От тестов на проникновение к управлению уязвимостями – на что обратить внимание?

ЭЛВИС-ПЛЮС

РУСАЛ

ИФД-КапиталЪ

НТВ

ГАЗПРОМ НЕФТЬ-ХАНТОС
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

ВОЛГАТЕЛЕКОМ

Компания ЭЛВИС-ПЛЮС обладает большим опытом проведения работ по тестированию на проникновение в КИС компаний различных отраслей.

ХОЛДИНГ МРСК

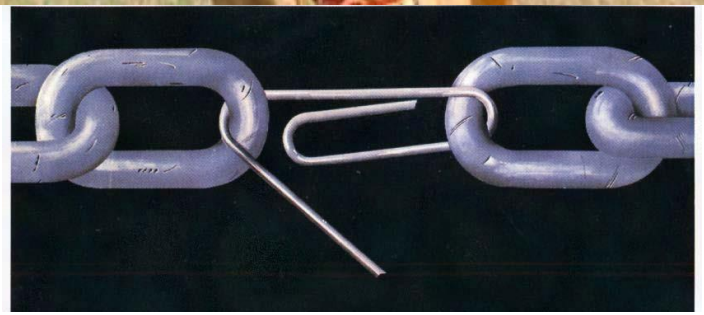
ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

ИНТЕР РАОЕЭС
ЭНЕРГИЯ БЕЗ ГРАНИЦ

Федеральная Сетевая Компания
Единой Энергетической Системы

Тест на проникновение

— процесс моделирования действий потенциального злоумышленника, направленных на получение НСД к конфиденциальной информации



Существующие угрозы

ТОП-10 уязвимостей в корпоративных сетях*

Ранг	Уязвимость	% сетей
1	Недостаточная сложность пароля системного администратора	89%
2	Передача критичных данных в незашифрованном виде	88%
3	Недостаточная сложность пароля доступа к БД	86%
4	Отсутствие защиты от атак подмены на протокол ARP	83%
5	Отсутствие защиты от атак подмены на протокол Netbios	79%
6	Использование протокола WEP для защиты беспроводных сетей	43%
7	Использование слабого механизма аутентификации в ОС Windows	67%
8	Ошибки настройки межсетевого экрана, защищающего периметр	22%
9	Доступ к системам/хранилищам, содержащим критичные данные	80%
10	Передача критичных данных по Bluetooth	16%

*согласно данным отчета Global Security Report, подготовленного компанией Trustwave в 2013 году

Примеры распространенных «уязвимостей» по опыту ЭЛВИС-ПЛЮС

- Использование простых паролей
- Отсутствие установленных обновлений ПО
- Отключенный/не установленный антивирус, антивирус с не обновленными базами
- Недостаточное разграничение прав доступа к файлам/ИР
- Отсутствие ограничений сетевого доступа к критичным узлам/ИР
- …

Процесс управления уязвимостями

Продукты, используемые в процессе управления уязвимостями

1. Системы анализа защищенности

ERPScan
Security Scanner for SAP

Продукты, используемые в процессе управления уязвимостями

2. Системы визуализации и анализа рисков сетевой безопасности

Системы визуализации и анализа рисков сетевой безопасности

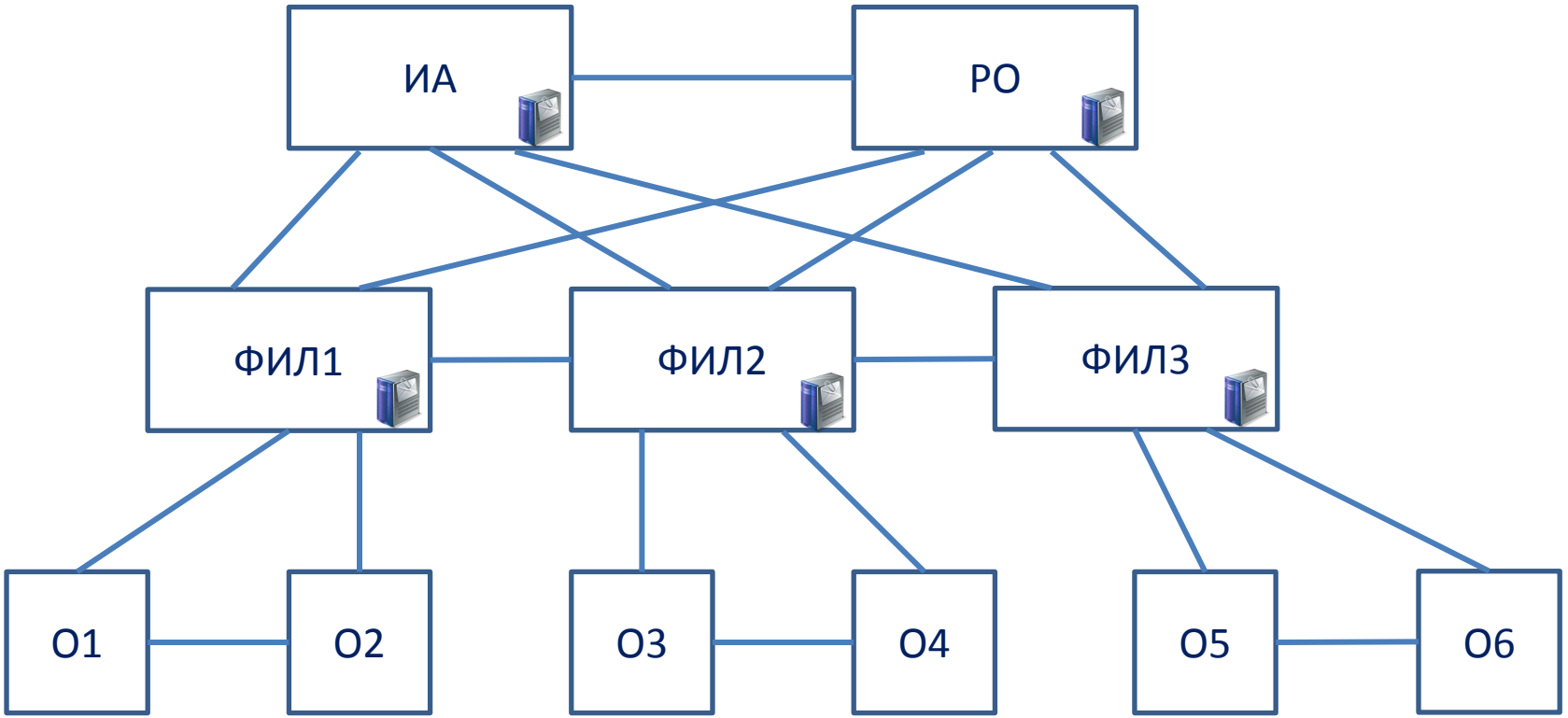
Преимущества использования:

