АНАЛИТИЧЕСКОЕ ИССЛЕДОВАНИЕ ПО РЕЗУЛЬТАТАМ СОРЕВНОВАНИЙ PHDAYS CTF 2012

Оглавление

1. Введение

Соревнования проводятся по игровому принципу CTF (Capture the Flag). Несколько команд в течение заранее определенного времени защищают свои сети и атакуют чужие. Основная задача участников — выявлять уязвимости в системах противников и получать доступ к секретной информации (флагам), при этом обнаруживая и устраняя подобные уязвимости в своей системе.

Ключевое отличие Positive Hack Days CTF от аналогичных соревнований — условия, максимально близкие к реальным. Все уязвимости — не выдуманы, а действительно встречаются в современных информационных системах. Более того, формат PHDays CTF необычайно широк благодаря насыщению игровой среды уникальными элементами (захват и удержание систем по принципу «Царь горы», возможность решать игровые задачи вслепую — атаковать системы, не обладая доступом к ним, и др.).

Участники CTF испытали свои силы в настоящей борьбе и получили шанс разработать собственные решения, направленные на защиту информационных ресурсов.

Чтобы придать изюминку соревнованиям, организаторы PHDays CTF подготовили игровую инфраструктуру в соответствии с уникальной для каждого соревнования сюжетной линией. Это помогло создать особую атмосферу и выделило Positive Hack Days CTF на фоне других подобных соревнований.

1.1. Спонсоры соревнований

Компания Positive Technologies выражает благодарность всем спонсорам, которые помогли в проведении соревнований по защите информации CTF в рамках международного форума Positive Hack Days 2012.

Генеральный спонсор — Лаборатория Касперского

«Лаборатория Касперского» — крупнейший в Европе производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама. Компания входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности. В «Лаборатории Касперского» работают более 2300 высококвалифицированных специалистов. Продукты компании надежно защищают компьютеры и мобильные устройства более 300 млн пользователей во всем мире, технологии используются в продуктах крупнейших мировых поставщиков программных и аппаратных решений. Более подробную информацию можно получить на сайте www.kaspersky.ru.

Технологический партнер — Cisco

Cisco — мировой лидер в области сетевых технологий, меняющих способы человеческого общения, связи и совместной работы. Чистый объем продаж компании в 2010-м финансовом году составил 40 млрд долл. Информация о решениях, технологиях и текущей деятельности компании публикуется на сайтах www.cisco.ru и www.cisco.com.

Технологический партнер — ICL

«ICL-КПО ВС» (http://www.icl.ru/) — высокотехнологичная, динамично развивающаяся компания, входящая в число крупнейших IT-предприятий России. «ICL-КПО ВС» предлагает комплексные решения в области информационных технологий и услуги по консалтингу, проектированию, внедрению, гарантийному и сервисному обслуживанию информационных систем любого масштаба. Компания интегрирована с корпорацией Fujitsu (Япония). Продукция и услуги «ICL-КПО ВС» востребованы в государственных и коммерческих структурах, в вооруженных силах и правоохранительных органах, в различных сферах экономики, промышленности, в частности в добыче и распределении нефти и газа, в торговле. Большой опыт

разработки и внедрения крупных проектов в области системной интеграции, наличие команды талантливых и высококвалифицированных специалистов обеспечивают успех и высокое качество обслуживания клиентов.

1.2. Участники CTF

0daysober (Швейцария)

Совершенно новая команда, созданная друзьями, выходцами из французской части Швейцарии, которых объединяет увлечение информационной безопасностью.

BIOS (Индия)

Команда BIOS из университета Amrita Vishwa Vidyapeetham (Амиртапури, Индия) принимает участие в соревнованиях CTF с 2008 года. Первое выступление состоялось на соревнованиях CIPHER4 (2008), где команда заняла 24-е место. За время своего существования команде удалось поучаствовать во многих международных соревнованиях CTF, таких как CODEGATE, ruCTFe, rwthCTF, Mozilla CTF (14-е место) и pCTF. Кроме того, уже в течение трех лет команда успешно проводит InCTF — первые национальные соревнования CTF в Индии.

C.o.P (Франция)

Consortium of Pwners (C.o.P.) — французская команда безопасности, созданная в 2011 году бывшими участниками Nibbles. Члены команды постоянно участвуют в проектах по исследованию уязвимостей и в соревнованиях CTF.

Eindbazen (Нидерланды)

Команда Eindbazen была создана в марте 2011 года для участия в соревнованиях Codegate 2011 Prequals. Команда отметила свою годовщину на соревнованиях Codegate 2012 Prequals. Большинство членов команды знали друг друга еще до ее создания. В состав Eindbazen входят только голландские участники — как студенты, так и профессионалы.

FluxFingers (Германия)

Команда FluxFingers представляет Рурский университет (г. Бохум) на соревнованиях CTF с 2007 года. На протяжении нескольких последних лет команда организует известные соревнования hack.lu CTF. Подробная информация об успехах команды доступна по адресу: https://www.fluxfingers.net/scoring.html.

ForbiddenBITS (Тунис)

ForbiddenBITS — это команда из Туниса, созданная в 2011 году. Команда выиграла ряд местных CTF-конкурсов (Security Challenge Days 1 и 2, Securinet Challenges 2011 и 2012), а также участвовала в

некоторых других соревнованиях.

HackerDom (Россия)

Команда HackerDom была создана в 2005 году на математико-механическом факультете Уральского государственного университета. Участники проводят еженедельные семинары под названием «Секреты ХакерДома». Команда регулярно участвует в CTF и других подобных соревнованиях, а также проводит всероссийские (RuCTF) и международные (RuCTFE) межвузовские соревнования по защите информации.

Int3pids (Испания)

Int3pids — это испанская команда, созданная в 2010 году в на базе команды Sexy Pandas. Участники команды принимали участие во многих крупнейших соревнованиях CTF.

Leet More (Россия)

Команда Leet More возникла в 2008 году в ИТМО. Среди достижений команды:

II место на PHDays 2011 CTF;
IV место на DEFCON 19 CTF в составе сборной России;
I место на Enowars 2011 CTF;
I место на Mozilla CTF 2012 (в составе More Smoked Leet Chicken);
I место на IFSF CTF Quals (в составе More Smoked Leet Chicken);
I место на NeoQuest 2012;
I место на CodeGate 2012 Quals и CodeGate 2012 Final (в составе Leet Chicken).

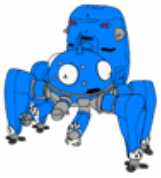
Plaid Parliament of Pwning (США)

Команда PPP была образована из числа студентов университета Carnegie Mellon University в 2009 году. В ее состав входят студенты, выпускники, магистранты, аспиранты и сотрудники университета. За последние годы команда PPP выиграла многочисленные соревнования CTF, включая Codegate, iCTF, CSAW, HUST, Ghost in the Shellcode, Secuinside и PHDays.

Shell-Storm (Франция/Швейцария)

Shell-Storm.org — группа энтузиастов, работающих над проектами по разработке свободного ПО с открытым кодом в области систем GNU/Linux. На своем портале члены Shell-Storm.org публикуют полезную информацию для специалистов в области тестирования безопасности информационных систем.

Tachikoma (Япония)



В состав команды Tachikoma входят студенты таких японских университетов, как University of Tokyo, Tokyo Denki University, Tokyo University of Technology и University of Aizu. Команда образована в феврале 2012 года, ее дебют состоялся на PHDays 2012.

2. Описание соревнований

2.1. Общие положения

Каждая команда состоит из 7 участников, среди которых обязательно присутствует капитан. Одновременно на игровой площадке (за игровым столом команды) может находиться 5 человек; оставшиеся двое членов команды считаются запасными. Замены можно производить в любой момент, с разрешения жюри.

Команды используют собственные компьютеры (например, ноутбуки).

Все флаги представлены в виде 32-символьной строки в формате MD5.

Баллы начисляются за:

- отправку флагов, захваченных с сервисов команд соперников;
- отправку флагов, захваченных с сервисов общего сегмента игровой инфраструктуры (black-box);
- время удержания сервисов игровой системы в рамках задания «Царь горы»;
- победу в бонусном задании;
- отправку бонусных флагов, захваченных с сервисов общего сегмента игровой инфраструктуры.

Баллы снимаются за:

- захват флагов с сервисов команды игроками команд соперников;
- нарушение доступности собственных сервисов;
- нарушение функционирования уязвимых сервисов;
- нарушение общих правил соревнований.

Во время игры командам разрешается:

- использовать не более 15 компьютеров и единиц сетевого оборудования не ниже второго уровня стека ISO OSI;
- вносить любые изменения в предоставленные серверы, если это прямо не запрещено жюри;
- проводить атаки на серверы команд соперников с целью захвата флагов;
- проводить атаки на серверы общего сегмента игровой инфраструктуры с целью захвата флагов;
- проводить атаки на серверы системы в рамках задания «Царь горы»;
- обеспечивать защиту серверов системы в рамках задания «Царь горы» любыми способами, которые прямо не запрещены правилами;
- проводить атаки на канал беспроводной передачи данных с целью захвата управления (в рамках бонусного задания).

Во время игры командам запрещается:

- проводить атаки на компьютеры жюри;
- осуществлять фильтрацию трафика к любым ресурсам CTF (например, по IP-адресам);
- генерировать неоправданно большой объем трафика (флуд);
- проводить деструктивные атаки на серверы команд соперников (например, rm -rf /);
- преднамеренно нарушать нормальное функционирование сервисов, включая сервисы команд соперников, сервисы общей игровой инфраструктуры и сервисы инфраструктуры системы «Царь горы»;
- удалять флаги с предоставленных серверов, на серверах команд соперников и серверах общей игровой инфраструктуры;
- осуществлять деструктивные действия в отношении объектов игровой инфраструктуры;
- осуществлять указанные выше действия от имени команд соперников.

Работа жюри

- Жюри может уточнять правила в любой момент до начала игры.
- Жюри может оштрафовать или дисквалифицировать команду за нарушение правил.
- Жюри определяет победителя, основываясь на количестве баллов, полученных командами.

2.2. Инфраструктура CTF

В начале игры команды получают идентичные серверы с заранее установленным набором уязвимых сервисов. Задача участников — найти уязвимости, устранить их у себя и воспользоваться ими для получения секретной информации (флагов) от команд соперников.

За процессом игры непрерывно следит проверяющая система жюри, регулярно изменяя состояние игровой инфраструктуры, помещая новые флаги и уязвимости на сервера команд, отслеживая наличие ранее установленных флагов и выполнение уязвимыми сервисами своих функций.

Организаторы заранее готовят ограниченное число уязвимых сервисов, выполняющих определенные функции и уже содержащих набор уязвимостей. Участники работают с двумя типами систем — открытыми (участники обладают привилегированным доступом к системе на уровне операционной системы) и закрытыми (участники обладают доступом к уязвимым сервисам и секретной информации только по сети — black-box). В указанном сегменте сети любой участник Positive Hack Days CTF может попробовать свои силы в эксплуатации реальных уязвимостей и побороться за дополнительные призы. В отличие от PHDays CTF 2011, участникам предоставляется возможность соревноваться в атаке и удержании системы сервисов в рамках задания «Царь горы», в котором начисляются баллы за время удержания сервисов командой участников.

В рамках PHDays CTF 2012 проводятся дополнительные бонусные конкурсы и задания, которые направлены на развлечение участников и повышение зрелищности мероприятия. Бонусные задания могут принести командам дополнительные баллы в общем зачете CTF.

Бонусные конкурсы включают:

- проведение атаки с целью перехвата дистанционного управления устройством (AR.Drone);
- поиск заданной информации в контейнерах с бумажным мусором;
- сбор флагов, появляющихся в определенные моменты времени на сервисах команд участников.

2.2.1. Типы заданий

Участникам соревнования предлагаются задания следующих типов:

- выявление и эксплуатация уязвимостей в сервисах игровых инфраструктур команд соперников и защита собственных сервисов от аналогичных атак;
- выявление и эксплуатация уязвимостей в сервисах общей игровой инфраструктуры;
- выявление и эксплуатация уязвимостей в сервисах инфраструктуры «Царь горы» с целью получения и удержания контроля над сервисами;
- бонусное задание — поиск бонусных флагов в сервисах команд соперников, появляющихся в заданные промежутки времени;
- бонусные конкурсы — поиск заданной информации среди бумажного мусора и перехват контроля над дистанционным управлением радиоуправляемым устройством (AR.Drone);
- защита интернет-банка.

2.2.2. Типы флагов

Флаги представлены в виде 32-символьной строки в формате MD5.

Флаги командных сервисов

Флаги данного типа обладают следующими характеристиками:

- содержат идентификатор команды (команда не может выдавать флаги своих сервисов за флаги, захваченные с сервисов соперника);
- команда может захватить аналогичные флаги с сервисов нескольких (всех) команд соперников;
- каждый флаг может быть захвачен несколькими (всеми) командами соперников, но каждой командой лишь один раз.

Флаги сервисов общей инфраструктуры

Флаги данного типа обладают следующими характеристиками:

- флаги доступны для захвата всем командам в равной степени;
- каждый флаг может быть захвачен несколькими (всеми) командами, но каждой командой лишь один раз.

Флаги сервисов инфраструктуры «Царь горы»

Флаги данного типа обладают следующими характеристиками:

- флаги доступны для захвата всем командам в равной степени;
- флаги содержат информацию о принадлежности к конкретному сервису 1-го или 2-го уровня сценария;
- каждый флаг может быть захвачен только одной командой лишь один раз.

Флаги бонусного задания

Флаги данного типа обладают следующими характеристиками:

- содержат идентификатор команды (команда не может выдавать флаги своих сервисов за флаги, захваченные с сервисов соперника);
- команда может захватить аналогичные флаги с сервисов нескольких (всех) команд соперников;
- каждый флаг может быть захвачен только один раз и лишь одной из команд.

2.2.3. Правила начисления баллов

С подробным описанием правил соревнований можно ознакомиться на официальном сайте PHDays 2012 по адресу: http://phdays.ru/ctf/rules/.

Командные сервисы

За каждый захваченный у соперников флаг команда получает по 10 баллов. За каждый потерянный флаг своей инфраструктуры команда штрафуется на 10 баллов. Если один и тот же флаг потерян дважды или трижды, команда лишается по 10 штрафных баллов за каждую потерю.

Примечание. При многократной потере одного флага в случае реализации атак несколькими командами соперников штрафные баллы начисляются только за первые три факта потери данного флага.

Штрафные баллы начисляются также за нарушение доступности своих сервисов и (или) функций, выполняемых уязвимыми сервисами. Штраф за нарушение доступности сервиса — 40 баллов.

Общая инфраструктура

За отправку флагов, найденных в общей игровой инфраструктуре, команда получает баллы в зависимости от сложности задачи нахождения флага. Суммарно в данном задании команда может заработать 2000 баллов.

Царь горы

Организованы три вида сервисов, два — 1-го уровня сложности и один — 2-го уровня сложности. Доступ к сервису 2-го уровня возможен лишь при решении задачи 1-го уровня. Максимально в данном задании каждая команда может заработать 2640 баллов.

При удержании сервиса 1-го уровня сложности команда получает 1 бал за каждые полные 3 минуты непрерывного контроля сервиса. При удержании сервиса 2-го уровня сложности начисляется по 2 балла за каждые полные 3 минуты непрерывного контроля сервиса. При потере контроля сервиса и его повторном захвате таймер отсчитывает трехминутные интервалы заново.

Бонусное задание

Баллы начисляются за победу в бонусных конкурсах и взятие бонусных флагов. Всего предусмотрено 804 бонусных балла, с учетом баллов за победу в бонусных конкурсах.

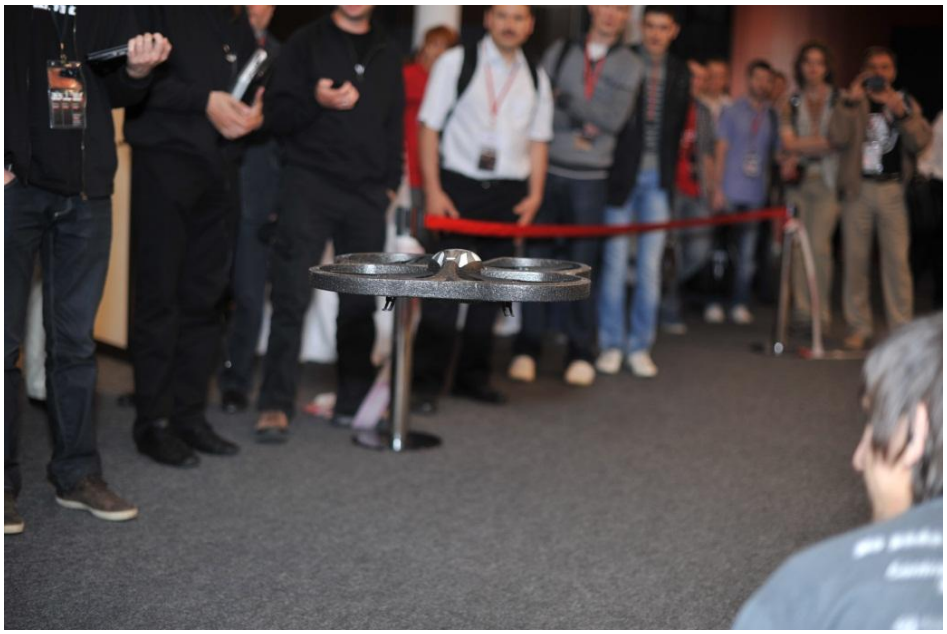
Каждые 10 минут в течение 7 часов проведения бонусного задания (в ночное время с 00:00 до 7:00) происходит изменение состояния командных сервисов. Каждое состояние сервисов игровой инфраструктуры команды содержит 1 бонусный флаг, за отправку каждого флага команде начисляется 1 балл.

Бонусные конкурсы

По 7 баллов начисляется команде за каждый флаг, найденный в рамках конкурса по поиску информации в контейнере с мусором.

Фотография 1. Контейнер с бумажным мусором

При победе в каждом из двух этапов конкурса по перехвату управления AR.Drone команда получает 150 баллов.



Фотография 2. Квадрокоптер AR.Drone

Защита интернет-банка

Данное задание является завершающим и проводится после основных этапов CTF. Условия задания объявляются командам во второй день проведения соревнования.

По условиям задания организуется игровая инфраструктура интернет-банка, в котором на счет каждой команды перечисляется определенная, равная для всех команд, сумма денег. Конкретная сумма определяется организаторами в зависимости от текущего рейтинга команд за 3 часа до конца соревнования CTF и объявляется командам.

Командам необходимо организовать защиту своих банковских счетов от атак из сети Интернет. Количество денег потерянных командой в данном задании соответствует количеству баллов, которые команда потеряет в общем зачете соревнования.

Выявление победителя

Итоговое количество баллов соответствует рейтингу «Тотал» (суммарному количеству баллов) на момент окончания завершающего задания по защите интернет-банка. Побеждает команда, первой набравшая наибольшее количество баллов.

3. Легенда соревнований

XXI век стал веком триумфа биотехнологий. Массовое использование ГМО обещало решить проблему голода, излечить болезни, дать человеку власть над природой... Но к середине века ГМО встречались уже везде — от тундры и до сельвы.

Не выдержав грубого вмешательства, Флора нанесла ответный удар и стала бороться за выживание. Гигантские деревья-сорняки и микроскопические насекомые заполонили леса и поля планеты. Не остался в стороне от генетического безумия и человек. По планете прокатилась череда опустошительных эпидемий, некоторые из которых были вызваны искусственно. Так началась Четвертая мировая война — самая стремительная и смертоносная за всю историю.

Начало второй половины века встретило деморализованное, сократившееся на треть человечество; каждый второй ребенок рождался с невиданными прежде мутациями. Потеряв надежду, люди поспешили скрыться от агрессивной среды в герметичных городах. И вот сейчас, спустя двести лет, жалкие остатки человечества ведут непрекращающуюся борьбу за выживание. С одной стороны — непрерывно враждующие города-государства, с другой — скитающиеся по разрушенным городам и чудовищным лесам мутанты. Основой выживания стали несколько компьютеризированных ферм по выращиванию «чистой» пищи, охраняемых как зеница ока.

Неизбежный технологический регресс заставил выживших вести постоянную борьбу за немногие сохранившиеся технологии и за работоспособность оставленных предками систем управления. Из построенных когда-то сотен подземных городов выжили только двенадцать. И сколько из них выстоит до завтра — не знает никто.

Игровые сервисы схематично представлены на рис. 1 и 2.

В блоге Дмитрия Евтеева, одного из ключевых представителей организаторов соревнований, можно ознакомиться с подробным описанием легенды CTF 2012, а также увидеть специально подготовленные брошюры и видеоролики: http://devteev.blogspot.com/2012/06/phdays-2012.html.

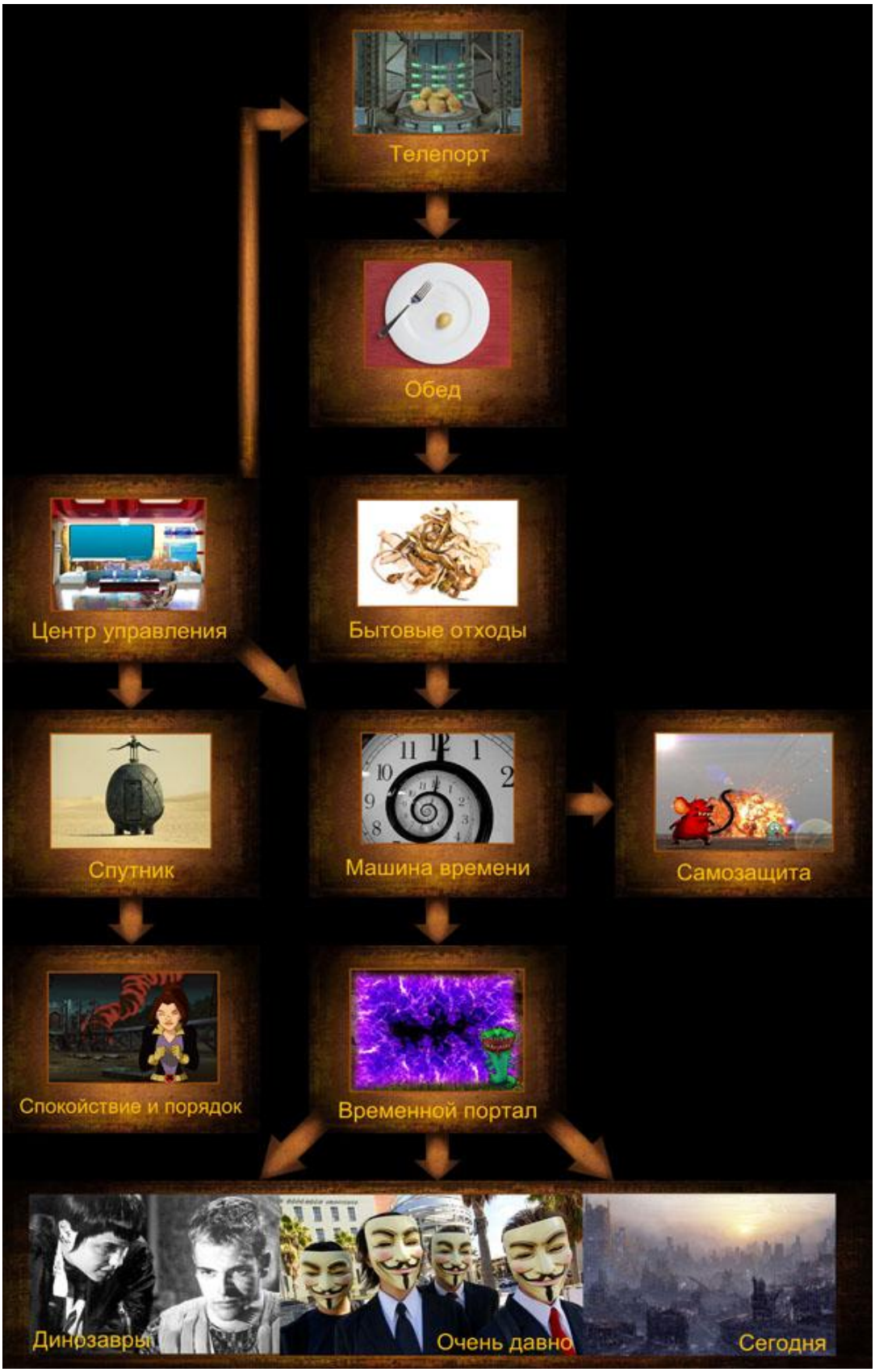


Рисунок 1. Игровые сервисы первого дня

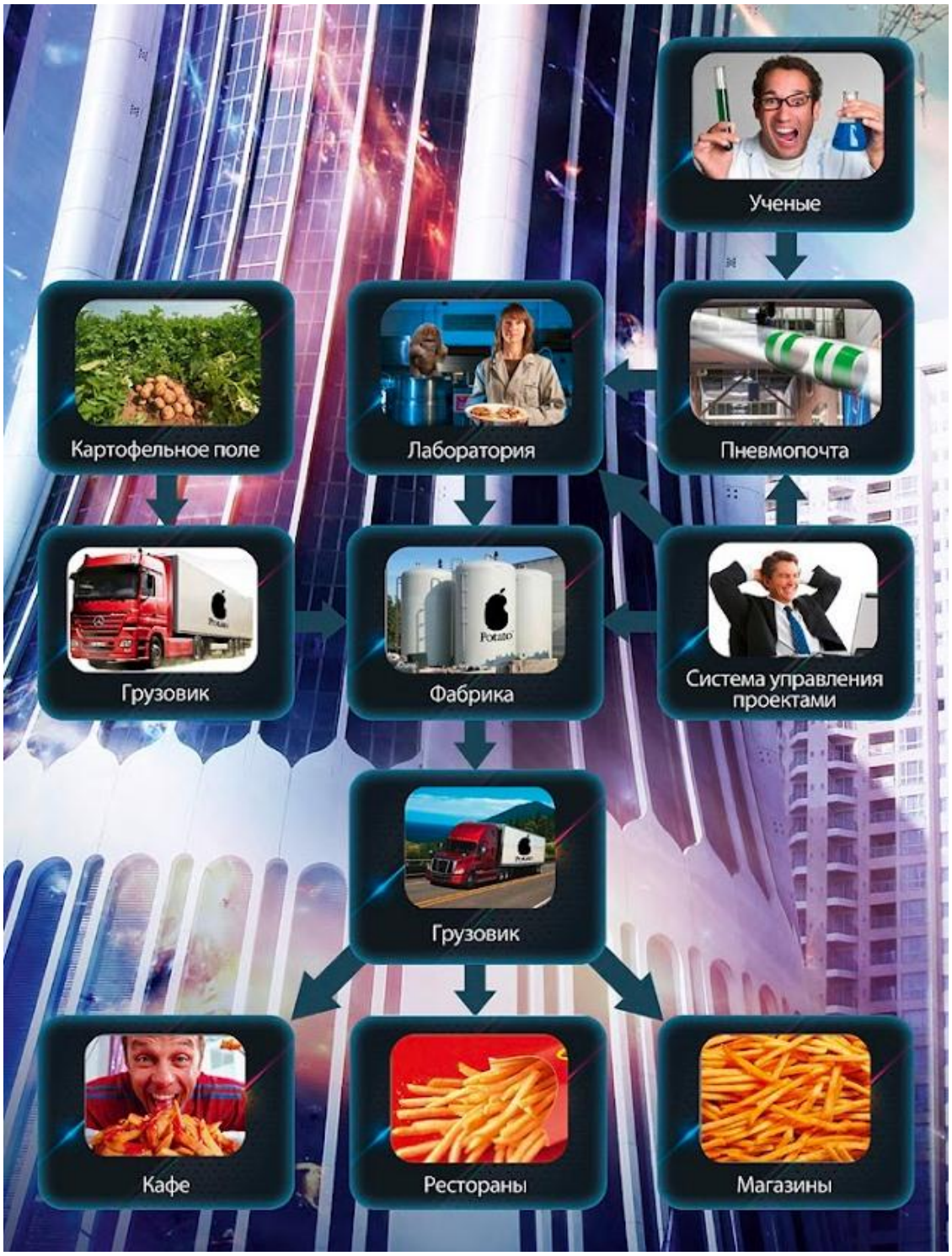


Рисунок 2. Игровые сервисы второго дня

3.1. День первый

Описание игровых сервисов первого дня

Телепорт

Картофель — основа нашего рациона. Это одна из немногих культур, переживших годы Конца. К сожалению, несмотря на усилия наших ученых, мутагенные факторы все-таки оказывают свое пагубное влияние на выращиваемый картофель. Поэтому для того, чтобы пополнять наши хранилища генетически чистых семян, мы используем уникальную систему телепортов. Телепорты позволяют нам доставлять семена из других Городов, избегая многодневных, полных опасностей вылазок во внешний мир. Без обновления фонда семян с помощью телепортов мы вскоре останемся без чистой пищи. А без пищи мы перестанем быть Живыми.

Поддержание работоспособности и охрана телепортов от внешних посягательств — важнейшая из задач вашего подразделения. Помните: от этого зависит, будет ли полна тарелка, когда завтра Живые придут на обед. От вас зависит, останутся ли Живые в живых.

Боевые спутники

Жители нашего Города находятся под постоянной угрозой. Мутанты с нарастающими темпами предпринимают попытки проникнуть на нашу территорию, а враждебно настроенные Города хотят получить доступ к нашим ресурсам и отобрать все, что у нас есть. Спокойствие и порядок в Городе напрямую зависят от работоспособности наших боевых спутников, которые используются для нашей защиты и для предупредительных ударов по врагам. Если спутники будут выведены из строя, мы окажемся беззащитными, как котята: все наши продовольственные запасы и производственные мощности вскоре будут захвачены другими Городами, а население останется на растерзание разъяренным мутантам.

Машина времени

Уже много лет мы остаемся Живыми только благодаря чистой пище. Однако мутационные изменения подбираются и к нашим фермам, а запасы генетически чистых семян в хранилищах невозможно пополнять бесконечно. Машина времени — наша единственная надежда на спасение. Если нам удастся с ее помощью открыть временной Портал, мы сможем попасть в прошлое, когда жизнь была легкой и безоблачной, а вода была чистой, когда существовали крем для обуви, зубочистки и множество других прекрасных вещей. С Машиной времени у нас будет шанс остановить это безумие и предотвратить Конец.

Несмотря на то что Машина времени обладает продвинутой системой самозащиты, которая позволяет ей очищать окружающую территорию от крыс и бомжей, она не может использовать эту систему для защиты от атак со стороны других Городов. И если в результате этих атак у наших врагов получится разрушить Машину времени — мы обречены.

Центр управления

Так как Город находится в условиях постоянной борьбы за выживание, любое промедление в решении вопросов управления всеми системами чревато гибелью. Быстрое принятие правильных решений нашим командованием — это необходимое условие для того, чтобы мы оставались Живыми. Центр управления используется для того, чтобы отслеживать состояние всех важнейших систем Города: от Телепорта до Машины времени. Если враг подберется к Центру управления, наше командование перестанет получать актуальную информацию о состоянии защиты в Городе и мы будем поставлены под удар.

Кантина

«Малиновый пони» — лучшая (и единственная) кантина на Земле. Здесь бывают все видные политические деятели, лучшие ученые и самые влиятельные люди из всех Городов. Все важнейшие политические решения принимаются именно здесь, под крылышком мадам Дондон. Кроме того, если заполучить компромат на кого-нибудь из ученых, то это, вполне вероятно, поможет сделать шаг вперед к открытию Портала времени. Кто владеет кантиной — владеет миром.

