Часто задаваемые вопросы (FAQ)

Блокнот:	Лента		
Создана:	07.04.2020 10:05	**Изменена:**	22.04.2020 8:29
Метки:	aps		
Источник:	http://z-oleg.com/secur/aps/faq.php		

Часто задаваемые вопросы (FAQ)

Может ли утилита APS заменить Firewall ?

Нет. Утилита предназначена для обнаружения факта подключения к защищаемым портам, а не для защиты имеющихся сервисов за счет фильтрации трафика в соответствии с заданными в настройке правилами. Более того, одно из основных предназначений APS состоит в тестировании работы Firewall

Как необходимо настроить Firewall при работе с APS ?

При использовании APS в качестве утилиты контроля за работой Firewall никаких особенностей нет - APS просто запускается на защищаемом ПК (при этом на Firewall **не нужно** вносить правила, затрагивающие APS).

Обменивается ли утилита APS с сетью ?

По умолчанию - нет. Утилита не загружает из сети никакой информации и ничего не передает в сеть. Однако сам пользователь может настроить оповещение о сканировании сети по электронной почте, по сети или при помощи службы SysLog. В этом случае программа передает данные в сеть и для успешной передачи необходимо внести в Firewall ряд настроек:

- Оповещение по Email - для работы оповещения по Email необходимо на Firewall разрешить программе APS обмениваться с указанным в настройке сервером электронной почты по порту 25 (SMTP)
- Оповещение по сети - ведется по порту 137, необходимо разрешить соединения с компьютерами, перечисленными в настройке
- Протоколирование с использованием SysLog - запись в Syslog ведется при помощи передачи пакетов по порту 514 UDP на сервера, перечисленные в настройке программы

Для упрощения настройки Firewall на совместную работу с APS в настроках есть кнопки "Тестировать настроку" - нажатие на эту кнопку

настроках есть кнопки "Тестировать настроку" - нажатие на эту кнопку производит передачу тестового письма (или тестового сообщения), что позволяет настраивать Firewall в режиме обучения.

Ошибка при передаче сообщения не влияет на работу программы - подобные ошибки игнорируются

Относится ли APS к категории "Honeypot"

Да, несомненно. Это одно из основных предназначений этой программы. Именно для этого в APS предусмотрены достаточно развитые средства протоколирования и оповещения администратора

Что такое Honeypot ?

Honeypot - это программа (сервис, система, компьютер), задачей которого является "принять удар на себя", т.е. Honeypot - это специально подготовленный для взлома компьютер. В буквальном переводе Honeypot = "горшок с медом". Встречаются альтернативные термины, имеющие аналогичное значение, например "обманные системы" (deception toolkit). Лично я в шутку называю такие системы "мышеловка".

В различной литературе под понятием honeypot (honeypots) понимают различные вещи: некоторые подразумевают под ним программу типа APS, которая имитирует (эмулирует) уязвимые сервисы и провоцирует атаки на них; другие подразумевают под honeypot реальную систему в целом, специально предназначенную для взлома и последующего изучения причин и последсвий взлома. Мне лично нравится определение "Honeypot – это средство безопасности, значение которого состоит в подверженности его сканированиям, атакам и взломам"

Конфликт APS и программы X из-за порта NNN

Некая программа X использует порт с NNN. Этот же порт есть в базе APS и после запуска APS программа X не может работать. Как быть ? У проблемы есть как минимум два решения:

1. Настроить программу X на использование другого порта - если порт находится в базе APS, то это означает, что он достаточно хорошо известен как порт некоторого сервиса или программы. Присвоение нестандартного номера порта в ряде случаев очень полезно, например для прокси-серверов. По умолчанию атакующий ищет в сети прокси по портам 3128 или 8080. В таком случае лучше присвоить прокси-серверу некий нестандартный порт (например 13128), а на стандартном оставить APS
2. Выключить мониторинг порта в APS и устанить тем самым конфликт. Отключение и включение ведется в меню, вызываемом при нажатии правой кнопки над таблицей портов. Информация об отключенных портах запоминается в файле aps_dp.xml

Что делать, если APS выдает сигнал тревоги ?

Если APS выдает сигнал тревоги, то интерпретация этого события зависит от условий применения APS:

- APS применяется для контроля за работой Firewall (т.е. в правилах персонального Firewall программе APS не разрешено работать с сетью). В этом случае сигнал тревоги свидетельствует о том, что кто-то пытается атаковать Ваш компьютер и Firewall по каким-то причинам не выполняет своих функций. Это очень опасно, т.к. при работающем Firewall сканирование портов и подключение к прослушиваемым программой APS портам должно быть невозможно. При возникновании подобной ситуации необходимо:
    1. Проверить, не разрешена ли работа программы APS с сетью. Если разрешена, то работу APS с сетью необходимо запретить (иначе APS не сможет выступать в роли тестера работы Firewall);
    2. Проверить, запущен ли Firewall. Многие сетевые вирусы (черви, троянские программы) могут обнаруживать процессы Firewall и останавливать их. Если после запуска работа Firewall внезапно прерывается, то это может быть сигналом о наличии на Вашем ПК вируса;
    3. Проверить настройки Firewall - возможно, он работает с настройками "по умолчанию" или неправильно настроен.
- APS применяется в качестве Honeypot (сетевой ловушки, открытой для взлома). В этом случае программе APS должно быть разрешено работать с сетью. Срабатывание APS сигнализирует о том, что кто-то проявил интерес в ПК, на котором сработал APS. Подробнее об анализе атаки с помощью APS можно прочитать в разделе Анализ атак по данным APS

Мой антивирус/Firewall X говорит о том, что APS возможно является Trojan/Backdoor - что это значит ?

Это значит, что у Вас на компьютере установлен антивирус (Firewall, антитроянская система ...) с действующим эвристическим механизмом. Дело в том, что APS прослушивает множество портов, присущих известным троянским и Backdoor программам и (в некоторых случаях) даже пытается имитировать ответы этих программ для введения атакующего (и его сканеров) в заблуждение - это одно из основных назначений APS. Естественно, никаких троянских функций у APS нет - он просто имитирует наличие трояна для сканера атакующего.