АНАЛИЗ АУДИТА В ОПЕРАЦИОННОЙ СИСТЕМЕ FREEBSD

Мищеряков А.Ю.
Научный руководитель – проф., Халимов Г.З.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, проспект Науки, 14, каф. Безопасности информационных технологий. Тел.702-14-25)
e-mail: anton.mishcheriakov@nure.ua

In this paper we consider the audit log integrity monitoring, and protection it against unauthorized access. We consider the possibilities of an attacker to modify the audit log in order to hide his presence in the system. Some solutions to this problem and the rationale for their adoption are given. The problems that may arise in connection with the implementation of the proposed solutions are considered.

На сегодняшний день операционная система FreeBSD обрела популярность в использовании, как для повседневной жизни, так и для рабочих целей. В работе данная система рассматривается в качестве сервера.

Данная операционная система является достаточно защищенной, надежной. В связи с этим поднимается вопрос безопасности системы, отслеживания работы пользователей с файлами, изменения файлов и т. д.

Одним из важнейших средств контроля событий в системе является журнал аудита. Его главным назначением является отслеживания событий о действиях пользователя и программного обеспечения, запускаемого пользователями. Журнал хранит информацию о том, кто, когда, с какими правами использовал файлы, запускал программы и т. д.

Журнал аудита является эффективным методом наблюдения за важными файлами утечка, изменение или удаление которых может нанести непоправимый ущерб.

Однако, реализация аудита в FreeBSD имеет известные ограничения. Не все события в настоящий момент протоколируемые. Также, некоторые механизмы входа в систему, такие как оконные менеджеры X11 или демоны от сторонних производителей, не настраивают аудит пользовательских сессий должным образом [1].

Для настройки журнала аудита используются конфигурационные файлы в которых прописывается какие файлы отслеживать, где хранятся файлы журнала аудита, резервные копии этих файлов и т. д.

Так как в журнале аудита хранятся действия над многими файлами возникает потребность ограничить доступ к этому файлу для всех сотрудников, для избегания нежелательной его модификации.

Вместе с тем, модификация, изменение или повреждение журнала аудита может происходить ненамеренно в результате сбоя программно-аппаратного обеспечения или злоумышленником.

В результате сбоя программно-аппаратного обеспечения, например, перебой электропитания, могут быть недоступны файлы системы. В следствии этого должен присутствовать механизм восстановления работоспособности системы и журналов аудита.

Злоумышленник может модифицировать файлы журнала аудита для сокрытия своих действий в системе. Для противодействия этому необходимо их защитить.

Для защиты журнала аудита можно хранить файлы в нестандартных местах и так же использовать шифрование. Для этих целей может использоваться как симметричное, так и ассиметричное шифрование.

Однако при применении шифрования возникает дополнительная нагрузка на систему. Таким образом администратору необходимо обеспечить выбор баланса между стойкостью шифрования и нагрузкой на вычислительную систему.

Вышеуказанную проблему можно решить шифрованием не самих файлов аудита, а путей к ним. Это серьезно затруднит злоумышленнику возможность определить расположение файлов аудита, следовательно, убрать все признаки своего присутствия в системе будет намного сложнее.

Несмотря на применяемые средства защиты существует вероятность того что злоумышленник все же может почистить следы своего пребывания в системе. Во избежание этого необходимо принять дополнительные меры проверки корректности, целостности файлов аудита. Для этих целей могут быть применены следующие решения: выполнять резервное копирование в реальном времени, желательно на другой сервер сети, для каждой вносимой в журнал аудита записи сохранять в отдельный скрытый файл отметки расположения записи в журнале, времени ее внесения в журнал, а также хеш-значение. Такой подход позволит отслеживать целостность файлов аудита и выявлять несанкционированные изменения в них.

Таким образом контроль действий пользователей и программного обеспечения и отслеживания целостности этих данных повышает нагрузку на систему, и каждый администратор должен решить для себя, повысить нагрузку на систему и повысить безопасность, или же пожертвовать безопасностью в пользу быстродействия системы.

Список источников:

1. Аудит событий безопасности. / Руководство FreeBSD [Электронное издание]. – Режим доступа: https://www.freebsd.org/doc/ru/books/ handbook/audit.html.