Победа на PHDays 9. Делимся лайфхаками в трёх частях. Часть 1

Издание: Хабр, 28 мая 2019 г.

Спикер: Виталий Малкин, руководитель отдела анализа защищенности «Информзащиты»

Всем привет! Меня зовут Виталий Малкин. Я руководитель отдела анализа защищённости компании «Информзащита» и по совместительству капитан команды True0xA3. Этой статьей мы начинаем цикл из 3-х материалов, посвящённых нашему выступлению на PHDays IX Standoff. В этой статье мы расскажем, почему грамотная подготовка — это половина успеха, почему так важно вовремя собрать «фрукты» и как можно организовать взаимодействие пентест-команды в рамках одного отдельно взятого проекта.

TL;DR статья содержит огромное количество англицизмов и сложных технических терминов, за что отдельно прошу прощения.

I. Входные данные

У нас было 16 отборных пентестеров, 4 стажера, 6 серверов, своя CUDA-станция и огромное желание победить.

Мы начали активную фазу подготовки за 8 дней до старта StandOff. Это была наша 3-я попытка, как атакующих, и многие из нас уже имели достаточно опыта, чтобы понять на что обратить внимание в этом году. Мы видели 5 приоритетных направлений для проработки:

1. Эффективная координация;
2. Сбор Low Hanging Fruits;
3. Эксплуатация уязвимостей нетиповых (для нас) технологий (АСУ ТП, IoT, GSM);
4. Подготовка внешней инфраструктуры и оборудования;
5. Разработка доп. методов persistence и hardening.

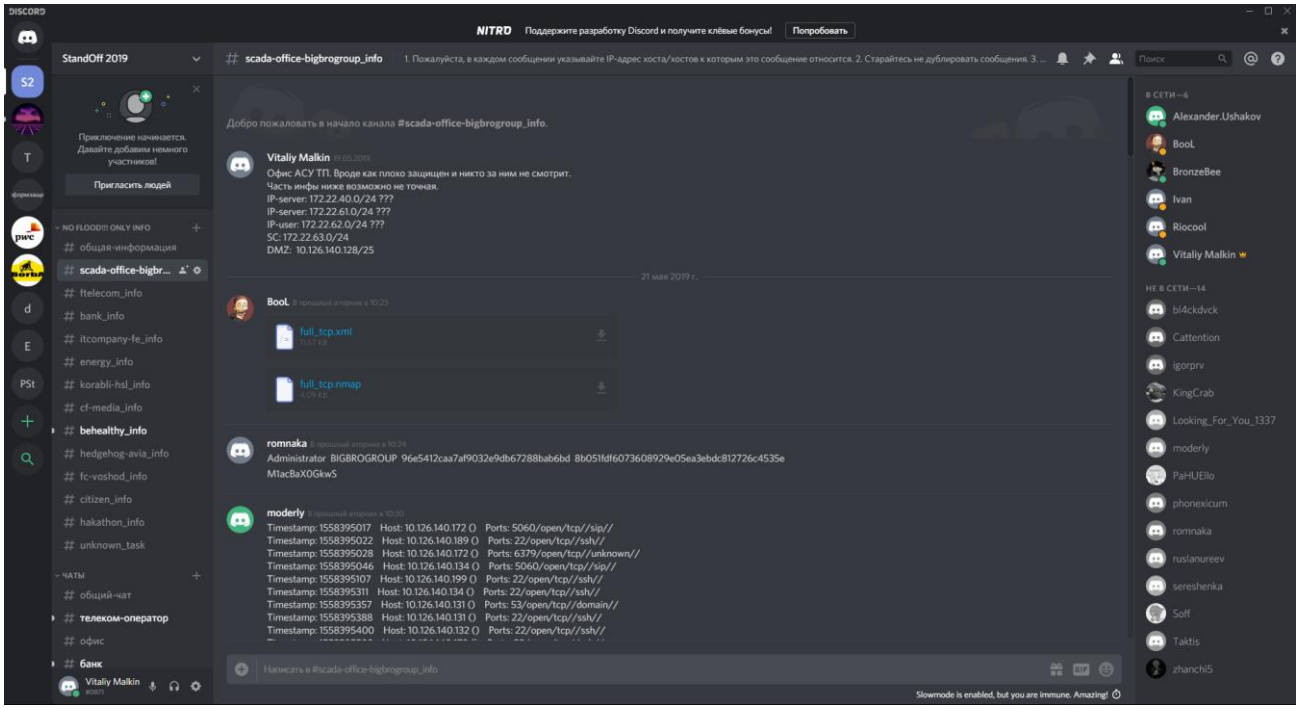
Давайте попробуем разобрать эти пункты по порядку.

