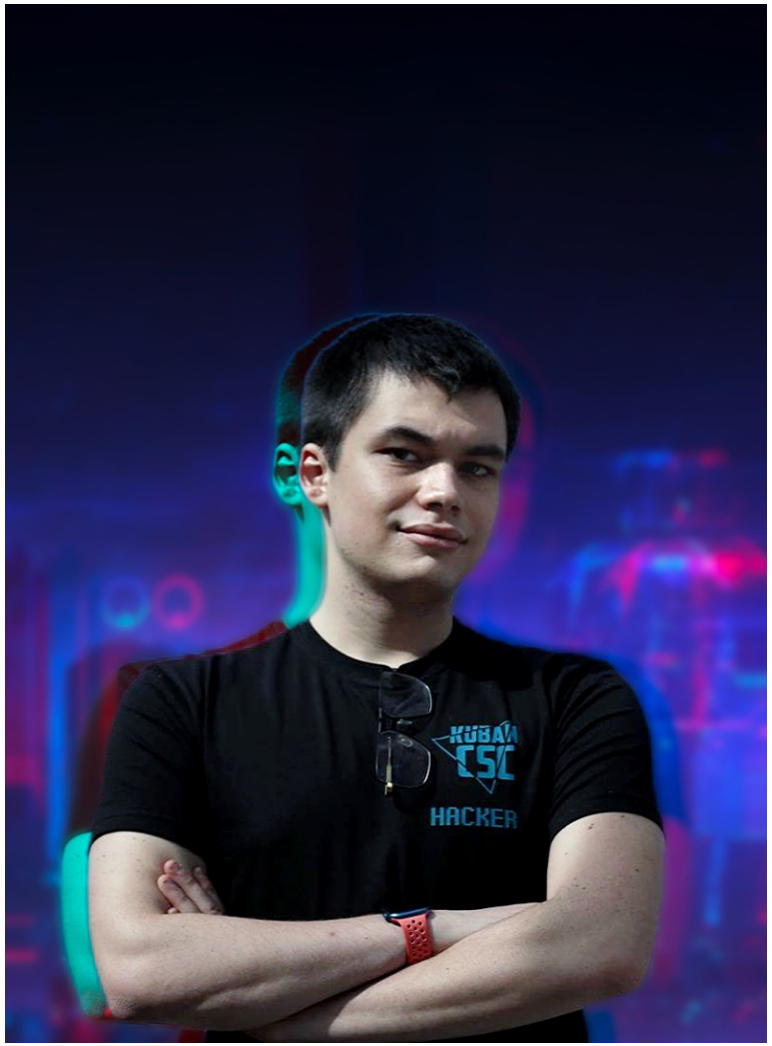
CTF as a Service

Хакимов Лев

Wildberries Security TechLead

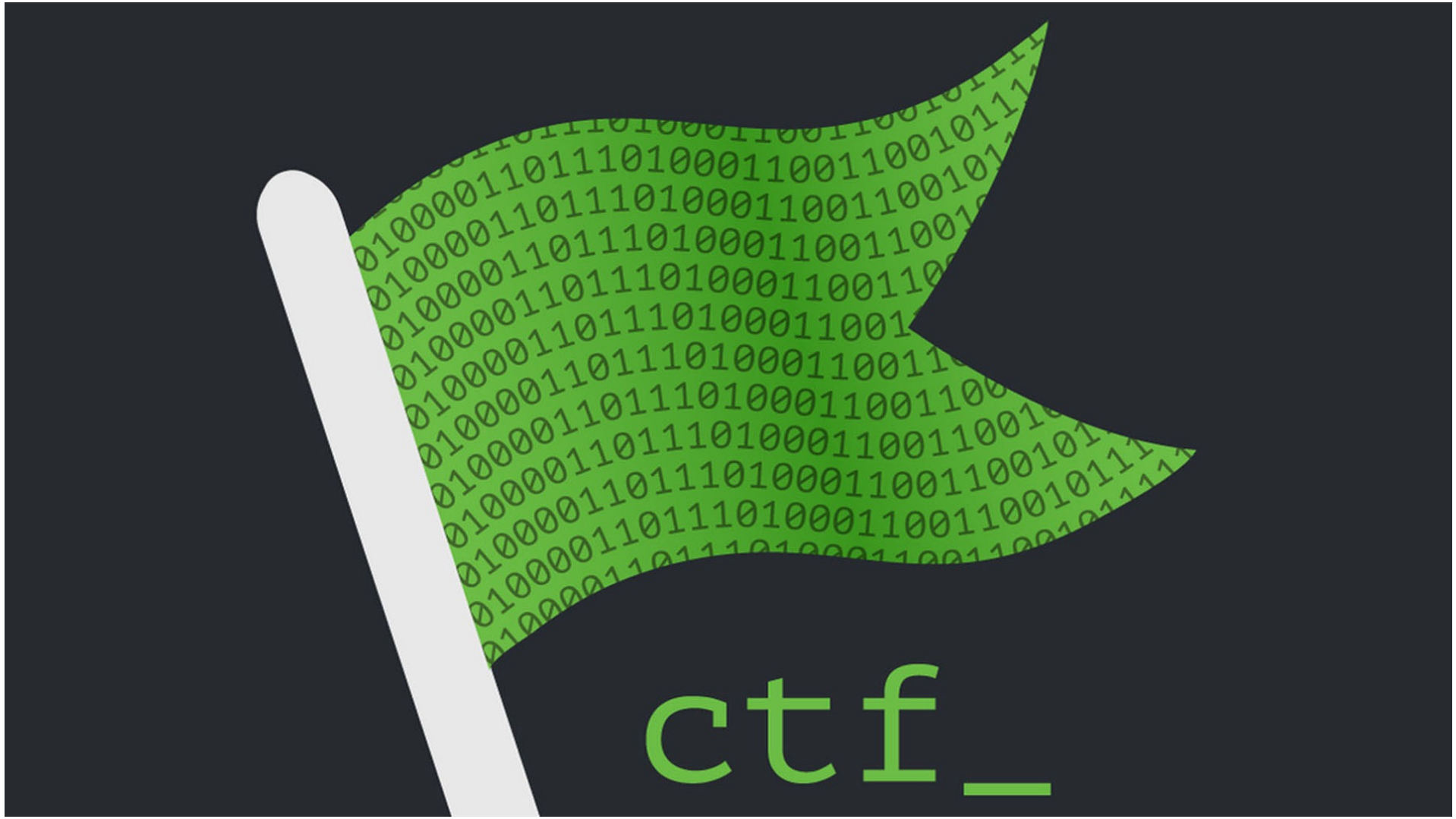
whoami

- Java/Python разработчик
- Увлекающийся реверсер на дому с IDA и паяльником
- Играю в CTF в команде ONO
- Руководитель команды разработки и DevOps на VrnCTF & CentralCTF
- Руководитель команды разработки и поддержки сервисов ИБ в Wildberries



Да кто такой этот ваш CTF?

Capture The Flag



Есть два типа

Jeopardy

- Task-based

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки
- Задания разбиты по категориям

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки
- Задания разбиты по категориям
- Хорош для новичков

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки
- Понятные категории заданий
- Хорош для новичков

Attack-Defence

- У команды есть сервер приложений

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки
- Понятные категории заданий
- Хорош для новичков

Attack-Defence

- У команды есть сервер приложений
- В каждом уязвимость(ти)

Есть два типа

Jeopardy

- Task-based
- Много заданий, за выполнение - очки
- Понятные категории заданий
- Хорош для новичков

Attack-Defence

- У команды есть сервер приложений
- В каждом уязвимость(ти)
- Ваша задача – найти их, запатчить у себя и эксплуатировать у других

Jeopardy (categories)

- WEB

Jeopardy (categories)

- WEB
- Reverse

Jeopardy (categories)

- WEB
- Reverse
- PWN

Jeopardy (categories)

