沖縄 ICT フォーラム 2017 in 宮古島
僕ホワイトハッカーですが, 何か聞きたいことあります？

NTTセキュリティ・ジャパン株式会社
羽田 大樹

NTT Security

普通の人には中々理解されない

「ハッキング」

の技術的な世界を

誰でも分かるように解説します

ハッキング（ハック）って何？

NTT Security

- ハッキング（ASCII.jp デジタル用語辞典）
  - システムやネットワークに通常ではない方法でアクセスすること。
  - もともとは、合法的なアクセスを含めてこう呼んでいたが、転じてデータの改ざんや破壊、盗用などの違法行為を指すことが多くなっている。正しくは、違法なアクセスはクラッキングと呼ぶ。
- ハッキング（デジタル大辞泉）
  - コンピューターに関する高い技術力や豊富な知識をもつ者が、プログラムを解析して巧妙に改良したり、コンピューターネットワークの安全性を検証したりすること。
  - [補説]2について、悪意ある不正行為はクラッキングと呼んで区別することが多い。

ハッキング（ハック）って何？

NTT Security

- ハッキング（大辞林 第三版）
  - コンピューターに熱中すること。
  - 不法に他のコンピューターシステムに侵入し、データの改変やコピーを行うこと。
- ハッキング（Wikipedia）
  - コンピュータの隅々までを熟知した者が行うハードウェア・ソフトウェアのエンジニアリングを広範に意味する言葉。
  - 他人のコンピューターに不正に侵入するなどの行為がハッキングと呼ばれる場合もあるが、これは正式にはクラッキングと呼ぶ。本来ハッキングという言葉はエンジニアリングという行為そのものを指す用語であり、悪意・害意を持った行為に限定されるものではない。

今日の話における用語の定義

NTT Security

- (広義の) ハッキング
  - コンピューターを熟知した者が行うエンジニアリング全般
- (狭義の) ハッキング
  - コンピューターを熟知した者が, システムの制限を回避して開発者が想定していない動作をさせること
- 脆弱性
  - システムの制限を回避するための抜け穴

すごいことをするのは分かったけど, イメージが湧かない
どうせエンジニアしか理解できない世界の話なんでしょ？

ご安心ください, 誰でも分かるように解説します

他に出てくるハッキング（ハック）という言葉 (1)

NTT Security

- ライフハック（デジタル大辞泉）
  - 仕事の質や効率、高い生産性を上げるための工夫や取り組み。
  - 2004年に米国のテクニカルライター、ダニー＝オブライエンが考案した言葉であり、主に情報産業に携わるプログラマーや技術者の間で使われるようになった。
  - アプリケーションソフトやデジタル機器を効率良く使いこなすためのちょっとしたこつやテクニックから、**業務目標の設定や健康管理にいたる、いわゆる仕事術、生活術を指す。**


固定された蛇口（制約）
から
水をバケツにくむ（回避）

他に出てくるハッキング（ハック）という言葉 (2)

NTT Security

- ソーシャルエンジニアリング（デジタル大辞泉）
  - コンピューター犯罪の手法の一。パスワードや暗証番号などのセキュリティー上重要な情報を、身分を詐称して聞き出したり、キーボード操作を盗み見たりするなどの人的手段で不正に入手することを指す。ソーシャルハッキング。ソーシャルクラッキング。

