

CyberED

АТАКИ НА ACTIVE DIRECTORY

[ЯРОСЛАВ ШМЕЛЕВ]



О ЧЁМ СЕГОДНЯ

- КАКОЕ МЕСТО ЗАНИМАЕТ ACTIVE DIRECTORY ВО ВНУТРЕННЕМ ПЕНТЕСТЕ?
 - СУТЬ РАБОТЫ, КЛЮЧЕВЫЕ НАВЫКИ, ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ
 - КАК МЫ ОБУЧАЕМ АТАКАМ НА ACTIVE DIRECTORY
 - ПОЧЕМУ ИМЕННО CYBERED?

[СПИКЕР]

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





[СПЕЦИАЛИСТ]

ПО ТЕСТИРОВАНИЮ
НА ПРОНИКНОВЕНИЕ
ACTIVE DIRECTORY

УРОВНИ СПЕЦИАЛИСТОВ

ПЕНТЕСТЕР

JUNIOR PENTESTER

Начинающий специалист, владеющий базовыми техниками тестирования и инструментами

Навыки:

Умение пользоваться базовыми инструментами: MSF, psexec, mimikatz, умение повышать привилегии в Windows и Linux, уверенное владение bash и powershell, навыки автоматизации.

MIDDLE PENTESTER

Уверенный специалист, способный самостоятельно проводить пентесты разных типов

Навыки:

Хорошее знание безопасности AD и Windows, умение проводить продвинутые атаки и не оставлять следов, навыки программирования для разработки своих модулей.

SENIOR PENTESTER

Эксперт, который понимает архитектуру систем и способен находить сложные, нетривиальные уязвимости

Навыки:

Очень глубокие знания устройства корпоративных сетей, осуществление всех этапов Kill Chain, ведение Red Teaming, обширные знания и экспертиза в различных областях.

[ПЕНТЕСТЕР]

[ВОЗМОЖНЫЕ ТРАЕКТОРИИ РАЗВИТИЯ]

ПЕНТЕСТЕР

Горизонтальный рост

Web / API Pentest
Mobile Pentest
Infra / Red Team
Cloud Pentest

Переход в защиту

Detection Engineer
Threat Hunter
Security Engineer

Архитектура

Security Architect

Менеджмент

Lead Pentester
Red Team Lead
Head of Offensive Security
CISO

Исследования

Reverse Engineering
Bug Bounty

Продукт/Бизнес

Security Consultant
Product Manager
Pre-Sale

ПЕНТЕСТ — это технически сложный и сильный вход в профессию, который открывает глубоко специализированные и высокооплачиваемые направления в ИБ

СХОЖИЕ ДОЛЖНОСТИ,

—> КОТОРЫЕ ПОМОГАЮТ ПЕРЕЙТИ **В ПЕНТЕСТ**

- Системный администратор (Linux/Windows)
- Специалист техподдержки (IT Support / Help Desk)
- SOC-аналитик (Tier 1 / Junior)
- Аналитик уязвимостей (Vulnerability Assessment Analyst)
- Разработчик (Web / Backend)
- DevOps / Cloud-инженер

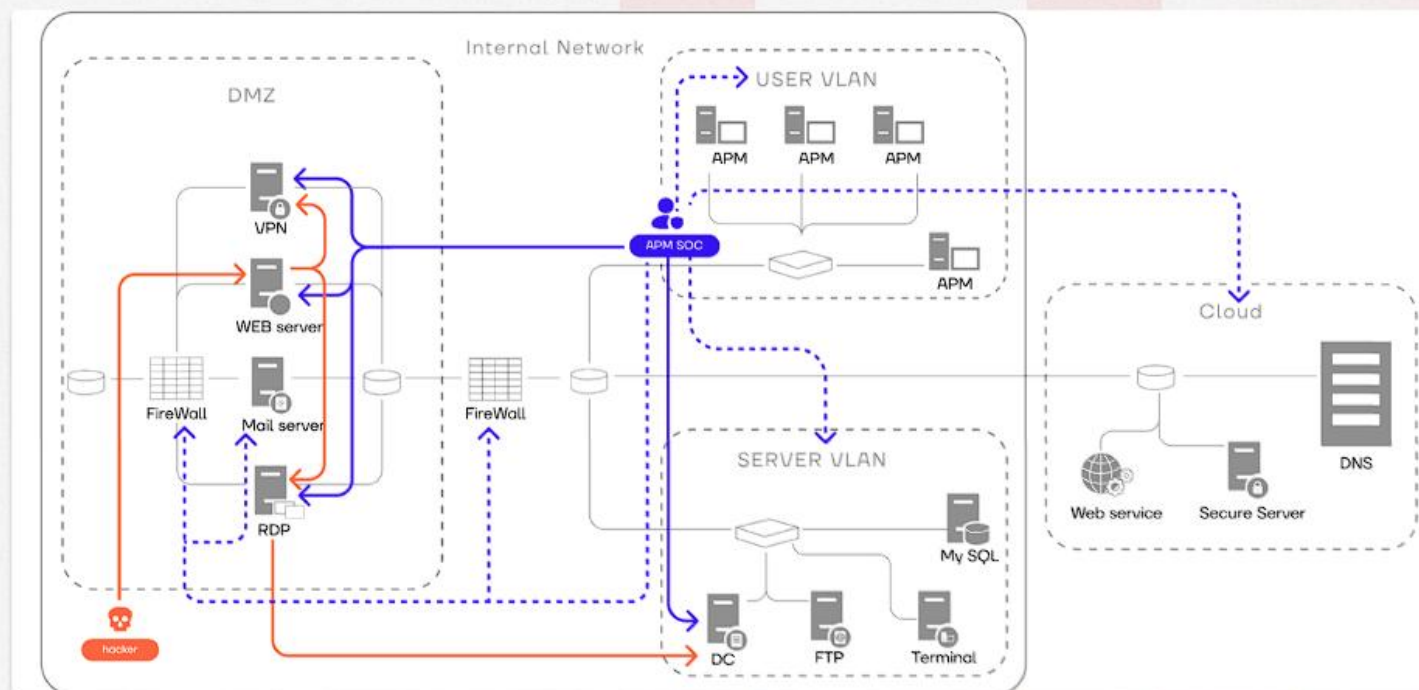
ПЕН
ТЕСТЕР



ПОЧЕМУ

ACTIVE DIRECTORY

- Active Directory – основа архитектуры крупных корпоративных сетей
- Аналоги Active Directory часто совместимы с оригиналом и основаны на схожих принципах



ПОЧЕМУ



ACTIVE DIRECTORY

- Проведение атак требует глубокого понимания каждого этапа, иначе высок риск нарушения бизнес-процессов
- Active Directory применяется и активно развивается уже более 25 лет, фундаментальные знания AD будут актуальными ещё долгое время



На курсе мы глубоко изучаем пентест инфраструктуры на основе AD, не отвлекаясь на смежные направления.



