Раздел: Жизненный цикл ИБ
Модуль 4: Целенаправленные атаки. Модуль 4. Практическое задание. Создание тактики реализации компьютерной атаки (HW).
Выполнил: Александр Ганицев

Условия задания:

Дана коммерческая организация, которая занимается грузоперевозками. В организации работает несколько отделов:

- менеджеры по грузоперевозкам,
- бухгалтерия,
- кадровая служба,
- служба ИТ.

Дополнительная информация, которая вам известна:

- есть сайт, размещённый на собственных мощностях;
- DMZ-зона отсутствует;
- удалённых сотрудников нет;
- менеджеры звонят с использование IP-телефонии.

Что нужно сделать

Постройте жизненный цикл атаки, используя матрицу MITRE. Формат представления жизненного цикла атаки можете посмотреть в примере из модуля «Целенаправленные атаки»:

1. Разведка — сканирование публичных IP-адресов, чтобы найти открытый порт 445.
2. Подготовка ресурсов — подготавливаем необходимые средства для атаки (готовим эксплойты, ищем в сети «слитые» корпоративные учетные записи).
3. Первоначальный доступ — эксплуатация найденных уязвимостей и получение первоначального доступа к системе.
4. Выполнение — имея первоначальный доступ, находим критическое ПО и начинаем шифрование данных.
5. Закрепление — прописываем себя в автозапуск, чтобы при перезагрузке или выключении рабочего места пользователя доступ сохранялся.
6. Повышение привилегий — нет точной информации.
7. Предотвращение обнаружений — нет точной информации.
8. Получение учётных данных — в этом нет необходимости.
9. Исследование — попытки сканировать заражённую сеть для поиска дополнительных уязвимых компьютеров.
10. Перемещение внутри периметра — дополнительное заражение известных машин.
11. Сбор данных — нет точной информации.
12. Управление и контроль — создаём новый защищённый VPN-канал до управляющего сервера злоумышленника.

13. Эксфильтрация данных — передаём данные по защищённому каналу связи.
14. Воздействие — проводим дефейс ресурсов организации.

В отличие от приведённого примера, у вас не должно остаться ответов в формате «нет информации», «не требуется» и т. д.

Выполнение задания.

1. Разведка.

Собираем информацию об данной коммерческой организации из всевозможных источников. Пробиваем порт 445 публичных IP адресов организации. Выясняем IP сайта организации и другие возможные зарегистрированные IP адреса. Также выясняем, чьими услугами IP-телефонии пользуется организации, проверяем, если открыт стандартный порт 5060 (sip). Так как организация не использует VPN, DMZ, должна существовать возможность взлома. Используем следующие инструменты:

- RIPE
- Nmap
- Сканеры: OpenVAS, Masscan и т. д.
- OSINT

2. Подготовка ресурсов — подготавливаем необходимые средства для атаки (готовим эксплойты, ищем в сети «слитые» корпоративные учетные записи). После проведённой разведки, по полученным данным, используем следующие инструменты:

- theHarvester
- Результаты OSINT — собранные из разных источников данные, например одни и те же «ники» в соцсетях, также могут быть логином в корпоративных системах.
- Exploit-DB, Metasploit Framework — результаты сканирования известных адресов (открытые порты, службы).

Оцениваем сложность подготовки эксплойта, также проверяем наличие публичного эксплойта.

3. Первоначальный доступ — эксплуатация найденных уязвимостей и получение первоначального доступа к системе. Используем следующие инструменты:

- Gophish — бесплатная утилита для формирования фишинговых писем. На выявленные адреса электронной почты высылаем подобные письма.
- Существующие учётки (OSINT) — результаты OSINT и theHarvester используем для попыток зайти под легальным пользователем в инфраструктуру компании. Пробуем зайти в учётные записи используя “слитые” пароли.
- Exploit-DB — выявив версии ОС, пробуем реализовать подготовленные эксплойты.

4. Выполнение — имея первоначальный доступ, находим критическое ПО и начинаем шифрование данных. Наши инструменты на этом этапе:

- Успешный фишинг (Gophish) — открытие ссылок в фишинговых письмах или запуск файлов, скачанных с неправильных ресурсов, позволят нам выполнять команды на компьютере жертвы, и возможно получить полный доступ к целевой системе.
- Intercepter-NG — пробуем разместить наш вредоносный баннер на сайте организации.

