Tower of Hanoi CTF team

Daniele Iamartino
ダニエレ・ヤマルティーノ

Tower of Hanoi の紹介

- イタリア最大の工科大学である “Politecnico di Milano” の20人で構成するチーム
- ほぼ全員がコンピュータエンジニアの学生：学部、 修士課程、 博士課程の学生

Tower of Hanoi の紹介

- プログラミングチャレンジやシステム管理を愛し、エクスプロイト／リバースエンジニアリング／フォレンジックス／暗号にワクワクするメンバーが大半
- コンピュータセキュリティの新しいトピックに触れることを楽しんでいる

ヒストリー

- Tower of Hanoi (ToH) は、Stefano Zanero 教授と彼のコンピュータセキュリティコースの学生が創設
- ToHは2004年のUCSB iCTFから参加
- iCTF 2004、2005で優勝
- それ以来 iCTF に毎年参戦。多くの学生も毎年新しく参加
- 2010年よりその他のCTFにも参戦：DEFCON予選、CSAW、PPPCTF、RuCTFe、codegateなど。。。 楽しみを求めて ;)

イタリアのハッキングシーン

- 何人かの人は “終わっている”と言う...
- コミュニティは現在より以前のほうが活動的であった：
  - *ハックミーティング*（1998年よりアクティブ。自立したハッキングキャンプ)
  - *Sikurezza.org* (イタリアで最も重要なセキュリティのメーリングリストかも)
- 現在 (たぶん？)：
  - *MOCA*（講演を含むハッキングキャンプ、4年毎に開催）
  - *ESC*（ハッキングキャンプ）
  - 一部の人は *Chaos Communication Congress*（ドイツ）に参加
- *CAT*（ミラノで開催されるWiFiハッキング競技）*のような興味深いイベント*
- 過去の“ハッキングプレイヤー”の大半は現在は経済的理由で活動。現在はその他の公的な活動はそれほどない
- CTFチームは大学で構成される主要な３チームが存在 （ミラノ×２チーム、ベニス×１チーム）

ToHの参戦スタイル

- チームリーダであるAlessandro Barenghi (“キャプテン”と呼ばれる）がメンバーの “召集”を行い会議をとりしきる
- 大学内で興味を持つ学生を探す
- CTF競技前にたいていブリーフィングがある
  - 競技中に誰がトピックを研究/評価するべきか、誰がネットワークを管理し、IRC/通信を誰が管理するのかを相談
- 競技終了後は、結果、なにをレビューすべきでどのWriteupを読むべきか、良かった点・悪かった点、をショートミーティングで議論する

ToHの参戦スタイル

- インタラクティブなCTFの設定：**ISO/OSIスタックスタイル**
  - VPN、FW、ネットワークトラフィック、 内部LANの設定の監視役
  - 脆弱なアプリとそのリバースプロキシ、VM（“テスト用”と“脆弱な本番用”VM）の監視役
  - 脆弱なアプリの管理役
- Webアプリ“***Hanoi tasks***”: 多くのメンバーで参戦するので（時には３０名）いかに素早く誰が何をしているのかを把握するツール
  - 各自が自分は現在何をしているのかを記載し、全員で全員を監視する
  - Webアプリ上からピザをオーダーできる(笑)
- スコアボードのプロジェクタ投影は便利! :)

ツールボックス

- GDB、 wireshark、バイナリエディタ、ファイル復元 (photorec、 binwalk、 foremost...)、IDA
- インタラクティブなCTF向け：Etherape、 iptables 、 tcpdump/ngrepを活用する優秀なスキルはとても便利。（RuCTFsで利用した）flagをポストするシステムを開発
- クレイジーなプログラミング言語に精通した知識

おすすめ資料集

- DEFCON 予選の過去問など:
  http://www.nopsr.us/
- UCSB iCTF の過去問のページ:
  http://ictf.cs.ucsb.edu/
- Google検索で最近のCTFの“writeups” をググる
- CTF開催予定のカレンダーなど
  http://capture.thefl.ag/
- CTFを始めたい人向けの書籍:
- The Shellcoder's Handbook（シェルコーダーのハンドブック）

最終的に我々は何を学んだか

- チーム内のエキスパートと参戦する中で、限られた時間で（よりよいパフォームをするために）アイデアや考えの素早い切り替えとタスク分散の重要性を学ぶ
- 大学では学べない多くの事を学んだ (プログラミング言語、ネットワークプロトコル、エクスプロイト作成テクニック等)
- インタラクティブなCTFに挑戦する中で、リアルな環境下のネットワーク攻撃の防御方法を学ぶ
- 最も重要なことは、CTF競技を通じてセキュリティ的視点を磨けること。僕がプロジェクトに携わるときは、他の人が気づいていないすべてのセキュリティ問題の可能性について考えるようになった

直近のCTF (明朝(ていうか今夜!))：PoliCTF

- 「自分たちでCTF競技を開催しよう」

http://www.polictf.it/

日本時間: (11月18日 4:00AM → 19日 4:00AM)

- 今晩... ちょw 直前すぎるんですけど...
- でもまだ登録可能！ぜひ挑戦してね!

Thanks!

- 質問ある? :)

- 連絡先: otacon22@otacon22.it