Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.492.3

Горелик
Андрей Александрович

Методика автоматизированного анализа защищенности узлов вычислительной сети

АВТОРЕФЕРАТ ДИССЕРТАЦИИ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Бойправ О.В., к.т.н., доцент

_____

Минск 2020

ВВЕДЕНИЕ

В настоящее время вычислительные сети используются для реализации большого количества производственных процессов, а также процессов, связанных с обработкой информации распространение и (или) предоставление которой ограничено. Одним из мероприятий, реализуемых в целях обеспечения непрерывности указанных процессов является анализ защищенности узлов вычислительной сети. Защищенность данных, циркулирующих в пределах вычислительной сети, зависит от настроек аппаратных и программных средств, на основе которых она построена, а также от ее конфигурации. Рациональным представляется проводить на регулярной основе оценку корректности этих настроек. Данный процесс затруднительно реализовывать в ручном режиме. В связи с этим в настоящее время проводятся работы, направленные на создание методик по автоматизированной оценке корректности настроек аппаратных и программных средств вычислительной сети. Большинство этих методик являются многошаговыми, что обуславливает большой объем временных ресурсов, необходимых для их реализации. Таким образом, необходимо проводить исследования, направленные усовершенствование существующих или создание новых методик с целью уменьшения временных затрат на реализацию рассматриваемых процессов.

Целью данной работы является разработки методики для оценки защищенности устройств, функционирующих в составе вычислительных сетей. Для достижения данной цели необходимо решить следующие задачи:

1) анализ методов и средств оценки защищенности вычислительных сетей и циркулирующих в их пределах данных;

2) выбор и обоснование устройств вычислительной сети, которые должны подлежать оценке с точки зрения защищенности;

3) обоснование выбора программных средств для реализации методики по оценке защищенности вычислительных сетей и циркулирующих в их пределах данных;

4) настройка выбранных программных средств;

5) апробация разработанной методики.

Разработанная методика была апробирована на реальных информационных системах, функционирующих в настоящее время на предприятиях Республики Беларусь.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи проводимых исследований

Целью работы является разработка методики для оценки защищенности устройств, функционирующих в составе вычислительных сетей.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать методы и средства оценки защищенности вычислительных сетей и циркулирующих в их пределах данных.
2. Выбрать устройства вычислительной сети, которые должны подлежать оценке с точки зрения защищенности.
3. Настроить программное средство для анализа защищенности.
4. Апробировать разработанную методику.

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует пункту 7, в части средств технической и криптографической защиты информации, Указа Президента Республики Беларусь от 22.04.2015 г. № 166 «О приоритетных направлениях научно-технической деятельности в Республике Беларусь на 2016-2020 годы».

Апробация результатов диссертации

Основные результаты диссертации докладывались и обсуждались на XVII Белорусско-российской научно – технической конференции (г. Минск, 11 июня 2019 г.), а также на XV Международной научно-практической конференции (г. Минск, 7 декабря 2018 г.)

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе рассмотрена классификация локальных вычислительных сетей (ЛВС) в зависимости от территориального расположения, по принципу действия, по топологическим признакам и в зависимости от используемых методов доступа. Представлены основные принципы построения ЛВС и рассмотрены основные протоколы стека TCP/IP, которые являются неотъемлемой частью при функционировании ЛВС. Проанализированы уязвимости ЛВС, атаки на такие сети и используемые для реализации атак технические средства съема информации. Определено, что наиболее критичными уязвимостями ЛВС являются атаки типа «отказ в обслуживании», ошибки в программном обеспечении, анализаторы протоколов и прослушивающие программы («снифферы»).

Во второй главе обосновано целесообразность использования программного средства (ПС) «Сканер» для поиска уязвимостей ЛВС. Это программное средство характеризуется следующими основными преимуществами по сравнению с аналогами:

– ПС «Сканер» в настоящее время имеет сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, регистрационный номер сертификата соответствия № BY/112 02.01. 036 00784, срок действия сертификата до 03.07.2024 г.;

– возможность одновременного сканирования нескольких целевых устройств;

– низкая стоимость;

– построение топологии проверяемой вычислительной сети;

– создание в автоматизированном режиме отчетов, содержащих сведения об обнаруженных уязвимостях вычислительной сети.

