Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Селезнев М.Н. Классификация систем обнаружения вторжений и построение абстрактной модели нарушителя // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2018. – №5 (май). – АРТ 268-эл. – 0,4 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Селезнев Михаил Николаевич,
студент 2 курса магистратуры,
Национальный Исследовательский Ядерный Университет «МИФИ»
Научный руководитель: **Бочкарев Петр Владимирович,**
аспирант кафедры экономики и менеджмента в промышленности.
Национальный Исследовательский Ядерный Университет «МИФИ»
г. Москва, Российская Федерация.
E-mail: seleminx@gmail.com

КЛАССИФИКАЦИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ПОСТРОЕНИЕ АБСТРАКТНОЙ МОДЕЛИ НАРУШИТЕЛЯ

Аннотация: В данной работе проведена классификация систем обнаружения вторжений, рассмотрены актуальные в настоящее время методы обнаружения вторжений. Приводится анализ возможностей, которыми обладает нарушитель.

Ключевые слова: система обнаружения вторжений, информационная безопасность, система предотвращения утечек данных, абстрактная модель нарушителя.

Seleznev Mikhail Nikolaevich,
Second-year master's student,
National Research Nuclear University MEPhI
Supervisor: **Bochkarev Petr Vladimirovich,**
post-graduate student, department of economics and management of industry.
National Research Nuclear University MEPhI
Moscow, Russian Federation.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

A TAXONOMY OF INTRUSION DETECTION SYSTEMS AND AN ABSTRACT MODEL OF THE INTRUDER

Abstract: In this work author created a taxonomy of intrusion detection systems considering relevant intrusion detection techniques existing today. In addition, this research provides an analysis of intruder's possibilities.

Keywords: intrusion detection system, information security, data leak prevention system, an abstract model of an intruder.

Обеспечение сетевой безопасности является одной из наиболее серьезных проблем для любого предприятия. Однако на сегодняшний день не существует ни одной системы с идеальной защитой. Данное несовершенство приводит к нарушению целостности, доступности и конфиденциальности информации, что в свою очередь ставит всю организацию под угрозу. Одной из главных проблем, с которой сталкиваются специалисты в области обеспечения информационной безопасности является сбор данных методах и способах атак, которые привели к НСД. Эти данные позволяют сделать выводы о сетевых атаках, узнать, как действуют нарушители, а также получить сведения о их мотивах. Анализ этих материалов и их практическое применение помогают не только получить больше информации о нарушителе, но и на их основе усовершенствовать системы защиты.

Согласно данным компании Symantec Corporation количество атак, а также уязвимостей, растет из года в год. Так, например, за 2014 год число направленных атак возросло на 91%, число обнаруженных брешей в системах безопасности возросло на 62% (через такие бреши было украдено около 552 миллионов учетных записей), количество веб-атак возросло на