1. Эффективная координация

Мне проще всего рассказывать про этот пункт, потому что общим решением ответственным за его реализацию был я. В ходе StandOff самой частой проблемой новичков, на мой взгляд, является слабая координация. Участники команды решают одни и те же таски, нет четкого понимания что уже посмотрели, а что нет. Полученная информация по таску не передается друг другу, в итоге эффективность работы сильно падает. И чем больше участников, тем сильнее падает эффективность. Более того, очень полезным является наличие человека, который хорошо понимает общую картину инфраструктуры и может связать отдельные уязвимости в полноценный вектор атаки.

В этом году для взаимодействия команды была выбрана платформа Discord. В целом она очень похожа на старый добрый IRC-чат с дополнительными фишечками типа file-upload-а и голосовой связи. Мы взяли описание всех объектов из Agend-ы соревнований и создали под каждый из них канал, в который размещали информацию. Таким образом любой человек, который подключался к задаче, мог посмотреть всё, что накопали до него, в том числе результаты запуска различных инструментов и ручных изысканий.

На всех инфо-каналах был установлен лимит на одно сообщение в минуту, чтобы не допускать флуда. А всё обсуждение велось в отдельных чатах, которые также были созданы под каждый объект.



Также для улучшения координации был принят ряд организационных решений. Вообще, у нас в команде не принято ставить задачи с формулировкой «НАДО». Мы стараемся обсуждать, почему поставлена та или иная задача, к чему приведёт ее выполнение, а также как выполнить её более эффективно. Но в рамках StandOff-а такая модель может привести к ненужным препирательствам, поэтому мы решили доверить координатору полную власть над процессом. В течение 28 часов соревнования его решения практически не обсуждались, что безусловно сэкономило нам немало времени. Хоть, возможно, и сказалось на качестве коммуникаций. Дополнительно к этому, мы решили очень чётко разграничить зоны ответственности: несмотря на то, что некоторым из членов команды достались не самые увлекательные задания.

2. Сбор Low Hanging Fruits

На мой взгляд главным секретом нашего успеха были: огромный ежедневный опыт проектов и правильная приоритизация задач. Еще в прошлом году мы смогли захватить целый офис и удерживать его всю игру просто за счёт быстро взломанных простых уязвимостей. В этом году мы подошли к проблеме централизовано и составили список таких уязвимостей.

ms17-010; ms08-67; SMBCRY; LibSSH RCE; HP DATA Protectoer; HP iLo; ipmi; Cisco Smart Install; Java RMI; JDWP; JBOSS; drupalgeddon2; weblogic; heartbleed; shellshock; ibm websphere; iis-webdav; rservices; vnc; ftp-anon; NFS; smb-null; Tomcat

Далее был написаны два сервиса checker и penetrator, которые в автоматизированном режиме, используя публичные эксплойты и metasploit, сначала проверяли уязвимости, а потом пытались их проэксплуатировать. На вход утилита принимала отчёт nmap-а, что в итоге дополнительно ускорило процесс.

