УДК 004
ББК 32.81

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SOLARIS 10

С.С. Царегородцев

Проанализированы существующие атаки на операционную систему Solaris 10, выявлены наиболее уязвимые ее места. Исследованы штатные средства безопасности. Предложены дополнительные меры по мониторингу.

Ключевые слова: *мониторинг, безопасность, Solaris 10, операционная система, атака на операционную систему.*

На сегодняшний день серверы Solaris 10 применяются в различных компаниях для управления своими корпоративными сетями, таких как РосНефть, Национальный Олимпийский Комитет, в научно-производственных комплексах федерального значения и т. д. Поэтому обеспечение комплексной информационной безопасности корпоративных серверов под управлением Sun Solaris 10 трудно переоценить.

Проводя анализ атак на операционную систему Solaris 10, можно разделить их на следующие группы:

1. Позволяющие обойти установленные разграничения прав доступа.

2. Позволяющие осуществить несанкционированные операции чтения/записи файловых или других объектов.

3. Использующие недостатки системы хранения или выбора (недостаточная длина) данных об аутентификации (пароли) и позволяющие путем реверсирования, подбора или полного перебора всех вариантов получить эти данные.

4. Использующие встроенные недокументированные возможности (ошибки и закладки), возникшие в результате ошибок разработчиков.

5. Приводящие к отказу (Denial of Service) в обслуживании (системный сбой).

6. Позволяющие несанкционированно запустить исполняемый код.

7. Вредоносное программное обеспечение.

Операционная система Solaris 10 обладает богатым набором средств защиты, позволяющих защититься от большинства из них.

Наиболее эффективными из них являются аудит, использование ролевого доступа и зонной технологии.

Аудит в Solaris позволяет понять, что происходит с системой. Данный механизм встроен в ядро, поэтому может видеть и записывать все, что происходит. Процесс аудита играет весьма важную роль в работе организации.

Система ролевого доступа (RBAC – Role Based Access Control) предназначена для решения «проблемы суперпользователя» – ситуации, когда один пользователь имеет доступ ко всем ресурсам системы. Такой подход нельзя назвать безопасным, поэтому в Solaris введена возможность разделения прав суперпользователя между несколькими пользователями. Одному пользователю может быть предоставлено только право чтения системных журналов (например, для аудита), другому – право добавления новых пользователей, третьему – право подключения и конфигурирования внешних устройств. В идеале в системе вообще не должно быть суперпользователя, а все его права должны быть разделены между пользователями, выполняющими различные роли.

Технология программного разбиения на зоны «Solaris Zones» используется для виртуализации служб операционной системы и формирования изолированной и безопасной среды для выполнения приложений. Зона представляет собой виртуализированную среду операционной системы, созданную внутри одного экземпляра операционной системы Solaris. При создании зоны формируется среда выполнения приложений, в которой процессы изолированы от всех других зон. Такая изоляция не позволяет процессам, выполняющимся в одной зоне, проводить мониторинг или воздействовать на процессы, выполняющиеся в других зонах. Даже процесс, осуществляемый с правами доступа суперпользователя, не дает возможности просматривать и корректировать действия, выполняемые в других зонах.

Применение вышеуказанных средств увеличит степень защищенности операционной системы Solaris 10. Однако ими нельзя защититься от атак в полной мере, в частности от атак, использующих недокументированные возможности (с помощью средств Solaris можно лишь минимизировать ущерб от таких атак). Средства Solaris не позволяют защититься от уязвимостей в прикладном программном обеспечении. Это приводит к удаленному или локальному выполнению кода. Существуют закладки и уязвимости, от которых защититься стандартными средствами не представляется возможным. Действия злоумышленника, пытающегося проникнуть в систему, влекут за собой определенные изменения в ее работе: он может несанкционированно загрузить модули в ядро операционной системы, нарушив целостность системы, запустить сторонний вредоносный процесс, нарушить работоспособность зон путем остановки или запуска процессов в них.

Вследствие этого возникает необходимость в разработке дополнительного средства, проводящего мониторинг безопасности Sun Solaris 10. Основная цель программы – отслеживать изменения профиля правильного функционирования и оповещать об этом администратора.

Параметрами мониторинга являются:

- количество загруженных модулей ядра операционной системы Solaris 10;
- установленные зоны в операционной системе и их настройки;
- количество выполняемых процессов внутри каждой зоны, включая глобальную зону global;
- степень загрузки как всей операционной системы, так и каждой из зон.

Должны быть реализованы следующие способы предупреждения администратора о выявленных нарушениях:

- вывод сообщения на системную консоль;
- запись сообщения в указанный лог-файл в операционной системе;
- отсылка сообщения по электронной почте на адрес, указанный администратором.

MONITORING OF SOLARIS 10 INFORMATION SECURITY

S.S. Tsaregorodtsev

The existing attacks on Solaris 10 operating system were analyzed. The most widespread disadvantages of it were found. Then the Solaris's common security tools were studied and additional measures for monitoring were proposed.

Key words: *monitoring, security, Solaris 10, operating system, attack on the operating system.*