Born2beRoot

Вступление

Этот проект призван познакомить вас с чудесным миром виртуализации. Вы создадите свою первую машину в VirtualBox (или UTM, если вы не можете использовать VirtualBox) в соответствии с конкретными инструкциями. Затем, в конце этого проекта, вы сможете настроить свою собственную операционную систему, соблюдая строгие правила.

Общие рекомендации

• Использование VirtualBox (или UTM, если вы не можете использовать VirtualBox) обязательно.

• Вам нужно только включить файл signature.txt в корень вашего репозитория. Вы должны вставить в него подпись виртуального диска вашей машины. Перейдите в раздел Подача и экспертная оценка для получения дополнительной информации.

Обязательная часть

Этот проект состоит из того, что вы настраиваете свой первый сервер, следуя определенным правилам.

Поскольку речь идет о настройке сервера, вы установите минимум услуг. По этой причине графический интерфейс не имеет смысла.

используйте здесь. Поэтому запрещено устанавливать X.org или любой другой эквивалентный графический сервер. В противном случае ваша оценка будет 0.

Вы должны выбрать в качестве операционной системы либо последнюю стабильную версию Debian (без тестирования / нестабильную), либо последнюю стабильную версию CentOS. Debian настоятельно рекомендуется, если вы новичок в системном администрировании.

Настроить CentOS довольно сложно. Следовательно, вам не нужно настроить KDump. Однако SELinux должен быть запущен при запуске, а его

конфигурация должна быть адаптирована к потребностям проекта. AppArmor для Debian также должен быть запущен при запуске.

Вы должны создать как минимум 2 зашифрованных раздела с помощью LVM. Ниже приведен пример ожидаемого разбиения:

Во время защиты вам зададут несколько вопросов о выбранная вами операционная система. Например, вы должны знать

различия между aptitude и apt, или что SELinux или AppArmor является. Короче поймите, чем пользуетесь!

Служба SSH будет работать только на порту 4242. По соображениям безопасности не должно быть возможности подключиться с использованием SSH от имени пользователя root.

Использование SSH будет проверено во время защиты путем настройки нового учетная запись. Поэтому вы должны понять, как это работает.

Вы должны настроить свою операционную систему с помощью брандмауэра UFW и, таким образом, оставить открытым только порт 4242.

Ваш брандмауэр должен быть активен при запуске виртуальной машины. Для CentOS вы должны использовать UFW вместо брандмауэра по умолчанию. Для его установки вам, вероятно, понадобится DNF.

• Имя хоста вашей виртуальной машины должно соответствовать вашему логину, оканчивающемуся на 42 (например, wil42). Вам нужно будет изменить это имя хоста во время оценки.

• Вы должны внедрить надежную политику паролей.

• Вы должны установить и настроить sudo в соответствии со строгими правилами.

• В дополнение к пользователю root должен присутствовать пользователь с вашим логином в качестве имени пользователя.

• Этот пользователь должен принадлежать к группам user42 и sudo.

Во время защиты вам нужно будет создать нового пользователя и назначить его в группу.

Чтобы настроить политику надежных паролей, вы должны соответствовать следующим требованиям:

• Срок действия вашего пароля должен истекать каждые 30 дней.

• Минимальное количество дней до изменения пароля будет установлено равным 2.

• Пользователь должен получить предупреждающее сообщение за 7 дней до истечения срока действия пароля.

• Ваш пароль должен состоять не менее чем из 10 символов. Он должен содержать заглавную букву и цифру. Кроме того, он не должен содержать более 3 одинаковых символов подряд.

Пароль не должен включать имя пользователя.

• Следующее правило не применяется к паролю root: пароль должен содержать не менее 7 символов, которые не являются частью предыдущего пароля.

• Конечно, ваш пароль root должен соответствовать этой политике.

После настройки файлов конфигурации вам нужно будет изменить все пароли учетных записей, имеющихся на виртуальной машине,

включая корневую учетную запись.

Чтобы настроить надежную конфигурацию для вашей группы sudo, вы должны соответствовать следующим требованиям:

• Аутентификация с использованием sudo должна быть ограничена 3 попытками в случае неверного пароля.

• Пользовательское сообщение по вашему выбору должно отображаться, если при использовании sudo возникает ошибка из-за неправильного пароля.

