CTF 各ジャンル紹介

～ Pwn, Forensics, Programming, Cryptography and Misc ～

totti

Ver. 資料用

目次

○自己紹介

○セキュリティ業界とCTF

- CTFとは
- セキュリティ業界とCTFの関係
- CTFをやる意味

○各ジャンル紹介

- Pwn
- Forensics
- Programming
- Cryptography

自己紹介（totti：二年目社員）

○業務

- プラットフォーム診断　（2016年 7月～9月）
- APT先制攻撃サービス　（2016年 10月～）

○業務（副）

- アカデミー補助講師（雑用）
- LACCON 運営
- 即！西本面接問題作成

○その他

- 学内 CTF 運営、問題作成、スコアサーバ作成
- CTF の専門ジャンルは Pwn、Exploit（その他のジャンルは初級程度）
- ずっと軽音やってた（中学時代からライブ出てた）
- にわかオタク

目次

セキュリティ業界と CTF

○CTF とは

情報技術に関する問題に対して適切な形で対処し、
それに応じて得られた得点で勝敗を決める（※右引用）

今は調べれば情報いろいろ落ちてるので各自でよろ

・例

- Webサーバに存在する脆弱性によってDBの内容を取得し
  本来一般の利用者には閲覧できない情報からフラグ（答え）を得る

- なんらかの脆弱性をついて相手のサーバを乗っ取ることによって
  サーバ上に存在するファイルを閲覧しフラグ（答え）を得る

※ https://www.amazon.co.jp/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-碓井-利宣/dp/4839956480

？🤔？

CTF やるのはいいけどセキュリティ “業界” とどう関係するの？

セキュリティ業界とCTF

○セキュリティ業界におけるセキュリティ

一般的にお客さんが知りたいのは

「現状どんな脆弱性があって、どう対策すればいいのか」
「我々が抱えているリスクはどの程度のものなのか」

などであって攻撃手法ってのは割とぶっちゃけどうでもいい。

そして現在、診断員側にとっても診断は**基本脆弱性を検知するツールを用いて診断する**ので実際診断員に攻撃手法の知見はなくてもできてしまう。

！  ！

そんな事思ってるからいつまでも守る側が後手引いてるんじゃないですかねぇ…

セキュリティ業界と CTF

○CTF をやる意味

・攻撃手法がわかれば、セキュリティベンダの対策手法も見えてくる
→検知率99.9%？ふむふむそうしてるのね。
「え、別にそれなら○○するだけで突破できるのでは？」

・次への攻撃の予測が可能
→ struts2 の時とか「OGNLねぇ、いやこれこういうのあれば S2-046 いけるのでは」

・脆弱性に対して正確に理解でき、お客さんへ的確に説明ができる
→「いやそれはないですね🤔」とか普通に言える（「IPA がこう言ってますので～」とかありえないんだよな～）

・N氏
→「いや本当にセキュリティできる人なら別に CTF でもできるでしょ」

ぶっちゃけ誰が何言おうがどうでもよくて、好きでやってるだけっていうね

目次

○自己紹介

○セキュリティ業界とCTF
- CTFとは
- セキュリティ業界とCTFの関係
- CTFをやる意味

○各ジャンル紹介
- ジャンル一覧
- Pwn
- Forensics
- Programming
- Cryptography

ジャンル一覧

○ジャンル一覧

過去 CTF の問題のジャンルとして挙がったもの
CTF time から抜粋

ジャンル一覧

Pwning (Pwnable／Pwn)
Web
Network
bin (binary)
Forensics (For)
Reversing (Reverse)
Cryptography (Crypto)
Steganography (Stego)
PPC (Professional Programming and Coding)
Programming
Trivia
Miscellaneous (misc)
Recon (Reconnaissance)
Exploitation (Exploit)
Puzzle
Crazy
Game (Joy)
Shellcode
assembly
exif
php
SPARC
android
otp (One Time Password)
ACM (Association for Computing Machinery)
Strange
Packet
Vuln (Vulnerability)
zpool
GPG
ARM
mongoDB
PRNG (暗号論的擬似乱数生成器)
GAE (Google App Engine)
Qt (C++)
GPU (Graphics Processing Unit)
cuda (GPU向けC統合開発環境)
LaTeX
js
node.js
vernam
apache
haskell
vm (vm ware)
Bochs (PC/AT emulator)
django
dumpster_diving (Garbage picking)
Gopher
rickroll
ascii
ANSI
pcap
DTMF
QBasic
trollface
RSA
XSS
admin
Delphi
sqli
8085
MK61 (calculator)
sha1
DES
freebsd
Dalvik (vm)

ジャンル一覧(まとめ)

○ジャンル一覧

- Pwning, Exploit
- Reversing, Binary
- Web
- Network
- Cryptography, Steganography
- Forensics
- Recon
- Misc, Trivia

ジャンル一覧(まとめ)

〇めちゃめちゃ簡単に説明するよ

- Pwning, Exploit
- Forensics
- Programming
- Cryptography
- Misc, Trivia

ジャンル一覧（まとめ）

〇以下の流れで説明するんな

- 一言でいうと
- 実世界との関係
- 必要な知識
- 備考

Pwning, Exploit

○一言で言うと

プログラムのバグを突いて端末の不正なリモート操作を行う
(端末を乗っ取る)

○実世界との関係

バッファオーバーフローによって任意のコードが実行可能
任意のPoCの作成

○必要な知識

各CPUの機械語、アセンブリ言語
OSに関わるその他諸々(OSそのもののセキュリティ機構、リンカ、ローダ、プロセス、仮想メモリ)
リバースエンジニアリング
共有ライブラリとその仕様

Pwning, Exploit

○備考

圧倒的に配点が高い(解くのに必要な知識が圧倒的に多い)
資料が少なくこの分野の人何言ってるのかわからないことが多いため難解(決して難しい話してるわけじゃない)
このジャンルに入ってくるには覚悟が必要(口が悪くなる)
このジャンルが理解できるようになるとすべてのジャンルを理解できるようになる

Forensics

○一言で言うと

証跡調査

○実世界との関係

コンピューター関係の犯罪とかの証拠探し

○必要な知識

ファイルシステム
メモリ調査
コンピュータ関連の何かしらの復元

○備考

CTF においてフォレンジックは、正直問題として出たタイミングではその知識はなく
とりあえず時間内に検索して復元するというパターンが多い（気がする）

Programming

○一言で言うと

手作業では面倒／不可能なものを、プログラムを組むことによって解決する

○実世界との関係

プログラミングによる問題解決能力

○必要な知識

応用力？

○備考

CTF ではあまり競プロのような速さを求められる問題は出ない

Cryptography

○一言で言うと

暗号の世界(そのまま)

○実世界との関係

機密性そのもの

○必要な知識

数学

○備考

The 知

もう最近このジャンルは世界の論文から探す感じ

Misc, Trivia

○一言で言うと

一般的なジャンルから外れた問題はだいたいこのジャンル

○実世界との関係

トリビア的な感じなので面白クイズ的なものが多い

○必要な知識

検索力

○備考

なぞなぞみたいなのも多く初心者はとっかかりやすいかも
エスパー力も結構必要だったりするときがある

目次

おしまい

興味がある事を好きにやってくのが一番！