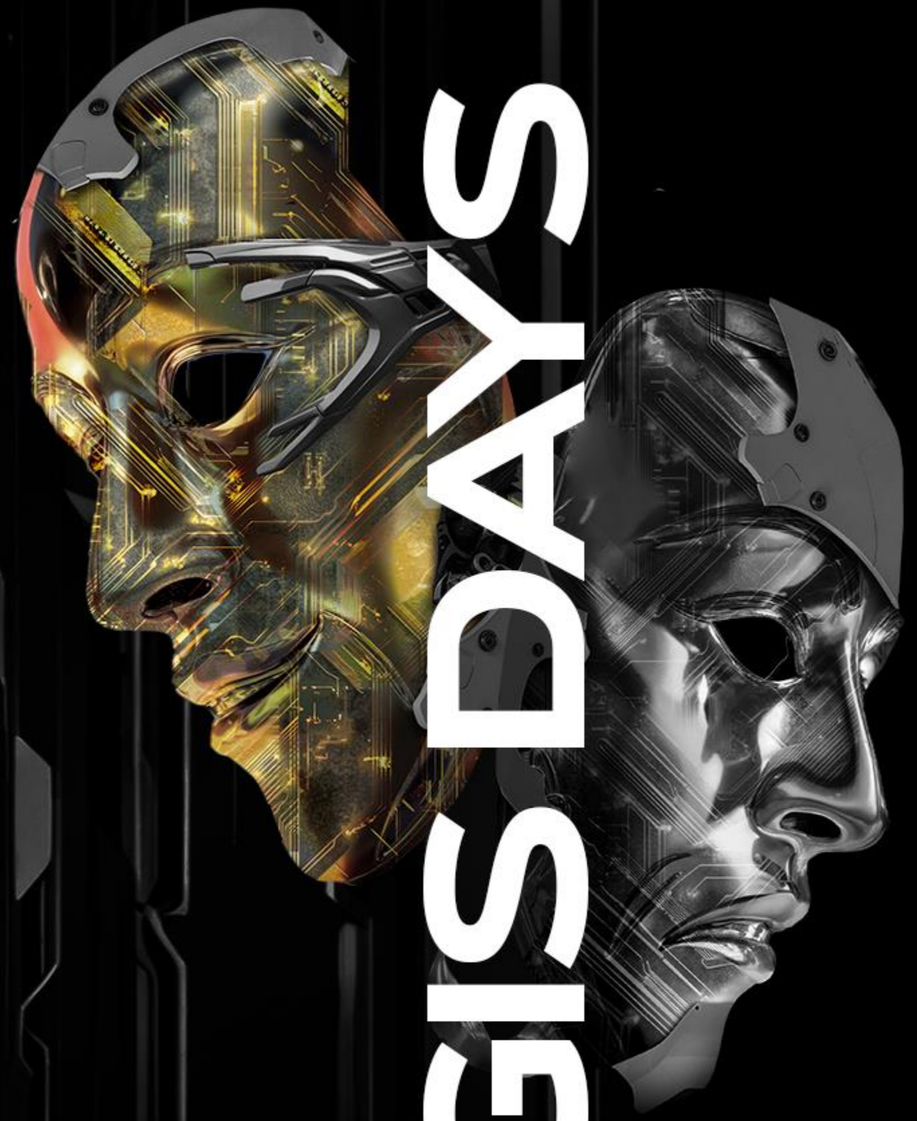
GIS DAYS

УЦСБ

Пентест не для галочки



GIS DAYS

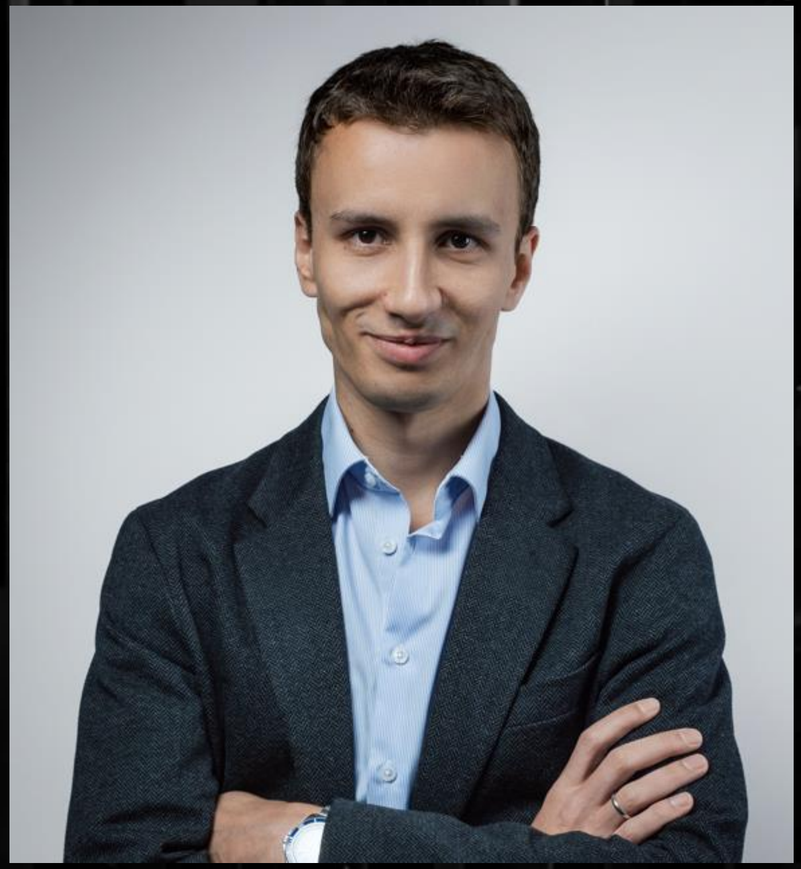
Дмитрий Зубарев
Заместитель директора аналитического центра УЦСБ

