Awillix

Защита от уязвимостей ВКС–Инфраструктуры

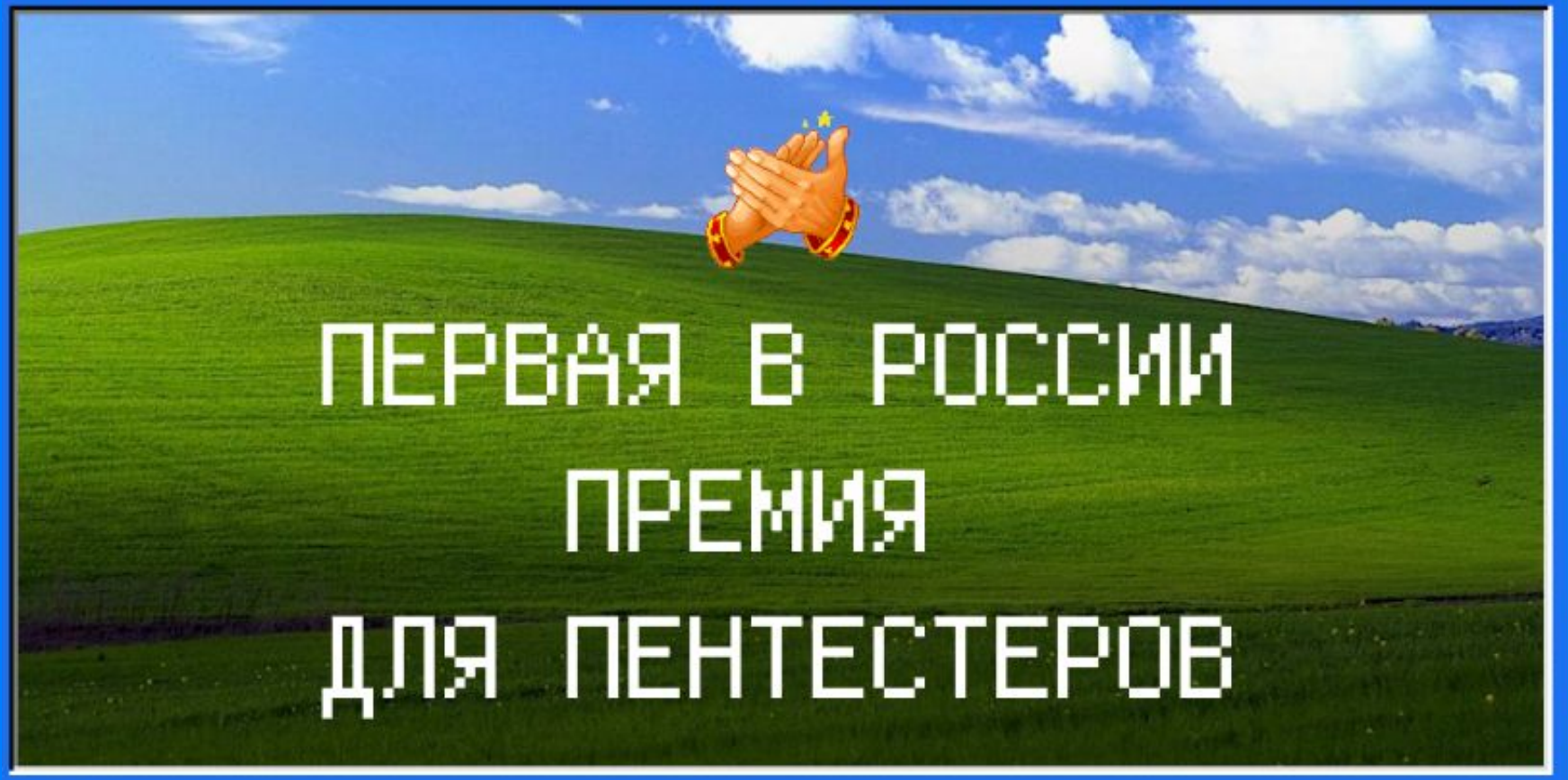
Александр Герасимов

Белый хакер, сооснователь Awillix

Awillix

Одна из лучших offensive-компаний на рынке кибербезопасности.

Главная экспертиза — имитация хакерских атак: тесты на проникновения, анализ защищенности, Red Team-проекты повышенной сложности. У нас есть свой продукт для регулярного мониторинга уязвимостей и собственный киберполигон.