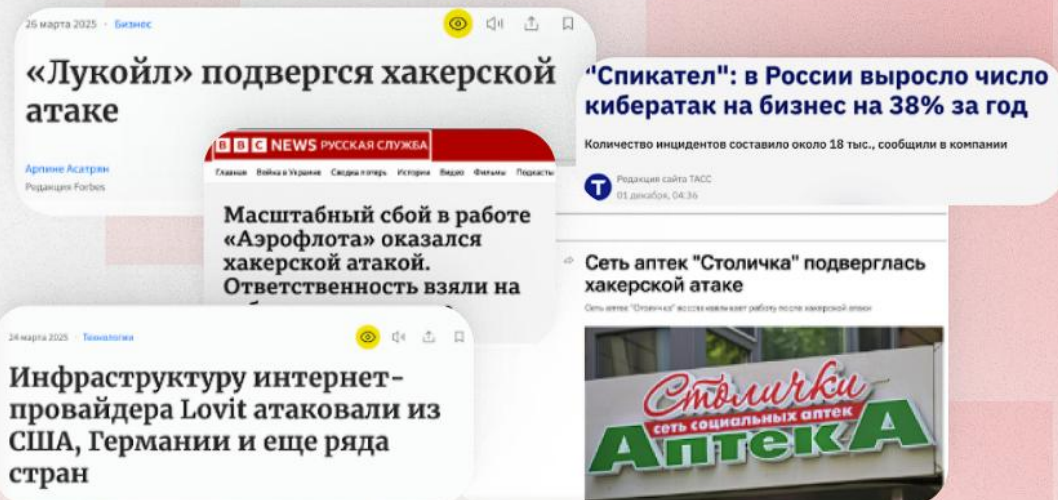
Направлений в пентесте много, но фундамент внутреннего пентеста — это Active Directory.

ПОЧЕМУ ACTIVE DIRECTORY

- Компрометация домена – одна из наиболее частых целей для шифровальщиков и APT-группировок
- Такие атаки могут надолго нарушить бизнес-процессы компании и нанести огромный ущерб бизнесу
- Изучение методов атакующих позволяет как лучше их детектировать, так и убеждаться в адекватности реакции на них при проведении Red Team



Используемые атакующими методы постоянно совершенствуются, для их детекта и воспроизведения нужно глубоко понимать Active Directory.

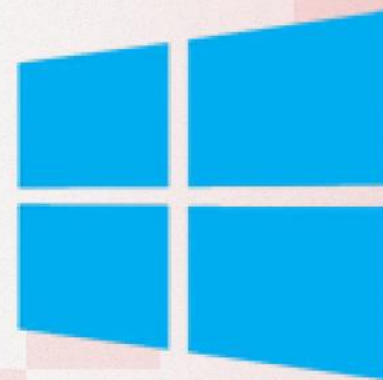


Примеры громких кибератак за 2025

ПОЧЕМУ

ACTIVE DIRECTORY

- Знание методик атак на AD актуально как для Red, так и для Blue/Purple команд
- Изучение атак на AD – отличный вариант для перехода из IT в ИБ, особенно для тех у кого уже есть опыт администрирования корпоративных сетей
- Понимание общей картины атак на AD – основа для роста в архитектора ИБ/CISO



Active Directory



Понимание атак на Active Directory усиливает множество других специализаций и открывает карьерные перспективы.

ТРЕБОВАНИЯ

Опыт работы: 1-3 года

[АНАЛИЗ ВАКАНСИЙ] РАБОТОДАТЕЛЕЙ

➤ Что предстоит:

- + Проведение мероприятий по анализу защищенности **внутренней инфраструктуры заказчика**
- + Проведение мероприятий по анализу защищенности **внешнего периметра** инфраструктуры заказчика
- + Проведение мероприятий по анализу защищенности **мобильных приложений**
- + Оценка уровня защищенности **информационных систем**
- + **Разработка сценариев** для проведения проверок сотрудников заказчика на предмет устойчивости к атакам методами социальной инженерии
- + **Подготовка отчета** по результатам проведенных мероприятий по анализу защищенности инфраструктуры
- + **Формирование рекомендаций** по повышению уровня защищенности инфраструктуры заказчика

Что необходимо:

- + Знание основных методик по анализу защищенности и тестированию на проникновение
- + Уверенные знания и навыки по анализу защищенности web-приложений, OWASP Top-10
- + Уверенные знания и навыки по анализу защищенности Active Directory, FreeIPA
- + Умение работы с инструментами для проведения анализа защищенности
- + Умение работы с инструментами для проведения фишинговых атак
- + Владение языками программирования (Python, Go, Java, PHP и др.)
- + Знание организационных и технических способов и методов защиты информации
- + Знание сетевых технологий и принципов организации локально-вычислительных сетей
- + Знание английского языка (на уровне, достаточном для свободного чтения технической литературы)

[АНАЛИЗ ВАКАНСИЙ]

CyberED



Rutube

Пентестер инфраструктуры



Опыт работы: 1-3 года

Обязанности:

- Проведение регулярного анализа инфраструктуры для выявления уязвимостей в сетевых компонентах, операционных системах и прикладных сервисах методами black box, grey box, white box;
- Проведение комплексного тестирования на проникновение и имитация действий реального противника (Red Teaming) для проверки эффективности мер защиты и работы SOC;
- Проведение тестирования беспроводных сетей;
- Проведение социотехнического тестирования, включая фишинг-атаки и проверку уровня осведомленности сотрудников о правилах безопасности;
- Подготовка рекомендаций по устранению выявленных уязвимостей и улучшению общей безопасности.

