Раздел: Жизненный цикл ИБ
Модуль 4: Целенаправленные атаки. Модуль 4. Практическое задание. Защитные механизмы).
Выполнил: Александр Ганицев

Продолжаем изучать матрицу MITRE на практике.

Представьте, что вам как специалисту по информационной безопасности поручили организовать защиту организации от всевозможных компьютерных атак. Дополнительно вы сами расписали жизненные циклы атак, или же вам принесли уже готовые материалы. Ваша задача (на этом этапе) высокоуровнево построить систему защиты: подобрать классы средств защиты информации.

Способов реализации этой задачи достаточно много, но вы решили воспользоваться готовыми сценариями атак.

Задание:

Составьте список средств защиты информации, которые вы можете предложить для нейтрализации атаки,придуманной в юните 3.

Предоставьте ответ в виде решений по обеспечению информационной безопасности, таких как:

- разделение локальных сетей,
- обучение пользователей,
- установка сетевых средств защиты информации
- установка хостовых средств защиты информации и другие решения.

Дополнительное условие:

Предложенные средства защиты информации должны быть указаны с названием вендора и модели (примеры мы разбирали в модуле, посвящённом Blue Team). Также должны быть прописаны номера этапов в вашем сценарии (согласно матрице MITRE), которые перекрываются данным средством защиты, например межсетевой экран CheckPoint перекрывает этап 3 (первоначальный доступ).

Обратите внимание, что ещё необходимо предусмотреть организационные (обучение персонала, разработка приказов и инструкций) и технические (разделение сетей) меры защиты.

План атаки.

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.

Нейтрализация 14-ти этапов атаки по матрице MITRE.

Учитываем особенности IT инфраструктуры - коммерческая организация, которая занимается грузоперевозками. В организации работают отделы:

1. менеджеры по грузоперевозкам,
2. бухгалтерия,
3. кадровая служба,
4. служба ИТ.

IT инфраструктура была устроена таким образом:

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

1. Разведка.

1.1. Самым важным этапом для усложнения/предотвращения попыток разведки это создание DMZ зоны, в которую выносится веб-сайт, почтовый сервер и IP-телефония организации. Сетевая структура разделяется на две подсети: внутреннюю и DMZ, для усложнения возможности взлома и получения несанкционированного доступа к ресурсам организации.

1.2. На обоих брэндмауэрах закрываем порт 445 для входящих соединений.

1.3. Для IP-телефонии закрываем порт 5060 (стандартный), на сервере добавляем адреса наших sip-провайдеров в исключения, остальные блокируем, устанавливаем и настраиваем fail2ban.

1.4. Взаимодействуем только с разрешенными адресами, вводим контроль по IP или MAC адресам.

1.5. Сменяем все пароли по умолчанию на свои, сложные, длинной не меньше 12 символов. Настраиваем правильную реакцию IP-АТС на ввод неверной пары логин/пароль (для Astersk – alwaysauthreject=yes).

1.6. Устанавливаем доступ к международной связи только для сотрудников, которым она необходима. Список сотрудников строго коррелируется с новыми/уходящими сотрудниками. В обязательства сотрудников техподдержки входит настройка и блокирование доступа к IP телефонии (равно и других учётных записей) в организации (найм, временное отстранение от службы, увольнение, долгий отпуск по болезни и т.д.).

2. Подготовка ресурсов.

2.1. Для предотвращения атакующими использования эксплойтов все компоненты информационной системы организации обновляются до последних доступных версий: серверные и клиентские ОС, специализированное ПО, firmware брэндмауров, коммутаторов, принтеров и прочего оборудования.

2.2. Сотрудники IT отдела проводят исследование на тему hardening the perimeter, закрывают порты, отключают неиспользуемые службы.

2.3. Для всех сотрудников организации планируются и проводятся не реже, чем раз в 3-6 месяца курсы и образовательные лекции на тему информационной безопасности.

2.4. Сотрудники обязаны жёстко разделять личные учётные записи и все остальные, связанные с работой. Все почтовые учётные записи, различные публичные и облачные эккаунты переводятся на 2ФА.

3. Первоначальный доступ.

3.1. IT отдел должен статъ родным для всех сотрудников компании. Сотрудники отдела решая различные технические проблемы и помогая людям, периодически проводят инструктаж и напоминают о важности бдительности в области защиты информации. Проводят семинары, где объясняют как различать и противодействовать фишинговым, ransomware и прочим атакам.

3.2. Политика паролей настраивается на регулярную смену паролей (45 дней), пароли должны соответствовать уровню сложности (8-12 символов, состоящих из циферно-буквенного ряда с использованием специальных символов.

3.3. В компании настраивается средства антивирусной защиты (Лаборатория Касперского) и защиты от спама на уровне входящего почтового трафика. (Proofpoint, MS Quarantine)

4. Выполнение.

4.1. Проводится антифишинговая кампания среди сотрудников, устанавливается и настраивается антивирус Лаборатории Касперского. Все системы организации должны быть защищены пакетом антивирусных программ, регулярно обновляться и сканироваться. Инциденты купируются специалистами IT отдела.

