

ЗАЩИТА ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПОЛЬЗОВАТЕЛЯ ОТ АТАК ПОДМЕНЫ ИНФОРМАЦИИ

В.Ю. Мандрик

Пользователи персональных компьютеров часто эксплуатируют сервисы, обеспечивающие их упрощенную аутентификацию при доступе к электронной почте и другим аккаунтам. Такая тенденция усложняет проблему информационной безопасности. Ее решение лежит в плоскости разработки организационно-технических мероприятий, направленных на противодействие атакам подмены и снижению риска несанкционированного доступа к персональным данным.

В результате исследования была смоделирована атака ARP-spoofing. В случае данной атаки компьютер начинает считать шлюзом не маршрутизатор, а компьютер атакующего. Атакующий получает запросы от «жертвы» и передает их в пункт назначения (например, запрашивает содержимое веб-сайта в Интернете), получив ответ от сервера, он направляет его «жертве». В этой ситуации атакующий становится посредником – отсюда другое название атаки человек-посередине – «атака посредника».

Атака ARP-spoofing используется в локальной сети, построенной на коммутаторах. С ее помощью можно перенаправить поток ethernet-фреймов на другие порты, в соответствии с MAC-адресом. После чего злоумышленник может перехватывать все пакеты на своем порту. Таким образом, атака ARP-spoofing позволяет перехватывать трафик машин, расположенных на разных портах коммутатора. В ходе исследования выполнена оценка эффективности различных средств защиты информации от указанного типа атаки.

КОНЦЕПЦИЯ ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Ф. Марко

Рассматривается предложенная концепция тестирования разрабатываемого программного обеспечения для технических средств защиты информации, которая реализуется с помощью комплексной системы Team Foundation Server [1]. В качестве инструмента для осуществления процесса тестирования используется тест-трекинг-система Microsoft Test Manager, которая предназначена для организации планов тестирования, создания и управления тестовыми случаями. В этом случае также присутствует возможность связать ручные тестовые случаи с автоматическими.

Нами предлагается следующая концепция тестирования. В системе МТМ создается базовый план тестирования. Тестовые случаи в базовом плане сортируются по модулям в зависимости от тестируемой функциональности ПО и виду тестирования. Сортировка тестовых случаев осуществляется с помощью таких объектов системы МТМ, как статические наборы тестов, наборы тестов на основе запросов и теги. Каждой версии тестируемого ПО соответствует итерация, в которой хранится два плана тестирования: базовый и текущий. Базовый план копируется из предыдущей итерации, а также расширяется новыми тестовыми случаями, текущий план формируется из базового путем клонирования определенных тестовых наборов с учетом поставленных задач тестирования.

Таким образом разработана гибкая концепция тестирования разрабатываемого ПО, которая позволяет эффективно выполнять тестирование и автоматизировано предоставлять результаты его выполнения.

Список литературы

1. Командная разработка с использованием Visual Studio Team Foundation Server / Д. Мейер [и др.]. Microsoft Visual Studio Team System, 2008. 564 с.