МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра «Информационная безопасность»

|  |
| --- |
| Утверждено на заседании кафедры  «Информационная безопасность»  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2022 г., протокол № \_\_\_\_\_ |
| Заведующий кафедрой  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Сычугов |

**ОПЕРАЦИОННЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению курсовой работы для студентов

специальности 075500 – Комплексное обеспечение информационной безопасности автоматизированных систем

Форма обучения: очная

Идентификационный номер образовательной программы: 090301-01-20

Тула, 2022 год

Методические указания к выполнению курсовой работы составлены к.т.н., доцентом Д.М. Антоновым и обсуждены на заседании кафедры «Информационная безопасность».

Протокол №\_\_\_ от "\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Зав. кафедрой ИБ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Сычугов

Оглавление

[1. Цель и задачи курсовой работы 5](#_Toc104006667)

[2. Тематика курсовой работы 5](#_Toc104006668)

[3. Исходные данные к курсовой работе 5](#_Toc104006669)

[4. Основные требования к курсовой работе 6](#_Toc104006670)

[4.1. Построение модуля анализ защищенности 6](#_Toc104006671)

[4.2. Построение модуля обнаружения атак 7](#_Toc104006672)

[4.3. Механизмы обнаружения атак 8](#_Toc104006673)

[5. Задание на курсовую работу 9](#_Toc104006674)

[6. Методические указания к работе 10](#_Toc104006675)

[6.1. Основные этапы проектирования 10](#_Toc104006676)

[6.2. Методические указания к выполнению отдельных этапов проектирования 11](#_Toc104006677)

[6.3. Объем и оформление курсовой работы 15](#_Toc104006678)

[7. Защита курсовой работы 15](#_Toc104006679)

[Список рекомендуемой литературы 16](#_Toc104006680)

[Приложение 1. Пример проверки, осуществляемой системой WebTrends Security Analyzer 18](#_Toc104006681)

[Приложение 2 Описание служб и параметров реестра в ОС Windows XP 21](#_Toc104006682)

## Цель и задачи курсовой работы

Курсовая работа по курсу «Безопасность операционных систем» выполняется для изучения устройства, принципов организации и взаимодействия подсистем защиты в ОС различной архитектуры, изучения защищенности заданных конфигураций различных операционных систем, изучения влияния различных настроек на уровень безопасности ОС и приобретения навыков построения комплексной системы безопасности в заданной конфигурации операционной системы.

## Тематика курсовой работы

Порядок функционирования систем безопасности ОС в общем случае определяется большим числом настроек параметров и элементов ее структуры, которые при инсталляции ОС по умолчанию устанавливаются таким образом, что решению задачи защиты информации в ОС отводится второстепенная роль. Данное обстоятельство вынуждает администратора ОС самостоятельно выбрать различные пути решения задачи обеспечения информационной безопасности информации в ОС.

В большинстве случаев особое внимание уделяется многочисленным настройкам параметров ОС с целью приведения порядка ее функционирования в соответствие неким формальным требованиям, а также проверке корректности работы отдельных защитных механизмов. В то же время вопросам определения ролей администратора и других привилегированных пользователей ОС, правил безопасного администрирования, порядка взаимодействия распределенных компонентов системы защиты уделяется недостаточно внимания. Не учитывается тот факт, что даже некоторые штатные действия пользователей могут нести угрозу безопасности всей системе, не говоря уже об ошибках администрирования или злонамеренных действиях по взлому отдельных элементов системы защиты.

## Исходные данные к курсовой работе

Основные этапы осуществления атаки: первый, подготовительный, этап заключается в поиске предпосылок для осуществления той или иной атаки. На этом этапе ищутся уязвимости, использование которых приводит к реализации атаки, т.е. ко второму этапу. На третьем этапе завершается атака, уничтожаются следы и т.д. При этом первый и третий этапы сами по себе могут являться атаками.

Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Первый, и самый распространенный, способ – это обнаружение уже реализуемых атак. Данный способ функционирует на втором этапе осуществления атаки. Этот способ применяется в "классических" системах обнаружения атак, межсетевых экранах и т.п. «Недостаток» средств данного класса в том, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. И так далее, до бесконечности. Второй путь – предотвратить атаки еще до их реализации. Осуществляется это путем поиска уязвимостей, которые могут быть использованы для реализации атаки. И, наконец, третий путь – обнаружение уже совершенных атак и предотвращение их повторного осуществления. Таким образом, системы обнаружения атак могут быть классифицированы по этапам осуществления атаки:

Системы, функционирующие на первом этапе осуществления атак и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners).

Системы, функционирующие на втором этапе осуществления атаки и позволяющие обнаружить атаки в процессе их реализации, т.е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании.

Системы, функционирующие на третьем этапе осуществления атаки и позволяющие обнаружить уже совершенные атаки. Эти системы делятся на два класса – системы контроля целостности, обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации.

## Основные требования к курсовой работе

В данной курсовой работе необходимо разработать сканер безопасности ОС, который состоит из двух основных компонентов. Первый производит анализ защищенности заданной конфигурации ОС, второй выполняет обнаружение реализуемых атак.

## Построение модуля анализ защищенности

Анализ защищенности проводится в несколько этапов:

1. *Сбор информации об узле*

На данном этапе идентифицируются все активные на нем сервисы и демоны.

1. *Обнаружение потенциальных уязвимостей*

Сканер использует базу данных для сравнения собранных данных с известными уязвимостями при помощи проверки заголовков или активных зондирующих проверок. Все уязвимости ранжируются по степени риска. Сетевые уязвимости (например, воздействующие на маршрутизаторы) считаются более серьезными по сравнению с уязвимостями, характерными только для рабочих станций. Аналогичным образом «поступает» и Internet Scanner. Все уязвимости в нем делятся на три степени риска: высокая (High), средняя (Medium) и низкая (Low).

1. *Подтверждение выбранных уязвимостей*

Сканер использует специальные методы и моделирует (имитирует) определенные атаки для подтверждения факта наличия уязвимостей на выбранных узлах сети.

1. *Генерация отчетов*

На основе собранной информации система анализа защищенности создает отчеты, описывающие обнаруженные уязвимости. Отчеты могут создаваться для различных категорий пользователей, начиная от администраторов сети и пользователей, и заканчивая руководством подраздления. Если первых в первую очередь интересуют технические детали, то для руководства компании необходимо представить красиво оформленные с применением графиков и диаграмм отчеты с минимумом подробностей. Немаловажным аспектом является наличие рекомендаций по устранению обнаруженных проблем. Отчет для каждой уязвимости может содержать пошаговые инструкции для устранения уязвимостей, специфичные для каждой операционной системы. Во многих случаях отчеты также содержат ссылки на FTP- или Web-сервера, содержащие patch'и и hotfix'ы, устраняющие обнаруженные уязвимости.

