СЕТЕВОЙ ТРАФИК ПРИМЕНЯЕМЫЙ ПРИ ПОДГОТОВКЕ ПЕРВОНАЧАЛЬНЫХ ОБУЧАЮЩИХ ДАННЫХ ДЛЯ СРЕДСТВА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Чипига А.Ф., Пелешенко В.С., Лазарев Н.В.

Северо-Кавказский государственный технический университет,

zik@ncgtu.ru, Ставрополь

При подготовке сетевого трафика предложено использовать следующие средства.

1. Генерация трафика, содержащего сигнатуры, приводящие к несанкционированному доступу к веб-ресурсам сервера, осуществлялась средствами анализа безопасности веб-узлов. В качестве таких средств использованы следующие программы:
   - Pandora ver 1.8.0.502;
   - Retina Network Security Scanner demo ver 4.9.199;
   - NetBrute Scanner;
   - Nmap ver beta 3.50;
   - XSpider 6.50;
   - XSpider demo 7.0;
   - S-Xaker v 1.0;
   - встроенный генератор пакетов снифера commview.
2. Генерация пакетов, содержащих параметры и характеристики, характерные для известных атак, осуществлялась с помощью сканеров уязвимостей узлов ЛВС, программ-эксплойтов, программ-вирусов и программ-шпионов, таких как:

- Apache-nosejob;
- Apache Artificially Long Slash Path Directory Listing Exploit;
- Jportknock;
- Brutus AET2;
- Wwwhack v 1.1;
- XArp v 0.1;
- Pandora ver 1.8.0.502;

– S-Xaker v 1.0;
– XSpider 6.50;
– XSpider demo 7.0;
– Mydoom;
– vipGsm;
– Win32Bagle.AI worm;
– Win32Bagle.AL worm;
– Win32Bagle.AS worm;
– Win32Mydoom.L worm;
– bagle32gen;
– встроенный генератор пакетов снифера commview.

3. Генерация «чистого» трафика осуществлялась с помощью пакетного генератора, встроенного в пакетный снифер commview путем отправки пакетов в тестируемую сеть на тестируемые узлы.

После этого осуществляется обучение нейросетевых анализаторов обнаружения атак в сетевом трафике, загрузка сигнатур известных атак в модуль сигнатурного анализа и обучение итоговой нейросети принятия решений (корреляции) выводов анализаторов. Предварительно в программу загружаются обучающие выборки в виде «чистого» и «грязного» трафиков, содержащиеся в лог файлах пакетного снифера.

Показанные средства позволяют составить общую картину параметров и характеристик пакетов, содержащих основные данные по сетевым атакам. С помощью пакетного генератора представляется возможным изменять необходимым образом параметры и характеристики обучающих выборок.

СПИСОК ЛИТЕРАТУРЫ

1. В.С. Пелешенко. Подход к построению аппаратно-программного комплекса для обнаружения и предотвращения сетевых атак на защищаемые информационные системы. // Материалы международной научно практической конференции «Информационные системы, технологии и модели управления производством». Ставрополь, 2005.

2. А.Ф. Чипига, В.С. Пелешенко. Построение нейросистем выявления и предотвращения атак // Материалы V региональной научно-практической конференции «Совершенствование методов управления социально-экономическими процессами и их правовое регулирование». Ставрополь, 2005.