Документация по APS

Блокнот:	Лента
Создана:	07.04.2020 10:04
Метки:	aps
Источник:	http://z-oleg.com/secur/aps/docum.php

Документация по APS

Главное окно программы

Главное окно программы (рис. 1) содержит четыре закладки, на которых отображаются все основные данные и настройки:

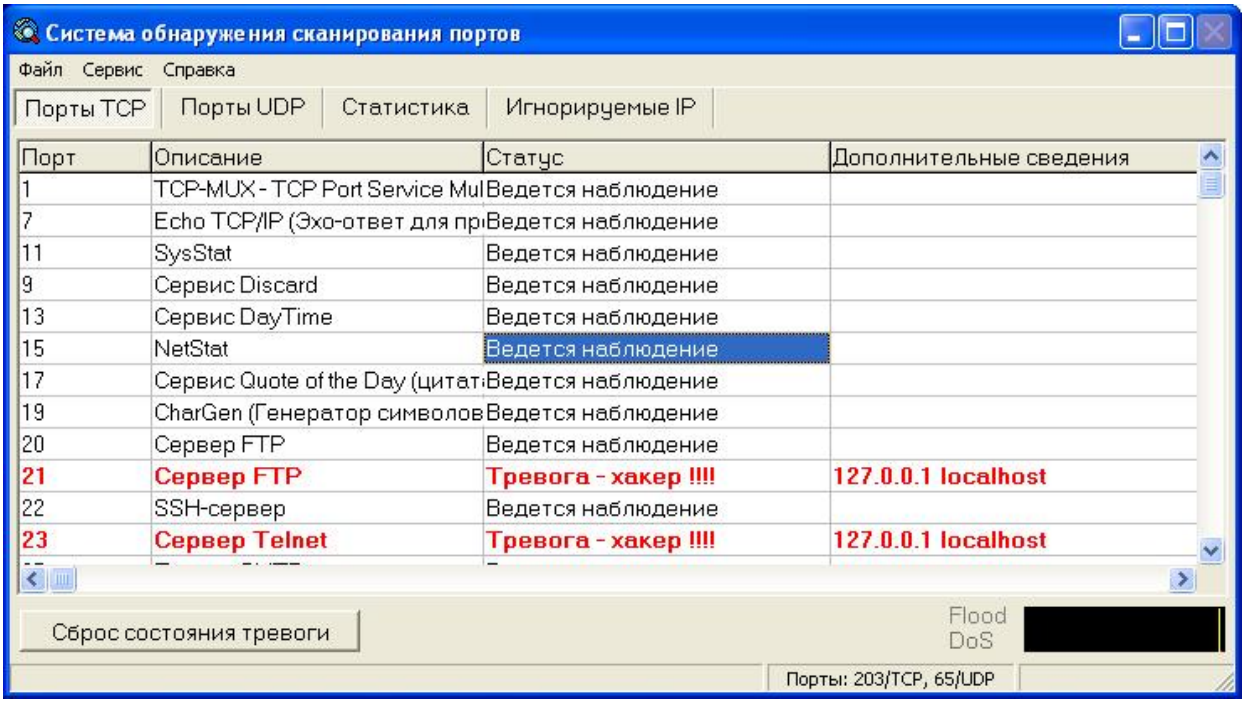

Рис. 1 Главное окно программы

- Порты TCP - таблица прослушиваемых портов TCP/IP
- Порты UDP - таблица прослушиваемых портов TCP/UDP
- Статистика - статистическая информация о зарегистрированных попытках сканирования портов
- Игнорируемые IP - список IP адресов, сканирование с которых допустимо (оно не фиксируется в протоколе и не приводит к выдаче сигналов тревоги)

Закладка "Порты TCP"

Закладка "Порты TCP" содержит список портов, прослушиваемых программой. Столбец "Порт" отображает номер порта, столбец "Описание" содержит краткое текстовое описание (но может редактироваться пользователем в файле настройки). Столбец "Описание" как правило содержит название сервиса, использующего данный порт (или название троянской программы, для которой данный порт является портом по умолчанию). Столбец "Статус" отображает статус данного порта. Возможны следующие состояния:

- Ведется наблюдение. Этот статус означает, что порт успешно открыт программой и ведется наблюдение за его состоянием;
- Порт занят другой программой. Означает, что утилите APS не удалось открыть порт (открыть порт невозможно, если он используется другой ранее запущенной программой);
- Тревога xxx !. Означает, что обнаружена попытка подключения по данному порту. На месте xxx идет формулировка события. Если в описании встречается отметка "DoS", то это означает, что по мнению программы по данному порту проведена попытка DoS атаки;

- Наблюдение запрещено. Означает, что в настройках запрещен контроль за данным портом. Программа не пытается открыть данный порт и не отслеживает его состояние. Запрещенные к использованию APS порты описываются в файле aps_dp.xml

Столбец "Дополнительная информация" содержит уточняющие данные о последней попытке сканирования данного порта. Как минимум там отображается IP адрес атакующего. Кроме того, в данном столбце отображаются дополнительные данные (доменное имя атакующего хоста и т.п.).
Столбец "Попытка" отображает количество зарегистрированных попыток сканирования данного порта с момента запуска программы или последнего сброса статистики.

Закладка "Порты UDP"

Закладка порты UDP аналогична закладке порты "TCP" за исключением того, что в столбце "Порт" кроме номера порта может отображаться буква "B" - признак того, что по данному порту фиксируется приход Broadcast пакетов.

