1. Разведка.

Целью данного этапа является сбор информации для определения целей, планирования атаки и выполнения первоначального доступа. В данной ситуации собираем информацию об организации, сотрудниках. Сканируем публичные IP-адреса, чтобы найти открытый порт 445.

Собираем информацию следующего характера:

- Бизнес — информация об атакуемой рганизации (контрагенты, определение ролей сотрудников, изучение графика работы и режима поставок)
- Информация на сайтах организации
- Техническая информация из открытых источников (DNS-записи, цифровые сертификаты)
- Сбор информации об атакуемой сетевой инфраструктуре (Свойства доменов, топология сети, IP-адреса, средства сетевой защиты)
- Сбор информации об атакуемых пользователях (Имена сотрудников, адреса электронной почты, учетные данные)
- Активное сканирование (Сканирование блоков IP-адресов, поиск уязвимостей)

Инструменты для проведения разведки:

- OSINT
- OpenVAS, Masscan, Nmap
- RIPE
- Сайты поиска и социальные сети

2. Подготовка ресурсов.

Разработка ресурсов состоит из методов, в которых создаются, покупаются или компрометируются ресурсы, которые могут быть использованы для проведения атаки. К таким ресурсам относятся инфраструктура и учетные записи.

Используеются следующие возможные действия:

- Приобретение инфраструктуры (сервер, ботнет, домены, DNS-сервер, вредоносная реклама)
- Подготовка необходимых средств (вредоносное ПО, цифровые сертификаты, эксплойты)
- Создание и компрометация учетных записей (учетные записи эл. почты, учетные записи соцсетей)

Будут использованы следующие инструменты:

- Результаты OSINT

3. Первоначальный доступ.

Первоначальный доступ состоит из методов, которые используют различные векторы для входа и закрепления в сети. Методы, используемые для закрепления, включают целевой фишинг и использование уязвимостей общедоступных веб-серверов.

Возможны следующие действия:

- Фишинг (целевой фишинг с вложением, целевой фишинг со ссылкой)
- Эксплуатация уязвимостей общедоступного приложения
- Доступ через действительные аккаунты

Используются следующие интсрументы:

- Gophish
- Exploit-DB, Metasploit Framework
- Существующие учётки (OSINT)

4. Выполнение.

Выполнение состоит из методов, которые приводят к запуску кода в локальной или удаленной системе.
На данном этапе возможны следующие действия и инструменты:

- Эксплуатация уязвимостей в клиентском ПО
- Инструментарий управления Windows
- Интерпретаторы командной строки и сценариев
- Выполнение с участием пользователя (вредоносные файлы, ссылки и образы)

5. Закрепление.

Обеспечение автоматического восстановления соединения при перезапуске заражённой машины или сервера

- Загрузка раньше ОС (буткит, ROMMONkit, прошивка системы)
- Создание или изменение системных процессов
- Автозапуск при загрузке или входе в систему
- Запланированная задача (задание)
- Манипуляции с учетной записью
- Расширения браузеров

6. Повышение привилегий.

Получение более привилегированного доступа к системе (обычно административного). Чаще всего получение первоначального доступа к системе происходит под правами пользователя.
Распространенные подходы заключаются в использовании слабых мест системы, неправильных конфигураций и уязвимостей.
Возможны слежующие действия и интсрументы:

- Эксплуатация уязвимостей для повышения привилегий
- Изменение доменной политики
- Обход механизмов контроля привилегий
- Создание или изменение системных процессов
- Сценарии инициализации при загрузке или входе в систему

7. Предотвращение обнаружений.

Методы, используемые для уклонения от защиты, включают удаление/отключение защитного программного обеспечения или запутывание/шифрование данных и сценариев.
Возможные варианты действий и инструменты:

- Руткит
- Ослабление защиты (отключение или перенастройка средств защиты, отключение журналирования событий Windows, подмена предупреждений системы безопасности)
- Изменение процесса аутентификации
- Эксплуатация уязвимостей для предотвращения обнаружения
- Поддельный контроллер домена

8. Получение учётных данных.

Доступ к учетным данным состоит из методов кражи учетных данных, таких как имена учетных записей и пароли. Методы, используемые для получения учетных данных, включают кейлоггинг или сброс учетных данных.
Возможны следующие варианты действий и инструменты:

- Получение дампа учетных данных

- Прослушивание сетевого трафика
- Перехват вводимых данных
- Эксплуатация уязвимостей для получения учетных данных
- Незащищенные учетные данные
- Enum4linux — инструмент, предназначенный для сбора информации о домене Active Directory.
- Mimikatz — утилита, позволяющая «разбирать» NTLM-хэш паролей в системе.

9. Исследование.

Расширение кругозора о скомпрометированной инфраструктуре. Для этой цели сбора информации после компрометации часто используются собственные инструменты операционной системы.
Применяются следующие действия и инструменты:

- Изучение конфигурации сети
- Прослушивание сетевого трафика
- Изучение системных и сетевых служб
- Изучение учетных записей
- Zenmap — автоматически строит карты сети организации.
- Enum4linux — соберёт доступные логины Active Directory.

10. Перемещение внутри периметра.

Поиск дополнительных компьютеров и серверов для получения доступа и управления ими.
Возможные варианты:

- 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.

Получение доступа к данным, передаваемым внутри организации. Общие целевые источники включают в себя различные типы дисков, браузеры, аудио, видео и электронную почту. Общие методы сбора включают в себя захват снимков экрана и ввод с клавиатуры.
Возможны следующие действия и инструменты:

- Перехват вводимых данных
- Захват экрана
- Автоматизированный сбор данных
- Перехват сессии браузера
- Wireshark — сниффер трафика. Популярное программное обеспечение для прослушивания трафика внутри сети. Позволит получить доступ к передаваемым данным при условии отключённого шифрования.
- Ettercap — утилита, позволяющая проводить большой спектр атак. Наиболее часто применяется для организации различных видов «спуфинга», то есть перенаправления трафика жертвы через себя.

12. Управление и контроль.

При получении полноценного удалённого доступа в инфраструктуре просто необходимо проводить управление заражёнными ресурсами. Создаём новый защищённый VPN-канал до управляющего сервера злоумышленника. Возможные варианты:

- Metasploit Framework — создание серверов для принятия удалённого соединения и возможности управления заражёнными компонентами инфраструктуры
- Собственный сервер управления — самостоятельно написанный сервер со своими протоколами передачи информации, которые не сможет проверить IDS/IPS.

13. Эксфильтрация данных.

Методы получения данных из целевой сети обычно включают их передачу по каналу управления и контроля или альтернативному каналу. Могут включать сжатие и шифрование.
Для этих целей используем следующие возможные инструменты и действия:

- 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.

Воздействие состоит из методов, которые используют для нарушения доступности или целостности путем манипулирования бизнес-процессами и операционными процессами. Методы воздействия могут включать уничтожение или подделку данных.

Возможны следующие варианты действий и инструменты:

- Уничтожение и/или шифрование данных
- Манипуляции с данными
- Несанкционированное использование ресурсов
- Собственный сервер управления — отправка команд на совершение действий, например выключение, перезагрузка и т. д.
- Metasploit Framework — отправка по готовым протоколам команд.
- Задания по расписанию — в этом случае нет отправки команды, которая может быть перехвачена IPS.