ПЕРВАЯ В РОССИИ
ПРЕМИЯ
ДЛЯ ПЕНТЕСТЕРОВ


Павел Топорков (Paul Aw)
Илья Карпов
Егор Богомолов
Роман Шемякин
Михаил Сидорук
Николай Хечумов
Роман Панин

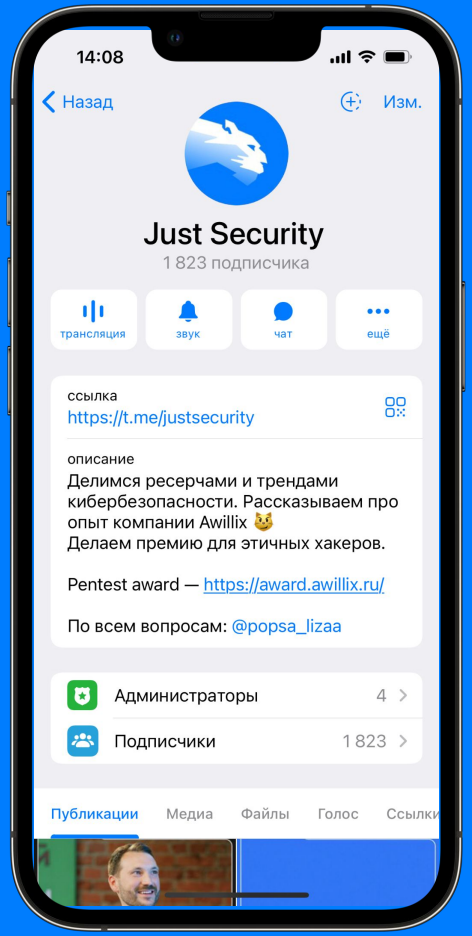

PENTEST
AWARD


Награждение
победителей номинации
«**ck the logic»

Awillix

ЛУЧШИЙ КОНТЕНТ ПРО БЕЗОПАСНОСТЬ БИЗНЕСА

t.me/justsecuriity



ЗАЧЕМ ЗАЩИЩАТЬ ВКС?

В определенных случаях возможны реализации следующих рисков:

- перехват информации (атаки «человек посередине»);
- несанкционированное подключение к конференции;
- компрометация всего внутреннего сегмента сети;
- утечка чувствительной информации;
- отказ в обслуживании.

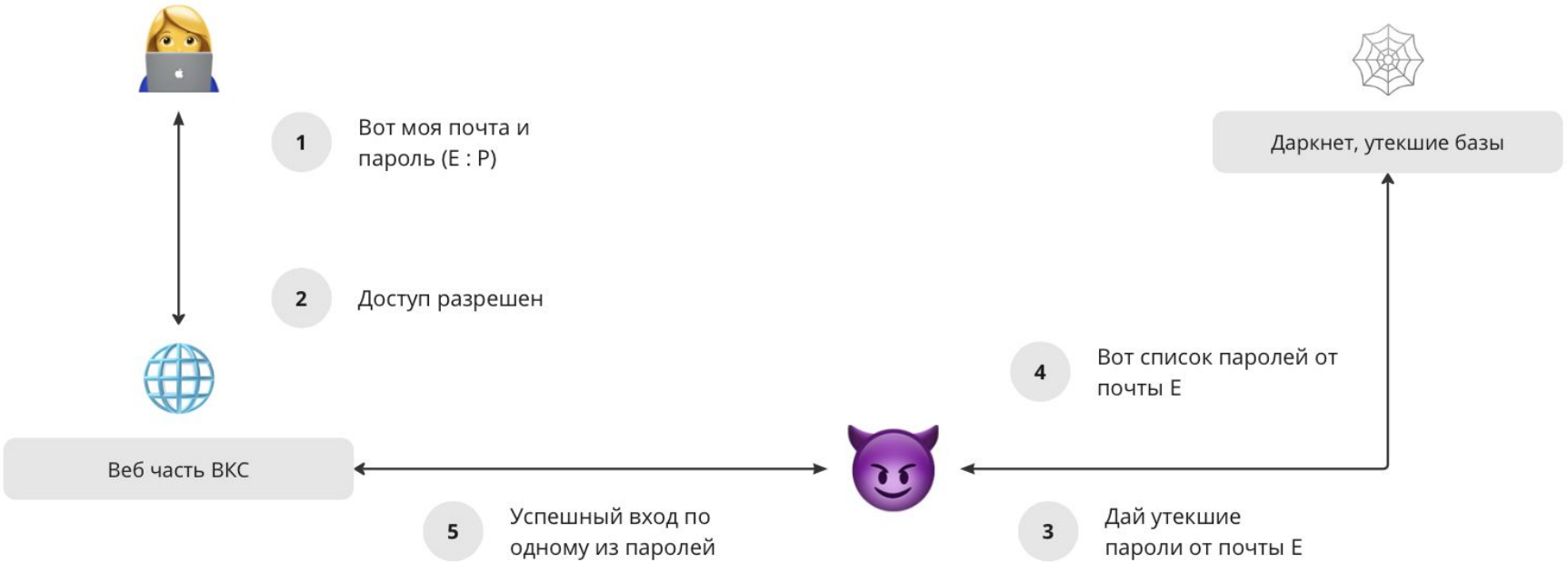
С ЧЕМ СВЯЗАНЫ ВОЗМОЖНЫЕ РИСКИ?