4.2. Настраивается и поддерживается средство для мониторинга веб-трафика и блокирования атак на веб-приложения (Positive Technologies Application Firewall,«Континент WAF», Nemesida WAF, BI.ZONE WAF – выбор и конфигурация согласуется и утверждается начальником IT отдела).

4.3. Настраиваются файерволы UserGate NGFW или Check Point NGFW для внешнего периметра и подобный NGFW или Ideco UTM решения для внутреннего барьера защиты.

4.4. Почтовый сервер настраивается для фильтрации входящей почты от потенциального спама, фишинговых и ransomware атак. Возможно использование систем Proofpoint, Barracuda.

5. Закрепление.

5.1. Сотрудники IT отдела планово проводят сканирование всех систем организации на наличие rootkit, вирусов, червей, malware, adware, и прочих вредоносных программ.

5.2. В систему на объектах КИИ, рассмотреть вопрос внедрения СЗИ от НСД (Dallas Lock СД3, «Аккорд-АМД3», ПАК «Соболь»,ViPNet SafeBoot.) российского производства.

6. Повышение привилегий.

6.1. Для предотвращение повышения привилегий при взломе системы, или первоначальном проникновении злоумышленников, необходимо приобрести, настроить и проводить круглосуточный мониторинг состояния SIEM системы - Kaspersky KUMA.

6.2. Необходимо настроить IDS/IPS: HIDS – OSSEC и NIDS – Snort.

7. Предотвращение обнаружений.

7.1. Плановый мониторинг всей инфраструктуры организации посредством SIEM и IDS/IPS системы.

7.2. Плановый мониторинг антивирусного барьера.

8. Получение учётных данных.

8.1. Проводится hardening AD домена.

8.2. Настраиваются политики учётных записей (создание, заморозка, деактивация, удаление, лишение доступа, ограничения доступа).

8.3. Проведение регулярных сессий с пользователями компьютерных систем. Повышаем бдительность сотрудников к приходящим почтовым сообщениям, звонкам, объясняем принципы социальной инжинерии. Даём советы по обеспечению профессиональной и личной информации.

9. Исследование.

9.1. Предотвращаем любые попытки вторжения, аномальных обращений к объектам сетевой инфраструктуры организации посредством мониторинга систем обнаружения SIEM.

9.2. Предотвращаем попытки вторжения поредством вирусов, звонков и установки устройств для снятия информации. В процессе разрастания инфраструктуры организации рассматриваем возможности масштабирования процессов ИБ.

9.3. Исследуем все системы на наличие потенциальных уязвимостей посредством сканеров уязвимости, рассмотреть следующие продукты - OpenVAS, Nikto, OWASP ZAP.

10. Перемещение внутри периметра.

10.1. Постоянное обновление ПО, firmware для всех элементов инфраструктуры.

10.2. Периодическая смена паролей.

10.3. При необходимости, для ключевых систем в финансовом отделе, для доступа к важным приложениям, используем комбинацию 2ФА и OTP, а также системы уровня DLP, которые

предлогается встроить в решения контроля рабочего времени и мониторинга персонала. (“Стахановец” и “Staffcop”).

10.4. Мониторинг аномальной активности учётных записей, вне обычных временных режимов работы, смены паролей, добавления новых систем в домен, и т.д.

10.5. Одним из важнейших компонентов поддержания системы в нормальном состоянии, создаём и поддерживаем систему резервного копирования.

11. Сбор данных.

11.1. Вырабатываем методы распознавания сниффинг и спуффинг атак. Повышаем бдительность сотрудников. Определяем вознаграждение при выявлении подобного инциента.

11.2. Используя DLP решение, выявляем нестандартную активность сотрудников и принимаем меры.

12. Управление и контроль.

12.1. Используя SIEM систему, отслеживаем неспецифический для организации исходящий и входящий сетевой трафик, исследуем пакеты, в которых может маскироваться управленческая деятельность злоумышленников.

12.2. В своей сети ведём чёткую инвентаризацию всех существующих хостов и систем, при добавлении новых, расследуем и действуем.

12.3. Регулярно проводим события Disaster Recovery, для скорейшего восстановления работоспособности организации при серьёзной атаке.

12.4. Для предотвращения утечки информации и нанесения организации ущерба вырабатываем процедуры отрезания сети от внешнего мира для скорейшего восстановления работоспособности всех поражённых систем. Тщательным образом проверяем всю инфраструктуру перед подключением в сеть Интернет.

13. Эксфильтрация данных.

13.1. Смотри описаное выше.

14. Воздействие.

14.1. Здесь сходятся все вышеупомянутые шаги по обеспечению безопасности организации.

Обеспечение безопасности любой организации – процесс модульный и ступенчатый, он охватывает весь жизненный цикл, от создания до закрытия структуры, посему, безопасностью необходимо заниматься в режиме предиктор-корректор. Решения вырабатываемые на каждом этапе способны серьёзнейшим образом повлиять на остальные. Важнейшим элементом безопасности является сотрудник, от повышения квалификации, осознанности которого во многом зависит безопасность цифровой инфраструктуры.