

---

CTRLHACK ART BEZDNA

ИТОГИ ТЕСТИРОВАНИЯ НОВОГО РЕШЕНИЯ  
СРЕДИ ЗАКАЗЧИКОВ АО «ДИЛОГНАУКА»



ПЯТАКОВ МАКСИМ  
Сооснователь CTRLHACK



СОЛОВЬЕВ ВЛАДИМИР  
Руководитель направления внедрения средств защиты  
отдела технических решений

## BAS FELIX

Симуляция кибератакующих техник.

Проверка работы СЗИ и правил детектирования в SIEM.

Выполнение атомарных техник.



## APT BEZDNA

Автоматический pentest.

Проверка выполнимости векторов атак.

Связные сценарии симуляции.

## ПЛАТФОРМА АВТОМАТИЗИРОВАННЫХ ВНУТРЕННИХ ПЕНТЕСТОВ

Реализует различные возможные сценарии проведения атак

### РОБОТ

Автоматически обрабатывает основные действия, выполняемые пентестерами в большинстве пентестов

### СЦЕНАРИИ

сценарии внутреннего пентеста включают хакерские техники, методы пентестеров, эксплуатацию уязвимостей, методы выявления ошибок в конфигурациях

**Цель** - определить выполнимость векторов атак, запрограммированных в системе, без ограничений человеческого фактора

## РЕЗУЛЬТАТ

- приоритизация уязвимостей,
- выявление слабых мест в конфигурациях,
- выявление слабых паролей,
- выявление проблем в списках доступа,
- выявление проблем в сегментации сети,
- достижение критичных целей



без агентов

автоматическое  
выполнение

техники  
Windows, Linux

повторный  
запуск теста

## ПРОСТОЙ ЗАПУСК

Три шага  
Не требуются знания  
методов пентеста или  
хакерских техник

## РЕЗУЛЬТАТ

Детальный отчет о  
каждом шаге  
выполнения теста

## ВАРИАНТЫ ТЕСТА:

- «Черный ящик»
- «Серый ящик»

## ЗАПУСК ТЕСТА

### «ЧЕРНЫЙ ЯЩИК»

Имитация ситуации в которой хакер имеет доступ к сети и не обладает дополнительными данными

- выбор начальной точки атаки
- выбор диапазона IP-адресов

### «СЕРЫЙ ЯЩИК»

Оценка риска в случае компрометации определенного пользователя

- дополнительно задаются данные пользователя



# ИНТЕРФЕЙС



## ХОД ВЫПОЛНЕНИЯ

каждый шаг выполнения теста отображается на экране и в отчете

main company@demo.demo

НОДЫ ЗАДАНИЯ БАЗА ЗНАНИЙ

Задание 949 ОБЗОР ХОД АТАКИ ХОСТЫ УЧЕТНЫЕ ЗАПИСИ АРТЕФАКТЫ ОТЧЕТ

Выполняемые атакующие действия

Уязвимости и достижения

- Получен хеш пользователя для перебора (3)
- Уязвимость CVE-2022-33679 (1)
- Получен Kerberos билет на пользователя (1)
- Успешная эксплуатация уязвимости EternalBlue (1)
- Добавлен локальный администратор на компьютер (1)

Ход атаки

ЗАГРУЗИТЬ

2024.10.15 22:40:11

Результаты (1)

1. Сбор данных для BloodHound

Действия (1)

1. Сбор данных для BloodHound

2024.10.15 22:40:32

Результаты (1)

## ЗАДАНИЯ

все тесты отображаются в одном окне

main company@demo.demo

СОСТОЯНИЕ ПЕНТЕСТЫ ДААННЫЕ ОТЧЕТЫ БАЗА ЗНАНИЙ

Пентест задания

Поиск по имени задания

НОВОЕ ЗАДАНИЕ

	Имя задания	Создание	Обновление	Действия
В работе	LT-106009 Новый пентест Демонстрация	несколько секунд назад	несколько секунд назад	
Завершен	LT-105795 CA - 11/28/2023 16:05:31	21 час назад	21 час назад	
Завершен	LT-105736 CA - 11/28/2023 15:54:32	21 час назад	21 час назад	
Завершен	LT-105637 CA - 11/27/2023 21:00:56	2 дня назад	2 дня назад	
Завершен	LT-105471 CA - 11/27/2023 18:48:33	2 дня назад	2 дня назад	
Завершен	LT-105409 CA - 11/27/2023 01:18:00	3 дня назад	3 дня назад	
Завершен	LT-105354 CA - 11/27/2023 00:47:38	3 дня назад	3 дня назад	
Завершен	LT-105296 CA - 11/27/2023 00:15:23	3 дня назад	3 дня назад	