ТЕХНОЛОГИЧЕСКИЕ НЕДОСТАТКИ В ПО

Отсутствие сквозного шифрования

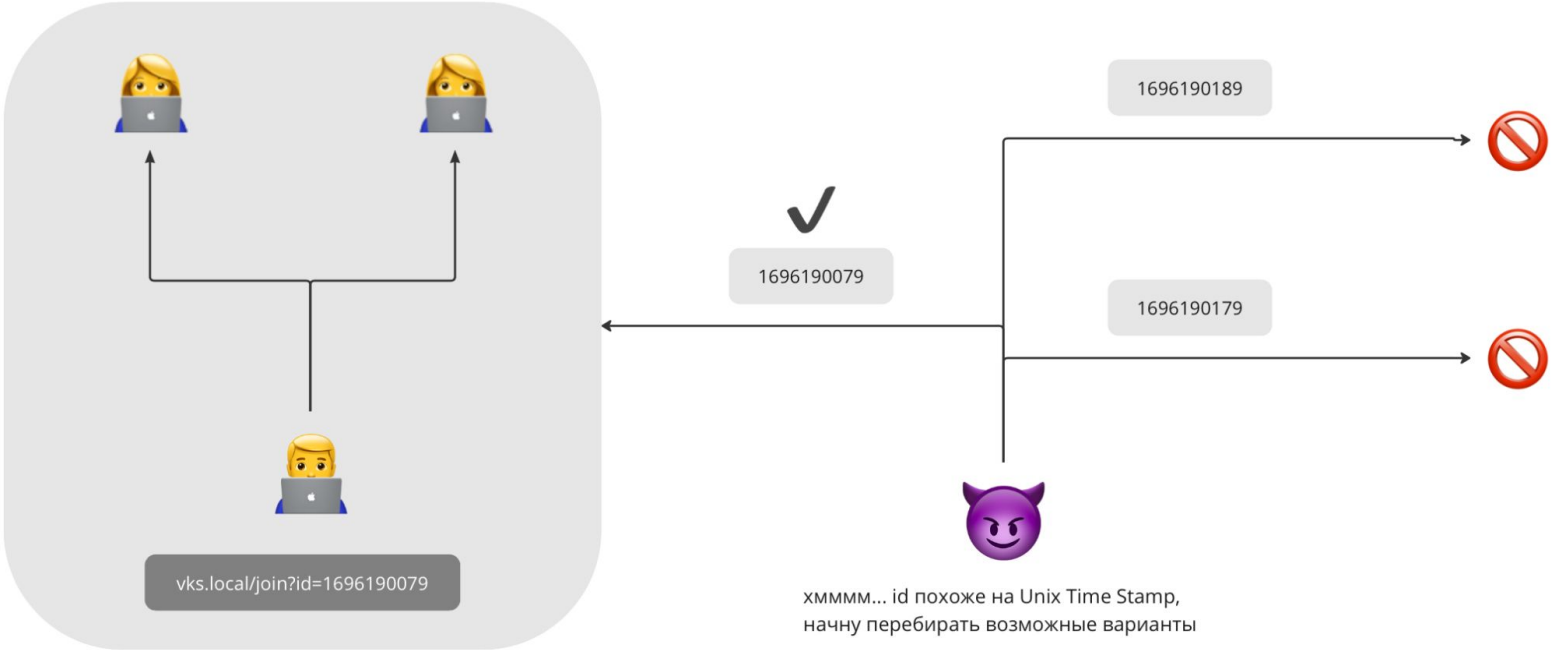
Awillix

ТЕХНОЛОГИЧЕСКИЕ НЕДОСТАТКИ В ПО



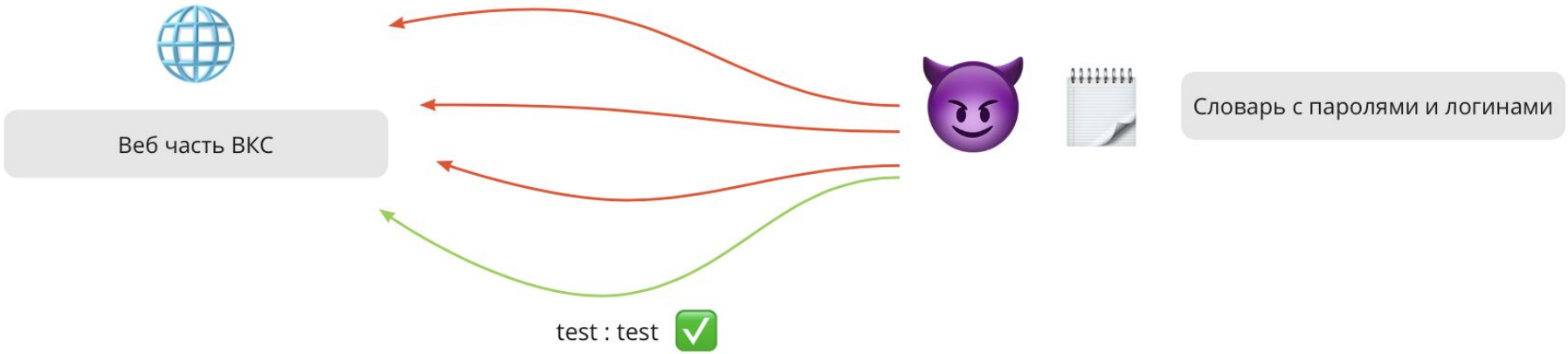
Отсутствие многофакторной аутентификации

