УДК 381.3

АНАЛИЗ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

© 2019 И. Я. Львович, А. П. Преображенский, О. Н. Чопоров

Воронежский институт высоких технологий (г. Воронеж, Россия)
Воронежский государственный технический университет (г. Воронеж, Россия)

В статье рассматриваются основные механизмы, используемые для создания безопасных сетевых соединений в организациях.

Ключевые слова: корпоративная сеть, безопасность, сетевая атака.

В современном мире существует множество компьютерных атак, которые вызывают серьезные проблемы в корпоративной сети. Чтобы защитить сеть от подобных воздействий, администратор сети должен провести работы по обнаружению в ней имеющихся уязвимости, на основе чего выбрать адекватные меры для повышения информационной безопасности и смягчения последствий возможных атак.

Изначально злоумышленники могут иметь ограниченную информацию об интересующей их сети, поэтому одной из основных задач злоумышленников является сбор информации о ней [1].

После того, как информация собрана, злоумышленники могут организовать несколько атак [2]. Информация может быть получена, например, при помощи WHOIS, чтобы найти доменное имя и IP-адрес целевой сети. Это нельзя рассматривать как преступление. Такие сведения можно использовать позже для выполнения атаки. Все сетевые атаки можно разделить на две части:

1. Атаки, требующие незначительного количества информации о целевой сети.

2. Атаки, требующие значительного количества информации о целевой сети.

Атаки, требующие меньше информации о целевой сети, делятся на:

- разведывательные атаки,
- атаки доступа,
- DOS и распределенные DOS-атаки.

Львович Игорь Яковлевич – Воронежский институт высоких технологий, д. т. н., профессор, office@vivt.ru.

Преображенский Андрей Петрович – Воронежский институт высоких технологий, д. т. н., профессор, app@vivt.ru.

Чопоров Олег Николаевич – Воронежский государственный технический университет, д. т. н., профессор, choporov_oleg@mail.ru.

Атаки, требующие дополнительной информации о целевой сети, подразделяются на:

- черви, вирусы и троянские кони;
- атаки прикладного слоя;
- угрозы протоколам управления.

Далее кратко описываются все нападения и методы их устранения, и уделяется больше внимания разведывательным нападениям и методам их обработки.

Рассмотрим разведывательные атаки. Данный вид нападения определяется как несанкционированное обнаружение и сопоставление систем, служб или уязвимостей целевой сети. Если злоумышленник или нарушитель хочет атаковать сеть, он нуждается в некоторой информации о целевой сети, IP-адресах, активных портах и сервисах, операционной системе на компьютере. С помощью разведывательных атак злоумышленник может собирать такую информацию и выполнять реальную атаку на целевую сеть. В течение значительного времени разведывательные атаки не обнаруживаются, так как не оказывают никакого влияния на сеть.

Разведывательные атаки – это начальный шаг злоумышленника для атаки на сеть. Для сбора информации о целевой сети, во-первых, злоумышленник выполняет ping целевой сети, чтобы получить список активных IP-адресов. Затем злоумышленник выполняет сканирование портов, чтобы определить, какие порты или службы активны на этих IP-адресах.

После определения динамических портов злоумышленник начинает запрашивать порты, чтобы узнать, какая операционная система работает, тип и версию приложений, запущенного программного обеспечения и конфигурации, которая была применена на целевом узле. Разведывательная ата-

ка может быть использована как административный инструмент или как атакующий инструмент.

При атаке используются следующие инструменты и технологии:

- анализатор пакетов;
- сканирование портов;
- команда PING;
- информационные запросы в Интернете.

Рассмотрим далее более подробно каждый из компонентов. Анализатор пакетов (сниффер) – это метод захвата каждого пакета, который передается по сети. Сквозной режим – это режим, в котором сетевая карта передает каждый пакет, полученный на физическом уровне в приложение для обработки.

Захват пакетов может быть разработан очень легко, когда сетевое приложение отправляет пакеты в обычном виде, без шифрования. Когда пакеты отправляются в простом виде, их легко захватить и получить из них информацию. Захват пакетов можно использовать как средство администрирования для мониторинга и проверки сетевого трафика или как средство атаки.

