

// открытый вебинар • 90 минут практики

Как атакуют Active Directory

Две практические техники на учебном стенде CyberED
Портал — от разведки до пароля.

Evgeny Stroeв • Security Expert





// кто ведёт

Evgeny Stroev

Security Expert · вирусный аналитик, Exness

Pentest

Threat Modeling

AppSec

15 лет в информационной безопасности: Positive Technologies, Group-IB, Т-Банк, Альфа-Банк. Специализация — пентест и моделирование угроз.

// точка входа получена — что дальше

Вы попали во внутреннюю сеть

Неважно, как: VPN, фишинг, физический доступ. Вопрос — с чего начать.



Какие компьютеры?

Карта хостов и серверов в домене



Какие пользователи?

Учётные записи, группы, привилегии



Где слабое место?

Ошибки конфигурации и доверия

// что разберём за 90 минут

От основ до рабочей техники

01

Почему AD так важна

центральный узел управления сетью

02

Как её видит атакующий

четыре вопроса разведки

03

Реальные кейсы

BlackMatter · CISA · Microsoft

04

Enumeration: live demo

разведка на учебном стенде

05

Kerberos и AS-REP Roasting

где рождается атакуемый материал

06

Вторая практика

находим ошибку конфигурации

07

После credentials

движение и эскалация по сети

08

Курс «Атаки на AD»

36 техник · 7 модулей

// фундамент, который атакуют

Что такое Active Directory

Служба каталогов Windows — центральный узел управления сетью. Хранит объекты и связи между ними.



Users

учётные записи



Computers

хосты и серверы



Services

сервисы и SPN



Groups

права доступа



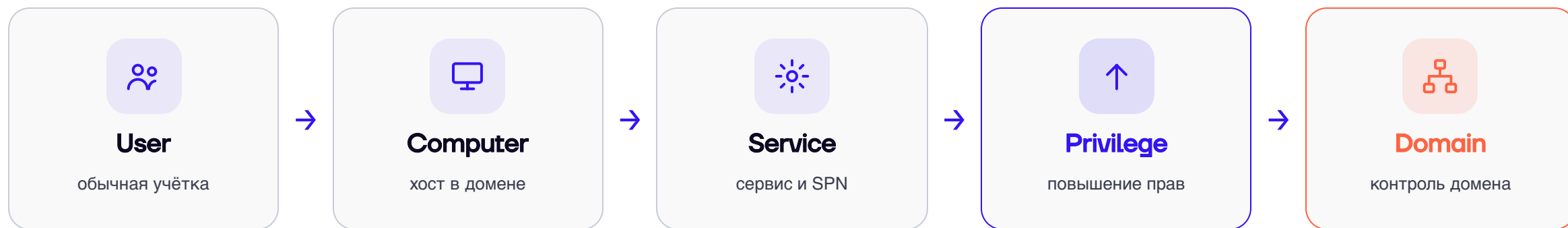
Policies

политики

// почему AD — цель №1

Одна слабость открывает путь к другим системам

AD — связанная система: доступ к одному объекту используется, чтобы продвинуться дальше.



// первый шаг атакующего — разведка

AD глазами атакующего

Четыре вопроса, с которых начинается любая атака на домен.



Кто?

Пользователи и группы



Что?

Компьютеры и серверы



Где?

Сервисы и SPN



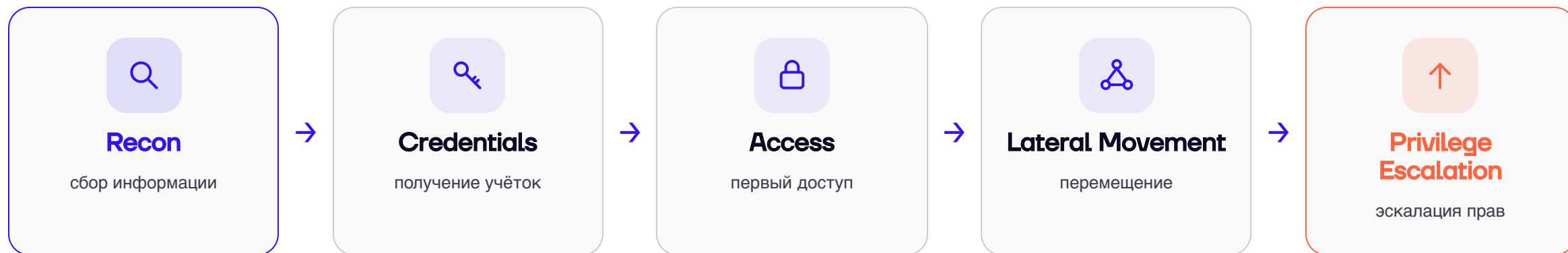
Как?

