ANALYTICS ON THE PHDAYS CTF 2012 CONTESTS RESULTS

Table of Contents

1. Introduction 3
1.1. Sponsors 4
1.2. CTF Participants 5
2. The Contests Description 7
2.1. General Description 7
2.2. CTF Infrastructure 8
2.2.1. Tasks type 9
2.2.2. Flags type 9
2.2.3. Scoring Rules 10
3. Legend 13
3.1. Day 1 16
3.2. Day 2 19
4. Winners at PHDays CTF 2012 22
5. Contestants About PHD CTF 2012 23
6. Analytics 24
6.1. Point distribution for the team infrastructure tasks (classic CTF) 24
6.1.1. Score history 24
6.1.2. Score dynamics 29
6.1.3. Analysis of the participants' actions 30
6.2. Point distribution for the shared infrastructure tasks 36
6.2.1. Score history 36
6.2.2. Score dynamics 41
6.2.3. Online HackQuest results 48
6.3. Point distribution for the King of the Hill contest 52
6.3.1. Point distribution among the CTF teams 52
6.3.2. Point distribution among the online participants of the King of the Hill contest 54
6.4. Point distribution for the bonus tasks 65
6.5. Total statistics and CTF results 67
6.5.1. Total score history 67
6.5.2. Total score dynamics 72
6.5.3. CTF results 77
7. Conclusion 83

1. Introduction

The contests are held in the CTF (Capture the Flag) format. Several teams are to defend their own networks and attack the networks of the other teams for a specified period of time. The aim of the contestants is to detect vulnerabilities in the systems of other competing teams and obtain sensitive information (flags), and at the same time to detect and fix vulnerabilities in their own systems.

The key feature of Positive Hack Days CTF is its closeness to real-life conditions. All the vulnerabilities are not fictional, but indeed occur on present-day information systems. Moreover, the format of PHDays CTF is really wide due to the game environment's saturation with unique elements (capture and holding systems according to the "King of the Hill" principal, ability to implement a blind attack etc.).

The CTF participants tested their strength in a real struggle and got an opportunity to develop their own information security solutions.

To add a special appeal to the contest, the game infrastructure is prepared according to the story lines which are unique for each contest within PHDays CTF. Such conditions create a remarkable ambiance and make the Positive Hack Days CTF contest to stand out against background of other similar contests.

1.1. Sponsors

Positive Technologies is grateful to the sponsors which helped holding the CTF contests on information security within the Positive Hack Days 2012 international forum.

General Sponsor: Kaspersky Lab

Kaspersky Lab is the largest antivirus company in Europe, a developer of the security systems providing protection against malicious and undesirable software, hackers attacks, and spam. The company is ranked among the world's top four vendors of information security solutions. There are more than 2300 highly skilled employees in Kaspersky Lab. The company's products protect computers and mobile devices of more than 300 million clients worldwide; the technologies are used in the products of the largest vendors of software and hardware solutions. For more information, please visit www.kaspersky.com/.

Technological Partner: Cisco

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. The net sales in fiscal year 2010 were 40 billion dollars. For information about solutions, technologies, and current activities please go to www.cisco.com.

Technological Partner: ICL

ICL – KMECS (http://www.icl.ru/web/guest) is a high-tech dynamic company, one of the largest IT companies in Russia. ICL – KMECS offers integrated IT solutions and services, ranging from consultancy, design, implementation through to warranty service and maintenance of information systems regardless of scale. The alliance with the world's IT leader Fujitsu Limited provides ICL-KME CS access to state-of-the-art technologies and projects. The company's customer base includes federal ministries and agencies, Russia's biggest enterprises in telecommunications and fuel and energy sectors, banks, industrial and commercial groups, state and private companies. The company's extensive expertise in development and implementation of the large-scale IT projects and highly experienced team of specialists are the key to its success and ensure high level of customer service.

1.2. CTF Participants

0daysober, Switzerland

0daysober is a brand new team emerging from the French part of Switzerland and made by friends who share the same passion for IT security.

BIOS, India

The BIOS team from Amrita Vishwa Vidyapeetham, Amritapuri, India has been a regular at CTF contests since 2008. Starting off with finishing 24th at CIPHER4 (2008), they have taken part in most worldwide CTF contests such as CODEGATE, ruCTFe, rwthCTF, Mozilla CTF (14th place) and pCTF. They have also succeeded in organizing InCTF, India's first national CTF contest, for 3 years now.

C.o.P, France

Consortium of Pwners (C.o.P.) Consortium of Pwners (C.o.P.) is a French security team created in 2011 by former members of Nibbles team. The team regularly participates in vulnerability research and CTF contests.

Eindbazen, the Netherlands

The team was founded in March 2011 to compete in the Codegate 2011 Prequals. Eindbazen celebrated its 1st anniversary at the Codegate 2012 Prequals. Most team members met in real life and knew each other before the team creation. The team consists only of Dutch members, including both students and professionals.

FluxFingers, Germany

The FluxFingers team has represented the Ruhr University (Bochum) in CTF contests since 2007. In the past years, it has also organized the famous hack.lu CTFs. The team's rankings are listed here: https://www.fluxfingers.net/scoring.html

ForbiddenBITS, Tunisia

ForbiddenBITS is a Tunisian team created in 2011. The team won the Tunisian CTFs (Security challenge Days 1 & 2, Securinet Challenges 2011 & 2012) and participated in several other challenges.

HackerDom, Russia

The HackerDom team was created in 2005 at the Mathematics and Mechanics Department of the Ural State University. The members give weekly seminars named HackerDom's Secrets. The team regularly participates in CTF and CTF-like contests, and also holds national (RuCTF) and international (RuCTFE) interuniversity contests in information security.

Int3pids, Spain

Int3pids is a Spanish team which was created in 2010 and formed on the basis of Sexy Pandas. They participated in many well-known CTFs.

Leet More, Russia

The Leet More team was created in 2008 at the University of Information Technologies, Mechanics and Optics (ITMO). The team's achievements:

2nd place at PHDays 2011 CTF
4th place at DEFCON 19 CTF as part of Russia team
1st place at Enowars 2011 CTF
1st place at Mozilla CTF 2012 (as part of More Smoked Leet Chicken)
1st place at IFSF CTF Quals (as part of More Smoked Leet Chicken)
1st place at NeoQuest 2012
1st place at CodeGate 2012 Quals and CodeGate 2012 Final (as part of Leet Chicken)

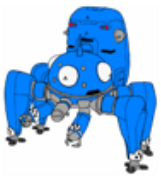
Plaid Parliament of Pwning, USA

The team was founded by several students of the Carnegie Mellon University in 2009. The team consists of students, graduates, postgraduates and the university employees. Over the years, PPP has won numerous CTF competitions, including Codegate, iCTF, CSAW, HUST, Ghost in the Shellcode, Secuinside, and PHDays.

Shell-Storm, France/Switzerland

Shell-Storm.org is a development organization based on GNU/Linux systems that provide free projects and source codes. Shell-storm.org provides useful information to the specialists in performing security testing.

Tachikoma, Japan



The Tachikoma team is formed from the students of the following universities in Japan: the University of Tokyo, Tokyo Denki University, Tokyo University of Technology, and University of Aizu. The team was created in February 2012. Its first appearance was made at PHDays 2012.

2. The Contests Description

2.1. General Description

Each team consists of 7 participants and has a captain. Only 5 participants are at a table; the remaining 2 participants are considered as replacement players. Replacement can be done at any time upon the jury's permission.

Teams use their own computer devices (a laptop, for instance).

Each flag represents a 32-character string in the MD5 format.

Points are scored for:

- Sending flags captured from the competitors' services.
- Sending flags captured in the shared segment of the game infrastructure (black-box).
- The hold-down time at the King of the Hill contest.
- Winning the bonus contests.
- Sending bonus flags captured in the shared segment of the game infrastructure.

Points are deducted from teams' score for:

- Capturing flags from the team's servers by the opposition.
- Failing to ensure the availability of their own servers.
- Failing to ensure the availability of functions performed by the vulnerable services.
- Failing to follow the general rules of the contests.

During the game, teams are allowed to:

- Use not more than 5 computers and network devices not lower than the second level of the ISO OSI protocol stack.
- Make any modifications of the provided servers unless it is explicitly prohibited by the jury.
- Conduct attacks against the competitors' servers in order to capture their flags.
- Conduct attacks against the servers of the shared infrastructure segment in order to capture the flags.
- Conduct attacks against the services of the King of the Hill contest.
- Ensure the security of the services of the King of the Hill contest using all methods except those explicitly prohibited by the rules.
- Conduct attacks against wireless data transmission channels in order to get the control (bonus task).

During the game, teams are prohibited from:

- Attacking jury's computers.
- Filtering the traffic to any CTF resource (e.g. filtering by IP addresses).

- Generating unreasonably high volume of traffic (flooding).
- Conducting destructive attacks against the rivals' servers (such as rm-rf/).
- Intentionally hindering normal functioning of the services, including those of competitor teams and shared game infrastructure, and the services of the King of the Hill infrastructure.
- Removing flags from the provided servers, rivals' servers and those of the shared game infrastructure.
- Performing destructive actions against the subjects of the game infrastructure.
- Performing the above actions in the guise of a rival team.

Work of the jury:

- The jury may specify the rules at any time before the game begins.
- The jury may impose a penalty/disqualify a team for a foul.
- The jury decide the winner by calculating the total scores.

2.2. CTF Infrastructure

At the beginning of the game, the teams are provided with identical servers with preinstalled set of vulnerable services. The teams' aim is to detect the vulnerabilities, fix them on their servers, and exploit them to obtain sensitive information (capture the flags) of the competitor teams.

The game process is constantly monitored by the jury's supervising system, which regularly modifies the state of the game infrastructure by adding new flags and vulnerabilities to the teams' servers, and checks the state of the previously added flags and the functioning of vulnerable services.

A limited number of vulnerable services performing specified functions is developed beforehand. Participants deal with two types of systems: white box (participants have a privileged access to the system on the OS level) and black-box (participants have access to vulnerable services and sensitive information via network). Any participant of the Positive Hack Days CTF may challenge to exploit real vulnerabilities within the said network segment and compete for additional awards. As opposed to the PHDays CTF 2011, teams can compete in capturing and holding down a system of services within the King of the Hill contest, in which teams score points for the time of holding down services.

During the PHDays CTF 2012, additional bonus contests are held, which are intended to entertain the participants and make the event more spectacular. Bonus tasks can bring additional points in CTF total.

Bonus contests include:

- Conduct attacks in order to take over the remote device control (AR.Drone).
- Search for information in containers with scrap paper.
- Collect flags which pop up in the services of the teams in specified periods of time.

2.2.1. Tasks type

The task types offered are as follows:

- To detect and exploit vulnerabilities in the services of the game infrastructure of the opponents and defend your own services from the like attacks.
- To detect and exploit vulnerabilities in the services of the shared game infrastructure.
- To detect and exploit vulnerabilities in the services of the King of the Hill infrastructure in order to obtain and keep control over the servers.
- Bonus task: to collect flags which pop up in the services of the teams in specified periods of time.
- Bonus task: to search for information in containers with scrap paper and to take over the remote device control (AR.Drone).
- I-Bank protection.

2.2.2. Flags type

Each flag represents a 32-character string in the MD5 format.

Team services flags

Team services flags have the following characteristics:

- Flags have a team identifier (the team can not claim its services flags as the flags captured from the opponents' services).
- The team can capture similar flags from services of several (all) other competing teams.
- Each flag can be captured by several (all) competing teams, but only once by each team.

Shared infrastructure flags

Shared infrastructure flags have the following characteristics:

- Flags can be captured by each team to the same extent.
- Each flag can be captured by several (all) competing teams, but only once by each team.

King of the Hill infrastructure flags

King of the Hill infrastructure flags have the following characteristics:

- Flags can be captured by each team to the same extent.
- Flags contain information on belonging to a particular service of 1 or 2 scenario level.
- Each flag can be captured only once and by one team.

Bonus task flags

Bonus task flags have the following characteristics:

- Flags have a team identifier (the team can not claim its services flags as the flags captured from the opponents' services).
- The team can capture similar flags from services of several (all) other competing teams.
- Each flag can be captured only once and by one team.

2.2.3. Scoring Rules

For detailed contests rules please visit the PHDays 2012 official site http://phdays.com/ctf/.

Team services

For each flag captured from the competitors the team scores 10 points. The team penalty for failing to hold the flag of its infrastructure is 10 points. The team penalty for failing to hold the same flag two or three times is 10 points for each loss.

Note. If the team fails to hold a flag for several times in case attack is implemented by several competitive teams, penalty is charged for the first 3 lose of the flag.

Penalty is also charged for failing to ensure the availability of their own servers and/or functions performed by the vulnerable services. Penalty for failing to ensure the availability of servers is 40 points.

Shared infrastructure

Number of points for sending flags captured from shared game infrastructure depends on the sophistication level of the searching of the flag. Total score for this task is up to 2000 points.

King of the Hill

Three types of services are available: two services of the first level of sophistication and one server of the second level of sophistication. Access to the service of the second level of sophistication is available only upon the first level task is done. Total score for each team in this task is up to 2640 points.

If the team holds the service of the first level of sophistication, it scores 1 point for every 3 full minutes of continuous control over the service. If the team holds the service of the second level of sophistication, it scores 2 point for every 3 full minutes of continuous control over the service. If the team fails to control the service and then captures it for the second time, 3 minutes intervals counted out over again.

Bonus task

Points are scored for winning the bonus contests and capturing the bonus flags. Total score is 804 points, including points for winning the bonus contests.

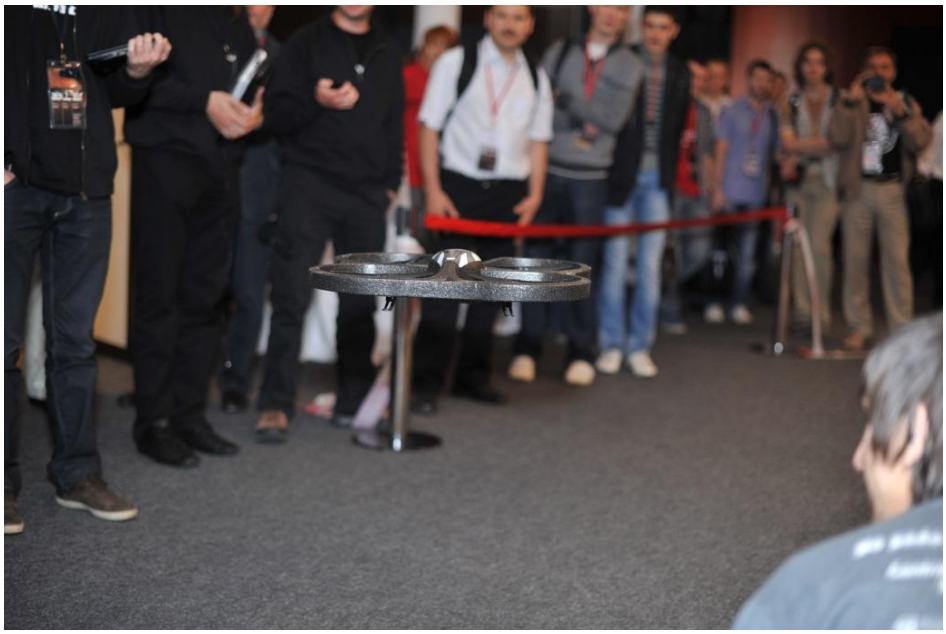
Teams services state is amended every 10 minutes during 7 hours of the bonus task (from 12.00 am to 7.00 am at night). Every state of the game infrastructure services includes 1 bonus flag; the team scores 1 point for sending a flag.

Bonus contests

The team scores 7 points for each flag found during the contests of searching information in containers with scrap paper.

Picture 1. Container with scrap paper

The team scores 450 points for winning one of the two stages of the contest of taking the remote control over AR.Drone.



Picture 2. AR.Drone Quadrotor

I-Bank protection

It is a final task to be held upon completion of the main stages of CTF. The description of the final contest will be announced on the second day of PHDays CTF 2012.

According to the description of the contest, the game infrastructure of the I-Bank is organized; within the infrastructure a particular amount of money (equal for each team) is transferred to the account of the competitive teams. This particular amount of money is announced and defined due to current ranking of the teams 3 hours before CTF completes.

The teams are to protect their banking accounts against Internet attacks. The amount of money the teams loose during this task is equal to points deducted from teams' total.

Defining a winner

Total score is equal to total raking (general number of points) upon the completion of the final task of I-Bank protection. The team which scored maximum points is declared the winner.

3. Legend

The XXI century is the Era of Biotechnologies. Mass production of genetically-modified products was supposed to deal with hunger, diseases and give the humanity the power over the Nature. However, by the middle of the century genetically-modified organisms were everywhere: from tundra to rainforests.

In response to the intervention Flora struck back to survive. Gigantic weed-trees and tiny bugs flooded forests and fields of the Earth. People also suffered from the genetic chaos. Numerous epidemics spread over the planet, some of them were artificially induced. That was when World War IV broke out to become the fastest and most devastating war of all.

The second half of the century saw demoralized population that was cut by a third because every other child was born with significant genetic deviations. Having lost their last bit of hope, people ran to airproof cities to cover from the aggressive environment. And now, two hundred years later, few people who managed to survive are fighting every day to stay alive. On the one hand, there are city states that are constantly fighting against each other, on the other hand – mutant nomads wandering about destroyed cities and dangerous forests. People are surviving off of a few highly-secured automated farms growing "clean" food.

Inevitable technological setback forced people to fight for remaining technologies and for serviceability of management systems left by their ancestors. Only twelve underground cities out of hundreds erected in the past still exist. And nobody knows how many of them, if any, will be there tomorrow.

Figures 1 and 2 present the layout view of the game services.

You can find a detailed description of the Legend CTF 2012 as well as specially prepared booklets and videos here: http://blog.phdays.com/2012/06/for-those-who-missed-phdays-ctf-2012.html.

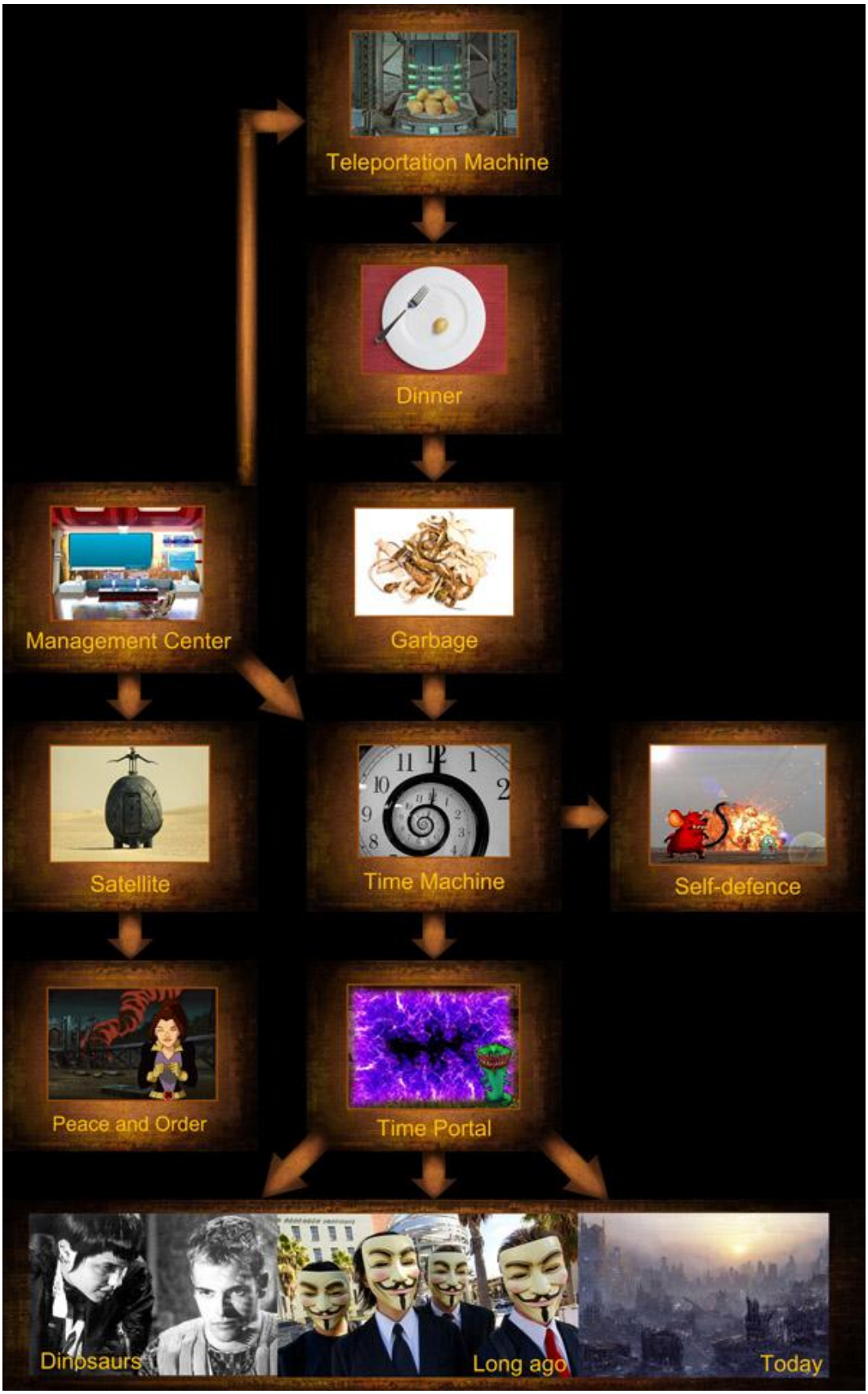


Figure 1. Game services of the first day

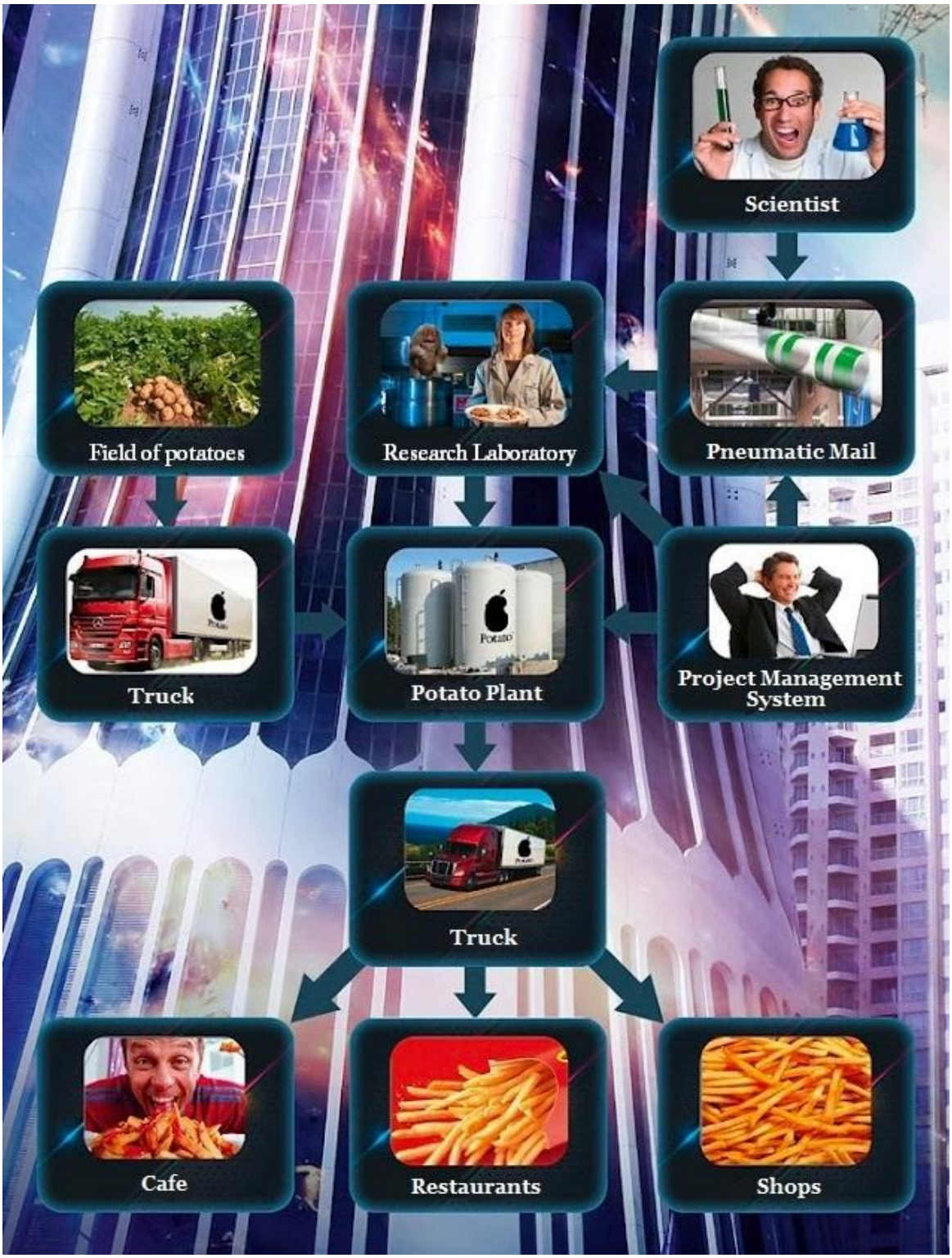


Figure 2. Game services of the second day

3.1. Day 1

Description of the game services of the first day

Teleportation Machine

Potatoes are our food source. It is one of a handful of crops that managed to survive the years of the End. Unfortunately, despite the best efforts of our scientists, mutagenic agents are affecting the potatoes that we cultivate. So, in order to replenish our stock of genetically clean seeds, we use the unique teleportation system allowing us to supply seeds from other Cities without very dangerous multi-day trips to the outside world. If we are not able to use teleportation machines to replenish the seed fund, we will be left without clean food, and that's when we will no longer be Living People.