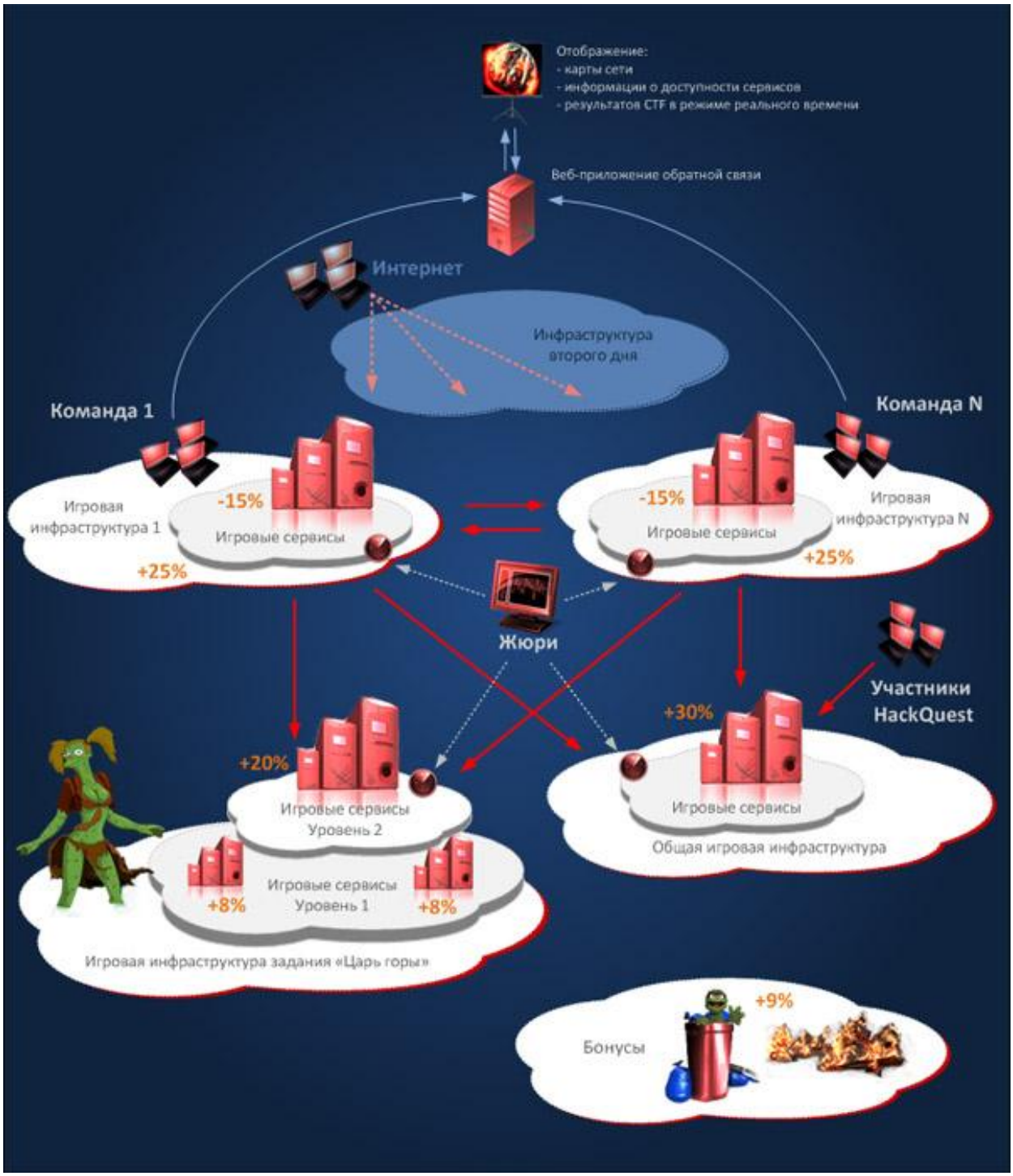


Рисунок 3. Схема игровой инфраструктуры первого дня соревнований

3.2. День второй

Описание игровых сервисов второго дня

Завод по производству картошки

Potato — один из ведущих мировых производителей картошки. На нашем заводе используются передовые технологии по очистке и переработке картофеля, которые являются ноу-хау нашей компании. Именно здесь сосредоточено производство таких известных торговых марок картошки, как Ringlets, Happy Bubbles, Potato Fingers, Luxury Delicacies. Для того чтобы обеспечить эффективное управление процессом производства, на заводе используется SCADA-система Potato Multifunctional Universal Treatment and Assortment Technological System (MUTANTS).

Ваша задача — всеми силами обеспечивать безопасность и бесперебойность функционирования MUTANTS. Малейший сбой в работе системы ведет к остановке всего производства и крупнейшим финансовым потерям.

Исследовательская лаборатория

Чтобы только лучшая картошка попадала к вам на стол, мы используем новейшие научные разработки в области генной инженерии. Благодаря достижениям наших ученых только картошка Potato может храниться в течение 12 лет. Хотя она настолько вкусная, что обычно ее съедают за первые 8 часов после поступления на прилавки, и это тоже результат работы сотрудников лаборатории. Сейчас наши ученые работают над тем, чтобы придать картошке кубическую форму и удобные размеры 20x20x20 см.

Лаборатория — важнейшее подразделение нашей компании, без нее мы быстро утратим конкурентное преимущество и потеряем лидерство на рынке.

Пневматическая почта

Для быстрого и безопасного обмена документами и опытными образцами картошки в компании развернута система пневматической почты. Она также используется сотрудниками Исследовательской лаборатории для взаимодействия с лучшими учеными из различных институтов в рамках обмена опытом. Необходимо обеспечить бесперебойное функционирование пневмопочты, чтобы ученые нашей лаборатории могли получать актуальную информацию о новейших разработках в области генной инженерии — и не организовали забастовку из-за отсутствия свежего номера журнала Naked Genetics.

Система управления проектами

Эффективное управление процессами в такой высокотехнологичной компании, как Potato, немыслимо без автоматизированной Системы управления проектами. Каждый день миллионы картофелин проходят через конвейеры Potato, ученые Исследовательской лаборатории работают над десятками проектов одновременно, тысячи писем пересылаются по пневмопочте, но без Системы управления проектами вся деятельность компании быстро погрузилась бы в хаос, который неизбежно ведет к разорению.

I-Bank

Годовой оборот компании Potato исчисляется сотнями тысяч, а в урожайный год — миллионами долларов. Безусловно, все эти деньги хранятся не под матрасом у Президента компании (хотя и там тоже), а в надежном банке. Банковские счета Potato должны быть защищены на самом высоком уровне. Кража денег со счета Potato приведет к банкротству компании и потере рабочих мест тысячами сотрудников Potato — включая, кстати, и вас.

Медиахолдинг

Sleepwalker Media Holding Inc. является крупнейшим мировым медиахолдингом, в который входят десятки СМИ, в том числе телеканал Hypnotoad TV, радиостанция Lacklustre Voice, еженедельники Young and Sclerotic и Beer Belly. Несмотря на то что издания SMH в большинстве своем фантастически скучны и бесполезны (кроме шоу Гипножабы, конечно же!), размещение рекламы на этих ресурсах приносит рекламодателям огромную прибыль. В редких публикациях независимой прессы время от времени сообщается о том, что грандиозный успех SMH связан с применением методов психического воздействия на аудиторию, вплоть до гипноза. Однако достоверных доказательств этому нет. Владелец SMH обладает неограниченными возможностями использования его ресурсов, поэтому представители ведущих мировых компаний, включая Potato, неустанно борются за власть над холдингом.

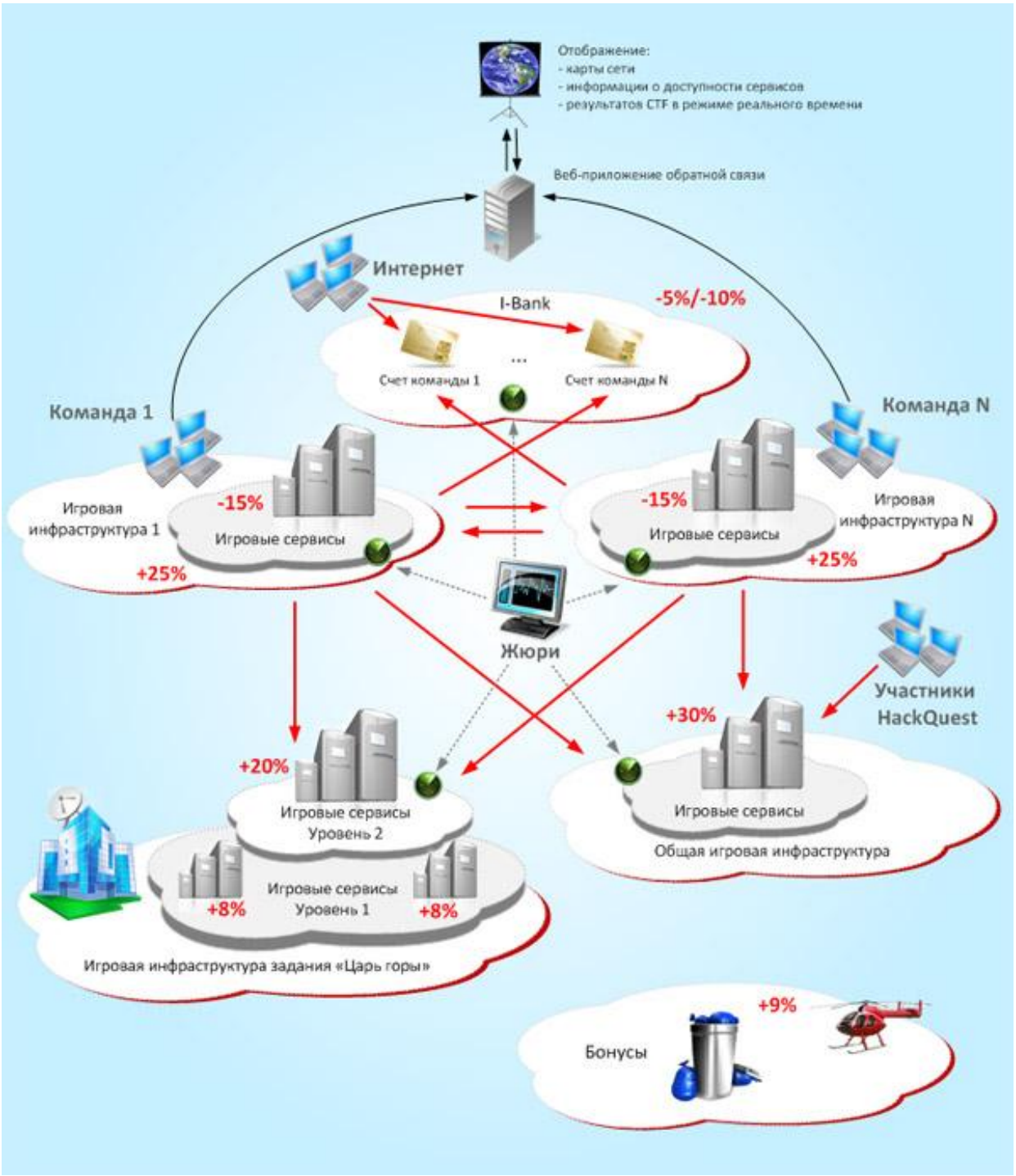


Рисунок 4. Схема игровой инфраструктуры второго дня соревнований

4. Победители PHDays CTF 2012

I место

Leet More (Россия)

II место

0daysober (Швейцария)

III место

Int3pids (Испания)

5. Отзывы о PHDays CTF 2012

В соревнованиях CTF 2012 участвовали представители 11 стран со всего мира. Никто из участников мероприятия не остался равнодушным, многие представители команд опубликовали в блогах и на форумах свои отзывы о самом CTF, форуме PHDays 2012 и о посещении Москвы.

К примеру, один из участников команды BIOS написал в своем блоге: «The CTF was cool. In short, we didn't do so well and finished last but managed to exploit the python twisted service (reminded of my service for sCTF 2012) as well as solve a few side challenges. We also managed to capture a few flags from the dumpster diving». Статья доступна по адресу: http://arvindsraj.wordpress.com/2012/07/11/phdays-ctf-2012/.

Отзыв от команды Eindbazen, опубликованный в Twitter: https://twitter.com/ThiceNL/status/209653337912655872/photo/1

Фотография 3. Памятные трофеи команды Eindbazen

Отчет команды 0daysober о мероприятии:

http://blog.scrt.ch/2012/06/04/ctf-phdays-2012/

Отчет о PHDyas CTF 2012 на сайте Хабрахабр:

http://habrahabr.ru/company/pt/blog/145792/

6. Аналитика

6.1. Распределение баллов в рамках заданий командной инфраструктуры (классический CTF)

Данные, отражающие количество баллов, заработанных командами только путем захвата флагов на уязвимых ресурсах соперников (включая ночные бонусные флаги), приведены на рис. 5. Таким образом, позиции команд в рейтинге по захвату флагов командной инфраструктуры отличаются от общего распределения призовых мест: на первом месте команда PPP, на втором — Leet More, на третьем — Int3pids.

Как видно по диаграмме, в данной части соревнований нет ярко выраженного лидера, целый ряд команд претендуют на первое место с относительно небольшой разницей баллов. Выделяется явный аутсайдер — команда BIOS, которая не смогла должным образом защитить свои сервисы и осуществила всего три успешные атаки на сервисы соперников в рамках основных соревнований (все три атаки были проведены во второй день CTF).

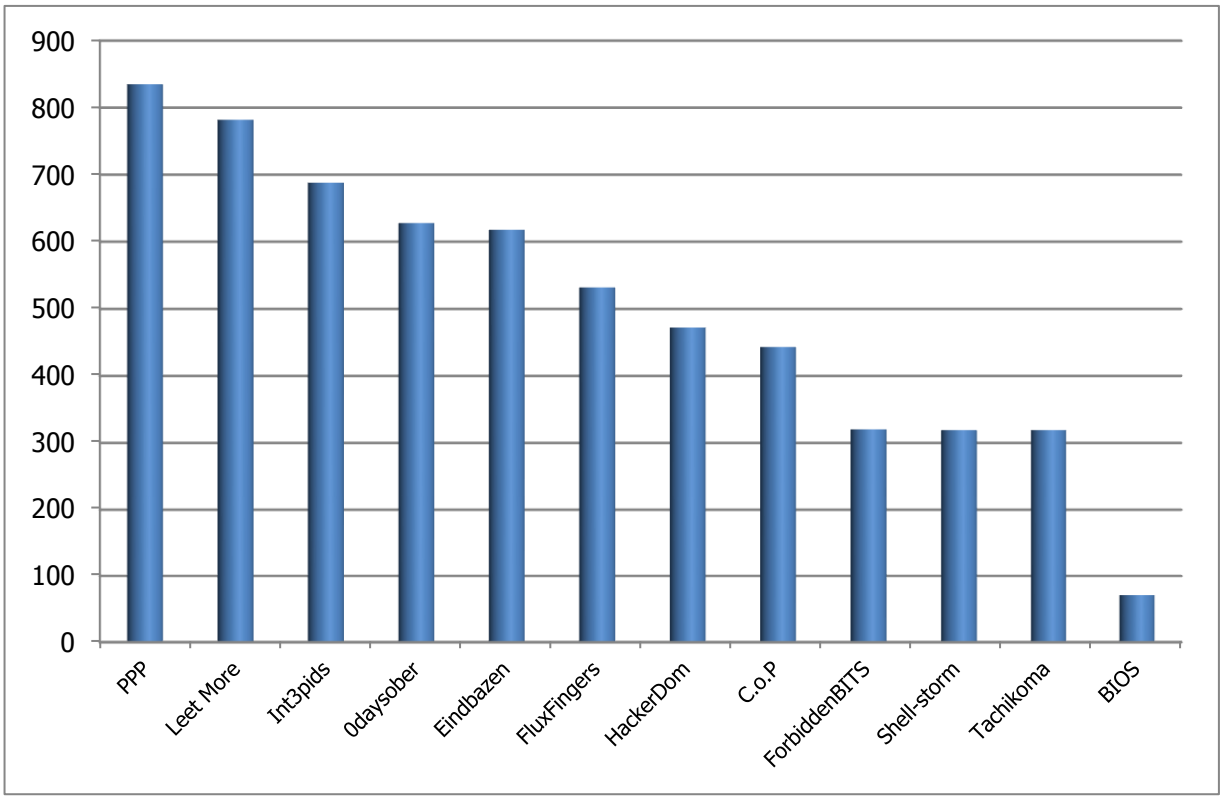


Рисунок 5. Баллы, заработанные командами в заданиях командной инфраструктуры

6.1.1. Хронология начисления баллов

Хронология начисления баллов представлена в табл. 1 и на рис. 6—8, отдельно для первого и второго дней соревнований и ночных заданий.

Таблица 1. Хронология начисления баллов в заданиях командной инфраструктуры

Временной интервал	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	110	0	0
10:00 - 10:30	80	0	60	90	50	0	90	10	110	110	50	0
10:30 - 11:00	90	0	100	90	50	50	90	40	110	190	70	0
11:00 - 11:30	160	0	100	90	50	50	90	40	110	190	70	0
11:30 - 12:00	160	0	170	97	50	50	90	40	180	190	70	0
12:00 - 12:30	160	0	170	97	57	50	90	40	180	190	70	0
12:30 - 13:00	170	0	170	147	137	50	130	40	180	190	100	0
13:00 - 13:30	170	0	170	147	147	50	130	47	270	190	100	0
13:30 - 14:00	170	0	170	147	147	57	130	47	280	200	100	0
14:00 - 14:30	170	7	170	147	147	57	133	47	280	200	100	0
14:30 - 15:00	184	7	170	147	147	57	133	47	280	200	100	10
15:00 - 15:30	184	7	170	147	147	57	133	47	360	250	100	10
15:30 - 16:00	184	7	170	237	217	57	133	47	360	310	100	27
16:00 - 16:30	244	7	170	237	217	57	183	47	381	350	100	27
16:30 - 17:00	244	7	170	307	217	107	183	107	381	450	160	27
17:00 - 17:30	244	7	170	307	277	107	183	197	381	450	160	27
17:30 - 18:00	244	7	170	307	277	107	183	197	381	450	160	27
18:00 - 18:30	244	7	230	307	297	107	183	257	381	450	160	47
18:30 - 19:00	244	7	230	327	297	107	183	257	381	450	160	117
19:00 - 19:30	244	7	230	327	297	107	183	257	381	450	160	117
19:30 - 20:00	244	7	230	327	297	107	183	257	381	450	160	117
20:00 - 20:30	244	7	230	327	297	107	183	257	381	450	160	117
20:30 - 21:00	244	7	230	327	297	107	183	257	381	450	160	117
21:00 - 21:30	247	7	230	327	297	107	183	257	381	450	160	117
21:30 - 22:00	247	7	230	327	297	107	183	257	381	450	163	117
22:00 - 22:30	247	7	230	327	297	107	183	257	381	450	163	117
22:30 - 23:00	247	7	230	327	297	107	183	257	381	450	163	117
23:00 - 23:30	247	7	230	327	297	107	183	257	381	450	163	117
23:30 - 00:00	247	7	230	327	297	107	183	257	381	450	163	117
Ночь												
0:00 - 0:30	0	0	0	0	0	0	0	0	0	0	0	0
0:30 - 1:00	3	0	13	0	0	0	0	0	0	0	0	0
1:00 - 1:30	7	0	24	0	0	0	0	0	0	0	2	0
1:30 - 2:00	7	0	28	9	0	0	9	1	1	0	6	0
2:00 - 2:30	25	0	40	31	12	0	24	15	23	10	11	0
2:30 - 3:00	33	0	51	43	23	0	35	34	31	22	11	0
3:00 - 3:30	43	0	62	57	38	0	36	57	43	36	27	0
3:30 - 4:00	56	6	78	66	47	0	36	75	54	48	38	0
4:00 - 4:30	65	12	90	75	53	0	36	96	63	57	47	0
4:30 - 5:00	71	16	97	83	59	0	38	116	69	64	50	0
5:00 - 5:30	76	21	102	88	63	1	38	135	74	70	50	0
5:30 - 6:00	89	21	102	93	63	6	38	157	80	78	50	0
6:00 -6:30	100	23	102	103	63	11	38	178	86	89	51	0
6:30 - 7:00	109	26	102	109	63	14	38	195	89	98	51	0
7:00 -7:30	112	27	102	111	63	15	48	201	90	100	51	0
7:30 - 8:00	112	27	102	111	63	15	48	201	90	100	51	0
8:00 - 8:30	112	27	102	111	63	15	88	201	90	100	51	0
8:30 - 8:45	112	27	102	111	63	15	88	201	90	140	51	0
2 день 31.05.2012												
8:45 - 9:30	20	0	0	0	20	10	10	0	10	10	0	0
9:30 - 10:00	20	0	20	0	90	30	20	10	130	10	0	0
10:00 - 10:30	90	0	20	130	100	160	100	60	130	10	0	0
10:30 - 11:00	110	30	20	130	100	160	110	110	150	50	40	10
11:00 - 11:30	170	30	20	130	100	160	110	110	150	120	40	70
11:30 - 12:00	170	30	30	130	100	160	120	120	180	120	47	90
12:00 - 12:30	198	30	30	130	100	160	120	120	180	120	64	100
12:30 - 13:00	199	30	31	130	100	160	121	120	181	121	74	101
13:00 - 13:30	199	37	31	130	100	160	121	120	181	121	75	101
13:30 - 14:00	199	37	31	130	100	168	121	130	201	121	75	121
14:00 - 14:30	229	37	31	130	100	168	131	170	231	121	75	121
14:30 - 15:00	229	37	31	130	160	168	141	170	231	121	75	141
15:00 - 15:30	239	37	61	172	170	168	161	180	261	151	95	161
15:30 - 16:00	239	37	61	172	172	168	161	180	261	151	95	161
16:00 - 16:30	239	37	61	172	172	168	161	180	261	165	95	161
16:30 - 17:00	239	37	101	179	172	168	161	230	311	235	95	191
17:00 - 17:30	259	37	111	179	172	168	191	230	311	245	95	201
17:30 - 18:00	269	37	111	179	172	168	201	230	311	245	105	201
18:00 - 18:30	269	37	111	179	172	198	201	230	311	245	105	202
18:30 - 19:00	269	37	111	180	172	198	201	230	311	245	105	202

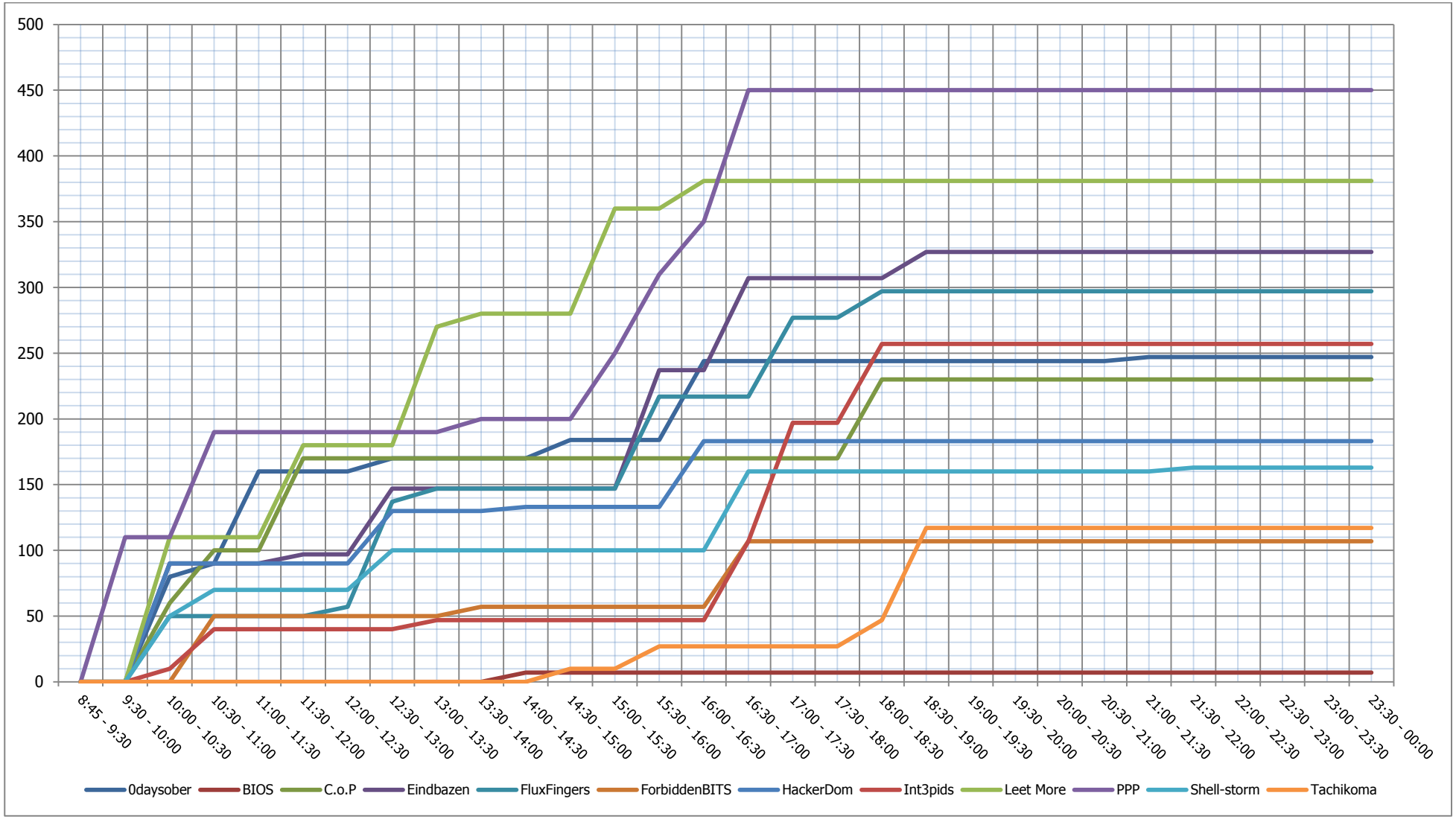


Рисунок 6. Хронология начисления баллов в рамках заданий командной инфраструктуры в первый день соревнований

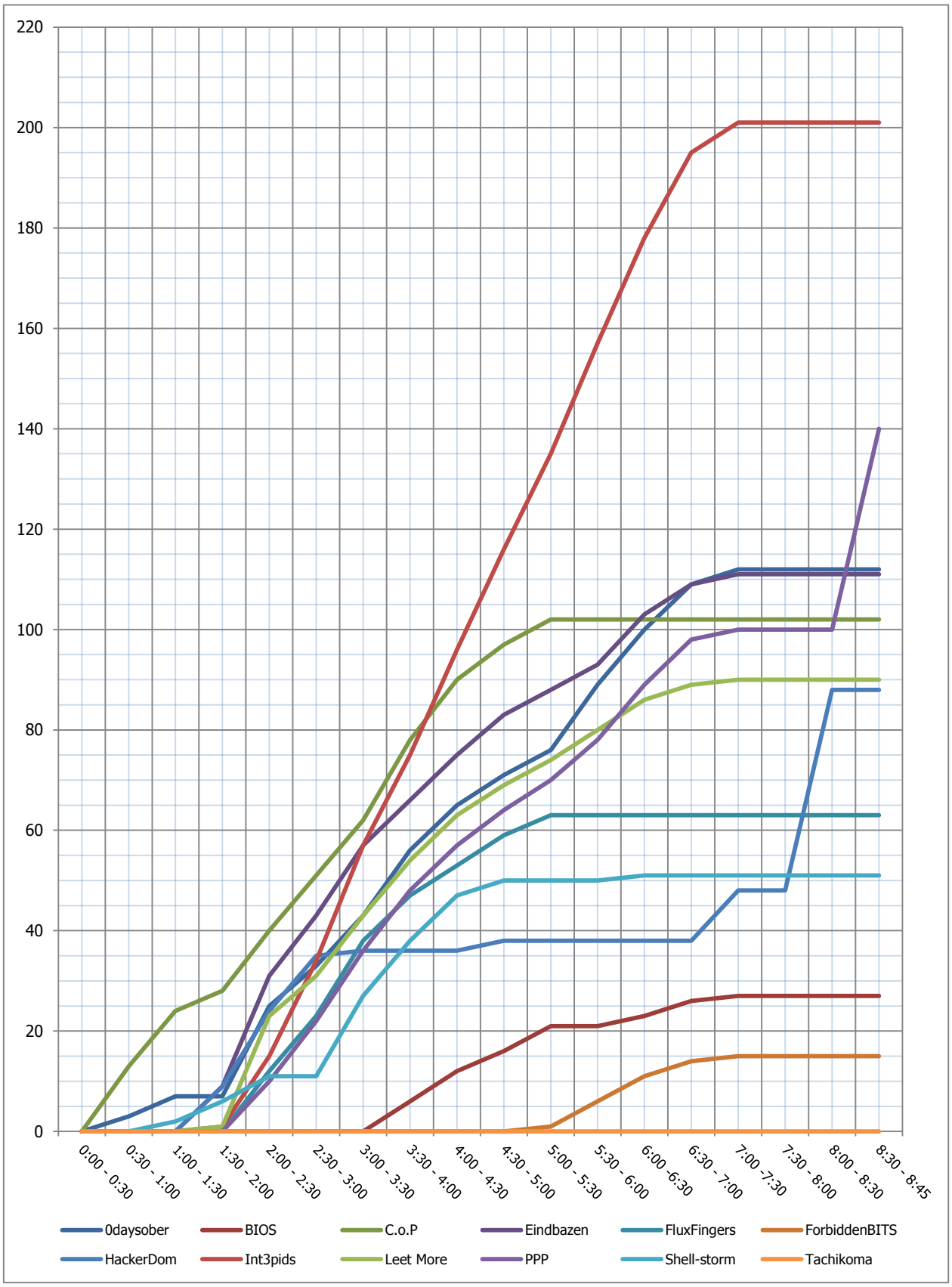


Рисунок 7. Хронология начисления баллов в рамках заданий командной инфраструктуры в ночное время

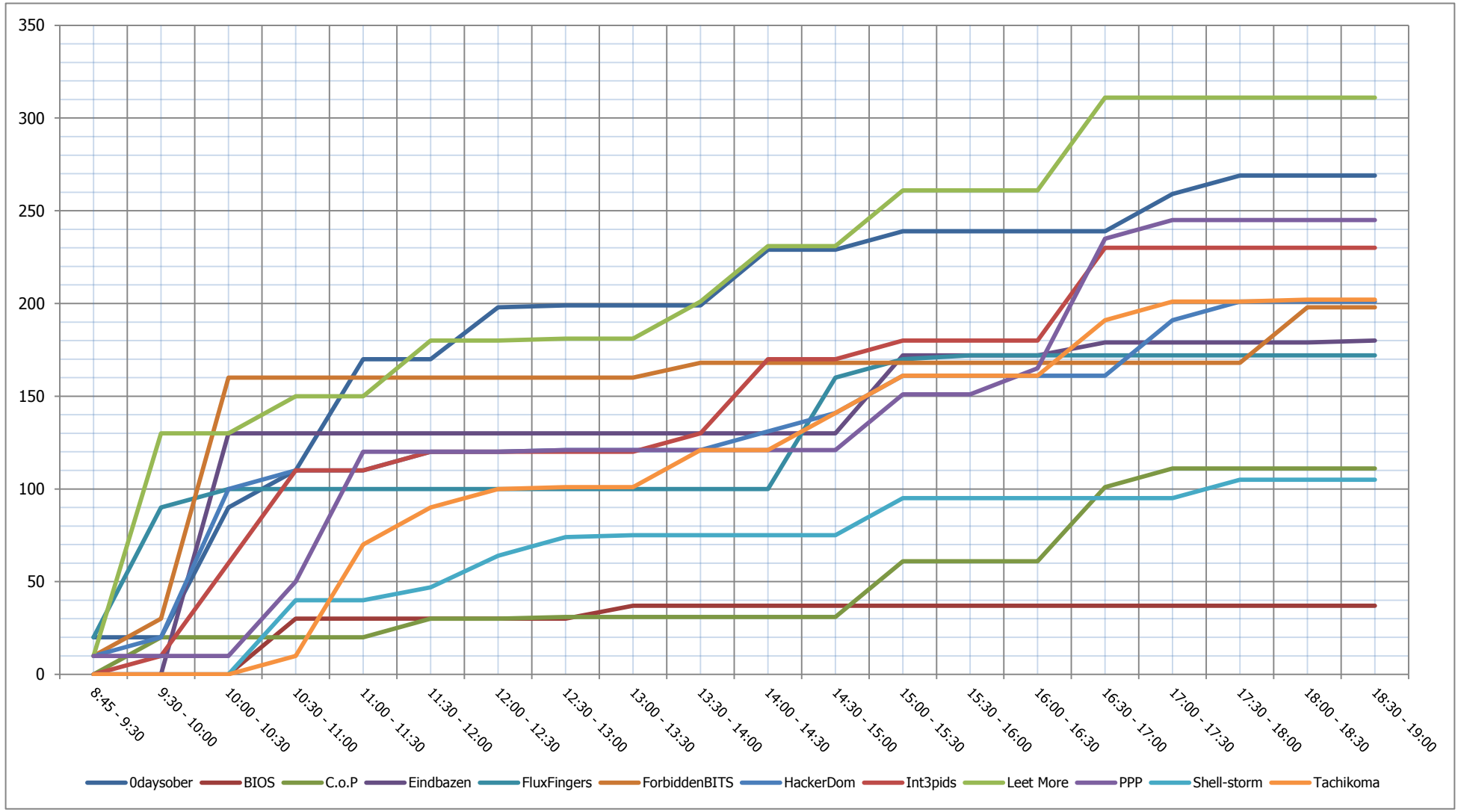


Рисунок 8. Хронология начисления баллов в рамках заданий командной инфраструктуры во второй день соревнований

6.1.2. Динамика начисления баллов

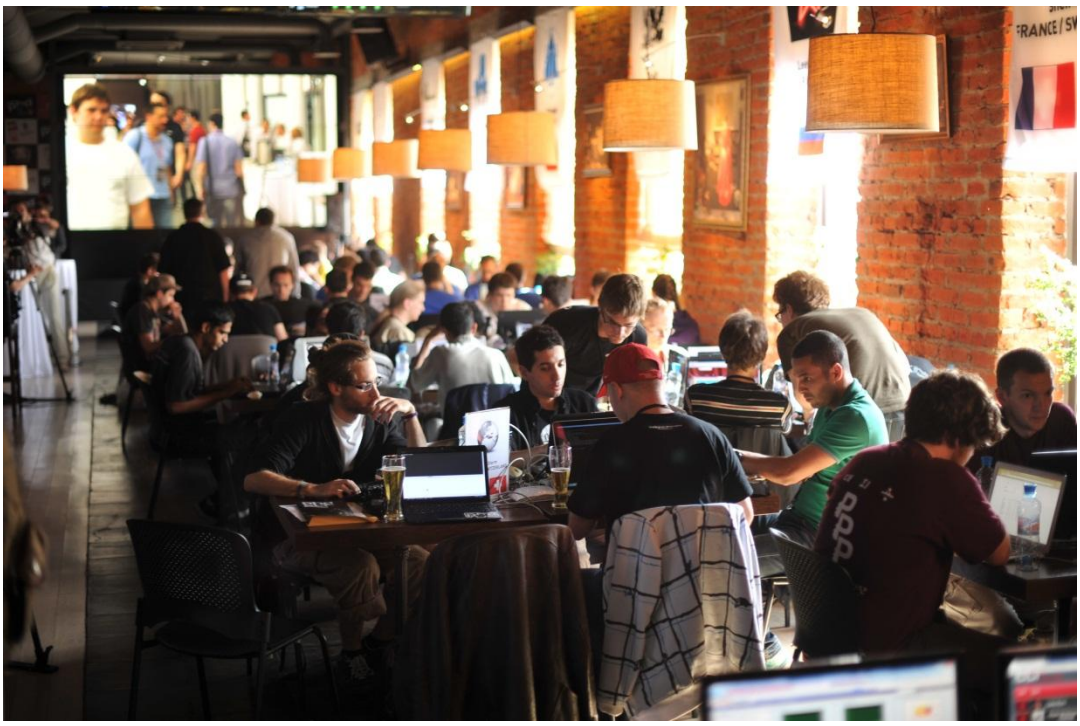
Динамика начисления баллов представлена в табл. 2 и на рис. 9—11, отдельно для первого и второго дней соревнований и ночных заданий.

