МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Институт сферы обслуживания и предпринимательства (филиал)
федерального государственного бюджетного образовательного
учреждения высшего образования «Донской государственный
технический университет» в г. Шахты Ростовской области
(ИСОиП (филиал) ДГТУ в г. Шахты)

КОЛЛЕДЖ ЭКОНОМИКИ И СЕРВИСА

На правах рукописи

ИНФОРМАЦИОНАЯ БЕЗОПАСНОСТЬ

Методические указания
по выполнению практических работ
для подготовки обучающихся специальности
09.02.03 Программирование в компьютерных системах

Рассмотрены и рекомендованы для
использования в учебном процессе на
заседании педагогического совета
Протокол № 1от «31» сентября 2018 г

Шахты
ИСОиП (филиал) ДГТУ в г. Шахты
2019

Составитель:

Преподаватель высшей категории _____Е.Н. Семеренко
«___» _____ 2018

Рецензенты:

Преподаватель высшей категории
ГБПОУ РО «Дон-Текс» _____ Н.О.Бабаджанян
«___» _____ 2018

Преподаватель высшей категории
КЭС ИСОиП (филиал) ДГТУ в г. Шахты _____ Л.В. Завгородняя
«___» _____ 2018

Информационная безопасность: метод. указания по выполнению практических работ для подгот. обучающ. спец. 09.02.03 Программирование в компьютерных системах оч. и заоч. форм обучения / сост.преп Е.Н. Семеренко : Шахты, 2019. – 30 с.

Настоящие методические указания определяют цели и задачи, содержание работ, общие требования к выполнению практических работ, форму отчетов, краткие теоретические сведения.

Данные методические указания предназначены для углубления и закрепления теоретических знаний, полученных обучающимися на уроках теоретического обучения, а также приобретения навыков самостоятельной работы по дисциплине Информационная безопасность.

Предназначено для обучающихся специальности 09.02.03 Программирование в компьютерных системах.

.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данные методические указания предназначены для студентов специальности 09.02.03 Программирование в компьютерных системах.

Методические указания по выполнению практических заданий разработаны в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.03 Программирование в компьютерных системах с учетом соответствующей учебной основной образовательной программы.

Методические указания могут быть использованы как для проведения практических занятий, так и для индивидуального усовершенствования имеющихся навыков работы с компьютерными программными продуктами.

В методических указаниях приведены 4 практические работы. Для выполнения практических работ необходимы программные среды: ОС Windows, офисное программное обеспечение (текстовый процессор, табличный процессор).

Задания и вопросы методических указаний соответствуют уровню подготовленности студентов к изучению данной дисциплины.

В методических указаниях определены цели, требования к выполнению заданий и сдаче отчёта, приведены контрольные вопросы для самоподготовки и рекомендованы литературные источники.

Письменный отчет оформляется согласно «Правилам оформления и требованиям, введённым в действие приказом ректора ДГТУ № 227 от 30.12. 2015 года.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Практическое занятие - это занятие, проводимое под руководством преподавателя в учебной аудитории, направленное на углубление теоретических знаний и овладение определенными методами самостоятельной работы. В процессе таких занятий вырабатываются практические умения.

Перед практическим занятием следует изучить конспект лекции и рекомендованную преподавателем литературу, обращая внимание на практическое применение теории и на методику решения типовых ситуаций. На практическом занятии главное – уяснить связь решаемых ситуаций с теоретическими положениями.

Для ведения записей на практических занятиях обычно заводят журнал практических занятий. Логическая связь лекций и практических занятий заключается в том, что информация, полученная на лекции, в процессе самостоятельной работы на практическом занятии осмысливается и перерабатывается, при помощи преподавателя анализируется до мельчайших подробностей, после чего прочно усваивается.

Успешное освоение курса «Информационная безопасность» предполагает активное, творческое участие обучающегося путем планомерной, повседневной работы, которая позволит:

знать:

- знать основы информационной безопасности и защиты информации
- типовые средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем.

уметь:

- использовать принципы криптографических преобразований;
- использовать типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа.

Представленные, в данных методических указаниях, практические задания направлены на формирование общих и профессиональных компетенций:

ОК-1: Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес

ОК-2: Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК-3: Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК-4: Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК-5:. Использовать информационно-коммуникационные технологии в профессиональной деятельности

ОК-6: Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК-7: Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК-8: Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК-9: Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК-1.2: Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.