Аутентификация и доверие

// как разворачивается атака

Сначала информация. Потом доступ. Потом развитие.

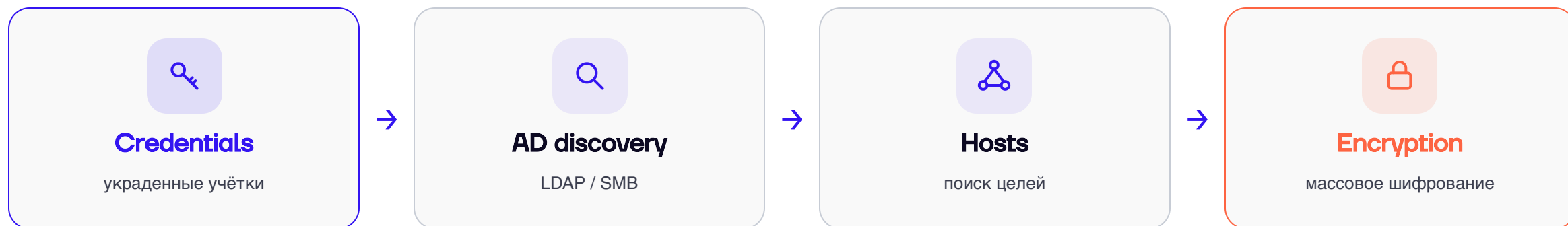
Атака — это цепочка, а не один шаг.



// так это происходит в реальности

Скомпрометированный доступ → массовое воздействие

BlackMatter использовал украденные credentials, через LDAP и SMB обращался к AD, находил хосты и удалённо шифровал системы.

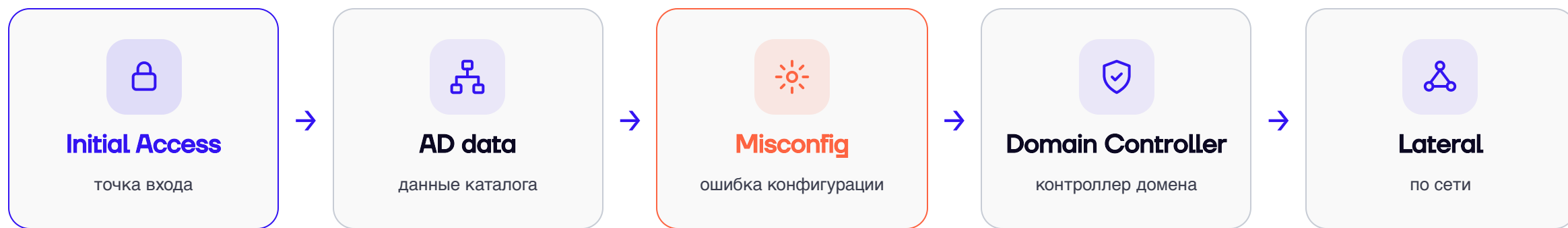


// источник • CISA • BlackMatter

// так это происходит в реальности

Одна точка входа. Потом — домен. Потом — сеть

Начальный доступ привёл к полному контролю над доменом через ошибку конфигурации сервера.