3. Эксплуатация уязвимостей нетиповых (для нас) технологий (АСУ ТП, IoT, GSM)

Мы чаще всего делаем проекты для банков и прочих финансовых организаций. SCADA-системы если и встречаются, то скорее в стиле: «Если вы смогли получить сетевой доступ к скаде, зафиксируйте это и зачтём это одним из критериев успеха проекта». Поэтому хорошего прикладного опыта анализа защищенности АСУ ТП у нас нет. Это в свою очередь привело к тому, что за неделю до StandOff-а мы экстренно сели изучать типовые уязвимости. С IoT и GSM ситуация еще плачевнее: если IoT иногда встречается в проектах, то GSM мы видели только на предыдущих StandOff-ах.

Таким образом, во время подготовки мы выделили двух отдельных людей на АСУ ТП, и еще двоих —на GSM и IoT. 1-я группа за подготовительную неделю выписала типовые подходы к пентесту SCADA-систем, а также подробно изучила видео, посвящённое прошлогодней инфраструктуре АСУ ТП. Также ребята выкачали порядка 200 гб различных HMI, драйверов и другого софта, имеющего прямое отношение к контроллерам. Что касается GSM и IoT-а, то тут мы подготовили несколько железок, прочитали все доступные статьи по GSM и надеялись, что этого будет достаточно. (SPOILER: На самом деле нет!)

4. Подготовка внешней инфраструктуры и оборудования

Понимая, что наша команда в этом году будет достаточно большой, мы сразу решили, что нам нужно дополнительное оборудование. Далее будет список предложений, который мы собрали внутри команды, знаком "+" отмечено что мы в итоге взяли:

— кофемашина;
+- CUDA-сервер (с собой не брали, но при этом использовали);
+ запасной ноутбук;
+ WI-FI роутер;
+ управляемый свитч;
+ сетевые кабели различной длины (20 шт);
+ пилот (3 шт);
+ Wi-fi Alfa (3 шт);
+ rubber-duck (2 шт);
— proxmark;
— фотоаппарат.

Что касается инфраструктуры, это отдельная песня. Уже в прошлом году мы поняли, насколько полезно использовать CUDA-станцию, взломав несколько хендшейков, поэтому не было никаких сомнений в необходимости её применения. Важно, что в этом году, также как и в прошлом, все атакующие были за NAT-ом, что в целом отметало возможность reverse-коннектов из DMZ. Зато у абсолютно всех хостов должен был быть доступ в интернет, кроме узлов АСУ ТП. В связи с этим мы приняли решение поднять три сервера listener-а, доступных из сети интернет. Также для простоты pivoting-а и закрепления мы использовали собственный OpenVpn сервер с включенным режимом client-to-client. К сожалению, автоматизировать процесс подключения шлюза невозможно, поэтому примерно 12 часов из 28 один из членов команды занимался работой со шлюзами.

5. Разработка доп. методов persistence и hardenin

Наш прошлый опыт выступления на StandOff очень наглядно показал, что мало успешно взломать сервер: важно не дать другим на нём закрепиться. Поэтому достаточное внимание было уделено RAT-у с новыми сигнатурами и скриптам по укреплению защиты Windows. RAT мы использовали свой стандартный, немножко поменяв методы обфускации. С правилами всё было немного сложнее. В целом мы определили для себя следующий набор скриптов:

- закрытие SMB и RPC;
- перенос RDP на нестандартный порт;
- отключение обратимого шифрования, guest-аккаунтов и других настроек из security baseline.

Для Linux был разработан специальный init-script, который закрывал все порты, открывал SSH на нестандартном порту и прописывал публичные ключи команды для доступа к SSH.

II. Брифинг

17-го мая, за 5 дней до StandOff-а был проведен брифинг для атакующих. В ходе него всплыло множество информации, которая оказала влияние на нашу подготовку.

Во-первых, организаторы опубликовали карту сети, и это стало для нас большим подспорьем. Мы смогли заранее поделить зоны ответственности, актуализировать сегменты сети, а главное понять, что же все-таки сеть из себя представляет. На мой взгляд самым важным заявлением, которое прозвучало на брифинге, была фраза о том, что сеть АСУ ТП будет доступна только из одного сегмента, и этот сегмент не будет защищен. Более того, больше всего баллов будут давать за АСУ ТП и защищённые офисы, а организаторы прямо поощряют борьбу за сети между хакерами.

