Победа на PHDays 9. Делимся лайфхаками в трёх частях. Часть 3

Издание: ХабраХабр, июль 2019 г.

Всем привет! Прошло уже несколько недель с момента нашей победы, эмоции схлынули, поэтому время браться за оценку и разбор того, что у нас не получилось. В нашей работе не важно — победили мы в соревновании или нашли уязвимость в реальном проекте, но всегда важно провести работу над ошибками и понять, что можно было сделать лучше. Ведь в следующий раз команды-соперники могут быть сильнее, а инфраструктура клиента защищена лучше. В общем, статья, с которой предлагаю вам ознакомиться ниже, спорная и носит скорее дискуссионный характер, нежели содержит гарантировано работающие рецепты. Впрочем, судите сами.

Подготовка

Как я уже писал в первой части, невероятно важным элементом нашей победы была подготовка. В рамках этого этапа нами был заложен фундамент будущей победы. Но также, в виду некоторых ошибок, в этот фундамент мы заложили несколько бомб замедленного действия, которые могли взорваться и похоронить всю конструкцию.

1. Команда

Наша команда состояла из 20 человек, и если честно — это очень много. Объективно, оборачиваясь сейчас на всё по прошествии времени, вижу, что для такой же уверенной победы нам хватило бы 7-8 человек. А для менее уверенной — было бы достаточно и 4-5 нацеленных на результат специалистов. Чем больше людей в команде, тем выше вероятность конфликтов, ведь такие соревнования — это огромный стресс, особенно на второй день соревнования и без нормального сна. К сожалению, реалии таковы, что вы не найдете 20 одинаково хороших хакеров, а это значит, что вам всё равно придется делать некий quality assurance более молодых специалистов, который по итогу будет выливаться в дублирование их работы.

Немаловажным фактором может являться разница в отношении к соревнованиям. Я участвую не первый год и практически каждый раз вижу следующую ситуацию: кто-то из членов команды уходит в 18-19.00 со словами «рабочий день окончен», и это ОЧЕНЬ сильно демотивирует остальных. И с одной стороны вроде бы правильно, ведь для многих людей это просто работа. А с другой — это очень сильно демотивирует ребят, для которых такие соревнования значат гораздо больше, чем просто работа. Для них это часть жизни. Возможно такие вещи имеет смысл обсуждать заранее внутри команды ещё до старта соревнований.

TL;DR: Качество важнее количества. Много участников — не всегда хорошо.

2. Эксплуатация нетиповых уязвимостей

Объективно говоря, тут тоже вышло не так, как задумывалось. Как вы помните, в качестве подготовки к неизвестным нам уязвимостям мы выписали типовые подходы, а также скачали инструментарий для проведения таких атак. Это было правильным шагом, но нужно было сделать еще пару других. Во-первых, при подготовке к таким соревнованиям, в первую очередь необходимо изучать техническую базу и архитектуру решений. К примеру, в случае с АСУ ТП, далеко не всем из ответственных за данное направление в нашей команде была понятна разница между контроллером, SCAD-ой и серверами, которые были разбросаны и тут и там. Что в итоге приводило к необходимости изучения всего этого во время соревнований. Так утекло много драгоценного времени. Ну и, конечно, необходимо наличие человека который бы не только мог скачать весь необходимый инструментарий, но понимал для чего он нужен и как его ставить, а лучше — заранее установил себе все необходимое ПО на виртуальные машины.

Пример с PHDays: один из дистрибутивов необходимого ПО состоял из образов 16 дискет (олды помнят), ставился только на Windows XP и для запуска требовал наличие дискеты в Floppy Disk Drive. Установить нам его так и не удалось.

TL;DR: Начинайте готовиться за месяц, а то и раньше. Не будьте скрипт-кидди, разбирайтесь в основах.

3. Подготовка оборудования

Ни для кого не секрет, что очень часто для того чтобы оставаться в состоянии потока нужны тишина и покой. Ну что ж, покой нам только снится, а тишина на PHDays — это вообще проблема. Поэтому я рекомендую помимо всего оборудования, перечисленного в наших статьях, обязательно брать с собой набор беруш и звукоизолирующих наушников. Они спасут вас и от гомона толпы, и от неожиданных саундчеков.

TL;DR: Возьмите с собой беруши. Лучше возьмите пару-тройку запасных, другие участники будут вам ОЧЕНЬ благодарны.

