここを「何もしない」に書き換えると、SSRとSR以外は出ないようになるはず

手順

1. 端末に`ghex gacha`と打ち込んでエンターキーを押す
2. スクロールして`00001910`から始まる行を探す
3. その行のうち、`7F 1E`と書いてあるところを探す
4. `7`をクリックし、`9090`と打ち込む
5. `Ctrl`キーと`S`キーを同時に押してからghexを閉じる
6. ghexを閉じる
7. 端末に`./gacha`と入力して閉じる

## おまけ

SSRしか出てこないようにバイナリを書き換えてみる

`objdump -M intel -S gacha`をして出力される中の`000000000000186c <gacha>:`を見てみると、もう一つ`jg`という命令が書かれた行が見つかる

この命令はghexでバイナリを見たとき、`000018F0`から始まる行のどこかに存在する
→`90 90`に書き換えてSSRしか排出されないようにしてみよう

# ハッキングを学ぶ

## Capture the Flag(CTF)

「ハッキングコンテスト」と呼ばれている(世界各地やオンラインで開催されている)
大会型と常設型があるので初めての人は常設で練習するのがおすすめ

今回扱った分野(Reversing, Binary)以外にもWeb, Pwn, Crypto, Networkなど様々

セキュリティコンテストチャレンジブックなど、CTFやセキュリティを学ぶための書籍もある

### 講師の連絡先

はすみ(mail: skytea922@gmail.com)(Twitter: @hsm_hx)

- 宇部高専コンピュータ部 部長
- 非公式学生サークル 情報技術研究会 Circ:RE代表
- CTFをしたりwebサービスを作っています

CTFに興味を持ったり、部活や学校のことについて質問があれば気軽に連絡してね