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

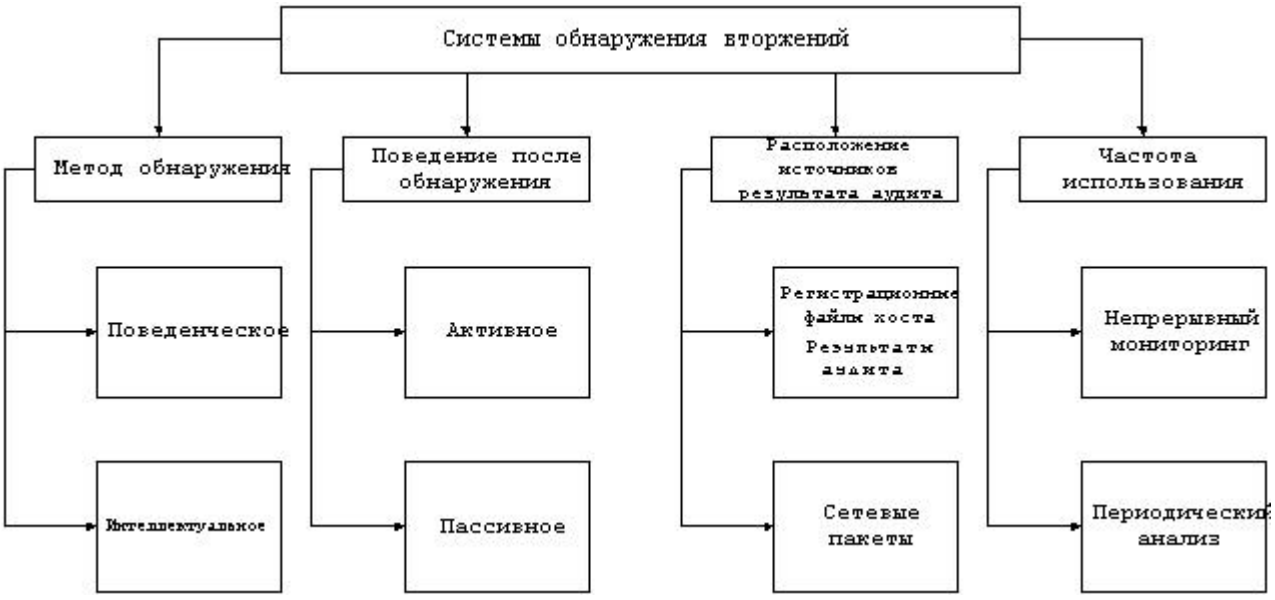
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

23%. Такая тенденция говорит о том, что, как и прогресс в обеспечении информационной безопасности, не стоит на месте, так и нарушители безопасности развиваются и прогрессируют каждую секунду находя все новые лазейки, причем последние, судя по статистике, ушли далеко вперед. То есть злоумышленники на шаг впереди. Чтобы устранить разрыв между злоумышленниками и специалистами по ИБ, необходимо знать каждый следующий шаг нарушителя ИБ.

Классификация СОВ

Классификация СОВ опирается на перечень факторов, без которых ее проведение невозможно (рисунок 1.1.) [2].

Говоря о методе обнаружения вторжений, следует обратить внимание на характеристики анализатора, которые он описывает. В случае, если IDS владеет информацией о нормальном поведении подконтрольной ей системы и эта информация используется при анализе текущего состояния, она называется поведенческой. Если анализ производится, опираясь на собранные ранее данные об атаках, такие системы относят в разряд интеллектуальных.



Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Рисунок 1.1 — Характеристики систем обнаружения вторжений [2]

Следующий фактор – поведение системы после обнаружения угрозы. Он описывает ответные действия СОВ при регистрации атаки. В некоторых случаях IDS производит различные корректирующие действия, устраняя возможные лазейки, которыми пользуется нарушитель, или же действует решительно, закрывая доступ к сервису до того момента, пока угроза не будет устранена. Если система не предпринимает никаких действий, а просто регистрирует и уведомляет об атаках, она называется пассивной.

Расположение источников результата аудита подразделяет IDS в зависимости от вида исходной информации, которую они анализируют. Входными данными для них могут быть результаты аудита, системные регистрационные файлы или сетевые пакеты.

Частота использования является последним фактором классификации. Он показывает, ведется ли со стороны СОВ непрерывный мониторинг подконтрольной системы, либо анализ производится время от времени. Второй вариант, разумеется, куда более опасен, ведь за относительно короткий временной промежуток системе может быть нанесен колоссальный ущерб.

Также существует еще несколько параметров, по которым могут классифицироваться системы обнаружения вторжений (рисунок 1.2):

- Существует два типа СОВ по способам реагирования – динамические и статические.

  Статические работают на основе снэпшотов всей среды, проводя анализ наличия уязвимостей в используемом ПО, ошибок настроек и конфигураций и т.д. Они производят проверку версий всех приложений на наличие уже известных уязвимостей, проверяют надежность паролей

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

и содержимое пользовательских файлов, подвергают анализу конфиги общедоступных сетевых сервисов с целью обнаружить следы уже свершенного вторжения. В этом их главное отличие от динамических IDS, осуществляющих непрерывный мониторинг всех внутрисистемных действий. Они следят за передаваемым сетевым трафиком и файлами аудита, позволяя безостановочно следить за безопасностью системы.

- По способу сбора информации различают сетевые и системные IDS. Сетевыми (NIDS, Network-Based Intrusion Detection System) производится контроль пакетов в сетевом окружении с целью обнаружения умышленных попыток проникновения внутрь системы, путем работы с сетевыми потоками информации. В качестве стандартного примера можно привести систему контроля TCP-запросов на соединение (SYN) с портами на защищаемом компьютере в поисках информации об осуществлении сканирования TCP-портов. Подобную IDS можно развернуть локально на компьютере и просматривать собственный трафик или использовать маршрутизатор, полностью контролирующий сетевой трафик. В основном, сетевые системы обнаружения вторжений запускаются с целью контроля одновременно множества компьютеров, в чем и заключается их главное отличие от других IDS.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Рисунок 1.2 — Классификация систем обнаружения вторжений [2]

Преимущества NIDS:

- Управление централизовано, что связано с масштабным покрытием для анализа;
- Можно использовать для мониторинга большой сети используя ограниченное количество ресурсов путем настройки оптимального расположения NIDS;
- Подключенные в защищаемую сеть маршрутизаторы не влияют на ее производительность и топологию;
- С целью повышения качества мониторинга, можно производить модификацию топологии сети, что не повлияет на ее функционирование, т.к. NIDS, в подавляющем большинстве, просматривают сегменты сети пассивным образом, напрямую не вмешиваясь в ее деятельность.

Недостатки NIDS:

- При отсутствии достаточной ресурсоемкости, соответствующей объему трафика подконтрольной сети, NIDS может выявить с

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

опозданием, либо не выявить вовсе атаку, начавшуюся одновременно со скачком внутреннего трафика;

- Зачастую требуют повышенной функциональности сетевых устройств, ведь встречаются сетевые коммутаторы, не предоставляющие универсального мониторинга портов, что сокращает диапазон мониторинга со стороны СОВ до одного хоста;
- Возрастает проблема, связанная с использованием организацией или злоумышленниками VPN, т.к. NIDS неспособны анализировать зашифрованную информацию;
- Регистрируют исключительно информацию о старте атаки без возможности проведения анализа о ее успешности, что повышает трудозатраты на ручное исследование перечня атакованных хостов для выявления свершившегося проникновения;
- К нестабильному функционированию NIDS может привести использование атакующим фрагментированных пакетов максимального допустимого размера, определяемого физическим уровнем, что повлечет со временем исчерпание системных ресурсов и отказ сервера.

IDS, которые устанавливаются на хосте и обнаруживают злонамеренные действия на нём называются хостовыми или системными IDS (Host-based IDS, HIDS). Примерами хостовых IDS могут быть системы контроля целостности файлов (СКЦФ), которые проверяют системные файлы с целью определения, когда в них были внесены изменения. Мониторы регистрационных файлов (Log-file monitors, LFM), контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами. Обманные системы, работающие с псевдосервисами, цель которых

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

заключается в воспроизведении хорошо известных уязвимостей для обмана злоумышленников.

Преимущества HIDS:

- Имеют возможностью следить за событиями локально относительно хоста, могут определять атаки, которые не могут видеть NIDS;
- Работают с зашифрованным сетевым трафиком благодаря тому, что источники информации на хосте создаются перед шифрованием данных и после того, как на хосте назначения производится расшифровка данных;
- На работу СОВ не влияет функциональность сетевых устройств.