The priorities of your unit are smooth operation and protection of teleportation machines against attacks from outside. Remember — this determines whether there will be food on the plates when Living People come for dinner tomorrow. The survival of all Living People depends on you.

Combat Satellites

The citizens of our City are constantly in danger. Mutants attacks aimed at penetrating our territory become more and more frequent, and enemy Cities desperately want to get hold of our resources and basically of everything that we have. Peace and order of the City directly depend on efficiency of our combat satellites to protect our citizens and strike preventative blows. If our satellites fail, we are as helpless as kittens — it will not take long before other Cities take over all of our food supplies and production facilities, and our citizens are killed by mutants.

Time Machine

We managed to get through all these years and remain Living People only thanks to clean food. However, mutative changes are approaching our farms and we will not be able to replenish our stock of genetically clean seeds forever. The Time Machine is our only hope for survival. If we manage to open the Time Portal, we will go back in time when the life was a box of chocolates, the water was clean, and people had access to shoe polish, toothpicks and many other wonderful things. The Time Machine will give us a chance to stop the chaos and avert the End.

Even though the Time Machine is equipped with an advanced self-protection system which rids the surroundings of rats and tramps, we cannot apply the system to protect us from attacks of other Cities. If as a result of any of those attacks our enemies destroy the Time Machine, we are doomed.

Management Center

Since the City is constantly struggling for survival, any delay in the system management process might lead to total destruction. Quick and efficient decision making is essential for us to stay Living People. The Management Center monitors all fundamental systems of the City, such as Teleportation and Time Machines. If an enemy gets hold of the Management Center, our officers will be unable to receive relevant information on the City's protection status, which will put all of us in danger.

Cantina

Raspberry Pony is the best (and only) cantina on the Planet. It is frequented by leading politicians, scientists and influential people from all Cities. It is the venue of major decision making carefully supervised by Madam Dondon. Moreover, if you manage to compromise any of the scientists, you may get a step closer to opening the Time Portal. He, who owns the Cantina, owns the world.

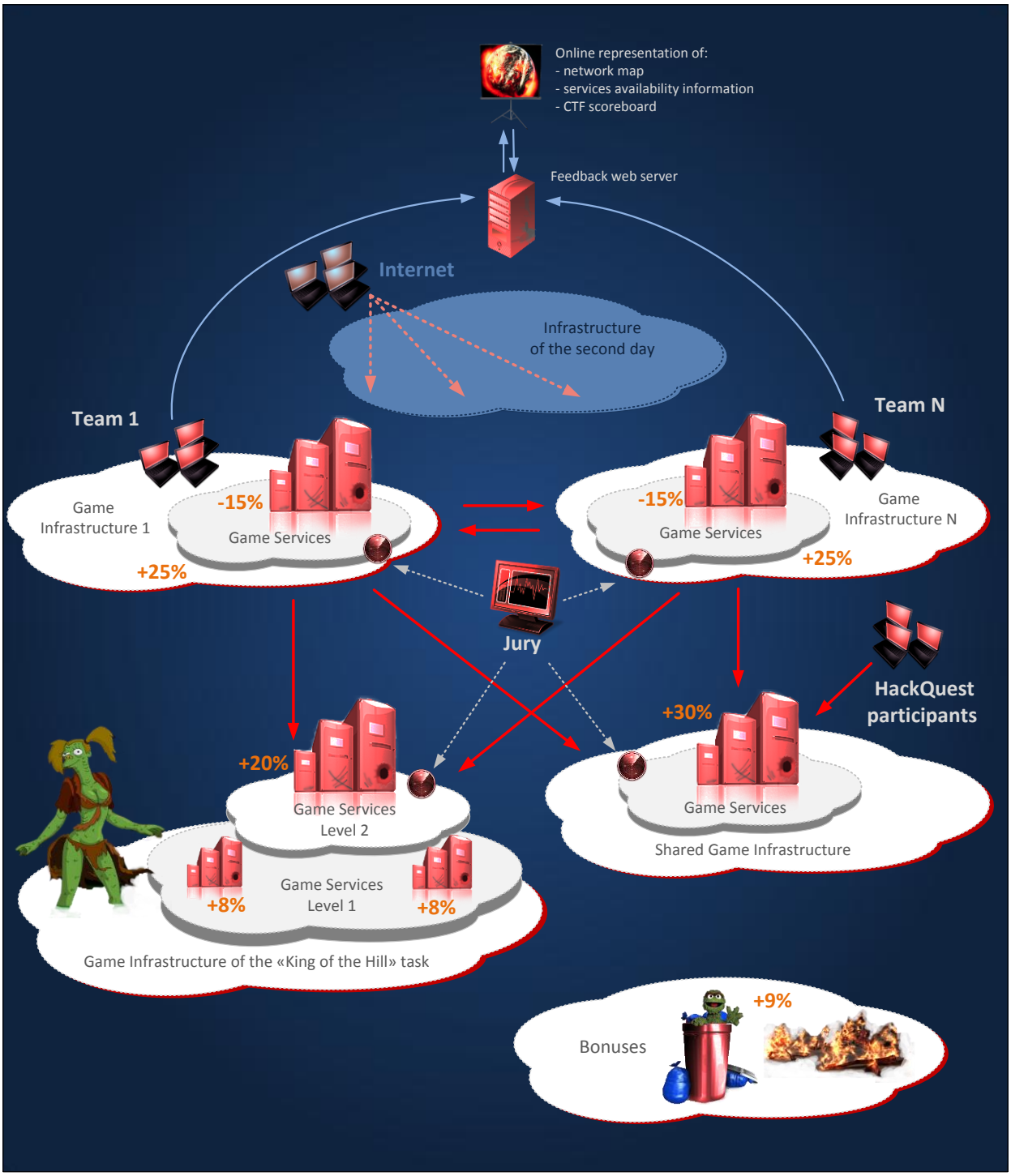


Figure 3. Layout of the game infrastructure of the first day

3.2. Day 2

Description of the game services of the second day

Potato Plant.

Being the world's leading potato manufacturer, Potato uses advanced, know-how potato cleaning and processing techniques. It produces such well-known global potato brands as Ringlets, Happy Bubbles, Potato Fingers, and Luxury Delicacies. In order to ensure smooth production process, the plant utilizes a SCADA system — Potato Multifunctional Universal Treatment and Assortment Technological System (MUTANTS).

Your aim is to procure for safe and uninterrupted operation of MUTANTS. A minor fault in the system's performance will stop the whole production process and result in major financial losses.

Research Laboratory

We employ advanced genetic engineering innovations so that you to could enjoy the most high-quality potatoes. Our scientists worked out a way to be able to store Potato products for 12 years (not that you will want to do that, because the company also made sure the potatoes were so delicious they would be usually devoured within 8 hours after hitting the racks). Currently our scientists are working to shape a potato into a user-friendly cube of 20x20x20 cm.

The Lab is a fundamental department of our company ensuring our competitive advantage and market leadership.

Pneumatic Mail

In order to quickly and safely exchange documents and potato samples the Potato company uses pneumatic mail. The Research Lab also takes advantage of pneumatic mail to interact and exchange knowledge with leading scientists from various institutes. It is essential to ensure uninterrupted operation of pneumatic mail so that the Lab receives relevant information on the latest genetic engineering developments, and its employees do not stage a strike failing to get hold of the latest issue of the Naked Genetics magazine.

Project Management System

Smooth operation of a hi-tech company like Potato calls for automated Project Management System. On a daily basis Potato's conveyor belts process millions of potatoes, scientists at the Research Lab are working on dozens of projects at the same time and handle thousands of letters delivered via pneumatic mail, so a breakdown of the Project Management System would inevitably cause chaos and, subsequently, downfall of the entire company.

I-Bank

Potato's annual turnover equals hundreds of thousand reaching millions of dollars in the year of plenty. No doubt, the President does not keep the money at his house (well, not all of the money) preferring the safety of a bank. Potato's bank accounts must be highly secured. If any money is stolen from the Potato's account, the company will go bankrupt resulting in lost jobs for thousands of Potato's employee including you.

Media Holding

Sleepwalker Media Holding Inc., the world's largest media holding, controls dozens of mass media outlets including Hypnotoad TV Channel, Lacklustre Voice radio station, and weekly newspapers Young and Sclerotic and Beer Belly. Despite the fact that SMH publications are mostly outstandingly boring and useless (except for the Hypnotoad Show, of course!), product placement generates enormous incomes for advertisers. There are scarce publications in the independent mass media arguing that the SMH's success is due to mental effect on the audience (even including hypnosis). However, nobody can provide reliable evidence. The SMH owner has unlimited resources, that is why all international leaders (including Potato) are trying to gain control over the holding.

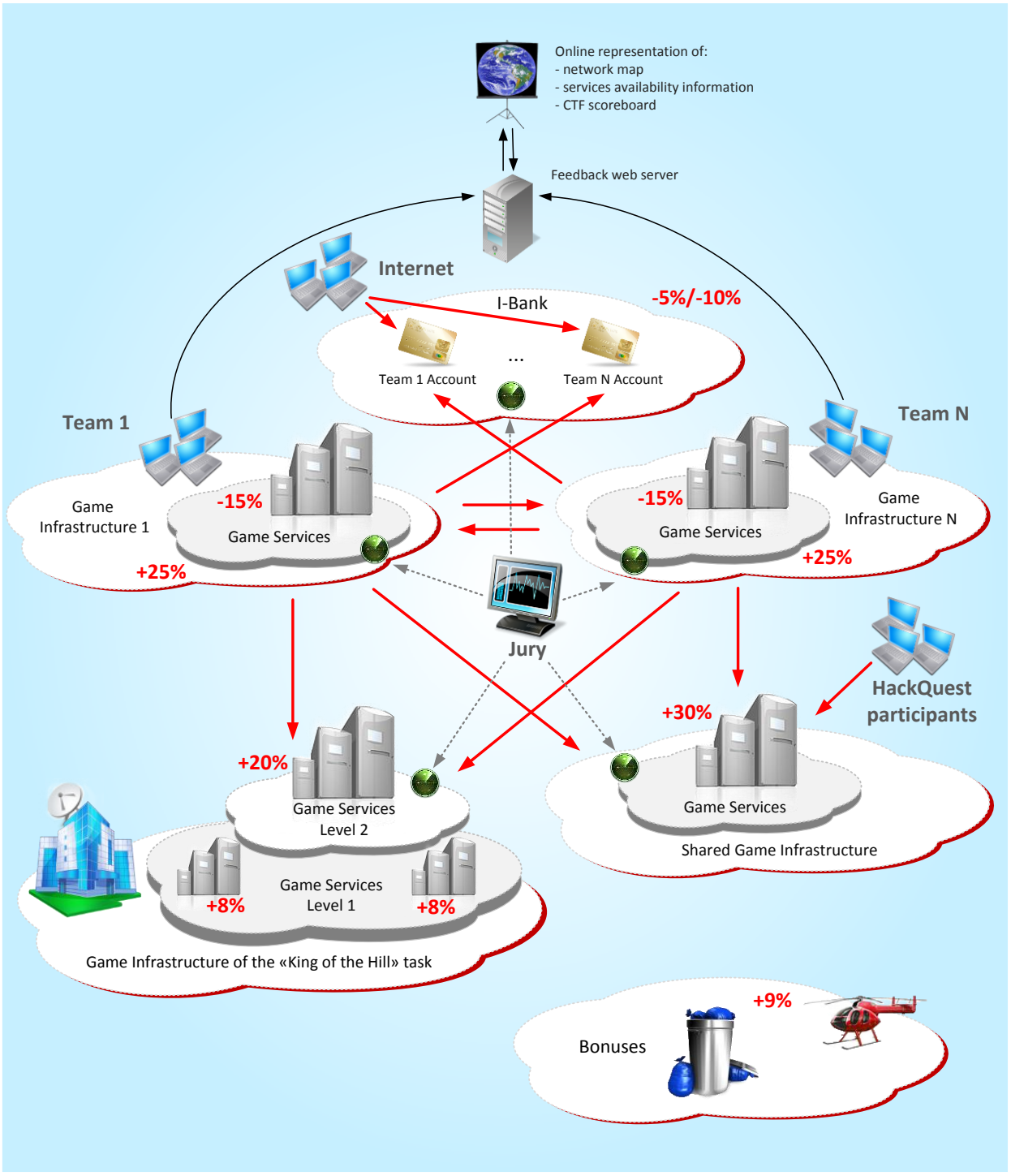


Figure 4. Layout of the game infrastructure of the second day

4. Winners at PHDays CTF 2012

1st place

Leet More, Russia

2nd place

0daysober, Switzerland

3rd place

Int3pids, Spain

5. Contestants About PHD CTF 2012

CTF 2012 brought together specialists from 11 countries. The event left no indifferent; contestants posted their opinion about CTF, the PHDays 2012 forum and about Moscow as well.

BIOS participant posted: "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". You can find the whole article at: http://arvindsraj.wordpress.com/2012/07/11/phdays-ctf-2012/.

Eindbazen's comment (published on Twitter): https://twitter.com/ThiceNL/status/209653337912655872/photo/1

Photo 3. Eindbazen team's commemorative trophies

0daysober about the contest:

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

Report on PHDays CTF 2012 on Habrahabr:

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

6. Analytics

6.1. Point distribution for the team infrastructure tasks (classic CTF)

Figure 5 provides the data reflecting the number of points earned by the teams only by capturing flags on the vulnerable resources of the competitors (including bonus flags captured at night). Therefore, the team scores, if rated by the capture of the team infrastructure flags only, differ from the final ratings: PPP is the leading team, Leet More holds the second place, Int3pids is the third.

The diagram makes it clear that there's no obvious leader yet, a lot of teams can claim the first place as they have approximately the same number of points. BIOS stands apart from other teams, because it could not protect its services and conducted only three successful attacks on the competitors' services as part of the main competition (all three attacks were conducted on the second day of CTF).

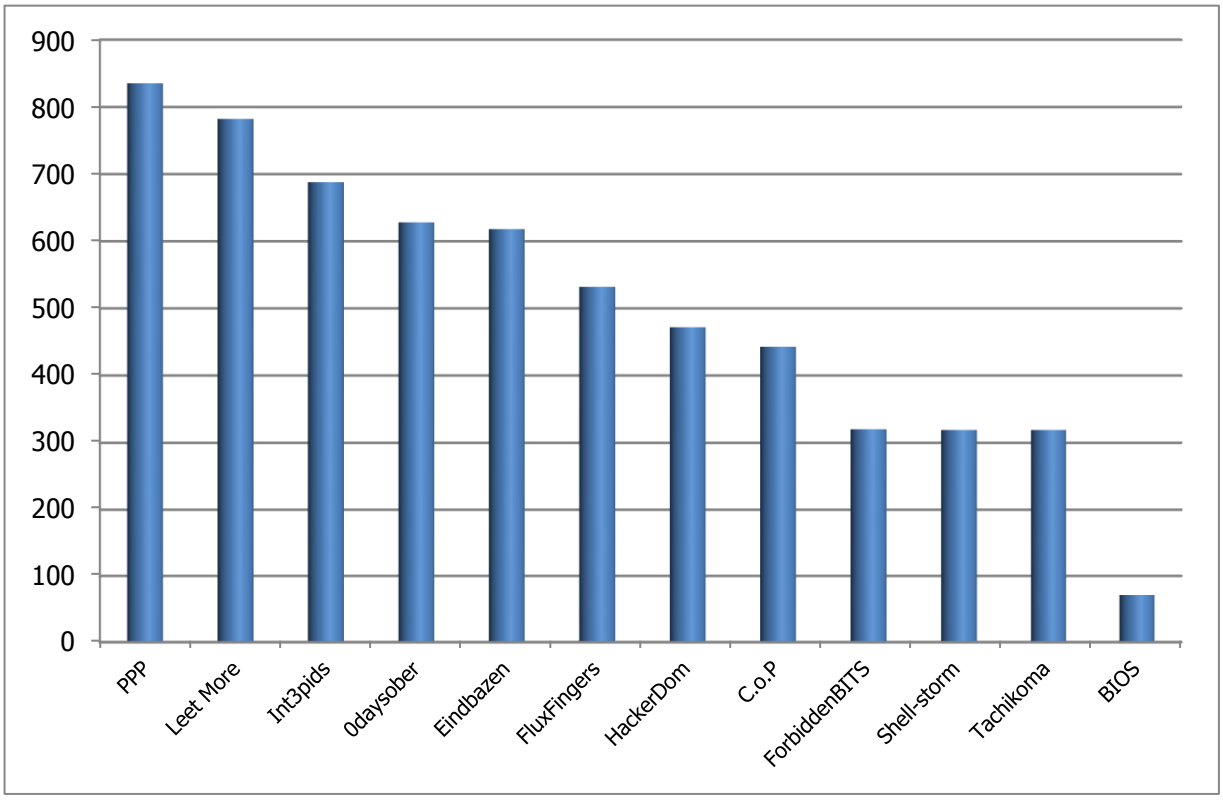


Figure 5. Points earned by the teams in the team infrastructure tasks

6.1.1. Score history

Score history is provided in table 1 and in figures 6-8 separately for the first and second day of the competition and night tasks.

Table 1. Score history for the team infrastructure tasks

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

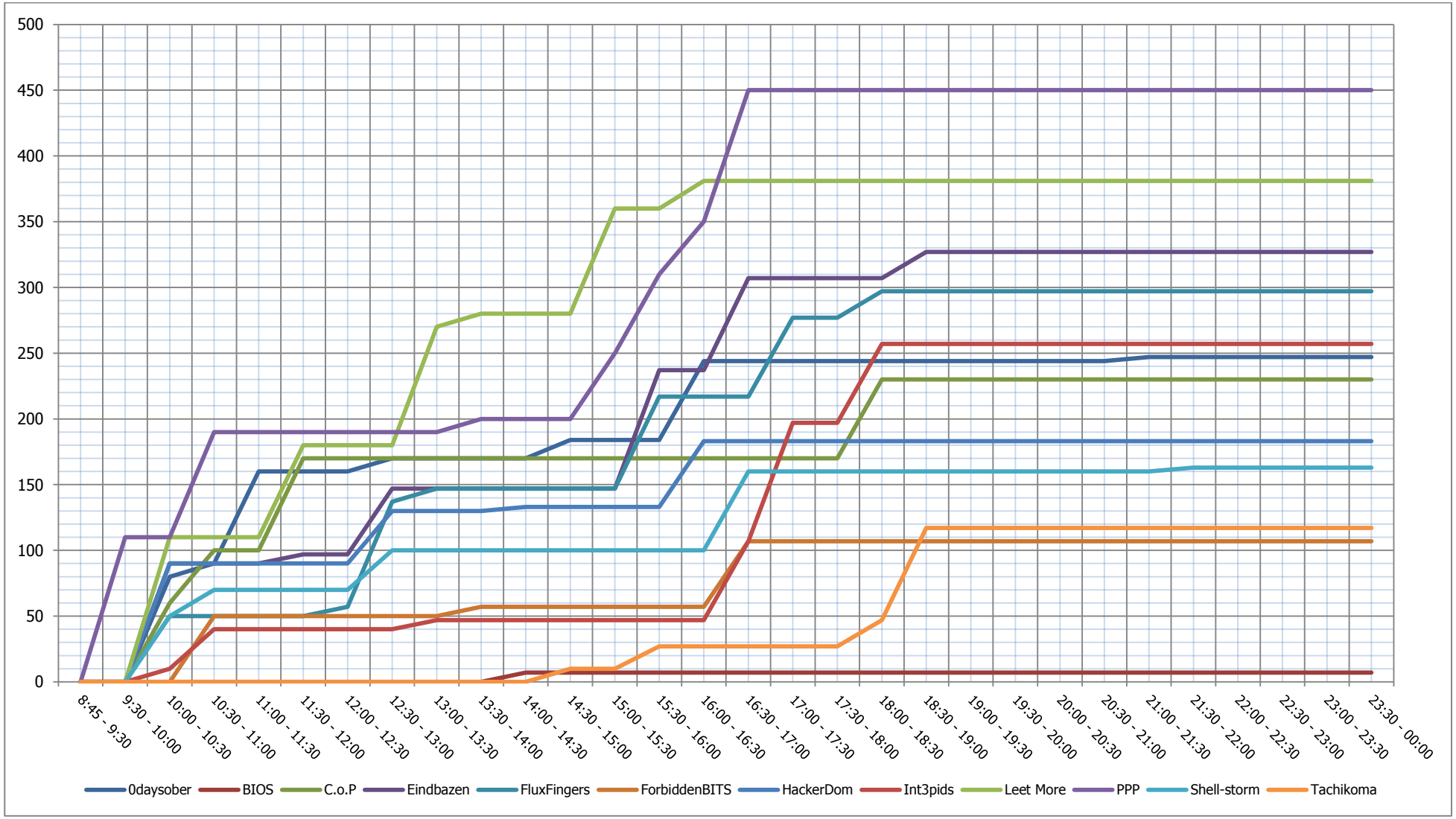


Figure 6. Score history for the team infrastructure tasks solved during the first day of the competition