ПК-1.3: Выполнять отладку программных модулей с использованием специализированных программных средств.

ПК-1.5: Осуществлять оптимизацию программного кода модуля.

ПК-2.4: Реализовывать методы и технологии защиты информации в базах данных.

Наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания при решении задач.

При выполнении заданий обучающиеся имеют возможность пользоваться лекционным материалом, с разрешения преподавателя осуществлять деловое общение с товарищами.

Оценка компетентности осуществляется следующим образом: по окончании выполнения задания обучающиеся оформляют отчет, который затем выносится на завершающий этап формы изучения дисциплины. В процессе защиты выявляется информационная компетентность в соответствии с заданием на практическое занятие, затем преподавателем дается комплексная оценка деятельности обучающегося.

Задачи:

- подтверждение теоретических положений;
- закрепление нового материала;
- взаимосвязь нового материала с пройденными темами;
- формирование исследовательских умений (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты);
- обучение навыкам работы с текстом (понимать текст, различать его виды, анализировать содержащуюся в тексте информацию, делать выводы, различать точки зрения);
- формирование навыков работы в группе;
- обучение формулированию и аргументации своего мнения.

Требования к оформлению практических работ:

- цель работы;
- оснащение (оборудование, материалы и др.);
- теоретическая часть;
- практическая часть (порядок выполнения);
- выводы по работе;
- источники (литература);
- форма отчета практической работы (приказ № 227, раздел 5)
- Пример оформления практической работы показан в Приложении А

Критерии оценки выполненной работы:

- процент выполнения работы;
- достижение заданного результата;
- правильность выполнения заданий;
- наличие всех элементов работы;
- время выполнения работы.

2. ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа № 1
Модели нарушений информационных систем

1. **Цель работы:** изучить классификацию моделей нарушителей информационных систем, получить навыки формирования методологии модели нарушителей информационной системы предприятия.

Оснащение: OS Windows, MS Office.

Формируемые компетенции: ОК-2 ОК-3 ОК-4 ОК-6 ОК-7 ОК-9 ПК-1.2 ПК- 1.3

Теоретическая часть

Модель нарушителя — (в информатике) абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель нарушителя определяет:

категории (типы) нарушителей, которые могут воздействовать на объект;

цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.;

типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

Модель нарушителей может иметь разную степень детализации.

Содержательная модель нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.

Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны.

Под нарушителем в общем виде можно рассматривать лицо или группу лиц, которые в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону нарушители могут подразделяться на два типа:

нарушители, не имеющие права доступа в контролируемую зону территории (помещения) — внешние нарушители;

нарушители, имеющие право доступа в контролируемую зону территории (помещения) — внутренние нарушители.

Руководящим документом [2] в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ.

Нарушители в указанном РД классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ, подразделяются на четыре уровня.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, то есть воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования. Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

При этом в своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

Так же, модель нарушителя можно представить так: 1) Разработчик; 2) Обслуживающий персонал (системный администратор, сотрудники обеспечения ИБ); 3) Пользователи; 4) Сторонние лица.

Модели злоумышленников

Хакер-одиночка, обладающий стандартным персональным компьютером на базе Pentium 4, с модемным (реже выделенным) выходом в Интернет. Данный тип злоумышленников очень сильно ограничен в финансовом плане. Он необязательно обладает глубокими знаниями в области компьютерных технологий, чаще всего использует готовые компьютерные программы, доступные из Интернета, для реализации угроз через давно известные уязвимости. Вряд ли такой тип нарушителя обладает достаточными знаниями о построении информационной системы банка. Его действия больше носят экспериментальный характер, он не стремится получить доступ к определенной информации или модифицировать ее с целью извлечения выгоды. Ему просто

интересно провести некоторые действия с информационной системой банка, недоступными и неиспользуемыми простыми пользователями Интернета. Характер действия -- скрытый, в меру своих способностей. Чаще всего останавливается после проведения первого успешного воздействия. Для борьбы с подобными "исследователями" администраторам безопасности необходимо четко выполнять правила, предписанные политикой безопасности организации. Устанавливать самые последние версии используемых программных продуктов и ОС, а также выпускаемые к ним патчи и расширения. Отслеживать публичные списки обнаруживаемых уязвимостей в аппаратных и программных продуктах известных производителей и совершать рекомендуемые действия для предотвращения реализации угроз с использованием обнаруженных уязвимостей.

