情報セキュリティプロジェクト 4月 月例報告会

小俣直史

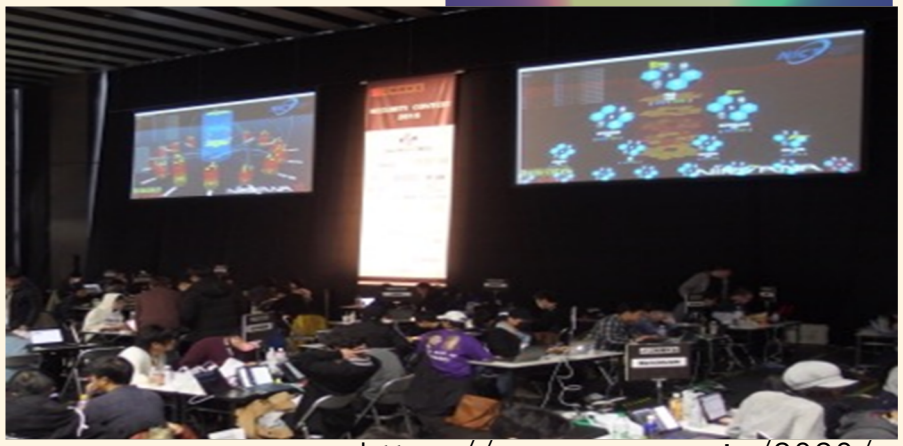
工学部 知能情報システムプログラム 3年

1. プロジェクト概要
2. 今年度の目標
3. 今年度の活動予定
    1. 全体
    2. 高レイヤ
    3. 低レイヤ
    4. 1年生
    5. 参戦CTFについて

プロジェクト概要

- **活動内容**
  CTF という競技を通じ、情報セキュリティ技術を学習する
- **目標**
  日本最大級のCTFである
  SECCON CTF という大会で**優勝**
- **活動予定:週3回（当面の間）**
  1. 高レイヤ
  2. 低レイヤ
  3. １年生

  *曜日・時間帯は各部員の時間割を把握した上でタームごとに決定
- **活動場所**
  - 基本**Zoom, Discord**上



https://www.seccon.jp/2020/
http://www.security-next.com/101404

プロジェクト概要

- **CTFとは?**
  - サイバーセキュリティの技術を競い合うコンテスト
  - 問題の中から隠されたFLAGと呼ばれるもの
    を見つけ出し、得点を稼ぐ競技

問題のジャンル一例:

Reversing: プログラム解析

Pwn: コンピュータの脆弱性攻撃

Web: サイト/サーバ間処理の知識

Network: 通信(TCP/IP等)の知識

プロジェクト概要

- 二つのチームに分かれて、活動を行います。

低レイヤ班
(コンピュータシステム)

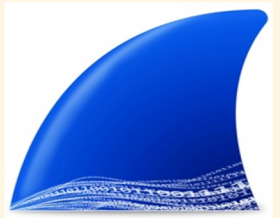
サーバーの乗っ取りを行う
技術の学習

CTF では
- **Pwn**
- **Reversing**

を担当

高レイヤ班
(ネットワーク)

ウェブや通信を介した
情報漏洩に関する知識の学習



CTF では
- **Web**
- **Network**

を担当

今年度の目標

- **前年度の副次的活動**: (CTF以外)
  - 高レイヤ: バグバウンティ(脆弱性報酬金制度)
  - 低レイヤ: OS作成
  - 目的: CTFにおける基礎技術を学習する

- 反省:
  - 戦力の分散
    - CTF向けの学習と副次的な活動がどっちつかずになっていた
    - それにより，部員のプロジェクトへのモチベーションも低下していた
      →多くの離脱者

今年度の目標

- **今年度はCTFに集中し，CTFを中心としたコンピュータ/ネットワークのセキュリティ技術の習得を目指す。**
  - 3-4ヶ月の周期でCTFに取り組む
  - “技術習得” → “CTFへの参戦” → “ハンズオン(復習)”
    というサイクルを繰り返す

今年度の活動予定 – 全体

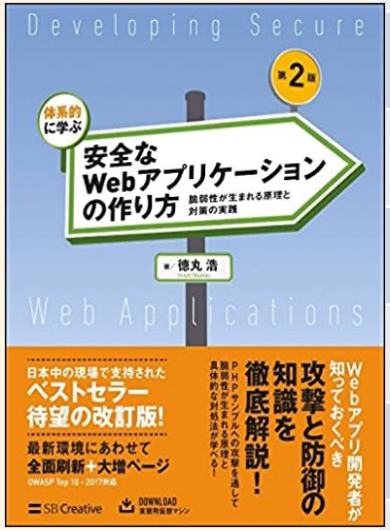
未定の箇所については，チームの学習進度や開催状況を考慮して決定後，報告させていただきます。