- 代表的な目標はパスワードの不正入手だが, パスワードを聞き出すだけとは限らない

アメリカの 911（緊急電話番号）で実際にあった事例

NTT Security

911です。どちらで緊急事態が発生しましたか？

大通りの 123番地です

OK, そこで何が起きましたか？

ピザの配達をお願いしたいのですが

アメリカの 911（緊急電話番号）で実際にあった事例

NTT Security

奥さん, あなたは 911に電話していますよ

はい, 分かっています。ラージサイズのピザをペパロニ, キノコとトウガラシのハーフ&ハーフでお願いします。

申し訳ありません。あなたは 911におかけになったことを承知してますよね？

はい, どのくらいかかりますか？

アメリカの 911（緊急電話番号）で実際にあった事例

NTT Security

OK, 奥さん。
そちらは大丈夫？ 緊急事態なの？

はい

誰かがそこにいるから, 正直な話ができないの？

はい, そうです。どれくらいかかりますか？

アメリカの 911（緊急電話番号）で実際にあった事例

NTT Security

そちらまで約1マイルの距離に警官がいます。あなたの家に武器はありますか？

いえ。

このまま会話を続けられますか？

いえ。それでは, ありがとう。

アメリカの 911（緊急電話番号）で実際にあった事例

NTT Security

- 会話内容を監視されながら目的を達成することができた

- 話しても良い単語・文章が限定された状況で（制約）
- 助けを呼ぶことができた（回避）

じゃあ, コンピューターの世界のハッキングって何？

NTT Security

- 難しそうに聞こえるけど, 必ずしも難しい話とは限らない
- でも, 通常では思いつかないような発想が必要（コロンブスの卵）
- 分かりやすい例でいうと……


MARIO
031300
×00
WORLD
3-1
TIME
260
1UP

マリオの無限 1UP

NTT Security

- 想定された仕様と実行できる機能にズレ（脆弱性）がある
- 決められたルールの中でプレイしている（制約）が, 開発者の意図に反してゲームの難易度を下げられてしまう（回避）
- ゲームならまだ良いが, 銀行口座のお金が無限に増えたら大変！
- （狭義の）ハッキングとは、平たくいうと裏技を使うこと

（参考）バックドア

NTT Security

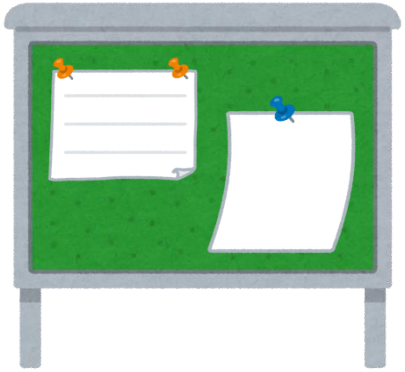
- 似て非なるものに「バックドア」がある
- ゲームに例えるなら, 隠しコマンドに相当する
- 開発者が意図して埋め込んだというところが異なる
- たまに脆弱性として報告されるが, 実は違うもの（対処が必要という意味ではあまり区別する必要はない）

よりコンピューターの世界に近い問題設定を考えてみましょう

[例1] 制約を回避する易しめの問題

NTT Security

- 太郎くんは掲示板を管理していて, アルバイトの花子さんに依頼された掲示物を受け取って掲示するようにお願いしています
- ただし "スクリプト" という文字だけはどうしても掲示したくないので, 花子さんに『内容を確認して "スクリプト" という文字が含まれていたら, その文字だけを削除して掲示するように』という指示を出しました
- ところが, しばらくして掲示板を見ると "スクリプト" という文字が書いてありました
- 花子さんが指示通りに従っていたとしたら, これはなぜ起こってしまったでしょうか？



- 花子さんが人間であれば通常は起きない誤り
- 花子さんがコンピューターであれば発生しうる
- "スクリプト" という文字を削除するだけでは不十分

[例2] 制約を回避する少し難しい問題

NTT Security

- 太郎くんは花子さんに唯一の連絡手段である電話を掛けて話しかけることができます
- 花子さんはパスワードが書かれた封筒を持っています
- 太郎くんは花子さんに電話で何でもお願いをすることができます
- ただし「管理人」に行動を監視されていて, 花子さんが一言でも話をしようとすると, 強制的に電話を切られてしまいます
- 太郎くんが花子さんのパスワードを知る方法はあるでしょうか？

[例2] 制約を回避する少し難しい問題

NTT Security

- 太郎くんは花子さんに唯一の連絡手段である電話を掛けて話しかけることができます
- 花子さんはパスワードが書かれた封筒を持っています
- 太郎くんは花子さんに電話で何でもお願いをすることができます
- ただし「管理人」に行動を監視されていて, 花子さんが一言でも話をしようとすると, 強制的に電話を切られてしまいます
- 太郎くんが花子さんのパスワードを知る方法はあるでしょうか？

実は, 今年の DEFCON CTF 予選で出題された問題（をデフォルルメしたもの）

[例3] コンピューターの仕組みに関わる問題

NTT Security

- 太郎くんはツアーを申し込もうと旅行代理店に来ています
- 窓口の花子さんは, 手元のマニュアルに従いながら申込み用紙に記入します

申込み用紙

山	田	太	郎						
沖	縄	県	宮	古	島	市	平	良	下
里	3	1	5	宮	古	島	市	中	央
公	民	館							×
こ	こ	は	事	務	連	絡	欄	で	す
申	請	書	の	記	入	が	完	了	し
た	ら	受	付	カ	ウ	ン	タ	ー	に
転	送	し	て	く	だ	さ	い		

マニュアル

1. 名前を聞く. 10文字以下なら 1マス目から記入する. そうでないなら聞きなおす.
2. 住所を聞く. 30文字未満なら 10マス目から記入する. そうでないなら聞きなおす.
3. 学生かどうか聞く. 学生であればその場で学生証を確認して, 40文字目に○を入れる. そうでないなら×を記入する.
4. 申込み完了. 申請書の 40文字目以降に書いてある指示に従い, 支払い処理に進む.