GLOBAL INFORMATION SECURITY DAYS*

*Дни глобальной информационной безопасности

О себе

- Заместитель директора аналитического центра УЦСБ
- Занимаюсь ИБ более 8 лет
- OSEP, CVE



УЦСБ

GISDAYS

Содержание

На что обратить внимание при выборе исполнителя и во время работ? Как обеспечить нужный результат?

УЦСБ

GISDAYS

Вступление

- Пентесты проводятся для решения задач бизнеса, но не всегда этому способствуют
- Основные механизмы контроля — грамотное ТЗ и общение с исполнителем
- Разные исполнители могут понимать под пентестом разные мероприятия

Сканеры и ручная работа

УЦСБ

GISDAYS

Почему запуска сканеров может быть недостаточно

- Под пентестом может пониматься запуск сканеров
- Сканирование не предполагает эксплуатацию уязвимостей
- Результат сканирования — сухой перечень уязвимостей и рекомендации по устранению
- Перечень не даёт понимания о пригодности к эксплуатации и реальном влиянии на ИБ

Сканеры и ручная работа

УЦСБ

GISDAYS

Почему запуска сканеров может быть недостаточно

- Перечень не даёт понимания о пригодности к эксплуатации и реальном влиянии на ИБ
- Выявленные сканером уязвимости — это лишь «верхний слой»
- Существуют уязвимости, которые можно выявить, только проэксплуатировав другие
  - Пример: локальные уязвимости повышения привилегий, побег из контейнера
- Сканер не выстраивает уязвимости в цепочки

Сканеры и ручная работа

УЦСБ

GIS DAYS

Как обезопасить себя от такого подхода?

Примеры формулировок для ТЗ:

- В ходе работ должна осуществляться эксплуатация выявленных критичных уязвимостей
- В случае успешной атаки исполнитель должен рассматривать возможность её развития с целью получения доступа к критичным данным или системам
- Отчёт о проведении работ должен содержать материалы, демонстрирующие эксплуатацию выявленных критичных уязвимостей
- Отчёт о проведении работ должен содержать описание реализованных векторов атак

Сканеры и ручная работа

УЦСБ

GISDAYS

Почему атака не развивалась вглубь?

- Приемлемый ответ: необходимости не было, команда фокусировалась на других векторах — если в отчёте действительно описаны другие векторы

- Приемлемый ответ: уязвимый сервер не относится к критичным, не включён в домен, служит для выполнения некритичных задач, перспектива развития отсутствовала — если это действительно так

- Неприемлемо: исполнитель не развивал атаки, которые имели очевидные перспективы

Критерии успешности пентеста

УЦСБ

GISDAYS

Домен взят — работы завершены

- Позиция исполнителя: компрометация инфраструктуры показана, значит, цель работ достигнута
- Реальная цель бизнеса зачастую — узнать, как его можно взломать и как от этого защититься
- Возможны разные векторы, поэтому требуется работа «в ширину», по нескольким векторам

Критерии успешности пентеста

УЦСБ

GISDAYS

Адекватная полнота проверки

- Пентест — эффективный и незаменимый инструмент, но не даёт гарантий
- В каждом проекте возможна адекватная полнота проверки
- Адекватная полнота достигается за счёт опыта исполнителей и чек-листов

Критерии успешности пентеста

УЦСБ

GISDAYS

Как достичь «адекватной полноты»?

- Формулировка для ТЗ: работы продолжаются до исчерпания исполнителем возможностей проведения атак
  - Контроль выполнения этого требования — без фанатизма, просто просим пояснять, что рассматривали и почему что-то не получилось

- Поинтересоваться на предварительной встрече, какие векторы рассматриваются и продолжаются ли работы после успешной реализации одного из них

- Команда с серьёзным подходом останавливается только из-за исчерпания возможностей или времени

- Пентестеры нередко сами просят выделить «дополнительное время»

Критерии успешности пентеста

УЦСБ

GIS DAYS

Ещё один способ получить нужный результат

- Укажите в ТЗ, какие «недопустимые события» вас интересуют
  - Пример: доступ к 1С, нарушение технологического процесса, утечка кодовой базы
- На первый взгляд это абстрактные, но на деле очень понятные цели
- Компрометация домена не гарантирует доступ к целевым системам
- Стоит отметить в ТЗ, что доступ должен подтверждаться скриншотами или полученными данными

Отчётная документация

УЦСБ

GISDAYS

Разные исполнители готовят отчёты по-разному

- Отчёт может быть оказаться недостаточно подробным и информативным

- Нормальные ожидания от отчёта по комплексному пентесту:
  - Перечень исследованных ресурсов
  - Описание эксплуатации уязвимостей
  - Описание цепочек атак
  - Риски от эксплуатации уязвимостей
  - Рекомендации по устранению с учётом особенностей инфраструктуры
  - Возможные компенсирующие меры
  - План дальнейших мероприятий

Отчётная документация

УЦСБ

GIS DAYS

Как получить отчёт нужного качества и формата?

