**Глава 9. Защита веб-сервера.**

**1) Основные положения**

* Делаем резервные копии (желательно каждый день)
* Применяем все обновления ПО (если боимся за работоспособность текущей системы, то тестируем все обнровления на тестововй среде, которая зеркальна основной-рабочей)

**2) Контроль доступа**

**Брендмауэр (файервол)** – набор правил для вхождение в сетевое пространство, контроль трафика по протоколу, порту, источнику и назначению.

На уровне ядра за это отвечает (iptables), но есть и более высокоуровневые инструменты *firewalld и uncommicated firewall* (которые и будут тут рассмотрены).

***firewalld***

**Установка и настройка:**

* Устанавливаем: apt install firewalld
* Проверяем : firewall-cmd –state

После установки по-умолчанию firewalld будет активен и будет отклонять весь входящий трафик (за исключением SSH). Поэтому следует открыть некоторые порты, чтобы у пользователей была возможность зайти на сервер (сайт).

* Firewall-cmd --permanent --add-port=80/tcp
* Firewall-cmd--permanent --add-port=443/tcp
* Перезагрузим сессию firewall-cmd –reload
* Узнать текущие настройки: firewall-cmd –list-services

Или можно использовать другой подход – установить предопределенные значения (когда нет времени или пофиг)

* Firewall-cmd --permanent --add-service=http
* Firewall-cmd --permanent --add-service=https
* Firewall-cmd --permanent –add-service=mysql

Далее следует настроить SSH, чтобы запросы по этому протоколу могли исходить только с определенных IP-Адресов с целью предоствращения несанкционированного доступа.

1. Закрываем всем доступ: firewall-cmd –permanent –remove-service=ssh

2. Перезагружаем: firewall-cmd –reload

3. firewall-cmd –add-rich-rule=’rule family=”ipv4” source address=”192.168.x.x” port protocol=”tcp” port=”22” accept’

***UncomlicatedFirewall (uwf)***

**Установка:**

* apt install ufw

**Открываем SSH до запуска ufw:**

* uwf allow ssh

**Заупскаем ssh:**

* ufw enable

**Если произошли ошибки** (например в контейнерах LXC нет поддержки ipv6), то в файле *etc*/default/ufw следует указать IPV6=no

Чтобы **разрешить доступ по портам**:

* http: ufw allow 80
* https: ufw allow 443
* Проверяем: ufw status

Далее следует **настроить SSH,** чтобы запросы по этому протоколу могли исходить только с определенных IP-Адресов с целью предоствращения несанкционированного доступа.

* Отключаем ufw : ufw disable
* Удаляем из ufw ssh, если подключили его: ufw delete x (x-номер строки в ufw status для ssh)
* Открываем доступ: ufw allow from (ip\_addr) to any port 22
* Запускаем ufw: ufw enable
* Проверяем: ufw status

**Использование нестандартных портов (для лучшей защиты):**

Можно подправить файлы (изменить порт) : *etc/ssh/sshd\_conf , Potr xx; Затем можно заходить удаленно: ssh -pxx* [*user@ip\_addr*](mailto:user@ip_addr)

*Можно настроить ufw: ufw allow xxxxx/tcp (xxxxx:yyyyy/tcp – для диапазона)*

***Напоминание :***

*Порты 1-1023: общеизвестные порты (для http, ssh…)*

*Порты 1024-49151: для компаний (MySQL-3306, RADIUS – 1812)*

***Порты 49152-65535: для частного пользования (их и надо выбирать)***

***3) Шифрование данных при передаче.***

*Чекай Let’s Encrypt.*

***4) Усиление процесса Аутентификации.***

***Основные действия:***

**Следует избегать входа на серверы от ROOT пользователя:**

* Прописываем в /*etc*/ssh/sshd\_conf: PermitRootLоgin no

**Использовать доступ SSH по ключам, а не через пароли.**

* Принудительно отлючить пароли: /*etc*/ssh/sshd\_conf: PasswordAuthentication no

После изменений перезагружаем ssh:

* systemctl restart sshd

Для промышленного уровня защиты следует включать SELinux.

**5) SELinux и группы.**

Разработчики при тестировани программ могут столкнуться с проблемой доступа к файлам. Зачастую, может отсутствовать доступ на запись. Чтобы на время разработки устранить эту проблему, они могут установить себе разрешения (777), что означает – общий доступ. По заврешении работы и переносе на работающую производственную среду можно забыть про то, что права были изменены и тогда все пользователи будут иметь возможность совершать над файлами любые действия. Так обычно и происходит утечка данных.