- WEB
- Reverse
- PWN
- Crypto

Jeopardy (categories)

- WEB
- Reverse
- PWN
- Crypto
- OSINT

Jeopardy (categories)

- WEB
- Reverse
- PWN
- Crypto
- OSINT
- Stegano

Jeopardy (categories)

- WEB
- Reverse
- PWN
- Crypto
- OSINT
- Stegano
- Misc

Jeopardy (как форма)

«+»

- Простые правила
- Работа как в команде, так и поодиночке
- Гибкий уровень сложности
- Проще проводить

«-»

- В целом как форма – достаточно скучная

Attack-Defence

- Есть несколько команд (10-20)

Attack-Defence

- Есть несколько команд (10-20)
- У каждой команды свой сервер с приложениями

Attack-Defence

- Есть несколько команд (10-20)
- У каждой команды свой сервер с приложениями
- Все команды находятся в одной сети

Attack-Defence

- Есть несколько команд (10-20)
- У каждой команды свой сервер с приложениями
- Все команды находятся в одной сети
- В каждом сервисе одна или несколько уязвимостей

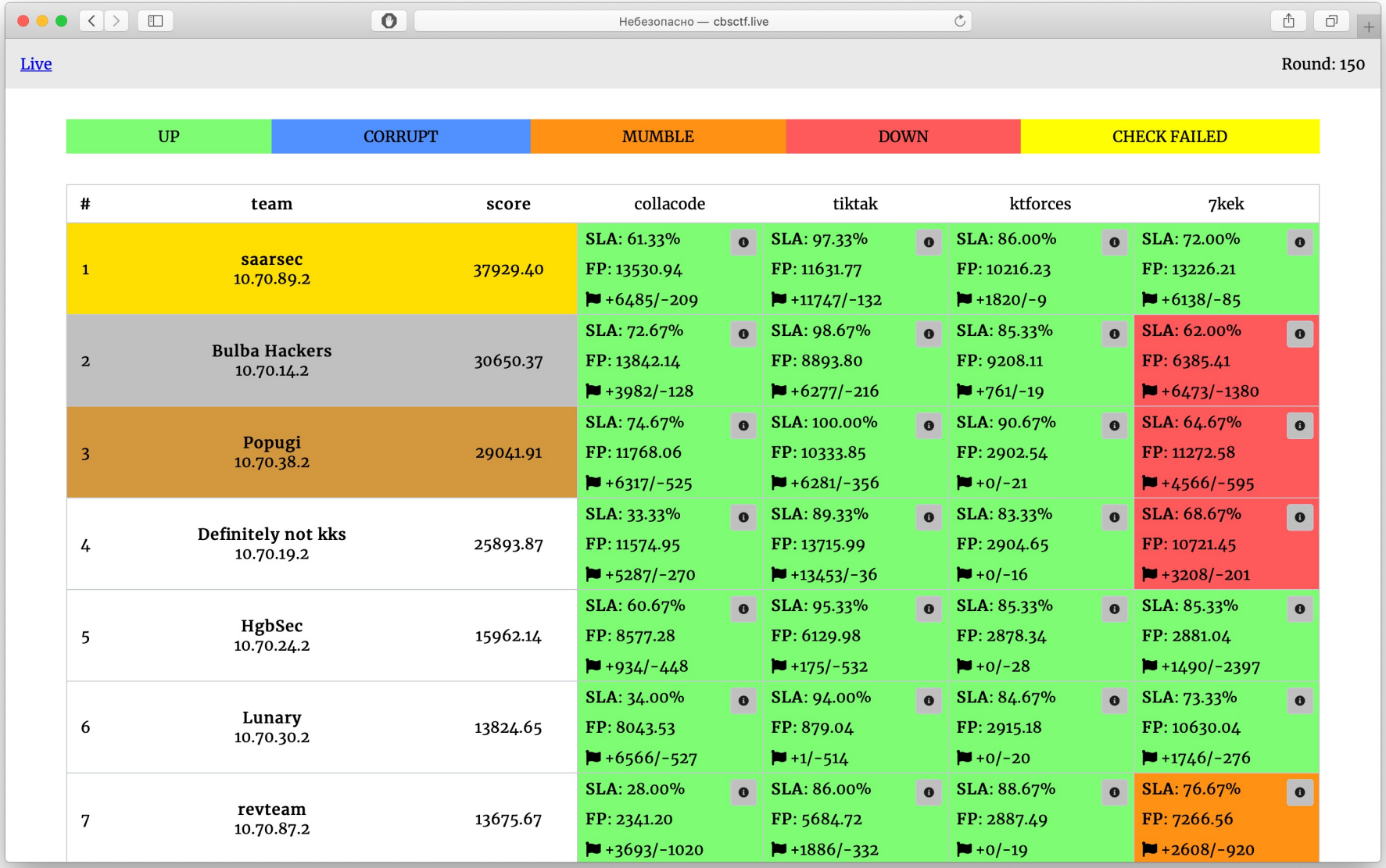
Attack-Defence

- Есть несколько команд (10-20)
- У каждой команды свой сервер с приложениями
- Все команды находятся в одной сети
- В каждом сервисе одна или несколько уязвимостей
- Раз в раунд чекер делает smoke по сервису и размещает в нем флаг

Attack-Defence

- Есть несколько команд (10-20)
- У каждой команды свой сервер с приложениями
- Все команды находятся в одной сети
- В каждом сервисе одна или несколько уязвимостей
- Раз в раунд чекер делает smoke по сервису и размещает в нем флаг
- Задача команды – найти их и устранить, а также написать скрипт захвата флагов у соседних команд

Жюри