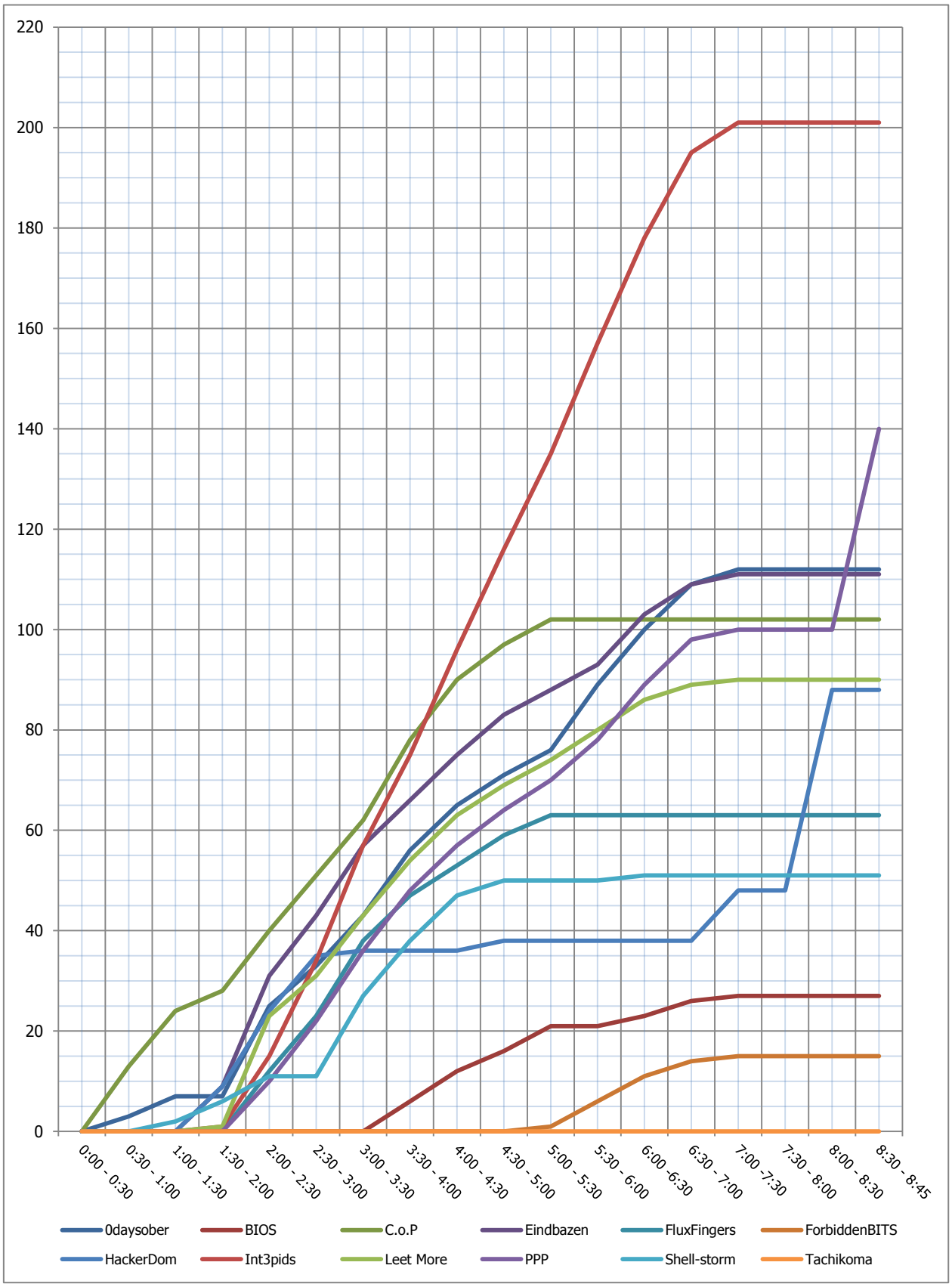


Figure 7. Score history for the team infrastructure tasks solved at night

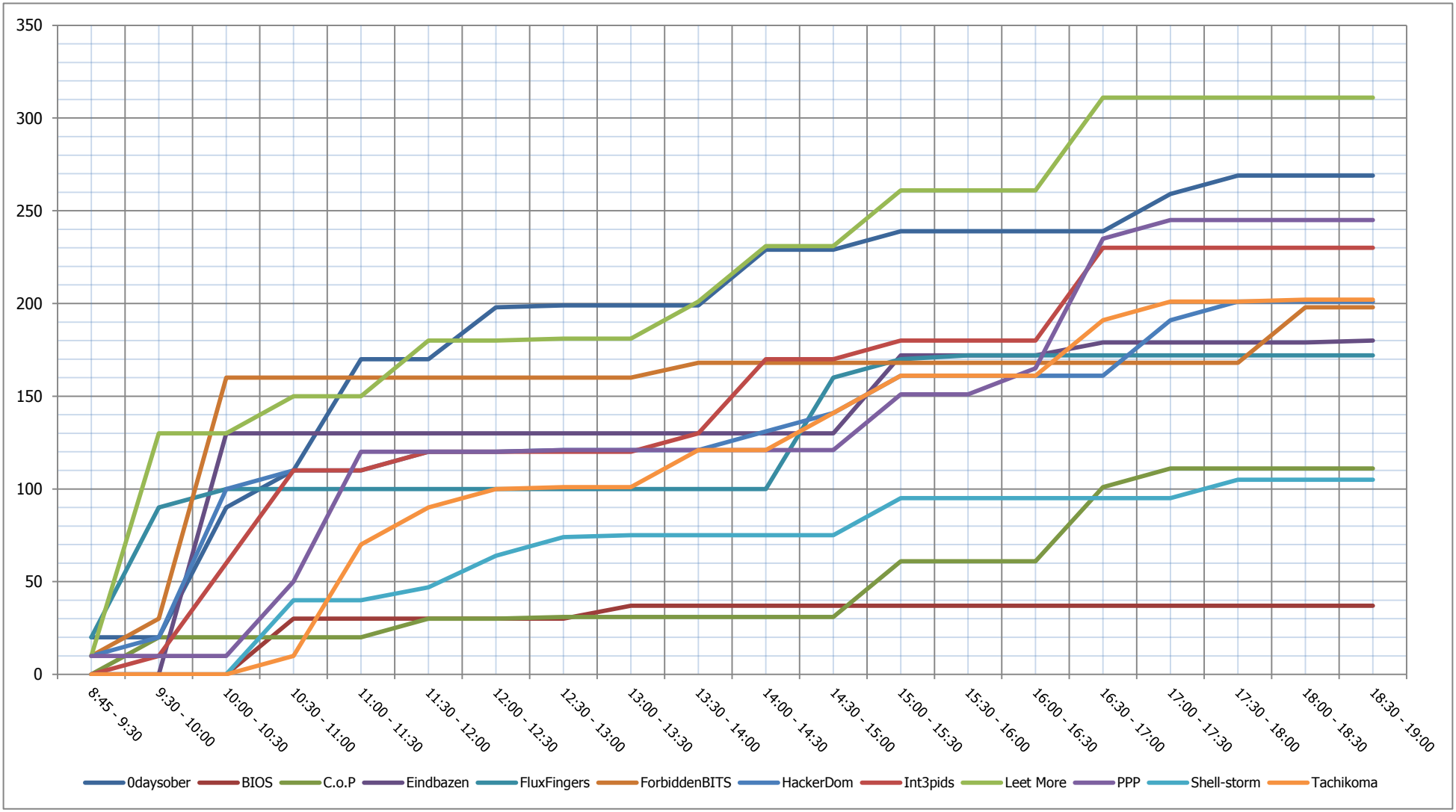


Figure 8. Score history for the team infrastructure tasks solved during the second day of the competition

6.1.2. Score dynamics

Score dynamics is provided in table 2 and in figures 9-11 separately for the first and second day of the competition and night tasks.

The diagrams show that the teams needed approximately an hour to understand the task and attack the competitors' systems on the first day. PPP were the fastest and the most active, and BIOS failed to score points in this type of tasks either on the first day or at night.

Int3pids were the most active at night — they earned more than 200 points capturing bonus flags of the competitors' services.

The second day made the teams less active. Leet More managed to take the lead by the end of the second day and hold the second position according to the team ratings in this contest type.

Team activity dynamics reflected on the diagrams shows that the majority of the teams coped with the tasks and captured flags on the contestants' services both during the day and at night. The activity of the teams until the last minutes of the competition evidences how fierce the contest was.

Photo 4. CTF hall

6.1.3. Analysis of the participants' actions

The analysis of the competition results showed that some teams tried to automate exploitation of the vulnerabilities detected in the competitors' services making use of the contest terms ensuring identical systems to the teams.

PPP from the USA was the first to score points as part for the team infrastructure. The participants managed to exploit the same vulnerability (task PHPWWW/ST0) on the services of all teams within practically 4 minutes, and 8 flags were entered into the system within 3 minutes. This fact suggests that the participants from the USA were not only the first to find the vulnerability, but to write a code automating its exploitation. Besides they did it before their contestants could secure their services. This fact is reflected in figures 6 and 9.

Log analysis showed that the members of PPP followed this tactics during the whole CTF — the flags were entered into the system with difference of no more than 2 seconds. Therefore, the number of points earned by a team as part of the team infrastructure directly depended on how quickly the competitors eliminated the vulnerabilities.

The same tactics was used by C.o.P. and Leet More.

BIOS and Tachikoma might input the flags manually. This technique did not allow the teams to earn many points, so they were the last ones in this part of the competition.

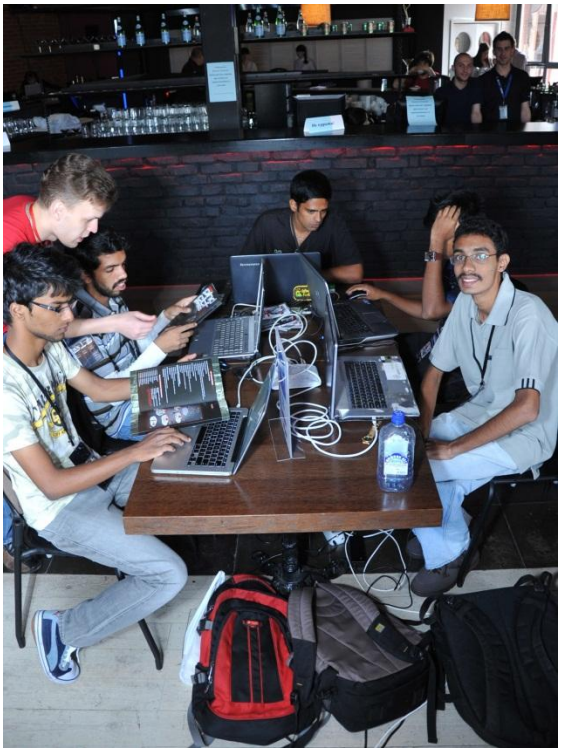


Photo 5. BIOS

The score dynamics diagrams including those provided in figures 9-11 allow tracing the teams' activity. Team scoring corresponds to the peaks of the diagrams.

It is difficult to draw an accurate conclusion regarding the other teams, because it took more than 15 minutes to input other flags. Within this time the teams could both input all detected flags manually and conduct attacks automatically. In some cases, judging by the same time interval between flag input and repeat of the sequence of the attacked teams, it can be supposed that practically all the teams tried to automate exploitation of the detected vulnerabilities.

The moments, when the teams implemented the automated technique for vulnerability exploitation on the services of the competitors, correspond to the diagram peaks standing out from the total score dynamics. These peaks are the result of the bigger number of points earned by a team for the least time comparing with other teams that have hardly input the found flags or have not solved a task yet.

The difference in the dynamics of the first and the second days is obvious. The attacks of the teams were more numerous during the first day: this suggests that the participants paid less attention to protection of their own services. According to the statistics, the majority of the teams managed to fix vulnerabilities in their infrastructures before their competitors could exploit them during the next day. Only at the beginning of the day the leaders managed to score a lot of points due to unfixed vulnerabilities of other teams.

Basing on the score history, it is difficult to conclude when exactly this or that team fixed a vulnerability in the infrastructure. It can be explained by the fact that the time, when points for the capture of flags from the service of a specific contestant team were deposited, varied by several hours. There were time intervals when the teams stopped losing flags being attacked by the competitors, and the vulnerability seemed fixed, but later some attacks were successfully conducted again. Relying on this fact, we suppose that the teams, which exploited the vulnerabilities manually, collected the flags at first and then input them one by one into the system. This tactics does not allow defining the accurate time when a task was solved and thus when a vulnerability was fixed.

Moreover, we suggest that the teams used different attacking algorithms, that is why some of them managed to bypass their contestant's protection mechanisms and some failed. Therefore, a service that was considered secure was targeted by the rivals again.

Table 2. Score dynamics for the team infrastructure tasks

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

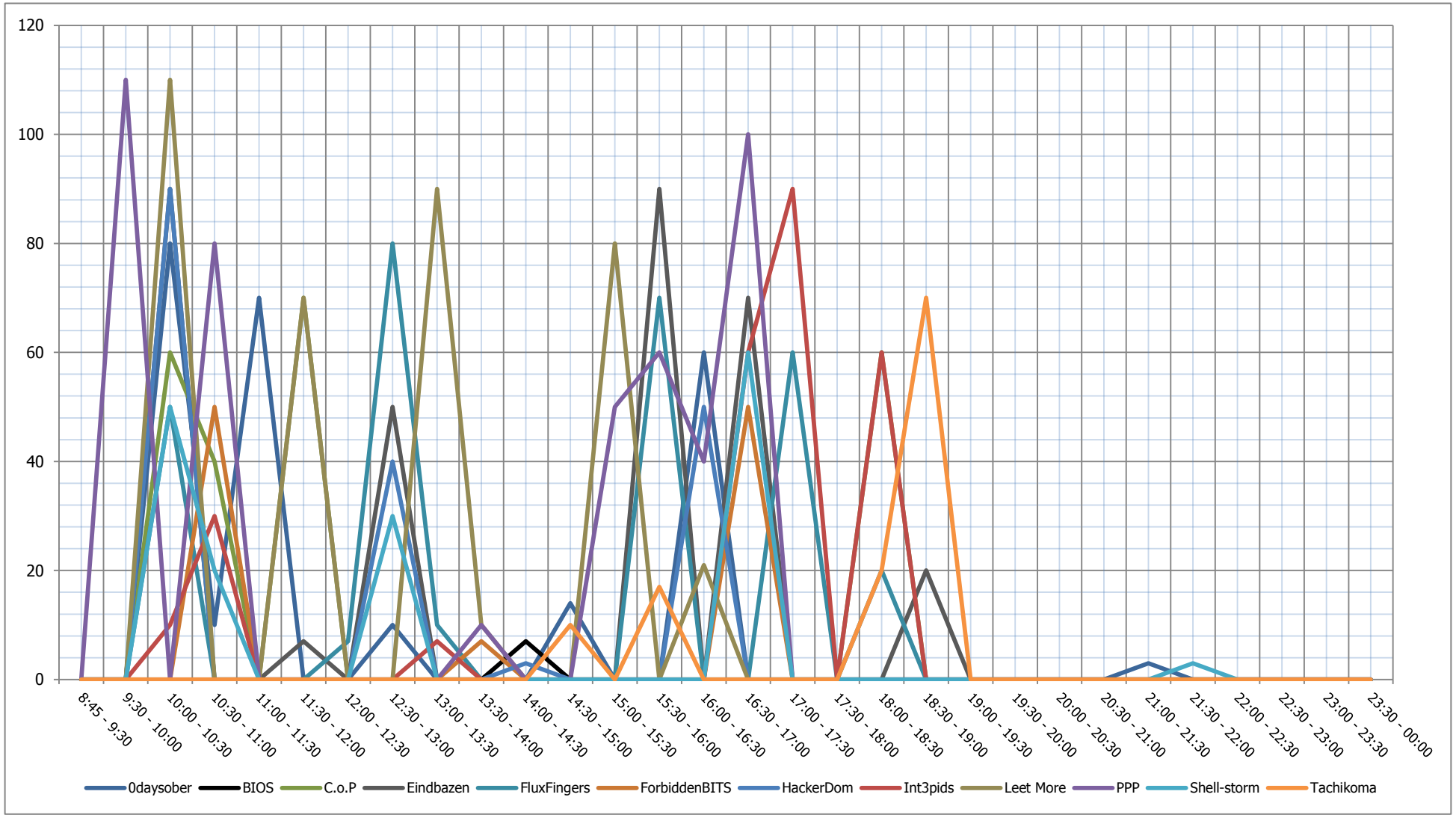


Figure 9. Score dynamics for the team infrastructure tasks solved during the first day of the competition

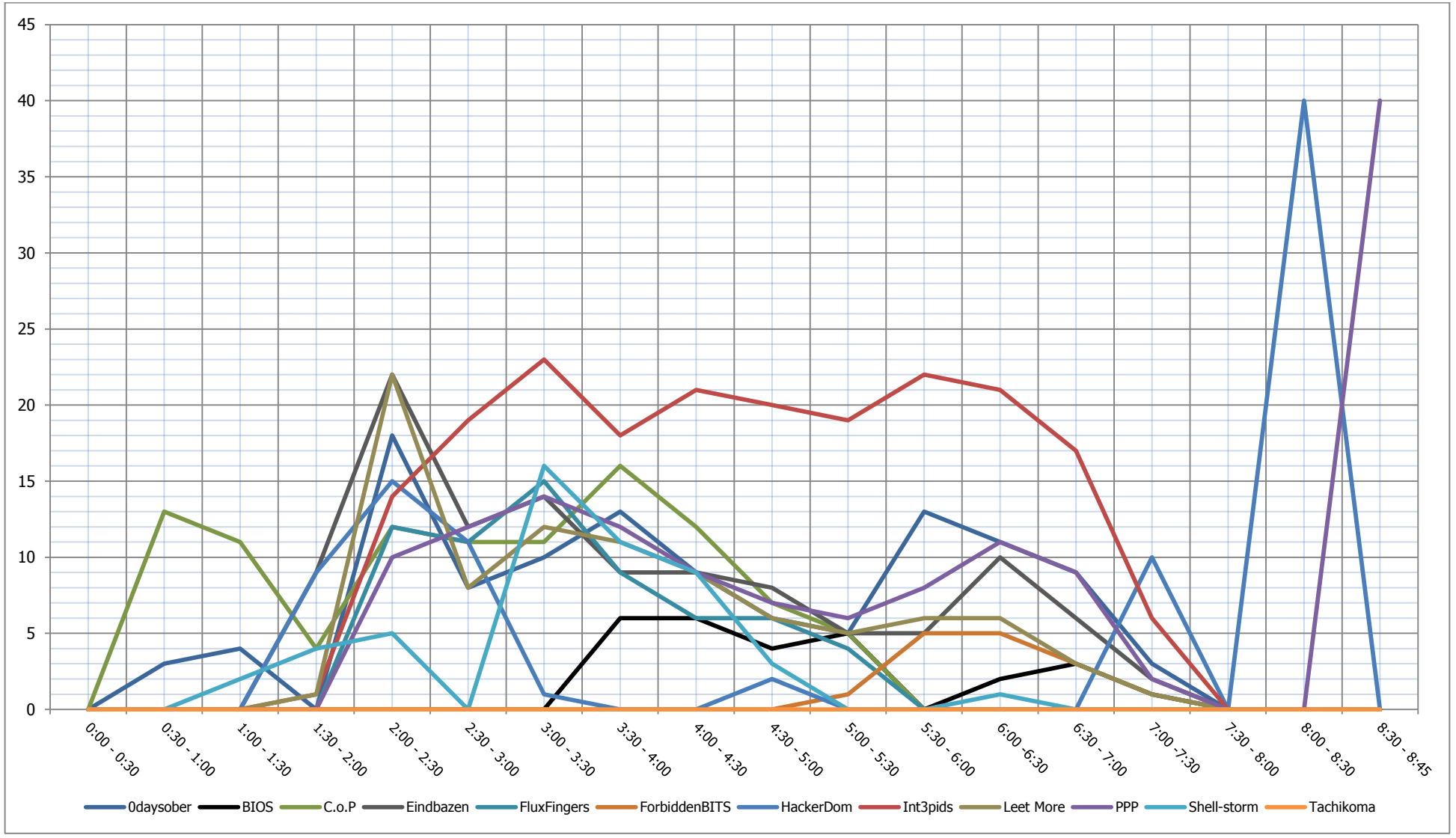


Figure 10. Score dynamics for the team infrastructure tasks solved at night

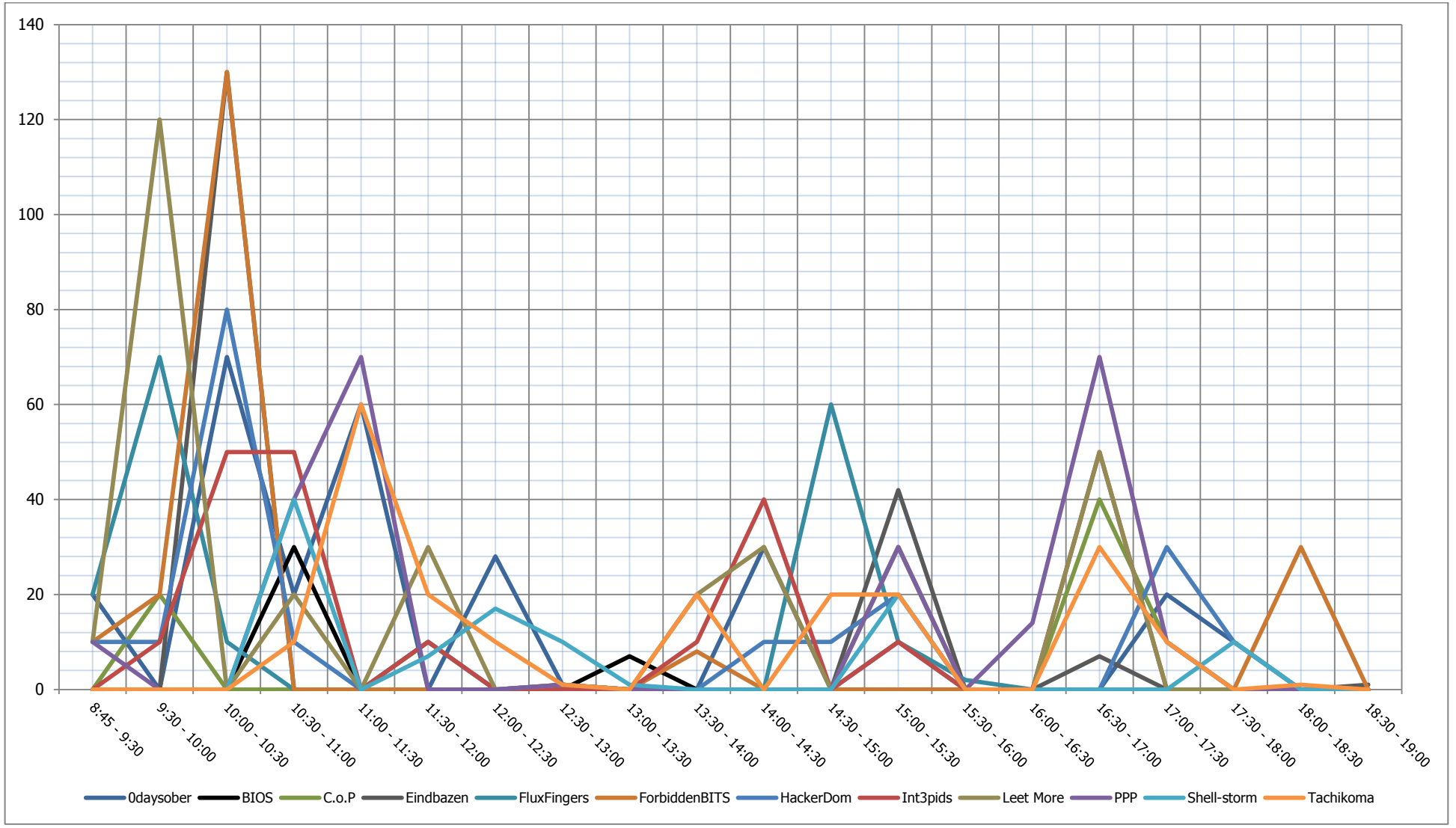


Figure 11. Score dynamics for the team infrastructure tasks solved during the second day of the competition

6.2. Point distribution for the shared infrastructure tasks

Figure 12 provides the data reflecting the number of points earned by the teams only by capturing flags on the vulnerable services of the shared infrastructure. For the purpose of this contest type, the winning places were distributed as follows: Int3pids were the leaders, C.o.P. held the second place, Eindbazen were the third.

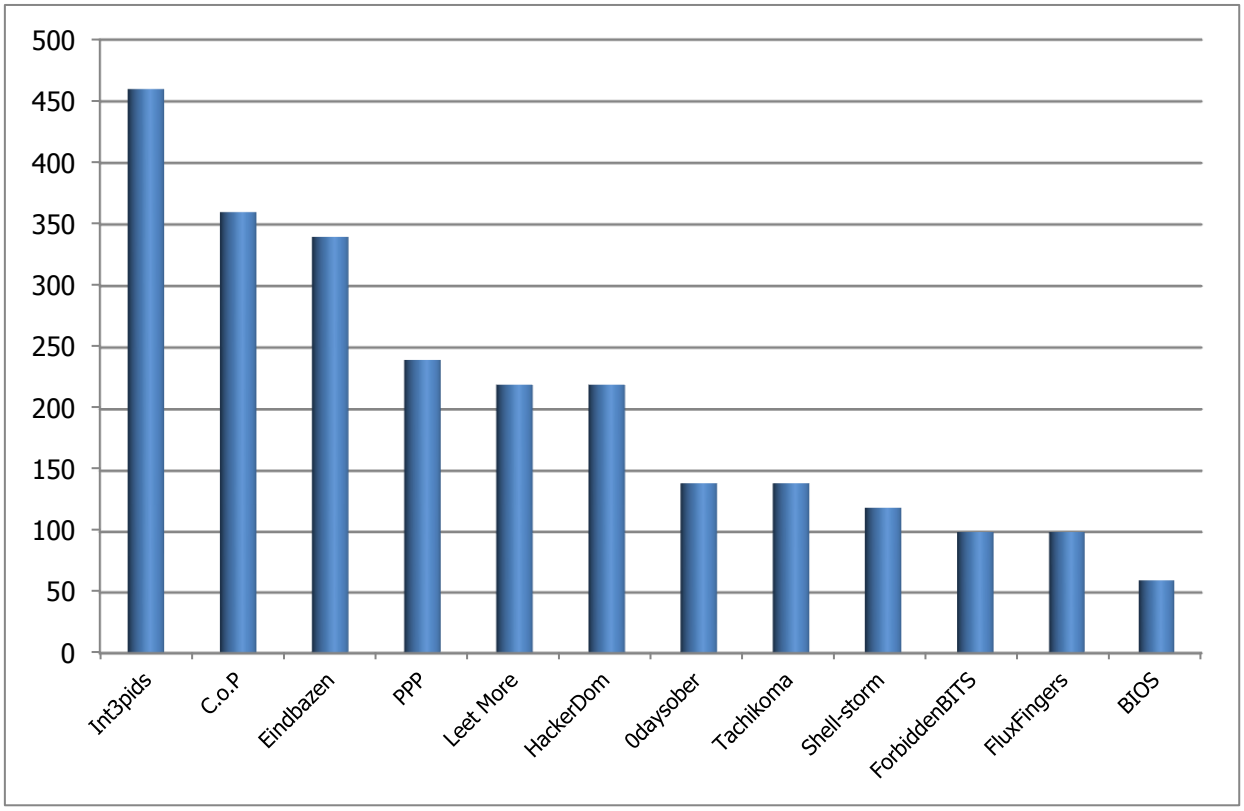


Figure 12. Points earned by the teams in the shared infrastructure tasks

6.2.1. Score history

Score history is provided in table 3 and in figures 13-15 separately for the first and second day of the competition and night tasks.