Рассмотрим сканирование портов и ping-сканирование. Как сканирование портов, так и ping-сканирование являются наиболее распространенным видом разведывательных атак. Они могут использоваться в качестве административных инструментов или в качестве средств взлома. Сетевой администратор будет использовать это средство для поиска уязвимых служб в сети. Хакер будет применять, чтобы службы использовать незаконным способом.

С помощью ping-сканирования злоумышленник получит IP-адреса целевой сети. Это можно сделать, отправив протокол ICMP-сообщение (Internet Control message Protocol) ping на каждый IP-адрес целевой сети или отправив сетевой пинг. ICMP-пинг будет отправлять Эхо-запросы к нескольким узлам. Если узел посылает ответные запросы, то компьютер с таким IP-адресом присутствует в сети. ping-сканирование относится к медленным и старым методам, используемым для сканирования сети.

С помощью сканирования портов злоумышленник может узнать открытые порты и сервисы, которые активны на компьютере с заданным IP-адресом. Сканирование портов выполняется путем отправки ряда сообщений целевым узлам. В зависимости от типа полученного ответа злоумышленник обнаружит, какие порты открыты, какие порты закрыты и какие службы связаны с этим портом. Всем службам присваиваются известные номера портов. Например, простой протокол передачи почты (SMTP) и порт 25. Если сканирование порта обнаружит номер порта 25, злоумышленник узнает, что узел использует SMTP. Чаще всего используются инструменты сканирования портов SAINT, Nmap и Nessus.

Рассмотрим запросы информации в Интернете. Запросы к Интернету для получения информации о веб-сайте или организации называются запросами к информации в Интернете. DNS - крупнейшие и активные распределенные базы данных, которые сейчас используются. Функция DNS заключается в том, чтобы перевести удобочитаемый доменное имя в машиночитаемые IP-адреса. Злоумышленники могут использовать этот интернет-инструмент, для получения информации из Интернета [3]. Нет способов для того, чтобы уменьшить эту угрозу. Предоставляя информацию DNS, организации должны убедиться в том, что должна быть предоставлена только определенная информация, которая не причиняет для них вреда.

Рассмотрим атаки доступа. Атаки доступа можно представить, как доступ к сетевому трафику незаконным способом. С помощью атак доступа злоумышленники могут получать данные, получать доступ и могут повышать свои права доступа в сетях или системах. Они используются для получения доступа к конфиденциальным базам данных, веб-счетов и другой конфиденциальной информации. Атака доступа может происходить различными способами.

Атаки доступа состоят из:

- атаки на пароль;
- эксплуатации доверия;
- перенаправления портов;
- атаки Man-in-the-middle;
- переполнения буфера.

Рассмотрим каждый их этих методов атаки.

Атаки на пароль. Пароли используются для проверки подлинности пользователей. Пароли являются очень конфиденциальными данными и легко захватываются хакерами, потому что они понятны человеку. Атаки паролей используются для угадывания системных паролей. Это делается путем серии попыток подобрать пароль системы злоумышленником. Атака по словарю является распространенным примером атаки паролем. Атака по словарю будет перебирать все возможные пароли пока не найдет нужный пароль.

Атаки паролем могут осуществляться следующими способами:

- перебор;
- троянская программа;
- Р-спуфинг;
- анализатор пакетов.

Эксплуатация доверия и перенаправление портов состоит в следующем. Устройства, работающие в общей среде, должны доверять информации, поступающей от других устройств. Хакеры попытаются использовать это доверие, получив доступ к одному из скомпрометированных устройств в сети [4]. При использовании доверия хакер может прослушивать или отправлять или изменять данные в качестве доверенного пользователя. Например, если хост демилитаризованной зоны (ДМЗ) скомпрометирован, то злоумышленник может воспользоваться этим для атаки на узел, подключенный к внутреннему интерфейсу брандмауэра.