ТЕХНОЛОГИЧЕСКИЕ НЕДОСТАТКИ В ПО



Слабая энтропия уникальной ссылки для подключения к ВКС

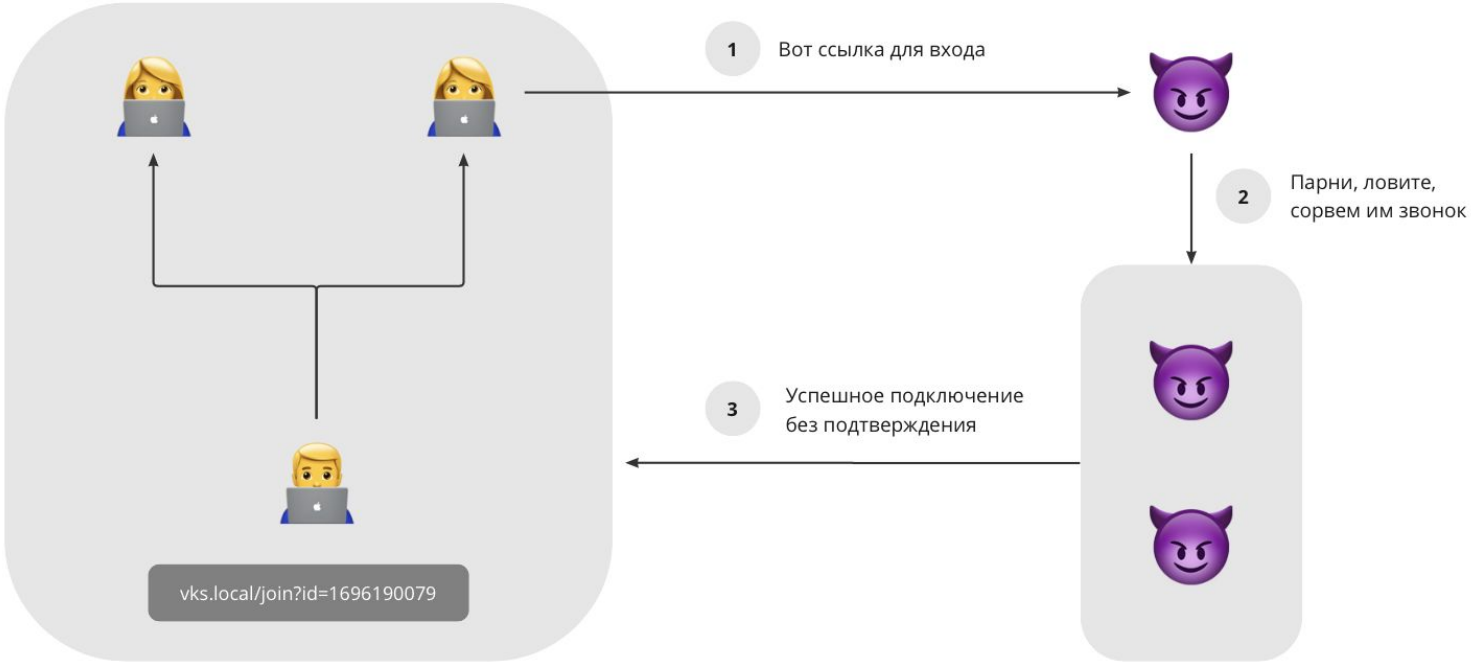
ТЕХНОЛОГИЧЕСКИЕ НЕДОСТАТКИ В ПО



Возможность перебора аутентификационных данных

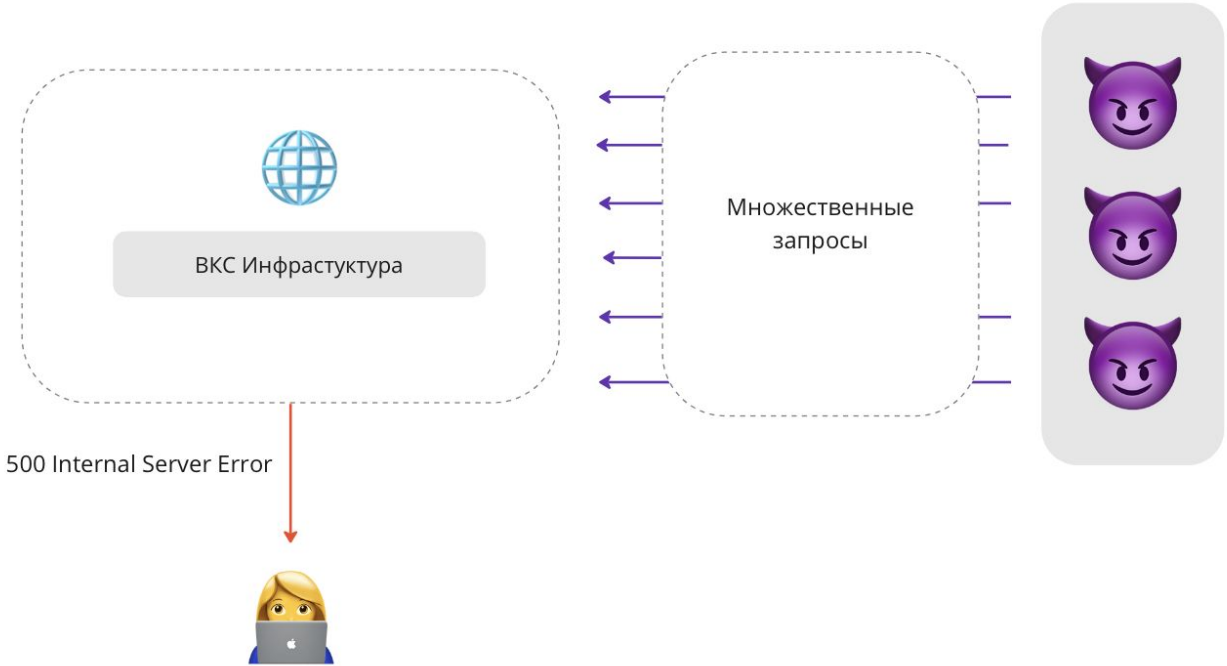
Awillix

ТЕХНОЛОГИЧЕСКИЕ НЕДОСТАТКИ В ПО



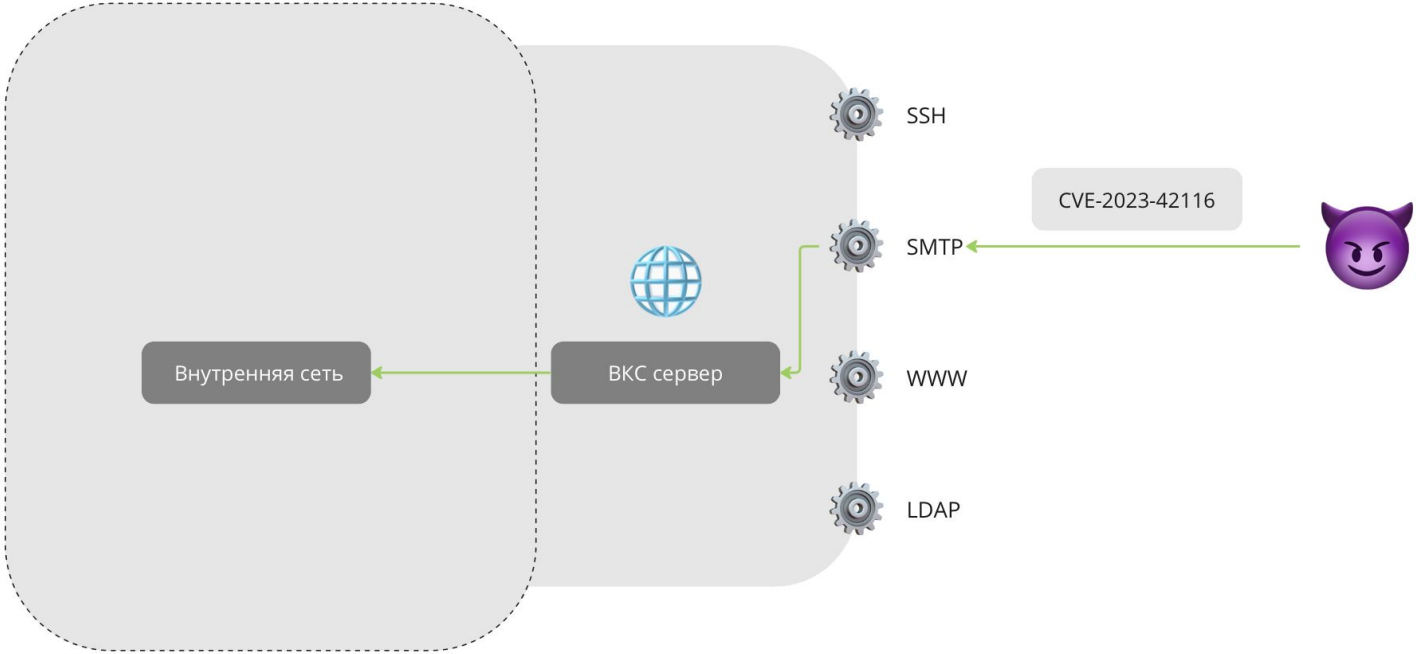
Отсутствие подтверждения входа в конференцию от организатора

НЕДОСТАТКИ КОНФИГУРАЦИИ ВКС-СЕРВЕРА



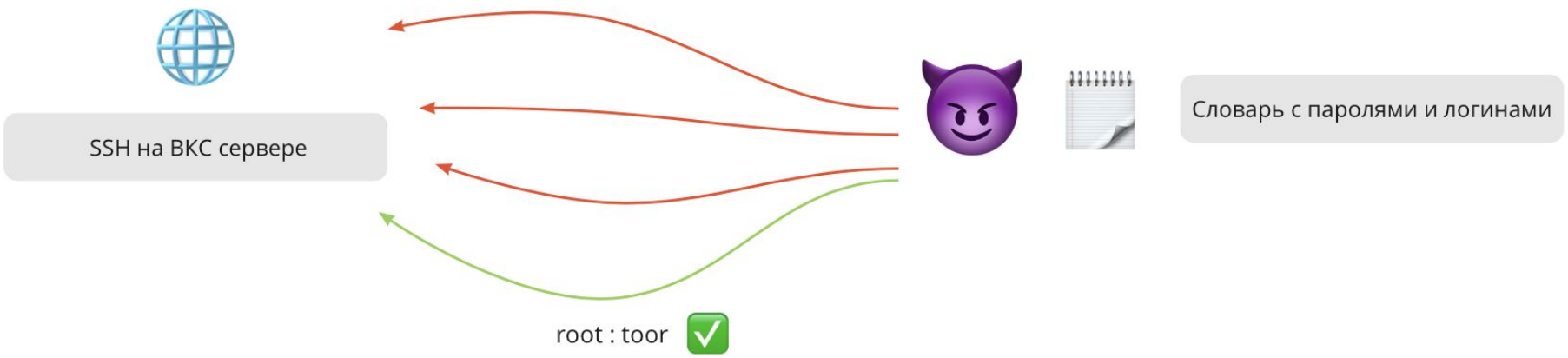
Отсутствие защиты от DDoS атак

НЕДОСТАТКИ КОНФИГУРАЦИИ ВКС-СЕРВЕРА



Недостаточная фильтрация трафика к внутренним сервисам STUN сервера(SSH и т.д.)

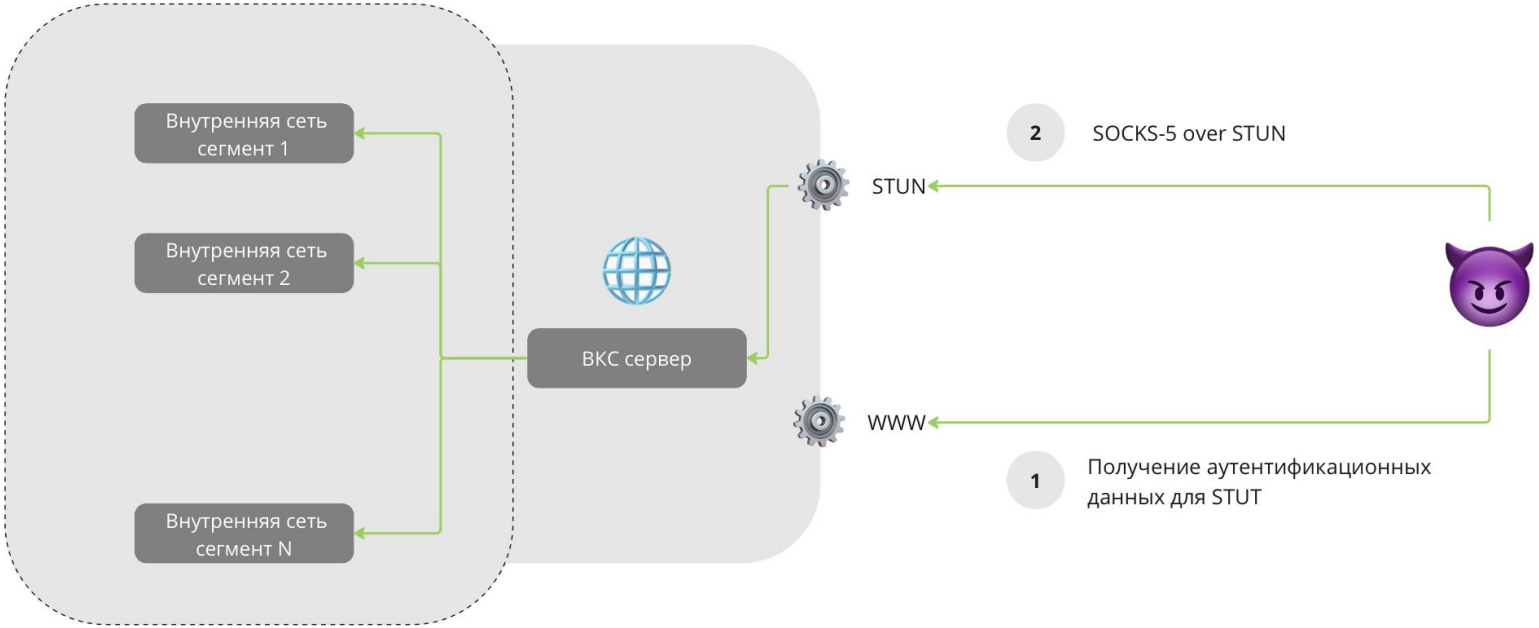
НЕДОСТАТКИ КОНФИГУРАЦИИ ВКС-СЕРВЕРА



Использование стандартных или словарных учетных данных для подключения к STUN серверу.