Table 3. Score history for the shared infrastructure tasks

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

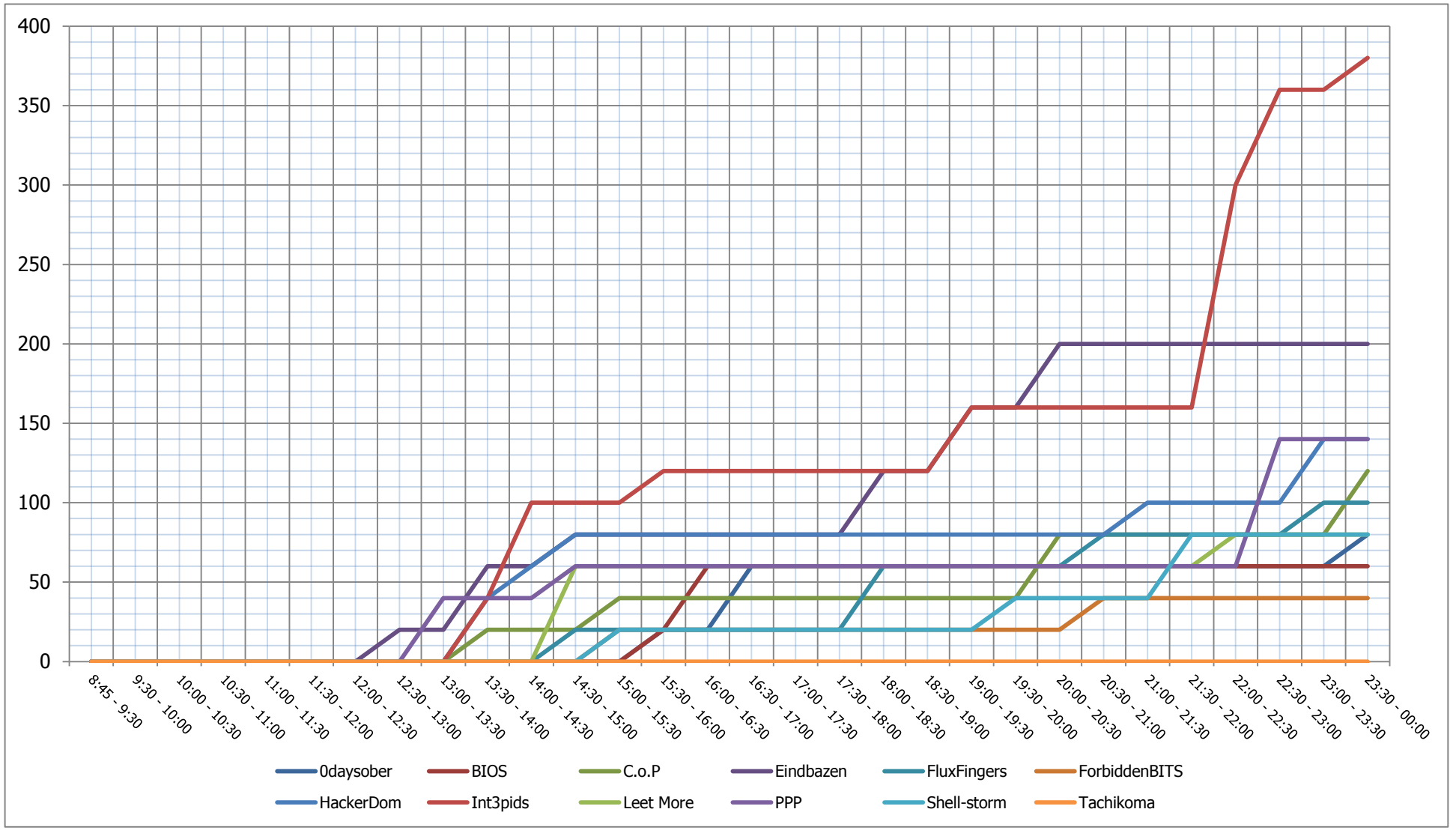


Figure 13. Score history for the shared infrastructure tasks solved during the first day of the competition

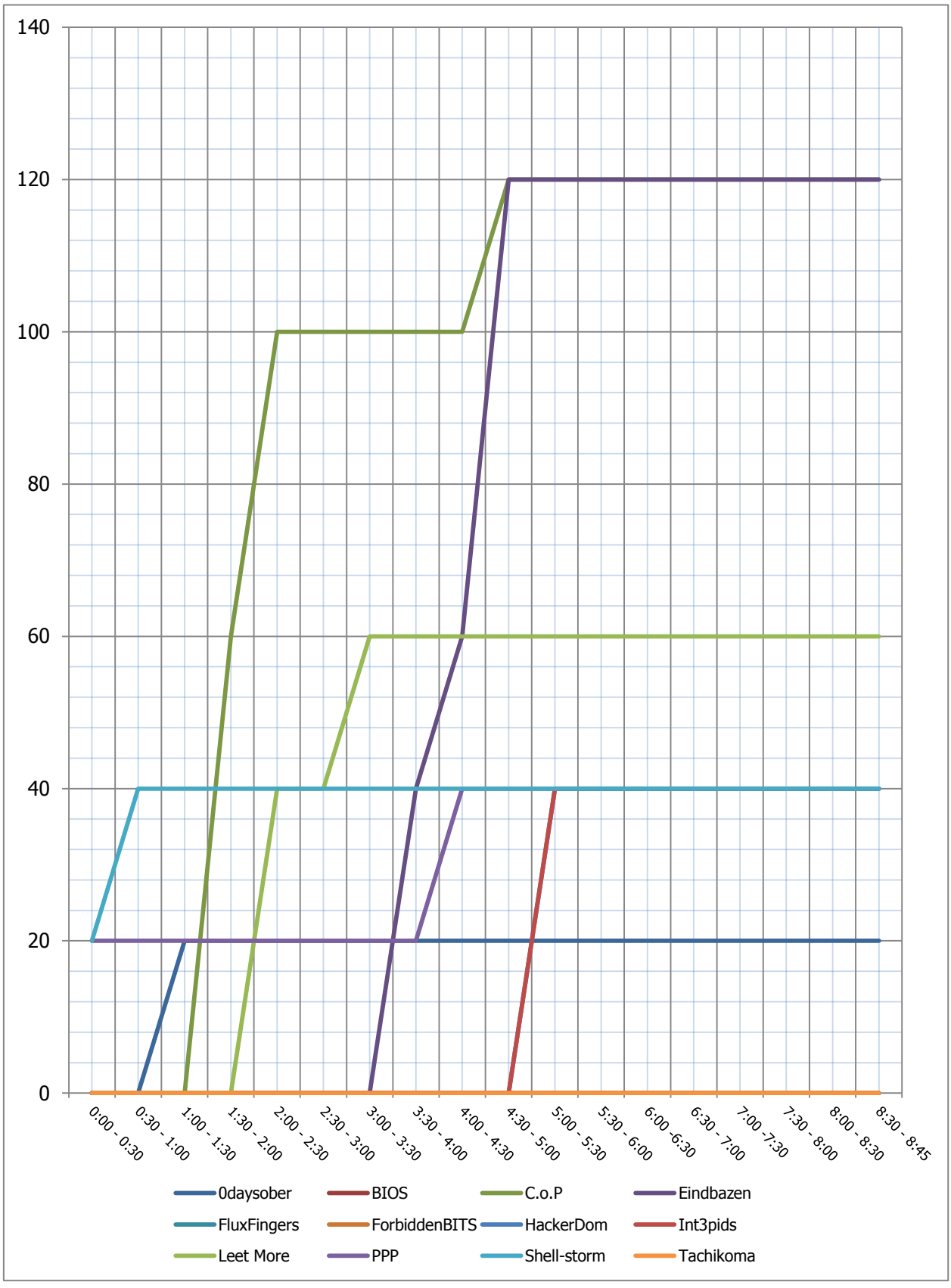


Figure 14. Score history for the shared infrastructure tasks solved at night

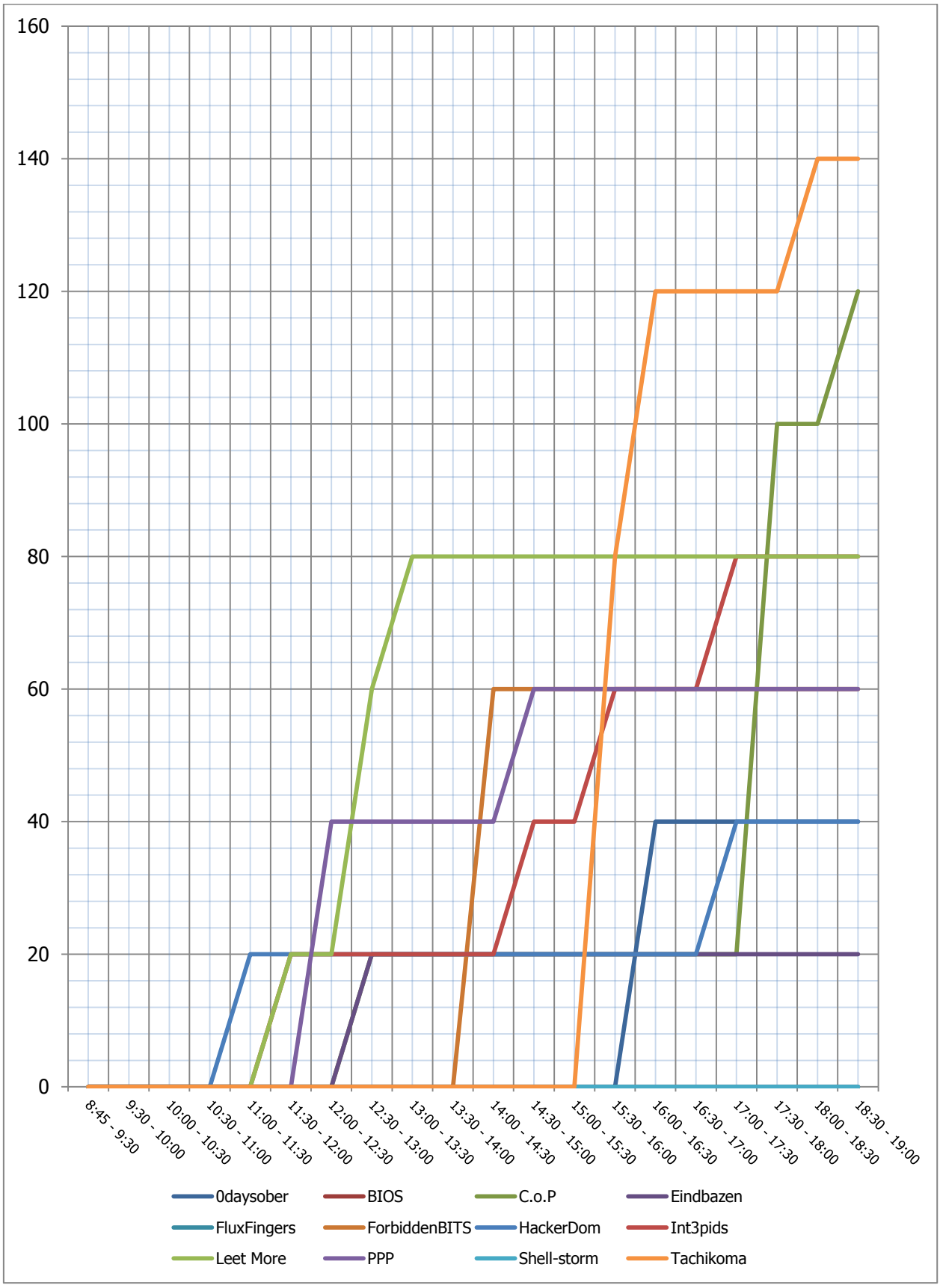


Figure 15. Score history for the shared infrastructure tasks solved during the second day of the competition

6.2.2. Score dynamics

Score dynamics is provided in table 4 and in figures 17-19 separately for the first and second day of the competition and night tasks.

The results of the tasks related to the shared infrastructure showed that the teams needed about three hours to understand the tasks and obtain the first results. There were three leaders among the teams and no outsiders: three teams were not able to score more than 100 points, and a half of the teams scored less than 150 points.

Int3pids held the leading position at the end of the first day with regard to this rating, and Tachikoma had no points at all. According to the first-day diagram, there were two succeeding teams. All teams scored no more than 60 points per an hour during this day on the average. Int3pids scored 200 points within an hour. They had to solve 10 tasks. PPP scored 80 points within half an hour having solved only one task (THECUBE). However, it did not help them to become the second by the end of the day — Eindbazen topped their score by 60 points earning their points quite evenly throughout the day. Bursts of team activity correspond to the diagram peaks (fig. 17).

Photo 6. Eindbazen members

The analysis of the tasks solved by the teams showed that Eindbazen managed to score such a big number of points within an hour due to the tasks with the same subject (ANDROID com.gia.bot). We suppose that the team included an expert of the necessary qualification — they managed to solve practically all the tasks of this type. Only PPP could solve the task THECUBE among all the CTF participants.

It is worth noting that the teams were spending their resources throughout the day, in particular on the team infrastructure tasks, and in the evening they had more time to deal with the shared infrastructure tasks, what Int3pids and PPP possibly made use of.

Photo 7. PPP members

The teams were not so active at night — only two of them scored more than 60 points throughout the night. It should be noted that almost the half of the teams scored no points of the shared infrastructure at night.

According to fig. 19 depicting score dynamics, the second day was less active. C.o.P. and Tachikoma stood out.

The second day showed that even outsiders (Tachikoma) could solve tasks of this type. The team from Japan became the second-day leader in the total score of the shared infrastructure tasks and left behind many competitors, besides they solved three tasks within an hour and scored 120 points. It is worth noting that the team did not earn a point in this type of tasks during the first day and the night.

The C.o.P. members solved only one task (crackme_Artefact) and earned 80 points. It was the only team among the CTF participants that coped with the task.

Bursts of team activity correspond to the diagram peaks (fig. 19).

All in all, this part of the competition provided 72 tasks of different challenge levels (and values). No team managed to solve 37 tasks (more than a half), less than a

half coped with 30 tasks (only one team solved 22 tasks), only 5 tasks were solved by the majority of the teams. The diagram provides the obtained statistics (fig. 16).

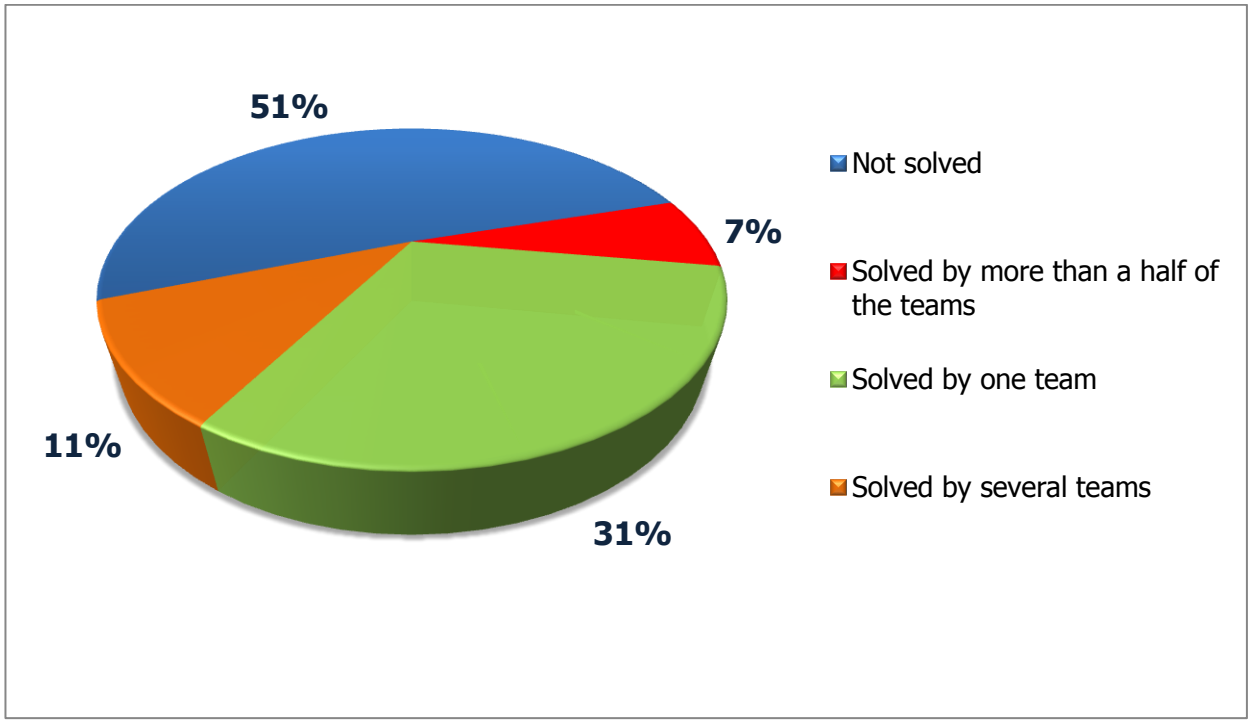


Figure 16. The statistics for the solved tasks of the shared infrastructure

Each team could earn up to 2,000 points solving all the tasks of the shared infrastructure. Therefore, all the teams could earn 24,000 points in total. According to the CTF results, all the teams jointly earned 2,500 points in the contests of the shared infrastructure (approximately 10% of the possible amount). Int3pids were the leaders in this part of the competition. They earned 460 points (23% of the possible amount).

Table 4. Score dynamics for the shared infrastructure tasks

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

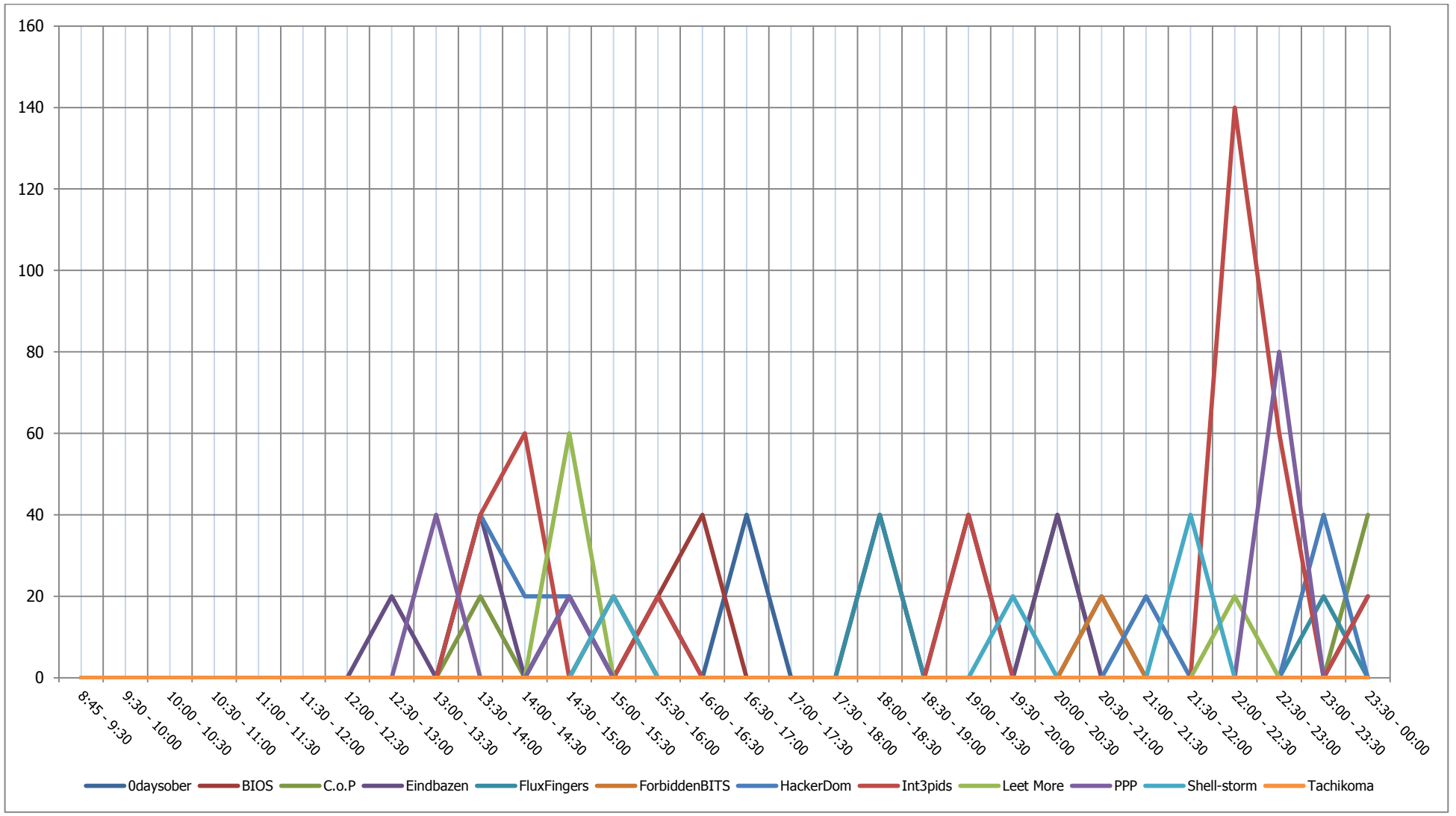


Figure 17. Score dynamics for the shared infrastructure tasks solved during the first day of the competition

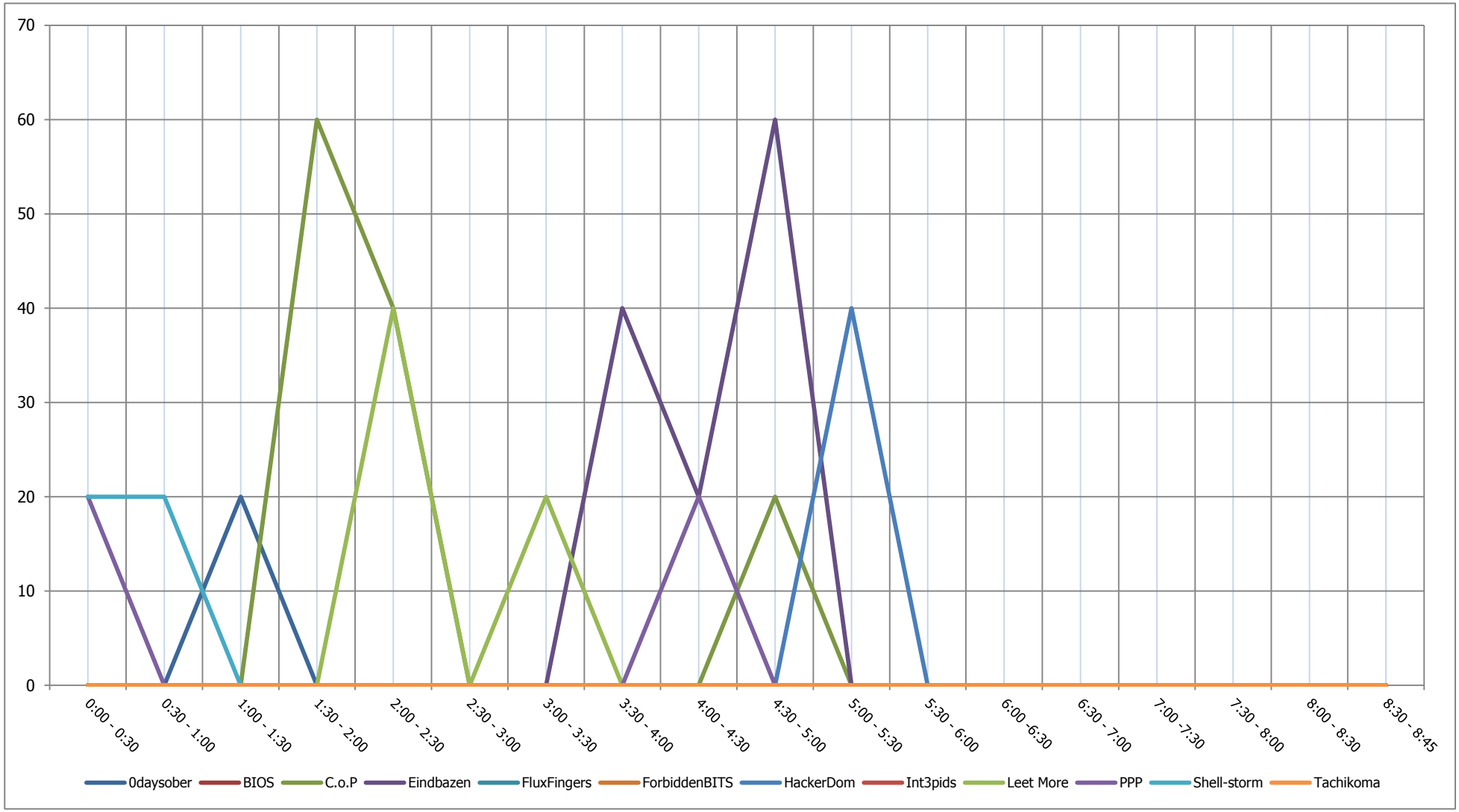


Figure 18. Score dynamics for the shared infrastructure tasks solved at night

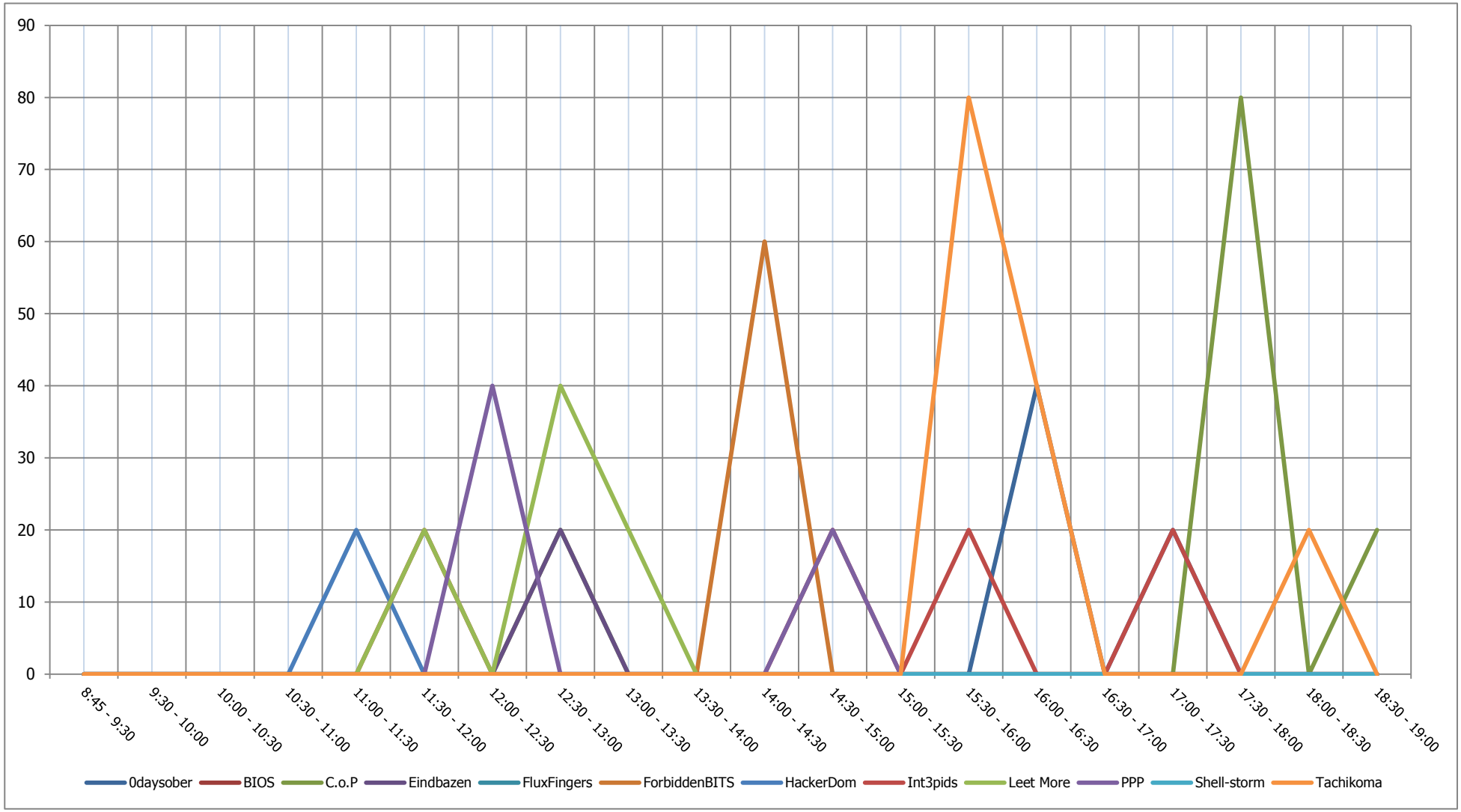


Figure 19. Score dynamics for the shared infrastructure tasks solved during the second day of the competition

6.2.3. Online HackQuest results

Beside CTF, PHDays 2012 also held online competition HackQuest for anyone from the Internet, who wanted to partake in the contests. The tasks coincided with the CTF tasks of the shared infrastructure, they basically differed in time and points scored for task solution. The Internet participants had access to the game services of the shared infrastructure during the period from May 30 to June 21, 2012.