5. Закрепление — прописываем себя в автозапуск, чтобы при перезагрузке или выключении рабочего места пользователя доступ сохранялся. Наши варианты действий:

◦ Добавление себя в автозагрузку системы.
◦ Внедрение в исполняемый файл (например запуск браузера) для постоянного запуска удалённого доступа после определённых действий пользователя.

6. Повышение привилегий — после этапа закрепления, на основании данных разведки и подготовки ресурсов, осуществляем “взлом”:

◦ Exploit-DB — поиск существующих эксплойтов под скомпрометированную версию операционной системы.
◦ SearchSploit — поиск готового эксплойта для выявленной нами операционной системы.

7. Предотвращение обнаружений — проводим отключение средств защиты информации или сокрытие исполнения нашего боевого файла. Варианты дальнейших действий:

◦ Exploit-DB — поиск эксплойтов для обхода средств защиты информации.
◦ Внедрение в исполняемый файл, например запуск браузера, для того, чтобы средства защиты информации думали, что все действия выполняет браузер.

8. Получение учётных данных — Сбор информации о пользовательских данных в инфраструктуре. Используем следующие инструменты:

◦ Enum4linux — инструмент, предназначенный для сбора информации о домене Active Directory (если мы нащупали его в результате нашей разведки).
◦ Mimikatz — утилита, позволяющая «разбирать» NTLM-хэш паролей в системе, если нам удалось сделать дамп памяти процесса.

9. Исследование — пытаемся сканировать заражённую сеть для поиска дополнительных уязвимых компьютеров, строим новые вектора атак на целевую инфраструктуру. Возможные инструменты здесь:

◦ Zenmap — автоматически строит карты сети организации.
◦ Enum4linux — соберёт доступные логины Active Directory.

10. Перемещение внутри периметра — дополнительное заражение известных машин, для получения доступа к ним. Тут мы используем:

◦ Exploit-DB — поиск существующих эксплойтов под найденные компьютеры и серверы.
◦ SearchSploit — поиск готового эксплойта для найденного компьютера или сервера.
◦ Ручной запуск программ для удалённого доступа — в случае получения доступа к паролям разных учётных записей возможен легитимный заход на найденное рабочее место и запуск программ для удалённого доступа.

11. Сбор данных — получаем доступ к данным, передаваемым внутри организации. Основые инструменты:

◦ Wireshark — сниффер трафика. Прослушиваем трафик внутри сети. Пытаемся получить доступ к передаваемым данным организации.
◦ Ettercap — применяем для организации различных видов «спуфинга», то есть перенаправления трафика жертвы через себя.

12. Управление и контроль — создаём новый защищённый VPN-канал до нашего управляющего сервера, проводим управление скомпрометированными ресурсами. На этом этапе пользуемся:

◦ Metasploit Framework — создаём сервера для принятия удалённого соединения и возможности управления заражёнными компонентами инфраструктуры.
◦ Создаём собственный сервер управления — самостоятельно написанный сервер со своими протоколами передачи информации, которые не сможет проверить IDS/IPS.

13. Эксфильтрация данных — передаём данные по защищённому каналу связи. Для этих целей используем вышеупомянутые инструменты:

◦ Собственный сервер управления — самостоятельно написанный сервер со своими протоколами передачи информации, которые не сможет проверить IDS/IPS.
◦ Metasploit Framework — сервер, созданный с помощью этого фреймворка.

14. Воздействие — проводим дефейс ресурсов организации или, в зависимости от целей данной атаки, осуществляем:

◦ Собственный сервер управления — отправляем команды на совершение таких действий, как например выключение, перезагрузка систем и т. д.
◦ Metasploit Framework — отправка по готовым протоколам необходимых нам команд.
◦ Задания по расписанию — в этом случае нет отправки команды, которая может быть перехвачена IPS.

Последний пункт предполагает, какое воздействие ставится целью, в данном задании, по моему мнению, основная цель – это доступ к бухгалтерским и финансовым данным компании и кража или вымогательство финансовых средств с дальнейшим их обналичиванием. Не порядочные действия, хороши для использования в обучающих целях!