Awillix

НЕДОСТАТКИ КОНФИГУРАЦИИ ВКС-СЕРВЕРА



Недостаточная фильтрация трафика от STUN сервера из DMZ во внутренний сегмент

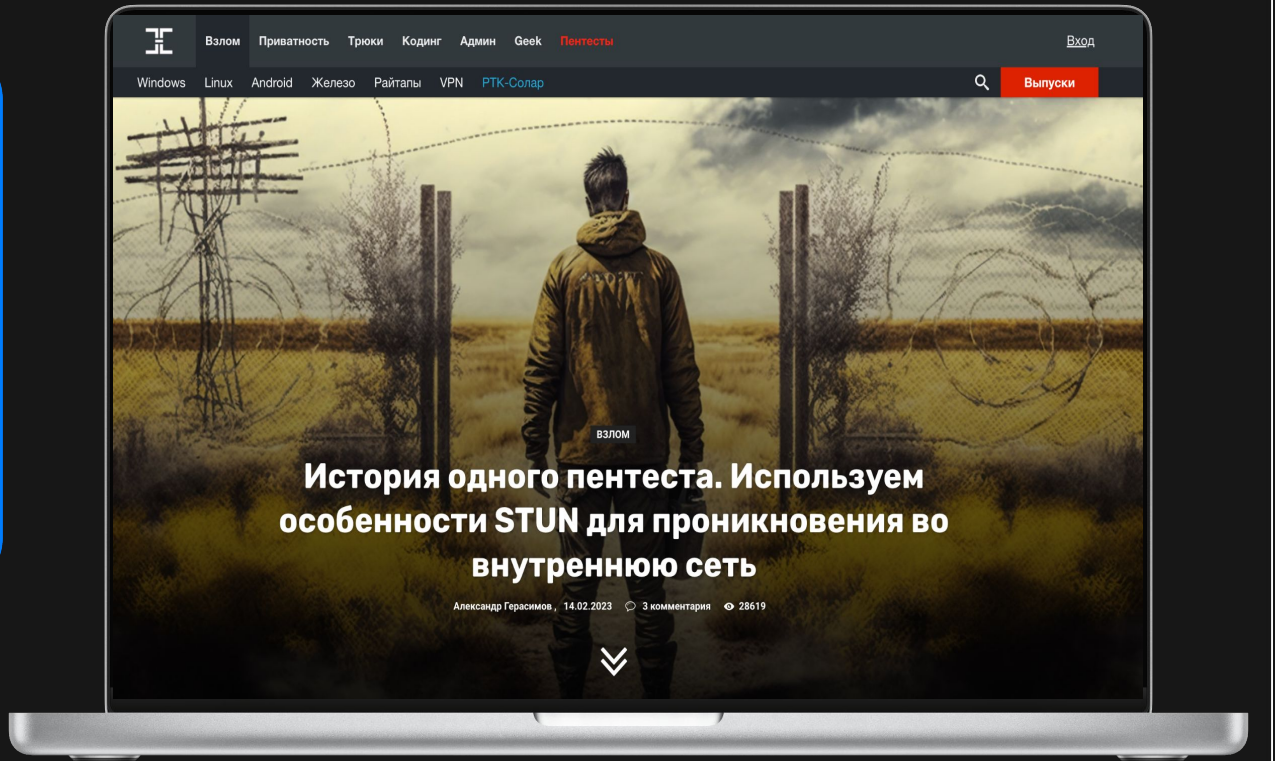
Awillix

НАСКОЛЬКО РЕАЛЬНА РЕАЛИЗАЦИЯ АТАКИ НА ВКС?

