

IT РЕШЕНИЯ



www.mmtr.ru

Тестирование на проникновение

IT РЕШЕНИЯ

www.mmtr.ru

О

докладчике Лапаков Олег



- Руководитель проектов в ММТР
- 2 года опыт управления проектами
- В ИТ с 1997 года
- В управлении проектами с 2006 года – МВД России, ФМС России, ООО ММТР
- КГУ, ФМФ, 2002

Penetration Test



Приказы ФСТЭК России № 17, № 21 и № 31 требуют анализировать защищённость информационных систем. Приказ № 21 содержит требование к периодичности — не реже одного раза в 3 года.



Три вида пентестов:

Тест на проникновение, основанный на технических методах.

Тест на проникновение, основанный на методах социальной инженерии.

Социотехнический пентест.



Категорирование пентестов

- внешний без учётных данных,
- внешний с учётными данными клиента,
- внутренний без учётных данных,
- внутренний с учётными данными клиента,
- внутренний с учётными данными администратора.

Тест на проникновение

- Внешний периметр (из Интернет).
- Внутренний периметр (внутри корпоративной сети).

Алгоритм проникновения

- Поиск уязвимостей.
- Реализация уязвимостей.
- **Продвижение вглубь системы.**
- Обход существующих систем защиты.

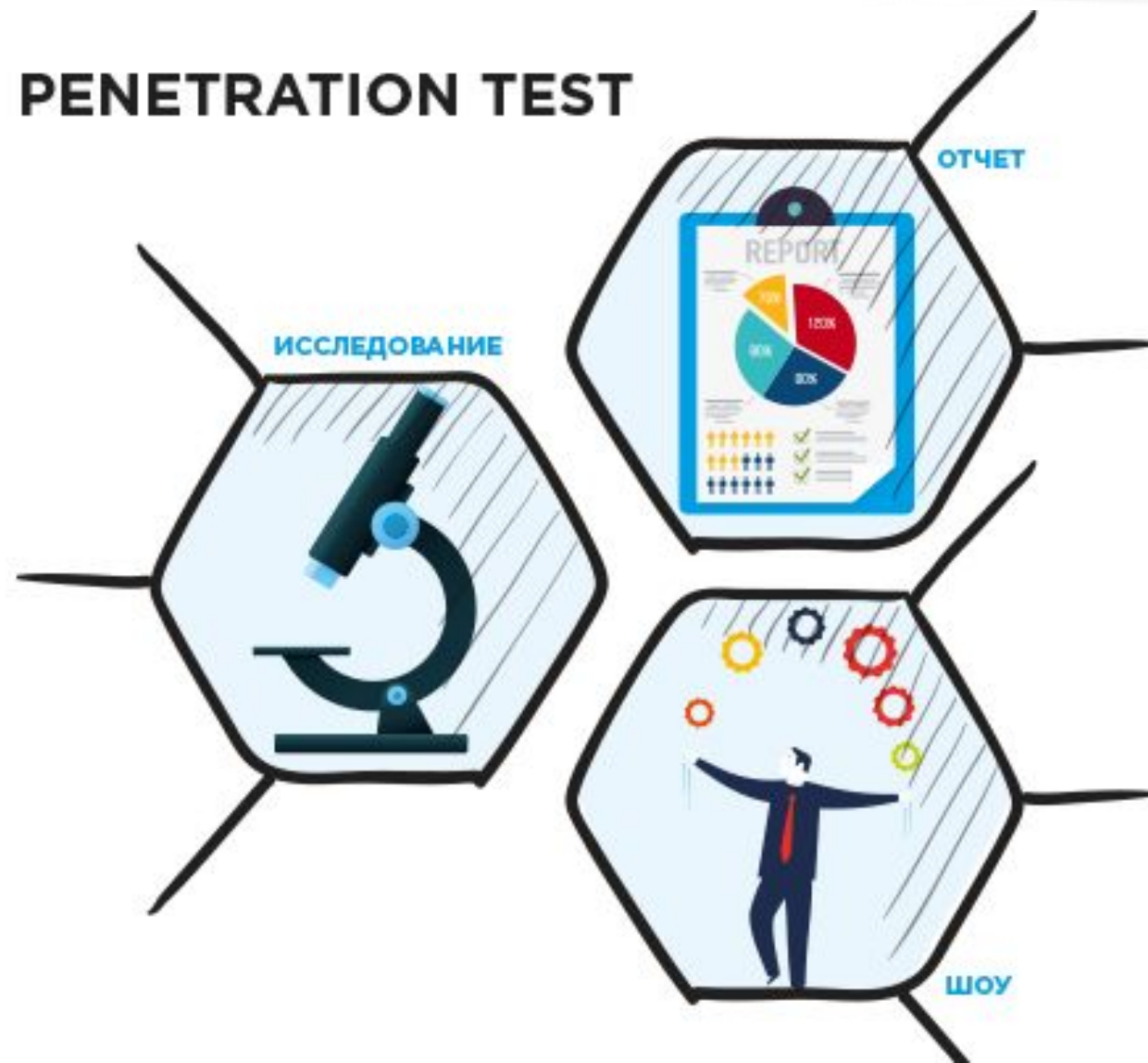
Алгоритм сканера

- Поиск уязвимостей по сигнатурам.
- Генерирования отчёта.

Объекты исследований

- Сайты и веб-приложения.
- СУБД.
- Сетевые службы и сервисы (электронная почта, прокси, VoIP, FTP и пр.).
- Протоколы различных уровней сетевой модели OSI.
- Сетевое оборудование.
- Беспроводные технологии.
- Средства защиты информации.
- Серверные и пользовательские операционные системы.
- Прикладное ПО.

PENETRATION TEST



Спасибо за
внимание