# РЕЗУЛЬТАТ

## РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ТЕСТА представлен в виде таймлайна

- можно оценить ход развития атаки
- можно определить первичную корневую проблему, позволившую выполнить атаку

The screenshot displays the APT Bezdna interface for task 'Задание 949'. The top navigation bar includes 'НОДЫ', 'ЗАДАНИЯ', and 'БАЗА ЗНАНИЙ'. The main content area is divided into several sections:

- Выполняемые атакующие действия**: A section for active attack actions, currently empty.
- Уязвимости и достижения**: A list of vulnerabilities and achievements:
  - Получен хеш пользователя для перебора (3)
  - Уязвимость CVE-2022-33679 (1)
  - Получен Kerberos билет на пользователя (1)
  - Успешная эксплуатация уязвимости EternalBlue (1)
  - Добавлен локальный администратор на компьютер (1)
  - Найден метаданные пользователя/администратора/сервера (0)
- Ход атаки**: A timeline view showing attack progress:
  - ЗАГРУЗИТЬ**: 2024.10.15 22:40:11
  - Результаты (1)**: 1. Сбор данных для BloodHound
  - Действия (1)**: 1. Сбор данных для BloodHound
  - ЗАГРУЗИТЬ**: 2024.10.15 22:40:32
  - Результаты (1)**: (empty)

# РЕЗУЛЬТАТЫ

## ДЛЯ ВСЕХ ШАГОВ ТЕСТА :

- дано детальное описание
- приведены все полученные результаты
- даны рекомендации по устранению

Обзор действий и их описание

☰ ДАННЫЕ *i* АТАКА NoPac (CVE-2021-42278 и CVE-2021-42287)

Показать данные

Действие	Входные данные	Результаты
ET-106042 Атака NoPac (CVE-2021-42278 и CVE-2021-42287)	<b>КД уязвимый к NoPac</b> 2023.11.29 13:21:34 Контроллер Домена Имя КД dc2 Имя домена pentest_type_name.fullname contoso.LOCAL pentest_type_name.name contoso ip адрес 192.168.0.4	<b>TGS билет пользователя</b> 2023.11.29 13:21:47 Получен TGS билет /opt/saved_tgs/mssql_admin_dc1.contoso.local.ache
ET-106043 Атака NoPac (CVE-2021-42278 и CVE-2021-42287)	<b>КД уязвимый к NoPac</b> 2023.11.29 13:21:34 Контроллер Домена Имя КД dc1 Имя домена pentest_type_name.fullname contoso.LOCAL pentest_type_name.name contoso ip адрес 192.168.0.3	<b>TGS билет пользователя</b> 2023.11.29 13:21:47 Получен TGS билет /opt/saved_tgs/mssql_admin_dc1.contoso.local.ache

Обзор действий и их описание

☰ ДАННЫЕ *i* АТАКА NoPac (CVE-2021-42278 и CVE-2021-42287)

**Название:**  
Атака NoPac (CVE-2021-42278 и CVE-2021-42287)

**Краткое описание:**  
NoPac это цепочка атак из состоящая из двух уязвимостей. CVE-2021-42278 и CVE-2021-42287  
[CVE-2021-42278](#) позволяет обойти уязвимость системы безопасности, которая позволяет потенциальным злоумышленникам выдать себя за контроллер домена с помощью спуфинга учетной записи **sAMAccountName** учетной записи компьютера.  
**CVE-2021-42287**  
[CVE-2021-42287](#) уязвимость обхода безопасности, которая влияет на сертификат атрибута привилегий Kerberos (PAC) и позволяет потенциальным злоумышленникам олицетворять контроллеры домена.

**Рекомендации по снижению выявленного риска:**

- <https://support.microsoft.com/ru-ru/topic/kb5008380-обновления-проверки-подлинности-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041#~:text=Сводка потенциальным%20злоумышленникам%20олицетворять%20контроллеры%20дом ена.>
- <https://support.microsoft.com/ru-ru/topic/kb5008102-изменение-изменений-диспетчера-учетных-записей-безопасности-active-directory-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e#~:text=Сводка записи%20sAMAccountName%20учетной%20записи%20компьютера.>

# ЧТО УЖЕ ИСПОЛЬЗУЕТСЯ?

## СКАНЕРЫ УЯЗВИМОСТЕЙ

для выявления уязвимостей, которые могут использоваться в атаках

### МИНУСЫ

- выдают очень большой объем данных
- сложная приоритезация уязвимостей
- не учитывают наличие СЗИ
- не показывают возможность эксплуатации во время атаки

