Утилита APS

Блокнот:	Лента		
Создана:	07.04.2020 9:55	**Изменена:**	22.04.2020 8:28
Метки:	aps		
Источник:	http://z-oleg.com/secur/aps/index.php		

Утилита APS

Данный раздел посвящен программе APS. APS расшифровывается как **A**nti **P**ort **S**canner. Основное назначение утилиты состоит в прослушивании нескольких сотен портов (описанных в обновляемой базе данных программы), имитации наличия на них уязвимых сервисов и анализа всех подключений по этим портам.

Назначение утилиты и решаемые задачи

Основным назначением данной программы является обнаружение хакерских атак. Как известно, первой фазой большинства хакерских атак является инвентаризация сети и сканирование портов на обнаруженных хостах. Сканирование портов помогает произвести определение типа операционной системы и обнаружить потенциально уязвимые сервисы (например, почту или WEB-сервер). После сканирования портов многие сканеры производят определение типа сервиса путем передачи тестовых запросов и анализа ответа сервера. Утилита APS проводит обмен с атакующим и позволяет однозначно идентифицировать факт атаки. Кроме этого, назначением утилита предназначена:

- Для обнаружения разного рода атак (в первую очередь сканирования портов и идентификации сервисов) и появления в сети троянских программ и сетевых червей (в базе APS более сотни портов, используемых червями и Backdoor - компонентами)
- Для тестирования сканеров портов и сетевой безопасности. Для проверки работы сканера необходимо запустить на тестовом компьютере APS и провести сканирование портов - по протоколам APS нетрудно установить, какие проверки провидит сканер и в какой последовательности
- Для тестирования и оперативного контроля за работой Firewall. В этом случае утилита APS запускается на компьютере с установленным Firewall и проводится сканирование портов и (или иные атаки) против ПК. Если APS выдает сигнал тревоги, то это является сигналом о неработоспособности Firewall или о его

неправильной настройке. APS может быть постоянно запущен за защищенном при помощи Firewall компьютере для контроля за исправным функционирование Firewall в реальном времени
- Блокирования работы сетевых червей и Backdoor модулей и их обнаружение - принцип обнаружения и блокирования основан на том, что один и тот-же порт может быть открыт на прослушивание только один раз. Следовательно, открытие портов, используемых троянскими и Backdoor программами до их запуска помешает их работе, после запуска - приведет к обнаружению факта использования порта другой программой
- Тестирования антитроянских и антивирусных программ, систем IDS - в базе APS заложено более сотни портов наиболее распространенных троянских программ. Некоторые антитроянских средства обладают способностью проводить сканирование портов проверяемого ПК (или строить список прослушиваемых портов без сканирования при помощи API Windows) - такие средства должны сообщать о подозрении на наличие троянских программы (с выводом списка "подозрительных" портов) - полученный список легко сравнить со списком портов в базе APS и сделать выводы о надежность применяемого средства

Основным достоинством программы является малое потребление ресурсов - программа не нагружает процессор и практически не использует системные ресурсы. Это связано с тем, что программа открывает описанные в базе данных порты и уходит в ждущий режим, выходя из него только в моменты обращения к прослушиваемым портам (это отличает ее от Firewall, который анализирует каждый приходящий и уходящий пакет).

Утилита для обнаружения сканирования портов предназначена для решения задач:

- Обнаружения факта сканирования портов (TCP, UDP) и рассылки UDP broadcast пакетов для заданных портов. Список прослушиваемых портов задан в базе данных формата XML. При установлении соединения программа может имитировать ответ сервера (передаваемые в качестве ответа данные хранятся в базе данных настроек). Программа содержит настраиваемый фильтр, который позволяет игнорировать попытки сканирования портов с заданных хостов или сетей;
- Ведения протоколирования попыток сканирования портов (текстовый протокол, разделитель полей - табуляция);
- Передачи оповещения администраторам при помощи электронной почты или NET SEND. Администратор может настраивать периодичность и состав передаваемой в письме информации;
- Передачи данных о попытках сканирования портов службе SysLog на заданных серверах;
- Ведения детализированной статистики процесса сканирования

портов для каждого хоста и порта. Статистика может просматриваться в реальном времени или экспортироваться в текстовый файл;
- Обнаружения попыток атак DoS (отказ в обслуживании) на прослушиваемые порты;
- Блокирования работы описанных в базе настроек троянских программ (использование прослушиваемых программой портов другими приложениями невозможно);

Программа не модифицирует системные настройки и реестр, поэтому не нуждается в инсталляции и деинсталляции. Программа может запускаться из любой папки.
Во время работы программа создает иконку в tray, при обнаружении сканирования портов включается анимация иконки, выдается звуковой сигнал, возможен автоматический вывод на экран главного окна программы (реакция программы определяется настройками). Настройки программы хранятся в INI файле aps.ini - поэтому можно настроить программу и копировать ее вместе с настройками.

Принципы работы

Принцип работы программы основан на прослушивании портов, описанных в базе данных. База данных портов обновляется и если Вам известен порт, используемый троянской или Backdoor программой, присылайте его мне - я добавлю его в базу данных. База данных содержит краткое описание каждого порта - краткие описания содержат или названия использующих порт вирусов, или название стандартного сервиса, которому этот порт соответствует. При обнаружении попытки подключения к прослушиваемому порту программа фиксирует факт подключения в протоколе, анализирует полученные после подключения данные и для некоторых сервисов передает так называемый баннер - некоторый набор текстовых или бинарных данных,передаваемых реальным сервисом после подключения.