#	team	score	collacode	tiktak	ktforces	7kek
1	saarsec 10.70.89.2	37929.40	SLA: 61.33% FP: 13530.94 ⚑ +6485/-209	SLA: 97.33% FP: 11631.77 ⚑ +11747/-132	SLA: 86.00% FP: 10216.23 ⚑ +1820/-9	SLA: 72.00% FP: 13226.21 ⚑ +6138/-85
2	Bulba Hackers 10.70.14.2	30650.37	SLA: 72.67% FP: 13842.14 ⚑ +3982/-128	SLA: 98.67% FP: 8893.80 ⚑ +6277/-216	SLA: 85.33% FP: 9208.11 ⚑ +761/-19	SLA: 62.00% FP: 6385.41 ⚑ +6473/-1380
3	Popugi 10.70.38.2	29041.91	SLA: 74.67% FP: 11768.06 ⚑ +6317/-525	SLA: 100.00% FP: 10333.85 ⚑ +6281/-356	SLA: 90.67% FP: 2902.54 ⚑ +0/-21	SLA: 64.67% FP: 11272.58 ⚑ +4566/-595
4	Definitely not kks 10.70.19.2	25893.87	SLA: 33.33% FP: 11574.95 ⚑ +5287/-270	SLA: 89.33% FP: 13715.99 ⚑ +13453/-36	SLA: 83.33% FP: 2904.65 ⚑ +0/-16	SLA: 68.67% FP: 10721.45 ⚑ +3208/-201
5	HgbSec 10.70.24.2	15962.14	SLA: 60.67% FP: 8577.28 ⚑ +934/-448	SLA: 95.33% FP: 6129.98 ⚑ +175/-532	SLA: 85.33% FP: 2878.34 ⚑ +0/-28	SLA: 85.33% FP: 2881.04 ⚑ +1490/-2397
6	Lunary 10.70.30.2	13824.65	SLA: 34.00% FP: 8043.53 ⚑ +6566/-527	SLA: 94.00% FP: 879.04 ⚑ +1/-514	SLA: 84.67% FP: 2915.18 ⚑ +0/-20	SLA: 73.33% FP: 10630.04 ⚑ +1746/-276
7	revteam 10.70.87.2	13675.67	SLA: 28.00% FP: 2341.20 ⚑ +3693/-1020	SLA: 86.00% FP: 5684.72 ⚑ +1886/-332	SLA: 88.67% FP: 2887.49 ⚑ +0/-19	SLA: 76.67% FP: 7266.56 ⚑ +2608/-920

Чекер

- Скрипт, запускающийся раз в раунд
- Проверяет, весь ли ваш сервис доступен
- Если есть возможность, кладет флаг в хранилку через API сервиса

Vulnbox & services

- Образ ВМ с установленными на нее сервисами
- Может выдаваться участникам для развертывания у себя
- Может предоставляться уже готовый во внутренней платформе соревнований

А оно нам надо?