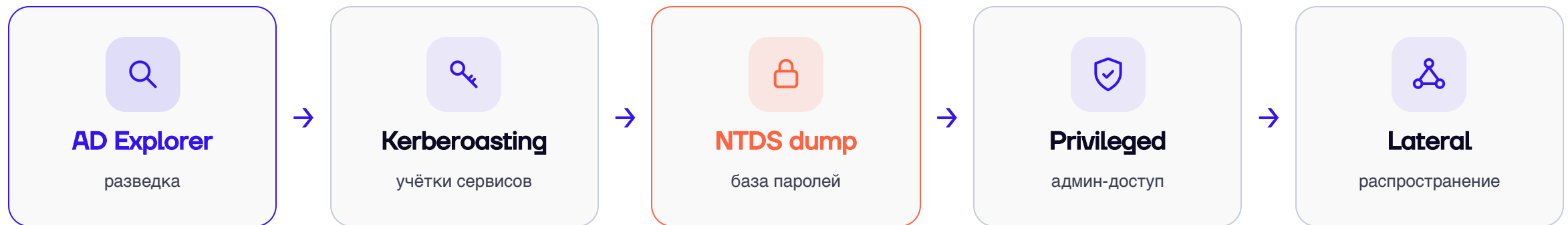


// источник • CISA Red Team

// так это происходит в реальности

Контроль над AD меняет масштаб инцидента

Microsoft: цепочка от разведки до полного контроля. Domain Admin и Group Policy использовались для развёртывания ransomware.



// источник • Microsoft IR

// практика 01 · enumeration

А теперь сделаем это сами

Учебный стенд CyberED Портал — без риска для реальных систем.

// задача перед вами

Условия практики 01



Домен

corp.local



Credentials

нет — начинаем «вслепую»



Цель

enumeration → объекты → флаг

Что вы будете искать
первым?

// live demo · CyberED Портал

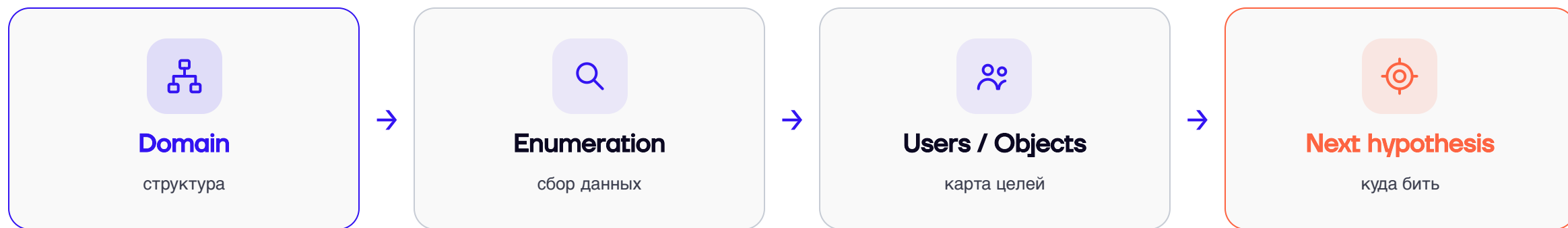
Enumeration

Сначала узнать, потом атаковать.

// разведка без единой атаки

Мы ещё ничего не «взломали». Но уже знаем, куда смотреть.

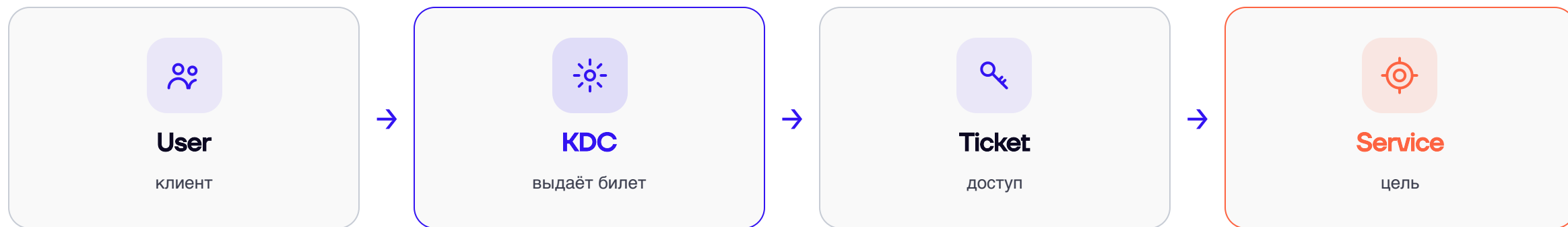
Информация — основа для следующей гипотезы.



// где рождается атакуемый материал

Kerberos за 60 секунд

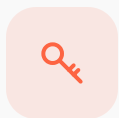
Нам не нужен весь протокол — только точка, где появляется материал для атаки.