Only 18 from the whole number of registered participants managed to earn points. All in all, 127 correct flags were registered.

According to the CTF results, only 88 correct flags were registered as part of the shared infrastructure. Taking into account the fact that the CTF participants had only two days to solve the tasks and that they needed to solve other CTF tasks, it can be concluded that the Internet participants were not able to cope with the tasks as well as the CTF participants.

Figure 20 provides the results of the online competition.

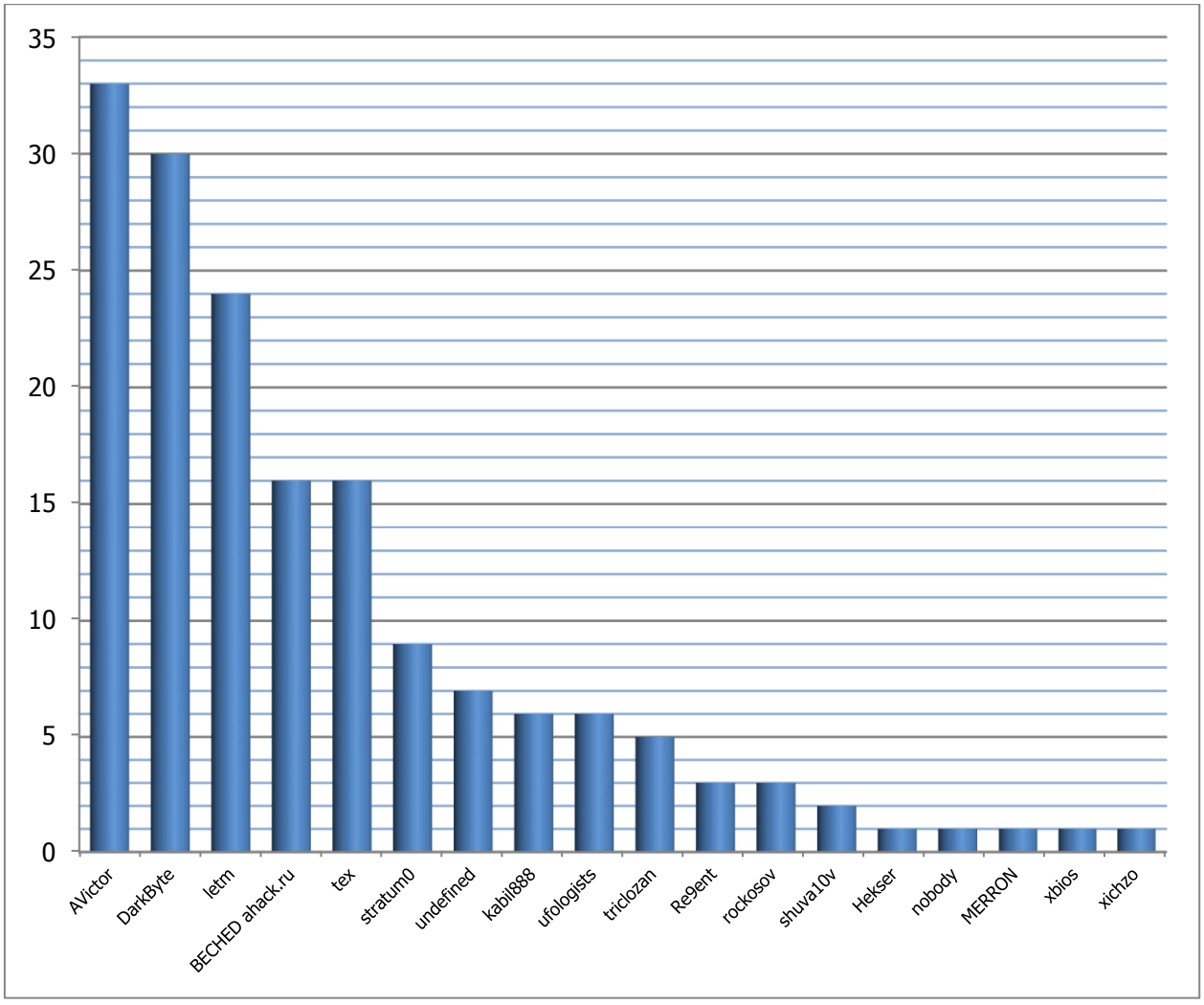


Figure 20. Online HackQuest results

Table 5 compares results by the number of solved tasks.

Table 5. Results comparison

PARAMETER	CTF TEAMS	INTERNET PARTICIPANTS
All tasks	72	
Not solved	37	37
Solved by the majority of the participants (teams)	5	2
Solved by a participant (team)	22	5
Solved by several participants (teams)	8	28

The diagram provides the obtained statistics of the online competition (fig. 21).

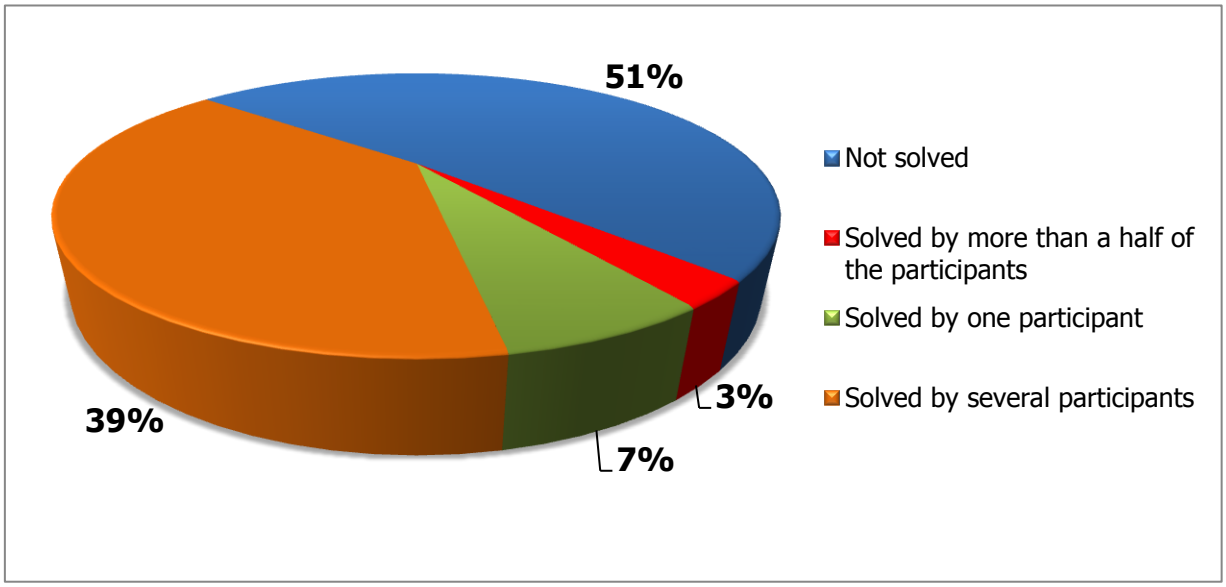


Figure 21. Statistics for the solved HackQuest tasks

Figure 22 provides the HackQuest score history.

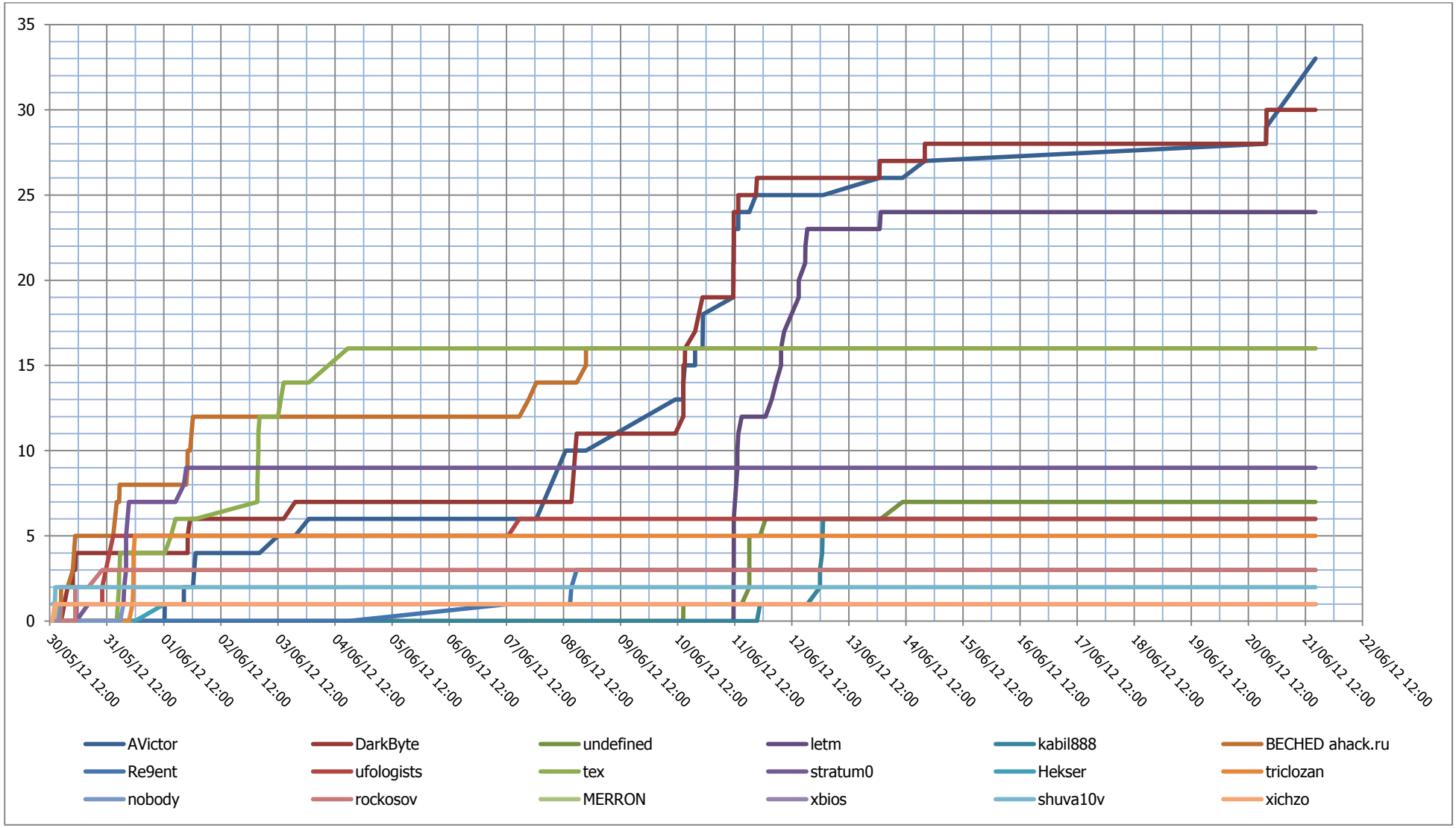


Figure 22. HackQuest score history

Joint statistics for the CTF and Internet participants are provided in the diagram (fig. 23) and table 6.

Table 6. Joint statistics for the shared infrastructure tasks

ALL TASKS	72
Not solved	22
Solved only by the CTF teams	16
Solved only by the HackQuest participants	15
Solved by both groups of the participants	19

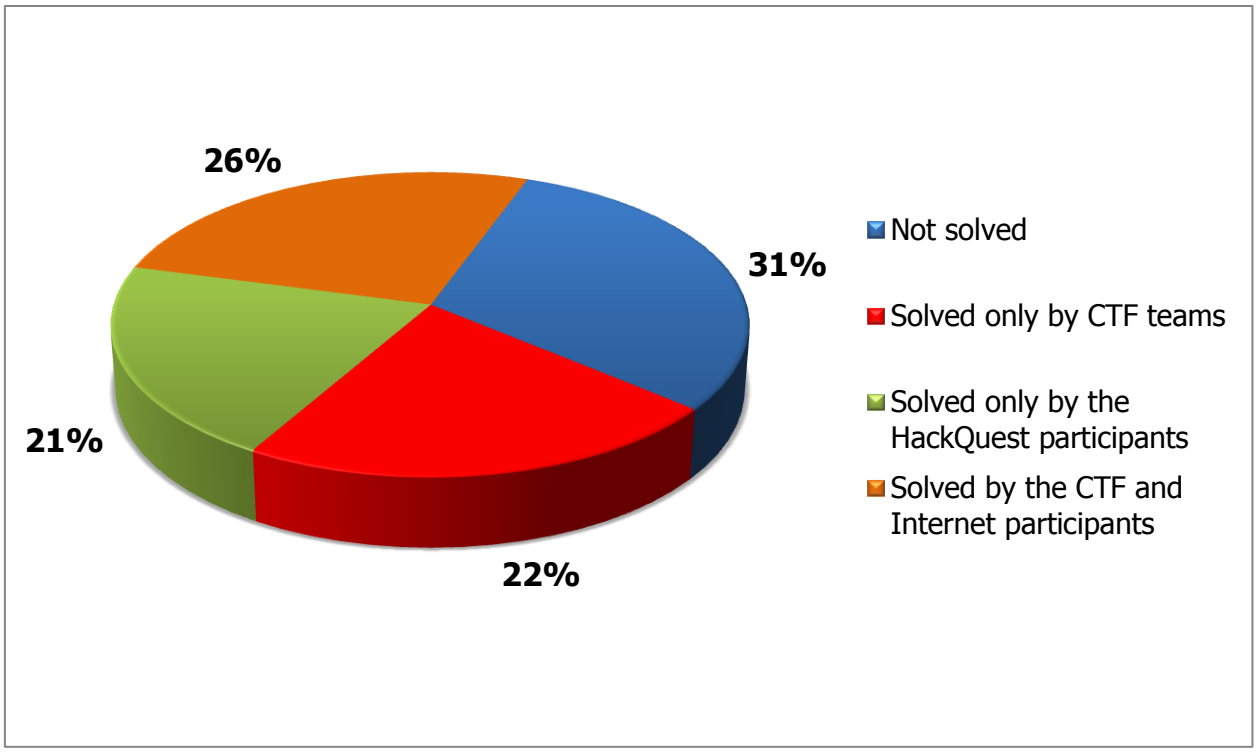


Figure 23. Joint statistics for the shared infrastructure tasks

This statistics showed that the third part of the tasks was not solved either by the Internet or CTF participants. Another third part was solved by both groups of the participants. The big number of unaccomplished tasks evidences the high level of the competition and encourages future participants to improve their professional skills and knowledge.

6.3. Point distribution for the King of the Hill contest

6.3.1. Point distribution among the CTF teams

Score history as part of the King of the Hill contest is provided in table 7 and in figure 24.

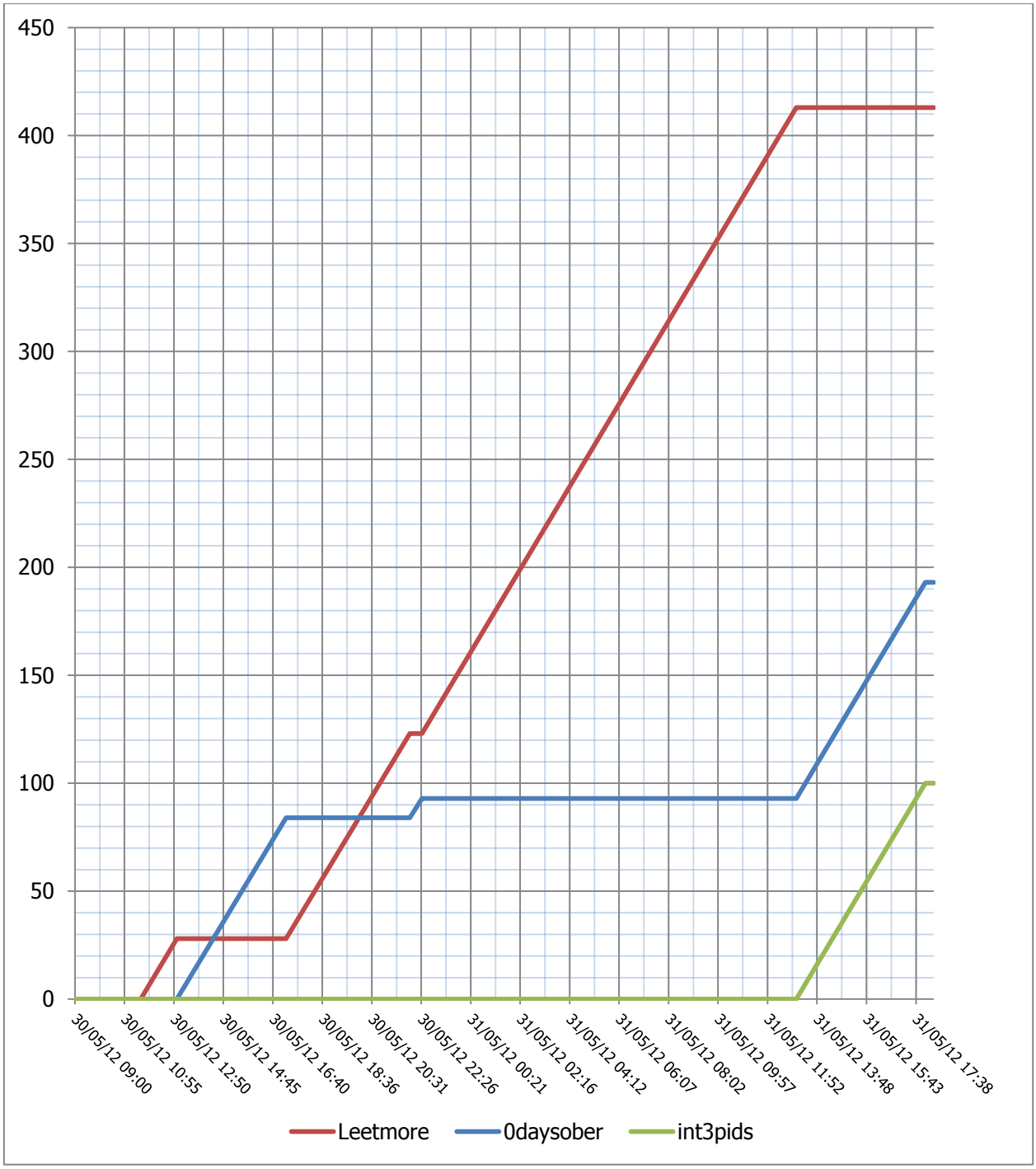


Figure 24. Score history for the King of the Hill contest

Table 7. Score history for the King of the Hill contest

Team	Time interval	Game service	Duration	Scored points	Current points
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

According to the results provided in table 7, all three teams coped with the first-level tasks of the King of the Hill infrastructure.

Photo 8. 0daysober members

Statistics show that only 0daysober solved the task of 1vulnerableService. The teams had been fighting to control the service 1vulnerableWeb for two days.

Leet More managed to earn the largest number of points (413). They'd been keeping control over the service for more than fourteen hours. Points earned by Leet

More in this contest turned the competition around and finally handed the win to the team.

rank	team	attack	kings!	bonuses	def.	avail.	total
1	Leet More	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	0daysober	582	L1: 864 L2: 0	186	30	0	1602
3	Int3pids	681	L1: 329 L2: 0	467	30	0	[illegible]
4	Plaid Parliament of Pwning	780	L1: 0 L2: 0	295	30	4	1041
5	eindbazen	556	L1: 0 L2: 0	401	30	0	927
6	C.o.P	442	L1: 0 L2: 0	341	30	0	753
7	HackerDom	427	L1: 0 L2: 0	265	30	0	662
8	FluxFingers	523	L1: 0 L2: 0	109	30	0	602
9	Tachikoma	311	L1: 0 L2: 0	148	30	0	429
10	Shell-storm	301	L1: 0 L2: 0	138	30	0	409
11	ForbiddenBITS	305	L1: 0 L2: 0	115	30	0	390
12	BIOS	57	L1: 0 L2: 0	74	30	0	101

Photo 9. Competition results displayed on the video wall in the CTF hall

No team participated in the competition was able to access services of the second level, for control of which they could earn twice as many points as for the services of the first level in accordance with the rules.

6.3.2. Point distribution among the online participants of the King of the Hill contest

Total results of the online competition

When PHDays CTF 2012 was over, all the registered Internet participants were provided with access to the King of the Hill infrastructure. The online contest was held from August 20 to September 3, 2012. 200 participants were registered, and only seven of them managed to earn points.

Their points were calculated in a different way. A point was scored for each complete minute of control over the service (both the first-level and the second-level services). If the scores were even, the control over the second-level service prevailed.

Point distribution as part of the online competition is provided in table 8 and figure 25. The score history is provided in table 9 and figure 26.