[例3] コンピューターの仕組みに関わる問題

NTT Security

- 太郎くんはツアーを申し込もうと旅行代理店に来ています
- 窓口の花子さんは, 手元のマニュアルに従いながら申込み用紙に記入します
- 2と3 が逆で,「未満」を「以下」とすると問題がありますか？

申込み用紙

山	田	太	郎						
沖	縄	県	宮	古	島	市	平	良	下
里	3	1	5	宮	古	島	市	中	央
公	民	館							×
こ	こ	は	事	務	連	絡	欄	で	す
申	請	書	の	記	入	が	完	了	し
た	ら	受	付	カ	ウ	ン	タ	ー	に
転	送	し	て	く	だ	さ	い		

マニュアル

1. 名前を聞く. 10文字以下なら 1マス目から記入する. そうでないなら聞きなおす.
2. 学生かどうか聞く. 学生であればその場で学生証を確認して, 40文字目に○を入れる. そうでないなら×を記入する.
3. 住所を聞く. 30文字以下なら 10マス目から記入する. そうでないなら聞きなおす.
4. 申込み完了. 申請書の 40文字目以降に書いてある指示に従い, 支払い処理に進む.

[例4] コンピューターの仕組みに関わる深刻な問題

NTT Security

- 太郎くんはツアーを申し込もうと旅行代理店に来ています
- 窓口の花子さんは, 手元のマニュアルに従いながら申込み用紙に記入します
- 「30文字未満」という制限を忘れるとどうなるでしょうか？

申込み用紙

山	田	太	郎						
沖	縄	県	宮	古	島	市	平	良	下
里	3	1	5	宮	古	島	市	中	央
公	民	館							×
こ	こ	は	事	務	連	絡	欄	で	す
申	請	書	の	記	入	が	完	了	し
た	ら	受	付	カ	ウ	ン	タ	ー	に
転	送	し	て	く	だ	さ	い		

マニュアル

1. 名前を聞く. 10文字以下なら 1マス目から記入する. そうでないなら聞きなおす.
2. 学生かどうか聞く. 学生であればその場で学生証を確認して, 40文字目に○を入れる. そうでないなら×を記入する.
3. 住所を聞く. ~~30文字以下なら~~ 10マス目から記入する. ~~そうでないなら聞きなおす.~~
4. 申込み完了. 申請書の 40文字目以降に書いてある指示に従い, 支払い処理に進む.


CTF 風景

CTF (Capture the Flags) とは

NTT Security

- CTF とは
  - 日本語で「旗取り合戦」という意味
  - ルールに則っている限り合法的に参加できる，「（広義の）ハッキング」の技術力を競うコンテスト
  - 世界中で毎週のように開催されている
- CTF で必要となる (身に付く) スキル
  - コンピューターに関するあらゆる技術・知識
  - 自分でプログラムを書いたり解析する実践的なスキル
  - 攻撃手法を知り脅威に対する具体的な対策を考えリスク評価ができるスキル

CTF の競技形式

NTT Security

- **オンライン型**
  - 予選はオンラインで問題出題型で行われることが多い
  - 一般的にチームの人数制限はなく, パソコンとインターネット接続環境があれば誰でも自由に参加可能
  - 競技時間が48時間など長丁場となるため, 上位を狙うのであればチームで取り組む
- **オフライン型**
  - チームの人数制限や競技時間はコンテストごとに様々
  - 攻防戦型など
- **問題出題型**
  - 問題に解答して得たフラグをスコアサーバーに送って得点する
  - 最初は一部の問題しか提供されず, 一番に解いたチームが次の問題を選択するものもある (Jeoperdy 形式)