Как видно из графиков, в первый день соревнований командам потребовалось всего около часа, чтобы вникнуть в задание и осуществить первые атаки на системы соперников. Быстрее и активнее всех оказалась команда PPP, а команда BIOS так и не набрала баллов в данном виде заданий ни в первый день, ни ночью.

Ночью активнее всех была команда Int3pids, заработавшая более 200 баллов, собирая бонусные флаги с сервисов команд соперников.

Во второй день соревнований команды были не столь активны, как в первый. Команде Leet More удалось вырваться вперед по итогам второго дня и выйти на второе место в рейтинге команд по данному виду соревнований.

Динамика активности команд, отраженная на графиках, показывает, что большинство команд справлялись с заданиями и захватывали флаги с сервисов соперников как днем, так и ночью. Активность команд до последних минут соревнований показывает, насколько ожесточенной была борьба.



Фотография 4. Зал, в котором проводился CTF

6.1.3. Анализ действий участников

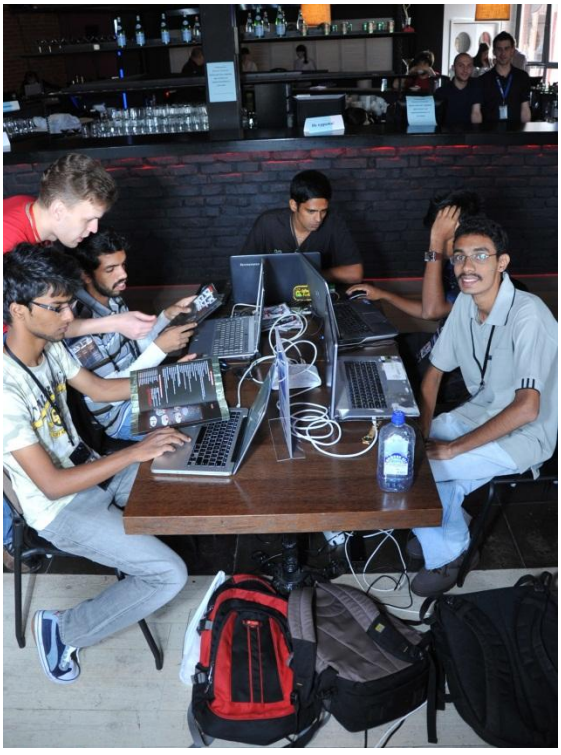
Анализ результатов соревнований показал, что отдельные команды старались автоматизировать эксплуатацию уязвимостей, найденных в сервисах соперников, пользуясь тем, что по условиям соревнований командам предоставляются полностью идентичные системы.

Команда PPP из США первой набрала баллы в рамках командной инфраструктуры, при этом участникам удалось проэксплуатировать одну и ту же уязвимость (задание PHPWWW/ST0) на сервисах всех команд практически за 4 минуты, причем 8 флагов были введены в систему всего за 3 секунды. Данный факт позволяет предположить, что участники из США успели не только раньше всех найти уязвимость, но и написать код, автоматизирующий процесс ее эксплуатации. Причем сделали они это прежде, чем кто-либо из соперников смог защитить свои сервисы. Данный факт отражен на рис. 6 и 9.

Анализ журналов показал, что участники команды PPP придерживались данной тактики на протяжении всего CTF: разница по времени между вводами флагов в систему зачастую не превышала 2 секунд. Таким образом, количество баллов, набранных командой в рамках командной инфраструктуры, напрямую зависело от скорости устранения уязвимостей командами соперников.

Подобная тактика была выявлена также у команд C.o.P и Leet More.

Команды BIOS и Tachikoma предположительно вводили флаги только вручную. Данная тактика не позволила командам заработать большого количества баллов, в данном рейтинге они заняли два последних места.



Фотография 5. Команда BIOS

Активность команд позволяют отследить диаграммы динамики начисления баллов, в частности диаграммы на рис. 9—11. Начисление баллов командам отражено в виде пиков.

Относительно других команд трудно сделать точные выводы, поскольку интервалы времени между вводами последующих флагов составляют более 15 секунд. За это время команды могли как вводить все предварительно найденные флаги вручную, так и автоматизировано проводить атаки. В отдельных случаях, судя по идентичности временного интервала между вводами флагов и повторению последовательности атакуемых команд, можно предположить, что почти все команды периодически пытались автоматизировать процесс эксплуатации найденных уязвимостей.

Моменты, когда команды применяли автоматизированный способ эксплуатации уязвимостей на сервисах команд соперников, отражаются на графиках в виде пиков, выделяющихся из общей динамики начисления баллов. Данные пики образуются за счет того, что команда получает большее количество баллов за меньшее время относительно других команд, которые в данный момент не успели ввести найденные флаги либо еще не решили задание.

Отчетливо видна разница в динамике первого и второго игровых дней. В первый день командам удавалось атаковать намного больше соперников в каждом задании: можно сделать вывод о том, что участники уделяли меньше внимания защите собственных сервисов. Во второй день, согласно статистике, большинство команд закрывало уязвимости в своей инфраструктуре раньше, чем их успевал эксплуатировать соперник. Лишь в начале дня лидерам удалось набрать большое количество баллов за счет незакрытых уязвимостей других команд.

Опираясь на хронологию начисления баллов, трудно сделать вывод, в какой именно момент времени та или иная команда закрыла уязвимость сервиса своей инфраструктуры. Это связано с тем, что время начисления баллов различным командам за захват флага с сервиса конкретной команды соперников зачастую различается на несколько часов. Существуют интервалы времени, когда команды перестают терять флаги при атаках соперников, и создается впечатление, что уязвимость закрыта, но позднее снова фиксируются факты успешных атак. В связи с этим мы делаем предположение, что команды, которые производили эксплуатацию уязвимостей вручную, сначала собирали найденные флаги, а затем вводили их последовательно в систему. Данная тактика не позволяет с точностью определить время решения задачи, а следовательно, и время закрытия уязвимости.

Кроме того, можно предположить, что команды использовали различные алгоритмы при атаках, поэтому одним удавалось обойти защиту соперника и захватить флаг, а другим нет. Таким образом, защищенный, по мнению команды, сервис снова становился целью соперников.

Таблица 2. Динамика начисления баллов в рамках заданий командной инфраструктуры

Временной интервал	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	110	0	0
10:00 - 10:30	80	0	60	90	50	0	90	10	110	0	50	0
10:30 - 11:00	10	0	40	0	0	50	0	30	0	80	20	0
11:00 - 11:30	70	0	0	0	0	0	0	0	0	0	0	0
11:30 - 12:00	0	0	70	7	0	0	0	0	70	0	0	0
12:00 - 12:30	0	0	0	0	7	0	0	0	0	0	0	0
12:30 - 13:00	10	0	0	50	80	0	40	0	0	0	30	0
13:00 - 13:30	0	0	0	0	10	0	0	7	90	0	0	0
13:30 - 14:00	0	0	0	0	0	7	0	0	10	10	0	0
14:00 - 14:30	0	7	0	0	0	0	3	0	0	0	0	0
14:30 - 15:00	14	0	0	0	0	0	0	0	0	0	0	10
15:00 - 15:30	0	0	0	0	0	0	0	0	80	50	0	0
15:30 - 16:00	0	0	0	90	70	0	0	0	0	60	0	17
16:00 - 16:30	60	0	0	0	0	0	50	0	21	40	0	0
16:30 - 17:00	0	0	0	70	0	50	0	60	0	100	60	0
17:00 - 17:30	0	0	0	0	60	0	0	90	0	0	0	0
17:30 - 18:00	0	0	0	0	0	0	0	0	0	0	0	0
18:00 - 18:30	0	0	60	0	20	0	0	60	0	0	0	20
18:30 - 19:00	0	0	0	20	0	0	0	0	0	0	0	70
19:00 - 19:30	0	0	0	0	0	0	0	0	0	0	0	0
19:30 - 20:00	0	0	0	0	0	0	0	0	0	0	0	0
20:00 - 20:30	0	0	0	0	0	0	0	0	0	0	0	0
20:30 - 21:00	0	0	0	0	0	0	0	0	0	0	0	0
21:00 - 21:30	3	0	0	0	0	0	0	0	0	0	0	0
21:30 - 22:00	0	0	0	0	0	0	0	0	0	0	3	0
22:00 - 22:30	0	0	0	0	0	0	0	0	0	0	0	0
22:30 - 23:00	0	0	0	0	0	0	0	0	0	0	0	0
23:00 - 23:30	0	0	0	0	0	0	0	0	0	0	0	0
23:30 - 00:00	0	0	0	0	0	0	0	0	0	0	0	0
Ночь												
0:00 - 0:30	0	0	0	0	0	0	0	0	0	0	0	0
0:30 - 1:00	3	0	13	0	0	0	0	0	0	0	0	0
1:00 - 1:30	4	0	11	0	0	0	0	0	0	0	2	0
1:30 - 2:00	0	0	4	9	0	0	9	1	1	0	4	0
2:00 - 2:30	18	0	12	22	12	0	15	14	22	10	5	0
2:30 - 3:00	8	0	11	12	11	0	11	19	8	12	0	0
3:00 - 3:30	10	0	11	14	15	0	1	23	12	14	16	0
3:30 - 4:00	13	6	16	9	9	0	0	18	11	12	11	0
4:00 - 4:30	9	6	12	9	6	0	0	21	9	9	9	0
4:30 - 5:00	6	4	7	8	6	0	2	20	6	7	3	0
5:00 - 5:30	5	5	5	5	4	1	0	19	5	6	0	0
5:30 - 6:00	13	0	0	5	0	5	0	22	6	8	0	0
6:00 -6:30	11	2	0	10	0	5	0	21	6	11	1	0
6:30 - 7:00	9	3	0	6	0	3	0	17	3	9	0	0
7:00 -7:30	3	1	0	2	0	1	10	6	1	2	0	0
7:30 - 8:00	0	0	0	0	0	0	0	0	0	0	0	0
8:00 - 8:30	0	0	0	0	0	0	40	0	0	0	0	0
8:30 - 8:45	0	0	0	0	0	0	0	0	0	40	0	0
2 день 31.05.2012												
8:45 - 9:30	20	0	0	0	20	10	10	0	10	10	0	0
9:30 - 10:00	0	0	20	0	70	20	10	10	120	0	0	0
10:00 - 10:30	70	0	0	130	10	130	80	50	0	0	0	0
10:30 - 11:00	20	30	0	0	0	0	10	50	20	40	40	10
11:00 - 11:30	60	0	0	0	0	0	0	0	0	70	0	60
11:30 - 12:00	0	0	10	0	0	0	10	10	30	0	7	20
12:00 - 12:30	28	0	0	0	0	0	0	0	0	0	17	10
12:30 - 13:00	1	0	1	0	0	0	1	0	1	1	10	1
13:00 - 13:30	0	7	0	0	0	0	0	0	0	0	1	0
13:30 - 14:00	0	0	0	0	0	8	0	10	20	0	0	20
14:00 - 14:30	30	0	0	0	0	0	10	40	30	0	0	0
14:30 - 15:00	0	0	0	0	60	0	10	0	0	0	0	20
15:00 - 15:30	10	0	30	42	10	0	20	10	30	30	20	20
15:30 - 16:00	0	0	0	0	2	0	0	0	0	0	0	0
16:00 - 16:30	0	0	0	0	0	0	0	0	0	14	0	0
16:30 - 17:00	0	0	40	7	0	0	0	50	50	70	0	30
17:00 - 17:30	20	0	10	0	0	0	30	0	0	10	0	10
17:30 - 18:00	10	0	0	0	0	0	10	0	0	0	10	0
18:00 - 18:30	0	0	0	0	0	30	0	0	0	0	0	1
18:30 - 19:00	0	0	0	1	0	0	0	0	0	0	0	0

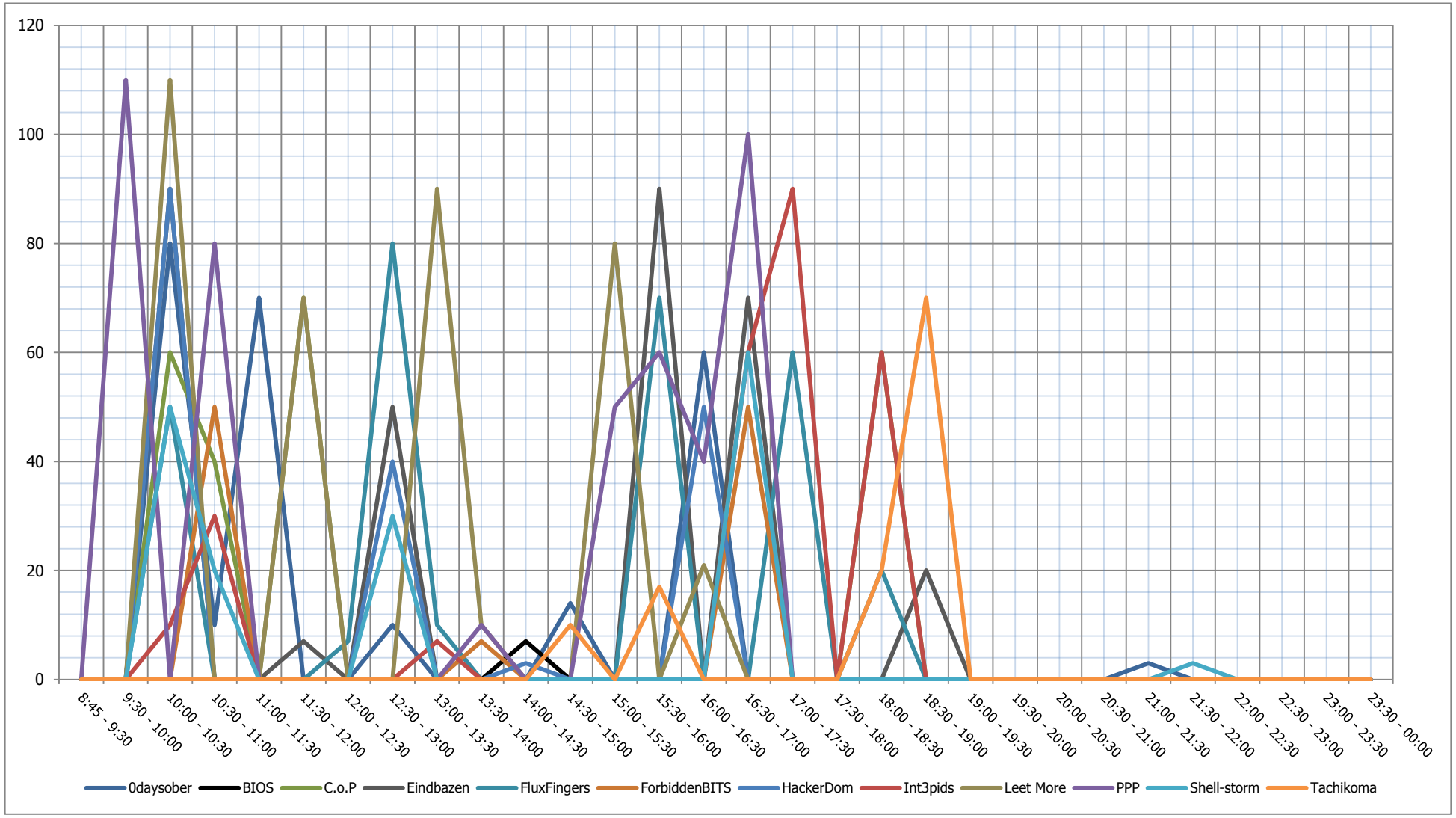


Рисунок 9. Динамика начисления баллов в рамках заданий командной инфраструктуры в первый день соревнований

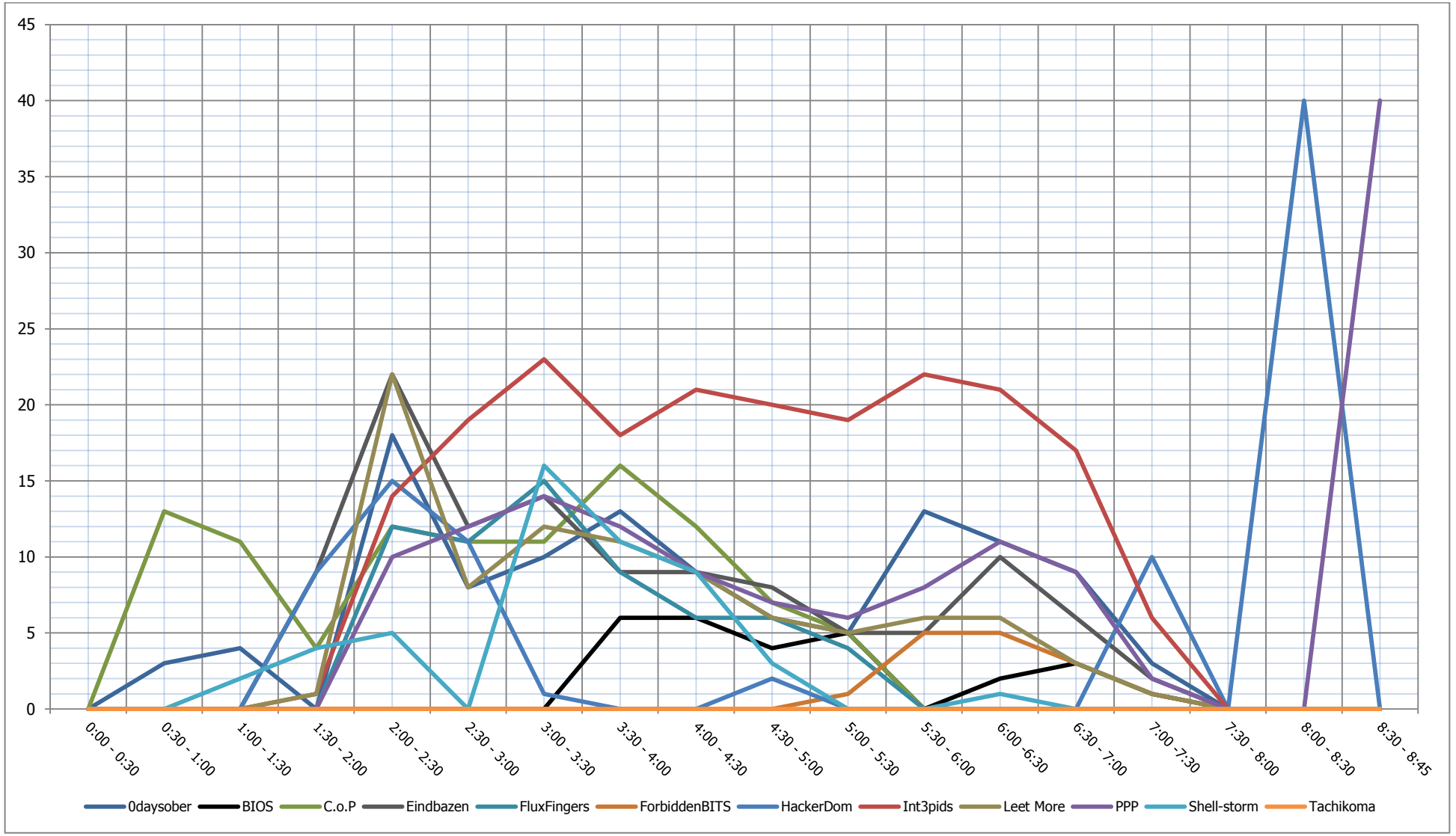


Рисунок 10. Динамика начисления баллов в рамках заданий командной инфраструктуры в ночное время

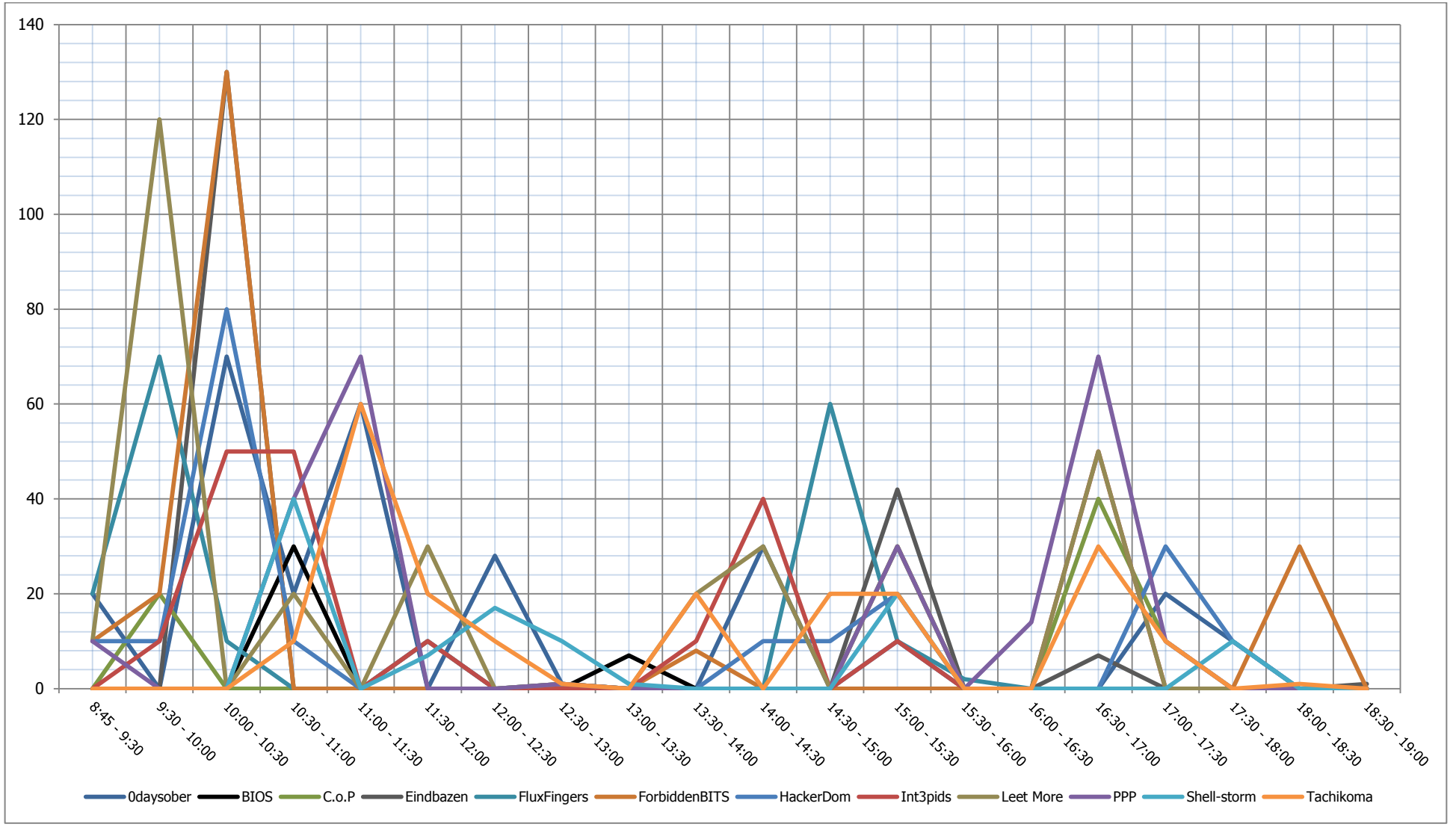


Рисунок 11. Динамика начисления баллов в рамках заданий командной инфраструктуры во второй день соревнований

6.2. Распределение баллов в рамках заданий общей инфраструктуры

Данные, отражающие количество баллов, заработанных командами только путем захвата флагов на уязвимых сервисах общей инфраструктуры, приведены на рис. 12. В рамках данного типа заданий места распределились следующим образом: на первом месте команда Int3pids, на втором — C.o.P, на третьем — Eindbazen.

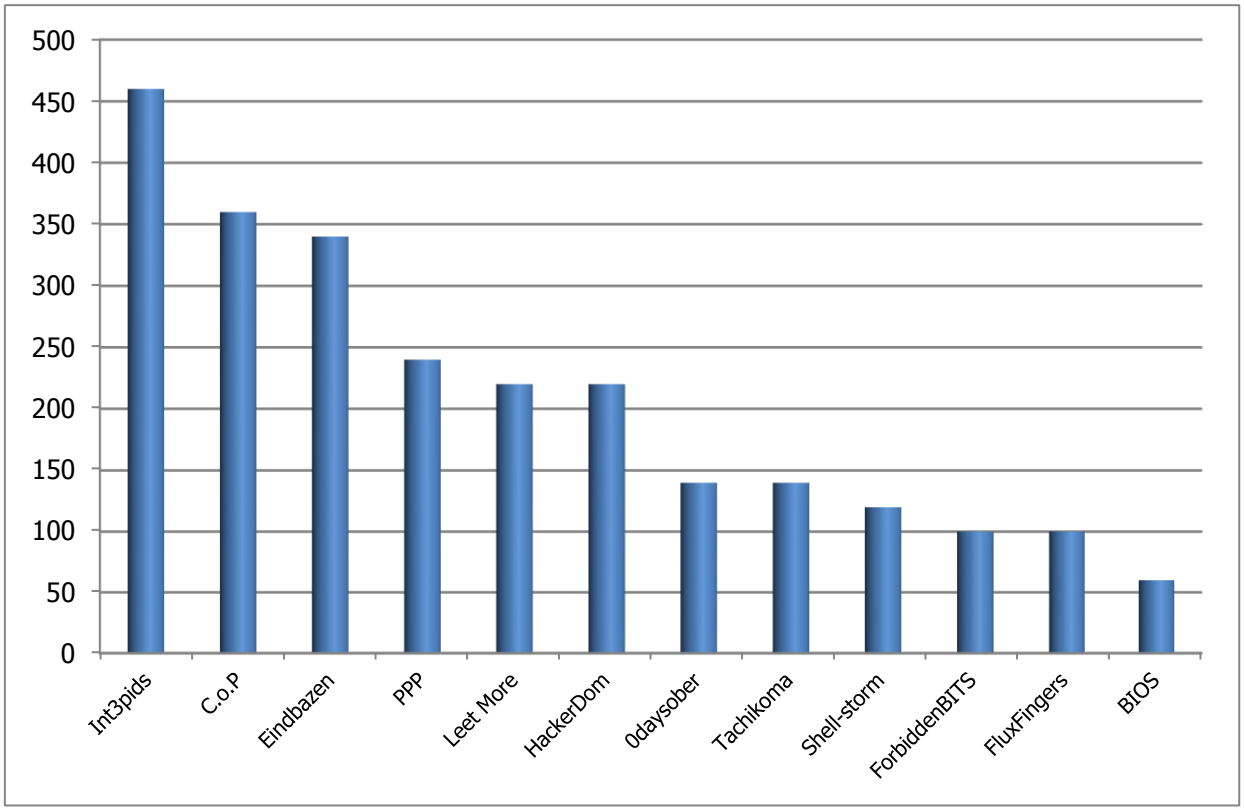


Рисунок 12. Баллы, заработанные командами в заданиях общей инфраструктуры

6.2.1. Хронология начисления баллов

Хронология начисления баллов представлена в табл. 3 и на рис. 13—15, отдельно для первого и второго дней соревнований и ночных заданий.

