Lateral Movement

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

- Узнать, что такое Lateral Movement

Lateral Movement

Lateral movement (или перемещение внутри периметра) характеризует то, как атакующий, используя существующие в системе механизмы, может перемещаться от одной машины к другой.

К таким механизмам относятся:

- программы для удалённого обновления приложений
- удалённое копирование файлов
- протокол удалённого рабочего стола

Перемещение внутри периметра

Этапы

1. Атакующий проводит внешнюю разведку (Recon)
2. Компрометирует систему (Initial Compromise)
3. Старается сохранить своё присутствие на этой системе (Establish Persistence)
4. Повышает права (Escalate Privileges)
5. Проводит внутреннюю разведку (Internal Recon)
6. Выбирает удобный для себя транспорт и осуществляет подключение к жертве (Lateral Movement)
7. Собирает и анализирует найденные данные (Data Analysis)
8. Опционально повторяет действия 4–7 (для других компонентов системы)
9. В завершение злоумышленник выносит найденные ценные данные (Exfiltration and Complete Mission)

Защита от Lateral Movement

Шаги для защиты:

- блокировать учётные записи после большого количества ошибок аутентификации
- ограничить права учётных записей helpdesk
- запретить удалённый вход для учётных записей локальных администраторов
- блокировать использование ненужных библиотек и прочих dll

Выводы урока

- Разобрали понятие Lateral Movement
- Изучили этапы атаки
- Изучили защиту от Lateral Movement

Выводы модуля

- Познакомились с утилитами
для работы с текстовыми файлами
- Обсудили конвейерную обработку файлов
- Прошли практику в ОС Linux
- Обсудили сбор данных и эксфильтрацию данных
- Поговорили про перемещение внутри периметра