МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Выявление сетевых протоколов удаленного управления

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Кузнецова Игоря Сергеевича

Научный руководитель
доцент, к. ю. н., доцент _____ А. В.Гортинский
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

За последний год использование программ удаленного доступа превратилось из полезной возможности в критическую необходимость для большинства компаний в мире. Множество из них столкнулось с необходимостью противостоять сетевым атакам на их системы, после появления в них угроз безопасности, связанных с использованием удаленного доступа их сотрудниками. В этой ситуации системному администратору необходимо обладать знаниями и программными возможностями для поиска и выявления сетевых протоколов удаленного доступа для поиска среди них возможных несанкционированных подключений.

Цели работы: изучить признаки сетевой активности средств удаленного доступа, выявить их на фоне работы других сервисов в системе и локальной сети, определить признаки, указывающие на конкретные программы удаленного управления и создать систему, способную анализировать и выводить получаемую из сети информацию и оказывать поддержку для решения задачи выявления протоколов удаленного управления.

Структура и объём работы (Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 66 страниц, из них 46 страниц – основное содержание, включая 23 рисунка и 1 таблицу, список использованных источников из 16 наименований.)

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе излагаются основные понятия, которые потребуются для понимания принципов работы сетевых соединений, передачи данных по сети и сетевых протоколов, рассматриваемых в данной работе.

Подраздел 1.1 определяет понятие сетевого пакета данных, дает определение заголовка, полезной нагрузки пакета и сетевого протокола пакета данных.

Подраздел 1.2 описывает принципы работы сетевых портов подключения и диапазоны номеров для регистрации новых сетевых портов в системе. Указывается роль портов в соединении различных программ по сети. Приводятся состояния, в которых порт может находиться в операционной системе компьютера. Определяется понятие сокета и необходимость их уникальности для установления корректного соединения. Показывается необходимость знания номера используемых портов в решении задач безопасности системы.

Подраздел 1.3 описывает сетевой протокол транспортного уровня TCP, его основные задачи и свойства. Таблица 1 показывает структуру заголовков пакетов протокола TCP. Даются определения для таких элементов заголовка пакетов как порт отправителя и получателя, номер в последовательности, номер подтверждения, смещение данных, флаги URG, ACK, PSH, RST, SYN, FIN, размера окна внутреннего буфера TCP-модуля, контрольная сумма заголовка и данных пакета, указателя и дополнительных данных заголовка.

Подраздел 1.4 описывает сетевой протокол прикладного уровня SMB, использующийся в операционной системе Windows для удаленного доступа к файлам, принтерам, COM-портам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. Рассматриваются возможности этого протокола, структура используемых им пакетов, принципы соединений между машинами, использующими данный протокол и возможности операционной

системы для совместного использования протоколов SMB и TCP для передачи больших объемов данных.

Второй раздел посвящен рассмотрению используемых в работе средств удаленного управления, принципы их работы, используемые ими механизмы защиты данных и приводит угрозы безопасности, связанные с использованием программ удаленного управления.

Подраздел 2.1 описывает службу создания сеансов удаленного управления по локальной сети на основе протокола Remote Desktop (сокращенно RDP). Приводится история развития службы, возможности пользователя для работы с локальными или сетевыми принтерами, подключению к машине локальных ресурсов, обмена данными через буфер обмена и изменению сетевых портов подключения службы через средства редактирования реестра.

Далее рассматриваются характеристики сетевого протокола RDP, порядок установления подключения, принципы использования примитивов для передачи данных и команд. Приведены методы шифрования данных, поддерживаемые протоколом RDP, методы установления безопасного соединения между клиентами и сервером и различные способы шифрования полезной нагрузки пакетов данных.

Подраздел 2.2 содержит информацию о рассматриваемых коммерческих программ удаленного управления Radmin и TeamViewer. Для Radmin описываются особенности используемого им сетевого протокола и шифрования передаваемой информации алгоритмом блочного шифрования AES-256, а также принципы установки элементов программы и использования средств безопасности. Описана возможность изменения используемого программой сетевого порта.

Для TeamViewer указаны используемые им сетевые протоколы, средства шифрования передаваемой информации, инструкции по работе через различные устройства и возможности создания безопасного соединения.

Рассмотрен список используемых портов и порядок их использования для программы и различных ее версий для работы с мобильных устройств.

Подраздел 2.3 посвящен описанию различных угроз безопасности, связанных со службами удаленного управления. Приводится статистика числа сетевых узлов, уязвимых для несанкционированного доступа к носителям информации и внедрению вредоносное программное обеспечение с использованием протоколов удаленного управления.

Рассмотренные угрозы разделены на две категории. Первая категория предполагает существование в атакуемой системе средств удаленного доступа и, пользуясь халатностью при проведении работ по установке и настройке программного обеспечения служб удаленного доступа или списком существующих уязвимостей программы, получает полный доступ к атакованной системе с возможностью просматривать, изменять и удалять информацию и устанавливать новое программное обеспечение. Вторая категория предполагает внесение модификаций в оригинальный код внедряемой программы удаленного управления для маскировки ее существования от проверок системных средств безопасности.

Третий раздел рассматривает существующие средства анализа сетевой активности. Приводится определение снифферов как программ для проведения операций перехвата проходящих по сети пакетов данных и их анализа. Рассматриваются возможности снифферов к фильтрации отображемых пакетов по типу их сетевого протокола, разделению пакетов между адресами их отправителей, отображению времени начала и конца индивидуальных сессий подключения и их продолжительности, анализу информацию в перехваченных пакетах, поиску в незашифрованных паролей и других данных аутентификации пользователя, реконструированию сессии общения.

Также приводится определение неразборчивого режима сетевых карт и его необходимость в решении задачи получения всех проходящих по сети пакетов данных.

Четвертый раздел посвящен созданию среды для проведения исследования сетевой активности рассматриваемых средств удаленного доступа, описанию разработанной программы сетевого анализа, использованию программы для изучения сетевой активности и выявления признаков существования протоколов удаленного управления в сети и сравнению этих признаков с признаками активности других сетевых протоколов.

Подраздел 4.1 определяет следующий список этапов исследования сетевой активности, необходимых для решения задачи выявления признаков удаленного управления в сети:

1. Проведение множества сессий удаленного управления системой, состоявших из передачи управляемой машине наборов однотипных команд, сбор данных, проходивших в этот момент по сети.

2. Анализ полученных данных, поиск участков сетевой активности, повторявшихся между проводимыми сессиями, сопоставление этих участков с действиями оператора управляющей машины.

3. Проведение сессий сетевой активности, отличной от удаленного управления, сравнение результатов с полученными в предыдущем этапе, выявление признаков, уникальных для сессий удаленного управления.

4. Сравнение полученных признаков между сессиями, использовавшими разные протоколы удаленного управления, выявление уникальных признаков для рассматриваемых протоколов. Далее приводится список ключевых наборов данных анализа сетевой активности, используемых для задачи выявления.

Этот подраздел также описывает создание экспериментальной сети из трех виртуальных машин и определяет порядок действий оператора во время использования программ удаленного управления в данной сети. Дополнительно определен порядок действий оператора при работе с общими сетевыми папками.

Подраздел 4.2 посвящен описанию интерфейса и возможностей разработанной программы анализа сетевой активности. Созданная на языке программирования Python программа позволяет получать проходящие по сети пакеты и извлекать из их заголовков ключевые для анализа данные, оценивать возможность существования сессии удаленного доступа в сети и тип используемой программы, предупреждать об этой возможности оператора, строить графики на основе характеристик пакета в режиме реального времени и сохранять результаты сессии для их последующего анализа позднее. Проводится демонстрация возможностей программы по сбору, анализу и визуализации характеристик сетевого трафика, рассматриваются режимы отображения и фильтрации получаемой информации. Показана возможность программы к определению используемой службы удаленного управления и выведению предупреждающих сообщений.

Также приводится сравнение разработанной программы с другим популярным сервисом анализа сетевого трафика Wireshark, рассматриваются преимущества программы в решении задач выявления признаков существования сетевых протоколов удаленного управления.

Подразделы 4.3, 4.4 и 4.5 приводят данные о сетевой активности службы удаленного рабочего стола Windows RDP, программы удаленного управления TeamViewer и программы удаленного управления Radmin соответственно. Приводятся графические примеры поведения программ в сети, проводится сопоставление между выполняемыми оператором действиями и изменениями характеристик передачи информации. Были выявлены особенности поведения, характерные для всех рассмотренных программ удаленного управления, а также обнаружены уникальные особенности работы каждой из рассматриваемых программ.

Подраздел 4.6 посвящен описанию сетевой активности при работе с общей сетевой папкой Windows по протоколу SMB и сравнению полученных данных с данными, полученными в подразделах 4.3, 4.4 и 4.5. Демонстрируется

разница в поведении между общими сетевыми папками и средствами удаленного управления.

В результате работ по анализу и сравнению особенностей сетевой активности программ удаленного доступа был сделан следующий вывод: появление в сети канала связи между двумя машинами по протоколу TCP, в котором объем передаваемых данных от одной из машин значительно превосходит объем получаемых данных, интенсивность передачи пакетов различается между машинами и получение машиной пакета данных не приводит к задержкам в отправке ответных пакетов, является признаком существования сетевого протокола удаленного управления.

Также были выявлены уникальные признаки сетевой активности для каждой из рассмотренных в работе программ удаленного управления, совокупность которых позволяет точно определить используемую программу управления.

Для RDP это:

1. Изменение сетевого порта управляющей машины после установления подключения в начале сессии.

2. Использование стандартного порта подключения 3389 (изменение номера порта требует наличия прав администратора на управляемой машине).

3. Меньший объем передаваемой информации от управляемой машины относительно других рассмотренных программ.

4. Больший объем передаваемой информации от управляющей машины относительно других рассмотренных программ.

Для Teamviewer это:

1. Обмен идентичными по структуре сообщениями в начале сессии управления.

2. Использование исключительно портов 5938, 443 или 80 (изменение невозможно без вмешательства в исходный код программы).

3. Непрерывный обмен пакетами на протяжении всей сессии удаленного управления.

Для Radmin это:

1. Использование порта 4899 (изменение требует доступа к серверному компоненту программы на управляемой машине).

2. Сочетание особенностей поведения RDP и больших объемов передаваемой информации, характерных для Teamviewer.

ЗАКЛЮЧЕНИЕ

В этой работе были рассмотрены некоторые программы удаленного управления, особенности их работы в сети и их отличия в поведении друг от друга. На основе этих отличий была построена система анализа, выявления сессий удаленного доступа и графической визуализации их особенностей. На примере была продемонстрирована возможность обнаружения, анализа и визуализации признаков сервисов удаленного управления RDP, Teamviewer и Radmin при помощи программы анализатора и визуализации трафика локальной сети. Были сделаны выводы о признаках, указывающих на присутствие в сети протоколов удаленного управления для каждой из рассмотренных программ. Работая с подобной программой, администратор сети может реагировать на появление возможной вредоносной активности, не нарушая при этом работу необходимых программ.