Закладка "Статистика"

Содержит статистику по каждому из хостов, с которых зафиксированы попытки сканирования портов. Статистика ведется с момента запуска программы или с момента последнего сброса статистики. Содержит следующие столбцы:

- IP - IP адрес атакующего хоста;
- Хост - доменное имя атакующего хоста;
- Кол-во попыток - отображает текущее значение счетчика попыток сканирования портов, произведенных с данного хоста;
- Подозрения DoS - количество подозрений на атаку DoS;
- Порты - количество атакованных портов (если зафиксировано сканирование более 3-5 портов, то можно практически однозначно говорить о целенаправленном сканировании портов)

Кнопка "Сброс статистики" предназначена для сброса накопленной статистической информации (при этом таблица на закладке "Статистика" очищается). Перед сбросом статистики выдается окно с запросом о подтверждении операции.

Кнопка "Сохранение статистики" запрашивается имя файла для сохранения текстового файла с подробной статистикой.

Кнопка "Подробности по атаке" выводит на экран окно с детальным текстовым описанием статистики по текущему хосту (в статистике перечисляются все атакованные порты с указанием количества попыток сканирования и попыток DoS атак). Текстовая информация в данном окне может быть скопирована в буфер обмена.

Закладка "Игнорируемые IP"

Содержит список IP адресов, с которых допускается сканирование портов на данном ПК. При попытке сканирования портов с одного из перечисленных в списке IP адресов программа устанавливает соединение, производит имитацию сервиса и т.п., но факт сканирования не считается хакерской атакой - он не регистрируется в протоколах и статистике, не срабатывает выдача сигнала тревоги, сканирование портов не отмечается на закладках "Порты TCP" и "Порты UDP".

В список игнорирования рекомендуется занести IP адреса администраторов сети для исключения срабатывания программы.

Столбец "IP/маска" содержит IP адрес и маску (маска может отсутствовать). Маска позволяет внести в список игнорирования подсеть. При отсутствии маски сравнение адресов до полного совпадения. При заданной маске сравнение адресов идет побитно - сравниваются только биты адресов, для которых соответствующий бит маски равен "1".

Т.е. условие сравнения имеет вид:

([IP атакующего] **and** [маска] **=** [IP списка игнорирования] **and** [маска]).

Легко заметить, что маска 0.0.0.0 приведет к игнорированию сканирования портов со всех возможных адресов.

Пример: необходимо игнорировать сканирование портов с адресов 172.20.97.1 по 172.20.97.255. В этом случае задаем IP = 172.20.97.0 и маску 255.255.255.0

Под таблицей правил игнорирования находятся кнопки "Добавить", "Изменить" и "Удалить". При нажатии кнопки "Добавить" отображается окно ввода нового условия игнорирования, при нажатии кнопки "Изменить" - окно редактирования текущего условия, "Удалить" - производится удаление текущего условия после запроса подтверждения на удаление.

Все изменения в списке игнорирования немедленно сохраняются в настройках программы (файл aps_il.xml).

Настройка программы

Настройка

Настройка программы производится в диалоговом окне "Настройка", которое вызывается из пункта меню "Сервис/Настройка". Все настройки программы сгруппированы по группам в виде древовидного списка-навигатора, размещенного в левой части окна (обратите внимание, что такая организация окна настроек появилась в версии 1.70+). При нажатии кнопки "OK" диалоговое окно закрывается, все сделанные настройки вступают в действие и сохраняются в файле настроек программы aps.ini. При нажатии кнопки "Отмена" происходит закрытие окна и отмена всех сделанных в данном окне изменений.

Файлы конфигурации программы

Все настройки программа хранит в файлах, расположенных в той-же директории, что и исполняемый файл программы:

Файл	Назначение
aps.ini	Содержит все настройки программы
aps.log	Протокол работы программы. Разделителем полей протокола является знак табуляции, что упрощает анализ протокола в excel.
aps.xml	База данные с описанием портов, прослушиваемых программой. Периодически обновляется. Файл имеет формат XML
aps_usr.xml	Аналог aps.xml, но содержит порты, добавленные пользователем программы. В сущности пользователь может редактировать aps.xml, но aps.xml периодически обновляется разработчиком по мере появления новых троянских программ. Файл имеет формат XML
aps_il.xml	Настройки фильтра - содержит список хостов, сканирование портов с которых игнорируется. Файл имеет формат XML
aps_dp.xml	Настройки фильтра - содержит список портов, которые программе APS запрещено прослушивать. Файл имеет формат XML

Общие настройки

Закладка "Общие настройки"

Группа "Общие настройки" содержит общие настройки программы и интерфейса. В данной группе находится категория "Интерфейс"

Категория "Интерфейс" содержит следующие настройки:

- Переключатель "Звуковой сигнал при обнаружении атаки" - если переключатель включен, то при каждой попытке сканирования прослушиваемых программой портов выдается звуковой сигнал, записанный в файле "alarm.wav" (этот файл можно заменить своим звуковым файлом формата wav). При установке программы на сервера рекомендуется отключить звуковое оповещение.
- Переключатель "Раскрывать окно программы при обнаружении атаки" - если он включен, но при обнаружении попытки сканирования портов производится автоматическое отображение главного окна программы. Не рекомендуется при использовании программы на сервере.
- Переключатель "Автозапуск программы при старте системы" управляет автозагрузкой программы. Если переключатель включен, то при сохранении настроек в реестре создается ключ для автозапуска программы (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, значение с именем APS). При отключении переключателя ключ автозапуска удаляется в момент сохранения настроек программы
- Переключатель "Сортировка списка портов после их загрузки" включает автоматическую сортировку базы портов по номеру порта (в противном случае порты отображаются в порядке их следования в базе данных)
- Группа "Горячие клавиши" позволяет включить и настроить глобальные для системы сочетания клавиш, которые управляют APS. Рекомендуется использовать сложные сочетания (например: CTRL+ALT+SHIHT+<клавиша>) для уменьшения вероятности конфликта с другими приложениями в системе. Сочетание клавиш работает только в том случае, если перед ним установлен переключатель. В настоящий момент предусмотрено следующие настраиваемые горячие клавиши:
  - Сброс состояния тревоги. Нажатие этого сочетания клавиш аналогично нажатию на кнопку "Сброс состояния тревоги" на главном окне программы
  - Открытие/закрытие окна. Нажатие этого сочетания клавиш аналогично щелку мышью по иконке программы в Tray - если окно видимо, то оно сворачивается в Tray и наоборот.