Требования:

- Опыт работы от 1 года в роли **пентестера**;
- Понимание сетевых протоколов: стек TCP/IP, HTTP/S, DNS, DHCP, SMB, RPC, RDP;
- Понимание архитектуры современных ОС и корпоративных сред: Windows и Linux/Unix систем, Active Directory;
- Понимание механизмов аутентификации и авторизации: Kerberos, NTLM, LDAP, а также модели разграничения прав (DACL, ACE, GPO);
- Понимание техник перемещения внутри сети: Методы Lateral Movement, использование Pivot-хостов и обход сегментации;
- Знание BASH, *Python* или любого другого средства скриптовой автоматизации для решения прикладных задач.

[АНАЛИЗ ВАКАНСИЙ]

CyberED



Faberlic

RedTeam специалист



Опыт работы: 1-3 года

Чем предстоит заниматься:

1. Проводить оценку наших текущих правил детектирования в SIEM на предмет функционала их обнаружения.
2. Общаться с командой Аналитиков SOC в рамках разработки/улучшения детектирующей логики.
3. Проводить киберучения с использованием платформы BAS и фреймворков тестирования на проникновение.
4. Исследовать новые техники атак и совместно с командой SOC-аналитиков работать над устранением пробелов в детектировании.
5. Регулярно проводить воркшопы Аналитикам SOC для обмена опытом.
6. Подготовка квартального отчета руководству по текущему уровню зрелости сценариев обнаружения и roadmap по их улучшению.

Чем для нас важно:

1. Опыт работы в роли Инфраструктурного **пентестера** или RedTeam специалиста не менее 1 года
2. Опыт работы с BAS-платформами и создания кастомных сценариев эмуляции техник по MITRE ATT&CK
3. Опыт работы с Linux на уровне администратора
4. Понимание ключевых техник атак на инфраструктуру Windows и Active Directory и умеешь их воспроизводить на практике
5. Имеешь опыт применения популярных фреймворков тестирования на проникновение (например, Cobalt Strike, Metasploit, Empire, netexec и др)
6. Готовность активно развиваться в направлении RedTeam, работать в команде.

Что будет преимуществом:

1. Обладаешь опытом разработки правил детектирования в SIEM(мы используем ELK)
2. Имеешь опыт работ в задачах по управлению уязвимостями

[АНАЛИЗ ВАКАНСИЙ]



Сберкорус

Пентестер/Инженер по тестированию защищенности



Опыт работы: 1–3 года

Чем предстоит заниматься:

Основной задачей будет анализ возможности эксплуатации уязвимостей, в частности:

- Выявление уязвимостей и мисконфигураций в информационных системах, веб-приложениях, системном и прикладном ПО
- Проведение проверок применимости уязвимостей, выявленных различными СЗИ
- Оценка (триаж) уязвимостей
- Определение методов и приоритетов устранения уязвимостей
- Формирование аналитических отчетов об уязвимостях
- Инициирование работ по устранению уязвимостей

Ты идеальный для нас кандидат, если у тебя есть:

- Знание базовых мер обеспечения информационной безопасности
- Знание основных типов атак, способов эксплуатации уязвимостей и противодействия им
- Знание стандарта оценки уязвимостей CVSS
- Понимание архитектуры сети и сетевых технологий
- Способность к аналитической работе с данными и внимательность к деталям

Будет большим плюсом:

- Участие в CTF-соревнованиях
- Опыт поиска уязвимостей в качестве внешнего или внутреннего **пентестера** / Red Team / багхантера
- Навыки работы с OWASP ZAP, Burp, Nuclei, Acunetix
- Профильные сертификаты: CEH (Certified Ethical Hacker) и OSCP (Offensive Security Certified Professional)

КЛЮЧЕВЫЕ ВЫВОДЫ [ИЗ АНАЛИЗА ВАКАНСИЙ]

ОС и сети:

- + Уверенное знание и администрирование Windows / Linux (особенно **Astra, Kali, Parrot**)
- + Сетевые технологии:
- + Глубокое понимание протоколов **TCP/IP, HTTP/S, DNS, SMB, LDAP**
- + Принципов построения **корпоративных сетей** и **Active Directory**.

Безопасность приложений и инфраструктуры:

- + **Active Directory (AD)**: понимание принципов работы и методов ведения атак на AD
- + **Обход защиты**: опыт обхода EDR, AV и методов защит.

Программирование и автоматизация (скриптинг):

- + **Python, Bash, PowerShell** - обязательный минимум
- + Желательно также знание **JavaScript, PHP, Go, C/C++**

Зачем?

- написание собственных эксплойтов (PoC),
- доработка чужого кода
- автоматизация рутинных задач.

Инструменты и методологии

► Базовый набор:

- + **Nmap** - сканирование портов и сетей
- + **Impacket** - набор библиотек и скриптов, применяемых преимущественно для аудита AD
- + **Metasploit** - фреймворк для эксплуатации
- + **Cobalt, Empire** - C2-фреймворки
- + **Wireshark / tcpdump** - анализ трафика

КАК ОБЫЧНО ПРОИСХОДИТ НАЙМ

[СПЕЦИАЛИСТОВ ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ]

- | | | |
|-----------|------------------------------|--|
| 01 | Скрининг (HR): | Проверка на адекватность и наличие базы (техническое образование или профильные курсы) |
| 02 | Техническое интервью: | <ul style="list-style-type: none">— Глубокий опрос по знаниям инструментов, умение обходить СЗИ— Могут попросить рассказать примеры проведения пентеста из собственного опыта— Знания сетей и операционных систем, понимание основных протоколов— Написание собственных инструментов и эксплойтов |
| 03 | Практическое задание: | Решить CTF-задание или более реальный кейс (опционально) |

ПРИЧИНЫ ПРОБЛЕМ

[НА СОБЕСЕДОВАНИИ]