Table 8. Point distribution for the King of the Hill contest held online

Place	Participant	1-level services		2-level service	Total score
		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

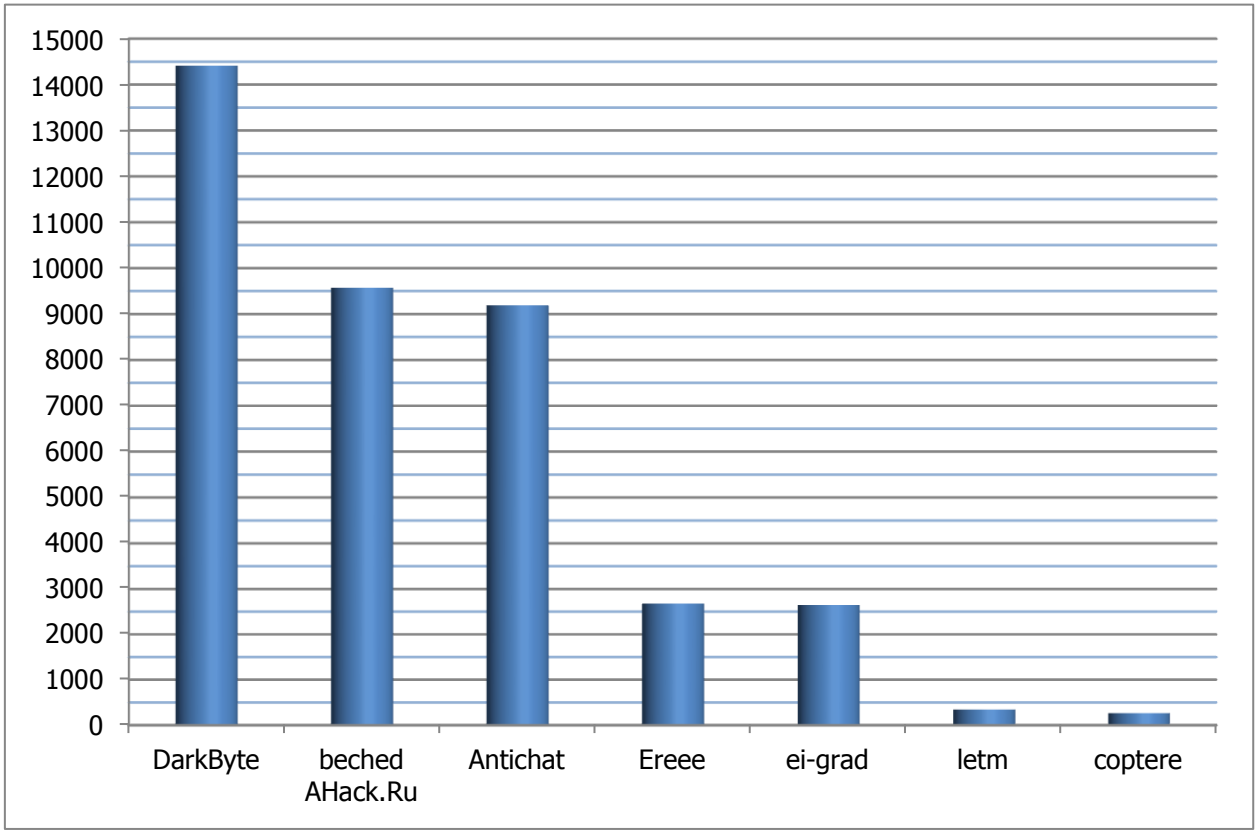


Figure 25. Point distribution for the King of the Hill contest held online

Table 9. Point distribution for the King of the Hill contest held online

TIME	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
25.08.12 22:58	4350	464	264	3080	340	2648	88
25.08.12 23:12	4350	464	264	3093	340	2648	88

TIME	BECHED AHACK.RU	EREEE	COPTERE	ANTICHAT	LETM	EI-GRAD	DARKBYTE
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
31.08.12 20:46	8980	780	264	7940	340	2648	7417
31.08.12 22:43	8980	897	264	7940	340	2648	7417

TIME	BECHED AHACK.RU	EREEE	COPTERE	ANTICHAT	LETM	EI-GRAD	DARKBYTE
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

Note. Yellow means the current 1st place, green — the current 2nd place, blue — the current 3rd place. The table cell put into a frame corresponds to the time when the points were scored for control over the second-level service.

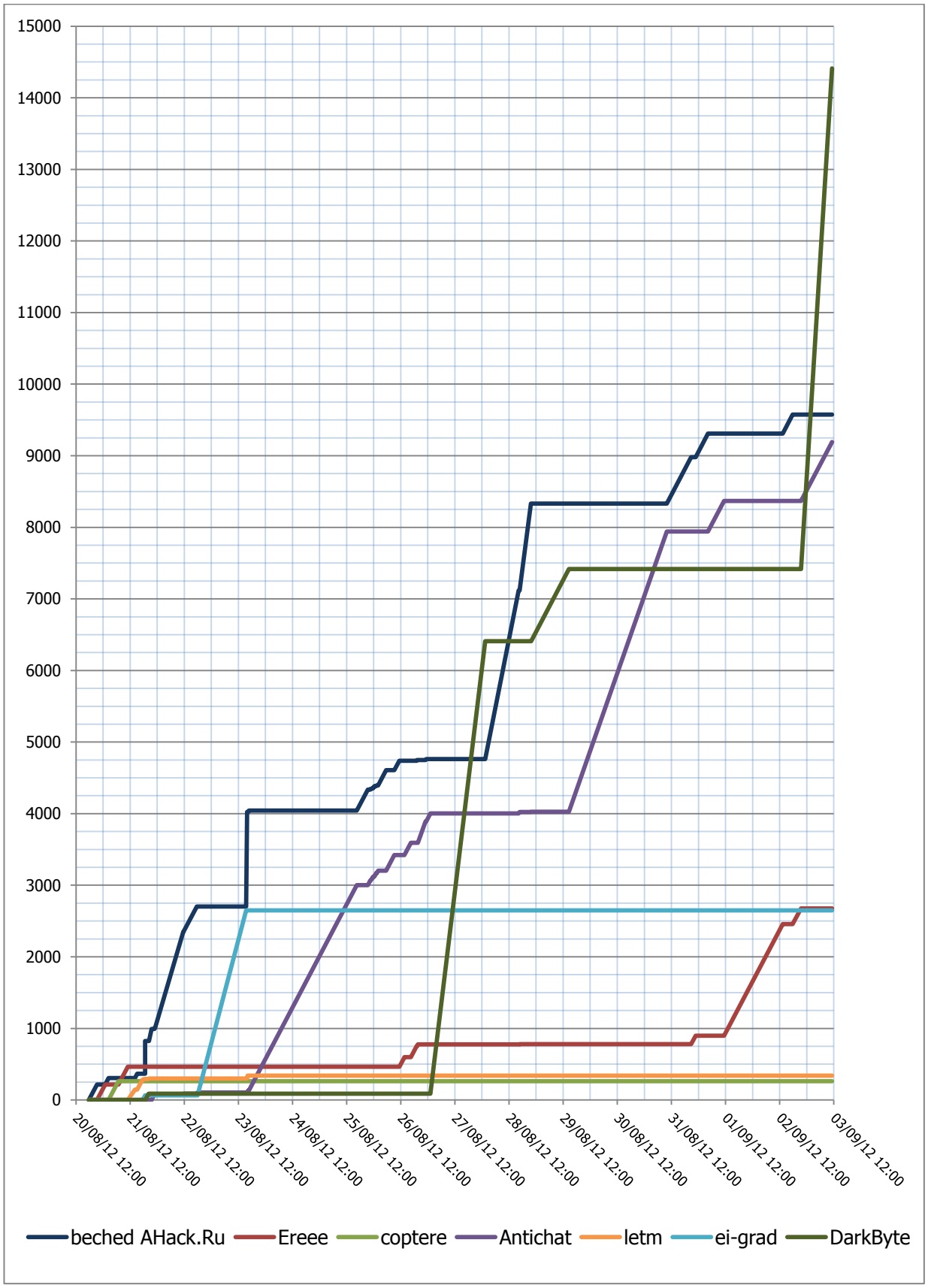


Figure 26. Score history for the King of the Hill contest held online

A participant under the assumed name of DarckByte managed to score the biggest number of points in the King of the Hill contest, but failed to become a winner. The only participant, who was able to control the second-level service, earned less points but took the first place. His contestants could not obtain control over the service Active Directory.

According to the obtained data, the Internet participants dealt much better with this task than the CTF teams. It can be explained by the fact that the CTF teams were constrained by time and spent their resources on other tasks throughout the whole competition.

Online competition results (first-level service WWW)

Only 4 of 7 participants coped with the tasks of the first level "WWW" as part of the online contest King of the Hill. A participant under the pseudonym Antichat took the leading position in this part of the competition.

The results are provided in figure 27, the score history is displayed in figure 28.

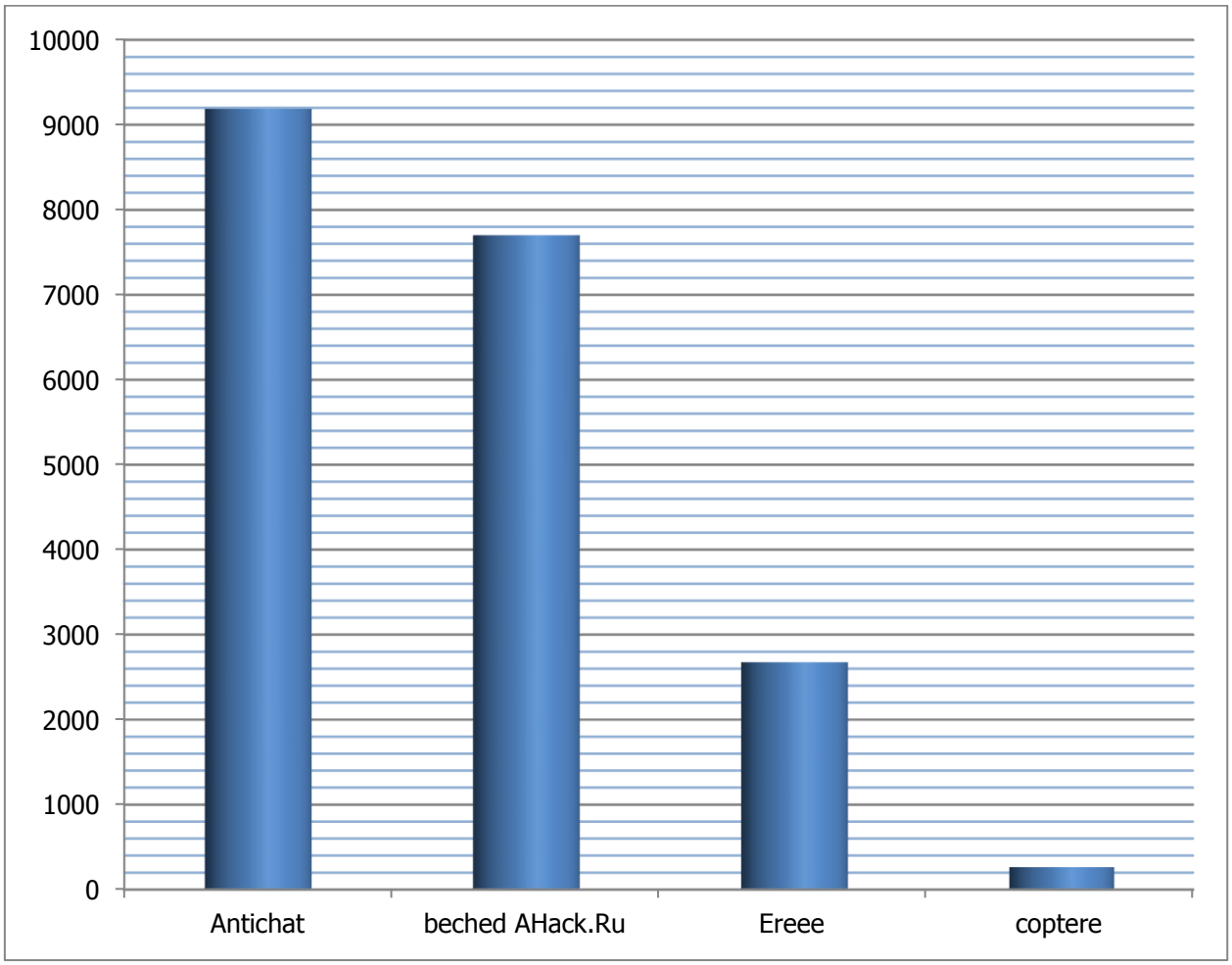


Figure 27. Results of the King of the Hill contest held online (first-level service WWW)

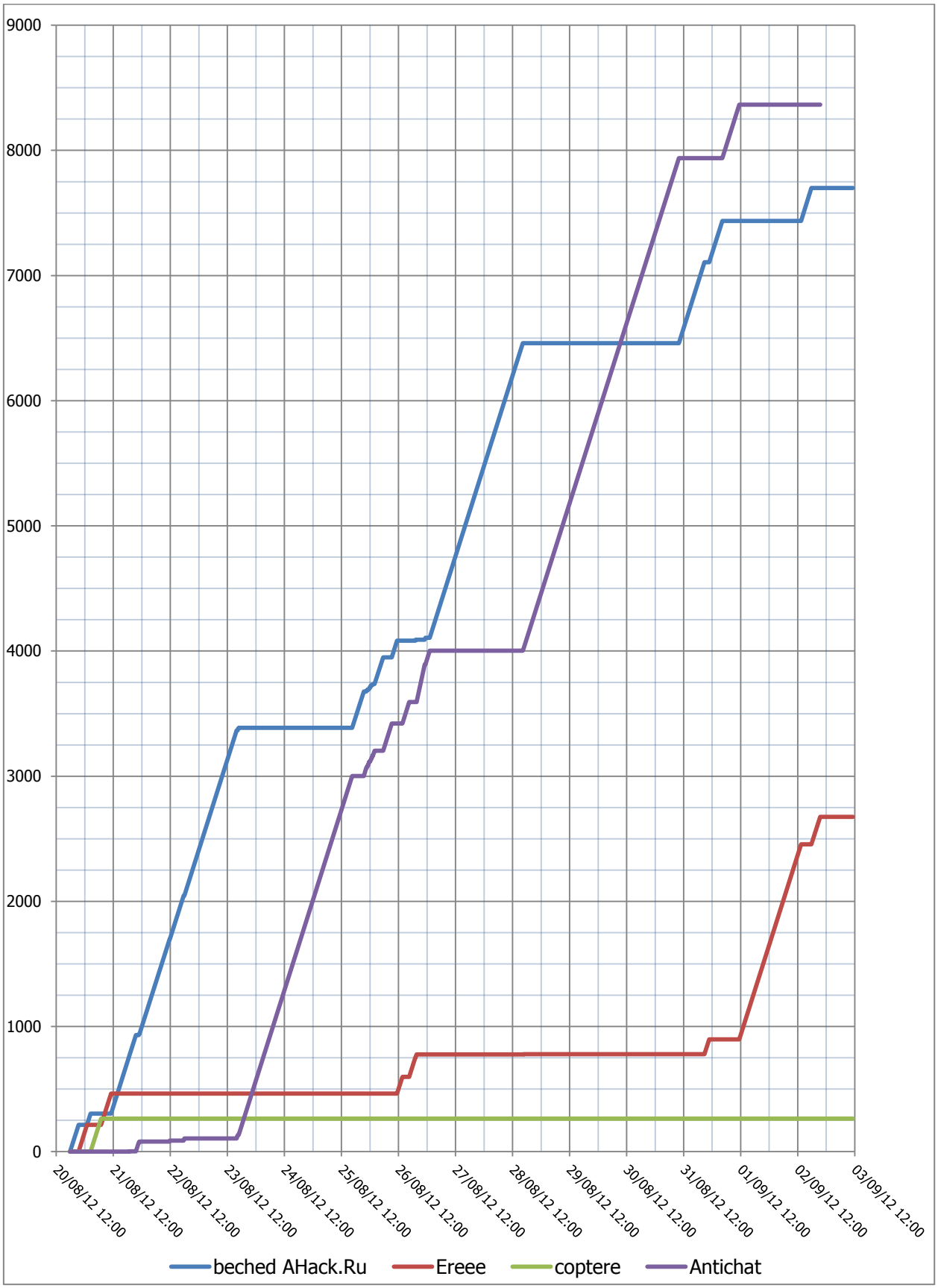


Figure 28. Score history with regard to the control over the first-level service WWW

Online competition results (first-level service Services)

Only 5 of 7 participants coped with the tasks of the first level "Services" as part of the online contest King of the Hill. DarkByte won by a wide margin in this category. Having lost control over the service, he managed to win it back and keep it until the end of the competition.

The results are provided in figure 29, the score history is displayed in figure 30.

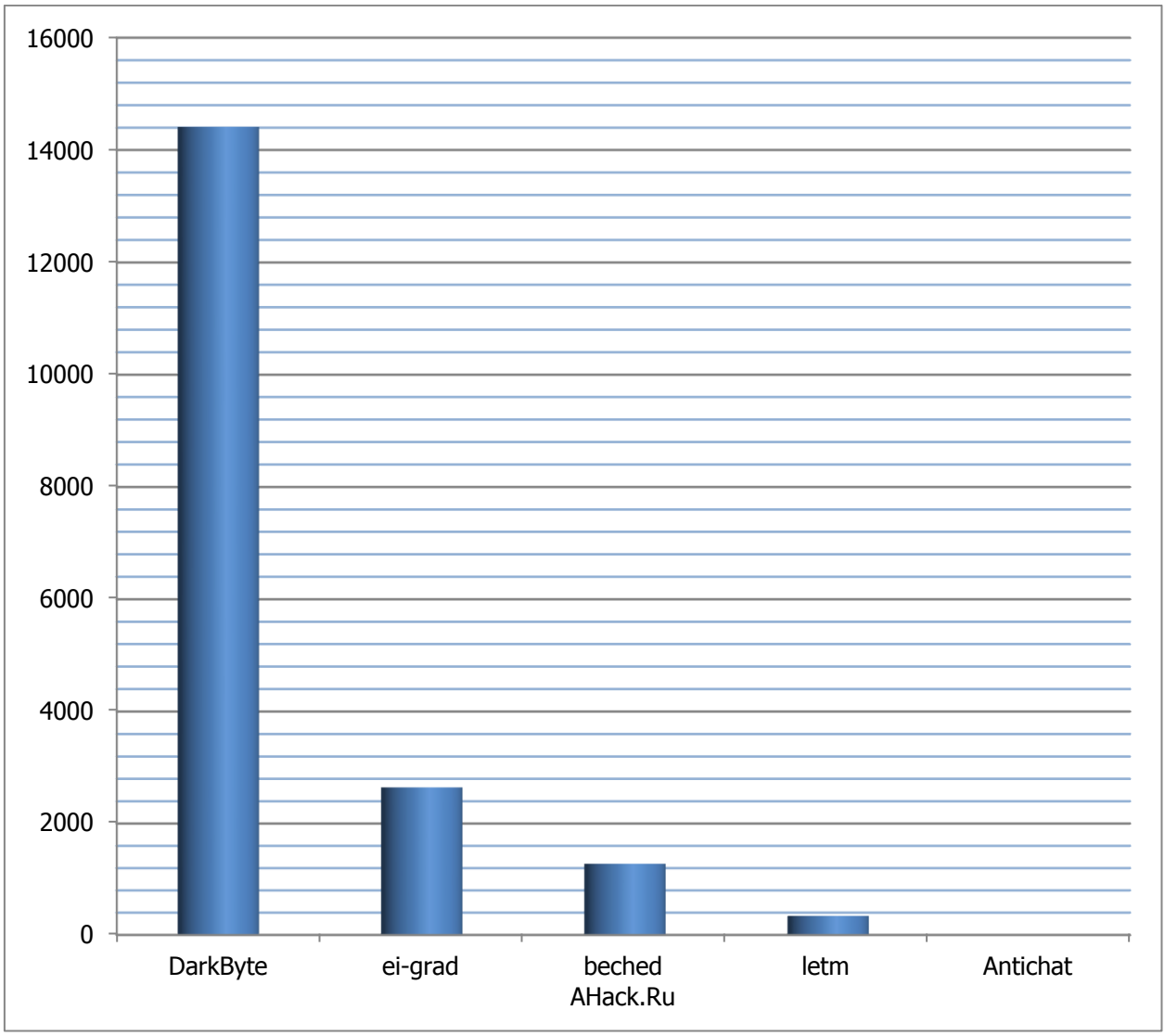


Figure 29. Results of the King of the Hill contest held online (first-level service Services)

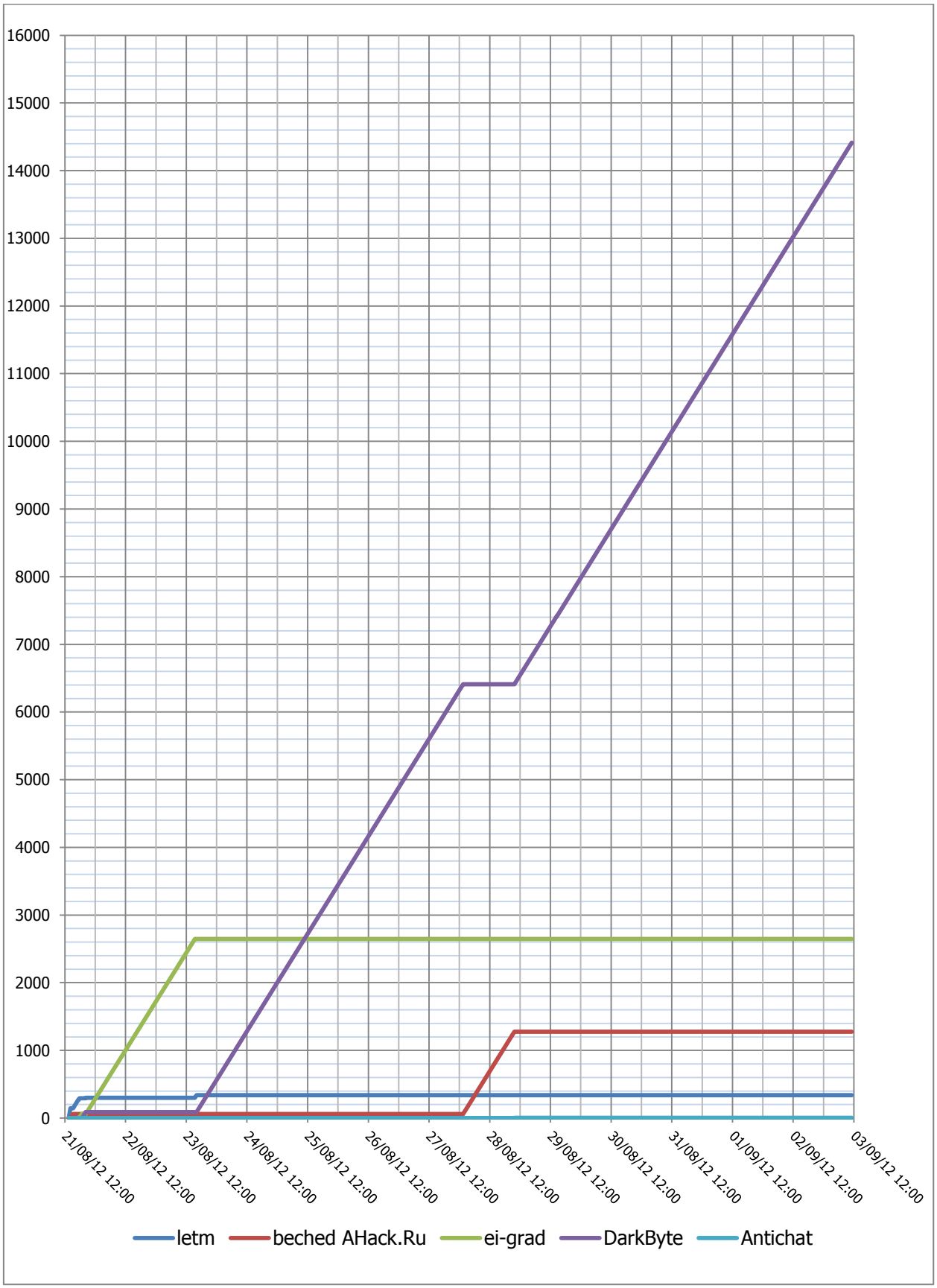
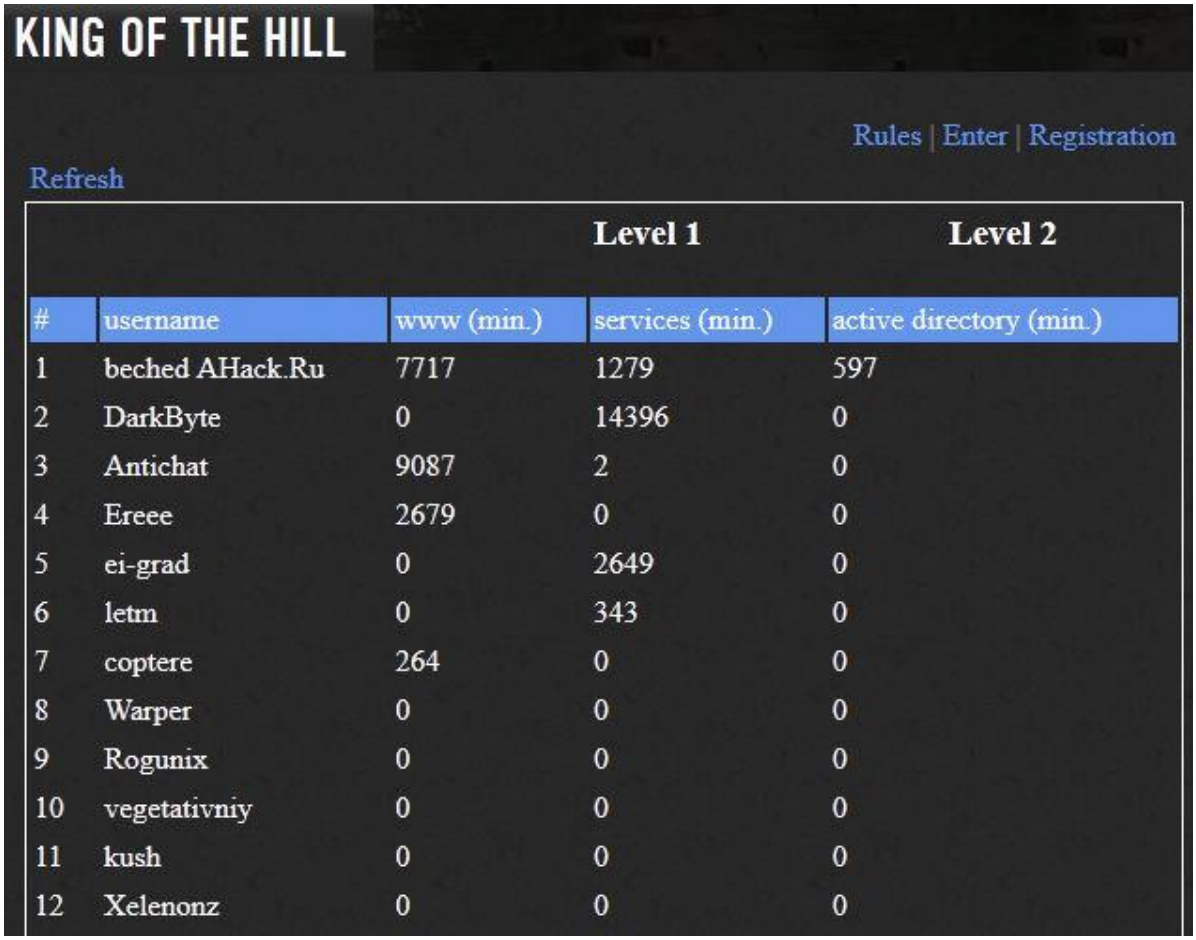


Figure 30. Score history with regard to the control over the first-level service Services

Online competition results (second-level service Active Directory)

In contrast to the CTF teams, one of the Internet participants managed to obtain control over the second-level service. Named as beched AHack.Ru, he had been controlling the second-level service for about 10 hours and earned 597 points. No one could achieve such a success. The battle concentrated on the first-level services of the King of the Hill infrastructure.

