

Capture The Flag

C T F の紹介

OAS Tech Meeting

オー・エイ・エス株式
会社

ソリューション本部
第二ソリューション部
製品開発グループ

目次

1. Capture The Flagとは？
2. ゲームの種類
3. 例題 1
4. 例題 2

1 . Capture The Flag とは？

(1)

- ▶ 本来は騎馬戦など、相手陣営にある旗を奪取して自陣に持ち帰ることを指している。
- ▶ 今回紹介するのは、コンピューターセキュリティ技術を使って行う競技、通称 C T F と呼ばれるものです。
- ▶ 毎年ラスベガスで開催される D E F C O N の中でハッキング大会として実施されている。

1 . Capture The Flag とは ?

(2)

▶ 必要な能力/知識

- コンピューターを外部から守る知識
 - ファイアウォールなど
- サイバー攻撃する知識
 - IP Spoofingやパケットキャプチャ、その他脆弱性など
- 第 6 感
 - 暗号解読系の問題は閃きも必要になる。

1 . Capture The Flag とは？

(3)

▶ 謎解きゲーム？

- 謎解きだけではなく、かなりの知識と技術を持っていないと、太刀打ちできない問題が多い。ただ上級者しか楽しめないわけではなく、問題のレベルもピンキリ。
- 大会会場で、優秀なハッカーを探すために F B I が張り込んでいるらしい。日本でもホワイトハッカーを探すことがあるらしい。

2 . ゲームの種類

- ▶ バイナリ
 - 解読系。R S A の暗号解読、ファイルの解析、パスワード解析など
- ▶ フォレンジック
 - 物理デバイスを解析する。(O S メモリ、H D D、U S B メモリなど)
- ▶ Pwnable (ownableのtypo?)
 - 脆弱性を突く。リバースエンジニアリングなどでプログラムを解析し、セキュリティホールを利用してフラッグを探す。
- ▶ Web系
 - X S S / 各インジェクション系など、Webアプリケーションの脆弱性を突いてサーバに侵入する。
- ▶ ネットワーク
 - パケットを解析して、その中にあるフラッグを探す。

3 . 例題 1 (1)

- ▶ 試しに問題を解いてみよう。(バイナリ系)

以下の公開鍵に対する暗号鍵を解いてください。

-----BEGIN PUBLIC KEY-----

MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhALYtZp8lgWNXI9trGI8S8EacvuDLxdrL

NsNuDJJa26nv8AgMBAAE=

-----END PUBLIC KEY-----

※ただし、このキーは1bitだけbit誤りがあります。
どうやって解きますか？

ヒント) $n=pq(p \neq q)$

3 . 例題 1 (1) 答え

- ▶ 1 . RSAキーを10進数に変換する。
(→82401872610398250859431855480217685317486932934710222647212042489320711027708)
- ▶ 2 . 素因数分解する。(n=pqのpqが分かればよい)
 - ※1bit誤りがあるため、素因数分解出来ない。
- ▶ 3 . Pythonなりで素因数分解する関数を作成し、片っ端から1bitずれた値を突っ込む (最大試行回数255回)
- ▶ 4 . 素因数分解できたら、pとqを使い秘密鍵を生成する。終了。
- ▶ ※ <http://www.factordb.com>にアクセスすると、素因数解析済みのデータベースを検索できる。

4 . 例題 2 (1)

- ▶ こういう問題も出る。
- ▶ 「ハッカーカンファレンスに焦点を合わせたXファイルのエピソードの名前は？」
- ▶ ヒント) ひたすらググるだけ。

5 . 例題 3

Crypto 100

問題：パスワードは何？

444	66	222	777	999	7	8	666	4	777
2	7	44	999	2	7777	88	22	7777	8
444	8	88	8	444	666	66	222	444	7
44	33	777	444	7777	2	6	33	8	44
666	3	666	333	33	66	222	777	999	7
8	444	666	66	22	999	9	44	444	222
44	88	66	444	8	7777	666	333	7	555
2	444	66	8	33	99	8	2	777	33
777	33	7	555	2	222	33	3	9	444
8	44	222	444	7	44	33	777	8	33
99	8	2	222	222	666	777	3	444	66
4	8	666	2	777	33	4	88	555	2
777	7777	999	7777	8	33	6	8	44	33
88	66	444	8	7777	6	2	999	22	33
7777	444	66	4	555	33	555	33	8	8
33	777	7777	7	2	444	777	7777	666	333
555	33	8	8	33	777	7777	8	777	444
7	555	33	8	7777	666	333	555	33	8
8	33	777	7777	6	444	99	8	88	777
33	7777	666	333	8	44	33	2	22	666
888	33	8	44	444	7777	222	444	7	44
33	777	8	33	99	8	444	7777	33	66
222	777	999	7	8	33	3	22	999	8
33	555	33	7	44	666	66	33	55	33
999	7	2	3	7777	666	9	33	222	2
555	555	8	44	444	7777	55	33	999	7
2	3	222	444	7	44	33	777		

5 . 例題 3 (回答)

Crypto 100

問題：パスワードは何？

444	66	222	777	999	7	8	666	4	777
2	7	44	999	2	7777	88	22	7777	8
444	8	88	8	444	666	66	222	444	7
44	33	777	444	7777	2	6	33	8	44
666	3	666	333	33	66	222	777	999	7
8	444	666	66	22	999	9	44	444	222
44	88	66	444	8	7777	666	333	7	555
2	444	66	8	33	99	8	2	777	33
777	33	7	555	2	222	33	3	9	444
8	44	222	444	7	44	33	777	8	33
99	8	2	222	222	666	777	3	444	66
4	8	666	2	777	33	4	88	555	2
777	7777	999	7777	8	33	6	8	44	33
88	66	444	8	7777	6	2	999	22	33
7777	444	66	4	555	33	555	33	8	8
33	777	7777	7	2	444	777	7777	666	333
555	33	8	8	33	777	7777	8	777	444
7	555	33	8	7777	666	333	555	33	8
8	33	777	7777	6	444	99	8	88	777
33	7777	666	333	8	44	33	2	22	666
888	33	8	44	444	7777	222	444	7	44
33	777	8	33	99	8	444	7777	33	66
222	777	999	7	8	33	3	22	999	8
33	555	33	7	44	666	66	33	55	33
999	7	2	3	7777	666	9	33	222	2
555	555	8	44	444	7777	55	33	999	7
2	3	222	444	7	44	33	777		

▶ ヒント：ガラケ携帯のキータッチ

その他

- ▶ 相手サーバの脆弱性を突く、サーバ攻防型。

サーバ攻防型



The image shows a screenshot of a scoreboard for the HKTUSGCC 2010 Malaysia competition. At the top, there is a banner with the event name and a photo of a group of people. Below the banner, there is a table with columns for Team, HP, and five categories (City 1 to City 5). Each category has sub-columns for Utility, Make, and a set of four checkboxes (Start, Safe, A, E). The table lists several teams with their corresponding HP values and scores. A red arrow points from a text box at the bottom to the table.

Team	HP	City 1				City 2				City 3				City 4				City 5			
		Utility	Make	Start	Safe	A	E	Utility	Make	Start	Safe	A	E	Utility	Make	Start	Safe	A	E		
138-er-Ar	122000																				
ERB-EU-Vol 2	129500																				
Terminators	119500																				
Army Strong	173500																				
Guardian Whop	160000																				
ILLAB	126500																				
Unigomaz	152500																				
ERB-EU-Vol 1	172000																				

サーバで動作しているサービスは、運営チームから監視されている

https://www.youtube.com/watch?v=rriCp_EC2NM

常設CTF

- ▶ いつでもCTFにチャレンジできるサイトがあります。
 - <http://ksnctf.sweetduet.info/>
 - VillagerAなどがお薦め。
 - <http://s01.elliptic-shiho.xyz/ctf/>
 - 比較的優しめ？
 - <http://cpaw.spica.bz/>
 - 色々解説も書いてある。

- ▶ OASでもCTFにチャレンジするチームを作って勉強会をするのも面白いかもしれません。
- ▶ ご清聴ありがとうございました。