УДК 004.056
ББК 32.973.202
Р24

Р24 **Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел**
Защита от хакеров беспроводных сетей: Пер. с англ. А. В. Семенова. – М.: Компания АйТи; ДМК-Пресс. – 480 с.: ил. (Серия «Информационная безопасность»).

ISBN 5-98453-012-0

Цель этой книги – предоставить максимально исчерпывающую информацию о беспроводных коммуникациях людям, работающим во всех сферах бизнеса и информационных технологий, подготавливают ли они реальный бизнес-план для беспроводного проекта, являются ли они IS/IT-специалистами, планирующими новое беспроводное внедрение, включают ли они беспроводные возможности в домашнюю сеть, реагируют ли на атаку на их сеть или просто любят заниматься проблематикой безопасности.

УДК 004.056
ББК 32.973.202

ISBN 1-928994-59-8 (англ.)
ISBN 5-98453-012-0 (АйТи)

Содержание

Ответы на ваши беспроводные вопросы

Вопрос: Будет ли i-Mode распространяться в Европе или Северной Америке?
Ответ: Хотя владелец i-Mode, компания NTT DoCoMo имеет заметные доли в пакетах акций нескольких северо-американских и европейский сотовых операторов, нет планов быстрого вывода i-Mode в современном виде на эти рынки. Это обусловлено прежде всего ограниченной скоростью доступа 9,6 Кб/с.

Средства и ловушки

Текстовая аутентификация

Пример генератора словаря паролей для атак грубой силы, который может создавать этот словарь на основе набора букв, можно отыскать в Интернете на сайте www.dmzs.com/tools/files. Есть и другие генераторы для атак грубой силы на POP: Telnet, FTP, Web и т. п., их можно найти на http://packetstormsecurity.com/crackers.

Фиксированные беспроводные технологии

В беспроводных фиксированных сетях и передатчик, и приемник постоянно находятся в определенном месте в отличие от мобильных сетей. Эти сети используют питание от переменного тока. Они могут быть организованы по схеме «точка-точка» или же «точка-многоточка» и могут использовать как лицензируемый, так и нелицензируемый спектр.

Заметки из подземелья

Шлюз компании Lucent Technologies сообщает SSID открытым текстом даже в сетях с шифрованием

Как было объявлено в Интернете на сайте www.securiteam. com/securitynews/5ZP0I154UG.html, шлюз компании Lucent открывает атакующему простой путь для соединения с закрытой сетью. Чтобы соединиться с беспроводной сетью, пользователь должен знать SSID сети. Даже если сеть защищена при помощи WEP, часть передаваемых посланий шлюз передает в незашифрованном виде, включая SSID. Все, что должен сделать атакующий, – это «вынюхивать» сеть для определения ее SSID, после этого он сможет соединиться с сетью.

Стратегии для анализа угроз

- определить активы компании;
- определить возможные доступы к ним в точки зрения авторизации;
- определить вероятность того, что неавторизованный пользователь сможет получить доступ к этим активам;
- определить потенциальные потери;
- определить стоимость восстановления после потерь и ремонтных работ или оценить потери;
- определить необходимые контрмеры безопасности;
- определить стоимость внедрения контрмер;
- сравнить стоимость обеспечения безопасности ресурсов с величиной потерь.

Активное вождение

Активное вождение – это термин, обозначающий действия людей, которые перемещаются, имея в своем распоряжении беспроводное оборудование для выслеживания других беспроводных сетей. Термин образован по аналогии с термином «активный обзвон», относящимся к хорошо известной практике постоянного перебора определенного набора номеров через модем, чтобы обнаружить соединенные с ними компьютеры.

Соображения об оборонительном мониторинге

- определите границы вашей беспроводной сети, чтобы точно знать, когда они буду нарушаться;
- ограничивайте силу сигнала, чтобы сохранить его в пределах сети;
- составьте список всех авторизованных беспроводных точек доступа (ТД) в расположении своей компании; подробное знание их поможет вам быстро локализовать ложную ТД.

Аудит

Аудит беспроводных сетей состоит из нескольких шагов, в которых для проведения определенных действий нужны различные ресурсы или устройства. Эти действия можно подразделить на шесть категорий:

- планирование аудита;
- сбор аудиторской информации;
- анализ собранной информации и создание отчета;
- представление аудиторского отчета;
- обзор ситуации после аудита;
- дальнейшие действия.

Создание сверхбезопасной WLAN

- Убедитесь, что ваша ТД позволяет вам изменить ESSID, пароли и поддерживает 128-битный WEP.
- Используйте ТД, которая поддерживает функциональность «закрытой сети».
- Будьте уверены, что ваши ТД позволяют проводить модернизацию.
- Изолируйте ТД и регулируйте доступ из их сети в вашу внутреннюю сеть.
- Проводите аудиты вашей сети с использованием NetStumbler или других средств беспроводного сканирования, чтобы убедиться в том, что неавторизованные хакеры не могут получить к ней доступа.
- Обновляйте политику безопасности, чтобы отразить в ней все опасности небезопасной беспроводной сети.