Digital Security
БЕЗОПАСНОСТЬ КАК ИСКУССТВО

Блеск и нищета пентеста в режиме Red Team

или "Не нужна тебе, Вовка, такая машина"

Илья Медведовский, к.т.н., генеральный директор Digital Security

Red Team

Red Team

Blue team

Purple team

Основные цели

Цель #1 - проникновение любым путем с максимальным количеством последующих действий

NB: Это не равно нахождению как можно большего количества уязвимостей!

Цель #2 - проверка уровня реагирования и оперативной готовности.

Все это - **Задачи отличные от анализа защищенности!**

Основные ожидания

Ожидание #1 «Хотим попробовать попасть в Москву через Париж и/или другие способы»

Ожидание #2 «Возможно пролезть даже в угольное ушко, нужно только постараться как следует»

Принципиальное отличие от концепции аудита:
- Ищутся только те уязвимости, которые позволят достичь определенной цели;
- Максимально эффективный метод не всегда самый сложный. Хотя бывает и наоборот и может потребоваться большое количество времени и ресурсов

Red Team?

Думать как злоумышленник
Подстраиваться под конкретную задачу
Большое количество времени
Большое количество ресурсов

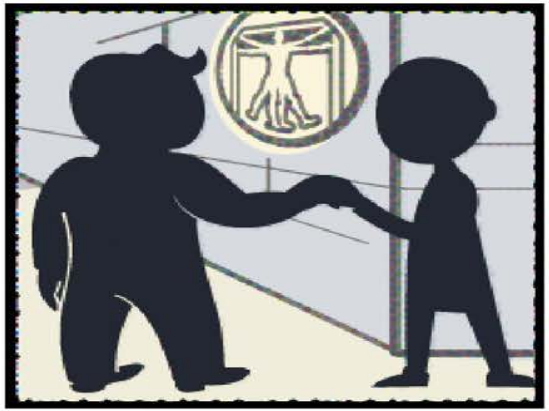
«Пентестеры» зачастую не имеют таких средств как злоумышленники.
Проект всегда ограничен во времени.
«Злоумышленнику» в отличие от пентестера спешить некуда

«Red Team» пентестер

Red team != «Реальные» действия злоумышленников

Пентестер НЕ злоумышленник

Возможности



Возможности злоумышленников для достижения цели:
- 0-day под целевую платформу
- Целенаправленное исследование ПО для нахождение 0-day
- Инсайдер
- Подкуп сотрудников

Все это требует большого количества времени и средств!

Потенциальные проблемы

Зачастую «жертвой» становятся не только Система, но и сотрудники (люди).

Легко можно выйти за пределы законности

Постэксплуатация

Была найдена уязвимость в «критичном» с точки зрения бизнеса продукте.
В случае эксплуатации — возможно получить доступ к КИС. В случае ЧП — отказ в обслуживании.

Пентест

Мы не знаем, что за система. Можем остановиться и спросить, обсудить последствия. Или попробуем сделать под контролем ИТ

VS

Red Team

Ок. Доступ в КИС это неплохо, главное чтобы не заметили

Не для всех

Red Team в первую очередь предназначен для организаций
с **серьезными**, **устоявшимися** мерами безопасности

Реагирование?

Должно быть частичное взаимодействие с службой реагирования и мониторинга.

«Мы вас поломали, ваша система не отреагировала, deal with it»

«Шпион выйди вон»

«Джеймс Бонд» - это хорошо. Только имеет очень мало общего с реальной жизнью.

Итог

Когда нужен «Red Team»:
#1 Проверка оперативности и реагирования
#2 Проверка уже существующей и четкой структуры информационной безопасности
#3 Проверка происходит в несколько этапов и под контролем

«Red Team» должен дополнять аудит, но не быть ему заменой!