// небольшая ошибка — большой эффект

Одна настройка учётной записи

🔒 Kerberos pre-authentication = disabled



KDC отдаёт AS-REP

без проверки



offline cracking

подбор пароля офлайн

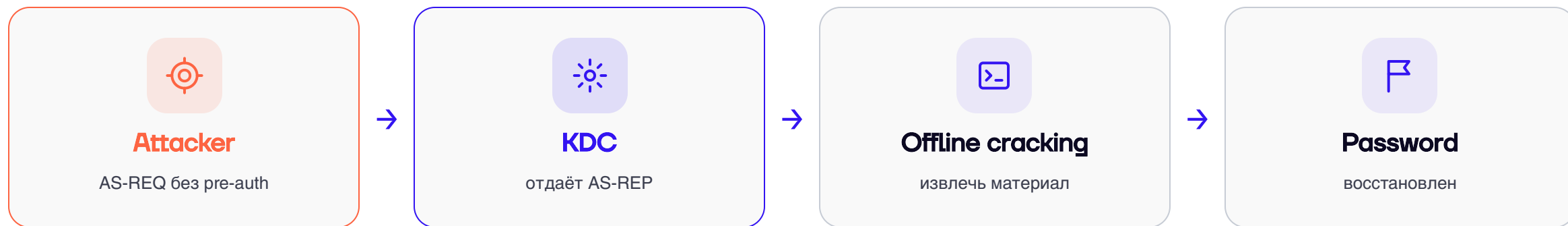


Password

восстановлен

// техника вебинара • практика 02

AS-REP Roasting



// практика 02

Найдём слабое место в настройке

домен corp.local • цель: user с disabled pre-auth

// шаг за шагом на стенде

Live Demo 02

01



Найти пользователя — с disabled pre-auth

02



Получить AS-REP — ответ KDC

03



Извлечь материал — для offline cracking

04



Восстановить пароль — перебор офлайн

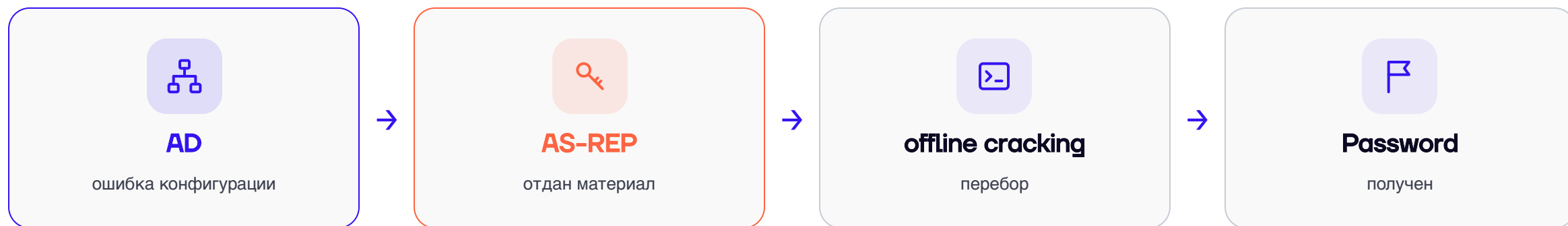
05



Получить флаг — задача решена

// материал отдала сама система

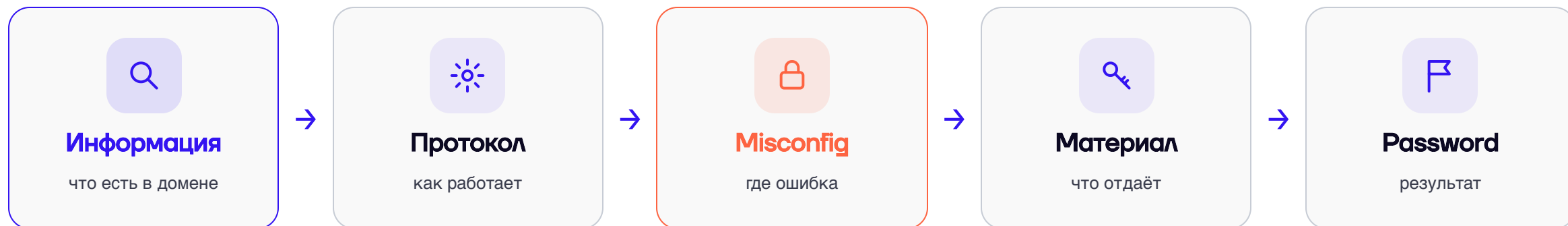
Пароль не нужно «доставать» напрямую



// это не магия, это метод

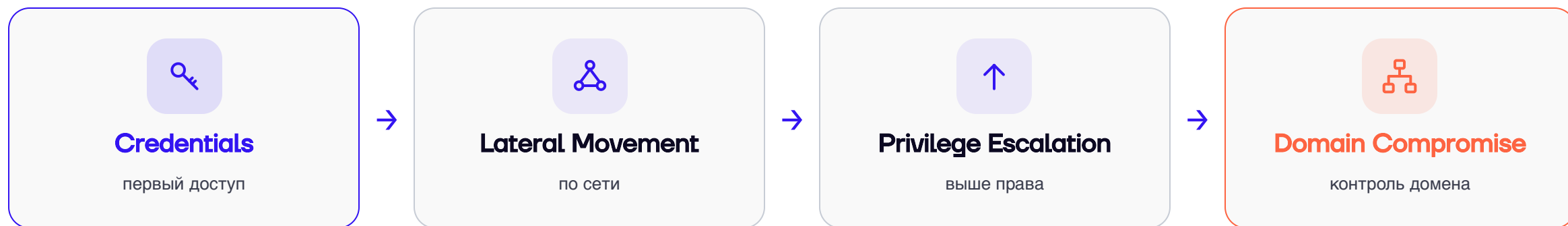
Что только что произошло

Инструменты только реализуют понятую атаку.



// первая учётка — не финиш

Credentials — ЭТО ТОЛЬКО НАЧАЛО



// две техники — только вход

Курс «Атаки на Active Directory» — 36 техник

7 модулей: от первой разведки до полного захвата AD — арсенал внутреннего пентестера.



Recon · Credentials · Kerberos

- Enumeration
- Kerberoasting · AS-REP Roasting
- NoPac · PrintNightmare



