Здравствуйте уважаемые члены комиссии! Вашему вниманию представляется выпуская квалификационная работа на тему “Метод и система сбора поверхности атаки для внешнего периметра организации”

Актуальность работы обусловлена желанием иметь простой и бесплатный инструмент для определения уязвимостей сетей небольших компаний и частных лиц, которые всё чаще предпочитают разворачивать используемые сервисы на собственных вычислительных мощностях, при этом не имея ни бюджетов, ни достаточной квалификации в области информационной безопасности.

Для реализации задачи используется интерпретируемый язык программирования Питон, сканер сетей Нмап и платформа для эмуляции действий АПТ группировок Митре Калдера. В качестве лабораторной среды средствами ВиртуалБокс разверернуты 3 машины: Атакующая с Кали Линукс, где установлены Калдера, Нмап, Питон и, собственно, работает скрипт. В качестве потенциально уязвимых машин развернута известная машина Метасплоитабле 3 и развернутые на Линукс Минт докер-контейнеры из репозитория ВулХаб.

В основу алгоритма работы скрипта легли первые 4 этапа килчейна митре атак.:

1 этап «РАЗВЕДКА», в нашем случае сведен к сканированию хоста или подсети средствами популярного сканера Нмап. Сканирование производится в 3 этапа: быстрый поиск хостов, полное сканирование портов и определение открытых, сканирование найденных портов на предмет запущенных служб и их версий на основании чего скрипт от портала Вулнерс.ком дает список уязвимостей с номером, CVSS, ссылкой на описание и меткой наличия эксплойта.

2 этап «Подготовка ресурсов» состоит из загрузки эксплойтов с сайта sploitus.com с сохранением в папку Пэйлоадс Калдеры, а так же формирование соответствующих ЯМЛ файлов Абилити и Адвёрсари для Калдеры.

3 этап «Первоначальный доступ» на этом этапе происходит выполнение созданных ранее инструкций. Скрипт запускат Калдеру, разворачивает локальный Агент, который будет использоваться в Операциях. После чего средствами АПИ Калдеры на основе созданных Адверсари создаются и запускаются Операции, т.е. непосредственное исполнение соответствующих Абилити и эксплойтов, входящих в Адверёрсари.

4 этап «Исполнение», происходит удаленное исполнение кода, содержащего команды загрузки и запуска Агента Калдеры Сэндкэт на атакуемом хосте.

На этом поставленная задача считается выполненной, так как получен доступ к удаленному хосту и дальнейшие действия уже зависят от целей злоумышленников и происходят во внутреннем периметре информационной системы.

На данном слайде представлены примеры результатов работы основных компонентов:

Nmap в результате своей работы формирует временный файл с простым текстовым выводом, который оказался удобнее для парсинга, чем структурированный XML файл.

Питон, помимо запуска Нмап и Калдеры, выполняет обработку данных и формирует файл VULNS.json, содержащий данные по каждой уязвимости от найденного IP до созданного UUID адверсари. Так же создаются файлы эксплойтов с расширениями, соответствующими языку, и ЯМЛ файлы абилити и адверсари, данные о которых так же включаются в VULNS.json.

Калдера в свою очередь создает и запускает операции получая команды от скрипта по АПИ и выступает средством отображения полученных результатов, таких ка ход операции и удачно установленные агенты.

В завершение хочу сказать, что бесплатными общедоступными средствами можно реализовать автоматическое выявление наиболее критичных уязвимостей небольшой сети к атакам злоумышленников низкого и среднего уровня подготовки. В качестве рекомендаций по устранению уязвимостей предлагается ознакомиться с описанием реализованных уязвимостей на сайте Вулнерс.ком (ссылки сохранены в файле Vulns.json).

Спасибо за внимание.