Skillbox

Linux как таргет-система

Анастасия Полякова

Старший инженер безопасности в «Alibaba cloud»

Цель урока

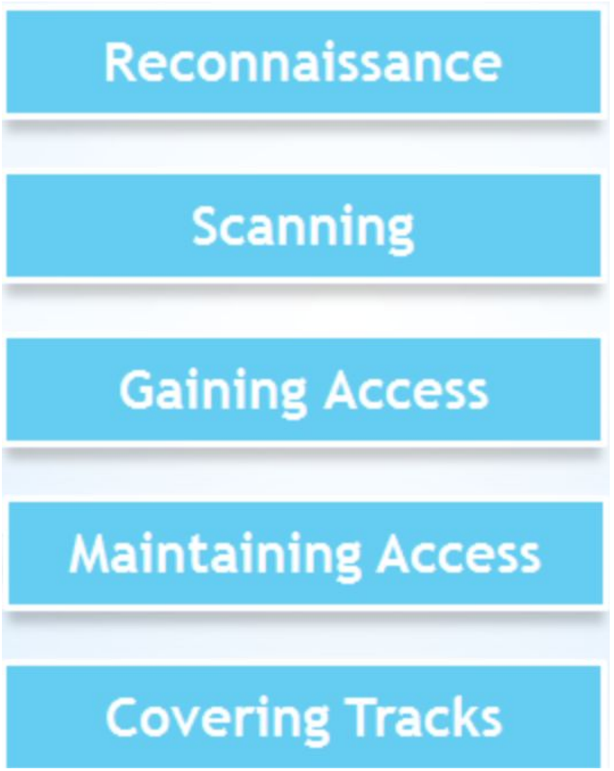
Цель: познакомиться с Linux-системой как с объектом атаки, рассмотреть особенности системы с точки зрения атакующего.

Мифы о Linux

- ОС семейства Linux самые безопасные
- Под Linux не существует вредоносных программ
- В Linux мало или совсем нет уязвимостей
- ОС семейства Linux экзотика, и потому не представляют интереса для хакеров

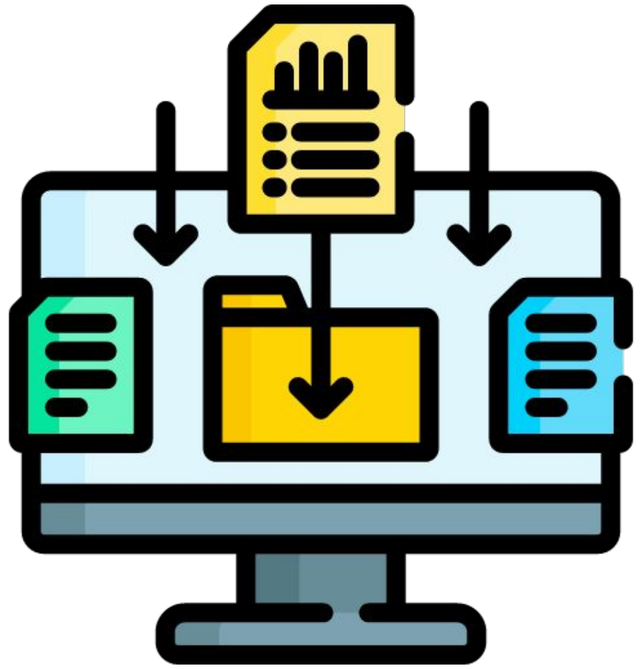
Основные этапы взлома

- Сбор информации
- Сканирование
- Получение доступа
- Сохранение доступа
- Заметание следов



Сбор сведений о системе (Recon)

- Активный
- Пассивный



Векторы атаки

- Уязвимости
- Повышение привилегий
- Закрепление в системе
- Запуск приложений
- Копирование/изменение/удаление данных

Сведения о системе на базе Linux

- Версия дистрибутива
- Версия ядра
- Сведения о сети
- Сведения об оборудовании
- Запущенные процессы
- Версии установленных программ
- Программы автозапуска
- Директории и файлы, доступные для записи

Сбор сведений с помощью bash

- Имя машины
- Информация о дистрибутиве
- Версия ядра
- Список пользователей
- Запущенные процессы

Демо

Вывод

Познакомились с Linux-системой как с объектом атаки, рассмотрели особенности системы с точки зрения атакующего и научились собирать первичные сведения о системе с помощью bash.

Спасибо за внимание!