БЕЗОПАСНОСТЬ СЕГМЕНТОВ КОРПОРАТИВНОЙ СЕТИ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

Кульгавик С. Г., Буй П. М.
Кафедра «Системы передачи информации», Белорусский государственный университет транспорта
Минск, Республика Беларусь
E-mail: kalashnikovn27.sk@gmail.com, pashabuoy@rambler.ru

В статье описано моделирование сегмента корпоративной сети Белорусской железной дороги в среде Cisco Packet Tracer при наличии внутреннего источника угроз. Представлена в первом приближении модель внутреннего нарушителя информационной безопасности корпоративной сети. Тезисно описана реализация одного из исследуемых методов нарушения информационной безопасности.

Введение

С внедрением и активным использованием автоматизированных систем управления технологическими процессами (АСУ ТП) на таком территориально разнесенном объекте, как Белорусская железная дорога, ее корпоративная сеть связи совместно с прочими объектами информатизации приобретает ключевое значение в процессе обеспечения безопасности грузо- и пассажироперевозок. Опираясь на требования нормативно-правовой и методической базы в области защиты информации для таких объектов организуется система комплексной защиты информации, соответствующая политике безопасности предприятия. Некоторые объекты информатизации относят к категории критически важных (КВОИ), что обуславливает предъявление к ним повышенных требования по информационной безопасности в соответствии с законодательством Республики Беларусь. Следует отметить, что необходимость системного подхода к вопросам обеспечения информационной безопасности объектов информатизации не находит должного понимания у их пользователей, а зачастую и у администраторов. Отсутствие системного подхода при обеспечении информационной безопасности может привести к тому, что не будут учтены возможности сотрудников Белорусской железной дороги по реализации несанкционированного доступа к информации, передаваемой в ее корпоративной сети. Не смотря на то, что в последние годы в статистике нарушений информационной безопасности зафиксирован резкий сдвиг от внешних к внутренним угрозам при реализации системы защиты внутренним нарушителям может уделяться гораздо меньше внимания [1]. Зачастую деятельность сотрудников в рамках мероприятий по защите информации регламентируется организационными мероприятиями. Примерно две трети от общего числа всех наиболее серьезных инцидентов, связанных с безопасностью, составляют нарушения или ошибки легальных пользователей сетей [1]. Причем больший интерес для исследования представляют преднамеренные действия внутренних нарушителей. Для защиты от преднамеренных внутренних угроз необходимо применять комплексную защиту, направленную против интеллекта нарушителя («защита от умного»), в то время как защита от непреднамеренных угроз предполагает мероприятия, в целом сводящиеся к классической «защите от дурака». С использованием среды моделирования Cisco Packet Tracer был реализован небольшой типовой сегмент корпоративной сети Белорусской железной дороги, включающий компьютеры пользователей и несколько коммутаторов второго уровня, которые объединяют компьютеры пользователей в сеть (рисунок 1). В реализованной подсети были произведены исследования возможности перехвата одним из пользователей не предназначенного ему трафика при наличии ряда уязвимостей организации и администрирования сети.

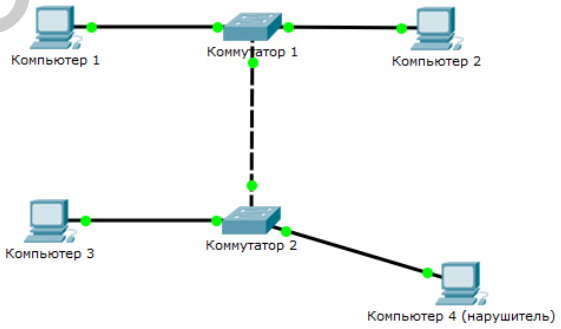

Рис. 1 – Небольшой типовой сегмент корпоративной сети

I. Модель нарушителя

В качестве нарушителя был выбран законный пользователь одного из компьютеров, подключенных к сети. Для него была составлена неформальная модель нарушителя информационной безопасности:

- нарушитель имеет точку доступа к сети и собственное помещение или закрытое пространство общего помещения, позволяющее ему скрытно подключать собственное сетевое оборудование;
- нарушитель обладает достаточно неплохими знаниями в сфере IT, в частности вклю-

Библиотека БГУИР

чающими знания о работе протоколов IP, TCP, UDP, SNMP, TFTP, стандарта IEEE 802.1Q для VLAN, навыками конфигурирования сетевого оборудования;
- нарушитель своей целью ставит доступ к трафику других пользователей сети;
- причинами, побуждающими внутреннего нарушителя к неправомерным действиям, могут быть: демонстрация своего превосходства (самоутверждение), «борьба с системой», корыстные интересы;
- характер действий нарушителя – скрытый;
- финансовые возможности нарушителя достаточны для приобретения в собственность необходимого сетевого оборудования.