Объединенная хакерская группа. Исследуемый тип злоумышленников достаточно скован в своих финансовых возможностях. Она еще не обладает вычислительными мощностями уровня крупного предприятия и подобным пропускным каналом в Интернет. Но обладание суммарными знаниями в области компьютерных технологий представляют большую опасность. Такие злоумышленники используют всевозможные приемы для организации сканирования информационных систем с целью выявления новых уязвимостей, применяются также методы реализации угроз через уже известные уязвимости. Они в состоянии написать программы, которые используют обнаруженные уязвимости: сетевые черви, вирусы, трояны и другие вредоносные программные средства. Для выполнения своих планов они могут встраивать вредоносные программы в вычислительные системы своих жертв. При использовании таких программ они могут получить доступ к большим компьютерным мощностям вычислительных сетей крупных научных или военных ведомств, а также к каналу с высокой пропускной способностью, который соединяет пораженную сеть (сети) с Интернетом. Описанные действия позволяют им производить мощные атаки на информационные системы в сети Интернет. Чаще всего они действуют целенаправленно и могут предпринимать определенные усилия для получения представления о принципах функционирования системы защиты банка. Спектр их действий -- от подделки суммы на счете (модификация данных) до получения или уничтожения критичных данных по заказу. Планируя свои действия, группа предпринимает все возможные усилия для сокрытия факта несанкционированного доступа. Хакерская группа не останавливается до момента достижения поставленной цели или столкновения с непреодолимыми препятствиями для проведения дальнейшего вторжения. Для противостояния действиям подобных групп необходимо использовать последние достижения в области обеспечения информационной безопасности объекта.

Предприятие-конкурент. Данная модель включает в себя: собственные мощные вычислительные сети и каналы передачи данных с высокой пропускной способностью для выхода в Интернет; большие финансовые возможности;

высокие знания компьютерных специалистов как самой компании, так и нанимаемых "под заказ". Возможны попытки подкупа сотрудников службы безопасности или иные действия из области социальной инженерии. Конкуренты могут предпринять серьезные усилия для получения сведений функционирования системы информационной защиты, в том числе внедрить своего представителя в службу безопасности. Среди целей могут быть: блокирование функционирования информационной системы конкурента, нанесение подрыва в имидже, деструктивные действия, направленные на причинение непоправимого ущерба конкуренту, вплоть до его разорения и банкротства. Для этого используются самые изощренные методы проникновения в информационные системы и воздействия на потоки данных в ней. Действия конкурентов могут носить как скрытый, так и открытый, демонстративный характер. При осуществлении своих намерений конкурирующая сторона бьется до победного конца. Служба безопасности должна быть начеку и сама вести наблюдение за компаниями, со стороны которых возможно проявление недобросовестной конкуренции. Может применяться сбор информации, другие разведывательные действия, подкуп и перевербовка сотрудников.

Коррумпированные представители различных структур ведомственного уровня, а также спецслужбы различных государств. Они обладают практически неограниченными вычислительными и финансовыми возможностями, самостоятельно регулируют и контролируют трафик в сети Интернет. На их службе состоят самые высокопрофессиональные компьютерные специалисты. В некоторых странах известны примеры, когда вместо тюремного заключения или после него известного хакера берут в службу национальной безопасности. Эти специалисты участвуют в разработке стандартов по безопасности информации, сетевых протоколов и досконально знают возможности и недостатки всех компьютерных технологий. В процессе сертификации вычислительной системы представители ведомственных органов могут получать достаточно полную информацию о ее построении. Цели, преследуемые такой группой, весьма разнообразны и их невозможно предугадать заранее. Подобные преступные элементы могут не утруждать себя сокрытием своих действий и, как уже говорилось, практически ничто неспособно их остановить. Они могут пользоваться поддержкой как законодательных, так и иных правовых актов, а также опекой органов исполнительной и судебной власти. Опасность может исходить и от спецслужб или разведывательных служб других государств, имеющих личные интересы в данном секторе экономики или оказывающих воздействие на различные направления деятельности государства. Что можно сказать о борьбе с этой группой... Требуется организация защиты информации на очень высоком уровне, что подразумевает существенные издержки. Кроме этого, требуется создавать собственные службы безопасности, оснащенные и обученные лучше ведомственных, но такой поворот событий чреват вступлением в открытое противостояние с этими органами.