The points, which beched AHack.Ru earned for the control over Active Directory, allowed him to top the overall standings and win the online competition.



		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

Photo 10. Results of the King of the Hill contest held online on the official website PHDays 2012

All the results of the online competition King of the Hill are provided on the official website PHDays 2012 (http://phdays.com/ctf/king/a.php).

6.4. Point distribution for the bonus tasks

Sergey Azovskov from HackerDom and Matt Dickoff from PPP became the winners of the bonus competition, in which they had to take over an AR.Drone. The teams received 150 extra points to their total score and each of the winners was awarded with the quadcopter AR.Drone.

Photo 11. Matt Dickoff from PPP, the winner of the bonus competition

The teams earned bonus points during two days of the competition rooting through a paper dumpster, looking for the necessary information and capturing the team service flags of the contestants at night.

Figure 31 and table 10 display bonus point distribution among the teams. PPP, HackerDom, and Int3pids earned the largest number of the bonus points. Int3pids scored more than 200 points collecting only bonus flags and failing to take over the AR.Drone.

Photo 12. The HackerDom members in the paper dumpster

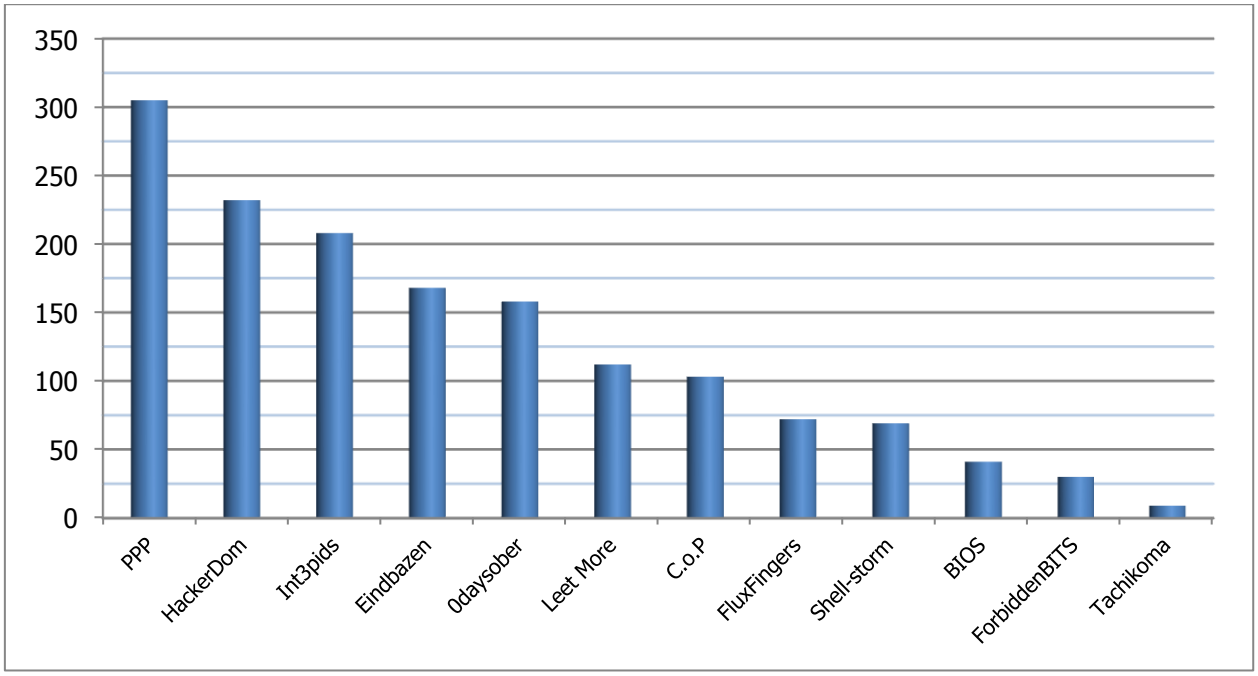


Figure 31. Bonus point distribution among the teams

Table 10. Bonus point distribution among the teams

Team	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Bonus tasks	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
Night flags	112	27	103	106	63	15	37	201	90	100	51	1

6.5. Total statistics and CTF results

6.5.1. Total score history

The score history related to all the task types of PHDays CTF 2012 is provided in table 11 and figures 32-34. These statistics specify the points earned by the teams (disregarding penalty).

According to table 11, there were four leading teams, three of which kept on struggling for a higher position in the top three up to the last minutes of the competition. 0daysober and Eindbazen were the closest to the leaders. BIOS remained an outsider during the whole CTF. The total team result is 10 times worse than the results of the teams from the top three.

According to the statistics, Int3pids holding the leading position by the end of the first day, throughout the night until the next morning then lost this position and finally took the second place in the overall standings.

Ending the morning of the second day on the third place in the total rating, Eindbazen then gave way to the leaders.

Photo 13. Int3pids on the awarding ceremony

Table 11. CTF total score history

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

Note. Yellow means the current 1st place, green — the current 2nd place, blue — the current 3rd place.

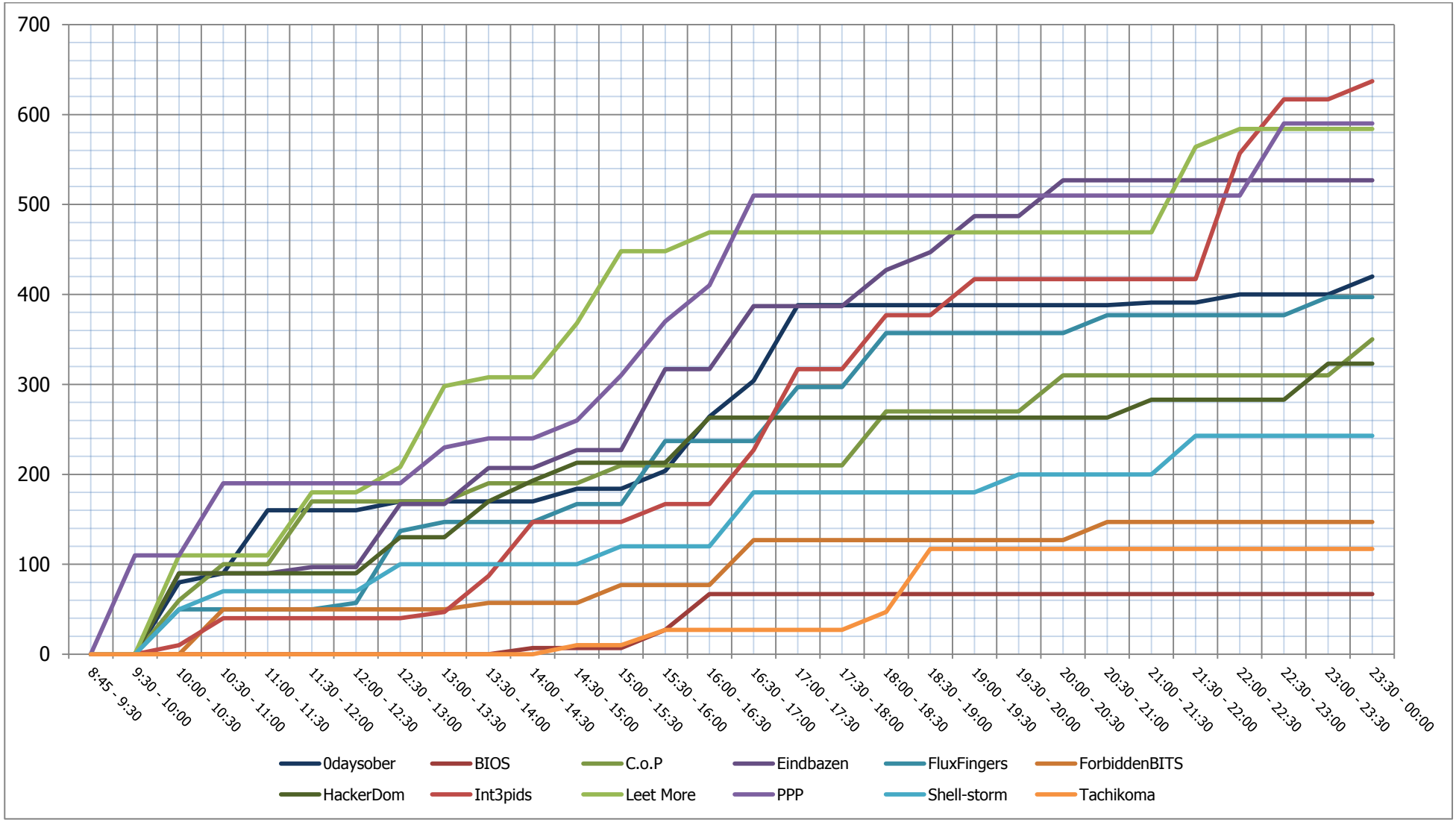


Figure 32. CTF overall score history for the 1st day

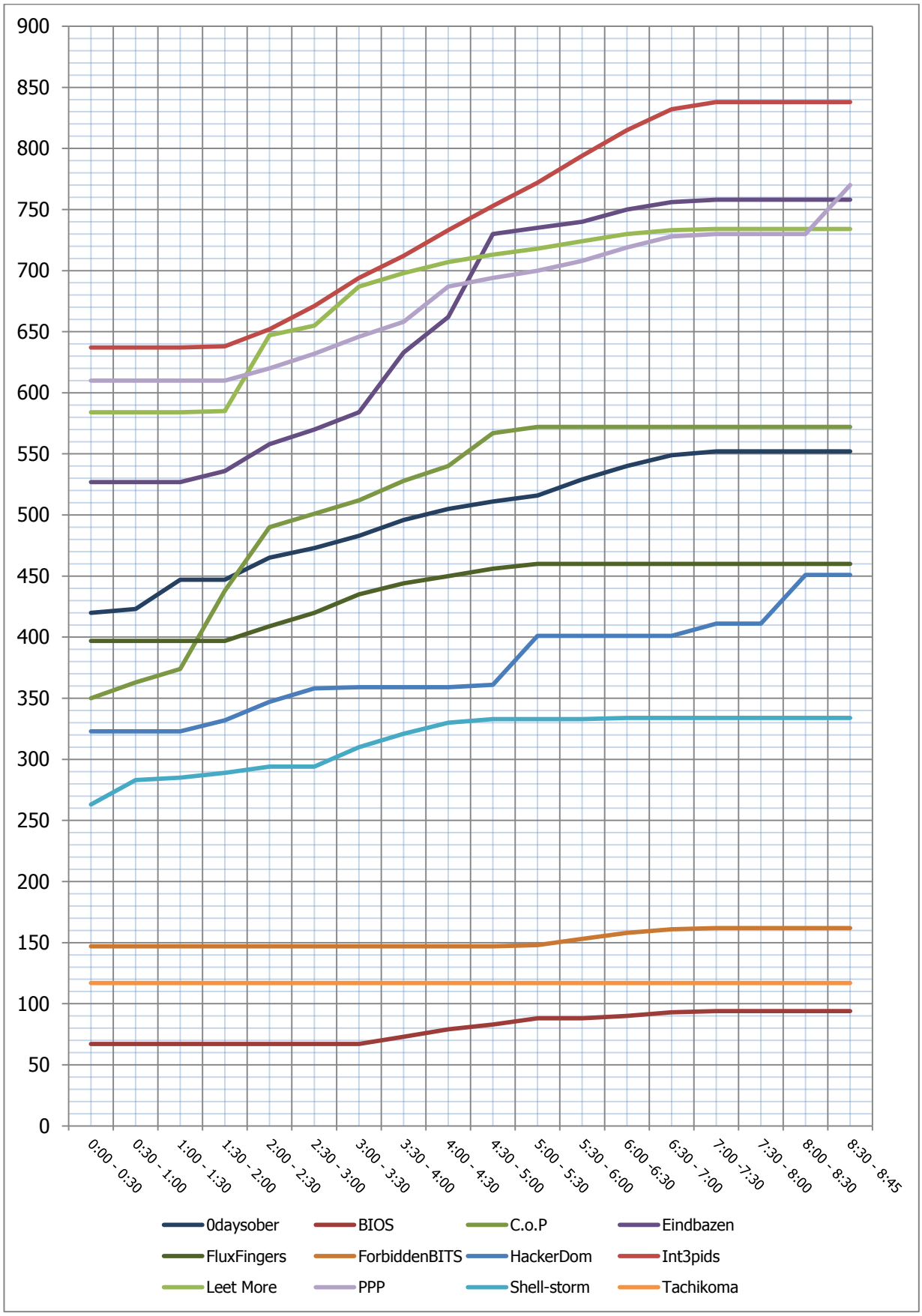


Figure 33. The history of the CTF overall points scored at night

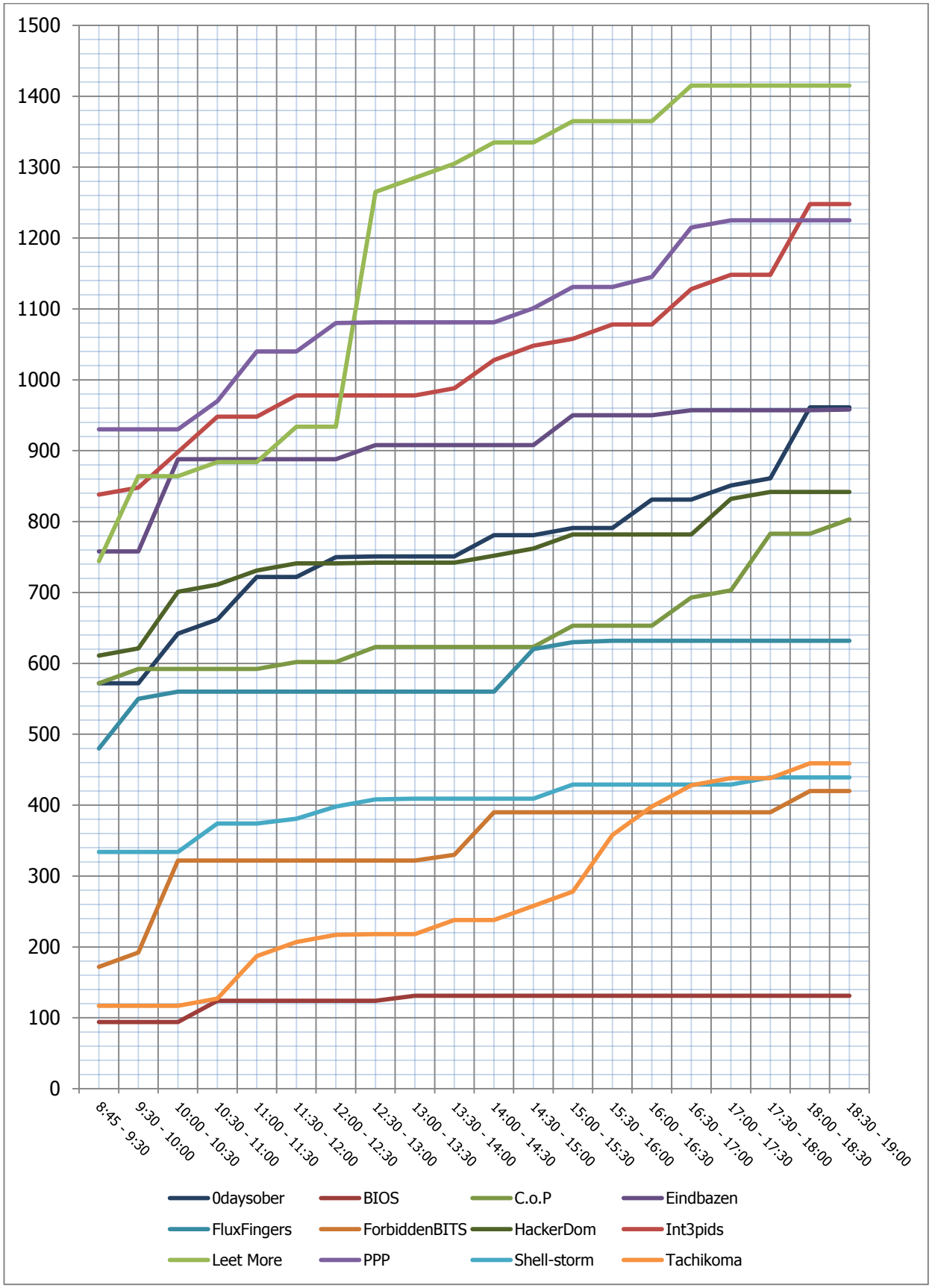


Figure 34. CTF overall score history for the 2nd day

6.5.2. Total score dynamics

The score dynamics related to all the task types of PHDays CTF 2012 is provided in table 12 and figures 35-37.

According to table 12, not only the leaders of the competition but the weaker teams as well were active during the CTF contest. Each half an hour a leader in the number of points scored within this time was changed, though the top three list in the overall standings was not frequently changed. This proves the fact that all the teams despite their ratings did not stop battling.

The teams were mostly active during the first half of the first and the second days. Contrary to the expectations of the organizers, the teams studied the specific features of the tasks and competition rules very quickly. It is proved by the score dynamics (figure 35).

The teams were less active at night, but a lot of participants kept playing despite the tiredness. However, Tachikoma did not score a point at night.

The team ratings by the beginning of the second CTF day became available only in the morning, the participants did not know the changes at night. This might become the reason for the teams to be as active as during the first day — the top three leaders had changed their positions.

According to table 12, the majority of the teams earned the maximum number of points for a half-an-hour interval on the second day of the competition. This fact evidences a very persistent struggle among all the CTF participants, not only among the leaders.

Note: due to the fact that the actions of the CTF participants were assessed with regard to the flag implementation, the obtained statistics may not depict the exact time when the tasks were solved by the teams, and indicate the time when the participants input flags into the system. That is why the teams' activity can be assessed only relatively taking into account this fact.

Leet More managed to earn the largest number of points for a half-an-hour interval (331 points). The points scored for holding control over the service of the King of the Hill infrastructure made a considerable contribution to the team's success: Leet More managed to keep control over the service for more than fourteen hours.

Table 12. CTF total score dynamics

Time interval	Team											
	0daysober	BIOS	C.o.P	Eindbazen	FluxFingers	ForbiddenBITS	HackerDom	Int3pids	Leet More	PPP	Shell-storm	Tachikoma
Day 1, May 30, 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
Night												
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
Day 2, May 31, 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

Note. Yellow means the maximum number of points earned during the current half-an-hour interval, green — the 2nd place by the number of points scored during the current half an hour, blue — 3rd place. The maximum number of points scored by the teams during all half-an-hour intervals are underlined.