Таблица 3. Хронология начисления баллов в рамках заданий общей инфраструктуры

Временной интервал	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	0	0	0
10:00 - 10:30	0	0	0	0	0	0	0	0	0	0	0	0
10:30 - 11:00	0	0	0	0	0	0	0	0	0	0	0	0
11:00 - 11:30	0	0	0	0	0	0	0	0	0	0	0	0
11:30 - 12:00	0	0	0	0	0	0	0	0	0	0	0	0
12:00 - 12:30	0	0	0	0	0	0	0	0	0	0	0	0
12:30 - 13:00	0	0	0	20	0	0	0	0	0	0	0	0
13:00 - 13:30	0	0	0	20	0	0	0	0	0	40	0	0
13:30 - 14:00	0	0	20	60	0	0	40	40	0	40	0	0
14:00 - 14:30	0	0	20	60	0	0	60	100	0	40	0	0
14:30 - 15:00	0	0	20	80	20	0	80	100	60	60	0	0
15:00 - 15:30	0	0	40	80	20	20	80	100	60	60	20	0
15:30 - 16:00	20	20	40	80	20	20	80	120	60	60	20	0
16:00 - 16:30	20	60	40	80	20	20	80	120	60	60	20	0
16:30 - 17:00	60	60	40	80	20	20	80	120	60	60	20	0
17:00 - 17:30	60	60	40	80	20	20	80	120	60	60	20	0
17:30 - 18:00	60	60	40	80	20	20	80	120	60	60	20	0
18:00 - 18:30	60	60	40	120	60	20	80	120	60	60	20	0
18:30 - 19:00	60	60	40	120	60	20	80	120	60	60	20	0
19:00 - 19:30	60	60	40	160	60	20	80	160	60	60	20	0
19:30 - 20:00	60	60	40	160	60	20	80	160	60	60	40	0
20:00 - 20:30	60	60	80	200	60	20	80	160	60	60	40	0
20:30 - 21:00	60	60	80	200	80	40	80	160	60	60	40	0
21:00 - 21:30	60	60	80	200	80	40	100	160	60	60	40	0
21:30 - 22:00	60	60	80	200	80	40	100	160	60	60	80	0
22:00 - 22:30	60	60	80	200	80	40	100	300	80	60	80	0
22:30 - 23:00	60	60	80	200	80	40	100	360	80	140	80	0
23:00 - 23:30	60	60	80	200	100	40	140	360	80	140	80	0
23:30 - 00:00	80	60	120	200	100	40	140	380	80	140	80	0
Ночь												
0:00 - 0:30	0	0	0	0	0	0	0	0	0	20	20	0
0:30 - 1:00	0	0	0	0	0	0	0	0	0	20	40	0
1:00 - 1:30	20	0	0	0	0	0	0	0	0	20	40	0
1:30 - 2:00	20	0	60	0	0	0	0	0	0	20	40	0
2:00 - 2:30	20	0	100	0	0	0	0	0	40	20	40	0
2:30 - 3:00	20	0	100	0	0	0	0	0	40	20	40	0
3:00 - 3:30	20	0	100	0	0	0	0	0	60	20	40	0
3:30 - 4:00	20	0	100	40	0	0	0	0	60	20	40	0
4:00 - 4:30	20	0	100	60	0	0	0	0	60	40	40	0
4:30 - 5:00	20	0	120	120	0	0	0	0	60	40	40	0
5:00 - 5:30	20	0	120	120	0	0	40	0	60	40	40	0
5:30 - 6:00	20	0	120	120	0	0	40	0	60	40	40	0
6:00 -6:30	20	0	120	120	0	0	40	0	60	40	40	0
6:30 - 7:00	20	0	120	120	0	0	40	0	60	40	40	0
7:00 -7:30	20	0	120	120	0	0	40	0	60	40	40	0
7:30 - 8:00	20	0	120	120	0	0	40	0	60	40	40	0
8:00 - 8:30	20	0	120	120	0	0	40	0	60	40	40	0
8:30 - 8:45	20	0	120	120	0	0	40	0	60	40	40	0
2 день 31.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	0	0	0
10:00 - 10:30	0	0	0	0	0	0	0	0	0	0	0	0
10:30 - 11:00	0	0	0	0	0	0	0	0	0	0	0	0
11:00 - 11:30	0	0	0	0	0	0	20	0	0	0	0	0
11:30 - 12:00	0	0	0	0	0	0	20	20	20	0	0	0
12:00 - 12:30	0	0	0	0	0	0	20	20	20	40	0	0
12:30 - 13:00	0	0	20	20	0	0	20	20	60	40	0	0
13:00 - 13:30	0	0	20	20	0	0	20	20	80	40	0	0
13:30 - 14:00	0	0	20	20	0	0	20	20	80	40	0	0
14:00 - 14:30	0	0	20	20	0	60	20	20	80	40	0	0
14:30 - 15:00	0	0	20	20	0	60	20	40	80	60	0	0
15:00 - 15:30	0	0	20	20	0	60	20	40	80	60	0	0
15:30 - 16:00	0	0	20	20	0	60	20	60	80	60	0	80
16:00 - 16:30	40	0	20	20	0	60	20	60	80	60	0	120
16:30 - 17:00	40	0	20	20	0	60	20	60	80	60	0	120
17:00 - 17:30	40	0	20	20	0	60	40	80	80	60	0	120
17:30 - 18:00	40	0	100	20	0	60	40	80	80	60	0	120
18:00 - 18:30	40	0	100	20	0	60	40	80	80	60	0	140
18:30 - 19:00	40	0	120	20	0	60	40	80	80	60	0	140

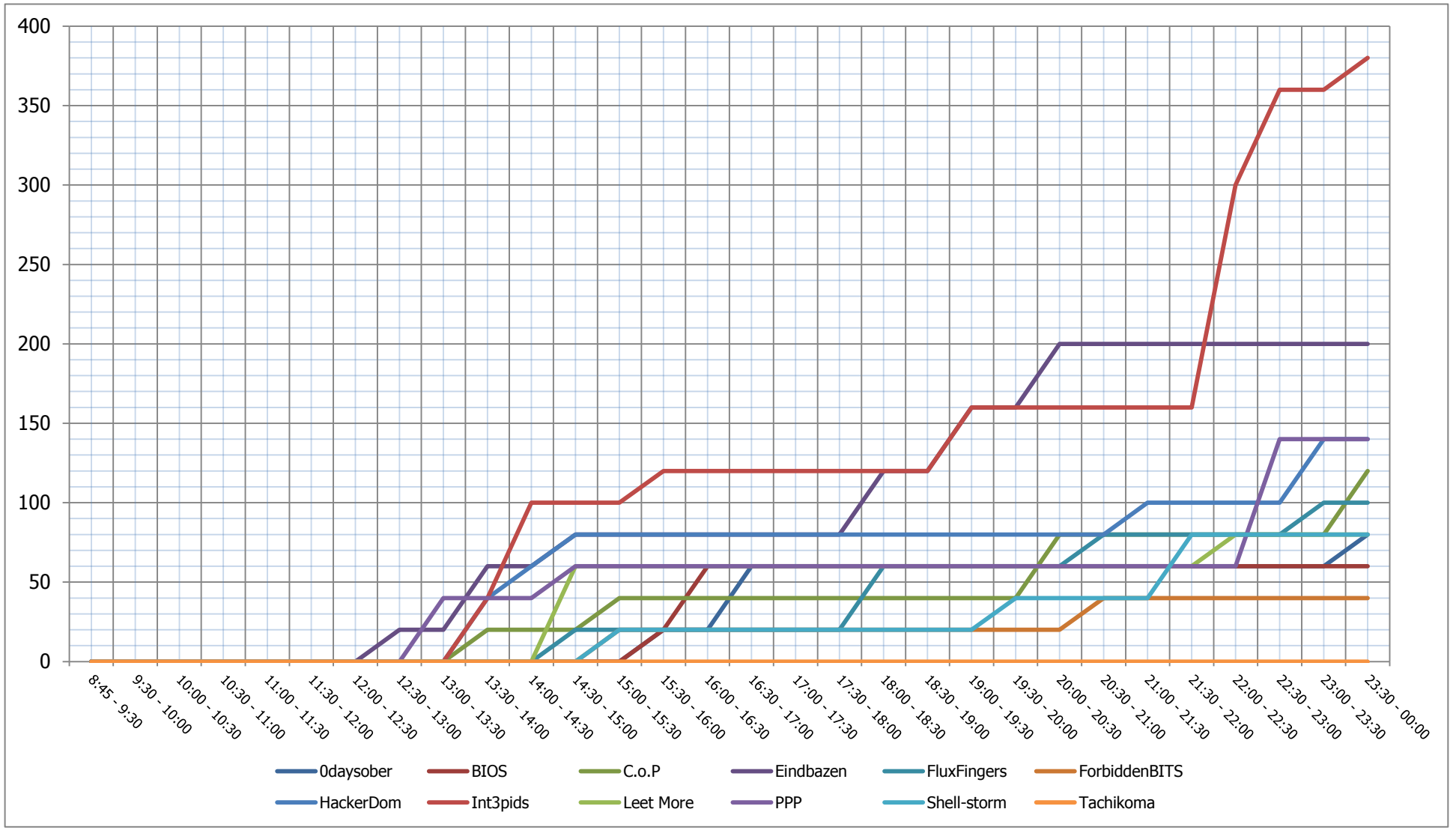


Рисунок 13. Хронология начисления баллов в рамках заданий общей инфраструктуры в первый день соревнований

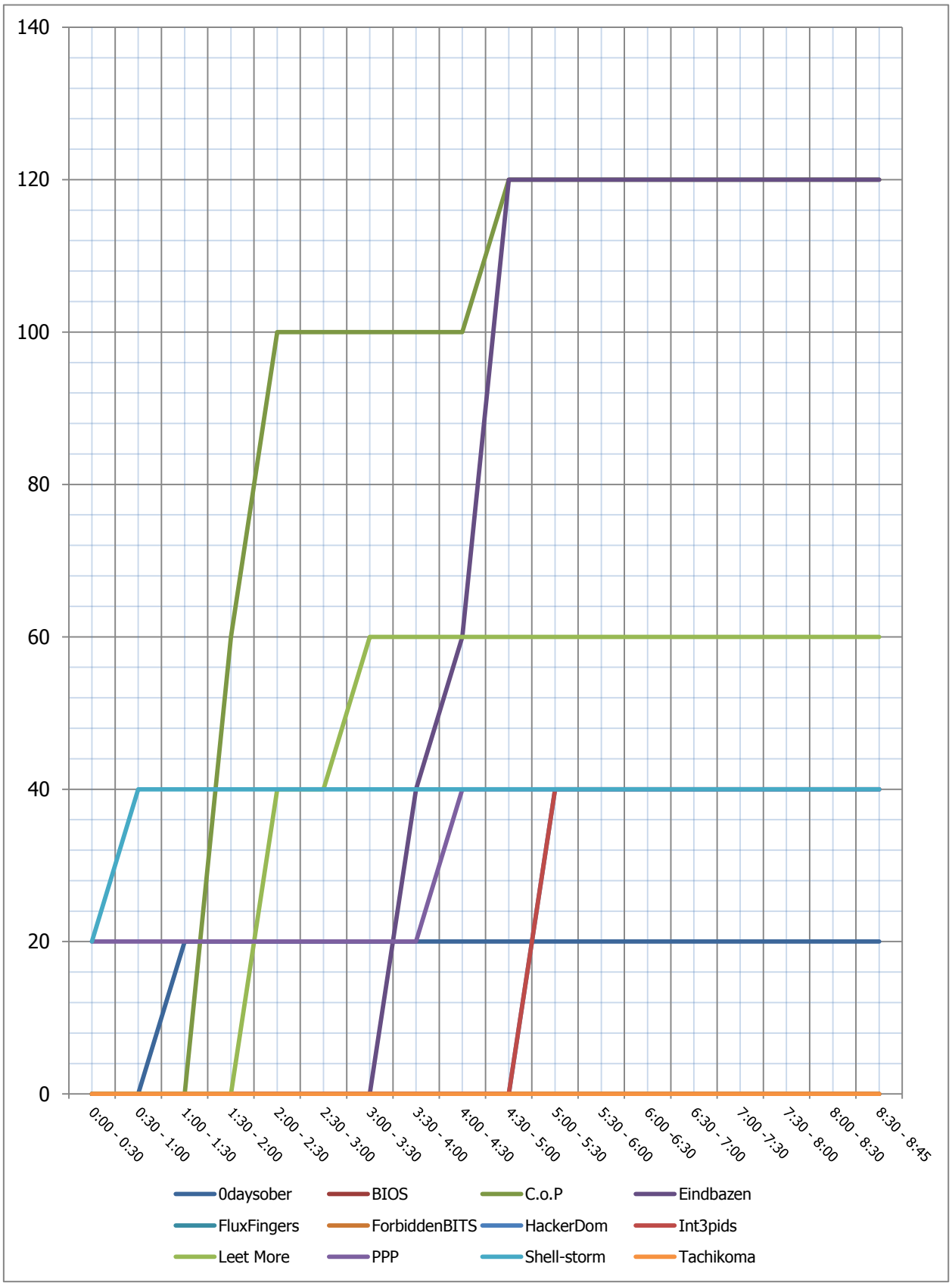


Рисунок 14. Хронология начисления баллов в рамках заданий общей инфраструктуры в ночное время

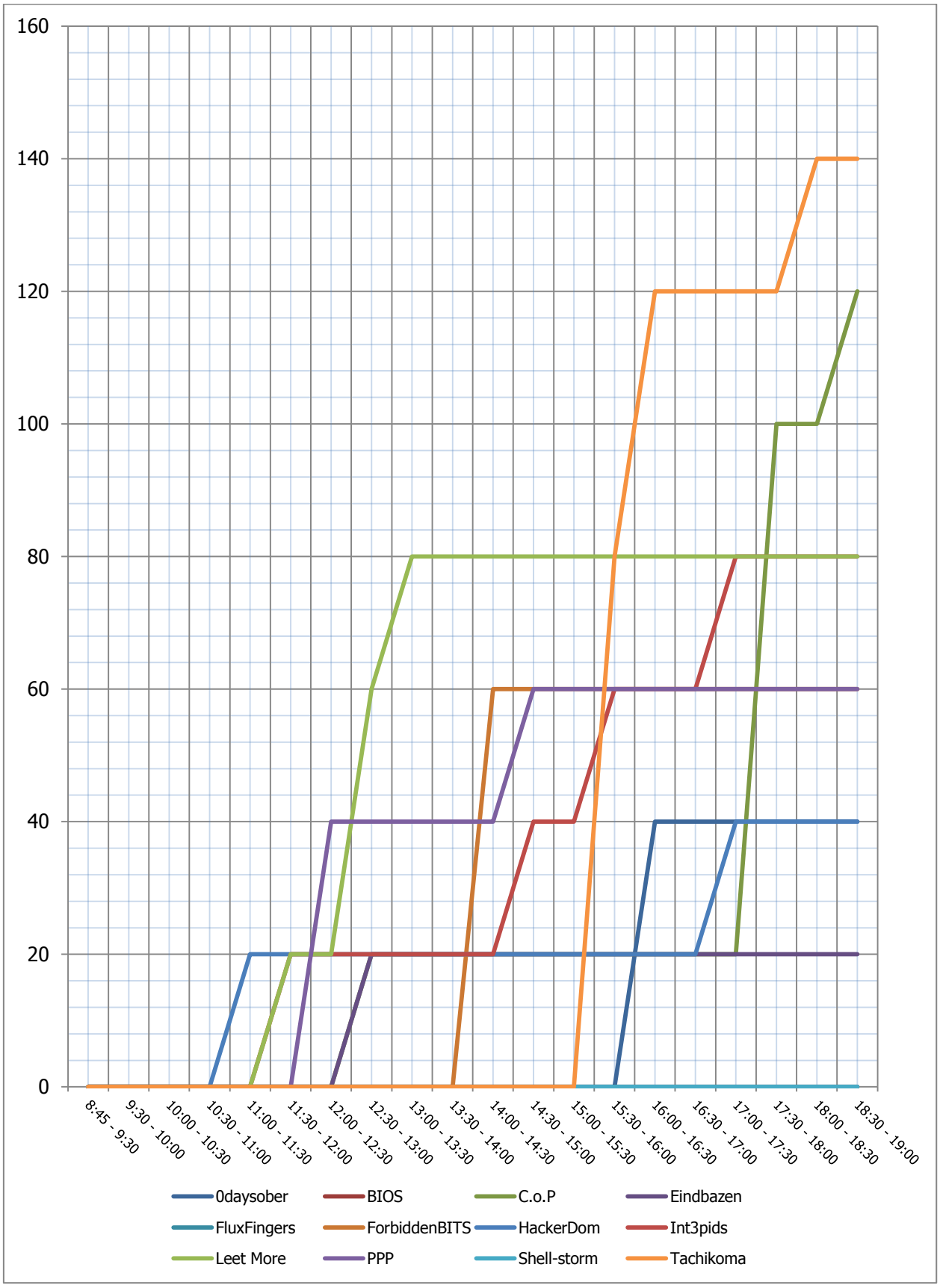


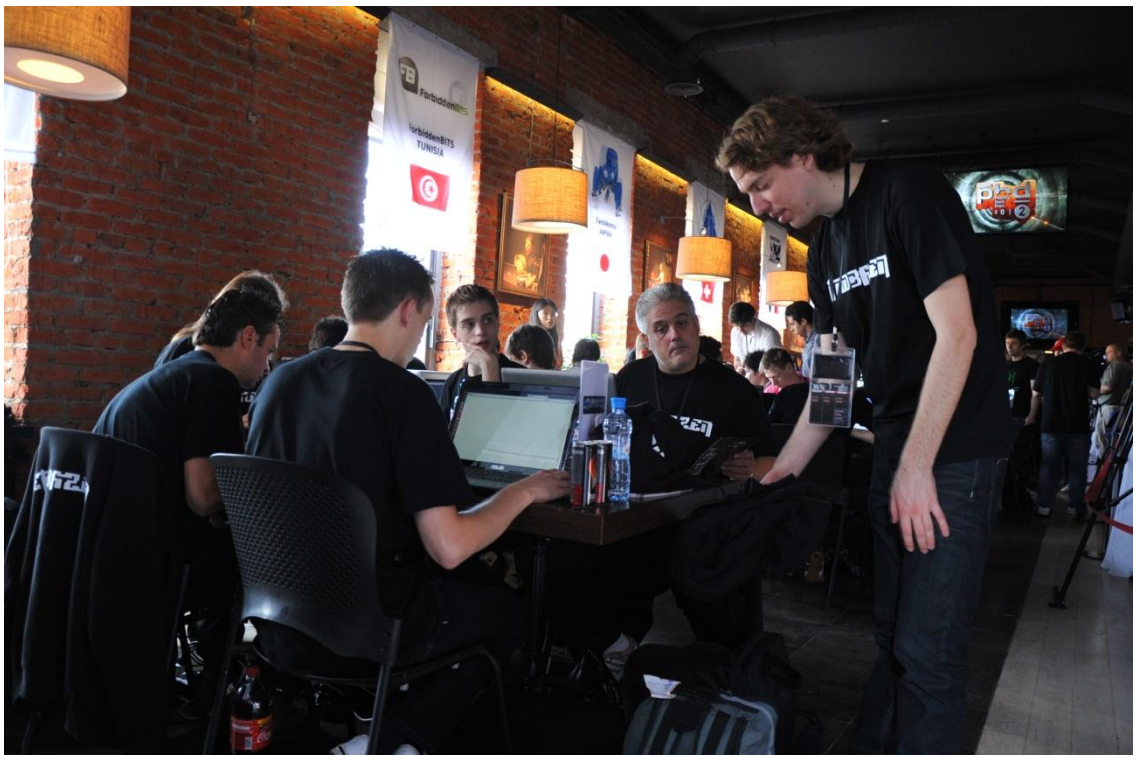
Рисунок 15. Хронология начисления баллов в рамках заданий общей инфраструктуры во второй день соревнований

6.2.2. Динамика начисления баллов

Динамика начисления баллов представлена в табл. 4 и на рис. 17—19 отдельно для первого и второго дней соревнований и ночных заданий.

Результаты соревнований в части заданий общей инфраструктуры показали, что командам потребовалось около трех часов, чтобы разобраться в заданиях и добиться первых результатов. Среди команд выделяется тройка лидеров, явных аутсайдеров нет: три команды не смогли набрать более 100 баллов, при этом половина команд заработала менее 150 баллов.

В первый день соревнований явным лидером в данном рейтинге стала команда Int3pids, в то время как команда Tachikoma не набрала ни одно балла. На графике первого дня соревнований (рис. 17) можно выделить две команды. В среднем все команды в течение этого дня набирали не более 60 баллов в час. Команда Int3pids набрала 200 баллов в течение одного часа, для этого участникам потребовалось решить 10 заданий. Команде PPP удалось набрать 80 баллов в рамках общей инфраструктуры в течение получаса, решив всего одно задание (THECUBE). Однако этот факт не помог участникам подняться на вторую строчку в зачете общей инфраструктуры по итогам дня: команда Eindbazen опередила их на 60 баллов, набирая свои баллы относительно равномерно на протяжении всего дня. Всплески активности команд отражены на диаграмме в виде пиков (рис. 17).



Фотография 6. Участники команды Eindbazen

Анализ решенных командами задач показал, что команда Eindbazen смогла набрать столь большое количество баллов в течение часа за счет решения заданий одной тематики (ANDROID com.gia.bot). Можно предположить, что среди участников команды был специалист соответствующий квалификации: команде удалось решить практически все задания данного блока. Среди всех участников CTF задание THECUBE в итоге смогла решить лишь команда PPP.

Стоит также отметить, что команды в течение дня расходовали свои ресурсы, в частности, на решение заданий командной инфраструктуры, а вечером у участников появилось больше времени на решение заданий общей инфраструктуры, чем, видимо, и воспользовались участники Int3pids и PPP.

Фотография 7. Участники команды PPP

Ночью команды были не так активны: лишь две из них набрали более 60 баллов за всю ночь. Стоит отметить, что почти половина команд не набрала за ночь ни одного балла общей инфраструктуры.

Согласно рис. 19, отражающему динамику начисления баллов, во второй день активность команд заметно снизилась. Можно выделить команды C.o.P. и Tachikoma.

Второй день соревнований показал, что даже аутсайдеры (команда Tachikoma) способны решать задания данного типа. Команда из Японии стала лидером второго дня в зачете общей инфраструктуры и обогнала многих своих соперников, при этом она смогла решить за час сразу три задания и набрать 120

баллов. Стоит отметить, что до этого команда на протяжении первого дня и ночи не набрала в данном виде соревнований ни одного балла.

Участники из команды C.o.P, решив всего одно задание (crackme_Artefact) заработали 80 баллов. Команда оказалась единственной среди участников CTF, кто справился с данным заданием.

Всплески активности команд отражены на диаграмме в виде пиков (рис. 19).

Всего в данной части соревнований было предусмотрено 72 задания различной степени сложности (и стоимости решения). Из них с 37 заданиями (это белее половины) не справилась ни одна команда, 30 заданий решили менее половины команд (с 22 заданиями справилась всего одна из команд); всего 5 заданий были решены более чем половиной команд. Полученная статистика представлена на диаграмме (рис. 16).

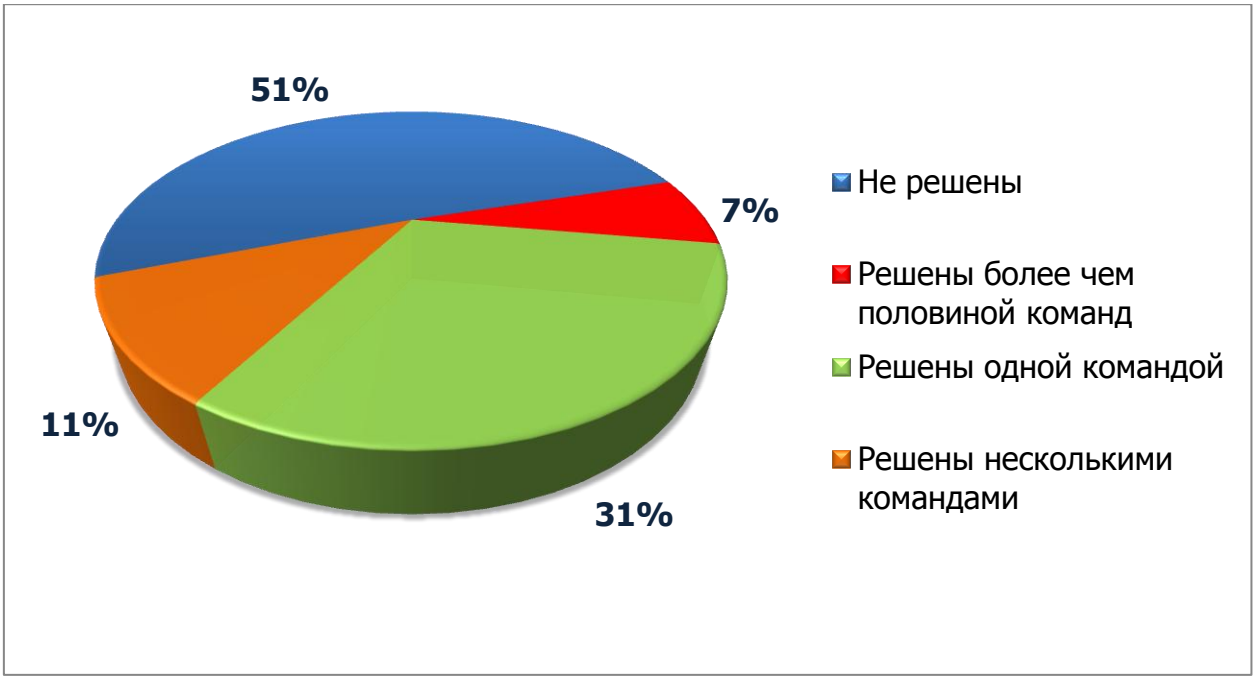


Рисунок 16. Статистика решенных задач общей инфраструктуры

Каждая команда могла заработать до 2000 баллов, решив все задания общей инфраструктуры; таким образом, в сумме все команды могли заработать 24 000 баллов. По результатам CTF все команды вместе набрали 2500 баллов в рамках заданий общей инфраструктуры (примерно 10% потенциально возможных). Лидером в данной части соревнований оказалась команда Int3pids, набравшая 460 баллов (23% потенциально возможных).

Таблица 4. Динамика начисления баллов в рамках заданий общей инфраструктуры

	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	0	0	0
10:00 - 10:30	0	0	0	0	0	0	0	0	0	0	0	0
10:30 - 11:00	0	0	0	0	0	0	0	0	0	0	0	0
11:00 - 11:30	0	0	0	0	0	0	0	0	0	0	0	0
11:30 - 12:00	0	0	0	0	0	0	0	0	0	0	0	0
12:00 - 12:30	0	0	0	0	0	0	0	0	0	0	0	0
12:30 - 13:00	0	0	0	20	0	0	0	0	0	0	0	0
13:00 - 13:30	0	0	0	0	0	0	0	0	0	40	0	0
13:30 - 14:00	0	0	20	40	0	0	40	40	0	0	0	0
14:00 - 14:30	0	0	0	0	0	0	20	60	0	0	0	0
14:30 - 15:00	0	0	0	20	20	0	20	0	60	20	0	0
15:00 - 15:30	0	0	20	0	0	20	0	0	0	0	20	0
15:30 - 16:00	20	20	0	0	0	0	0	20	0	0	0	0
16:00 - 16:30	0	40	0	0	0	0	0	0	0	0	0	0
16:30 - 17:00	40	0	0	0	0	0	0	0	0	0	0	0
17:00 - 17:30	0	0	0	0	0	0	0	0	0	0	0	0
17:30 - 18:00	0	0	0	0	0	0	0	0	0	0	0	0
18:00 - 18:30	0	0	0	40	40	0	0	0	0	0	0	0
18:30 - 19:00	0	0	0	0	0	0	0	0	0	0	0	0
19:00 - 19:30	0	0	0	40	0	0	0	40	0	0	0	0
19:30 - 20:00	0	0	0	0	0	0	0	0	0	0	20	0
20:00 - 20:30	0	0	40	40	0	0	0	0	0	0	0	0
20:30 - 21:00	0	0	0	0	20	20	0	0	0	0	0	0
21:00 - 21:30	0	0	0	0	0	0	20	0	0	0	0	0
21:30 - 22:00	0	0	0	0	0	0	0	0	0	0	40	0
22:00 - 22:30	0	0	0	0	0	0	0	140	20	0	0	0
22:30 - 23:00	0	0	0	0	0	0	0	60	0	80	0	0
23:00 - 23:30	0	0	0	0	20	0	40	0	0	0	0	0
23:30 - 00:00	20	0	40	0	0	0	0	20	0	0	0	0
Ночь												
0:00 - 0:30	0	0	0	0	0	0	0	0	0	20	20	0
0:30 - 1:00	0	0	0	0	0	0	0	0	0	0	20	0
1:00 - 1:30	20	0	0	0	0	0	0	0	0	0	0	0
1:30 - 2:00	0	0	60	0	0	0	0	0	0	0	0	0
2:00 - 2:30	0	0	40	0	0	0	0	0	40	0	0	0
2:30 - 3:00	0	0	0	0	0	0	0	0	0	0	0	0
3:00 - 3:30	0	0	0	0	0	0	0	0	20	0	0	0
3:30 - 4:00	0	0	0	40	0	0	0	0	0	0	0	0
4:00 - 4:30	0	0	0	20	0	0	0	0	0	20	0	0
4:30 - 5:00	0	0	20	60	0	0	0	0	0	0	0	0
5:00 - 5:30	0	0	0	0	0	0	40	0	0	0	0	0
5:30 - 6:00	0	0	0	0	0	0	0	0	0	0	0	0
6:00 -6:30	0	0	0	0	0	0	0	0	0	0	0	0
6:30 - 7:00	0	0	0	0	0	0	0	0	0	0	0	0
7:00 -7:30	0	0	0	0	0	0	0	0	0	0	0	0
7:30 - 8:00	0	0	0	0	0	0	0	0	0	0	0	0
8:00 - 8:30	0	0	0	0	0	0	0	0	0	0	0	0
8:30 - 8:45	0	0	0	0	0	0	0	0	0	0	0	0
2 день 31.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	0	0	0
10:00 - 10:30	0	0	0	0	0	0	0	0	0	0	0	0
10:30 - 11:00	0	0	0	0	0	0	0	0	0	0	0	0
11:00 - 11:30	0	0	0	0	0	0	20	0	0	0	0	0
11:30 - 12:00	0	0	0	0	0	0	0	20	20	0	0	0
12:00 - 12:30	0	0	0	0	0	0	0	0	0	40	0	0
12:30 - 13:00	0	0	20	20	0	0	0	0	40	0	0	0
13:00 - 13:30	0	0	0	0	0	0	0	0	20	0	0	0
13:30 - 14:00	0	0	0	0	0	0	0	0	0	0	0	0
14:00 - 14:30	0	0	0	0	0	60	0	0	0	0	0	0
14:30 - 15:00	0	0	0	0	0	0	0	20	0	20	0	0
15:00 - 15:30	0	0	0	0	0	0	0	0	0	0	0	0
15:30 - 16:00	0	0	0	0	0	0	0	20	0	0	0	80
16:00 - 16:30	40	0	0	0	0	0	0	0	0	0	0	40
16:30 - 17:00	0	0	0	0	0	0	0	0	0	0	0	0
17:00 - 17:30	0	0	0	0	0	0	20	20	0	0	0	0
17:30 - 18:00	0	0	80	0	0	0	0	0	0	0	0	0
18:00 - 18:30	0	0	0	0	0	0	0	0	0	0	0	20
18:30 - 19:00	0	0	20	0	0	0	0	0	0	0	0	0

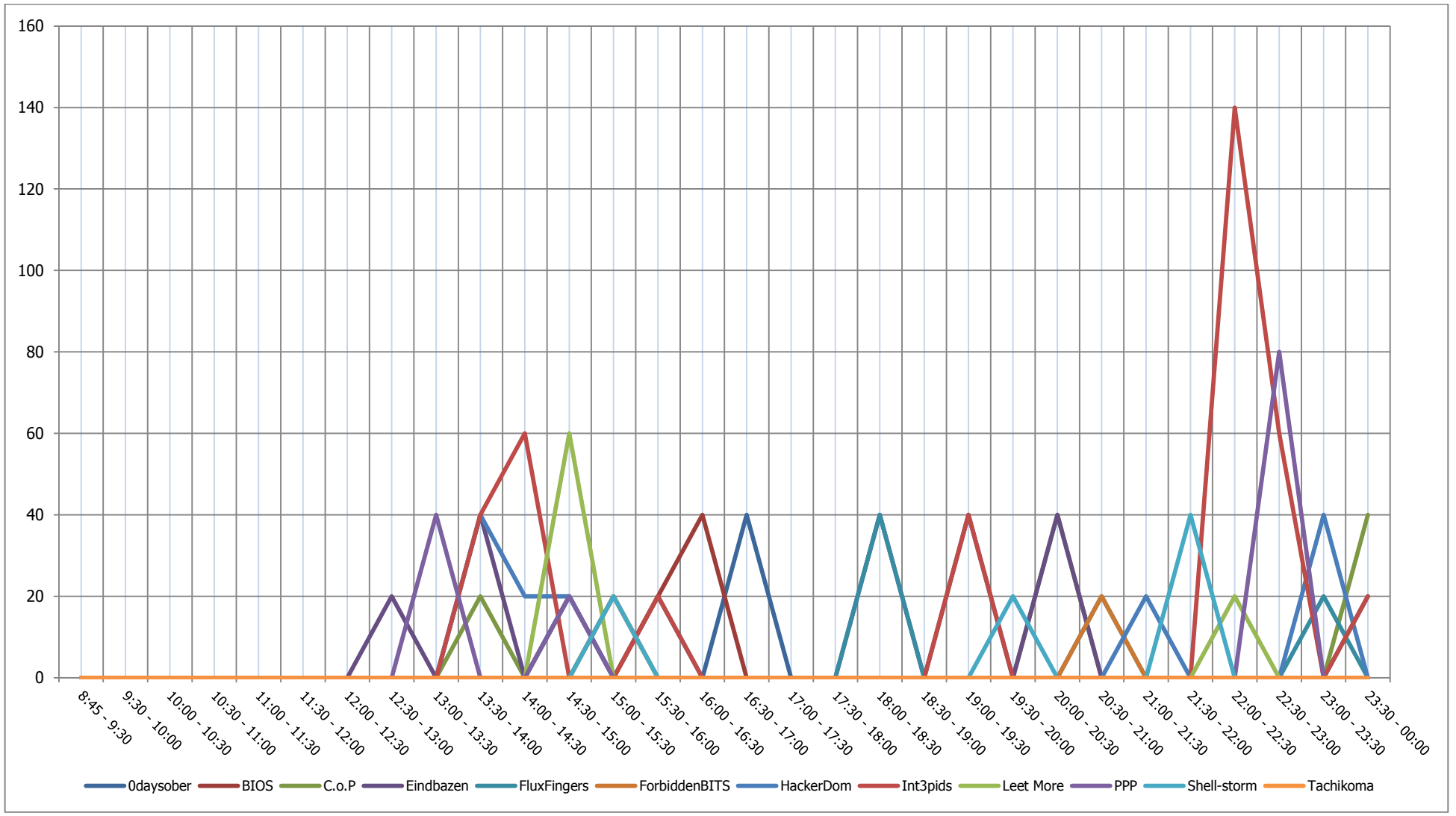


Рисунок 17. Динамика начисления баллов в рамках заданий общей инфраструктуры в первый день соревнований

