Red Team vs Pentest

Прохор Садков

Старший аналитик

19 апреля 2022 года

О ЧЕМ ВЕБИНАР

- Виды работ по анализу защищенности
- Что такое Red Team и Pentest?
- Юридические аспекты Red Team и Pentest
- Сравнение подходов Red Team и Pentest
- В каких случаях необходим Red Team, а в каких Pentest?

АТАКИ, УТЕЧКИ, ВЗЛОМЫ

USSC

Технологии и медиа, 28 фев, 12:21 | 17 453 | Поделиться

СДЭК заявил об утечке данных российских и украинских пользователей

Технологии и медиа, 01 мар, 19:13 | 13 510 | Поделиться

Сервис «Яндекс.Еда» сообщил об утечке информации о клиентах

16 мар, 06:24 | 132 320 | Поделиться

Сайты арбитражных судов России подверглись хакерской атаке

Бизнес, 28 мар, 23:59 | 33 972 | Поделиться

Росавиация из-за возможной кибератаки перешла на бумажный документооборот

Технологии и медиа, 01 апр, 10:21 | 10 865 | Поделиться

«Касперский» выявил рост числа DDoS-атак на компании России в 8 раз

ВИДЫ АНАЛИЗА ЗАЩИЩЕННОСТИ

USSC

ОЦЕНКА УЯЗВИМОСТЕЙ

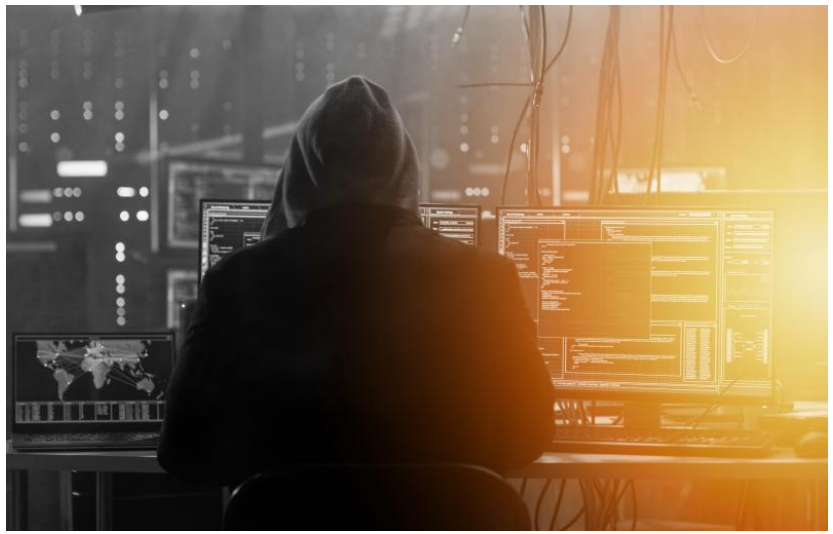
PENTEST

RED TEAM

ОЦЕНКА УЯЗВИМОСТЕЙ

- Выполняется преимущественно автоматизированными средствами
- Выявляет только известные уязвимости
- Не предполагает эксплуатации уязвимостей

