Проскурин В. Г.

Защита программ и данных : учеб. пособие для студ. учреждений высш. проф. образования / В.Г.Проскурин. — М. : Издательский центр «Академия», 2011. — 208 с. — (Сер. Бакалавриат)

ОГЛАВЛЕНИЕ

Предисловие

Глава 1. Анализ программных реализаций, защита программ от анализа

1.1. Общие сведения
1.2. Метод экспериментов с «черным ящиком»
1.3. Статический метод
1.4. Динамический метод
1.4.1. Программные отладочные средства
1.4.2. Методика изучения программ динамическим методом
Метод маяков
Метод Step-Trace первого этапа
Метод аппаратной точки останова
Метод Step-Trace второго этапа
1.4.3. Пример применения динамического метода
1.5. Особенности анализа некоторых видов программ
1.5.1. Особенности анализа оверлейных программ
1.5.2. Особенности анализа графических программ Windows
1.5.3. Пример анализа графической программы Windows
1.5.4. Особенности анализа параллельного кода
1.5.5. Особенности анализа кода в режиме ядра Windows
1.6. Вспомогательные инструменты анализа программ
Монитор активности процессов ProcMon
Утилита управления процессами Process Explorer
1.7. Защита программ от анализа
Динамическое изменение кода программы
Искусственное усложнение структуры программы
Нестандартные обращения к функциям операционной системы
Искусственное усложнение алгоритмов обработки данных
Выявление факта выполнения программы под отладчиком.

Глава 2. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам

2.1. Общие сведения
2.2. Субъектно-ориентированная модель компьютерной системы

2.3. Модели взаимодействия программной закладки с атакуемой системой
2.3.1. Модель «наблюдатель»
2.3.2. Модель «перехват»
2.3.3. Модель «искажение»
Несанкционированное использование средств динамического изменения полномочий
Порождение дочернего процесса системным процессом
Модификация машинного кода монитора безопасности объектов
2.4. Предпосылки к внедрению программных закладок
2.4.1. Общие сведения
Утверждение
Следствие
2.4.2. Переполнения буферов
2.4.3. Отсутствие необходимых проверок входных данных
GetAdmin
Уязвимость %00
2.4.4. Некорректный контекст безопасности
AdminTrap
Системные окна на рабочем столе пользователя
2.4.5. Устаревшие функции
NetDDE Exploit
WMF Exploit (MS06-001)
2.4.6. Другие уязвимости
Уязвимость program, exe
2.5. Методы внедрения программных закладок
Маскировка программной закладки под прикладное программное обеспечение
Маскировка программной закладки под системное программное обеспечение
Подмена системного программного обеспечения
Прямое ассоциирование
Косвенное ассоциирование
2.6. Компьютерные вирусы как особый класс программных закладок
2.7. Средства и методы защиты от программных закладок
Сканирование системы на предмет наличия известных программных закладок
Контроль целостности программного обеспечения
Контроль целостности конфигурации защищаемой системы
Антивирусный мониторинг информационных потоков
Программные ловушки
2.8. Организационные и административные меры антивирусной защиты
Инструктирование пользователей

Просмотр и анализ данных регистрации и мониторинга
Контроль качества аутентификационных данных пользователей
Регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной зашиты сети, в случае успешных вирусных атак
Регулярные инспекции состояния антивирусной защиты
2.9. Выявление программных закладок в ручном режиме

Приложение

Методические рекомендации по организации изучения дисциплины «Защита программ и данных»
Анализ требований ФГОС ВПО
Организация изучения защиты программ и данных

Список литературы

Рекомендуемая литература
Интернет-ресурсы