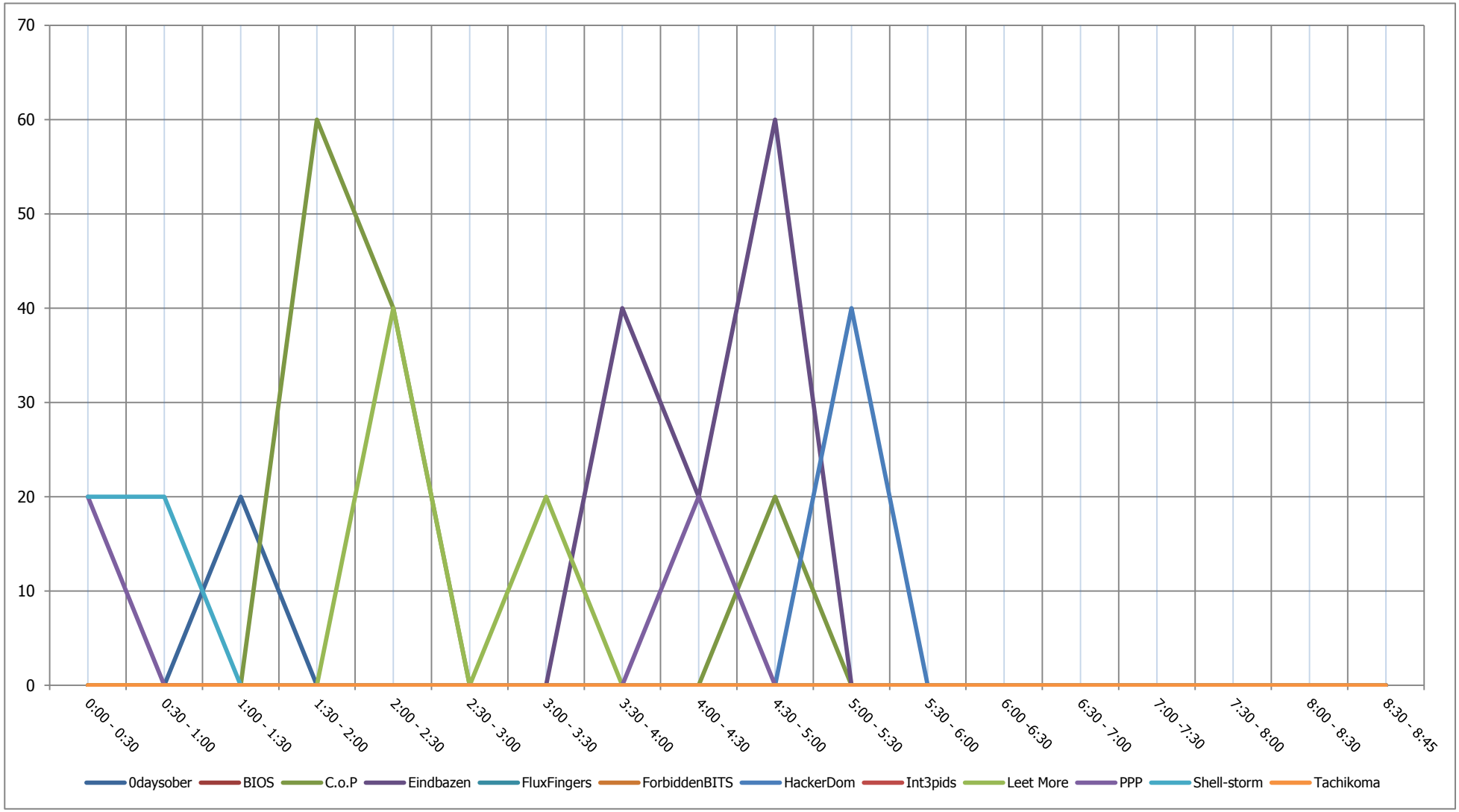


Рисунок 18. Динамика начисления баллов в рамках заданий общей инфраструктуры в ночное время

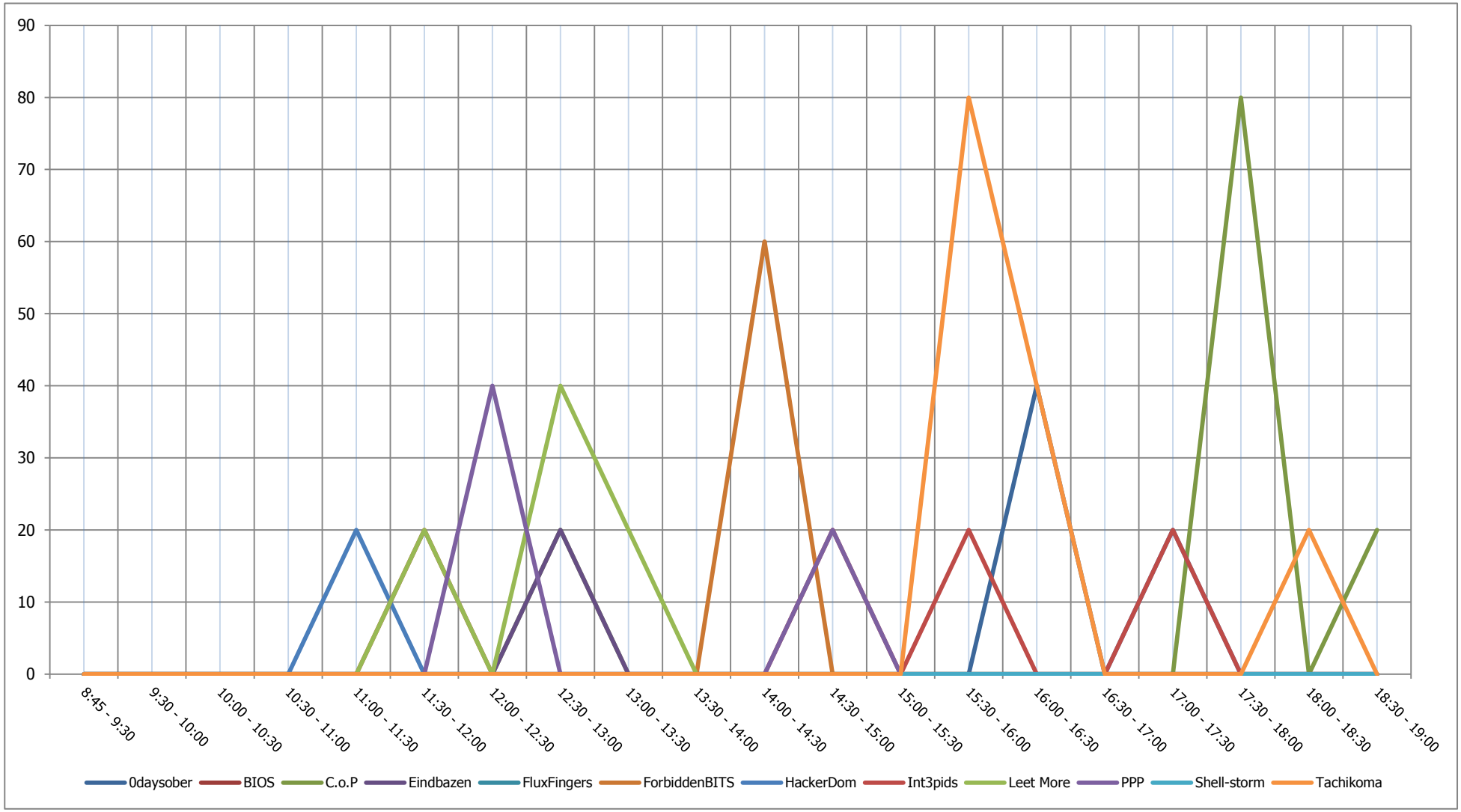


Рисунок 19. Динамика начисления баллов в рамках заданий общей инфраструктуры во второй день соревнований

6.2.3. Результаты Online HackQuest

Наряду с соревнованиями CTF в рамках PHDays 2012 проводились онлайн-соревнования HackQuest для всех желающих из сети Интернет. Задания полностью совпадали с заданиями общей инфраструктуры CTF, основное различие заключалось во времени проведения и баллах, начисляемых за решение задач. Участники из сети Интернет получили доступ к игровым сервисам общей инфраструктуры на период с 30 мая по 21 июня 2012 года.

Набрать баллы смогли только 18 человек из числа всех зарегистрированных участников. Суммарно было зафиксировано 127 верных флагов.

По результатам соревнований CTF в рамках общей инфраструктуры было зафиксировано всего 88 верных флагов. Учитывая, что участникам CTF было предоставлено всего два дня на решение задач, а также что им необходимо было решать другие задания CTF, можно сделать вывод, что интернет-пользователи справились с заданиями хуже.

Результаты онлайн-соревнований представлены на рис. 20.

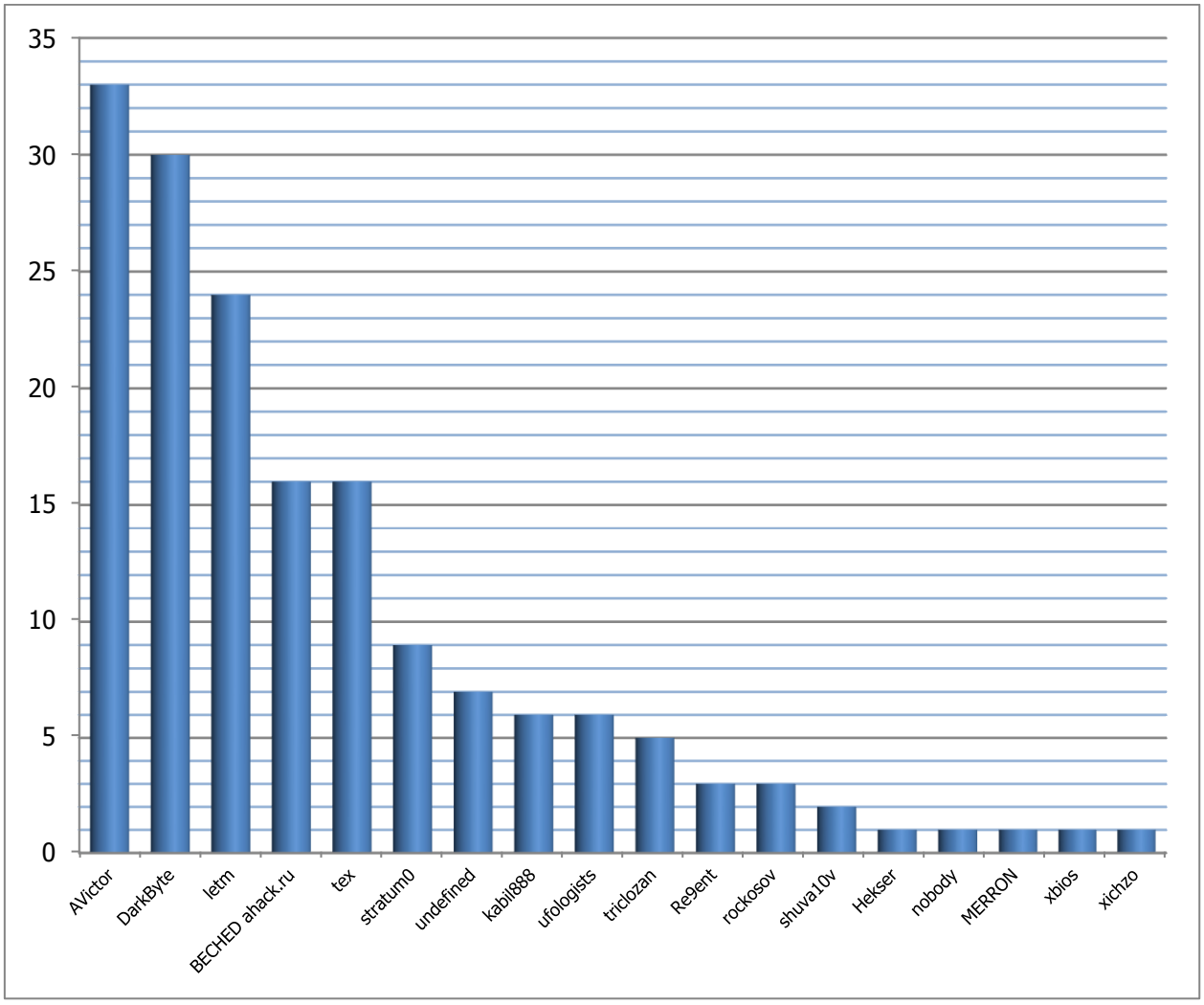


Рисунок 20. Результаты онлайн HackQuest

Сравнение результатов по количеству решенных заданий представлено в табл. 5.

Таблица 5. Сравнение результатов

ПАРАМЕТР	КОМАНДЫ CTF	УЧАСТНИКИ ИЗ ИНТЕРНЕТА
Всего заданий	72	
Не решены	37	37
Решены более чем половиной участников (команд)	5	2
Решены одним участником (командой)	22	5
Решены несколькими участниками (командами)	8	28

Полученная статистика онлайн-соревнований представлена на диаграмме (рис. 21).

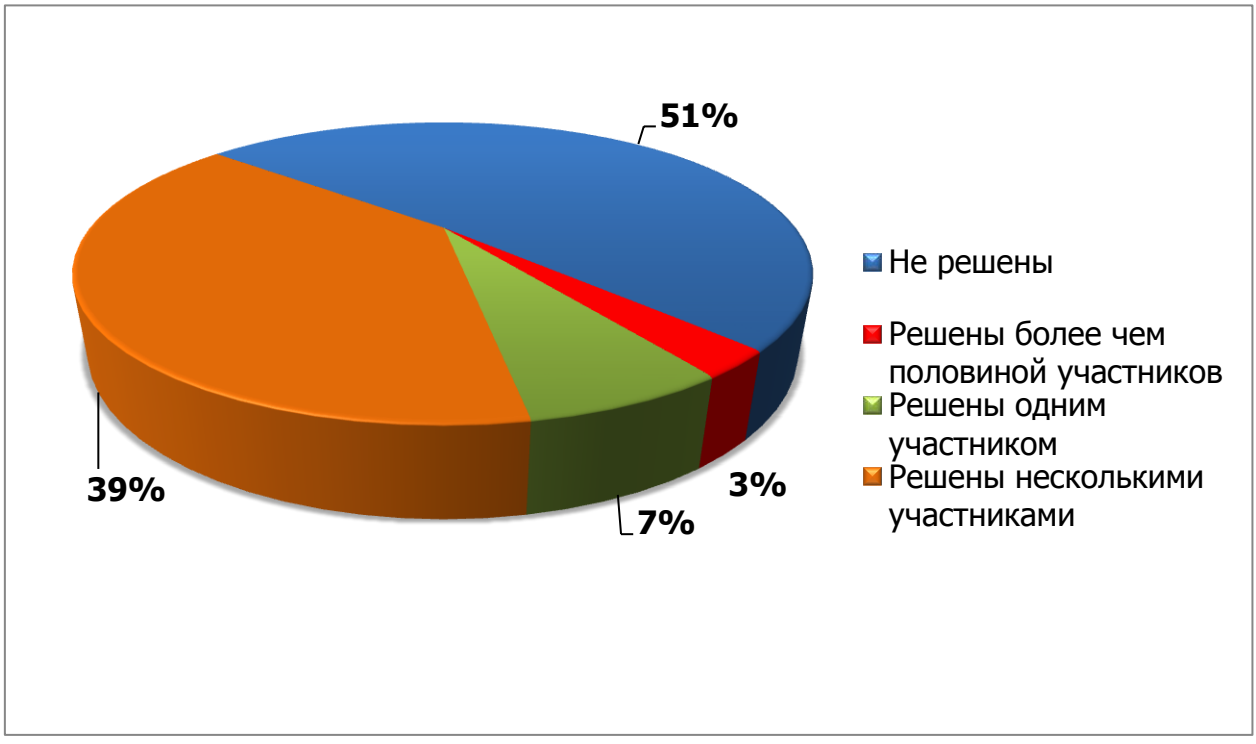


Рисунок 21. Статистика решенных заданий HackQuest

Хронология начисления баллов в рамках онлайн-соревнования HackQuest представлена на рис. 22.

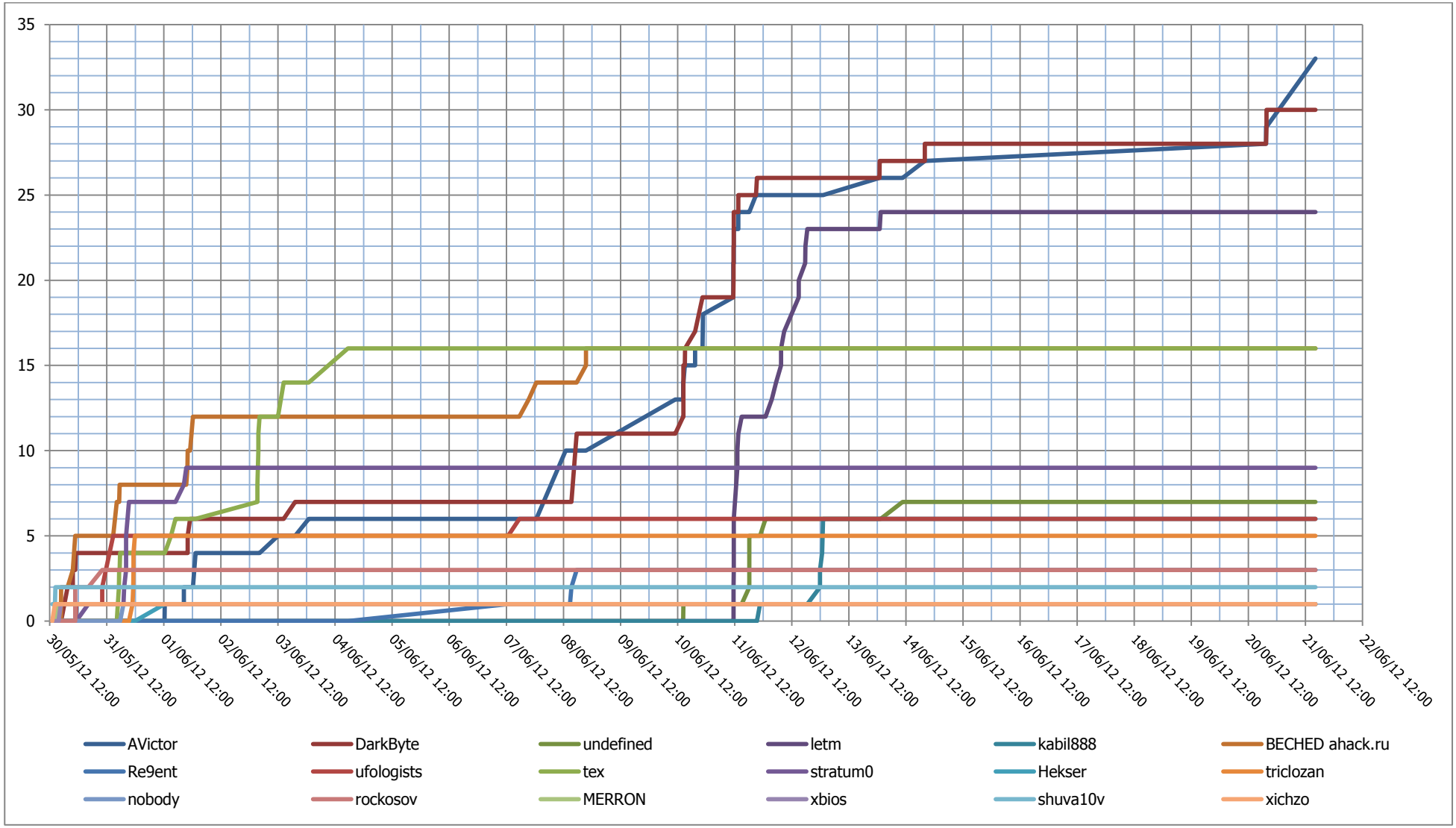


Рисунок 22. Хронология начисления баллов в рамках HackQuest

Объединенная статистика решения заданий командами CTF и участниками из Интернета представлена на диаграмме (рис. 23) и в табл. 6.

Таблица 6. Объединенная статистика заданий общей инфраструктуры

ВСЕГО ЗАДАНИЙ	72
Не решены	22
Решены только командами CTF	16
Решены только участниками HackQuest	15
Решены теми и другими участниками	19

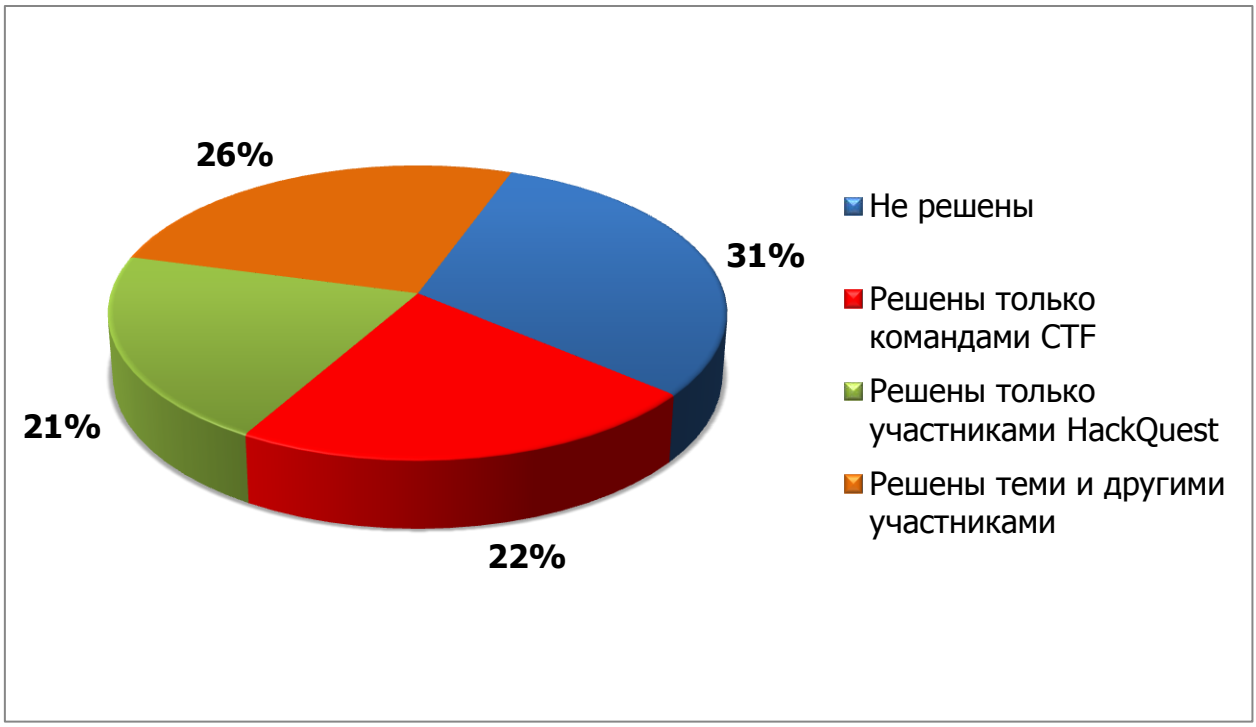


Рисунок 23. Объединенная статистика заданий общей инфраструктуры

Данная статистика показала, что треть заданий не были решены ни участниками из сети Интернет, ни командами во время проведения CTF. В то же время треть заданий были решены и теми и другими участниками. Большая доля нерешенных задач свидетельствует о высоком уровне соревнований и мотивирует будущих участников подобных мероприятий к совершенствованию своих профессиональных навыков и знаний.

6.3. Распределение баллов в рамках заданий инфраструктуры «Царь горы»

6.3.1. Распределение баллов среди команд CTF

Хронология начисления баллов в рамках заданий инфраструктуры «Царь горы» представлена на рис. 24 и в табл. 7.

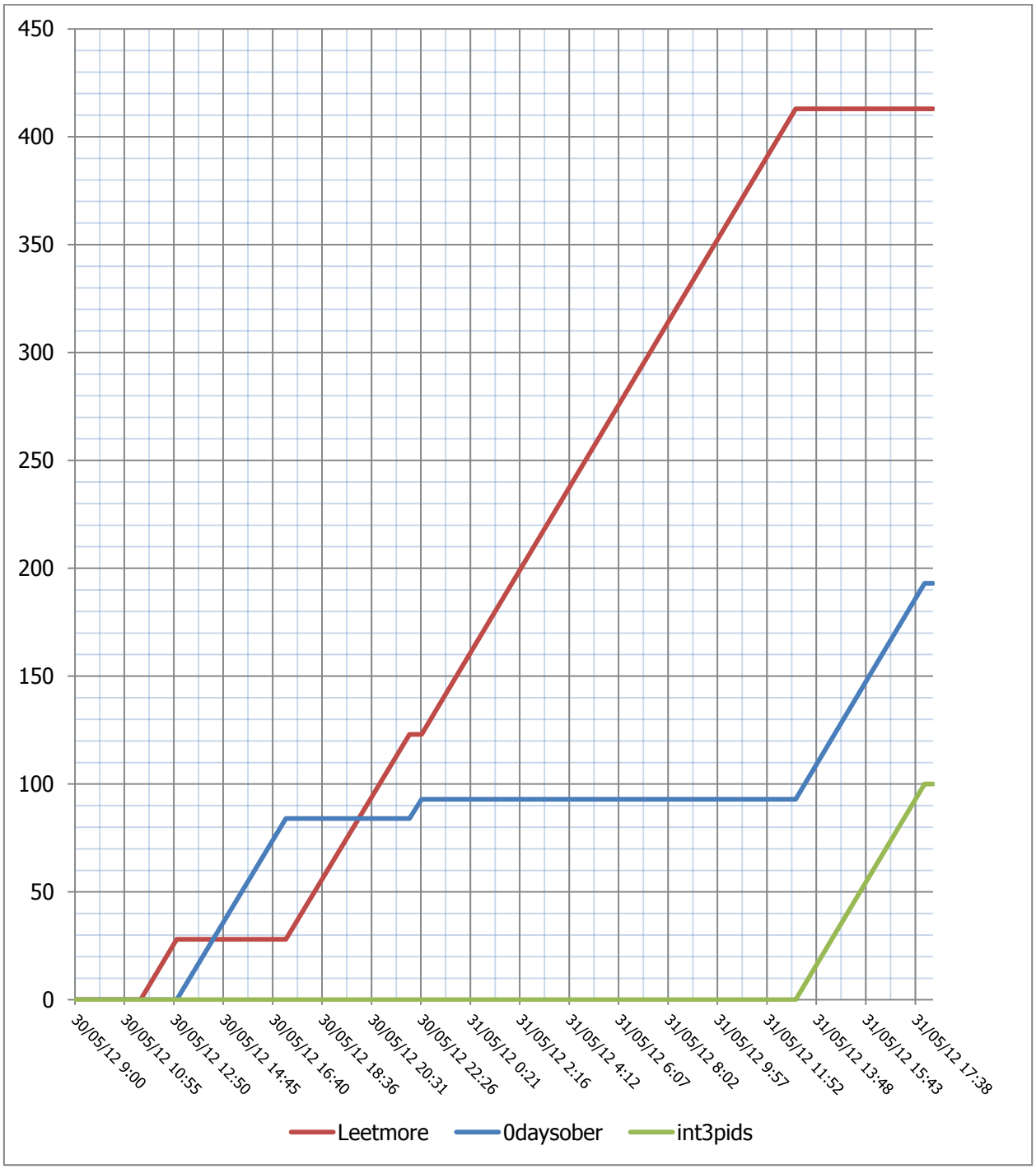


Рисунок 24. Хронология начисления баллов в рамках заданий инфраструктуры «Царь горы»

Таблица 7. Хронология начисления баллов в рамках заданий инфраструктуры «Царь горы»

Команда	Временной интервал	Игровой сервис	Продолжительность	Начисленные баллы	Текущие баллы команды
Leetmore	30.05.2012 11:32 30.05.2012 12:57	1vulnerableWeb	1:24:37	28	28
0daysober	30.05.2012 12:57 30.05.2012 17:11	1vulnerableWeb	4:14:09	84	84
Leetmore	30.05.2012 17:11 30.05.2012 21:59	1vulnerableWeb	4:47:59	95	123
0daysober	30.05.2012 21:59 30.05.2012 22:28	1vulnerableWeb	0:28:24	9	93
Leetmore	30.05.2012 22:28 31.05.2012 12:59	1vulnerableWeb	14:31:18	290	413
int3pids	31.05.2012 12:59 31.05.2012 18:00	1vulnerableWeb	5:00:26	100	100
0daysober	31.05.2012 12:59 31.05.2012 18:00	1vulnerableService	5:00:05	100	193

Согласно результатам, представленным в табл. 7, всего три команды справились заданиями первого уровня инфраструктуры «Царь горы».

Фотография 8. Участники команды 0daysober

Статистика показывает, что задание сервиса 1vulnerableService решили только участники команды 0daysober. За контроль сервиса 1vulnerableWeb велась борьба на протяжении двух дней соревнований.

Наибольшее количество баллов (413) удалось набрать команде Leet Moore. Участники из Leet More удерживали контроль над сервисом на протяжении более четырнадцати часов. Баллы, заработанные командой в данной категории, переломили ход соревнований и в итоге принесли команде победу.

Фотография 9. Таблица результатов соревнований на экране видео-стены в зале CTF

Ни одной из команд, принявших участие в соревнованиях, не удалось получить доступ к сервисам 2-го уровня, за контроль которого по правилам соревнований команды могли получить вдвое больше баллов, чем за контроль сервисов 1-го уровня.

6.3.2. Распределение баллов среди участников онлайн-соревнований «Царь горы»

Общие результаты онлайн-соревнований

После завершения соревнований PHDays CTF 2012 всем зарегистрировавшимся участникам из сети Интернет был предоставлен доступ к инфраструктуре «Царь горы». Онлайн соревнования проходили в период с 20 августа по 3 сентября 2012 года. Было зарегистрировано более 200 участников, среди которых только семеро смогли набрать баллы.

Подсчет баллов производился иначе, чем для команд, участвовавших в CTF. За каждую полную минуту контроля сервиса начислялся 1 балл (как за сервис 1-го

уровня, так и за сервис 2-го уровня). При равенстве начисляемых баллов, контроль сервиса 2-го уровня имел приоритетное значение.

Распределение баллов в рамках онлайн-соревнований представлено в табл. 8 и на рис. 25. Хронология начисления баллов представлена в табл. 9 и на рис. 26.

Таблица 8. Распределение баллов в рамках онлайн-соревнований «Царь горы»

Место	Участник	Сервисы 1 уровня		Сервис 2 уровня	Суммарное количество баллов
		«WWW»	«Services»	«Active Directory»	
1	beched AHack.Ru	7700	1277	597	9574
2	DarkByte	0	14412	0	14412
3	Antichat	9189	2	0	9191
4	Ereee	2676	0	0	2676
5	ei-grad	0	2648	0	2648
6	letm	0	340	0	340
7	coptere	264	0	0	264

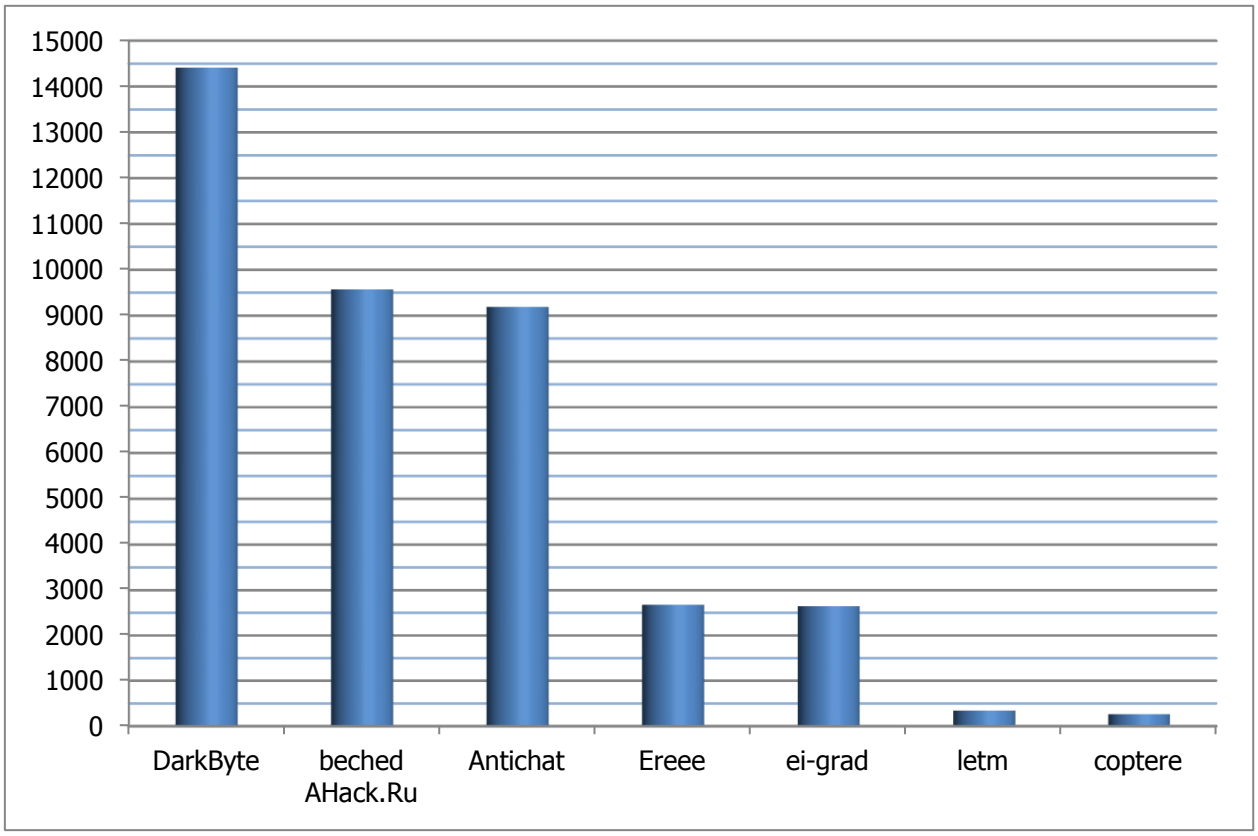


Рисунок 25. Распределение баллов в рамках онлайн-соревнований «Царь горы»

Таблица 9. Распределение баллов в рамках онлайн-соревнований «Царь горы»

ВРЕМЯ	BECHED AHACK.RU	EREEE	COPTERE	ANTICHAT	LETM	EI-GRAD	DARKBYTE
20.08.12 17:45	0	0	0	0	0	0	0
20.08.12 21:20	215	0	0	0	0	0	0
21.08.12 0:56	215	215	0	0	0	0	0
21.08.12 2:27	305	215	0	0	0	0	0
21.08.12 6:52	305	215	264	0	0	0	0
21.08.12 11:01	305	464	264	0	0	0	0
21.08.12 14:09	305	464	264	0	146	0	0
21.08.12 15:10	366	464	264	0	146	0	0
21.08.12 17:17	366	464	264	0	272	0	0
21.08.12 17:27	366	464	264	0	272	9	0
21.08.12 17:46	366	464	264	0	291	9	0
21.08.12 18:40	366	464	264	0	291	62	0
21.08.12 18:41	825	464	264	0	291	62	0
21.08.12 18:43	825	464	264	2	291	62	0
21.08.12 18:43	825	464	264	2	294	62	0
21.08.12 18:46	825	464	264	2	294	64	0
21.08.12 20:09	825	464	264	2	294	64	83
21.08.12 20:15	825	464	264	2	300	64	83
21.08.12 20:21	825	464	264	2	300	64	88
21.08.12 21:32	993	464	264	2	300	64	88
21.08.12 22:44	993	464	264	73	300	64	88
21.08.12 22:53	1002	464	264	73	300	64	88
21.08.12 23:02	1002	464	264	81	300	64	88
22.08.12 11:37	2354	464	264	81	300	64	88
22.08.12 11:44	2354	464	264	88	300	64	88
22.08.12 17:34	2703	464	264	88	300	64	88
22.08.12 17:52	2703	464	264	106	300	64	88
23.08.12 15:25	2703	464	264	106	300	2648	88
23.08.12 15:53	4023	464	264	106	300	2648	88
23.08.12 16:05	4023	464	264	106	340	2648	88
23.08.12 16:18	4023	464	264	131	340	2648	88
23.08.12 16:36	4041	464	264	131	340	2648	88
23.08.12 16:48	4041	464	264	142	340	2648	88
23.08.12 16:51	4044	464	264	142	340	2648	88
25.08.12 16:30	4044	464	264	3001	340	2648	88
25.08.12 21:22	4335	464	264	3001	340	2648	88
25.08.12 22:27	4335	464	264	3066	340	2648	88
25.08.12 22:37	4344	464	264	3066	340	2648	88
25.08.12 22:51	4344	464	264	3080	340	2648	88

ВРЕМЯ	BECHED AHACK.RU	EREEE	COPTERE	ANTICHAT	LETM	EI-GRAD	DARKBYTE
25.08.12 22:58	4350	464	264	3080	340	2648	88
25.08.12 23:12	4350	464	264	3093	340	2648	88
25.08.12 23:17	4354	464	264	3093	340	2648	88
25.08.12 23:38	4354	464	264	3114	340	2648	88
25.08.12 23:47	4363	464	264	3114	340	2648	88
25.08.12 23:51	4363	464	264	3117	340	2648	88
25.08.12 23:57	4369	464	264	3117	340	2648	88
26.08.12 0:04	4369	464	264	3124	340	2648	88
26.08.12 0:14	4378	464	264	3124	340	2648	88
26.08.12 0:30	4378	464	264	3140	340	2648	88
26.08.12 0:39	4386	464	264	3140	340	2648	88
26.08.12 0:58	4386	464	264	3158	340	2648	88
26.08.12 1:01	4389	464	264	3158	340	2648	88
26.08.12 1:09	4389	464	264	3166	340	2648	88
26.08.12 1:12	4391	464	264	3166	340	2648	88
26.08.12 1:16	4391	464	264	3169	340	2648	88
26.08.12 1:18	4393	464	264	3169	340	2648	88
26.08.12 1:37	4393	464	264	3187	340	2648	88
26.08.12 1:40	4395	464	264	3187	340	2648	88
26.08.12 1:57	4395	464	264	3203	340	2648	88
26.08.12 5:30	4607	464	264	3203	340	2648	88
26.08.12 9:09	4607	464	264	3421	340	2648	88
26.08.12 11:22	4740	464	264	3421	340	2648	88
26.08.12 13:21	4740	583	264	3421	340	2648	88
26.08.12 13:24	4740	583	264	3423	340	2648	88
26.08.12 13:39	4740	597	264	3423	340	2648	88
26.08.12 16:29	4740	597	264	3592	340	2648	88
26.08.12 19:06	4740	754	264	3592	340	2648	88
26.08.12 19:15	4748	754	264	3592	340	2648	88
26.08.12 19:38	4748	777	264	3592	340	2648	88
26.08.12 23:00	4748	777	264	3893	340	2648	88
26.08.12 23:17	4764	777	264	3893	340	2648	88
27.08.12 1:06	4764	777	264	4002	340	2648	88
28.08.12 1:27	4764	777	264	4002	340	2648	6410
28.08.12 16:19	7117	777	264	4002	340	2648	6410
28.08.12 16:41	7117	777	264	4024	340	2648	6410
28.08.12 16:44	7117	780	264	4024	340	2648	6410
28.08.12 21:43	8332	780	264	4024	340	2648	6410
28.08.12 21:46	8332	780	264	4026	340	2648	6410
29.08.12 14:33	8332	780	264	4026	340	2648	7417
29.08.12 14:35	8333	780	264	4026	340	2648	7417
31.08.12 9:58	8333	780	264	7940	340	2648	7417

ВРЕМЯ	BECHED AHACK.RU	EREEE	COPTERE	ANTICHAT	LETM	EI-GRAD	DARKBYTE
31.08.12 20:46	8980	780	264	7940	340	2648	7417
31.08.12 22:43	8980	897	264	7940	340	2648	7417
01.09.12 4:14	9310	897	264	7940	340	2648	7417
01.09.12 11:23	9310	897	264	8368	340	2648	7417
02.09.12 13:22	9310	2456	264	8368	340	2648	7417
02.09.12 17:46	9574	2456	264	8368	340	2648	7417
02.09.12 21:27	9574	2676	264	8368	340	2648	7417
03.09.12 11:11	9574	2676	264	9191	340	2648	14412

Примечание. Желтый цвет — текущее I место, зеленый — текущее II место, синий — текущее III место. Рамкой обведена ячейка таблицы, соответствующая моменту начисления баллов за контроль сервиса второго уровня.

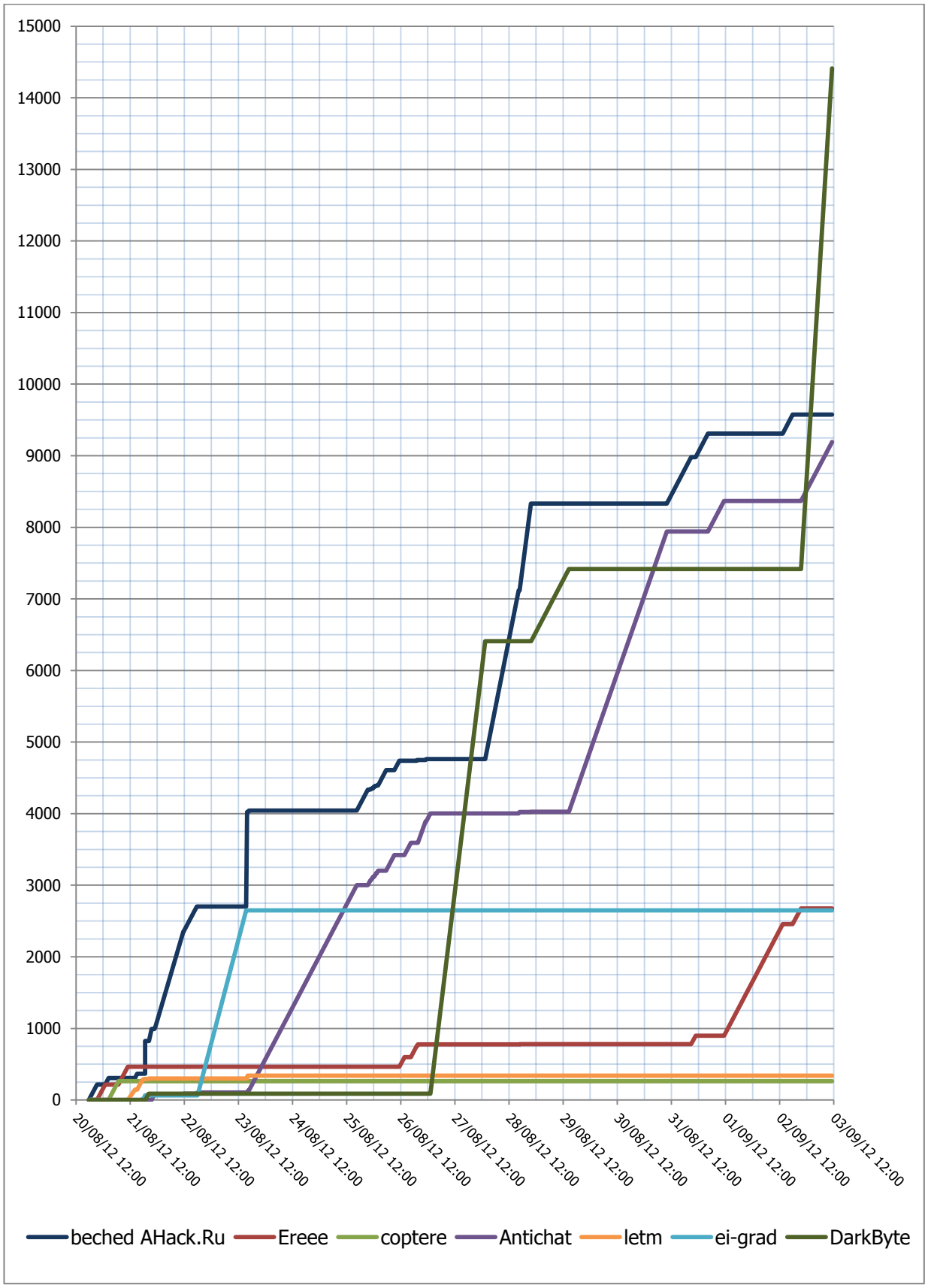


Рисунок 26. Хронология начисления баллов в рамках онлайн-соревнований «Царь горы»

Больше всех баллов в рамках соревнований «Царь горы» набрал участник под псевдонимом DarckByte, но ему не удалось стать победителем. Единственный участник, которому удалось набрать баллы за контроль сервисов второго уровня, заработал в итоге меньше баллов, но занял первое место. Никто из его соперников не смог получить контроль над сервисом Active Directory.

Согласно полученным данным, участники из Интернета лучше справились с заданием, чем команды во время проведения CTF. Данный факт обусловлен тем, что команды CTF находились в более жестких временных рамках и тратили ресурсы на решение других видов заданий на всем протяжении соревнований.

Результаты онлайн-соревнований (сервис 1-го уровня «WWW»)

Только 4 участника из 7 справились с заданиями 1-го уровня «WWW» в рамках онлайн-соревнований «Царь горы». Лидером в данном зачете стал участник под псевдонимом Antichat.

Результаты представлены на рис. 27, хронология событий представлена на рис. 28.

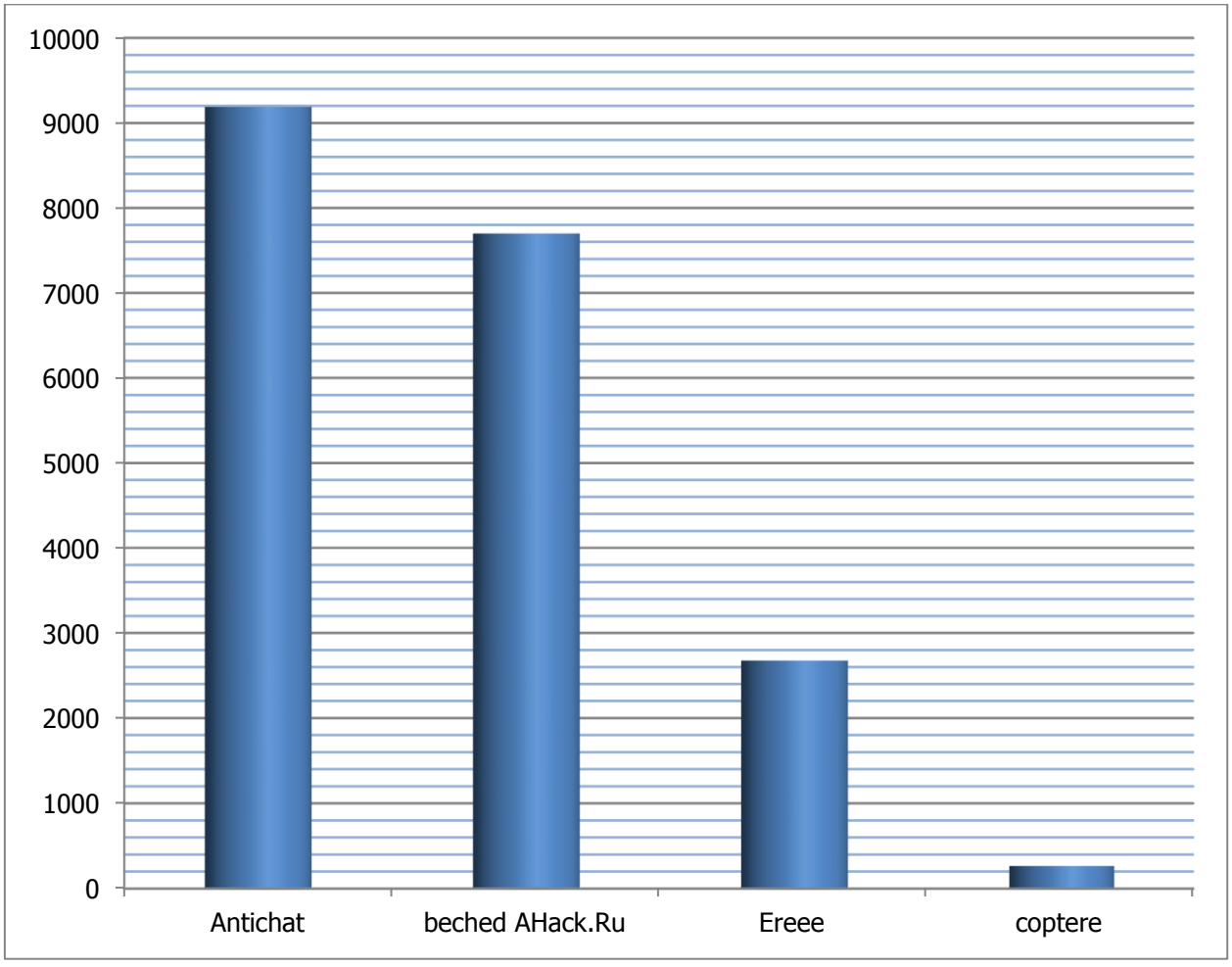


Рисунок 27. Результаты онлайн-соревнований «Царь горы» (сервис 1-го уровня «WWW»)

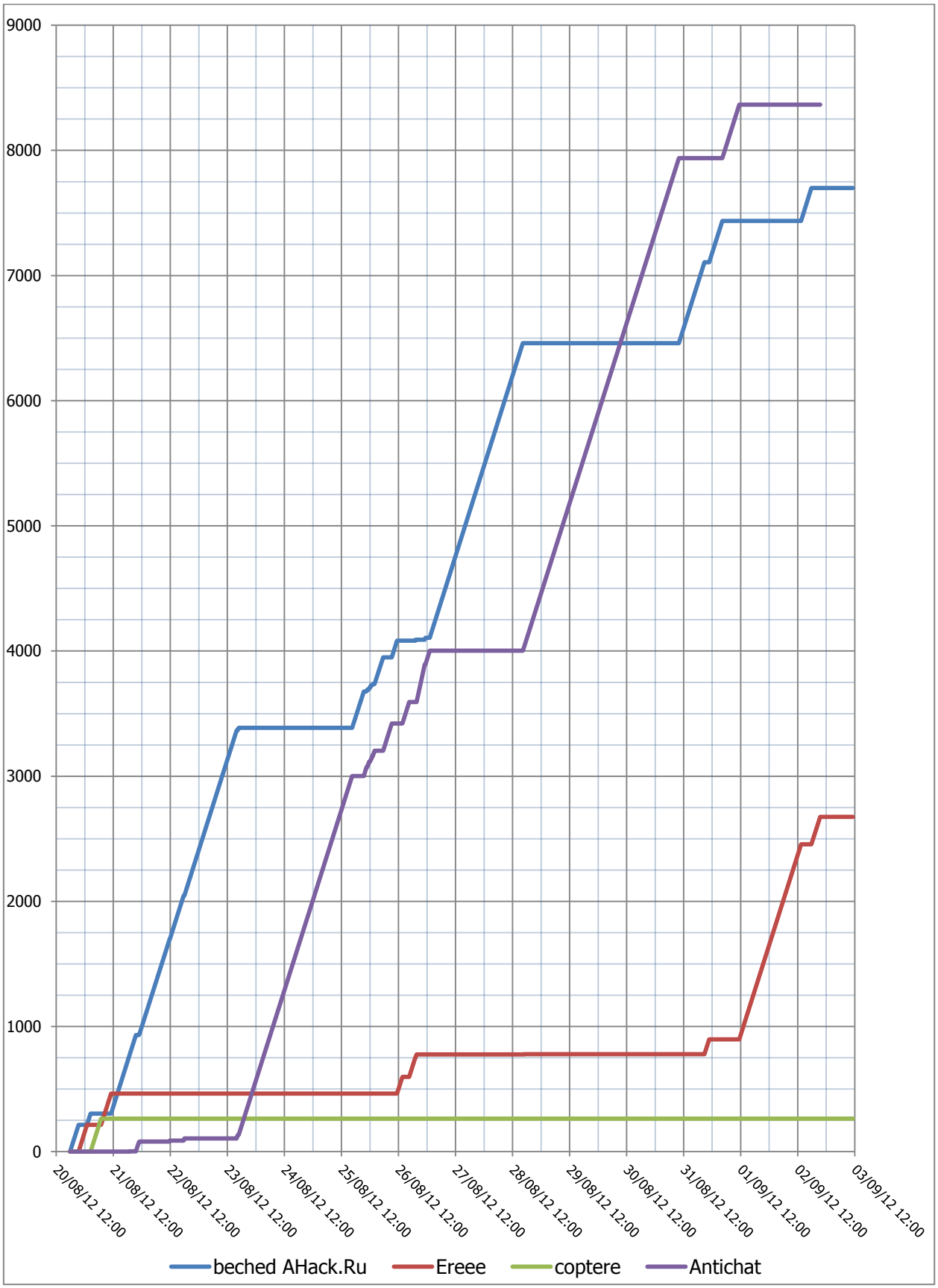


Рисунок 28. Хронология начисления баллов за контроль сервиса 1-го уровня «WWW»

Результаты онлайн-соревнований (сервис 1-го уровня «Services»)

Только 5 участников из 7 справились с заданиями 1-го уровня «Services» в рамках онлайн-соревнований «Царь горы». С большим отрывом I место в данной категории занял участник под псевдонимом DarkByte. Потеряв контроль над сервисом, он сумел вернуть его и сохранить до завершения соревнований.

Результаты приводятся на рис. 29, хронология представлена на рис. 30.

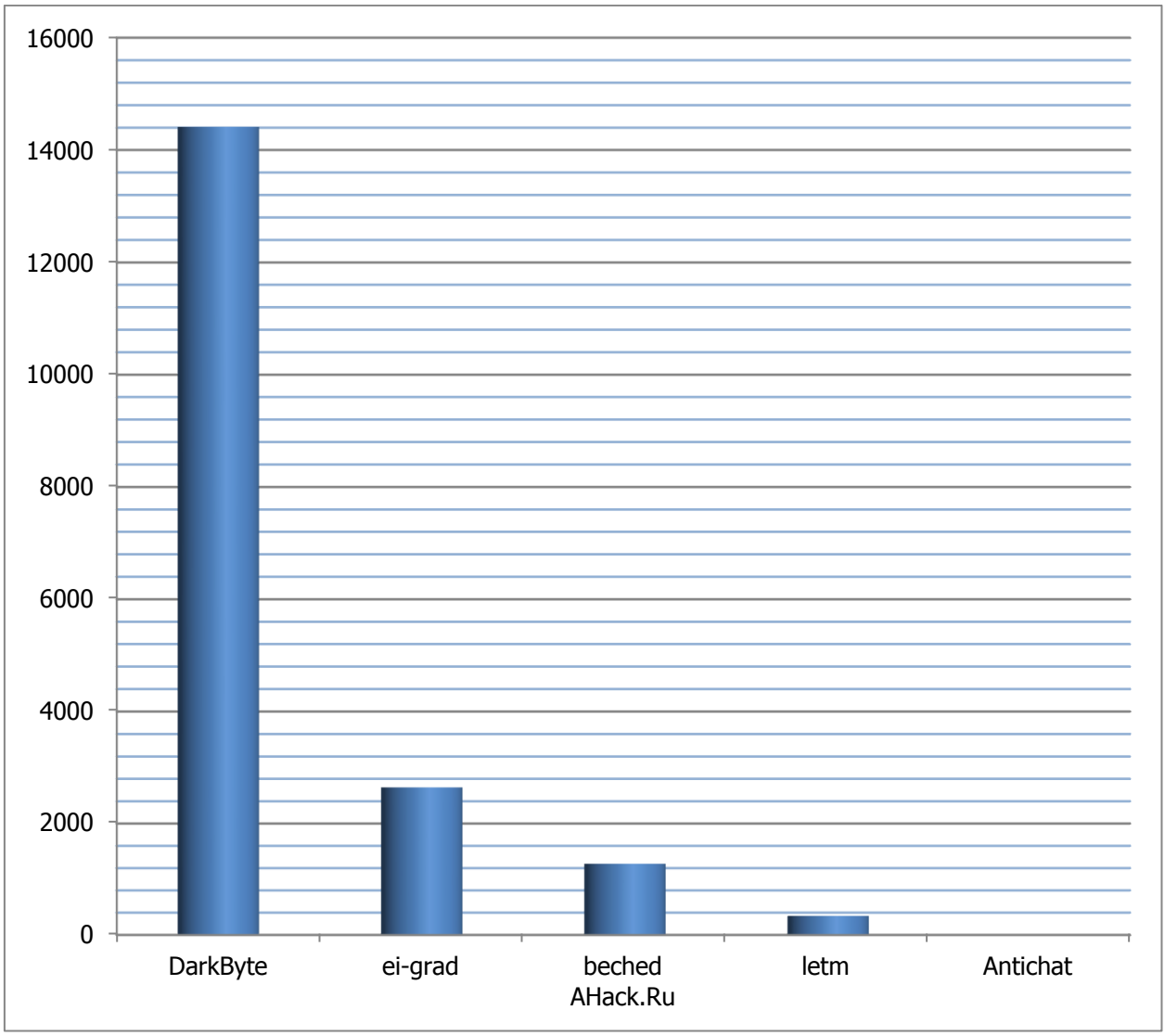


Рисунок 29. Результаты онлайн-соревнований «Царь горы» (сервис 1-го уровня «Services»)

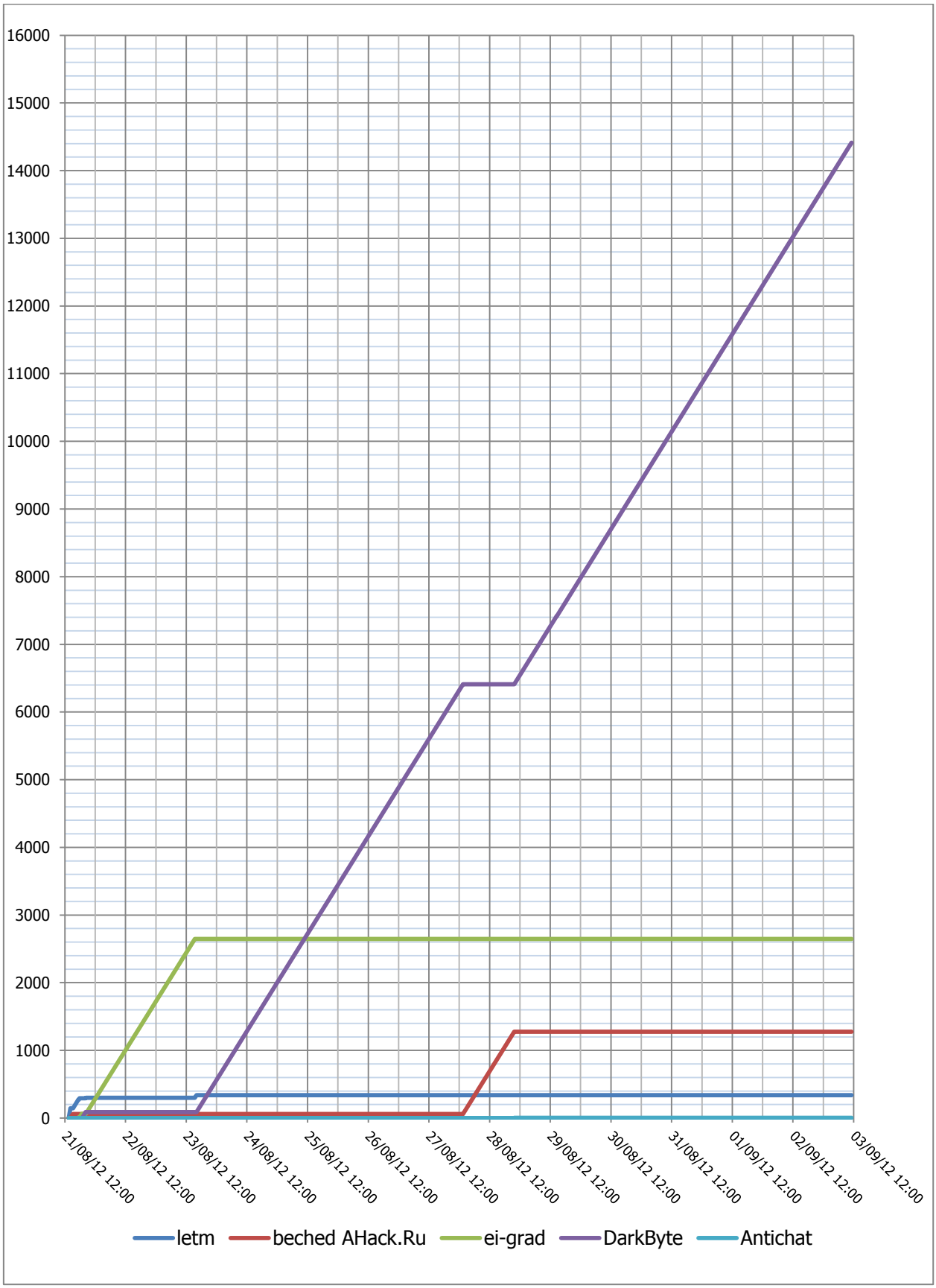
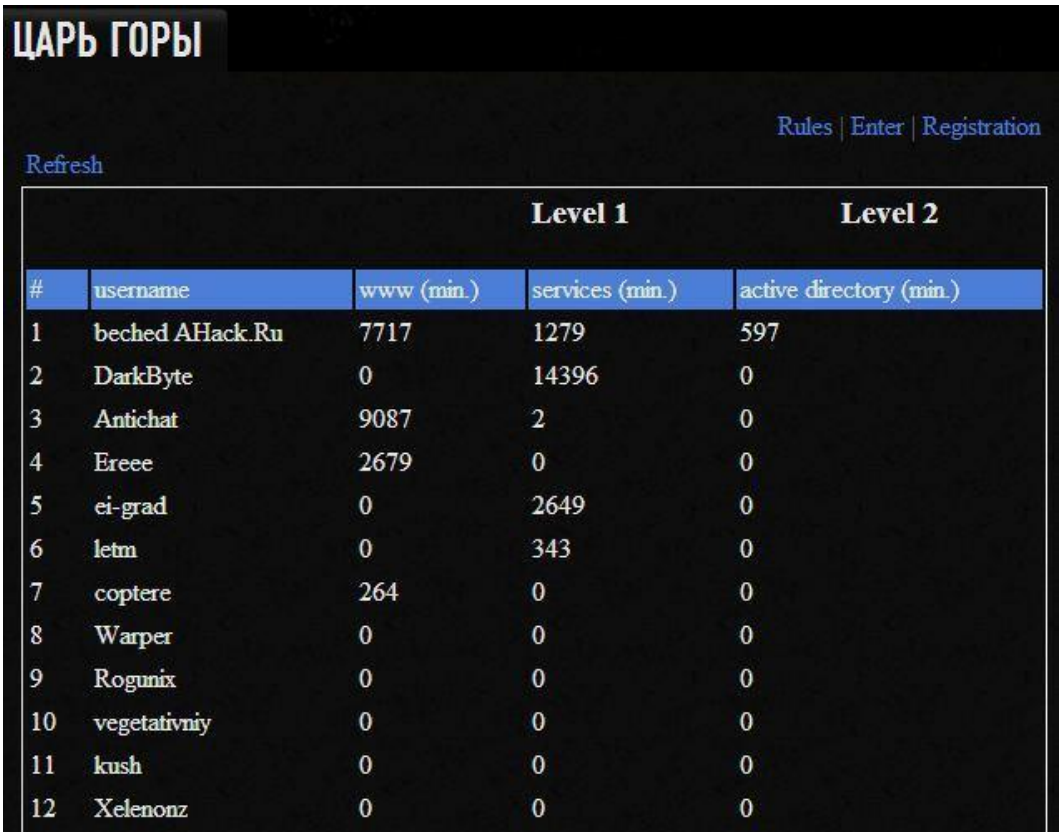


Рисунок 30. Хронология начисления баллов за контроль сервиса 1-го уровня «Services»

Результаты онлайн-соревнований (сервис 2-го уровня «Active Directory»)

В отличие от команд CTF, одному из интернет-пользователей удалось получить контроль над сервисом 2-го уровня. Участник под псевдонимом beched AHack.Ru контролировал сервис 2-го уровня почти 10 часов, заработав 597 баллов. Никто из его соперников не смог достичь подобного успеха. Основная борьба велась в рамках сервисов 1-го уровня инфраструктуры «Царь горы».