Результат: перечень уязвимостей и рекомендации по их устранению



МОДЕЛИРОВАНИЕ АТАК ПОТЕНЦИАЛЬНЫХ НАРУШИТЕЛЕЙ НА ИНФОРМАЦИОННЫЕ АКТИВЫ

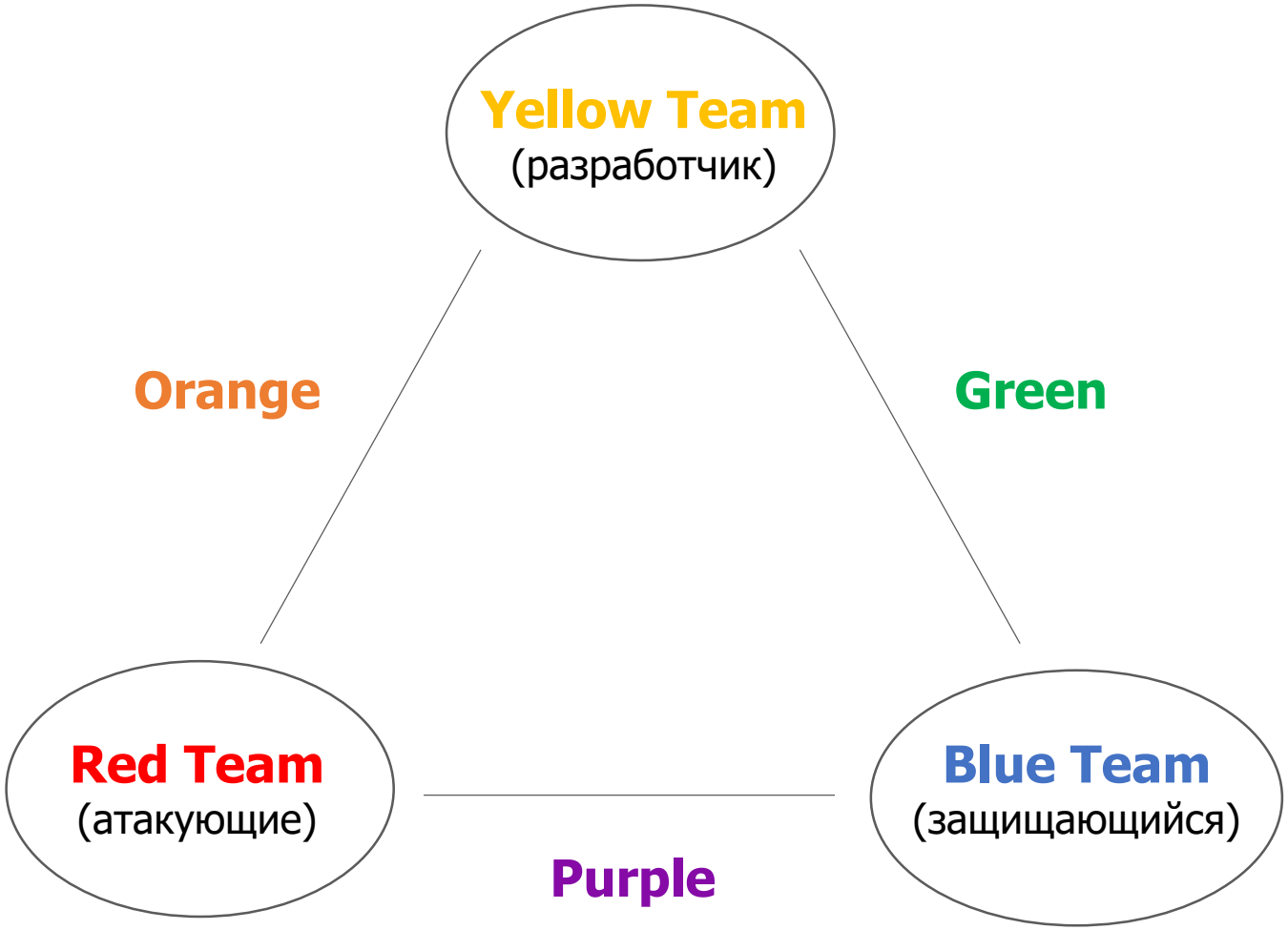
Особенности:

- дополнительно используются ручные методы поиска уязвимостей
- проводится ручная эксплуатация уязвимостей

ЗАДАЧИ PENTEST

- Выявление уязвимостей и их эксплуатация
- Подготовка рекомендации по устранению уязвимостей
- Определение векторов атак потенциальных злоумышленников

ДРУГИЕ КОМАНДЫ



МОДЕЛИРОВАНИЕ ЦЕЛЕНАПРАВЛЕННЫХ АТАК НА КОМПАНИЮ

Цель Red Team – повышение эффективности Blue Team

ЗАДАЧИ RED TEAM

- Длительная и непрерывная реализация сценариев атак
- Выявление уязвимостей и недостатков в системе защиты
- Обход средств защиты информации и мониторинга
- Подготовка рекомендации по предотвращению атак