- Определить в ТЗ:
  - Какие требуются разделы
  - Какая информация о работах нужна
  - Насколько подробными должны быть рекомендации

- Проводить приёмку отчёта вдумчиво и оценивать его полезность

- На этапе выбора подрядчика запросить пример отчёта
  - Возможно, он будет несколько устаревшим и «склеенным» из нескольких отчётов, но всё равно поможет понять, как исполнитель наполняет отчёты

Резюме

УЦСБ

GIS DAYS

Как получить максимум пользы от пентеста?

- Прописать в ТЗ требования:
  - Эксплуатации критичных уязвимостей и развития успешных атак
  - Описания эксплуатации уязвимостей и реализованных цепочек в отчёте
  - Продолжения работ до исчерпания возможностей
  - Проверки возможности реализации интересующих вас недопустимых событий
  - По наполнению отчёта:
    - Перечень ресурсов
    - Описание эксплуатации уязвимостей
    - Описание реализованных цепочек атак
    - Подтверждения реализации недопустимых событий скриншотами или другими материалами
    - Глубина проработки рекомендаций

Резюме

УЦСБ

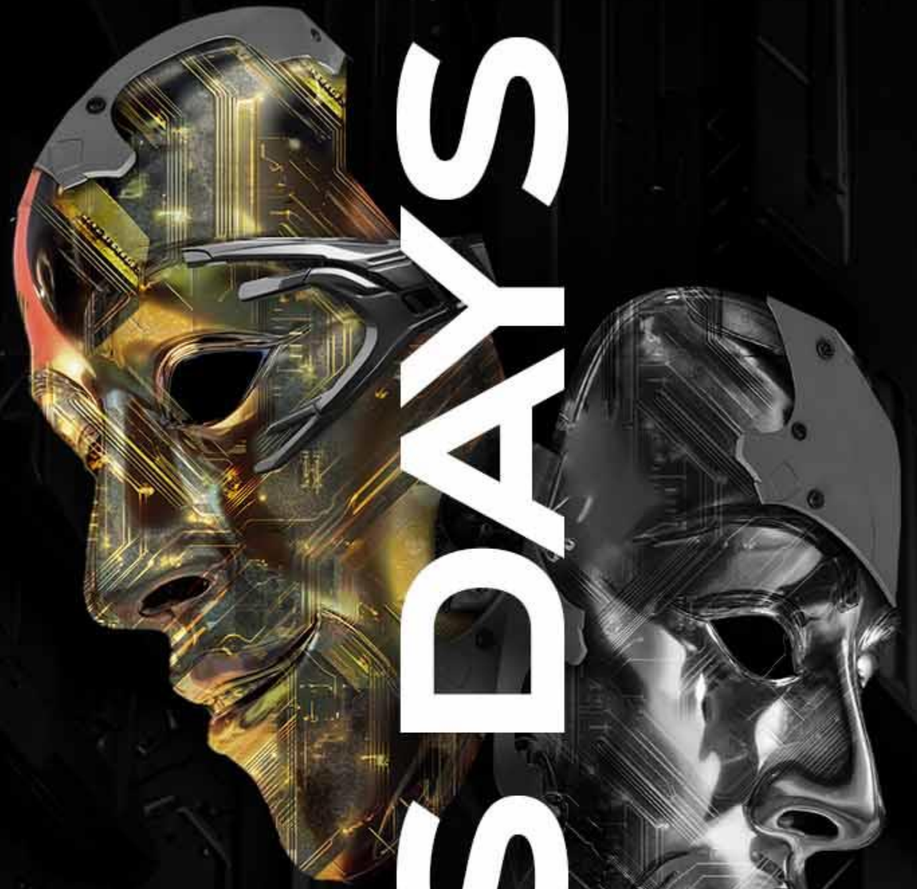
GISDAYS

Как получить максимум пользы от пентеста?

- Заранее пообщаться с потенциальным исполнителем:
  - Уточнить, какие векторы рассматриваются и каковы типовые критерии завершения работ
  - Запросить пример отчёта

- Задавать вопросы в ходе и после работ:
  - Уточнять в случае сомнений, почему не проводилась эксплуатация или не развивалась атака
  - Если рекомендация кажется недостаточной, спрашивать, может ли она быть уточнена

УЦСБ



GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ

dzubarev@ussc.ru
sec.ussc.ru