Мы восприняли эту информацию примерно так: «Тот кто захватит bigbrogroup — скорее всего победит в игре». Всё дело в том, что наш опыт подсказывал нам: какие бы наказания организаторы не придумывали за простой сервиса, защитники будут ронять уязвимые сервисы, если не смогут их запатчить. Ведь гораздо страшнее, когда со сцены крупнейшей конференции по ИБ объявят о том, что вы прошляпили хакеров, чем если у вас отнимут какие-то игровые баллы. Наша теория подтвердилась, но об этом мы подробно расскажем во 2-й статье.

В итоге мы решили разделить всю команду на 4 части:

1. Bigbrogroup. Это была задача, которой мы отвели наибольший приоритет. В команде были задействованы люди, имеющий наибольший опыт взлома внутренней инфраструктуры у разных заказчиков. Всего эта мини-команда состояла из 5 человек. Их цель была — как можно быстрее закрепиться в домене и отсечь другие команды от доступа в АСУ ТП.

2. Wireless Network. Команда, которая отвечала за наблюдениями за Wi-Fi, отслеживала новые точки, перехватывал хендшейки и брутила их. Также в их задачи входил GSM, но в первую очередь надо было всё-таки захватить Wi-Fi и отсечь от него другие команды.

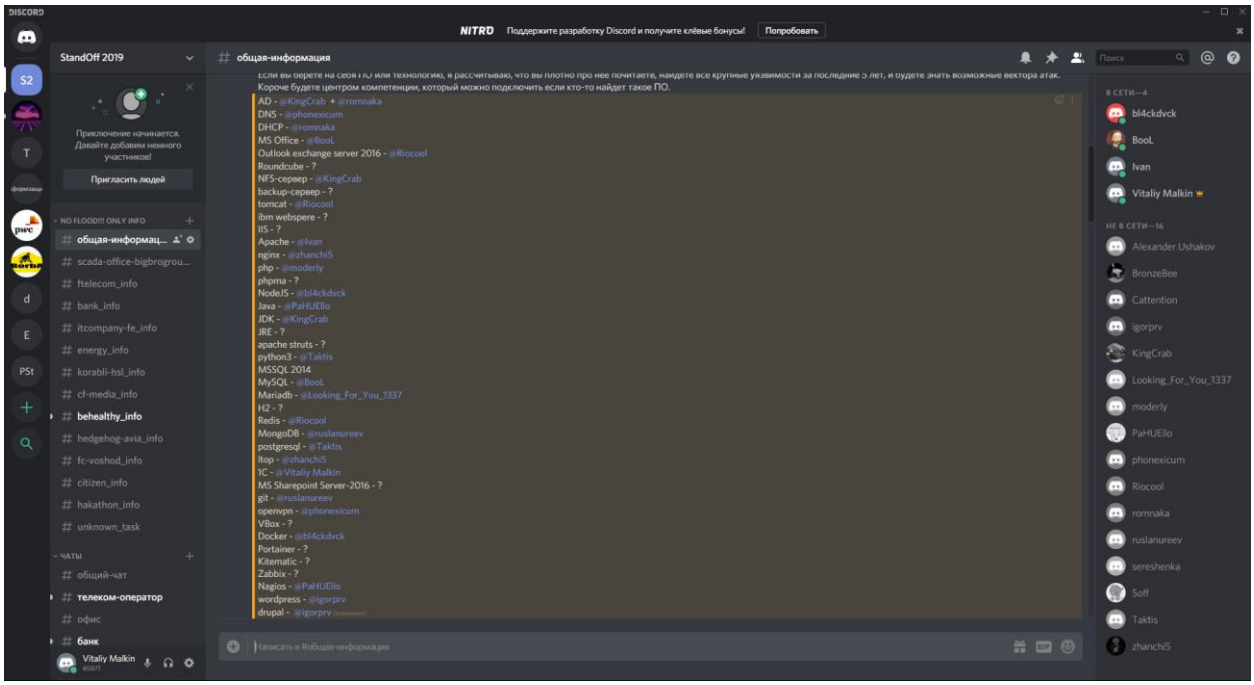
3. Unprotected networks. Команда, которая первые четыре часа ковыряла все незащищённые сети на предмет уязвимостей. Мы понимали, что за эти четыре часа в защищённых сегментах не произойдет ничего суперважного, а если и произойдет, то защитники это откатят.

