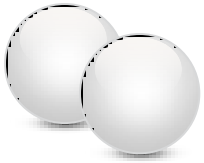
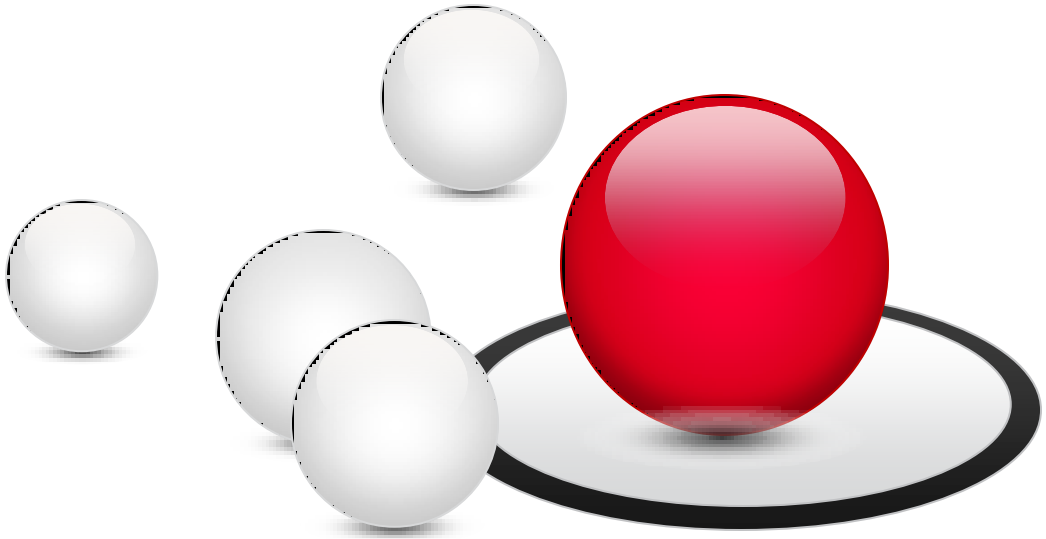
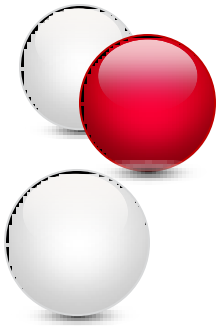


Эшелон
учебный центр

Тестирование на проникновение: можно ли научиться этичному взлому на курсах?





Подходы к оценке защищенности

Классический тест на проникновение

Сканирование на наличие уязвимостей

Анализ конфигурации системы

Комплексный подход

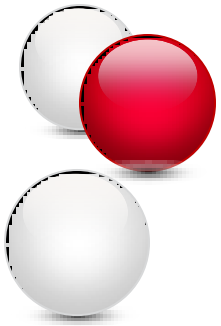
Эшелон
учебный центр

Что такое тестирование на проникновение?

- Метод оценки защищенности информационной системы или сети с помощью имитации атаки (действий злоумышленников).
- English: penetration testing, ethical hacking

Эшелон
учебный центр

Модель злоумышленника



Эшелон учебный центр

Классический тест на проникновение

- Имитация действий реального злоумышленника – поиск первой уязвимости, позволяющей получить доступ к системе
- Больше искусство, чем аудит. Качество сильно зависит от уровня специалиста
- Обычный результат: несколько опасных уязвимостей
- Высокий риск нарушения доступности систем

Эшелон
учебный центр

Сканирование

- Использование исключительно сканеров для поиска уязвимостей
- Качество сильно зависит от используемого сканера.
- Результат: множество уязвимостей различного уровня опасности
- Средний риск нарушения работоспособности систем

Эшелон
учебный центр

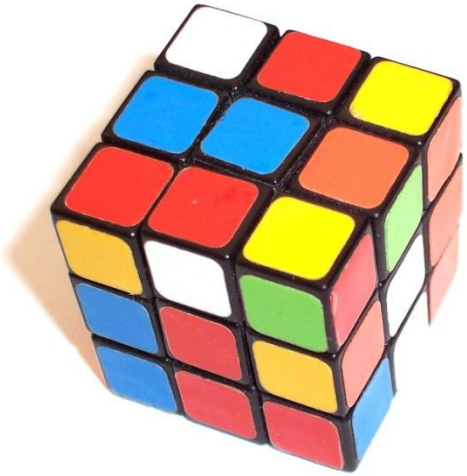
Анализ конфигурации системы

- Проверка настроек систем в соответствии с рекомендуемыми вендорами или сообществами профессионалов по ИБ (NIST, Center of Internet Security).
- Результат: множество уязвимостей различного уровня опасности
- Низкий риск нарушения работоспособности систем

Эшелон
учебный центр

Комплексный подход

- Использование комбинации упоминавшихся выше подходов
- Контролируемые риски нарушения доступности систем
- Контролируемое качество аудита



Эшелон
учебный центр

Основные цели работ

Классический тест на проникновение	• Демонстрация незащищенности систем
Сканирование	• Быстрый поиск уязвимостей для их устранения
Анализ конфигурации	• Поиск уязвимостей при минимальном воздействии на работу систем
Комплексный подход	• Поиск максимального количества уязвимостей с контролируемыми рисками проекта

