Практическое задание. Создание тактики компьютерной атаки.
(Последовательность действий в соответствии с тактиками матрицы MITRE)

Сценарий возможной атаки на коммерческую организацию
(Сценарий разработан с целью защиты организации от различных возможных киберугроз и обеспечения непрерывности её работы)

1. Разведка – сканируется веб-сайт организации на наличие уязвимостей. Проверяются ресурсы, размещенные на портах 80 или 8080. Сканирование на наличие поддоменов и имэйл адресов.

2. Подготовка ресурсов - подготовка необходимых средств для атаки, включая эксплойты и поиск «слитых» корпоративных учётных записей.
Эксплойты - это программы или скрипты, которые используют уязвимости в программном обеспечении для выполнения несанкционированных действий. Злоумышленники могут использовать эксплойты для эксплуатации уязвимостей в операционной системе, приложениях или сетевых службах для получения первоначального доступа к системе.
«Слитые» корпоративные учётные записи - это учётные данные пользователей, которые были украдены или проданы на чёрном рынке. Злоумышленники могут использовать эти учётные данные для получения доступа к системам организации даже без использования эксплойтов.

3. Первоначальный доступ - эксплуатация найденных уязвимостей и получение первоначального доступа к системе.
После того как злоумышленники определили уязвимость в системе, они могут попытаться её эксплуатировать для получения первоначального доступа. Для этого они могут использовать различные методы, например, переполнение буфера, внедрение SQL-кода или удалённый код выполнения. Так как в организации не используется DMZ (демилитаризованная зона), выступающая обычно буфером и затрудняя проникновение, то используя уязвимости веб-сайта, возможно сразу попадание во внутреннюю сеть компании.

4. Выполнение - после получения первоначального доступа злоумышленники могут попытаться найти критическое ПО и начать шифрование данных.
Критическое ПО - это программное обеспечение, которое необходимо для работы системы. Злоумышленники могут попытаться зашифровать критическое ПО, чтобы сделать его недоступным для пользователей. Это может привести к нарушению работы системы и потере данных.

5. Закрепление - прописывание себя в автозапуск для сохранения доступа при перезагрузке или выключении рабочего места пользователя.
Злоумышленники могут прописать себя в автозагрузку, чтобы сохранить доступ к системе даже после перезагрузки или выключения компьютера. Это позволит им продолжать свою деятельность даже после обнаружения и устранения уязвимости.

6. Повышение привилегий - получение права администратора системы. Подменяется токен доступа (Windows), редактируется матрицу доступа rwx в (Linux). Это позволит злоумышленникам получить полный контроль над системой и выполнять любые действия, включая установку вредоносного ПО, изменение конфигурации сети и т. д.

7. Предотвращение обнаружений - злоумышленники маскируют свою активность, используя техники обфускации кода и запутывания следов. Обфускация кода - это процесс преобразования исходного кода программы таким образом, чтобы его было сложно понять и проанализировать. Запутывание следов - это метод сокрытия следов своей активности в системе, например, путём удаления временных файлов или изменения лог-файлов. Отправка отчётов по действиям, по разрешённым протоколам и с разрешённых адресов.

8. Получение учётных данных - анализ авторизованных на сервере пользователей, попытки украсть или подделать учётные данные пользователей для получения дополнительного доступа к системе. Учётные данные могут быть украдены различными способами, такими как фишинг, социальная инженерия, брутфорс паролей, перехват и т. д.

9. Исследование - сканируется заражённая сеть для поиска дополнительных уязвимых компьютеров и внутренней АТС. Злоумышленники могут использовать различные инструменты, такие как Nmap, Metasploit и другие, для обнаружения открытых портов, уязвимостей и других потенциальных целей атаки. Могут анализироваться рабочие столы сотрудников, открытые вкладки в браузере, сетевые папки, может прослушиваться трафик, слушаться телефонные разговоры (т.к. в организации используется IP-телефония). Атакующие будут пытаться найти максимальное количество общих сетевых ресурсов для атаки на них.

10. Перемещение внутри периметра - заражаются дополнительные машины, внутренняя АТС. Злоумышленники будут пытаться положить заражённые файлы на сетевые папки, предпринимать попытки атаковать роутеры, пытаясь попасть в другие подсети, атаковать АТС, что помимо прослушивания разговоров, может позволить им совершать звонки от имени компании, а также принимать их. После получения первоначального доступа к системе злоумышленники могут установить дополнительные вредоносные программы на другие компьютеры в сети организации. Всё это может быть использовано для расширения зоны контроля и сбора дополнительной информации.

11. Сбор данных - собирается по максимуму всё что представляет интерес. Данные со всех носителей, данные вводимые пользователями, информация из браузеров, видео, аудио, список пользователей, их пароли, почты, персональные данные, данные о конфигурации сети и т.д. Эта информация может быть использована для продажи, шпионажа и проведения более сложных атак.

12. Управление и контроль - создаётся новый защищённый VPN-канал до управляющего сервера злоумышленников. Этот канал будет использоваться для удалённого управления системой и передачи данных.

13. Эксфильтрация данных - передача данных по защищённому каналу связи за пределы организации. Для этого злоумышленники могут использовать зашифрованные каналы связи, например Tor или VPN.

14. Воздействие - проведение дефейса ресурсов организации, чтобы нарушить её работу и привлечь внимание к атаке. Нарушается работа веб-сайта или другого ресурса. Злоумышленники могут изменить содержимое сайта, сделать его недоступным или перенаправить трафик на другой ресурс.