ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ WEB-СЕРВЕРОВ НА БАЗЕ ОС LINUX

Гоцкий А.Д.

Белорусский государственный университет информатики и радиоэлектроники
Институт информационных технологий,
г. Минск, Республика Беларусь

Скудняков Ю.А. -к.т.н., доцент

Разработаны рекомендации и алгоритм обеспечения информационной безопасности web-серверов на базе ОС Linux.

Web-серверы — неотъемлемая часть инфраструктуры компьютерной сети практически любой компании. Они являются теми посредниками, с помощью которых функционирует ресурс и неважно, сайт-визитка это или целая социальная сеть с количеством зарегистрированных пользователей более миллиона. Существенной проблемой для надежной работы web-серверов является обеспечение их информационной безопасности [1-2].

Естественно, при такой массовости данного класса, ПО к ним часто становятся целью злоумышленников. В зависимости от характера вторжения изменяется внешний вид Web-страниц, в файлах протоколов появляются новые записи, упрощающие обращение злоумышленников к системе, изменяются коды программ, а также появляются другие «сюрпризы". Предсказать конкретные действия взломщика довольно сложно, даже с применением системных программ.

В этом случае надежным решением является удаление с дисков компьютера всю информацию и повторная установка системы или восстановление ее с помощью резервной копии, сделанной еще до атаки. Поскольку взломщик модифицирует системные файлы, наличие измененных файлов может служить признаком атаки.

Обнаружить факт проникновения в систему можно лишь в том случае, если администратор заранее сохранил информацию о состоянии основных системных файлов, например, файла /etc/passwd и исполняемых программ в каталоге/bin. Эта информация должна храниться в закодированном виде либо ее следует записать на сменный носитель.

Эти данные необходимо периодически использовать для проверки целостности файлов. Если файл, который не должен был подвергаться изменениям, окажется модифицированным, есть все основания полагать, что система была взломана, при этом следует учитывать, что некоторые файлы могут быть изменены самим администратором.

Например, при создании новой учетной записи данные записываются в файл /etc/passwd. В сети Internet web-узлы передают информационные сообщения о состоянии компьютеров и информационно-вычислительной системы в целом.

Для защиты информационных ресурсов web-узлов системный администратор должен периодически осуществлять их мониторинг.

В сети Internet практически для каждого дистрибутивного пакета Linux имеется web-узел, содержащий информацию о данной версии системы. Значительный объем этой информации включает средства защиты данных сведения о вновь обнаруженных недостатках в защите программ и ссылки на

версии программ, в которых эти проблемы устранены.

В web-узле CIAC (Computer Incident Advisory Capability (CIAC) публикуются сведения о состоянии информационной безопасности компьютерной сети.

Раздел Linux Weekly News(http://lwn.net) — сетевая газета предназначена для использования ОС Linux и содержит сведения о способах повышения безопасности различных дистрибутивных пакетов Linux. (URL раздела часто изменяется, и для того, чтобы попасть на соответствующую web-страницу, следует активизировать ссылку Security на главной странице Linux Weekly News).

На web-узле SecurityFocus (http://www.securityfocus.com) публикуются новости о вопросах защиты. Информация на этом сервере представляет собой своеобразный дайджест, составленный на основе данных, представленных на узлах CERT/CC и CIAC.

На перечисленных выше узлах находятся сведения о средствах, используемых хакерами, и противодействии различным способам атаки, о выявленных недостатках в защите различных программных продуктов, о дополнительных модулях для различных программ, информацию о вирусах и борьбе с ними, а также другие данные подобного рода.

Системному администратору следует периодически просматривать содержимое одного - двух из этих узлов (желательно делать это ежедневно или, по крайней мере, раз в неделю) [3]. При этом цели хакеров могут варьироваться от атак «forfun» до атак с целью перехвата трафика пользователей для получения критичной информации, номеров карт и прочего.

Также целью может служить использование web-сервера как «входной» точки в локальную сеть компании. Поэтому грамотная настройка безопасности — один из немаловажных этапов при развёртывании любого web-ресурса. Большинство web-серверов управляются операционными системами на базе семейства ОС Linux. Наиболее часто используемые сервера на ОС Linux — это Apache и nginx [4].

Рекомендации по защите web-серверов:

1. Обновляйтесь. Часто именно несвоевременное обновление приводит к крайне печальным последствиям.

2. Изолируйте работу web-сервера, если это возможно. Docker или chroot — отличный способ оградить ПО и не дать злоумышленнику проникнуть дальше в систему в случае компрометации. Не стоит забывать, что в обоих случаях в контейнере/chroot-системе должен быть «минимум» ПО: если какая-то утилита не нужна, то она должна быть вырезана. Данная мера не поможет, если была скомпрометирована основная система, а не web-сервер.

3. Удалите «дефолтный» контент. Он служит только для диагностики того, что web-сервер запустился и работает, а злоумышленнику он поможет узнать, какое ПО используется.

4. Уменьшите информацию, возвращаемую сервером.