Разработана методика сканирования ЛВС с использованием выбранного программного средства. Она включает в себя следующие шаги:

– вход в веб-интерфейс ПС «Сканер» по адресу, общий формат которого следующий: *https://<IP-адрес сервера ПС «Сканер»>/*;

– запуск процесса сканирования, который включает в себя создание новых цели и задач сканирования, запуск выполнения каждой из поставленных задач;

– формирование отчета с результатами сканирования, в котором отражаются сведения о текущем состоянии сканирования и количестве найденных уязвимостей ЛВС.

В третьей главе выполнена апробация разработанной методики на трех ЛВС. Было установлено, что причинами наиболее критичных уязвимостей являются:

– не отключены не используемые алгоритмы шифрования при использовании протокола SSH;

– не отключены временны метки TCP, которые позволяют вычислить время непрерывной работы оборудования;

– не отключены не используемые алгоритмы хеширования при использовании протокола SSH;

– используются ключи шифрования Диффи-Хеллмана длинной менее 2048 бит;

– на ПЭВМ пользователей используются открытые порты.

– используется устаревший протокол TLS v1.0;

– на сервере управления СЗИ используются открытые порты;

– используются ключи шифрования Диффи-Хеллмана длинной менее 2048 бит;

– не отключены временны метки TCP, которые позволяют вычислить время непрерывной работы оборудования;

– используется не обновленное ПО.

Предложены меры по устранению выявленных причин.

ЗАКЛЮЧЕНИЕ

Выявление уязвимостей – это периодический процесс, частота повторения которого должна зависеть как от критичности обрабатываемой в информационной системе информации, так и от особенностей самой инфраструктуры ЛВС информационной системы. Устранение выявленных уязвимостей – это процесс постоянного совершенствования системы обеспечения ИБ, реализация которого позволит как устранить существующие уязвимости, так и снизить вероятность возникновения новых.

В диссертационной работе предложена методика выполнения сканирования ЛВС. По сравнению с аналогами эта методика заключается в использовании ПС «Сканер», с помощью которого реализуются следующие действия:

– сканирование целевых устройств, тип сканирования зависит от поставленной задачи;

– выявление уязвимостей устройств;

– рекомендации по устранению уязвимостей.

Основное преимущество ПС «Сканер» заключается в возможности реализации с его использования широкого перечня типов сканирования.

Выполнена апробация разработанной методики на трех ЛВС. В ходе апробации установлено, что наиболее частыми причинами уязвимостей сетей являются не обновленное ПО, не отключены не используемые алгоритмы шифрования при использовании протокола SSH, открытые порты и др.

В связи с этим для повышения уровня защищенности ЛВС необходимо реализовывать следующие меры:

– регулярно обновлять используемое ПО;

– проводить внешнюю и внутреннею ежегодную проверку отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения ИБ безопасности системы и сведения о которых подтверждены производителями (разработчиками) этих объектов информационных систем согласно положению о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) которой предоставление которой ограничено [20];

– перед тем как использовать в информационной системе новые средства вычислительной техники и (или) которые подверглись ремонту, необходимо провести его сканирование, а после сканирования уже подключать к ЛВС.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Горелик А. А. Методика анализа защищенности узлов вычислительной сети / А. А. Горелик, Н. В. Журавский, О. В. Бойправ // Управление информационными ресурсами : материалы XV Междунар. науч.-практ. конф., Минск, 7 дек. 2018 г. – Минск : Акад. упр. при Президенте Республики Беларусь, 2018. – С. 210.

2–А. Горелик, А. А. Методика настройки программного обеспечения для оценки защищенности информационной сети / А. А. Горелик, Н. В. Журавский // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции, Минск, 11 июня 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2019. – С. 22