Эшелон учебный центр

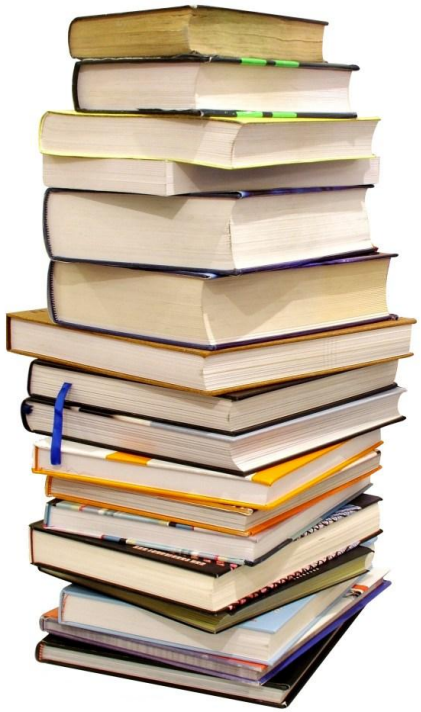
Комплексный подход: основные этапы

идентификация целевых сетевых узлов	• Nmap • Nslookup • Net view и т.д.
поиск уязвимостей	• Nessus, Nikto; • LanScope; • DumpSec, SID&USER и т.д.
эксплуатация уязвимостей, проведение атак	• THC-Hydra; • Metasploit; • Cain, LCP
расширение привилегий	• Локальные эксплойты.

Эшелон учебный центр

Методологии

- Information Systems Security Assessment Framework (ISSAF)
- Open Source Security Testing Methodology Manual (OSSTMM)
- OWASP Testing Guide
- Книги серии “Секреты хакеров”



Эшелон
учебный центр

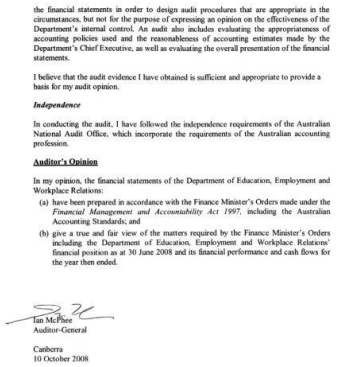
Инструменты

- Загрузочный диск Linux
- Предустановленные утилиты, готовых к работе(NMap, Hydra и др.)
- Примеры: Backtrack, Сканер-ВС

Эшелон
учебный центр

Хороший отчет

- Резюме для руководства
- Границы проекта
- Подход
- Описание каждой уязвимости в формате: обнаружение – риск – рекомендация
- Захватывающее последовательное описание действий аудитора интересно только администратору



the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by the Department's Chief Executive, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Independence

In conducting the audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Auditor's Opinion

In my opinion, the financial statements of the Department of Education, Employment and Workplace Relations:

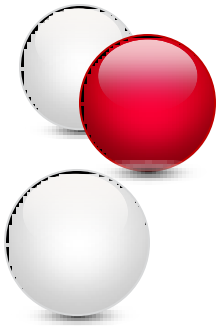
(a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards; and

(b) give a true and fair view of the matters required by the Finance Minister's Orders including the Department of Education, Employment and Workplace Relations' financial position as at 30 June 2008 and its financial performance and cash flows for the year then ended.

Ian McPhee
Auditor-General

Canberra
10 October 2008

Эшелон учебный центр



Наши курсы

- 003. Тестирование на проникновение: технологии хакеров для аудита информационной безопасности
- 012. Безопасность беспроводных сетей: взлом и защита
- Ряд специализированных курсов по тестированию на проникновение разрабатываются.
- Курсы читают только профессионалы практики

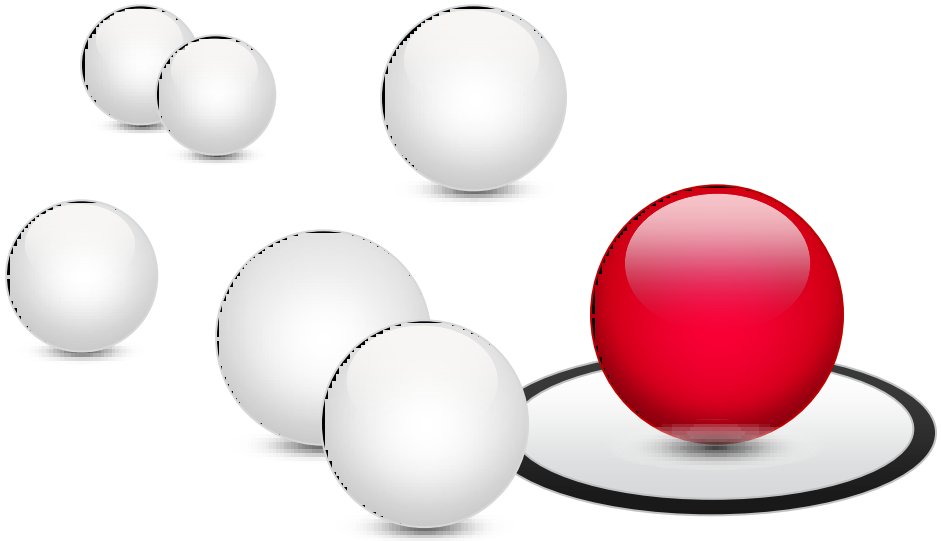
Эшелон
учебный центр

Полезные ссылки

1. www.uc-echelon.ru
2. www.backtrack-linux.org
3. www.nessus.org
4. www.owasp.org
5. www.oissg.org/issaf

Эшелон
учебный центр

Эшелон
учебный центр



Александр Дорофеев

CISSP, CISA

Директор

АНО “Учебный центр “Эшелон”

E-mail: a.dorofeev@npo-echelon.ru

Тел.: +7(495) 645-38-09