Оповещение

Закладка "Оповещение по сети"

Закладка "Оповещение по сети" содержит настройки оповещения администраторов по сети. Оповещение по сети ведется посредством отправки сообщений на mailslot с именем "messngr" и по сути является аналогом выполнения команды NET SEND.

Содержит следующие настройки:

- Переключатель "Использовать оповещение по сети (NET SEND)" управляет включением/выключением режима оповещение по сети;
- Поле "ПК администраторов" содержит список имен компьютеров администраторов (по одному адресу в каждой строке). Следует заметить, что необходимо указывать именно NetBios имена ПК администраторов, а не их IP адреса;
- Числовое поле "Отправлять сообщения не чаще, чем один раз в xxx минут" - задает интервал между сообщениями с информацией об атаке. Первое сообщение отправляется немедленно при обнаружении атаки с каждого нового хоста. Если атака продолжается длительное время, то сообщения отправляются через заданные интервалы времени - каждое новое письмо содержит информацию на момент его отправки. Рекомендуется задавать интервал не менее 5-15 мин, в противном случае длительное сканирование портов приведет к отправке большого сообщений, что может вызвать ситуацию DoS на ПК администраторов.

- Переключатель "Отправлять сообщения для каждого события" по умолчанию выключен и его включение не рекомендуется. При его включении сообщения отправляются для каждого события сканирования портов и содержат не статистику об атакующих, а данные о каждом конкретном сканировании. Опасности данного режима состоит в том, что сканирование ПК сканером типа XSpider или аналогичных вызывает не менее 2000 событий. Отправка на каждое из них сообщения создает серьезный сетевой трафик и существенно затрудняет работу на ПК администраторов из-за получения непрерывного потока сообщений.

Кнопка "Тестировать настройку" позволяет протестировать правильность настройки отправки оповещений по сети - при нажатии на эту кнопку программа отправляет тестовое сообщение в соответствии с текущими настройками.

Закладка "Запись в SysLog"

Закладка "Запись в SysLog" содержит настройки передачи информации службе SysLog серверов. Служба SysLog используется в основном на Unix, принцип работы службы основан на прослушивании порта 514 UDP - при получении сообщении по данному порту они записываются в протокол на сервере - данная служба очень удобна для протоколирования различных событий.

Содержит следующие настройки:

- Переключатель "Использовать запись в Syslog на указанных серверах)" управляет включением/выключением режима отправки информации для службы Syslog;
- Поле "Адреса серверов" содержит список адресов серверов (по одному адресу в каждой строке). Рекомендуется указывать IP адреса серверов, а не их доменные имена;
- Числовое поле "Отправлять сообщения не чаще, чем один раз в xxx минут" - задает интервал между сообщениями с информацией об атаке. Первое сообщение отправляется немедленно при обнаружении атаки с каждого нового хоста. Если атака продолжается длительное время, то сообщения отправляются через заданные интервалы времени - каждое новое письмо содержит информацию на момент его отправки. Рекомендуется задавать интервал не менее 5-15 мин, в противном случае длительное сканирование портов приведет к отправке большого сообщений, что может вызвать ситуацию DoS на сервере или переполнению протокола Syslog.

Кнопка "Тестировать настройку" позволяет протестировать правильность настройки отправки информации для службы Syslog - при нажатии на эту кнопку программа отправляет тестовое сообщение в соответствии с текущими настройками.

Закладка "Оповещение по Email"

Закладка "Оповещение по Email" содержит настройки оповещения администраторов по электронной почте. Оповещение высылается в виде писем с информацией о атакующих в адрес одного или нескольких администраторов.

Содержит следующие настройки:

- Переключатель "Использовать оповещение по электронной почте" управляет включением/выключением режима оповещение по электронной почты;
- Поле "почтовый сервер" содержит полное имя или IP адрес почтового сервера. Рекомендуется указывать IP адрес, т.к. сканирование портов может сопровождаться атакой сервера ложными DNS ответами;
- Поле "адрес отправителя" содержит почтовый адрес, от имени которого производится передача письма с оповещением - многое почтовые сервера принимают почту только от "своих" пользователей;
- Поле "адреса администраторов" содержит список адресов администраторов (по одному адресу в каждой строке);
- Поле "заголовок письма" содержит заголовок письма. Заголовок произвольный, рекомендуется в заголовке письма указать имя или адрес сервера для упрощения сортировки писем с сообщениями программы;
- Переключатель "Детализация письма" позволяет выбрать степень детализации информации в письме. Допустимо два варианта - "Только список атакующих" и "Список атакующих + данные о портах". В первом случае в письме передается список, содержащий IP адреса атакующих и краткую статистику о ходе атаки. Во втором случае в письме передается детализированная информация по каждому из атакованных портов. Естественно, что в первом случае размер письма на 1-5 кб меньше, чем во втором;
- Числовое поле "Отправлять письма не чаще 1 раз в xxx минут" - задает интервал между письмами с информацией об атаке. Первое письмо отправляется немедленно при обнаружении атаки с каждого нового хоста. Если атака продолжается длительное время, то письма отправляются через заданные интервалы времени - каждое новое письмо содержит информацию на момент его отправки. Рекомендуется задавать интервал не менее 5-15 мин, в противном случае длительное сканирование портов приведет к отправке большого количества писем и создаст ненужную нагрузку на почтовый сервер.
- Группа параметров "Аутидентификация" позволяет настроить аутидентификацию на SMTP сервере (данная возможность появилась в версии 1.30)
    - Переключатель "Включить" предназначен для включения аутидентификации. Использование аутидентификации для сервера, не поддерживающего аутидентификацию и наоборот приведет к невозможности отправки письма
    - Текстовое поля "Имя" - имя пользователя (обратите внимание - часто в качестве имени выступает целиком почтовый адрес)
    - Текстовое поля "Пароль" - пароль пользователя. Пароль хранится в ini файле в зашифрованном виде

Кнопка "Тестировать настройку" позволяет протестировать правильность настройки отправки почтовых оповещений - при нажатии на эту кнопку программа отправляет тестовое письмо в соответствии с текущими настройками.