Awillix

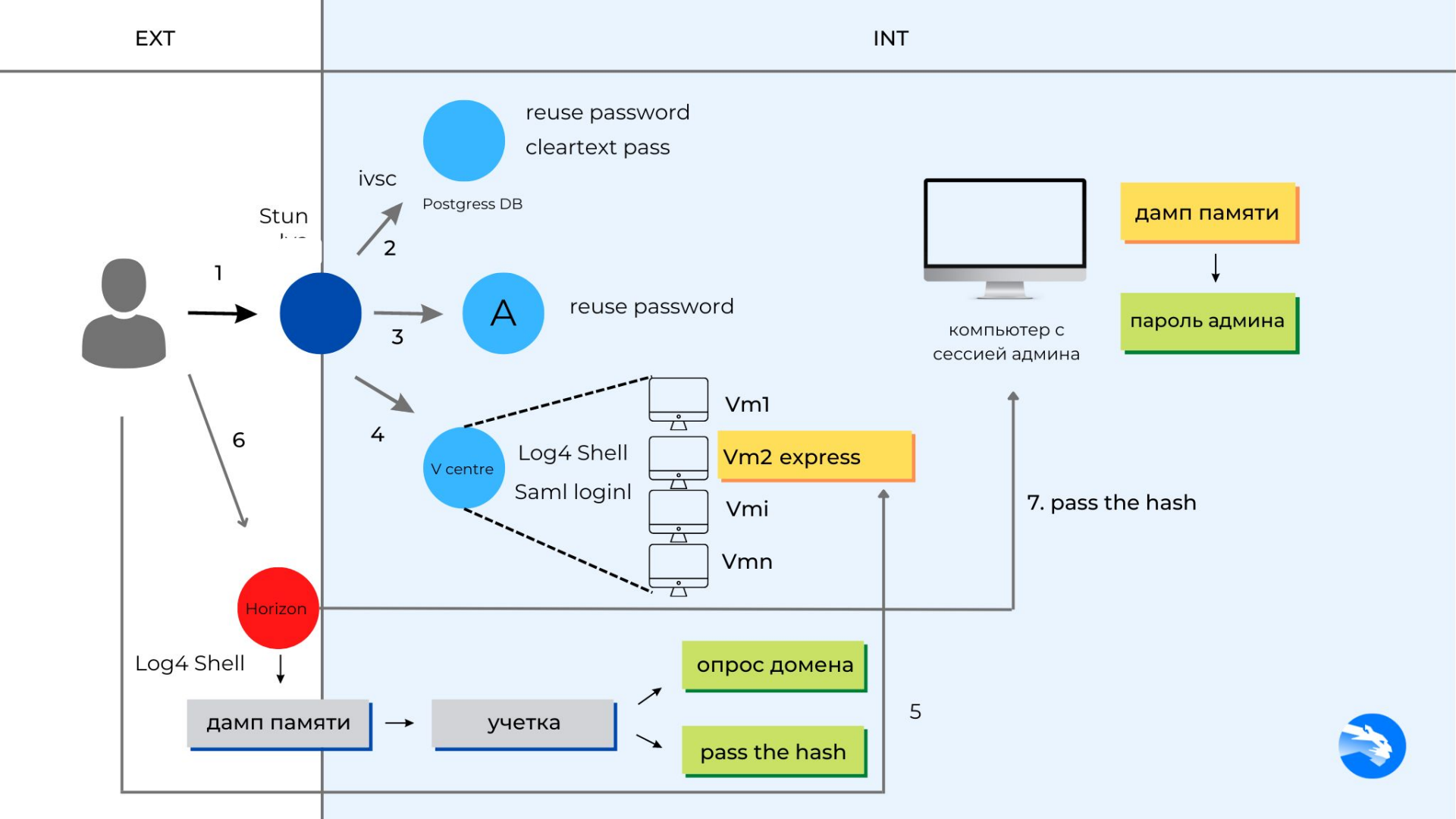
ПРИМЕР РЕАЛЬНОГО ПРОЕКТА

https://xakep.ru/2023/02/14/stun-pentesting/



ПРИМЕР РЕАЛЬНОГО ПРОЕКТА

- Обнаружение веб-части ВКС;
- Подбор ID-комнат, не требующих аутентификации;
- Анализ трафика при подключении к комнате: получение информации об IP-адресации, аутентификационные данные к STUN;
- Построение SOCKS-5 туннеля через STUN для доступа к внутренней сети.


EXT
INT
reuse password
cleartext pass
ivsc
Postgress DB
Stun
1
2
3
A
reuse password
компьютер с
сессией админа
дамп памяти
пароль админа
4
V centre
Log4 Shell
Saml loginl
Vm1
Vm2 express
Vmi
Vmn
6
7. pass the hash
Horizon
Log4 Shell
дамп памяти
учетка
опрос домена
pass the hash
5

НЕСКОЛЬКО ИЗВЕСТНЫХ СЛУЧАЕВ

- Zoombombing – вторжения посторонних в видеоконференции с целью их срыва (особенно популярно в ~2020 году):
- DDoS атаки на ВКС инфраструктуры, расположенные в РФ;
- Критические уязвимости в клиентской части (например, CVE-2023-39216*)

* Improper input validation in Zoom Desktop Client for Windows before version 5.14.7 may allow an unauthenticated user to enable an **escalation of privilege via network access.**

Awillix

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ВКС

1

НА УРОВНЕ ПО

- Ограничьте доступ к встречам при помощи паролей и обязательной аутентификации;
- Используйте функцию "зал ожидания";
- Ограничьте возможность гостей (показ экрана, запись звонка …);
- Используйте двухфакторную аутентификацию;
- Используйте стойкие пароли для своей учетной записи.

2

НА УРОВНЕ СЕРВЕРА

- Ограничьте доступ к внутренним сервисам STUN сервера;
- Убедитесь, что трафик от STUN сервера во внутреннюю сеть ограничен нужными подсетями;
- Используйте Proxy/Балансировщики нагрузки перед веб-частью ВКС, доступной из сети интернет (в случае self-hosted);
- Ограничьте доступ к серверам ВКС по GeoIP правилам;
- Своевременно обновляйте ПО.

БОНУС ДЛЯ УЧАСТНИКОВ КОНФЕРЕНЦИИ

Автоматизированное сканирование внешней инфраструктуры

awillix.ru

Ручная верификация найденных уязвимостей

КОНТАКТЫ

Александр Герасимов

CISO и сооснователь Awillix

Telegram: @gerasimov_a_n

Почта: info@awillix.ru

Awillix

ЛУЧШИЙ КОНТЕНТ ПРО БЕЗОПАСНОСТЬ БИЗНЕСА

t.me/justsecuriity