Атака перенаправления портов – это тип атаки на использование доверия. С помощью взломанного хоста, атака перенаправление порта отправляет все пакеты на другой адрес. Она осуществляется путем установки программного обеспечения проброса портов, такого как HTTPtunnel или NetCat. С помощью перенаправления портов хакер может знать о коммуникациях, ID пользователя/пароле и протоколах, используемых в сети.

Man-in-the-Middle (MitM) атаки являются одним из самых интересных и сложных атак в плане обеспечении безопасности сети. Атака MitM может быть определена как атака, при которой злоумышленник будет читать и записывать данные, передаваемые между двумя хостами, не зная хостов. Для выполнения этой атаки злоумышленник должен иметь доступ к сетевым пакетам, передаваемым по сети. Атаки MitM также называются атаками на сессии. Атака MitM реализуется с помощью сетевых пакетов и протоколов маршрутизации и транспорта.

Основными целями атаки являются:

- нанесение ущерба конфиденциальности, целостности и доступности;
- сбор информации;
- повреждение передаваемых данных;
- внедрение новой информации в сетевые сессии.

Атака переполнения буфера является наиболее распространенной атакой, которая может поставить под угрозу безопасность компьютерной системы в сетевой среде. Переполнение буфера – это процесс переполнения или перегрузки пространства в буфере. Это делается путем программы, которая записывает данные за выделенный конец буфера в памяти.

Переполнение буфера обычно возникает как следствие ошибок и неправильного использования таких языков, как C или C++. Атаки переполнения буфера помогают всем существующим вредоносным червям распространяться с одной машины на другую. При атаке переполнения буфера злоумышленник может вставить свой собственный код в компьютер жертвы, чтобы контролировать или компрометировать службы хоста.

Рассмотрим особенности DOS и распределенных DOS-атак. После разведывательных атак DOS-атаки являются наиболее распространенной формой атак безопасности. DOS-атаки являются наиболее сложными для полного устранения, поскольку они не направлены на получение доступа к сети или информации в сети [5]. Злоумышленники используют DOS-атаки для предотвращения доступа законных пользователей к информации или службам в сети. DOS-атаки также могут быть направлены на целевую сеть, чтобы предотвратить исходящий трафик или предотвратить входящий трафик для определенных сетевых служб. DOS-атаки делают сервисы бесполезными для законного пользователя. DOS-атака может быть выполнена как Flood-атака, атака Ping of Death и SYN-атака. Наиболее распространенным типом атаки DOS является распределенная DOS-атаки.

Распределенная DOS-атака использует DOS-атаку на сервер и отправляет в сеть очень большое количество запросов. Чтобы обработать все запросы, сервер использует много времени и резко замедляет свою работу, вследствие чего становится недоступным для законного доступа и использования. Для выполнения распределенных DOS-атак, злоумышленникам требуется очень мало усилий, потому что они могут воспользоваться слабыми сторонами протоколов. Эти атаки очень трудно устранить, поскольку они атакуют трафик, который обычно разрешен в сети.

Вирусы, черви и троянские программы имеют следующие особенности. Вирус – это вредоносное программное обеспечение, прикрепленное к программе или файлу, способному выполнять определенную нежелательную функцию на компьютере. Вирус может сделать серьезные повреждения, такие как удаление файлов или стирание всего

диска. Некоторые вирусы очень просты и не нанесут никакого вреда. Вирус не может распространяться из одной системы в другую без человеческого взаимодействия. Вирус может распространяться путем совместного использования зараженного файла или открытия зараженного файла, или открытия вложения электронной почты, содержащего вирус.

Червь – это подкласс вируса, который может влиять на систему так же, как и вирус. Червь устанавливает свои копии в памяти компьютера и выполняет произвольный код. Черви могут распространяться из одной системы в другую систему без взаимодействия с пользователем. Черви имеют возможность заражать всю сеть. Черви используют преимущества автоматической отправки и получения файлов для распространения.

Троянский конь – это название программного обеспечения, которое выглядит полезным, но будет наносить урон после установки или запуска на системе. Троянский конь может нанести серьезный ущерб, как удаление файлов и уничтожения информации на вашей системе. Некоторые трояны просты и не причиняют никакого вреда. Троянские программы не могут воспроизвести или повторить себя, но они могут сделать систему уязвимой для многих атак.

Для расширения области вычислительной среды за пределы одной локальной сети или нескольких компьютеров требуется набор автоматизированных средств управления сетью. Для работы в среде с несколькими поставщиками необходима система сетевого управления [6, 7], основанная на стандартизированных протоколах сетевого управления и приложениях. Наиболее часто используемые протоколы управления Simple Network Management Protocol (SNMP), SysLog, Trivial File Transfer Protocol (TFTP) и Network Time Protocol (NTP). Если необходимые меры безопасности не будут приняты, эти протоколы могут быть скомпрометированы. SNMP используется для извлечения информации из сетевого устройства или удаленной настройки параметров устройства. SNMP версии 1 и 2 использует пароли в каждом сообщении в качестве простой формы безопасности. Эти версии SNMP отправляют пароли в виде обычного текста вместе с сообщением. Таким образом, эти версии могут быть перехвачены любым пользователем, у которого по пути к данным между устройством и сервером управления установлен приемник пакетов. SNMP версии 3 позволяет преодолеть эти недостатки путем предоставления аутентификации и шифрования для обмена сообщениями.

Протокол SysLog предназначен для передачи сообщений в виде устройства, настроенного для ведения журнала на сервере syslog, который собирает сведения. Сообщения отправляются в виде обычного текста между управляемым устройством и узлом управления. Syslog не имеет проверки целостности на уровне пакета, чтобы убедиться, что содержимое пакета не было перехвачено и изменено при передаче. Таким образом, злоумышленник может изменить данные SysLog, чтобы запутать администратора сети во время атаки.

TFTP используется для передачи системных файлов или конфигураций по сети. Системные файлы и конфигурации очень важны для защиты, потому что они могут раскрыть всю информацию сети, которая может привести к большому ущербу, как только злоумышленник захватывает данные.

Проблемы, связанные с повышением безопасности информационной сферы, требуют, чтобы в обществе и государстве на них обращалось постоянное внимание. Для обеспечения комплексной безопасности информационно-телекоммуникационных структур в организациях необходимо знать особенности возможных действий злоумышленников и использовать современный программный инструментарий, позволяющий максимально возможным образом смягчить возможные потери.

ЛИТЕРАТУРА

1. Львович, И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

2. Преображенский, Ю. П. Некоторые аспекты информатизации образовательных учреждений и развития медиакомпетентности преподавателей и руководителей / Ю. П. Преображенский, Н. С. Преображенская, И. Я. Львович // Вестник Воронежского государственного технического университета. – 2013. – Т. 9. – № 5-2. – С. 134-136.

3. Львович, И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова. – Воронеж, Издательство: Воронежский институт высоких технологий (Воронеж). – 2014. – 339 с.

4. Львович, И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

5. Lvovich, Ya. Оценка производительности и состава оборудования локальных компьютерных сетей / Ya. Lvovich, O. Choporov, Yu. Preobrazhenski // Information Technology Applications. – 2017. – № 2. – С. 18-33.

6. Колесников, А. С. Алгоритмизация оптимизационно-вариационного моделирования многокомпонентных систем / А. С. Колесников, Я. Е. Львович // Экономика и менеджмент систем управления. – 2016. – Т. 22. – № 4-1. – С. 170-177.

7. Львович, Я. Е. Оптимизация проектирования систем защиты информации в автоматизированных информационных системах промышленных предприятий / Я. Е. Львович, Д. С. Яковлев // Вестник Воронежского государственного университета инженерных технологий. – 2014. – № 2 (60). – С. 90-94.

THE ANALYSIS OF CORPORATE NETWORK SECURITY MECHANISMS

© 2019 I. Ya. Lvovich, A. P. Preobrazhensky, O. N. Choporov

Voronezh Institute of high technologies (г. Воронеж, Россия)
Voronezh state technical University (г. Воронеж, Россия)

The paper discusses the basic mechanisms on the basis of which there are opportunities to create secure network connections in organizations.

Keywords: corporate network, security, network attack.