• Каждое действие, использующее sudo, должно быть заархивировано, как входные, так и выходные. Файл журнала необходимо сохранить в папке / var / log / sudo /.

• Режим телетайпа должен быть включен из соображений безопасности.

• Также по соображениям безопасности пути, которые может использовать sudo, должны быть ограничены.

Пример:

/ usr / local / sbin: / usr / local / bin: / usr / sbin: / usr / bin: / sbin: / bin: / оснастка / bin

Наконец, вам нужно создать простой скрипт с именем monitoring.sh. Его нужно разрабатывать на bash.

При запуске сервера скрипт будет отображать некоторую информацию (указанную ниже) на всех терминалах каждые 10 минут (посмотрите на стену). Баннер не является обязательным. Никакой ошибки не должно быть видно.

Ваш скрипт всегда должен отображать следующую информацию:

• Архитектура вашей операционной системы и ее версия ядра.

• Количество физических процессоров.

• Количество виртуальных процессоров.

• Текущая доступная оперативная память на вашем сервере и ее коэффициент использования в процентах.

• Текущая доступная память на вашем сервере и ее коэффициент использования в процентах.

• Текущий коэффициент использования ваших процессоров в процентах.

• Дата и время последней перезагрузки.

• Активен LVM или нет.

• Количество активных подключений.

• Количество пользователей, использующих сервер.

• IPv4-адрес вашего сервера и его MAC-адрес (Media Access Control).

• Количество команд, выполненных с помощью программы sudo.

Во время защиты вас попросят объяснить, как работает этот скрипт. Вам также придется прервать его, не изменяя его. Взгляните на cron.

Это пример ожидаемой работы сценария:

Ниже приведены две команды, которые можно использовать для проверки некоторых требований объекта:

Для CentOS:

Для Debian:

Бонусная часть

Список бонусов:

• Правильно настройте разделы, чтобы получить структуру, аналогичную приведенной ниже:

• Создайте функциональный веб-сайт WordPress со следующими услугами: lighttpd, MariaDB и PHP.

• Настройте службу по вашему выбору, которая, по вашему мнению, будет полезной (за исключением NGINX / Apache2!). Во время защиты вам придется обосновать свой выбор.

Для завершения бонусной части у вас есть возможность настроить дополнительные Сервисы. В этом случае вы можете открыть больше портов в соответствии с вашими потребностями. Конечно, правила UFW должны быть адаптированы соответствующим образом.

Бонусная часть будет оцениваться только в том случае, если обязательная часть ИДЕАЛЬНА. Идеально означает, что обязательная часть выполнена полностью и работает без сбоев. Если вы не выполнили ВСЕ обязательные требования, ваша бонусная часть вообще не будет оцениваться.

Представление и экспертная оценка

Вам нужно только включить файл signature.txt в корень вашего репозитория Git. Вы должны вставить в него подпись виртуального диска вашей машины. Чтобы получить эту подпись, вам сначала нужно открыть папку установки по умолчанию (это папка, в которой хранятся ваши виртуальные машины):

• Windows:% HOMEDRIVE %% HOMEPATH% \ VirtualBox VMs \

• Linux: ~ / виртуальные машины VirtualBox /

• MacM1: ~ / Библиотека / Контейнеры / com.utmapp.UTM / Data / Documents /

• MacOS: ~ / виртуальные машины VirtualBox /

Затем получите подпись из файла .vdi (или .qcow2 для пользователей UTM) вашей виртуальной машины в формате sha1. Ниже приведены 4 примера команд для файла centos\_serv.vdi:

• Windows: certUtil -hashfile centos\_serv.vdi sha1

• Linux: sha1sum centos\_serv.vdi

• Для Mac M1: shasum Centos.utm / Images / disk-0.qcow2

• MacOS: шасум centos\_serv.vdi

Это пример того, какой результат вы получите:

• 6e657c4619944be17df3c31faa030c25e43e40af

Обратите внимание, что подпись вашей виртуальной машины может быть изменена.

после вашей первой оценки. Чтобы решить эту проблему, вы можете продублировать свою виртуальную машину или использовать состояние сохранения.

Разумеется, ЗАПРЕЩАЕТСЯ включать вашу виртуальную машину в репозиторий Git. Во время защиты подпись файла signature.txt будет сравниваться с подписью вашей виртуальной машины. Если два из них не идентичны, ваша оценка будет 0.