1. Что такое Ad-Hoc?

Режим беспроводного соединения между устройствами. Клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу “точка-точка”, и компьютеры взаимодействуют напрямую без применения точек доступа.

Основное достоинство – простота организации. Недостатки: Максимальная скорость до 11 Мбит/с. Реальная скорость 11/N Мбит/с, где N – количество устройств в сети. Дальность связи не более 100 метров. Скорость резко падает с увеличением расстояний.

1. Назначение протокола SMB?

Протокол блока серверных сообщений (SMB). Вариант данного протокола – протокол CIFS, реализованный вWindows NT4.

Протокол уровня приложения/представления данных. Это зависит от протокола транспортировки (чаще всего NetBIOS протокол через TCP/IP или NBT).

Главное назначение – совместное использование файла несколькими компьютерами в локальной сети.

Другие возможности:

- Определение других серверов в SMB в сети

- Печать через сеть

- Файл, каталог и аутентификация коллективного доступа

- Файл и блокировка записи

- Файл и уведомление об изменении каталога

- Согласнование диалекта (набора пакетов сообщений, который определят верисю протокола)

- Дополнительная обработка атрибутов файла

- Поддержка Unicode

- Уступающие блокировки(блокировки, которые помещаются клиентами в файл, находящийся на сервере).

1. Общий формат кадра зондирования.

Процесс зондирования – один из этапов установки соединения в стандарте IEEE802.11.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Octets:2 | 2 | 6 | 6 | 6 | 2 | 0-2312 | 4 |
| Frame  Control | Duration | DA | SA | BSSID | Sequence  Control | Frame  Body | FCS |
| MAC - Header | | | | | |  |  |

Формат запроса и формат ответа различаются только полем Frame Body, где находятся передаваемые данные.

- Заголовок MAC Header

\* Frame Contol - тип кадра. В данном случае это кадр зондирующего запроса или кадр ответа на зондирование.

\* Duration – время, необходимое на передачу кадра,а также получения, подтвердения его приема.

\* DA – MAC адрес назначения

\* SA – MAС адрес отправителя

\* BSSID – идентификатор BSS. Идентификатор точки доступа, зондирование которой требуется , либо широковещательный идентификатор.

\* Sequence Control – порядковый номер кадра в потоке кадров.

\* FCS – контрольная сумма

\* Frame Body – информационное тело кадра

Содержит в себе:

Кадр запроса:SSID(идентификатор зоны обслуживания) и

Supported Rates (список поддерживаемых скоростей)

Кадр ответа:Набор различных параметров сети, определяющих какой режим взаимодействия необходимо устаналивать.

1. Общий формат кадра ассоциирования

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Octets:2 | 2 | 6 | 6 | 6 | 2 | 0-2312 | 4 |
| Frame  Control | Duration | DA | SA | BSSID | Sequence  Control | Frame  Body | FCS |
| MAC - Header | | | | | |  |  |

Все тоже самое, что и у кадра зондирования. Отличие только во Frame Body

Здесь он содержит:

Запрос содержит: SSID, Capability Info (инфа о совместимости), Listen Interval (интервал прослушивания), Supported Rates (поддерживаемые скорости).

Ответ содержит: Status Code (код состояния), Association ID, Supported Rates

1. Что такое сниффер?

Программы, способные перехватывать и впоследствии проводить анализ сетевого трафика. Снифферы полезны в тех случаях, когда нужно перехватить пароли или провести диагностику сети. Программу можно установить на одном устройстве, к которому есть доступ и в течение короткого времени получить все передаваемые данные из подсети.

6. Возможности сниффера WireShark

основные возможности программы:

Захват пакетов в реальном времени из проводного или любого другого типа сетевых интерфейсов, а также чтение из файла;

Поддерживаются такие интерфейсы захвата: Ethernet, IEEE 802.11, PPP и локальные виртуальные интерфейсы;

Пакеты можно отсеивать по множеству параметров с помощью фильтров;

Все известные протоколы подсвечиваются в списке разными цветами, например TCP, HTTP, FTP, DNS, ICMP и так далее;

Поддержка захвата трафика VoIP-звонков;

Поддерживается расшифровка HTTPS-трафика при наличии сертификата;

Расшифровка WEP-, WPA-трафика беспроводных сетей при наличии ключа и handshake;

Отображение статистики нагрузки на сеть;

Просмотр содержимого пакетов для всех сетевых уровней;

Отображение времени отправки и получения пакетов.

7. Формат заголовка SMB?

|  |  |  |  |
| --- | --- | --- | --- |
| 8 | 16 | 24 | 32 bits |
| Command | RCLS | Reserved | ERR |
| ERR (cont) | REB/FLG | Reserved | |
| Reserved | | | |
| Reserved | | | |
| Reserved | | | |
| Tree ID | | Process ID | |
| User ID | | Multiplex ID | |
| WCT | VWV | | |
| BCC | | BUF | |

**Command** — команда протокола.   
   • **RCLS** — код класса ошибки.   
   • **ERR** — код ошибки.  
   • **Tree ID (TID)** — идентификатор соединения с сетевым ресурсом.   
   • **Process ID (PID)** — идентификатор клиентского процесса фактического соединения.   
   • **User ID (UID)** — идентификатор пользователя; используется сервером для проверки прав доступа пользователя.   
   • **Multiplex ID (MID)** — идентификатор группы пользователя; используется сервером для проверки прав доступа группы пользователя.  
   • **WCT** — количество параметров, следующих за заголовком.  
   • **BCC** — количество байт данных, следующих за параметрами.

8. Принцип работы протокола SMB?

Пример работы:

9. Методы взлома SMB.

10. Алгоритм шифрования WEP

11. Уязвимость шифрования WEP

12. Проблемы управления статическими WEP-ключами

13. Процесс создания шифрованного сообщения в WPA

14. Контроль целостности сообщений WPA