Проблемы безопасности беспроводных сетей. Методы и способы защиты Wi-Fi сетей. Реалии и перспективы.

МИНИСТЕРСТВО ИНФОРМАЦИОННОГО РАЗВИТИЯ РЕСПУБЛИКИ МОЛДОВА

Инженер-проектировщик
Центра прикладных исследований
технологий информационного общества
Игорь АНДРУШКА

Тел: (373 22) 201011
Факс: (373 22) 22 65 72
E-mail: andrushca@registru.md

Введение

Принимая решение о переходе к беспроводной сети, не стоит забывать, что на сегодняшнем этапе их развития они имеют одно уязвимое место - *безопасность беспроводных сетей.*

Аспекты безопасности беспроводных сетей

- защита от несанкционированного доступа ;
- шифрование передаваемой информации.

- «аутентификация не пройдена и точка не опознана»;
- «аутентификация пройдена, но точка не опознана»;
- «аутентификация принята и точка присоединена».

Механизмы защиты

- Wired Equivalent Protocol (WEP);
- WEP 2;
- Open System Authentication;
- Access Control List;
- Closed Network Access Control.

Виды атак на беспроводные сети

- Access Point Spoofing & Mac Sniffing;
- WEP Attacks;
- Plaintext атака;
- XOR;
- Повторное использование шифра;
- Атака Fluther-Mantin-Shamir;
- Low-Hanging Fruit.

Способы защиты

- фильтрация MAC адресов;
- SSID (Network ID);
- Firewall;
- AccessPoint.

Атака против неассоциированного клиентского хоста

1. Находится неассоциированное клиентское устройство, либо используется «затопление» сети фреймами деассоциации или деаутентификации для его получения.
2. Специфически эмулируется точка доступа для подсоединения этого хоста.
3. Выдается IP адрес, а также IP адреса фальшивых шлюза и DNS сервера через DHCP.
4. Атакуется устройство.
5. Если это необходимо и удаленный доступ к устройству был успешно получен, хост «отпускается» обратно на «родную» сеть, предварительно запускается на нем «троян».

Процесс работы Алгоритма беспроводной самонастройки (АБС)

1. Составление СДС путем посылки широковещательных Probe Request фреймов с пустым полем ESSID по одному на каждый из используемых 802.11 каналов.
2. Клиентское устройство ассоциируется с самой верхней сетью СПС, которая присутствует в СДС.
3. Посылка Probe Request фреймов специфически для поиска сетей, перечисленных в СПС.
4. Поиск ad-hoc сетей.
5. Установление клиентского устройства в режим ad-hoc и присваивание IP адреса, принадлежащего диапазону RFC 3330.
6. Проверка флага «Присоединение к Непредпочитаемым сетям».

Благодарю за внимание!