1. Визуализация (построение модели сети организации), моделирование сетевого доступа
2. Анализ конфигурации сети (соответствие требованиям стандартов, рекомендаций)
3. Моделирование угроз безопасности (интеграция со сканерами безопасности, «пентест оффлайн»)
4. Реальная приоритезация уязвимостей на основе полученной модели использования уязвимостей
5. Мониторинг изменений сети (интеграция с SIEM, аргументированный диалог ИБ и бизнеса)

Системы визуализации и анализа рисков сетевой безопасности

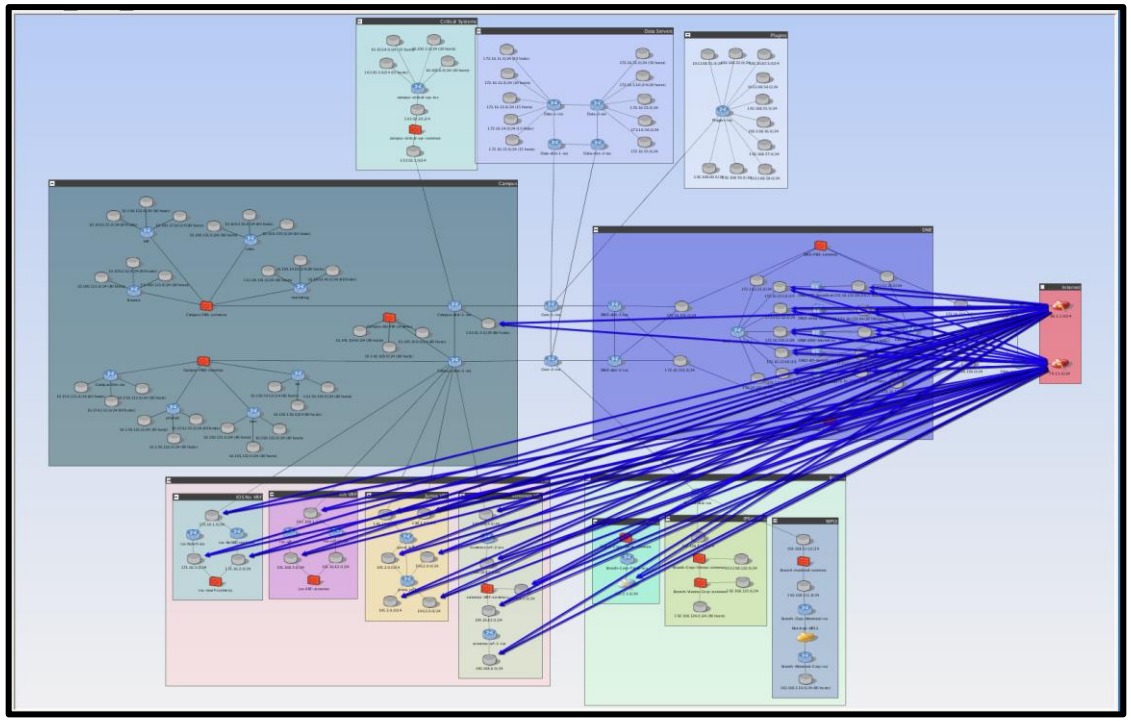
Система анализа защищенности и соответствия стандартам