Баллы, заработанные beched AHack.Ru за контроль сервиса Active Directory, позволили участнику выйти на I место в общем зачете и одержать победу в онлайн-соревновании.



ЦАРЬ ГОРЫ

Rules | Enter | Registration

Refresh

		Level 1		Level 2
#	username	www (min.)	services (min.)	active directory (min.)
1	beched AHack.Ru	7717	1279	597
2	DarkByte	0	14396	0
3	Antichat	9087	2	0
4	Ereee	2679	0	0
5	ei-grad	0	2649	0
6	letm	0	343	0
7	coptere	264	0	0
8	Warper	0	0	0
9	Rogunix	0	0	0
10	vegetativniy	0	0	0
11	kush	0	0	0
12	Xelenonz	0	0	0

Фотография 10. Результаты онлайн-соревнований «Царь горы» на официальном сайте PHDays 2012

Полная таблица результатов онлайн-соревнований «Царь горы» представлена на официальном сайте PHDays 2012 (http://phdays.ru/ctf/king/a.php).

6.4. Распределение баллов в рамках бонусных заданий

Победителями бонусного конкурса по перехвату управления устройством AR.Drone стали Сергей Азовсков из команды HackerDom и Мэтт Дикоф из PPP. Команды получили по 150 баллов в зачет соревнований, а победители забрали с собой по призовому квадракоптеру AR.Drone.

Фотография 11. Мэтт Дикоф из команды PPP — победитель бонусного конкурса по перехвату управления AR.Drone

В течение двух дней соревнований команды зарабатывали бонусные баллы, копаясь в контейнере с бумажным мусором в поисках необходимой информации и захватывая флаги командных сервисов соперников в ночное время.

Распределение бонусных баллов среди команд участников представлено на рис. 31 и в табл. 10. Больше всех бонусных баллов заработали команды PPP, HackerDom и Int3pids. При этом участники команды Int3pids набрали более 200 баллов, собирая только бонусные флаги и не сумев одержать победу в конкурсе по захвату управления устройством AR.Drone.

Фотография 12. Участники команды HackerDom в контейнере с бумажным мусором

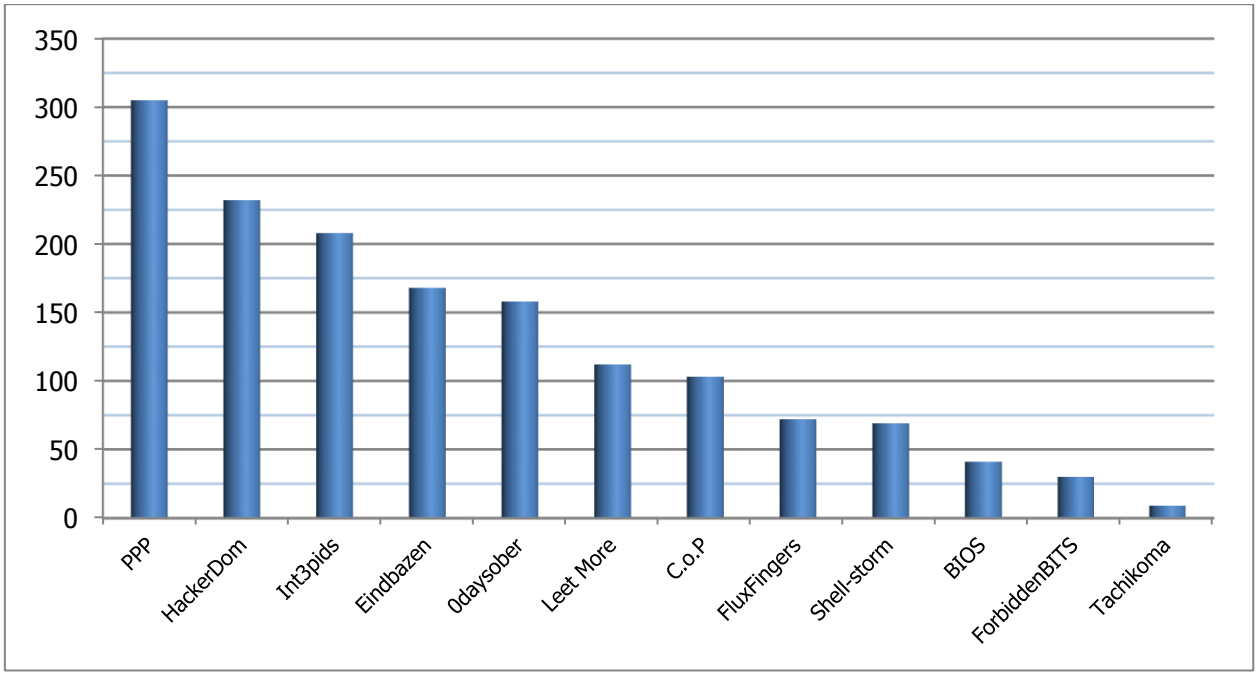


Рисунок 31. Распределение бонусных баллов среди команд

Таблица 10. Распределение бонусных баллов среди команд

Команда	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Бонусные задания	46	14	0	62	9	15	45	7	22	55	18	8
ARDrone	0	0	0	0	0	0	150	0	0	150	0	0
Ночные флаги	112	27	103	106	63	15	37	201	90	100	51	1

6.5. Общая статистика и результаты CTF

6.5.1. Хронология начисления баллов по всем заданиям

Хронология начисления баллов по всем видам заданий на протяжении всего PHDays CTF 2012 представлена в табл. 11 и на рис. 32—34. Данная статистика отражает заработанные командами баллы (не учитывается количество штрафных баллов).

Согласно табл. 11, в общей для всех видов заданий статистике выделяются четыре команды-лидера, три из которых борются за более высокое положение в первой тройке до последних минут соревнований. Наиболее близко к лидерам оказались команды 0daysober и Eindbazen. Аутсайдером соревнований на протяжении всего времени проведения CTF является команда BIOS. Итоговый результат команды практически в 10 раз ниже, чем результаты команд из лидирующей тройки.

По статистике, команда EInt3pids, лидирующая по набранным баллам в конце первого игрового дня, сохранила лидерство на утро второго дня по результатам ночи, но во второй день CTF положение сил в первой тройке изменилось, и участники Int3pids заняли лишь второе место по заработанным баллам.

Команда Eindbazen, поднявшаяся на третью строчку рейтинга на утро второго дня, в итоге уступила место лидерам.

Фотография 13. Участники команды Int3pids на церемонии награждения

Таблица 11. Хронология начисления баллов по всем заданиям на протяжении CTF

Временной интервал	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	110	0	0
10:00 - 10:30	80	0	60	90	50	0	90	10	110	110	50	0
10:30 - 11:00	90	0	100	90	50	50	90	40	110	190	70	0
11:00 - 11:30	160	0	100	90	50	50	90	40	110	190	70	0
11:30 - 12:00	160	0	170	97	50	50	90	40	180	190	70	0
12:00 - 12:30	160	0	170	97	57	50	90	40	180	190	70	0
12:30 - 13:00	170	0	170	167	137	50	130	40	208	190	100	0
13:00 - 13:30	170	0	170	167	147	50	130	47	298	230	100	0
13:30 - 14:00	170	0	190	207	147	57	170	87	308	240	100	0
14:00 - 14:30	170	7	190	207	147	57	193	147	308	240	100	0
14:30 - 15:00	184	7	190	227	167	57	213	147	368	260	100	10
15:00 - 15:30	184	7	210	227	167	77	213	147	448	310	120	10
15:30 - 16:00	204	27	210	317	237	77	213	167	448	370	120	27
16:00 - 16:30	264	67	210	317	237	77	263	167	469	410	120	27
16:30 - 17:00	304	67	210	387	237	127	263	227	469	510	180	27
17:00 - 17:30	388	67	210	387	297	127	263	317	469	510	180	27
17:30 - 18:00	388	67	210	387	297	127	263	317	469	510	180	27
18:00 - 18:30	388	67	270	427	357	127	263	377	469	510	180	47
18:30 - 19:00	388	67	270	447	357	127	263	377	469	510	180	117
19:00 - 19:30	388	67	270	487	357	127	263	417	469	510	180	117
19:30 - 20:00	388	67	270	487	357	127	263	417	469	510	200	117
20:00 - 20:30	388	67	310	527	357	127	263	417	469	510	200	117
20:30 - 21:00	388	67	310	527	377	147	263	417	469	510	200	117
21:00 - 21:30	391	67	310	527	377	147	283	417	469	510	200	117
21:30 - 22:00	391	67	310	527	377	147	283	417	564	510	243	117
22:00 - 22:30	400	67	310	527	377	147	283	557	584	510	243	117
22:30 - 23:00	400	67	310	527	377	147	283	617	584	590	243	117
23:00 - 23:30	400	67	310	527	397	147	323	617	584	590	243	117
23:30 - 00:00	420	67	350	527	397	147	323	637	584	590	243	117
Ночь												
0:00 - 0:30	420	67	350	527	397	147	323	637	584	610	263	117
0:30 - 1:00	423	67	363	527	397	147	323	637	584	610	283	117
1:00 - 1:30	447	67	374	527	397	147	323	637	584	610	285	117
1:30 - 2:00	447	67	438	536	397	147	332	638	585	610	289	117
2:00 - 2:30	465	67	490	558	409	147	347	652	647	620	294	117
2:30 - 3:00	473	67	501	570	420	147	358	671	655	632	294	117
3:00 - 3:30	483	67	512	584	435	147	359	694	687	646	310	117
3:30 - 4:00	496	73	528	633	444	147	359	712	698	658	321	117
4:00 - 4:30	505	79	540	662	450	147	359	733	707	687	330	117
4:30 - 5:00	511	83	567	730	456	147	361	753	713	694	333	117
5:00 - 5:30	516	88	572	735	460	148	401	772	718	700	333	117
5:30 - 6:00	529	88	572	740	460	153	401	794	724	708	333	117
6:00 -6:30	540	90	572	750	460	158	401	815	730	719	334	117
6:30 - 7:00	549	93	572	756	460	161	401	832	733	728	334	117
7:00 -7:30	552	94	572	758	460	162	411	838	734	730	334	117
7:30 - 8:00	552	94	572	758	460	162	411	838	734	730	334	117
8:00 - 8:30	552	94	572	758	460	162	451	838	734	730	334	117
8:30 - 8:45	552	94	572	758	460	162	451	838	734	770	334	117
2 день 31.05.2012												
8:45 - 9:30	572	94	572	758	480	172	611	838	744	930	334	117
9:30 - 10:00	572	94	592	758	550	192	621	848	864	930	334	117
10:00 - 10:30	642	94	592	888	560	322	701	898	864	930	334	117
10:30 - 11:00	662	124	592	888	560	322	711	948	884	970	374	127
11:00 - 11:30	722	124	592	888	560	322	731	948	884	1040	374	187
11:30 - 12:00	722	124	602	888	560	322	741	978	934	1040	381	207
12:00 - 12:30	750	124	602	888	560	322	741	978	934	1080	398	217
12:30 - 13:00	751	124	623	908	560	322	742	978	1265	1081	408	218
13:00 - 13:30	751	131	623	908	560	322	742	978	1285	1081	409	218
13:30 - 14:00	751	131	623	908	560	330	742	988	1305	1081	409	238
14:00 - 14:30	781	131	623	908	560	390	752	1028	1335	1081	409	238
14:30 - 15:00	781	131	623	908	620	390	762	1048	1335	1101	409	258
15:00 - 15:30	791	131	653	950	630	390	782	1058	1365	1131	429	278
15:30 - 16:00	791	131	653	950	632	390	782	1078	1365	1131	429	358
16:00 - 16:30	831	131	653	950	632	390	782	1078	1365	1145	429	398
16:30 - 17:00	831	131	693	957	632	390	782	1128	1415	1215	429	428
17:00 - 17:30	851	131	703	957	632	390	832	1148	1415	1225	429	438
17:30 - 18:00	861	131	783	957	632	390	842	1148	1415	1225	439	438
18:00 - 18:30	961	131	783	957	632	420	842	1248	1415	1225	439	459
18:30 - 19:00	961	131	803	958	632	420	842	1248	1415	1225	439	459

Примечание. Желтый цвет — текущее I место, зеленый — текущее второй II место, синий — текущее III место.

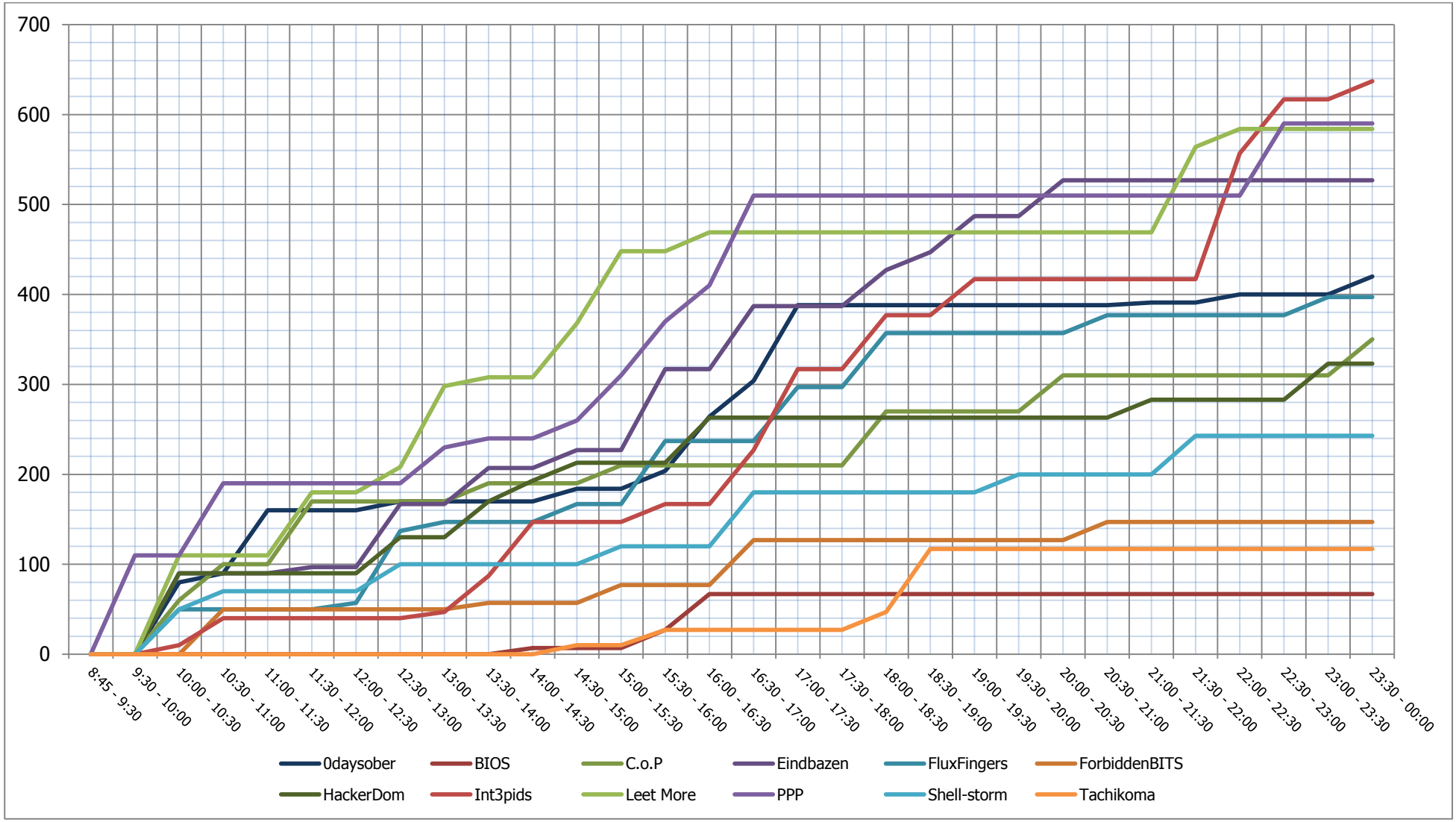


Рисунок 32/ Хронология начисления баллов по всем заданиям на протяжении первого дня CTF

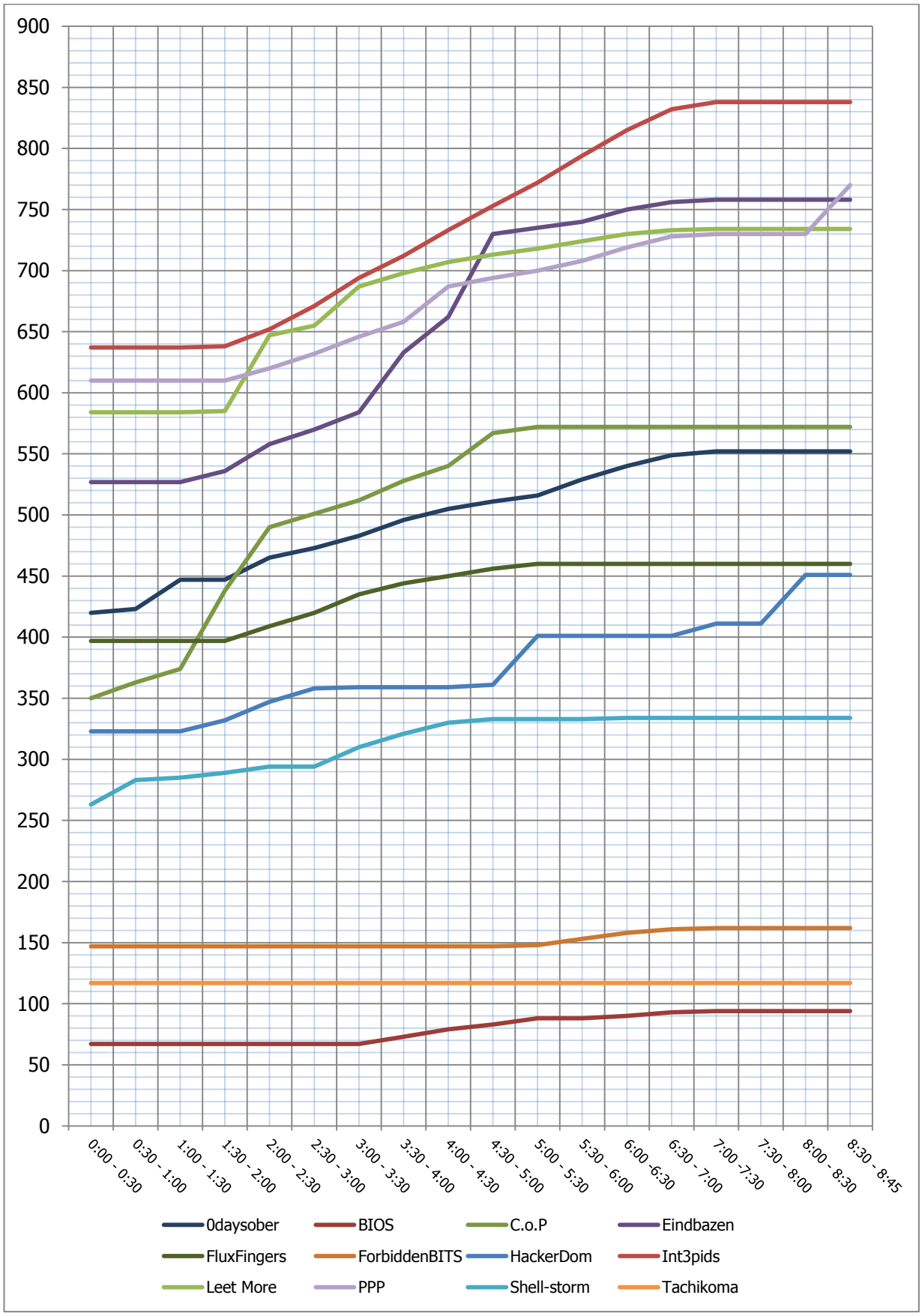


Рисунок 33/ Хронология начисления баллов по всем заданиям CTF на протяжении ночи

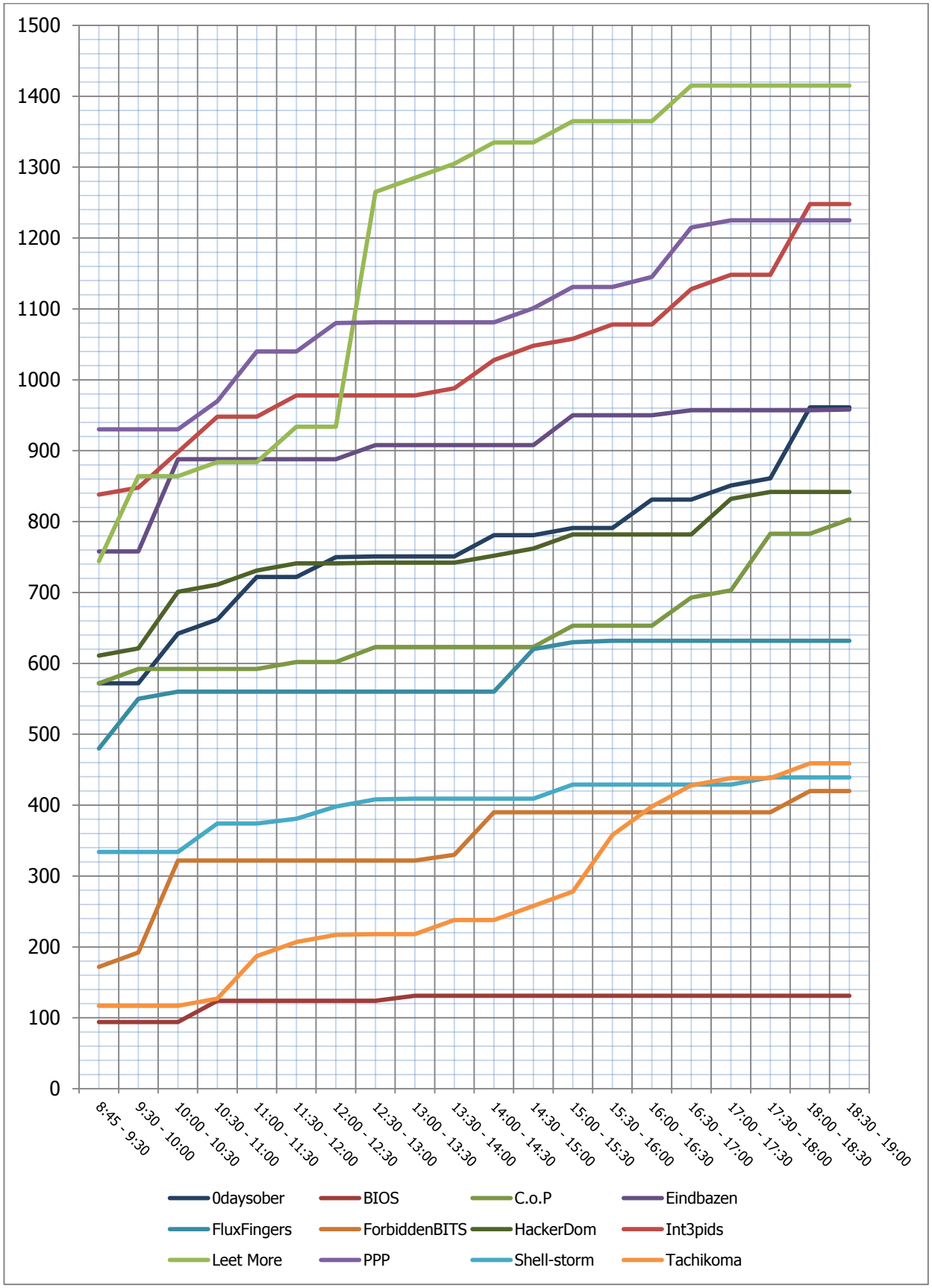


Рисунок 34. Хронология начисления баллов по всем заданиям на протяжении второго дня CTF

6.5.2. Динамика начисления баллов по всем заданиям

Динамика начисления баллов по всем видам заданий на протяжении всего PHDays CTF 2012 представлена в табл. 12 и на рис. 35—37.

Согласно табл. 12, на протяжении всего времени проведения CTF активность проявляли не только лидеры соревнований, но и отстающие команды. Каждый получасовой отрезок времени менялся лидер по набранным за это время баллам, в то время как в общем зачете список команд первой тройки изменялся не столь часто. Данный факт свидетельствует о том, что все команды, на каком бы месте они ни находились в рейтинге, не прекращали борьбу.

Наибольшая активность команд наблюдается в первой половине первого дня соревнований и во второй день. Вопреки ожиданиям организаторов, команды достаточно быстро изучили специфику заданий и правила соревнований, о чем свидетельствует динамика начисления баллов, отраженная на рис. 35.

Активность команд в ночное время заметно ниже, но многие участники продолжали игру, несмотря на усталость. Однако команда Tachikoma, к примеру, не набрали за ночь ни одного балла.

Рейтинг команд к началу второго дня CTF стал доступен командам только утром, в ночное время участники не знали, как изменяется их позиция в рейтинге. Возможно, именно поэтому активность команд во второй день оказалась сравнима с активностью, проявленной в первый день: позиции в первой тройке лидеров изменились.

Согласно табл. 12, большинство команд заработало максимальное количество баллов за один получасовой интервал во второй день соревнований. Данный факт показывает насколько упорная шла борьба — среди всех участников CTF, а не только в тройке лидеров.

Примечание: поскольку система оценки действий участников CTF построена на применении флагов, полученная статистика может не отражать точное время решения задач командами, а свидетельствует лишь о времени, когда участники ввели флаг в систему. Поэтому активность команд на протяжении соревнований можно оценивать только относительно, с учетом данного факта.

Наибольшее количество баллов за один получасовой интервал удалось набрать команде Leet Moore (331 балл). Существенный вклад в этот успех внесли баллы, начисленные команде за удержание контроля сервиса в рамках инфраструктуры «Царь горы»: участникам из Leet More удалось удерживать контроль над сервисом на протяжении более чем четырнадцати часов.

Таблица 12. Динамика начисления баллов по всем заданиям на протяжении CTF

Временной интервал	Команда											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
1 день 30.05.2012												
8:45 - 9:30	0	0	0	0	0	0	0	0	0	0	0	0
9:30 - 10:00	0	0	0	0	0	0	0	0	0	110	0	0
10:00 - 10:30	80	0	60	90	50	0	90	10	110	0	50	0
10:30 - 11:00	10	0	40	0	0	50	0	30	0	80	20	0
11:00 - 11:30	70	0	0	0	0	0	0	0	0	0	0	0
11:30 - 12:00	0	0	70	7	0	0	0	0	70	0	0	0
12:00 - 12:30	0	0	0	0	7	0	0	0	0	0	0	0
12:30 - 13:00	10	0	0	70	**80**	0	40	0	28	0	30	0
13:00 - 13:30	0	0	0	0	10	0	0	7	90	40	0	0
13:30 - 14:00	0	0	20	40	0	7	40	40	10	10	0	0
14:00 - 14:30	0	7	0	0	0	0	23	60	0	0	0	0
14:30 - 15:00	14	0	0	20	20	0	20	0	60	20	0	10
15:00 - 15:30	0	0	20	0	0	20	0	0	80	50	20	0
15:30 - 16:00	20	20	0	90	70	0	0	20	0	60	0	17
16:00 - 16:30	60	**40**	0	0	0	0	50	0	21	40	0	0
16:30 - 17:00	40	0	0	70	0	50	0	60	0	100	**60**	0
17:00 - 17:30	84	0	0	0	60	0	0	90	0	0	0	0
17:30 - 18:00	0	0	0	0	0	0	0	0	0	0	0	0
18:00 - 18:30	0	0	60	40	60	0	0	60	0	0	0	20
18:30 - 19:00	0	0	0	20	0	0	0	0	0	0	0	70
19:00 - 19:30	0	0	0	40	0	0	0	40	0	0	0	0
19:30 - 20:00	0	0	0	0	0	0	0	0	0	0	20	0
20:00 - 20:30	0	0	40	40	0	0	0	0	0	0	0	0
20:30 - 21:00	0	0	0	0	20	20	0	0	0	0	0	0
21:00 - 21:30	3	0	0	0	0	0	20	0	0	0	0	0
21:30 - 22:00	0	0	0	0	0	0	0	0	95	0	43	0
22:00 - 22:30	9	0	0	0	0	0	0	140	20	0	0	0
22:30 - 23:00	0	0	0	0	0	0	0	60	0	80	0	0
23:00 - 23:30	0	0	0	0	20	0	40	0	0	0	0	0
23:30 - 00:00	20	0	40	0	0	0	0	20	0	0	0	0
Ночь												
0:00 - 0:30	0	0	0	0	0	0	0	0	0	20	20	0
0:30 - 1:00	3	0	13	0	0	0	0	0	0	0	20	0
1:00 - 1:30	24	0	11	0	0	0	0	0	0	0	2	0
1:30 - 2:00	0	0	64	9	0	0	9	1	1	0	4	0
2:00 - 2:30	18	0	52	22	12	0	15	14	62	10	5	0
2:30 - 3:00	8	0	11	12	11	0	11	19	8	12	0	0
3:00 - 3:30	10	0	11	14	15	0	1	23	32	14	16	0
3:30 - 4:00	13	6	16	49	9	0	0	18	11	12	11	0
4:00 - 4:30	9	6	12	29	6	0	0	21	9	29	9	0
4:30 - 5:00	6	4	27	68	6	0	2	20	6	7	3	0
5:00 - 5:30	5	5	5	5	4	1	40	19	5	6	0	0
5:30 - 6:00	13	0	0	5	0	5	0	22	6	8	0	0
6:00 -6:30	11	2	0	10	0	5	0	21	6	11	1	0
6:30 - 7:00	9	3	0	6	0	3	0	17	3	9	0	0
7:00 -7:30	3	1	0	2	0	1	10	6	1	2	0	0
7:30 - 8:00	0	0	0	0	0	0	0	0	0	0	0	0
8:00 - 8:30	0	0	0	0	0	0	40	0	0	0	0	0
8:30 - 8:45	0	0	0	0	0	0	0	0	0	40	0	0
2 день 31.05.2012												
8:45 - 9:30	20	0	0	0	20	10	**160**	0	10	**160**	0	0
9:30 - 10:00	0	0	20	0	70	20	10	10	120	0	0	0
10:00 - 10:30	70	0	0	**130**	10	**130**	80	50	0	0	0	0
10:30 - 11:00	20	30	0	0	0	0	10	50	20	40	40	10
11:00 - 11:30	60	0	0	0	0	0	20	0	0	70	0	60
11:30 - 12:00	0	0	10	0	0	0	10	30	50	0	7	20
12:00 - 12:30	28	0	0	0	0	0	0	0	0	40	17	10
12:30 - 13:00	1	0	21	20	0	0	1	0	**331**	1	10	1
13:00 - 13:30	0	7	0	0	0	0	0	0	20	0	1	0
13:30 - 14:00	0	0	0	0	0	8	0	10	20	0	0	20
14:00 - 14:30	30	0	0	0	0	60	10	40	30	0	0	0
14:30 - 15:00	0	0	0	0	60	0	10	20	0	20	0	20
15:00 - 15:30	10	0	30	42	10	0	20	10	30	30	20	20
15:30 - 16:00	0	0	0	0	2	0	0	20	0	0	0	**80**
16:00 - 16:30	40	0	0	0	0	0	0	0	0	14	0	40
16:30 - 17:00	0	0	40	7	0	0	0	50	50	70	0	30
17:00 - 17:30	20	0	10	0	0	0	50	20	0	10	0	10
17:30 - 18:00	10	0	**80**	0	0	0	10	0	0	0	10	0
18:00 - 18:30	**100**	0	0	0	0	30	0	**100**	0	0	0	21
18:30 - 19:00	0	0	20	1	0	0	0	0	0	0	0	0

Примечание. Желтый цвет — максимальное количество заработанных баллов за текущий получасовой интервал, зеленый — II место по заработанным баллам за текущие полчаса, синий — III место. Подчеркнуты максимальные баллы, полученные командами за все получасовые интервалы.

