УДК:004.4

Автоматический анализатор блокировки сетевых пакетов SNORT

Выполнил: Доманов А.О. группа 11-ИБ

Snort является свободно распространяемой программой с открытым исходным кодом под лицензией GPL. Snort создан одним из известнейших людей в мире информационной безопасности, автором многих книг Мартином Рошем в 1998 году. Основной причиной создания этой IDS было отсутствие на тот момент достаточно эффективного, тем более бесплатного, инструмента оповещения об атаках.

Snort является самой распространенной IDS в мире, во многом благодаря ее открытости и великолепной работе авторов.

В Snort происходит разработка, распространение и поддержка одноименной сетевой системы обнаружения вторжений, предназначенной для мониторинга небольших сетей. Система Snort распространяется свободно в исходных текстах или в откомпилированном двоичном формате при условии соблюдения лицензии GNU GPL (General Public License).

Snort позволяет в режиме реального времени анализировать сетевой трафик, проверяя корректность структуры сетевых пакетов и соответствие содержимого определенным правилам. Для описания сетевых инцидентов и определения реакции системы используется гибкий язык сценариев. Встроенная база знаний позволяет определить распространенные типы сетевых нападений: «скрытое» сканирование (использующее установленные в сетевых пакетах флаги FIN, ASK), сбор баннеров сетевых сервисов (Services & OS fingerprinting), переполнение буфера различных сервисов, атаки, использующие преднамеренное нарушение структуры сетевых пакетов (ping of death), атаки вида «отказ

в обслуживании» (DOS). Включено описание множества атак, эксплуатирующих определенные «дыры» в различных сетевых сервисах.

При фиксировании системой Snort описанного сетевого инцидента можно, конфигурируя брандмауэр, предотвратить сетевую атаку или передать предупреждающее сообщение через syslog-сервер, определенный пользовательский файл, Unix-сокет или службу Windows WinPopup.

Snort выявляет следующее:

- Плохой трафик
- Использование эксплоитов (выявление Shellcode)
- Сканирование системы (порты, ОС, пользователи и т.д.)
- Атаки на такие службы как Telnet, FTP, DNS, и т.д.
- Атаки DoS/DDoS
- Атаки связанные с Web серверами (cgi, php, frontpage, iss и т.д.)
- Атаки на базы данных SQL, Oracle и т.д.
- Атаки по протоколам SNMP, NetBios, ICMP
- Атаки на SMTP, imap, pop2, pop3
- Различные Backdoors
- Web-фильтры (порнография)
- Вирусы

А если еще учесть

- Возможность написания собственных правил
- Расширение функциональности, используя возможность подключения модулей

Гибкую систему оповещения об атаках (Log файлы, устройства вывода, БД и.д.) то мы получаем мощнейшую систему, которая действительно является одним из лучших инструментов в борьбе против злоумышленников.

Snort поддерживает следующие интерфейсы для прослушивания:

- Ethernet

- SLIP

- PPP

IDS Snort может работать на многих операционных системах :Linux, Windows, IRIX, SunOS, *BSD и др. Настройка на всех платформах одинакова.

Так же отличное расширение функциональности для Snort под названием inline, который позволяет связать firewall с действиями правил. К примеру, можно передать firewall IP адрес того хоста, с которого пришел подозрительный пакет, и дать команду игнорировать весь трафик с этого IP.

Это применяется при DDoS атаках.

Но существует и обратная сторона, когда злоумышленник поймет как происходит блокирование и воспользуется этим.

Поэтому специалисты по безопасности крайне не рекомендуют реализовывать данную возможность или же использовать ее только в исключительных случаях. Лучше устанавливать Snort сразуна двух машинах до и после - это обеспечит максимальную надежность получения нужной информации.

Опции в командной строке имеют более высокий приоритет, чем snort.conf.

Написание собственных правил - не сложное занятие, а часто даже необходимое, так как ежедневно обнаруживаются уязвимости, а вместе с ними появляются и программы эксплуатирующие программное обеспечение.

Протоколы:TCP, UDP, IP, ICMP. Разработчики обещают в скором времени сделать поддержку следующих протоколов: IPX, ARP, IGRP, GRE, RIP, OSPF.

Далее следуют два IP адреса. Первый, как правило, с которого приходит пакет, а второй, на какой пакет отсылается. Но это не обязательно, так как между двумя адресами можно использовать так

называемый оператор направления "->", "<>" (двустороннее), который подобно стрелкам указывает направление передачи. Важно отметить отсутствие оператора "<-".

Поскольку Snort не имеет встроенного механизма получения IP адреса, используя доменное имя.

После IP адреса указывается номер порта, с которого отсылаются данные и на который приходит информация.

Можно указать диапазон портов: 1:1024 (все порты в диапазоне от 1 до 1024 включая 1 и 1024). Часто используется оператор отрицания "!" (Например: !123:321 исключает все порты в диапазоне от 123 до 321). Если опущен один из параметров диапазона (:321 или 123:), то пропускаемый параметр принимает крайнее значение общего количества портов, то есть 0 или 65535.

Список литературы:

1.IDS Snort [Электронный ресурс]: (с изменениями и дополнениями) — Режим доступа: http://www.opennet.ru/base/sec/snort_ids.txt.html (дата обращения 21.10.2012).

2.Snort [Электронный ресурс]: (с изменениями и дополнениями) - Режим доступа: http://www.osp.ru/win2000/2004/05/177049/ (дата обращения 21.10.2012).

3.Snort [Электронный ресурс]: (с изменениями и дополнениями) - Режим доступа: http://ru.wikipedia.org/wiki/Snort (дата обращения 22.10.2012).