Поэтому сфокусировались на том, что могло необратимо измениться. Как оказалось — не зря. Эта же группа через четыре часа приступила к анализу защищённых сегментов.

4. Scanners group. Организаторы напрямую заявили, что сети будут меняться, поэтому у нас было два человека которые непрерывно сканировали сеть на предмет изменений. Автоматизировать это было не так легко, потому что под разные сети, в разное время необходимы были различные настройки. К примеру, в первый час на сеть fe.phd у нас отлично работал nmap в T3 режиме, а через 12 часов еле-еле работал в T1.

Ещё одним важным вектором для нас стал список ПО и технологий, опубликованный организаторами. Мы постарались для каждой из технологий создать свой центр компетенций, который мог очень быстро помочь и посмотреть типовые уязвимости.

Для некоторых сервисов мы нашли очень интересные уязвимости, но эксплойтов в публичном доступе не было. Так было, например, с Redis Post-exploitation RCE. Мы были уверены, что эта уязвимость появится в игровой инфраструктуре, поэтому решили написать свой собственный 1-day эксплойт. Конкретно для этой уязвимости 1-day написать не удалось, но в целом у нас на руках было около пяти непубличных эксплойтов, которые мы были готовы использовать.



К сожалению, мы не успели разделить все технологии, но это было не так страшно. Основной набор мы охватили, и этого оказалось достаточно. Был также список контроллеров АСУ ТП, который мы тоже разобрали и постарались к нему подготовиться.

Готовясь к битве, мы готовили несколько инструментов для незаметного подключения к физической сети АСУ ТП. Например, мы реализовали дешевый аналог Pineapple-а при помощи raspberry. Модуль подключался по Ethernet к промышленной сети и по GSM — к управляющему сервису. Далее мы могли удаленно сконфигурировать Ethernet-подключение и раздать его на месте при помощи встроенного Wi-Fi модуля. К сожалению, на брифинге организаторы чётко дали понять, что подключаться физически к АСУ ТП нельзя, поэтому мы оставили этот модуль до лучших времен.

Достаточно много информации было касательно банка, оффшорного банка и работы антифрода. Но узнав, что денег в нём не очень много, мы решили не готовиться к этому заранее, а придумать что-то по ходу.

Суммируя, нами был проделан достаточно большой объём работы при подготовке. Важно отметить, что помимо очевидных плюсов в виде успешного выступления на StandOff были ещё и не очевидные.

- Такая подготовка — это отличный способ отвлечься и заняться тем, что давно хотел попробовать и поисследовать, а в рамках проектной деятельности просто не было времени.
- У нас не бывает проектов, которые задействуют всю команду целиком в рамках одной задачи, поэтому получился неплохой тимбилдинг, преследующий конкретные цели.
- Многое из того что мы сделали можно будет использовать в реальных проектах, так что помимо расширения компетенций мы еще и получили готовые инструменты.

Сейчас, описав вот это всё в тексте, я понимаю, что ничего такого грандиозного мы не совершили, как казалось до этого со стороны. Мне вообще кажется, что основной причиной победы нашей команды стал правильно организованный этап подготовки. А что непосредственно происходило в ходе самого StandOff — я расскажу во второй статье цикла.

Подробнее: https://habr.com/ru/post/453834/