Курсовая работа «Анализ методов защиты беспроводных сетей»

Выполнила:
Пушкова К.С.,
студентка 4 курса
очной формы обучения,
направление подготовки
«Прикладная информатика»
направленность (профиль) Прикладная информатика в экономике
Научный руководитель:
К.б.н, доцент Широкова Н.П.

Объект исследования в данной работе – средства защиты информации в беспроводных сетях.

Предмет исследования – технологии защиты информации в беспроводных сетях от несанкционированного доступа.

Целью курсовой работы является изучение методов повышения защиты данных при передаче с помощью беспроводных сетей.

Основные угрозы беспроводных сетей

Угрозы, возникающие в беспроводных сетях при передаче информации, разделяют на два вида:

I. *Прямые – возникают при передаче информации по беспроводному интерфейсу IEEE 802.11;*

II. *Косвенные – связаны с присутствием на определённой территории и рядом с ней большого количества Wi-Fi-сетей.*

Наиболее распространенными угрозами являются чужаки и нефиксированная связь.

СРЕДСТВА ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ

Как средства защиты от часто встречающихся угроз в беспроводных сетях используется такие технологии:

- ***Режим безопасности WEP***
- ***Режим безопасности WPA***
- ***Режим безопасности WPA-PSK***

НАСТРОЙКА БЕЗОПАСНОСТИ В БЕСПРОВОДНОЙ СЕТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ

Исследование систем обнаружения вторжения

Системой обнаружения вторжений можно использовать для нахождения определённой вредоносной активности, нарушающей безопасность компьютерной сети, а именно:

- *сетевые атаки против уязвимых сервисов,*
- *атаки,*
- *направленные на повышение привилегий,*
- *неавторизованный доступ к важным файлам,*
- *действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей) .*

Программа Kismet

Данный инструмент выполняет следующие функции:

- ✔ *обнаруживает перегрузки запросами на остановку сеанса и отключение;*
- ✔ *анализирует порядковые номера фреймов стандарта 802.11;*
- ✔ *выявляет пользователей Air Jack в наблюдаемой сети;*
- ✔ *обнаруживает пробные запросы, посылаемые программой NetStumbter;*
- ✔ *обнаруживает атаки по словарю на ESSID, проводимые при помощи Wellenreiter;*
- ✔ *обнаруживает клиентов, посылающих пробные запросы, но не присоединяющихся к сети;*
- ✔ *выполняет различение сетей 802.11 DSSS и FHSS;*
- ✔ *выполняет сохранение фреймов с информацией в именованный FIFO-канал для дальнейшего анализа;*
- ✔ *выполняет дешифровку WEP;*
- ✔ *обнаруживает увеличение шума в канале;*
- ✔ *обнаруживает беспроводные сети Lucent Outdoor Router/ Turbocell/Karlnet, построенные не на базе стандарта 802.11.*

Изучение системы обнаружения вторжений на примере Kismet

Для установки программы необходимо выполнить следующие действия:

1. *Загрузить Kismet с установочного компакт-диска или с web-сайта.*

2. *Распаковать установочный файл.*

3. *При компиляции приложения Kismet необходимо выполнить команду./configure с некоторыми подходящими настройками, которые задаются ключами, перечисленными в таблице 1.(ключи компиляции можно задавать в настройках конфигурации.)*

4. *При окончании процесса настройки необходимо выполнить команды makedep и maketmakeinstall от имени супер-пользователя, для окончания компиляции и установки программы;*