Отчеты

Закладка "Отчеты по Email"

Закладка "Отчеты по Email" содержит настройки системы периодической отправки отчетов о сосотоянии программы. Отправка отчетов позволяет решить ряд задач:

1. Контроль за состоянием программы APS
2. Получение статистической информации, накопленной программой

Отчет высылается в виде писем с информацией о версии загруженной базы портов и статистикой атак. Для каждого атакующего хоста программа выводит данные эжкспресс-оценки (распознается сканирование портов, флуд и атаки DoS).

Содержит следующие настройки:

- Переключатель "Передавать отчеты о состоянии по электронной почте" управляет включением/выключением режима отправки отчетов по электронной почте;
- Поле "почтовый сервер" содержит полное имя или IP адрес почтового сервера. Рекомендуется указывать IP адрес, т.к. сканирование портов может сопровождаться атакой сервера ложными DNS ответами;
- Поле "адрес отправителя" содержит почтовый адрес, от имени которого производится передача письма с оповещением - многое почтовые сервера принимают почту только от "своих" пользователей;
- Поле "адреса администраторов" содержит список адресов администраторов (по одному адресу в каждой строке);
- Поле "заголовок письма" содержит заголовок письма. Заголовок произвольный, рекомендуется в заголовке письма указать имя или адрес сервера для упрощения сортировки писем с сообщениями программы;
- Переключатель "Детализация письма" позволяет выбрать степень детализации информации в письме. Допустимо два варианта - "Только список атакующих" и "Список атакующих + данные о портах". В первом случае в письме передается список, содержащий IP адреса атакующих и краткую статистику о ходе атаки. Во втором случае в письме передается детализированная информация по каждому из атакованных портов. Естественно, что в первом случае размер письма на 1-5 кб меньше, чем во втором;
- Переключатель "Режим отправки отчета" позволяет выбрать один из двух режимов отправки отчета:
    - В заданное время - отчет передается один раз в сутки в заданное время
    - Через заданный интервал - отчет передается через заданные интервалы времени. Минимальный интервал ограничен алгоритмом программы - отчеты отправляются не чаще одного раза в 15 минут незевисимо от заданного интервала
- Группа параметров "Аутентификация" позволяет настроить аутидентификацию на SMTP сервере
    - Переключатель "Включить" предназначен для включения аутидентификации. Использование аутидентификации для сервера, не поддерживающего аутидентификацию и наоборот приведет к невозможности отправки письма
    - Текстовое поля "Имя" - имя пользователя (обратите внимание - часто в качестве имени выступает целиком почтовый адрес)
    - Текстовое поля "Пароль" - пароль пользователя. Пароль хранится в ini файле в зашифрованном виде

Кнопка "Тестировать настройку" позволяет протестировать правильность настройки отправки почтовых отчетов - при нажатии на эту кнопку программа отправляет тестовое письмо в соответствии с текущими настройками.

Следует отметить, что данный режим удобен в случае установки APS на сервере - ежедневное получение отчетов позволит администратору делать вывод о том, что программа APS запущена и работает нормально (и получать данные о накопленной статистике, что в ряде случаев удобнее немедленного почтового оповещения). Особенностью режима отправки отчета является встроенная "антиспам" защита - отчет может передаваться не чаще одного раза в 15 минут, причем первый отчет отправляется не ранее 15 минут с момента запуска программы.

Закладка "WEB интерфейс"

Закладка "WEB интерфейс" предназначена для управления встроенным WEB сервером, который позволяет дистанционно получать отчеты о состоянии APS. Встроенный WEB сервер реализует минимальный протокол HTTP с авторизацией и простейший Firewall для ограничения доступа к WEB серверу.

Содержит следующие настройки:

- Переключатель "Включить встроенный WEB сервер формирователя отчетов" позволяет включить встроенный WEB сервер.
- Поле "Порт WEB сервера" позволяет задать порт, используемый WEB сервером. Порт не должен пересекаться с портами, описанными в базе APS (в случае пересечения WEB сервер не активируется). По умолчанию используется порт 8077, но рекомендуется изменить его
- Поле "Имя" - логин пользователя для идентификации на WEB сервере
- Поле "Пароль" - пароль пользователя для идентификации на WEB сервере. Рекомендуется задавать пароли длиной не менее 4 символов
- Группа "Ограничение доступа по IP адресу" - настройки простейшего встроенного фильтра, который позволяет ограничить доступ к встроенному WEB серверу только с адресов (или подсетей), описанных в настройке.
    - Переключатель "Разрешить доступ только с перечисленных в списке IP адресов" - включает фильтр - если он выключен, то доступ возможен с любого IP. Если включен - то только с перечисленных в списке. В списке в одной строке должен указываться один IP адрес. Формат записи:
      IP - для конктретного адреса. Пример - 192.168.0.1
      IP/маска - для подсети. Пример - 192.168.0.1/255.255.255.0
      При наличии маски сравнение адресов идет побитно - сравниваются только биты, для которых в маске

соотвествеющие биты равны 1. В примере задана маска для сети класса "C".

Протоколирование

Закладка "Протоколирование"

Закладка "Протоколирование" позволяет настроить режим протоколирования. Начиная с версии 1.50 протокол размещается в подкаталоге LOG (подкаталог создается автоматически).