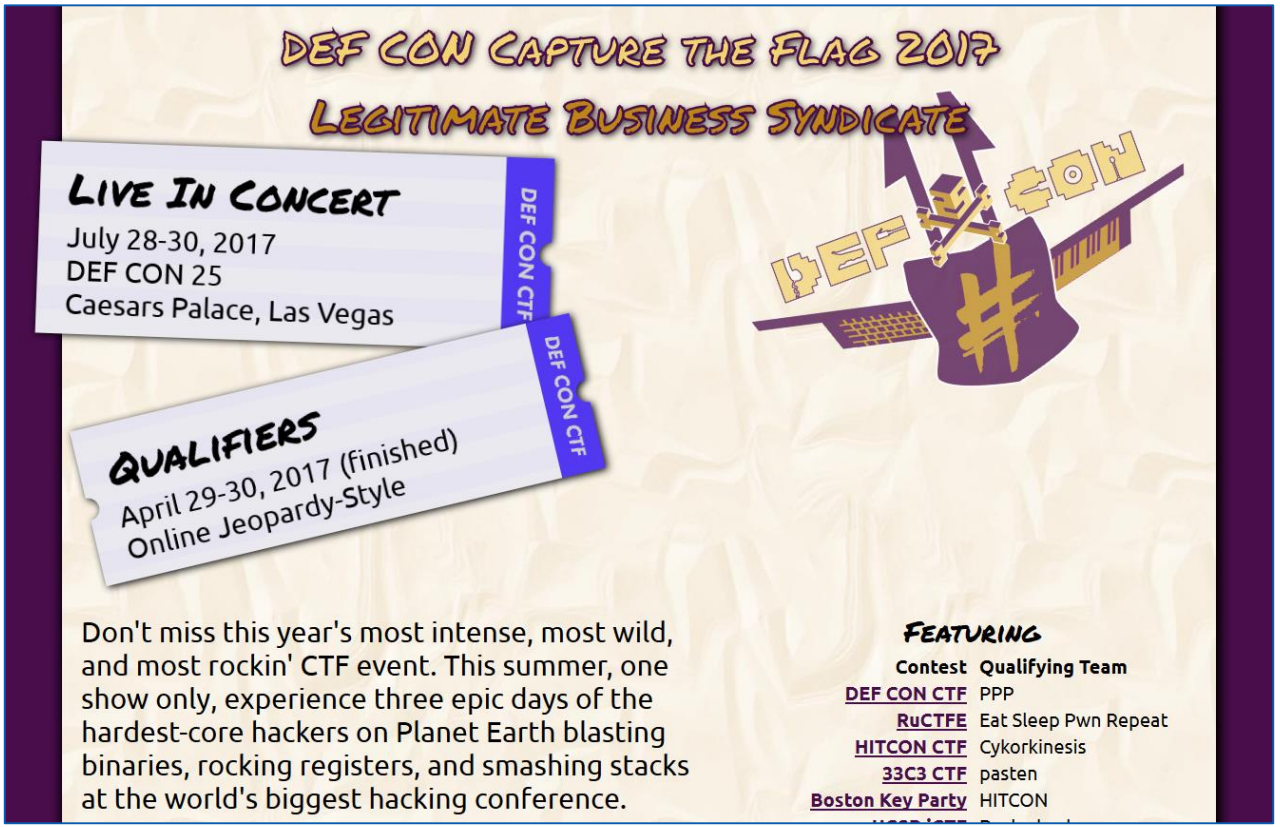
スコアサーバー（例）

NTT Security

3dub	0x41414141	\xff\xe4\xcc	OMGACM	gnireenigne
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4
5	5	5	5	5

CTF の紹介 (1)

- **DEFCON CTF (legitbs.net)**
  - 毎年ラスベガスで開催されるセキュリティイベント「DEFCON」で行われるコンテストで, 難易度は CTF の中でも最高峰
  - 毎年 5月頃に予選, 8月頃に本戦が行われる
  - 2017年は予選の成績上位8位とシード枠の7チームが本戦へ



CTF の紹介 (2)

NTT Security

- **SECCON CTF (seccon.jp)**
  - 2012年から開始した国内発の中で最大規模のコンテスト
  - 初心者向けの「SECCON Beginners」や女性向けの「CTF for GIRLS」などのイベントも実施し，育成にも積極的

問題配布のイメージ

- 各問題のページを開くとファイルがダウンロードできる
- 問題文はあってないような場合が多い

CTF の問題ジャンルを大きく分類すると……

NTT Security

- 「攻略問題」（狭義のハッキング問題）
  - 制約を回避して何かしらの目的を達成する（今までの話）
- 「宝探し問題」（広義のハッキング問題）
  - ファイルやプログラムを解析して埋め込まれた情報を発見する