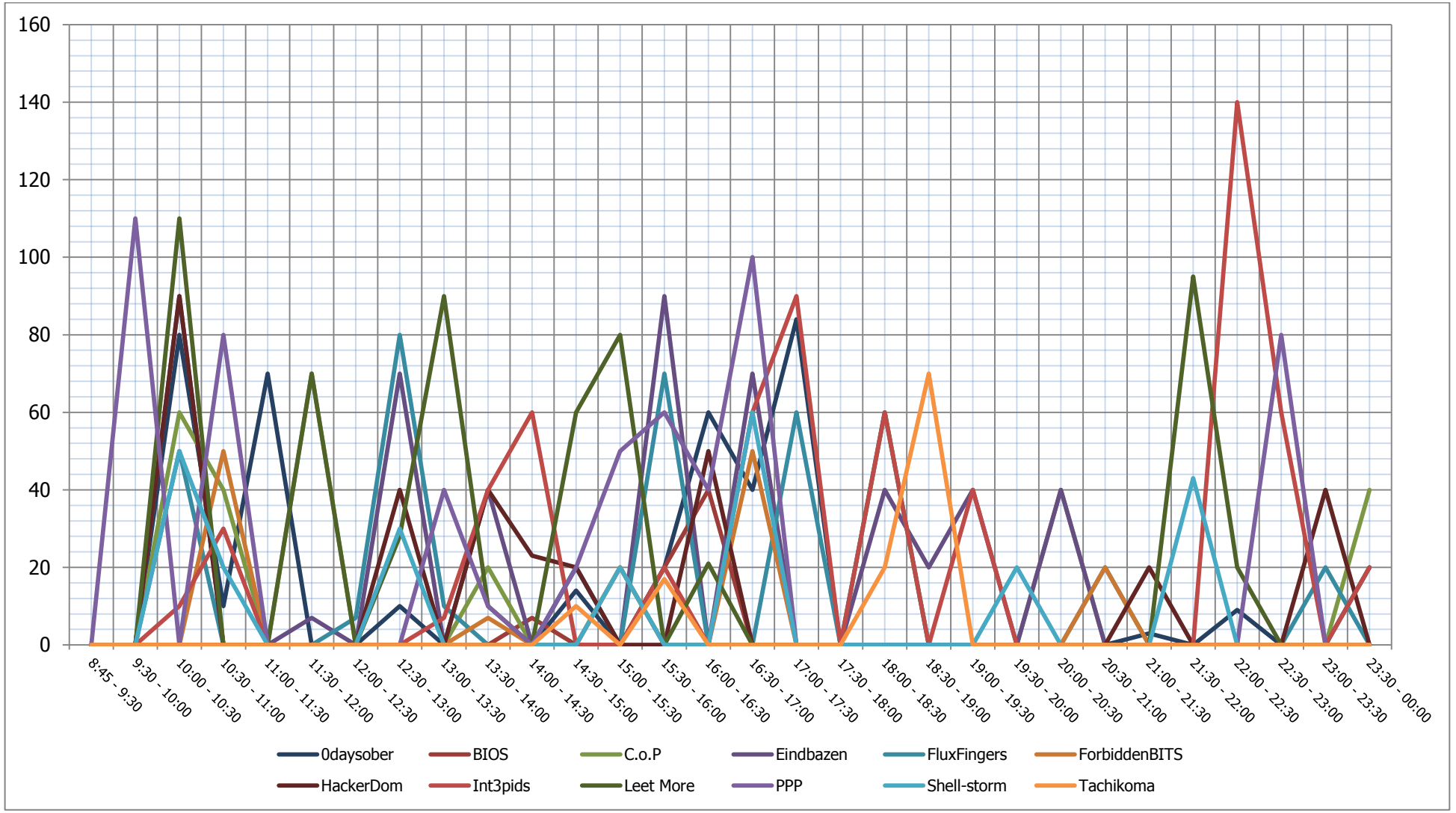


Figure 35. CTF overall score dynamics for the 1st day

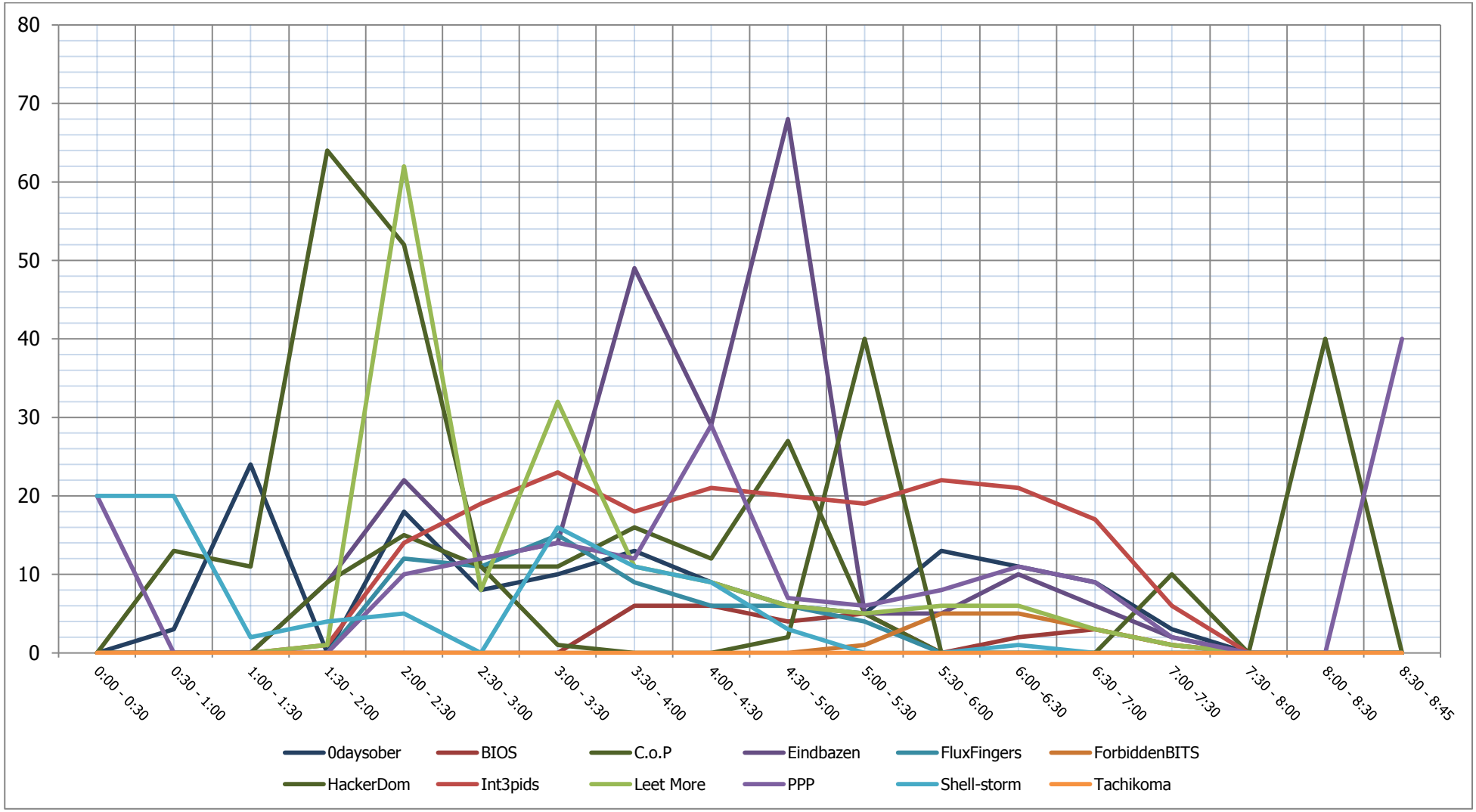


Figure 36. The dynamics of the overall points scored at night

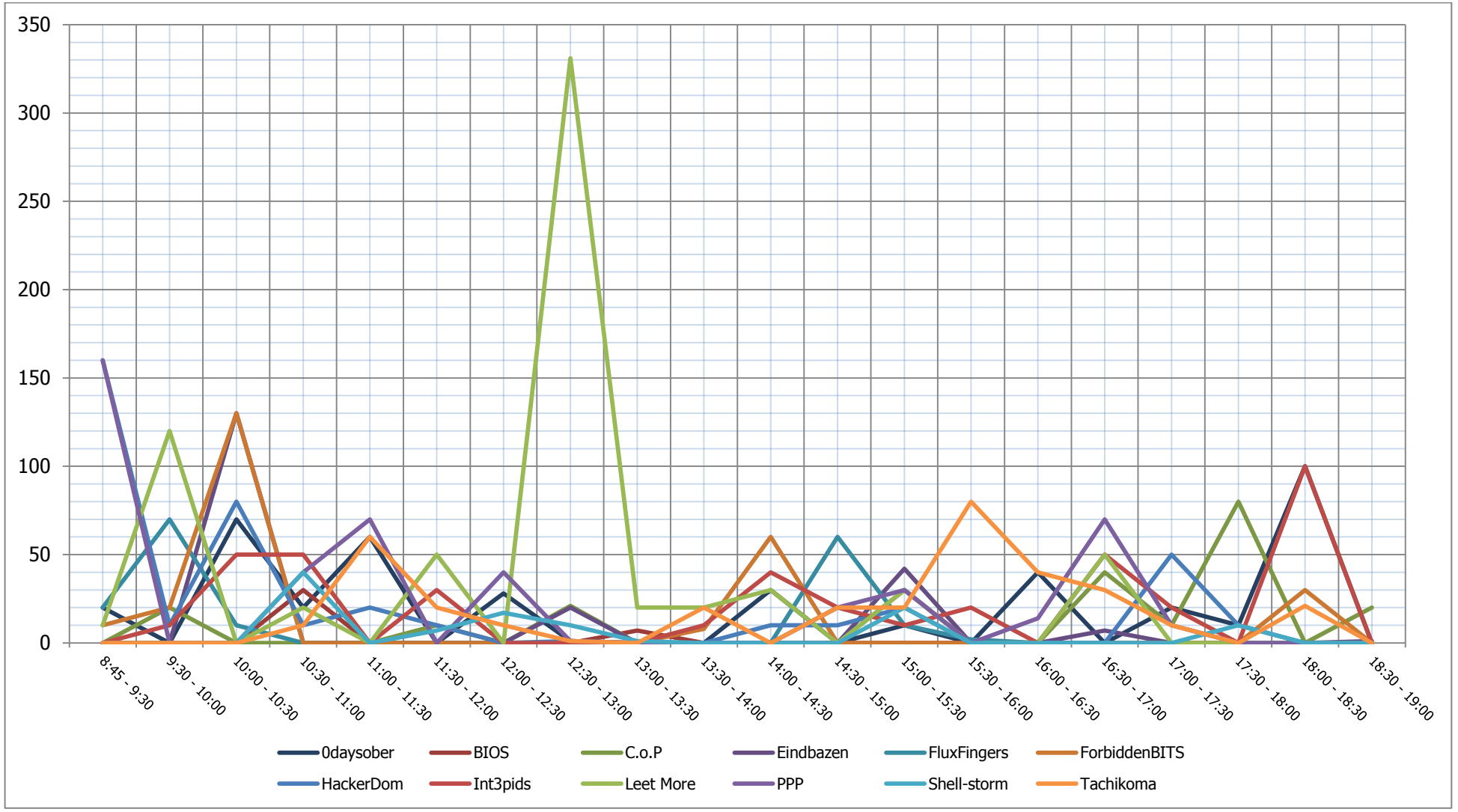


Figure 37. CTF overall score dynamics for the 2nd day

6.5.3. CTF results

The total score of the teams is provided in table 13 and figure 38. Figure 39 includes the number of points earned by the teams in various contests and the total score at the end of the competition.

The diagrams of figure 39 show that it is not enough to solve tasks of only one or two types to win the CTF contest — it is necessary to score points in all game infrastructures. Those teams, which managed to allocate time and resources, choose a correct game strategy, took the leading positions in the rating table.

Leet More, Int3pids, and 0daysober managed to earn a significant number of points within each infrastructure and bonus tasks. The PPP participants scored enough points to enter the top three on the basis of the total score, but they did not solve any task of the King of the Hill infrastructure. This might not allow the team from the USA to take the 1st place in the overall rating and repeat the result of 2011. These were the points earned for holding down the services of the King of the Hill infrastructure that helped Leet More to occupy the top of the rating list.

Photo 14. Leet More — the winners of CTF 2012

Photo 15. 0daysober, the 2nd place in CTF 2012

Photo 16. Int3pids, the 3rd place in CTF 2012

The only team that became an outsider following the CTF results was BIOS. The participants from India managed to score points both for the shared infrastructure tasks, bonus tasks and for capturing flags from the contestants' services, but, unfortunately, these points were not enough to keep up with the competitors.

Figure 40 provides the percentage of the points scored by each team in specific task types in the ratio to their total number of points.

PHDays CTF 2012 was closed by a musical band named Undervud.

Photo 17. The musical band Undervud closes PHDays 2012

Table 13. The total score of the teams at the end of the CTF contest

Contest types	Team											
	Leet More	Int3pids	PPP	0daysober	Eindbazen	HackerDom	C.o.P	FluxFingers	Tachikoma	Shell-storm	ForbiddenBITS	BIOS
Team services	670	480	680	470	450	390	340	460	310	250	290	30
Shared Game Infrastructure	220	460	240	140	340	220	360	100	140	120	100	60
King of the Hill	413	100	0	193	0	0	0	0	0	0	0	0
Bonus tasks	112	208	305	158	168	232	103	72	9	69	30	41
Total score	1415	1248	1225	961	958	842	803	632	459	439	420	131

Note to table 13: Yellow means the first place, green — the second, blue — the third.

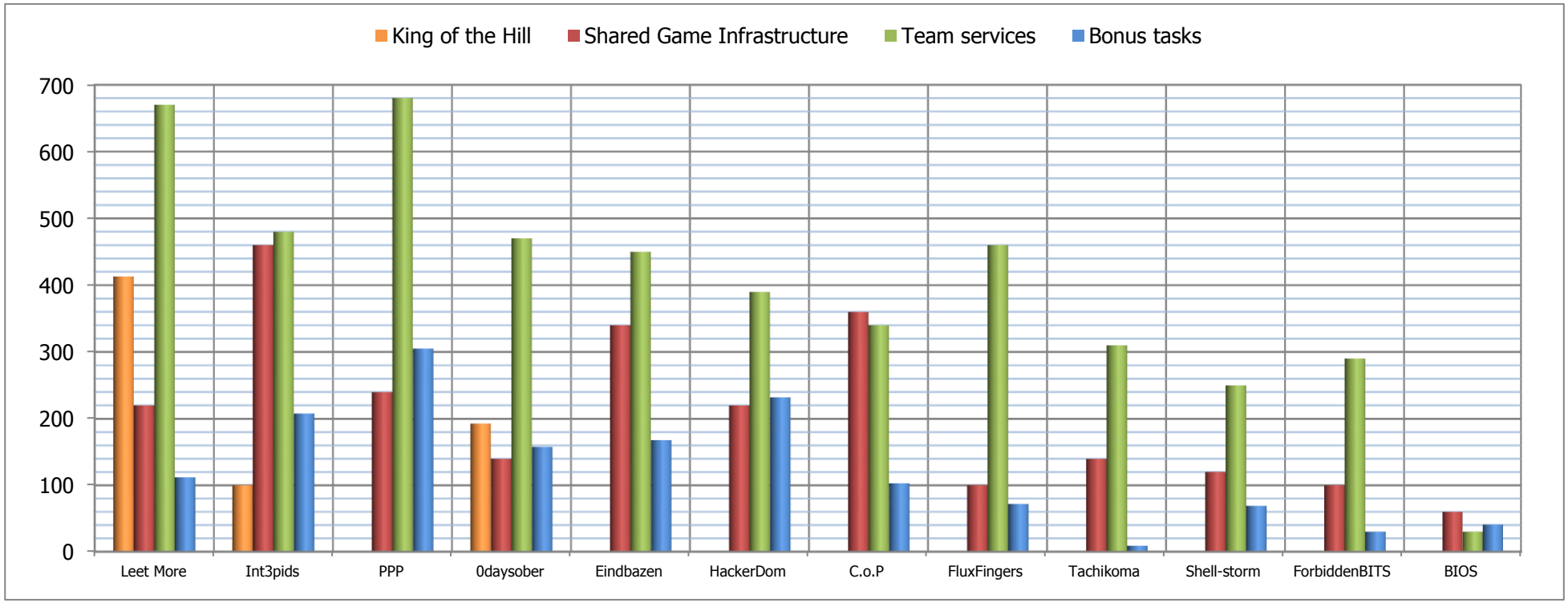


Figure 38. The total score of the teams at the end of the CTF contest (by the contest types)

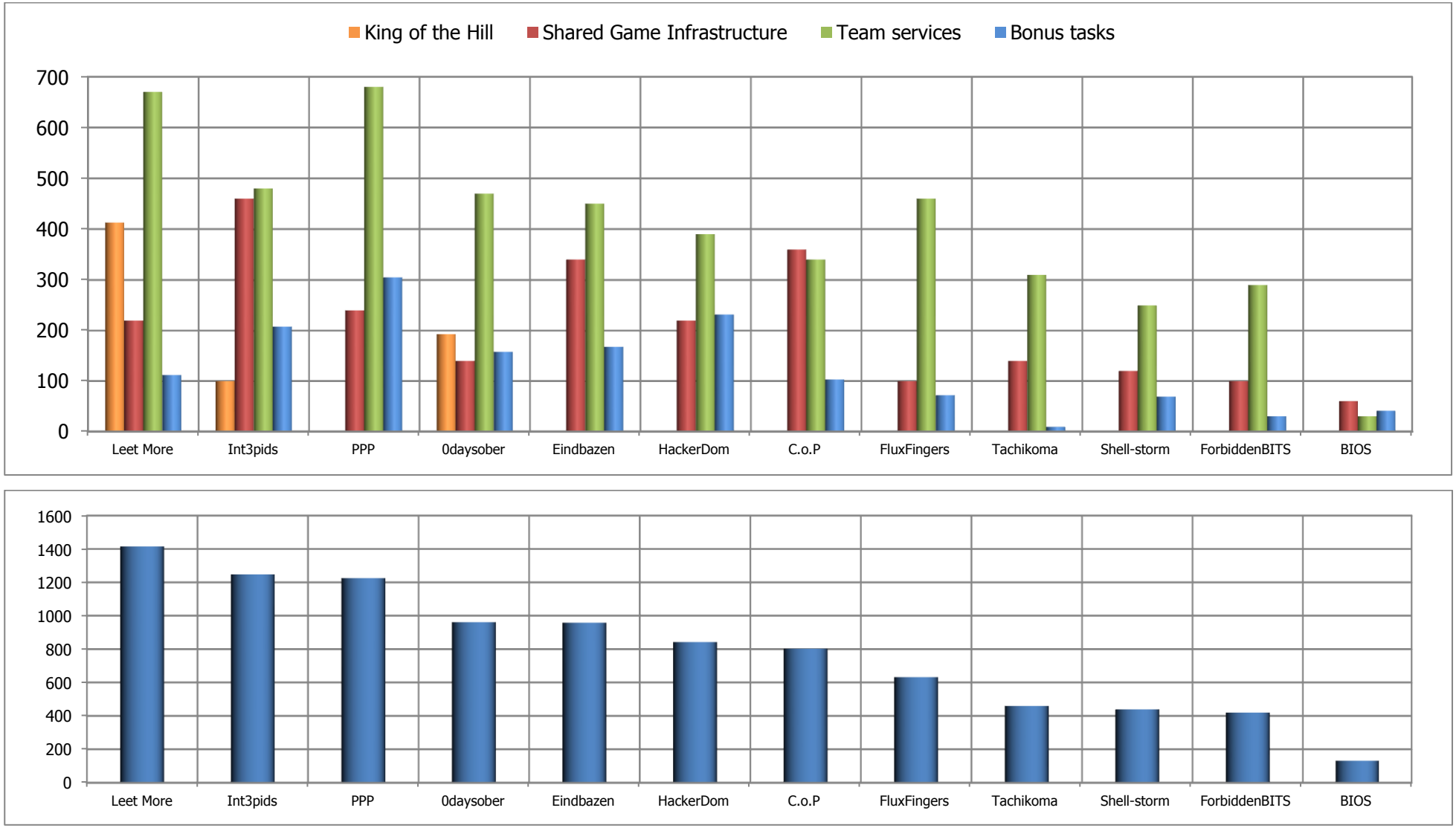


Figure 39. The number of points earned by the teams in various contests corresponding to the total score at the end of the competition

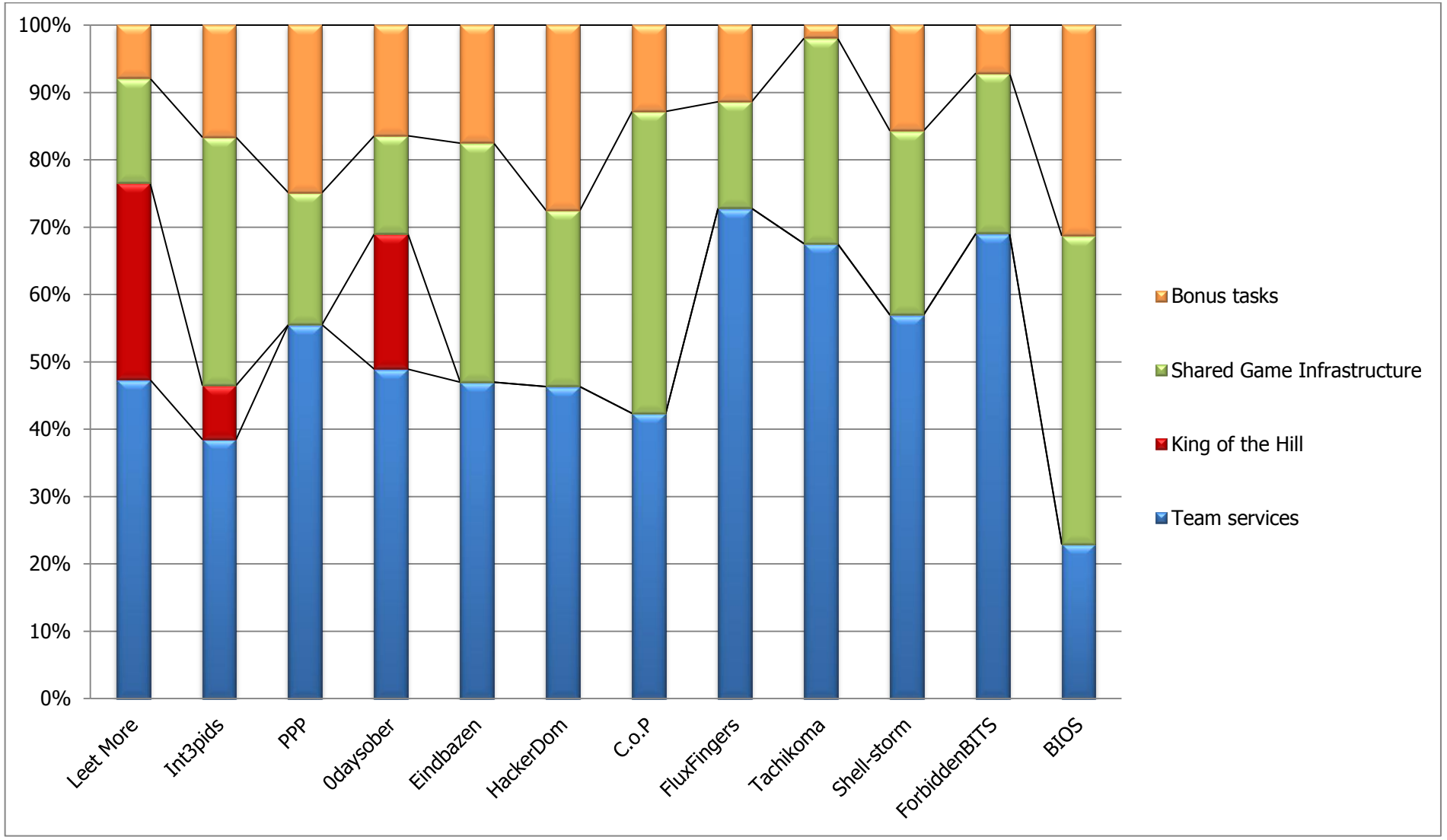


Figure 40. The percentage of the points scored by each team in the ratio to their total number of points

7. Conclusion

This data do not comply with the official final ratings, because these statistics include only the earned points and do not take into account points lost by the teams as a result of attacks on their services as part of the team infrastructure contests and on the I-bank accounts of the teams, and as a result of the penalty for unavailability of their services.

Figure 41 provides a diagram displaying the total team ratings (in descending order).

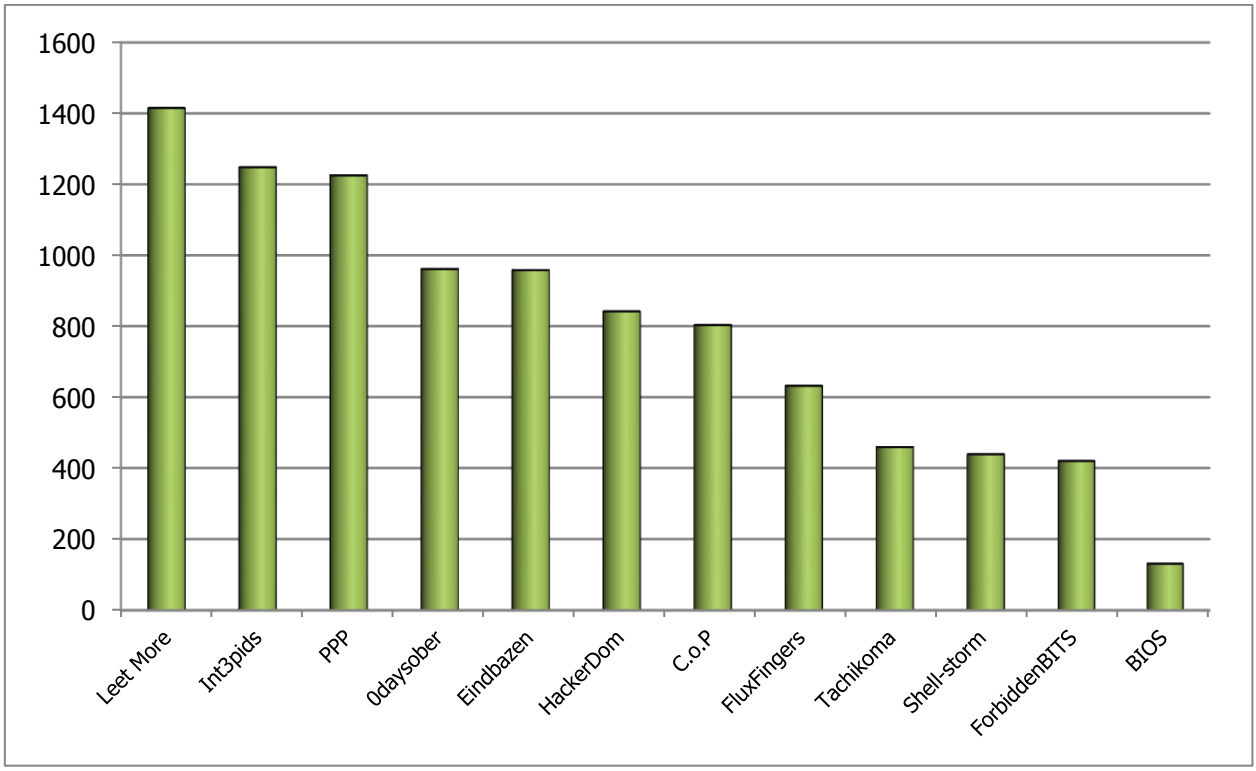


Figure 41. Total team ratings

The diagram of figure 41 proves that all the teams fought a good battle both for the top three places and for the other rating rows. The leading teams failed to leave their competitors far behind, the suspense of the competition kept increasing up to the very last minutes. The points of the neighboring rows of the total rating table differ just a little.

When the PHDays CTF 2012 competition was being prepared, the models of the possible course of events were developed. These models were developed to create a balanced system for evaluation of the CTF participants' actions. Rules for calculation of points earned and lost by the teams were implemented for each specific contest type. All the contests differed in the subject and degree of complexity.

According to preliminary estimates, it was supposed that the following scenarios were the most possible:

1) Domination of one of the teams in all contest types and a big number of outsiders (both in classic CTF and in the tasks of the King of the Hill and shared infrastructures)
2) Several (two or three) teams dominating in all contest types and other teams dragging behind
3) Domination of different teams in different contest types
4) No leaders or outsiders in any contest type

The rules for point calculation were developed in such a way so that the teams unable to solve the tasks of the same type could compensate the gap and keep winning chances by solving other tasks. The teams needed to be active dealing with all the infrastructures not to lose the lead and win the competition. The organizers wanted to make PHDays CTF 2012 as entertaining as possible, to keep up the interest not only of its participants but of the audience as well.

The event history provided in table 11 shows that in the course of CTF there were three-four leading teams constantly struggling for the top three. However, according to the statistics, the CTF results correspond to model 3 most fully. The CTF winner, the Leet More team, lost to PPP by the points scored in classic CTF and to Int3pids in the contest of the shared infrastructure, but the points earned in the tasks of the King of the Hill infrastructure brought the team to the leading position in the overall rating. At the same time C.o.P. and Eindbazen were in the top three on the basis of the score for the shared infrastructure tasks, but couldn't enter the overall top list at the end of the competition.

The results of PHDays CTF 2012 showed that the organizers completed their goals. Such tasks as protection of an I-Bank and bonus contests (paper duster and AR.Drone) made the competition more appealing. The teams were surprised when they received a task to protect their bank accounts on the second day of the competition. This task allowed the Internet participants from all over the world to affect the CTF results. One more peculiar feature of PHDays CTF 2012 was the King of the Hill infrastructure, which played a lead role in the election of the winner.