

БОЛЬШОЙ РАЗБОР ONE TASK

КАК РЕШАТЬ СТФ-ЗАДАЧИ БЫСТРЕЕ,
ГЛУБЖЕ И КАЧЕСТВЕННЕЕ

[СПИКЕР]

CyberED

ЯРОСЛАВ ШМЕЛЕВ

■ Старший вирусный аналитик в Kaspersky Lab

■ Ключевые навыки:

ИССЛЕДОВАНИЕ УГРОЗ, ВИРУСНАЯ АНАЛИТИКА, ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ,
КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА, АДМИНИСТРИРОВАНИЕ LINUX

■ Участие в профильных соревнованиях и награды:

2024: SOC FORUM (СРЕДИ АТАКУЮЩИХ В РОЛИ КАПИТАНА КОМАНДЫ) - 1 МЕСТО

2022: THE STANDOFF 2022 (В СОСТАВЕ КОМАНДЫ INVULS) - 3 МЕСТО

2021: THE STANDOFF 365 (БЕТА ЗАПУСК) - 1 МЕСТО

2018: ВСЕРОССИЙСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - 1 МЕСТО

2016: МЕЖДУНАРОДНАЯ ОЛИМПИАДА «IT-ПЛАНЕТА», НОМИНАЦИЯ «АДМИНИСТРИРОВАНИЕ LINUX» - 1 МЕСТО

■ Телеграм

@HUMMELCHENO



ЧТО БУДЕТ НА ВЕБИНАРЕ

А)

ЧТО ТАКОЕ ONE TASK

В)

КАК ЭКСПЕРТ ПОДХОДИТ
К ЗАДАЧЕ

Б)

ПОЧЕМУ CTF ПОЛЕЗЕН БЕЛОМУ
ХАКЕРУ

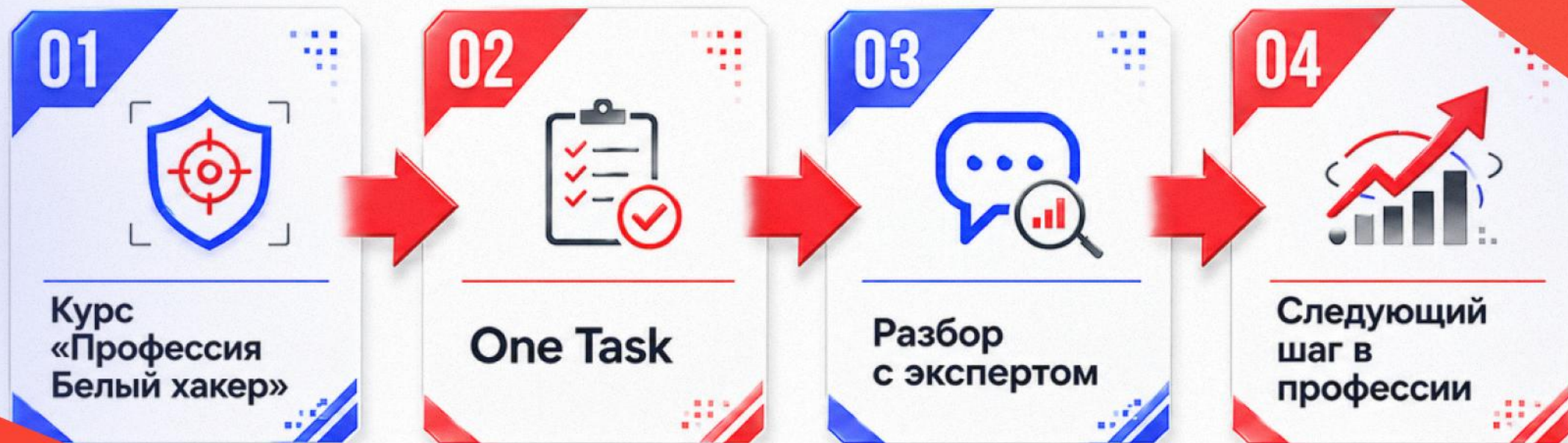
В)

РАЗБОР 3 ТАСКОВ ОТ УСЛОВИЯ
ДО ФЛАГА



CYBERED, КУРС “ПРОФЕССИЯ БЕЛЫЙ ХАКЕР И ПРОЕКТ ONE TASK

[ОТ ТЕОРИИ К РЕГУЛЯРНОЙ ПРАКТИКЕ]



ЧТО ТАКОЕ ONE TASK?



Одна CTF-задача каждую неделю

1. Самостоятельное решение

2. Накопились 3 задачи

3. Проходит большой разбор с экспертом



[Почему CTF — это не просто игра]

CTF ТРЕНИРУЕТ МЫШЛЕНИЕ АТАКУЮЩЕГО



анализ вводных



поиск зацепок



проверка гипотез



работа с инструментами



внимание к деталям



умение не застревать



[Что CTF даёт профессии]

CyberED

ЧТО ПЕРЕНОСИТСЯ В РАБОТУ БЕЛОГО ХАКЕРА

CTF развивает:



разведку



анализ артефактов



поиск слабого места

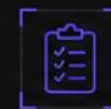


эксплуатацию



работу с неизвестностью

В профессии нужно добирать:



методологию



отчётность



контекст инфраструктуры



коммуникацию



ответственность



МЕТОДИКА РЕШЕНИЯ СТФ-ЗАДАЧ

- 01 ПРОЧИТАТЬ УСЛОВИЕ И ВЫДЕЛИТЬ ЗАЦЕПКИ.
- 02 ОПРЕДЕЛИТЬ КАТЕГОРИЮ ЗАДАЧИ И ВОЗМОЖНЫЕ КЛАССЫ УЯЗВИМОСТЕЙ.
- 03 СОБРАТЬ МАКСИМУМ ИНФОРМАЦИИ ИЗ ДОСТУПНЫХ АРТЕФАКТОВ.
- 04 СФОРМИРОВАТЬ ПЕРВЫЕ ГИПОТЕЗЫ.
- 05 ПРОВЕРИТЬ БЫСТРЫЕ И ДЕШЕВЫЕ ГИПОТЕЗЫ.
- 06 ЗАФИКСИРОВАТЬ, ЧТО НЕ СРАБОТАЛО.
- 07 УГЛУБИТЬСЯ В САМЫЙ ВЕРОЯТНЫЙ ПУТЬ.
- 08 ПОЛУЧИТЬ РЕЗУЛЬТАТ И ПРОВЕРИТЬ ЕГО.
- 09 СФОРМУЛИРОВАТЬ УНИВЕРСАЛЬНЫЙ ВЫВОД: ЧЕМУ ЭТА ЗАДАЧА УЧИТ И КАК ЭТО СВЯЗАНО С ПРОФЕССИЕЙ.

ONE TASK: BACKUPS

КЕЙС – ОШИБКА КОНФИГУРАЦИИ **SUDO**, ПРИВОДЯЩАЯ К ВЫПОЛНЕНИЮ ПРОИЗВОЛЬНЫХ КОМАНД ОТ **ROOT**

ПОДХОД К РЕШЕНИЮ

- ❑ Энуменрация в системе
- ❑ Изучение правил sudo и задач cron
- ❑ Построение цепочки: удаление и подмена диагностического скрипта
- ❑ Выполнение полезной нагрузки

ОСНОВНЫЕ СЛОЖНОСТИ

- ❑ Понимание особенностей ФС: выход из директории через “..” и символические ссылки
- ❑ Нестандартный вектор: удаление файла
- ❑ Состояние гонки: определение имени диагностического скрипта
- ❑ Подготовка и отладка полезной нагрузки

ONE TASK: FORGOTTEN SERVER

КЕЙС – СКАНИРОВАНИЕ ПРОМЕЖУТОЧНОЙ СЕТИ И АТАКА НА ВЕБ-ПРИЛОЖЕНИЕ
ЧЕРЕЗ ПРОМЕЖУТОЧНЫЙ ХОСТ С АРХИТЕКТУРОЙ MIPS.

ПОДХОД К РЕШЕНИЮ

- ❑ Эnumерация
- ❑ Настройка трансляции трафика
- ❑ Сканирование внутренней сети
- ❑ Атака на веб-приложение

ОСНОВНЫЕ СЛОЖНОСТИ

- ❑ Проблемы с использованием проксирования через SSH
- ❑ Выбор pivoting-клиента под целевую архитектуру
- ❑ Выбор и настройка сканера сети
- ❑ Ведение атаки через проху

ONE TASK: STRANGE AND DIRTY

КЕЙС – МОДИФИКАЦИЯ ИЗВЕСТНОГО ЭКСПЛОЙТА ПОД ЯДРО LINUX ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT.

ПОДХОД К РЕШЕНИЮ

- ❑ Подготовка отладочного стенда
- ❑ Выбор эксплойта
- ❑ Отладка эксплойта и его модификация
- ❑ Загрузка эксплойта на атакуемую машину и получение прав root

ОСНОВНЫЕ СЛОЖНОСТИ

- ❑ Выбор подхода к эксплуатации
- ❑ Организация удобной работы со стендом для тестирования
- ❑ Понимание полезной нагрузки
- ❑ Модификация кода на ассемблере



**ЗАДАВАЙТЕ
ВОПРОСЫ**
И ПРЕДЛАГАЙТЕ ОБСУДИТЬ КЕЙСЫ

БАТТЛ-КАРТА

САМОСТОЯТЕЛЬНО **vs** С ЭКСПЕРТОМ



Самостоятельно / write-up:

- непонятно, с чего начать
- много ложных гипотез
- легко скопировать, но не понять
- нет обратной связи



С экспертом CyberED:

- понятная методика
- объяснение логики
- разбор тупиков
- перенос навыка на новые задачи

VS



КАК ONE TASK УСКОРЯЕТ КАРЬЕРНЫЙ ТРЕК

Почему регулярная CTF-практика ускоряет не только решение задач, но и путь в профессию



1 помогает
увидеть уровень

Реальные задачи показывают ваш текущий уровень по сравнению с другими.



2 показывает
пробелы

CTF-формат быстро выявляет слабые места в знаниях и навыках.



3 подсвечивает
сильные стороны

Вы понимаете, в чём вы сильны, и куда стоит направить фокус для роста.



4 даёт следующий
шаг после R-101

Практика формирует портфолио, уверенность и готовит к более сложным вызовам.



R-101

Базовые знания



ONE TASK

Регулярная CTF-практика

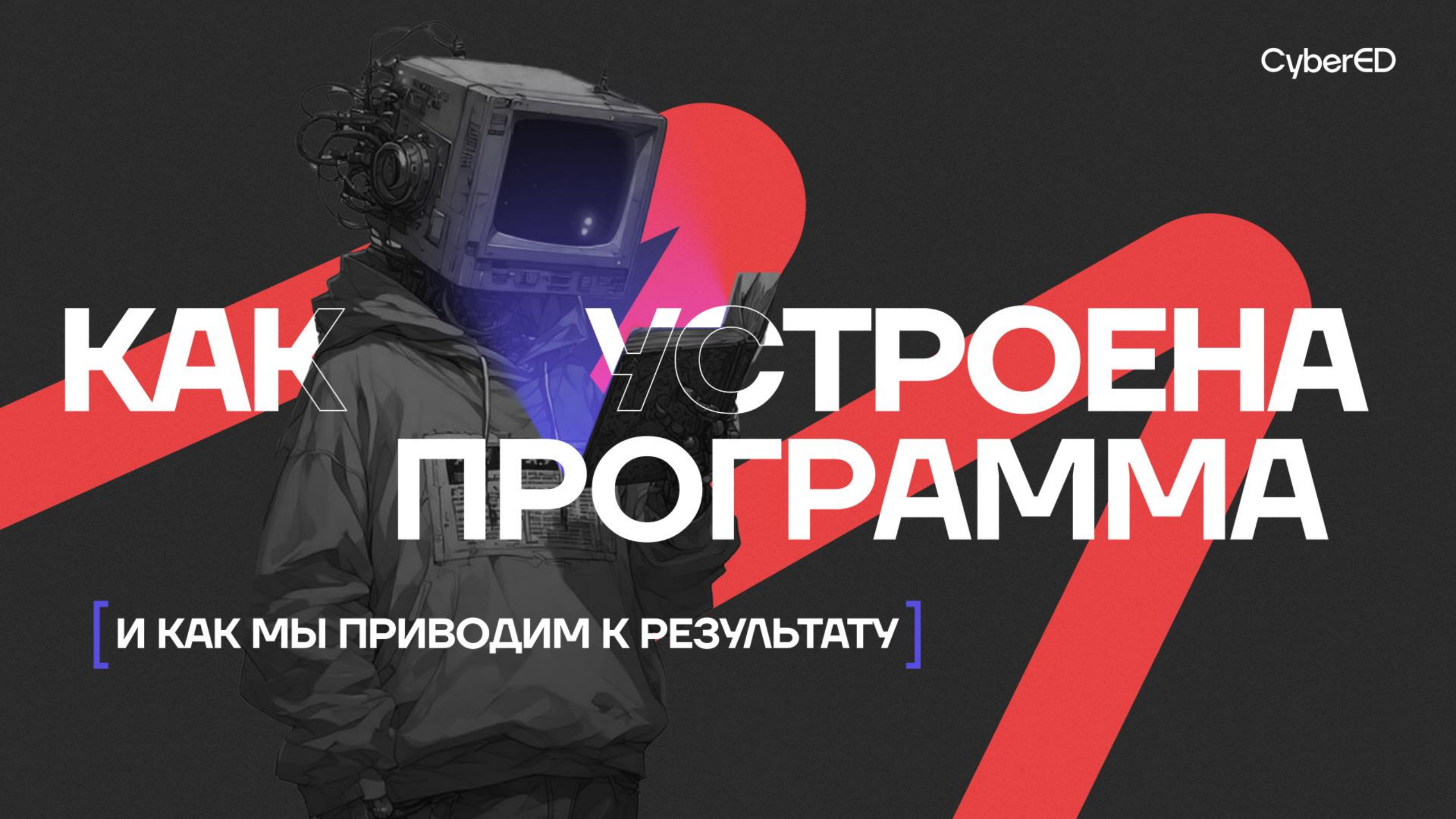


R-301 «Пентестер»

Продвинутый уровень и карьера



R-301 «Пентестер» — системный карьерный маршрут для тех, кто хочет развиваться дальше



КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

Этап 1. Разведка

Модуль 1. Исследование целей тестирования (Reconnaissance)

+

Модуль 2. Получение первичного доступа через атаки на аутентификацию (Authentication)

+

Модуль 3. Получение первичного доступа через атаки на веб-приложения

+

Модуль 4. Получение первичного доступа через атаки социальной инженерии

+

Этап 2. Получение первоначального доступа

Модуль 5. Эксплуатации известных уязвимостей

+

Этап 3. Повышение привилегий/закрепление

Модуль 6. Повышение привилегий в Linux

+

Модуль 7. Повышение привилегий в контейнерных средах

+

Модуль 8. Повышение привилегий в Windows

+

Этап 4. Боковое перемещение в сети

Модуль 9. Проброс сетевого трафика (Pivoting)

+

Модуль 10. Проведение атак на локальные сети

+

Модуль 11. Проведение атак на Active Directory

+

Этап 5. Получение импакта

Модуль 12. Написание отчета

+

Дополнительный модуль. Оценка устойчивости средств защиты

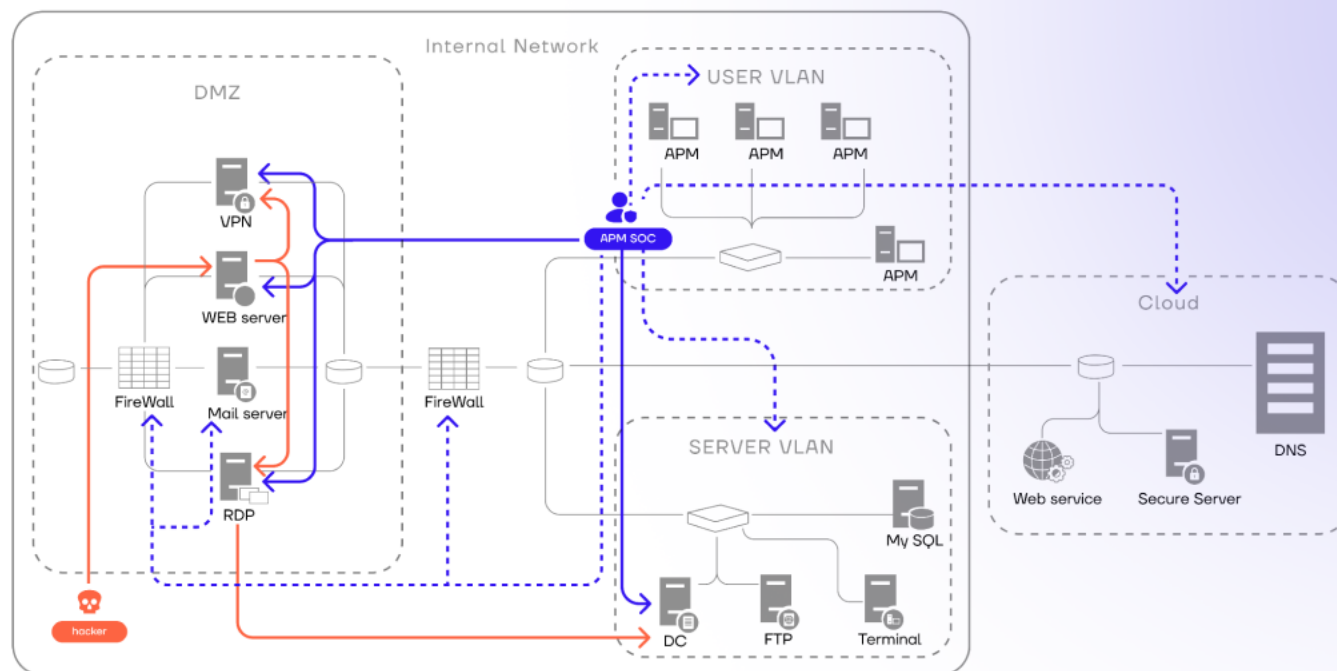
+

Встречи с экспертами по развитию своего профессионального трека: 5 встреч, 20 ак.ч.

CyberED

ТЕМЫ МОДУЛЕЙ

**ЭТО ГОТОВЫЙ ПЛАН ВЫПОЛНЕНИЯ
ВСЕЙ ЦЕПОЧКИ АТАКИ В КОМПАНИЯХ**



[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

Формат: асинхрон + live разбор 🔴



ПРОХОДИШЬ ТЕОРИЮ САМ

+ разбираешь с наставником



ВСТРЕЧА С ЭКСПЕРТОМ

- + ответы на вопросы по практике
- + углубление
- + дополнительные техники

Формат помогает понять материал и сформировать навык, а **не** просто посмотреть материал.

ЭТО НЕ

«ПОСМОТРЕЛ И ПОШЁЛ ДАЛЬШЕ»

ЭТО

«РАЗОБРАЛ, ДОКРУТИЛ, ПОНЯЛ, ГДЕ **ОШИБСЯ**»

[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

КАЖДАЯ ТЕХНИКА
= ОТДЕЛЬНЫЙ СКИЛЛ
= ОТДЕЛЬНАЯ ПРАКТИКА

■ 120+ техник (скиллов) для пентеста из MITRE ATT&CK и от архитекторов программы

- 1–2 задачи на ⚠️ каждую технику
- от 1 до 3 уровня сложности
- 3й уровень - на 🏠 киберполигоне

Не «один раз попробовал»
→ а закрепление через повторение

MITRE ATT&CK									
Матрицы Тактика Методы Защитные сооружения CTI Ресурсы Благотворители Способствовать Блог									
Поиск Q									
Разведка	Разработка ресурсов	Первоначальный доступ	Исполнение	Упорство	Повышение привилегий	Оборонительное уклонение	Доступ по учетным данным	Открытие	Боковое движение
11 техник	8 техник	11 техник	17 техник	23 техники	14 техник	47 методов	17 техник	34 техники	9 техник
Активное сканирование (1)	Получить доступ	Вставка контента	Команда администрирования облака	Манипулирование учетной записью (7)	Механизм контроля за повышением уровня насилия (5)	Механизм контроля за повышением уровня насилия (5)	Противник посредник (4)	Обнаружение учетных записей (4)	Использование удаленных сервисов
Соберите информацию о пострадавшем хостине (4)	Приобретение инфраструктуры (8)	Компромисс проеда	Интерпретатор команд и скриптов (18)	Вакансии в BITS	Манипулирование токенами доступа (1)	Манипулирование токенами доступа (1)	Грубая сила (4)	Обнаружение окон приложений	Внутренний фишинг
Соберите информацию о личности жертвы (3)	Компромиссные счета (3)	Использование уязвимостей в общедоступных приложениях	Команда управления контейнерами	Выполнение автозапуска при загрузке или входе в систему (14)	Манипулирование учетной записью (7)	Вакансии в BITS	Учетные данные из хранилищ паролей (6)	Обнаружение информации в браузере	Боковая передача инструмента
Соберите информацию о личности жертвы (3)	Компромиссная инфраструктура (10)	Внешние удаленные сервисы	Развернуть контейнер	Сценарии инициализации загрузки или входа в систему (5)	Выполнение автозапуска при загрузке или входе в систему (14)	Создание образа на хосте	Эксплуатация для получения доступа к учетным данным	Обнаружение облачной инфраструктуры	Перехват сеанса удаленной службы (2)
Соберите информацию о сети жертвы (8)	Развитие потенциала (4)	Дополнительные аппаратные средства	Команда администрирования ESX	Интеграция облачных приложений	Сценарии инициализации загрузки или входа в систему (5)	Отклонение исполнения	Принудительная аутентификация	Панель управления облачными сервисами	Удаленные сервисы (8)
Соберите информацию об организации-жертве (4)	Создание счетов (3)	Фишинг (4)	Эксплуатация для исполнения клиентскими операциями	Компрометировать двоичный файл программного обеспечения хоста	Сценарии инициализации загрузки или входа в систему (5)	Деобфускация/декодирование файлов или информации	Подделка веб-учетных данных (2)	Обнаружение облачных сервисов	Размножение с помощью системных носителей
Фишинг информации (4)	Получить возможности (7)	Размножение с помощью системных носителей	Ввод входных данных	Создать аккаунт (3)	Создание или изменение системного процесса (16)	Развернуть контейнер	Захват ввода (4)	Обнаружение объектов в облачном хранилище	Инструменты развертывания программного обеспечения
Поиск в закрытых источниках (7)	Возможности сцен (6)	Компромисс в цепочке поставок (3)	Межпроцессная коммуникация (3)	Создание или изменение системного процесса (16)	Изменение политики домена или арендатора (2)	Прямой доступ к тому	Изменение процесса аутентификации (3)	Обнаружение объектов в облачном хранилище	Загрязнение общего контента
Поиск в открытых технических базах данных (1)	Действительные учетные записи (4)	Доверительные отношения	Нативный API	Выполнение, инициированное событием (18)	Изменение политики домена или арендатора (2)	Изменение политики домена или арендатора (2)	Перевод многофакторной аутентификации	Обнаружение контейнеров и ресурсов	Используйте альтернативные материалы аутентификации (4)
Поиск	Сети Wi-Fi	Запланированная	Запланированная	Побег к хосту	Использование	Использование	Генерация запроса на многофакторную аутентификацию	Обход отладчика	Обнаружение