- 「宝探し問題」をデモを交えて紹介

SECCON つくば大会: この城の名前は何ですか？

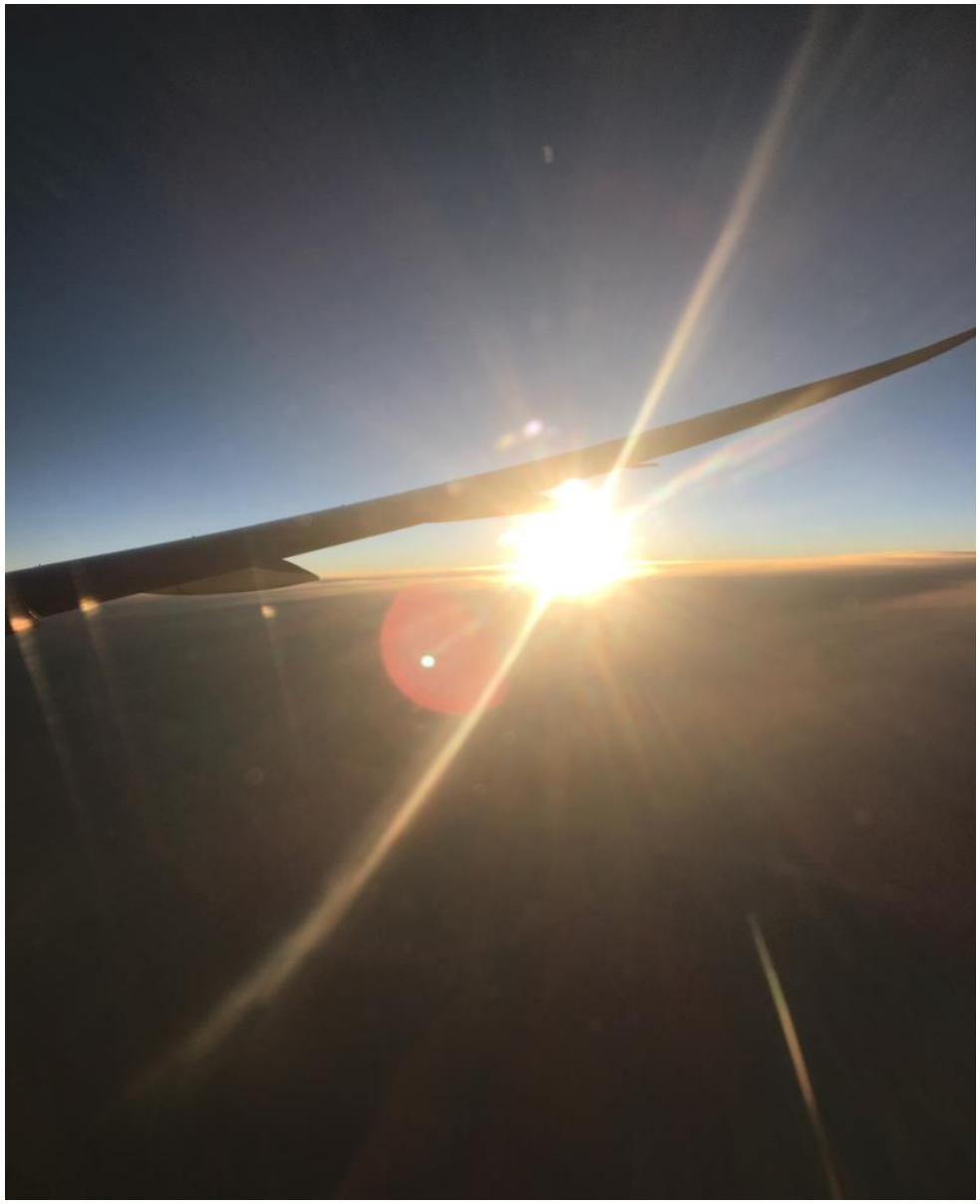
NTT Security

SECCON CTF 2013 予選: ここはどこ？

NTT Security

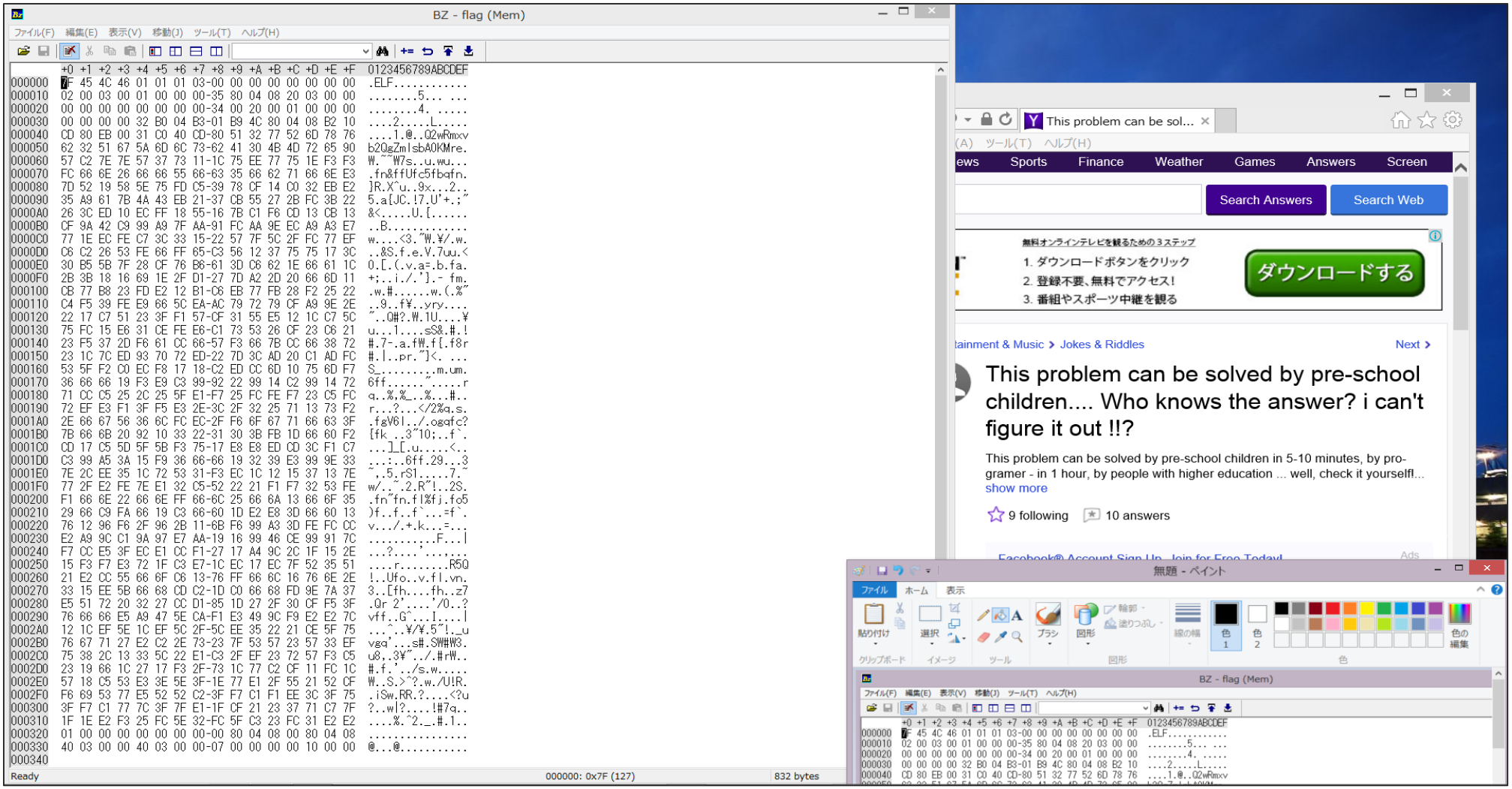
SECCON CTF 2015 予選: Steganography 2

NTT Security

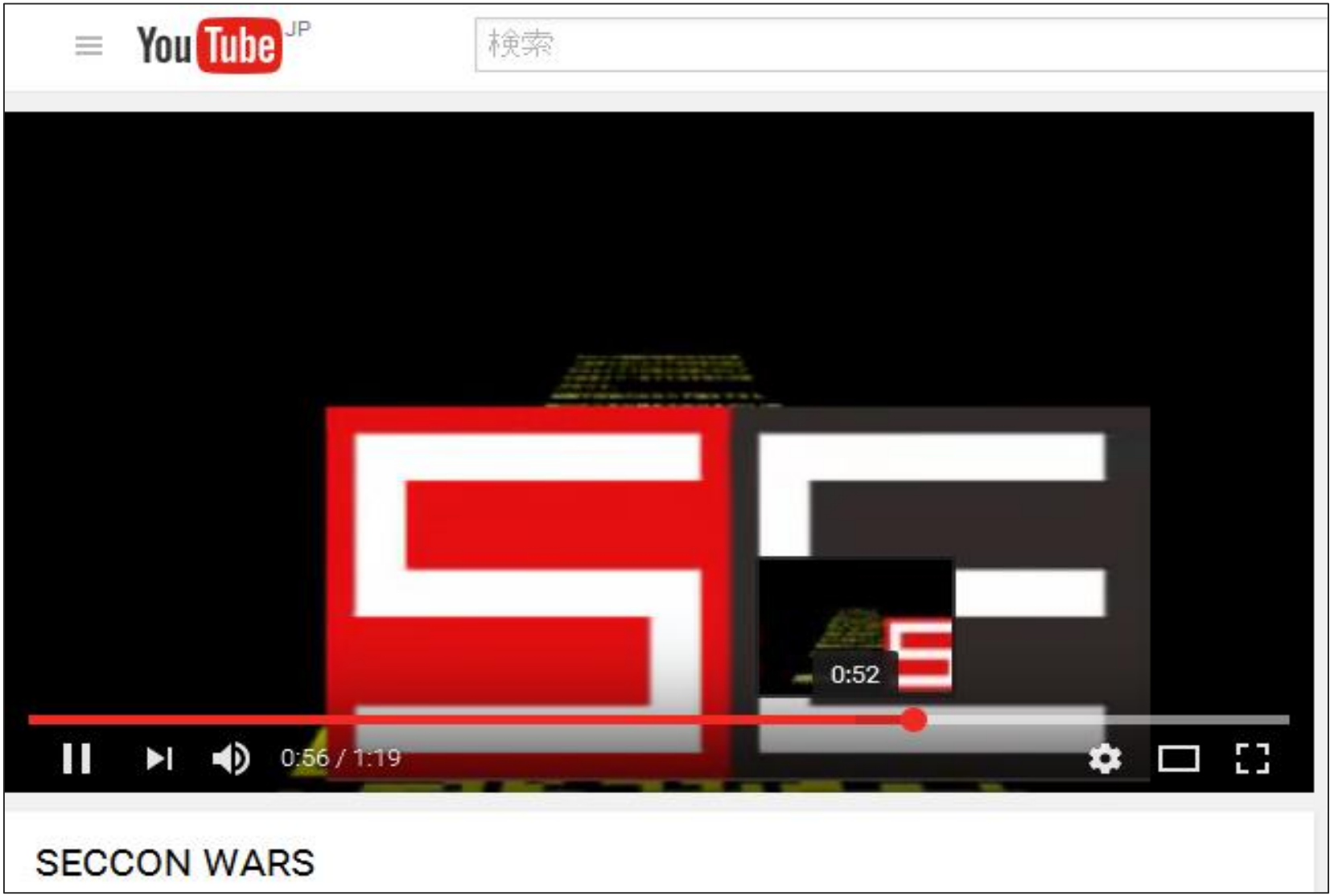


SECCON CTF 2015 予選: Steganography 3

NTT Security



- 動画のリンクが与えられる



SECCON 2014 予選2: BBQR

NTT Security

参加したいと思ったら

NTT Security

- まずは登録してみよう
  - CTF Time (ctftime.org) で CTFを探す
  - 年齢や参加資格など制限がある場合があるので注意
  - オンライン形式は不参加でもペナルティはない
  - 1人でも良いので登録してみよう
  - 時間がなくても登録してみよう
  - 1時間でも参加して, まずは問題を見てみよう
- メンバーを集めよう
  - 可能であればメンバーがいると良い (相談したり, 競争したり)
  - 情報共有の方法を決めておこう

勉強したいと思ったら

NTT Security

- 勉強会や初心者向けイベントに参加しよう
  - SECCON Beginners (seccon.jp)
  - SECCON CTF for GIRLS (seccon.jp)
- 書籍・資料
  - セキュリティコンテストチャレンジブック CTFで学ぼう! 情報を守るための戦い方 (ISBN-13: 978-4839956486)
  - セキュリティコンテスト攻略のためのCTF問題集 (ISBN-13: 978-4839962135) **7/28発売**

「team enu」の DEF CON CTF 参加レポート

NTT Security

2016年

NTTセキュリティ・ジャパン株式会社 @NTTSec_JP · 7月28日

DEF CON CTF 2016 予選の参加レポートを公開しました。今年のコンテストの傾向、「Team Enu」の取り組みの様子、そして解答した問題の解説（7問）など、例年より充実した内容となっています。

ntt.com/content/dam/nt …

2017年

NTTセキュリティ・ジャパン株式会社 @NTTSec_JP · 6月9日

「Team Enu」で DEF CON CTF 2017 予選の反省会を開催しました。得点と順位の振り返り、チーム内の連携方法などの作戦についての議論、時間内に解答できなかった問題の解説を行いました。nttsecurity.com/-/media/nttsec…

サーバ接続時に "YUM, got 32 bytes!" と表示されなかった場合がありましたが、これは SSP によって子プロセスがダウンし、後続の出力処理が実行されなかったということです。

ここで SSP の機能について考えます。SSP は、関数が呼ばれた際に Stack Canary と呼ばれるランダム値をスタックに挿入します。そして関数からのリターン時に Stack Canary の値を検証し、値が変わっていた場合はエラーを出力し終了する仕組みです。よって、バッファオーバーフローを用いてサーバの制御を奪取するには、**Stack Canary を書き換えずにその先にあるリターンアドレスを書き換える**必要があります。

次に攻略方針を練ります。Stack Canary はプログラム起動時にランダムな値が設定されますが、今回のサーバは fork 関数で生成された子プロセスが入力を受け付けています。Stack Canary を書き換えると子プロセスが終了しますが、このときに親プロセスはそのまま生きているため、Stack Canary の値は変わりません。つまり、800 回のループの中では Stack Canary は不変ということになります。

Stack Canary の値を 1 バイトずつ順番に試していき、プロセスが強制終了するかどうか（SSP が発生するかどうか）で Stack Canary の値を特定することができないでしょうか。

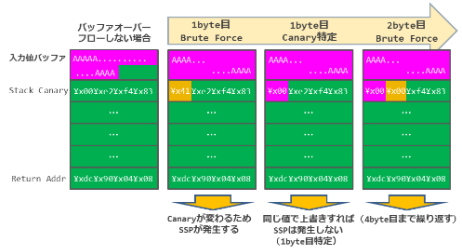


図 3-2 Byte-by-Byte Brute Force による Stack Canary 特定のイメージ

NTT Communications Corporation
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo
100-8019, Japan

NTT Communications Global ICT Partner

40

今年の問題ジャンルの振り返り（詳細1）

※難易度は主観です

問題	得点	ジャンル（公式）	ジャンル（実際）	Reverse 難易度	解答 難易度	攻撃手法、理解すべき脆弱	解答
beatmeonthedl	40	Baby	Pwn	易	易	leak, unlink attack	○
crackme1	15	Baby	RE	易	易	Angr	○
empanada	98	Baby	Pwn	易	中	UAF	○
floater	65	Baby	SC	易	中	float	○
smashme	24	Baby	Pwn	易	易	ROP	○
Leo es Pequeno	70	Pwn	Pwn	易	中	ROP	○
bedint	94	Pwn	Pwn	中	中	leak, fastbins attack	△
peROPdo	69	Pwn	Pwn	易	易	ROP	○
mute	62	Pwn	SC	易	易	blind attack	○
insanity	143	Pwn	Pwn	易	中	PCM, stack BoF	△
reeese revenge	234	Pwn	Pwn	?	?	MIPS , stack BoF	×
nobinaloth	436	Pwn	?	?	?	?	×
faggin	234	Pwn	?	?	?	?	×

[凡例]
・ジャンル（実際）
Pwn: Pwnable
RE: Reverse Engineering
SC: Shellcode
・解答
○: 解けた
△: 惜しかった，解決方針は合っていた
×: 見当つかず

ご清聴ありがとうございました

参考

- ASCII.jp デジタル用語辞典 ハッキング
  http://yougo.ascii.jp/caltar/ハッキング
- goo辞書 ハッキング
  https://dictionary.goo.ne.jp/jn/177243/meaning/m0u/ハッキング
- Wikipedia ハッキング
  https://ja.wikipedia.org/wiki/ハッキング
- goo辞書 ライフハック
  https://dictionary.goo.ne.jp/jn/244724/meaning/m0u/ライフハック
- 「それをそこで使うのか！」と思わず叫んでしまうライフハック画像集
  http://rocketnews24.com/2014/03/09/420600/
- goo辞書 ソーシャル-エンジニアリング
  https://dictionary.goo.ne.jp/jn/129716/meaning/m0u/ソーシャルエンジニアリング
- アメリカの緊急電話番号「911」に掛かってきた電話のやりとり
  https://www.youtube.com/watch?v=oH4GKN3j2F8
- Super Mario Bros. - World 3-1 Infinite Lives Trick
  https://www.youtube.com/watch?v=J-cWQFk9bi8
- DEF CON Capture the Flag 2017
  https://legitbs.net/
- SECCON 2017
  https://2017.seccon.jp/
- SECCON Wars
  http://youtu.be/1pC56S17-_A