КОГДА КОРПОРАТИВНЫЙ WI-FI ПРОСИТ ЛОГИН?

Как Evil Twin клонирует сеть
и перехватывает учётные данные

@lionsoulbatyshchikov

ЧТО ТАКОЕ EVIL TWIN?

Evil Twin — это фальшивая точка доступа, которая имитирует легитимный Wi-Fi компании.
Тот же SSID, тот же внешний вид. Цель — заставить вас подключиться, думая, что это настоящая сеть, и перехватить ваши данные.



@lionsoulbatyshchikov

WPA2-Enterprise за 1 минуту

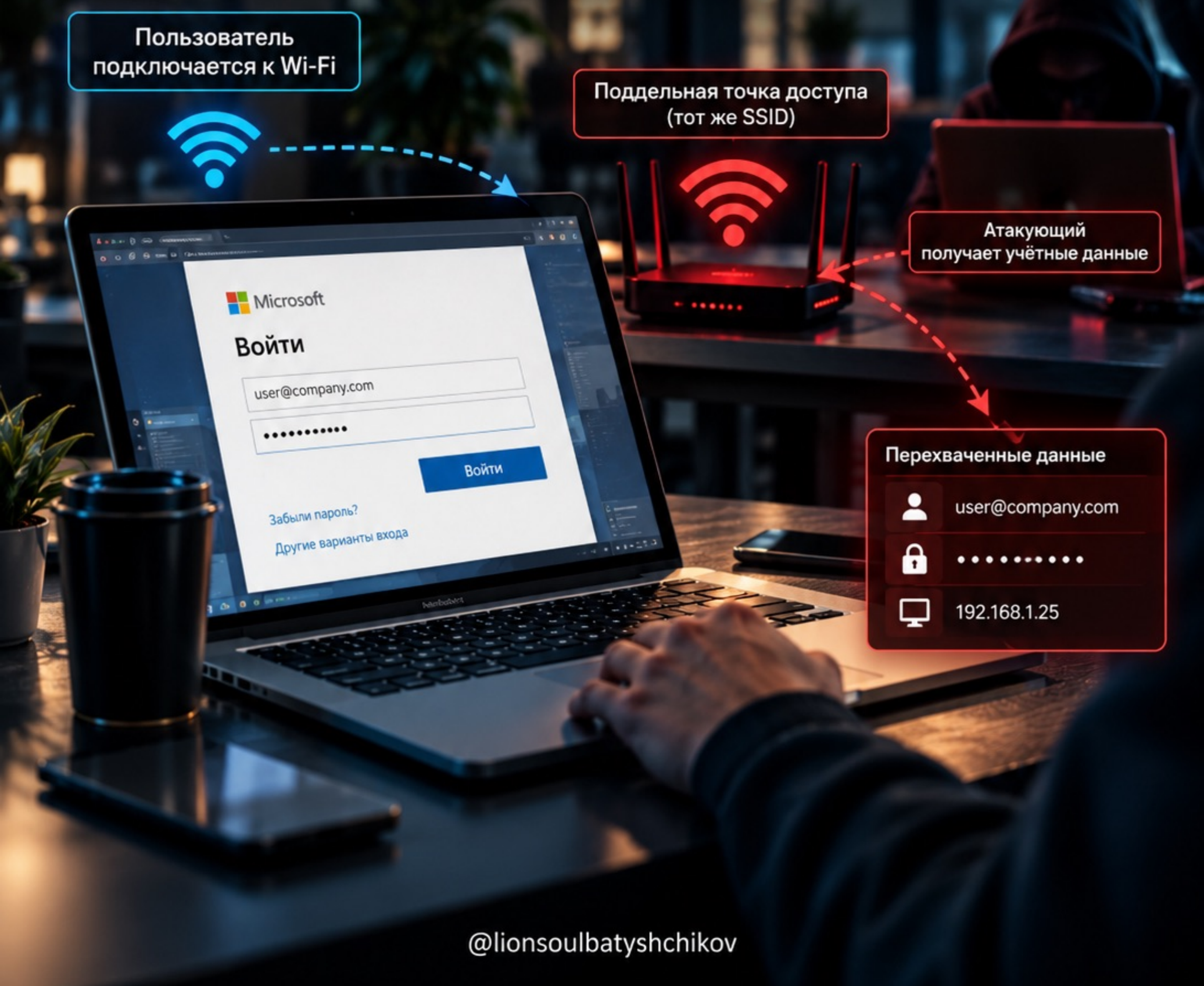
В отличие от домашнего Wi-Fi, здесь используется аутентификация на уровне пользователя через **802.1X**. Проверка учётных данных происходит на **RADIUS**-сервере — и именно его пытается скомпрометировать **Evil Twin**.



@lionsoulbatyshchikov

КАК РАБОТАЕТ АТАКА НА Wi-Fi

Злоумышленник поднимает поддельную точку доступа с тем же **SSID**, заставляет устройство подключиться и показывает фальшивый портал входа, идентичный корпоративному. Когда пользователь вводит учётные данные, они попадают в руки атакующего.



@lionsoulbatyshchikov

ЗАХВАТ HANDSHAKE

Вместо портала, Eaphammer может перехватить handshake с **RADIUS** и перевести устройство в offline-атаку. Инструменты вроде **hostapd-wpe** и **eaphammer** автоматизируют весь процесс.





