Лабораторная работа 14. Анализ и настройка параметров безопасности операционной системы

Цель лабораторной работы: ознакомление с встроенными в операционную систему Windows возможностями по оценке текущего состояния подсистемы безопасности и контролю целостности настроек безопасности.

Задачи лабораторной работы:
1. Структура шаблона безопасности
2. Управление шаблонами безопасности
3. Анализ параметров безопасности операционной системы
4. Настройка параметров безопасности операционной системы

Задание

Контрольные вопросы

Содержание лабораторной работы:

Оценка текущего состояния проводится на основе сравнения текущих значений параметров безопасности с эталонными. Применение эталона позволяет автоматизировать настройку безопасности операционной системы и дальнейший контроль установленного уровня безопасности.

В операционной системе Windows XP для работы с текущими и эталонными настройками безопасности предназначены оснастки «Шаблоны безопасности» и «Анализ и настройка безопасности».

Войдите в операционную систему под учётной записью «Администратор». Откройте Microsoft Management Console («Пуск - Выполнить» и введите команду «mmc») и добавьте оснастки «Анализ и настройка безопасности» и «Шаблоны безопасности».

1. Структура шаблона безопасности

Шаблон безопасности - набор эталонных настроек операционной системы, влияющих на информационную безопасность. В Windows XP существует набор встроенных шаблонов безопасности. По умолчанию встроенные шаблоны безопасности расположены в каталоге C:\Windows\security\templates\. Просмотр и редактирование настроек, входящих в шаблон, осуществляется через оснастку «Шаблоны безопасности» (рис. 1).

Ниже приведён перечень встроенных шаблонов безопасности и их краткое описание.

а) Безопасность по умолчанию (Setup security.inf) - содержит параметры безопасности, которые применяются по умолчанию во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. Этот шаблон можно использовать полностью или частично в целях аварийного восстановления.

б) Совместимый (Compatws.inf) - содержит разрешения по умолчанию для рабочих станций и серверов (не контроллеров домена). Учитывается иерархия прав локальных групп: "Администраторы", "Опытные пользователи" и "Пользователи".

в) Защита (Securews.inf и Securedc.inf) - шаблоны для настройки рабочих станций (ws - workstations) и контроллеров домена (dc - domain controllers). В них определяются параметры повышенной безопасности: определяются параметры надёжных паролей, блокировки и аудита; правила работы с протоколом NTLM; определяются дополнительные ограничения для анонимных пользователей.

г) Повышенная защита (Hisecws.inf и Hisecdc.inf) - шаблоны повышенной защиты для рабочих станций и контроллеров домена, налагающие дополнительные

ограничения на уровни кодировки и подписи, необходимые для проверки подлинности и для данных, передаваемых по безопасным каналам между клиентами SMB и серверами.

д) *Безопасность системного корневого каталога (Rootsec.inf) - включает разрешения, по умолчанию применяемые для корневого каталога системного диска.*

Каждый шаблон состоит из следующих разделов (рис. 1):

- *Политики учётных записей;*
- *Локальные политики;*
- *Журнал событий;*
- *Группы с ограниченным доступом;*
- *Системные службы;*
- *Реестр;*
- *Файловая система.*

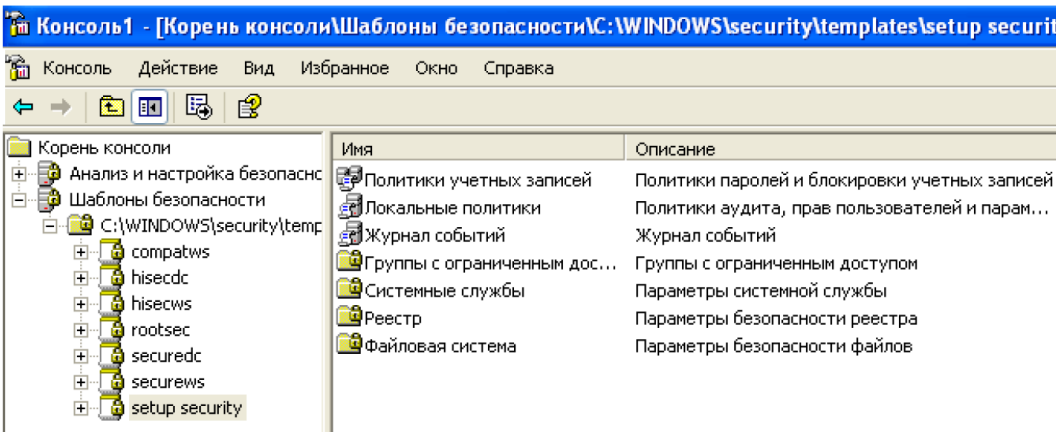

Рис. 1 - Структура шаблона безопасности

Дальнейшее рассмотрение структуры шаблона и изменение его настроек осуществляется на основе встроенного шаблона «setup security».

Разделы «Политики учётных записей» и «Локальные политики» включают в себя все параметры аналогичных разделов «Групповой политики». Измените значение минимальной длины пароля на 6 символов в разделе «Политики учётных записей» - «Политика паролей» (рис. 2). Добавьте группу «Пользователи» в параметре «Управление аудитом и журналом безопасности» раздела «Локальные политики» - «Назначение прав пользователя» (рис. 3).

Рис. 2 - Изменение параметра в разделе «Политики учётных записей»

Рис. 3 - Изменение параметра в разделе «Локальные политики»

Раздел «Журнал событий» включает настройки правил работы с журналами аудита. Разрешите доступ локальной группе гостей к журналу безопасности (рис. 4).

Рис. 4 - Изменение параметра в разделе «Журнал событий»

Раздел «Группы с ограниченным доступом» позволяет настраивать состав групп пользователей. При помощи контекстного меню добавьте в список группу «Администраторы» и в качестве члена группы добавьте пользователя «user» (рис. 5).

Рис. 5 - Изменение параметра в разделе «Группы с ограниченным доступом»

Раздел «Системные службы» содержит настройки по запуску служб и разграничению доступа к управлению ими. Запретите запуск службы «Диспетчер очереди печати» (рис. 6). Эта служба запускается как процесс с именем spoolsv.exe.

Рис. 6 - Изменение параметра в разделе «Системные службы»

Раздел «Реестр» содержит правила разграничения доступа к основным ветвям реестра: software, system, users. Настройте доступ к разделу HKEY_LOCAL_MACHINE\SOFTWARE (рис. 7), разрешив полный доступ к нему группе «Опытные пользователи» (рис. 8).

Рис. 7 - Изменение параметра в разделе «Реестр»

Рис. 8 - Установка прав доступа к разделу реестра

Раздел «Файловая система» содержит правила разграничения доступа к каталогам на системном диске. Запретите всем пользователям доступ к «Косынке» («C:\WINDOWS\system32\sol.exe», рис. 9-10).

Рис. 9 - Изменение параметра в разделе «Файловая система»

Рис. 10 - Установка прав доступа к файлу

2. Управление шаблонами безопасности

В оснастке «Шаблоны безопасности» существует возможность создавать собственные шаблоны. Создать новый шаблон можно через контекстное меню каталога, содержащего шаблоны (рис. 11). При этом будет создан шаблон, у которого все параметры будут иметь значение «Не определено».

Рис. 11 - Создание нового шаблона безопасности

Кроме того, собственный шаблон можно создать на основе существующего. Вызовите контекстное меню шаблона «setup security», выберите «Сохранить как...» (рис. 12) и сохраните шаблон под новым именем (например, «test»). При этом будет создан новый шаблон, включающий все сделанные ранее изменения значений параметров.

Рис. 12 - Сохранение изменённого шаблона

3. Анализ параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» (рис. 13), выберите пункт «Открыть базу данных.». Задайте имя для создаваемой базы данных эталонных настроек. После этого необходимо занести в базу значения параметров из интересующего шаблона. Выберите созданный шаблон (рис. 14).

Рис. 13 - Создание базы данных настроек безопасности

Рис. 14 - Выбор шаблона для импорта в базу данных

Занесение в базу настроек из другого шаблона возможно через команду контекстного меню «Импорт шаблона» (рис. 15).

Рис. 15 - Импорт шаблона

Выберите в контекстном меню оснастки пункт «Анализ компьютера.» и подтвердите предложенный путь к лог-файлу. После этого начнётся анализ текущих настроек безопасности операционной системы (рис. 16). Результатом анализа является сравнение текущих (Параметр компьютера) и эталонных (Параметр базы данных) значений параметров безопасности. Структура представления результатов совпадает со структурой шаблона (рис. 17).

Результаты сравнения значений параметров представляются в виде специальных пиктограмм, находящихся рядом с названием каждого параметра (табл. 1).

Рис. 16 - Анализ настроек безопасности операционной системы

Рисунок

Рис. 17 - Результат анализа безопасности операционной системы

Таблица 1. Описание пиктограмм результатов анализа

Пиктограмма	***Описание***
	Элемент определён в базе данных анализа и в системе, но значения параметров безопасности не совпадают.
	Элемент определён в базе данных анализа и в системе; значения параметров безопасности совпадают.
	Элемент не анализировался. Возможно, он не был определён в базе данных анализа или пользователь, выполняющий анализ, не имеет достаточных разрешений на анализ данного объекта или области
	Элемент определён в базе данных анализа, однако, не существует в текущей конфигурации системы. Например, может существовать группа с ограниченным доступом, определённая в базе данных анализа и не существующая в анализируемой системе
	Элемент не определён в базе данных анализа или в системе

Удостоверьтесь, что в результате проведенного анализа изменённые параметры безопасности отмечены как несовпадающие.

Если какая-нибудь из текущих настроек системы предпочтительнее эталонной, то её можно занести в базу (рис. 18). Изменённую базу можно сохранить в качестве шаблона из контекстного меню оснастки, сохранив базу и выбрав пункт «Экспорт шаблона».

Рис. 18 - Изменение настроек в базе данных

В итоге, был создан шаблон, в котором запрещён доступ к «Косынке», запрещён запуск службы «Диспетчер очереди печати» и пользователь с учётной записью «user» является членом группы «Администраторы». Проверьте текущее состояние этих настроек: возможность запуска «Косынки», наличие запущенного процесса spoolsv.exe в «Диспетчере задач» и отсутствие пользователя «user» в группе «Администраторы».

4. Настройка параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» и выберите пункт «Настроить компьютер...». После подтверждения пути к лог-файлу начнётся настройка операционной системы в соответствии со значениями параметров, указанных в базе данных (рис. 19).

Рис. 19 - Настройка параметров безопасности операционной системы

Проведите повторный анализ системы для проверки изменения не совпадавших параметров (рис. 20).

Рис. 20 - Результат настройки параметров операционной системы

Удостоверьтесь в применении настроек, установленных в изменённом шаблоне: попытайтесь запустить «Косынку», проверьте отсутствие процесса spoolsv.exe в «Диспетчере задач» и наличие учётной записи «user» в группе «Администраторы».

Задание

Создайте шаблон безопасности в соответствии с Вашим вариантом и настройте операционную систему, используя созданный шаблон.

Вариант 1

Политики учётных записей	Политики учётных записей	Локальные политики
Минимальная длина пароля - 10 символов	Пороговое значение блокировки - 3 ошибки входа	Включите аудит отказов входа в систему

Вариант 2

Локальные политики	Журнал событий	Группы с ограниченным доступом
Запретите группе «Операторы архива» восстановление архивных	Сохранение событий в журнале безопасности - вручную	Включите учётную запись «user» в группу «Операторы архива»

файлов		

Вариант 3

Локальные политики	Журнал событий	Файловая система
Включите аудит доступа к объектам (успех и отказ)	Сохранение событий в журнале безопасности - 30 дней	Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Вариант 4

Локальные политики	Локальные политики	Системные службы
Запретите отображение имени последнего пользователя при входе в систему	Включите обязательное нажатие Ctrl-Alt-Del при входе в систему	Автозапуск службы «Центр обеспечения безопасности»

Вариант 5

Локальные политики	Журнал событий	Группы с ограниченным доступом
Разрешите учётной записи «user» работу с журналом аудита	Максимальный размер журнала безопасности - 2 МБ	Включите учётную запись «user» в группу «Опытные пользователи»

Вариант 6

Политики учётных записей	Локальные политики	Системные службы
Включите применение требований к сложности паролей	Включите аудит управления учётными записями	Автозапуск службы «Автоматическое обновление»

Вариант 7

Локальные политики	Группы с ограниченным доступом	Файловая система
Запретите группе «Пользователи» завершение работы системы	В группу «Пользователи» добавьте пользователя «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к редактору реестра группе «Пользователи»

Вариант 8

Политики учётных записей	Локальные политики	Системные службы
Срок действия пароля - 90 дней	Запретите учётной записи «user» доступ к компьютеру из сети	Запретить запуск службы «Диспетчер сеанса справки для удалённого рабочего стола»

Вариант 9

Локальные политики	Группы с ограниченным доступом	Файловая система
Включите очистку файла подкачки при завершении	В группу «Пользователи» добавьте учётную запись	Запретите доступ к оснастке «Службы» (services.msc)

работы системы	«user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	группе «Пользователи»

Вариант 10

Локальные политики	Локальные политики	Файловая система
Запретите изменение системного времени группе «Опытные пользователи»	Включите аудит системных событий (успех и отказ)	Запретите учётной записи «user» доступ к оснастке «Просмотр событий» (eventvwr.msc)

Контрольные вопросы

1. Каким образом при помощи встроенных средств операционной системы Windows XP можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?
2. Каким образом при помощи встроенных средств Windows XP можно автоматизировать настройку операционной системы в соответствии с требуемыми параметрами безопасности?
3. Что такое «Шаблон безопасности»?
4. Для чего предназначена оснастка «Шаблоны безопасности»?
5. Какие группы настроек входят в шаблон безопасности?
6. Для чего предназначена оснастка «Анализ и настройка безопасности»?
7. Опишите последовательность действий администратора при проведении анализа настроек безопасности операционной системы.
8. Опишите последовательность действий администратора при настройке безопасности операционной системы.
9. Приведите возможные типы результатов анализа параметров безопасности операционной системы.
10. Каким образом можно внести в шаблон текущие настройки безопасности операционной системы?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях