

УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



Аудит информационной безопасности компьютерных систем

Горячая линия-Телеком



Оглавление

Введение	3
1. Понятие аудита информационной безопасности	5
1.1. Типы аудита информационной безопасности	6
1.2. Методология проведения аудита информационной безопасности в национальных и отраслевых стандартах.	10
1.3. Классификация средств проведения аудита ИБ	13
1.4. Требования к средствам анализа защищенности	17
1.5. Особенности сканеров безопасности	19
1.6. Поиск информации по уязвимостям компьютерных систем	22
2. Методика проведения инструментальных проверок	27
2.1. Постановка задачи для проведения инструментальных проверок	29
2.2. Обнаружение сетевых узлов	32
2.3. Сканирование портов и идентификация ОС	37
2.4. Использование DNS для обнаружения и выяснения назначения сетевых узлов	41
2.5. Создание карт сети	44
2.6. Использование сканера безопасности Nessus	46
2.7. Сравнительный анализ сканеров безопасности	65
2.8. Анализ защищенности Web-серверов	74
2.9. Этап внутреннего аудита	80
2.10. Автоматизация получения итоговой оценки уровня информационной безопасности	85
2.11. Перечень и состав работ по проведению аудита информационной безопасности	92
2.12. Структура отчета по результатам аудита информационной безопасности	95
3. Поиск уязвимостей Web-приложений	97
3.1. Подготовка стенда	97
3.2. Анализ уязвимости типа «Подделка HTTP-запросов»	99
3.3. Анализ уязвимости типа «Внедрение команд»	102

3.4. Анализ уязвимости типа «Обход директории»	105
3.5. Анализ уязвимости типа «Выполнение команд на сервере»	109
3.6. Анализ уязвимости типа «Внедрение операторов SQL»	116
Обозначения и сокращения	121
Литература	122