@lionsoulbatyshchikov

ПОЧЕМУ ЭТА АТАКА ТАК ЭФФЕКТИВНА

Устройство подключается к уже знакомой сети, а сам процесс **полностью автоматизирован.** Пользователь видит привычный интерфейс входа — идентичный корпоративному, и не подозревает, что это поддельная точка доступа.

@lionsoulbatyshchikov

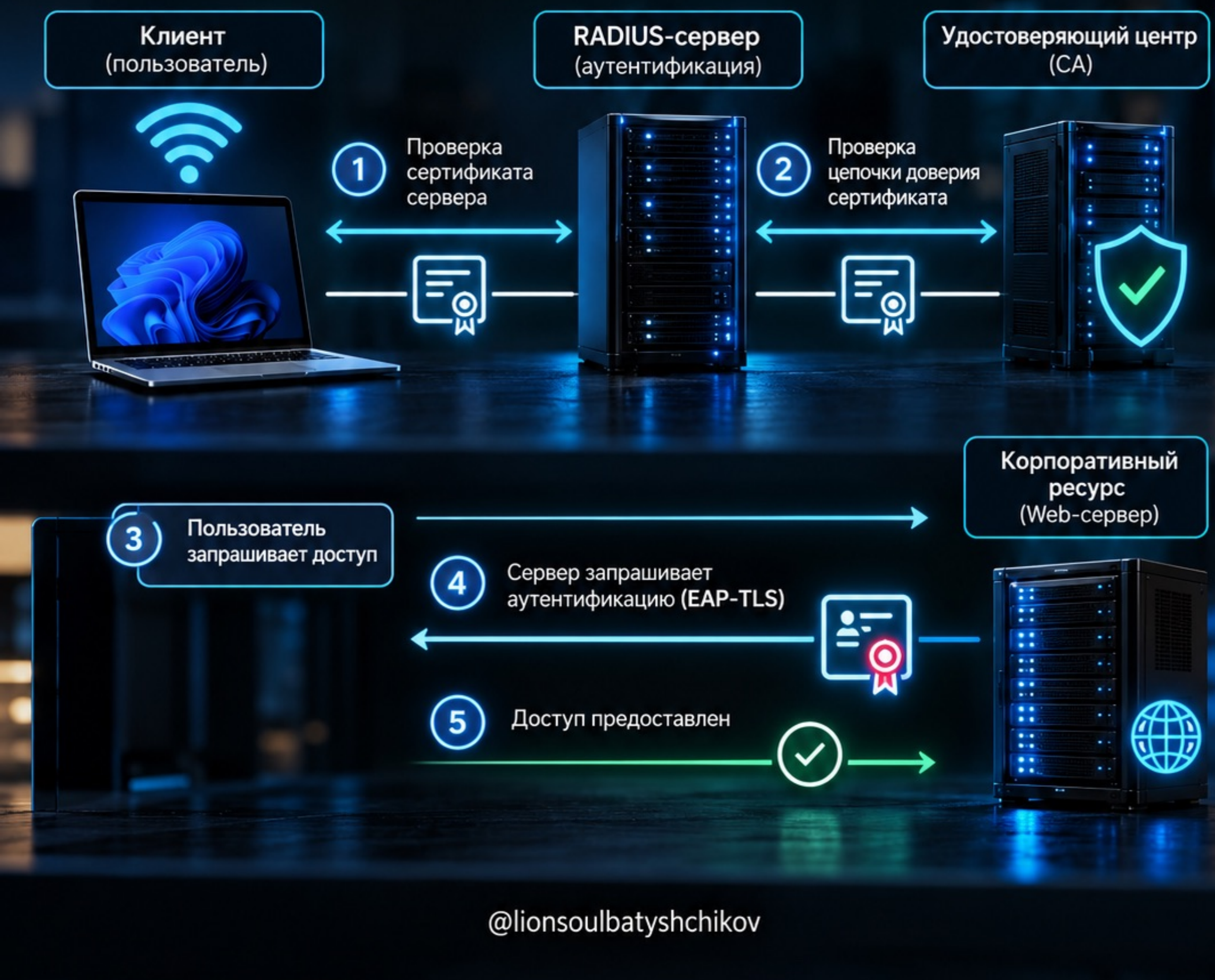
КАК ОБНАРУЖИТЬ ПОДДЕЛЬНЫЕ ТОЧКИ ДОСТУПА

Следите за AP с одинаковым **SSID** и странным **BSSID**, используйте **WIDS/WIPS**, чтобы выявлять **rogue AP**. Обучайте команду не доверять привычным сетям и проверять, откуда появляется окно авторизации.

@lionsoulbatyshchikov

КАК ЭТО ЗАЩИЩАЕТ

Клиент проверяет сертификат сервера **RADIUS** с помощью **EAP-TLS**. Используются доверенные сертификаты, и подключение происходит только к легитимной инфраструктуре. Это блокирует атаки типа **Evil Twin**.



@lionsoulbatyshchikov

ПРОВЕРЯЙТЕ ТОЛЬКО С РАЗРЕШЕНИЕМ

Evil Twin тестируйте только в своей **lab** или на **pentest** с письменным разрешением. Перехват **Wi-Fi** третьих лиц — это преступление. Для защиты, наоборот, ищите неправильно настроенный **802.1X** (как открытую дверь).



@lionsoulbatyshchikov