Соревнования

4. Координация

Мне гораздо проще писать критические пассажи по координации команды, ведь занимался ею я, и здесь точно никого не обижу. Итак, для эффективной координации вам нужен человек, который очень хорошо понимает, что тут вообще происходит, как работает пентест, разбирается в kill chain-ах, и в целом он должен понимать специфику работы каждого человека. Очевидно, что это человек с пентестерским бэкграундом, который активно практикует, или практиковался в недавнем прошлом (менее полугода).

С другой стороны, смотреть со стороны как ребята что-то взламывают, где-то ищут выходы из

тупика, но при этом активно не вовлекаться не в одну из проблем очень тяжело. Это стало для меня проблемой, и я объективно с этим не справился. В определенный момент я активно занялся эксфильтрацией данных и стал помогать бороться с конкурирующей командой. Из-за этого на протяжении 3-4 часов часть команды (примерно 30% участников) просто потерялась и не знала, чем заниматься. Сейчас я осознаю, что куда правильнее было бы делегировать эту задачу кому-то из членов команды, а самому продолжать отслеживать общую картину состязаний. Ведь координатор всегда должен знать, что происходит на каждом из направлений работы.

Пример с PHDays IX: Мы еще на втором часу соревнований заметили зависимость между доменом Bigbrogroup и cf-media. В итоге имея учетную запись enterprise-админа, мы только через 5 часов догадались, что её также можно использовать и во втором домене. Просто ранее никто не обратил внимания на связующий домен, который фигурировал в обоих заданиях. Предполагаю, что если бы мы использовали эту учетную запись, то мы бы могли задолго до официально объявленного слияния захватить контроль над вторым доменом и сэкономить себе кучу времени и нервов.

TL;DR: Координатор должен стараться не закапываться в мелочах, а смотреть на картину в целом.

5. Взаимодействие с организаторами

Конкретно этот момент в нашем случае работал как часы. Но мы заметили, что многие команды взаимодействуют с организаторами очень пассивно или не взаимодействуют вообще. Во-первых, нужно очень внимательно следить за обновлениями в чатах телеграма. Многие команды даже не видели результатов соц. инженерии, пока о них не объявили со сцены, но было уже поздно. Все мы люди и всем свойственно ошибаться. Так, в рамках игры мы нашли 3-4 бага, которые напрямую влияли на наши очки, сообщили об этом организаторам и они исправили ситуацию. То же самое касается формата флагов.

TL;DR: Обращайте внимание на всё, что говорят организаторы. Не стесняйтесь их спрашивать, если вам вдруг что-то не понятно.

6. Доклады

Уже второй год подряд организаторы в рамках своих докладов рассказывают о исследованиях, которые, в том числе, нашли свое применение в рамках StandOff. Поэтому абсолютно точно нужен человек или группа людей, которые обойдут всё секции с техническими докладами с близкими к StandOff темами и сделают краткие пересказы для тех, кто воюет на площадке StandOff. В частности, в этом году был доклад, используя который можно было получить доступ к одной из систем АСУ ТП.

TL;DR: Постарайтесь выделить человека или группу людей, чтобы они посетили все технические доклады.

Закончить этот цикл статей хотелось бы небольшой обратной связью по самим соревнованиям. Как я уже не раз говорил, основной проблемой Standoff последние 3 года является один и тот же факт: безопасность всегда была и будет частью компромисса между

функциональностью, удобством использования и непосредственно безопасностью. И в случае реальной жизни функциональность и удобство использования очень жёстко отстаивает бизнес.

Безопасность — это не самоцель, а лишь один из инструментов, помогающих бизнесу. И далеко не все желания специалистов по ИБ выполняются. Именно потому что они противоречат интересам бизнеса. Мы не раз в ходе соревнований натыкались на ситуацию, когда хакеры находили уязвимый сервис, а защитники его просто отключали. Представьте, что такое происходит в каком-нибудь банке. Какой-то хакер нашел уязвимость в системе ДБО и начал ее прорабатывать, а служба ИБ, увидев это, отключила данную систему, причем не на час, а на несколько дней. Компания несла бы колоссальные убытки. Сотрудник, принявший решение отключить сервис, был бы уволен, а сервис — тут же восстановлен. Но увы, в текущем формате соревнований такое невозможно, и именно это является основным фактором, мешающим показать реальную картину в мире, где, к сожалению, ИБ «догоняет» возможности хакеров, а не наоборот.

Подробнее: https://habr.com/ru/post/461325/