1. *Автоматическое устранение уязвимостей*

Этот этап очень редко реализуется в сетевых сканерах, но широко применяется в системных сканерах (например, System Scanner). При этом данная возможность может реализовываться по-разному. Например, в System Scanner создается специальный сценарий (fix script), который администратор может запустить для устранения уязвимости. Одновременно с созданием этого сценария, создается и второй сценарий, отменяющий произведенные изменения. Это необходимо в том случае, если после устранения проблемы, нормальное функционирование узла было нарушено. В других системах возможности «отката» не существует. Пример проверки, осуществляемой системой WebTrends Security Analyzer, приведен в приложении 1

## Построение модуля обнаружения атак

Основные компоненты модуля обнаружения атак:

1. *Подсистема управления компонентами*

Данная подсистема позволяет управлять различными компонентами системы обнаружения атак. Управление может осуществляться, как при помощи внутренних протоколов и интерфейсов, так и при помощи уже разработанных стандартов, например, SNMP. Под термином "управление" понимается как возможность изменения политики безопасности для различных компонентов системы обнаружения атак (например, модулей слежения), так и получение информации от этих компонент (например, сведения о зарегистрированной атаке).

1. *Подсистема обнаружения атак*

Основной компонент системы обнаружения атак, который осуществляет анализ информации, получаемой от модуля слежения. По результатам анализа данная подсистема может идентифицировать атаки, принимать решения относительно вариантов реагирования, сохранять сведения об атаке в хранилище данных и т.д.

1. *Подсистема реагирования*

Подсистема, осуществляющая реагирование на обнаруженные атаки и иные контролируемые события.

1. *Модуль слежения*

Компонент, обеспечивающий сбор данных из контролируемого пространства (журнала регистрации или сетевого трафика). У разных производителей называется также сенсором (sensor), монитором (monitor), зондом (probe) и т.д. В зависимости от архитектуры построения системы обнаружения атак может быть физически отделен (архитектура "агент-менеджер") от других компонентов, т.е. находиться на другом компьютере.

1. *База знаний*

В зависимости от методов, используемых в системе обнаружения атак, база знаний может содержать профили пользователей и вычислительной системы, сигнатуры атак или подозрительные строки, характеризующие несанкционированную деятельность. Эта база может пополняться производителем системы обнаружения атак, пользователем системы или третьей стороной, например, аутсорсинговой компанией, осуществляющей поддержку этой системы.

1. *Хранилище данных*

Обеспечивает хранение данных, собранных в процессе функционирования системы обнаружения атак.

## Механизмы обнаружения атак

Основными механизмами обнаружения атак являются

1. *Анализ журналов аудита*

Этот один из самых первых реализованных методов обнаружения атак. Он заключается в анализе журналов регистрации (log, audit trail), создаваемых операционной системой, прикладным программным обеспечением, маршрутизаторами и т.д. Записи журнала регистрации анализируются и интерпретируются системой обнаружения атак.

К достоинствам этого метода относится простота его реализации. Однако за этой простотой скрывается немало недостатков. Во-первых, для достоверного обнаружения той или иной подозрительной деятельности необходима регистрация в журналах большого объема данных, что отрицательно сказывается на скорости работы контролируемой системы. Во-вторых, при анализе журналов регистрации очень трудно обойтись без помощи специалистов, что существенно снижает круг распространения этого метода. В-третьих, до настоящего момента нет унифицированного формата хранения журналов. Анализ уже записанных в журнал регистрации записей говорит о том, что анализ осуществляется не в реальном режиме времени.

Как правило, анализ журналов регистрации является дополнением к другим методам обнаружения атак, в частности, к обнаружению атак "на лету". Использование этого метода позволяет проводить "разбор полетов" уже после того, как была зафиксирована атака, для того чтобы выработать эффективные меры предотвращения аналогичных атак в будущем.

1. *Анализ «на лету»*

Этот метод заключается в мониторинге сетевого трафика в реальном или близком к реальному времени и использовании соответствующих алгоритмов обнаружения. Очень часто используется механизм поиска в трафике определенных строк, которые могут характеризовать несанкционированную деятельность. К таким строкам можно отнести '\\WINNT\SYSTEM32\CONFIG' (данная строка описывает путь к файлам Sam, Security и т.д.) или '/etc/passwd' (данная строка описывает путь к списку паролей ОС Unix).

Использование метода обнаружения атак в сетевом трафике дает два основных преимущества. Во-первых, один агент системы обнаружения атак может просматривать целый сегмент сети с многочисленными хостами, в то время как, для предыдущего метода необходимо на каждый анализируемый узел устанавливать свой агент. Этот метод позволяет обнаруживать атаки против всех элементов сети предприятия, начиная от атак на маршрутизаторы и заканчивая атаками на прикладные приложения. Во-вторых, системы, построенные с учетом этого метода, могут определять атаки в реальном масштабе времени и останавливать атаки до достижения ими цели.

1. *Использование профилей «нормального» поведения*

Профили нормального поведения используются для наблюдения за пользователями, системной деятельностью или сетевым трафиком. Данные наблюдения сравниваются с ожидаемыми значениями профиля нормального поведения, который строится в период обучения системы обнаружения атак.

Этот метод используется в современных системах защиты информации при анализе лог-журналов и журналов аудита. Использование профилей нашло свое практическое применение в системах обнаружения мошенничества (fraud detection systems), используемых в финансовых структурах или у операторов связи.

1. *Использование сигнатур атак*

Данный метод очень часто сопоставляют с анализом "на лету". Метод заключается в описании атаки в виде сигнатуры (signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике, журнале регистрации и т.д.). В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Эти сигнатуры хранятся в базе данных, аналогичной той, которая используется в антивирусных системах. Собственно говоря, антивирусные резидентные мониторы являются частным случаем системы обнаружения атак, но т.к. эти направления изначально развивались параллельно, то принято разделять их.

## Задание на курсовую работу

При выполнении курсовой работы студент должен разработать программу-анализатор заданной конфигурации определенной ОС. Разработанная программа в соответствии с заданными параметрами должна оценить безопасность конфигурации ОС и указать пути ее улучшения.