Relay · делегирование Kerberos

- Relay-атаки · NTLM Reflection
- Unconstrained · Constrained
- Resource-Based (RBCD)



ADCS · DACL · Domain

- ADCS: ESC1·4·7·8·15
- DACL: 11 техник
- DCSync · Zerologon

145 ак.ч · 36 с преподавателем + 109 практики · 9 недель · 30+ заданий · удостоверение о ПК

// навык, а не заучивание

Ты не запоминаешь технику — ты решаешь задачу

Реальные задачи в CyberED Портал, с разным уровнем сложности.

Enumeration

Easy

AS-REP Roasting

Easy

Kerberoasting

Medium

Blind Kerberoasting

Medium

Pre2k

Black Box

Timeroasting

Black Box

// от повторения к самостоятельности

Как растёт сложность



01

Есть подсказки

Пошаговое руководство



02

Есть часть данных

Самостоятельный анализ



03

Нужно найти путь

Полная самостоятельность

// что забрать с собой

Четыре вывода



01

AD — ключевая цель

одна из главных в Windows-инфраструктуре



02

Атака — с разведки

хорошая атака начинается с информации



03

Ошибка → credentials

misconfiguration превращается в доступ



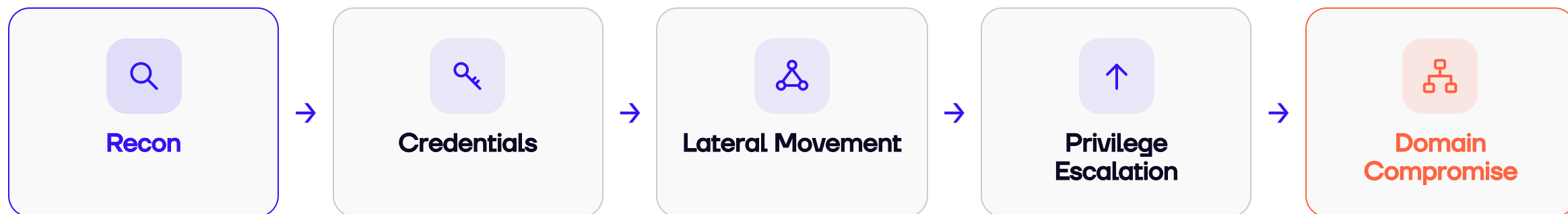
04

Учётка — начало

первый доступ запускает цепочку

// следующий шаг

Пройти всю цепочку самостоятельно



// это только начало

Сегодня — два фрагмента большой цепочки

Дальше начинается самостоятельная практика.

CyberED · cybered.ru