Недостатки HIDS:

- Трудны в управлении, потому как сконфигурированы не централизовано, а привязаны к каждому целевому хосту;
- Под воздействием атаки на хост, сенсоры могут быть частично или полностью отключены, т.к. находятся на являющемся конечной целью атаки хосте. В результате атака частично затрагивает еще и саму СОВ, к чему она может быть не готова;
- Требует повышенной ресурсоемкости, поскольку забирает под свои нужны часть вычислительных ресурсов хоста, защиту которого производит.
- Позволяет производить мониторинг малой части сети, т.к. наблюдает лишь за трафиком отдельного хоста. Потому сетевые системы обнаружения вторжений не до конца покрывают задачи сканирования сети целиком или прочих исследований в поисках уязвимостей.

Методы обнаружения вторжений

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Впервые примененным методом обнаружения вторжений был именно метод анализа сигнатур. Суть заключается в проверке совместимости полученной последовательности с эталонным образцом. Во время данной проверки производится сравнение входящего пакета с сигнатурой, которая содержит в себе характеристики (в виде команд или ключевых фраз) вредного для системы трафика, после чего может быть объявлена тревога, если совпадение было обнаружено.[1]

Преимущества сигнатурного метода:

- Минимальный процент ложных сообщений вследствие высокой эффективности определения атак;
- Точная диагностика технологии атаки, либо использованного во время нападения инструментального средства.

Эти преимущества позволяют администраторам любого уровня квалификации в области информационной безопасности запустить обработку инцидента и принять меры обеспечения безопасности.

К недостаткам стоит отнести тот факт, что для поддержания эффективной работы СОВ необходимо частое обновление базы сигнатур новых атак.

Второй метод анализа заключается в анализе протоколов, имеющих строгий формат данных сетевого трафика. При передаче пакетов, каждый из них сопровождается соответствующими протоколами, чем и пользуются IDS, сравнивая протоколы с официальными стандартами. В случае нарушения стандартов по заполнению полей, в которых, разумеется, ожидаются нормальные значения, система сигнализирует о возможной злонамеренности со стороны отправителя.

Преимущества метода аномалий:

- Определение атаки без знания конкретных деталей (сигнатуры);

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур атак.

Недостатки метода аномалий:

- Повышенная частота ложных срабатываний в условиях непредсказуемости поведения пользователей и сетевой активности;
- Большие временные затраты на настройку и обучение системы в процессе определения нормальных характеристик поведения.

Дополнительно, отмечая преимущества и недостатки этих двух методов обнаружения вторжений, важно упомянуть еще несколько важных сторон систем анализа сигнатур:

- Несмотря на проведения полного анализа пакетов, его временной лог достаточно короткий;
- Правила, по которым будет анализироваться информация, легко написать и настроить;
- Перечень сигнатур новых угроз пополняется стремительно благодаря активной работе всего компьютерного сообщества в этой сфере;
- Наиболее эффективны при отлове простых атак, т.к. их основная масса использует ряд предварительных легко распознающихся действий.

Аналогичным образом, описывая системы обнаружения вторжений, использующих исключительно анализ сигнатур, важно дополнить и перечень их слабостей:

- В новой системе работоспособность будет невероятно высока, но с ростом количества проверяемых сигнатур и неизменных вычислительных ресурсах, скорость обработки событий начнет снижаться. В большинстве случаев каждая новая атака, если она хорошо спланирована, будет изучена и расширит список сигнатур. В

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

этом случае не смогут помочь даже эффективные на сегодняшний день методы работы с данными и вскоре большое количество немного отличных друг от друга атак смогут проникнуть сквозь подобную систему защиты;

- Важным моментом является то, что метод анализа сигнатур не подойдет для восприятия атак, с которыми система ранее не сталкивалась, т.к. такая система работает лишь со списком имеющихся в наличии сигнатур.

Однако статистика утверждает, что около 80% атак происходит по известным ранее сценариям. А это означает, что наличие в СОВ сигнатур этих известных атак значительно повысит шансы обнаружить несанкционированное вторжение и защитить конфиденциальные сведения организации.