Задание на проектирование выдается студенту в течение первых двух недель шестого семестра. Задание оформляется на типовом бланке отдельно на каждый проект, включая индивидуальные задания. На бланке типового задания указывается тема работы “Сканер безопасности ОС” и исходные данные, определенные по номеру варианта, заданному преподавателем. В течение первых четырех недель с момента выдачи задания исходные данные могут быть откорректированы по согласованию с руководителем работы. Индивидуальное задание должно быть согласовано с ведущим лектором курса «Безопасность операционных систем».

Проектируемый модуль определить:

* + вид операционной системы. (Windows 10, Windows 8, Windows 2003 и т.д.
  + тип и роль узла, DNS и NetBIOS, (выделенная рабочая станция, станция в локальной сети, сервер в локальной сети, контроллер домена, Web-сервер).
  + установленные обновления (согласно базы Microsoft).
  + примененную политику учетных записей (число администраторов, в локальной группе администраторов, имеющих высокие полномочия).
  + примененную политику паролей. (Выполнять проверку на простые пароли, слабые пароли, срок действия паролей, минимальная длина паролей).
  + примененную политику аудита (какие параметры включены/выключены).
  + сетевые настройки (TCP IP и т.д.)Открытые ресурсы (совместно используемые ресурсы, разделяемые ресурсы NetBIOS (NetBIOS Share)
  + запущенные сервисы (какие необходимы в различных случаях, особенно сетевые, анализ редко используемых сетевых сервисов)
  + файловую систему (тип файловой системы, определить права на доступ к особо важным файлам, разрешения на основные файлы и папки)
  + дополнительные параметры (шифрование SAM, агент восстановления, гостевой вход, кэширование паролей).
  + анализ журналов аудита – наиболее типичные атаки (Распознавание атак). Распознавание того, что были проведены подозрительные действия (непосредственно действия которые могут классифицироваться как подозрительные, нормальные, но произошедшие в неразрешенный момент времени, частота нормальных событий превышает некоторый порог).

**«Анализ журнала аудита ОС WINDOWS»**

В операционной системе проведены следующие настройки параметров протоколирования событий (Пример):

|  |  |
| --- | --- |
| **Политики** | **Значение** |
| Account Logon Events | Success and Failure |
| Account Management Events | Failure |
| Directory Service Access Events | Failure |
| Logon Events | Failure |
| Object Access Events | Failure |
| Policy Change Events | Failure |
| Privilege Use Events | No Auditing |
| Process Tracking | No Auditing |
| System Events | No Auditing |

1. Дать предложения по корректировке предложенной политики аудита;
2. Написать программу анализа журнала аудита по выявлению сомнительных/критичных. Анализируются не менее 10 видов событий.

## Методические указания к работе

## Основные этапы проектирования

Выполнение курсовой работы включает в себя следующие этапы:

Этап 1: Написание программного модуля, осуществляющего определение основных параметров ОС: роль узла, вид ОС, установленные обновления и т.д.

Этап 2: Реализация программного модуля работы с учетными записями и паролями. Определение учетных записей администраторов и политики безопасности в области паролей.

Этап 3: Реализация программного модуля сканирования реестра. Определение прав и привилегии пользователей. Системные настройки. Определение используемых сервисов. Оценка их необходимости.

Этап 4: Реализация программного модуля работы с файловой системой. Определение вида файловой системы, контроль доступа к системным файлам и т.д.

Этап 5: Написание программного модуля анализа журналов аудита ОС. Определение совершенных атак на ОС. Проверка целостности файлов настроек ОС. Формирование отчета: общая оценка защищенности заданной конфигурации ОС.

## Методические указания к выполнению отдельных этапов проектирования

Получение сведений об операционной системе в ОС Windows NT осуществляется функцией GET\_SYSTEM\_INFORMATION(). Входным данным которой является указатель на структуру MY\_SYSTEM\_INFO. Данная функция позволяет получить название операционной системы, роль, серийный номер, версию Service Pack. Для определения названия операционной системы, роли, серийного номера, версии Service Pack используется API функция GetVersionExA, в которую передаётся указатель на структуру типа OSVERSIONINFOEXA. Тип, версия и системный номер ОС определяются по сочетанию минорной и мажорной версии ОС и платформе.

Получение информации об имени DNS и NetBIOS происходит при помощи API функции GetComputerNameEx с соответствующими флагами ComputerNameNetBIOS и ComputerNameDnsHostname. Для получения размера буфера необходимо вызвать эту функцию с нулевым указателем на буфер, для возврата имени. Повторный вызов функции с указанием буфера возвращает в него имя DNS и NetBIOS.

Получение списка установленных заплаток осуществляется функцией void FUNK\_GET\_HOT\_FIXSES(), установленные хотфиксы прописываются в ключе реестра. Установленные заплатки прописываются в реестре в ключе HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\currentversion\hotfix. Этот ключ содержит список подключей заплаток, каждый из которых имеет два параметра: Installed (0 – заплатка не установлена, 1 – установлена) и Description (описание заплатки).

Для получения информации о блокировке учётных записей используется API функция NetUserModalsGet(). Правила блокировки учетных записей заносятся в структуру типа LPUSER\_MODALS\_INFO\_3.

Для получения информации о наличии у пользователей паролей без ограниченного срока действия используется API функция NetUserGetInfo(). Даная функция заносит информацию об учётной записи в структуру типа USER\_INFO\_1. Функция NetUserGetInfo() позволяет получить данные о заблокированных учётных записях.

При помощи функции NetUserEnum() получаем список всех пользователей на данном компьютере, который хранится в структуре типа USER\_INFO\_1. Затем перебираем всех пользователей и смотрим, является ли он администратором (имеет права администратора). Для этого служит элемент структуры usri1\_priv (если он равен USER\_PRIV\_ADMIN, то пользователь имеет права администратора). Затем смотрим на имя данного пользователя (элемент структуры usri1\_name). Если это имя похоже на имя администратора, т.е. «администратор», «Администратор», «админ», «Админ» и др., то выдаем сообщение о наличии непереименованной учетной записи «администратор».

При помощи функции NetUserModalsGet() получить данные о паролях в структуре типа USER\_MODALS\_INFO\_0. В данной структуре имеются два элемента: usrmod0\_max\_passwd\_age – хранит максимальный срок действия паролей; usrmod0\_min\_passwd\_age – хранит минимальный срок действия паролей. Если максимальный срок действия пароля не задан (= 0), то значение usrmod0\_max\_passwd\_age равно 0xFFFFFFFF, если минимальный срок не задан, то значение usrmod0\_min\_passwd\_age также равно 0xFFFFFFFF. Если сроки действия паролей заданы, то в элементах usrmod0\_max\_passwd\_age и usrmod0\_min\_passwd\_age хранятся максимальный и минимальный сроки действия паролей в секундах соответственно.