Для кого делать?

- Ваши сотрудники

Для кого делать?

- Ваши сотрудники
- Школьники и студенты первого-второго курсов

How-to guide

- Определитесь с целевой аудиторией соревнований

How-to guide

- Определитесь с целевой аудиторией соревнований
- Определитесь с форматом

How-to guide

- Определитесь с целевой аудиторией соревнований
- Определитесь с форматом
- Набрать команду разработки

How-to guide

- Определитесь с целевой аудиторией соревнований
- Определитесь с форматом
- Набрать команду разработки
- Выберите тему

How-to guide

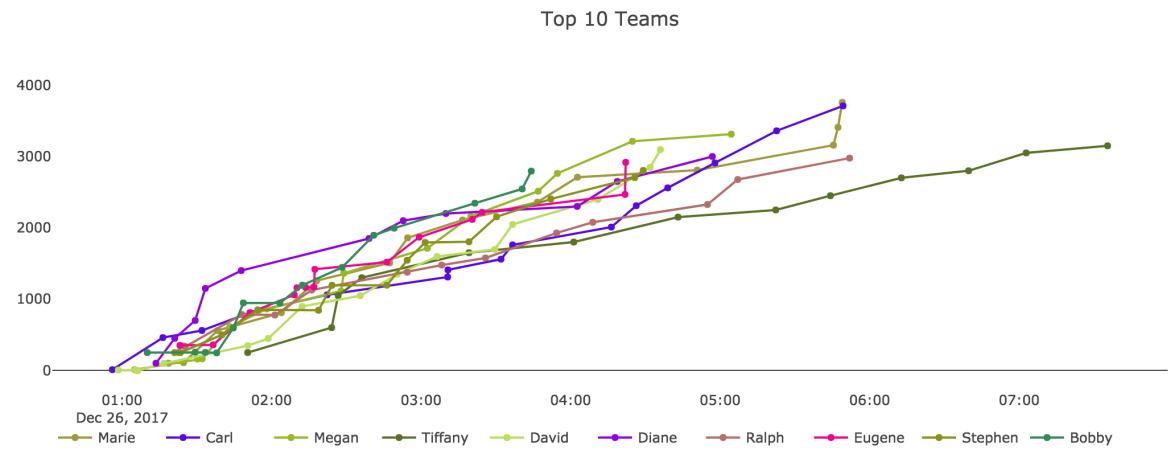
- Определитесь с целевой аудиторией соревнований
- Определитесь с форматом
- Набрать команду разработки
- Выберите тему
- Трезво оценивайте свои силы и опыт ☺

А что нам поможет?