В случае проведения анализов протоколов также есть перечень недостатков:

- Процесс анализа может проистекать довольно медленно по причине необходимости проведения тщательной экспертизы протоколов;
- Правила проверки протоколов для системы достаточно сложно описать из-за большого количества и четкой структуры каждого из них

В качестве дополнения иногда выделяют еще один способ анализа входящего трафика – метод политик. Его отличительной особенностью является то, что в нем существует свод правил в части распределения доступов, к примеру, какие из сетей могут взаимодействовать друг с другом и какие протоколы возможны при этом взаимодействии.

Преимущества метода политик:

- Имеет преимущества перед остальными методами в части обнаружения неизвестных ранее атак.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Недостатки метода политик:

- Процесс создания базы политик чрезвычайно трудоемкий, особенно в условиях большого масштаба подконтрольной СОВ сети.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Основные способы реализации угроз информационной безопасности

При определении основных способов реализации угроз информационной безопасности ресурсов ИС, учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла ИС, компонентов, условий функционирования ИС, а также - предположения о вероятных нарушителях.

Существует целый перечень способов реализации угроз информационной безопасности системы:

1. Использование штатных устройств и недостатков в разграничении доступов для несанкционированного взлома защищенной информации;
2. Внедрение вредоносного ПО в программные средства с целью оказания негативного воздействия на атакуемый объект;
3. Перенастройка доступов с последующей маскировкой под администратора с необходимым нарушителю перечнем прав к штатным средствам ИС;
4. Физическое хищение носителей информации или элементов системы, которые хранят в себе конфиденциальные данные;
5. Получение аутентификационной информации путем визуального несанкционированного просмотра;
6. Получение поверхностных сведений об ИС с использованием методов социальной инженерии, что может способствовать созданию благоприятной среды для применения иных способов реализации угроз;
7. Доступ к незаблокированным средствам администрирования ИС;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

8. Отказы в обслуживании и сбои программных средств информационной системы;
9. Негативное физическое воздействия на технические компоненты ИС с целью внесения неисправностей;
10. Осуществление несанкционированного доступа к информации в процессе ее передачи.

Действия нарушителя при атаке

Атаку можно описать как совокупность действий со стороны нарушителя, направленных на подрыв целостности информационной безопасности системы. Если атака была завершена успешно, обладатель несанкционированного доступа может не только нарушить работоспособность ИС, но и может внести искажения в хранящиеся в системе данные, выявить которые можно будет только путем проведения глубоко анализа. Серверы, пользовательские рабочие станции либо коммуникации и связанные с ними оборудование – все это потенциальные цели для атаки.

Существует три основных стадии организации атаки:

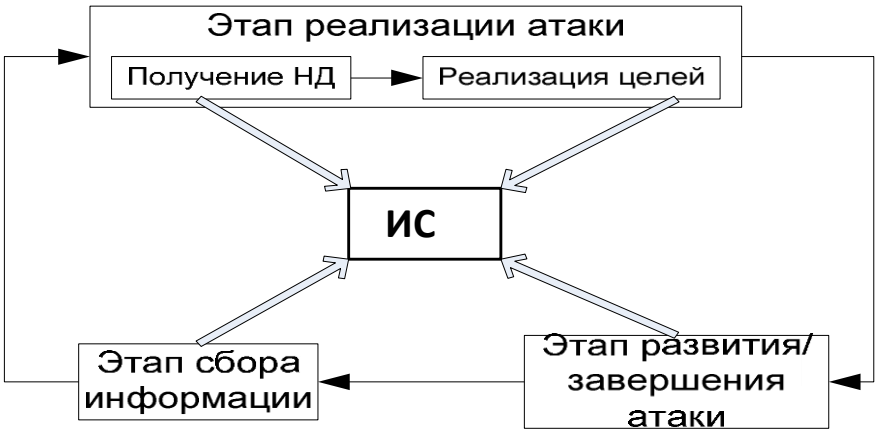


Рисунок 1.3 — Жизненный цикл атаки

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

На этапе рекогносцировки происходит сбор информации об объекте атаки для дальнейшего ее развития, а именно:

- тип операционной системы и ее версия, установленная на хостах ИС;
- перечень зарегистрированных в системе пользователей и уровни их прав доступов;
- различные сведения о прикладном ПО. [4]

Если осуществлять работы по данному этапу систематически, это поможет атакующему собрать полный перечень данных для описания профиля состояния информационной защиты сети.

Когда нарушителем собрана вся необходимая информация для вторжения, он переходит к получению несанкционированного доступа к ресурсам атакуемых им хостов. Это вторжение заключается в активации найденной на первом этапе уязвимости в системе. Примерами подобных уязвимостей могут служить не совсем точная настройка конфигурации внутрисетевых служб ИС, старые версии ПО, в которых еще не были исправлены известные атакующему ошибки в безопасности, использование администраторами и рядовыми пользователями слабых паролей, либо их редкое обновление, полное отсутствие средств защиты на некоторых узлах сети и т.д. Если злоумышленнику удалось получить доступ к объекту, обладающему ограниченными правами, с помощью специальных программных средств он будет стараться расширить свои полномочия в сети до статуса, когда будет возможен доступ не только к взломанной машине, но и остальной части сети. Другими словами, он запускает процесс расширения привилегий. Обычно этот процесс заканчивается на получении прав, равных учетной записи администратора или записи SYSTEM.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

На стадии атакующего воздействия на ИС нарушителем достигаются все цели, для которых была предпринята атака. Примерами успешного завершения атаки являются такие характеристики, как нарушение работоспособности ИС, на которую была направлена атака, получение конфиденциальной информации (примеры – извлечение из СУБД хоста номера кредитных карточек клиентов организации или ее сотрудников, доступ к зарплатным ведомостям), модификация или полное удаление данных, хранящихся в системе. При этом злоумышленник может предпринимать действия, направленные на сокрытие следов его нахождения в системе. Три самых широко используемых варианта удаления информации о присутствии в ИС это:

- установка руткитов
- использование шифрования к скачиваемым данным
- очистка логов

Дополнительно на данной стадии в информационную систему может внедряться вредоносное ПО, которое позже может использоваться нарушителем для атаки на другие хосты ИС. В этом случае атака снова переходит на первый этап своего жизненного цикла – этап сбора информации о следующей цели атаки.

В процессе реализации информационных атак злоумышленники могут использовать специализированное программное обеспечение, позволяющее автоматизировать действия, выполняемые различных стадиях атаки.

Техники и поведения нарушителей постоянно меняются, обнаруживая все новые и новые уязвимости, хакеры все больше совершенствуются, как и эксплуатировать их так и избегать быть обнаруженными. Несмотря на это, можно всё-таки выделить определенное поведение нарушителя, который

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

обычно действует по заранее продуманному плану. Такие действия, как правило, не всегда просто отличить от активности обычного пользователя и понять, что мы имеем дело с нарушителем ИБ. [3]

Список использованной литературы:

1. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Текст] / Сердюк В.А.: ГУ-ВШЭ, 2011 – 575с.
2. Таназ М. Анализ сигнатур или анализ протоколов, что лучше? [Электронный ресурс] / Таназ М. – Электрон. текстовые дан. - http://www.securitylab.ru/, свободный.
3. Тихонов А.Ю. Системы обнаружения вторжений [Электронный ресурс] / http://www.elibrary.ru/ - Проблемы информационной безопасности. Компьютерные системы, 2015 – 187-194с.
4. Толстой, А.И. Интрасети: обнаружение вторжений [Текст] / Толстой А.И., Милославская Н.Г.: ЮНИТИ-ДАНА, 2001. – 587с.

Дата поступления в редакцию: 25.05.2018 г.
Опубликовано: 26.05.2018 г.