Возможность задавать более строгие правила фильтрации вводимых пользователями паролей определятся использованием библиотекой PASSFILT.DLL. При ее использовании производится проверка того, что новый пароль:

* + содержит не менее 6 символов;
  + содержит в себе символы по крайней мере 3-х наборов из 4-х возможных (прописные буквы латинского алфавита; строчные буквы латинского алфавита; цифры 0, 1,...9; специальные символы);
  + не содержит в себе имя пользователя или любую часть его полного имени.

Узнать, какие программные коррекции уже установлены в Windows Vista, можно, просмотрев ветку реестра HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\ .NETFramework\\ v3.0\\Windows Presentation Foundation\\RED\\1033\\Hotfix

Для работы с файлами и каталогами на жестких дисках операционная система Microsoft Windows NT поддерживает две файловые системы: FAT (File Allocation Table) и NTFS4 (New Technology File System), начиная с Windows 2000 – NTFS5. Между файловыми системами FAT и NTFS много различий в производительности, предоставляемых возможностях и т. д., но главное, что только NTFS обеспечивает защиту файлов и каталогов при локальном доступе (NTFS – единственная файловая система в Windows NT, которая позволяет назначить разрешения для отдельных файлов).

Файлы и каталоги – это частный вид разделяемых ресурсов, доступ к которым операционная система должна контролировать. В самом общем случае права доступа могут быть описаны матрицей прав доступа, в которой столбцы соответствуют всем файлам системы, строки – всем пользователям, а на пересечении строк и столбцов указываются разрешённые операции. Практически во всех ОС матрица прав доступа хранится «по частям», т.е. для каждого файла или каталога создаётся так называемый список управления доступом (Access Control List, ACL), в котором описываются права на выполнение операций пользователей по отношению к этому ресурсу. ACL являются частью характеристик файла или каталога. Список ACL состоит из элементов управления доступом (Access Control Element, ACE). Все объекты, включая файлы, потоки, события, токены доступа, когда они создаются, снабжаются дескриптором безопасности, который и содержит список управления доступом ACL.

Реестр (registry) Windows NT – это централизованная база данных, уникальная для каждого компьютера с данной операционной системой. В нем хранятся конфигурационные параметры для всех компонентов системы, включая установки оборудования, драйверов устройств, сетевых протоколов и плат адаптеров.

Для защиты локального доступа к реестру необходимо ограничить права группы Все (everyone для английской версии) для следующих ключей ветви HKEY\_LOCAL\_MACHINE:

* + Software;
  + Software\Microsoft\RPC (и подразделы);
  + Software\Microsoft\Windows\currentversion\Run;
  + Software\Microsoft\Windows\currentversion\runonce

В последних двух разделах перечислены приложения, которые выполняются (по крайней мере один раз) при запуске операционной системы Windows 2000. Они работают в контексте безопасности ОС и имеют доступ ко всем ресурсам компьютера;

* + Software\Microsoft\Windows\currentversion\Uninstall

Здесь расположен список программ, позволяющих убрать те или иные из ранее установленных на компьютере приложений; эти программы могут быть запущены от имени администратором Windows 2000 и будут выполняться в его контексте безопасности;

* + Software\Microsoft\Windows NT\currentversion\aedebug;
  + Software\Microsoft\Windows NT\currentversion\Compatibility;
  + Software\Microsoft\Windows NT\currentversion\Drivers;

Эти ветви реестра содержат информацию о производительности системы, поэтому следует ограничить доступ для группы Все к этим ветвям.

* + Software\Microsoft\Windows NT\currentversion\Ports (и подразделы);
  + System\currentcontrolset\Services\lanmanserver\Shares;

Регулируя разрешения на доступ к данному разделу, администратор может четко определить круг пользователей, имеющих право удаленного доступа к реестру данного компьютера.

Сервисом или службой называется обычное Windows-приложение, содержащую дополнительную инфраструктуру, которая позволяет рассматривать его особым образом, например, давать возможность администратору запускать и останавливать это приложение с удалённой машины.

Сама ОС Windows включает много служб, например Event Log, Net Logon, Messenger и др. Работа служб обеспечивается взаимодействием компонентов трёх типов:

* + диспетчер управления службами (Service Control Manager, SCM);
  + приложение-служба;
  + программа управления службой (Service Control Program, SCP).

SCP – это приложение, которое (в отличие от обыкновенной службы) имеет пользовательский интерфейс, позволяющий пользователю запустить, остановить, продолжить работу и выполнить другие функции управления службами, установленными на машине.

Информация о системных сервисах может быть получена непосредственно из реестра, где в разделе HKLM\System\CurrentControlSet\Services располагается информация о каждом из системных сервисов и его настройках, либо с помощью функций Win32 API для работы с сервисами.

Злоумышленник может попытаться подменить существующие сервисы своими, выполняющими вредоносные функции. Поэтому важно вовремя выявлять и удалять из системы «чужеродные» сервисы. Для выявления, например, можно проанализировать командную строку, и, если системный сервис запускается не из подкаталога каталога Windows, есть повод провести более детальную проверку.

Многие службы зависимы от других, поэтому если отключить слишком много лишнего, то можно столкнуться с такой ситуацией, что не удастся включить все обратно. Раздел реестра, отвечающий за запуск системных служб – HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Serviсes]. Основные стандартные службы при обычной установке Windows XP Porfessional приведены в Приложении 1 1.

Информацию о дополнительном шифровании SAM можно получить из реестра Windows. Необходимо анализировать ключ «SecureBoot» из ветки реестра HKEY\_LOCAL\_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Lsa. Значения данного ключа говорят о том, используется ли дополнительное шифрование SAM и как хранятся ключи. Например, если значение равно 0 – следовательно, дополнительное шифрование не используется; 1 – ключ располагается на локальном компьютере; 2 – не хранится, а генерируется при загрузке по паролю администратора; 3 – хранится на отдельной дискете.

DoS являются наиболее известной формой хакерских атак. Они просты в реализации и могут причинить огромный вред. Кроме того, против атак такого типа труднее всего создать гарантированную защиту. Типы DoS атак:

* + TCP SYN Flood
  + Ping of Death
  + Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K)
  + Trinco
  + Stacheldracht
  + Trinity

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к вашей сети или на получение из нее какой-либо информации. Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP. Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры.

Разработчики Microsoft предлагают осуществлять настройку определенных параметров для защиты от атак типа Dos и SYN Dos, которые представлены в таблице 2. Все параметры находятся в ключе реестра: HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters.