-  Слабая фундаментальная база (сети, протоколы, архитектура AD)
-  Недостаток практических навыков (Linux/CLI, работа с инструментами, поиск уязвимостей)
-  Нет подтвержденной практики

Например:

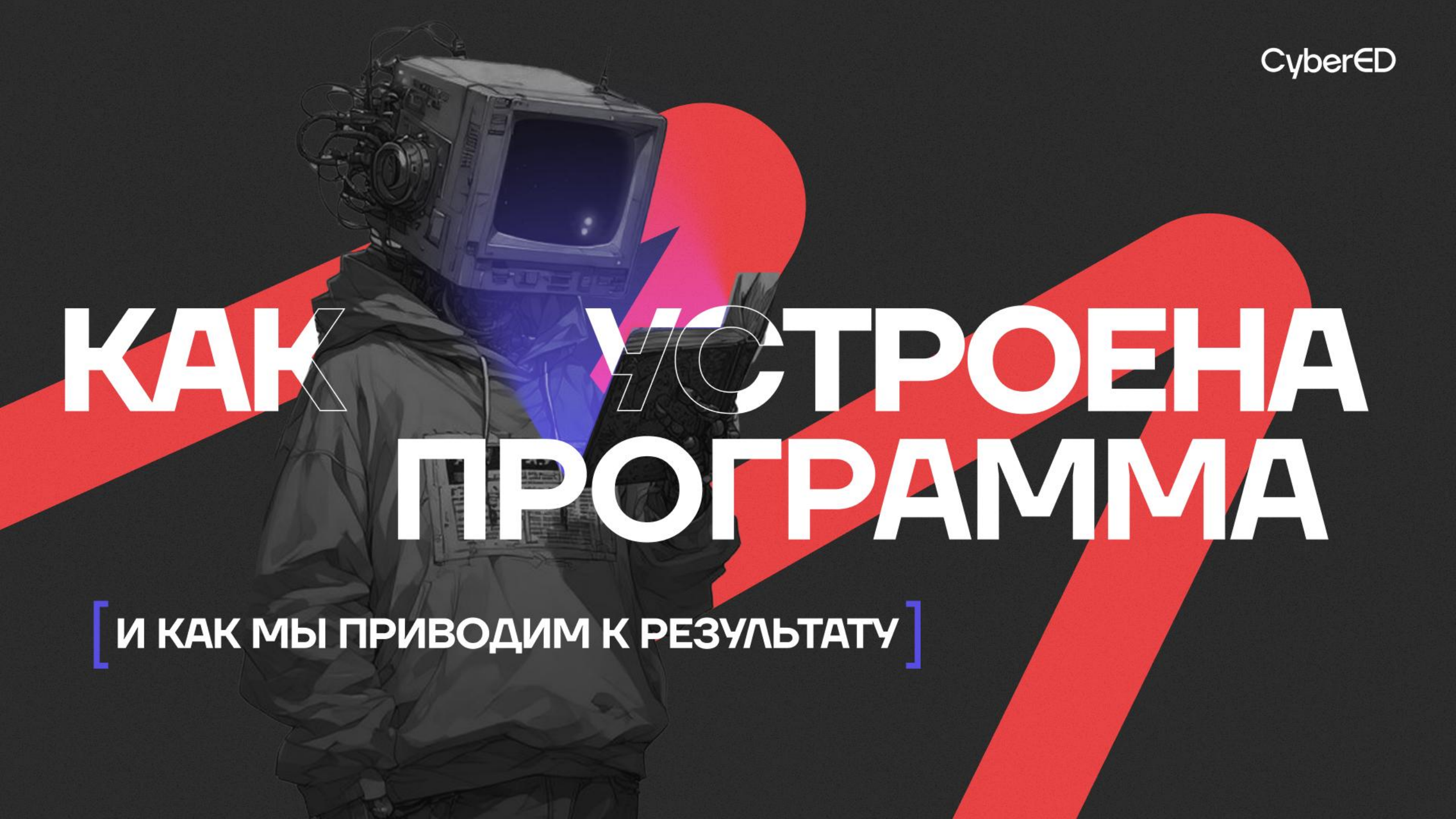
- + Решение CTF
- + Прохождение курсов
- + Кейсы в портфолио



На собеседовании нужно показать: база + логика + практика



Работодатели часто жалуются, что соискатели **не могут** объяснить, почему инструмент работает принцип работы инструмента и какие уязвимости проверяет данный инструмент на уровне работы протоколов



КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

КОМБИНАЦИЯ ИНСТРУМЕНТОВ

[✓] [ОПРЕДЕЛЯЮЩИХ СПЕЦИАЛИСТА]

01



РАЗВЕДКА В ДОМЕНЕ

BloodHound, ADexplorer, средства PowerShell/impacket.

02



СКАНИРОВАНИЕ

Nmap, Masscan, nxc

03



ГОРИЗОНТАЛЬНОЕ ПЕРЕМЕЩЕНИЕ:

Impacket, evil-winrm, xfreerdp

04



ВЕДЕНИЕ АТАК:

bloodyAD, certipy, ntlmrelayx, krbrelayx, responder

05



АНАЛИЗ ТРАФИКА И СНИФФИНГ

Above, Wireshark

06



ВЕДЕНИЕ ОТЧЕТА И КОЛЛАБОРАЦИЯ:

Obsidian, PCF, Faraday.