Классификация нарушителей (разделение делается по целям, преследуемым злоумышленником):

- хакеры -- собственное удовлетворение, без материальной выгоды;
- шпионы -- получение информации, которая может быть использована для каких-либо политических целей;
- террористы -- с целью шантажа;
- промышленные шпионы -- кража промышленных секретов, материальная выгода конкурентов;
- профессиональные преступники -- получение личной финансовой выгоды.

Среди целей, преследуемых нарушителями, отмечаются:

- любопытство;
- вандализм;
- месть;
- финансовая выгода;
- конкурентная выгода;
- сбор информации;
- военная или политическая выгода.

Для защиты вычислительных сетей от злоумышленного воздействия необходимо использовать программные и программно-аппаратные комплексы и системы обеспечения информационной безопасности. Для организации защиты от внешней потенциально враждебной информационной системы используются межсетевые экраны, системы построения виртуальных частных сетей (VPN), защищенные каналы передачи данных (протоколы SSL, SOCKS,IPsec), криптографические средства (ГОСТ, AES, RSA и др.), протоколы распределения ключей и сертификаты (X.509, SKIP, ISAKMP, PKCS, PEM и др.), системы аутентификации пользователей (PAP, S/Key, CHAP) и удаленного доступа (TACACS и RADIUS).

Модели угроз безопасности систем и способы их реализации

Моделирование процессов нарушения информационной безопасности целесообразно осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации – уязвимость – последствия» (рис. 1.).

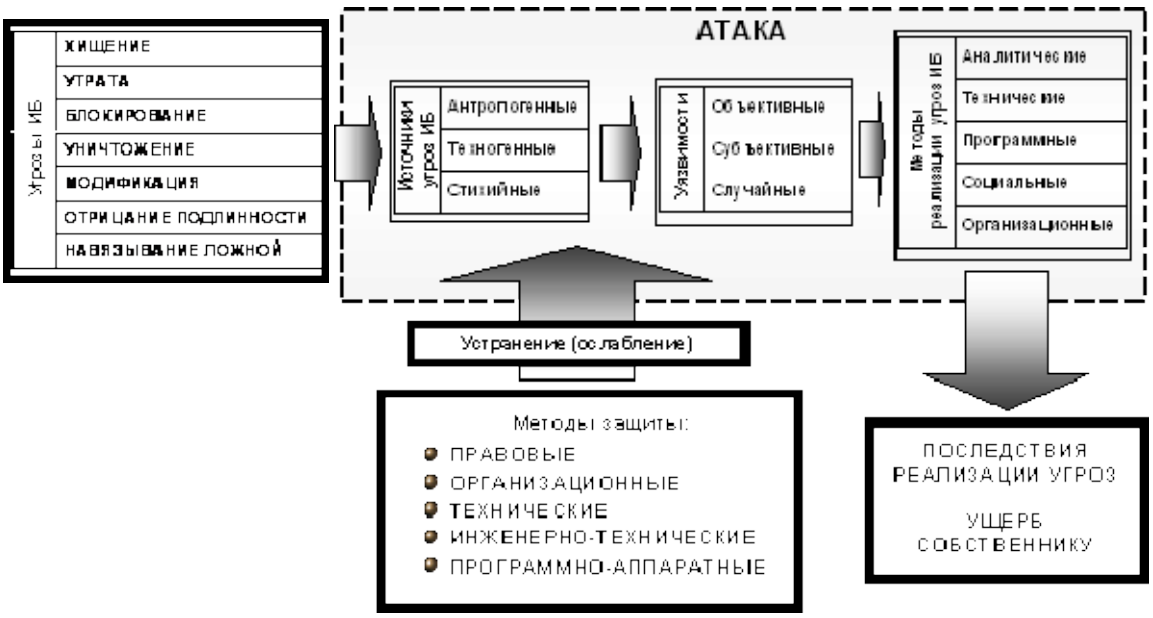


Рис. 1. Модель реализации угроз ИБ

В ходе анализа необходимо убедиться, что все возможные источники угроз идентифицированы, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, всем идентифицированным источникам угроз и уязвимостям (факторам) сопоставлены методы реализации.

При этом важно иметь возможность, при необходимости, не меняя самого методического инструментария, вводить новые виды источников угроз, методов реализации, уязвимостей, которые станут известны в результате развития знаний в этой области /2/.

Как видно, анализ негативных последствий реализации угроз предполагает обязательную идентификацию (например, присвоение уникального кода) возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации, то есть классификацию (рис. 2.).

Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также явиться следствием независящим от субъекта проявлений. Угроз не так уж и много.

Рис. 2. Цели и угрозы безопасности информации

Все источники угроз можно разделить на классы, обусловленные типом носителя, классы делятся на группы по местоположению (рис. 3.).

Рис. 3. Структура классификации «Источники угроз»

Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, классы на группы и подгруппы по проявлениям (рис. 4.).

Рис. 4. Структура классификации «Уязвимости»

Методы реализации можно разделить на группы по способам реализации (рис. 5.). При этом необходимо учитывать, что само понятие «метод», применимо только при рассмотрении реализации угроз антропогенными ис-

точниками. Для техногенных и стихийных источников, это понятие трансформируется в понятие «предпосылка».

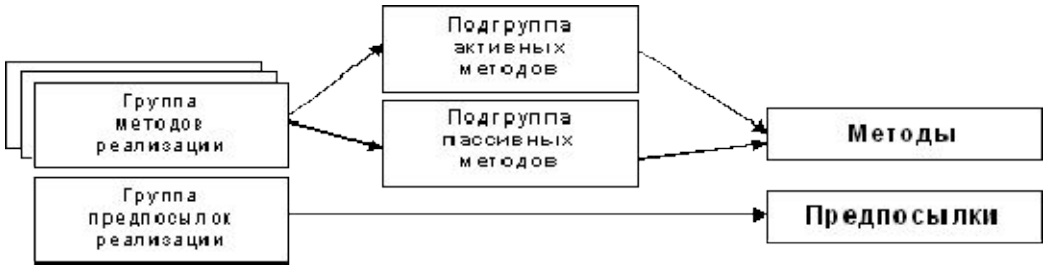


Рис. 5. Структура классификации «Методы реализации»

Классификация возможностей реализации угроз, то есть атак, представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки.

Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получения промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае не совпадения целей атаки с целью реализации угрозы, сама атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, то есть как «подготовка к совершению» противоправного действия.

Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Сам подход к анализу и оценке состояния безопасности информации основывается на вычислении весовых коэффициентов опасности для источников угроз и уязвимостей, сравнения этих коэффициентов с заранее заданным критерием и последовательном сокращении (исключении) полного перечня возможных источников угроз и уязвимостей до минимально актуального для конкретного объекта.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых АС и условий расположения и эксплуатации объекта

Практическая часть

Ответить письменно на вопросы:

1. Что такое модель нарушителя и что она определяет
2. Перечислите модели злоумышленников
3. Классификация нарушителей
4. Назовите модели угроз безопасности систем и способы их реализации
5. Классификация угроз безопасности
6. Классификация каналов утечки информации

Содержание отчета:

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Ответы на вопросы.
4. Вывод по работе.

Практическая работа № 2
Защита информации с помощью пароля

Цель работы: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Оснащение: OS Windows, MS Office.

Формируемые компетенции: ОК-2 ОК-3 ОК-5 ОК-6 ОК-7 ПК- 1.2 ПК-1.3 ПК-1.5 ПК- 2.4

Теоретическая часть

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1) минимальная длина пароля должна быть не менее 6 символов;

2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);

3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;

2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);

3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$ – число всевозможных паролей длины L, которые можно составить из символов алфавита A, V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия V определяется по следующей формуле:

$P = (V \cdot T) / S = (V \cdot T) / A^L$.

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$S^* = [V \cdot P / T]$, (1)

где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$S^* \le S = A^L$. (2)

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, T = 7 дней = 1 неделя, V = 10 (паролей / минуту) = 10 · 60·24·7 = 100800 паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие комбинации A и L, как A = 26, L = 8 (пароль состоит из восьми малых символов английского алфавита), A = 36, L = 6 (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Практическая часть

1. В табл. 1 найти для указанного варианта значения характеристик *P, V, T*.

2. Вычислить по формуле (1) нижнюю границу S^* для заданных *P, V, T*.

3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.

2. Коды цифр : «0» = 48, «9» = 57.

3. «!» = 33, «“» = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘» = 39.

4. Коды русских символов : «А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Таблица 1 - Варианты заданий

Вариант	*P*	*V*	*T*
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней

9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Содержание отчета.

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение, скриншоты.
4. Вывод по работе.

Контрольные вопросы:

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Практическая работа № 3
Работа с антивирусом

Цель работы: изучить теоретические основы вредоносных программ и антивирусного программного обеспечения, выполнить установку антивирус-

ной программы, тестирование съемных носителей и локальных дисков компьютера на наличие компьютерных вирусов.

Оснащение: OS Windows, MS Office.

Формируемые компетенции: ОК-1 ОК-3 ОК-4 ОК-5 ОК-8 ОК-9 ПК-1.2 ПК- 1.3 ПК-1.5

Теоретическая часть

Вредоносная программа — компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, ***препятствующего нормальному функционированию компьютерной системы. К*** вредоносному программному обеспечению относятся *сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты* и прочие программы, наносящие вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации — *угрозы нарушения целостности, конфиденциальности, доступности*.

1. Сетевые черви. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Некоторые черви обладают свойствами других разновидностей вредоносного программного обеспечения. *Например*, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

2. Классические компьютерные вирусы. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые

компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

3. Троянские программы. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

4. Хакерские утилиты и прочие вредоносные программы. К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Руткит (Rootkit) - *программа или набор программ, использующих технологии сокрытия системных объектов* (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) *посредством обхода механизмов системы*.

В системе Windows под термином руткит принято считать программу, *которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек*. Перехват и модификация низкоуровневых API функций в первую очередь *позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО*. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие

руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

Блокировать хакерские атаки;

- Не допускать проникновение сетевых червей;
- Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Практическая часть

Задание. Установить антивирусную программу. В операционной системе Windows проверить выбранные объекты на наличие вредоносных объектов, выполнить лечение или удаление зараженных объектов

Порядок работы

1) Запустить на выполнение антивирусную программу.
2) Запустить обновление из контекстного меню.
3) Выполнить проверку съемного носителя. Сделать скриншоты и вставить в работу
4) Выполнить проверку локального диска. Сделать скриншоты и вставить в работу
5) Отчет о работе антивирусной содержит информацию о результатах проверки.

Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение, скриншоты.
4. Вывод по работе.

Контрольные вопросы:

1. Дайте понятие компьютерного вируса.
2. Какие угрозы информации способны нанести вредоносные программы?
3. Для чего предназначены антивирусные программы?
4. Каковы функции брандмауэра?
5. В чем разница между антивирусными сканерами и мониторами?
6. Какие существуют признаки заражения компьютерным вирусом?
7. Что необходимо сделать в первую очередь в случае заражения компьютерным вирусом?

Практическая работа № 4
Межсетевые экраны

Цель работы: изучение теоретических аспектов, механизмов работы и вариантов совместного применения межсетевого экрана и сетевого сканера на примере ПО Agnitum Outpost и XSpider.

Оснащение: OS Windows, MS Office.

Формируемые компетенции: ОК-2 ОК-3 ОК-6 ОК-7 ОК-9 ПК- 1.2 ПК-1.3

Теоретическая часть

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую

Ярким примером наличия подобных уязвимостей могут послужить популярные операционные системы WindowsXP и FreeBSD. Так, в MS Windows, по умолчанию, работает довольно много неиспользуемых сервисов, которые в большинстве своем связаны с открытыми портами, через которые злоумышленник может провести атаку.

Что касается FreeBSD, то здесь также после стандартной установки в системе работают демоны, которые в обычных случаях не требуются, а значит, являются дополнительными источниками уязвимостей в компьютере. Атаки на почтовый сервер sendmail приводят к полному получению злоумышленником контроля над хостом.

Основными средствами защиты на сегодняшней день являются две категории специализированных программ:

- *Межсетевые экраны (брандмауэры, FireWall, МСЭ);*
- *Сканеры (сканеры открытых портов и сервисов).*

Следует сказать, что *брандмауэр* – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls).

Архитектура firewall

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания правил. В сущности, создаются два списка: отрицание (deny) и разреше-

ние (permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

- если никакое правило соответствия не найдено, то удалить пакет из сети;
- если соответствующее правило найдено в списке разрешений, то пропустить пакет;
- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. *Отметим преимущества firewall, основанного на фильтрации пакетов:*

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;
- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

- нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
- нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
- работа ведется с ограниченной информацией пакета;
- в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
- слабо защищен сам компьютер, на котором запущен firewall, то есть предметом атаки может стать сам этот компьютер;
- нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
- возможно, что большой объем правил будет тормозить проверку.

Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку пер-

вый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи.

Содержание таблицы следующее:

- уникальный идентификатор сессии передачи, который используется для контроля;
- состояние сессии передачи: установлено, передано или закрыто;
- информация о последовательности пакетов;
- адрес источника цепи;
- адрес получателя цепи;
- физический интерфейс, используемый для получения цепи;
- физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи. Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре.

Основные преимущества firewall цепного уровня:

- firewall цепного уровня быстрее программного, так как производит меньше проверок;
- firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
- возможно скрытие внутренней топологии сети.

Недостатки firewall цепного уровня:

- нет проверки пакетов на программном уровне;
- слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
- нет проверки передаваемых данных;
- трудно проверить разрешение или отрицание передачи пакетов.

Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется *proxy-сервис*, который кэширует информацию для более быстрой ее обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через *proxy*, который является шлюзом. У *proxy* две части: *сервер* и *клиент*. *Сервер* принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях.

Достоинства proxy:

понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;

- сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;
- возможен запрет доступа к некоторым сетевым сервисам;
- есть возможность управления пакетами данных;
- есть сокрытие внутренних адресов и топологии сети, так как proxy является фильтром;
- остается видимость прямого соединения сетей;
- proxy может перенаправлять запросы сетевых сервисов на другие компьютеры;
- есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
- возможно создание подробных отчетных записей для администратора.

Недостатки proxy:

- требует изменения сетевого стека на машине, где стоит firewall;
- нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как proxy перехватывает работу портов;
- неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно proxy;
- так как proxy должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой proxy;
- нет proxy для UDPи RPC;
- иногда необходима специальная настройка клиента для работы с proxy;
- proxy не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;
- корректность работы proxy напрямую связана с правильностью обработки сетевого стека;
- использование proxy может требовать дополнительных паролей, что неудобно для пользователей.

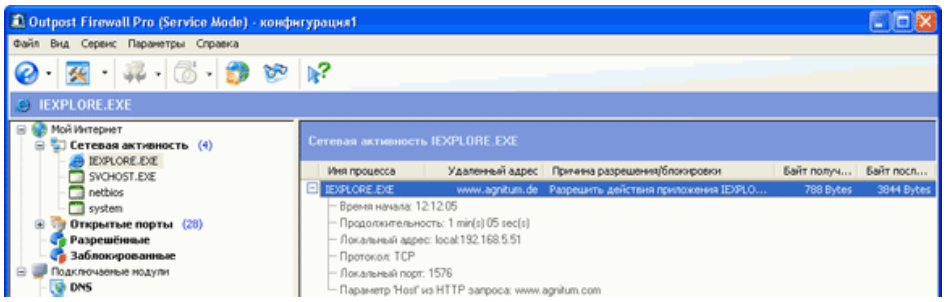
Примеры межсетевых экранов

1. Аппаратный (D-Link)

DFL-1100

Межсетевой экран для сетей крупных предприятий

2. Программный (Agnitum Outpost)



Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

Архитектура сканера

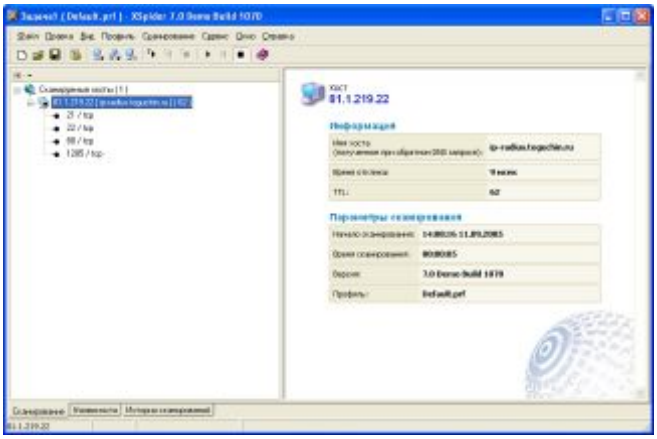
Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы. Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 10000.