После установки SELinux применяется обязательное управление доступом(mondatary access control, MAC) к объектам файловой системы не зависимо от владельца объекта. Так, накладываются общесистемные ограничения на то, что может делать пользователь, предотвращая опасные действия. Так, если бы разработчики попытались бы применить права (777), то система отказала бы им в доступе. Тогда для решения проблемы доступа следует создавать группы и добавлять в них учетные записи.

У SELinux бывают сложные взаимоотношения с приложениями… Сбои т.к приложения создаются как в окальном, так и в глобальном пространстве пользователей

**5.1 Установка и активация**

* apt install setools policycoreutils selinux
* Перезагружаем linux
* Проверяем текущее состяние: sestatus
* Может понадобиться выполнить команду selinux-activate (для включекния настроек SELinux в процессе загрузки)
* Затем опять перезагружаем LINUX

Контроль поведения : /*etc*/selinux/. Файл содержит 2 настройки : Сотсояние и Тип SELinux.

1. Состояние : disable | enforcing | permissive = откл | по политике безоп | запись в журнал( полезно для тестирования)
2. Тип политики: targeted | minimum | mls

Так же можно устанавливать состояние SELinux из командной строки, используя setenforce:

* setenforce 0 – установка в разрешающее состояние (регистрация нарушений)
* setenforce 1 – состояние enforcing

**5.2. Применение политики**

Если применить команду ls -Z /*var*/www/html/ то можно увидеть сведения о файле.

* -rw-r—r--. root root unconfined\_u:object\_r:httpd\_sys\_content\_t:s0 index.html

Чтобы изменить состояние контекста unconfined\_u:object\_r:httpd\_sys\_content\_t:s0, можно использовать команду chcon -t, rкоторая заменить тип httpd на сявязный с Samba:

* chcon -t samba\_share\_t /var/www/html/index.html

До изменения команда (wget localhost) позволила бы сохранить файл index.html в домашний каталог, после применения chcon будет выведена ошибка отказа в доступе 403.

**5.3. Системные группы**

Для примера можо создать файл и применить к нему права (770), затем присвоить файлу группу и включить в группу другого пользователя, кто не владеет этим файлом, тогда он сможт пользоваться им:

1. nano data.txt
2. chmod 770 data.txt
3. groupadd new\_test\_group - создаем новую группу
4. chown user:new\_test\_group data.txt - присваиваем группу файлу
5. usermod -aG new\_test\_group new\_user -добавляем в группу нового пользователя
6. Теперь new\_user модет использовать файл data.txt (до этого не мог).

В файле *etc*/group/ можно посмотерть соотвествия пользователь <=> группа

**5.4 Изоляция процессов в контейнерах.**

Для безопасности нужно применять виртуализация или применять физическое разделение для отдельных сервисов. При виртуализации такую архитектуру называют микросервисами. Это поможет запускать несколько контейнеров: для Apache, БД, Медиафайлов.

В итоге мы получим большую производителность и безопасность.

**5.5 Сканирование на анличие опасных идетнификаторов**

Пользователи могут временно получать права root из под sudo, но это не значит, что они становятся root. Только один-настоящий root имеет все права.

Идентификатор root и его идентификатор группы всегда равны 0!

Это можно посмотреть в файле /etc/passwd, который содержит запись о каждой учетной записи, которые существуют в данный момент.

Ни у кого, кроме root идентификатора или группы 0 быть не должно!

Проверка:

* awk -F: ‘($3 == “0”) {print}’ /*etc/passwd (Ответ: root:x:0:0:root:/root:/bin/bash)*

**6) Аудит системных ресурсов**

**6.1 Сканирвание на наличие открытых портов.**

Получение информации об открытых портах:

* netstat -npl (n- вывод портов/адресов в числовом формате, l – только прослушивающие сокеты, -p – идентификатор процесса прослушивающей программы)
* ss -o state established (замена netstat)

**6.2 Сканироване на педмет активных служб**

Получение снимка служб под управлением systemd, включенных на компьютере.

* Systemctl list-unit-files --type=service –state=enabled

Если нужно что-то остновить:

* systemctl stop <name>
* systemctl disable <name>

6.3 Поиск установленного ПО

Проверка установленных программ:

* dpkg –list || yum list installed

Удаление пакетов:\

* apt-get remove <name> || yum remove <name>