5. Составьте список модулей, которые вам действительно необходимы, остальные же требуется удалить. Например, если ваш сервис не подразумевает управление файлами для клиентов, смело комментируйте нужные строки с модулем WebDAV в файле конфигурации. Другой пример — autoindex, позволяющий автоматически создать структуру директорий. Рекомендуется делать это вручную, оставив только необходимые файлы и папки.

6. Отключайте ненужные опции для директорий. В директории нет исполняемого контента? Отключайте ExecCGI. Не требуется FollowSymlinks? Смело удаляйте. А если опция все же требуется, смотрите на SymLinksIfOwnerMatch.

7. Настройте фильтры для файлов. Здесь каждая настройка уникальна, суть её сводится к тому, чтобы пользователь мог получать доступ только к тем файлам, которые ему необходимы. Таким образом, можно заблокировать выполнение PHP в различных директориях, доступ к служебным папкам и прочее.

8. Внимательно проверяйте CGI. У CGI довольно богатая история, связанная с различными инцидентами безопасности. И даже несмотря на то, что сейчас он считается относительно безопасным, рекомендуется удалять скрипты, которые вам не требуются и которые могут привести к неожиданным последствиям.

9. Отключите неиспользуемые HTTP-методы. Trace, который часто используется при дебаге, в продуктивной среде может привести к получению cookie сторонним лицом, а выключить его зачастую забывают.

10. Отключайте старые версии HTTP. Версии ранее 1.1 не должны поддерживаться, а на текущий момент происходит миграция на более быстрый HTTP/2. Старые и некорректные версии HTTP позволяют отследить специальные модули для web-серверов, повышающие безопасность, о которых будет сказано далее.

11. Отключите доступ к сайту по IP. Большинство обычных пользователей подключаются к сайту по доменному имени, в то время как сканеры, анализирующие в поисках уязвимого софта, «идут» по IP-адресам.

12. Указывайте конкретный IP-адрес, на котором web-сервер должен обслуживать клиентов. Это избавит от проблем, вызванных добавлением новых интерфейсов и отсутствием либо некорректной настройкой межсетевого экрана.

13. ContentSecurityPolicy. Полезная опция, защищающая от некоторых атак, например, ряда XSS или CodeInjection. Для каждого сервиса требуется уникальная настройка, где следует указать, с каких доменов разрешено загружать различный контент, будь то скрипты сбора статистики или изображения.

14. Защитите веб-сервер от DoS/DDoS атак.

15. HTTPS/HTTP Strict Transport Security. Настройте и используйте шифрование, откажитесь от HTTP. Используйте TLS не ниже v1.2. При настройке обратите внимание на используемые алгоритмы, некоторые из них уже устарели и признаны ненадежными. Среди таких: SHA-1, RC4, DES, 3DES, AES-CBC, MD5.

16. После настройки шифрования необходимо обезопасить файлы cookie, для чего требуется включить опции secure (для передачи только по HTTPS) и httpOnly (что обеспечит защиту от XSS).

17. Проверьте, что ведётся запись журналов доступа и журналов ошибок. Это крайне важный пункт, ведь именно с помощью логов вы сможете понять, что с вашим сервером что-то не так, будь-то странные запросы, какие-то попытки атак, да и просто аномальная нагрузка.

Действия в случае инцидента. В первую очередь, необходимо понять, каким образом действовал злоумышленник. Получил ли он доступ к web-серверу в результате взлома ОС? Или же какая-то уязвимость/недоработка присутствует в самом сервере? А, может быть, уязвим код web-приложения? Во всех ситуациях алгоритм последующих действий индивидуален.

Общие шаги работы алгоритма следующие:

1. Определите уязвимую точку входа, не дайте злоумышленнику повторно взломать вашу инфраструктуру.

2. Выявите, что именно делал хакер после попадания на сервер. Может случиться так, что, закрыв «дыры» на web-сервере, мы пропустим мимо внимания ботнет, который появился на других машинах. Проверить можно при помощи журналов. Но лучше иметь какое-либо средство агрегации и мониторинга логов со всех систем, либо же использовать SOC, который позволит выявить инцидент «на лету».

3. Очистите все следы злоумышленника. Для этого неплохо бы иметь утилиты, позволяющие отследить появление/редактирование файлов. Отдельно стоит заметить, что журналы, в которых сохранилась информация о деятельности преступника, лучше сохранить, так как они могут пригодиться в дальнейшем расследовании.

В любом случае, при компрометации web-сервера, вам понадобится перевыпустить сертификат шифрования вместе с закрытым ключом, так как текущий может быть украден и использоваться в дальнейшем для просмотра зашифрованного трафика.

Список использованных источников:

1.Вострецова, Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.

2.Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. — М.: ФОРУМ: ИНФРА-М, 2021. — 432 с.

3.Кенин, А. М. Самоучитель системного администратора / А. М. Кенин, Д. Н. Колисниченко. — 5-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2019. — 608 с.: ил.

4.Смит, Родерик, В. Сетевые средства Linux.: Пер. с англ. — М.: Издательский дом «Вильяме», 2003. — 672 с.: ил.