## 安全基线脚本使用指导V1.1

### 说明

安全基线脚本，本地部份使用python3编写，远程部分使用bash shell编写。

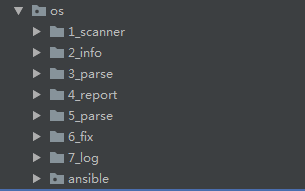
安全基线脚本，当前具有合规巡检、生成报告、生成修复脚本等几项功能。

安全基线脚本，当前共实现OS、Nginx、MySQL和Tomcat四项。各项目录结构和操作过程都类似，下文只以OS为例。

因为代码中使用f-Strings所以需要python3.6及以上版本，另外需要安装lxml、requests-file、requests-html三个依赖库：pip install lxml requests-file requests-html

### 二、目录结构

以操作系统为例，整体目录结构如下



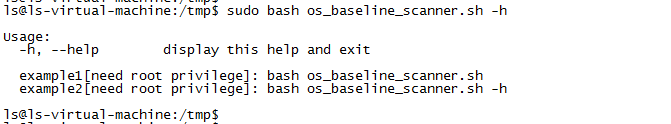
### 三、执行流程

#### 3.1 扫描

将1\_scanner中的os\_baseline\_scanner.sh传到目标主机的任意目录，以root用户或sudo使用bash执行：

sudo bash os\_baseline\_scanner.sh

可使用-h参数查看执行帮助：



#### 3.2 获取扫描结果

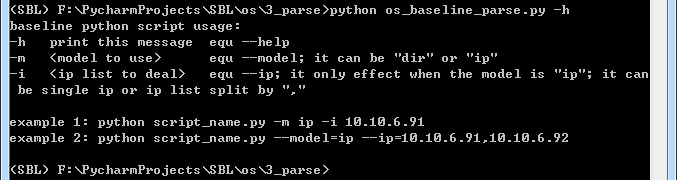
上一步扫描完成后，会在/tmp目录下生成ip\_os\_info.xml格式的扫描报告，需要将其取回放到2\_info目录中

#### 3.3 生成扫描报告

使用python3执行3\_parse目录下的os\_baseline\_parse.py，该文件默认会解析2\_info目录下的所有ip\_os\_info.xml格式的文件，并在4\_report目录下生成相应的ip\_os\_report.html；可使用-m参数指定为ip模式并通过-i参数指出仅要处理的ip：

python os\_baseline\_parse.py -m ip -i 10.10.6.91

可使用-h参数查看执行帮助：



#### 3.4 查看扫描报告

使用浏览器打开上一步生成的html文件即可。

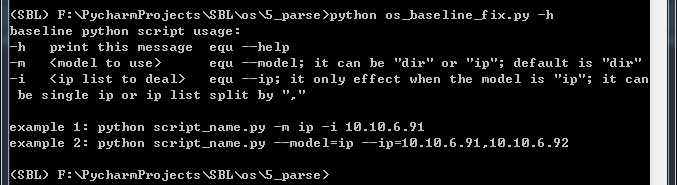
另外注意4\_report目录下的bootstrap和highcharts两个文件夹下是html报告用到的js和css，一是不要将这两个文件删除，二是想将报告移到别处查看时应同时拷贝这两个文件。

#### 3.5 生成修复脚本

使用python3执行5\_parse目录下的os\_baseline\_fix.py，该文件默认会解析4\_report目录下的所有ip\_os\_report.html格式的文件，并在6\_fix目录下生成相应的ip\_os\_fix.sh；可使用-m参数指定为ip模式并通过-i参数指出仅要处理的ip：

python os\_baseline\_fix.py -m ip -i 10.10.6.91

可使用-h参数查看执行帮助：

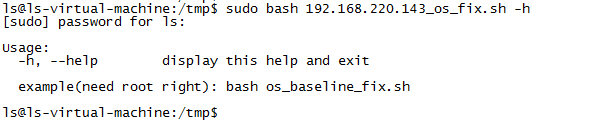


#### 3.6 执行修复

将6\_fix下生成的ip\_os\_fix.sh传到目标主机的任意目录，以root用户或sudo使用bash执行：

sudo bash ip\_os\_fix.sh

可使用-h参数查看执行帮助：



#### 3.7 取回日志

Ip\_os\_fix.sh执行完后会在/tmp目录下生成ip\_nginx\_fix.log格式的日志文件，该文件主要记录了修复时执行的命令，如果需要可以将其取回放到7\_log目录下。