

Лабораторная работа №1

Параметры безопасности Windows XP

1. Интерфейсы безопасности Windows XP.

Основным средством управления настройками безопасности служит MMC (Microsoft Management Console). Вызов MMC осуществляется через командную строку с помощью команды `mmc`. Основным предназначением MMC является вызов оснасток. Оснастки обеспечивают интерфейсы для управления настройками Windows. Настройки операционной системы хранятся в объектах, которые собраны в контейнеры. Набор настроек, обеспечивающих безопасность системы, принято называть политикой безопасности. Оснастки вызываются через командную строку.

Рассмотрим основные средства проведения политики безопасности:

1. Локальные параметры безопасности – Local Security Policy (оснастка `Secpol.msc`). Настройки безопасности локальной рабочей станции.

2. Групповая политика – Group Policy (оснастка `GPedit.msc`). Служит для организации групповой политики безопасности (GPO) в рамках домена.

3. Конфигурация безопасности и анализ – Security Configuration and Analysis (SCA). Настройка локальных параметров безопасности, а также параметров безопасности файловой системы и реестра.

Рассмотрим контейнеры оснастки `Secpol.msc`:

1. Политики учетных записей – отвечает за политику выбора паролей и блокировку учетных записей. Включает в себя контейнеры:

1.1 Политика паролей – отвечает за параметры паролей

1.2 Политика блокировки учетных записей – определяет, когда и на какое время должна блокироваться учетная запись.

2. Локальные политики – содержит параметры аудита и прав пользователя. Содержит контейнеры:

2.1 Политика аудита – содержит настройки регистрируемых событий.

2.2 Назначение прав пользователя – содержит описание прав конкретных пользователей или групп пользователей.

2.3 Параметры безопасности – общие настройки системы. Имена объектов этого контейнера имеют следующий формат

категория: название или краткое описание

Категория показывает, какую часть системы регламентирует данный объект.

Для сохранения действующей политики безопасности в виде шаблона, применения существующего шаблона или сравнения существующей политики безопасности с шаблоном применяется «Конфигурация безопасности и анализ». Запуск данной оснастки осуществляется через консоль MMC. Наберите в командной строке `mmc`. Рассмотрим несколько операций для работы с шаблонами безопасности:

1. Для создания шаблона безопасности выберите в меню «Консоль->Добавить/Удалить оснастку». Нажмите на кнопку «Добавить» и выберите «Шаблоны безопасности». В созданной оснастке нажать правой кнопкой мыши на строку с путем к папке, в которой хранятся шаблоны, и выбрать «Создать шаблон ...». Вновь созданный шаблон не будет содержать никаких настроек. В этой же оснастке можно изменять отдельные объекты шаблона.

2. Для сравнения настроек компьютера с существующим шаблоном необходимо в консоли `mmc` добавить оснастку «Анализ и настройки безопасности». В созданной оснастке нажать правой кнопкой мыши на «Анализ и настройки безопасности» и выполнить создание базы данных и импортирование шаблона, на соответствие которому надо проверить компьютер. После этого нажать правой кнопкой мыши на «Анализ и настройки безопасности» и выполнить анализ компьютера. В результате напротив всех объектов политики безопасности в виде двух колонок будет выведены значения шаблона и настройки компьютера.

3. После анализа компьютера, нажав правой кнопкой мыши на «Анализ и настройки безопасности», можно экспортировать текущие настройки в шаблон безопасности.

2. Автоматизация задач настройки системы безопасности

Настройка и анализ политики безопасности также может быть осуществлена из пакетного файла с помощью команды `secedit`. Возможны следующие варианты данной команды:

1. `secedit /analyze` - анализирует безопасность системы, сравнивая текущую конфигурацию хотя бы с одним шаблоном.

```
secedit /analyze /db имя_файла [/cfg имя_файла] [/log имя_файла] [/quiet]
```

`/db имя_файла` - обязательный параметр. Указывает путь к базе и имя файла базы, содержащей сохраненную конфигурацию, по которой будет производиться анализ. Если значение `имя_файла` соответствует новой базе, необходимо указать параметр командной строки `/cfg имя_файла`.

`/cfg имя_файла` - определяет путь к шаблону безопасности и имя файла шаблона, который будет импортироваться в базу данных для анализа. Данный параметр командной строки может использоваться только вместе с параметром `/db`. Если параметр не указан, анализ выполняется по конфигурации, хранящейся в базе данных.

`/log имя_файла` - отображает имя и путь файла журнала для анализа. Если данный параметр не указан, используется файл журнала по умолчанию.

`/quiet` - предотвращает вывод на экран и в файл журнала. Имеется возможность посмотреть результаты анализа, используя оснастку «Анализ и настройка безопасности».

2. `secedit /configure` - Служит для настройки безопасности системы с использованием сохраненного шаблона.

```
secedit /configure /db имя_файла [/cfg имя_файла] [/overwrite][/areas область1 область2...] [/log имя_файла] [/quiet]
```

`/db имя_файла` - обязательный параметр. Представляет имя файла базы данных, содержащей применяемый шаблон безопасности.

`/cfg имя_файла` - имя файла шаблона безопасности, который будет импортироваться в базу данных и применяться при настройке безопасности. Данный параметр командной строки может использоваться только вместе с параметром `/db`. Если данный параметр не указан, будет использоваться шаблон, хранящийся в базе данных.

`/overwrite` - следует указывать в том случае, если шаблон безопасности, указанный в параметре `/cfg`, должен замещать любой шаблон или составной шаблон, хранящийся в базе данных, вместо того, чтобы добавлять результаты в хранящуюся базу данных. Данный параметр командной строки может использоваться только вместе с параметром `/cfg`. Если параметр не указан, шаблон, указанный в аргументе `/cfg`, будет добавлен в шаблон, хранящийся в базе данных.

`/areas область1 область2...` - Определяет области безопасности, которые следует применить в системе. Если область не указана, в системе применяются все области. Имена областей должны разделяться пробелами.

SECURITYPOLICY - Локальная политика и политика для домена, включая политики учетных записей, политики аудита и т. п.

GROUP_MGMT - Настройка ограничений для всех групп, указанных в шаблоне безопасности

USER_RIGHTS - Права пользователей на вход в систему и предоставление привилегий

REGKEYS - Безопасность разделов локального реестра

FILESTORE - Безопасность локальных устройств хранения файлов

SERVICES - Безопасность для всех определенных служб

`/log имя_файла` - отображает имя и путь файла журнала для анализа. Если путь не задан, используется путь по умолчанию.

`/quiet` - Предотвращает вывод на экран и в файл журнала.

3. secedit /export Служит для экспорта сохраненного шаблона из базы данных безопасности в файл шаблона безопасности.

`secedit /export [/mergedpolicy] [/DB имя_файла] [/CFG имя_файла] [/areas область1 область2...] [/log имя_файла] [/quiet]`

`/mergedpolicy` - объединяет и экспортирует настройку безопасности локальной политики и настройку политики домена.

`/db имя_файла` - указывает файл базы данных, содержащий экспортируемый шаблон. Если база данных не указана, используется база данных системной политики.

`/db имя_файла` - определяет имя файла, где должен быть сохранен шаблон.

`/areas область1 область2...` - задает области безопасности, которые следует экспортировать в шаблон. При неуказанной области экспортируются все области. Имена областей должны разделяться пробелами.

SECURITYPOLICY - Определяет локальную политику и политику для домена, включая политики учетных записей, политики аудита и т. п.

GROUP_MGMT - Задает настройку ограничений для всех групп, указанных в шаблоне безопасности

USER_RIGHTS - Указывает права пользователей на вход в систему и предоставляет привилегии

REGKEYS - Определяет безопасность раздела локального реестра

FILESTORE - Определяет безопасность локальных устройств хранения файлов

SERVICES - Задает безопасность для всех определенных служб

`/log имя_файла` - отображает имя и путь файла журнала для анализа. Если путь не задан, используется путь по умолчанию.

`/quiet` - предотвращает вывод на экран и в файл журнала.

4. secedit /validate Служит для проверки синтаксиса шаблона безопасности при его импорте в базу данных или применении к системе.

`secedit /validate имя_файла`

`имя_файла` - указывает имя файла шаблона безопасности, который был создан с помощью средства «Шаблоны безопасности».

3. Стандартные шаблоны безопасности

Compatws - ослабляет используемые по умолчанию разрешения доступа группы Пользователи к файлам и реестру таким образом, чтобы это соответствовало требованиям большинства несертифицированных приложений. Обычно, следует использовать группу Опытные пользователи для работы с несертифицированными приложениями. Дополнительные сведения об этом содержатся в справке.

Hisecdc - охватывающий набор для SECURED.C. Накладывает дальнейшие ограничения на проверку подлинности LanManager и новые требования для шифрования и подписывания данных, передаваемых по безопасным каналам и данных SMB. Чтобы применить HISECDC к контроллеру домена, все другие контроллеры в доверенных и доверяющих доменах должны работать под управлением Windows 2000 или более новых систем. Дальнейшие сведения содержатся в справке.

Hisecws - охватывающий набор для SECUREWC. Накладывает дальнейшие ограничения на проверку подлинности LanManager и новые требования для шифрования и подписывания данных, передаваемых по безопасным каналам и данных SMB. Чтобы применить HISECWC к входящим в домен компьютерам, все контроллеры домена, хранящие учетные записи всех пользователей, которые могут выполнить вход на этот клиентский компьютер, должны работать под управлением NT4 SP4 или более новых систем. Дальнейшие сведения содержатся в справке.

rootsecПрименение стандартных корневых разрешений для раздела операционной системы и распространение их на дочерние объекты, наследующие разрешения от корня. Время распространения зависит от количества незащищенных дочерних объектов.

Securedc - предоставляет расширенные политики для управления учетными записями в домене, ограничивает использование проверки подлинности LanManager, накладывает дальнейшие ограничения для анонимных пользователей. Если контроллер домена использует securedc, то пользователь с учетной записью в этом домене не сможет подключаться к рядовым серверам только с помощью клиента LanMan.

Securews - предоставляет расширенные политики для управления локальными учетными записями, ограничивает использование проверки подлинности LanManager, включает подписывание SMB со стороны сервера, накладывает дальнейшие ограничения для анонимных пользователей. Для применения к входящим в домен компьютерам, все контроллеры домена, хранящие учетные записи всех пользователей, которые могут выполнить вход на этот клиентский компьютер, должны работать под управлением NT4 SP4 или более новых систем.

Setup security - используемые по умолчанию параметры безопасности.

4. Создание пользователя в Windows XP

Для добавления пользователей необходимо выполнить **«Пуск -> Панель управления -> Учетные записи пользователей»**. Для добавления пользователей выберите действие **«Создание учетной записи»**. После выбора типа учетной записи нажмите кнопку **«Создать учетную запись»**. Для задания пароля пользователя следует выбрать пункт **«Создание пароля»**, после чего дважды ввести пароль пользователя в соответствующих полях ввода. Для управления группами пользователей и более детального управления пользователями в ОС Windows XP Professional следует воспользоваться оснасткой **«Локальные пользователи и группы»** консоли управления (**mmc**). Для запуска консоли управления необходимо выполнить: **«Пуск -> Панель управления -> Администрирование -> Управление компьютером»**. Доступ к этой оснастке также можно получить, набрав в командной строке `lusrmgr.msc`. Чтобы добавить учетную запись нового пользователя, щелкните правой кнопкой мыши на папке Пользователи и выберите из выпадающего меню команду **«Новый пользователь...»**. В открывшемся окне введите данные для создания новой учетной записи. Чтобы удалить учетную запись пользователя, щелкните правой кнопкой мыши на названии учетной записи в правом окне программы и выберите из выпадающего меню Удалить. Для каждого пользователя можно отключить срок действия пароля, запретить смену пароля пользователем, отключить учетную запись, а также назначить путь к профилю и сценарий входа в систему.

5. Журнал аудита

Журнал аудита формируется согласно установкам аудита. События журнала доступны через консоль **«Пуск -> Панель управления -> Администрирование -> Управление компьютером -> Просмотр событий»**. Для журнала аудита можно применять фильтр, позволяющий просматривать только события с определенными характеристиками.

Задания к лабораторной работе:

Задание 1. Реализуйте перечисленные ниже настройки с помощью графического интерфейса оснасток mmc, Secpol.msc и GPedit.msc.

1. Определите следующую политику паролей:
 - 1.1 Установите количество запоминаемых паролей равное 10.
 - 1.2 Установите срок действия паролей равным 10 дням.
 - 1.3 Установите минимальный срок действия пароля равным 5 дням.
 - 1.4 Потребуйте установку пароля, отвечающего требованиям сложности.
 - 1.5 Установите длину пароля не менее 5 символов
 - 1.6 Отключите использование обратного шифрования при хранении паролей
2. Задайте политику блокировки учетных записей:
 - 2.1 Определите блокировку учетной записи через 3 неудачных попытки входа в систему
 - 2.2 Определите блокировку учетной записи после неудачных попыток входа на 10 мин
 - 2.3 Определите время в течение, которого подсчитываются неудачные попытки входа равным 15 мин.
3. Залайте регистрацию следующих событий:
 - 3.1 Вход в систему (успех)
 - 3.2 Доступ к объектам (успех)
 - 3.3 Доступ к службе каталогов (успех)
 - 3.4 Изменение политики (успех)
 - 3.5 Использование привилегий (успех)
 - 3.6 Отслеживание процессов (успех)
 - 3.7 Системные события (успех)
 - 3.8 События входа в систему (успех)
 - 3.9 Управление учетными записями (успех)
4. Создайте группу пользователей Group1.
5. Создайте учетную запись пользователя User1 и поместите его в Group1. Запретите пользователю User1 смену пароля.
6. Выдайте учетной записи User1 следующие права:
 - Архивирование файлов и каталогов
 - Восстановление файлов и каталогов
 - Вход в качестве пакетного задания
7. Выдайте группе пользователей Group1 следующие права:
 - Восстановление файлов и каталогов
 - Вход в качестве пакетного задания
 - Вход в качестве службы

Задание 2. Создайте шаблон безопасности secp1.inf с настройками указанными выше. Сравните установленные настройки с шаблоном compatws.

Задание 3. Реализуйте перечисленные ниже действия с помощью пакетного файла, использующего команду **secedit**.

1. Сравните текущую политику безопасности с шаблоном compatws
2. Экспортируйте текущую политику безопасности в шаблон shab1.inf
3. Настройте политику безопасности, используя шаблон hisecdc

Задание 4. Осуществите попытку входа в систему из под несуществующего пользователя Kevin. Зайдите в систему и найдите в журнале аудита соответствующую запись.

Задание 5. Верните исходные настройки системы