СПИСОК ЛИТЕРАТУРЫ

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд., стер. - М.: Академия, 2008. - 336 с.
2. Черней Г.Л, Охрименко С. А., Ляху Ф. С. Безопасность автоматизированных информационных систем. Ruxancia, 1996. - 225 с.
3. Галатенко, ВЛ. Основы информационной безопасности.
4. Лепешкин О.М., Харечкин П. В. Функционально-ролевая модель управления доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
5. Бурлов В.Г., Лепешкин О.М.Методологический подход к оценке безопасности функционирования социальной и экономической системы управления регионаПроблемы экономики и управления в торговле и промышленности. 2013. № 2. С. 99-103.
6. Лепешкин О.М.Разработка подхода по оценке функциональной безопасности критической социотехнической системы. Инфокоммуникационные технологии. 2008. Т. 6. № 3. С. 113-116.

УДК 004

О НЕКОТОРЫХ МЕТОДАХ СЕТЕВОГО АНАЛИЗА

Гапочкин Артем Владимирович[1], Михайличенко Николай Валерьевич[2]
[1]Московский политехнический университет
Россия, Москва, ул. Большая Семеновская, 38
[2]Военная академия связи имени Маршала Советского Союза С.М.Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: Warrior_555@rambler.ru,23esn2008@rambler.ru

Аннотация. Сниффинг пакетов в сети без коммутаторов. Данные, полученные с помощи сниффера, могут быть использованы хакером для получения легального доступа к сервисам системы на правах законного пользователя. В докладе рассматриваются существующие 3 меры противодействия данному виду атак на основе сканирования сети. До выполнения активных атак злоумышленнику необходимо узнать всю информацию о самой структуре сети и сервисах. В статье моделируется с помощью сети Петри-Маркова процесс сканирования сети.

Ключевые слова: *сниффинг; сетевой анализ; сеть Петри-Маркова.*

SOME METHODS OF NETWORK ANALYSIS

Gapochkin Artem[1],Mikhaylichenko Nikolay[2]
[1]Moscow Polytechnic University, Russia, Moscow, Bolshaya Semenovskaya, 38
[2]Military Academy of communications named after Marshal of the Soviet Union S. M. Budyonny"
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: Warrior_555@rambler.ru, 23esn2008@rambler.ru

Abstract. Sniffing of packages in network without switchboards. The data received from the help of a sniffer can be used by the hacker for receiving legal access to services of system as the lawful user. In the report the existing 3 measures of counteraction to this type of the attacks on the basis of scanning of network are considered. Before performance of the active attacks the malefactor needs to find all information on the structure of network and services. In article process of scanning of network is modelled by means of Petri-Markov's network.

Keywords: *sniffing; network analysis; Petri net and Markov.*

Активной называется такая атака, при которой оппонент имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Пассивной называется такая атака, при которой оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Она является подготовительным этапом при реализации многих активных сетевых атак. Когда вместо коммутаторов в сети установлены концентраторы, то пакеты, полученные рассылаются всем компьютерам в сети, и только после этого компьютеры определяют для кого этот пакет [1]. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

Если хакер получит доступ к такой сети или непосредственно к компьютеру, то ему станет доступна вся передаваемая информация в сети, он может также перехватывать пакеты, если вставит сетевую карту в режим прослушивания. Несанкционированное прослушивание и наблюдение за данными сети, с помощью которых хакер получает легальный доступ к сервисам системы на правах законного пользователя, производится с помощи специальной программы - пакетного сниффер.

В данном примере сети позиции не имеют инцидентные дуги, следовательно, вероятности перемещения из них в переходы равны единице.

Полушаг из перехода в позицию срабатывает мгновенно и динамика срабатывания сети может определяться только вероятностями перемещений этой сети, а также плотностями распределения времени нахождения процесса в каждом из процессов. Следовательно, в сети необходимо рассмотреть только процесс перехода из s1 (начального состояния) в t2 (конечный переход) [2].

До выполнения активных атак злоумышленнику необходимо узнать всю информацию о самой структуре сети и сервисах. Смоделируем с помощью сети Петри-Маркова сканирование сети. После настройки параметров, осуществляется посылка ICMP- эхо - запросов, хостов, IP-адресов в режиме многопоточном. Путем посылки нестандартных пакетов, злоумышленник может определить тип ОС, однако стандарты упускают реакцию на недопустимые входные данные. Следовательно, индивидуальные реакции каждой определенной ОС на нестандартные пакеты формируют сигнатуру, по которой злоумышленник может определить под каким управлением работает данный компьютер. В случае, если хост определен как активный, то определяется наличие работающего сервиса. Результатом данной проверки является выявление наиболее уязвимых компьютеров. Смоделируем данную атаку с помощью модели Петри-Маркова.

В докладе рассмотрены способы моделирования процессов сетевого анализа при угрозах доступа к элементам ИТКС. Данные методы являются подготовительными этапами для проведения активных атак злоумышленниками. Моделирование этих процессов может позволить более детально проанализировать отдельные стадии атак на сеть и эффективно предотвращать активные атаки на стадии их подготовки.

СПИСОК ЛИТЕРАТУРЫ

1. Радько Н.М. Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. РадиСофт, 2010 – 232с. С.122-127.
2. Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В. Проблема формирования системы динамической защиты государственных информационных систем. / Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т./ под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – 550 с. С. 239-243.
3. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов. 2016. С. 758-762.

УДК 004.056.57

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Гладков Владимир Владиславович, Тараскина Анастасия Геннадьевна,
Кузнецов Сергей Иванович, Тесля Сергей Петрович, Акишин Андрей Владимирович
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: akishin1977@mail.ru

Аннотация. В работе рассматриваются методы построения систем обнаружения DDoS-атак на основе нейронных сетей и их эффективность.

Ключевые слова: *искусственнаянейронная сеть; DDoS-атака; сетевая атака; информационная угроза; альтернативные методы.*

THE USE OF NEURAL NETWORKS TO DETECT NETWORKS ATTACKS

Gladkov Vladimir, Taraskina Anastasiya, Kyznecov Sergey, Tesla Sergey, Akishin Andrey
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: akishin1977@mail.ru

Abstract. In the paper method of construction of system of detection of DDoS-attacks on the basic of neural networks and their efficiency.

Keywords: *artificial of neural networks; DDoS-attack; network attack; alternative methods.*

В последнее время в разных отраслях науки и техники отмечается интерес к применению искусственных нейронных сетей. Популярность нейронных сетей объясняется возможностью их эффективного использования в задачах плохо решаемых "аналитическими" методами. В теоретических работах [1, 2, 3, 4], посвященных нейронным сетям отмечается целесообразность их использования в задачах: классификации образцов, кластеризации/категоризации, аппроксимации функций, предсказания/прогноза, создания информационно-вычислительных систем, обладающих памятью, адресуемой по содержанию, т.е. ассоциативной.

Отметим, что частично или в комплексе, решать перечисленные задачи приходиться при разработке методов и средств защиты информации.

Среди множества видов сетевых атак наибольшее распространение получила атака типа DDoS. По данным статистики данный вид угрозы занимает одно из лидирующих мест ежегодно. Причинами распространения подобного вредоносного сетевого воздействия является простота реализации, исчерпывающие сведения о механизме исполнения и малые требования к знаниям и вычислительным ресурсам злоумышленника.