Матрица ATT&CK – всемирно признанная карта действий хакеров, основанная на реальных атаках.

[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ
ДО УРОВНЯ **СЛОЖНОСТИ**,
→ КОТОРЫЙ ПОТЯНЕШЬ

The screenshot shows the CyberED interface with a sidebar on the left containing a navigation menu. The main content area displays a task description and a list of materials. The task description includes a command prompt output and a description of the result. The materials list includes links to Process Injection Mitre&Attack, a report on Process Injection using Windows Threads, and a link to detect Process Injection. Below the materials list, there are two green buttons labeled 'Средняя задача' and 'Сложная задача'.

Принципы действия

Инструменты

Последовательность шагов

Пример

Дополнительные материалы

T-R049 - Техника обхода динамического анализа антивируса

Входные требования

Задача

Принципы действия

Инструменты

Последовательность шагов

Пример

Дополнительные материалы

Средняя задача

Сложная задача

T-R050 - Техника обхода AMSI

Входные требования

Задача

Принципы действия

Инструменты (Tools)

Последовательность шагов

Пример

и на атакующей машине сразу устанавливается шелл.

```
rlwrap nc -lvnp 1337
listening on [any] 1337 ...
connect to [192.168.1.18] from (UNKNOWN) [192.168.1.1] 52766
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop>
```

Описание результата

Применяя подвид техники [Process Injection](#), а именно Portable Executable [Injection](#), а также шифрование исполняемой нагрузки, удалось успешно избежать динамического анализа со стороны Microsoft Defender.

Дополнительные материалы

- [Process Injection Mitre&Attack](#)
- [Доклад про Process Injection используя потоки Windows Threads](#)
- [Как можно задектить Process Injection](#)

Средняя задача

Сложная задача

■ Встроенная система давления на результат → Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

ИНДИВИДУАЛЬНЫЙ СТЕНД ПОД КАЖДОГО

КАЖДОМУ СТУДЕНТУ ПОДНИМАЕТСЯ
→ СВОЯ ИНФРАСТРУКТУРА

01 

Ты не зависишь от других

02 

Никто не «сломал всё за тебя»

03 

Можно спокойно копать и ошибаться

04 

Доступ 24/7 к машинам



ПРАКТИКА, БЛИЗКАЯ К BUG BOUNTY / РЕАЛЬНОЙ РАБОТЕ

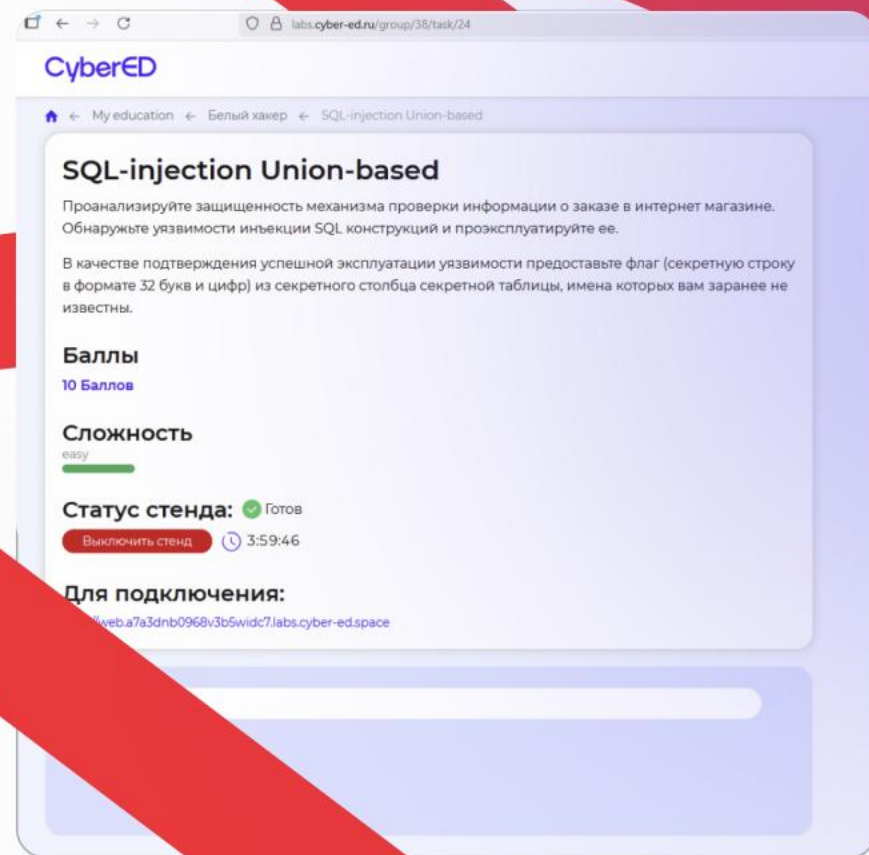
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



Ты **не** «решаешь тест»



Ты работаешь в инфраструктуре
и получаешь **результат** ⚡ (флаг)



ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую
технику применять

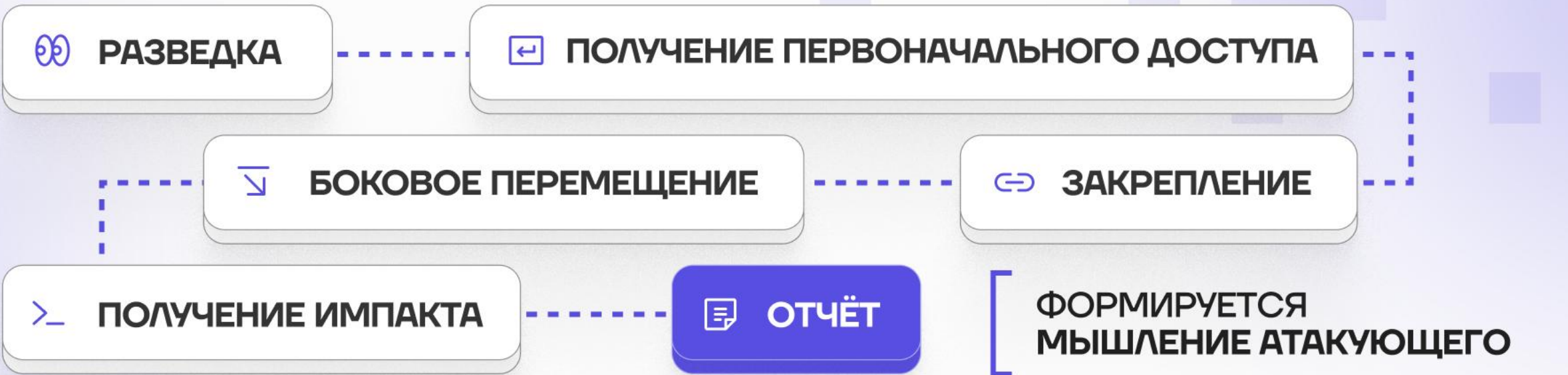


ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

Не изолированные упражнения, а **связанный процесс**

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



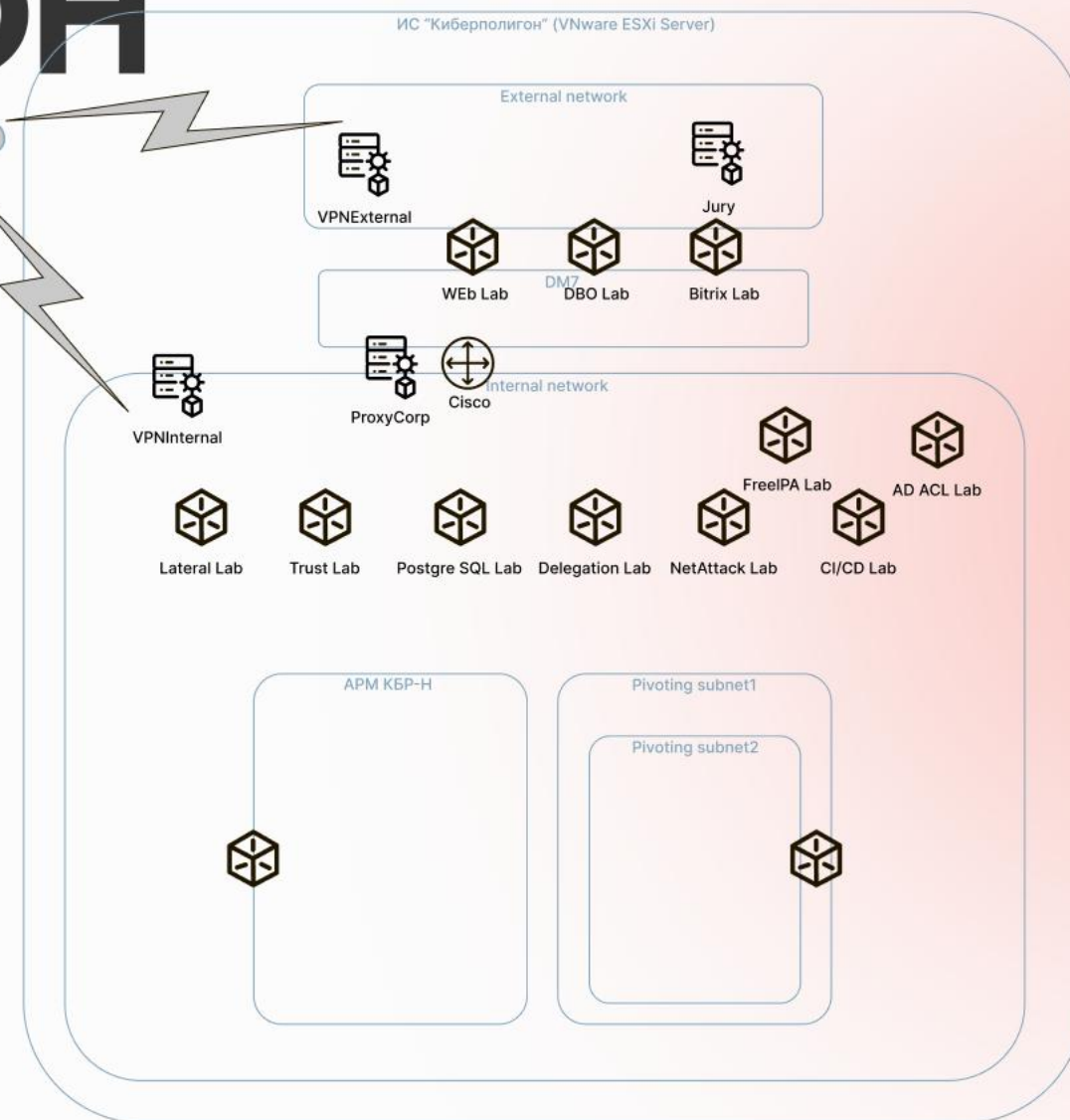
КИБЕРПОЛИГОН

*** CyberED

- ▶ Имитация инфраструктуры компании
- ▶ Цепочки атак
- ▶ Нет подсказок, **нет** «правильного пути»

Максимально близко к работе:

« **ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ** »



КИБЕРПОЛИГОН

*** CyberED

6

Цепочек

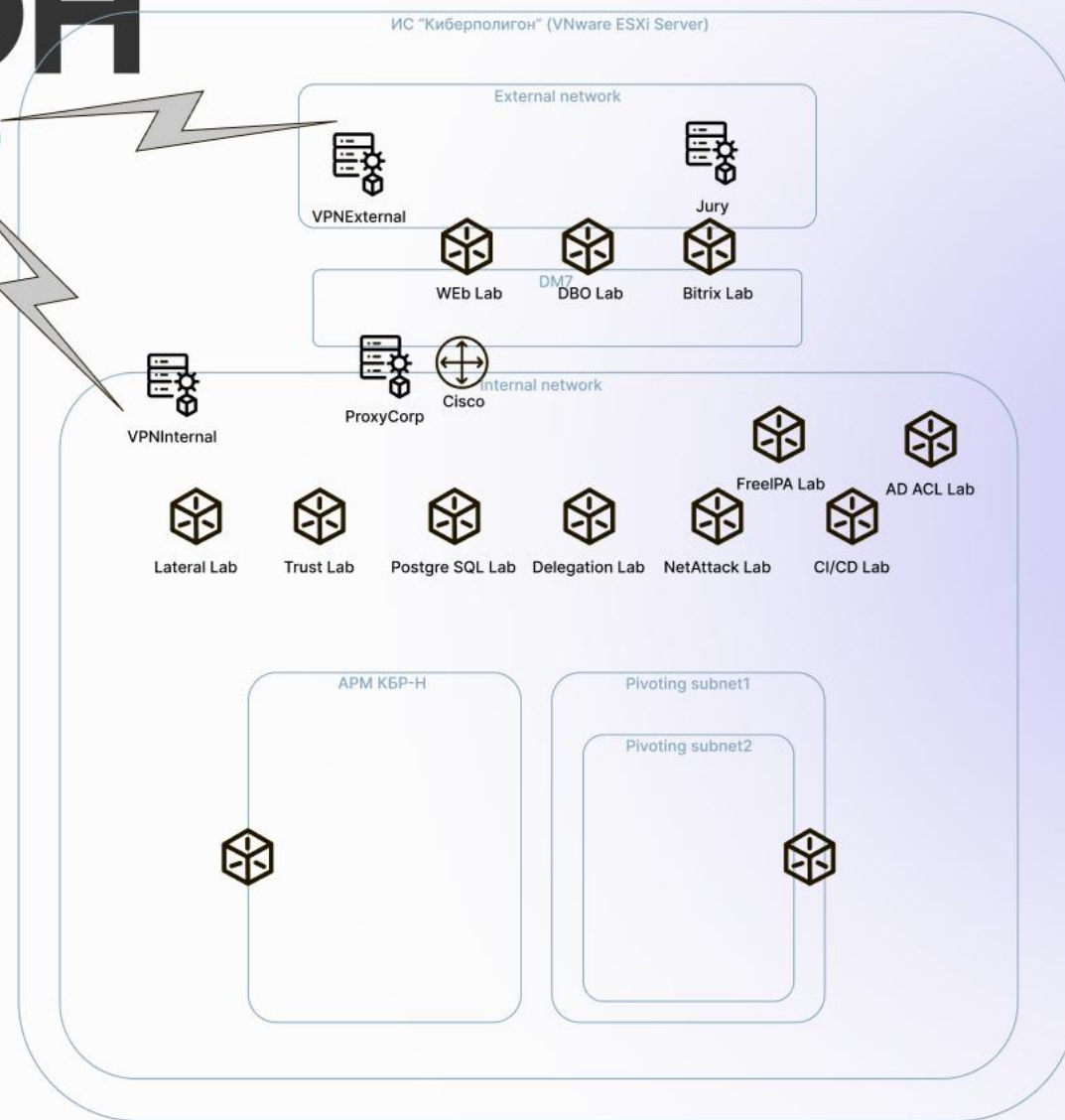
18

Задач

ЗАДАЧИ

- ▶ атаки на операционные системы (Windows, Linux),
- ▶ веб
- ▶ сетевые атаки.

- + Нарбатываете насмотренность по сценариям атак
- + Сталкиваетесь с вариативностью уязвимостей



УКАЖЕТЕ В РЕЗЮМЕ КОНКРЕТНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

 **Не так:** умею применять BurpSuite - X

 **А так:** нашел уязвимость path traversal в таком-то сервисе, используя инструмент BurpSuite, эксплуатировал данную уязвимость и получил учетные данные для последующей компрометации инфраструктуры Заказчика - Y.

 **Не так:** умение работать в среде Active Directory - X

 **А так:** реализовал цепочку атаки до компрометации AD и захвата инфраструктуры с помощью обнаруженной уязвимости в центре сертификации - Y.

ПРИМЕР 1

 **Не так:** умею сканировать порты и подбирать пароли.

 **Так:** обнаружил открытый порт 3389 на непубличном хосте, осуществил подбор пароля для учётной записи локального администратора через RDP, получил shell и развернул прокси для дальнейшего движения по внутренней сети Заказчика.

ПРИМЕР 2

 **Не так:** знаю Docker и Kubernetes.

 **Так:** через уязвимость в конфигурации GitLab CI (незащищенные переменные окружения) получил токен доступа к приватному registry, внедрил вредоносный образ, извлёк секреты production-окружения и достиг компрометации оркестратора кластера.

Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии
работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через
механизм аутентификации 0 / 0

Общие показатели по направлениям



Модуль: Не выбрано ▾

☐ Скрыть неосвоенные

Аналитик SOC. Демо-курс



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: **БАЗОВЫЙ** / **СРЕДНИЙ** / **СЛОЖНЫЙ**

■ Видно, что ты
реально умеешь

■ Не «написал в CV»
а подтвердил

Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через механизм аутентификации 0 / 0

Общие показатели по направлениям



Модуль: Не выбрано

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

■ Это уже не обучение, это **переход к найму**

[ИНТЕНСИВ] AI-УСИЛЕННЫЙ ПЕНТЕСТ: СБОРКА AI-ПАЙПЛАЙНА ДЛЯ OFFENSIVE SECURITY

АВТОР КУРСА:

СЕРГЕЙ ЗЫБНЕВ

- Тимлид пентестеров в «Бастиян» с 5+ лет опыта в ИБ
- Автор Telegram-канала «Похек» (16к+ подписчиков)
- Опыт в AI/LLM:
- \$5 000+ инвестировано в эксперименты с AI-агентами
- 1,5 года R&D в AI для пентеста

**В ОСНОВЕ ИНТЕНСИВА –
РЕАЛЬНЫЙ ПРАКТИЧЕСКИЙ
ОПЫТ ЭКСПЕРТА:**

- 01** Разбор рабочих кейсов
- 02** Тестирование AI-инструментов в задачах offensive security
- 03** Эксперименты с различными подходами к автоматизации пентеста

Основная аудитория:

- + Пентестеры
- + Специалисты offensive security
- + Bug bounty-исследователи
- + Red team инженеры

Также будет полезен:

- + Blue Team специалистам – для понимания логики атакующего
- + AppSec-инженерам
- + DevSecOps-специалистам
- + Security engineers, участвующим в security-тестировании инфраструктуры



АВТОРСКИЙ КУРС ЕГОРА ЗАЙЦЕВА



**REDLAB: ОЦЕНКА УСТОЙЧИВОСТИ
СРЕДСТВ ЗАЩИТЫ.**

ФОРМАТ

Видео-лекции + практики
на виртуальных стендах.

ОСНОВА

Курс базируется на ряде
материалов трека «Пентестер»



Во время курса вы сможете напрямую
общаться с экспертом в чате курса.



В РЕАЛЬНЫХ КОМПАНИЯХ

ПРИВАТНЫЕ КИБЕРИСПЫТАНИЯ СОВМЕСТНО С АО “КИБЕРИСПЫТАНИЕ” И STANDOFF 365

50+ участников ■ 2 программы

УНИКАЛЬНАЯ ВОЗМОЖНОСТЬ ОТРАБОТАТЬ ПРАКТИЧЕСКИЕ НАВЫКИ НА ИНФРАСТРУКТУРЕ РЕАЛЬНЫХ КОМПАНИЙ И ПОЛУЧИТЬ ФИНАНСОВОЕ ВОЗНАГРАЖДЕНИЕ ЗА ВЫПОЛНЕННЫЕ ЗАДАНИЯ.

- 01 Будут проходить на платформе Standoff
- 02 Каждый проект сопровождается ментором (помощь в организации работы и подготовке итогового отчёта)
- 03 Экспертную поддержку обеспечит Егор Зайцев


Возможность
заработать более
100 000 рублей

ЗАДАЧА

Проверить компанию в закрытом режиме перед выходом на открытые КИ

ПРИМЕР ЗАДАЧИ И НЕДОПУСТИМОГО СОБЫТИЯ

Получить ключевые права к шифрованию инфраструктуры тендерной площадки



365

CyberED



КУРС «BUG BOUNTY HUNTER» СОВМЕСТНО С ПЛАТФОРМОЙ BUG BOUNTY STANDOFF 365 ПОМОГАЕТ НАЧИНАЮЩИМ ПЕНТЕСТЕРАМ И БАГХАНТЕРАМ ПОНЯТЬ, КАК УСТРОЕН СОВРЕМЕННЫЙ РЫНОК BUG BOUNTY, КАКИЕ СТРАТЕГИИ РАБОТАЮТ НА СТАРТЕ И КАК ВЫСТРОИТЬ СОБСТВЕННЫЙ ПРОЦЕСС ПОИСКА УЯЗВИМОСТЕЙ.

КУРС ПОДХОДИТ КАК ПЕРВАЯ ПРАКТИЧЕСКАЯ ТОЧКА ВХОДА В BUG BOUNTY И ПОМОГАЕТ СФОРМИРОВАТЬ БАЗОВОЕ ПОНИМАНИЕ ПРОЦЕССОВ, ИНСТРУМЕНТОВ И СТРАТЕГИЙ РАБОТЫ БАГХАНТЕРА.

Standoff Bug Bounty

Крупнейшая российская платформа
для поиска уязвимостей в системах компаний

ПОВЫШЕНИЕ ЦЕНЫ В ИЮЛЕ! ОСТАВЛЯЙ ЗАЯВКУ!



ИИ в пентесте от Похек



Участие в кибериспытаниях



DETA / Авторский курс Егора Зайцева «Обход антивирусов»



1 любой мини-курс из платных программ на выбор



программа «Bug Bounty Hunter» совместно со Standoff 365