ЮРИДИЧЕСКИЕ АСПЕКТЫ PENTEST И RED TEAM

USSC

- Определить правовые основания тестирования
- Зафиксировать границы работ
- Установить порядок взаимодействия сторон
- Распределить ответственность сторон
- Уведомить задействованных третьих лиц

ЮРИДИЧЕСКИЕ АСПЕКТЫ PENTEST И RED TEAM

USSC

- Оценить риски при проведении тестирования
- Обсудить этические вопросы
- Принять меры защиты от непредвиденного сбоя
- Получить подтверждение согласия на тестирование
- Документировать все процедуры и результаты тестирования

ВЗАИМОДЕЙСТВИЕ С SOC

Уведомить о плановых сроках тестирования

Анализ защищенности объектов КИИ рекомендуется проводить на тестовых стендах

Любые воздействия на активы должны быть согласованы

Не использовать реальные IP-адреса компании-тестировщика

КАКОЕ ПРИНЦИПИАЛЬНОЕ ОТЛИЧИЕ PENTEST И RED TEAM?

USSC

СКРЫТНОСТЬ ТЕСТИРОВАНИЯ

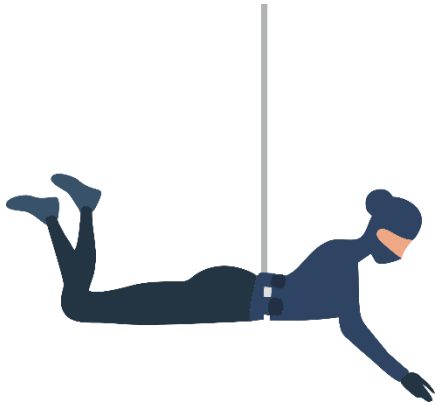
USSC

Pentest

- действуют «шумно»
- не обходят средства обнаружения вторжений

Red Team

- действуют «скрытно»
- обходят средства обнаружения вторжений



ВСЕ ЗАВИСИТ ОТ ЦЕЛЕЙ ТЕСТИРОВАНИЯ

ВЗАИМОДЕЙСТВИЕ С BLUE TEAM

USSC

Pentest	Red Team
• постоянно взаимодействуют с Blue Team • эксплуатация уязвимостей согласуется с Blue Team	• действует без контроля Blue Team • эксплуатация уязвимостей не согласуются с Blue Team

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОПРЕДЕЛЯЕТСЯ ЦЕЛЯМИ ТЕСТИРОВАНИЯ