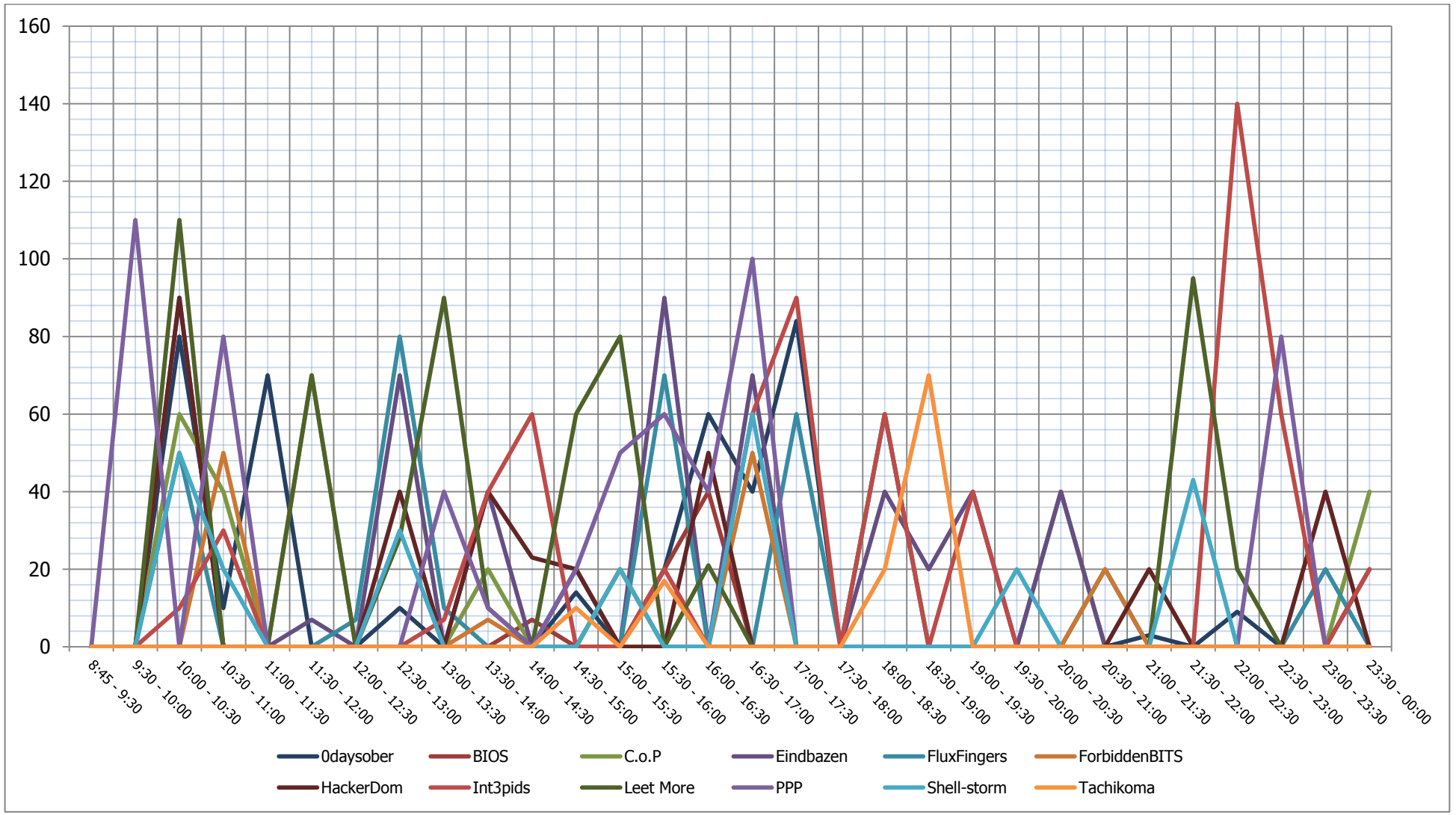


Рисунок 35. Динамика начисления баллов по всем заданиям на протяжении первого дня CTF

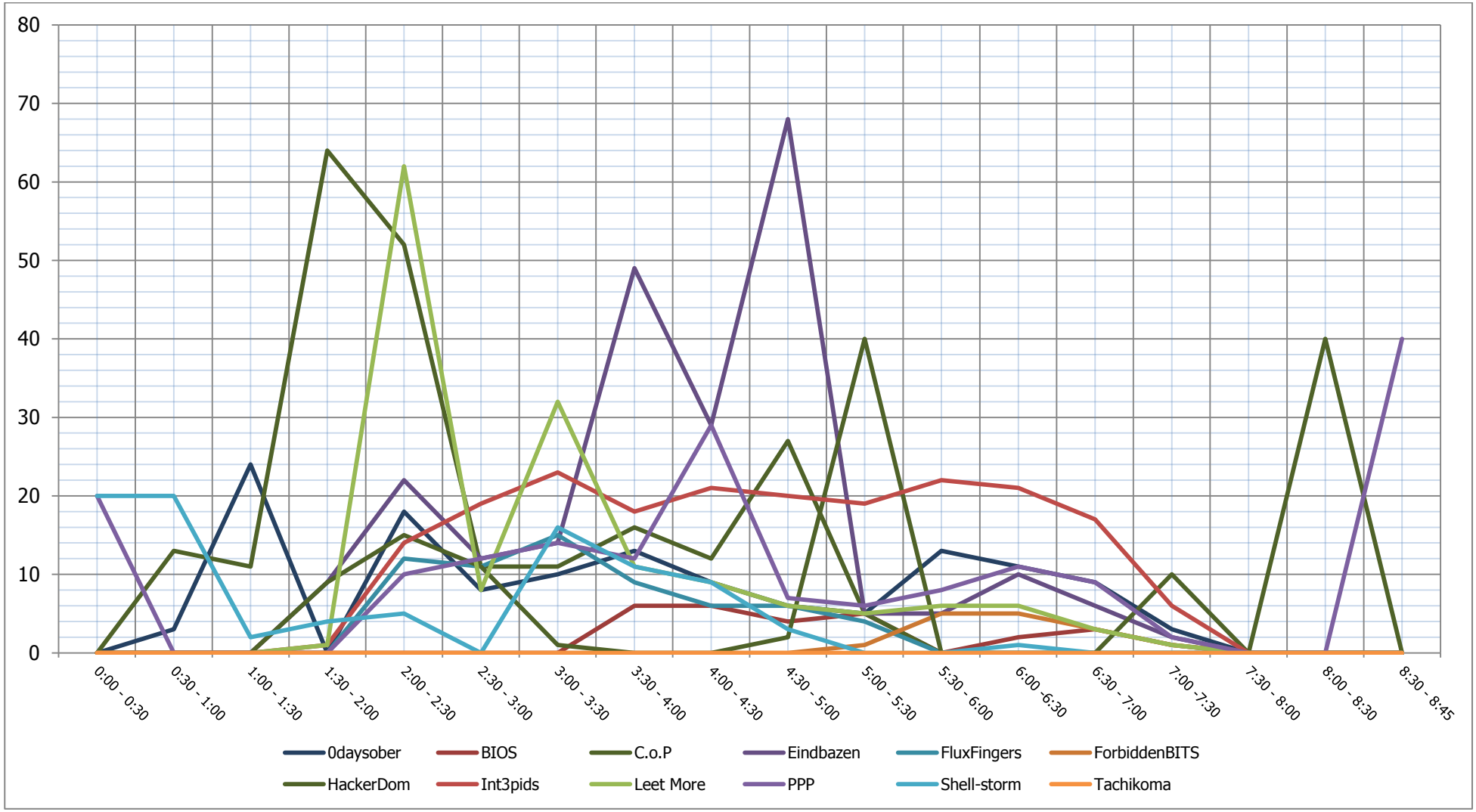


Рисунок 36. Динамика начисления баллов по всем заданиям в ночное время

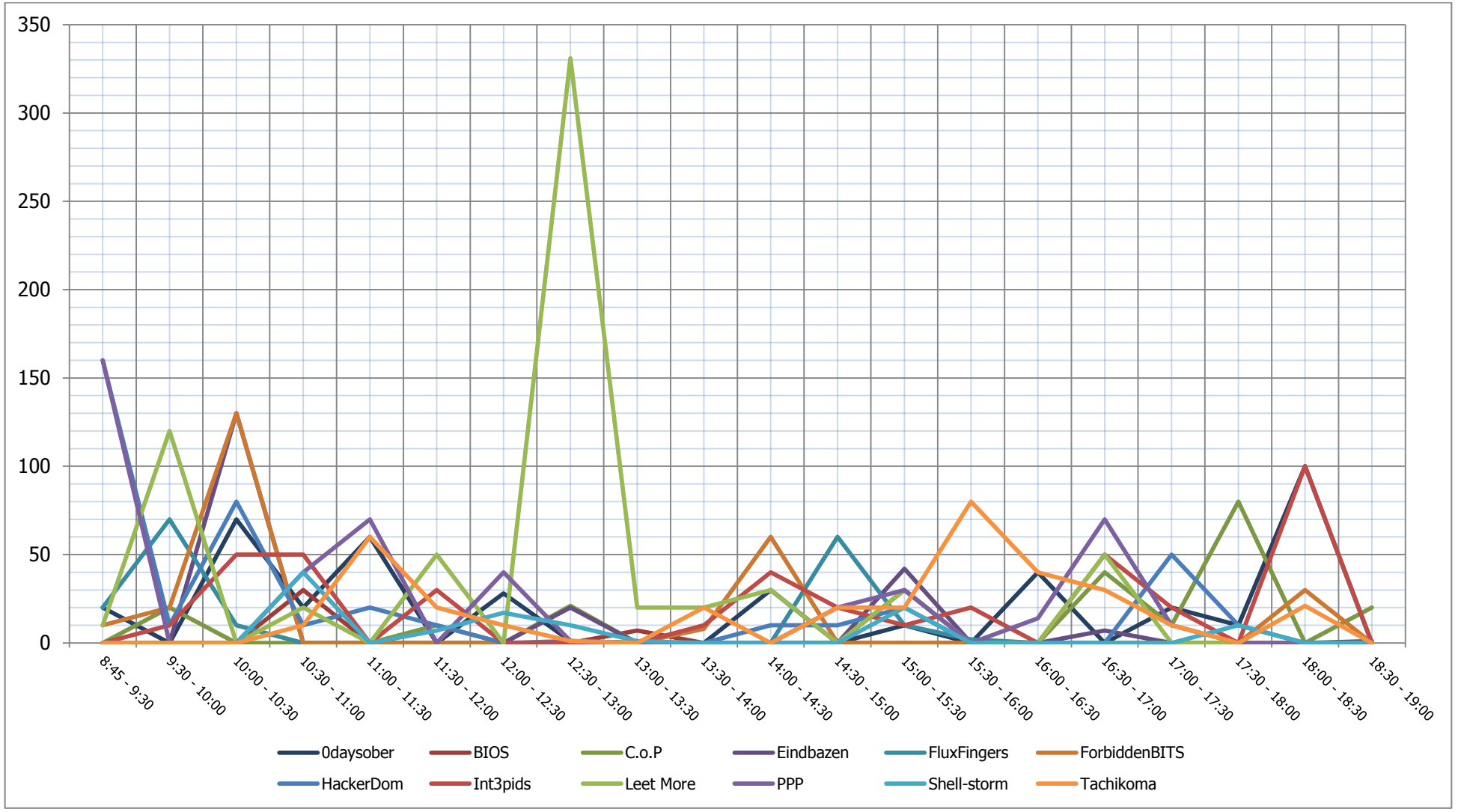


Рисунок 37. Динамика начисления баллов по всем заданиям на протяжении второго дня CTF

6.5.3. Итоговые результаты CTF

Заработанные командами по итогам CTF баллы представлены в табл. 13 и на рис. 38. На рис. 39 представлено соответствие заработанных командами баллов в различных видах заданий суммарному количеству заработанных баллов по итогам соревнований.

Диаграммы на рис. 39 показывают, что для победы в CTF недостаточно решать задачи только одного или двух видов: необходимо набирать баллы во всех игровых инфраструктурах. Те команды, которым удалось распределить время и ресурсы, выбрать грамотную стратегию игры, — заняли первые строчки рейтинговой таблицы.

Командам Leet More, Int3pids и 0daysober удалось набрать существенное количество баллов в рамках каждой из инфраструктур, а также в бонусных заданиях. Участникам из команды PPP удалось набрать достаточное количество баллов, чтобы войти в первую тройку по заработанным баллам, не решив ни одного задания инфраструктуры «Царь горы». Возможно, именно этот факт не позволил команде из США занять I место в итоговом рейтинге и повторить результат 2011 года. Именно баллы, заработанные за счет удержания сервисов инфраструктуры «Царь горы», вывели команду Leet More на вершину рейтинга.

Фотография 14. Победители CTF 2012 — команда Leet More

Фотография 15. Команда 0daysober, занявшее II место в CTF 2012

Фотография 16. Команда Int3pids, занявшее III место в CTF 2012

По результатам CTF можно выделить всего одну команду, ставшую явным аутсайдером, — BIOS. Участникам из Индии удалось набрать баллы как в заданиях общей инфраструктуры, бонусных заданиях, так и при захвате флагов с сервисов соперников, однако набранных баллов, к сожалению, оказалось недостаточно, чтобы догнать конкурентов.

Доля баллов, заработанных каждой командой за выполнение отдельных видов заданий, представлена на рис. 40 в соотношении с общим количеством полученных баллов.

По окончании PHDays CTF 2012 состоялось выступление группы «Ундервуд».

Фотография 17. Группа «Ундервуд» закрывает PHDays 2012

Таблица 13. Баллы, заработанные командами по итогам CTF

Виды заданий	Команды											
	Leet More	**Int3pids**	**PPP**	**0daysober**	**Eindbazen**	**HackerDom**	**C.o.P**	**FluxFingers**	**Tachikoma**	**Shell-storm**	**ForbiddenBITS**	**BIOS**
Командные сервисы	670	480	680	470	450	390	340	460	310	250	290	30
Общая инфраструктура	220	460	240	140	340	220	360	100	140	120	100	60
Царь горы	413	100	0	193	0	0	0	0	0	0	0	0
Бонусные задания	112	208	305	158	168	232	103	72	9	69	30	41
Все заработанные баллы	1415	1248	1225	961	958	842	803	632	459	439	420	131

Примечание к таблице 13: желтый цвет – первое место, зеленый – второе, синий – третье.

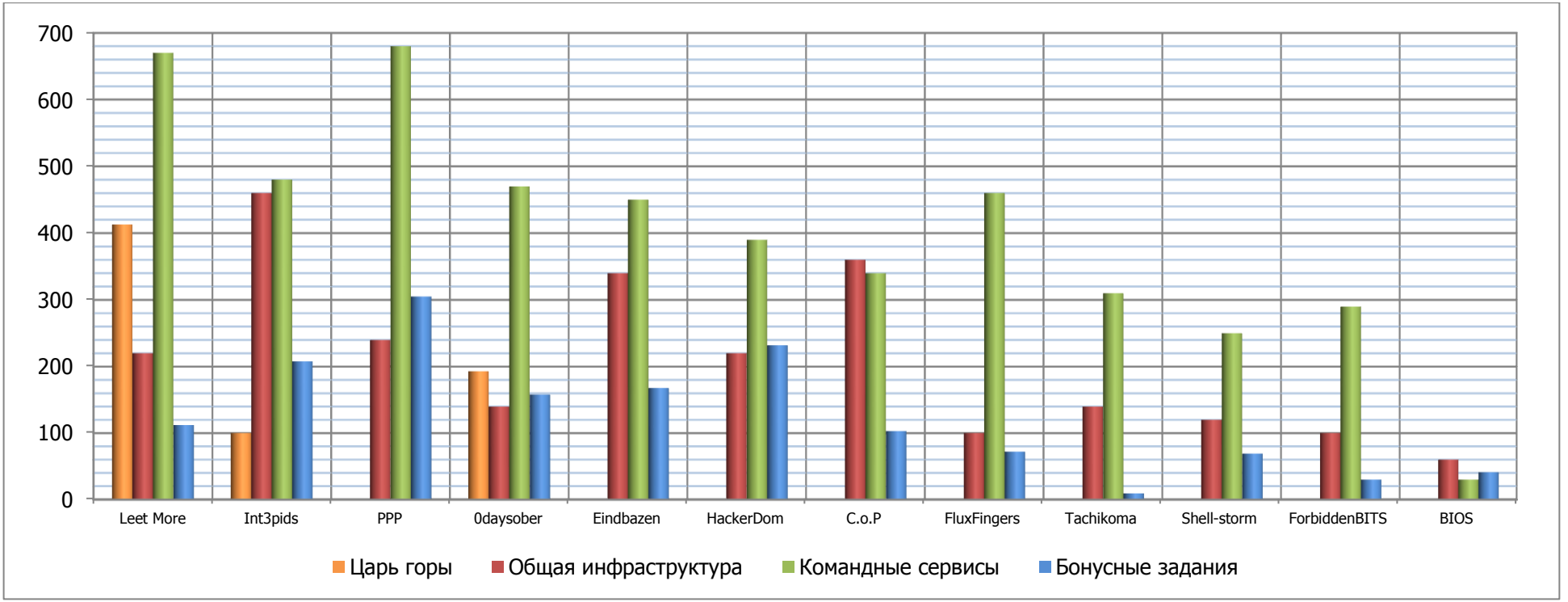


Рисунок 38. Баллы, заработанные командами по итогам CTF (по видам заданий)

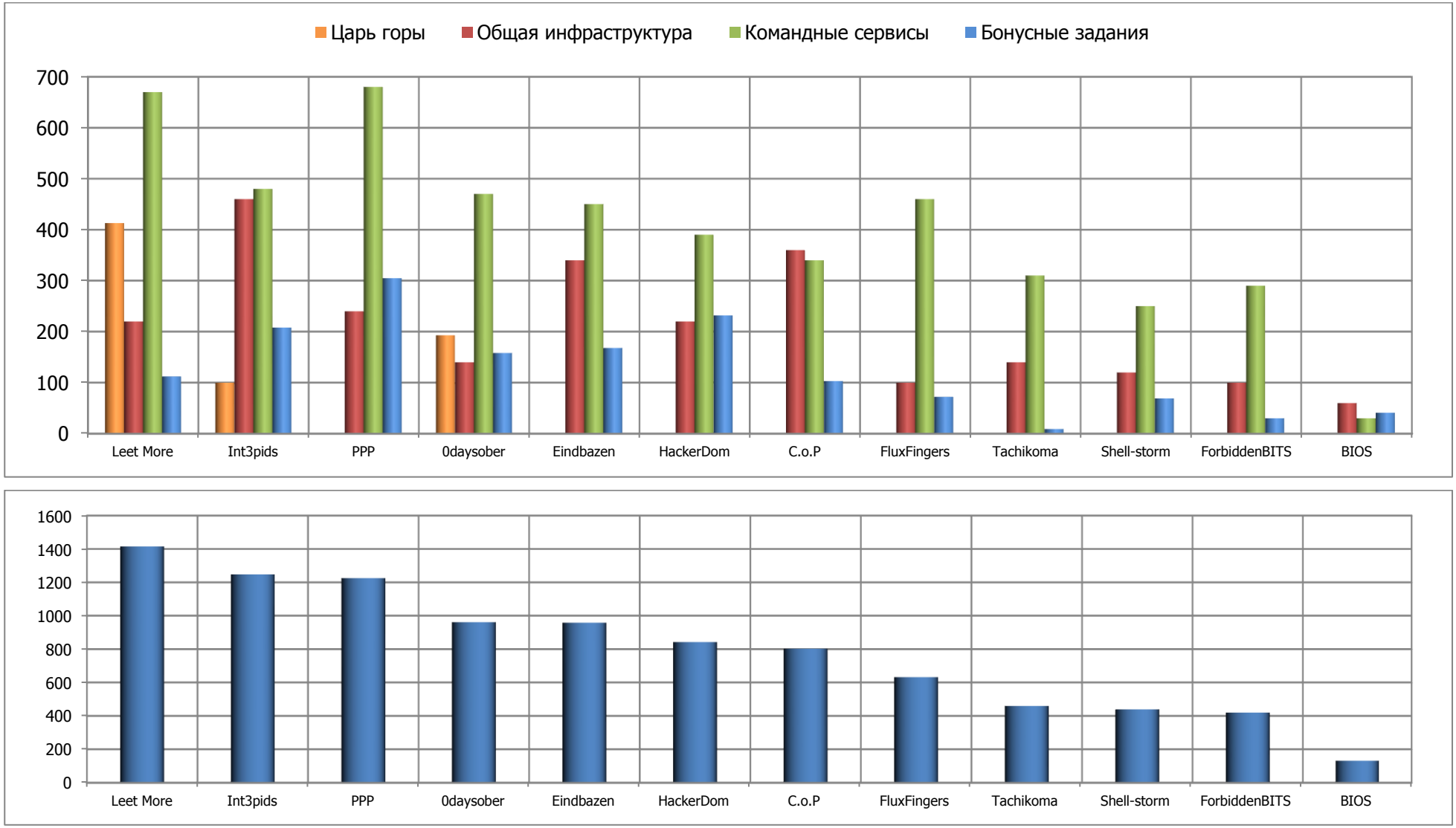


Рисунок 39. Соответствие заработанных командами в разных видах заданий баллов суммарному количеству заработанных баллов

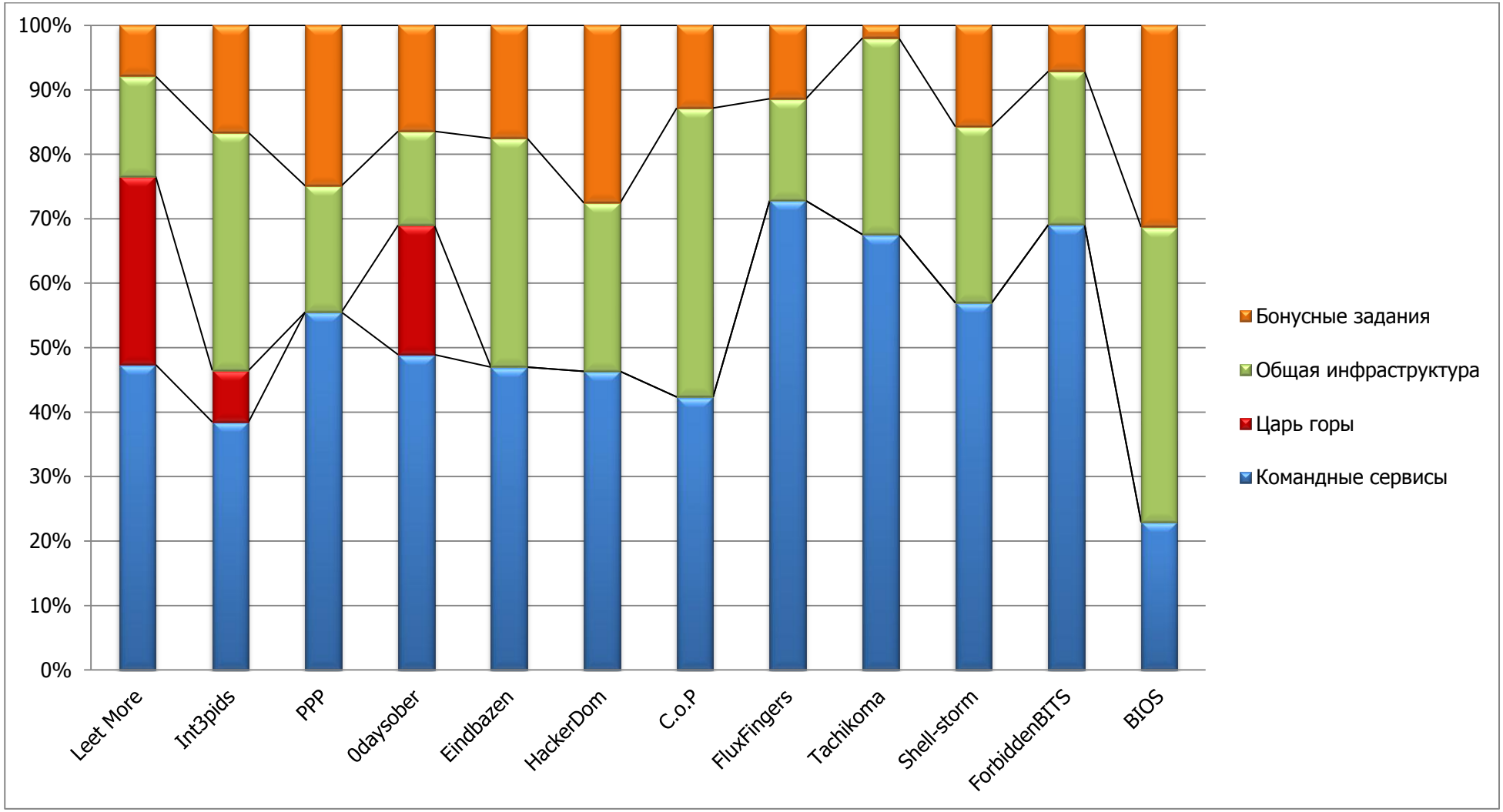


Рисунок 40. Доля заработанных каждой командой баллов в соотношении с общим количеством заработанных баллов

7. Заключение

Полученные данные не соответствуют официальному распределению призовых мест, поскольку данная статистика учитывает только заработанные баллы и не отражает баллы, потерянные командами в результате атак на их сервисы в рамках заданий командной инфраструктуры CTF, в результате атак на счета интернет-банков команд, и штрафные баллы за нарушение доступности сервисов.

На рис. 41 представлена диаграмма, отражающая итоговый рейтинг команд (в порядке убывания заработанных баллов).

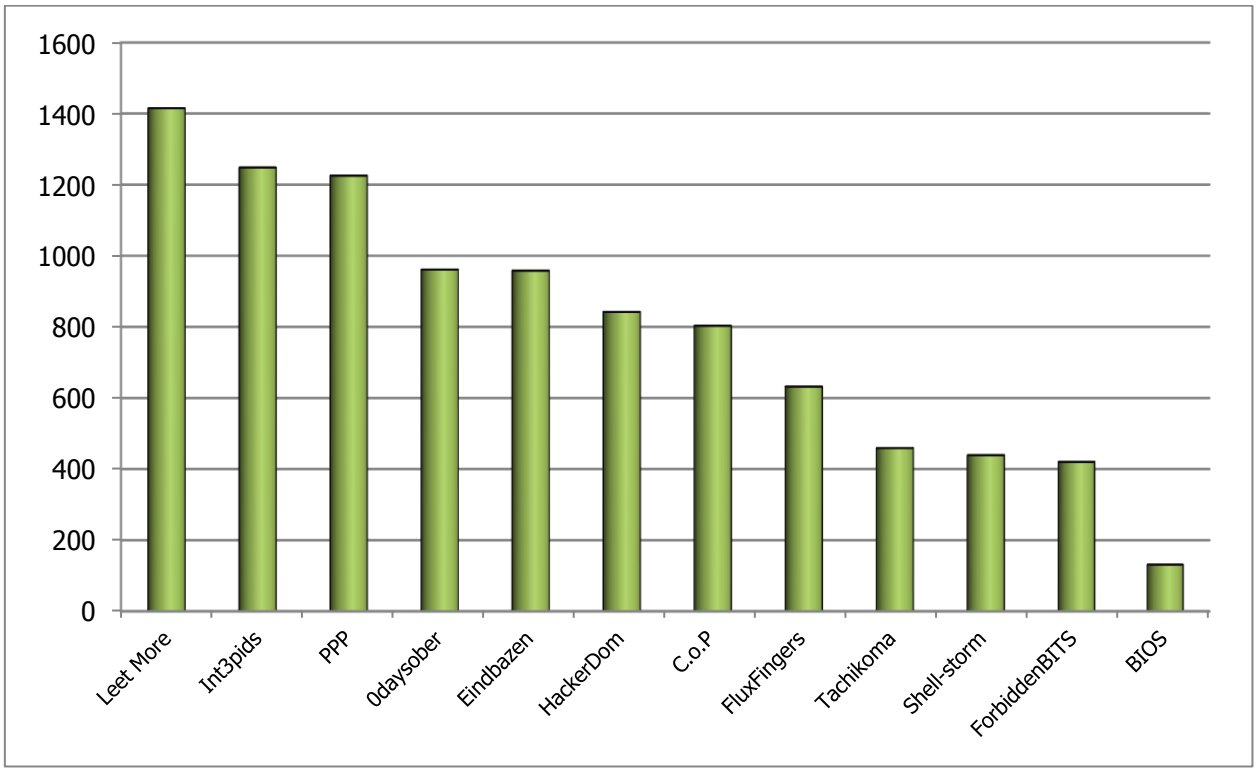


Рисунок 41. Итоговый рейтинг команд

Диаграмма на рис. 41 подтверждает, что в ходе соревнований все команды вели упорную борьбу как за места в тройке призеров, так и за строчки рейтинга отстающих команд. Лидирующим командам не удалось получить подавляющего преимущества, интрига соревнований нарастала до самых последних минут. Разница в баллах между соседними строчками итоговой таблицы относительно невелика.

При подготовке PHDays CTF 2012 были составлены модели возможного развития событий в ходе соревнований. Данные модели были разработаны с целью создания сбалансированной системы оценки действий участников CTF. Правила подсчета заработанных командами баллов и начисления штрафных

баллов были рассчитаны для каждого вида заданий в отдельности. Все задания отличались по тематике и степени сложности.

По предварительным оценкам было принято решение считать наиболее вероятными следующие случаи:

1) доминирование одной из команд во всех видах заданий и наличие большого числа явных аутсайдеров (как в классическом командном CTF, так и в заданиях инфраструктуры «Царь горы» и общей инфраструктуры);
2) доминирование нескольких (двух или трех) команд во всех видах заданий и отставание всех остальных команд;
3) доминирование различных команд в разных видах соревнований;
4) отсутствие явных лидеров и аутсайдеров во всех видах соревнований.

Правила расчета баллов были составлены таким образом, чтобы команды, не справляющиеся с заданиями одного вида, могли компенсировать отставание, решая задания других видов и тем самым сохраняя шансы на победу. Для победы командам необходимо было проявлять активность в рамках всех игровых инфраструктур, чтобы не упустить преимущество. Цель организаторов состояла в том, чтобы сделать PHDays CTF 2012 как можно более зрелищным, поддерживать интерес не только его участников, но и зрителей.

Хронология событий, представленная в табл. 11, показывает, что на протяжении всего CTF выделялись три-четыре лидирующие команды, ведя постоянную борьбу за распределение мест в первой тройке. Однако согласно полученной статистике, результаты CTF наиболее полно соответствуют модели 3. Победитель CTF, команда Leet More, уступила в «классическом CTF» команде PPP по набранным баллам и команде Int3pids в рамках общей инфраструктуры, но за счет баллов, заработанных в заданиях инфраструктуры «Царь горы», вышла на первое место в рейтинге. В то же время команды C.o.P и Eindbazen, занимавшие позиции в тройке лидеров в зачете общей инфраструктуры, так и не смогли войти в тройку призеров по итогам соревнований.

Результаты PHDays CTF 2012 показали, что цели, поставленные организаторами, были достигнуты в полной мере. Зрелищности соревнованиям добавили такие задания, как защита интернет-банка и бонусные конкурсы (контейнер с бумажным мусором и AR.Drone). Задание по защите своего банковского счета стало для команд сюрпризом во второй день соревнований, и позволило многочисленным участникам из сети Интернет по всему миру повлиять на результаты очного противостояния CTF. Особенностью PHDays CTF 2012 стало также введение в сюжет соревнований инфраструктуры «Царь горы», которая сыграла ключевую роль в определении победителя.