Представленная модель является демонстрационной, поэтому она далеко не полная и весьма субъективная. Максимально объективно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности [2].

II. Реализация сетевой атаки

Одной из субъективных уязвимостей такого объекта информатизации, как сетевое оборудование, являются навыки, опыт, а иногда и самоуверенность, сетевого администратора, который это оборудование конфигурирует и выполняет мероприятия по защите информации в рамках политики безопасности предприятия в целом. Например, системные администраторы или не знают, или забывают о существовании протокола SNMP и соответствующей службы, в которой используется крайне ненадежный механизм обеспечения информационной безопасности. В результате SNMP достаточно часто становится целью нарушителей информационной безопасности. Известно, что по умолчанию информация SNMP защищается простыми паролями, имеющими известные значения, и распространяющимися по сети в открытом виде. После взлома SNMP представляется возможность переконфигурации сетевого оборудования за счет организации ложного TFTP-сервера. Получив возможность переконфигурировать коммутаторы, нарушитель организует на первом коммутаторе (рисунок 2) две виртуальные сети по одной для каждого из пользователей (например, VLAN 11 и VLAN 12), чей трафик он собирается перехватывать. Для сохранения передачи данных между этими пользователя необходимо передавать трафик с VLAN 11 на VLAN 12 и обратно. Для этого нарушитель подключает свой собственный коммутатор (коммутатор нарушителя на рисунке 2) настроенный таким образом, что канал между ним и коммутатором 2 является транкинговым (общим для VLAN 11 на VLAN 12), один из свободных портов, например, FastEthernet 0/2 закреплен за VLAN 11, другой, например, FastEthernet 0/3 – за VLAN 12. Канал между коммутатором 1 и коммутатором 2 также является транкинговым.

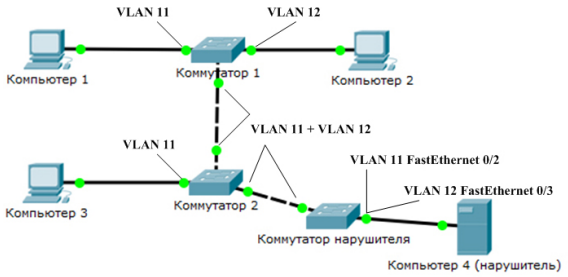

Рис. 2 – Реализация перехвата внутренним нарушителем трафика в сети

При такой конфигурации весь сетевой трафик из компьютера 1, адресованный компьютеру 2 будет проходить следующий путь: компьютер 1 – коммутатор 1 – коммутатор 2 – коммутатор нарушителя – FastEthernet 0/2 коммутатора нарушителя – устройство нарушителя (Компьютер 4 на рисунке) – FastEthernet 0/3 коммутатора нарушителя – коммутатор нарушителя – коммутатор 2 – коммутатор 1 – компьютер 1. От компьютера 2 к компьютеру 1 трафик будет проходить по этому же маршруту в обратном направлении. Таким образом, до первого обнаружения неправильной конфигурации коммутаторов администраторами весь нужный нарушителю трафик будет проходить через его устройство.

Представленная выше одна из исследованных в среде моделирования Cisco Packet Tracer внутренняя преднамеренная угроза информационной безопасности сегмента корпоративной сети Белорусской железной дороги, исходящая от ее законного пользователя, обладающего минимумом необходимых знаний и средств, наглядно демонстрирует необходимость объективного подхода к защите от внутренних источников угроз. Помимо организационных мероприятий необходимо использовать специализированные программные средства для мониторинга действий пользователей сети, оценивать и повышать квалификацию системных администраторов для устранения уязвимостей корпоративной сети, а также повышать мотивацию сотрудников не совершать преднамеренных угроз информационной безопасности.

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер // Учебник для ВУЗов. 5-е изд. – СПб. : Питер, 2016. – 992 с.
2. Бочков, К. А. Модель внутреннего нарушителя информационной безопасности сети дистанции сигнализации и связи / К. А. Бочков, П. М. Буй, М. В. Лукашеня // Проблемы и перспективы развития транспортных систем и строительного комплекса: материалы III Международной науч.-практ. конф. / М-во образования Респ. Беларусь, М-во трансп. И коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т трансп.; под общ. ред. В. И. Сенько. – Гомель: БелГУТ, 2013. – с. 109 – 110;

Библиотека БГУИР