МЕТОДИКА ТЕСТИРОВАНИЯ

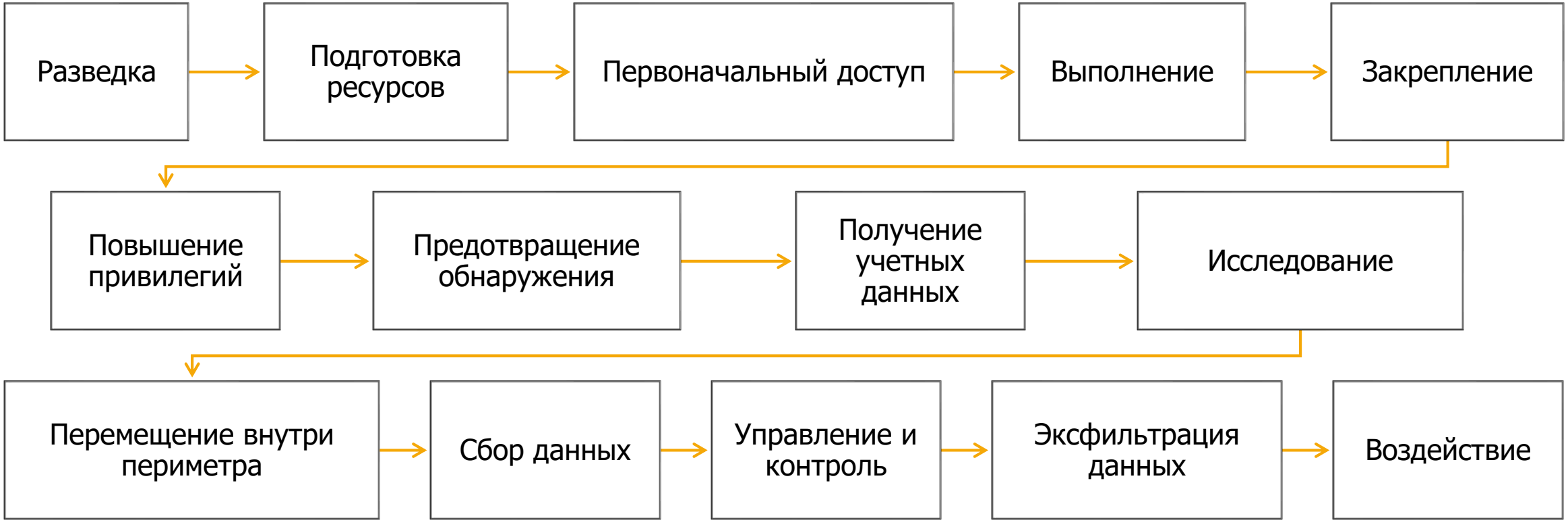
Pentest	Red Team
• жестко ограничены методикой тестирования • используется ограниченный перечень техник	• не ограниченны методикой • используются все доступные техники

