Apache基线检查

一、确保对OS根目录禁用覆盖

当AllowOverride设置为None时，.htaccess文件不具有访问上下文权限。当此指令设置为All时，任何具有.htaccess .htaccess文件中允许使用上下文。开启时增加了更改或查看配置的风险。

操作方法

找到配置文件路径。 通过vim path（path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径） 在配置文件中 找到以`<Directory />`开头的配置项，按如下配置

```
<Directory />
  ...
  AllowOverride None
   ...
</Directory>
```

二、确保默认情况下拒绝访问OS根目录

通过禁止访问OS根目录，限制直接访问服务器内部文件的行为 使得运行web的服务器更加安全

操作方法

找到配置文件路径。 通过vim path（path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径）编辑配置文件 找到以`<Directory />`开头的配置项，按如下配置

```
<Directory />
  ...
  Require all denied
   ...
</Directory>
```

如没有，请增加

三、确保禁用http跟踪方法

TRACE方法不需要，并且很容易受到滥用，因此应该将其禁用。

操作方法

1.`vim path`（path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径）

```
  2.找到选项`TraceEnable`将其值设置为`off` 如没有请增加
```

四、确保Web根目录的选项受到限制 禁止 Apache 列表显示文件

Web根目录或文档根目录级别的Options指令应限于所需的最少选项。

操作方法

1.使用 vim path (path为主配置文件的绝对路径，如果您的主配置文件中包含`include`，则为您的子配置文件路径)

2.找到`<Directory "apache网页存放路径">`(默认网页存放路径`/usr/local/apache2`或`/var/www/html`，自定义路径请自行查找)

```
<Directory "apache存放网页路径">
Options Indexes FollowSymLinks
</Directory>
```

将其设置为

```
<Directory "apache存放网页路径">
    Options None
</Directory>
```

如配置虚拟主机，请确保虚拟主机配置项中含有Options None 如没有，请增加

```
<Directory "apache存放网页路径">
Options None
</Directory>
```

五、配置专门用户账号和组用于运行 Apache

为服务器应用程序创建一个唯一的，没有特权的用户和组。

操作方法

根据需要，为Apache服务创建用户及用户组。如果没有设置用户和组，则新建用户，并在Apache配置文件中进行指定。

（1） 创建Apache用户和Apache用户组：

```
groupadd apache

useradd apache –g apache
```

（2）将修改Apache配置文件httpd.conf中的 User、Group 两行参数设置下面的样子**(yum安装的httpd配置文件所在位置为 /etc/httpd/conf/httpd.conf)**

```
User apache
Group apache
```

六、确保apache用户帐户具有无效的shell

apache帐户不得用作常规登录帐户，因此应为其分配一个无效或nologin Shell，以确保无法用于登录

操作方法

为确保apache用户帐户具有无效的shell,使用命令`chsh -s /sbin/nologin <apache_username>`修改apache账户的shell（可以使用命令`ps -ef | egrep "apache2|httpd"`查看<apache_username>）

七、确保已锁定apache用户帐户

Apache运行下的用户帐户不应该具有有效的密码，应该被锁住。

操作方法

使用如下passwd命令锁定apache帐户：

`passwd -l <apache_username>`

<apache_username>为apache的启动账户（可以使用命令`ps -ef | egrep "apache2|httpd"`查看<apache_username>）

八、授权设置， 严格控制Apache服务主目录的访问权限，非超级用户不能修改该目录中的内容

Apache的主目录对应于 配置文件 httpd.conf 中的 Server Root 控制项 ， 该目录属主应为root用户，其它用户不能修改该目录中的文件。默认设置一般即符合要求。

操作方法

严格设置配置文件和日志文件的权限，防止未授权访问。

```
chmod 600 /etc/httpd/conf/httpd.conf    #执行该命令设置配置文件为属主可读写，其他用户无读写权限。
chmod 644 /var/log/httpd/*.log  #执行该命令设置日志文件为属主可读写，其他用户拥有只读权限。
chmod 644 /etc/httpd/logs/*.log

注：/etc/httpd/conf/httpd.conf 配置文件的默认权限是 644，可根据需要修改权限为600。
   /var/log/httpd/*.log 日志文件的默认权限为 644，默认设置即符合要求。
```

九、确保超时设置正确

DoS的一种常用技术，常见的是发起与服务器的连接。 通过减少旧连接超时后，服务器可以更快，更多地释放资源反应灵敏。 通过提高服务器效率，它将对DoS攻击的抵御性更好

操作方法

1.使用vim编辑器对配置文件进行编辑 `vim path`(path为apache配置文件路径，或查找include文件或自定义安装请自行查找)

2.找到`Timeout`将其设置为`Timeout 10`如没有，请增加

十、确保keepAlive已启用

允许每个客户端重用TCP连接，减少了系统和网络请求所需的资源。 这种效率提高可以提高服务器对DoS攻击的抵御性

操作方法

1.使用vim编辑器对配置文件进行编辑 `vim path` （path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径）

2.找到`KeepAlive`将其设置为 `KeepAlive On` 如没有，请增加该项

十一、确保正确设置KeepAliveTimeout

KeepAliveTimeout指令指定Apache等待等待的秒数在关闭保持活动的连接之前的后续请求。减少Apache HTTP服务器保留未使用资源的秒数分配的资源将增加服务其他请求的资源的可用性。 这个效率收益可能会提高服务器抵御DoS攻击的能力。

操作方法

1.使用vim编辑器对配置文件进行编辑 `vim path` （path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径）

2.找到`KeepAliveTimeout`将其设置为 `KeepAliveTimeout 15` 如没有，请增加

十二、确保MaxKeepAliveRequests设置为适当值

MaxKeepAliveRequests指令限制每个连接允许的请求数，打开KeepAlive时，如果将其设置为0，则将允许无限制的请求。 推荐将MaxKeepAliveRequests指令设置为100，以防患DoS攻击

操作方法

1.使用vim编辑器对配置文件进行编辑 `vim path` （path为主配置文件的绝对路径，如果您的主配置文件中包含`include <path>`，则为您的子配置文件路径）

2.找到`MaxKeepAliveRequests`将其设置为 `MaxKeepAliveRequests 100` 如没有，请增加

十三、隐藏Apache的版本号及其它敏感信息

修改 httpd.conf 配置文件，找到下列两项并将他们改为如下的样式，如果配置文件中不存在下列两项，那么直接在文件末尾添加下方的内容即可。

```
ServerSignature Off
ServerTokens Prod
```