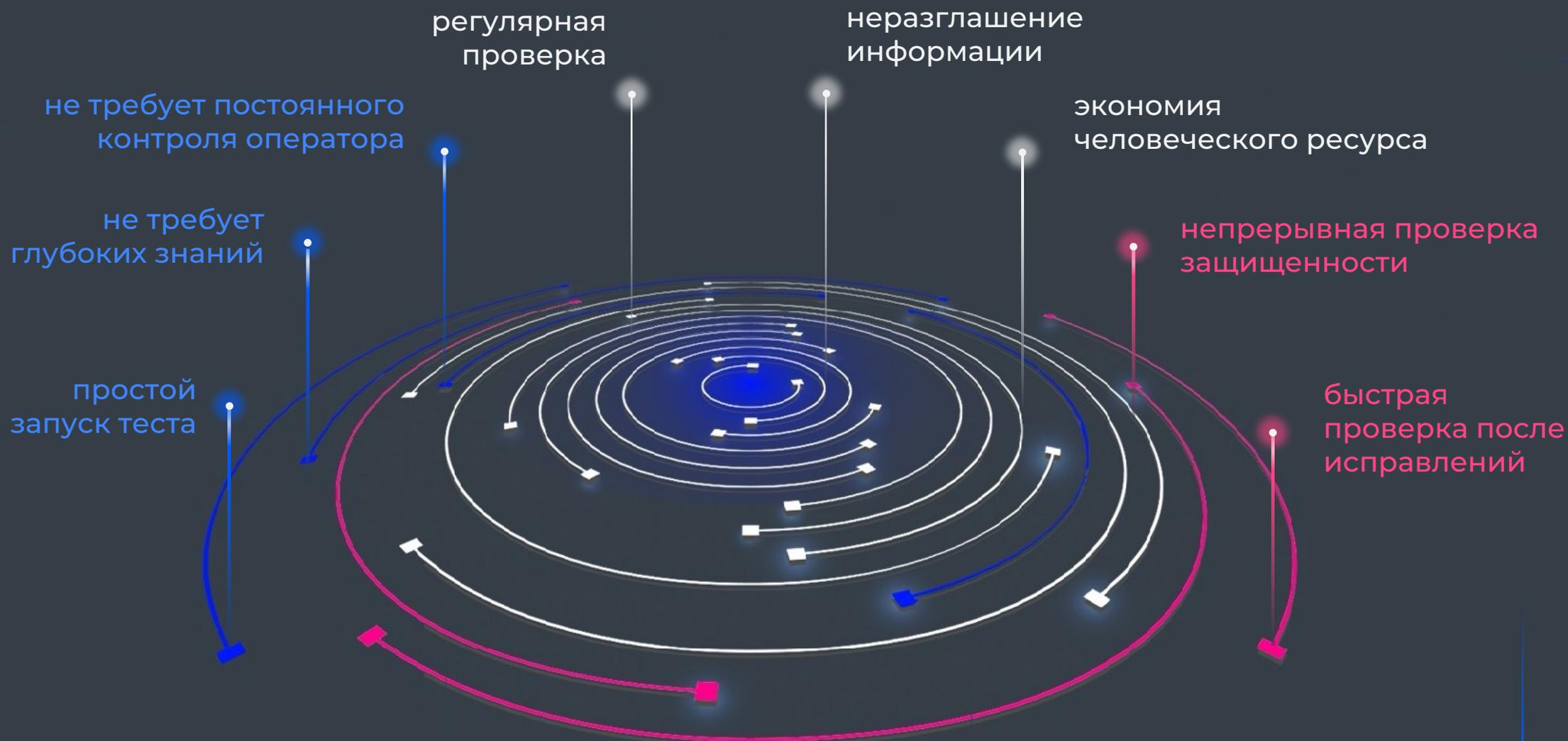
## РУЧНОЙ PENTEST

для определения возможности выполнения векторов атаки

### МИНУСЫ

- ограниченный набор техник
- только часть инфраструктуры
- зависимость от квалификации пентестеров
- длительный срок
- результат раз в полгода или год

# ПРЕИМУЩЕСТВА



## ЧТО ДАЕТ РЕЗУЛЬТАТ В ПЕНТЕСТАХ?

- Ошибки конфигурации в центре сертификации MS AD
- Слабые пароли пользователей
- Перенаправление трафика NTLM-Relay
- Ошибки конфигурации ACL в MS AD
- PrintNightmare (CVE-2021-34527)

ЕСТЬ В АРТ ВЕЗДНА



## РЕЗУЛЬТАТЫ ПИЛОТОВ

### КОНТРОЛЬ ДОМЕНА

- Права администратора домена
- Атака на центр сертификации

### МЕНЕЕ ЗНАЧИМЫЕ РЕЗУЛЬТАТЫ

- Доступ к центру сертификации
- Уязвимые машины в сети
- Слабые пароли
- Локальные администраторы в сети
- Неправильная настройка ACL в домене