Таблица 1. Некоторые параметры конфигурации TCP/IP

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Описание** | **Рекомендуемые Значения** |
| DeadGWDetectDefault | Возможность использования резервного шлюза | 0 – не использовать |
| EnableSecurityFilters | Фильтрование IP-дейтаграмм | 1 – использовать |
| EnablePMTUDiscovery | Обнаружение MTU (максимальный размер пакета) | 0 – ограничение MTU до 576Б |
| SynAttackProtect | Уровень защиты от SYN атаки | 2 – высокий уровень защиты |
| TcpMaxHalfOpen | Максимальное количество состояний **SYN RECEIVED**, которые могут быть одновременно обработаны, прежде чем сработает **SYN** защита | 500 |
| TcpMaxHalfOpenRetried | Максимальное количество полуоткрытых подключений, для которых операционная система выполнила по крайней мере одну повторную передачу, прежде, чем сработает **SYN** защита. | 400 |
| TcpMaxPortsExhausted | Определяет число отклоненных **SYN** запросов, после которого **сработает** защита от **SYN** атак. | 5 |

## Объем и оформление курсовой работы

Курсовая работа состоит из пояснительной записки и информационно-программных средств, реализующих задание на курсовое проектирование.

Пояснительная записка (ПЗ) выполняется на листах белой бумаги формата А4 (210x297 мм) машинописным или рукописным способом, оформляется согласно требованиям ЕСПД и должна содержать: титульный лист; бланк задания; введение; основное содержание (1 часть – общая постановка задачи и пути ее решения, 2 часть – решение в общем виде, 3 часть – назначение отдельных модулей и их взаимодействие, 4 часть – контрольный пример); заключение; библиографический список; приложение, содержащее фрагменты программ и изображения входных и выходных документов, подтверждающие выполнение основных этапов курсовой работы и отражающие ее отличия от других вариантов заданий.

Работающие варианты программ вместе с исходными текстами предоставляются преподавателю в электронном виде.

## Защита курсовой работы

Выполненная и оформленная полностью курсовая работа предоставляется руководителю на проверку, который после проверки пояснительной записки и информационно-программного обеспечения подписывает ее к защите или возвращает студенту на доработку в зависимости от готовности работы.

Защищается курсовая работа перед комиссией из двух-трех преподавателей кафедры.

Защита работы заключается в кратком докладе студента об основных проблемах, возникших при разработке информационно-программного обеспечения, принятых им способах их решения и полученных результатах, и ответа им на вопросы членов комиссии, с демонстрацией работы программы.

Комиссия оценивает защиту, как по качеству выполненной работы (эффективности работы программы и соответствия ее заданию), так и по уровню знаний студента, проявленных им в процессе защиты.

В случае неудовлетворительной оценки студент получает новое задание и выполняет работу заново.

## Список рекомендуемой литературы

1. ГОСТ 28388 - 89 СОИ. Документы на магнитных носителях данных. Порядок выполнения и обращения.
2. ГОСТ 2.105 – 95 «Общие требования к текстовым документам»
3. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»
4. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»
5. ГОСТ 34.201-89\* . «Информационная технология. Комплекс стандартов на автоматизированные системы. Документация на АСУ. Виды, комплектность и обозначения документов при создании автоматизированных систем»
6. ГОСТ 51188-98. «Испытания программных средств на наличие компьютерных вирусов»
7. Оформление текстовых и графических документов по вычислительной технике: методические указания / Составитель Т.И. Матикашвили, ТулГУ, Тула, 1997. -56 с.
8. Компьютерное оформление отчетных документов / Составитель Т.И. Матикашвили, ТулГУ, Тула, 2000. -36 с.
9. Курило А.П., Зефиров С.Л., и др. «Аудит информационной безопасности». – М. Издательская группа БДЦ Пресс» ,2006г – 304 стр.
10. Девятин П.Н. «Модели безопасности компьютерных систем: Учебн.пособие для студентов высших учебных заведений». – М.: Издательский центр «Академия», 2005г – 144ст.
11. Норткат Стивен, Новак Джуди «Нарушения безопасности в сетях, 3-е издание», –М.: изд. дом «Вильямс», 2003г –448ст.
12. Р.Брагг, «Система безопасности Windows 2000». – М.: Вильямс, 2001г
13. Х. Кастер. Основы Windows NT и NTFS. Русская Редакция. М. 1996.
14. С.В. Крутов. Операционные системы. М. в/ч 33965. 1996.
15. В. Г. Проскурин, С.В. Крутов, И.В. Мацкевич. Защита в операционных системах. М. Радио и связь. 2000.
16. Лукацкий А.В. Атаки на информационные системы. Типы и объекты воздействия. Электроника: Наука, Технология, Бизнес. №1, 2000г.
17. Лукацкий А.В. Средства анализа защищенности. "Мир Internet", №3, 1999г
18. Курило А.П., Зефиров С.Л. и др Аудит информационной безопасности. М: Издательская группа «БДЦ-пресс», 2006г
19. Щеглов А.Ю. Защита компьютерной информации от НСД. СПБ: Издательство Наука и Техника, 2004г
20. Скембрей Д, Мак-Клар С. Секреты хакеров. Безпасность Windows Server 2003 – готовые решения – М. Издательский дом «Вильямс» , 2004 – 512 с

## Приложение 1. Пример проверки, осуществляемой системой WebTrends Security Analyzer

<TestAuthor> WebTrends Corporation </TestAuthor>

<TestCopyright> Copyright 1998, WebTrends Corporation, All Rights Reserved.

</TestCopyright>

<TestVersion> 2.0 </TestVersion>

====================================================================

<TestDependency>estabvc</TestDependency>

<TestCategory>inventory</TestCategory>

====================================================================

<TestTitle>Query OS Type via Netbios</TestTitle>

<TestVulnerabilityDescription>

This test attempts to determine the operating system type and version

running on the specified hosts.

</TestVulnerabilityDescription>

====================================================================

<Test>

# osdetectnt.pl

# attempt to detect OS using a netbios over tcp/ip call

require "crowbar.pl";

$theTargetNetbiosName = GetStringParam($crowbar::WTDB\_NetbiosName);

crowbar::WTDebugOutput

("OSDetect -- the target netbios name is $theTargetNetbiosName");

if($theTargetNetbiosName){

$a = crowbar::WTGetNTOSInfo($theTargetNetbiosName);

if($a){

$a =~ /^OSTYPE (.\*):VERSION (.\*)/;

$type = $1;

$version = $2;

crowbar::WTDebugOutput("Type is $type, version is $version\n");

if($version =~ m/OSVersion\_Unknown/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSVersion,

length("Unknown") + 1,

"Unknown", -1);

}

elsif($version =~ m/OSVersion\_WindowsNT\_3\_5\_0/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSVersion,

length("Version 3.5") + 1,

"Version 3.5", -1);

}

elsif($version =~ m/OSVersion\_WindowsNT\_3\_5\_1/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSVersion,

length("Version 3.51") + 1,

"Version 3.51", -1);

}

elsif($version =~ m/OSVersion\_WindowsNT\_4\_0/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSVersion,

length("Version 4.0") + 1,

"Version 4.0", -1);

}

elsif($version =~ m/OSVersion\_WindowsNT\_5\_0/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSVersion,

length("Version 5.0") + 1,

"Version 5.0", -1);

}

if($type =~ m/OSType\_Unknown/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Unknown") + 1,

"Unknown", -1);

}

elsif($type =~ m/OSType\_Unix/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Unix Server") + 1,

"Unix Server", -1);

}

elsif($type =~ m/OSType\_WindowsNTServer/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows NT Server") + 1,

"Windows NT Server", -1);

}

elsif($type =~ m/OSType\_WindowsNTPDC/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows NT Primary Domain Controller") + 1,

"Windows NT Primary Domain Controller", -1);

}

elsif($type =~ m/OSType\_WindowsNTBDC/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows NT Backup Domain Controller") + 1,

"Windows NT Backup Domain Controller", -1);

}

elsif($type =~ m/OSType\_WindowsNTWorkstation/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows NT Workstation") + 1,

"Windows NT Workstation", -1);

}

elsif($type =~ m/OSType\_WindowsNT/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows NT") + 1,

"Windows NT", -1);

}

elsif($type =~ m/OSType\_Windows95/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows 95/98") + 1,

"Windows 95/98", -1);

}

elsif($type =~ m/OSType\_Windows98/){

crowbar::WTAddRecord( $crowbar::WTDB\_OSType,

length("Windows 98") + 1,

"Windows 98", -1);

}

}

}

</Test>

Пример проверки, осуществляемой системой CyberCop CASL

# spoof\_check.cape

# this script is used by the built-in filter checks

# please do not modify it

ip

ip\_version=4

ip\_proto=IPPROTO\_UDP

ip\_flags=0

ip\_id=42

ip\_done

udp

udp\_sport=6834

udp\_dport=5574

udp\_done

data=SAS-ipspoofing

end\_of\_packet

## Приложение 2 Описание служб и параметров реестра в ОС Windows

* **Alerter (Оповещатель)**

Посылает выбранным пользователям и компьютерам административные оповещения. Если служба остановлена, программа, использующая административные оповещения их не получит. При обычных условиях эта служба не нужна.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Alerter]

"Start"=dword:00000004

* **Application Layer Gateway Service (Служба шлюза уровня приложения)**

Оказывает поддержку протоколов третьей стороны протоколов PnP для общего доступа к подключению к Интернету и подключений к Интернету с использованием брандмауэра. Эта служба нужна при использовании Брандмауэра Интернета / Общего доступа к Интернету для подключения к сети. Служба занимает около 1.5 Mb в оперативной памяти. У кого нет сети можно отключить эту службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ALG]

"Start"=dword:00000004

* **Automatic Updates (Автоматическое обновление)**

Нужен для подключения компьютера к центру Windows Update для автоматического скачивания обновлений для вашей системы. Если вы отключите эту службу то переодически будет значок в трее. Для того чтобы это убрать выключите Центр безопастности (на Брандмауэр не влияет).

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv]

"Start"=dword:00000004

* **COM+ Event System (Система событий COM+)**

Поддержка службы уведомления о системных событиях (SENS), обеспечивающей автоматическое распространение событий подписавшимся компонентам COM. Если данная служба остановлена, SENS будет закрыта и не сможет предоставлять уведомления входа и выхода.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventSystem]

"Start"=dword:00000004

* **Cryptographic Services (Службы криптографии)**

Предоставляет три службы управления: службу баз данных каталога, которая проверяет цифровые подписи файлов Windows; службу защищенного корня, которая добавляет и удаляет сертификаты доверенного корня центра сертификации с этого компьютера; и службу ключей, которая позволяет подавать заявки на сертификаты с этого компьютера. Если эта служба остановлена, все эти службы управления не будут работать. По сути, эта служба проверяет подписи файлов Windows. Однако, вы все равно можете получать окошко с предупреждением о неподписанном драйвере. Эта служба необходима для обновления Windows в ручном и автоматическом режимах, а также для инсталляции Service Pack’ов и DirectX 9.0. Windows Media Player и некоторые .NET приложения могут требовать эту службу для функционирования некоторых функций. Служба занимает около 1.9 Мб в оперативной памяти.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CryptSvc]

"Start"=dword:00000004

* **DCOM Server Process Launcher (Запуск серверных процессов DCOM)**

Provides launch functionality for DCOM services.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DcomLaunch]

"Start"=dword:00000004

* **DHCP Client (DHCP-клиент)**

Управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Эта служба автоматически получает ваш динамический IP адрес от вашего DHCP сервера и DNS обновлений. Необходима для ISC (интернет клиента) и в случае, если у вас используется IPSEC. Может быть отключена на системах со статическим ip-адресом. Примечание: Имейте ввиду, что многие DSL или кабельные подключения требуют эту службу для предоставления доступа в Интернет. Если вы отключите эту службу и ваше Интернет соединение перестанет работать, то верните значение в Автоматически.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp]

"Start"=dword:00000004

* **Distributed Link Tracking Client (Клиент отслеживания изменившихся связей)**

Поддерживает связи NTFS-файлов, перемещаемых в пределах компьютера или между компьютерами в домене.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TrkWks]

"Start"=dword:00000004

* **DNS Client (DNS-клиент)**

Разрешает для данного компьютера DNS-имена в адреса и помещает их в кэш. Если служба остановлена, не удастся разрешить DNS-имена и разместить службу каталогов Active Directory контроллеров домена. Данная служба получает и кеширует DNS имена и фнкции контроллера домена Active Directory. Однако, DNS клиент необходим для IPSEC. Если вы пытаетесь "исправить" ваше сетевое соединение и получаете диалоговое окно: "DNS resolver failed to flush the cache", то данная служба является причиной возникновения данной ошибки.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache]

"Start"=dword:00000004

* **Error Reporting Service (Служба регистрации ошибок)**

Позволяет регистрировать ошибки для служб и приложений, выполняющихся в нестандартной среде. При возникновении ошибки отправляет информацию об ошибки в корпорацию Microsoft. Я считаю, что это пустая трата памяти. Однако, если ваша система постоянно "падает", то данная служба является одним из лучших способов решить ваши проблемы.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ERSvc]

"Start"=dword:00000004

* **Event Log (Журнал событий)**

Обеспечивает поддержку сообщений журналов событий, выдаваемых Windows-программами и компонентами системы, и просмотр этих сообщений. Эта служба не может быть остановлена. C помощью данной службы можно посмотреть какие программы "вылетают" при работе операционной системы, очень полезный инструмент для опытного пользователя.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog]

"Start"=dword:00000004

* **Fast User Switching Compatibility (Совместимость быстрого переключения пользователей)**

Данная служба осуществляет управление приложениями, которые требуют поддержки в многопользовательской среде. Службу имеет смысл включить, если в вашей системе работает несколько пользователей, в противном случае нет необходимости в запуске этой службы. Если вы все-таки решили включить службу, то она позволит переключаться между пользователями без закрытия работающих программ, что бывают очень удобно.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FastUserSwitchingCompatibility]

"Start"=dword:00000004

* **Help and Support (Справка и поддержка)**

Обеспечивает возможность работы центра справки и поддержки на этом компьютере. Если эта служба остановлена, центр справки и поддержки не будет доступен. Данная служба необходима для запуска справочных документов Microsoft. Если вы запускаете программу Справка и Поддержка через меню Пуск, то данная служба будет включена в любом случае, даже если стоит значение Отключена.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\helpsvc]

"Start"=dword:00000004

* **HID Impus Service (Доступ к HID-устройствам)**

Обеспечивает универсальный доступ к HID-устройствам (Human Interface Devices), который активизирует и поддерживает использование заранее определенных клавиш быстрого вызова на клавиатуре, устройствах управления или иных устройствах мультимедиа. Если эта служба остановлена, клавиши быстрого вызова, управляемые этой службой, не будут работать. Вы можете не иметь проблем с внешними устройствами при отключении этой службы. Если же какая-нибудь "уникальная" функция вашего устройства перестанет работать, то измените значение на "Автоматически".

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HidServ]

"Start"=dword:00000004

* **IPSEC Services (Службы IPSEC)**

Управляет политикой IP-безопасности и запускает ISAKMP/Oakley (IKE) и драйвер IP-безопасности. Данная служба может понадобиться при использовании VPN или домена. Для домашнего использования данную службу можно отключить.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent]

"Start"=dword:00000004

* **Logical Disk Manager (Диспетчер логических дисков)**

Обнаружение и наблюдение за новыми жесткими дисками и передача информации о томах жестких дисков службе управления диспетчера логических дисков. Если эта служба остановлена, состояние динамических дисков и информация о конфигурации может оказаться устаревшей. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\dmserver]

"Start"=dword:00000004

* **Network Connections (Сетевые подключения)**

Управляет объектами папки Сеть и удаленный доступ к сети, отображающей свойства локальной сети и подключений удаленного доступа. Данная служба необходима для поддержки сетевых соединений. Отключите данную службу, если ваш компьютер находится ВНЕ СЕТИ. Если после отключения данной службы у вас появились проблемы с сетевыми подключениями, то поставьте значение в Автоматически. Примечание: Если вы отключите данную службу, то у вас больше в системном трее не будет появляться значок соединения (2 мониторчика) даже для модемных соединений.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netman]

"Start"=dword:00000004

* **Network Location Awareness NLA (Служба сетевого расположения NLA)**

Данная служба собирает и хранит сведения о размещении и настройки сети, а также уведомляет приложения об их изменении.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Nla]

"Start"=dword:00000004

* **Plug and Play**

Позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо, не требуя вмешательства пользователя, либо сводя его к минимуму. Остановка или отключение этой службы может привести к нестабильной работе системы. Это служба является "сердцем" всей системы Plug and Play устройств на компьютере. Я крайне не рекомендую отключать данную службу, так как вы можете столкнуться с множеством проблем. Имейте ввиду, что UPnP НЕ ТОЖЕ самое, что и PnP. UPnP служит для связи через TCP/IP с оборудованием (сканерами, принтерами и т.д.). Ваше звуковая карта - это PnP устройство. НЕ ОТКЛЮЧАЙТЕ службу Plug and Play.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PlugPlay]

"Start"=dword:00000004

* **Print Spooler (Диспетчер очереди печати)**

Загружает в память файлы для последующей печати. Если вы не используете печать и у вас в системе не установлено ни одного принтера, то отключите данную службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler]

"Start"=dword:00000004

* **Protected Storage (Защищенное хранилище)**

Обеспечивает защищенное хранение секретных данных, таких, как закрытые ключи, для предотвращения несанкционированного доступа служб, процессов или пользователей. Позволяет сохранять локальные пароли или веб-информацию (автозаполнение). По умолчанию данная служба включена в автоматическом режиме. Но из соображений безопасности я рекомендую отключить ее. С другой стороны, данная служба может вам понадобиться при работе с зашифрованными данными и ключами от различных программ, в таком случае верните службу в значение Автоматически. Если вы сохраняете пароли в Outlook Express`е, подключениях к Интернету по модему или через контроллер домена, что требует идентификации, то оставьте службу в режиме Автоматически.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ProtectedStorage]

"Start"=dword:00000004

* **Remote Access Connection Manager (Диспетчер подключений удаленного доступа)**

Создает сетевое подключение. Данная служба необходима, если вы используете общий доступ к Интернету. Попробуйте отключить ее, если у вас перестал работать интернет, то верните значение службы в Автоматически. Имейте ввиду, что данная служба может потребоваться для некоторых прямых подключений или DSL-подключений.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan]

"Start"=dword:00000004

* **Remote Procedure Call (Локатор удаленного вызова процедур (RPC))**

Обеспечивает сопоставление конечных точек и иных служб RPC. Я ни разу не видел необходимости в использовании этой службы, поэтому рекомендую ее отключить, так как она использует 1.2 Мб оперативной памяти. Если же после отключения данной службы у вас появились проблемы при работе с сетью, то измените значение службы на Вручную.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RpcLocator]

"Start"=dword:00000004

* **Remote Registry (Удаленный реестр)**

Позволяет удаленным пользователям изменять параметры реестра на этом компьютере. Если эта служба остановлена, реестр может быть изменен только локальными пользователями, работающими на этом компьютере. Данной службы нет в операционной системе Windows XP Home. Да и в Windows XP Pro она абсолютно не нужна, эта служба является одной из первых, которую я отключаю после установки операционной системы.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry]

"Start"=dword:00000004

* **Secondary Logon (Вторичный вход в систему)**

Позволяет запускать процессы от имени другого пользователя. Если эта служба остановлена, этот тип регистрации пользователя недоступен.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\seclogon]

"Start"=dword:00000004

* **Security Accounts Manager (Диспетчер учетных записей безопасности)**

Хранит информацию о безопасности для учетной записи локального пользователя. Без этой службы не будет работать служба IIS Admin (IIS Admin). Если вы не делали никаких изменений в локальной политике безопасности (gpedit.msc), то можете отключить данную службу. Если же вы делали изменения в локальной политике безопасности и отключите данную службу, то все изменения, которые вы делали, перестанут работать. Поэтому я рекомендую оставить режим запуска этой службы по умолчанию, то есть Автоматически.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SamSs]

"Start"=dword:00000004

* **Security Center (Центр обеспечения безопасности)**

Центр обеспечения безопасности помогает управлять параметрами безопасности Windows. Можно отключить эту службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc]

"Start"=dword:00000004

* **Server (Сервер)**

Обеспечивает поддержку общий доступ к файлам, принтерам и именованным каналам для данного компьютера через сетевое подключение. Если служба остановлена, такие функции не удастся выполнить. Данная служба используется для открытия на доступ ваших файлов и принтеров, а также для работы сервиса Message Queuing. Вы можете отключить эту службу для дополнительной безопасности, если у вас нет необходимости открывать доступ к вашим файлам и принтерам. У кого нет сети можно отключить эту службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver]

"Start"=dword:00000004

* **Shell Hardware Detection (Определение оборудования оболочки)**

Служит для автозапуска оборудования: CD-ROM и т.д.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ShellHWDetection]

"Start"=dword:00000004

* **SSDP Discovery Service (Служба обнаружения SSDP)**

Данная служба включает обнаружение UPnP-устройств в домашней сети. Однако, необходимость данного сервиса в домашних условиях вызывает большое сомнение.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SSDPSRV]

"Start"=dword:00000004

* **System Event Notification (Уведомление о системных событиях)**

Данная служба протоколирует системные события, такие как регистрация в Windows, в сети и изменения в подаче электропитания. Уведомляет подписчиков из разряда COM+ системное событие, рассылая оповещения.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SENS]

"Start"=dword:00000004

* **System Restore Service (Служба восстановления системы)**

Выполняет функции восстановления системы. Чтобы остановить данную службу, следует отключить восстановление системы на вкладке Восстановление системы, в которую можно попасть, нажав правой кнопкой мыши на ярлыке Мой компьютер на рабочем столе и выбрав пункт Свойства.Примечание: Крайне не рекомендуется отключать восстановление системы, так как в случае сбоя в работе компьютера вы не сможете вернуться к работоспособному состоянию.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\srservice]

"Start"=dword:00000004

* **Task Scheduler (Планировщик заданий)**

Позволяет запускать процессы от имени другого пользователя. Если эта служба остановлена, этот тип регистрации пользователя недоступен.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Scheduler]

"Start"=dword:00000004

* **TCP/IP NetBIOS Helper Service (Модуль поддержки NetBIOS через TCP/IP)**

Включает поддержку службы NetBIOS через TCP/IP (NetBT) и разрешения NetBIOS-имен в адреса. Данная служба необходима для нормальной поддержки NetBIOS через TCP/IP. Если ваша сеть не использует NetBIOS или WINS, то отключите данную службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LmHosts]

"Start"=dword:00000004

* **Telephony (Телефония)**

Обеспечивает поддержку Telephony API (TAPI) для программ, управляющих телефонным оборудованием и голосовыми IP-подключениями на этом компьютере, а также через ЛВС - на серверах, где запущена соответствующая служба.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TapiSrv]

"Start"=dword:00000004

* **Terminal Services (Службы терминалов)**

Данная служба предоставляет возможность нескольким пользователям интерактивно подключаться к компьютеру и отображает рабочий стол и приложения на удаленных компьютерах. Является основой для удаленного рабочего стола (включая удаленное администрирование), быстрого переключения пользователей, удаленного помощника и служб терминалов.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]

"Start"=dword:00000004

* **Themes (Темы)**

Данная служба позволяет управлять темами оформления. Если вы хотите использовать темы, то оставьте значение Автоматически. В противном случае выберите вариант Отключена.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Themes]

"Start"=dword:00000004

* **WebClient (Веб-клиент)**

Позволяет Windows-программам создавать, получать доступ и изменять файлы, хранящиеся в Интернете. Если эта служба остановлена, эти функции не доступны. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient]

"Start"=dword:00000004

* **Windows Audio (Центр Аудио Windows)**

Управление звуковыми устройствами для Windows-программ. Если эта служба остановлена, звуковые устройства и эффекты не будут работать должным образом. Эта служба необходимо для воспроизведения ЛЮБОГО звука. Отключать можно только при отсутствии звуковой карты, иначе вы не будете слышать звуки вообще.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AudioSrv]

"Start"=dword:00000004

* **Windows Firewall/Internet Connection Sharing (Брандмауэр Windows / Общий доступ к Интернету (ICS))**

Обеспечивает поддержку служб трансляции адресов, адресации и разрешения имен или предотвращает вторжение служб в домашней сети или сети небольшого офиса. Позволяет тонко настроить фильтрацию сетевого траффика. Если вы используете файерволл сторонних производителей (Outpost firewall, Norton Personal Firewall, ZoneAlarm и т.п.), то необходимо отключить данную службу.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]

"Start"=dword:00000004

* **Windows Management Instrumentation (Инструментарий управления Windows)**

Предоставляет общий интерфейс и объектную модель для доступа к информации об управлении операционной системой, устройствами, приложениями и службами. После остановки данной службы многие Windows-приложения могут работать некорректно.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Winmgmt]

"Start"=dword:00000004

* **Windows Time (Служба времени Windows)**

Управляет синхронизацией даты и времени на всех клиентах и серверах в сети. Если эта служба остановлена, синхронизация даты и времени не будет доступна.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time]

"Start"=dword:00000004

* **Wireless Zero Configuration (Беспроводная настройка)**

Предоставляет автоматическую настройку 802.11 адаптеров. Если к компьютеру не подключено адаптеров беспроводной связи, то рекомендуется отключить данную службу для экономии системных ресурсов.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WZCSVC]

"Start"=dword:00000004

* **Workstation (Рабочая станция)**

Обеспечивает поддержку сетевых подключений и связь. Данная служба нужна для подключения локального компьютера на удаленный компьютер. Многие службы требуют работу данного сервиса для нормального функционирования, поэтому рекомендуются оставить данную службу в режиме Автоматически.

Отключить службу:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation]

"Start"=dword:00000004