

世界最高峰のセキュリティコンテスト DEFCON CTFとは

ネットエージェント株式会社
愛甲健二

自己紹介



- 愛甲健二
- ネットエージェント株式会社
- セキュリティエンジニア 兼 取締役
- CTF歴1年半くらい
- <http://d.hatena.ne.jp/kenjaiko/>

目次

- セキュリティコンテストとは？
 - セキュリティコンテスト (Capture The Flag) とは
 - 出題されるセキュリティ分野
 - 大会の状況など
- 主題される問題の紹介 & 解答
 - Binary - マシン語解析系
 - Exploit - 脆弱性監査系
 - Web - HTTP(S)関連のセキュリティ系
 - Forensic- データ解析に関する調査系
 - Trivia - 業界や技術に関するトリビア系
- まとめ (CTFから得られるもの)
 - 競技を通じて世界中のエンジニアと分かり合える

目次

- **セキュリティコンテストとは？**
 - セキュリティコンテスト (Capture The Flag) とは
 - 出題されるセキュリティ分野
 - 大会の状況など
- **主題される問題の紹介 & 解答**
 - Binary - マシン語解析系
 - Exploit - 脆弱性監査系
 - Web - HTTP(S)関連のセキュリティ系
 - Forensic- データ解析に関する調査系
 - Trivia - 業界や技術に関するトリビア系
- **まとめ (CTFから得られるもの)**
 - 競技を通じて世界中のエンジニアと分かり合える

セキュリティコンテストとは？

- セキュリティ技術を競い合う、競技タイプの戦争ゲーム
- 世界では一般的に“Capture the Flag”（旗取り合戦）と呼ばれる
- 問題の多くは、サーバの脆弱性を探したり、データを解析し、隠されたパスワードを発見するというタイプのもの

どんな問題が出題される？

- 問題は5つくらいの分野に分かれている
 1. Binary - マシン語を解析する問題
 2. Exploit - 脆弱性を探す問題
 3. Web - HTTP(S)に関する問題
 4. Forensic - データ解析の問題
 5. Trivia - 業界に関するトリビア問題
- チームを組み、それぞれの得意分野に挑む

世界のセキュリティコンテスト

- DEFCON CTF
 - USAのカンファレンスであるBlackHat & DEFCONが主催するCTF、もっとも有名なハッキングコンテスト(予選有り)
- CODEGATE CTF
 - 韓国で主催されるカンファレンスCODEGATEが統括を行なうハッキングコンテスト(予選有り)
- Hack In The Box CTF
 - マレーシアで行なわれるカンファレンスHack In The Boxが主催するハッキングコンテスト(決勝のみ)

他にも企業が行なっているものを中心に多数あり

目次

- セキュリティコンテストとは？
 - セキュリティコンテスト (Capture The Flag) とは
 - 出題されるセキュリティ分野
 - 大会の状況など
- **主題される問題の紹介 & 解答**
 - Binary - マシン語解析系
 - Exploit - 脆弱性監査系
 - Web - HTTP(S)関連のセキュリティ系
 - Forensic- データ解析に関する調査系
 - Trivia - 業界や技術に関するトリビア系
- まとめ (CTFから得られるもの)
 - 競技を通じて世界中のエンジニアと切磋琢磨できる

Binary問題の例

- Binary問題って具体的にどんなもの？
 1. Binary - マシン語を解析する問題
 2. Exploit - 脆弱性を探す問題
 3. Web - HTTP(S)に関する問題
 4. Forensic - データ解析の問題
 5. Trivia - 業界に関するトリビア問題
- DEFCON CTF'08のBinary レベル100問題は…

Binary レベル100

問題: 以下のライブラリ関数名を答えよ

```
00000000 89C7      MOV EDI, EAX
00000002 89DE      MOV ESI, EBX
00000004 89CA      MOV EDX, ECX
00000006 C1E9 02    SHR ECX, 2
00000009 F3:A5     REP MOVS DWORD PTR ES:[EDI], DWORD PTR DS:[ESI]
0000000B 89D1      MOV ECX, EDX
0000000D 81E1 04    AND ECX, 3
00000013 F3:A4     REP MOVS BYTE PTR ES:[EDI], BYTE PTR DS:[ESI]
00000015 C3        RETN
```

バイナリ分野におけるもっとも簡単な問題(レベル100)
アセンブラコードの読解力が試される

Binary レベル100

問題: 以下のライブラリ関数名を答えよ

```
00000000 89C7    MOV EDI, EAX
00000002 89DE    MOV ESI, EBX
00000004 89CA    MOV EDX, ECX
00000006 C1E9 02  SHR ECX, 2
00000009 F3:A5   REP MOVS DWORD PTR ES:[EDI], DWORD PTR DS:[ESI]
0000000B 89D1    MOV ECX, EDX
0000000D 81E1 04  AND ECX, 3
00000013 F3:A4   REP MOVS BYTE PTR ES:[EDI], BYTE PTR DS:[ESI]
00000015 C3      RETN
```

バイナリ分野におけるもっとも簡単な問題(レベル100)
アセンブラコードの読解力が試される

解答は「**memcpy**」

Exploit問題の例

- Exploit問題って具体的にどんなもの？

1. Binary - マシン語を解析する問題
2. Exploit - 脆弱性を探す問題
3. Web - HTTP(S)に関する問題
4. Forensic - データ解析の問題
5. Trivia - 業界に関するトリビア問題

- CODEGATE CTF'08のExploit レベル500問題は…

Exploit レベル500

出題側がリモートに用意したLinux環境へのログインIDが配布され、以下の問題文が提示される

問題: そこに置いてあるfusプログラムのソースコードは…

```
void main(void)
{
    char buff[20];
    scanf("%s", buff);
}
```

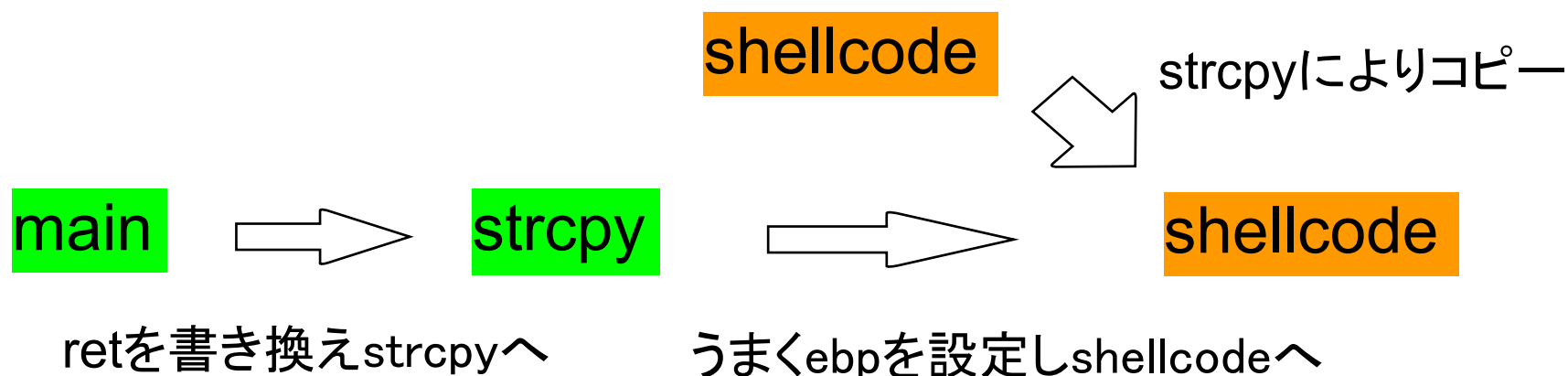
単純なオーバーフローのように思えるが、実はpackerらしいものが実行ファイルに対して施されている
詳細にプログラムを解析していくと…

解析していくうちに分かったこと

- スタックアドレスがrandomize(ランダム化)されており、かつ、実行権限がない
 - shellcodeをスタックに置いていても実行できない
- shellcodeを環境変数に格納されないように、環境変数領域が、先頭から0x15000バイト分、ゼロクリアされる
- retとebpは書き換え可能である

辿りついた解答

1. まずはscanfでbuffをオーバーフロー、ebpとretを上書き
2. retのジャンプ先はstrcpy関数にする
3. ebpをうまく操作して、実行権限のある領域(ヒープなど)へ、strcpyにより、shellcodeをコピーする
4. strcpy終了後に、retがコピー先のshellcodeへ飛ぶようにebpを適切に操作する



Web問題の例

- Web問題って具体的にどんなもの？
 1. Binary - マシン語を解析する問題
 2. Exploit - 脆弱性を探す問題
 3. Web - HTTP(S)に関する問題
 4. Forensic - データ解析の問題
 5. Trivia - 業界に関するトリビア問題
- DEFCON CTF'07のWeb レベル400問題は…

Web レベル400

DEMO

<http://192.168.100.34:8093/oneLastmidget/>

Forensic問題の例

- Forensic問題って具体的にどんなもの？

1. Binary - マシン語を解析する問題
2. Exploit - 脆弱性を探す問題
3. Web - HTTP(S)に関する問題
4. Forensic - データ解析の問題
5. Trivia - 業界に関するトリビア問題

- DEFCON CTF'08のForensic レベル500問題は…

Forensic レベル500

右のpngファイルが配布され、
次の問題文が提示される

問題: 君が魔法のデコードをすれば、
欲しがっているものはきっと見つかる

問題文はほとんど無意味?

見
性
戸

透明色の排除

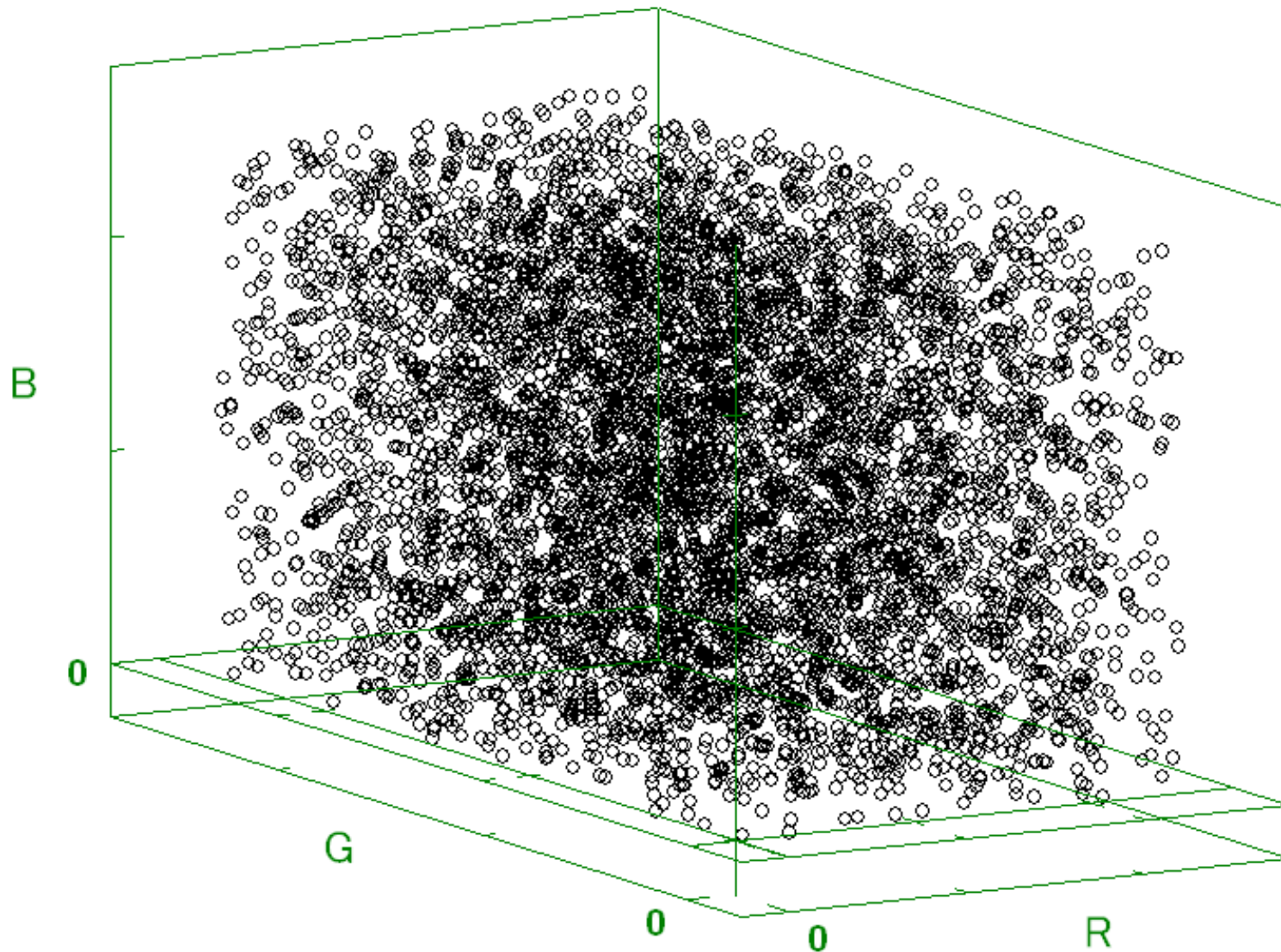
RGBAの「A(透明色)」を無視すると、右のような画像になる

透明色なのにRGBにデータが入っているのは何故？

よって、透明色でRGBにデータが入っているドットを集めて、 (x, y, z) でグラフ化



(R, G, B)で3Dグラフ化



さらに別の角度からRGBを評価

RGBを24ビットデータ値としてソートすると…

```
# cat a | more (aファイルには、すべてのpixelのRGB値が入っている)
00031f9d
0048a690
.....
# for i in `cat a`;do c=`grep $i a|wc -l`;echo $i $c;done > b
# grep -v 1¥$ b | sort -u | grep -v 2¥$ | sort -u
000ebb02 20
00cca44d 3
00e0a6f2 3
```

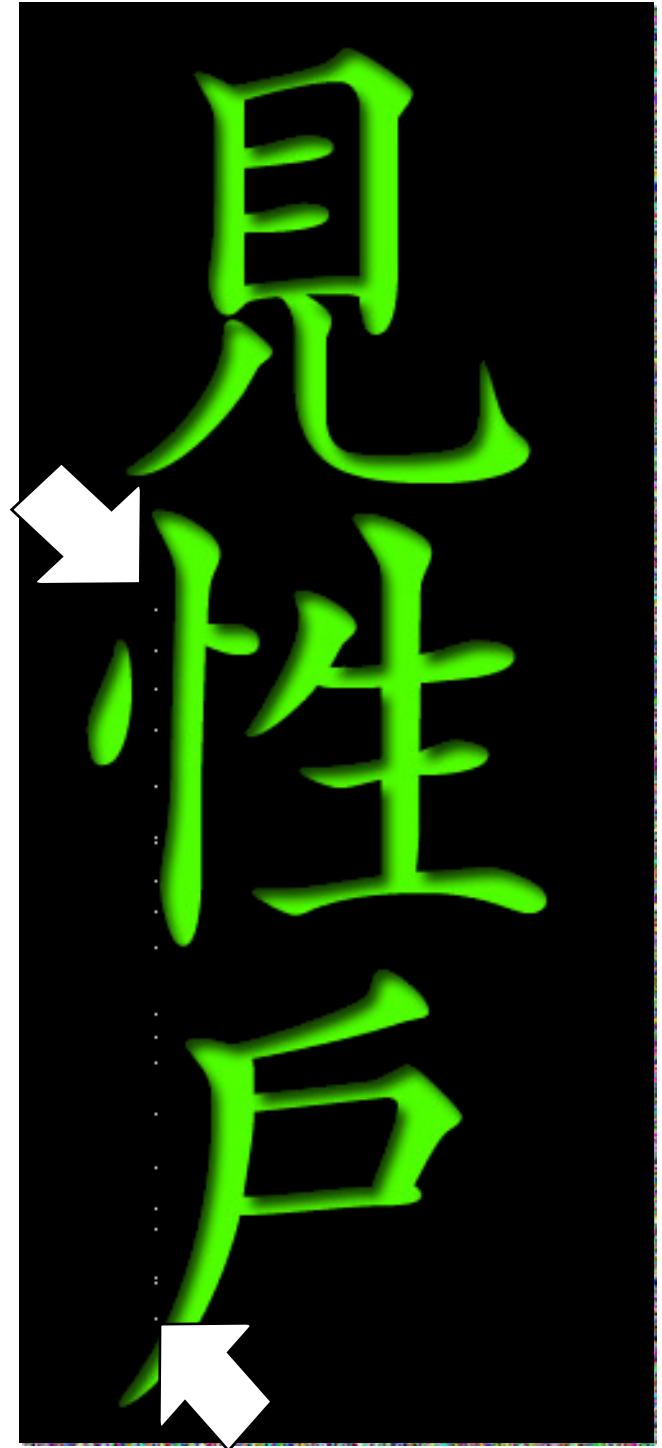
それぞれランダムなRGBが設定されているかのように見えた透明色の背景の中に、同じ色が20pixelも存在！

20pixelを強調すると…

縦一列にpixelの列が見える

このpixelの列の「差」を取ると、どれも0～26までの値

よって、pixelの「差」が、アルファベットに対応していると推測することで解答が得られる



Trivia問題の例

- Trivia問題って具体的にどんなもの？
 1. Binary - マシン語を解析する問題
 2. Exploit - 脆弱性を探す問題
 3. Web - HTTP(S)に関する問題
 4. Forensic - データ解析の問題
 5. Trivia - 業界に関するトリビア問題
- DEFCON CTF'08のTrivia レベル200問題は…

Trivia レベル200

問題: EAX = 0. EDX is undefined.

EAXとEDXの両方を0にする1バイトアセンブリ命令は何？

- Triviaは「知識」や「検索力」を試すものが多い
- この問題はアセンブラ命令を知っていれば簡単に分かるが、それを知らずとも、Webで検索すれば解答できる
- x86命令セットリファレンスから検索

Trivia レベル200

問題: EAX = 0. EDX is undefined.

EAXとEDXの両方を0にする1バイトアセンブリ命令は何？

- Triviaは「知識」や「検索力」を試すものが多い
- この問題はアセンブラ命令を知っていれば簡単に分かるが、それを知らずとも、Webで検索すれば解答できる
- x86命令セットリファレンスから検索

解答は「 **CDQ** 」

目次

- セキュリティコンテストとは？
 - セキュリティコンテスト (Capture The Flag) とは
 - 出題されるセキュリティ分野
 - 大会の状況など
- 主題される問題の紹介 & 解答
 - Binary - マシン語解析系
 - Exploit - 脆弱性監査系
 - Web - HTTP(S)関連のセキュリティ系
 - Forensic- データ解析に関する調査系
 - Trivia - 業界や技術に関するトリビア系
- **まとめ (CTFから得られるもの)**
 - 競技を通じて世界中のエンジニアと切磋琢磨できる

まとめ(CTFから得られるもの)

- 世界のエンジニアと切磋琢磨できる
- 問題が解けると、ひとつ成長した気分になれる
- 専門分野以外にも興味がわく
- なにより楽しい！

ご清聴、有難うございました
m(_ _)m

Any Questions?