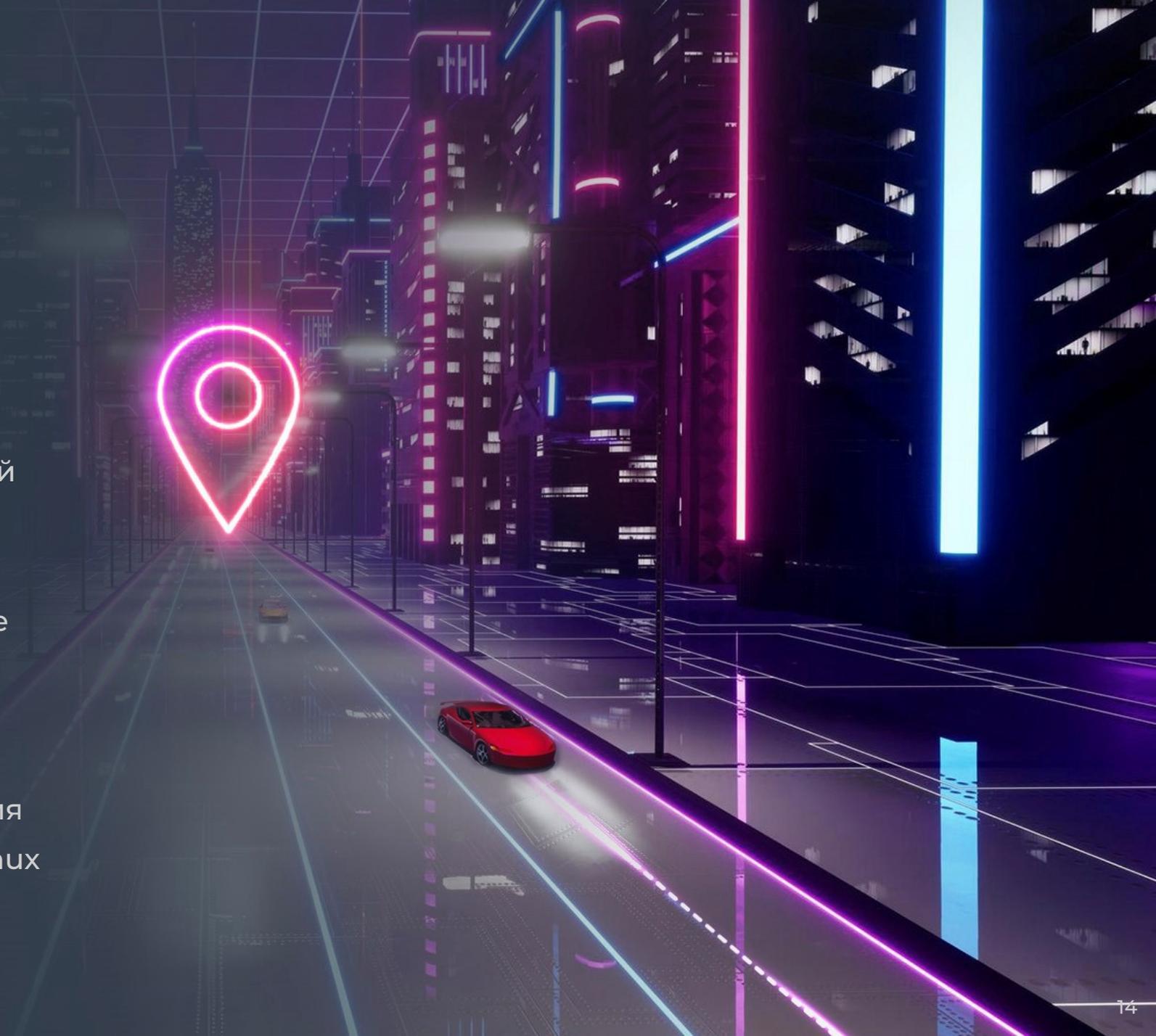
# ТЕКУЩИЙ СТАТУС И ПЛАНЫ

## СТАТУС

- готовность к проведению пилотов и внедрению
- реализовано 29 атакующих действий
- до конца 2024 г – плюс 18 действий
- в 2024 г только Windows
- до 1000 «живых» IP в одном пентесте

## ПЛАН

- в реализации 35 атакующих действия
- в 2025 г атакующие действия для Linux
- в 2025 г ежемесячные обновления



# DEMO





# СПАСИБО ЗА ВНИМАНИЕ

ООО «КОНТРОЛХАК»

+7 (495) 789 72 97

[info@ctrlhack.ru](mailto:info@ctrlhack.ru)

[www.ctrlhack.ru](http://www.ctrlhack.ru)

