сеть, чем фиксированная, и в то же время, характеристики сети для 2-х путевой маршрутизации близки к варианту альтернативной маршрутизации (при увеличении нагрузки до 1.7 раза), то есть 2-х путевая маршрутизация достаточно близка к оптимальной маршрутизации. Следовательно, можно сделать вывод о целесообразности применения алгоритма 2-х путевой маршрутизации в сетях передачи данных.

Перечень ссылок

1. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003 – 512 с.
2. В. Столингс. Современные компьютерные сети. 4-е изд. – СПб.: Питер, 2005. – 961 с.
3. Клейнрок Л. Вычислительные сети с очередями: пер. с англ. – М. Мир, 1979, – 1979. – 600с.

ИСПОЛЬЗОВАНИЕ СТАНДАРТНЫХ СРЕДСТВ ОС LINUX ДЛЯ ВЫЯВЛЕНИЯ НЕЛОЯЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ СЕРВЕРОВ КОРПОРАТИВНЫХ СЕТЕЙ

Тума А.Н., группа ТКС-00н
Руководитель: д.т.н. Скобелев В.Г.

Постановка задачи: Эта работа направлена на то, чтобы создать программу мониторинга за действиями локальных пользователей сервера под управлением ОС LINUX , способную выявлять малейшие изменения в их поведении и анализировать эти аномалии на предмет элементов злоупотреблений.

Краткий анализ существующих решений: На сегодняшний день проблема защиты информации стоит очень остро. Существует как большое количество известных и даже реально осуществленных атак, так и большое количество методов обнаружения атак и защиты от них. Современные программные

продукты защиты от атак локальных пользователей можно условно разделить на две группы, в зависимости от направления разработки: это методы обнаружения злоупотреблений и методы обнаружения аномалий. Под злоупотреблениями понимаются известные на сегодняшний день и наиболее распространенные типы атак, использующие уязвимости системы, на которую совершается атака. Обнаружение аномалий – это обнаружение малейших изменений в поведении пользователей, заведенных в системе. Анализ аномалий предполагает тщательный анализ большого числа ситуаций, из которых только малая доля может реально представлять угрозы системе. То есть анализ аномалий – это анализ потенциальных угроз безопасности. Методы обнаружения аномалий на сегодняшний день недостаточно исследованы и разработаны. Современные принципы построения систем обнаружения аномалий не позволяют сочетать высокие показатели обнаружения с приемлемо низким уровнем ложных срабатываний.

Предлагаемое решение: В этой работе были объединены две группы методов обнаружения атак. Слежение с целью выявления отклонений в работе локальных пользователей проводилось в консольном режиме ОС LINUX. Каждый пользователь выполняет на сервере определенную работу и использует определенный набор приложений, которые необходимы для выполнения этой работы. Таким образом можно предположить, что набор приложений, характерный для работы конкретного пользователя и есть образец (стандарт), отклонения от которого предполагается выявлять. Список команд (приложений), с которыми работал пользователь, будем брать из файлов истории bash_history, которые ведутся системой и в которых хранится список вводимых пользователем команд . Образец можно формировать динамически из файлов истории за последние десять дней, выбирая из них общее, то есть то, с чем пользователь работает изо дня в день. Примем следующие обозначения: И1, И2…И10 – это история команд за 1, 2…10 дни работы. S(И1), S(И2),..., S(И10) = S – это общее во всех этих файлах, то есть команды, которые

пользователь вводил все эти 10 дней. Это общее и есть образец, с которым сравнивается история И11 для выявления аномалии в поведении пользователя на 11й день.

Выявление аномалий позволяет только классифицировать пользователей по их поведению на группы «свой», «чужой». Результатом работы так же могут быть ложные срабатывания. И если для группы «свой» эти срабатывания можно свести к минимуму, то для группы чужой любая детализация может быть критичной, поэтому необходим дополнительный анализ. Дополнительный анализ выявляет не аномалии, а злоупотребления в поведении тех пользователей, которые анализом аномалий были признаны, как чужие. Для решения задачи необходим прежде всего анализ всех существующих типов атак (злоупотреблений), которые могут осуществить пользователи системы, а так же выбор «характерных» элементов таких атак, то есть элементов, без которых осуществить атаки невозможно. История каждого пользователя анализируется на наличие этих элементов.

Результаты работы: В результате работы данной программы, администратор системы имеет возможность выявления не только наименьших изменений в работе пользователя с системой, но и возможность обнаружения угрозы для безопасности системы в тех случаях, когда эти изменения зловредны. Исследования проводились на сервере Интернет провайдера, работающий под управленим ОС Linux (ASPLinux 7.3),на котором установлена программная оболочка bash-2.05a-13.asp и доступ к которому имеют 11 пользователей. Результаты работы приведены в таблице 1.

Таблица 1 – Результаты работы программы-анализатора на сервере.

Критерии	Всего	Верно	Неверно
"Свой"	6	4	2
"Чужой"	5	5	0
"Злоупотребления"	3	3	0
"Аномалии"	4	4	0

Область применения: Корпоративные сервера, сервера Интернет провайдеров, работающие под управлением операционных систем семества Unix.

Перечень ссылок

1. Б. Хатч, Д. Ли, Д. Курц «Секреты хакеров.Безопасность Linux – готовые решения». – М.:Издательский дом «Вильямс», 2002. – 544 с.
2. К. Рейчард, П. Фолькердинг «LINUX: справочник» – СПб: Питер Ком, 1998. – 480 с.
3. Материалы VI Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2004.464 с.

ПЛАНИРОВАНИЕ СЕТИ СОТОВОЙ СВЯЗИ НА ОСНОВАНИИ ДИСКРЕТНЫХ ХАРАКТЕРИСТИК ТРАФИКА

Шебанов А.О., группа ТКС-01н
Руководитель к.т.н., доц. Попов В.А.

Современные тенденции проектирования сетей сотовой связи сталкиваются с тремя основными проблемами. Во-первых, быстрый рост числа пользователей сети с момента ее создания требует от операторов возможности гибкого проектирования и оптимизации систем для обработки трафика высокой интенсивности. Во вторых, новые технологии сетей третьего поколения, например CDMA, предполагают применение новых подходов в планировании, основанных на изменении конфигурации сети “по требованию” (demand based planning methods), так как область охвата передатчика в этих системах зависит и от распространения радиоволн, и от интенсивности текущего трафика. В-третьих, стремительное развитие телекоммуникационных технологий и рынка услуг связи вынуждают новых операторов сети разворачивать и настраивать сети сотовой связи в очень короткие сроки. Поэтому операторы сетей сотовой