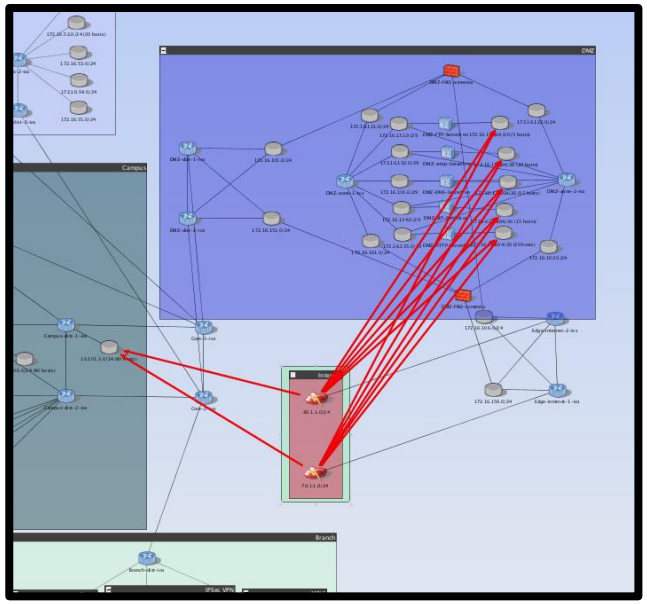
Системы визуализации и анализа рисков сетевой безопасности



Системы визуализации и анализа рисков сетевой безопасности

Моделирование сетевого доступа и угроз безопасности





Системы визуализации и анализа рисков сетевой безопасности

Приоритезация уязвимостей

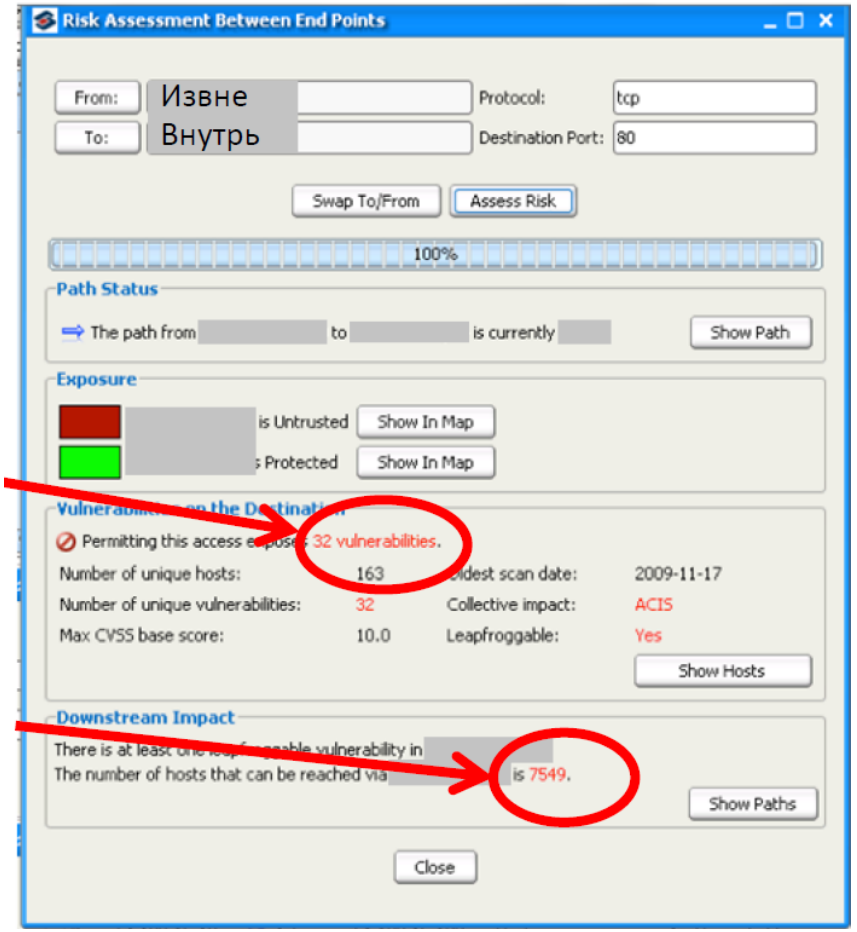
Системы визуализации и анализа рисков сетевой безопасности

Оценка возможных изменений сети

- Создание модели сети
- Ввод данных об изменении (потребность бизнеса: открыть одну сеть класса С :80)

Моделирование изменения выявляет 32 уязвимости

Нисходящий эффект - выявлено 7 549 уязвимостей



Услуги ОАО «ЭЛВИС-ПЛЮС»

- Презентации, в т.ч. с участием вендоров
- Реализация пилотных проектов
- Проектирование/внедрение и т.д.

Услуги ОАО «ЭЛВИС-ПЛЮС»

Пентест?

Антон Юдаков
начальник Отдела решений по управлению ИБ
a.yudakov@elvis.ru
+7 (495) 276-02-11, доб. 102
www.elvis.ru