Таблица 1

Конфигурационные ключи Kismet

Ключ	**Описание**
--disable-curses	Отключает интерфейс пользователя на основе curses
--disable-panel	Отключает расширения панели ncurses
--disable-gps	Отключает поддержку GPS
--disable-netlink	Отключает перехват сокетов Linux NetLink (с заплатами для prism2/orinoco)
--disable-wireless	Отключает беспроводные расширения ядра Linux
--disable-pcap	Отключает поддержку перехвата посредством libpcap
--enable-syspcap	Использует системную библиотеку libpcap (не рекомендуется)
--disable-setuid	Отключает возможность переустановки действующего идентификатора пользователя (не рекомендуется)
--enable-wsp100	Включает устройство перехвата - удаленный сенсор WSP100
--enable-zaurus	Включает звуковые функции.
--enable-local-dumper	Заставляет использовать локальные средства дамповой памяти.
--with-ethereal=DIR	Поддерживает прослушивание Ethereal для записи протоколов.
--without-ethereal	Отключает поддержку прослушивания Ethereal
--enable-acpi	Включает поддержку продвинутого интерфейса конфигурирования и питания ядром Linux

Таблица 2

Интерфейсные и протокольные опции Kismet

Параметр	Описание
Capture source	Определяет, какие интерфейсы будут прослушиваться программой Kismet. При необходимости добавления дополнительных интерфейсов, можно сделать это в формате source=тип,интерфейс,имя.
Fuzzy encryption	Настройка отображает все принятые пакеты как нешифрованные для тех станций, которые применяют неизвестные методы шифрования.
Filtering packet logs	Настройка ограничивает множество пакетов, подлежащих протоколированию. Опция noiselog даёт возможность отбросить все пакеты, испорчены или фрагментированы из-за помех. Опция beaconlog предоставляет возможность отбросить все пакеты отдельной точки доступа. Настройка phylog отбрасывает все пакеты физического уровня.
Decrypt WEP keys	Расшифровывает перехваченные пакеты данных на лету. Для этого, следует иметь ключ, который иногда можно добыть с помощью программы Air Snort. Для каждой точки доступа требуется отдельная инструкция вида bssid:key, где bssid - это MAC-адрес точки доступа, a key - ключ для нее
Using an external IDS	Посылает пакеты внешней системе обнаружения вторжений для дальнейшего анализа. В этой инструкции задается именованный канал, а сетевой системе обнаружения вторжений следует предписать чтение из него.

5. *После завершения установки программы Kismet, необходимо найти файл kismet.conf, который располагается в каталоге /usr/local/etc. В этом файле пользователем задаются настройки интерфейса и протоколов программы.*

6. *Теперь нужно отредактировать файл kismet_ui.conf, также находящийся в /user/local/etc. В нем задаются некоторые настройки интерфейса. В таблице 3 перечислены возможные варианты.*

7. *Сохранить оба файла.*

Теперь все готово к применению Kismet для аудита беспроводной сети. В нем задаются некоторые настройки интерфейса.

Таблица 3

Настройки интерфейса Kismet

Настройка	Описание
Columns	Определяет, какие столбцы и в каком порядке появятся в интерфейсе Kismet. Измените значение columns или clientcolumns в соответствии с тем, что вы хотите видеть. Полный список столбцов имеется в оперативной справке Kismet
Colors	Определяет цвета элементов изображения. Измените значение colorxxx на требуемый код цвета. Придется немного поэкспериментировать с этой настройкой, чтобы правильно подобрать цвета.

Применение Kismet Wireless

Рис. 1.

Основной экран Kismet Wireless

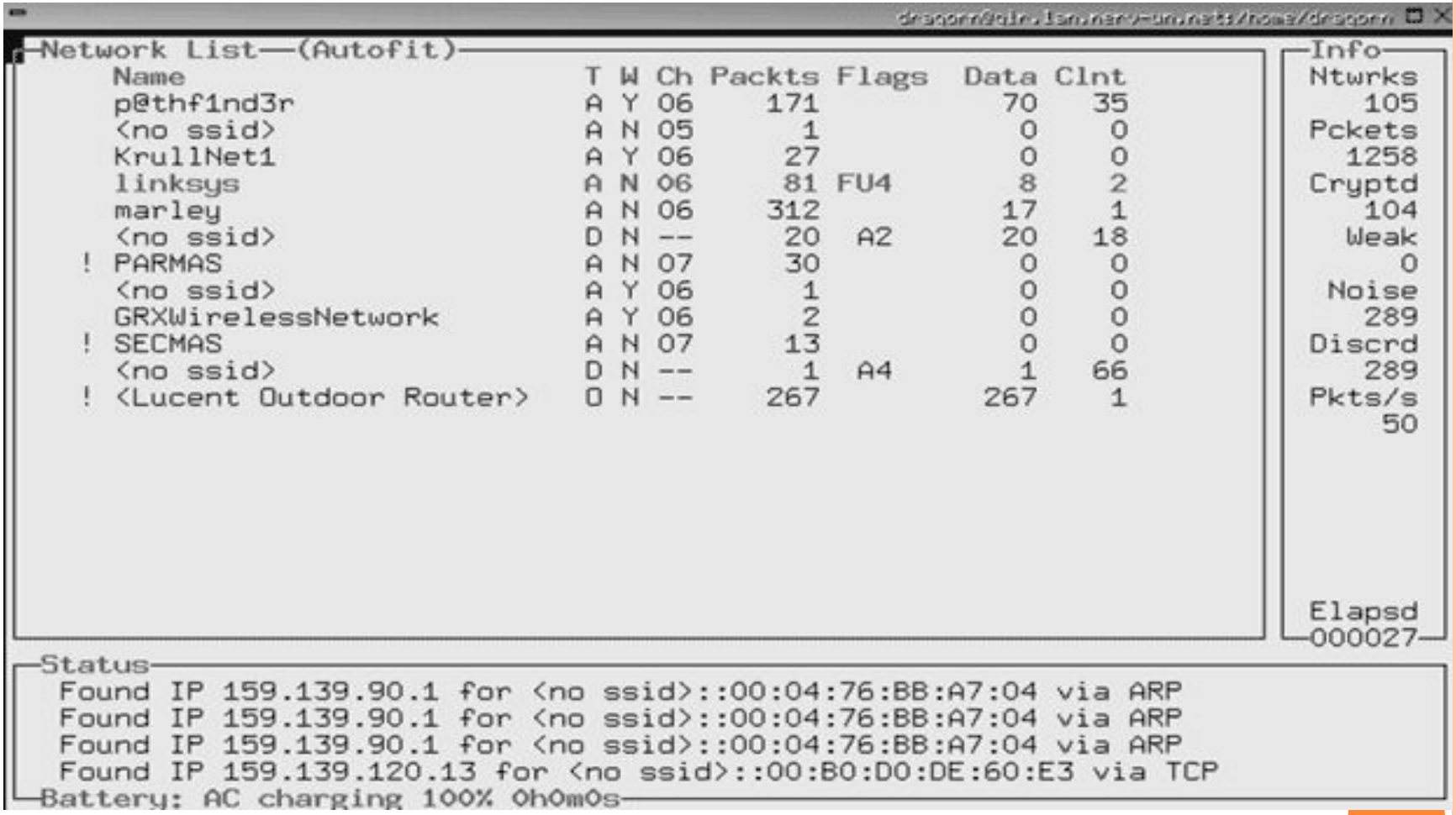


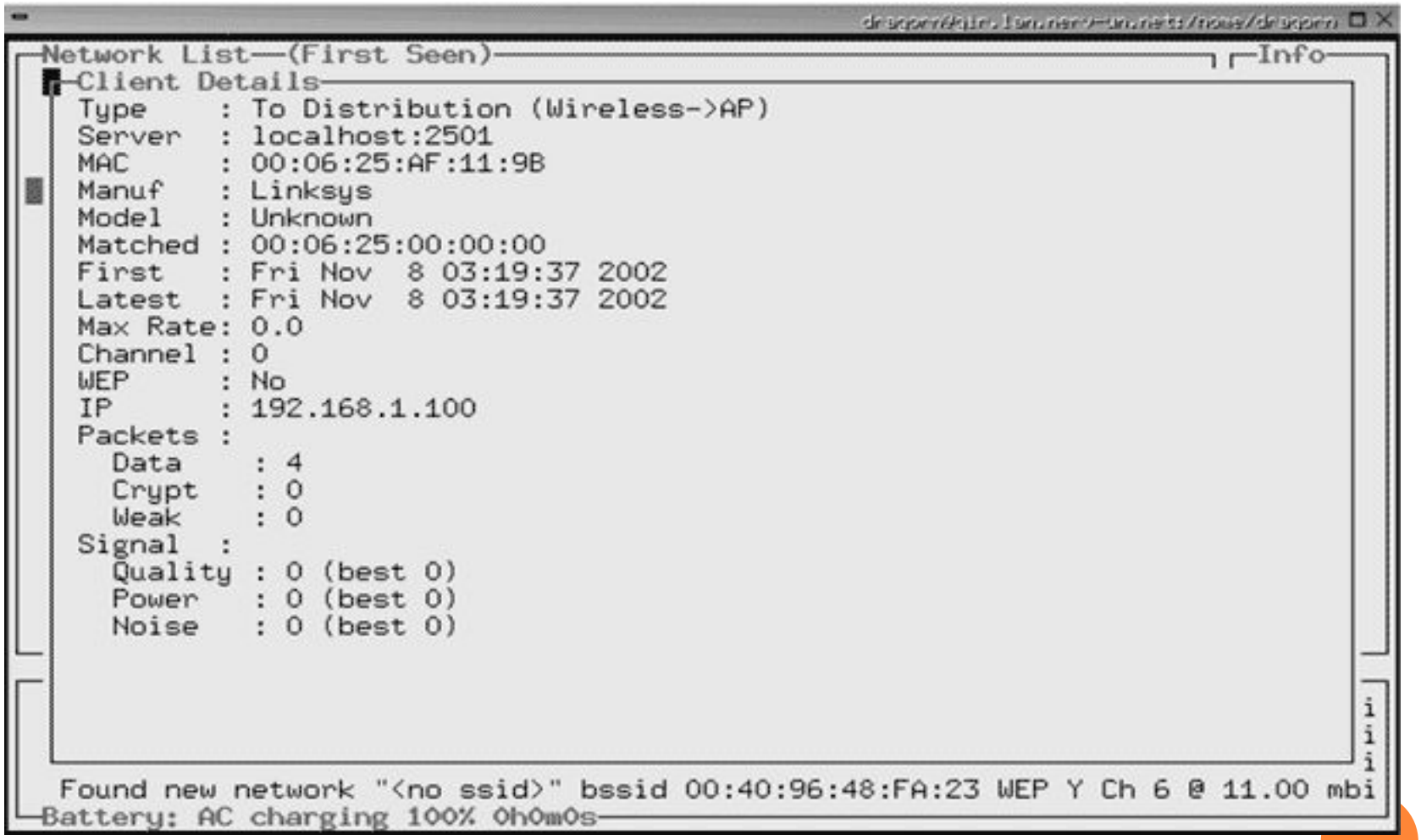
Таблица 4

Клавишные команды Kismet

Клавишная команда	**Описание**
g	Группирует помеченные в данный момент сети
h	Выдает список возможных команд
i	Выдает подробную информацию о текущей сети или группе
t	Помечает текущую сеть или снимает метку с нее
u	Исключает текущую сеть из группы
w	Выдает все предыдущие сигналы и предупреждения
z	Увеличивает панель вывода сети на весь экран (или возвращает ей нормальный размер, если она уже увеличена)

Рис. 2.

Экран Kismet с подробными данными о сети



Для достижения цели курсовой работы, были выполнены следующие задачи:

1) изучен принцип работы беспроводной сети;
2) были исследованы виды угроз и их отрицательное воздействие на работу беспроводных сетей;
3) проанализированы средства защиты информации беспроводных сетей от несанкционированного доступа;
4) проанализированы системы отслеживания вторжений и рассмотрена работа одной из них.