ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 621.189.28

NGFW xFirewall КАК СРЕДСТВО ЗАЩИТЫ СЕТЕВОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ

М.Ф. Никульченко, А.С. Исмагилова
ФГБОУ Башкирский Государственный Университет, г. Уфа

Ключевые слова: пак, ngfw, xfirewall.

Важнейшим условием защиты сетевой инфраструктуры предприятия является правильная оценка угроз, их конкретный перечень и меры по закрытию их. Большинство актуальных угроз безопасности информации и векторов атак на сетевую инфраструктуру среднего и крупного бизнеса перекрывают современные NGFW (Next-Generation Firewall) в сочетании с правильно подобранными SIEM агрегаторами событий ИБ [1].

Целью настоящей работы является демонстрация одной из возможностей ПАК xFirewall-VA, а именно отражение сетевой атаки.

Для реализации поставленной задачи был создан стенд на базе платформы виртуализации VMWare Workstation (рисунок 1).

Атакуемый – персональная ЭВМ на базе MS Windows 7 x64;
NGWF xFirewall – межсетевой экран следующего поколения от компании «Инфотекс»;
Атакующий – персональная ЭВМ на базе Debian Linux

Рисунок 1 – Стенд для демонстрации возможностей по отражению сетевой атаки

Одной из важных функций NGFW является разграничение внутренней и внешней сети. Как правило, атакующие видят именно внешний интерфейс. На него чаще приходятся попытки сканирования, проверки на уязвимости служб запущенных на ПАК и т.д. За противодействие атакам извне отвечает IPS (система предотвращения атак) на базе свободного ПО

snort. Она содержит в себе некоторую базу сигнатур, которые путем сравнения и поиска в проходящем через интерфейсы трафике данная система пытается вычленить и заблокировать. На примере работы некоторой такой уязвимости продемонстрируем возможности данного NGFW.

С атакующего хоста путем использования ПО Metasploit запускаем зловредные пакеты, как на рисунке 2:

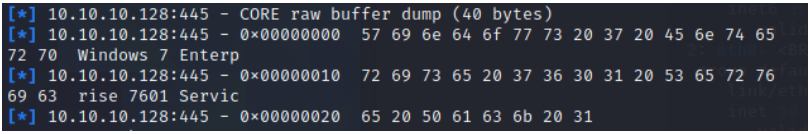

Рисунок 2 – Зловредная последовательность байт в пакете

На ЭВМ атакуемого запускаем ПО для анализа трафика Wireshark (рисунок 3), фильтруем вывод по протоколу SMB и после анализа пакетов удостоверяемся, что соединение установить не удалось.

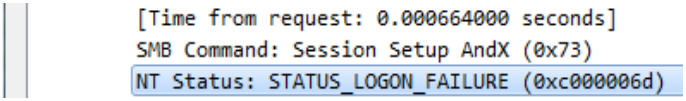

Рисунок 3 – Анализ дампа трафика

Далее удостоверяемся в том, что на xFirewall данные об атаке, IP-адресах, портах, названии эксплоита и его сигнатурах отобразились корректно (рисунок 4).

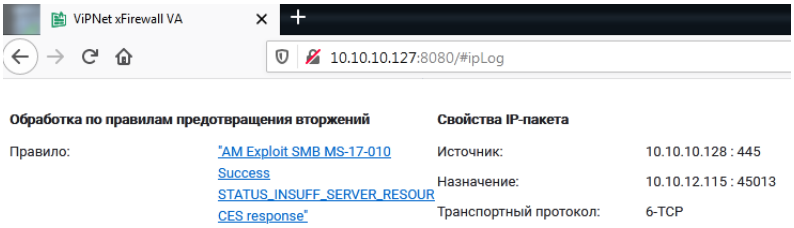

Рисунок 4 – Факт перехвата системой IPS зловредного пакета

Встраивание в действующую инфраструктуру данного решения позволяет сократить до приемлемого минимума любые известные и потенциальные риски кибербезопасности, в том числе атаки, организуемые известными APT-группировками.

Список использованных источников
1. Никульченко М.Ф., Исмагилова А.С. Анализ защищенности и обнаружения атак с помощью уязвимости протокола SMB // Защита информации. Инсайд. 2020. № 5 (95). С. 52-56.

Никульченко Максим Филиппович, аспирант ФГБОУ ВО «Башкирский государственный университет», E-mail: RQWZ@protonmail.com
Исмагилова Альбина Сабирьяновна, доктор физико-математических наук, доцент, заведующий кафедрой управления информационной безопасностью ФГБОУ ВО «Башкирский государственный университет», E-mail: IsmagilovaAS@yandex.ru

УДК 004.056.5

МОДЕЛИРОВАНИЕ И ИЗМЕРЕНИЕ ЭНЕРГОПОТРЕБЛЕНИЯ УСТРОЙСТВА ПРИ ВЫПОЛНЕНИИ ШИФРА AES

Е.А. Маро
Южный федеральный университет, г. Таганрог

Ключевые слова: энергопотребление устройств, криптографический алгоритм, Advanced Encryption Standard (AES)

Метод анализа побочных каналов криптографических устройств заключается в поиске математической зависимости в параметрах функционирования шифрующего устройства, например, времени вычислений, энергопотреблении, электромагнитном и акустическом излучении. Целью работы является теоретический и экспериментальный анализ трасс энергопотребления устройств при выполнении криптографических алгоритмов. Для реализации поставленной задачи был смонтирован аппаратный стенд на основе платы Arduino Nano, выполняющей алгоритм шифрования AES в различных вариантах реализации, и высокоточного осциллографа RIGOL DS1054. Моделирование трасс энергопотребления проводилось в программном обеспечении ELMO [1]. В результате работы сформирована модель трассы энергопотребления при выполнении шифра AES (рисунок 1) и получены трассы для устройства Arduino Nano.

Проведенное моделирование и выполненные на аппаратном стенде измерения энергопотребления позволяют оценить число инструкций, содержащих информацию о защищаемых данных (секретном ключе) на основе выполнения t-теста (с пороговым значением |4.5|) для фиксированного и случайных открытых текстов. В Таблице 1 представлены результаты моделирования утечек первого порядка по побочным каналам для нескольких реализаций шифра AES.