СТРУКТУРА КУРСА



ОСНОВЫ ACTIVE DIRECTORY

- 01 Структура Active Directory
- 02 Основы протоколов аутентификации: Kerberos, NTLM , PKInit
- 03 Эксплуатация низковисящих фруктов: NoPac, PrintNightmare
- 04 Сбор информации, password spraying, горизонтальное перемещение

Понимание основ архитектуры Active Directory и используемых в ней протоколов аутентификации позволяет эффективно эксплуатировать известные уязвимости

СТРУКТУРА КУРСА



АТАКИ PRE2K И TIMEROASTING

- 01 Атака Pre2k
- 02 Атака Timeroasting

Получение первичного доступа открывает путь для дальнейшего продвижения в инфраструктуре

СТРУКТУРА КУРСА



АТАКИ НА KERBEROS

- 01 Атака ASREQroasting
- 02 Атака ASREProasting
- 03 Атака Kerberoasting
- 04 Атака Blind Kerberoasting
- 05 Перечисление пользователей и распыление паролей

Kerberos – основной протокол аутентификации в Active Directory

СТРУКТУРА КУРСА



АТАКИ НА ЦЕНТР СЕРТИФИКАЦИИ

- 01 ESC1
- 02 ESC4
- 03 ESC7
- 04 ESC8
- 05 ESC15

Атаки на центр сертификации зачастую могут приводить к компрометации домена

СТРУКТУРА КУРСА



АТАКИ НА ACL

- | | |
|-----------------------|--|
| 01 GPO Abuse | 06 ForceChangePassword |
| 02 SPN Jacking | 07 AddMember |
| 03 Shadow Credentials | 08 ReadGMSAPassword |
| 04 Abuse Logon Script | 09 ReadLAPSPassword |
| 05 TargetedKerberoast | 010 Grant Ownership и Grant FullContol |

Небезопасная конфигурация ACL может открыть множество возможностей для горизонтального перемещения и других атак

СТРУКТУРА КУРСА



RELAY-АТАКИ

- 01 NTLM Relay
- 02 Kerberos Relay
- 03 NTLM Reflection

Релеинг протоколов аутентификации – классический, но все ещё крайне эффективный вектор атаки

СТРУКТУРА КУРСА



АТАКИ НА ДЕЛЕГАЦИЮ

- 01 Основы делегации Kerberos и Protected Users
- 02 Атаки на неограниченную делегацию
- 03 Атаки на ограниченную делегацию
- 04 Атаки на RBCD

Делегирование в Kerberos – сложный механизм, на него существует множество атак и вариантов их исполнения

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

При покупке одного
из курсов:

- Атаки на Active Directory
- Анализ безопасности мобильных приложений
- Программирование на Python для пентестеров

+



В подарок

**2 МИНИ-КУРСА
НА ВЫБОР В
ПОДАРОК**

из трека R301 и
курса DETA

+



Скидка

**скидка 10% за
покупку в
течение недели**



@CYBERED_RUSSIA

СТРУКТУРА ОБУЧЕНИЯ НА КУРСЕ

ИЗУЧЕНИЕ ТЕОРИИ

7 модулей с подробным изложением принципов работы 36 техник атак и примеры их применения в различных ситуациях.

CYBERED LABS

Проверка знаний на практике через самостоятельное применение техник на обучающих стендах, развернутых в инфраструктуре CyberEd.

СЕМИНАРЫ С ЭКСПЕРТОМ

9 встреч с преподавателем курса для разбора сложных кейсов и ответов на вопросы по изучаемому материалу



[ИЗУЧЕНИЕ ТЕОРИИ]

РАБОТА С LMS

ПОДРОБНОЕ ИЗЛОЖЕНИЕ ПРИНЦИПОВ РАБОТЫ ТЕХНИК И ИНСТРУМЕНТОВ

Алгоритм действий по сканированию узлов сети

На примере самого распространенного сканера сети `nmap` рассмотрим, как можно просканировать произвольное пространство сети:

1. Определить адрес подсети, в которой будет производиться поиск узлов. Например, `192.168.88.0/24`.
2. Провести Ping-сканирование сети: `nmap -sn --traceroute <network>`.
 - `-sn` — ping-сканирование. По умолчанию посылаются запрос на ICMP-эхо-запрос и TCP-ACK пакет на порт 80;
 - `--traceroute` — также для того, чтобы проводить трассировку маршрута до каждого найденного узла. Эта опция может помочь в составлении карты подсети.
3. Если есть подозрение, что ICMP-пакеты и TCP-ACK сообщения блокируются сетевым экраном, можно применить другие виды сканирования:
 - `-ps` — TCP-SYN сканирование;
 - `-pu` — UDP сканирование;
 - `-pe`; `-pp`; `-pm` — ICMP-сканирование других типов: запрос временной метки (13), информационный запрос (15), запрос адресной маски (17). Многие узлы и брандмауэры могут блокировать исключительно ICMP-пакеты типа echo request, но в спецификации ICMP присутствуют еще несколько типов запросов, позволяющих получить ответ от узлов.

Введение в курс

Текст и медиа: 0 Страницы: 8

Онлайн-встреча программы «Профессия Белый Хакер»

Текст и медиа: 1

Белый хакинг

Текст и медиа: 2

Разведка во внешней инфраструктуре заказчика

Текст и медиа: 0 Задания: 1 Тест: 1

Прогресс: 0 / 1

Вебинар 2. Воркшоп: разведка, Initial Access, Web

Текст и медиа: 1

Атаки первичного доступа

Текст и медиа: 2 Тест: 1

Взлом веб-приложений

Текст и медиа: 0 Задания: 7 Тест: 1

Эксплуатация известных уязвимостей сетевых сервисов

Текст и медиа: 2 Задания: 1 Тест: 1

[ЖИВАЯ ПРАКТИКА]

ПРАКТИКА НА LABS

ЗАКРЕПЛЕНИЕ ТЕОРИИ
НА МНОЖЕСТВЕ РЕАЛЬНЫХ ПРИМЕРОВ



Enumeration (Easy)

Домен: corp.local. Вам известна только информация о домене....

Легко

Сдано решений: 1



Timeroasting (Easy)

Домен: corp.local. Проведите атаку Timeroasting (NTP) на машинные...

Легко

Сдано решений: 1



AS-REQ Roasting (Medium)

Домен: corp.local. Флаг: C:\Users\Administrator\flag.txt на...

Средне

Сдано решений: 0



AS-REQ Roasting

Ответом является пароль пользователя в открытом виде....

Легко

Сдано решений: 1

[ЖИВАЯ ПРАКТИКА]

ПРАКТИКА НА LABS

СТЕНДЫ **ДЛЯ ЗАКРЕПЛЕНИЯ КАЖДОЙ ТЕХНИКИ**

AS-REP Roasting (Medium)

Домен: corp.local. Начальной доменной учётки нет.

Флаг: C:\Users\Administrator\flag.txt на доменном контроллере.

