【超初心者向け】CTFをやってみよう

Pico CTFで遊んでみる

作成 : yunagaha

CTFとは

- Capture The Flag の頭文字をとったもの
- 大会形式で世界中で行われている競技
- Cryptography(暗号)、Reverse Engineering(バイナリ解析や逆コンパイルなど)、Forensics(隠されたデータの復元)、Networking(ネットワーク関連)など多種多様な分野の問題が出題される

参加のながれ

1. PicoCTFに登録する
2. クラスルームに参加する
3. Assignmentを解く

PicoCTFに登録する

https://play.picoctf.org/login?redirect=/login

Docker環境構築について

今日は無くても大丈夫だが後々準備しておくと役立つ

Dockerのディレクトリ下に/CTFディレクトリが作成されるので、ブラウザでCTF用のプロファイルを作成し、デフォルトのファイルのダウンロード先を/CTFに指定するとシームレスにkali linuxを使った解析が行える

詳しくはhttps://github.com/sudolifeagain/ctf-Docker を参照してね

クラスルームに参加する

https://play.picoctf.org/classrooms

クラスコードは

`C50rgYcdX`

問題選定について

- 前提知識がほとんどいらないものに絞って問題を選んだ
- CTF経験者なら赤子の手をひねるように解けるはず
- Flagは `picoCTF{FLAG}` の形式で隠されている

それでは解いてみましょう

Good luck and don't panic !!

解説フェーズ

どうだったでしょうか
次ページからWrite Up(解説)がはじまります

13

与えられた文字列：cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}

問題文「do you know what ROT13 is?」

Googleで調べてみよう

13 -write up

ROT13は単換字式暗号（シーザー暗号）の一つである。アルファベットを一文字毎に13文字後のアルファベットに置き換える。
例：Aは Nに、 B は O になる。(wikipediaより)

https://rot13.com/
のようなサイトが有用

暗号化の方式に心当たりがあればその名称をググると大体変換サイトがヒットします

暗号関連の問題のTips

易しめの問題であれば、暗号化後の文字列の外見的な特徴からほしきを推測することができる場合がある

今回はcvpbPGS{...}の形式だった

→大文字小文字が保存されているので換字式暗号のどれかが怪しい

MOD26 -write up

与えられた文字列は`cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_jdJBFOXJ}`

前の問題と全く同じ方法で解けます

Tips

https://gchq.github.io/CyberChef/

このサイトは一つのサイトで様々な暗号化・復号化の処理を試すことができるので便利

Obedient Cat

「flag」という名前のファイルがダウンロードできる
拡張子が無いファイルをどのように扱うのか

Obedient Cat - Write up

今回の場合はただダブルクリックするだけでテキストエディターが開き、flagがそのまま表示される

しかしこのファイルの中身を知らない状態でクリック(実行)するのはリスクもある

Linux系のOSであれば`file`コマンドを使うことができ、静的にファイルに関する情報を集めることができる

```
$ file flag
flag: ASCII text
```

今回であればASCII text(ただの平文)であることがわかるため、テキストエディターで開けば良いとわかる

※`cat`コマンドなどでも可だが、`file`コマンドはより多くの情報を提供してくれるので便利

Python Wrangling

Pythonのソースコード + pw.txt + flag.txt.en の3つのファイルがある

ソースコードを読み解き、どの操作をすればflagが取れるのかを考えていく問題

Python Wrangling -write up

sys.argvは実行の際に使えるコマンドライン引数が格納されているもの。

`ende.py`はファイルを暗号化・復号化する機能を持つ

`-e`と`-d`でそれぞれ暗号化、復号化

今回は`-e`で暗号化されたflag.txt.enが与えられているので、`-d`を用いて復号化するのがよい

```
$ python3 ende.py -d flag.txt.en 192ee2db192ee2db192ee2db192ee2db
picoCTF{4p0110_1n_7h3_h0us3_192ee2db}
```

※`192ee2db...`はpw.txtの中身

Inspect HTML

水色の「Launch Instance」ボタンをクリックすると
数十秒後に画面が更新されて画面左のDescriptionにリンクがでてくる
そこから専用のサイトにアクセスできる

Inspect HTML - write up

ブラウザで「here」リンクをクリックするとサイトが表示される。

`shift + ctrl + C`を押すとウェブサイトのソースコードが表示される

ソースコードから怪しいデータを探してくる

平文でフラグがある

WebDecode

Inspect HTMLと同様にインスタンス(実行環境)をその都度作成して解く。

WebDecode -write up

about.htmlに

```
<section class="about" notify_true="cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfZGYwZGE3Mjd9">
   <h1>
    Try inspecting the page!! You might find it there
   </h1>
```

があり、Cyberchefで「From Base64」でデコードすると
「picoCTF{web_succ3ssfully_d3c0ded_df0da727}」が得られる

おわりに

- 今回は【超初心者向け】としてかなり簡単な問題を選びました
- 超高難易度の問題もあるので挑戦してみてください

おまけ

alpacahackというサイトでは毎日一問CTFの問題が公開されます
全問正解を目指して解いていきましょう！

ちなみにyunagahaはこんな感じ(2回寝過ごして24h以内に解けなかった)