Тесты на проникновение в корпоративных сетях

Антон Карпов,
компания Digital Security

Содержание

- Введение
- Комплексный аудит ИБ и тест на проникновение (пентест)
- Методика пентеста
- Пентест в корпоративной сети: сценарии и вектора атак
- Примеры из практики

Аудит информационной безопасности

- Этап жизненного цикла системы управления ИБ

- Комплексный аудит:
  - ❖ Технологический аудит
  - ❖ Аудит соответствия СУИБ требованиям стандартов ISO/IEC 27001:2005 и ISO/IEC 17799:2005
  - ❖ Анализ информационных рисков

Технологический аудит ИБ

- Тест на проникновение
- «Анализ конфигов» + сканирование

- Объективность?
- Полнота?
- Формализация?
- Критерии оценки защищенности системы?

Методика «активного аудита» ИБ

Пентест + «традиционный» аудит:

- Наличие модели нарушителя
- Инвентаризация ресурсов ИС
- Неформальный подход к анализу защищенности ИС
- Анализ влияния обнаруженных уязвимостей на защищенность всей ИС в целом
- Система классификации уязвимостей
- Частичный отказ от сканеров уязвимостей
- Социальная инженерия

Проверено на практике!

Активный аудит в корпоративной сети

- Модель нарушителя: внутренний пользователь ИС, имеющий физическое подключение к сети, но не имеющий никаких логических прав
- Область аудита – вся сеть (сервера, рабочие станции, активное сетевое оборудование)
- Цель – «все сломать ;)». Творческий подход аудиторов принципиально отличает аудит от бесхитростного запуска сканера уязвимостей

Активный аудит. Сервера. Что?

- Контроллеры домена
- СУБД (Oracle, MSSQL)
- Бизнес-системы (SAP)
- Внутрикорпоративные порталы
- Сервера обновлений
- ...

Активный аудит. Сервера. Как?

- «Тупые уязвимости» в критичных серверах («смерть за 5 минут»)
- Взлом веб-приложений
- Взлом СУБД (см. следующий доклад)
- Доступ вследствие misconfiguration (низкая квалификация администраторов)
- Тестовая (или legacy) среда в production environment

Повышение привилегий!

Взлом паролей!

Активный аудит. Рабочие станции

- Некоторым пользователям – особое внимание (бухгалтерия, и т.п.)
- Рабочие станции администраторов - !!!
- Рассылка реверсивного трояна из интернета

Data mining!

Активный аудит. Сетевое оборудование

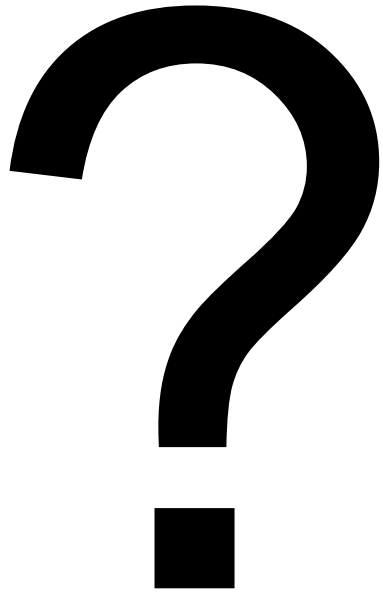
- Стандартные пароли и SNMP community string
- Протоколы удаленного администрирования с plaintext auth (telnet)
- Отсутствие ACL

Доступ с рабочих станций администраторов

Активный аудит. Что еще?

- Нелегитимные беспроводные сети
- Социальная инженерия: «звонок из службы поддержки»

Немного примеров из практики



Антон Карпов (a.karpov@dsec.ru)
http://www.dsec.ru

DIGITAL SECURITY