[Посмотреть write-up](#)

Сложность

medium



Статус стенда:  Выключен

[Развернуть стенд](#)

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

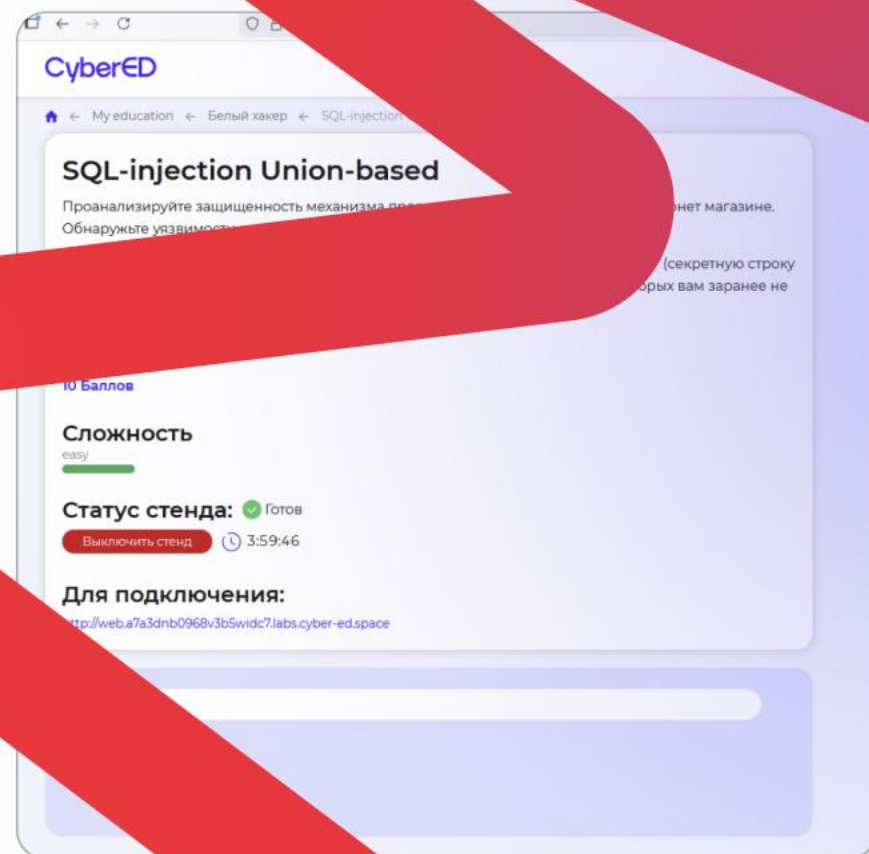
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



Ты **не** «решаешь тест»



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



ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую
технику применять



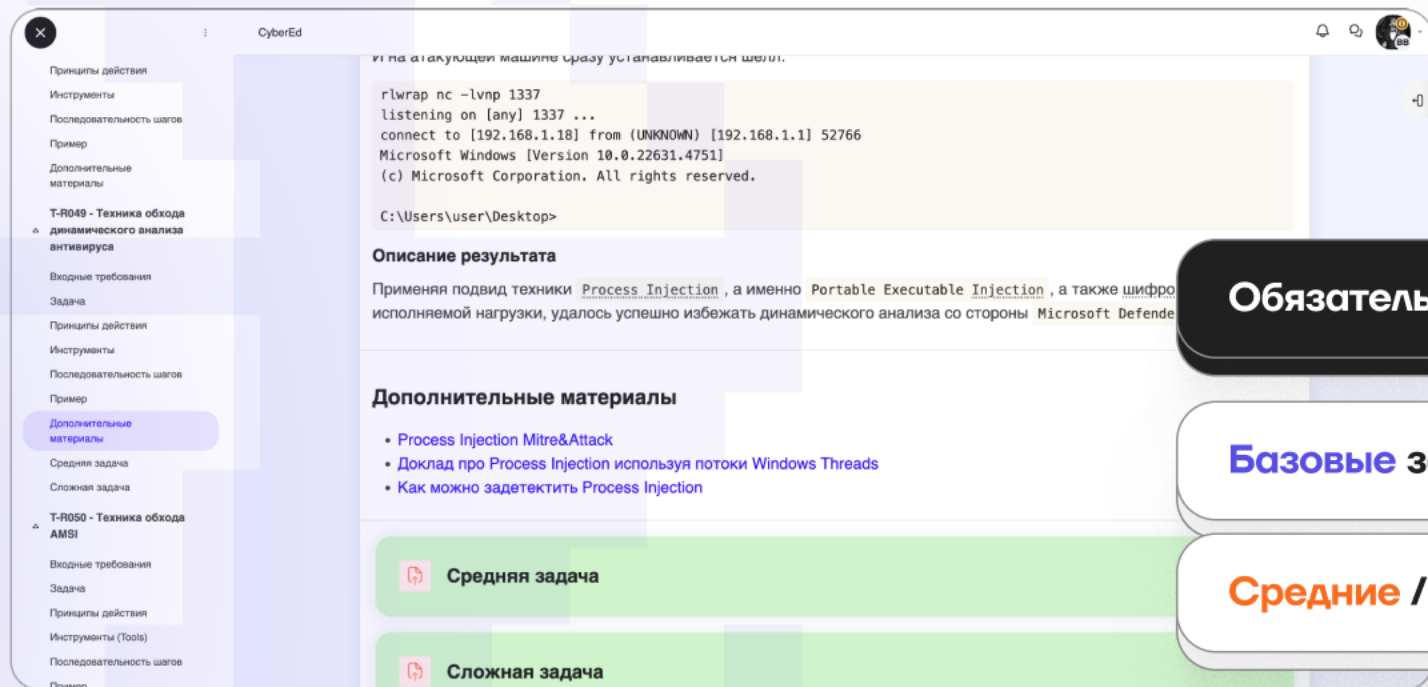
ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ
ДО УРОВНЯ **СЛОЖНОСТИ**,
→ КТОРЫЙ 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