Содержит следующие настройки:

- Радиогруппа "Режим именования файла протокола". Позволяет выбрать один из трех возможных режимов именования протокола:
  - "Неизменное имя aps.log" - название говорит само за себя - имя файла статическое, ротации протокола нет
  - "Имя содержит год и месяц" - имя файла протокола содержит год и месяц, соответственно производится автоматическая ротация протокола (один раз в месяц)
  - "Имя содержит год, месяц и день" - имя файла протокола содержит год, месяц и день, соответственно производится автоматическая ротация протокола (один раз в день)
- Радиогруппа "Методика сохранения протокола" позволяет задать метод сохранения протокола. Поддерживается два метода:
  - Динамическое имя файла (LOG\apsYYYYMMDD.log) - все файлы протокола хранятся в папке LOG и имеют имена вида apsYYYYMMDD.log, где YYYY - текущий год, MM - текущий месяц, DD - текущий день
  - Динамический путь к файлу (LOG\YYYY\MM\DD\aps.log) - имя файла всегда aps.log, но путь к нему имеет вид YYYY\MM\DD\

Проверка необходимости ротации протокола проводится один раз в минуту, с той-же периодичностью проводится проверка существования необходимого для сохранения протокола пути (при отсутствии одной из папок, необходимых для сохранения протокола, производится ее автоматическое создание).

Я рекомендую использовать режими именования "Имя содержит год, месяц и день" и методику сохранени протокола "Динамическое имя файла (LOG\apsYYYYMMDD.log)"

Закладка "Протоколирование по IP"

Закладка "Протоколирование по IP" позволяет настроить включить и настроить ведение дополнительного протокола - протокола, в котором данные сгруппированы по IP атакующих. Этот вид протоколирования является дополнительной формой ведения протоколирования (запись в основной протокол ведется независимо от основного протокола). Протоколы с группировкой по IP атакующего формируются в папке LOG\IP, имена файлов протокола формируются из IP адресов атакующих. Папки LOG и IP создаются автоматически при необходимости.

Содержит следующие настройки:

- Переключатель "Включить протоколирование с группировкой по IP" - позволяет включить или выключить ведение протоколирования с группировкой по IP. Как говорилось выше, протоколирование по IP является дополнительной формой протокола и не влияет на ведение основного протокола
- Радиогруппа "Режим сохранения файла протокола" - позволяет настроить ротацию протокола. Возможны следующие режимы:
  - Неизменный путь LOG\IP - все протоколы хранятся в папке LOG\IP и их очистка производится вручную, ротации нет
  - Путь содержит год (LOG\IP\<год>) - протоколы группируются по году
  - Путь содержит год и месяц (LOG\IP\<год>\<месяц>) - протоколы группируются по году и месяцу
  - Путь содержит год, месяц и день (LOG\IP\<год>\<месяц>\<день>) - протоколы группируются по году, месяцу и дню

Включение ротации протокола упрощает работу с протоколами, удаление и архивирование старых протоколов.

Имитация сервисов

Закладка "Имитация TCP"

Закладка "Имитация TCP" содержит настройки системы имитации сервисов TCP. Система имитации может быть выключена, в этом случае APS не проводит активного взаимодействия с атакующим и немедленно разрывает соединение с ним. При включении системы имитации APS может передавать атакующему описанные в базе портов блоки данных (т.н. баннеры), которые содержат типовые отклики имитируемых сервисов. Кроме того, можно включить и настроить режим передачи случайных данных - наличие в ответе APS случайной информации вводит в заблуждение сканеры сетевой безопасности, затрудняет и замедляет их работу. В настройках имитации сервисов TCP можно включить режим удержания соединения - по умолчанию соединение разрывается сразу после завершения обмена с атакующим, но оно может удерживаться, что существенно замедляет работу некоторых сканеров сетевой безопасности.

Содержит следующие настройки:

- Переключатель "Включить эмуляцию сервисов TCP" - позволяет включить или выключить систему имитации сервисов TCP. Если имитация выключена, то соединение с атакующим хостом немедленно разрывается без передачи атакующему какой либо информации. Если система имитации включена, то программа передает атакующему отклик, сформированный в соответствии с настройками имитатора.

- Радиогруппа "Действия для портов, у которых в базе APS задан отклик (баннер)" - позволяет настроить действия APS при соединении атакующего с портом, для которого в базе данных заготовлен отклик сервиса. Возможны следующие варианты:
    - передать отклик - атакующему передается отклик из базы данных программы APS (эта опция включена по умолчанию);
    - передать отклик + случайные данные - атакующему передается отклик из базы данных APS, плюс блок данных переменной длинны (от 100 до 500 байт), заполненный случайными данными (бинарным мусором). Это полезный режим, т.к. некоторые сканеры проводят несколько последовательных соединений и сравнивают отклики - при их совпадении делается вывод о наличие заглушки;
    - передать случайные данные вместо отклика - отклик из базы данных игнорируется и вместо него передаются случайные данные. Включение этой опции подавляет передачу смысловых откликов сервисов из базы данных
    - не передавать отклик - передача отклика не производится.
- Радиогруппа "Действия для портов, у которых в базе APS **не** задан отклик (баннер)" - позволяет настроить действия APS при соединении атакующего с портом, для которого в базе данных заготовлен отклик сервиса. Возможны следующие варианты:
    - Не передавать ничего - при отсутствии в базе APS отклика атакующему ничего не передается (это настройка по умолчанию).
    - передать случайные текстовые данные - атакующему передается текстовая строка, заполненная случайными симовлами
    - передать случайные бинарные данные - атакующему передается буфер, заполненный случайными байтами
- Радиогруппа "Действия после обмена с атакующим" позволяет настроить действия программы после обмена с атакующим. Возможны следующие варианты:
    - разрыв соединения (рекомендуется в случае опасности Flood) - после обмена с атакующим соединение разрывается по инициативе APS. При этом (как можно заметить из названия опции) Flood менне опасен, т.к. не происходит накопление открытых соединений
    - удержание соединения - соединение удерживается открытым в течении длительного времени
    - удержание соединения с защитой от Flood - соединение удерживается открытым при отсутствии Flood и разрывается при его наличии (порог - более 60 подключений в минуту)
- Группа "Отклик с заданной вероятностью" - позволяет включить и настроить отклик с заданной вероятностью. Если переключатель "Включить режим передачи отклика с заданной вероятностью)" отключен, то отклики передаются всегда в соответствии с настройками. Если переключатель включен, то передача отклика производится с заданной при помощи регулятора вероятности (крайнее правое положение регулятора соответствует 100%, крайнее левое - 1%. Таким образом, если задать вероятность, равную скажем 75% (это значение установлено по умолчанию), то отклик будет производится примерно на 75 соединений из 100. По моим наблюдениям передача отклика с вероятностью менее 20% мало эффективна, рекомендуются значения 40-80%. Формирование отклика с заданной вероятностью вносит дополнительный фактор случайности и искажает результаты сканирования - повторные сканирования одного и того-же ПК с APS будут давать разные результаты.

Закладка "Имитация UDP"

Закладка "Имитация UDP" содержит настройки системы имитации сервисов UDP. Система имитации может быть выключена, в этом случае APS не проводит активного взаимодействия с атакующим (при этом следует отметить, что для протокола UDP соединения с атакующим естественно нет и предача отклика ведется путем передачи UDP пакета на IP адрес атакующего). При включении имитации сервисов UDP следует учитывать то, что отклик по UDP портам может применяться для организации распределенной атаки (атакующий передает на хост с APS UDP пакеты с поддельным IP адресом источника - отклики APS пойдут на этот поддельный IP, а не атакующему. Особой опасности в этом нет, но все-же пользоваться имитацией сервисов UDP в ЛВС следует с осторожностью. Для предотвращения зацикливания APS не передает отклики по UDP на адрес 127.0.0.1 и на IP, соответствующий текущему адресу компьютера (в противном случае локальное сканирование UDP портов привело бы к зацикливанию - APS принял бы собственный ответ, передал бы на него отклик и так до бесконечности).

Содержит следующие настройки:

- Переключатель "Включить эмуляцию сервисов UDP" - позволяет включить или выключить систему имитации сервисов UDP. Если имитация выключена, то атакующему не передаются ответные UDP пакеты - это состояние по умолчанию.
- Радиогруппа "Действия для портов, у которых в базе APS задан отклик (баннер)" - позволяет настроить действия APS при получении UDP пакета атакующего по порту, для которого в базе данных заготовлен отклик сервиса. Возможны следующие варианты:
    - передать отклик - атакующему передается UDP пакет с откликом из базы данных программы APS (эта опция включена по умолчанию);
    - передать отклик + случайные данные - атакующему передается отклик из базы данных APS, плюс блок данных переменной длинны (от 100 до 500 байт), заполненный случайными данными (бинарным мусором).
    - передать случайные данные вместо отклика - отклик из базы данных игнорируется и вместо него передаются случайные данные. Включение этой опции подавляет передачу смысловых откликов сервисов из базы данных
    - не передавать отклик - передача отклика не производится.
- Радиогруппа "Действия для портов, у которых в базе APS **не** задан отклик (баннер)" - позволяет настроить действия APS при получении UDP пакета атакующего по порту, для которого в базе данных нет отклика сервиса. Возможны следующие варианты:
    - Не передавать ничего - при отсутствии в базе APS отклика атакующему ничего не передается (это настройка по умолчанию).
    - передать случайные текстовые данные - атакующему передается UDP пакет, заполненный случайными символами

    - передать случайные бинарные данные - атакующему передается UDP пакет, заполненный случайными байтами
- Группа "Отклик с заданной вероятностью" - позволяет включить и настроить отклик с заданной вероятностью. Если переключатель "Включить режим передачи отклика с заданной вероятностью)" отключен, то отклики передаются всегда в соответствии с настройками. Если переключатель включен, то передача отклика производится с заданной при помощи регулятора вероятности (крайнее правое положение регулятора соответствует 100%, крайнее левое - 1%. Таким образом, если задать вероятность, равную скажем 75% (это значение установлено по умолчанию), то отклик будет производится примерно на 75 соединений из 100. По моим наблюдениям передача отклика с вероятностью менее 20% мало эффективна, рекомендуются значения 40-80%. Формирование отклика с заданной вероятностью вносит дополнительный фактор случайности и искажает результаты сканирования - повторные сканирования одного и того-же ПК с APS будут давать разные результаты.

Редактирование пользовательской базы портов

Назначение пользовательской базы

Основная база портов хранится в файле aps.xml, файл имеет XML формат и может редактироваться пользователем. Однако редактирование данной базы нежелательно, т.к. периодически выходят ее обновления и при замене файла aps.xml все изменения будут потеряны. Для устранения данной проблемы и для упрощения ввода своих портов в программе APS начиная с версии 1.35 предусмотрена база портов пользователя. Она загружается после основной, при этом пересечение баз (наличие в основной и пользовательской базе описания одного и того-же порта) не является ошибкой - основная база имеет приоритет над пользовательской.

Пользовательская база хранится в файле aps_usr.xml (формат базы aps_usr.xml польностью аналогичен формату основной базы)

Редактор базы портов

Редактор базы портов вызывается из меню "Сервис / Редактирование пользовательской базы портов". Окно редактора содержит таблицу портов со следующими столбцами:

- Порт. Номер порта (естественно, должен содержать число 1..65535). Заполнение обязательно
- Протокол. Возможны варианты "TCP" и "UDP"
- Комментарий. Текстовое описание, выводимое в таблице портов на основном окне программы
- Передаваемый текст. Содержит текст так называемого баннера. Заданная в этом поле информация передается атакующему хосту после подключения к порту. Может содержать динамические элементы

Редактирование базы производится при помощи кнопок "Добавить", "Изменить" и "Удалить" в нижней части окна.