CTFd

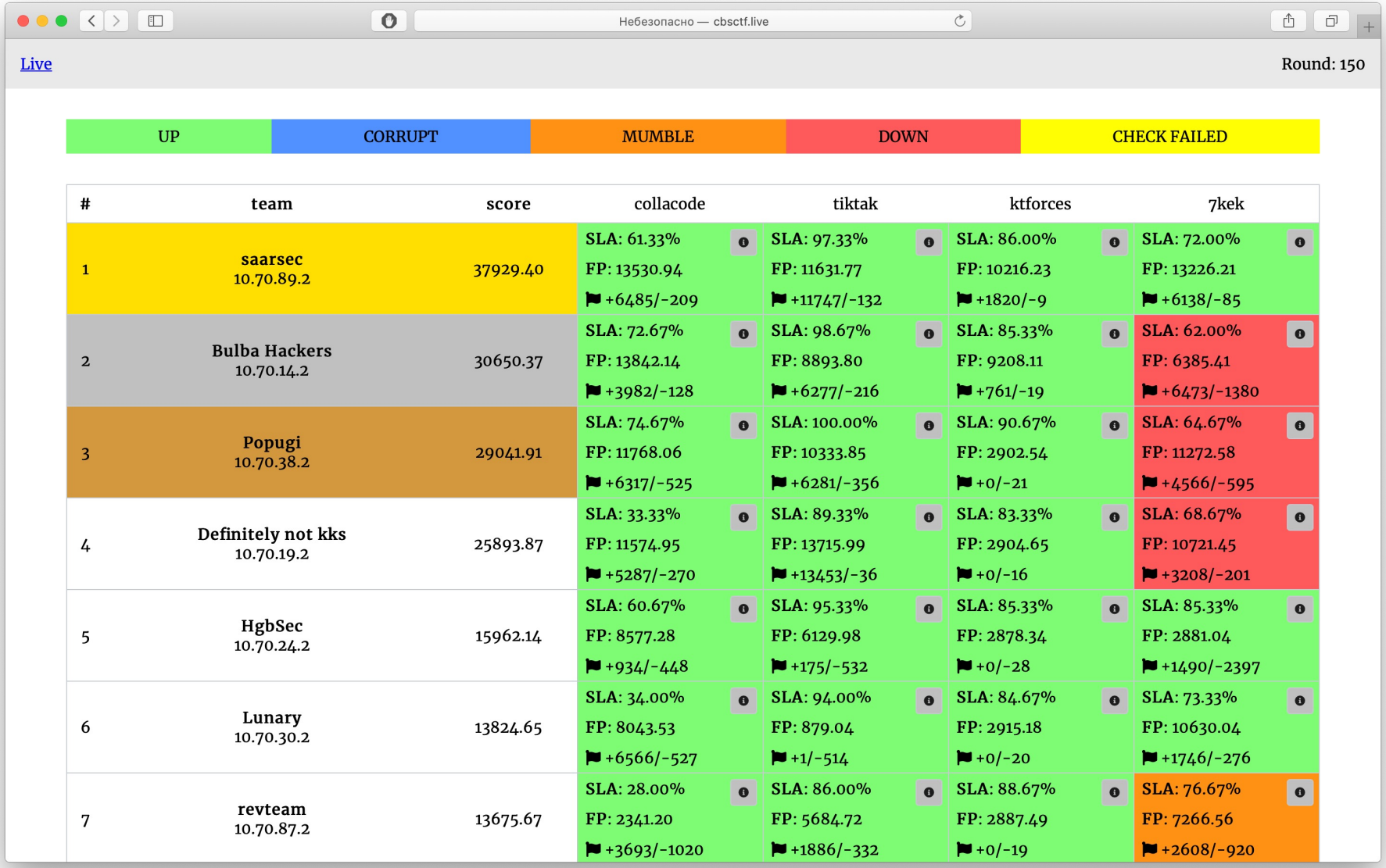
CTFd Teams Scoreboard Challenges Admin Team Profile Logout

Scoreboard



Place	Team	Score
1	Marie	3759
2	Carl	3710
3	Megan	3313
4	Tiffany	3150
5	David	3097
6	Diane	3000