МЕТОДИКА ФОРМИРУЕТСЯ НА ОСНОВАНИИ ЦЕЛЕЙ ТЕСТИРОВАНИЯ

МЕТОДИКА ТЕСТИРОВАНИЯ

USSC

MITRE ATT&CK



МЕТОДИКА ТЕСТИРОВАНИЯ: ПОДГОТОВКА

USSC

Разведка

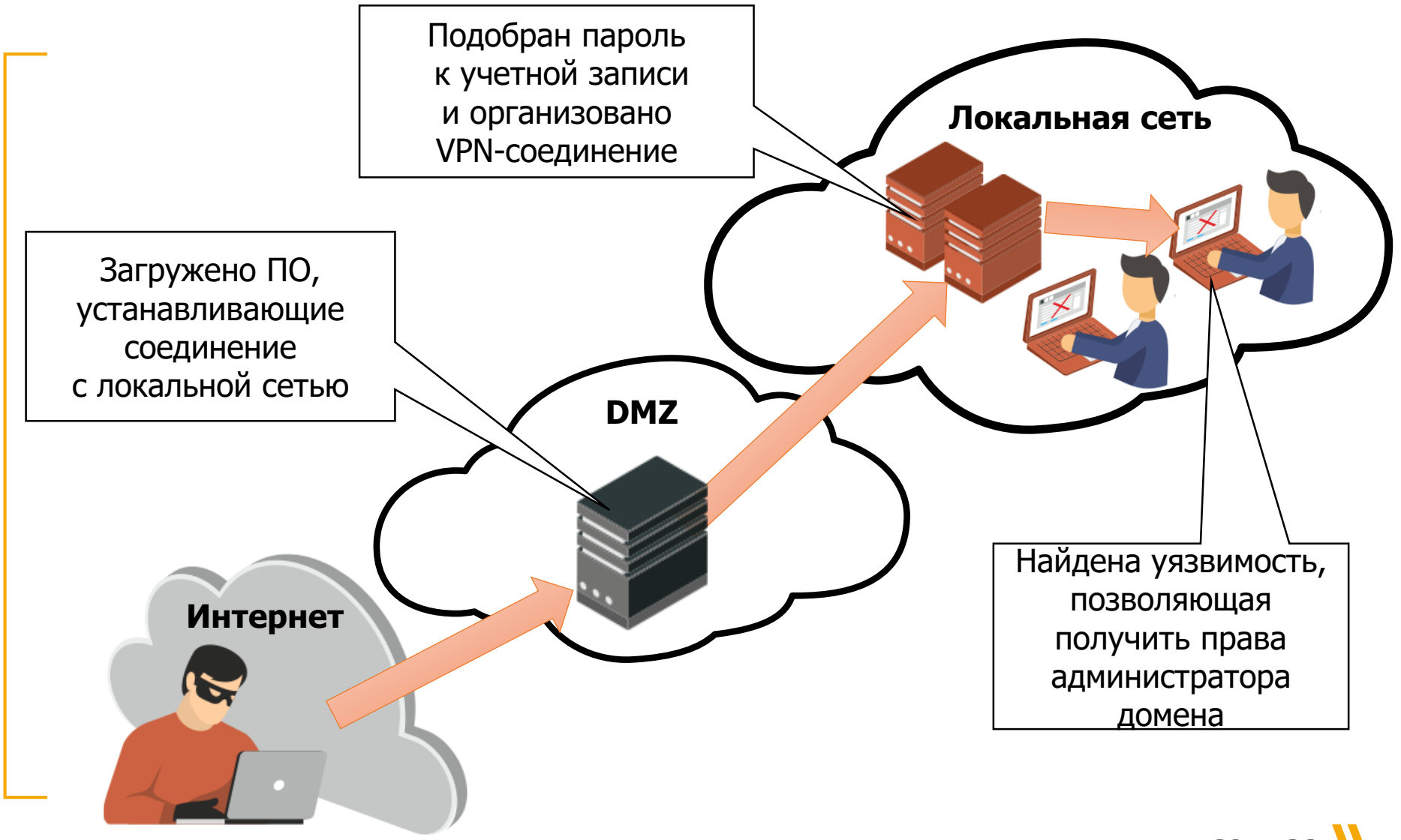
Подготовка ресурсов

Первоначальный доступ

МЕТОДИКА ТЕСТИРОВАНИЯ: ЭКСПЛУАТАЦИЯ

USSC

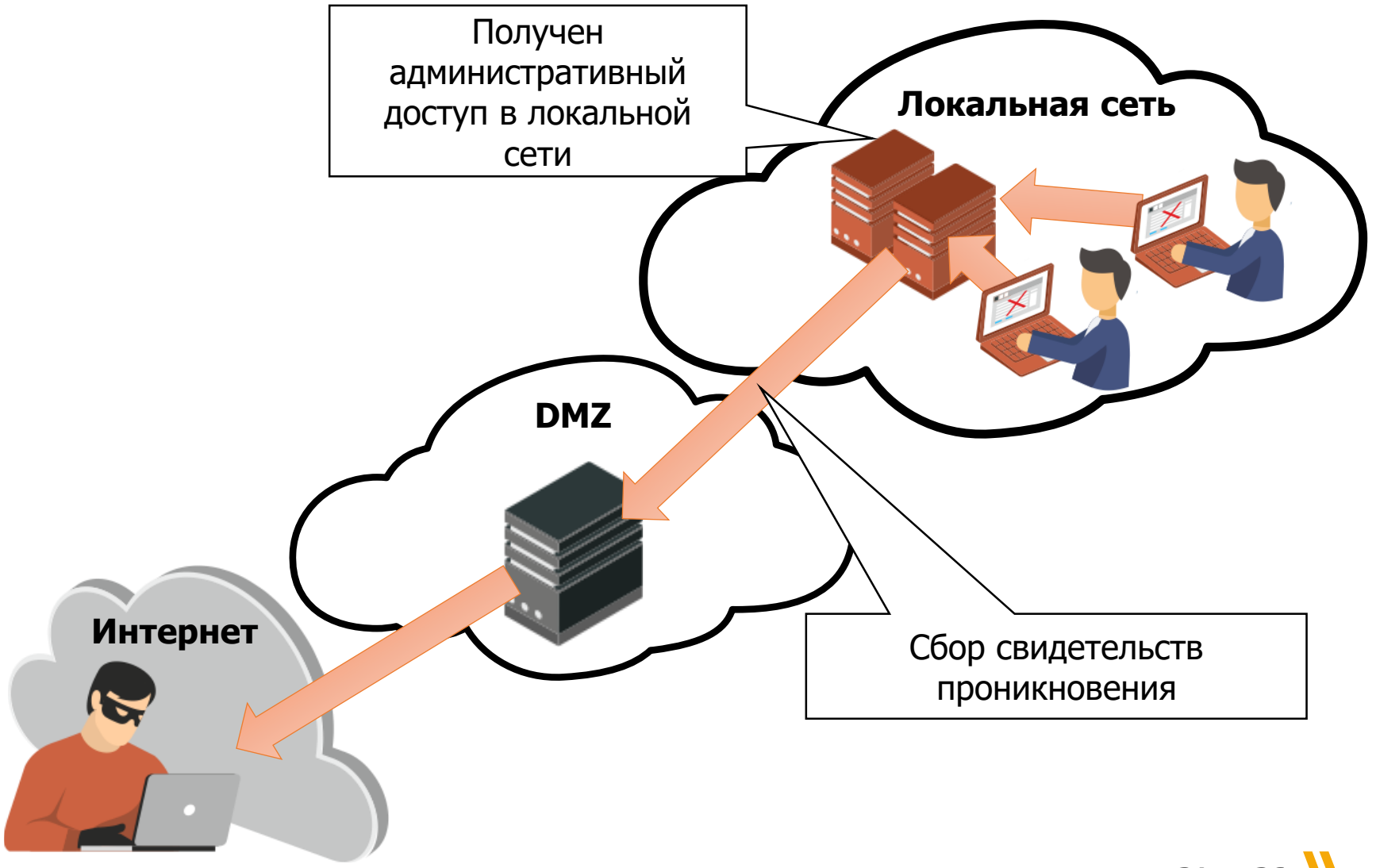
- Выполнение
- Закрепление
- Повышение привилегий
- Предотвращение обнаружения
- Получение учетных данных
- Исследование
- Перемещение внутри периметра