Порты пользовательской базы данных, имеющиеся в основной выделяются красным цветом.

В передаваемом баннере возможны макросы, заменяемые в момент отправки на их значения. В настоящий момент поддерживаются следующие макросы:

- - заменяется на текущую дату, отформатированную в соответствии с настройками системы (как правило, формат DD.MM.YYYY)
- #TIME# - заменяется на текущее время, отформатированное в соответствии с настройками системы (как правило, формат HH24.MI.SS)
- #DATETIME# - заменяется на текущую дату и время, отформатированное в соответствии с настройками системы (как правило, формат DD.MM.YYYY HH24.MI.SS)
- #UNIXDATE# - дата в формате, принятом в Интернет (не зависит от локализации, пример *Mon, 24 May 2004*)
- #UNIXDATETIME# - дата и время в формате, принятом в Интернет (пример - *Mon, 24 May 2004 23:02:26*)
- #RAND_BIN# - случайные бинарные данные случайной длины (минимальная длина блока данных составляет 50 байт, максимальная - 250)
- #RAND_TXT# - случайные текстовые данные случайной длины (минимальная длина блока данных составляет 50 байт, максимальная - 250). Отличается от #RAND_BIN# тем, что состоит из байтов с кодами 32 - 127 (текст, цифры и пробелы)
- $xx - байт, xx - значение в шеснадцатиричном формате (для символов с кодами 0 - 9 обязателен предшествующий ноль, т.е. $00, $01 ...). Применяется для ввода в передаваемый текст бинарных данных, применяется в первую очередь для передачи символов перевода строки и перевода каретки ($0D и $0A)

Параметры , #TIME#, #DATETIME#, #UNIXDATE#, #UNIXDATETIME# применяются для придания ответам APS реалистичности (многие современные сканеры имеют некий интеллект и сразу понимают, что вместо сервиса стоит заглушка - это достигается сравнением баннеров, полученных в результате нескольких подключений к порту. Параметры #RAND_BIN# и #RAND_TXT# существенно затрудняют работу интеллектуального сканера, т.к. он пытается анализировать полученные данные

Закладка "Оповещение по Email"

Закладка "Оповещение по Email" содержит настройки оповещения администраторов по электронной почте. Оповещение высылается в виде писем с информацией о атакующих в адрес одного или нескольких администраторов.

Содержит следующие настройки:

- Переключатель "Использовать оповещение по электронной почте" управляет включением/выключением режима оповещение по электронной почты;

- Поле "почтовый сервер" содержит полное имя или IP адрес почтового сервера. Рекомендуется указывать IP адрес, т.к. сканирование портов может сопровождаться атакой сервера ложными DNS ответами;
- Поле "адрес отправителя" содержит почтовый адрес, от имени которого производится передача письма с оповещением - многое почтовые сервера принимают почту только от "своих" пользователей;
- Поле "адреса администраторов" содержит список адресов администраторов (по одному адресу в каждой строке);
- Поле "заголовок письма" содержит заголовок письма. Заголовок произвольный, рекомендуется в заголовке письма указать имя или адрес сервера для упрощения сортировки писем с сообщениями программы;
- Переключатель "Детализация письма" позволяет выбрать степень детализации информации в письме. Допустимо два варианта - "Только список атакующих" и "Список атакующих + данные о портах". В первом случае в письме передается список, содержащий IP адреса атакующих и краткую статистику о ходе атаки. Во втором случае в письме передается детализированная информация по каждому из атакованных портов. Естественно, что в порвом случае размер письма на 1-5 кб меньше, чем во втором;
- Числовое поле "Отправлять письма не чаще 1 раз в xxx минут" - задает интервал между письмами с информацией об атаке. Первое письмо отправляется немедленно при обнаружении атаки с каждого нового хоста. Если атака продолжается длительное время, то письма отправляются через заданные интервалы времени - каждое новое письмо содержит информацию на момент его отправки. Рекомендуется задавать интервал не менее 5-15 мин, в противном случае длительное сканирование портов приведет к отправке большого количества писем и создаст ненужную нагрузку на почтовый сервер.
- Группа параметров "Аутидентификация" позволяет настроить аутидентификацию на SMTP сервере (данная возможность появилась в версии 1.30)
    - Переключатель "Включить" предназначен для включения аутидентификации. Использование аутидентификации для сервера, не поддерживающего аутидентификацию и наоборот приведет к невозможности отправки письма
    - Текстовое поля "Имя" - имя пользователя (обратите внимание - часто в качестве имени выступает целиком почтовый адрес)
    - Текстовое поля "Пароль" - пароль пользователя. Пароль хранится в ini файле в зашифрованном виде

Кнопка "Тестировать настройку" позволяет протестировать правильность настройки отправки почтовых оповещений - при нажатии на эту кнопку программа отправляет тестовое письмо в соответствии с текущими настройками.

Создание шаблонов для очетов по EMail

Назначение шабловнов

Шаблоны отчетов по email позволяют пользователю отконфигурировать формат и содержание письма, отправляемого программой APS. Это может быть актуально в ряде типовых случаев:

- Письмо отправляется администратору через SMS шлюз на мобильный телефон - необходимо передавать минимум информации (размер SMS ограничен и для пинимания сущности проблемы достаточно сокращенной информации)
- Письмо обрабатывается не человеком, а некоторой программой или скриптом - в этом случае данные можно представить в виде, удобном для парсига и анализа

Возможность подключения шаблонов появилась начиная с версии 1.90

Формат шаблона

Шаблон хранится в текстовом файле с расширением etf в папке template и имеет следующий формат:

```
[Info]
Name=название шаблона

[Header]
 ...
[Footer]
 ...
[HackerInfo]
 ...
[HackerPortInfo]
...
```

Шаблон содержит несколько секций, причем наличие секции [Info] обязательно.

Секция Info
Секция Info должна содержать обязательный параметр Name=<название шаблона>. Этот параметр задает имя, под которым шаблон отображается в окне настроек. Кроме имени можно указать параметр MaxRecCount, который задает максимальное количество записей, выводимых в письмо (по умолчанию выводятся все доступные записи об атакующих)

Секции Header и Footer
Секции Header и Footer содержат данные, однократно выводимые в начале письма (Header) и в конце письма (Footer). В этих секциях кроме произвольного текста допустимы макросы, заменяемые в момент генерации письма значениями (эти макросы допустимы в любой секции):

- #VERSION# - Версия программы APS (пример - *1.90*)
- #DB_VERSION# - Дата обновления и версия базы портов (пример - *1.30 от 16.08.2004*)

- - Дата формирования письма
- #TIME# - Время формирования письма
- #LOCAL_IP# - IP адрес компьютера, на котором сработал APS
- #LOCAL_HOST# - имя компьютера, на котором сработал APS

Важно отметить, что макросы секции Header и Footer поддерживаются во всех остальных секциях (что полезно при формировании отчета в виде таблицы или XML файла)

Секция HackerInfo
Секция HackerInfo содержит шаблон, по которому формируются данные по кождому из атакующих хостов. В этой секции допустимы макросы, заменяемые в момент генерации письма значениями:

- #HACKER_IP# - IP адрес атакующего компьютера
- #HACKER_HOST# - Имя хоста для атакующего IP (не всегда доступно)
- #ATTACK_START_DATE# - Дата начала атаки (т.е. первой попытки соединения с APS)
- #ATTACK_START_TIME# - Время начала атаки
- #ATTACK_END_DATE# - Дата завершения атаки (т.е. последней попытки соединения с APS)
- #ATTACK_END_TIME# - Время завершения атаки
- #ATTACK_COUNT# - Количество атак (т.е. суммарное количество попыток соединения по TCP и пакетов UDP)
- #ATTACK_DOS_COUNT# - Количество подозрений DOS
- #ATTACK_PORT_COUNT# - Количество атакованных портов
- #ATTACK_PORT_COUNT# - Количество атакованных портов
- #ATTACK_PORT_DETAIL# - Детализированные данные о портах (формат и содержимое детализированных данных определяется секцией [HackerPortInfo]
- #ATTACK_EXPRESS_TEST# - Результаты экспресс-оценки (есть ли DoS, Flood, сканирование - выводится в текстовом виде в три строки)

Секция HackerPortInfo
Секция HackerInfo содержит шаблон, по которому формируются данные по кождому из атакованных портов. В этой секции допустимы макросы, заменяемые в момент генерации письма значениями:

- #HACKER_IP# - IP адрес атакующего компьютера
- #HACKER_HOST# - Имя хоста для атакующего IP (не всегда доступно)
- #PORT_NUM# - Номер порта
- #PORT_PROTO# - Протокол (TCP или UDP)
- #PORT_ATTACK_COUNT# - Количество атак по данному порту
- #PORT_DOS_COUNT# - Количество подозрений DOS по данному порту
- #PORT_DATA_SIZE# - Объем данных, полученных по данному порту от атакующего
- #PORT_FLOOD_INFO# - Признак флуда в текстовом виде

Примеры шаблонов

Примеры шаблонов

Расссмотрим несколько типовых примеров шаблонов:

1. Типовой шаблон, формирующий письмо, похожее на стандартной письмо APS

```
[Info]
Name=Типовой шаблон письма

[Header]
Почтовое оповещение программы APS, сформировано  в #TIME#
Версия программы APS: #VERSION#, база портов #DB_VERSION#

[Footer]

[HackerPortInfo]
 #PORT_NUM#/#PORT_PROTO# - количество атак:#PORT_ATTACK_COUNT#, Dos: #PORT_DOS_COUNT#, объем: #PORT_DATA_SIZE#

[HackerInfo]
 Атакующий хост: #HACKER_IP# #HACKER_HOST#
 Дата и время начала атаки: #ATTACK_START_DATE# #ATTACK_START_TIME#
 Дата и время последнего сканирования: #ATTACK_END_DATE# #ATTACK_END_TIME#
 кол-во сканирований:      #ATTACK_COUNT#
 кол-во подозрений на DoS: #ATTACK_DOS_COUNT#
 Атаковано портов: #ATTACK_PORT_COUNT#, подробности:
 #ATTACK_PORT_DETAIL#
 #ATTACK_EXPRESS_TEST#
 --------------------------------
```

2. Типовой шаблон, формирующий отчет в формате XML

```
[Info]
Name=Шаблон письма с XML документом

[Header]




[Footer]


[HackerPortInfo]


[HackerInfo]

 #ATTACK_PORT_DETAIL#
```

3. Типовой шаблон, формирующий минимальный по объему отчет для отправки по SMS

```
[Info]
Name=Типовой шаблон SMS

[HackerInfo]
 #HACKER_IP# #HACKER_HOST#: #ATTACK_COUNT#/#ATTACK_DOS_COUNT#/#ATTACK_PORT_COUNT#
 -
```

4. Типовой шаблон, формирующий таблицу CSV формата для анализа в Excel

```
Name=Типовой шаблон письма в формате SMS

[HackerPortInfo]
#HACKER_IP#;#HACKER_HOST#;#PORT_NUM#;#PORT_PROTO#;#PORT_ATTACK_COUNT#;#PORT_DOS_COUNT#;#PORT_DATA_SIZE#

[HackerInfo]
#ATTACK_PORT_DETAIL#
```