ForkAD



#	team	score	collacode	tiktak	ktforces	7kek
1	saarsec 10.70.89.2	37929.40	SLA: 61.33% FP: 13530.94 +6485/-209	SLA: 97.33% FP: 11631.77 +11747/-132	SLA: 86.00% FP: 10216.23 +1820/-9	SLA: 72.00% FP: 13226.21 +6138/-85
2	Bulba Hackers 10.70.14.2	30650.37	SLA: 72.67% FP: 13842.14 +3982/-128	SLA: 98.67% FP: 8893.80 +6277/-216	SLA: 85.33% FP: 9208.11 +761/-19	SLA: 62.00% FP: 6385.41 +6473/-1380
3	Popugi 10.70.38.2	29041.91	SLA: 74.67% FP: 11768.06 +6317/-525	SLA: 100.00% FP: 10333.85 +6281/-356	SLA: 90.67% FP: 2902.54 +0/-21	SLA: 64.67% FP: 11272.58 +4566/-595
4	Definitely not kks 10.70.19.2	25893.87	SLA: 33.33% FP: 11574.95 +5287/-270	SLA: 89.33% FP: 13715.99 +13453/-36	SLA: 83.33% FP: 2904.65 +0/-16	SLA: 68.67% FP: 10721.45 +3208/-201
5	HgbSec 10.70.24.2	15962.14	SLA: 60.67% FP: 8577.28 +934/-448	SLA: 95.33% FP: 6129.98 +175/-532	SLA: 85.33% FP: 2878.34 +0/-28	SLA: 85.33% FP: 2881.04 +1490/-2397
6	Lunary 10.70.30.2	13824.65	SLA: 34.00% FP: 8043.53 +6566/-527	SLA: 94.00% FP: 879.04 +1/-514	SLA: 84.67% FP: 2915.18 +0/-20	SLA: 73.33% FP: 10630.04 +1746/-276
7	revteam 10.70.87.2	13675.67	SLA: 28.00% FP: 2341.20 +3693/-1020	SLA: 86.00% FP: 5684.72 +1886/-332	SLA: 88.67% FP: 2887.49 +0/-19	SLA: 76.67% FP: 7266.56 +2608/-920

Hackerdom AD CTF

#	team	score	ChessBase	cubic	QExecute
1	C4T BuT S4D	3517.48	SLA 95.71% FP 2183.04 ⚑ 591 / -92	SLA 77.62% FP 1513 ⚑ 569 / -31	SLA 88.1% FP 287.89 ⚑ 87 / -10
2	SPRUSH	2501.69	SLA 89.52% FP 2566.14 ⚑ 742 / -178	SLA 89.52% FP 1 ⚑ 0 / -119	SLA 99.52% FP 204.45 ⚑ 98 / -48
3	FAKAPPA	2198.43	SLA 93.33% FP 1987.08 ⚑ 502 / -35	SLA 64.29% FP 51.34 ⚑ 21 / -51	SLA 96.19% FP 323.12 ⚑ 78 / -5
4	Команда Лучкиных Вячеславов	2034.38	SLA 90.95% FP 1 ⚑ 0 / -898	SLA 97.14% FP 2092.4 ⚑ 388 / -43	SLA 84.76% FP 1 ⚑ 0 / -102
5	Lunary	1267.14	SLA 97.62% FP 1296.3 ⚑ 587 / -235	SLA 86.19% FP 1 ⚑ 0 / -79	SLA 83.81% FP 1 ⚑ 36 / -84
6	SFT0	1203.21	SLA 97.62% FP 1230.78 ⚑ 178 / -398	SLA 92.86% FP 1 ⚑ 0 / -146	SLA 80.48% FP 1 ⚑ 0 / -94
7	Импактный SUSIo.PAS	1073.73	SLA 77.62% FP 1 ⚑ 639 / -645	SLA 99.52% FP 1 ⚑ 0 / -149	SLA 88.57% FP 1210.27 ⚑ 207
8	N0N@me13	873.38	SLA 67.62% FP 1288.89 ⚑ 162 / -409	SLA 99.52% FP 1 ⚑ 0 / -143	SLA 85.24% FP 1 ⚑ 0 / -101
9	Red Cadets	583.77	SLA 64.76% FP 641.79 ⚑ 138 / -104	SLA 92.86% FP 1 ⚑ 0 / -69	SLA 88.1% FP 189.81 ⚑ 27 / -23
10	Punk Souls	350.84	SLA 90.48% FP 265.01	SLA 99.52% FP 1	SLA 83.81% FP 131.34

Спасибо за внимание!

Хакимов Лев

Wildberries Security Techlead