МЕТОДИКА ТЕСТИРОВАНИЯ: ПОСТЭКСПЛУАТАЦИЯ

USSC

- Сбор данных
- Управление и контроль
- Эксфильтрация данных
- Воздействие



СОСТАВ КОМАНДЫ

USSC

Pentest	Red Team

• в команде только пентестеры	• в команду входят специалисты разного профиля:
	  • руководитель Red Team
	  • разработчики эксплойтов и тестовой инфраструктуры
	  • эксперты по веб, социальной инженерии, сетевым технологиям
	  • аналитики
	  • специалисты по безопасной разработке

КОМАНДА ФОРМИРУЕТСЯ ИСХОДЯ ИЗ ЦЕЛЕЙ ТЕСТИРОВАНИЯ

СОДЕРЖАНИЕ ОТЧЕТОВ

USSC

Pentest

- описание обследованных информационных активов
- перечень уязвимостей и порядок их эксплуатации
- рекомендации по устранению уязвимостей

Red Team

- описание реализованных сценариев атаки с указанием времени их проведения
- перечень недостатков системы защиты информации
- рекомендации по предотвращению атак

СОДЕРЖАНИЕ ОТЧЕТА ФОРМИРУЕТСЯ В ЗАВИСИМОСТИ ОТ ЦЕЛЕЙ

ДЛИТЕЛЬНОСТЬ ТЕСТИРОВАНИЯ

Pentest	Red Team
• Проводится в ограниченный период времени	• Проводится в длительный период времени или постоянно

КЛЮЧЕВОЕ ОТЛИЧИЕ

ДЛЯ КАКИХ ЗАДАЧ ВЫБРАТЬ PENTEST И RED TEAM

USSC

Pentest

- разовый анализ защищенности информационных активов
- разовая отработка навыков Blue Team по предотвращению атак
- обнаружение уязвимостей на определенный момент времени

Red Team

- постоянный анализ защищенности информационных активов
- непрерывное улучшение навыков Blue Team по предотвращению атак
- постоянная проверка на наличие уязвимостей

USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

Прохор Садков

Старший аналитик
направления анализа защищенности

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU