Практическая работа

Возможности оснасток, предназначенных для диагностики, мониторинга, настройки и оптимизации

В широком смысле аудитом называется регистрация каких-либо действий, процессов или событий, предназначенная для обеспечения комплексной безопасности чего-либо. В частности, средства аудита в среде ОС Windows предназначены для отслеживания действий пользователей путем регистрации системных событий определенных типов в журнале безопасности сервера или рабочей станции. Кроме того, отображение и фиксация системных событий необходимы для определения злоумышленников или попыток поставить под угрозу данные операционной системы. Примером события, подлежащего аудиту, является неудачная попытка доступа к системе.

Наиболее общими типами событий, подлежащих аудиту в ОС, являются:

· доступ к таким объектам, как файлы и папки;

· управление учетными записями пользователей и групп;

· вход пользователей в систему и выход из нее.

Чтобы обеспечить возможность аудита в среде ОС Windows, сперва необходимо выбрать политику аудита, указывающую категории событий аудита, связанных с безопасностью. При инсталлировании ОС все категории аудита по умолчанию выключены; включая их последовательно администратор может создать политику аудита, удовлетворяющую всем требованиям организации.

К числу категорий событий, предназначенных для контроля, относятся:

· аудит событий входа в систему;

· аудит управления учетными записями;

· аудит доступа к службе каталогов;

· аудит входа в систему;

· аудит доступа к объектам;

· аудит изменения политики;

· аудит использования привилегий;

· аудит отслеживания процессов и системных событий.

В частности, если выбран аудит доступа к объектам как часть политики аудита, необходимо включить либо категорию аудита доступа к службе каталогов (для аудита объектов на контроллере домена), либо категорию аудита доступа к объектам (для аудита объектов на рядовой сервер или рабочую станцию).

Кроме того, с целью уменьшения риска угроз системной безопасности в целом администратор должен предпринять следующие базовые шаги, направленные на обеспечение аудита в системе. Основные события аудита и угрозы безопасности, отображаемые при помощи этого события, сведены в табл. 20.

Таблица 20.Основные события аудита в ОС Windows

№ п.п.	Событие аудита	Потенциальная угроза
	Аудит отказов входа/выхода.	Случайный взлом пароля
	Аудит успехов входа/выхода.	Вход с украденным паролем
	Аудит успехов использования привилегий, управления пользователями и группами, изменений политик безопасности, перезагрузки, выключения и системных событий.	Неправильное использование привилегий
	Аудит успехов и отказов событий доступа к файлам и объектам. Аудит успехов и отказов диспетчера файлов в доступе подозрительным пользователям или группам к важным файлам для чтения и записи.	Неправильный доступ к важным файлам

	Аудит успехов и отказов событий доступа к принтерам и объектам. Аудит успехов и отказов диспетчера печати в доступе подозрительным пользователям или группам к принтерам.	Неправильный доступ к принтерам
	Аудит успехов и отказов доступа для записи к программным файлам с расширениями .exe и .dll. Аудит успехов и отказов для отслеживания процессов в системе при запуске подозрительных программ.	Эпидемия вирусов

Формирование политики аудита объектов в системе осуществляется посредством оснастки «Групповая политика»; в частности, с ее помощью устанавливается и настраиваются параметры политики аудита.

Таблица 21. Типы системных событий в ОС Windows

№ п.п.	Тип события	Описание
	Ошибка	Возникает при серьезных трудностях, связанных с потерей данных или функциональности ОС (например, при сбое загрузки службы в момент ее запуска).
	Предупреждение	Возникает при событии, которое в момент записи в журнал не было существенным, но может привести к ошибкам в будущем (например, если на диске осталось мало свободного места).
	Уведомление	Возникает при событии, описывающее удачное завершение действия приложением, драйвером или службой (например, после успешной загрузки драйвера).

	Аудит успехов	Возникает при событии, которое соответствует успешно завершенному действию, связанному с поддержкой безопасности ОС (например, в случае успешного входа пользователя в систему).
	Аудит отказов	Возникает при событии, которое соответствует неудачно завершенному действию, связанному с поддержкой безопасности ОС (например, в случае неудачной попытки доступа пользователя к сетевому диску).

В журнале службы каталогов содержатся события, заносимые службой каталогов ОС Windows. Например, проблемы соединения между сервером и общим каталогом записываются в этот журнал.

Журнал службы репликации файлов содержит записи о системных событиях, внесенных службой репликации файлов ОС Windows. В этот журнал записываются неудачи при репликации файлов, а также события, которые происходят пока контроллеры домена обновляются данными об изменениях из общей папки Sysvol, где хранится серверная копия общих файлов, реплицируемых между всеми контроллерами домена.

Кроме того, существует журнал DNS-сервера, в который записываются сообщения об системных событиях, зарегистрированных службой DNS. В этот журнал записываются события, связанные с разрешением DNS-имен IP-адресам.

В ОС Windows за регистрацию системных событий в описанных выше журналах отвечает специальная служба, называемая службой журнала событий, которая загружается автоматически при старте системы. Эта служба контролирует ведение журналов и осуществляет внесение в них соответствующих записей системных событий в реальном масштабе времени. При этом любой пользователь может просматривать журналы приложений и системы, однако журналы безопасности доступны только системному администратору, который предварительно должен настроить параметры системных событий аудита (табл. 20), воспользовавшись компонентом «Групповая политика».

· сделайте вывод о проделанной работе и запишите его в отчет.