

CyberED

PIVOTING

[ЯРОСЛАВ ШМЕЛЕВ]



[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

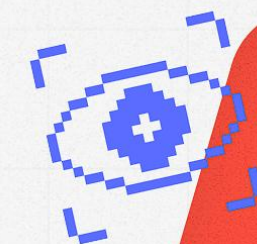
2021: THE STANDOFF 365 (БЕТА ЗАПУСК) - 1 МЕСТО

2018: ВСЕРОССИЙСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - 1 МЕСТО

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

■ Телеграм

@HUMMELCHENO

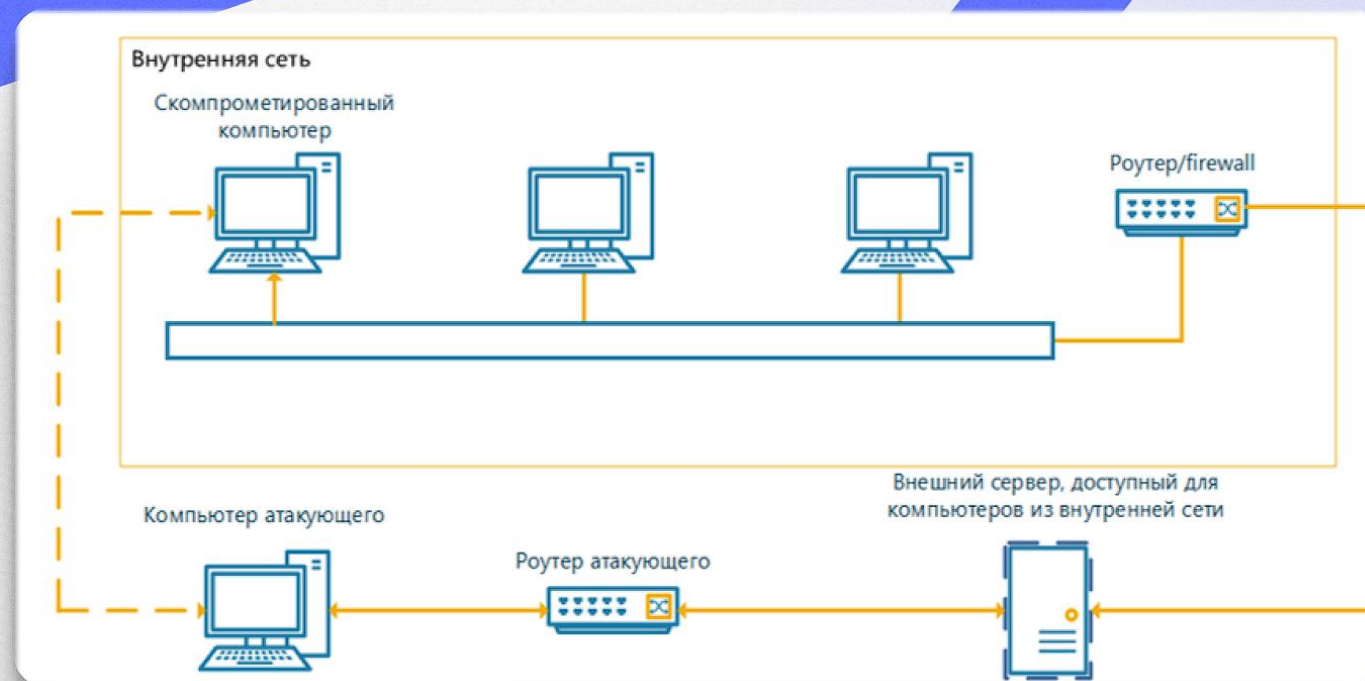


**⚡ ТЫ СКАЗАЛ,
ЧТО ТЫ ШАРИШЬ!**

23 апреля, 19:00 мск

● онлайн

**ПРОЖАРКА ТРЕНДОВ КИБЕРБЕЗА
В ПРЯМОМ ЭФИРЕ**



PIVOTING

- это набор техник, позволяющих обходить сегментацию сетей: получать доступ к закрытым сегментам через один или несколько промежуточных узлов.

Эти техники позволяют развивать атаку после проникновения через внешний периметр: сканировать системы на уязвимости, эксплуатировать их, вести горизонтальное перемещение и закреплять свой доступ с той же эффективностью, как если бы атакующий физически находился во внутренней сети.

ОСНОВНЫЕ ЗАДАЧИ

ПРОКСИРОВАНИЕ ТРАФИКА:

- 01 Сканирование и эnumерация
- 02 Эксплуатация уязвимостей
- 03 Удаленное управление (SSH, WinRM, RDP и т.п.)
- 04 L2-туннелирование для ведения сетевых атак

ПРОБРОС УДАЛЕННЫХ ПОРТОВ НА ЛОКАЛЬНУЮ МАШИНУ:

- 01 Для клиентов, не поддерживающих проксирование
- 02 Для обеспечения доступа к порту для нескольких машин

ПРОБРОС ЛОКАЛЬНЫХ ПОРТОВ НА УДАЛЕННУЮ МАШИНУ:

- 01 Прием соединений от полезных нагрузок при эксплуатации уязвимостей
- 02 Подключение клиентов C2
- 03 Инфильтрация и эксфильтрация (передача файлов и других данных)
- 04 Атаки, требующие подключения от клиента (уязвимости браузера, forced authentication и т.п.)

ИНСТРУМЕНТЫ

☒ C2-клиенты

☒ Специализированные утилиты

☒ SSH

SSH

Плюсы

- Не требует установки дополнительного ПО
- Надежность работы туннелей, шифрование трафика
- Удобство настройки
- Опция ProxyJump позволяет собирать цепочки из произвольного количества хостов
- При наличии прав root можно использовать VPN-туннелирование

Минусы

- Не все пользователи могут заходить в систему по ssh
- Проброс своего порта на удаленную машину регулируется опцией GatewayPorts и в стандартной конфигурации работает только на 127.0.0.1
- Подключения журналируются

```
Host server
  User user
  Hostname 10.0.0.1
  ServerAliveInterval 10
  ServerAliveCountMax 5
  TCPKeepAlive yes
  ProxyJump bastion
  LocalForward 10000 10.0.0.1:3306
  RemoteForward 0.0.0.0:4444 4444
```

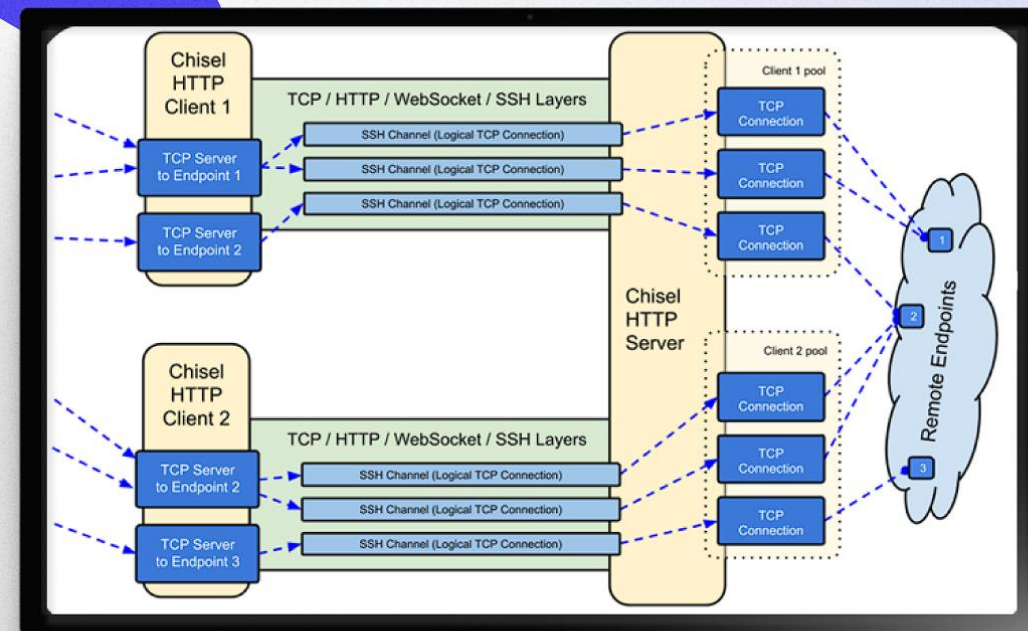
СПЕЦИАЛИЗИРОВАННЫЕ УТИЛИТЫ

Плюсы

- Практически не зависят от прав пользователя и установленного в системе ПО
- Совместимы с абсолютным большинством Linux/Windows систем, в том числе и в их IoT-версиях
- Гибкость настройки и многообразие возможностей по маскировке трафика

Минусы

- Запуск таких утилит может быть слишком подозрительным для некоторых сценариев RedTeam
- Требуют постоянной работы процесса и открытого порта/исходящего соединения



ПРОЕКТ	ССЫЛКА	ОПИСАНИЕ
GO Simple Tunnel	https://github.com/ginuerzh/gost	Многофункциональная утилита, поддерживает множество протоколов и способов обфускации, позволяет составлять цепочки прокси из нескольких хостов, относительно сложна в освоении
Chisel	https://github.com/jpillora/chisel	Утилита для туннелинга TCP/UDP трафика, поддерживает шифрование, проброс портов и работу в качестве SOCKS5-сервера
Ligolo-ng	https://github.com/Nicocha30/ligolo-ng	Утилита для pivoting через tun-интерфейс, позволяет работать с удаленной сетью без использования SOCKS-сервера
Iodine	https://github.com/yarrick/iodine	Утилита для туннелирования IPv4 через DNS-сервер
Neo-reGeorg	https://github.com/L-codes/Neo-reGeorg	Утилита для туннелирования через веб-приложения, поддерживает php, aspx, jsr и другие платформы.
Socat	http://www.dest-unreach.org/socat	Утилита для проброса портов и иных манипуляций при передаче данных, часто используется как вспомогательная

C2-КЛИЕНТЫ

Плюсы

- Возможность управления всеми клиентами из единого C2-сервера
- Интеграция с эксплойтами/сканерами/whatever из используемого фреймворка
- Не требует отдельного процесса под pivoting, может работать при миграции C2 в легитимный процесс

Минусы

- Клиенты C2 зачастую поддерживают только Windows-системы и плохо портируются под не-Intel архитектуры
- Качество реализации механизмов pivoting в некоторых фреймворках приводит к падениям самих C2-клиентов, что может приводить к полной потере контроля над машиной

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(windows/local/ms13_053_schlamperei) > route add 172.16.20.0 255.255.255.0 2
[*] Route added
msf exploit(windows/local/ms13_053_schlamperei) > route

IPv4 Active Routing Table
=====
```

Subnet	Netmask	Gateway
-----	-----	-----
172.16.20.0	255.255.255.0	Session 2

```

[*] There are currently no IPv6 routes defined.
```

ПРИЕМЫ РАБОТЫ С PIVOTING-КЛИЕНТАМИ



Гибридные подходы



Работа через tun-интерфейс: `ligolo-ng`



Работа через socks-проxy: `proxychains`

SOCKS-PROXY: PROXYCHAINS

PROXYCHAINS – ПРОГРАММА ДЛЯ ПРИНУДИТЕЛЬНОГО ПРОКСИРОВАНИЯ ТРАФИКА ЧЕРЕЗ ПЕРЕХВАТ ВЫЗОВОВ СЕТЕВЫХ ФУНКЦИЙ В СТАНДАРТНОЙ БИБЛИОТЕКЕ.

ОСОБЕННОСТИ

- ❑ Поддерживает socks 4a/socks 5/http proxy
- ❑ Может соединять несколько прокси в цепочку
- ❑ Есть несколько реализаций, имеющих значительные различия в функциональности
- ❑ Гибко конфигурируется через proxychains.conf

ПРОБЛЕМЫ ПОДХОДА

- ❑ Перехват функций серьёзно замедляет работу различных сканеров
- ❑ В некоторых случаях возможны падения программы и появление неожиданных ошибок
- ❑ Работает только для динамически скомпонованных исполняемых файлов
- ❑ Не проксирует UDP-трафик

TUN-ИНТЕРФЕЙС: LIGOLO-NG

LIGOLO-NG ИСПОЛЬЗУЕТ ИНОЙ ПОДХОД К ТУННЕЛИРОВАНИЮ: С ЕГО ПОМОЩЬЮ СОЗДАЕТСЯ ВИРТУАЛЬНЫЙ TUN-ИНТЕРФЕЙС, ОБЕСПЕЧИВАЮЩИЙ VPN-LIKE СОЕДИНЕНИЕ.

ОСОБЕННОСТИ

- ❖ Использует реализацию сетевого стека в userland, поддерживает протоколы TCP, UDP и ICMP (echo requests)
- ❖ Заменяет socks-прокси и избавляет от необходимости использовать proxychains
- ❖ Одновременная работа с несколькими агентами
- ❖ Управление сессиями
- ❖ Не требует прав root на стороне клиента
- ❖ Высокая скорость работы
- ❖ Интеграция с Let's Encrypt



ГИБРИДНЫЕ ПОДХОДЫ

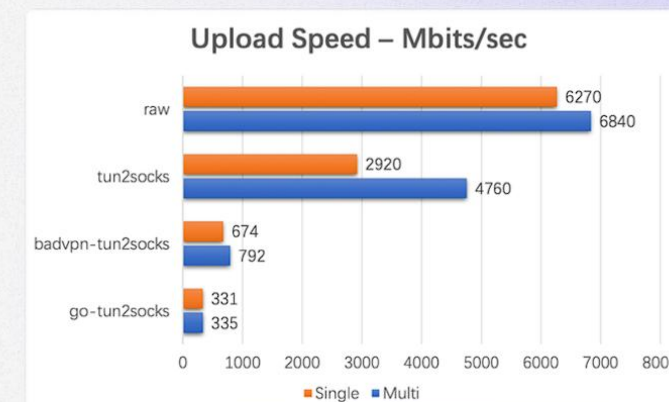
TUN2SOCKS СОЗДАЕТ TUN-ИНТЕРФЕЙС, СОЕДИНЕННЫЙ С ПРОИЗВОЛЬНЫМ SOCKS5-СЕРВЕРОМ, ЕСТЬ ПОДДЕРЖКА WINDOWS.

REDSOCKS ПЕРЕНАПРАВЛЯЕТ TCP-ТРАФИК ПРИЛОЖЕНИЯ В SOCKS5-СЕРВЕР С ПОМОЩЬЮ ПРАВИЛ IPTABLES.

GRAFTCP ПЕРЕХВАТЫВАЕТ СОЗДАНИЕ СЕТЕВЫХ СОЕДИНЕНИЙ С ПОМОЩЬЮ PTRACE

ОСОБЕННОСТИ

- ❑ Относительная независимость от утилиты для pivoting
- ❑ Высокая производительность и надежность работы
- ❑ Поддержка проксирования трафика для любых приложений, в том числе статически скомпонованных



ЭКЗОТИЧЕСКИЕ СЦЕНАРИИ PIVOTING

Зона Nightmare: pivoting и выполнение L2-атак через туннели:

- Требуется права суперпользователя
- Для выполнения атаки нужно находиться в одном сегменте сети с целями
- Высокий риск DoS при ошибках конфигурации
- Наиболее импактная и актуальная техника – развертывание VM с маршрутизатором на контролируемой машине, но многие атаки можно выполнить и напрямую через сетевые мосты

Туннелирование через web-приложения:

- Туннелирование ведется через HTTP-запросы к серверу, что повышает скрытность, но снижает производительность
- Скорость туннелирования зависит от платформы
- Сравнительно небольшое количество реализаций клиентов: neo-regeorg, pivotnacci

Туннелирование через IoT-устройства:

- Специфические архитектуры процессора, преимущественно ARM и MIPS
- Крайне ограниченный объем RAM и свободного места в ФС

МАСКИРОВКА И ОБФУСКАЦИЯ ТРАФИКА



ИНКАПСУЛЯЦИЯ И ОБФУСКАЦИЯ ТРАФИКА



ПРИ PIVOTING ДЛЯ ЛУЧШЕЙ МАСКИРОВКИ ОБЫЧНО ПРИМЕНЯЕТСЯ ИНКАПСУЛЯЦИЯ ПЕРЕДАВАЕМЫХ ДАННЫХ В НЕКИЙ ПРОТОКОЛ И ИХ ПОСЛЕДУЮЩЕЕ ШИФРОВАНИЕ И ОБФУСКАЦИЯ.

Наиболее часто для этого используются протоколы http/https, но есть и утилиты, организующие туннелирование через UDP, ICMP, DNS и иные распространенные протоколы.

ТРАНСПОРТЫ, ИСПОЛЬЗУЕМЫЕ В УТИЛИТЕ GOST

- TCP - RAW TCP
- TLS - TLS
- MTLS - MULTIPLEX TLS
- WS - WEBSOCKET
- MWS - MULTIPLEX WEBSOCKET
- WSS - WEBSOCKET SECURE
- MWSS - MULTIPLEX WEBSOCKET SECURE
- KCP - KCP
- QUIC - QUIC
- SSH - SSH
- H2 - HTTP2 (2.4+)
- H2C - HTTP2 CLEARTXT (2.4+)
- OBFS4 - OBFS4 (2.4+)
- OHTTP - HTTP OBFUSCATION (2.7+)
- OTLS - TLS OBFUSCATION (2.11+)

STANDALONE-УТИЛИТЫ

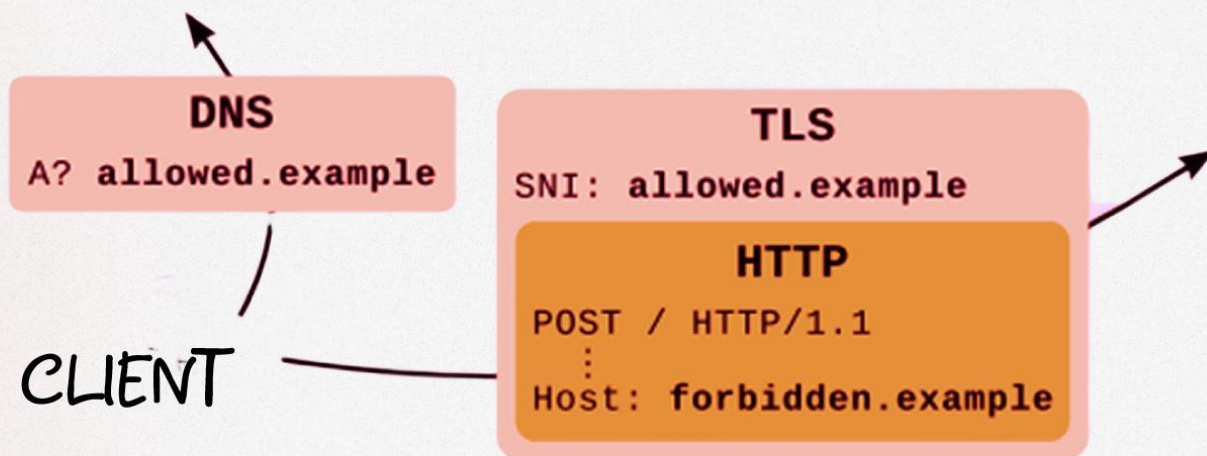
- ICMP_TUNNEL
- UDP_TUNNEL

DOMAIN FRONTING



DOMAIN FRONTING – ТЕХНИКА СОКРЫТИЯ КОММУНИКАЦИЙ С С2 ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ОСОБЕННОСТЕЙ CDN.

Принцип её работы состоит в том что SSL-соединение устанавливается с одним “доверенным” доменом, а HTTP-запрос перенаправляется CDN на хост атакующего.

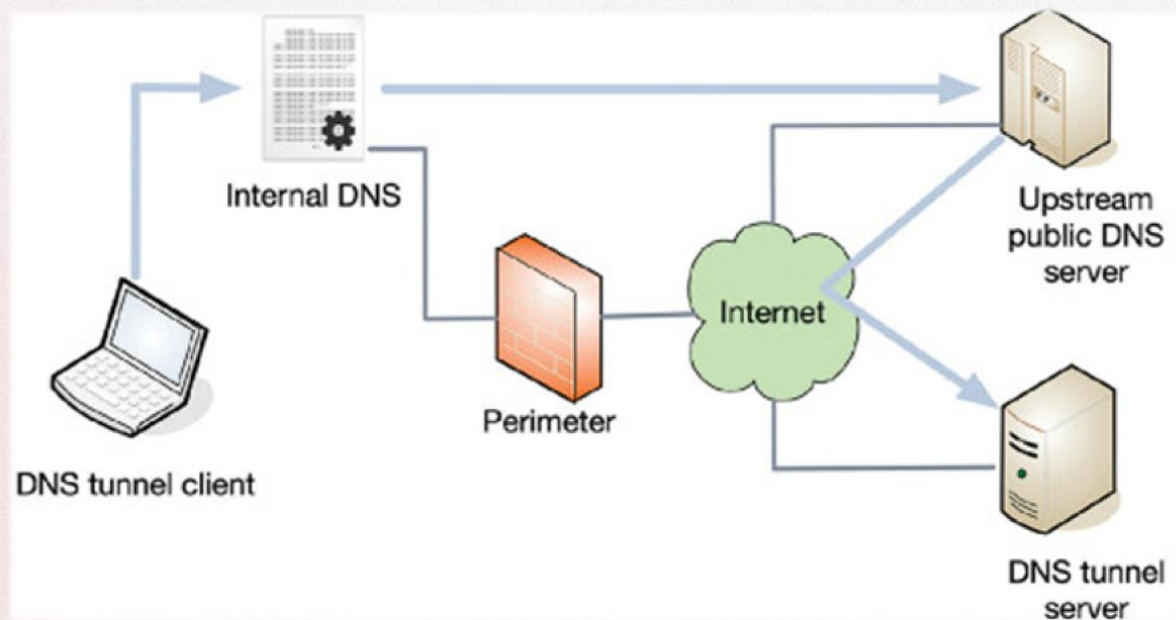


DNS TUNNELING



DNS TUNNELING – ТЕХНИКА ПЕРЕДАЧИ ПРОИЗВОЛЬНЫХ ДАННЫХ ЧЕРЕЗ ПРОТОКОЛ DNS.

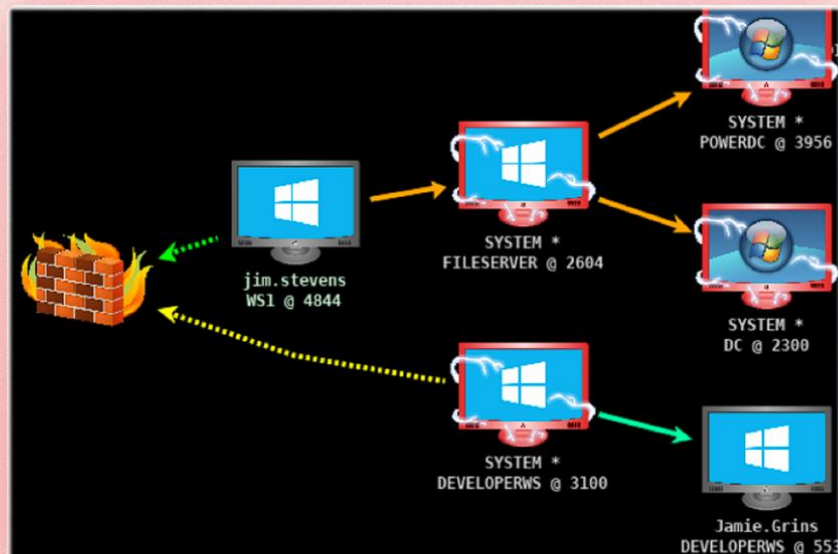
- ❑ Данные кодируются в имени хоста и ответах сервера
- ❑ Применима в изолированных сетях, если локальный DNS-сервер отвечает на произвольные запросы
- ❑ Скорость передачи данных ограничена и несимметрична, выгрузка данных медленнее загрузки



SMB NAMED PIPES



SMB tunneling позволяет передавать данные с помощью именованных каналов SMB. Этот протокол очень активно используется в Windows-сетях, поэтому трафик атакующих может легко затеряться среди обычного.



Pivot graph из C2 Cobalt

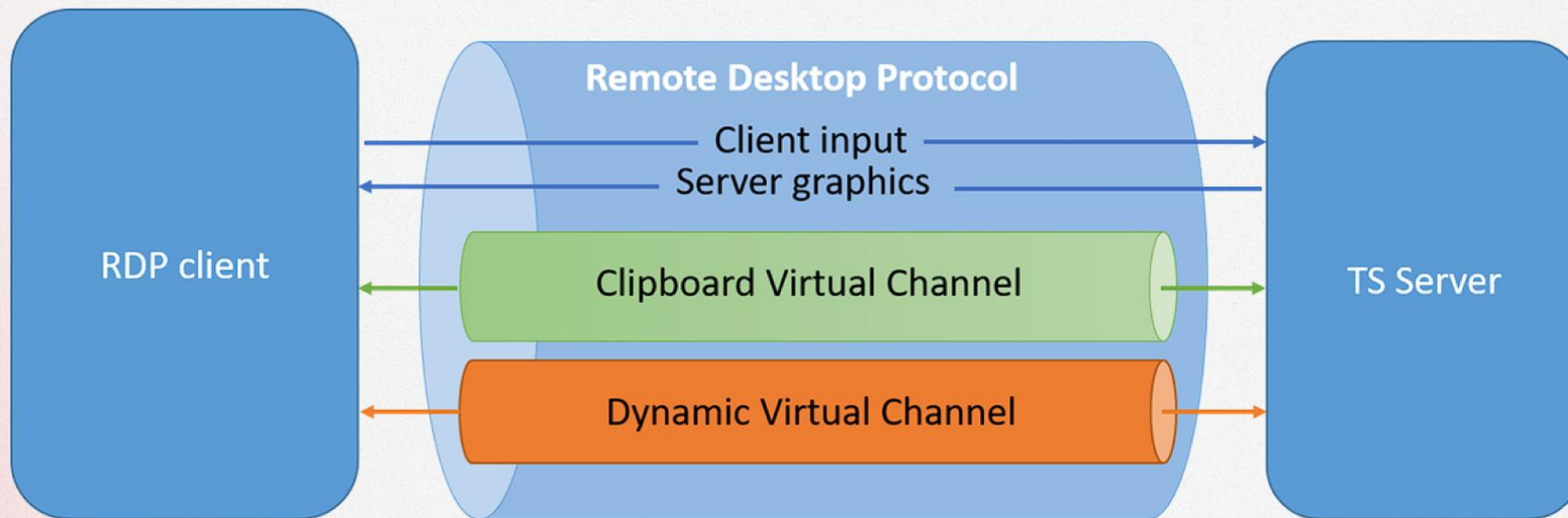
ПРИМЕР ПОДДЕРЖКИ В C2:

- COBALT STRIKE
- METERPRETER
- SLIVER
- BRUTE RATEL

RDP CHANNELS



Динамические виртуальные каналы RDP можно использовать для связи с pivoting-утилитой от имени непривилегированного аккаунта, что позволяет обходить правила файрвола и не открывать новых соединений.



Примеры реализаций: rdp2tcp, SocksOverRDP



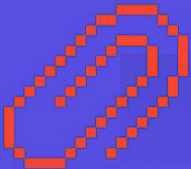
ДОПОЛНИТЕЛЬНАЯ ПРАКТИКА И МАТЕРИАЛЫ

Платформы для тренировок

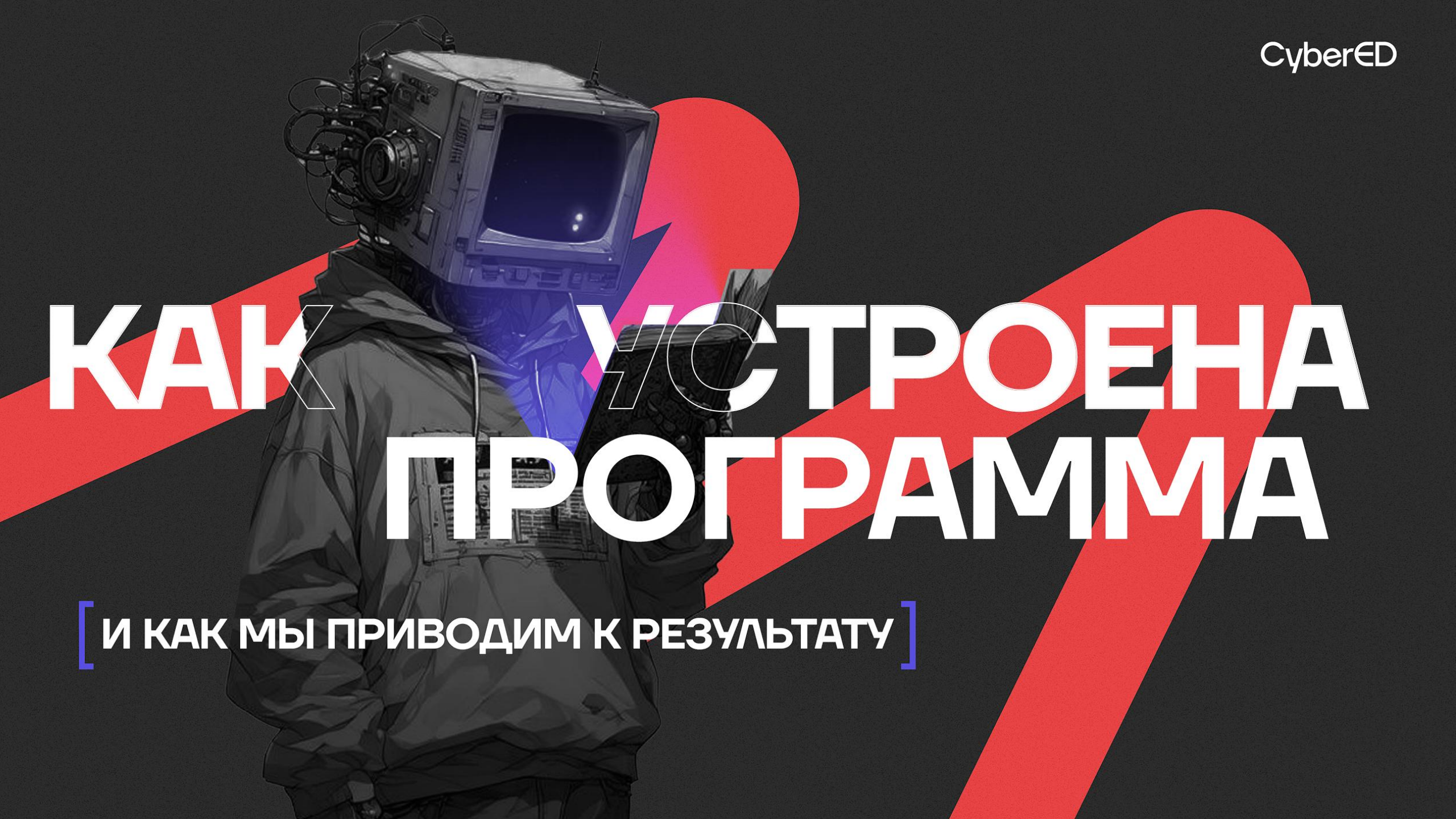
- <https://www.hackthebox.com> – все Endgame и Fortress требуют pivoting для попадания в внутреннюю сеть.
- <https://range.standoff365.com/> – крупные сети со сложной сегментацией.

Примеры команд и тактик

- [PayloadAllTheThings](#) – команды для выполнения популярных утилит для pivoting
- [HackTricks](#) – методология туннелирования и проброса портов
- [Caster Remix](#) – техника развертывания виртуального маршрутизатора в Windows-системе от ИБ-специалиста под псевдонимом Caster
- [Магия SSH](#) – методы проксирования трафика через ssh
- [Meterpreter pivoting](#) – пример реализации pivoting через meterpreter
- [Windows pivoting](#) – тактики передачи файлов и pivoting в Windows
- [DNS tunneling](#) – утилиты для туннелирования через DNS

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ





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

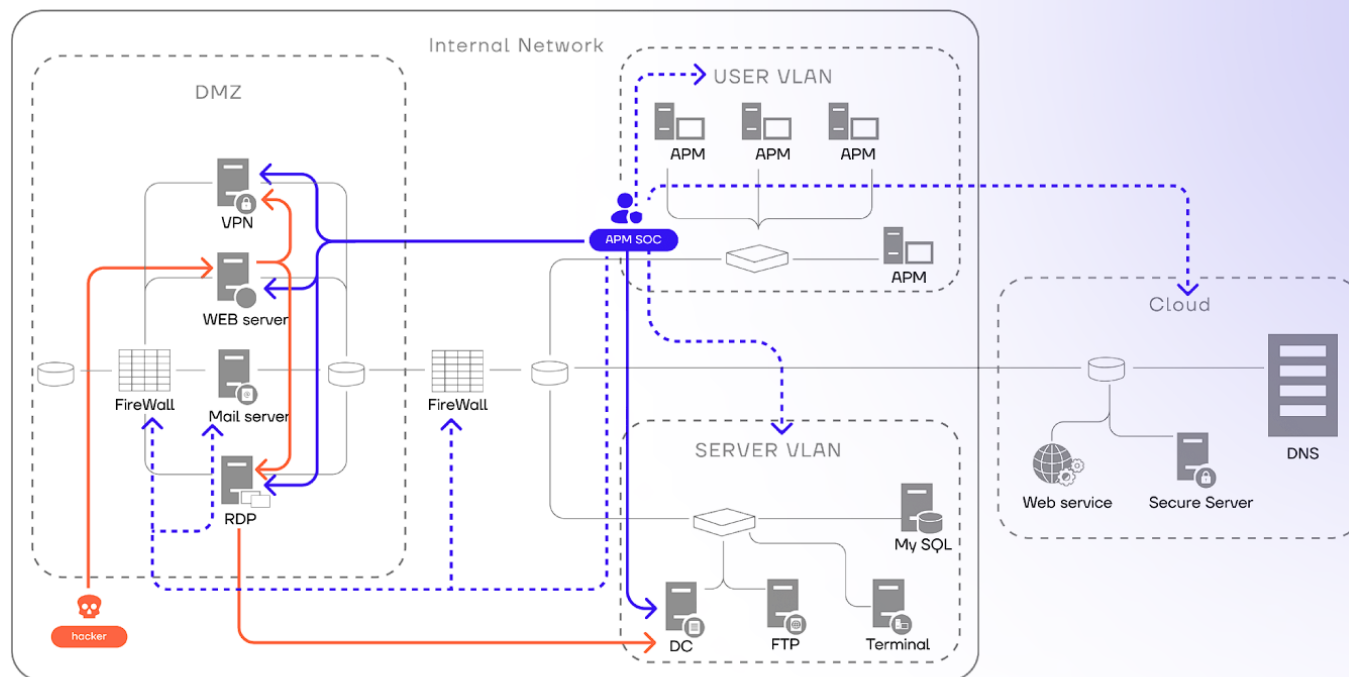
+

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**



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

35%

Red

66%

Blue

24%

AppSec

24%

Fundamentals

Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - M0A

Техника прерывения локальных активностей в
пользовательской среде рабочих станций через

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - M0A

Форензика

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - M0A

Аудит безопасности

Базовый 3/3 Средний 3/3 Продвинутый 3/3

КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: **БАЗОВЫЙ** / **СРЕДНИЙ** / **СЛОЖНЫЙ**■ Видно, что ты
реально умеешь■ Не «написал в CV»
а подтвердил

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

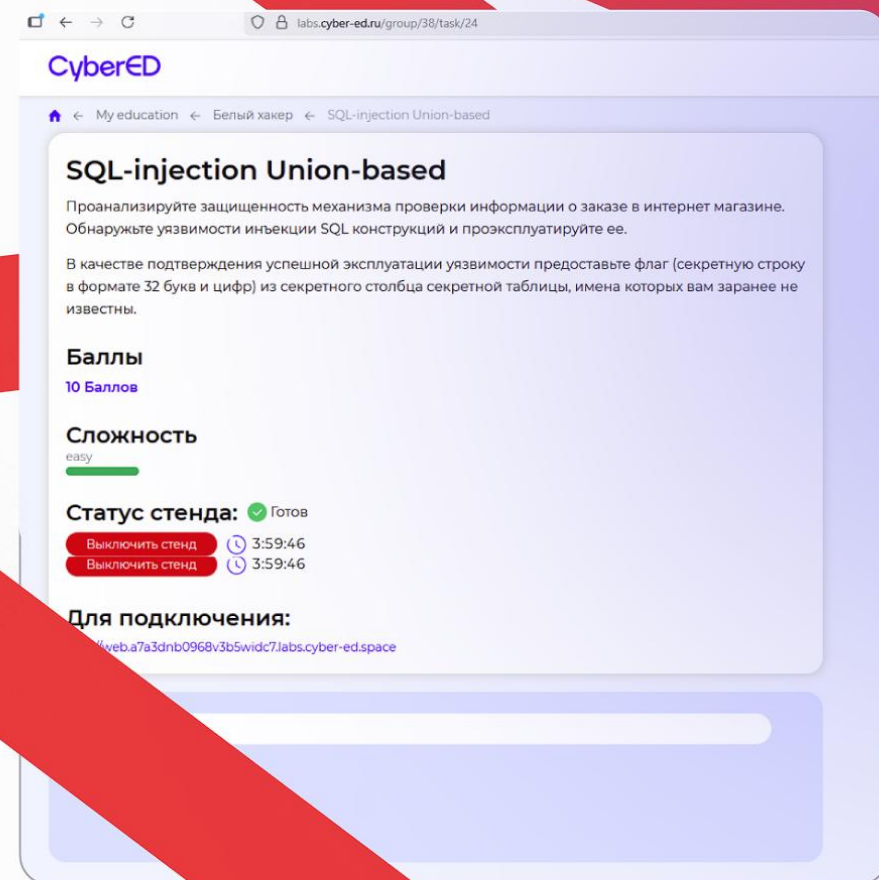
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



Ты **не** «решаешь тест»



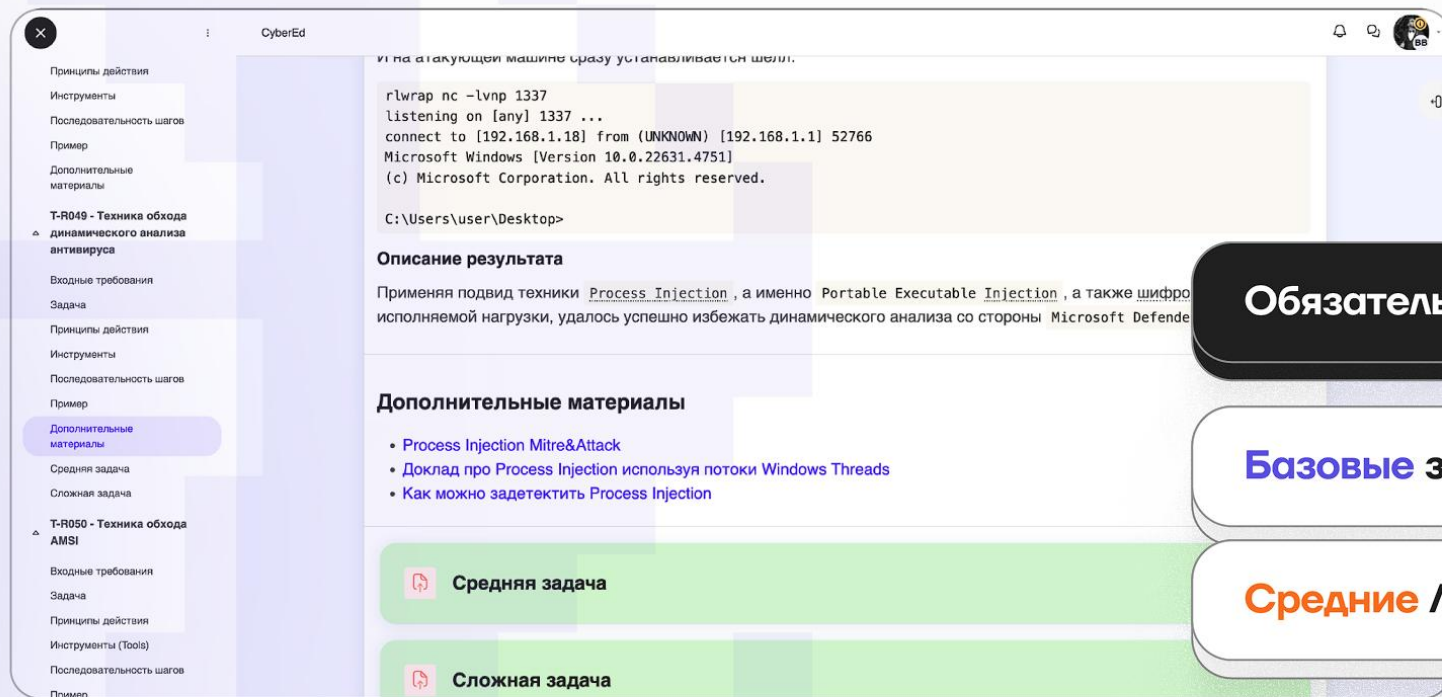
Ты работаешь в инфраструктуре
и получаешь **результат** ⚡ (флаг)



[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

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



- Встроенная система давления на результат → Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

[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

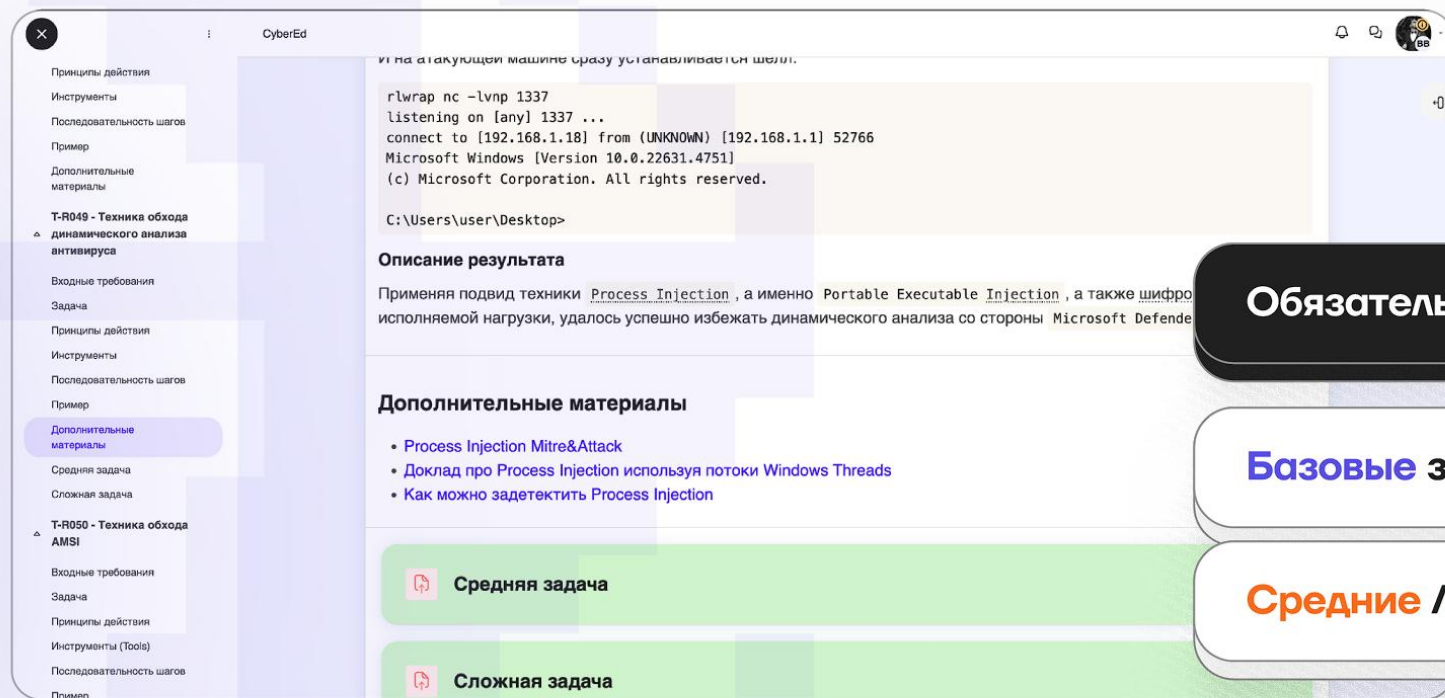
MITRE ATT&CK									
Матрицы Тактика Методы Защитные сооружения СТИ Ресурсы Благотворители Способствовать Блог									
Поиск									
Разведка	Разработка ресурсов	Первоначальный доступ	Исполнение	Упорство	Повышение привилегий	Оборонительное уклонение	Доступ по учетным данным	Открытие	Боковое движение
11 техник	8 техник	11 техник	17 техник	23 техники	14 техник	47 методов	17 техник	34 техники	9 техник
Активное сканирование (3) Соберите информацию о пострадавшем хозяине (4) Соберите информацию о личности жертвы (3) Соберите информацию о сети жертв (5) Соберите информацию об организации-жертве (4) Фишинг информации (4) Поиск в закрытых источниках (2) Поиск в открытых технических базах данных (5) Поиск	Получить доступ Приобретение инфраструктуры (3) Компромишенные счета (2) Компромишенная инфраструктура (3) Развитие потенциала (4) Создание счетов (3) Получить возможности (7) Возможности сценария (6) Поиск в открытых технических базах данных (5) Поиск	Вставка контента Компромисс проеда Использование уязвимостей в общедоступных приложениях. Внешние удаленные сервисы Дополнительные аппаратные средства Фишинг (4) Размножение с помощью съемных носителей Компромисс в цепочке поставок (3) Доверительные отношения Действительные учетные записи (4) Сети Wi-Fi	Команда администрирования облака Интерпретатор команд и скриптов (13) Команда управления контейнерами Развернуть контейнер Команда администрирования ESXi Эксплуатация для исполнения клиентскими операциями Ввод входных данных Микропроцессная коммуникация (3) Нативный API Исполнение отравленного трубопровода Запланированная	Манипулирование учетной записью (7) Вакансии в BITS Выполнение автозапуска при загрузке или входе в систему (14) Сценарий инициализации загрузки или входа в систему (3) Интеграция облачных приложений Компрометировать двоичный файл программного обеспечения хоста Создать аккаунт (3) Создание или изменение системного процесса (5) Изменение политики домена или арендатора (2) Выполнение, инициализированное событием (18) Побег к хосту	Механизм контроля за повышением уровня насилия (6) Манипулирование токенами доступа (3) Вакансии в BITS Создание образа на хосте Обход отладчика Отложенное исполнение Деобфускация/декодирование файлов или информации Развернуть контейнер Прямой доступ к тому Изменение политики домена или арендатора (2) Ограничения исполнения (2) Использование	Механизм контроля за повышением уровня насилия (6) Манипулирование токенами доступа (3) Вакансии в BITS Создание образа на хосте Обход отладчика Отложенное исполнение Деобфускация/декодирование файлов или информации Развернуть контейнер Прямой доступ к тому Изменение политики домена или арендатора (2) Ограничения исполнения (2) Использование	Противник посередине (2) Грубая сила (4) Учетные данные из хранилищ паролей (5) Эксплуатация для получения доступа к учетным данным Принудительная аутентификация Захват ввода (4) Изменение процесса аутентификации (9) Перехват многофакторной аутентификации Генерация запроса на многофакторную аутентификацию	Обнаружение учетных записей (4) Обнаружение окон приложений Обнаружение информации в браузере Обнаружение облачной инфраструктуры Панель управления облачными сервисами Обнаружение облачных сервисов Изменение процесса аутентификации (9) Обнаружение объектов в облачном хранилище Обнаружение контейнеров и ресурсов Обход отладчика	Использование удаленных сервисов Внутренний фишинг Боковая передача инструмента Перехват сеанса удаленной службы (2) Удаленные сервисы (6) Размножение с помощью съемных носителей Инструменты развертывания программного обеспечения Заграждение общего контента Используйте альтернативные материалы аутентификации (4)

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



- Встроенная система давления на результат → Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую
технику применять

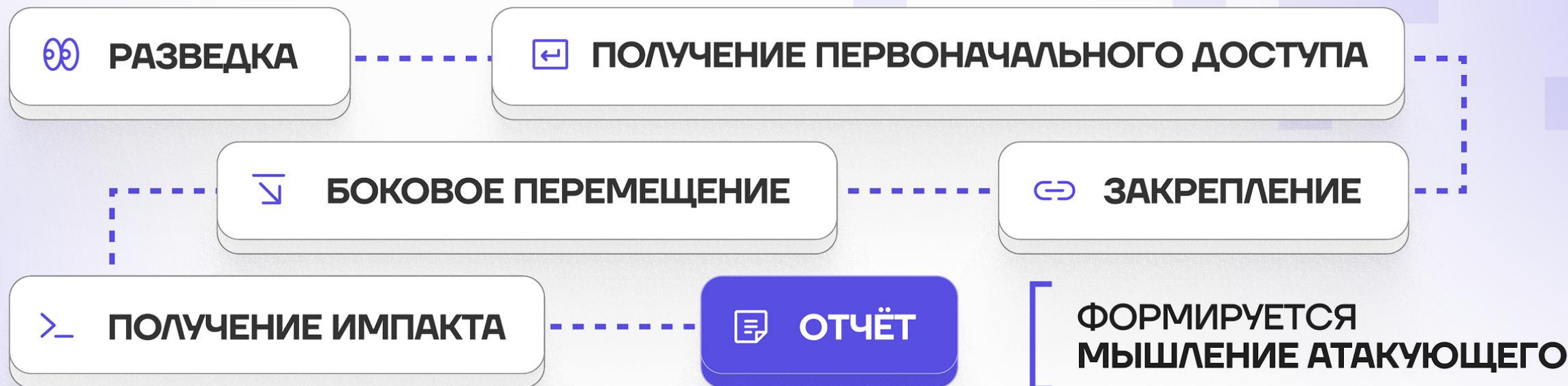


ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

Не изолированные упражнения, а **связанный процесс**

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



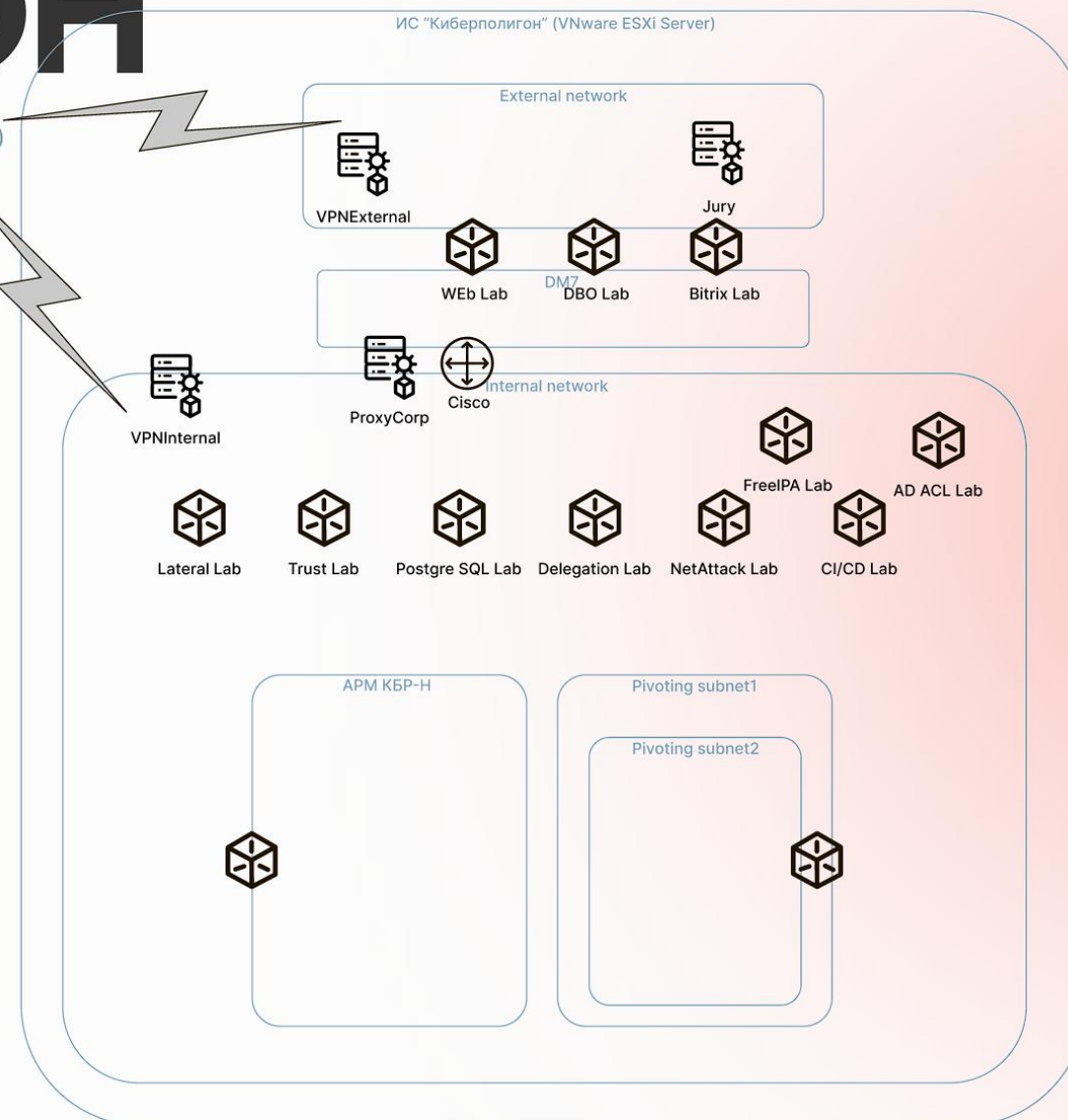
КИБЕРПОЛИГОН

| *** CyberED

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

Максимально близко к работе:

« **ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ** »



КИБЕРПОЛИГОН

| **

CyberED

30

Сценариев

30

Виртуальных
машин

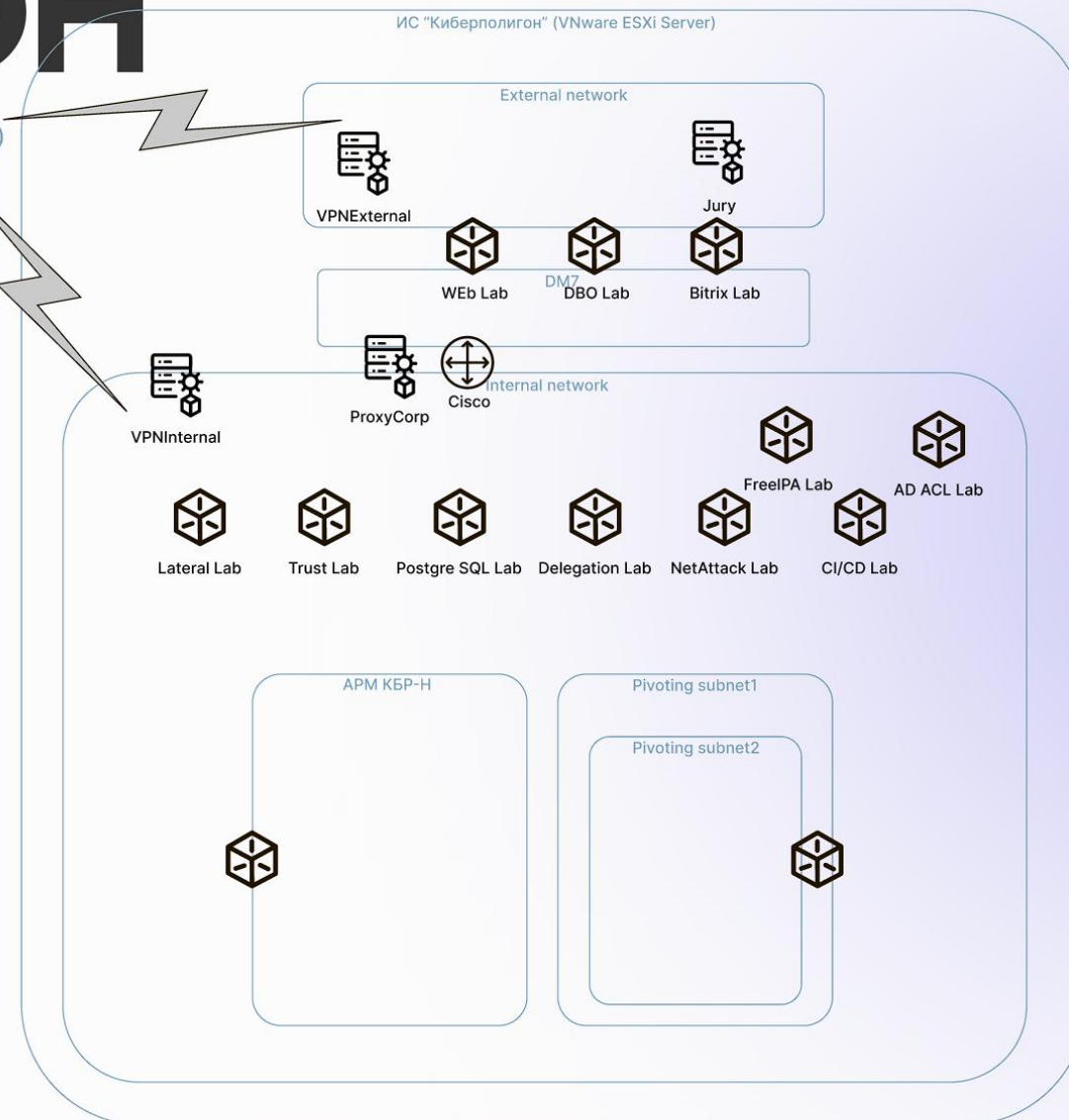
60+

Тасок,
в каждой из которых может быть
несколько уязвимостей.

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.

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

АВТОР КУРСА:

СЕРГЕЙ ЗЫБНЕВ

- Тимлид пентестеров в «Бастион» 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



ОСТАВЛЯЙ ЗАЯВКУ!



ИИ в пентесте от Похек



DETA / Авторский курс Егора Зайцева «Обход антивирусов»



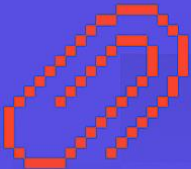
1 **любой** мини-курс из платных программ на выбор



программа «**Bug Bounty Hunter**» совместно со Standoff 365



Карьерный модуль по трудоустройству

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ