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

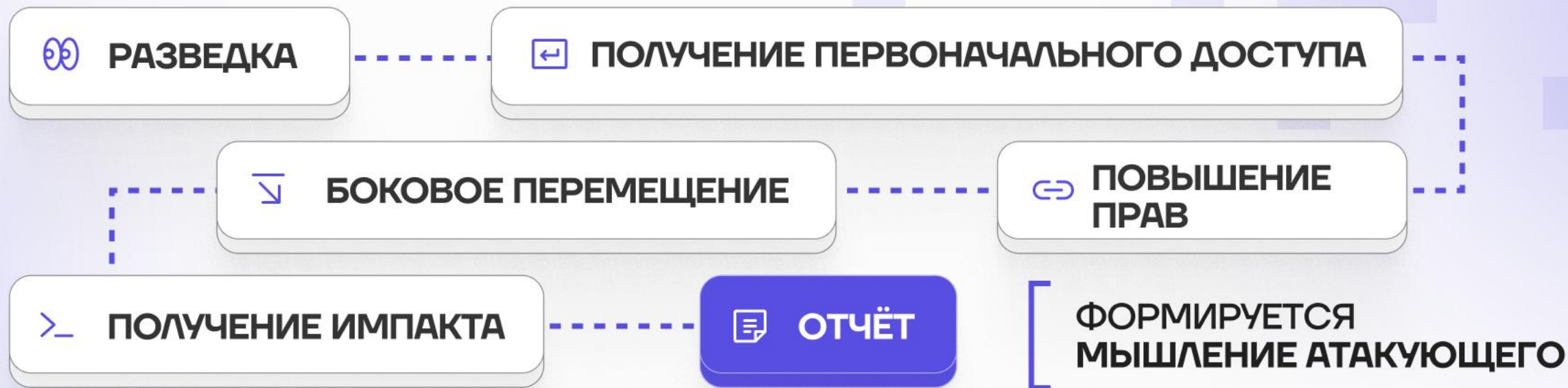
«ПОСМОТРЕЛ И ПОШЁЛ ДАЛЬШЕ»

ЭТО

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

Не изолированные упражнения, а **связанный процесс**

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



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 - MOA

Техника обнаружения аномальных активностей в
локальных сетях и работе рабочих станций через
активные соединения

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

R301 - MOA

Форензика

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

R301 - MOA

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

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 - MOA

Техника обнаружения аномальных активностей в
локальных сетях с помощью рабочих станций через

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

R301 - MOA

Форензика

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

R301 - MOA

Аудит безопасности

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

КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

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

ПРЕИМУЩЕСТВА КУРСА

- РАЗБОР СЛОЖНЫХ КЕЙСОВ НА СЕМИНАРАХ С ЭКСПЕРТОМ-ПРЕПОДАВАТЕЛЕМ
 - ГЛУБОКОЕ ИЗУЧЕНИЕ АКТУАЛЬНЫХ ПРАКТИЧЕСКИХ ТЕХНИК
 - ИНДИВИДУАЛЬНАЯ ИНФРАСТРУКТУРА ДЛЯ КАЖДОГО СТУДЕНТА
 - ФОКУС ИСКЛЮЧИТЕЛЬНО НА ACTIVE DIRECTORY

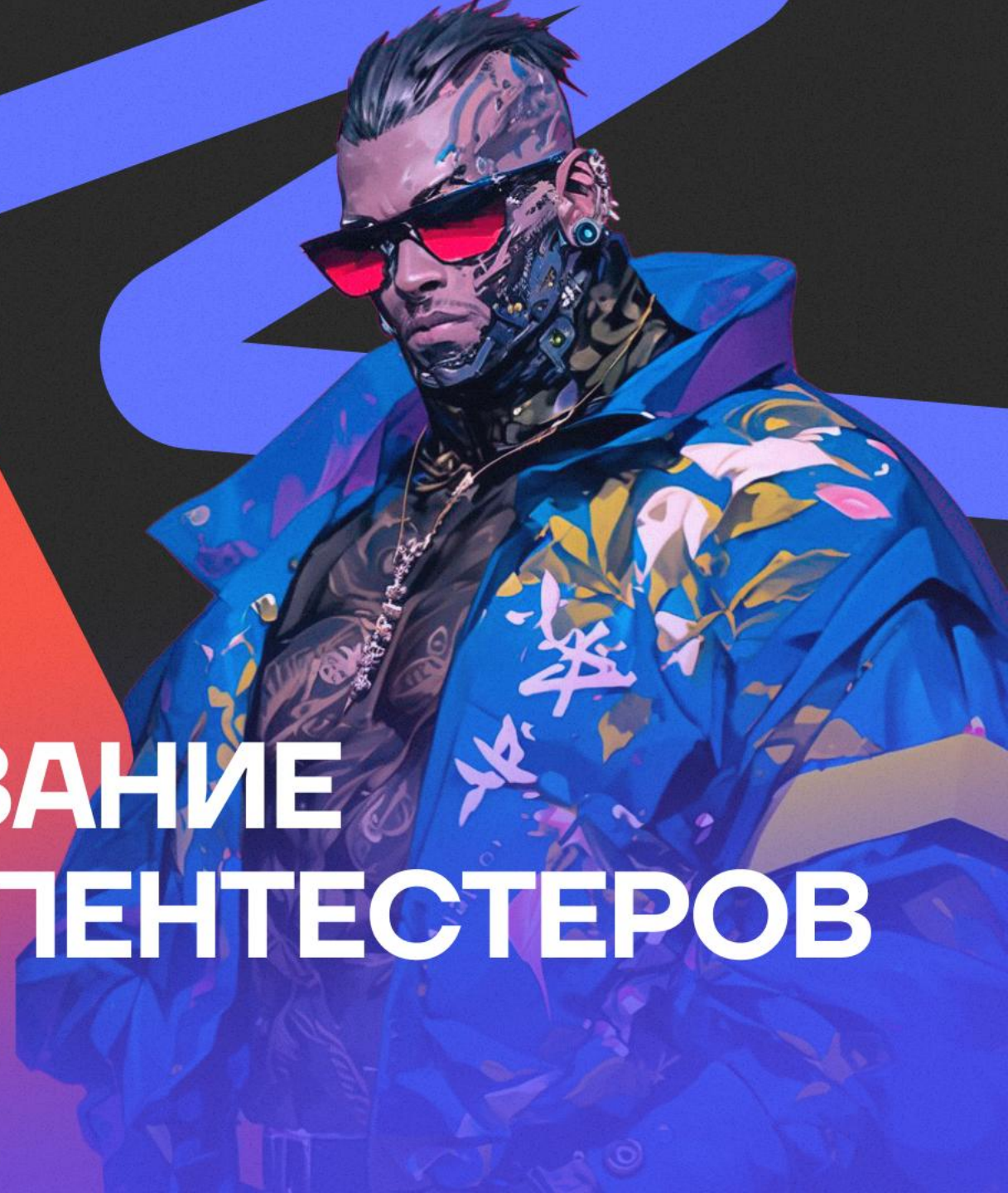
РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

- ПОНИМАНИЕ АРХИТЕКТУРЫ AD И ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ, ДЕЛЕГИРОВАНИЯ И DACL
 - ЗНАНИЕ ТИПОВЫХ ПРОБЛЕМ AD, ВЕДУЩИХ К КОМПРОМЕТАЦИИ ДОМЕНА
 - ПРАКТИКА ТЕХНИК АТАК НА KERBEROS, NTLM, DACL, ADCS И МНОГОЕ ДРУГОЕ
 - ОПЫТ ВЫСТРАИВАНИЯ ЦЕПОЧЕК АТАК И ГОРИЗОНТАЛЬНОГО ПЕРЕМЕЩЕНИЯ

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ



ПРОГРАММИРОВАНИЕ НА PYTHON ДЛЯ ПЕНТЕСТЕРОВ



ПРОГРАММИРОВАНИЕ НА PYTHON ДЛЯ ПЕНТЕСТЕРОВ

ПРАКТИЧЕСКИЙ КУРС ПО PYTHON ДЛЯ ЗАДАЧ OFFENSIVE SECURITY И АВТОМАТИЗАЦИИ ПЕНТЕСТА.

СТУДЕНТЫ УЧАТСЯ ПИСАТЬ СОБСТВЕННЫЕ ИНСТРУМЕНТЫ ДЛЯ РАБОТЫ С СЕТЯМИ, ПРОТОКОЛАМИ, АНАЛИЗОМ ТРАФИКА И АВТОМАТИЗАЦИЕЙ АТАК.



12 ЗАНЯТИЙ / 48 АК.Ч. • 70% ПРАКТИКИ, 30% ТЕОРИИ • ОНЛАЙН С ПРЕПОДАВАТЕЛЕМ + САМОСТОЯТЕЛЬНАЯ РАБОТА

[ЧТО БУДЕТ НА КУРСЕ:]

- PYTHON3 И РАБОТА С ОС
- ФАЙЛОВАЯ СИСТЕМА И ПРОЦЕССЫ
- HTTP, SSH, FTP, СОКЕТЫ
- ПАРСИНГ ВЕБ-СТРАНИЦ
- МНОГОПОТОЧНОСТЬ И МНОГОПРОЦЕССНОСТЬ
- СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ
- SCAPY И АНАЛИЗ ТРАФИКА
- REVERSE SHELL
- BRUTE FORCE И СЕТЕВЫЕ УТИЛИТЫ

[ПРАКТИКА И АРТЕФАКТЫ]

- PORT SCANNER
- HOST SCANNER
- HTML-PARSER
- REVERSE SHELL
- СЕТЕВЫЕ КЛИЕНТ-СЕРВЕРНЫЕ ПРИЛОЖЕНИЯ
- МНОГОПОТОЧНЫЕ УТИЛИТЫ
- ИНСТРУМЕНТЫ ДЛЯ РАБОТЫ С СЕТЕВЫМ СТЕКОМ

АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ



АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

ПРОДВИНУТЫЙ КУРС ПО АНАЛИЗУ ЗАЩИЩЁННОСТИ
ANDROID- И IOS-ПРИЛОЖЕНИЙ.

СТУДЕНТЫ ИЗУЧАЮТ REVERSE ENGINEERING
АРК/ИРА, ДИНАМИЧЕСКИЙ АНАЛИЗ,
ЭКСПЛУАТАЦИЮ МОБИЛЬНЫХ УЯЗВИМОСТЕЙ И
МЕТОДЫ ОБХОДА ЗАЩИТ МОБИЛЬНЫХ
ПРИЛОЖЕНИЙ.



15 ЗАНЯТИЙ / 60 АК.Ч. • ПРАКТИКА НА ANDROID И IOS • ОНЛАЙН С ПРЕПОДАВАТЕЛЕМ + САМОСТОЯТЕЛЬНАЯ РАБОТА

[ЧТО БУДЕТ НА КУРСЕ:]

- АРХИТЕКТУРА ANDROID И IOS
- РАБОТА С APK И IPA
- REVERSE ENGINEERING И PATCHING
- FRIDA И RUNTIME MANIPULATION
- SSL-PINNING BYPASS
- MOBSF И DROZER
- ДИНАМИЧЕСКИЙ АНАЛИЗ ПРИЛОЖЕНИЙ
- ТИПОВЫЕ MOBILE VULNERABILITIES
- JAILBREAK / ROOT

[ПРАКТИКА И АРТЕФАКТЫ]

- РАЗРАБАТЫВАЮТ СОБСТВЕННОЕ ANDROID-ПРИЛОЖЕНИЕ
- ПРОВОДЯТ REVERSE ENGINEERING APK/IPA
- ОБХОДЯТ SSL-PINNING И MOBILE SECURITY CONTROLS
- АНАЛИЗИРУЮТ РЕАЛЬНЫЕ MOBILE VULNERABILITIES
- ФОРМИРУЮТ ОТЧЁТ ПО АНАЛИЗУ ЗАЩИЩЁННОСТИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

При покупке одного
из курсов:

- Атаки на Active Directory
- Анализ безопасности мобильных приложений
- Программирование на Python для пентестеров

+



В подарок

**2 МИНИ-КУРСА
НА ВЫБОР В
ПОДАРОК**

из трека R301 и
курса DETA

+



Скидка

**скидка 10% за
покупку в
течение недели**



@CYBERED_RUSSIA

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ

