CTF
как инновационный подход в подготовке специалистов по информационной безопасности

Минин Виктор
mvv@aciso.ru
Зеленчук Илья
ilya@hackerdom.ru

2012, г.Москва

Специалист по информационной безопасности - кто он?

- Администратор
- Разработчик
- Архитектор
- Программист
- Аудитор (white/black box)
- Криптоаналитик
- Вирусный аналитик
- …

XSS, CSFR

OWASP

PCI DSS

SQL Injection

PHP Including

SNORT

Buffer Overflow

IDS, IPS

Suricata

Reverse Engineering

Криптография

HoneyPot

DNS poison

DDOS

ГОСТ

BotNet

Атаки наWi-Fi

Университет

- Общеобразовательные курсы
- Математические предеты
- Компьютерные курсы
- Предметы по специальности

Нельзя объять необъятное!

Семинары и спец. курсы немного помогают

- Научная тусовка
- Погружение в тему
- Обмен опытом
- Самообразование

А кто их будет вести?

Соревнования – стимул для обучения

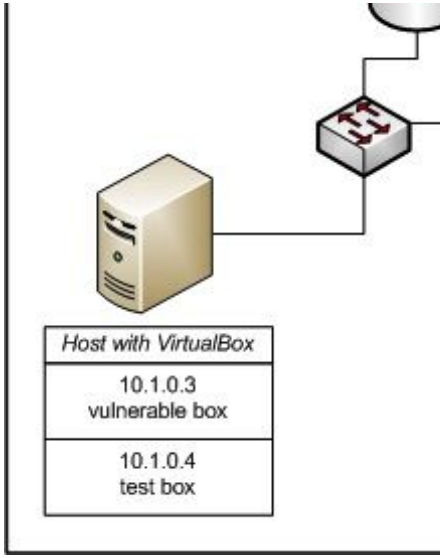
Capture The Flag

Командные соревнования для специалистов по информационной безопасности

Сервис

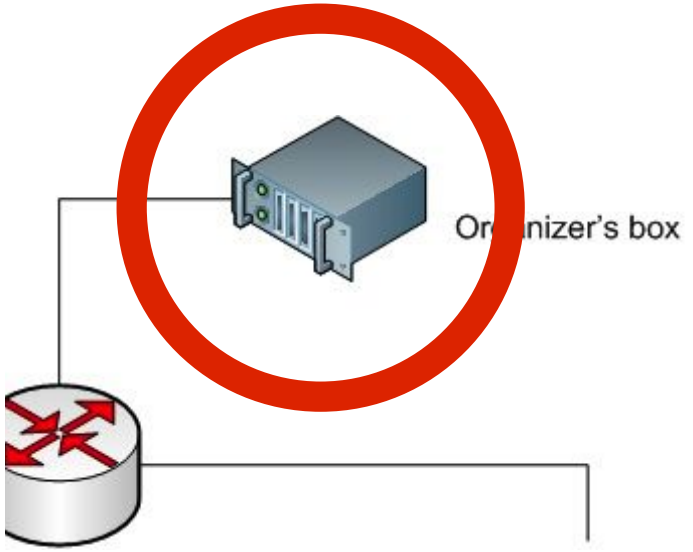
- Сетевое приложение
- Аутентификация пользователей
- Наличие частной информации

- Примеры:
  - Web форум
  - FTP
  - Почтовый сервер
  - …



Проверяющая система

- Имитирует работу легитимного пользователя
- Проверяет работу сервисы
- Устанавливает флаги
- Начисляет баллы



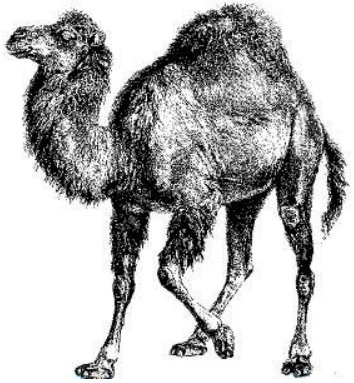
- Принимает флаги у команд
- Отображает текущую игровую ситуацию
- Визуализирует игру

Начисление баллов

- Захват чужого флага
- Защита собственных флагов
- Уведомления о безопасности (advisory):
  - Описание уязвимости (description)
  - POC (Exploit)
  - Исправления (Patch)

Что надо уметь/знать?

- Комьютерные сети
- Операционные системы
- Уязвимости в ПО
- IDS, IPS
- Средства для анализа ПО
- Криптографию
- Языки и архитектуры



python™

Haskell
A Purely Functional Language

Ruby

Java™

Prolog

OPENVPN™

C++

Microsoft®
.net™

C#

php

C

SQL

mongoDB

Разработчики соревнований (навыки)

- Работа в команде, совместное владение кодом
- Умение реализовывать согласованные с другими разработчиками интерфейсы
- Умение интегрировать результаты работ нескольких разработчиков
- Планирование разработки с жесткими сроками
- Опыт доведения разработки до конечного продукта
- Работа с трекером задач
- Работа с системой контроля версий
- Использование различных техник разработки: Agile, экстремальное программирование, …
- Документирование разработки.

Кто начал?

The UCSB iCTF

Первый CTF в России UralCTF 2006г.

Всероссийские межвузовские соревнования по защите информации с 2008г.

КОРДЭК

АРСИБ
АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АЗИ

Общероссийский Союз ИТ-директоров
СОДИТ

- Доклады от ведущих специалистов
- Доклады от участников
- Мастер-классы
- Финал CTF
- Конкурсы:
  - Соревнования роботов «Миссия на Марсе»
  - FlagRush
  - Cluster Wars
  - Клавогонки для админов

Computer Science E-Days

CTF в мире

The UCSB iCTF

rwthCTF: Cyberwar the Flag

CTF движение в РФ

- UralCTF (Екатеринбург, Челябинск)
- RuCTF (Екатеринбург)
- UFOCTF (Таганрог)
- РусКрипто CTF (Москва)
- LeetMore CTF, Rf CTF (Санкт-Петербург)
- SibCTF (Томск)
- PHD CTF (Москва)
- SamaraCTF (Самара)
- BaltCTF (Калининград)

Вы думаете, что я отклонился от основной темы?

Что имеем?

- Студенческие команды
- Исследовательские проекты:
  - Победа в тендере от «Лаборатория Касперского»
  - Исследование BotNet
  - HoneyPot
  - IDS
  - Различные сканирования (например: SNMP)
  - Декомпилятор Python
  - Статический и динамический анализ бинарных файлов
  - …
- Собственные разработки:
  - Система проверки
  - http://blackbox.sibears.ru
  - Разработка утилит
  - …
- Теория **подкрепленная практикой**.

Неравнодушные к таким специалистам

Информзащита
Системный интегратор

4 4 4

Champions!

FlagRush

Вопросы?

Duel

Bank, Mafia, Gagarin, Android, BotNet, Search Engine, … ?