CLPWN for C.T.F

	高レイヤ	低レイヤ	新入生
4月	新歓活動，新入生指導用資料の整備，顔合わせ(4/26予定)		
5月	**昨年度学習内容の振り返り**		Linux基礎 / C言語学習(各自)
6月	**SECCON Beginners CTF(予定)に参加, ハンズオン**		低レイヤ基礎 / C言語
7月	ウェブアプリの機能	C++プログラムの解析	高レイヤ基礎 / C言語
8月	SQL等処理系の脆弱性	Mallocの学習	習熟度テスト，レイヤ配属
9月	I/O, OSに関する脆弱性		
10月	**SECCON CTF 2021 に参加, ハンズオン**		
11月	(未定)	(未定)	
12月	(未定)	(未定)	
1月	**CTFに参加(大会は未定), ハンズオン**		
2月	成果発表会		

今年度の活動予定 – 高レイヤ

- 使用テキストは
  体系的に学ぶ
  安全なWebアプリケーションの作り方
  第2版 脆弱性が生まれる原理と対策の実践
  徳丸 浩 著



- Webアプリケーションの動作原理から，サーバーサイドとクライアント(ユーザー)サイドの処理における脆弱性を学び，CTF Web 分野の攻略に活かす。
- 予備知識として，
  PHP: http://bashalog.c-brains.jp/category/series/php/ ，
  HTML: https://dotinstall.com/lessons/basic_html_v5 ,
  SQL: http://sql.main.jp/

  上記言語の学習を行う。各自で進める

	高レイヤ
5月	**昨年度学習内容の振り返り**
6月	SECCON Beginners CTF に参加, ハンズオン
7月	ウェブアプリの機能
8月	SQL等処理系の脆弱性
9月	I/O, OSに関する脆弱性
10月	SECCON CTF 2021 に参加, ハンズオン
11月	(未定)
12月	(未定)
1月	CTFに参加(大会は未定), ハンズオン
2月	**成果発表会**

今年度の活動予定 – 低レイヤ

- 使用テキストは
  - **CTFを解きながら学ぶバイナリ解析**
    電気羊 著
  - **Malleus CTF Pwn Second Edition**
    kusano_k 著

- 筆者が作成したCTF例題を基に，CPUの命令など計算機の動作原理を学び，実行ファイルの脆弱性を解析してCTF Pwn 分野の攻略に活かす。
  前者の方が難易度が低いため
  11月からの1年生の学習には
  前者から使用していく。

	低レイヤ
5月	**昨年度学習内容の振り返り**
6月	SECCON Beginners CTF に参加, ハンズオン
7月	C++プログラムの解析
8月	Mallocの学習
9月	
10月	SECCON CTF 2021 に参加, ハンズオン
11月	(未定)
12月	(未定)
1月	CTFに参加(大会は未定), ハンズオン
2月	**成果発表会**

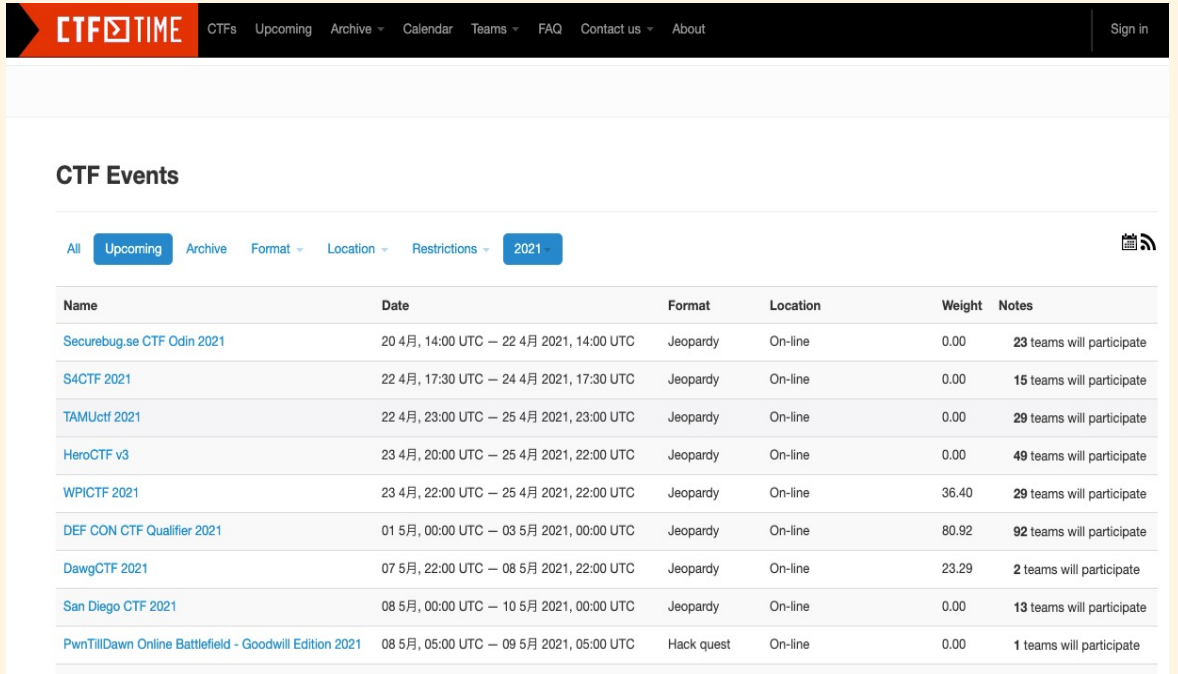
今年度の活動予定 – 新入生

- 上級生が作成した資料を用いて
  最初の３ヶ月で以下を習得してもらう:
  - Linux(セキュリティツールの利用，シミュレートに最適なOS)の利用方法
  - 各レイヤの基礎知識
  - C言語(独習。苦しんで覚えるC言語 https://9cguide.appspot.com/ を使用)
    - 先輩で質問対応&サポート
- その後，習熟度確認を行いレイヤ配属を行う。
  CTFにも少しずつ参加してもらう。

	新入生
5月	Linux基礎 / C言語学習(各自)
6月	低レイヤ基礎 / C言語
7月	高レイヤ基礎 / C言語
8月	習熟度テスト，レイヤ配属
9月	(配属先による)
10月	SECCON CTF 2021 に参加, ハンズオン
11月	(配属先による)
12月	(配属先による)
1月	CTFに参加(大会は未定), ハンズオン
2月	**成果発表会**

今年度の活動予定 – 参戦CTFについて

- 3-4ヶ月の周期でCTFに取り組む
  - SECCON CTF 2021(10月開催予定)
  - SECCON Beginners CTF 2021 (5-6月開催予定)
  - 1月周辺に開催のCTF(未定)
    - CTFTIME.org(CTFの開催告知サイト)より，内容や難易度を確認した上で今後決めていく。



Name	Date	Format	Location	Weight	Notes
Securebug.se CTF Odin 2021	20 4月, 14:00 UTC — 22 4月 2021, 14:00 UTC	Jeopardy	On-line	0.00	**23** teams will participate
S4CTF 2021	22 4月, 17:30 UTC — 24 4月 2021, 17:30 UTC	Jeopardy	On-line	0.00	**15** teams will participate
TAMUctf 2021	22 4月, 23:00 UTC — 25 4月 2021, 23:00 UTC	Jeopardy	On-line	0.00	**29** teams will participate
HeroCTF v3	23 4月, 20:00 UTC — 25 4月 2021, 22:00 UTC	Jeopardy	On-line	0.00	**49** teams will participate
WPICTF 2021	23 4月, 22:00 UTC — 25 4月 2021, 22:00 UTC	Jeopardy	On-line	36.40	**29** teams will participate
DEF CON CTF Qualifier 2021	01 5月, 00:00 UTC — 03 5月 2021, 00:00 UTC	Jeopardy	On-line	80.92	**92** teams will participate
DawgCTF 2021	07 5月, 22:00 UTC — 08 5月 2021, 22:00 UTC	Jeopardy	On-line	23.29	**2** teams will participate
San Diego CTF 2021	08 5月, 00:00 UTC — 10 5月 2021, 00:00 UTC	Jeopardy	On-line	0.00	**13** teams will participate
PwnTillDawn Online Battlefield - Goodwill Edition 2021	08 5月, 05:00 UTC — 09 5月 2021, 05:00 UTC	Hack quest	On-line	0.00	**1** teams will participate

ご静聴ありがとうございました。