ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ WPA2

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информациив сетях Wi-Fi является протокол WPA второго поколения. WPA2 заменил WPA. WPA2, который требует тестирования и сертификации Wi-Fi Alliance, реализует обязательные элементы IEEE 802.11i. Со стандартом 802.11i вся цепочка модуля безопасности (вход в систему, обмен полномочиями, аутентификация и шифрование данных) становится более надежной и эффективной защитой от ненаправленных и целенаправленных атак. Стандарт 802.11r является модификацией стандарта 802.11i. Данный стандарт был ратифицирован в июле 2008 года. Технология стандарта более быстро и надежно передает ключевые иерархии, основанные на технологии Handoff (передача управления) во время перемещения пользователя между точками доступа. Стандарт 802.11r является полностью совместимым с WiFi стандартами 802.11a/b/g/n. Также существует стандарт 802.11w, предназначенный для усовершенствования механизма безопасности на основе стандарта 802.11i. Этот стандарт разработан для защиты управляющих пакетов.Стандарты 802.11i и 802.11w – механизмы защиты сетей WiFi стандарта 802.11n [1]. Но в данной технологии, как и, естественно, во всем есть недостатки, а именно: слабая стойкость пароля на взлом, отсутствие прямой секретности (дешифровка по разделенному ключу), hole196 (по GTK), атака KRACK (Key Reinstallation Attack) и т.д. Также 16 октября 2017 г. эксперты по бесопасности сообщили, что WPA2 официально взломан и больше не может обеспечивать необходимый уровень безопасности. Исходя из вышеизложенного, можно сделать вывод о том, что WPA2 на сегодняшний день является весьма небезопасным протоколом, которым люди вынуждены пользоваться, так как альтернатив пока нет. С другой стороны, в январе 2018 года Wi-Fi Alliance сообщила, что ведутся работы над новым протоколом WPA3. Остается надеяться, что все эти недостатки будут устранены в новой версии.

Литература

1. Geier, J. WPA Security Enhancements. 2003. 137 p.

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА БАЗЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Е.В. Кармаз, Г.А. Пухир

Для того чтобы обезопасить информационную систему, ряд организаций регулярно проводят тестирование на проникновение в рамках аудита информационной безопасности, что позволяет получить объективную оценку возможности осуществить несанкционированный доступ к ресурсам корпоративной сети или сайта. Процесс тестирования на проникновение является моделированием реальных действий злоумышленника с целью поиска уязвимостей системы защиты. Эта услуга позволяет получить независимую оценку и экспертное заключение о состоянии защищенности информации ограниченного распространения.

Технологии тестирования на проникновение могут осуществляться на базе технических методов и/или социотехнических методов, а также с применением методов социальной инженерии. С их помощью осуществляются санкционированные попытки получения несанкционированного доступа к корпоративной сети и защищаемым активам целевой организации. Методы, как правило, направлены на пользователей конечных систем и позволяют определить реакцию персонала в штатных и нештатных ситуациях, уровень знаний персонала о требованиях безопасности. К некоторым из таких методов можно отнести:

1. Фишинг (побуждение пользователей к вводу конфиденциальных данных (например, паролей) на фальшивой веб-странице легального сервиса.
2. Троянский конь (побуждение пользователя к открытию писем с вредоносными вложениями за счет целевых сопроводительных писем, звонков, наименований файлов и др.).
3. Претекстинг (моделирование определенного сценария, предполагающего вход в доверие к пользователю (за счет предварительного сбора данных об организации, отдельных работниках и их зонах ответственности), с целью побудить выполнить определенное действие).