Пример сканера XSpider



Практическая часть

Содержание отчета:

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Ответы на вопросы.
4. Вывод по работе.

Контрольные вопросы:

Письменно ответить на вопросы:

1. Назовите две категории специализированных программ, которые являются основными средствами защиты на сегодняшней день ?
2. Что такое брандмауэр
3. Что такое Сканер
4. Опишите архитектуру Firewall
5. Что такое фильтрация пакетов (packet filtering firewalls)
6. Как осуществляется механизм фильтрации пакетов
7. Что еще может изменять firewall, основанный на фильтрации пакетов,
8. Назовите преимущества Firewall, основанного на фильтрации пакетов:
9. Назовите недостатки Firewall:
10. Каковы основные преимущества firewall цепного уровня:
11. Недостатки firewall цепного уровня:
12. Firewall программного уровня
13. Вместе с firewall программного уровня используется proxy-сервис, как это работает,

СПИСОК ОСНОВНЫХ ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ

1. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах (Приказ Министерства образования и науки РФ от 28 июля 2014. № 804 " Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Дополнительная литература

Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

1 Васильков А. В.Безопасность и управление доступом в информационных системах : учеб. пособие / А.В. Васильков, И.А. Васильков. — М. : ФОРУМ : ИНФРА-М, 2017. — 368 с. — (Среднее профессиональное образование).http://znanium.com/catalog.php?item=bookinfo&book=537054

2 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с. — (Профессиональное образование).http://znanium.com/catalog/product/775200

3 Партыка Т. Л. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2017. - 432 с.: 60x90 1/16. ISBN 978-5-91134-627-0 http://znanium.com/catalog/product/882007

ПРИЛОЖЕНИЕ А
(обязательное)
ФОРМА ТИТУЛЬНОГО ЛИСТА

Форма титульного листа

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ СФЕРЫ ОБСЛУЖИВАНИЯ И ПРЕДПРИНИМАТЕЛЬСТВА (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» В Г. ШАХТЫ РОСТОВСКОЙ ОБЛАСТИ (ИСОиП (филиал) ДГТУ в г. Шахты)

КОЛЛЕДЖ ЭКОНОМИКИ И СЕРВИСА

Журнал практических работ

по дисциплине "Информационная безопасность" .

Выполнил _____ Паршина Т.П. группа КВ 9-212
(подпись) (инициалы, фамилия, группа)

Проверил _____ преподаватель Е.Н. Семеренко .
(подпись) ученая степень, зание, инициалы, фамилия)

ПРИЛОЖЕНИЕ Б
(обязательное)
ПРИМЕР ОФОРМЛЕНИЯ ПЕРВОЙ СТРАНИЦЫ ОТЧЕТА
Пример оформления первой страницы отчета

Практическая работа № 6

Тема: «Операционная система. Графический интерфейс. Windows XP. Работа с файловой системой»

Цель работы: Научиться отображать информацию о файлах разными способами; изучить стандартные действия над файлом.

Оснащение: OS Windows, MS Office.

Теоретическая часть

Windows - на русский язык переводится как окна. Окном называется ограниченная рамкой поверхность экрана. Все программы, которые выполняются с участием операционной системы, отображаются в окне. Пользователь может использовать окна для работы с папками и файлами, для запуска одного или нескольких приложений, для обмена данными между ними, для подключения и настройки различных устройств.

Окно может занимать весь экранили только его часть. Границы окна очерчены прямыми линиями. Различают три варианта представления окна на экране:

- свернутое окно. Оно занимает минимальную площадь и изображается в виде кнопки на панелизадач (taskbar). В свернутом окне приложение продолжает работать;
- окно нормального размера. Оно занимает часть площади экрана;
- полноэкранное окно (занимает весь экран и имеет максимальный размер).

…

Практическая часть

Задание 1.
Технология работы
1. Откройте папку «Мои документы».
2. Измените вид отображения папок и файлов внутри окна.

					И.23.02.03 120000.000 ПЗ		
Изм.	Лист	№ докум.	Подп.	Дата			
Разраб.		Иванов А.С.			Практическая работа № 6 Тема: «Операционная система. Графический интерфейс. Windows XP. Работа с файловой системой»	Лит.	Лист 1 / Листов 3
Проверил		Загородняя Л.В					
Н. Контр.						ИСОиП (филиал) ДГТУ гр.КВ9-118	
Утв.							